Možnosti pro vícenásobný elektronický podpis, jeho vytváření a ověřování

Dokument projektu YA512006005

„Vícenásobný elektronický podpis“

MathAn Praha, s.r.o.

Obsah

1. Úvod

Schválením zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu – ZoEP)[1] se v ČR otevřela široká oblast pro používání elektronického podpisu. V současné době již tři poskytovatelé certifikačních služeb vydávají kvalifikované certifikáty dle vyhlášky č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb.

Legislativa upravuje tu základní situaci, kdy jedna zpráva je podepsána jedním podpisem, učiněným jednou podepisující stranou. Zároveň však předem nevylučuje možnost podpisů učiněných několika stranami.

To je právě oblast vícenásobného elektronického podpisu (v anglické literatuře *Multi-Signature* nebo *multisignature*). Jde o oblast kryptologie, která je značně široká a poměrně složitá, nemá zcela ostře vymezené hranice, a v současné době prochází bouřlivým vývojem. Již nyní se rýsují naprosto zásadní aplikace, například pro elektronické volby.

Tato studie je výsledkem řešení projektu výzkumu a vývoje „Vícenásobný elektronický podpis“. Hlavním cílem tohoto projektu je vytvoření softwarové aplikace realizující některý, vhodně zvolený, přístup k vícenásobnému elektronickému podpisu. Tomuto cíli je podřízeno i zaměření studie. Ta si klade za cíl popsat známé přístupy k vícenásobnému elektronickému podpisu, a to spíše do šíře nežli do hloubky. U jednotlivých přístupů je cílem ukázat možnosti jejich využití. Nakonec je třeba provést výběr jednoho přístupu, na jehož základě vznikne softwarová aplikace, která bude podporovat základní činnosti vytvoření a ověření vícenásobného elektronického podpisu. Přitom se budeme zaměřovat na ty přístupy, které mají oporu v ZoEP.

Zároveň musíme zmínit i to, co cílem této studie není. Nelze od ní očekávat vyčerpávající popis a rozbor všech jednotlivých přístupů – ten by v daných časových a kapacitních mezích projektu nebyl možný, a z hlediska cílů projektu ani účelný. Budeme též věnovat relativně menší pozornost přístupům, u kterých je jasné, že nemají oporu v ZoEP. Některé takové přístupy jsou motivovány spíše zvědavostí kryptologů, jak by bylo možné některé problémy řešit, aniž by byli vedeni požadavky z praxe – což je ovšem postup v oblasti teoretického výzkumu plně oprávněný.

Kritérium souladu se ZoEP pro nás bude naprosto primárním. Z hlediska způsobu konstrukce v zásadě existují dvě základní skupiny přístupů k vícenásobnému elektronickému podpisu:

a) Přístupy, které jako základní prvek používají elektronický podpis tak, jak je definován v ZoEP, a vícenásobný podpis realizují skládáním těchto podpisů. U přístupů z této skupiny je předmětem každého dílčího podpisu buď primární zpráva, nebo objekt, který obsahuje výtah z této primární zprávy.

1 Zákon o elektronickém podpisu byl následně modifikován změnami provedenými zákonem č. 226/2002 Sb., zákonem č. 517/2002 Sb. a zákonem č. 440/2004 Sb.

b) Jiné přístupy. Tato řešení obecně nemají oporu v ZoEP, například proto, že vyžadují speciálně generované klíče. Motivací pro hledání těchto řešení je jednak snaha redukovat výpočetní složitost vytvoření a/nebo ověření vícenásobného podpisu oproti prostému skládání běžných podpisů, jednak snaha získat některé specifické aspekty chování takových přístupů.

V dalších kapitolách popíšeme řešení z obou skupin.

Konečně není ani cílem této studie navrhovat úpravy stávající legislativy tak, aby se některé další přístupy octly s ní v souladu.

Budeme popisovat všechny součásti procesu elektronického podpisu: generování klíčů, vlastní podepsání zprávy a ověřování podpisů.

Nástin problematiky různých druhů elektronických podpisů, souvisejících s vícenásobným elektronickým podpisem, provedeme dle následujícího členění:

a) Problematika šifrování a klasický elektronický podpis

b) Speciální druhy jednonásobných elektronických podpisů

- Elektronický podpis bez zviditelnění textu podepisující osoby (tzv. *blind signature*)
- Elektronický podpis, u kterého podpisovatel může zjistit podvrh padělatele s neomezenou výpočetní silou (tzv. *fail-stop signature*)
- Tzv. *forward-secure* elektronický podpis
- Tzv. *Proxy elektronický podpis* (podpis s plnou mocí – zplnomocněný podpis)
- Elektronický podpis šifrovaného textu (tzv. *signcryption*)
- Nezpochybnitelný elektronický podpis (tzv. *undeniable signature*)

c) Vícenásobný elektronický podpis

- Skupinový elektronický podpis (tzv. *group signature*)
- Skupinově-orientovaný elektronický podpis (tzv. *group-oriented signature*), včetně speciálních případů kruhového podpisu (tzv. *ring signature*) a hromadného podpisu (tzv. *aggregate signature*)
- Threshold signatures

Závěrem studie pak provedeme doporučení optimálního přístupu pro realizaci v softwarové aplikaci, která bude hlavním výsledkem projektu.

Součástí této studie je i obsáhlý přehled literatury, který je řazen dle tohoto členění a v rámci jednotlivého druhu podpisu pak chronologicky podle roků publikování prací. Tato literatura je u některých kapitol rozšířena o části či citace vztahující se k problematice v kapitole uvedené. Někdy jsou citace uvedeny v textu s případným internetovým odkazem.

2. Šifrování a klasický elektronický podpis

V této kompilační kapitole provedeme nástin základních pojmů problematiky šifrování a klasického elektronického podpisu, které jsou nezbytné pro porozumění další analýzy. V samostatné příloze to provedeme způsobem nevyžadujícím hlubší základy diskrétní matematiky aplikované v kryptologii. Pro podrobnější přehled odkazujeme na učebnici A.J.Menezes, P.C.van Oorschot, S.A.Vanstone „Handbook of Applied Cryptography“, CRC Press, Inc., ISBN 0-8493-8523-7 (1997) a články v informačním sešitu Crypto-World.

2.1 Šifrování

Zašifrováním dat může být zpráva s otevřeným textem přeměněna tak, že vypadá jako náhodný shluk znaků. Bez tajného klíče je velmi obtížné převést tato zakódovaná data zpět do původní zprávy. V tomto dokumentu se pod termínem zpráva rozumí jakákoliv část dat.

Tato zpráva může obsahovat ASCII text, databázový soubor nebo jakákoliv jiná data, která chcete bezpečně uložit nebo přenést. *Plaintext* (otevřený text) se používá k označení dat, která nejsou zašifrována, zatímco šifrovaná data se označují jako *ciphertext* (šifrovaný text).

Jakmile byla zpráva zašifrována, může být uložena na nezabezpečeném médiu nebo přenášena po nezabezpečené síti a stále zůstává tajná - chráněna. Později může být zpráva dešifrována do své původní podoby.

2.1.1 Symetrické šifry

Symetrický algoritmus je nejpoužívanějším typem algoritmu šifrování. Symetrické šifrovací algoritmy (také se jim říká šifry s tajným klíčem) používají tentýž klíč jak pro šifrování tak i pro dešifrování (při dešifrování je použita inverzní funkce). Všechny klíče zde musí zůstat utajeny, aby bylo zajištěno, že třetí neoprávněná strana nemůže použít klíč k dešifrování tajných zpráv. Klíč má být často střídán a být dostatečně náhodný.

Různé symetrické algoritmy používají různé délky klíčů. Delší klíč obvykle znamená větší bezpečnost algoritmu.

2.1.2 Asymetrické šifry

Asymetrické šifry používají jiný klíč pro šifrování (tzv. *veřejný klíč*) a jiný klíč pro dešifrování (tzv. *soukromý klíč*). Veřejné klíče však nemusí být utajovány. Systémy s veřejným klíčem jsou významně pomalejší než symetrické šifry. Z hlediska svých unikátních vlastností tvoří však jejich vhodný doplněk. Jsou používány zejména k

přenosu klíčů, k vytváření digitálních (elektronických) podpisů (autentizace zpráv), jsou vhodným prostředkem při konstruování řady kryptografických protokolů. Autentizace pomocí systémů s veřejným klíčem vede k zavedení nepopiratelnosti.

Nejznámější asymetrické systémy jsou RSA (jednoznačně nejpoužívanější systém), DSS (diskrétní logaritmus) a ECC (algoritmy založené na vlastnostech vhodných eliptických křivek).

Nevýhodou systémů s veřejným klíčem je jejich pomalost (uvádí se, že asymetrické šifry jsou obvykle 1000-krát pomalejší než šifry symetrické). Proto při řešení konkrétního systému ochrany dat opírajícího se o kryptografické algoritmy je nejlépe kombinovat oba základní přístupy, tj. symetrické a asymetrické algoritmy. Je přitom využívána rychlost symetrických algoritmů na jedné straně a flexibilita nesymetrických šifer na straně druhé.

2.2 Hashovací funkce

Výstupem hashovací funkce je takzvaný *otisk zprávy* (*message digest*, hash). Vstupem hashovací funkce může být libovolná zpráva (prakticky libovolně dlouhá, až na omezení daná konkrétním algoritmem), na výstupu obdržíme její otisk, který má pevnou délku (např. 128 nebo 160 bitů). Pokud bychom ve zprávě změnili byť i jediné písmenko, dostaneme na výstupu úplně jiný otisk.

Algoritmy hashovacích funkcí jsou známé, a kdokoli si proto může z jakékoliv zprávy takový otisk udělat. Navíc platí, že je výpočetně velice obtížné vytvořit k libovolné zprávě jinou zprávu, která má stejný otisk. (Asi tak stejně obtížné jako rozšifrovat zprávu bez klíče).

2.3 Postup při generování a ověření podpisu

Digitální podpisy umožňují uživatelům ověřit, zda dokument přichází od držitele soukromého klíče, a zda nebyl obsah dokumentu změněn po provedení podpisu. (Dokument může, ale nemusí být zašifrován. Běžnou procedurou je podepsat dokument před šifrováním - víte totiž, co podepisujete. Navíc zákon vyžaduje, aby podepisující osoba měla možnost se seznámit s obsahem).

Digitální podpis je hash otevřeného dokumentu, šifrovaný soukromým klíčem pro podpisy. Ověření digitálního podpisu se provádí dešifrováním podpisu pomocí veřejného klíče pro podpisy a porovnáním výsledku s hashem původního dokumentu.

2.4 Certifikáty a certifikační autority

Certifikáty jsou v podstatě podepsané dokumenty, které zajišťují soulad veřejných klíčů s dalšími informacemi, jako je jméno nebo např. adresa elektronické pošty. Certifikáty jsou vydávány a podepsány tzv. certifikačními autoritami (*certificate authority* - CA).

Jedná se o třetí stranu, požívající všeobecnou důvěru, která ověřuje souhlas veřejných klíčů například s identitou, jménem elektronické pošty nebo přístupovými právy. Certifikační autority se podobají státním notářům.

Výhodou certifikátů a CA je to, že pokud dva lidé věří stejné CA, potom výměnou certifikátů, podepsaných CA, si mohou zjistit navzájem veřejné klíče. Tyto klíče potom mohou bezpečně používat k šifrování vyměňovaných dat a k ověřování podpisů na dokumentech.

Kromě hierarchické struktury certifikačních autorit založených na standardu ITU-T X.509 existuje i distribuovaný systém PGP (*Pretty Good Privacy*), který je ovšem vhodný spíše pro homogenní skupiny osob, proto se jím nijak nebudeme zabývat.

Další informace o této šifrování, elektronických podpisech, certifikátech a certifikačních autoritách jsou všeobecně dostupné, jsou dobře známy a lze je najít např. na webu pomocí odkazů

http://crypto-world.info/casop6/crypto11_04.pdf

http://crypto-world.info/casop7/crypto01_05.pdf

http://crypto-world.info/casop7/crypto04_05.pdf

3. Formáty elektronického podpisu

Standardizací formátů elektronického podpisu se zabývá několik norem. Nejrozšířenějším způsobem uložení podepsaného dokumentu je binární formát CMS (*Cryptographic Message Syntax* – syntaxe šifrované zprávy). Dalším formátem, jehož použití je v poslední době stále rozšířenější, je formát XML-Signature (XMLDsig), který, jak už jeho název napovídá, je založen na formátu XML. V následujících oddílech přiblížíme tyto dva formáty podpisu, přičemž se zaměříme na jejich podporu vícenásobných podpisů, a dále porovnáme jejich výhody a nevýhody.

3.1.1 CMS

Formát CMS definuje RFC 3852 (http://www.ietf.org/rfc/rfc3852.txt), Tento formát byl odvozen ze standardu PKCS#7 verze 1.5 v roce 1998.

V tomto textu pouze naznačíme strukturu CMS, bližší podrobnosti lze nalézt na výše uvedené webové adrese. K definici formátu CMS je použita syntaxe ASN.1, v níž jsou postupně definovány struktury a údaje, z nichž se CMS skládá. Hlavní struktura `ContentInfo` obsahuje informaci o typu obsahu a dále vlastní obsah.

```
ContentInfo ::= SEQUENCE {
        contentType ContentType,
        content [0] EXPLICIT ANY DEFINED BY contentType }
```

Možné typy obsahu jsou následující:

- *data* otevřený formát dat
- *signed-data* podepsaná data
- *enveloped-data* data šifrovaná symetrickým klíčem, který je šifrován asymetrickým klíčem
- *digested-data* data a jejich hash
- *encrypted-data* zašifrovaná data, neobsahuje žádné klíče ani dodatečné informace
- *authenticated-data* zašifrovaná data, zašifrovaný klíč (nebo více klíčů) a zašifrovaný hash dat

Našich potřeb se týká typ `signed-data`, který v sobě dále obsahuje popis algoritmů, kterým se získá hash, zapouzdřený vlastní obsah dokumentu, certifikáty, seznamy zneplatněných certifikátů (CRL) a informace o podpisech.

```
SignedData ::= SEQUENCE {
        version CMSVersion,
        digestAlgorithms DigestAlgorithmIdentifiers,
        encapContentInfo EncapsulatedContentInfo,
```

```
        certificates [0] IMPLICIT CertificateSet OPTIONAL,
        crls [1] IMPLICIT RevocationInfoChoices OPTIONAL,
        signerInfos SignerInfos }

SignerInfos ::= SET OF SignerInfo
```

Dokument může obsahovat libovolné množství nezávislých podpisů. Formát podpisu popisuje struktura `SignerInfo`, která obsahuje identifikaci podpisovatele, algoritmus výpočtu hashe, podepsané atributy, algoritmus podpisu, hodnotu podpisu a nepodepsané atributy.

```
SignerInfo ::= SEQUENCE {
        version CMSVersion,
        sid SignerIdentifier,
        digestAlgorithm DigestAlgorithmIdentifier,
        signedAttrs [0] IMPLICIT SignedAttributes OPTIONAL,
        signatureAlgorithm SignatureAlgorithmIdentifier,
        signature SignatureValue,
        unsignedAttrs [1] IMPLICIT UnsignedAttributes OPTIONAL }
```

Jako nepodepsaný atribut může být uveden atribut `countersignature`, který je typu `SignerInfo` a obsahuje podpis podpisu dokumentu. Atribut `countersignature` v sobě může obsahovat vnořený jako nepodepsaný atribut další `countersignature`, a takto mohou být podpisy dále zřetězeny.

Popis formátu CMS rozšiřuje specifikace *ETSI TS 101 733*, která popisuje rozvinuté formáty elektronického podpisu založené na CMS (*CAdES - CMS Advenced Electronic Signatures*) . V této specifikaci jsou zavedeny jednotlivé typy podpisu dle účelu užití a jsou zde popsány atributy, které tyto typy musí obsahovat.

3.1.2 XML-Signature

Formát XML Signature (XMLDsig, XS podpis) vyvíjí společně konsorcium W3C (http://www.w3.org/TR/xmldsig-core/) a organizace IETF (RFC 3275 - http://www.ietf.org/rfc/rfc3275.txt). Norma XML Signature definuje schéma pro uložení výsledku operace digitálního podpisu aplikované na libovolná (ale nejčastěji XML) data. Stejně tak jako další digitální podpisy (např. CMS), tak i XML Signature poskytuje autentizaci, kontrolu integrity dat a podporu pro nepopiratelnost (non-repudiation).

XML-Signature definuje tři typy podpisu dle umístění podepisovaných dat:

- *enveloped* – podpis je elementem XML dokumentu, který je podepisován (samozřejmě je podepisován bez elementu podpisu)
- *enveloping* – podpisovaná data jsou součástí podpisu
- *detached* – podpis a podepisovaný obsah jsou navzájem nezávislé, mohou to být sousední elementy v XML dokumentu (podepisovaný obsah určuje transformace), nebo může být podepisovaný dokument určen URI odkazem.

Struktura elementu podpisu je následující (pro lepší přehlednost byly některé části struktury vypuštěny):

```
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">

    <SignedInfo> <!-- povinný element -->
       <!-- informace o způsobu výpočtu podpisu -->
       <CanonicalizationMethod
           Algorithm="algoritmus kanonizace
           elementu SignedInfo"/> <!-- povinný element -->
       <SignatureMethod
        Algorithm="algoritmus podpisu"/> <!-- povinný element -->

       <Reference URI=""> <!-- 1 až libovolný počet výskytů -->
          <!-- obsahuje odkaz na podpisovaná data -->
          <Transforms>
             <!-- popis transformací jejichž provedením
                  se získá podpisovaný objekt -->
             <Transform Algorithm="..."/>
          </Transforms>
          <DigestMethod Algorithm="algoritmus výpočtu hashe"/>
          <DigestValue><!-- hodnota hashe --></DigestValue>
       </Reference>

    </SignedInfo>

    <SignatureValue> <!-- povinný element -->
      <!-- hodnota digitálního podpisu -->
    </SignatureValue>

    <KeyInfo> <!-- nepovinný element -->
      <!-- certifikáty, veřejné klíče či jiné informace k
           validaci podpisu -->
    </KeyInfo>

    <Object> <!-- 0 až libovolný počet výskytů -->
       <!-- zde může být cokoliv, např. podpisovaná data
            enveloping podpisu nebo také dodatečné
            podepsané i nepodepsané atributy -->
    </Object>

</Signature>
```

XML dokument může obsahovat libovolný počet elementů `Signature`, tedy může obsahovat libovolné množství nezávislých podpisů. Jak je vidět z uvedené ukázky struktury, jeden podpis může být vytvořen nad více dokumenty či nezávislými částmi dokumentu (vícenásobný výskyt elementu `Reference`), což otevírá široký prostor možností, co vše a kým vším je možné podepsat.

Základní specifikaci XML-Signature rozšiřuje dále specifikace *ETSI TS 101 903* popisující *XAdES* (*XML Advanced Electronic Signatures*). Tato specifikace je pro XML-Signature obdobným rozšířením jako specifikace CadES pro CMS formát.

XAdES definuje tyto typy XML podpisu:

- *XadES-BES* základní elektronický podpis
- *XadES-EPES* elektronický podpis s explicitní politikou
- *XadES-T* elektronický podpis s časem
- *XadES-C* elektronický podpis s úplnými údaji k validaci

Dále jsou v informativním dodatku zmíněny tyto typy:

- *XadES-X* rozšířený elektronický podpis s časem
- *XadES-X-L* rozšířený dlouhý elektronický podpis s časem
- *XadES-A* archivační elektronický podpis

Dokument určuje, které podepsané a nepodepsané atributy musí nebo mohou jednotlivé typy podpisu obsahovat a definuje strukturu elementu `Object`, jehož potomky tyto dodatečné atributy jsou. Takto vypadají atributy základního elektronického podpisu *XadES-BES*:

```
<ds:Object>
  <QualifyingProperties>

    <SignedProperties>

      <SignedSignatureProperties>
        (SigningTime)?
        (SigningCertificate)?
        (SignatureProductionPlace)?
        (SignerRole)?
      </SignedSignatureProperties>

      <SignedDataObjectProperties>
        (DataObjectFormat)*
        (CommitmentTypeIndication)*
        (AllDataObjectsTimeStamp)*
        (IndividualDataObjectsTimeStamp)*
      </SignedDataObjectProperties>

    </SignedProperties>

    <UnsignedProperties>

      <UnsignedSignatureProperties>
        (CounterSignature)*
      </UnsignedSignatureProperties>

    </UnsignedProperties>

  </QualifyingProperties>
```

```
</ds:Object>
```

Zřetězené podpisy - countersignature

Pro zřetězené podpisy (podpis podpisu - countersignature) je zde zaveden nepodepsaný atribut `CounterSignature`, který má stejný význam jako atribut `countersignature` v CMS podpisu. Element `CounterSignature` obsahuje element `Signature`, který podpisuje element `SignatureValue` z podpisovaného podpisu.

Druhou standardizovanou možností vytvoření zřetězeného podpisu, již XadES zavádí, je v podpisu uvést element `Reference` odkazující se na podpisovaný podpis. Že se jedná o countersignature určuje přítomnost následujícího atributu:

```
Type="http://uri.etsi.org/01903#CountersignedSignature"
```

Podpis vybrané části dokumentu

Základním rysem XML podpisu je schopnost podepsat pouze část dokumentu XML, spíše než celý kompletní dokument. To je velmi významné, když máme dokument,který má dlouhou historii, ve které jsou různé části dokumentu vytvořeny v různých časech a různými autory, a přitom každá má být podepsána pouze tím, kdo je pro danou část relevantní.

Tato flexibilita je důležitá pro vícenásobné podepisování, když je nutné zajistit integritu určité části XML dokumentu, zatímco jiné části dokumentu je nutné nechat otevřené pro možnost změn.

Zvídavý čtenář si jistě dovede představit řadu aplikací například při podpisu referátníku, kdy podepisující osoby v hierarchii připojí komentář k dokumentu, nebo když je uživateli doručen určitý formulář k dovyplnění (zdravotní karta, informace o studentovi atd.).

Související technologie

Pro formát XML existuje řada bezpečnostních technologií, které jsou dnes v různé fázi vývoje. Jsou to *XML Signature* (*XS*), *XML Encryption* (*XE*), *XML Key Management Specification* (*XKMS*), *Secure Assertion Markup Language* (*SAML*), *XML Access Control Markup Language* (*XACML*), *WS - security* (*Web Services Security*), *EbXML Messege Services*. Dále se jedná o *Liberty Alliance Project*.

Následující tabulka ukazuje, kdo je hlavním tvůrcem a v jaké fázi vývoje je daná technologie

XML DSIG	W3C Recommendation
XML Encryption	W3C Recommendation
WS – Security	OASIS Committee Draft
SAML	OASIS Standard
XKMS	W3C Working Draft
XACML	OASIS Standard
EbXML	OASIS Standard

3.1.3 Porovnání

Jak je vidět již z hrubého popisu struktur obou formátů podpisu, je XML syntaxe na rozdíl od CMS čitelná i při pouhém otevření v libovolném textovém editoru bez použití speciálního programu, který by ji musel dekódovat.

Další výhodou XML-Signature je jeho univerzálnější struktura, umožňující podepisovat libovolné části XML dokumentu, více dokumentů či částí dokumentu zároveň.

Také možnost se na podpisovaný dokument pouze odkazovat pomocí URL může být výhodná pro některé případy použití elektronického podpisu, například jsou-li podpisované dokumenty uloženy v nějakém standardním úložišti, není nutné při jejich podpisu tyto dokumenty nijak měnit ani duplikovat. Dále jeden podpis může pokrýt HTML data, JPG data, XML data a specifickou část XML dat, což využívají např. MS Office 2007 a OpenOffice.org ve svém řešení podpisu dokumentu (viz části 8.3 a 8.4). Ověření podpisu samozřejmě vyžaduje, aby datový objekt, na nějž se podpis odkazuje, byl přístupný.

4. Speciální druhy jednonásobných elektronických podpisů

Tyto podpisy mají vztah k vícenásobnému podepisování např. tím, že se vícenásobně podepíší různé části textu, i když jedním podpisovatelem, popřípadě tím, že k naplnění vlastností těchto podpisů je potřeba více účastníků.

Je zřejmé, že i tyto speciální podpisy lze využít k vícenásobnému podepisování ve smyslu podepsání textu více osobami.

4.1 Elektronický podpis bez viditelnosti textu podepisujícího (blind signature)

Pojem *blind signature* byl poprvé zaveden D.Chaumem v r.1982 (viz Příloha A část A3).

Elektronický podpis bez viditelnosti podepisujícího (tedy jeho „zaslepením“) spočívá v tom, že podepisující osoba realizuje podpis a poskytovatel systému si přeje uchovat text osoby která jej podepsala v tajnosti, během podepisováni.

Podle D.Chauma tento podpis má dvě strany **podpisovatele**, který je schopen se elektronicky podepsat a **poskytovatele**, který by rád obdržel podpis od podpisovatele k textu M, který poskytne podpisovateli.

Poskytovatel si může přát zneviditelnit podpisovateli text (tj. během podepisování), jak jen to bude možné (tj. do okamžiku, kdy bude později zveřejněn). Od okamžiku, kdy budou podpisy textu zveřejněny, se předpokládá , že podpisovatel se je dozví. Poskytovatel tedy může zabránit podpisovateli v aktuálním přístupu k podepisovanému textu (tj. zaslepit jej během podepisování) až do jeho zveřejnění.

Základní vlastností tohoto podpisu je tzv. *unlinkability*, tedy zaslepení textu před podpisovatelem během podpisování, neoddělitelnost od podepisující osoby a možnost pozdějšího zveřejnění.

Realizace tohoto podpisu na bázi RSA může být následovná:

Podpisovatel vybere dvě velká prvočísla p, q a zveřejní jejich produkt n. Podpisovatel vybere v „veřejných exponentů“ $e1, \ldots ev$ a vypočítá utajené exponenty $d1, \ldots dv$, kde

$di = (ei)^{-1} \bmod ((p-1)(q-1))$, kde i je v intervalu $(1,v)$.

Podpis i-tý na číslo m realizuje podpisovatel jako $m´i = m^{di} \bmod n$.

Každý ověřovatel může použít veřejné n a e_i, aby ověřil i-tý podpis, tak že ověří platnost $m = (m' i)^{ei} \bmod n$

D.Chaum v r.1985 realizoval tento podpis tak, že poskytovatel zaslepil text M, použitím klíče k z (1,…,n), tak že vygeneroval $t = [M] k^{ei} \bmod n$. Podpis t řeší

$$t' = [Mk^{ei}]^{di} = M^{di} k \bmod n$$

Poskytovatel může odkrýt obdržený t´ vytvořením

$$M' = [M^{di} k]\ k^{-1} \bmod n = M^{di} \bmod n$$

Podpisovatel tedy zná dvě množiny informací: množinu podepsaných zaslepených zpráv ti' (nebo ekvivalentně k podpisovateli t).

Pro každé částečné t' a Mi' podpisovatel je schopen určit pouze jedno

$$k = t' (Mi')^{-1} \bmod n,$$

což je provozovatelův tajný zaslepovací klíč, pokud spolu nekorespondují.

Jelikož však poskytovatel vybírá k náhodně a rovnoměrně, podpisovatel nic nezjistí o ostatním.

Poznamenejme, že poskytovatel musí „předvídat„ dílčí d, které bude použito podpisovatelem. To je v principu možné, i když výpočetně náročné, jelikož poskytovatel musí předvídat několik di najednou, aby určil například $t = Mr^{e1e2} \bmod n$ a odhalil podpis s d1 a d2 vytvořením

$$M1' = (Mr^{e1e2})^{d1} r^{-e2} \bmod n \text{ nebo } M2' = (Mr^{e1e2})^{d2} r^{-e1} \bmod n,$$

a to v závislosti, kde d1 a d2 byly použity k podpisu. Toto je výpočetně náročné se vzrůstajícím počtem d1,d2 …..dj, tedy pro velké j. Tento systém navržený D.Chaumem má aplikace např. v bankovnictví, elektronických volbách apod. Zde v těchto aplikacích je požadováno, aby podepsaný text byl pro ostatní zaslepen např. výše směnky, hlasování ano-ne apod.

Tento podpis lze porovnat např. proti kruhovému podpisu, kde je podobná myšlenka – zakrytí, kdo podepsal. Pojem zaslepení se zde však používá v jiném významu, nekryje se kdo podepsal (jako u kruhového), ale co podepsal. Z toho právě vyplývá použití v bankovnictví, aby bylo možné ověřit podpis osoby pod dokumentem (třeba fakturou), ale nebylo se možné podívat na některé části faktury apod.

4.2 Elektronický podpis, u kterého podpisovatel může zjistit podvrh padělatele s neomezenou výpočetní silou (tzv. fail-stop signature)

Elektronický podpis v angličtině nazývaný *fail-stop signature* umožní podpisovateli dokázat libovolné další osobě, že podpis, který by mu byl podvržen, je padělán. Plnohodnotná konstrukce tzv. fail-stop signature byla prezentována van Heijstem a Pedersenem na Eurocryptu 92, kde nepadělatelnost je založena na použití matematických vlastností diskrétního logaritmu.

Zde nastíníme jeho konstrukci založenou opět na matematických vlastnostech faktorizace.

Konstrukce vychází z homeomorfní funkce h mezi dvěma Abelovskými grupami, která má následující vlastnosti: máme-li obraz $h(a)$, pak existuje nejméně 2^t možných předobrazů. Zároveň je nemožné pro tuto funkci najít kolizi, tj. pro dvě různé proměnné stejná hodnota funkce h.

Ve skutečnosti existuje celá řada takových funkcí a generace klíčů v tomto systému spočívá na výběru h, dále t a bezpečnostním parametru, který zde označíme jako k.

Komponenty systému tzv. „fail-stop signature“ jsou následující:

a) Předklíč : příjemce vybere funkci h z množiny takových funkcí s doménou D a rozsahem H.

b) Předklíčový test: příjemce musí prokázat, že jeho výběr je správný a h splňuje dané požadavky

c) Tajný klíč : $sk:=(sk_1, sk_2)$, kde sk_1 a sk_2 jsou vybrány náhodně z G

d) Veřejný klíč: $pk:=(pk_1, pk_2)$, kde $pk_i= h\ (sk_i)$ pro $i =1,2$.

e) Podepisování: $Sign\ (s_k,m)' = sk_1.sk_2^m$ text m z množiny Z

f) Test: $test\ (pk,m,s) = OK$ tj, ekvivalentní $pk_1.\ pk_2^m = h(s)$.

g) Prokázání nepodvrženosti: mějme podvržený podpis sf na textu m^* Podpisovatel vypočítá s = Sign (sk, m^*), a je-li s různé od sf, použije pár (s,sf) k prokázání padělání podpisu

h) Test prokázání padělání: vezmou se dva elementy z G, a ověří se že kolidují vzhledem k h.

Platí tedy následující tvrzení :

Nezávisle na výběru h je v platnosti následující:

a) Správný podpis projde testem: $h(s) = h(sk_1.sk_2^{m}) = pk_1.pk_2$

b) Podpisovatel omezený polynomiální výpočetní silou nemůže konstruovat podpis a prokázat , že je podvržen

c) Je-li sf podvržený podpis na m^* a sf je různé od s, potom podpisovatel obdrží platný důkaz o podvrhu.

Podrobné rozpracování této problematiky lze najít v literatuře v Příloze A , část A3.

Aplikace tzv. „fail-stop signature“ pro vícenásobné podepisování může být např. v e-archivnictví, jelikož v budoucnu mohou existovat možnosti blížící se „neomezené výpočetní síle“ a možnosti vytvořit padělek. Zpětné prokázání, že se jedná o padělek, je tedy důležité.

4.3 Tzv. forward-secure elektronický podpis

Cílem tzv. *forward-secure* elektronického podpisu je ochrana podpisu proti riziku znehodnocení nebo vyzrazení tajného privátního klíče. Jelikož nelze garantovat absolutní bezpečnost a víme, že je-li jednou privátní klíč vyzrazen, může útočník falzifikovat (neoprávněně vytvořit) podpis. Tomu zabraňuje tzv. forward-secure elektronický podpis.

Princip ochrany je zde založen na pravidelném přepodepisování minule podepsaných textů novými klíči před znehodnocením starého (viz literatura Příloha A část A5).

Předpokládá se zde běžné PKI s veřejným klíčem PK a tajným klíčem SK0. Doba, po kterou je tajný klíč v platnosti, je rozdělena na periody číslované 1,…T. Zatímco veřejný klíč zůstává fixní, tajný klíč podpisovatele má časový vývoj tak, že v každé periodě používá tajný klíč Ski, i = 1,…T. Tajný klíč pro i-tou periodu je odvozen jako jednosměrná funkce h předchozí periody SKi = h(SK(i -1)). Tedy útočník, který získá klíč SKi během periody i, nezíská předchozí klíče SK0,…SK(i-1), jelikož ty byly zničeny. Útočník rovněž ze znalosti SKi nezíská předchozí, jelikož Ski bylo z předchozí získáno jednosměrnou funkcí.

Podpis obsahuje zároveň časový údaj periody, kdy byl realizován.

Aplikace tzv. forward-secure elektronického podpisu může být např. v archivnictví, kdy z hlediska dlouhodobé archivace může v budoucnu být kvantovým počítačem prolomeno PKI.

Právě v e-archivnictví, když se bude aplikovat vícenásobný podpis např. pro elektronické přepodepisování svazků z důvodu vypršení platnosti certifikátů předchozího elektronického podepisování, by vícenásobné použití forward-secure elektronické podpisu bylo výhodnější.

4.4 Zplnomocněný elektronický podpis (tzv. Proxy signature)

Ve schématu tzv. *proxy signature* podpisovatel deleguje svou podepisovací schopnost zplnomocněné entitě, která podepisuje dokument na přání podpisovatele.

Ukážeme si to na Schnorrově podepisovacím schématu:

Nechť p a q jsou velká prvočísla s $q|p-1$ a nechť g je generátor multiplikativní podgrupy Z^{*p} řádu q. Označme $H(,)$ bezkolizní hashovací funkci.

Podpisovatel A má pár klíčů (xA,yA) , kde soukromý klíč xA je elementem Z^{*p} a veřejný klíč $yA=g^{xA}$.

Při normálním elektronickém podpisu textu M podpisovatel A vybere náhodně k ze Z^{*q}.

Potom vypočítá $r = q^{k} \bmod p$ a dále $s = k + xA\ H(M,r) \bmod q$. Pak podpisem podpisovatele A na textu M je pár (r,s).

Ověřovatel ověří podpis výpočtem $q^{s} = r\ (yA)^{H(M,r)} \bmod q$.

U zplnomocněného podpisu zplnomocněný podpisovatel B má pár klíčů (xB,yB), kde veřejný klíč $yB=g^{xB}$.

Generace tzv. zplnomocněného klíče probíhá tak, že A použije Schnorrovo schéma na příkazový text Mw, jenž specifikuje, který text chce A podepsat. Podpisovatel tedy A vybere náhodně, k A ze Z^{*q} vypočítá

$$rA = q^{kA} \bmod p \text{ a dále } sA = kA + xA\ H(M,rA) \bmod q$$

a pošle zplnomocněnému podpisovateli B hodnoty (Mw,rA,sA). Hodnoty Mw a rA mohou být zveřejněny, sA musí zůstat utajena mimo B. Zplnomocněnec B provede ověření

$$q^{sA} = r\ A(yA)^{H(M,rA)} \bmod q$$

a je li v pořádku, vytvoří svůj zplnomocněný pár klíčů ze svých klíčů hodnot (Mw,rA,sA), určený k pověřenému podpisu daného textu:

$$(xP = xB + sA,\ yP = g^{xP} = yB\ rA\ (yA)^{H(Mw,rA)} \bmod q$$

Generování tzv. proxy elektronického podpisu určeného textu M zplnomocněním Mw, realizuje B použitím Schnorrova podepisovacím schématu s párem klíčů (xP,yP) na text M, přičemž obdrží podpis (rP,sP) textu M. Platným tzv. proxy elektronickým podpisem je množina hodnot (M,rP,sP,Mw,rA).

Ověřování probíhá následovně: nejprve se ověří ,že příkaz Mw určuje k podepsání text M, dále se ověří, že $g^{SP} = rP(yB\ rA\ (yA)^{H(Mw,rA)})$.

Aplikace zplnomocněného elektronického podpisu pro vícenásobné delegované podepisování může řešit problém spojení elektronické značky se zplnomocněnou osobou (např. řešení razítkování tj. podpisu organizace, který může realizovat jen zplnomocněná osoba). Podpis organizace (el. značka by byla tvořena pomocí bezpečného HSM (viz popis tzv. pdfproof a razítkovače od firmy nCipher) a měla váhu např. klasického kulatého razítka, jehož použití je svázáno s určitou zplnomocněnou osobou) by tak byl právně vyřešen jako „zplnomocněný“ podpis. To by mohlo být zajímavé pro aplikace vícenásobného podepisování ve veřejné správě.

4.5 Elektronický podpis šifrovaného textu (tzv. signcryption)

Elektronicky podepsaný a zašifrovaný text je jednou ze základních aplikací bezpečnostního výzkumu v informatice. Běžný postup podepsat a pak zašifrovat prostým složením těchto operací může být různě modifikován, jak je popsáno v literatuře v Příloze A, část A6.

Tzv. *signcryption* schéma je kryptografická metoda, která spojuje obojí, tj. bezpečné zašifrování a podepsání. optimálněji než prostým složení podepsání a pak zašifrování. Využívá páru algoritmů (v polynomiální čase), které nazveme `(S,U)`, kde `S` je podepisovací algoritmus a `U` je podpis šifrující algoritmus. Přitom `(S,U)` splňují následující:

a) *Jednoznačná vlastnost podpis-dešifrovatelnosti* - mějme text `m`, algoritmus `S` (podepisuje-šifruje) jehož použitím na `M` získáme podepsaný a zašifrovaný text `C`. Algoritmus `U` podpis –dešifrující `C` dá původní text `M` nedvojsmyslně.

b) *Bezpečnost* – tj. `S` a `U` současně splňují vlastnosti bezpečného šifrovacího schématu a bezpečného podepisovacího schématu

c) *Výkonnost* – výpočetní cena musí být nižší než prosté složení podpisu a zašifrování

Použití tzv. signcryption schématu může vycházet ze zkrácených verzí ElGamalova podpisu, tak jak je uvedeno v práci Y.Zhenga, což je včetně příkladu tzv. signcryption uvedeno na následujících obrázcích:

Shortened schemes	Signature (r, s) on a message m	Recovery of $k = g^x \bmod p$	Length of signature
SDSS1	$r = hash(g^x \bmod p, m)$ $s = x/(r + x_a) \bmod q$	$k = (y_a \cdot g^r)^s \bmod p$	$\|hash(\cdot)\| + \|q\|$
SDSS2	$r = hash(g^x \bmod p, m)$ $s = x/(1 + x_a \cdot r) \bmod q$	$k = (g \cdot y_a^r)^s \bmod p$	$\|hash(\cdot)\| + \|q\|$

p: a large prime (public to all),
q: a large prime factor of $p - 1$ (public to all),
g: a (random) integer in $[1, \ldots, p-1]$ with order q modulo p (public to all),
$hash$: a one-way hash function (public to all),
x_a: Alice's secret key,
y_a: Alice's public key ($y_a = g^{x_a} \bmod p$).

Obr. 1: Příklady zkrácených verzí podpisu

Signcryption by Alice the Sender

1. Pick x randomly from $[1, \ldots, q]$, and let $k = y_b^x \bmod p$. Split k into k_1 and k_2 of appropriate length. (Note: one-way hashing, or even simple folding, may be applied to k prior splitting, if k_1 or k_2 is too long to fit in E or KH, or one wishes k_1 and k_2 to be dependent on all bits in k.)
2. $r = KH_{k_2}(m)$.
3. $s = x/(r + x_a) \bmod q$ if SDSS1 is used, or
   $s = x/(1 + x_a \cdot r) \bmod q$ if SDSS2 is used instead.
4. $c = E_{k_1}(m)$.
5. Send to Bob the signcrypted text (c, r, s).

Unsigncryption by Bob the Recipient

1. Recover k from r, s, g, p, y_a and x_b:
   $k = (y_a \cdot g^r)^{s \cdot x_b} \bmod p$ if SDSS1 is used, or
   $k = (g \cdot y_a^r)^{s \cdot x_b} \bmod p$ if SDSS2 is used.
2. Split k into k_1 and k_2.
3. $m = D_{k_1}(c)$.
4. accept m as a valid message originated from Alice only if $KH_{k_2}(m)$ is identical to r.

Obr. 2: Příklad protokolu tzv. signcryption podepisovacího schématu

Význam tzv. signcryption je především v tom, že výkonnost – výpočetní cena je nižší než prosté skládání podpisů a zašifrování. Nicméně může mít význam i opačné pořadí, tj. nejprve zašifrovat a pak podepsat (může mít smysl v případech, kdy se nechce vyzradit tajné M v hierarchii podepisujícím osobám, které svým podpisem stvrzují podpis předcházejícího v hierarchii – např. vojáci předávají text a podpis určuje, že je skutečně od nějakého útvaru..., jde tedy o původ, původ se ověří a pošle se (zašifrovaně) dále apod.).

To také souvisí s aplikacemi, které vyžadují kombinace zaslepování textu, podepisování a šifrování.

Problematika šifrování a podepisování v XML formátu je rozebrána v nedávné práci D. Brechlerové *XML bezpečnost, část I* (http://crypto-world.info/__crypto01_07.pdf).

Zde je také uvedena řada aplikací, ze kterých vybíráme následující:

Předpokládejme, že chceme poslat XML soubor společnosti, která publikuje knihy. Tento soubor obsahuje detaily o knize, kterou chceme koupit. Navíc obsahuje informace o kreditní kartě zákazníka. Pro komunikaci o takto soukromých údajích chceme samozřejmě použít bezpečnou komunikaci.

XML dokument, stejně tak jako jiné dokumenty, může být zašifrován vcelku, např. SSL, a poslán jednomu nebo více příjemcům. Mnohem zajímavější ale je, jak řešit situaci, kdy různé části stejného dokumentu potřebují různé zacházení. Možností je právě kombinování XML šifrování a vícenásobného XS podepisování. Samotné XML šifrování není alternativou SSL/TLS.

Pokud aplikace vyžaduje zabezpečit celou komunikaci, je lepší SSL. Na druhé straně XML šifrování je nejlepší možností, pokud aplikace vyžaduje kombinaci bezpečné a nebezpečné komunikace, tedy část bude vyměňována zabezpečeně a část nezabezpečeně. Navíc ovšem SSL nezajišťuje trvalou ochranu při uložení na disku. Cílem vyvíjené normy pro XS (viz 2.7) je právě schopnost rozlišit, zda je podpis aplikován na zašifrované části nebo naopak.

4.6 Nezpochybnitelný elektronický podpis (tzv. undeniable signature)

Tzv. *undeniable signature* je elektronický podpis, který vyžaduje při ověření souhlas podpisovatele a nemůže být zpochybněn (poznamenejme že překlad undeniable jako nepopiratelný jsme nepoužili z důvodu, že se v české terminologii již používá při definici zaručeného el. podpisu a vzniká překladem slova non-repudiation).

Je známo, že klasický elektronický podpis může být kopírován a ověřován bez souhlasu podepisující osoby, což v některých aplikacích (např. v bankovnictví nebo v obchodních transakcích) není žádoucí, aby k tomu docházelo. Toto řeší

nezpochybnitelný elektronický podpis, který vyžaduje pro ověření souhlas podpisovatele.

Nezpochybnitelný podpis zavedl D.Chaum a literatura k této problematice je uvedena v Příloze A, část A8. Tento podpis oproti klasickému elektronickému podpisu vyžaduje souhlas podpisovatele, takže v případě ověřování negativní výsledek znamená, že buď podpis je neplatný nebo že ověřovatel neměl právo k ověření.

Protokol odsouhlasení ověření podpisu je následující:

Předpokládá se grupa řádu p a prvočíslo g, které jsou veřejně dostupné množině podepisujících osob. Předpokládejme konkrétního podpisovatele S vlastnícího soukromý klíč x a odpovídající veřejný klíč g^x. Text **M** je podepsaný podpisovatelem S, aby vytvořil podpis $z = m^x$.

Ověřovatel V, který ověřuje podpis z obdržený od podpisovatele S a chce bezprostředně ověřit jeho platnost, musí vyzvat S k souhlasu, což je realizováno protokolem výzva/odpověď:

Výzva má tvar $z^a (g^x)^b$, kde V vybere a a b nezávisle z grupových elementů. Odpověď vytvoří S povýšením výzvy inversním násobením $x \bmod p$.

Když V vypočte $m^a g^b$ a zjistí, že je to rovné odpovědi S, pak V ví s pravděpodobností p^{-1}, že podpis z není roven m^x.

Nezpochybnitelný podpis díky nutnosti nezpochybnitelné spolukomunikace ověřovatele a podpisovatele by mohl být použit v aplikaci doporučené e-pošty, kdy na e-doručence je nutný nezpochybnitelný podpis příjemce.

5. Vícenásobný elektronický podpis

Někteří kryptologové chápou pouze jako „vícenásobný elektronický podpis“ ten, kdy jeho ověření musí být vždy kratší než ověření všech `n` podpisů, a když existuje společný veřejný klíč. V naší analýze jsou zahrnuty všechny druhy podpisů souvisejících s vícenásobným podepisováním, tedy i přístup se skládáním jednoduchých podpisů, kdy každý z podepisujících má svůj vlastní soukromý i veřejný klíč (tj. že veřejný klíč není společný), a když více osob podepíše text, a nebo když jedna osoba vícekrát podepíše různé části textu.

5.1 Přístup skládáním jednoduchých elektronických podpisů

Předpokládejme, že `n` různých podpisovatelů má podepsat zprávu `M` a každý z nich má k dispozici prostředky pro „běžný“ elektronický podpis – svůj soukromý a veřejný klíč. V takovém případě existují dva základní, přirozené přístupy:

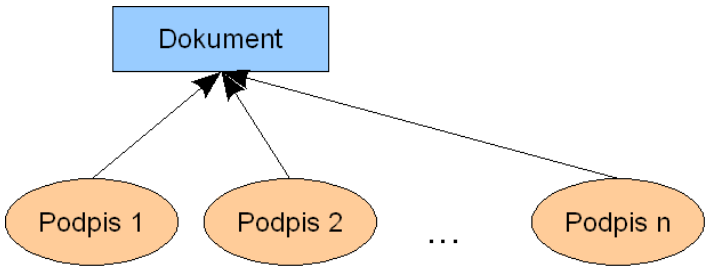
1. Všechny podpisy jsou na sobě nezávislé a podepisují právě jen zprávu `M`. Pořadí podpisů není určeno. Tuto variantu budeme nazývat *nezávislé podpisy*.
2. Je stanoveno určité pořadí podpisovatelů. Každý z podpisovatelů dostává k podpisu původní zprávu včetně podpisů všech podpisovatelů před ním. Tento celek podepíše, svůj podpis připojí a předá dalšímu podpisovateli v pořadí. Tuto variantu budeme nazývat *postupně zaobalující podpisy*.

V dalším popíšeme tyto přístupy podrobněji.

Platností podpisu zde rozumíme ověření toho, že zpráva byla podepsána soukromým klíčem odpovídajícím veřejnému klíči podpisovatele. Platnost certifikátu, který spojuje podpisovatele s jeho veřejným klíčem, je oddělenou otázkou.

5.1.1 Nezávislé podpisy

Ve variantě nezávislých (nebo také paralelních) podpisů podepisuje každý z podpisů pouze dokument, jak ukazuje následující obrázek. Podpisovatelé mohou podepsat každý svou vlastní kopii zprávy, a následně dojde k jejich sloučení, nebo si mohou zprávu předávat a podpisy k ní přidávat postupně.



Obr. 3: Nezávislé podpisy

Každý z podpisovatelů I_i, $i=1, \ldots, n$, vypočte otisk $h(M)$ zprávy M a ten zašifruje svým soukromým klíčem SK_i. Tím vytvoří svůj podpis:

$$S_i = SK_i(h(M)).$$

Všechny tyto podpisy se připojí ke zprávě M a vznikne tak celek vícenásobně podepsané zprávy

$$(M + S_1 + S_2 + \ldots + S_n).$$

Při ověřování takovéhoto podpisu si ověřovatel vypočte vlastní otisk zprávy $h'(M)$. Potom pro každý z podpisů S_i, $i=1, \ldots, n$, pomocí veřejného klíče odpovídajícího podpisovatele VK_i vypočte otisk, který byl tím kterým podpisem podepsán

$$h_i = VK_i(S_i).$$

Pokud se h_i shoduje s $h'(M)$, podpis S_i je platný. Jsou-li platné všechny podpisy S_i, $i=1, \ldots, n$, pak je platný i podpis vícenásobný. Případná neplatnost některého z podpisů nemá vliv na platnost podpisů ostatních, avšak vícenásobný podpis v takovém případě platný není.

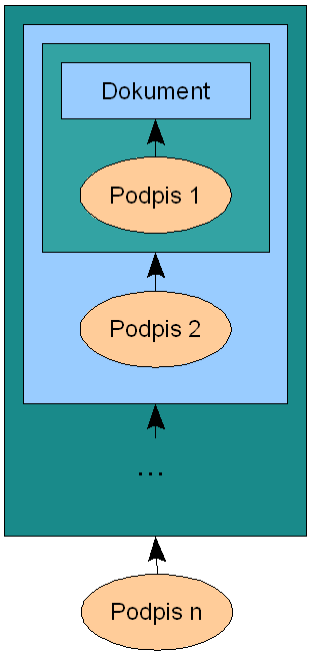
5.1.2 Postupně zaobalující podpisy

Ve variantě postupně zaobalujících podpisů každý podpisovatel podepisuje dokument včetně všech dříve přiložených podpisů, viz Obr. 4: Postupně zaobalující podpisy podepisující dokument včetně podpisů.

Postup tvorby podpisů je následující. První z n podpisovatelů podepíše svým soukromým klíčem SK_1 otisk $h(M)$ zprávy M. Tento podpis označme S_1,

$$S_1 = SK_1(h(M)).$$

Tento podpis připojí ke zprávě, čímž vznikne poprvé podepsaná zpráva $M^{(1)}$:



Obr. 4: Postupně zaobalující podpisy podepisující dokument včetně podpisů

$M^{(1)} = (M + S_1)$.

Tento celek obdrží druhý podpisovatel. Vytvoří si jeho otisk a ten podepíše svým soukromým klíčem. Vznikne tak podpis

$S_2 = SK_2(h(M^{(1)})) = SK_2(h(M+S_1))$,

který přidá k $M^{(1)}$, čímž vznikne podruhé podepsaná zpráva $M^{(2)}$:

$M^{(2)} = (M^{(1)} + S_2) = (M + S_1 + S_2)$,

kterou bude podepisovat podpisovatel třetí. Obecně i-tý podpisovatel v pořadí obdrží zprávu $M^{(i-1)}$, tedy zprávu M s postupně zaobalujícími podpisy předchozích podpisovatelů I_1, ..., I_{i-1}. Tuto zprávu podepíše svým soukromým klíčem SK_i, čímž vznikne podpis

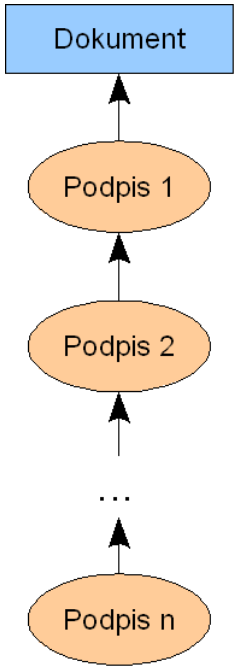
$S_i = SK_i(h(M^{(i-1)})) = SK_i(h(M+S_1+...+S_{i-1}))$

a tento podpis k obdržené zprávě připojí, čímž vznikne zpráva $M^{(i)}$

$M^{(i)} = (M^{(i-1)} + S_i) = (M + S_1 + ... + S_i)$.

Po podpisu posledního podpisovatele I_n vzniká zpráva $M^{(n)}$, která je zprávou M s vícenásobnými, postupně zaobalujícími podpisy:

$M^{(n)} = (M + S_1 + ... + S_n)$.



Obr. 5: Postupné podpisy podpisů (bez dokumentu)

Při ověření podpisu se pro každý podpis S_i, $i=1$, ..., n, zkontroluje rovnost

$$h'(M^{(i-1)}) = h_i,$$

kde

$$h_i = VK_i(S_i).$$

Vícenásobný podpis je platný v případě, že se podařilo ověřit všechny podpisy S_1, ..., S_n. V případě neplatnosti rovnosti otisků u i-tého z podpisů je třeba za neplatné považovat všechny podpisy S_i, S_{i+1}, ..., S_n, neboť v tom případě se nelze spolehnout na ověřovatelem vypočtené otisky $h'(M^{(k)})$, $k=i$, ..., $n-1$.

U každého z podpisů S_i je (mimo jiné) podepisována i původní zpráva M. Možnou podvariantou postupně zaobalujícího podpisu je i ta, ve které i-tý podpisovatel podepíše zprávu M a pouze předchozí podpis S_{i-1}.

Existuje též podvarianta, že i-tý podpisovatel podepíše pouze předchozí podpis bez původní zprávy M, viz Obr. 5: Postupné podpisy podpisů (bez dokumentu). Pak je však diskutabilní, zda takto vzniklý celek může být interpretován jako vícenásobný podpis zprávy M. Druhý a další podpisovatelé mohou své podpisy vytvořit i bez znalosti zprávy M, a není tedy jisté, zda je oprávněné tyto jejich podpisy chápat jako podpisy původní zprávy. Existují však zdroje ([20]), které výše zmíněné podpisy zprávy považují za ekvivalentní.

5.1.3 Srovnání nezávislých a postupně zaobalujících podpisů

Srovnejme základní aspekty obou variant.

Aspekt	Zhodnocení	
	Nezávislé podpisy	**Postupně zaobalující podpisy**
Způsob vzniku	Libovolný (paralelní, sekvenční, i kombinace těchto)	Pouze sekvenční
Postavení podpisovatelů	Rovnocenné	Hierarchie, nadřízený podepisuje po podřízeném
Typické využití	Podpis smlouvy, dohody, petice	Oběh dokumentů v organizaci

Srovnejme obě varianty z hlediska možnosti zjištění posloupnosti podpisů.

Aspekt	Zhodnocení	
	Nezávislé podpisy	**Postupně zaobalující podpisy**
Možnost časovou posloupnost podpisů	Pouze s využitím dalších prvků jako časová razítka	Ano
Možnost zjistit kauzální posloupnost podpisů	Záleží na podepisovacím protokolu (nelze při paralelním podepisování, lze při podepisování sekvenčním)	Každý podpisovatel vidí podpisy podpisovatelů v pořadí před ním

Srovnejme odolnost obou variant vůči manipulaci s podpisy. Je nutno rozlišovat podle množství informace, která je dostupná z kontextu.

Situace	**Aspekt**	**Zhodnocení**	
		Nezávislé podpisy	**Postupně zaobalující podpisy**
Pokud z kontextu nevyplývá cílový počet podpisů	Lze zjistit odebrání některého podpisu	Nelze zjistit odebrání libovolných podpisů	Nelze zjistit odebrání libovolného počtu podpisů od konce
	Lze zjistit přidání podpisu	Nelze	Nelze
	Lze zjistit nahrazení některého podpisu jiným	Nelze	U posledního podpisu nelze, u ostatních lze
Pokud z kontextu vyplývá cílový počet podpisů, avšak ne veřejné klíče podpisovatelů	Lze zjistit odebrání některého podpisu	Ano	Ano
	Lze zjistit přidání podpisu	Ano	Ano
	Lze zjistit nahrazení některého podpisu jiným	Nelze	U posledního podpisu nelze, u ostatních lze
Pokud z kontextu vyplývá cílový počet i veřejné klíče podpisovatelů	Lze zjistit odebrání některého podpisu	Ano	Ano
	Lze zjistit přidání podpisu	Ano	Ano
	Lze zjistit nahrazení některého podpisu jiným	Ano	Ano

Srovnejme ještě další aspekty obou variant podpisů.

Aspekt	Zhodnocení	
	Nezávislé podpisy	**Postupně zaobalující podpisy**
Vztah každého podpisu k původní zprávě	Přímočarý	Nepřímý – přes předchozí podpisy, druhý a další podpisovatelé podpisují jinou zprávu
Prokázání, že některý podpis je podpisem původní zprávy dle ZoEP	Přímočaré	Obtížnější Vyžaduje, aby předchozí podpisy byly platné
Výpočetní náročnost ověření podpisů	1-krát výpočet otisku, `n`-krát aplikace veřejného klíče	`n`-krát výpočet otisku, `n`-krát aplikace veřejného klíče

5.2 Přechod ke složitějším schématům

Vícenásobný elektronický podpis optimalizuje výpočetní náročnost ověření podpisů v případě, kdy se musí vždy všichni podepsat a je k tomu jen jeden veřejný klíč, který se použije k ověření, a jedním ověřením se najednou ověří, že text byl podepsán všemi odpovídajícími šifrovými klíči.

Demonstrujeme to na elektronickém podpisu založeném na šifrovacím algoritmu RSA, který je běžný, i když to platí na libovolný šifrovací algoritmus s multiplikativní vlastností.

Šifrovací algoritmus RSA (poznamenejme, že bezpečnost RSA je založena na skutečnosti, že je obtížné rozložit na součin velká čísla, z nichž každé je součinem dvou velkých prvočísel, závisí tedy na možnostech řešit úlohu tzv. faktorizace, která může v budoucnu být kvantovými počítači řešena i pro dnes bezpečná, dostatečně velká prvočísla), lze stručně popsat následovně:

Vytvoření klíčů

Jednotliví uživatelé si vytváří veřejný `VK` a soukromý klíč `SK` pro RSA následovně:

1. nejprve náhodně (a nepredikovatelně – viz následující odstavec) si vygenerují dvě dostatečně velká prvočísla p a q (jejich přibližná velikost - tj. počet bitů - je zadána)

2. spočtou $n = pq$ a $\Phi = (p-1)(q-1)$

Poznámka: stačí použít číslo $\lambda = NSN(p-1,q-1)$, tj. nejmenší společný násobek čísel $p-1$ *a* $q-1$.

3. zvolí náhodné číslo e, kde $1<e<\Phi$ *, tak, že* $NSD(e,\Phi)=1$. NSD značí největšího společného dělitele

4. užitím Eukleidova algoritmu spočte jednoznačně definované číslo d *takové, že* $1<d<\Phi$ *a* $ed \equiv 1 \mod \Phi$

Veřejným klíčem je potom (n,e), tajným klíčem uživatele je d.

Šifrování a dešifrace

Popíšeme nyní, jak probíhá vlastní šifrování a dešifrace. Předpokládejme, že strana B zná autentický veřejný klíč strany A, kterým je (n,e) a zašifrovává zprávu M pro A. Strana B vyjádří zprávu M jako číslo m, $0 \leq m \leq n-1$ (resp. jako posloupnost takových čísel). Dále strana B spočte

$$c = m^e \mod n$$

a zašle šifrový text straně A. Strana A nyní při dešifraci spočte pomocí tajného klíče d

$$m = c^d \mod n$$

Důkaz platnosti

Výsledkem je skutečně m, což lze dokázat následovně (např. Menezes at all.: Handbook of Applied Cryptography):

Jelikož $ed \equiv 1 \mod \Phi$, existuje tedy k tak, že $ed = 1 + k\Phi$. Dále, pokud $NSD(m,p) = 1$, pak podle Fermatovy věty

$$m^{p-1} \equiv 1 \mod p$$

Umocníme obě strany této kongruence číslem $k(q-1)$ a posléze vynásobíme obě strany rovnice číslem m. Dostaneme

$$m^{1 + k(p-1)(q-1)} \equiv m \mod p$$

Pokud je $NSD(m,p) = p$ (druhá možná situace), pak tato rovnost platí rovněž (obě strany jsou rovny nule $\mod p$). Vždy tedy

$$m^{ed} \equiv m \bmod p$$

Obdobně se dokáže $m^{ed} \equiv m \bmod q$. Odsud plyne $m^{ed} \equiv m \bmod n$, a tedy

$$c^d \equiv (m^e)^d \equiv m \bmod n.$$

Souvislosti

Myšlenka vychází z rozšíření šifry na více privátních klíčů a jeden veřejný, díky vlastnosti multiplikativnosti RSA, jak je patrno z následujícího:

Je vybráno (např. společností, či skupinou, která chce podepsat M apod.) číslo n jako součin dvou velkých prvočísel.

Soukromé klíče uživatelů, tj. podepisujících osob dokument M, které nazveme Alice (A) a Bob (B) , označíme r, s pro A, B resp.

Jednotliví uživatelé si vytváří veřejný a tajný klíč pro RSA dle 2.3.1 přičemž nyní platí:

$$r.s.t \equiv 1 \bmod \Phi(n)$$

Veřejným klíčem je potom t.

První podepisující M vypočítá:

$$S1 = M^r \bmod n$$

a pošle $S1$ druhému podepisujícímu. Druhý podepisující nyní obdrží M' z $S1$ podepsáním:

$$M' = S1^{(s.t)} \bmod n$$

jelikož zná svůj soukromý klíč s a veřejný t. Je-li $M = M'$ podepíše $S1$

$$S2 = S1^s \bmod n$$

a pošle $S2$ prvnímu podepisujícímu. Jelikož t je veřejný klíč, může první uživatel a kdokoliv jiný ověřit platnost:

$$M = S2^t \bmod n$$

Tedy text M musí být podepsán dvěma autorizovanými podpisy, aby vzniklo $S2$ přičemž nezáleží na pořadí podepisování A, B.

Rozšíření ze dvou na n uživatelů je zřejmé a vychází z multiplikativní vlastnosti podpisu. Podrobně je tento způsob podepisování stejného dokumentu více osobami popsán v knize B.Schneiera (Applied Cryptography str.510) a jeho výhody oproti dvěma předchozím jsou zřejmé.

V současnosti v ČR dosud žádná CA takovéto klíče pro vícenásobné podepisování zaručeným elektronickým podpisem s kvalifikovaným certifikátem nenabízí. Toto je limitující faktor pro navržení optimální varianty možnosti více elektronickými podpisy podepsat dokument, obzvláště ve smyslu ZoEP.

Konkrétně není nabízeno skupině `n` uživatelů, aby k `n` soukromým klíčům `SKi`, byl vystaven certifikát s jedním veřejným klíčem `VK` pro celou skupinu `n` účastníků, právě pro vytvoření tohoto vícenásobného elektronického podpisu. Zde by mohl být prostor pro legislativu, týkající se ZoEP a CA.

5.3 Skupinový elektronický podpis

Pojem *skupinového elektronického podpisu* (tzv. *Group Signatures*) zavedl ve své práci D.Chaum a E. van Heyst (viz literatura Příloha A 2.1). Označil jím elektronický podpis pro situaci, kdy dokument `M` má být podepsán skupinou lidí.

Skupinový podpis, oproti vícenásobnému podpisu, má tyto vlastnosti:

a) pouze členové skupiny mohou podepsat `M`

b) příjemce může ověřit, že se jedná o platný podpis člena skupiny

c) je-li to nezbytné, podpis může být „otevřen“ a člen skupiny, který dokument podepsal identifikován.

Skupinový podpis je zobecněním kryptografického autentizačního protokolu, kdy člen skupiny chce důvěryhodně prokázat že do skupiny patří.

Realizace skupinového podpisu vychází z následujících předpokladů:

a) Pro každého člena skupiny je nemožné vypočítat RSA klíče (a podobně v případě elektronického podpisu založeném na diskrétním logaritmu člen skupiny nemůže vypočítat diskrétní log modulo 2)

b) Žádný člen skupiny nemůže určit, kdo realizoval podpis (kromě sebe samotného)

c) Existuje důvěryhodná autorita `Z`, která vytváří schéma skupinového podpisu

Existuje již celá řada různých modifikací schémat skupinového podpisu. Ve schématu představeném Chaumem a Heystem v roce 1991 se předpokládá vytvoření skupiny `n` uživatelů, která je spravována jedním manažerem `Z`. Pro tuto skupinu je vytvořen jeden ověřovací klíč nazývaný `gpk` (*group public key*). Každý člen skupiny má svůj vlastní podepisovací soukromý klíč, který je vytvořen tak, že „relativně odpovídá“ veřejnému skupinovému klíči `gpk`.

Vlastnosti požadované po skupinovém podpisu jsou pak splněny následovně:

a) každý může ověřit, že někdo ze skupiny, kterou manažer spravuje, zprávu podepsal
b) manažer skupiny pomocí speciálního klíče `gmsk` může zjistit, kdo ze skupiny zprávu podepsal (*traceability*)
c) kdo nemá k dispozici `gmsk` maskovací klíč, nemůže zjistit, kdo ze skupiny podpis vytvořil (*anonymity*)
d) zveřejnění klíče `gmsk` nevede k „oslabení“ podpisového schématu (tj. podpisy, které lze ověřit klíčem `gpk`, mohou i nadále vytvořit pouze členové skupiny daného manažera)

Postupem času bylo schéma modifikováno, kdy kromě nefalzifikovatelnosti (*unforgeabilty*), byla zapracována i analyzována řada dalších možných požadavků např. neoddělitelnosti ze skupiny (*unlinkability*), omluvitelnost (*exculpability*), různé typy odolnosti (*collusion resistence* - “koaliční resistence“, tj. zabránění vzniku podskupiny, která by podepsala bez souhlasu důvěryhodné autority `Z`, *framing resistence*), plná anonymita (*full anonymity*), či možnosti pro `Z` vysledování toho, kdo podepsal (*traceability*).

Pro pochopení skupinového podpisu skupiny o `g` členech prezentujeme jeho základní schéma:

Důvěryhodná autorita `Z` vygeneruje dvě velká prvočísla `p` a `q`, `N=pq` a vybere hashovací funkci `h`. `Z` dá členu skupiny `i` soukromý klíč `S Ki`, což je náhodně vybrané velké číslo z intervalu `Phi=(Sqrt N,… 2 Sqrt N)`, a vypočte `v=S K1. S K2… S Kg`, a zveřejní `N`, *v* a `h`.

Chce-li `i`-tý člen skupiny podepsat text `M`, jeho podpis bude $S_i = (h(M)^{SK1} \bmod N$.

Zde se samozřejmě otevírá široké spektrum pro praktické aplikace v bankovnictví, státní správě, elektronických volbách apod. Dovedeme si jistě představit správní radu o `g` členech, která při realizaci elektronického hlasování bude využívat funkce skupinového podpisu, jako je neoddělitelnost ze skupiny, plná anonymita, omluvitelnost apod. Rovněž role důvěryhodné autority `Z` a nároky na klíč `gmsk` musí být jednoznačně stanoveny.

Pro použití skupinového podpisu ve státní správě to vyžaduje legislativní podporu (bez této v současnosti nelze dle našeho názoru tuto aplikaci využít). Toto chápeme jako prostor pro případnou legislativní podporu těchto aplikací pro vznik e-státu v ČR.

5.4 Skupinově orientovaný elektronický podpis

Zprávy jsou často určeny určité skupině lidí (např. pouze vrcholovému managementu).

Je-li použita asymetrická šifra a běžné PKI k ochraně informací ve zprávě, pouze legitimní členové skupiny mohou zprávy šifrovat , dešifrovat a podepisovat. Název *skupinově orientovaný elektronický podpis* je převzat z práce Y.Desmeta a týká se v podstatě problematiky definice skupiny, důvěryhodnosti Z a vychází z důvěryhodnosti členů skupiny apod. Zde vzniká celá řada kombinací vícenásobných podpisů a odlišnost je např. v možnosti vytvářet podpis skupiny bez důvěryhodné autority Z.

Jako příklad uvedeme

5.4.1 Kruhový podpis (Ring Signatures)

Jde vlastně o skupinový podpis bez autority Z.

Mějme tedy skupinu n různých uživatelů, kterou označíme U. Každý z těchto n uživatelů má svá párová data (soukromý a veřejný klíč). Párová data i-tého uživatele označíme : $(S\ K_i\ ,\ V\ K_i)$. Kruhový podpis skupiny uživatelů U se vytváří pomocí všech n veřejných klíčů uživatelů této skupiny a jednoho soukromého klíče libovolného (např. i-tého) uživatele ze skupiny U.

Formálně se tedy dá zapsat kruhový podpis skupiny U jako $R(V\ K_1\ ,\ V\ K_2\ ,\ \ldots\ ,\ V\ K_n\ ,\ S\ K_i\ )$, kde i je libovolná hodnota od 1 do n. Podmínkou, abychom takovou hodnotu R mohli nazývat kruhovým podpisem je, že:

a) ověřovatel musí být schopen ověřit podpis ze znalosti všech n veřejných klíčů,

b) nelze podpis R vytvořit bez znalosti alespoň jednoho z n soukromých klíčů,

c) ověřovatel nezjistí, čí soukromý klíč $S\ K_i$ byl použit .

Jinými slovy takto zkonstruovaný podpis může vytvořit každý ze skupiny U. Ověřovatel pouze zjistí, že podpis vytvořil jeden z uživatelů této skupiny, nezjistí však který.

Kruhový podpis se hodí k prokazování příslušnosti ke skupině U. Může být použit jako podpis za skupinu U, ale se zachováním anonymity podepisujícího a s možným nesouhlasem ostatních členů skupiny.

Definice a možné aplikace (hlasování na valných hromadách,volby apod.) takovéhoto podpisu naleznete podrobněji například v příspěvcích:

R.Rivest, A.Shamir, Y.Tauman : How to leak a secret. In Proceedings of Asiacrypt 2001, Volume 2248 of LNCS, pages 552-65. Springer - Verlag, 2001.

M.Bellare, D.Micciancio, B.Warinschi: Foundations of Group Signatures : Formal Definitions. Simplified Requirements, and a Construction Based on General Assumptions. In Proceedings of Eurocrypt 2003, volume 2656 of LNCS, pages 614-30. Springer - Verlag, 2003.

Poznamenejme, že aplikace hlasování na valných hromadách, volby apod. právě vyžadují zachování anonymity hlasujícího a nepřítomnost důvěryhodné autority Z, což nám skupinově orientovaný elektronický podpis vůči skupinovému podpisu poskytuje. V současnosti jsou tyto aplikace předmětem dalšího výzkumu a závěr z konference CRYPTO 2006 je, že v současnosti plně bezpečná aplikace pro e-volby není.

5.4.2 Hromadné podpisy (Aggregate Signatures)

Zobecněním předchozího problému je tzv. *hromadný podpis*. Stručně jej lze charakterizovat takto:

Hromadný podpis je podpisové schéma, které umožňuje shlukování stávajících podpisů – tj. z n podpisů n různých zpráv, které vytvořilo n osob, lze vytvořit jediný krátký podpis, jehož ověřením se ověří všech n dílčích podpisů n osob k n zprávám.

Hromadným podpisem tedy není podpis S nějaké osoby (byť by to byl některý z výše uvedených uživatelů ze skupiny U), který vznikne podepsáním zprávy sestavené z podpisů S1 … Sn. Takovýto podpis není závislý na platnosti, či neplatnosti jednotlivých podpisů Si, a proto nesplňuje požadavek, že jeho ověřením se ověří jednotlivé podpisy S_i.

Formální konstrukce hromadného podpisu je následující :

Označíme-li Si podpis i-tého uživatele ui ke zprávě Mi, pak hodnota A bude hromadným podpisem vytvořeným pomocí hromadného podpisového schématu AS, pokud

$$A = AS\ ((u_1, S_1, M_1), (u_2, S_2, M_2), \ldots, (u_n, S_n, M_n))$$

splňuje následující podmínky :

a) A nelze vytvořit bez podpisů $S_1 \ldots S_n$.

b) ověření A je možné pouze tehdy pokud jsou platné všechny podpisy $S_1 \ldots S_n$.

Hromadný podpis je výhodný vzhledem k tomu, že umožňuje snížit počet ověření n podpisů na jedno ověření a velkou výhodou je i snížení počtu certifikačních cest. To vede především k velké úspoře výpočetního času potřebného na ověření, což má klíčový význam pro e-archivaci.

Definice a možné aplikace takovéhoto podpisu naleznete např. v příspěvcích:

S.Kent, C.Lynn, K.Seo: Secure border gateway protocol (Secure-BGP).IEEE J.Selected Areas in Comm., 18(4), pages 582-92, April 2000.

D.Boneh, C.Gentry, B.Lynn, H.Schaham: Aggregate and Verifiably Encrypted Signatures from Bilinear Maps. In Proceedings of Eurocrypt 2003, volume 2656 of LNCS, pages 416-32. Springer - Verlag, 2003.

Práce, které takový hromadný ověřovací postup popisují: tj. ověřování RSA podpisů v dávce, jsou např. :

Bellare, J.Garay,T.Rabin: Fast Batch Verification for Modula Exponentiation and Digital Signatures, EUROCRYPT 98, LNCS 1403, Springer-Verlag 236-250, 1998

S.Lee, S.Cho. J.Choi, Y.Cho : Efficient Identification of Bad Signatures in RSA-Type Batch Signature, Udice Transactions on Fundamentals of Electronics, Communications and Computer, Vl. E-80, pp.74-80,2006)

V podstatě jde o dvě metody, jak podpisy ověřovat:

1. První metoda od samého počátku konstruuje vše tak, aby najednou došlo k ověření nebo odhalení chybného podpisu.

2. Druhá metoda je ověřovat normální podpisy tak, aby to nebylo jeden po druhém. Tedy vymyslet dávkový algoritmus a pokud to nevyjde – pak je alespoň jeden podpis neplatný, a potom je nutné jej následně vyhledat – tj. aplikovat algoritmus vyhledávání.

Režie v druhém případě je nula, ale pak se platí časem při hledání chybného podpisu, první přístup je opačný – režie je velká, ale samotné ověření a vyhledání je rychlé. Z toho také plynou možné způsoby použití. Kde se ten velký počet podpisů bude ověřovat jen jednou (málo) je výhodnější druhá metoda, při častém ověřování metoda první ..).

Výše uvedené typy podpisů nejsou jen kryptologickou hrátkou na sestavování nových

možných protokolů, ale vzhledem k zajímavým „ekonomickým“ vlastnostem při ověřování podpisu, případně vzhledem k zcela novým možnostem (podpis se zachováním plné anonymity, prokazatelnost příslušnosti ke skupině apod.) se dá očekávat, že budou využívány pro speciální situace nebo se dokonce stanou běžným vybavením podpisových prostředků.

Rozbor souvislostí mezi různými schématy vícenásobného podpisu, tzv. *prahového podpisu* (*threshold signature*) a *podpisu naslepo* (*blind signature*) ve skupině tzv. GDH (Gap Diffie-Hellman) je poměrně složitý a je předmětem výzkumu.

5.5 „Threshold“ podpis

Vícenásobný elektronický podpis byl podrobně zaveden v práci [1] (viz Příloha literatury k této kapitole) a rozpracován v řadě dalších prací, z nichž podstatné jsou [2,3,4,5,6,7,8].

Tato schémata viz např. [6,7] nepodporují vznik skupiny podpisovatelů a dovolují pouze, aby každý člen skupiny podepsal dokument. Původní řešení [1,5] nejsou navíc ani příliš efektivní, jelikož: vytvoření a ověření vícenásobného elektronického podpisu roste lineárně s počtem podpisovatelů.

V nezávislé práci [9] pak bylo navrženo nové hromadné podepisovací schéma, založené na skupinovém podepisování. Na rozdíl od vícenásobného podpisu, hromadné podepisovací schéma umožňuje skupině podpisovatelů podepisovat různé texty. Podepisovací schéma [9] vyžaduje zavést tzv. Gap Diffie-Hellmanovu (GDH) grupu (matematická definice viz [9]).

Řada nových podepisovacích schémat (např. [10]) využívá matematické GDH grupy, kde výpočetní Diffie-Hellmanův problém (Computational Diffie-Hellmann problem, zkráceno CDH) je obtížný a rozhodovací Diffie-Hellmanův problém (Decisional Diffie-Hellmann problem, zkráceno DDH) je jednoduchý.

V citované práci je ukázáno, že problém CDH spočívá ve výpočtu $h = g \cdot \log_g u \cdot \log_g v$ pro tři náhodně vybrané elementy grupy *(g,u,v)* a problém DDH požaduje rozhodnout, které ze čtyř grupových elementů (g,u,v,h) jsou náhodné, nebo naopak, že mají vlastnost $\log_g u = \log_g v$.

Podepisovací schéma s využitím GDH, jiné než v [10], bylo navrženo A.Lasyanskou[11].

V práci [12] pak je navrženo robustní důvěryhodné schéma vícenásobného podpisu na bázi GDH tzv. MGS, které nepožaduje znalost podepisujících se a je prokazatelně bezpečné, a navíc efektivnější než schéma navržené v [11] .

Podepisovací délka a ověřovací čas u MGS, jako i u jiných podepisovací schémat na bázi GDH, jsou nezávislé na počtu podpisovatelů. GDH lze rovněž aplikovat na elektronické podpisy bez viditelnosti podepisujícího, které mají využití v bankovnictví. Hlavním přínosem těchto schémat je, že pro uživatele nelze sehnat podpis od podepisujícího tak, že podepisující nezná podepisovaný text, a že uživatel neobdrží více než jeden podpis pro jednu interakci s podepisujícím.

Bylo rovněž definováno nové GDH prahové – (tzv. threshold) podepisovací schéma, vycházející z threshold kryptografie [12-15]. Tato myšlenka (t,n) threshold kryptografie je založena na sdílení a distribuci informace (např. tajného klíče) a výpočtu (např.dešifrování neb generace podpisu) mezi n stranami s vyloučení podvrhu. Cílem je umožnit libovolné podskupině s více než t-členy rekonstruovat tajnou informaci a realizovat výpočet tak, aby byla zachována bezpečnost v případě přítomnosti narušitele, tj. neoprávněné osoby, která chce získat utajenou informaci, podvrhnout podpis apod., a tak poškodit t-členů skupiny (t od slova threshold „práh“).

Pro pochopení tohoto rozvedeme podrobněji, aby byla patrna i případná bezpečnostní úskalí tohoto schématu. Samotná základní myšlenka threshold kryptografie byla prezentována Y.Desmethem v práci [16]. Z ní vychází ta threshold podepisovací schémata, kde tajný klíč je rozdělen mezi n podepisujících osob (s důvěryhodnou stranou nebo bez ní), a to nějakým protokolem mezi jednotlivými stranami tak, jak bylo popsána u různých variant skupinových podpisů v předchozích kapitolách.

Aby byl podepsán text M, nějaká podskupina více než t účastníků může využít sdílení jejich tajemství a vytvořit generující interaktivní podepisovací protokol, jehož výsledkem je podepsání M.

Každý pak může ověřit tento threshold podpis použitím jednoho fixního veřejného klíče.

Bezpečnost tohoto threshold podepisovacího schématu garantuje, že žádný protivník, disponující výpočetní silou polynomiální v čase nemůže přečíst text popřípadě realizovat podvrh.

Výhody threshold podepisovacího schématu jsou následující:

a) robustnost, která požaduje, že dokonce t-padělatelů nemůže zabránit vzniku platného podpisu,

b) proaktivnost (tj. periodocké obnovování sdíleného tajemství), což chrání systém proti podskupiny a v různém čase,

c) prokazatelnost bezpečnosti.

Vícenásobný elektronický podpis v základním pojetí je odlišný od threshold podpisu, jelikož cílem vícenásobného podpisu je prokázat, že každý člen dané skupiny podepsal text M, a velikost této skupiny není nijak omezena. U threshold podpisu je cílem dokázat, že na vytvoření podpisu je nějaká skupina o t-členech dostatečná k podpisu textu M. Na rozdíl od vícenásobného podpisu, threshold podpis neukáže, kdo podepsal, a tedy nezjeví jednotlivé podepisující osoby (proto může mít aplikace také např. v elektronických volbách [17]).

Dalším rozdílem je, že ověřovací protokol u threshold podpisu není závislý na stávající podskupině podpisovatelů.

Je zřejmé že vícenásobný podpis v základním pojetí je také rozdílný od skupinových podpisů a kruhových podpisů (které jsme zde pro úplnost analyzovali), protože u nich každý jednotlivý důvěryhodný člen skupiny může realizovat platný podpis na přání celé skupiny.

5.5.1 Poznámky k bezpečnosti vícenásobných elektronických podpisů

Podstatná u vícenásobného elektronického podepisování je však otázka bezpečnosti, která až do doby publikování prací [7] nebyla diskutována. Nebyla dosud ukázána žádná forma prokazatelné bezpečnosti ve schématech s vícenásobným podepisováním.

Taky např. podepisovací schémata [2,3] byla účinně napadena. Ani rozpracování bezpečnosti v průkopnické práci [7] není dostatečné, nepopisuje např. útoky při generaci klíčů.

Až teprve kolektiv autorů v práci [8] dal základ silné bezpečnosti pro vícenásobný elektronický podpis. Tito autoři modifikují vícenásobný podpis na bázi Schnorrova schématu navrženého v práci [7] a dokazují jeho bezpečnost. Model bezpečnosti v [8] předpokládá, že skupina podpisovatelů se zná, tj. že každý z podpisovatelů zná všechny ostatní.

Autoři Nicolosi and Mazieres [18] navrhli redukovat ověření v případě robustního vícenásobného podpisu společným odsouhlasením v elektronickém podpisu, navrženém v práci A. Boldyrevy [19] a založeném na GDH . Mimo jiné také ukázali bezpečnostní slabiny vícenásobného elektronického podpisu založeného na GDH. Také ukázali, jak je odstranit.

Nicméně problém bezpečnosti u všech druhů vícenásobného podpisu je předmětem neustálého výzkumu a je třeba říci, že se neustále nalézají nové útoky na jednotlivé druhy vícenásobných elektronických podpisů.

Příloha literatury k této kapitole:

[1] K. Itakura and K. Nakamura, “A public key cryptosystem suitable for digital multisignatures,” *NEC Research & Development*, 71:1-8, 1983.

[2] L. Harn, “Group-oriented (t,n) threshold digital signature scheme and digital multisignature,” *IEE Proc. Computers and Digital Techniques*, 141(5), 1994.

[3] C. Li, T. Hwang and N. Lee, “Threshold-multisignature schemes where suspected forgery implies traceability of adversarial shareholders,” *Eurocrypt 94*, 1994.

[4] P. Horster, M. Michels and H. Petersen, “Meta-multisignatures schemes based on the discrete logarithm problem,” *IFIP/Sec* 1995.

[5] T. Okamoto, “A digital multisignature schema using bijective public-key cryptosystems,” *ACM Transaction on Computer Systems*, 6(4): 432-441, 1988.

[6] K. Ohta and T. Okamoto, “A digital multisignature scheme based on the Fiat-Shamir scheme”, *Asiacrypt 91*, 1991.

[7] K. Ohta and T. Okamoto, “Multi-signature scheme secure against active insider attacks”, *IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences*, E82-A(1):21-31, 1999.

[8] S. Micali, K. Ohta and L. Reyzin, “Accountable-subgroup multisignatures,” *ACM Conference on Computer and Communications Security*, 2001.

[9] D. Boneh, C. Gentry, B. Lynn and H. Shacham, “Aggregate signatures from bilinear maps,” Manuscript.

[10] D. Boneh, B. Lynn and H. Shacham, “Short signatures from theWeil pairing,” *Asiacrypt 01*, 2001.

[11] A. Lysyanskaya, “Unique signatures and verifiable random functions from the DH-DDH separation”, *Crypto 02*, 2002.

[12] A. Boldyreva “Threshold signatures, multisignatures and blind signatures based on the Gap-Diffie-Hellman-group signature scheme,” Full version of this paper. Available at http://www-cse.ucsd.edu/users/aboldyre/.

[11] D. Chaum, “Blind signatures for untreaceable payments,” *Crypto 82*, 1982.

[12] C. Boyd, “Digital multisignatures,” *Cryptography and Coding*, 1986

[13] Y. Desmedt, “Society and group oriented cryptography,” *Crypto 87*, 1987.

[14] Y. Desmedt and Y. Frankel, “Threshold cryptosystems,” *Crypto 89*, 1989.

[15] A. Shamir, “How to share a secret,” *Communications of the ACM,* 22:612-613, (1979).

[16] Y. Desmedt, “Threshold cryptography,”, *European Transactions on Telecommunications*,5(4), 1994.

[17] J.Hrubý , Elektronické volby v ČR?, Crypto-World 2006, ISSN 1801-2140,16(2006).

[18] A. Nicolosi and D. Mazieres. Secure acknowledgement of multicast messages in open peer-to-peer networks. In *3rd International Workshop on Peer-to-Peer Systems (IPTPS '04)*, San Diego, CA, February 2004.

[19] A. Boldyreva. Efficient threshold signatures, multisignatures and blind signatures based on the gap-diffie-hellman-group signature scheme. In *Public Key Cryptography 2003*, 2003.

[20] A. Lioy, G. Ramunno: Multiple electronic signatures on multiple documents. http://security.polito.it/doc/pub/icete2004.pdf.

6. Vícenásobný podpis a podpisové politiky

Způsobem realizace vícenásobných podpisů se mimo jiné zabývá dokument *ETSI TR 102 045* (*Electronic Signatures and Infrastructures (ESI), Signature policy for extended business model*). Tento dokument v zásadě dospívá k názoru, že je to téma komplikované (např. může ale nemusí být důležité pořadí podpisů a čas jejich vzniku) a blíže se zabývá kontrasignací, podpisem se svědkem a notářským podpisem. Tato kapitola obsahuje stručný výtah relevantních části zmíněného dokumentu.

6.1 Kontrasignace

Termín *kontrasignace* obvykle označuje případ, kdy k platnosti podpisu dokumentu je potřeba přidat ještě nějaký další podpis podepsaného dokumentu. Takto chápanému pojmu vyhovuje ovšem více situací, uveďme tyto typické případy:

a) kontrasignující osoba neověřuje podpis ani nevyjadřuje souhlas s dokumentem, pouze stvrzuje, že dokument s podpisem viděla (např. při existenci procesu zahrnujícím více osob potvrzuje, že v tomto procesu vykonala svou roli)

b) kontrasignující osoba ověřuje podpis, který kontrasignuje, a stvrzuje jeho platnost (podpis před svědkem, notářský podpis atp.)

c) kontrasignující osoba ověřuje stávající podpis i obsah podepsaného dokumentu (nadřízený schvaluje rozhodnutí podřízeného atp.)

Obecná pravidla, co vše kontrasignace znamená, nelze stanovit, neboť to záleží na konkrétním případu.

Z hlediska technické specifikace je kontrasignace (`countersignature`) jasně vymezený termín definující podpis, který podepisuje jiný podpis, z hlediska obchodních modelů je tento termín ovšem mnohem širší.

6.2 Způsob uspořádání podpisů

Dle způsobu uspořádání podpisů dokument *ETSI TR 102 045* rozlišuje tyto případy:

Paralelní (nezávislé) podpisy (*parallel signatures*)

Pořadí podpisů není důležité, každý podpis podepisuje pouze hash dokumentu, nepodepisuje žádné podpisy. Jediným vztahem nezávislých podpisů je, že musejí být přítomny všechny, aby byl dokument platný (např. podpisy prodávajícího a kupujícího na kupní smlouvě, podpisy několika jednatelů společnosti).

Sekvenční (nezávislé) podpisy (*sequential signatures*)

Sekvenční podpisy jsou nezávislé podpisy, jejichž pořadí vzniku je důležité. Tyto podpisy mohou ale nemusejí podepisovat tentýž obsah, mohou např. podepisovat již dříve vložené podpisy, ale jen jako součást dat, smyslem není nahradit kontrasignace nebo zaobalující podpisy. Sekvenční podpisy zatím nejsou zcela prozkoumaným tématem.

Zaobalující podpisy (*embedded signatures*)

Při tomto scénáři se podpis vždy aplikuje na jiný, který je v něm zaobalen. Pořadí vzniku podpisů je důležité. Zaobalující podpis se použije, kdykoli je jednou z funkcí přidávaného podpisu dosvědčit příjem dokumentu s předchozím podpisem, tj. předchozí podpis je kontrasignován. Kontrasignace může navíc dosvědčit následující body, ať už samostatně nebo v nějaké kombinaci:

a) odsouhlasení či schválení dat původně podepsaných

b) ověření identity předchozího podpisovatele

c) ověření platnosti předchozího podpisu

Např. notářský podpis na kupní smlouvě pozemku v sobě obsahuje všechny výše uvedené body, nepodpisuje proto pouze podpisy prodávajícího a kupujícího, ale také dokument obsahující jejich kupní smlouvu.

V případě podpisu před svědkem svědka obsah podepsaného dokumentu nezajímá, zajímá jej pouze podpis, který kontrasignuje.

6.3 Správa vícenásobných podpisů

Podpisová politika (nebo přesněji pravidla vyvinutá v rámci podpisové politiky) může poskytnout rámec správě vícenásobných podpisů. Měla by být poskytnuta pravidla jak pro tvorbu podpisů, tak pro jejich ověřování, přičemž závisí od obchodního modelu, na která pravidla bude kladen větší důraz. Např. při podepisování interních dokumentů v rámci jedné společnosti může být kladen důraz na pravidla upravující tvorbu podpisů – budou-li taková, že vznik nepravého podpisu bude velmi nepravděpodobný, může být ověřování podpisů pouze

namátkové. Při podepisování obchodních kontraktů je naopak může být důraz na vytvoření dat dostatečných k zajištění důvěryhodnosti podpisu.

Prvním nutným krokem správy více podpisů je definice způsobu tvorby jednotlivých podpisů; každý podpis pak může být ověřen podle podpisové politiky (např. TS 101 733).

Druhým krokem je definice vztahů mezi podpisy, což může být učiněno v těchto bodech:

a) přiřazení podepisovací role (signing role) jednotlivým podpisovatelům
b) přičlenění atributů každému z podpisů, tyto atributy určují účel podpisu v kontextu podpisového protokolu

6.4 Podepisovací role (Signing roles)

Podepisovací role je role specifikovaná v podpisové politice, která byla podpisovateli přiřazena nebo kterou přijal; tato role určuje vztah mezi jeho podpisem a každým dalším podpisem požadovaným podpisovou politikou.

Podepisovací role je zavedena pouze z důvodu správy více podpisů, neurčuje žádné atributy podpisovatele, ani označuje-li jej prodávající nebo kupující. Podepisovací roli je třeba odlišit od role podpisu (signature role), jak je definována v dokumentu TS 101 733.

Základní podepisovací role jsou tyto:

a) Primární podpisy (Primary signatures – PS) – nezávislé podpisy, mohou být i sekvenční
b) Kontrasignatury (Countrasignatures – CS) – jsou aplikovány na nezávislé podpisy a eventuálně na další sekvenční kontrasignace

Politika vzniku podpisů definuje počet podpisů a jejich vzájemný vztah. Např. u smlouvy týkající se jednoho prodávajícího a jednoho kupujícího by byly podepisovací role tyto:

a) PS/1 – prodávající
b) PS/2 – kupující

Odehrává-li se transakce v jurisdikci, kde musí být notářsky ověřena, podepisovací role notáře by byla CS/1.

6.5 Typy závazku elektronického podpisu

Typy závazku mohou hrát užitečnou roli při ověření vztahů mezi více podpisy. Typ závazku je skupina informací, které určují účel podpisu a poskytují informace o úmyslech podpisujících osobám spoléhajícím se na podpisy. Typ závazku může být vyjádřený, tj. podepisující osoba vědomě vybere a potvrdí typ závazku, nebo implicitní.

Typy závazku pro primární podpisovatele jsou tyto:

a) pravomocný (zákonný) závazek

b) schválení datového obsahu

c) prokázání pravosti (authentication)

d) důkaz/potvrzení obdržení

Pravomocný závazek a schválení obsahu by mělo vždy zahrnovat oznámení podpisovateli, který by měl tento závazek explicitně vybrat či potvrdit. Aplikace, které toto neposkytují, a které nemohou spolehlivě prokázat úmysly podpisovatele, mohou skončit s podpisem nevynutitelným v soudním řízení. U prokázání pravosti je explicitní potvrzení podpisovatelem možné v závislosti na okolnostech.

Typy závazku pro kontrasignující podpisovatele jsou tyto:

a) autorizace

b) svědectví

c) notářský

6.6 Ověření vícenásobného podpisů

Ověření vícenásobných podpisů zahrnuje tyto tři stupně:

a) zajistit vytvoření a shromáždění příslušných údajů k ověření platnosti

b) předpovědět možné výsledky ověření v závislosti na ověřovacích datech

c) porovnat skutečné výsledky ověření s předpověděnými výsledky

Nejprve musejí být ověřeny samostatně jednotlivé podpisy podle podpisové politiky jednonásobného podpisu. Dále musejí být ověřeny vzájemné vztahy mezi podpisy:

a) ověření přítomnosti všech potřebných podpisů

b) ověření, že atributy rolí odpovídají každé z určených podepisovacích rolí

c) ověření, že typy závazku jednotlivých podpisů odpovídají požadavkům podpisové politiky a příslušným podepisovacím rolím

d) pokud je významné pořadí a čas podpisu ověření, že všechny časové značky souhlasí s očekávanými výsledky

Pozn: Další podrobnosti ohledně podpisových politik vícenásobných podpisů naleznete ve výše uvedeném dokumentu *ETSI TR 102 045* (http://portal.etsi.org).

7. Vícenásobný podpis na Slovensku

Na Slovensku je použití vícenásobného podpisu v obchodním styku popsáno vyhláškou *NBÚ č. 542/2002 Z.z.*, která upravuje používání elektronického podpisu v administrativě a obchodním styku. Tato vyhláška staví v obchodním styku na roveň zaručený elektronický podpis s vlastnoručním podpisem.

Pro použití zaručeného elektronického podpisu dokumentu při podpisu více osobami uvádí tato vyhláška dvě schémata podpisu:

1. Dokument podepisuje více fyzických osob nacházejících se na tomtéž místě

a) Vytvoří se hash dokumentu

b) Každá z fyzických osob podepíše hash dokumentu svým zaručeným podpisem

c) Každý z podpisů se opatří časovým razítkem

d) Všechny orazítkované podpisy se seřadí do jedné posloupnosti, z které se vytvoří hash

e) Určí se fyzické osoby reprezentující podpisující strany

f) Je-li podpisujících stran více, označí se každá z nich identifikátorem (např. A, B, C, ...)

g) Každá z fyzických osob reprezentujících podpisující strany podepíše zaručeným elektronickým podpisem souhrnný hash vytvořený v bodě d) a připojí jej k podpisovanému dokumentu

h) Každá z fyzických osob reprezentujících podpisující stranu zašle dokument vzniklý v bodě g) ostatním fyzickým osobám reprezentujícím podpisující strany

2. Dokument podepisuje více fyzických osob nacházejících se na různých místech

a) Každá z podpisujících osob se označí identifikátorem (např. A, B, C, ...), přičemž osoba s identifikátorem A je osoba vlastnící nepodepsaný dokument (primární podpisovatel)

b) Primární podpisovatel vyhotoví svůj zaručený elektronický podpis dokumentu opatřený časovým razítkem

c) Podpis připojí nebo logicky spojí s podpisovaným dokumentem a zašle jej osobě B

d) Osoba B zkontroluje integritu přijatého dokumentu a platnost podpisu A, a pak připojí svůj podpis opatřený časovým razítkem

e) Dokument podepsaný dle písmene d) zašle další osobě, která vykoná analogický úkon jako popisuje bod d)

f) Poslední osoba zašle dokument opatřený všemi podpisy primárnímu podpisovateli

g) Primární podpisovatel spojí všechny podpisy do jedné posloupnosti, ze které vytvoří hash. Tento hash podepíše svým zaručeným elektronickým podpisem opatřeným časovým razítkem a podpis připojí k dokumentu

h) Elektronický dokument s podpisy dle bodu g) rozešle primární podpisovatel všem ostatním podpisovatelům

Další podrobnosti ohledně vícenásobného podpisu obsahuje dokument NBÚ *Formáty zaručených elektronických podpisov*, který si klade za cíl vytvoření jednoznačného, minimálního a závazného profilu pro poskytovatele certifikačních služeb, tvůrce aplikací a uživatele elektronického podpisu.

Dokument nedoporučuje používat ke kvalifikovaným vícenásobným podpisům zřetězené podpisy (atribut `countersignature` ve formátu CMS, viz část , nebo atribut `CounterSignature` ve formátu XML-Signature, viz část 3.1.2) a zavádí speciální formát uložení podpisu ZEP, jehož použití doporučuje.

7.1 Popis formátu ZEP

Dokument typu ZEP je ZIP archív s definovanou adresářovou strukturou a standardními názvy souborů a adresářů. Jména souborů se skládají z prefixu, určujícího obsah souboru, času vložení do archívu ve formátu `RRRRMMDDHHmmssZ` (je-li ve stejný čas vloženo více souborů, rozlišují se pořadovým číslem vloženým do jména souboru za čas) a koncovkou určující typ souboru.

Tabulka prefixů jmen souborů:

Typ	Popis	Příklad položky
D	Hlavní adresář, není povinný, ale zpřehledňuje kopírování obsahu mimo ZEP soubor	D20040129084128Z
S	Externí podpis	S20040129084128Z.p7s
F	Uzavírací (finální) podpis vícenásobného podpisu; je ve formátu „zaručený elektronický podpis s úplnou informací k ověření platnosti“, podpisuje jen soubory s koncovkou .p7s a .p7m, podpisy, které uzavírá, musejí obsahovat úplnou informaci k ověření platnosti i časovou značku	F20040129124128Z.p7m

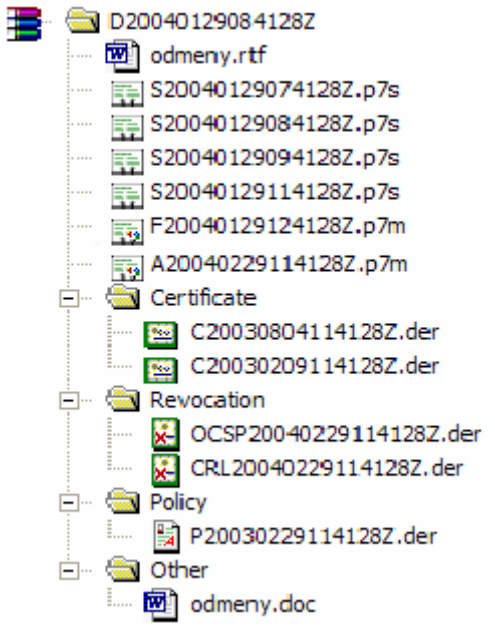
Typ	Popis	Příklad položky
A	Archivační podpis podepisuje soubory .p7s, .p7m, certifikáty, CRL nebo OCSP, podpisovou politiku a může podpisovat i další soubory. Podpisy podepisované pro archivaci musejí být ve formátu „zaručený elektronický podpis s úplnou informací k ověření platnosti“	A20040229114128Z.p7m
P	Podpisová politika	P20030229114128Z.der
C	Certifikát	C20030209114128Z.der
CRL	Seznam zneplatněných certifikátů	CRL20040229114128Z.der
OCSP	Stav platnosti certifikátu	OCSP20040229114128Z.der

Formát *.p7m uzavíracího a archivačního podpisu je textový formát kódovaný v UTF-8 a skládá se z těchto atributů:

```
FILE = < název souboru >CRLF
HASH (< algoritmus >:< OID algoritmu >) = < hash souboru - velká písmena >CRLF
NOTICE= < poznámka, například jméno archívního CD/DVD disku >CRLF
```

přičemž `CRLF` je znak (13) + znak (10)

Příklad ZEP archívu ukazuje následující obrázek.



Obr. 6: Příklad struktury ZEP archívu

8. Existující řešení pro vícenásobný elektronický podpis

V ČR jsou nabízena komerční i otevřená řešení, která realizují vícenásobné podepisování opakováním jednoduchého elektronického podpisu.

8.1 Řešení nCipher a Adobe Acrobat

Komerční řešení firem *nCipher* a *Adobe Acrobat* vychází z hardwarového podepisovacího zařízení - *DSE 200* (viz http://www.ncipher.com) pro podepisování formátu *PDF* od firmy Adobe, tzv. "pdf proof". Toto řešení umožní opakovaně podepsat dokument ve formátu *PDF*, a dále připojit i časové razítko. V ČR toto řešení nabízí firma *Deltax Systems a.s.* (*DS*).

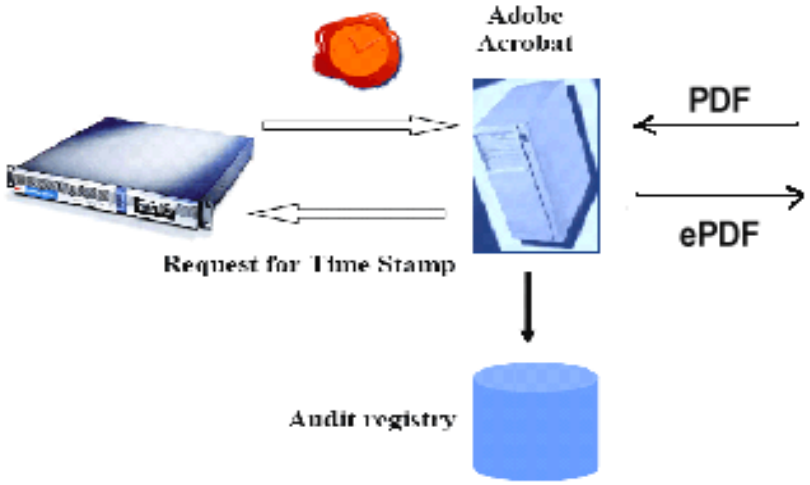
Technické řešení firmy *DS* vychází z přístupu k jednotlivým variantám řešení aplikací (např. e-fakturace, e-archivace), kde je potřeba opakovat jednoduchý el. podpis a tímto přepodepisováním vytvářet vícenásobný el. podpis, za spolupráce s akreditovanou certifikační autoritou I.CA (popř. jinou akreditovanou CA), která poskytne kvalifikovaný certifikát k veřejnému klíči držitele (pověřené zodpovědné osobě u zákazníka, která jako jediná má přístup k podepisovacím datům a má je pod výhradní kontrolou nebo systémový certifikát a kvalifikované časové razítko, a to dle různých aplikací řešení).

Certifikát s veřejnou částí klíče a ostatními charakteristickými údaji bude vystaven na www stránkách stránkách společnosti zákazníka.

Podstatnou částí řešení je podepisovací hardware - časový razítkovač firmy *N-cipher DSE-200* a software *Adobe Acrobat*. *DS*, jako systémový integrátor, napojí tento podsystém do IS zákazníka přes jeho rozhraní.

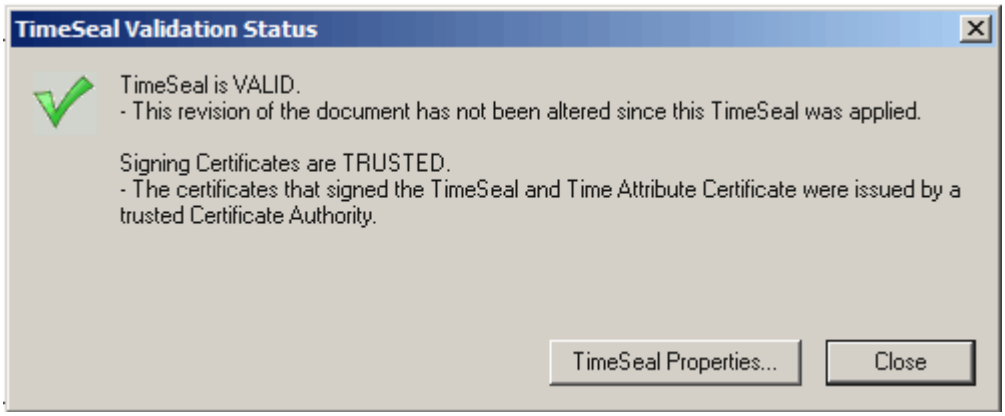
Při vnoření řešení do IS/ICT zákazníka může být vstupem pro řešení fronta dokumentů ve formátu např. *XML*. Na aplikačním serveru je nainstalován software provádějící transformaci *XML* na *PDF* a software přidávající prázdné podpisové pole k *PDF*. Na aplikačním serveru je rovněž nainstalována komponenta firmy *DELTAX* zabezpečující podepsání dokumentu na *DSE 200*. Tento server je propojen s *DSE 200*, který následně vytvoří časové razítko s elektronickým podpisem. Toto razítko je komponentou na centrálním serveru vloženo do dokumentu *PDF*. Privátní podepisující klíče jsou bezpečným způsobem uloženy na *DSE 200*. Certifikát tohoto podpisu spolu s veřejným klíčem je dostupný na webových stránkách vydavatele razítek.

Stručné globální schéma nabízeného řešení je následující:



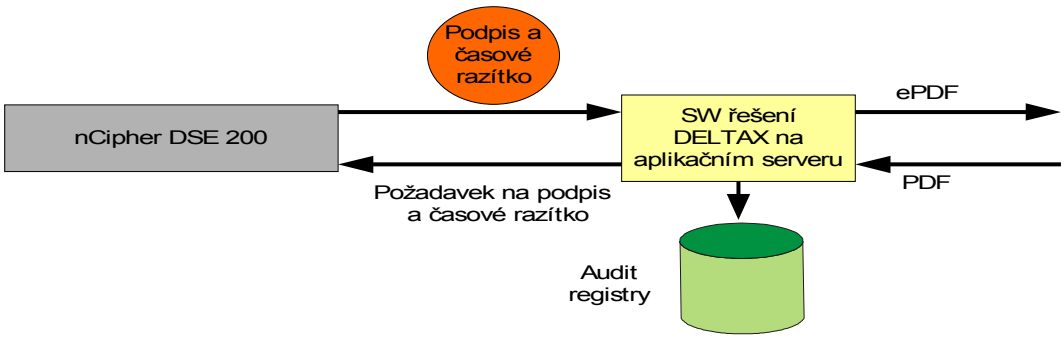
Obr. 7: Globálního schéma řešení

Výstupem je digitálně podepsaný dokument ve formátu *PDF* opatřený časovým razítkem. Příjemce může dokument zpracovat programem *Adobe Acrobat Reader* a ověřit jeho platnost.



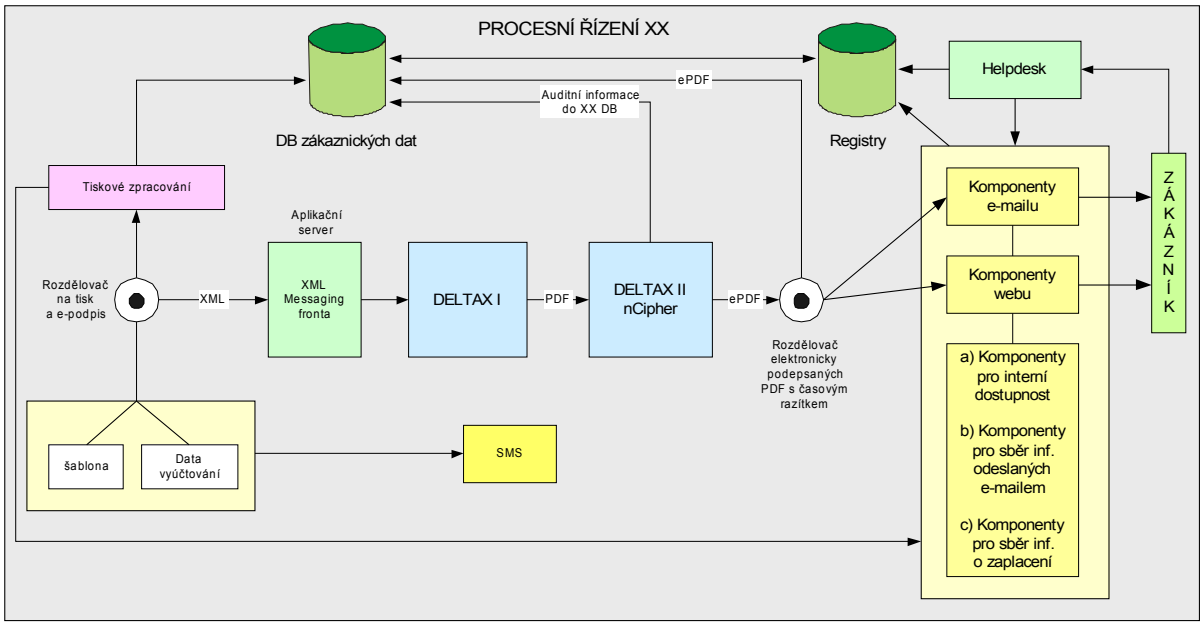
Obr. 8: Ověření platnosti podpisy pomocí Acrobat Reader v.6.0

Stručný popis řešení *DS* vytvoření *ePDF* dokumentu je následující:



Obr. 9: Globálního schéma vytvoření elektronické značky ePDF na PDF dokumentu

Schematické znázornění v blocích *DELTAX I, II* je následující např. v rámci modelového procesního řízení:



Obr. 10: Implementace řešení DELTAXu do IS společnosti

Tento podsystém je vnořen do části IS zákazníka (*XX*) a procesního řízení u *XX*, kde je již řešena problematika podepisování e-dokumentů klasickou cestou.

Vstupem *XX* pro řešení je fronta zpráv ve formátu *XML* např. výpisů z účtu těch zákazníků, kteří chtějí výpisy jako účetní doklady v elektronické formě (řešení může být samozřejmě aplikováno na libovolné e-dokumenty).

Na aplikačním serveru *XX* může být nainstalován software provádějící transformaci *XML* na *PDF* a software přidávající prázdné podpisové pole k *PDF*. V následujícím popíšeme příkladový modelový popis (centrální server, úložiště

otisků e-podepsaných dokumentů může být samozřejmě realizováno na existujícím HW společnosti *XX*). Model je koncipován k podepisování řádově až stotisíců e-dokumentů za hodinu.

Pro realizaci takovéhoto množství e-podpisů je na 4-procesorovém centrálním serveru (např. *IBM*) nainstalován software *Adobe Acrobat Document Server* a *Adobe Acrobat N-cipher Plugin*. Tento server je propojen s *DSE 200*, který opatřuje časovými razítky výše upravené *PDF* výpisy klientů ve formátu, které jsou podepsány zaručeným elektronickým podpisem. Certifikát tohoto podpisu je dostupný na webových stránkách v *XX*.

Předpokládá se, že certifikát a data k podepisování vlastní *XX* (buď vlastní certifikační autorita nebo zakoupení jednoho certifikátu u *I.CA* pro osobu, která je v *XX* s podepisovacím právem).

DSE přes rozhraní přijímá informace o čase z časového systému *XX* (nabídku je možno rozšířit o zaručený zdroj času pro tento podsystém na bázi produktu *nCipher*).

Celá důvěryhodnost elektronického podepsání a integrita dat výpisu včetně časové značky je založena na principu elektronického podpisu.

Při nahrání více podpisů lze razítkovačem *DSE 200* přepodepisovat dokumenty různými podepisujícími osobami. Klíčovou roli zde vždy hraje časové razítko, které garantuje validnost realizace el. podpisu v daném čase (el. podpis garantuje pouze integritu podepsaných dat a časové razítko jejich existenci v daném čase, proto je pro řadu aplikací nezbytné).

V této zde podepsané aplikaci pro *XX* se předpokládá využití hashovací funkce `SHA 1` , šifrovací funkce `E` šifry `RSA` s klíčem `K` 1024 bitů (je možné aplikovat `SHA 2`).

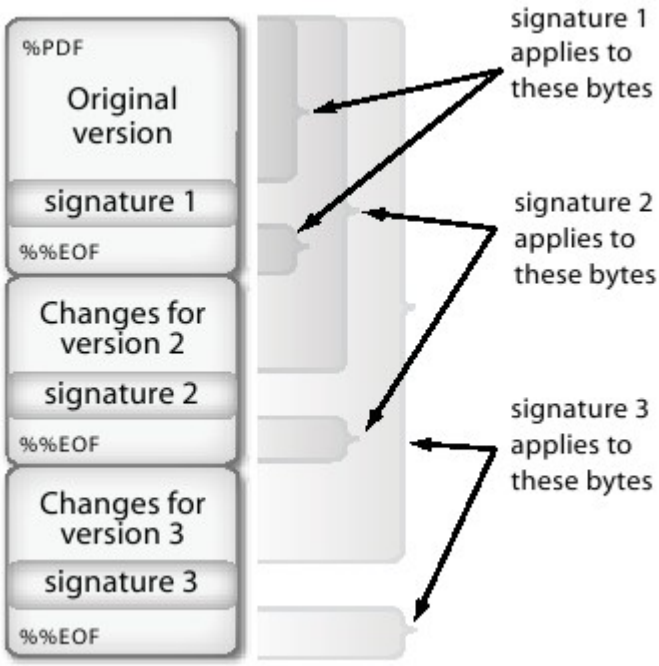
Hashovací funkce, kromě archivování celých podepsaných výpisů, jsou chronologicky automaticky ukládány na server do databáze *XX* a v daném časovém intervalu podepsány. To slouží pro důvěryhodnost systému a k auditní kontrole a ve schématu je tato část znázorněna jako *Audit registry*.

Nezbytné komponenty generující sestavy pro tuto aplikaci:

- komponenty pro přístup k databázi (J2EE platforma pro přístup),
- komponenty pro messaging a vytvoření fronty zpráv k transformaci a podpisu (J2EE),
- aplikační server na kterém je nainstalován software dodaný firmou *DELTAX*,
- komponenty pro řízení konfigurace (např. konfigurace databáze, apl. serveru),
- komponenty pro rozesílání e-mailu a využití www pro zobrazení faktur klientům s přístupovými právy,

- business komponenty na invoicing a accounting – programování a příprava rozhraní – předpokládá se připojení na existující komponenty,
- při výstupu komponenty pro rozesílání e-mailů, publikování na webu a ukládání do zákaznické databáze, včetně ukládání sufitních záznamů (chronologické řady otisků podepsaných faktur).

Schéma vkládání více podpisů do formátu PDF ukazuje obrázek.



Obr. 11: Schéma vkládání více podpisů do formátu PDF

8.1.1 Zdroje

http://www.adobe.com/devnet/acrobat/pdfs/DigitalSignaturesInPDF.pdf

http://www.adobe.com/devnet/acrobat/security.html

8.2 Řešení firmy AEC

Komerční řešení firmy AEC se nazývá *TrustPort eSign* a nabízí následující:

Vytváření a ověřování elektronických podpisů, používání časových razítek a provádění základních operací v rámci PKI.

Shrnutí hlavních vlastností TrustPort® eSign

- elektronické podepisování souborů/ověřování podpisů;

a) přidání (vytvoření) časového razítka k jakémukoliv podpisu.

b) šifrování/dešifrování souborů;

c) **vícenásobné podepisování stejného souboru několika uživateli (multisigning);**

d) šifrování dat pro více příjemců;

e) současné zašifrování a podepsání souboru;

f) nástroje pro správu soukromých podpisových klíčů, digitálních certifikátů (včetně jejich generování a žádostí o vydání certifikátu pro certifikační autoritu) a seznamů odvolaných certifikátů (CRL);

g) uložení soukromých klíčů a certifikátů v externích bezpečnostních hardwarových zařízeních (tokenech a čipových kartách);

h) možnost využití certifikátů uložených v úložištích operačního systému MS Windows;

i) možnost publikování lokálního úložiště – vytvoření centrálního úložiště certifikátů (LDAP serveru);

j) možnost připojení vzdáleného úložiště pomocí LDAP protokolu. Díky této vlastnosti lze například komunikovat s ActiveDirectory.

Podporované systémy

Microsoft Windows 98, Me, 2000, XP, NT 4.0 (nutný Service Pack 6).

8.2.1 Moduly aplikace TrustPort® eSign

PKI Storage Manager

Představuje základní grafické uživatelské rozhraní, které ve svých nabídkách sdružuje ovládání programu. Uživatel má k dispozici kompletní paletu nástrojů pro správu jednotlivých objektů v lokálních úložištích a externích hardwarových zařízeních, včetně prostředků pro generování nových klíčových párů a žádostí o vydání certifikátu u certifikační autority. K dispozici je také parametrické vyhledávání v jednotlivých úložištích (včetně LDAP).

TrustPort® eSign Configurator

Umožňuje nastavit základní vlastnosti programu (jako je výběr kryptografických algoritmů používaných k šifrování a vytváření elektronického podpisu, stanovení preferovaného lokálního úložiště nebo import licenčních klíčů).

Security Object Generator

Slouží ke generování nových klíčových párů. Celým procesem je uživatel veden podrobným průvodcem. V jeho průběhu lze nastavit druh použitého kryptografického algoritmu, hash algoritmu, délku klíče a účel použití generovaného klíčového páru. Uživatel má možnost zvolit mezi vytvořením self-signed certifikátu (je podepsán pouze pomocí soukromého klíče náležejícího k certifikátu) a žádosti o vydání digitálního certifikátu u poskytovatele certifikačních služeb (certificate request).

V případě generování klíčů do externích hardwarových zařízení se používá tzv. zástupný klíč, který objekt reprezentuje ve zvoleném lokálním úložišti. Tento zástupný klíč pak zjednodušuje práci s vlastním soukromým klíčem uloženým na hardwarovém zařízení.

Security Object Importer

Slouží k provedení importu objektů do existujících úložišť. Celým procesem importu, který je poměrně jednoduchý a sestává se pouze z výběru cílového úložiště, případně zadání potřebných hesel, je uživatel veden podrobným průvodcem.

Security Object Exporter

Slouží k exportu objektů z úložišť do souborů na pevný disk. Celým procesem je uživatel veden podrobným průvodcem. Export certifikátu včetně soukromého klíče lze provést pouze do souboru ve formátu PKCS#12, kde lze volitelně zahrnout všechny certifikáty v certifikační cestě (certifikáty certifikační autority) a obsah výsledného souboru je chráněn heslem. Při exportu certifikátu (bez soukromého klíče) lze zvolit mezi formátem X.509 (soubor CER, který obsahuje pouze certifikát) a PKCS#7 (lze zahrnout i kompletní certifikační cestu), a výsledný soubor není chráněn heslem.

Security Object Inspector

Slouží k zobrazení vlastností jednotlivých objektů. Lze jej spustit také pomocí kontextové nabídky v systému Windows.

8.2.2Závěr

Z hlediska naší analýzy je zajímavá možnost tohoto produktu AEC, realizovat vícenásobné podepisování. O způsobu realizace tohoto vícenásobného podpisování nejsou zveřejněny žádné bližší podrobnosti. Materiál je převzatý veřejně dostupný informační materiál firmy AEC, který nikterak nerozebíráme a nekomentujeme.

8.3 Microsoft Office

8.3.1 Microsoft Office 2000 – Microsoft Office 2003

Možnost elektronicky podepsat dokument nebo makra v dokumentu obsažená byla do aplikace Microsoft Office přidána v roce 2000. V tomto dokumentu se podrobně budeme zabývat jen nejnovější verzí Microsoft Office 2007, která možnosti podpisu výrazně vylepšila.

8.3.2Microsoft Office 2007

Nejnovější verze MS Office změnila proprietární binární formát ukládání na otevřený formát *Office Open XML*. Tento formát je podobný formátu ukládání dokumentů v kancelářském balíku OpenOffice.org, který používá *OpenDocument (ODF)* formát. Je to zip archív obsahující text dokumentu a další informace o jeho formátování ve formátu XML a dále obsahuje samostatně uložené obrázky a jiné vložené soubory.

Office 2007 nabízí dva způsoby podepsání dokumentu. První způsob (je k dispozici pro aplikace Word, Excel a PowerPoint) přidá k dokumentu digitální podpis, který není vidět v obsahu dokumentu. Tento podpis je možné si prohlédnout v menu a také ikona na stavovém panelu indikuje, že dokument je podepsaný. Použitý formát podpisu je XMLDsig.

Navíc je pro aplikace Word a Excel k dispozici rozšíření tohoto základního způsobu podpisu, které umožňuje do dokumentu vložit jednu či více *viditelných podpisových řádek*. Podpisová řádka při svém vzniku rezervuje místo pro budoucí podpis. Při jejím vložení může autor dokumentu blíže specifikovat osobu, která má dokument podepsat (jméno, titul, emailovou adresu). Autor dokumentu také může podpisovateli napsat nějaké dodatečné instrukce a může určit, zda podpisovatel ke svému podpisu může či nemůže vložit komentář, a zda se u podpisu zobrazí datum jeho vložení.

Podpisovatel zahájí podpis dokumentu dvojitým kliknutím myší na podpisovou řádku a vyplní v dialogu své jméno. Má-li se v dokumentu v místě podpisové řádky zobrazovat obrázek jeho podpisu, určí podpisovatel jeho umístění. Na Tablet PC také může svůj vlastnoruční podpis přímo vložit. V okamžiku přidání viditelné

reprezentace podpisu se k dokumentu zároveň přidá základní elektronický podpis a dokument se nastaví pouze ke čtení.

Uživatel si může v nastaveních elektronického podpisu ověřit, zda vidí všechny informace, které jsou podepsány. Není-li tomu tak, musí si ručně nastavit viditelné zobrazení všech informací, neexistuje k tomu funkce, která by vše nezobrazené zobrazila najednou.

Neplatné podpisy již nejsou automaticky odstraňovány, jak se dělo v dřívějších verzích MS Office.

Ověření podpisu

Při ověřování podpisu se mj. také kontrolují certifikáty v certifikační cestě oproti příslušným CRL (seznamům zneplatněných certifikátů). Pro tuto činnost používají aplikace MS Office nastavení aplikace Internet Explorer. Dle výchozího nastavení se z časových důvodů nový CRL nestahuje, ale toto nastavení je možné změnit. I u aplikace Outlook je možné nastavit povinné stahování CRL z internetu. Toto nastavení se provádí v registrech v položce

```
 HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\10.0\Outlook\Security\UseCRLChasing
```

8.3.3Microsoft Office InfoPath 2007

Aplikace InfoPath se poprvé objevila v kancelářském balíku Microsoft Office v roce 2003. Je zaměřena na návrh šablon formulářů a vyplňování formulářů. Formuláře nemusí být pouze statické, mohou také používat databázové zdroje nebo webové služby. Možným způsobem využití je například situace, kdy jsou všechny firemní formuláře uloženy na jednom serveru, odkud je možné si formulář stáhnout, vyplnit, a poté opět odeslat vyplněný na server.

Formát ukládání souborů je založen na XML. Šablona se skládá z archívu souborů, který obsahuje standardní XML soubory (XML, XML schéma, XSL transformace) a dále může obsahovat binární soubory jako obrázky nebo programový kód, který obstarává logiku formuláře. Vyplněná data formuláře se ukládají jako samostatný XML soubor, který obsahuje jako informaci odkaz na šablonu formuláře.

Možnost podepsat formulář elektronickým podpisem obsahuje aplikace od svého vzniku, ovšem nastavení související s elektronickým podpisem se dále vyvíjela a InfoPath 2007 umožňuje použít elektronický podpis těmito způsoby:

- Při návrhu šablony formuláře lze určit, zda uživatelé mohou formuláře elektronicky podepisovat

a) Šablonu formuláře je možné elektronicky podepsat

b) Podepsat lze celý formulář nebo jen vybrané části, které jsou určeny pomocí Xpath

c) Formulář může podepsat jeden uživatel či více uživatelů zároveň

d) Při vzniku šablony se určí, zda uživatel podepisující již podepsaný formulář (resp. část formuláře) vytváří podpis nezávislý na předchozích podpisech (co-sign), nebo zda podepisuje formulář (resp. část formuláře) včetně již existujících podpisů (counter-sign)

Formátem podpisu je XML Digital Signature.

Elektronický podpis formuláře v aplikaci InfoPath 2003 obsahuje jeden nedostatek
(viz http://lists.w3.org/Archives/Public/w3c-ietf-xmldsig/2003OctDec/0010.html), díky němuž je nejisté, zda platí podmínka, že podpisovatel vidí to, co podepisuje. Podpisovatel totiž vidí šablonu formuláře (označení polí) spolu s daty, která vyplnil, podepisuje však pouze XML soubor obsahující vyplněná data. Takže je např. možné v šabloně formuláře následně změnit text u formulářových polí nebo připsat nějaká závazná prohlášení, aniž by to mělo vliv na platnost podpisu formuláře.

8.3.4Zdroje

http://office.microsoft.com/

http://msdn2.microsoft.com/

8.4 OpenOffice.org

Formátem dokumentů kancelářského balíku *OpenOffice.org* je *OASIS OpenDocument* formát (ODF). Tento formát je obdobný jako formát *Office Open XML*, který používá *Microsoft Office 2007*. Je to zip archív obsahující text dokumentu a další informace o jeho formátování ve formátu XML a dále obsahuje samostatně uložené obrázky a jiné vložené binární soubory.

- Kancelářský balík OpenOffice.org umožňuje jen základní používání elektronických podpisů. Dokument lze podepsat pouze celý, není možné určit k podpisu menší podmnožinu dokumentu.

a) Jedinou výjimkou z předchozího bodu je možnost podepsat samostatně makra obsažená v dokumentu.

b) Dokument může podepsat více osob, přičemž každý z podpisovatelů podepisuje pouze dokument, nikoli již přiložené podpisy (nezávislé podpisy).

c) Byl-li obsah dokumentu změněn a podpisy tím pozbyly platnosti, jsou při uložení dokumentu odstraněny.

d) Aplikace ověřuje i platnost certifikátů, jimiž je dokument podepsán.

Formátem podpisu je *XML Digital Signature*, a to *detached* varianta, při které jsou podpisy uloženy v jiném souboru než podepisované dokumenty, na které se odkazuje relativními adresami. Podpisy jsou uloženy v souboru *META-INF/documentsignatures.xml* v archivu obsahujícím všechny soubory, které tvoří celý dokument. Úložištěm certifikátů se aplikace nezabývá, na operačním systému *Microsoft Windows* používá nativní MS Crypto API, na operačních systémech Linux a Solaris používá úložiště aplikace Mozilla/NSS.

Ukázka podpisu dokumentu:

```
<document-signatures
        xmlns="http://openoffice.org/2004/documentsignatures">
      <Signature xmlns="http://www.w3.org/2000/09/xmldsig#"
                 Id="ID_00e0009800bc007800a90093001100db00b5005c00
00000e00a6008c00620059">
            <SignedInfo>
                  <CanonicalizationMethod Algorithm="..."/>
                  <SignatureMethod Algorithm="..."/>
                  <Reference URI="content.xml">...</Reference>
                  <Reference URI="styles.xml">...</Reference>
                  <Reference URI="meta.xml">...</Reference>
                  <Reference URI="settings.xml">...</Reference>
                  <Reference
                        URI="#ID_00e0009800c000ec00a90093001100db0
09500c50000000e00a6008c00620059">...</Reference>
            </SignedInfo>

            <SignatureValue>...</SignatureValue>

            <KeyInfo>
                  <X509Data>
                        <X509IssuerSerial>
                              <X509IssuerName>...</X509IssuerName>
                              <X509SerialNumber></X509SerialNumber>
                        </X509IssuerSerial>
                        <X509Certificate>...</X509Certificate>
                  </X509Data>
            </KeyInfo>

            <Object>
                  <SignatureProperties>
                        <SignatureProperty
                              Id="ID_00e0009800c000ec00a9009300110
0db009500c50000000e00a6008c00620059"
                              Target="#ID_00e0009800bc007800a90093
001100db00b5005c0000000e00a6008c00620059">
      <dc:date xmlns:dc="http://purl.org/dc/elements/1.1/">
            2007-01-21T22:10:53
```

```
      </dc:date>
                        </SignatureProperty>
                    </SignatureProperties>
                </Object>
      </Signature>
</document-signatures>
```

8.4.1 Zdroje

http://marketing.openoffice.org/ooocon2004/presentations/friday/timmermann_digital_signatures.pdf

8.5 602 Software - 602XML Filler (verze 2)

Aplikace *602XML Filler* je aplikace určená k vyplňování formulářů podle šablon navržených v aplikaci *602XML Form Publishing*. Formuláře a jejich šablony jsou ve formátu XML. Tato aplikace je určena pouze pro operační systém Windows a umožňuje používat certifikáty nakonfigurované s použitím „Nastavení internetu“.

K podpisu je standardně využíván formát *XML Signature*. Jako alternativu je možné zvolit formát podpisu *PKCS#7* verze 1.5 (*RFC 2315*). Typ podpisu určuje tvůrce šablony. Obsah *PKCS#7* objektu, reprezentujícího datovou větu opatřenou elektronickým podpisem, splňuje následující podmínky:

a) je typu "`signedData`",

b) obsahuje podepsaná data (nikoliv reference),

c) obsahuje vložený certifikát podepisujícího.

602XML Filler umožňuje vícenásobně elektronicky podepsat, popř. přidat podpis k již podepsanému vyplňovanému formuláři. Tvůrce šablony formuláře může určit, zda se mají formuláře vždy podepisovat, nikdy nepodepisovat, nebo je-li podpis formuláře volitelný dle přání uživatele vyplňujícího formulář.

Aplikace umí zobrazit podpisy, připojené k formuláři, a informaci, zda byl formulář od přidání podpisu změněn (tedy jsou připojené podpisy neplatné). Platností certifikátu, jímž je podpis realizován, se aplikace nezabývá, k ověření jeho platnosti musí tedy uživatel použít jiné prostředky. Aplikace také neumožňuje podpis odstranit.

Elektronický podpis se k formuláři přidá volbou akce „Uložit s podpisem“. Uživatel vybere jméno souboru a dále jeden certifikát, kterým chce podpis realizovat. Po připojení podpisu ovšem tento podpis nepřibude do seznamu podpisů formuláře, aby se tam zobrazil, je třeba dokument nově otevřít. Při přidávání více podpisů se několikrát zopakuje akce „Uložit s podpisem“, což není příliš pohodlné.

Při změně položek v podepsaném formuláři se zobrazí u informací o zabezpečení údaj, že byl dokument změněn, ale seznam podpisů již neplatné podpisy obsahuje. Neplatné podpisy jsou sice při ukládání odstraněny a nejsou uloženy, ale v seznamu podpisů jsou stále uvedeny, ačkoli je již odstraněna informace o jejich neplatnosti. Aby uživatel skutečně viděl aktuální informace o obsahu souboru, musí editovaný soubor znovu otevřít.

Podrobnosti formátu podpisu

Jak již je uvedeno výše, formátem podpisu je *XML Signature*, a to *enveloping* varianta (podpisovaná data jsou potomkem elementu `Signature` obsahujícího podpis). Podpisy se *postupně zaobalují*. Při přidání podpisu k formuláři se kořenový element formuláře vloží do elementu `Object`, kterému se přiřadí jednoznačný identifikátor. Tento element `Object` se pak vloží do elementu `Signature` obsahujícího přidaný podpis. Přidaným podpisem je podepsán element `Object` v něm vnořený. Šablona formuláře a vyplněná data jsou obsažena v nejhlouběji vnořeném elementu `Signature`. Takto vypadá ukázka podpisu:

```
<?xml version="1.0"?>
<dsig:Signature Id="_8856448"
               xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">

     <dsig:SignedInfo>
          <dsig:CanonicalizationMethod
               Algorithm="..."/>
          <dsig:SignatureMethod
        Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>

          <dsig:Reference URI="#_8856453">
               <dsig:Transforms>...</dsig:Transforms>
               <dsig:DigestMethod
          Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
               <dsig:DigestValue>...</dsig:DigestValue>
          </dsig:Reference>
     </dsig:SignedInfo>

     <dsig:SignatureValue>...</dsig:SignatureValue>

     <dsig:KeyInfo>...</dsig:KeyInfo>

     <dsig:Object Id="_8856453" MimeType="text/xml">
          <dsig:Signature Id="_7058307"
               xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
             <!-- podepisovaný formulář -->
          </dsig:Signature>
          <dsig:SignatureProperties>
               <dsig:SignatureProperty Target="#_8856448">
                 <fm:systeminfo datetime="2007-01-21T17:09:42Z"
                     xmlns:fm="http://software602.cz/forms"/>
               </dsig:SignatureProperty>
          </dsig:SignatureProperties>
```

```
      </dsig:Object>
</dsig:Signature>
```

Závěr

Aplikace 602XML Filler sice elektronický podpis umožňuje, ale uživatelsky nepohodlným způsobem. Dokumentaci týkající se elektronického podpisu lze vytknout snad až přílišnou stručnost.

8.6 Srovnání

Aplikace	*Formát podpisu*	*Typ podpisu*	*Ověření platnosti*	*Operační systém*
MS Office 2007	XML Signature	Nezávislé podpisy Zřetězené podpisy Podpis vybrané části	ano	Windows
OpenOffice.org	XML Signature	Nezávislé podpisy	ano	Windows Linux Solaris Mac OS X FreeBSD
602XML Filler	XML Signature CMS	Postupně zaobalující podpisy	Ověřuje pouze, zda podpis podepisuje formulář, neověřuje platnost certifikátů	Windows
Adobe Acrobat	Vlastní otevřený formát speciální pro pdf	Postupně zaobalující podpisy	ano	Windows Mac OS X
TrustPort eSign	CMS	nezjištěno	ano	Windows

9. Závěry a doporučení

Napřed shrneme na základě provedeného rozboru, jaké možnosti přístupu k vícenásobnému elektronickému postupu existují a jaké existují možnosti používaného formátu. Potom uvedeme kritéria, podle kterých budeme tyto možnosti posuzovat, a nakonec popíšeme výsledné hodnocení.

Možnosti přístupů k vícenásobnému elektronickému podpisu

a) Skládáním jednoduchých podpisů (viz oddíl 5.1, hlavní myšlenky uvádíme znovu zde)
   - nezávislé podpisy – jedná se o případ, kdy k danému dokumentu D každý podpisovatel (tj. první, druhý až n-tý) vytvoří svůj podpis, tím vzniknou podpisy P_1, P_2, až P_n téhož dokumentu D a tyto podpisy spolu s dokumentem vytvoří jeden celek tzv. vícenásobně podepsaný dokument $VPD = (D + P_1 + P_2 + .. + P_n)$
   - postupně zaobalující podpisy – jedná se o případ, kdy první podpisovatel připojí k dokumentu D svůj podpis P_1, vznikne nový dokument $D_2 = (D + P_1)$, druhý podpisovatel podepíše dokument D_2 svým podpisem P_2 a vytvoří nový dokument $D_3 = (D_2 + P_2)$, třetí podpisovatel pak analogicky podepíše dokument D_3 atd. Vznikne tím relativně složitější struktura než v případě nezávislých podpisů charakterizovaná tím, že každý podpisovatel vlastně podepisuje jiný dokument.

b) Pokročilejší algoritmy využívající složitější generování klíčů – jedná se o případy popsané ve čtvrté a páté kapitole

Možnosti formátu

a) *Cryptographic Message Syntax* (*CMS*) popsaný v kapitole 3.1.1 – binární formát

b) *XML Signature* popsaný v kapitole 3.1.2, zejména ve variantě *XAdES-C* – založený na XML

Kritéria použitá při vyhodnocení

1. **Opora v ZoEP** – pouze elektronický podpis popisovaný v ZoEP může plnit svou úlohu v oblasti státní správy a pouze tento podpis může být relevantní při soudním přezkoumání případných sporů

2. **Založenost na standardech** – pokud je možné založit řešení na standardu, je vhodné preferovat co nejvíce rozšířený standard

3. Možnost **využití** existující **infrastruktury** kvalifikovaných certifikátů vydávaných akreditovanými poskytovateli certifikačních služeb – bez využití infrastruktury existujících poskytovatelů certifikačních služeb by praktické využití navrhované aplikace nebylo vůbec možné, a také není možné vázat navrhovanou aplikaci na případné rozšíření služeb stávajících poskytovatelů nebo na vznik nových poskytovatelů

4. **Jednoduchost** – tato podmínka vychází ze zadání projektu a je vhodné ji rozšířit také o hledisko určité universality možného použití aplikace

Vyhodnocení možností pro návrh aplikace z hlediska výběru typu podpisu

- Hledisko opory v ZoEP a opory v existující infrastruktuře jednoznačně vylučuje možnost použít pokročilejší algoritmy využívající složitější generování klíčů, neboť:
  - Tyto druhy podpisů nejsou podpisy dle ZoEP, a tedy nemají legislativní podporu – jejich použití by nebylo soudně přezkoumatelné a tyto podpisy by nebyly akceptovatelné v oblasti státní správy. ZoEP totiž stanoví, že pro účely elektronického podpisu je vytvořen jeden veřejný a jeden soukromý klíč. Přitom systémy vícenásobného elektronického podpisu popsané v kapitole 5 (mimo část 5.1) vyžadují vytváření soukromých a veřejných klíčů způsobem odlišným od způsobu stanoveného v ZoEP.
  - Zatím, pokud je nám známo, žádný existující poskytovatel certifikačních služeb takové podpisy nepodporuje (také z důvodů neexistující legislativní podpory)
- Zbývají tedy dvě možnosti – nezávislé podpisy a postupně zaobalující podpisy. Z těchto dvou možností se nám jeví jako podstatně výhodnější použití možnosti nezávislých podpisů. Vedou nás k tomu následující důvody:
  - Kriterium jednoduchosti – varianta postupně zaobalujících podpisů je pro uživatele méně přehledná a protokol vzniku takto podepsaného dokumentu je komplikovaný.
  - Ve variantě nezávislých podpisů všichni podepisující podepisují tentýž dokument, zatímco ve variantě postupně zaobalujících podpisů sice jde o jednotlivé podpisy podle ZoEP, ale podpisovatelé nepodepisují stejný původní dokument – např. druhý podpisovatel nepodepisuje dokument D, ale dokument (D + P1), třetí podpisovatel podepisuje dokument ((D + P1) + P2), čtvrtý dokument (((D + P1) + P2) + P3) atd.
  - Případné poškození některého podpisu ve variantě nezávislých podpisů ostatní podpisy neovlivní, zatímco ve variantě podpisů postupně zaobalujících poškození či odstranění některého podpisu by způsobilo nemožnost ověření podpisů následných.
  - Varianta nezávislých podpisů má širší možnosti využití a je tedy universálnější.

Vyhodnocení možností pro návrh aplikace z hlediska výběru formátu

- Obě varianty – CMS (Cryptographic Message Syntax) a XML Signature jsou standardizovány
- Následující rozdíly hovoří ve prospěch XML Signature:
  - Formát XML Signature je přímo čitelný v běžně dostupných internetových prohlížečích nebo textových editorech – zatímco formát CMS je binární a bez aplikace je nečitelný
  - Formát XML Signature umožňuje úplnou čitelnost v případě, že podepisovaný dokument je ve formátu XML
  - Formát XML Signature je plně rozšiřitelný a tím umožní pokrýt více případů použití – formát CMS tuto vlastnost rozšiřitelnosti (typickou pro XML) nemá
  - Formát XML Signature umožňuje používat také podepisování vzdáleně dostupných dokumentů určených jejich URL, což je může být výhodné
  - Formát XML Signature je vhodný pro státní správu vzhledem ke stále se rozšiřujícímu použití XML dokumentů ve státní správě
- Podpisy ve formátu CMS představují menší objem dat. To však není z hlediska cílů projektu příliš významné. Navíc XML lze velmi účinně komprimovat jak běžně dostupnými všeobecnými kompresními algoritmy, tak algoritmy konstruovanými speciálně pro XML.

Závěry a doporučení

a) Realizovat vícenásobný podpis skládáním podpisů jednonásobných

b) Použít variantu nezávislých podpisů

c) Použít formát XML Signature

10.Chronologický přehled literatury k jednotlivým druhům elektronického podpisu

10.1Přehled literatury ke klasickému elektronickému podpisu

1976

- W. Diffie, and M.E. Hellman. New directions in cryptography. *IEEE Trans. on Inform. Theory*, 22: 644-654, 1976.

1978

- R. L. Rivest , A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2): 120-126, Feb. 1978.
- R.C. Merkle. Secure communications over insecure channels. *Communications of the ACM*, 21(4): pp. 294-299, April 1978.
- M. Rabin. Digitalized signatures. In: *Foundations of Secure Computations*, edited by R. DeMillo, D. Dobkin, A. Jones, and R. Lipton. Academic Press, 1978, pp. 155-168.

1979

- M. Rabin. Digitalized signatures and public-key functions as intractable as factorization. In: *MIT/LCS/TR-212*, MIT Technical Memo, 1979.

1982

- S. Goldwasser, and S. Micali. Probabilistic encryption & how to play mental poker keeping secret all partial information. In: *STOC'82*, pp. 365-377. ACM Press, 1982.

1983

- S. Goldwasser, S. Micali, and A. Yao. Strong signature schemes. In: *STOC'83*, pp. 431-439. ACM Press, 1983.

1984

- D.E. Denning. Digital signatures with RSA and other public-key cryptosystems. *Communications of the ACM*, 27(4), pp. 388-392, April 1984.

- T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In: *Crypto'84, LNCS 196*, pp. 10–18. Springer-Verlag, 1985.
- S. Goldwasser, S. Micali, and R. Rivest. A "paradoxical" solution to the signature problem. In: *Proc. of the 25th FOCS*, pp. 441–448. New York: IEEE, 1984.
- H. Ong, C. P. Schnorr, and A. Shamir. An efficient signature scheme based on quadratic equations. In: *STOC'84*, pp. 208-216. ACM Press, 1984.

1985

- T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, IT–31(4): 469–472. July 1985.

1986

- A. Fiat and A. Shamir. How to prove yourself: practical solutions of identification and signature problems. In: *Crypto '86, LNCS 263*, pp. 186–194. Springer-Verlag, Berlin, 1987.

1988

- S. Goldwasser , S. Micali, and R. L. Rivest. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM Journal on Computing*, 17(2): 281-308, April 1988.
- L.C. Guillou, J.-J. Quisquater. A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory. In: *Eurocrypt'88, LNCS 330*, pp. 123–128. Springer-Verlag, 1988.
- L. Guillou, and J.-J. Quisquater. A paradoxical identity-based signature scheme resulting from zero-knowledge. In: *Crypto'88, LNCS 403*, pp. 216-231. Springer, Berlin, 1989.

1989

- C.P. Schnorr. Efficient identification and signatures for smart cards. In: *Crypto'89, LNCS 435*, 239-252. Springer-Verlag, 1990.

1990

- David Chaum and Sandra Roijakkers. Unconditionally secure digital signatures. In: *Crypto'90*, LNCS 537, pp. 206-214. Springer-Verlag, 1991.

1991

- C.P. Schnorr. Efficient signature generation by smart cards. *Journal of Cryptology*, 4(3): 161-174, 1991.

1992

- M. Bellare, and S. Micali. How to sign given any trapdoor permutation. *Journal of the ACM*, 39(1): pp. 214-233, Jan. 1992.
- T. Okamoto. Provably secure and practical identification schemes and corresponding signature schemes. In: *Crypto'92, LNCS 740*, pp. 31–53. Springer-Verlag, 1993.

1993

- M. Bellare, and P. Rogaway. Random oracles are practical: a paradigm for designing efficient protocols. In: *Proceedings of the 1st ACM conference on Computer and communications Security*, pp. 62-73. ACM press, 1993.

1994

- C. Dwork, and M. Naor. An efficient existentially unforegeable signature scheme and its applications. In: *Crypto'94, LNCS 839*, pp. 234-246. Springer-Verlag, 1994. An modified version appeared in Journal of Cryptology, 1998.

1995

- P. Bégiun and J.-J. Quisquater. Fast Server-Aided RSA Signatures Secure Against Active Attacks. In: *CRYPTO'95, LNCS 963*, pp. 57-69. Springer-Verlag, 1995.
- R. Cramer and I. Damgård. Escure Signature Schemes based on Interactive Protocols. In: *CRYPTO'95, LNCS 963*, pp. 297-310. Springer-Verlag, 1995.
- C. H. Lim and P. J. Lee. Server (Prover/Signer)-Aided Verification of Identity Proofs and Signatures. In: *EUROCRYPT'95, LNCS 921*, pp. 64-78. Springer-Verlag, 1995.
- C. H. Lim and P. J. Lee. Security and Performance of Server-Aided RSA Computation Protocols. In: *CRYPTO'95, LNCS 963*, pp. 70-83. Springer-Verlag, 1995.

1996

- R. Cramer and I. Damgard. New generation of secure and practical RSA-based signatures. In: *Crypto'96, LNCS 1109*, pp. 173-185. Springer-Verlag, 1996.
- Birgit Pfitzmann and Michael Waidner: Information-Theoretic Pseudosignatures and Byzantine Agreement for t = n/3. *IBM Research Report RZ 2882 (#90830) 11/18/96*, IBM Research Division, Zürich, Nov. 1996.
- D. Pointcheval, and J. Stern. Security proofs for signature schemes. In: *Eurocrypt'96, LNCS 1070*, pp. 387–398. Springer-Verlag, 1996.

1997

- D. Pointcheval, and J. Stern. New blind signatures equivalent to factorization (extended abstract)
  In *Proceedings of the 4th ACM conference on Computer and Communications Security,* pp. 92-99. ACM press, 1997.
- A. Herzberg, M. Jakobsson, S. Jarecki, H. Krawczyk, and M. Yung. Proactive public key and signature systems. In *Proceedings of the 4th ACM conference on Computer and Communications Security,* pp.100-110. ACM press, 1997.

1998

- C. Dwork, and M. Naor. An efficient existentially unforgeable signature scheme and its applications. *Journal of Cryptology*, 11(3): 187-208, 1998. An earlier version appeared in Crypto'94.

1999

- J.-S. Coron, D. Naccache, and J.P. Stern. On the Security of RSA Padding. In: *CRYPTO 1999, LNCS 1666*, pp. 1-18. Springer-Verlag, 1999.
- R. Cramer, and V. Shoup. Signature schemes based on the strong RSA assumption. In: *Proceedings of the 6th ACM conference on Computer and Communications Security*, pp. 46-51. ACM press, 1999.
- R. Gennaro, S. Halevi, and T. Rabin. Secure hash-and-sign signatures without the random oracle. In: *Eurocrypt'99, LNCS 1592*, pp. 123-139. Springer-Verlag, 1999.
- S. Micali and L. Reyzin. Improving the Exact Security of Fiat-Shamir Signature Schemes. In: *Secure Networking - CQRE (Secure) '99, LNCS 1740*, 167-182. Springer-Verlag, 1999.
- G. Poupard, and J. Stern. On the fly signatures based on factoring. In: *Proceedings of the 6th ACM conference on Computer and Communications Security*, pp. 37-45. ACM press, 1999.

2000

- J.-S. Coron. On the Exact Security of Full Domain Hash. In: *CRYPTO 2000, LNCS 1880*, pp. 229-235. Springer-Verlag, 2000.
- J.Souček,J.Hrubý,P.Vondruška Certifikační autorita , 2000.
- J.-S. Coron and D. Naccache. Security Analysis of the Gennaro-Halevi-Rabin Signature Scheme. In: *EUROCRYPT 2000, LNCS 1807*, pp. 91-101. Springer-Verlag, 2000.
- J.-S. Coron, F. Koeune, and D. Naccache. From Fixed-Length to Arbitrary-Length RSA Padding Schemes. In: *ASIACRYPT 2000, LNCS 1976*, pp. 90-96. Springer-Verlag, 2000.

- G. Durfee and P. Q. Nguyen. Cryptanalysis of the RSA Schemes with Short Secret Exponent from Asiacrypt '99. In: *ASIACRYPT 2000, LNCS 1976*, pp. 14-29. Springer-Verlag, 2000.
- G. Hanaoka, J, Shikata, Y. Zheng, and H. Imai. Unconditionally Secure Digital Signature Schemes Admitting Transferability. In: *ASIACRYPT 2000, LNCS 1976*, pp. 130-142. Springer-Verlag, 2000.
- D. Pointcheval, and J. Stern. Security arguments for digital signatures and blind signatures. *Journal of Cryptology*, 13(3): 361-396, 2000.
- C.-P. Schnorr and M.s Jakobsson. Security of Signed ElGamal Encryption. In: *ASIACRYPT 2000, LNCS 1976*, pp. 73-89. Springer-Verlag, 2000.
- A. Young and M. Yung. Towards Signature-Only Signature Schemes. In: *ASIACRYPT 2000, LNCS 1976*, pp. 97-115. Springer-Verlag, 2000.

2001

- M. Bellare, M. Fischlin, S. Goldwasser, and S. Micali. Identification Protocols Secure against Reset Attacks. In: *EUROCRYPT 2001, LNCS 2045*, pp. 495-511. Springer-Verlag, 2001.
- D. Boneh, B. Lynn, and H. Shacham. Short signatures from the Weil pairing. In: *Asiacrypt 2001, LNCS 2248*, pp.514-532. Springer-Verlag, 2001.
- E. Brier, C. Clavier, J.-S. Coron, and D. Naccache. Cryptanalysis of RSA Signatures with Fixed-Pattern Padding. In: *CRYPTO 2001, LNCS 2139*, pp. 433-439. Springer-Verlag, 2001.
- N. Courtois, M. Finiasz, and N. Sendrier. How to Achieve a McEliece-Based Digital Signature Scheme. In: *ASIACRYPT 2001, LNCS 2248*, pp. 157-174. Springer-Verlag, 2001.
- C. Gentry, J. Jonsson, J. Stern, and M. Szydlo. Cryptanalysis of the NTRU Signature Scheme (NSS) from Eurocrypt 2001. In: *ASIACRYPT 2001, LNCS 2248*, pp. 1-20. Springer-Verlag, 2001.
- D. Naccache, D. Pointcheval, and J. Stern. Twin signatures: an alternative to the hash-and-sign paradigm. In: *Proceedings of the 8th ACM conference on Computer and Communications Security (CCS 2001)*, pp. 20-27. ACM press, 2001.
- P. Q. Nguyen and I. Shparlinski. On the Insecurity of a Server-Aided RSA Protocol. In: *ASIACRYPT 2001, LNCS 2248*, pp. 21-35. Springer-Verlag, 2001.
- T. Okamoto and D. Pointcheval. The Gap-Problems: A New Class of Problems for the Security of Cryptographic Schemes. In: *Public Key Cryptography (PKC 2001), LNCS 1992*, pp. 104-118. Springer-Verlag, 2001.
- A. Shamir and Y. Tauman. Improved Online/Offline Signature Schemes. In: *CRYPTO 2001, LNCS 2139*, pp. 355-367. Springer-Verlag, 2001.

2002

- M. Abdalla, J. H. An, M. Bellare, and C. Namprempre. From Identification to Signatures via the Fiat-Shamir Transform: Minimizing Assumptions for Security and Forward-Security. In: *EUROCRYPT 2002, LNCS 2332*, pp. 418-433. Springer-Verlag, 2002.

- J. H. An, Y. Dodis, and T. Rabin. On the Security of Joint Signature and Encryption. In: *EUROCRYPT 2002, LNCS 2332*, pp. 83-107. Springer-Verlag, 2002.
- M. Bellare and A. Palacio. GQ and Schnorr Identification Schemes: Proofs of Security against Impersonation under Active and Concurrent Attacks. In: *CRYPTO 2002, LNCS 2442*, pp. 162-177. Springer-Verlag, 2002.
- M. Bellare and G. Neven. Transitive Signatures Based on Factoring and RSA. In: *ASIACRYPT 2002, LNCS 2501*, pp. 397-414. Springer-Verlag, 2002. Full version is available at http://eprint.iacr.org/2004/215/.
- J. Camenisch and A. Lysyanskaya. A Signature Scheme with Efficient Protocols. *Security in Communication Networks (SCN 2002), LNCS 2576*, pp. 268-289. Springer-Verlag, 2002.
- J.-S. Coron, M. Joye, D. Naccache, and P. Paillier. Universal Padding Schemes for RSA. In: *CRYPTO 2002, LNCS 2442*, pp. 226-241. Springer-Verlag, 2002.
- J.-S. Coron. Security Proof for Partial-Domain Hash Signature Schemes. In: *CRYPTO 2002, LNCS 2442*, pp. 613-626. Springer-Verlag, 2002.
- J.-S. Coron. Optimal Security Proofs for PSS and Other Signature Schemes. In: *EUROCRYPT 2002, LNCS 2332*, pp. 272-287. Springer-Verlag, 2002.
- I. Damgård and M. Koprowski. Generic Lower Bounds for Root Extraction and Signature Schemes in General Groups. In: *EUROCRYPT 2002, LNCS 2332*, pp. 256-271. Springer-Verlag, 2002.
- J. A. Garay and M. Jakobsson. Time release of standard digital signatures (Extended Abstract). In: *Financial Cryptography (FC 2002), LNCS ????*, pp. ??-??. Springer-Verlag, 2003.
- C. Gentry and M. Szydlo. Cryptanalysis of the Revised NTRU Signature Scheme. In: *EUROCRYPT 2002, LNCS 2332*, pp. 299-320. Springer-Verlag, 2002.
- L. Granboulan. Short Signatures in the Random Oracle Model. In: *ASIACRYPT 2002, LNCS 2501*, pp. 364-378. Springer-Verlag, 2002.
- L. Granboulan. How to Repair ESIGN. In: *Security in Communication Networks (SCN 2002), LNCS 2576*, pp. 234-240. Springer-Verlag, 2002.
- F. Hess. Exponent group signature schemes and efficient identity based signature schemes based on pairings. *Cryptology ePrint Archive*, Report 2002/012. Available at http://eprint.iacr.org/2002/012/.
- A. Lysyanskaya. Unique Signatures and Verifiable Random Functions from the DH-DDH Separation. In: *CRYPTO 2002, LNCS 2442*, pp. 597-612. Springer-Verlag, 2002.
- T. Malkin, D. Micciancio, and S. K. Miner. Efficient Generic Forward-Secure Signatures with an Unbounded Number Of Time Periods. In: *EUROCRYPT 2002, LNCS 2332*, pp. 400-417. Springer-Verlag, 2002.
- S. Micali and L. Reyzin. Improving the Exact Security of Digital Signature Schemes. *Journal of Cryptology*, 2002, 15(1): 1-18.
- J. Shikata, G. Hanaoka, Y. Zheng, and H. Imai. Security Notions for Unconditionally Secure Signature Schemes. In: *EUROCRYPT 2002, LNCS 2332*, pp. 434-449. Springer-Verlag, 2002.
- J. Stern, D. Pointcheval, J. Malone-Lee, and N.P. Smart. Flaws in Applying Proof Methodologies to Signature Schemes. In: *CRYPTO 2002, LNCS 2442*, pp. 93-110. Springer-Verlag, 2002.

2003

- Michael Backes, Birgit Pfitzmann, Michael Waidner. Reactively Secure Signature Schemes. In: *Information Security* (*ISC 2003*), LNCS 2851, pp. 84-95. Springer-Verlag, 2003.
- D. Boneh, C. Gentry, B. Lynn, and H. Shacham. Aggregate and Verifiably Encrypted Signatures from Bilinear Maps. In: *EUROCRYPT 2003, LNCS 2656*, pp. 416-432. Springer-Verlag, 2003.
- N. Courtois, M. Daum, and P. Felke. On the Security of HFE, HFEv- and Quartz. In: *Public Key Cryptography - PKC 2003, LNCS 2567*, pp. 337-350. Springer-Verlag, 2003.
- N. Courtois. Generic Attacks and the Security of Quartz. In: *Public Key Cryptography - PKC 2003, LNCS 2567,* pp. 351-364. Springer-Verlag, 2003.
- J. C. Cha and J. H. Cheon. An Identity-Based Signature from Gap Diffie-Hellman Groups. In: *Public Key Cryptography - PKC 2003, LNCS 2567*, pp. 18-30. Springer-Verlag, 2003.
- P.Vondruška, E-podpisy?, Crypto-Words 5/2003,2,2003.
- M. Fischlin. The Cramer-Shoup Strong-RSA Signature Scheme Revisited. In: *Public Key Cryptography - PKC 2003, LNCS 2567*, pp. 116-129. Springer-Verlag, 2003.
- P.-A. Fouque and G. Poupard. On the Security of RDSA. In: *EUROCRYPT 2003, LNCS 2656*, pp. 462-476. Berlin: Springer-Verlag, 2003.
- E.-J. Goh and S. Jarecki. A Signature Scheme as Secure as the Diffie-Hellman Problem. In: *EUROCRYPT 2003, LNCS 2656*, pp. 401-415. Berlin: Springer-Verlag, 2003.
- Ueli Maurer. Intrinsic Limitations of Sigital Signatures and How to Cope with Them. In: *Information Security* (*ISC 2003*), LNCS 2851, pp. 180-192. Springer-Verlag, 2003.
- M. Näslund, I. Shparlinski, and W. Whyte. On the Bit Security of NTRUEncrypt. In: *Public Key Cryptography - PKC 2003, LNCS 2567*, pp. 62-70. Springer-Verlag, 2003.
- J. Stern. Why Provable Security Matters? In: *Eurocrypt 2003, LNCS 2656*, pp. 449-461. Berlin: Springer-Verlag, 2003.
- M. Szydlo. Hypercubic Lattice Reduction and Analysis of GGH and NTRU Signatures. In: *EUROCRYPT 2003, LNCS 2656*, pp. 433-448. Springer-Verlag, 2003.
- S. Vaudenay. The Security of DSA and ECDSA. In: *Public Key Cryptography - PKC 2003, LNCS 2567*, pp. 309-323. Springer-Verlag, 2003.
- Y. Watanabe, J. Shikata, and H. Imai. Equivalence between Semantic Security and Indistinguishability against Chosen Ciphertext Attacks. In: *Public Key Cryptography - PKC 2003, LNCS 2567*, pp. 71-84. Springer-Verlag, 2003.

2004

- Giuseppe Ateniese, Breno de Medeiros. A Provably Secure Nyberg-Rueppel Signature Variant with Applications. http://eprint.iacr.org/2004/093/.

- Michael Backes, Dennis Hofheinz. How to Break and Repair a Universally Composable Signature Functionality. In: *Information Security* (*ISC 2004*), LNCS 3225, pp. 61-72. Springer-Verlag, 2004.
- Mihir Bellare, Chanathip Namprempre, Gregory Neven. Security Proofs for Identity-Based Identification and Signature Schemes. In: *EUROCRYPT 2004*, LNCS 3027, pp. 268-286. Springer-Verlag, 2004. Full version is available at http://eprint.iacr.org/2004/252/.
- Daniel Bleichenbacher: Compressing Rabin Signatures. In: *Topics in Cryptology - CT-RSA 2004*, LNCS 2964, pp. 126-128. Springer-Verlag, 2004.
- Jens-Matthias Bohli, Rainer Steinwandt. On Subliminal Channels in Deterministic Signature Schemes. In: *Information Security and Cryptology - ICISC 2004,* LNCS ????, pp. ??-??. Springer-Verlag, 2005.
- Dan Boneh, Xavier Boyen. Short Signatures Without Random Oracles. In: *EUROCRYPT 2004*, LNCS 3027, pp. 56-73. Springer-Verlag, 2004. Full version is available at http://eprint.iacr.org/2004/171/.
- Ran Canetti, Oded Goldreich, Shai Halevi. On the Random-Oracle Methodology as Applied to Length-Restricted Signature Schemes. In: *First Theory of Cryptography Conference* (*TCC 2004*), pp. 40-57. Springer-Verlag, 2004.
- Jung Hee Cheon, Yongdae Kim, Hyo Jin Yoon. A New ID-based Signature with Batch Verification. http://eprint.iacr.org/2004/131/.
- Jung Hee Cheon, Yongdae Kim, HyoJin Yoon. Batch Verifications with ID-based Signatures. In: *Information Security and Cryptology - ICISC 2004,* LNCS ????, pp. ??-??. Springer-Verlag, 2005.
- Nicolas T. Courtois. Short Signatures, Provable Security, Generic Attacks and Computational Security of Multivariate Polynomial Schemes such as HFE, Quartz and Sflash. http://eprint.iacr.org/2004/143/.
- Christophe Giraud, Erik Woodward Knudsen. Fault Attacks on Signature Schemes. In: *Information Security and Privacy* (*ACISP 2004*), LNCS 3108, pp. 478-491. Springer-Verlag, 2004.
- Bo Gyeong Kang, Je Hong Park, Sang Geun Hahn: A Certificate-Based Signature Scheme. In: *Topics in Cryptology - CT-RSA 2004*, LNCS 2964, pp. 99-111. Springer-Verlag, 2004.
- Aggelos Kiayias, Yiannis Tsiounis, Moti Yung. Traceable Signatures. In: *EUROCRYPT 2004*, LNCS 3027, pp. 571-589. Springer-Verlag, 2004. Primary version is available at http://eprint.iacr.org/2004/007/.
- Kaoru Kurosawa, Swee-Huay Heng. From Digital Signature to ID-based Identification/Signature. In: *Public Key Cryptography 2004*, LNCS 2947, pp. 248-261. Springer-Verlag, 2004.
- Benoît Libert, Jean-Jacques Quisquater. The Exact Security of an Identity Based Signature and its Applications. http://eprint.iacr.org/2004/102/.
- SungJun Min, Go Yamamoto, Kwangjo Kim. Weak Property of Malleability in NTRUSign. In: *Information Security and Privacy* (*ACISP 2004*), LNCS 3108, pp. 379-390. Springer-Verlag, 2004.
- Reihaneh Safavi-Naini, Luke McAven, Moti Yung. General Group Authentication Codes and Their Relation to "Unconditionally-Secure Signatures". In: *Public Key Cryptography 2004*, LNCS 2947 , pp. 231-247. Springer-Verlag, 2004.

- Siamak Fayyaz Shahandashti, Mahmoud Salmasizadeh, Javad Mohajeri. A Provably Secure Short Transitive Signature Scheme from Bilinear Group Pairs. In: *Security in Communication Networks* (*SCN 2004*), LNCS 3352, pp. 60-76. Springer-Verlag, 2005. BibTeX
- Zhou Sujing. Transitive Signatures Based on Non-adaptive Standard Signatures. http://eprint.iacr.org/2004/044/.
- Serge Vaudenay. Signature Schemes with Domain Parameters: Yet Another Parameter Issue in ECDSA. In: *Information Security and Privacy* (*ACISP 2004*), LNCS 3108, pp. 188-199. Springer-Verlag, 2004.
- Dae Hyun Yum, Pil Joong Lee. Generic Construction of Certificateless Signature. In: *Information Security and Privacy* (*ACISP 2004*), LNCS 3108, pp. 200-211. Springer-Verlag, 2004.

2005

- An Braeken, Christopher Wolf, Bart Preneel. A Study of the Security of Unbalanced Oil and Vinegar Signature Schemes. In: *Topics in Cryptology - CT-RSA 2005*, LNCS 3376, pp. 29-43. Springer-Verlag, 2005. BibTeX. Primary version is available at http://eprint.iacr.org/2004/222/.
- Dario Catalano, Rosario Gennaro. Cramer-Damgård Signatures Revisited: Efficient Flat-Tree Signatures Based on Factoring. In: *Public Key Cryptography - PKC 2005*, LNCS 3386, pp. 313-327. Springer-Verlag, 2005. BibTeX
- Jintai Ding, Dieter Schmidt. Rainbow, a New Multivariable Polynomial Signature Scheme. In: *Applied Cryptography and Network Security* (*ACNS 2005*), LNCS 3531, pp. 164-175. Springer-Verlag, 2005. BibTeX
- Yevgeniy Dodis, Dae Hyun Yum. Time Capsule Signature. In: *Financial Cryptography and Data Security* (FC 2005), LNCS 3570, pp. 57-71. Springer-Verlag, 2005. BibTeX
- Louis Granboulan. A Generic Scheme Based on Trapdoor One-Way Permutations with Signatures as Short as Possible. In: *Public Key Cryptography - PKC 2005*, LNCS 3386, pp. 302-312. Springer-Verlag, 2005. BibTeX
- Benoît Chevallier-Mames, Duong Hieu Phan, David Pointcheval. Optimal Asymmetric Encryption and Signature Paddings. In: *Applied Cryptography and Network Security* (*ACNS 2005*), LNCS 3531, pp. 254-268. Springer-Verlag, 2005. BibTeX
- Benoît Chevallier-Mames. New Signature Schemes with Coupons and Tight Reduction. In: *Applied Cryptography and Network Security* (*ACNS 2005*), LNCS 3531, pp. 513-528. Springer-Verlag, 2005. BibTeX
- Benoît Chevallier-Mames. An Efficient CDH-Based Signature Scheme with a Tight Security Reduction. In: *CRYPTO'05*, LNCS 3621, pp. 511-526. Springer-Verlag, 2005. BibTeX
- Steven D. Galbraith, Chris Heneghan, James F. McKee.Tunable Balancing of RSA. In: *Information Security and Privacy* (ACISP 2005), LNCS 3574, pp. 280-292. Springer-Verlag, 2005. BibTeX

- Thomas Pornin, Julien P. Stern. Digital Signatures Do Not Guarantee Exclusive Ownership. In: *Applied Cryptography and Network Security* (*ACNS 2005*), LNCS 3531, pp. 138-150. Springer-Verlag, 2005. BibTeX
- Lih-Chung Wang, Yuh-Hua Hu, Feipei Lai, Chun-yen Chou, Bo-Yin Yang. Tractable Rational Map Signature. In: *Public Key Cryptography - PKC 2005*, LNCS 3386, pp. 244-257. Springer-Verlag, 2005. BibTeX
- Bo-Yin Yang, Jiun-Ming Chen. Building Secure Tame-like Multivariate Public-Key Cryptosystems: The New TTS. In: *Information Security and Privacy* (ACISP 2005), LNCS 3574, pp. 518-531. Springer-Verlag, 2005. BibTeX
- Fangguo Zhang, Willy Susilo, Yi Mu. Identity-Based Partial Message Recovery Signatures (or How to Shorten ID-Based Signatures). In: *Financial Cryptography and Data Security* (FC 2005), LNCS 3570, pp. 45-56. Springer-Verlag, 2005. BibTeX

10.2 Přehled literatury k vícenásobnému elektronickému podpisu

1983

- K. Itakura, and K. Nakamura. A public key cryptosystem suitable for digital multisignatures. *NEC Research & Development*, 71:1-8, 1983.

1986

- C. Boyd. Digital multisignatures. *Cryptography and Coding*, 1986.

1987

- Y. Desmedt. Society and group oriented cryptography: a new concept. In: *Crypto'87,* LNCS 293, pp.120-127. Springer-Verlag, 1988.

1988

- T. Okamoto. A digital multisignature scheme using bijective public-key cryptosystem. *ACM Transactions on Computer Systems*, 1988, 6(8): 432-441.
-

1989

- C. Boyd. Digital multisignatures. In: Cryptography and Coding, pp. 241-246. Oxford University Press, 1989.
- Y. Desmedt, and Y. Frankel. Threshold cryptosystems. In: *Crypto'89,* LNCS 435, pp. 307-315. Springer-Verlag, 1990.
- L. Harn and T. Kresler. New scheme for digital multisignatures. *Electronics Letters*, July 1989, 25(15): 1002-1003.

1990

- T. Kiesler and L. Harn. RSA blocking and multisignature schemes with no bit expansion. *Electronics Letters*, Aug 1990, 26(18): 1490-1491.

1991

- C. Boyd. Multisignatures based on zero knowledge schemes. *Electronics Letters*, Oct 1991, 27(22): 2002-2004.

- Y. Desmedt, and Y. Frankel. Shared generation of authenticators and signatures. Crypto 91, 1991.
- T. Ohata, and T. Okamoto. A digital multisignature scheme based on the Fiat-Shamir scheme. In: *Asiacrypt'91,* LNCS 739, pp. 75-79. Springer-Verlag, 1991.
- T.P. Pedersen. A threshold cryptosystem without a trusted party. In: *Eurocrpt'91,* LNCS 547, pp. 522-526. Berlin: Springer-Verlag, 1991.

1992

- A. Fujioka, T. Okamoto, and K. Ohta. A practical digital multisignature scheme based on discrete logarithms. In: *Auscrypt'92,* LNCS 718, pp. 244-251. Springer-Verlag, 1992.
- L. Harn, and S. Yang. Group-oriented undeniable signature schemes without the assistance of a mutually trusted party. In: *Auscrypt'92,* LNCS 718, pp.133-142. Springer-Verlag, 1993.

1994

- Y. Desmedt. Threshold cryptography. *European Transactions on Telecommunications*, 5(4), 1994.
- L. Harn. Group-oriented (t, n) threshold digital signature scheme and multisignature. *IEE Proceedings - Computers and Digital Techniques*, 1994, 141(5): 307-313.
- L. Harn and Y. Xu. Design of generalised ElGamal type digital signature schemes based on discrete logarithm. *Electronics Letters*, Nov 1994, 30(24): 2025 -2026.
- L. Harn. New digital signature scheme based on discrete logarithm. *Electronics Letters*, Mar 1994, 30(5): 396-398.
- C-M. Li, T. Hwang and N-Y. Lee. Threshold-multisignature schemes where suspected forgery implies traceability of adversarial shareholders. In: *Eurocrypt'94,* LNCS 950, pp. 194-204. Springer-Verlag, 1995.

1995

- P. Horster, M. Michels, and H. Petersen. Meta-multisignature schemes based on the discrete logarithm problem. In: P*roc. of IFIP/SEC'95*, pp. 128-141. Chapman & Hall, 1995.
- P. Horster, M. Michels, and H. Peterson. Blind Multisignature Scheme Based on the Discrete Logarithm Problem. In: *Proc. of 12th Annual Computer Security Applications Conference* (*ACSAC'95*), 1996.
- C. G. Kang. New digital multisignature scheme in electronic contract systems. In: *Proc. of 1995 IEEE International Symposium on Information Theory*, pp. 486. IEEE, 1995.

1996

- R.Gennaro, S. Jarecki, H.Krawczyk, and T. Rabin. Robust threshold DSS signatures. In: *Eurocrypt'96,* LNCS 1070, pp. 354-371. Springer-Verlag, 1996. A modified version appeared in *Information and Computation*, 164(1): 54-84, 2001.
- S.K. Langford. Weaknesses in some threshold cryptosystems. In: *Crypto'96,* LNCS 1109, pp.74-82. Springer-Verlag, 1996.
- M. Michels, and P. Horster. On the risk of discruption in several multiparty signature schemes. In: *Asiacrypt'96,* LNCS 1163, pp.334-345. Springer-Verlag, 1996.
- C. Park, and K. Kurosawa. New Elgamal type threshold digital signature scheme. *IEICE Trans. Fundamentals*, January 1996, E79-A(1): 86-93.

1997

- C.-H. Wang, and T. Hwang. Threshold and Generalized DSS Signatures Without a Trusted Party. In: *Proceeding of the 13th Annual Computer Security Applications Conference (ACSAC'97)*, pp. 221-226. IEEE Computer Society, 1997.
- H. Petersen, and M. Michels. On signatures schemes with threshold verification detecting malicious verifiers. In: *Workshop on Security Protocols'97*, LNCS 1361, pp.67-78. Berlin: Springer-Verlag, 1997.
- S. Russell. Multisignature algorithms for ISO 9796. *ACM SIGSAC Security Audit & Control Review*, January 1997, 15(1): 11-14.

1998

- T. Rabin. A simplified approach to threshold and proactive RSA. In: Crypto 98, LNCS1462, pp. . 1998.

1999

- R. Canetti, R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin. Adaptive security for threshold cryptosystems. In *Crypto'99,* LNCS 1666, pp. 98-115. Berlin: Springer-Verlag, 1999.
- R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin. Secure distributed key generation for discrete-log based cryptosystems. In: Eurocrypt'99, LNCS 1592, pp. 295-310. Berlin: Springer-Verlag, 1999.
- L. Harn. Digital multisignature with distinguished signing authorities. *Electronics Letters*, Feb 1999, 35(4): 294-295.
- K. Ohta and T. Okamoto. Multi-signature scheme secure against active insider attacks. *IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences*, E82-A(1): 21-31, 1999.
- H.-M. Sun. An efficient nonrepudiable threshold proxy signature scheme with known signers. *Computer Communications*, May 1999, 22(8): 717-722.

2000

- Y.-S. Chang, T.-C. Wu and S.-C. Huang. ElGamal-like digital signature and multisignature schemes using self-certified public keys. *Journal of Systems and Software*, February 2000, 50(2): 99-105.
- H. Doi, M. Mambo, and E. Okamoto. On the Security of the RSA-Based Multisignature Scheme for Various Group Structures. In: *Information Security and Privacy (ACISP'00), LNCS 1841*, pp. 352-367. Springer-Verlag, 2000.
- B. King. Algorithms to Speed Up Computations in Threshold RSA. In: *Information Security and Privacy (ACISP'00),* LNCS 1841, pp. 2443-456. Springer-Verlag, 2000.
- B. King. Improved Methods to Perform Threshold RSA. In: *ASIACRYPT 2000,* LNCS 1976, pp. 359-372. Springer-Verlag, 2000.
- C-M. Li, T. Hwang, N-Y. Lee, and J-J.Tsai. (*t*, *n*) threshold-multisignature schemes and generalized-multisignature scheme where suspected forgery implies traceability of adversarial shareholders. Cryptologia, July 2000, 24(3): 250-268.
- Z.C Li, L.C.K. Hui, K.P. Chow, C.F. Chong, W.W. Tsang, and H.W. Chan. Cryptanalysis of Harn digital multisignature scheme with distinguished signing authorities [comment]. *Electronics Letters*, Feb 2000, 36(4): 314-315.
- J. Merkle. Multi-round passive attacks on server-aided RSA protocols. In: *Proc. of the 7th ACM Conference on Computer and Communications Security (CCS 2000)*, pp. 102 - 107. ACM, 2000.
- S. Mitomi and A. Miyaji. A Multisignature Scheme with Message Flexibility, Order Flexibility and Order Verifiability. In: *Information Security and Privacy (ACISP'00),* LNCS 1841, pp. 298-312. Springer-Verlag, 2000.
- S.-P. Shieh, C.-T. Lin; W.-B. Yang, and H.-M. Sun. Digital multisignature schemes for authenticating delegates in mobile code systems. *IEEE Transactions on Vehicular Technology*, Jul 2000, 49(4): 1464 -1473.
- V. Shoup. Practical Threshold Signatures. In: *Eurocrypt 2000,* LNCS 1807, pp. 207-220. Springer-Verlag, 2000.

2001

- I. Damgård, and M. Koprowski. Practical threshold RSA signatures without a trusted dealer. In: *Eurocrypt'01,* LNCS 2045, pp. 152-165. Springer-Verlag, 2001. .
- P.-A. Fouque, and J. Stern. One round threshold discrete-log key generation without private channels. In: *PKC'01,* LNCS 1992, pp. 300-316. Berlin: Springer-Verlag, 2001.
- P.-A. Fouque, and D. Pointcheval. Threshold cryptosystems secure against chosen-ciphertext attacks. In: *Asiacrypt'01,* LNCS 2248, pp. 351-368. Berlin: Springer-Verlag, 2001.
- P.-A. Fouque and J. Stern. Fully Distributed Threshold RSA under Standard Assumptions. In: *ASIACRYPT 2001,* LNCS 2248, pp. 310-330. Springer-Verlag, 2001.

- R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin. Robust threshold DSS signatures. *Information and Computation*, 164(1): 54-84, 2001. An earlier version appeared in *Eurocrypt'96*.
- J. Hoffstein, J. Pipher, and J. H. Silverman. NSS: An NTRU Lattice-Based Signature Scheme. In: *EUROCRYPT 2001,* LNCS 2045, pp. 211-228. Springer-Verlag, 2001.
- Chih-Yin Lin, Tzong-Chen Wu, Jing-Jang Hwang. ID-Based Structured Mulitsignature Schemes. *Network Security 2001*: 45-60. *IFIP TC11 WG11.4 First Annual Working Conference on Network Security*, November 26-27, 2001, Leuven, Belgium. IFIP Conference Proceedings 206 Kluwer 2001, ISBN 0-7923-7558-0.
- A. Lysyanskaya and C. Peikert. Adaptive Security in the Threshold Setting: From Cryptosystems to Signature Schemes. In: ASIACRYPT 2001, LNCS 2248, pp. 331-350. Springer-Verlag, 2001.
- P. D. MacKenzie and M. K. Reiter. Two-Party Generation of DSA Signatures. In: *CRYPTO 2001,* LNCS 2139, pp. 137-154. Springer-Verlag, 2001.
- S. Micali, K. Ohta, and L. Reyzin. Accountable-subgroup multisignatures: extended abstract. In: *Proc. of the 8th ACM Conference on Computer and Communications Security (CCS 2001)*, pp. 245-254. ACM, 2001.
- Reihaneh Safavi-Naini, Huaxiong Wang, Kwok-Yan Lam: A New Approach to Robust Threshold RSA Signature Schemes. In: ICISC 1999, LNCS 1787, pp. 184-196.
- D.R. Stinson, and R. Strobl. Provably secure distributed Schnorr signatures and a (t, n) threshold scheme for implicit certificates. In: *ACISP'01,* LNCS 2119, pp. 417-434. Springer-Verlag, 2001.
- T.-C. Wu, C.-C. Huang and D.-J. Guan. Delegated multisignature scheme with document decomposition. *Journal of Systems and Software*, January 2001, 55(3): 321-328.

2002

- H.-Y. Chien, J.-K. Jan, and Y.-M. Tseng. Forgery attacks on "Multisignature schemes for authenticating mobile code delegates". *IEEE Transactions on Vehicular Technology*, Nov 2002, 51(6): 1669-1671.
- Y. Frankel, P. D. MacKenzie, and M. Yung. Adaptively secure distributed public-key systems. *Theoretical Computer Science*, 2002, 287(2): 535-561.
- Yi Mu, Vijay Varadharajan. Group Cryptography: Signature and Encryption. *Informatica (Slovenia)*, 2002, 26(3): 249-254.
- S.-F. Pon, E.-H. Lu, and J.-Y. Lee. Dynamic reblocking RSA-based multisignatures scheme for computer and communication networks. *IEEE Communications Letters*, Jan 2002, 6(1): 43-44.
- Mitsuru Tada. An Order-Specified Multisignature Scheme Secure against Active Insider Attacks. In: *Information Security and Privacy (ACISP'02),* LNCS 2384, pp. 328-345. Springer-Verlag, 2002.
- G. Wang. On the security of the Li-Hwang-Lee-Tsai threshold group signatures scheme. In: *Information Security and Cryptography (ICISC 2002),* LNCS 2587, pp. 75-89. Springer-Verlag, 2003.

- X. Yi and C. K. Siew. Attacks on Shieh-Lin-Yang-Sun digital multisignature schemes for authenticating delegates in mobile code systems. *IEEE Transactions on Vehicular Technology*, Nov 2002, 51(6): 1313-1315.

2003

- A. Boldyreva. Threshold Signatures, Multisignatures and Blind Signatures Based on the Gap-Diffie-Hellman-Group Signature Scheme. In: *Public Key Cryptography - PKC 2003,* LNCS 2567, pp. 31–46. Springer-Verlag, 2003.
- D. Boneh, C. Gentry, B. Lynn, and H. Shacham. Aggregate and Verifiably Encrypted Signatures from Bilinear Maps. In: *EUROCRYPT 2003,* LNCS 2656, pp. 416-432. Springer-Verlag, 2003.
- I. Damgård and M. Jurik. A Length-Flexible Threshold Cryptosystem with Applications. In: *Information Security and Privacy (ACISP'03),* LNCS 2727, pp. 350-364. Springer-Verlag, 2003.
- Javier Herranz, Carles Padró, and Germán Sáez. Distributed RSA Signature Schemes for General Access Structures In: *Information Security* (*ISC 2003*), LNCS 2851, pp. 122-136. Springer-Verlag, 2003.
- K. Kawauchi and M. Tada. On the Exact Security of Multi-signature Schemes Based on RSA. In: *Information Security and Privacy (ACISP'03),* LNCS 2727, pp. 336-349. Springer-Verlag, 2003.
- Dongjin Kwak and Sangjae Moon. Efficient Distributed Signcryption Scheme as Group Signcryption. In: *Applied Cryptography and Network Security (ACNS'03)*, LNCS 2846, pp. 403-417. Springer-Verlag, 2003.
- Li-Shan Liu, Cheng-Kang Chu, and Wen-Guey Tzeng. A Threshold GQ Signature Scheme. In: *Applied Cryptography and Network Security (ACNS'03)*, LNCS 2846, pp. 137-150. Springer-Verlag, 2003.
- P. D. MacKenzie. An Efficient Two-Party Public Key Cryptosystem Secure against Adaptive Chosen Ciphertext Attack. In: *Public Key Cryptography - PKC 2003,* LNCS 2567, pp. 47-61. Springer-Verlag, 2003.
- A. Nicolosi, M. Krohn, Y. Dodis, and D. Mazieres. Proactive Two-Party Signatures for User Authentication. In: *Proceedings of NDSS'03*. http://www.isoc.org/isoc/conferences/ndss/03/proceedings/index.htm
- Rui Zhang and Hideki Imai. Round Optimal Distributed Key Generation of Threshold Cryptosystem Based on Discrete Logarithm Problem. In: *Applied Cryptography and Network Security (ACNS'03)*, LNCS 2846, pp. 96-110. Springer-Verlag, 2003.
- Guilin Wang, Xiaoxi Han, and Bo Zhu. On the Security of Two Threshold Signature Schemes with Traceable Signers. In: *Applied Cryptography and Network Security (ACNS'03),* LNCS 2846, pp. 111-122. Springer-Verlag, 2003.

- T.-C. Wu and C.-L. Hsu. Cryptanalysis of Digital Multisignature Schemes for Authenticating Delegates in Mobile Code Systems. *IEEE Transactions on Vehicular Technology*, March 2003, 52(2): 462 -465.
- S. Xu and R. Sandhu. Two Efficient and Provably Secure Schemes for Server-Assisted Threshold Signatures In: *CT-RSA 2003,* LNCS 2612, p. 355-372. Springer-Verlag, 2003.

- Anna Lysyanskaya, Silvio Micali, Leonid Reyzin, Hovav Shacham. Sequential Aggregate Signatures from Trapdoor Permutations. In: *EUROCRYPT 2004*, LNCS 3027, pp. 74-90. Springer-Verlag, 2004.

2004

- Masayuki Abe, Serge Fehr. Adaptively Secure Feldman VSS and Applications to Universally-Composable Threshold Cryptography. In: *CRYPTO 2004,* LNCS 3152, pp. 317-334. Springer-Verlag, 2004. Full version available at http://eprint.iacr.org/2004/119/.
- Claude Castelluccia, Stanislaw Jarecki, Jihye Kim, Gene Tsudik. A Robust Multisignatures Scheme with Applications to Acknowledgment Aggregation. In: *Security in Communication Networks (SCN 2004),* LNCS 3352, pp. 193-207. Springer-Verlag, 2005. BibTeX
- Xiaofeng Chen, Fangguo Zhang, Divyan M. Konidala, Kwangjo Kim. New ID-based Threshold Signature Scheme from Bilinear Pairings. In: *INDOCRYPT 2004*, LNCS 3348, pp. 371-383. Springer- Verlag, 2004.
- Giovanni Di Crescenzo, Gonzalo R. Arce, Renwei Ge. Threshold Cryptography for Mobile Ad Hoc Networks. In: *Security in Communication Networks (SCN 2004),* LNCS 3352, pp. 91-104. Springer-Verlag, 2005. BibTeX
- Sherman S. M. Chow, Lucas C.K. Hui, S.M. Yiu, K.P. Chow. Secure Hierarchical Identity Based Signature and its Application. In: *Information and Communications Security* (*ICICS 2004*), LNCS 3269, pp. 480-494. Springer-Verlag, 2004.
- Sherman S.M. Chow, Lucas C.K. Hui, S.M. Yiu. Identity Based Threshold Ring Signature. In: *Information Security and Cryptology - ICISC 2004,* LNCS ????, pp. ??-??. Springer-Verlag, 2005. Primary version is available at http://eprint.iacr.org/2004/179/.
- Javier Herranz, Germán Sáez. Distributed Ring Signatures for Identity-Based Scenarios. http://eprint.iacr.org/2004/190/.
- Fabien Laguillaumie, Damien Vergnaud. Multi-Designated Verifiers Signatures. In: *Information and Communications Security* (*ICICS 2004*), LNCS 3269, pp. 495-507. Springer-Verlag, 2004.
- Einar Mykletun, Maithili Narasimha, Gene Tsudik. Signature Bouquets: Immutability for Aggregated/Condensed Signatures. http://eprint.iacr.org/2004/091/.
- Patrick P. Tsang, Victor K. Wei, Tony K. Chan, Man Ho Au, Joseph K. Liu, and Duncan S. Wong. Separable Linkable Threshold Ring Signatures. In: *INDOCRYPT 2004*, LNCS 3348, pp. 384-398. Springer- Verlag, 2004. Full version available at http://eprint.iacr.org/2004/267/.
- Victor K. Wei. A Bilinear Spontaneous Anonymous Threshold Signature for Ad Hoc Groups. http://eprint.iacr.org/2004/039/.
- Jing Xu, Zhenfeng Zhang, Dengguo Feng. Identity Based Threshold Proxy Signature. http://eprint.iacr.org/2004/250/.

2005

- Ivan Damgård, Kasper Dupont. Efficient Threshold RSA Signatures with General Moduli and No Extra Assumptions. In: *Public Key Cryptography - PKC 2005*, LNCS 3386, pp. 346-361. Springer-Verlag, 2005. BibTeX
- Toshiyuki Isshiki, Keisuke Tanaka. An (n-t)-out-of-n Threshold Ring Signature Scheme. In: *Information Security and Privacy* (ACISP 2005), LNCS 3574, pp. 406-416. Springer-Verlag, 2005. BibTeX
- Stanislaw Jarecki, Nitesh Saxena. Further Simplifications in Proactive RSA Signatures. In: *Theory of Cryptography* (*TCC 2005*), LNCS 3378, pp. 510-528. Springer-Verlag, 2005. BibTeX
- Brian King. An Efficient Implementation of a Threshold RSA Signature Scheme. In: *Information Security and Privacy* (ACISP 2005), LNCS 3574, pp. 382-393. Springer-Verlag, 2005. BibTeX

10.3 Přehled literatury k tzv. skupinovému elektronickému podpisu

1991

- CvH91 D. Chaum, E. van Heyst. Group signatures. In: *EUROCRYPT'91,* LNCS 547, pp. 257-265. Springer-Verlag, 1991.

1994

- L. Chen and T.P. Pedersen. New group signature schemes. In: *EUROCRYPT'94,* LNCS 950, pp. 171-181. Springer-Verlag, 1995.

1995

- L. Chen and T.P. Pedersen. On the efficiency of group signatures providing information-theoretic anonymity. In: *EUROCRYPT'95,* LNCS 921, pp. 39-49. Springer-Verlag, 1995.

1996

- S.J. Kim, S.J. Park, and D.H Won. Convertible group signatures. In: *ASIACRYPT'96,* LNCS 1163, pp. 311-321. Springer-Verlag, 1996.

1997

- J. Camenisch. Efficient and generalized group signatures. In: *EUROCRYPT'97,* LNCS 1233, pp. 465-479. Springer-Verlag, 1997.
- J. Camenisch and M. Stadler. Efficient group signature schemes for large groups. In: *Crypto'97,* LNCS 1294, pp. 410-424. Springer-Verlag, 1997.
- C.H. Lim and P.J. Lee. Remarks on convertible signatures of ASIACRYPT'96. *Electronics Letters*, 1997, 33(5): 383-384.
- S. Park, S. Kim, and D. Won. ID-based group signature. *Electronics Letters*, 1997, 33(15): 1616-1617.
- H. Petersen. How to convert any digital signature scheme into a group signature scheme. In: *Proc. of Security Protocols Workshop'97,* LNCS 1361, pp. 67-78. Springer-Verlag, 1997.

1998

- J. Camenisch. Group signature schemes and payment systems based on the discrete logarithm problem. *Vol. 2 of ETH-Series in Information Security an Cryptography*, ISBN 3-89649-286-1, Hartung-Gorre Verlag, Konstanz, 1998.
- J. Camenisch and M. Michels. A group signature scheme with improved efficiency. In: *ASIACRYPT'98,* LNCS 1514, pp. 160-174. Springer-Verlag, 1998.
- J. Camenisch and M. Michels. A group signature scheme based on an RSA-variant. *Technical Report RS-98-27. BRICS, University of Aarhus*, November 1998. Primary version of this paper appeared at ASIACRYPT'98. http://citeseer.nj.nec.com/camenisch98group.html
- W-B. Lee and C-C. Chang. Efficient group signature scheme based on the discrete logarithm. *IEE Proc. Comput. Digit. Tech.*, 1998, 145(1): 15-18.
- A. Lysyanskaya and Z. Ramzan. Group blind digital signatures: A scalable solution to electronic cash. In: *Financial Cryptography (FC'98),* LNCS 1465, pp. 184-197. Springer-Verlag, 1998.
- W. Mao and C.H. Lim. Cryptanalysis in prime order subgroups in Z_n^*. In: *ASIACRYPT'98,* LNCS 1514, pp. 214-226. Springer-Verlag, 1998.
- Y.-M. Tseng and J.-K. Jan. A novel ID-based group signature. In: T.L. Hwang and A.K. Lenstra, editors, *1998 International Computer Symposium, Workshop on Cryptology and Information Security*, Tainan, 1998, pp. 159-164.

1999

- G. Ateniese and G. Tsudik. Group signatures a la carte. In: *Proceedings of the tenth annual ACM-SIAM symposium on Discrete algorithms* (*SODA'99*), pp. 848-849. New York: ACM Press, 1999.
- G. Ateniese, M. Joye, and G. Tsudik. On the difficulty of coalition-resistant in group signature schemes. In: *Second Workshop on Security in Communication Networks* (*SCN'99*), September 1999. http://www.ics.uci.edu/~gts/wo.html
- G. Ateniese and G. Tsudik. Some open issues and new directions in group signature schemes. In: *Financial Cryptography* (*FC'99*), LNCS 1648, pp. 196-211. Springer-Verlag, 1999.
- J. Camenisch and M. Michels. Separability and efficiency for generic group signature schemes. In: *Crypto'99,* LNCS 1666, pp. 413-430. Springer-Verlag, 1999.
- J. Camenisch. Efficient Anonymous Fingerprinting with Group Signatures. In: *ASIACRYPT 2000,* LNCS 1976, pp. 415-428. Springer-Verlag, 2000.
- M. Joye, N-Y. Lee, and T. Hwang. On the security of the Lee-Chang group signature scheme and its derivatives. In: *Information Security* (*ISW'99*), LNCS 1729, pp. 47-51. Springer-Verlag, 1999.
- M. Joye, S. Kim, and N-Y. Lee. Cryptanalysis of two group signature schemes. In: *Information Security* (*ISW'99*), LNCS 1729, pp. 271-275. Springer-Verlag, 1999.
- Z. Li, Y. Wang, Y.X. Yang and W. Wu. Cryptanalysis of convertible group signature. *Electronics Letters*, 1999, 35(5): 1071-1072.

- K.Q. Nguyen, Y. Mu, and V. Varadharajan. Divertible zero-Knowledge proof of polynominal relations and blind group signature. In: *ACISP'99,* LNCS 1587, pp. 117-128. Springer-Verlag, 1999.
- H. Sun. Comment: improved group signature scheme based on discrete logarithm problem. *Electronics Letters*, 1999, 35(13): 1323-1324.
- J. Traoré. Group signatures and their relevance to privacy-protecting off-line electronic cash systems. In: *ACISP'99,* LNCS 1587, pp. 228-243. Springer-Verlag, 1999.
- Y.-M. Tseng and J.-K. Jan. Improved group signature scheme based on the discrete logarithm problem. *Electronics Letters*, 1999, 35(1): 37-38.
- Y.-M. Tseng and J.-K. Jan. Reply: improved group signature scheme based on discrete logarithm problem. *Electronics Letters*, 1999, 35(13): 1324-1325.
- Y.-M. Tseng and J.-K. Jan. A group signature scheme using self-certified public keys. In: *Ninth National Conference on Information Security*, pp. 165-172. May 1999.
- Y.-M. Tseng and J.-K. Jan. A novel ID-based group signature. *Information Sciences*, 1999, 120: 131-141. Elsevier Science. Available from ``Full text articles'' at http://www.elsevier.nl/locate/ins
- C.-H. Wang, T. Hwang, and N.-Y. Lee. Comments on two group signatures. *Information Processing Letters*, 1999, 69: 95-97.
- C.K. Wu and V. Varadharajan. Many-to-one cryptographic algorithms and group signatures (extended abstract). In: Jenny Edward Ed., *Australian Computer Science Communications, Proceedings of the Twenty Second Australasian Computer Science Conference (ACSC'99)*, Auckland, New Zealand, January 18-21 1999, , Springer 1999, pp.432-444.

2000

- G. Ateniese, J. Camenisch , M. Joye, and G. Tsudik. A practical and provably secure coalition-resistant group signature scheme. In: *Crypto'2000,* LNCS 1880, pp. 255-270. Springer-Verlag, 2000.
- J. Camenisch and I. Damgård. Verifiable Encryption, Group Encryption, and Their Applications to Separable Group Signatures and Signature Sharing Schemes. In: *ASIACRYPT 2000,* LNCS 1976, pp. 331-345. Springer-Verlag, 2000.
- H-J. Kim, J.I. Lim, and D.H. Lee. Efficient and secure member deletion in group signature schemes. In: *Information Security and Cryptology* (*ICISC 2000*), LNCS 2015, pp. 150-161. Springer-Verlag, 2001.
- S. Popescu. A modification of the Tseng-Jan group signature scheme. *Studia Univ. Babes-Bolyai, Informatica*, 2000, XLV(2): 36-40. http://www.cs.ubbcluj.ro/~studia-i/2000-2/ or http://citeseer.nj.nec.com/504016.html.
- S. Saeednia. On the security of a convertible group signature schemes. *Information Processing Letters*, 2000, 73: 93-96.
- K. Sakurai, and S. Miyazaki. An anonymous electronic bidding protocol based on a new convertible group signature scheme. In: *Information Security and Privacy* (*ACISP'00*), LNCS 1841, pp. 385–399. Berlin: Springer-Verlag, 2000.

2001

- C.-C. Chang and K.-F. Hwang. Towards the forgery of a group signature without knowing the group center's secret. In: *Information and Communications Security* (*ICICS'01*), LNCS 2229, pp. 47-51. Springer-Verlag, 2001.
- G. Maitland and C. Boyd. Fair electronic cash based on a group signature scheme In: *Information Security and Cryptography (ICICS 2001),* LNCS 2229, pp. 461–465, Springer-Verlag: 2001.
- R. Rivest, A. Shamir, and Y. Tauman. How to leak a secret. In: *ASIACRYPT 2001,* LNCS 2248, pp. 552–565. Springer-Verlag, 2001.
- D. X. Song. Practical forward secure group signature schemes. In: *Proc. of the 8th ACM Conference on Computer and Communications Security (CCS 2001)*, pp. 225-234. ACM, 2001.

2002

- M. Abe, M. Ohkubo, and K. Suzuki. 1-out-of-n signatures from a variety of keys. In: *ASIACRYPT 2002,* LNCS 2501, pp. 415–432. Springer-Verlag, 2002.
- G. Ateniese, D. Song, and G. Tsudik. Quasi-efficient revocation in group signatures. In: *Financial Cryptography* (*FC'02*), LNCS 2357, 183-197. Springer-Verlag, 2002. Primary version available at http://eprint.iacr.org/2001/101/
- E. Bresson, J. Stern, and M. Szydlo. Threshold ring signatures and applications to ad-hoc groups. In: *CRYPTO 2002*, LNCS 2442, pp. 465–480. Springer-Verlag, 2002.
- J. Camenisch and A. Lysyanskaya. Dynamic accumulators and application to efficient revocation of anonymous credentials. In: *Crypto 2002,* LNCS 2442, pp. 61-76. Springer-Verlag, 2002.
- Sébastien Canard and Marc Girault. Implementing Group Signature Schemes With Smart Cards. In: *CARDIS'02*, the joint IFIP/USENIX International Conference on Smart Card Research and Advanced Applications.
- C. Castelluccia. How to convert any ID-based signature schemes into a group signature scheme. http://eprint.iacr.org/2002/116/.
- Y.-D. Lyuu and M.-L. Wu. Convertible group undeniable signatures. In: *Information Security and Cryptology – ICISC 2002,* LNCS 2587, pp. 48-61. Berlin: Springer-Verlag, 2003.
- G. Maitland and C. Boyd. Cooperatively Formed Group Signatures. In: *RSA Cryptographers Track (CT-RSA 2002),* LNCS 2271, pp.218-235. Springer-Verlag, 2002.
- M. Naor. Deniable ring authentication. In: *CRYPTO 2002*, LNCS 2442, pp. 481–498. Springer-Verlag, 2002.
- T. Nakanishi, M. Tao, and Y. Sugiyama. A group signature scheme committing the group. In: *Information and Communications Security (ICICS 2002),* LNCS 2513, pp. 73-84. Springer-Verlag, 2002.
- S. Popescu. An efficient ID-based group signature scheme. *Studia Univ. Babes-Bolyai, Informatica*, 2002, XLVII(2): 29-36. http://www.cs.ubbcluj.ro/~studia-i/2002-2/

- G. Wang. On the security of the Li-Hwang-Lee-Tsai threshold group signatures scheme. In: *Information Security and Cryptology - ICISC 2002,* LNCS 2587, pp. 75-89. Springer-Verlag, 2003.
- S. Xia and J. You. A group signature scheme with strong separability. *The Journal of Systems and Software*, 2002, 60(3): 177-182. Elsevier Science.
- F. Zhang and K. Kim. ID-based blind signature and ring signature from Pairings. In: *ASIACRYPT 2002*, LNCS 2501, pp. 533–547. Springer-Verlag, 2002.

2003

- Giuseppe Ateniese and Breno de Medeiros. Efficient Group Signatures without Trapdoors. In: *ASIACRYPT 2003*, LNCS 2894, pp. 246-268. Springer-Verlag, 2003. Primary version available at http://eprint.iacr.org/2002/173/.
- M. Bellare, D. Micciancio, and B. Warinschi. Foundations of Group Signatures: Formal Definitions, Simplified Requirements, and a Construction Based on General Assumptions. In: *EUROCRYPT 2003,* LNCS 2656, pp. 614-629. Berlin: Springer-Verlag, 2003.
- S. Canard and J. Traore. On Fair E-cash Systems Based on Group Signature Schemes. In: *Information Security and Privacy* (*ACISP'03*), LNCS 2727, pp. 237–248. Berlin: Springer-Verlag, 2003.
- Zewen Chen, Jilin Wang, Yumin Wang, Jiwu Huang, and Daren Huang. An Efficient Revocation Algorithm in Group Signatures. In: *Information Security and Cryptology - ICISC 2003,* LNCS 2971, pp. 339-351. Springer-Verlag, 2004.
- Chongzhi Gao, Zheng'an Yao, and Lei Li. A Ring Signature Scheme Based on the Nyberg-Rueppel Signature Scheme. In: *Applied Cryptography and Network Security (ACNS'03)*, LNCS 2846, pp. 169-175. Springer-Verlag, 2003.
- Javier Herranz, Germán Sáez. Forking Lemmas for Ring Signature Schemes. In: *INDOCRYPT 2003*, LNCS 2904, pp. 266-279. Berlin: Springer- Verlag, 2003.
- A. Kiayias and M. Yung. Extracting Group Signatures from Traitor Tracing Schemes. In: *EUROCYPT 2003,* LNCS 2656, pp. 630-648. Berlin: Springer-Verlag, 2003.
- Joseph K. Liu, Victor K. Wei, Duncan S. Wong. A Separable Threshold Ring Signature Scheme. In: *Information Security and Cryptology - ICISC 2003,* LNCS 2971, pp. 12-26. Springer-Verlag, 2004.
- Gene Tsudik1 and Shouhuai Xu. Accumulating Composites and Improved Group Signing. In: *ASIACRYPT 2003*, LNCS 2894, pp. 269–286. Springer-Verlag, 2003. Primary version available at http://eprint.iacr.org/2003/112/.
- Guilin Wang, Feng Bao, Jianying Zhou, and Robert H. Deng. Security Remarks on a Group Signature Scheme with Member Deletion. In: *Information and Communications Security* (*ICICS'03*), LNCS 2836, pp. 72-83. Springer-Verlag, 2003.
- Guilin Wang. Security Analysis of Several Group Signature Schemes. In: *INDOCRYPT 2003*, LNCS 2904, pp. 252-265. Springer- Verlag, 2003. Full version is available at http://eprint.iacr.org/2003/194/.

- Guilin Wang. On the Security of a Group Signature Scheme with Forward Security. In: *Information Security and Cryptology - ICISC 2003,* LNCS 2971, pp. 27-39. Springer-Verlag, 2004. Primary version available at http://eprint.iacr.org/2003/226/.
- Guilin Wang and Sihan Qing. Security Flaws in Several Group Signatures Proposed by Popescu. *Cryptology ePrint archive*, report 2003/207, Sep 2003. http://eprint.iacr.org/2003/207.
- Duncan S. Wong, Karyin Fung, Joseph K. Liu, and Victor K. Wei. On the RS-code Construction of Ring Signature Schemes and a Threshold Setting of RST. In: *Information and Communications Security* (*ICICS'03*), LNCS 2836, pp. 34-46. Springer-Verlag, 2003.
- Jianhong Zhang, Qianhong Wu, and Yumin Wang. A Novel Efficient Group Signature Scheme with Forward Security. In: *Information and Communications Security* (*ICICS'03*), LNCS 2836, pp. 292-300. Springer-Verlag, 2003.

2004

- Michel Abdalla, Bogdan Warinschi. On the Minimal Assumptions of Group Signature Schemes. In: *Information and Communications Security* (*ICICS 2004*), LNCS 3269, pp. 1-13. Springer-Verlag, 2004.
- Amit K Awasthi, Sunder Lal. ID-based Ring Signature and Proxy Ring Signature Schemes from Bilinear Pairings. http://eprint.iacr.org/2004/184/.
- Dan Boneh, Xavier Boyen, Hovav Shacham. Short Group Signatures. In: *CRYPTO 2004,* LNCS 3152, pp. 41-55. Springer-Verlag, 2004.
- Dan Boneh, Hovav Shacham. Group signatures with verifier-local revocation. In: *Proc. of the 11th ACM Conference on Computer and Communications Security (CCS 2004)*, pp. 168-177. ACM, 2004. BibTeX
- Ernest F. Brickell, Jan Camenisch, Liqun Chen. Direct anonymous attestation. In: *Proc. of the 11th ACM Conference on Computer and Communications Security (CCS 2004)*, pp. 132-145. ACM, 2004. BibTeX
- Jan Camenisch, Anna Lysyanskaya. Signature Schemes and Anonymous Credentials from Bilinear Maps. In: *CRYPTO 2004,* LNCS 3152, pp. 56-??. Springer-Verlag, 2004.
- Jan Camenisch, Jens Groth. Group Signatures: Better Efficiency and New Theoretical Aspects. In: *Security in Communication Networks (SCN 2004),* LNCS 3352, pp. 120-133. Springer-Verlag, 2005. BibTeX
- Liqun Chen, Caroline Kudla, and Kenneth G. Paterson. Concurrent Signatures. In: *EUROCRYPT 2004*, LNCS 3027, pp. 287-305. Springer-Verlag, 2004.
- Sherman S.M. Chow, Lucas C.K. Hui, S.M. Yiu. Identity Based Threshold Ring Signature. In: *Information Security and Cryptology - ICISC 2004,* LNCS ????, pp. ??-??. Springer-Verlag, 2005. Primary version is available at http://eprint.iacr.org/2004/179/.
- Xuhua Ding, Gene Tsudik, Shouhuai Xu. Leak-Free Group Signatures with Immediate Revocation. In: *Proc. of 24th International Conference on Distributed Computing Systems* (*ICDCS 2004*), pp.608-615. IEEE Computer Society, 2004.

- Yevgeniy Dodis, Aggelos Kiayias, Antonio Nicolosi, and Victor Shoup. Anonymous Identification in Ad Hoc Groups. In: *EUROCRYPT 2004*, LNCS 3027, pp. 609-626. Springer-Verlag, 2004.
- Jun Furukawa, Shoko Yonezawa. Group Signatures with Separate and Distributed Authorities. In: *Security in Communication Networks (SCN 2004)*, LNCS 3352, pp. 77-90. Springer-Verlag, 2005. BibTeX
- Ryotaro Hayashi, Tatsuaki Okamoto, and Keisuke Tanaka. An RSA Family of Trap-Door Permutations with a Common Domain and Its Applications. In: *Public Key Cryptography 2004*, LNCS 2947 , pp. 291-304. Springer-Verlag, 2004.
- Javier Herranz, Germán Sáez. New Identity-Based Ring Signature Schemes. In: *Information and Communications Security* (*ICICS 2004*), LNCS 3269, pp. 27-39. Springer-Verlag, 2004.
- Javier Herranz, Germán Sáez. Distributed Ring Signatures for Identity-Based Scenarios. http://eprint.iacr.org/2004/190/.
- Aggelos Kiayias and Moti Yung . Group Signatures: Provable Security, Efficient Constructions and Anonymity from Trapdoor-Holders. http://eprint.iacr.org/2004/076/.
- Joseph K. Liu, Victor K. Wei, Duncan S. Wong. Linkable Spontaneous Anonymous Group Signature for Ad Hoc Groups (Extended Abstract). In: *Information Security and Privacy* (*ACISP 2004*), LNCS 3108, pp. 325-335. Springer-Verlag, 2004.
- Joseph K. Liu, Duncan S. Wong. On The Security Models of (Threshold) Ring Signature Schemes. In: *Information Security and Cryptology - ICISC 2004,* LNCS ????, pp. ??-??. Springer-Verlag, 2005.
- Atsuko Miyaji and Kozue Umeda. A Fully-Functional Group Signature Scheme over Only Known-Order Group. In: *Applied Cryptography and Network Security* (*ACNS 2004*), LNCS 3089, pp. 164-179. Springer-Verlag, 2004.
- Toru Nakanishi, Yuji Sugiyama. A Group Signature Scheme with Efficient Membership Revocation for Reasonable Groups. In: *Information Security and Privacy* (*ACISP 2004*), LNCS 3108, pp. 336-347. Springer-Verlag, 2004.
- Lan Nguyen, Rei Safavi-Naini. Efficient and Provably Secure Trapdoor-free Group Signature Schemes from Bilinear Pairings. In: *ASIACRYPT 2004*, LNCS 3329, pp. 372-386. Springer-Verlag, 2004. Full version is available at http://eprint.iacr.org/2004/104/.
- Willy Susilo and Yi Mu. Deniable Ring Authentication Revisited. In: *Applied Cryptography and Network Security* (*ACNS 2004*), LNCS 3089, pp. 149-163. Springer-Verlag, 2004.
- Willy Susilo, Yi Mu, Fangguo Zhang. Perfect Concurrent Signature Schemes. In: *Information and Communications Security* (*ICICS 2004*), LNCS 3269, pp. 14-26. Springer-Verlag, 2004.
- Isamu Teranishi, Jun Furukawa, Kazue Sako. k-Times Anonymous Authentication. In: *ASIACRYPT 2004*, LNCS 3329, pp. 308-322. Springer-Verlag, 2004.
- Patrick P. Tsang, Victor K. Wei, Tony K. Chan, Man Ho Au, Joseph K. Liu, and Duncan S. Wong. Separable Linkable Threshold Ring Signatures. In: *INDOCRYPT 2004*, LNCS 3348, pp. 384-398. Springer- Verlag, 2004. Full version available at http://eprint.iacr.org/2004/267/.

- Victor K. Wei. A Bilinear Spontaneous Anonymous Threshold Signature for Ad Hoc Groups. http://eprint.iacr.org/2004/039/.
- Qianhong Wu, Xiaofeng Chen, Changjie Wang, Yumin Wang. Shared-Key Signature and Its Application to Anonymous Authentication in Ad Hoc Group. In: *Information Security* (*ISC 2004*), LNCS 3225, pp. 330-341. Springer-Verlag, 2004.
- Jing Xu, Zhenfeng Zhang, Dengguo Feng. A Ring Signature Scheme Using Bilinear Pairings. In: *Information Security Applications* (*WISA 2004*), LNCS 3325, pp. 160-169. Springer-Verlag, 2004. BibTeX

2005

- Mihir Bellare, Haixia Shi, Chong Zhang. Foundations of Group Signatures: The Case of Dynamic Groups. In: *Topics in Cryptology - CT-RSA 2005*, LNCS 3376, pp. 136-153. Springer-Verlag, 2005. BibTeX. Full version is available at http://eprint.iacr.org/2004/077/.
- Sherman S. M. Chow, Siu-Ming Yiu, Lucas Chi Kwong Hui. Efficient Identity Based Ring Signature. In: *Applied Cryptography and Network Security* (*ACNS 2005*), LNCS 3531, pp. 499-512. Springer-Verlag, 2005. BibTeX
- Jun Furukawa, Hideki Imai. An Efficient Group Signature Scheme from Bilinear Maps. In: *Information Security and Privacy* (ACISP 2005), LNCS 3574, pp. 455-467. Springer-Verlag, 2005. BibTeX
- Toshiyuki Isshiki, Keisuke Tanaka. An (n-t)-out-of-n Threshold Ring Signature Scheme. In: *Information Security and Privacy* (ACISP 2005), LNCS 3574, pp. 406-416. Springer-Verlag, 2005. BibTeX
- Aggelos Kiayias, Moti Yung. Group Signatures with Efficient Concurrent Join. In: *EUROCRYPT'05,* LNCS 3494, 198-214. Springer-Verlag, 2005. BibTeX
- Lan Nguyen. Accumulators from Bilinear Pairings and Applications. In: *Topics in Cryptology - CT-RSA 2005*, LNCS 3376, pp. 275-292. Springer-Verlag, 2005. BibTeX
- Lan Nguyen, Rei Safavi-Naini. Dynamic k-Times Anonymous Authentication. In: *Applied Cryptography and Network Security* (*ACNS 2005*), LNCS 3531, pp. 318-333. Springer-Verlag, 2005. BibTeX
- Toru Nakanishi, Fumiaki Kubooka, Naoto Hamada, Nobuo Funabiki. Group Signature Schemes with Membership Revocation for Large Groups. In: *Information Security and Privacy* (ACISP 2005), LNCS 3574, pp. 443-454. Springer-Verlag, 2005. BibTeX
- Patrick P. Tsang, Victor K. Wei. Short Linkable Ring Signatures for E-Voting, E-Cash and Attestation. In: *Information Security Practice and Experience* (*ISPEC 2005*), LNCS 3439, pp. 48-60. Springer-Verlag, 2005.
- Victor K. Wei. Tracing-by-Linking Group Signatures**.** In: *Information Security* (ISC 2005), LNCS 3650, pp. 149-163. Springer-Verlag, 2005. BibTeX
- Victor K. Wei, Tsz Hon Yuen, Fangguo Zhang. Group Signature Where Group Manager, Members and Open Authority Are Identity-Based. In: *Information Security and Privacy* (ACISP 2005), LNCS 3574, pp. 468-480. Springer-Verlag, 2005. BibTeX

10.4 Přehled literatury k tzv. skupinově orientovanému elektronickému podpisu (tzv. Group-Oriented signature)

1983

- K. Itakura, and K. Nakamura. A public key cryptosystem suitable for digital multisignatures. *NEC Research & Development*, 71:1-8, 1983.

1986

- C. Boyd. Digital multisignatures. *Cryptography and Coding*, 1986.

1987

- Y. Desmedt. Society and group oriented cryptography: a new concept. In: *Crypto'87,* LNCS 293, pp.120-127. Springer-Verlag, 1988.

1988

- T. Okamoto. A digital multisignature scheme using bijective public-key cryptosystem. *ACM Transactions on Computer Systems*, 1988, 6(8): 432-441.
-

1989

- C. Boyd. Digital multisignatures. In: Cryptography and Coding, pp. 241-246. Oxford University Press, 1989.
- Y. Desmedt, and Y. Frankel. Threshold cryptosystems. In: *Crypto'89,* LNCS 435, pp. 307-315. Springer-Verlag, 1990.
- L. Harn and T. Kresler. New scheme for digital multisignatures. *Electronics Letters*, July 1989, 25(15): 1002-1003.

1990

- T. Kiesler and L. Harn. RSA blocking and multisignature schemes with no bit expansion. *Electronics Letters*, Aug 1990, 26(18): 1490-1491.

1991

- C. Boyd. Multisignatures based on zero knowledge schemes. *Electronics Letters*, Oct 1991, 27(22): 2002-2004.

- Y. Desmedt, and Y. Frankel. Shared generation of authenticators and signatures. Crypto 91, 1991.
- T. Ohata, and T. Okamoto. A digital multisignature scheme based on the Fiat-Shamir scheme. In: *Asiacrypt'91,* LNCS 739, pp. 75-79. Springer-Verlag, 1991.
- T.P. Pedersen. A threshold cryptosystem without a trusted party. In: *Eurocrpt'91,* LNCS 547, pp. 522-526. Berlin: Springer-Verlag, 1991.

1992

- A. Fujioka, T. Okamoto, and K. Ohta. A practical digital multisignature scheme based on discrete logarithms. In: *Auscrypt'92,* LNCS 718, pp. 244-251. Springer-Verlag, 1992.
- L. Harn, and S. Yang. Group-oriented undeniable signature schemes without the assistance of a mutually trusted party. In: *Auscrypt'92,* LNCS 718, pp.133-142. Springer-Verlag, 1993.

1994

- Y. Desmedt. Threshold cryptography. *European Transactions on Telecommunications*, 5(4), 1994.
- L. Harn. Group-oriented (t, n) threshold digital signature scheme and multisignature. *IEE Proceedings - Computers and Digital Techniques*, 1994, 141(5): 307-313.
- L. Harn and Y. Xu. Design of generalised ElGamal type digital signature schemes based on discrete logarithm. *Electronics Letters*, Nov 1994, 30(24): 2025 -2026.
- L. Harn. New digital signature scheme based on discrete logarithm. *Electronics Letters*, Mar 1994, 30(5): 396-398.
- C-M. Li, T. Hwang and N-Y. Lee. Threshold-multisignature schemes where suspected forgery implies traceability of adversarial shareholders. In: *Eurocrypt'94,* LNCS 950, pp. 194-204. Springer-Verlag, 1995.

1995

- P. Horster, M. Michels, and H. Petersen. Meta-multisignature schemes based on the discrete logarithm problem. In: P*roc. of IFIP/SEC'95*, pp. 128-141. Chapman & Hall, 1995.
- P. Horster, M. Michels, and H. Peterson. Blind Multisignature Scheme Based on the Discrete Logarithm Problem. In: *Proc. of 12th Annual Computer Security Applications Conference* (*ACSAC'95*), 1996.
- C. G. Kang. New digital multisignature scheme in electronic contract systems. In: *Proc. of 1995 IEEE International Symposium on Information Theory*, pp. 486. IEEE, 1995.

1996

- R.Gennaro, S. Jarecki, H.Krawczyk, and T. Rabin. Robust threshold DSS signatures. In: *Eurocrypt'96,* LNCS 1070, pp. 354-371. Springer-Verlag, 1996. A modified version appeared in *Information and Computation*, 164(1): 54-84, 2001.
- S.K. Langford. Weaknesses in some threshold cryptosystems. In: *Crypto'96,* LNCS 1109, pp.74-82. Springer-Verlag, 1996.
- M. Michels, and P. Horster. On the risk of discruption in several multiparty signature schemes. In: *Asiacrypt'96,* LNCS 1163, pp.334-345. Springer-Verlag, 1996.
- C. Park, and K. Kurosawa. New Elgamal type threshold digital signature scheme. *IEICE Trans. Fundamentals*, January 1996, E79-A(1): 86-93.

1997

- C.-H. Wang, and T. Hwang. Threshold and Generalized DSS Signatures Without a Trusted Party. In: *Proceeding of the 13th Annual Computer Security Applications Conference (ACSAC'97)*, pp. 221-226. IEEE Computer Society, 1997.
- H. Petersen, and M. Michels. On signatures schemes with threshold verification detecting malicious verifiers. In: *Workshop on Security Protocols'97*, LNCS 1361, pp.67-78. Berlin: Springer-Verlag, 1997.
- S. Russell. Multisignature algorithms for ISO 9796. *ACM SIGSAC Security Audit & Control Review*, January 1997, 15(1): 11-14.

1998

- T. Rabin. A simplified approach to threshold and proactive RSA. In: Crypto 98, LNCS1462, pp. . 1998.

1999

- R. Canetti, R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin. Adaptive security for threshold cryptosystems. In *Crypto'99,* LNCS 1666, pp. 98-115. Berlin: Springer-Verlag, 1999.
- R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin. Secure distributed key generation for discrete-log based cryptosystems. In: Eurocrypt'99, LNCS 1592, pp. 295-310. Berlin: Springer-Verlag, 1999.
- L. Harn. Digital multisignature with distinguished signing authorities. *Electronics Letters*, Feb 1999, 35(4): 294-295.
- K. Ohta and T. Okamoto. Multi-signature scheme secure against active insider attacks. *IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences*, E82-A(1): 21-31, 1999.
- H.-M. Sun. An efficient nonrepudiable threshold proxy signature scheme with known signers. *Computer Communications*, May 1999, 22(8): 717-722.

2000

- Y.-S. Chang, T.-C. Wu and S.-C. Huang. ElGamal-like digital signature and multisignature schemes using self-certified public keys. *Journal of Systems and Software*, February 2000, 50(2): 99-105.
- H. Doi, M. Mambo, and E. Okamoto. On the Security of the RSA-Based Multisignature Scheme for Various Group Structures. In: *Information Security and Privacy (ACISP'00), LNCS 1841*, pp. 352-367. Springer-Verlag, 2000.
- B. King. Algorithms to Speed Up Computations in Threshold RSA. In: *Information Security and Privacy (ACISP'00),* LNCS 1841, pp. 2443-456. Springer-Verlag, 2000.
- B. King. Improved Methods to Perform Threshold RSA. In: *ASIACRYPT 2000,* LNCS 1976, pp. 359-372. Springer-Verlag, 2000.
- C-M. Li, T. Hwang, N-Y. Lee, and J-J.Tsai. (*t*, *n*) threshold-multisignature schemes and generalized-multisignature scheme where suspected forgery implies traceability of adversarial shareholders. Cryptologia, July 2000, 24(3): 250-268.
- Z.C Li, L.C.K. Hui, K.P. Chow, C.F. Chong, W.W. Tsang, and H.W. Chan. Cryptanalysis of Harn digital multisignature scheme with distinguished signing authorities [comment]. *Electronics Letters*, Feb 2000, 36(4): 314-315.
- J. Merkle. Multi-round passive attacks on server-aided RSA protocols. In: *Proc. of the 7th ACM Conference on Computer and Communications Security (CCS 2000)*, pp. 102 - 107. ACM, 2000.
- S. Mitomi and A. Miyaji. A Multisignature Scheme with Message Flexibility, Order Flexibility and Order Verifiability. In: *Information Security and Privacy (ACISP'00),* LNCS 1841, pp. 298-312. Springer-Verlag, 2000.
- S.-P. Shieh, C.-T. Lin; W.-B. Yang, and H.-M. Sun. Digital multisignature schemes for authenticating delegates in mobile code systems. *IEEE Transactions on Vehicular Technology*, Jul 2000, 49(4): 1464 -1473.
- V. Shoup. Practical Threshold Signatures. In: *Eurocrypt 2000,* LNCS 1807, pp. 207-220. Springer-Verlag, 2000.

2001

- I. Damgård, and M. Koprowski. Practical threshold RSA signatures without a trusted dealer. In: *Eurocrypt'01,* LNCS 2045, pp. 152-165. Springer-Verlag, 2001. .
- P.-A. Fouque, and J. Stern. One round threshold discrete-log key generation without private channels. In: *PKC'01,* LNCS 1992, pp. 300-316. Berlin: Springer-Verlag, 2001.
- P.-A. Fouque, and D. Pointcheval. Threshold cryptosystems secure against chosen-ciphertext attacks. In: *Asiacrypt'01,* LNCS 2248, pp. 351-368. Berlin: Springer-Verlag, 2001.
- P.-A. Fouque and J. Stern. Fully Distributed Threshold RSA under Standard Assumptions. In: *ASIACRYPT 2001,* LNCS 2248, pp. 310-330. Springer-Verlag, 2001.

- R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin. Robust threshold DSS signatures. *Information and Computation*, 164(1): 54-84, 2001. An earlier version appeared in *Eurocrypt'96*.
- J. Hoffstein, J. Pipher, and J. H. Silverman. NSS: An NTRU Lattice-Based Signature Scheme. In: *EUROCRYPT 2001,* LNCS 2045, pp. 211-228. Springer-Verlag, 2001.
- Chih-Yin Lin, Tzong-Chen Wu, Jing-Jang Hwang. ID-Based Structured Mulitsignature Schemes. *Network Security 2001*: 45-60. *IFIP TC11 WG11.4 First Annual Working Conference on Network Security*, November 26-27, 2001, Leuven, Belgium. IFIP Conference Proceedings 206 Kluwer 2001, ISBN 0-7923-7558-0.
- A. Lysyanskaya and C. Peikert. Adaptive Security in the Threshold Setting: From Cryptosystems to Signature Schemes. In: ASIACRYPT 2001, LNCS 2248, pp. 331-350. Springer-Verlag, 2001.
- P. D. MacKenzie and M. K. Reiter. Two-Party Generation of DSA Signatures. In: *CRYPTO 2001,* LNCS 2139, pp. 137-154. Springer-Verlag, 2001.
- S. Micali, K. Ohta, and L. Reyzin. Accountable-subgroup multisignatures: extended abstract. In: *Proc. of the 8th ACM Conference on Computer and Communications Security (CCS 2001)*, pp. 245-254. ACM, 2001.
- Reihaneh Safavi-Naini, Huaxiong Wang, Kwok-Yan Lam: A New Approach to Robust Threshold RSA Signature Schemes. In: ICISC 1999, LNCS 1787, pp. 184-196.
- D.R. Stinson, and R. Strobl. Provably secure distributed Schnorr signatures and a (t, n) threshold scheme for implicit certificates. In: *ACISP'01,* LNCS 2119, pp. 417-434. Springer-Verlag, 2001.
- T.-C. Wu, C.-C. Huang and D.-J. Guan. Delegated multisignature scheme with document decomposition. *Journal of Systems and Software*, January 2001, 55(3): 321-328.

2002

- H.-Y. Chien, J.-K. Jan, and Y.-M. Tseng. Forgery attacks on "Multisignature schemes for authenticating mobile code delegates". *IEEE Transactions on Vehicular Technology*, Nov 2002, 51(6): 1669-1671.
- Y. Frankel, P. D. MacKenzie, and M. Yung. Adaptively secure distributed public-key systems. *Theoretical Computer Science*, 2002, 287(2): 535-561.
- Yi Mu, Vijay Varadharajan. Group Cryptography: Signature and Encryption. *Informatica (Slovenia)*, 2002, 26(3): 249-254.
- S.-F. Pon, E.-H. Lu, and J.-Y. Lee. Dynamic reblocking RSA-based multisignatures scheme for computer and communication networks. *IEEE Communications Letters*, Jan 2002, 6(1): 43-44.
- Mitsuru Tada. An Order-Specified Multisignature Scheme Secure against Active Insider Attacks. In: *Information Security and Privacy (ACISP'02),* LNCS 2384, pp. 328-345. Springer-Verlag, 2002.
- G. Wang. On the security of the Li-Hwang-Lee-Tsai threshold group signatures scheme. In: *Information Security and Cryptography (ICISC 2002),* LNCS 2587, pp. 75-89. Springer-Verlag, 2003.

- X. Yi and C. K. Siew. Attacks on Shieh-Lin-Yang-Sun digital multisignature schemes for authenticating delegates in mobile code systems. *IEEE Transactions on Vehicular Technology*, Nov 2002, 51(6): 1313-1315.

2003

- A. Boldyreva. Threshold Signatures, Multisignatures and Blind Signatures Based on the Gap-Diffie-Hellman-Group Signature Scheme. In: *Public Key Cryptography - PKC 2003,* LNCS 2567, pp. 31–46. Springer-Verlag, 2003.
- D. Boneh, C. Gentry, B. Lynn, and H. Shacham. Aggregate and Verifiably Encrypted Signatures from Bilinear Maps. In: *EUROCRYPT 2003,* LNCS 2656, pp. 416-432. Springer-Verlag, 2003.
- I. Damgård and M. Jurik. A Length-Flexible Threshold Cryptosystem with Applications. In: *Information Security and Privacy (ACISP'03),* LNCS 2727, pp. 350-364. Springer-Verlag, 2003.
- Javier Herranz, Carles Padró, and Germán Sáez. Distributed RSA Signature Schemes for General Access Structures In: *Information Security* (*ISC 2003*), LNCS 2851, pp. 122-136. Springer-Verlag, 2003.
- K. Kawauchi and M. Tada. On the Exact Security of Multi-signature Schemes Based on RSA. In: *Information Security and Privacy (ACISP'03),* LNCS 2727, pp. 336-349. Springer-Verlag, 2003.
- Dongjin Kwak and Sangjae Moon. Efficient Distributed Signcryption Scheme as Group Signcryption. In: *Applied Cryptography and Network Security (ACNS'03)*, LNCS 2846, pp. 403-417. Springer-Verlag, 2003.
- Li-Shan Liu, Cheng-Kang Chu, and Wen-Guey Tzeng. A Threshold GQ Signature Scheme. In: *Applied Cryptography and Network Security (ACNS'03)*, LNCS 2846, pp. 137-150. Springer-Verlag, 2003.
- P. D. MacKenzie. An Efficient Two-Party Public Key Cryptosystem Secure against Adaptive Chosen Ciphertext Attack. In: *Public Key Cryptography - PKC 2003,* LNCS 2567, pp. 47-61. Springer-Verlag, 2003.
- A. Nicolosi, M. Krohn, Y. Dodis, and D. Mazieres. Proactive Two-Party Signatures for User Authentication. In: *Proceedings of NDSS'03*. http://www.isoc.org/isoc/conferences/ndss/03/proceedings/index.htm
- Rui Zhang and Hideki Imai. Round Optimal Distributed Key Generation of Threshold Cryptosystem Based on Discrete Logarithm Problem. In: *Applied Cryptography and Network Security (ACNS'03)*, LNCS 2846, pp. 96-110. Springer-Verlag, 2003.
- Guilin Wang, Xiaoxi Han, and Bo Zhu. On the Security of Two Threshold Signature Schemes with Traceable Signers. In: *Applied Cryptography and Network Security (ACNS'03),* LNCS 2846, pp. 111-122. Springer-Verlag, 2003.

- T.-C. Wu and C.-L. Hsu. Cryptanalysis of Digital Multisignature Schemes for Authenticating Delegates in Mobile Code Systems. *IEEE Transactions on Vehicular Technology*, March 2003, 52(2): 462 -465.
- S. Xu and R. Sandhu. Two Efficient and Provably Secure Schemes for Server-Assisted Threshold Signatures In: *CT-RSA 2003,* LNCS 2612, p. 355-372. Springer-Verlag, 2003.

- Anna Lysyanskaya, Silvio Micali, Leonid Reyzin, Hovav Shacham. Sequential Aggregate Signatures from Trapdoor Permutations. In: *EUROCRYPT 2004*, LNCS 3027, pp. 74-90. Springer-Verlag, 2004.

2004

- Masayuki Abe, Serge Fehr. Adaptively Secure Feldman VSS and Applications to Universally-Composable Threshold Cryptography. In: *CRYPTO 2004,* LNCS 3152, pp. 317-334. Springer-Verlag, 2004. Full version available at http://eprint.iacr.org/2004/119/.
- Claude Castelluccia, Stanislaw Jarecki, Jihye Kim, Gene Tsudik. A Robust Multisignatures Scheme with Applications to Acknowledgment Aggregation. In: *Security in Communication Networks (SCN 2004),* LNCS 3352, pp. 193-207. Springer-Verlag, 2005. BibTeX
- Xiaofeng Chen, Fangguo Zhang, Divyan M. Konidala, Kwangjo Kim. New ID-based Threshold Signature Scheme from Bilinear Pairings. In: *INDOCRYPT 2004*, LNCS 3348, pp. 371-383. Springer- Verlag, 2004.
- Giovanni Di Crescenzo, Gonzalo R. Arce, Renwei Ge. Threshold Cryptography for Mobile Ad Hoc Networks. In: *Security in Communication Networks (SCN 2004),* LNCS 3352, pp. 91-104. Springer-Verlag, 2005. BibTeX
- Sherman S. M. Chow, Lucas C.K. Hui, S.M. Yiu, K.P. Chow. Secure Hierarchical Identity Based Signature and its Application. In: *Information and Communications Security* (*ICICS 2004*), LNCS 3269, pp. 480-494. Springer-Verlag, 2004.
- Sherman S.M. Chow, Lucas C.K. Hui, S.M. Yiu. Identity Based Threshold Ring Signature. In: *Information Security and Cryptology - ICISC 2004,* LNCS ????, pp. ??-??. Springer-Verlag, 2005. Primary version is available at http://eprint.iacr.org/2004/179/.
- Javier Herranz, Germán Sáez. Distributed Ring Signatures for Identity-Based Scenarios. http://eprint.iacr.org/2004/190/.
- Fabien Laguillaumie, Damien Vergnaud. Multi-Designated Verifiers Signatures. In: *Information and Communications Security* (*ICICS 2004*), LNCS 3269, pp. 495-507. Springer-Verlag, 2004.
- Einar Mykletun, Maithili Narasimha, Gene Tsudik. Signature Bouquets: Immutability for Aggregated/Condensed Signatures. http://eprint.iacr.org/2004/091/.
- Patrick P. Tsang, Victor K. Wei, Tony K. Chan, Man Ho Au, Joseph K. Liu, and Duncan S. Wong. Separable Linkable Threshold Ring Signatures. In: *INDOCRYPT 2004*, LNCS 3348, pp. 384-398. Springer- Verlag, 2004. Full version available at http://eprint.iacr.org/2004/267/.
- Victor K. Wei. A Bilinear Spontaneous Anonymous Threshold Signature for Ad Hoc Groups. http://eprint.iacr.org/2004/039/.
- Jing Xu, Zhenfeng Zhang, Dengguo Feng. Identity Based Threshold Proxy Signature. http://eprint.iacr.org/2004/250/.

2005

- Ivan Damgård, Kasper Dupont. Efficient Threshold RSA Signatures with General Moduli and No Extra Assumptions. In: *Public Key Cryptography - PKC 2005*, LNCS 3386, pp. 346-361. Springer-Verlag, 2005. BibTeX
- Toshiyuki Isshiki, Keisuke Tanaka. An (n-t)-out-of-n Threshold Ring Signature Scheme. In: *Information Security and Privacy* (ACISP 2005), LNCS 3574, pp. 406-416. Springer-Verlag, 2005. BibTeX
- Stanislaw Jarecki, Nitesh Saxena. Further Simplifications in Proactive RSA Signatures. In: *Theory of Cryptography* (*TCC 2005*), LNCS 3378, pp. 510-528. Springer-Verlag, 2005. BibTeX
- Brian King. An Efficient Implementation of a Threshold RSA Signature Scheme. In: *Information Security and Privacy* (ACISP 2005), LNCS 3574, pp. 382-393. Springer-Verlag, 2005. BibTeX

10.5Přehled literatury k elektronickému podpisu bez viditelnosti podepisující osoby (tzv. blind signature)

1982

- D. Chaum. Blind signatures for untraceable payments. In *Crypto'82*, pp. 199-203. New York: Plenum Press, 1983.

1983

- D. Chaum. Blind signature system. In: *Advances in Cryptology, Proceedings of CRYPTO'83*, pp. 153. New York: Plenum Press, 1984.

1987

- D. Chaum. Blinding for unanticipated signatures. In: *Eucrypt'87, LNCS 304*, pp. 227-236. Springer-Verlag, 1987.

1988

- D. Chaum, A. Fiat, and M. Naor. Untraceable electronic cash. In: *Crypto'88, LNCS 403*, pp. 319–327. Springer-Verlag, 1990.

1990

- K. Ohta, T. Okamoto, and K. Koyama. Membership authentication for hierarchical multigroups using the extended Fiat-Shamir scheme. In: *Eurocrypt'90, LNCS 473,* , pp. 446-457. Springer-Verlag, 1990.

1992

- S. von Solms, and D. Naccache. On blind signatures and perfect crimes. *Computers & Security*, 11: 581–583, 1992.

1994

- J.L. Camenisch, J.-M. Piveteau, and M.A. Stadler. Blind signatures based on the discrete logarithm problem. In: *Eurocrypt'94, LNC 950*, pp. 428-432. Springer-Verlag, 1994.

- L. Chen, I.B. Damgard, and T.P. Pedersen. Parallel divertibility of proofs of knowledge. In: *Eurocrypt'94 LNCS 950*, pp. 140-155. Springer-Verlag, 1994.

1995

- S. Brands. Restrictive blinding of secret-Key certificates. In: *Eurocrypt'95, LNCS 921*, pp. 231-247. Springer-Verlag, 1995.
- M. Stadler, J.-M. Piveteau, and J. Camenisch. Fair blind signatures. In: *Eurocrypt'95, LNCS 921*, pp. 209-219. Springer-Verlag, 1995.

1996

- M. Abe, and E. Fujisaki. How to date blind signatures. In: *Asiacrypt'96, LNCS 1163*, pp. 244–251. Springer-Verlag, 1996.
- W. S. Juang and C. L. Lei. Blind threshold signatures based on discrete logarithm. In: *Proc. of the 2nd Asian Computing Science Conference, LNCS 1179*, pp. 172-181. Springer-Verlag, 1996.
- D. Pointcheval, And J. Stern. Provably secure blind signature schemes. In: *Asiacrypt '96, LNCS 1163*, pp. 252-265. Springer-Verlag, 1996.
- C. Radu, R. Govaerts, and J. Vanderwalle. A restrictive blind signature scheme with applications to electronic cash. In: *Communications and Multimedia Security II*, pp. 196–207. London: Chapman & Hall, 1996.

1997

- A. Juels, M. Luby, and R. Ostrovsky. Security of blind digital signatures. In: *Crypto'97, LNCS* 1294, pp. 150–164. Springer-Verlag, 1997.
- D. Pointcheval, and J. Stern. New blind signatures equivalent to factorization (extended abstract) In *Proceedings of the 4th ACM conference on Computer and Communications Security,* pp.92-99. ACM press, 1997.

1998

- M. Blaze, G. Bleumer, and M. Strauss. Divertible protocols and atomic proxy cryptography. In: *Eurocrypt'98, LNCS 1403*, pp. 127-144. Berlin: Springer-Verlag, 1998.
- C.I. Fan, and C.L. Lei. User efficient blind signatures. *Electronics Letters*, 1998, 34(6): 544–546.
- A. Lysyanskaya, and Z. Ramzan. Group blind digital signatures: A scalable solution to electronic cash. In: *Financial Cryptography (FC'98), LNCS 1465*, pp. 184-197. Springer-Verlag, 1998.

- S. Miyazaki, K. Sakurai. A more efficient untraceable e-cash system with partially blind signatures based on the discrete logarithm problem. In: *Financial Cryptography (FC'98), LNCS 1465*, pp. 296-308. Springer-Verlag, 1998.
- D. Pointcheval. Strengthened security for blind signatures. In: *Eurocrypt'98, LNCS 1403*, pp. 391–405. Springer-Verlag, 1998.
- A. de Solages, and J. Traor. An efficient fair offline electronic cash system with extensions to checks and wallets with observers. In: *Financial Cryptography (FC'98), LNCS 1465*, pp. 275-295. Springer-Verlag, 1998.

1999

- F. Bao, and R.H. Deng. A new type of "Magic Ink" signatures - Towards transcript-irrelevant anonymity revocation. In: *Public Key Cryptography* (*PKC'99*), *LNCS 1560*, pp. 1-11. Springer-Verlag, 1999.
- H.-W. Lee, and T.-Y. Kim. Message recovery fair blind signature. In: *Public Key Cryptography* (*PKC'99*), *LNCS 1560*, pp. 97-111. Springer-Verlag, 1999.

2000

- M. Abe, and T. Okamoto. Provably secure partially blind signatures. In: *Crypto 2000, LNCS 1880*, pp. 271–286. Springer-Verlag, 2000.
- G. Bleumer. Secure PC-franking for everyone. In: *Electronic Commerce and Web Technologies (EC-Web 2000), LNCS 1875*, pp. 94-109. Springer-Verlag, 2000.
- D. Pointcheval, and J. Stern. Security arguments for digital signatures and blind signatures. *Journal of Cryptology*, 13(3): 361-396, 2000.
- T. Sander, A. Ta-Shma, and M. Yung. Blind, Auditable Membership Proofs. In: *Financial Cryptography (FC'00), LNCS 1962*, pp. 53-71. Springer-Verlag, 2000.
- Z. Shao. Improved user efficient blind signatures. *Electronics Letters*, 2000, 36(16), pp. 1372–1374.

2001

- M. Abe. A secure three-move blind signature scheme for polynomially many signatures. In: *Eurocrypt'01, LNCS 2045*, pp. 136-151. Springer-Verlag, 2001.
- M. Abe, and M. Ohkubo. Provably secure fair blind signatures with tight revocation. In: *Asiacrypt 2001, LNCS 2248*, pp. 583-602. Springer-Verlag, 2001.
- M. Bellare, C. Namprempre, D. Pointcheval and M. Semanko. The one-more-RSA-inversion problems and the security of Chaum's blind signature scheme. In: *Financial Cryptography'01, LNCS 2339*, pp. 319-338. Springer-Verlag, 2001.
- C.-C. Chang, and I.-C. Lin. Cryptanalysis of the improved user efficient blind signatures. In: *Information and Communications Security* (*ICICS 2001*), *LNCS 2229*, pp. 42-46. Springer-Verlag, 2001.

- J. Kim, K. Kim, and C. Lee. An efficient and provably secure threshold blind signature. In: *ICISC 2001, LNCS 2288*, pp. 318-327. Springer-Verlag, 2002.
- C.P. Schnorr. Security of blind discrete Log signatures against interactive attacks. In: *Information and Communications Security* (*ICICS 2001*), *LNCS 2229*, pp. 1-12. Springer-Verlag, 2001.

2002

- S. Kim, and H. Oh. A New Electronic Check System with Reusable Refunds. *International Journal of Information Security*, 2002, 1(3): pp. 175-188.
- C.-L. Lei, W.-S. Juang, and P.-L. Yu. Provably Secure Blind Threshold Signatures Based on Discrete Logarithm. *Journal of Information Science and Engineering*, Jan. 2002, 18(1): 23-39.
- G. Maitland, and C. Boyd. A Provably Secure Restrictive Partially Blind Signature Scheme. In: *Public Key Cryptography* (*PKC 2002*), *LNCS 2274*, pp. 99–114. Springer-Verlag, 2002.
- D. Wagner. A Generalized Birthday Problem. In: *Crypto'02, LNCS 2442*, pp. 288-303. Springer-Verlag, 2002.
- F. Zhang, and K. Kim. ID-based Blind Signature and Ring Signature from Pairings. In: *Asiacrypt 2002, LNCS 2501*, pp. 533–547. Springer-Verlag, 2002.

2003

- A. Boldyreva. Threshold Signatures, Multisignatures and Blind Signatures Based on the Gap-Diffie-Hellman-Group Signature Scheme. In: *PKC 2003, LNCS 2567*, pp. 31–46. Springer-Verlag, 2003.
- Dang Nguyen Duc, Jung Hee Cheon, and Kwangjo Kim. A Forward-Secure Blind Signature Scheme Based on the Strong RSA Assumption. In: *Information and Communications Security* (*ICICS'03*), *LNCS 2836*, pp. 11-21. Springer-Verlag, 2003.
- Yan Wang, Shuwang Lu, Zhenhua Liu. A Simple Anonymous Fingerprinting Scheme Based on Blind Signature. In: *Information and Communications Security* (*ICICS'03*), *LNCS 2836*, pp. 260-268. Springer-Verlag, 2003.
- F. Zhang and K. Kim. Efficient ID-based Blind Signature and Proxy Signature from Bilinear Pairings. In: *Information Security and Privacy* (*ACISP'03*), *LNCS 2727,* pp. 312-323. Springer-Verlag, 2003.
- Fangguo Zhang, Reihaneh Safavi-Naini, and Willy Susilo. Efficient Verifiably Encrypted Signature and Partially Blind Signature from Bilinear Pairings. In: *INDOCRYPT 2003*, LNCS 2904, pp. 191-204. Berlin: Springer- Verlag, 2003. Revised version is available at http://eprint.iacr.org/2004/004/.

2004

- Jan Camenisch, Maciej Koprowski, Bogdan Warinschi. Efficient Blind Signatures Without Random Oracles. In: *Security in Communication Networks (SCN 2004),* LNCS 3352, pp. 134-148. Springer-Verlag, 2005. BibTeX

- Sherman S.M. Chow, Lucas C.K. Hui, S.M. Yiu, K.P. Chow. Two Improved Partially Blind Signature Schemes from Bilinear Pairings. http://eprint.iacr.org/2004/108/.
- Lihua Liu, Zhengjun Cao. Universal Forgeability of a Forward-Secure Blind Signature Scheme Proposed by Duc et al. http://eprint.iacr.org/2004/262/.
- Fuw-Yi Yang, Jinn-Ke Jan. A Provably Secure Scheme for Restrictive Partially Blind Signatures. http://eprint.iacr.org/2004/037/.
- Fuw-Yi Yang, Jinn-Ke Jan. A Provable Secure Scheme for Partially Blind Signatures. http://eprint.iacr.org/2004/230/.

2005

- Amit K Awasthi and Sunder Lal. Proxy Blind Signature Scheme. *Transaction on Cryptology*, 2(1): 5-11 , Jan 2005.
- Sherman S. M. Chow, Lucas Chi Kwong Hui, Siu-Ming Yiu, K. P. Chow. Two Improved Partially Blind Signature Schemes from Bilinear Pairings. In: *Information Security and Privacy* (ACISP 2005), LNCS 3574, pp. 316-328. Springer-Verlag, 2005. BibTeX

10.6 Přehled literatury k elektronickému podpisu, u kterého podepisovatel může zjistit podvrh padělatele s neomezenou výpočetní silou (tzv. fail-stop signature)

1990

- B. Pfitzmann, and M. Waidner. Formal aspects of fail-stop signatures. Interner Bericht, Fakultät für Informatik, 22/90, 1990.

1991

- Gerrit Bleumer, Birgit Pfitzmann, Michael Waidner. A remark on a signature scheme where forgery can be proved. In: *Eurocrypt '90*, LNCS 473, 441-445. Berlin: Springer-Verlag, 1991.
- Birgit Pfitzmann, Michael Waidner. Fail-stop signatures and their application. In: *Proc. of 9th Worldwide Congress on Computer and Communications Security and Protection* (*Securicom'91*), pp. 145-160. Paris, 19-22 March, 1991.
- Birgit Pfitzmann. Neu und sicher: Digitale Fail-stop-Signaturen KES - Zeitschrift für Kommunikations- und EDV-Sicherheit 7/5 (1991), pp. 321-326.
- B. Pfitzmann. Fail-stop signatures: Principles and applications. In: *Proc. Compsec'91, 8th world conference on computer security, audit and control*, pp. 125–134, 1991.
- B. Pfitzmann, and M. Waidner. Fail-stop-signaturen und ihre Anwendung. In: *VIS'91*, pp. 289-301. Berlin: Springer-Verlag, 1991.

1992

- E. van Heijst, and T. Pedersen. How to make efficient fail-stop signatures. In: *Eurocrypt'92,* LNCS 658, pp. 337–346. Berlin: Springer-Verlag, 1992.
- E. van Heijst, T. Pedersen, and B. Pfitzmann. New constructions of fail-stop signatures and lower bounds. In: *Crypto'92,* LNCS 740, pp.15–30. Berlin: Springer-Verlag, 1993.

1993

- I. Damgård, T.P. Pedersen, and B. Pfitzmann. On the existence of statistically hiding bit commitment schemes and fail-stop signatures. In: *Crypto'93,* LNCS 773, pp. 250-265. Berlin: Springer-Verlag, 1993.

1994

- B. Pfitzmann. Fail-stop signatures without trees. Hildesheimer Informatik-Berichte, Institut für Informatik, 16/94, 1994.

1996

- B. Pfitzmann. Digital signature schemes – General framework and fail-stop signatures. *Lecture Notes in Computer Science 1100*, Springer-Verlag, 1996.

1997

- N. Baric, and B. Pfitzmann. Collision-free accumulators and fail-stop signature schemes without trees. In: *Eurocrypt'97,* LNCS 1233, pp. 480–494. 1997. Berlin: Springer-Verlag, 1997.
- I. Damgård, T.P. Pedersen, and B. Pfitzmann. On the existence of statistically hiding bit commitment schemes and fail-stop signatures. *Journal of Cryptology*, 1997, 10(3): 163-194.
- T.P. Pedersen, and B. Pfitzmann. Fail-stop signatures. *SIAM Journal on Computing*, 1997, 26(2): 291–330.

1999

- R. Safavi-Naini, and W. Susilo. A general construction for fail-stop signature using authentication codes. In: *Proc. of Workshop on Cryptography and Combinatorial Number Theory* (*CCNT'99*), Birkhäuser, pp. 343–356, 1999.
- W. Susilo, R. Safavi-Naini, and J. Pieprzyk. RSA-based fail-stop signature schemes. *International Workshop on Security* (*IWSEC'99*), pp. 161-166. IEEE Computer Society Press, 1999.
- W. Susilo, R. Safavi-Naini, and J. Pieprzyk. Fail-stop threshold signature schemes based on elliptic curves. In: *Information Security and Privacy* (*ACISP'99*), LNCS 1587, pp. 103-116. Berlin: Springer-Verlag, 1999.

2000

- Y. Mu and V. Varadharajan: Fail-Stop Confirmer Signatures. In: *Information Security and Privacy (ACISP'00),* LNCS 1841, pp. 368-377. Springer-Verlag, 2000.

- R. Safavi-Naini, W. Susilo, and H. Wang. Fail-stop signature for long messages. In: *Indocrypt'00,* LNCS 1977, pp. 165-177. Berlin: Springer-Verlag, 2000.
- R. Safavi-Naini, and W. Susilo. Threshold fail-stop signature schemes based on discrete logarithm and factorization. In: *Information Security* (*ISW'00*), LNCS 1975, pp. 292-307.
- W. Susilo, R. Safavi-Naini, M. Gysin, and J. Seberry. A New and Efficient Fail-Stop Signature schemes. *The Computer Journal,* 2000, 43(5): 430–437.

2001

- R. Safavi-Naini, W. Susilo, and H. Wang. An efficient construction for fail-stop signatures for long messages. *Journal of Information Science and Engineering* (*JISE*) - *Special Issue on Cryptology and Information Security,* 2001, 17: 879 – 898.
- R. Safavi-Naini, W. Susilo, and H. Wang. How to construct fail-stop confirmer signature schemes. In: *Information Security and Privacy* (*ACISP'01*), LNCS 2119, pp. 435-444. Berlin: Springer-Verlag, 2001.

2002

- W. Susilo, and R. Safavi-Naini. An efficient fail-stop signature scheme based on factorization. In: *Information Security and Cryptology – ICISC 2002,* LNCS 2587, pp. 62-74. Berlin: Springer-Verlag, 2003.

2004

- Katja Schmidt-Samoa. Factorization-based Fail-Stop Signatures Revisited. In: *Information and Communications Security* (*ICICS 2004*), LNCS 3269, pp. 118-131. Springer-Verlag, 2004.

10.7Přehled literatury k tzv. forward-secure elektronickému podpisu

1997

- R. Anderson. Invited Lecture. *4th ACM Computer and Communications Security*, 1997.

1999

- M. Bellare and S. Miner. A forward-secure digital signature scheme. In: *CRYPTO'99,* LNCS 1666, pp. 431-448. Springer-Verlag, 1999.

2000

- M. Abdalla and L. Reyzin. A New Forward-Secure Digital Signature Scheme. In: *ASIACRYPT 2000,* LNCS 1976, pp. 116-129. Springer-Verlag, 2000.
- H. Krawczyk. Simple forward-secure signatures from any signature scheme. . In: *Proc. of the 7th ACM Conference on Computer and Communications Security (CCS 2000)*, pp. 108-115. ACM, 2000.
- D. Park, C. Boyd, and S.-J. Moon. Forward Secrecy and Its Application to Future Mobile Communications Security. In: *Public Key Cryptography* (*PKC'00*), LNCS 1751, pp. 433-445. Springer-Verlag, 2000.

2001

- Y. Dodis, A. Sahai, and A. Smith. On Perfect and Adaptive Security in Exposure-Resilient Cryptography. In: *EUROCRYPT 2001,* LNCS 2045, pp. 301-324. Springer-Verlag, 2001.
- G. Itkis and L. Reyzin. Forward-secure signatures with optimal signing and verifying. In: *CRYPTO'01,* LNCS 2139, pp. 332-354. Springer-Verlag, 2001.

2002

- Y. Dodis, J. Katz, S. Xu, and M. Yung. Key-Insulated Public Key Cryptosystems. In: *EUROCRYPT 2002,* LNCS 2332, pp. 65-82. Springer-Verlag, 2002.
- G. Itkis and L. Reyzin. SiBIR: Signer-Base Intrusion-Resilient Signatures. In: *CRYPTO 2002,* LNCS 2442, pp. 499-514. Springer-Verlag, 2002.

- G. Itkis. Intrusion-Resilient Signatures: Generic Constructions, or Defeating Strong Adversary with Minimal Assumptions. In: *Security in Communication Networks (SCN 2002),* LNCS 2576, pp. 102-118. Springer-Verlag, 2002.
- J. Katz, R. Ostrovsky, and Moti Yung. Forward Secrecy in Password-Only Key Exchange Protocols. In: *Security in Communication Networks (SCN 2002),* LNCS 2576, pp. 29-44. Springer-Verlag, 2002.
- A. Kozlov and L. Reyzin. Forward-Secure Signatures with Fast Key Update. In: *Security in Communication Networks (SCN 2002),* LNCS 2576, pp. 241-256. Springer-Verlag, 2002.
- D. Kwak, J. Ha, H. Lee, H. Kim, and S. Moon. A WTLS handshake protocol with user anonymity and forward secrecy. In: *CDMA International Conference - CIC'2002,* LNCS 2524, pp. 219-230. Springer-Verlag, 2002.
- G. Tsudik. Weak Forward Security in Mediated RSA. In: *Security in Communication Networks (SCN 2002),* LNCS 2576*,* pp. 45-54. Springer-Verlag, 2002.
- Jianying Zhou. Maintaining the Validity of Digital Signatures in B2B Applications. In: *Information Security and Privacy (ACISP'02),* LNCS 2384, pp. 303-315. Springer-Verlag, 2002.

2003

- R. Canetti, S. Halevi, and J. Katz. A Forward-Secure Public-Key Encryption Scheme. In: *EUROCRYPT 2003,* LNCS 2656, pp. 255-271. Springer-Verlag, 2003.
- Y. Dodis, J. Katz, S. Xu, and M. Yung. Strong Key-Insulated Signature Schemes. In: *Public Key Cryptography - PKC 2003,* LNCS 2567, pp. 130-144. Springer-Verlag, 2003.
- Y. Dodis, M. K. Franklin, J. Katz, A. Miyaji, and M. Yung. Intrusion-Resilient Public-Key Encryption. In: *CT-RSA 2003,* LNCS 2612, pp. 19-32. Springer-Verlag, 2003.
- Dang Nguyen Duc, Jung Hee Cheon, and Kwangjo Kim. A Forward-Secure Blind Signature Scheme Based on the Strong RSA Assumption. In: *Information and Communications Security* (*ICICS'03*), LNCS 2836, pp. 11-21. Springer-Verlag, 2003.
- Gene Itkis and Peng Xie. Generalized Key-Evolving Signature Schemes or How to Foil an Armed Adversary. In: *Applied Cryptography and Network Security (ACNS'03)*, LNCS 2846, pp. 151-168. Springer-Verlag, 2003.
- D.H. Yum and P.J. Lee. Efficient key updating signature schemes based on IBS. In: *Proc. of 9th IMA International Conference on Cryptography and Coding*. December 16-18, 2003. Cirencester, UK.
- Jianying Zhou. Efficient Signature Validation Based on a New PKI. In: *Proceedings of 2003 International Conference on Electronic Commerce and Web Technologies* (*EC-Web 2003*)*,* LNCS 2738, pp. 94-103. Springer-Verlag, 2003.
- Jianying Zhou, Feng Bao, and Robert Deng. Validating Digital Signatures without TTP's Time-Stamping and Certificate Revocation. In: *Information Security Conference (ISC'03),* LNCS 2851, pp.96-110. Springer-Verlag, 2003.

2004

- Yevgeniy Dodis, Matthew K. Franklin, Jonathan Katz, Atsuko Miyaji, Moti Yung. A Generic Construction for Intrusion-Resilient Public-Key Encryption. In: *CT-RSA 2004*, LNCS 2964, pp. 81-98. Springer-Verlag, 2004.
- Nicolas González-Deleito, Olivier Markowitch, Emmanuel Dall'Olio. A New Key-Insulated Signature Scheme. In: *Information and Communications Security* (*ICICS 2004*), LNCS 3269, pp. 465-479. Springer-Verlag, 2004.
- Bo Gyeong Kang, Je Hong Park, Sang Geun Hahn. A New Forward Secure Signature Scheme. http://eprint.iacr.org/2004/183/.
- Zhengyi Le, Yi Ouyang, James Ford, Fillia Makedon. A Hierarchical Key-Insulated Signature Scheme in the CA Trust Model. In: *Information Security* (*ISC 2004*), LNCS 3225, pp. 280-291. Springer-Verlag, 2004.
- Tal Malkin, Satoshi Obana, Moti Yung. The Hierarchy of Key Evolving Signatures and a Characterization of Proxy Signatures. In: *EUROCRYPT 2004*, LNCS 3027, pp. 306-322. Springer-Verlag, 2004.

2005

- Xingyang Guo, Quan Zhang, Chaojing Tang. On the Security of Two Key-Updating Signature Schemes. In: *Information Security and Privacy* (ACISP 2005), LNCS 3574, pp. 506-517. Springer-Verlag, 2005. BibTeX

10.8Přehled literatury k tzv. proxy elektronickému podpisu

1996

- M. Mambo, K. Usuda, and E. Okamoto. Proxy signatures: Delegation of the power to sign messages. *IEICE Trans. Fundamentals*, Sep. 1996, Vol. E79-A, No. 9, pp. 1338-1353.
- M. Mambo, K. Usuda, E. Okamoto. Proxy signatures for delegating signing operation. In: *3rd ACM Conference on Computer and Communications Security* (*CCS'96*), pp. 48-57. New York: ACM Press, 1996.

1997

- S. Kim, S. Park, and D. Won. Proxy signatures, revisited. In: *Information and Communications Security* (*ICICS'97*), *LNCS 1334*, pp. 223-232, 1997. Berlin: Springer-Verlag, 1997.
- K. Zhang. Threshold proxy signature schemes. In: *Information Security* (*ISW'97*), *LNCS 1396*, pp. 282-290. Berlin: Springer-Verlag, 1997.
- K. Zhang. Nonrepudiable proxy signature schemes. Manuscript, 1997. Available at http://citeseer.nj.nec.com/360090.html

1998

- M. Blaze, G. Bleumer, and M. Strauss. Divertible protocols and atomic proxy cryptography. In: *Eurocrypt'98, LNCS 1403*, pp. 127-144. Berlin: Springer-Verlag, 1998.
- N.-Y. Lee, T. Hwang, and C.-H. Wang. On Zhang's nonrepudiable proxy signature schemes. In: *Information Security and Privacy* (*ACISP'98*), *LNCS 1438*, pp. 415-422. Berlin: Springer-Verlag, 1998.

1999

- H. Ghodosi and J. Pieprzyk. Repudiation of cheating and non-repudiation of Zhang's proxy signature schemes In: *Information Security and Privacy* (*ACISP'99*), *LNCS 1587,* pp. 129-134. Berlin: Springer-Verlag, 1999.
- T. Okamoto, M. Tada, and E. Okamoto. Extended proxy signatures for smart cards. In: *Information Security* (*ISW'99*), *LNCS 1729*, pp. 247-258. Berlin: Springer-Verlag, 1999.

- H.-M. Sun. An efficient nonrepudiable threshold proxy signature scheme with known signers. *Computer Communications*, May 1999, 22(8): 717-722.
- H.-M. Sun, N.-Y. Lee, and T. Hwang. Threshold proxy signatures. *IEE Proc.-Computers & Digital Techniques,* Sept. 1999, 146(5): 259-263.

2000

- M. Hwang, I. Lin, and E.J. Lu. A secure nonrepudiable threshold proxy signature scheme with known signers. *International Journal of Informatica*, 2000, 11(2): 1-8.
- H.-M. Sun. Design of time-stamped proxy signatures with traceable receivers. *IEE Proc.-Computers & Digital Techniques,* Nov. 2000, 147(6): 462-466.

2001

- B. Lee, H. Kim, and K. Kim. Strong proxy signature and its applications. In: Proc. of the 2001 Symposium on Cryptography and Information Security (SCIS'01), vol 2/2 pp. 603-608. Oiso, Japan, Jan. 23-26, 2001.
- B. Lee, H. Kim, and K. Kim. Secure mobile agent using strong non-designated proxy signature. In: *Information Security and Privacy* (*ACISP'01*), *LNCS 2119*, pp.474-486. Berlin: Springer-Verlag, 2001.
- H.-U. Park, and I.-Y. Lee. A digital nominative proxy signature scheme for mobile communication. In: *Information and Communications Security* (*ICICS'01*), *LNCS 2229*, pp. 451-455, 2001.
- A. Romão, and M.M. da Silva. Secure mobile agent digital signatures with proxy certificates. In: *E-Commerce Agents, LNAI 2033*, pp. 206-220. Berlin: Springer-Verlag, 2001.

2002

- J. Herranz, and G. Saez. Fully distributed proxy signature schemes. http://eprint.iacr.org/2002/051.
- K. Shum and V.-K. Wei. A strong proxy signature scheme with proxy signer privacy protection. In: *Eleventh IEEE International Workshop on Enabling Technologies: Infrastucture for Collaborative Enterprises* (*WETICE'02*). IEEE, 2002.

2003

- Mohamed Al-Ibrahim and Anton Cerny. Proxy and threshold one-time signatures. In: *Applied Cryptography and Network Security (ACNS'03)*, LNCS 2846, pp. 123-136. Springer-Verlag, 2003.
- A. Boldyreva, A. Palacio, and B. Warinschi. Secure proxy signature schemes for delegation of signing rights. http://eprint.iacr.org/2003/096
- J. Herranz and Saez. Verifiable secret sharing for general access structures, with applications to fully distributed distributed proxy signatures. In: *Financial Cryptography* (*FC'03*) (to appear). Springer-Verlag, 2003.

- M.-S. Hwang, E. J.-L. Lu, and I.-C. Lin. A Practical (*t*, *n*) Threshold Proxy Signature Scheme Based on the RSA Cryptosystem. *IEEE Trans. Knowledge and Data Engineering*, 15(6): 1552-1560, Nov. 2003.
- A. Ivan and Y. Dodis. Proxy Cryptography Revisited. In: *Proc. of 10th Annual Network and Distributed System Security Symposium* (*NDSS'03*). The Internet Society, 2003. http://www.isoc.org/isoc/conferences/ndss/03/proceedings/index.htm
- S. Lal and A. K. Awasthi. Proxy blind signature scheme. http://eprint.iacr.org/2003/072.
- S. Lal and A. K. Awasthi. A Scheme for obtaining a warrant message from the digital proxy signatures. http://eprint.iacr.org/2003/073.
- J.-Y. Lee, J. H. Cheon, and S. Kim. An analysis of proxy signatures: Is a secure channel necessary? In: *CT-RSA'03, LNCS 2612*, pp. 68–79, 2003. Berlin: Springer-Verlag, 2003.
- Z. Shao. Proxy signature schemes based on factoring. *Information Processing Letters*, 2003, 85: 137-143.
- H.-M. Sun and B.-T. Hsieh. On the security of some proxy signature schemes. http://eprint.iacr.org/2003/068.
- Guilin Wang, Feng Bao, Jianying Zhou, and Robert H. Deng. Security Analysis of Some Proxy Signatures. In: *Information Security and Cryptology - ICISC 2003,* LNCS 2971, pp. 305-319. Springer-Verlag, 2004. Primary version available at http://eprint.iacr.org/2003/196/.
- Huaxiong Wang, Josef Pieprzyk. Efficient One-Time Proxy Signatures. In: *ASIACRYPT 2003*, LNCS 2894, pp. 507-522. Springer-Verlag, 2003.
- Fangguo Zhang and Kwangjo Kim. Efficient ID-based blind signature and proxy signature from bilinear pairings. In: *Information Security and Privacy* (*ACISP'03*), LNCS 2727, pp. 312-323. Berlin: Springer-Verlag, 2003.

2004

- Amit K Awasthi, Sunder Lal. ID-based Ring Signature and Proxy Ring Signature Schemes from Bilinear Pairings. http://eprint.iacr.org/2004/184/.
- Tal Malkin, Satoshi Obana, Moti Yung. The Hierarchy of Key Evolving Signatures and a Characterization of Proxy Signatures. In: *EUROCRYPT 2004*, LNCS 3027, pp. 306-322. Springer-Verlag, 2004. Full version is available at http://eprint.iacr.org/2004/052/.
- Javier Herranz, Germán Sáez. Revisiting Fully Distributed Proxy Signature Schemes. In: *INDOCRYPT 2004*, LNCS 3348, pp. 356-370. Springer- Verlag, 2004.
- Zhenjie Huang, Yumin Wang. Convertible Nominative Signatures. In: *Information Security and Privacy* (*ACISP 2004*), LNCS 3108, pp. 348-357. Springer-Verlag, 2004.
- Zuowen Tan, Zhuojun Liu. Provably Secure Delegation-by-Certification Proxy Signature Schemes. http://eprint.iacr.org/2004/148/.
- Zuo-Wen Tan, Zhuo-Jun Liu. On the security of some nonrepudiable threshold proxy signature schemes with known signers. http://eprint.iacr.org/2004/234/.

- Guilin Wang. Designated-Verifier Proxy Signatures For E-Commerce. Accepted for *the IEEE 2004 International Conference on Multimedia and Expo* (ICME 2004), Taipei, Taiwan. June 27th-30th, 2004.
- Guilin Wang, Feng Bao, Jianying Zhou, and Robert H. Deng. Comments on a Threshold Proxy Signature Scheme Based on the RSA Cryptosystem. Accepted for *IEEE Transactions on Knowledge and Data Engineering* (TKDE). Preliminary version: http://eprint.iacr.org/2004/054, Jan. 2004.
- Jing Xu, Zhenfeng Zhang, Dengguo Feng. ID-Based Proxy Signature Using Bilinear Pairings. http://eprint.iacr.org/2004/206/.
- Jing Xu, Zhenfeng Zhang, Dengguo Feng. Identity Based Threshold Proxy Signature. http://eprint.iacr.org/2004/250/.
- Fangguo Zhang, Reihaneh Safavi-Naini, and Willy Susilo. An Efficient Signature Scheme from Bilinear Pairings and Its Applications. In: *Public Key Cryptography 2004*, LNCS 2947 , pp. 277-290. Springer-Verlag, 2004.

2005

- Amit K Awasthi and Sunder Lal. Proxy Blind Signature Scheme. *Transaction on Cryptology*, 2(1): 5-11, Jan 2005.
- Zuowen Tan, Zhuojun Liu, Wang Mingsheng. On the Security of Some Nonrepudiable Threshold Proxy Signature Schemes. In: *Information Security Practice and Experience* (*ISPEC 2005*), LNCS 3439, pp. 374-385. Springer-Verlag, 2005.
- Guilin Wang. Designated-Verifier Proxy Signature Schemes. In: *Security and Privacy in the Age of Ubiquitous Computing* (*IFIP/ SEC 2005*), pp. 409-423. Springer, 2005.

10.9 Přehled literatury k problematice elektronického podpisu šifrovaného textu (tzv. signcryption)

(viz také Signcryption Central by Prof. Yuliang Zheng)

1997

- Y. Zheng. Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) + cost (encryption). In: *CRYPTO'97,* LNCS 1294, pp. 165-179. Springer Verlag, 1997.
- Y. Zheng. Signcryption and its application in efficient public key solutions. In: *Information Security Workshop (ISW '97),* LNCS 1396, pp. 291-312. Springer-Verlag, 1997.

1998

- F. Bao and R. H. Deng. A signcryption scheme with signature directly verifiable by public key. In: *Public Key Cryptography (PKC'98),* LNCS 1431, pp. 55-59. Springer-Verlag, 1998.
- Matt Blaze, Gerrit Bleumer, and Martin Strauss. Divertible Protocols and Atomic Proxy Cryptography. In: *EUROCRYPT'98*, LNCS 1403, pp. 127-144. Springer-Verlag, 1998.
- Y. Zheng and H. Imai. How to Construct Efficient Signcryption Schemes on Elliptic Curves. *Information Processing Letters*, 1998, 68(5): 227-233.
- Goichiro Hanaoka, Yuliang Zheng, Hideki Imai. LITESET: A Light-Weight Secure Electronic Transaction Protocol. In: *ACISP 1998,* LNCS 1438, pp. 215-226. Springer-Verlag, 1998.

1999

- Chandana Gamage, Jussipekka Leiwo, Yuliang Zheng. Encrypted Message Authentication by Firewalls. In: *PKC 1999,* LNCS 1560, pp. 69-81. Springer-Verlag, 1999.
- Y. Mu, V. Varadharajan, and K. Q. Nguyen. Delegated decryption. In: *Cryptography and Coding '99,* LNCS 1746, pp. 258-269. Springer-Verlag, 1999.

- M. Seo and K. Kim. Electronic Funds Transfer Protocol using Domain-verifiable Signcryption Scheme. In: *Information Security and Cryptology - ICISC'99,* LNCS 1787, pp. 269-277. Springer-Verlag, 2000.
- Chan Yeob Yeun . Digital Signature with Message Recovery and Authenticated Encryption (Signcryption) - A Comparison. In: *Cryptography and Coding 99,* LNCS 1746. pp. 307-312. Springer-Verlag, 1999.

2000

- R. Steinfeld and Y. Zheng. A Signcryption Scheme Based on Integer Factorization. In: *Information Security Workshop (ISW'00),* LNCS 1975, pp. 308-322. Springer-Verlag, 2000.
- Y. Mu and V. Varadharajan. Distributed signcryption. In: *INDOCRYPT'00,* LNCS 1977, pp. 155-164. Springer-Verlag, 2000.

2001

- Dae Hyun Yum, Pil Joong Lee. New Signcryption Schemes Based on KCDSA. . In: *Information Security and Cryptology - ICISC 2001,* LNCS 2288, pp. 305-317. Springer-Verlag, 2002.
- Y. Zheng. Identification, Signature and Signcryption Using High Order Residues Modulo an RSA Composite. In: *Public Key Cryptography (PKC 2001),* LNCS 1992, pp. 48-63. Springer-Verlag, 2001.

2002

- Jee Hea An, Yevgeniy Dodis, Tal Rabin. On the Security of Joint Signature and Encryption. In: *EUROCRYPT 2002,* LNCS 2332, pp. 83-107. Springer-Verlag, 2002.
- J. Baek, R. Steinfeld, and Y. Zheng. Formal Proofs for the Security of Signcryption. In: *Public Key Cryptography (PKC 2002),* LNCS 2274, pp. 80-98. Springer-Verlag, 2002.
- Ik Rae Jeong, Hee Yun Jeong, Hyun Sook Rhee, Dong Hoon Lee, Jong In Lim. Provably Secure Encrypt-then-Sign Composition in Hybrid Signcryption. In: *Information Security and Cryptology - ICISC 2002,* LNCS 2587, pp. 16-34. Springer-Verlag, 2003.
- D. Kwak, J. Ha, H. Lee, H. Kim, and S. Moon. A WTLS handshake protocol with user anonymity and forward secrecy. In: *CDMA International Conference - CIC'2002,* LNCS 2524, pp. 219-230. Springer-Verlag, 2002.
- Xiaolin Pang, Kian-Lee Tan, Yan Wang, Jian Ren. A Secure Agent-Mediated Payment Protocol. In: *ICICS 2002,* LNCS 2513, pp. 422-433. Springer-Verlag, 2002.
- Jun-Bum Shin, Kwangsu Lee, Kyungah Shim. New DSA-Verifiable Signcryption Schemes. In: *Information Security and Cryptology - ICISC 2002,* LNCS 2587, pp. 35-47. Springer-Verlag, 2003.

2003

- Mohamed Al-Ibrahim. A Signcryption Scheme Based on Secret Sharing Technique. In: *Computer Network Security, Second International Workshop on Mathematical Methods, Models, and Architectures for Computer Network Security* (*MMM-ACNS 2003*), LNCS 2776, pp. 279-288. Springer-Verlag, 2003.
- Xavier Boyen. Multipurpose Identity-Based Signcryption A Swiss Army Knife for Identity-Based Cryptography. In: *CRYPTO'03,* LNCS 2729, pp. 383-399. Springer-Verlag, 2003.
- Sherman S.M. Chow, S.M. Yiu, Lucas C.K. Hui, and K.P. Chow. Efficient Forward and Provably Secure ID-Based Signcryption Scheme with Public Verifiability and Public Ciphertext Authenticity. In: *Information Security and Cryptology - ICISC 2003,* LNCS 2971, pp. 352-369. Springer-Verlag, 2004.
- Yevgeniy Dodis, Jee Hea An. Concealment and Its Applications to Authenticated Encryption. In: *EUROCRYPT 2003*, LNCS 2656, pp. 312-329. Springer-Verlag, 2003.
- Hui-Feng Huang, Chin-Chen Chang. An Efficient Convertible Authenticated Encryption Scheme and Its Variant. In: *Information and Communications Security* (*ICICS'03*), LNCS 2836, pp. 382-392. Springer-Verlag, 2003.
- D.. Kwak and S. Moon. Efficient Distributed Signcryption Scheme as Group Signcryption. In: *Applied Cryptography and Network Security (ACNS'03),* LNCS 2846, pp. 403-417. Springer-Verlag, 2003.
- John Malone-Lee, Wenbo Mao. Two Birds One Stone: Signcryption Using RSA. In: *CT-RSA 2003,* LNCS 2612, pp. 211-225. Springer-Verlag, 2003.
- Josef Pieprzyk and David Pointcheval. Parallel Authentication and Public-Key Encryption. In: *ACISP 2003,* LNCS 2727, pp. 387- 401. Springer-Verlag, 2003.

2004

- Liqun Chen, John Malone-Lee. Improved Identity-Based Signcryption. http://eprint.iacr.org/2004/114/.
- Sherman S.M. Chow, Tsz Hon Yuen, Lucas C.K. Hui, S.M. Yiu. Signcryption in Hierarchical Identity Based Cryptosystem. http://eprint.iacr.org/2004/244/.
- Yevgeniy Dodis, Michael J. Freedman, Stanislaw Jarecki, Shabsi Walfish. Optimal Signcryption from Any Trapdoor Permutation. http://eprint.iacr.org/2004/020/.
- Yevgeniy Dodis, Michael J. Freedman, Stanislaw Jarecki, Shabsi Walfish. Versatile padding schemes for joint signature and encryption. In: *Proc. of the 11th ACM Conference on Computer and Communications Security (CCS 2004)*, pp. 344-353. ACM, 2004. BibTeX
- Benoît Libert, Jean-Jacques Quisquater. Efficient Signcryption with Key Privacy from Gap Diffie-Hellman Groups. In: *Public Key Cryptography 2004*, LNCS 2947, pp. 187-200. Springer-Verlag, 2004.
- Benoît Libert, Jean-Jacques Quisquater. Improved Signcryption from q-Diffie-Hellman Problems. In: *Security in Communication Networks (SCN 2004),* LNCS 3352, pp. 220-234. Springer-Verlag, 2005.BibTeX.

- Noel McCullagh, Paulo S. L. M. Barreto. Efficient and Forward-Secure Identity-Based Signcryption. http://eprint.iacr.org/2004/117/.
- Guilin Wang, Robert H. Deng, Dongjin Kwak, and Sangjae Moon. Security Analysis of Two Signcryption Schemes. In: *Information Security* (*ISC 2004*), LNCS 3225, pp. 123-133. Springer-Verlag, 2004.
- Guilin Wang, Feng Bao, Changshe Ma, and Kefei Chen. Efficient Authenticated Encryption Schemes with Public Verifiability. In: *Proc. of the 60th IEEE Vehicular Technology Conference* (*VTC 2004-Fall*) - *Wireless Technologies for Global Security*. IEEE Computer Society, 2004.

2005

- Liqun Chen, John Malone-Lee. Improved Identity-Based Signcryption. In: *Public Key Cryptography - PKC 2005*, LNCS 3386, pp. 362-379. Springer-Verlag, 2005. BibTeX
- Alexander W. Dent. Hybrid Signcryption Schemes with Insider Security. In: *Information Security and Privacy* (ACISP 2005), LNCS 3574, pp. 253-266. Springer-Verlag, 2005. BibTeX
- Alexander W. Dent. Hybrid Signcryption Schemes with Outsider Security. In: *Information Security* (ISC 2005), LNCS 3650, pp. 203-217. Springer-Verlag, 2005. BibTeX
- Sherman S. M. Chow, T. H. Yuen, L. C. K. Hui, S. M. Yiu. Signcryption in Hierarchical Identity Based Cryptosystem. In: *Security and Privacy in the Age of Ubiquitous Computing* (*IFIP/ SEC 2005*), pp. 443-457. Springer, 2005.
- Changshe Ma, Kefei Chen, Dong Zheng, Shengli Liu. Efficient and Proactive Threshold Signcryption. In: *Information Security* (ISC 2005), LNCS 3650, pp. 233-243. Springer-Verlag, 2005. BibTeX
- Guomin Yang, Duncan S. Wong, Xiaotie Deng. Analysis and Improvement of a Signcryption Scheme with Key Privacy. In: *Information Security* (ISC 2005), LNCS 3650, pp. 218-232. . Springer-Verlag, 2005. BibTeX
- Tsz Hon Yuen, Victor K. Wei. Fast and Proven Secure Blind Identity-Based Signcryption from Pairings**.** In: *Topics in Cryptology - CT-RSA 2005*, LNCS 3376, pp. 305-322. Springer-Verlag, 2005. BibTeX. Preliminary version is available at http://eprint.iacr.org/2004/121/.

10.10Přehled literatury k tzv. undeniable elektronickém podpisu

1989

- D. Chaum, and H. van Antwerpen. Undeniable signatures. In: *CRYPTO'89,* LNCS 435, pp. 212-216. Springer-Verlag, 1989.

1990

- J. Boyar, D. Chaum, I. B. Damgard, and T.P. Pedersen. Convertible undeniable signatures. In: *CRYPTO'90,* LNCS 537, pp. 189-205. Springer-Verlag, 1991.
- D. Chaum. Zero-knowledge undeniable signatures. In: *EUROCRYPT'90,* LNCS 473, pp. 458-464. Springer-Verlag, 1991.

1991

- D. Chaum, E. van Heijst, and B. Pfitzmann. Cryptographically strong undeniable signatures, unconditionally secure for the signer. In: *CRYPTO'91,* LNCS 576, pp. 470–484. Springer-Verlag, 1992.
- Y. Desmedt, and M. Yung. Weakness of undeniable signature schemes. In: *EUROCRYPT'91,* LNCS 547, pp: 205-220. Springer-Verlag, 1991.
- A. Fujioka, T. Okamoto, and K. Ohta. Interactive bi-proof systems and undeniable signature schemes. In: *EUROCRYPT'91,* LNCS 547, pp. 243-256. Springer-Verlag, 1991.
- T.P. Pedersen. Distributed provers with applications to undeniable signatures. In: *Eurocrpt'91,* LNCS 547, pp. 221-242. Springer-Verlag, 1991.

1992

- L. Harn, and S. Yang. Group-oriented undeniable signature schemes without the assistance of a mutually trusted party. In: *Auscrypt'92,* LNCS 718, pp. 133-142. Springer-Verlag, 1993.
- E. van Heyst, T.P. Pedersen. How to make efficient fail-stop signatures. In: *EUROCRYPT'92,* LNCS 658, pp. 366-377. Springer-Verlag, 1992.

1994

- D. Chaum. Designated confirmer signatures. In: *Eurocypt'94,* LNCS 950, pp. 86–91. Springer-Verlag, 1995.
- M. Jakobsson. Blackmailing using undeniable signatures. In: *EUROCRYPT'96,* LNCS 950, pp.: 425-427. Springer-Verlag, 1994.
- T. Okamoto. Designated confirmer signatures and public key encryption are equivalent. In: *CRYPTO'94,* LNCS 839, pp. 61–74. Springer-Verlag, 1994.

1996

- I. Damgard, and T. Pedersen. New convertible undeniable signature schemes. In: *EUROCRYPT'96,* LNCS 1070, pp. 372-386. Springer-Verlag, 1996.
- R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin. Robust and efficient sharing of RSA functions. In: *CRYPTO'96,* LNCS 1109, pp. 157-172. Springer-Verlag, 1996.
- M. Jakobsson and M. Yung. Proving without knowing: On oblivious, agnostic and blindolded provers. In: *CRYPTO'96,* LNCS 1109, pp. 186-200. Springer-Verlag, 1996.
- M. Jakobsson, K. Sako, and R. Impagliazzo. Designated verifier proofs and their applications. In: *EUROCRYPT'96,* LNCS 1070, pp. 143-154. Springer-Verlag, 1996.
- S.K. Langford. Weaknesses in some threshold cryptosystems. In: *CRYPTO'96,* LNCS 1109, pp.74-82. Springer-Verlag, 1996.
- C.-H. Lin, C.-T. Wang, and C.-C. Chang. A group-oriented (*t*, *n*) undeniable signature scheme without trusted center. In: *Information Security and Privacy* (*ACISP'96*), LNCS 1172, pp. 266-274. Springer-Verlag, 1996.
- M. Michels, H. Petersen, and P. Horster. Breaking and repairing a convertible undeniable signature scheme. In: *3rd ACM Conference on Computer and Communications Security* (*CCS'96*), pp. 148-152. New York: ACM Press , 1996.
- M. Michels, and P. Horster. On the risk of discruption in several multiparty signature schemes. In: *Asiacrypt'96,* LNCS 1163, pp.334-345. Springer-Verlag, 1996.
- K. Sakurai and Y. Yamane. Blind decoding, blind Undeniable signatures, and their applications to privacy protection. In: *Information Hiding 1996,* LNCS 1174, pp. 257-264. Springer-Verlag, 1996.

1997

- R. Gennaro, H. Krawczyk, and T. Rabin. RSA-based undeniable signatures. In: *CRYPTO'97,* LNCS 1294, pp. 132–149. Springer-Verlag, 1997. Also in *Journal of Cryptology*, 2000, 13: 397–416.
- M. Michels, and M. Stadler. Efficient convertible signature schemes. In: *Proc. 4th Workshop on Selected Areas in Cryptography* (*SAC'97*), pp. 231-244. Ottawa, Canada, 1997.

1998

- C. Boyd, and E. Foo. Off-line fair payment protocols using convertible signatures. In: *ASIACRYPT'98,* LNCS 1514, pp. 271-285. Springer-Verlag, 1998.
- D. Catalano, and R. Gennaro. New efficient and secure protocols for verifiable signature sharing and other applications. In: *CRYPTO'98,* LNCS 1462, pp. 105-120. Springer-Verlag, 1998.

- L. Chen. Efficient Fair Exchange with Verifiable Confirmation of Signatures. In: *ASIACRYPT'98,* LNCS 1514, pp. 286-299. Springer-Verlag, 1998.
- M. Michels, and M. Stadler. Generic constructions for secure and efficient confirmer signature schemes. In: *EUROCRYPT'98,* LNCS 1403, 406–421. Springer-Verlag, 1998.

1999

- M. Jakobsson. Efficient oblivious proofs of correct exponentiation. In: *Communications and multimedia security*, pp. 71–84. Kluwer, 1999.
- N.-Y. Lee, and T. Hwang. Group-oriented undeniable signature schemes with a trusted center. *Computer Communications*, 22(8): 730-734. Elsevier Science, May 1999.
- K. Nguyen, Y. Mu, V. Varadharajan. Undeniable confirmer signature. In: *Information Security* (*ISW'99*), LNCS 1729, pp. 235-246. Springer-Verlag, 1999.

2000

- J. Camenisch, and M. Michels. Confirmer signature schemes secure against adaptive adversaries. In: *EUROCRYPT'00,* LNCS 1870, pp. 243–258. Springer-Verlag, 2000.
- T. Miyazaki. An improved scheme of the Gennaro-Krawczyk-Rabin undeniable signature system based on RSA. In: *Information Security and Cryptology - ICISC 2000, LNCS 2015*, pp. 135-149. Springer-Verlag, 2001.
- Y. Mu and V. Varadharajan: Fail-Stop Confirmer Signatures. In: *Information Security and Privacy (ACISP'00),* LNCS 1841, pp. 368-377. Springer-Verlag, 2000.
- K. Sakurai, and S. Miyazaki. An anonymous electronic bidding protocol based on a new convertible group signature scheme. In: *Information Security and Privacy* (*ACISP'00*), LNCS 1841, pp. 385–399. Springer-Verlag, 2000.

2001

- Lee Jongkook, Ryu Shiryong, Kim Jeungseop, and Yoo Keeyoung. A new undeniable signature scheme using smart cards. In: *Cryptography and Coding,* LNCS 2260, pp. 387-394.
- D. Kugler, and H. Vogt. Marking: a privacy protecting approach against blackmailing. In: *Public Key Cryptography* (*PKC'01*), LNCS 1992, pp. 137-152. Springer-Verlag, 2001.
- T. Okamoto, and D. Pointcheval. The gap-problems: A new class of problems for the security of cryptographic schemes. In: *Public Key Cryptography* (*PKC'01*), LNCS 1992, pp. 104-118. Springer-Verlag, 2001.
- G. Wang, S. Qing, M. Wang and Z. Zhou. Threshold undeniable RSA signature scheme. In: *Information and Communications Security* (*ICICS 2001*), LNCS 2229, pp. 220-231. Springer-Verlag, 2001.

2002

- S.D. Galbraith, W. Mao, and K.G. Paterson. RSA-based undeniable signatures for general moduli. In: *Topics in Cryptology – CT-RSA 2002, LNCS 2271*, pp. 200–217. Springer-Verlag, 2002.
- D.-G. Han, H.-Y. Park, Y.-H. Park, S. Lee, D.H. Lee, and H.-J. Yang. A practical approach defeating blackmailing. In: *Information Security and Privacy* (*ACISP'02*), LNCS 2384, pp. 464-481. Springer-Verlag, 2002.
- Y.-D. Lyuu, and M.-L. Wu. Convertible group undeniable signatures. In: *Information Security and Cryptology – ICISC 2002,* LNCS 2587, pp. 48-61. Springer-Verlag, 2003.
- G. Wang, J. Zhou, and R. Deng. Cryptanalysis of the Lee-Hwang group-oriented undeniable signature schemes. Available from Cryptology ePrint Archive: http://eprint.iacr.org/2002/150.

2003

- Steven D. Galbraith and Wenbo Mao. Invisibility and anonymity of undeniable and confirmer signatures. In: *CT-RSA 2003*, LNCS 2612, pp. 80–97. Springer-Verlag, 2003.
- Shahrokh Saeednia, Steve Kremer, and Olivier Markowitch. An Efficient Strong Designated Verifier Signature Scheme. In: *Information Security and Cryptology - ICISC 2003,* LNCS 2971, pp. 40-54. Springer-Verlag, 2004.
- Willy Susilo and Yi Mu. Non-interactive Deniable Ring Authentication. In: *Information Security and Cryptology - ICISC 2003,* LNCS 2971, pp. 386-401. Springer-Verlag, 2004.

2004

- Giuseppe Ateniese, Breno de Medeiros. On the Key Exposure Problem in Chameleon Hashes. In: *Security in Communication Networks (SCN 2004),* LNCS 3352, pp. 165-179. Springer-Verlag, 2005. BibTeX. Full version is available at http://eprint.iacr.org/2004/243/.
- Ingrid Biehl, Sachar Paulus, and Tsuyoshi Takagi. Efficient Undeniable Signature Schemes based on Ideal Arithmetic in Quadratic Orders. *Designs, Codes and Cryptography*, 31 (2), pp.99-123, 2004.
- Xiaofeng Chen, Fangguo Zhang, Kwangjo Kim. Limited Verifier Signature from Bilinear Pairings. In: *Applied Cryptography and Network Security* (*ACNS 2004*), LNCS 3089, pp. 135-148. Springer-Verlag, 2004.
- Xiaofeng Chen, Fangguo Zhang, Kwangjo Kim. Chameleon Hashing Without Key Exposure. In: *Information Security* (*ISC 2004*), LNCS 3225, pp. 87-98. Springer-Verlag, 2004.
- Shafi Goldwasser, Erez Waisbard. Transformation of Digital Signature Schemes into Designated Confirmer Signature Schemes. In: *First Theory of Cryptography Conference* (*TCC 2004*), pp. 77-100. Springer-Verlag, 2004.
- Fabien Laguillaumie, Damien Vergnaud. Designated Verifier Signatures: Anonymity and Efficient Construction from Any Bilinear Map. In: *Security in*

Communication Networks (SCN 2004), LNCS 3352, pp. 105-119. Springer-Verlag, 2005. BibTeX
- Fabien Laguillaumie, Damien Vergnaud. Multi-Designated Verifiers Signatures. In: *Information and Communications Security* (*ICICS 2004*), LNCS 3269, pp. 495-507. Springer-Verlag, 2004.
- Benoît Libert, Jean-Jacques Quisquater. Identity Based Undeniable Signatures. In: *Topics in Cryptology - CT-RSA 2004*, LNCS 2964, pp. 112-125. Springer-Verlag, 2004.
- Seungjoo Kim, Dongho Won. Threshold Entrusted Undeniable Signature. In: *Information Security and Cryptology - ICISC 2004,* LNCS 3506, pp. 195-203. Springer-Verlag, 2005.
- Jean Monnerat, Serge Vaudenay. Undeniable Signatures Based on Characters: How to Sign with One Bit. In: *Public Key Cryptography 2004*, LNCS 2947, pp. 69-85. Springer-Verlag, 2004.
- Jean Monnerat, Serge Vaudenay. Generic Homomorphic Undeniable Signatures. In: *ASIACRYPT 2004*, LNCS 3329, pp. 354-371. Springer-Verlag, 2004.
- Ron Steinfeld, Huaxiong Wang, Josef Pieprzyk. Efficient Extension of Standard Schnorr/RSA Signatures into Universal Designated-Verifier Signatures. In: *Public Key Cryptography 2004*, LNCS 2947, pp. 86-100. Springer-Verlag, 2004.
- Willy Susilo, Fangguo Zhang, Yi Mu. Identity-Based Strong Designated Verifier Signature Schemes. In: *Information Security and Privacy* (*ACISP 2004*), LNCS 3108, pp. 313-324. Springer-Verlag, 2004.

2005

- Kaoru Kurosawa, Swee-Huay Heng. 3-Move Undeniable Signature Scheme. In: *EUROCRYPT'05,* LNCS 3494, 181-197. Springer-Verlag, 2005. BibTeX
- Fabien Laguillaumie, Damien Vergnaud. Time-Selective Convertible Undeniable Signatures. In: *Topics in Cryptology - CT-RSA 2005*, LNCS 3376, pp. 154-171. Springer-Verlag, 2005. BibTeX
- Jean Monnerat, Serge Vaudenay. Chaum's Designated Confirmer Signature Revisited. In: *Information Security* (ISC 2005), LNCS 3650, pp. 164-178. Springer-Verlag, 2005. BibTeX
- Wakaha Ogata, Kaoru Kurosawa, Swee-Huay Heng. The Security of the FDH Variant of Chaum's Undeniable Signature Scheme. In: *Public Key Cryptography - PKC 2005*, LNCS 3386, pp. 328-345. Springer-Verlag, 2005. BibTeX
- Willy Susilo, Yi Mu. Tripartite Concurrent Signatures. In: *Security and Privacy in the Age of Ubiquitous Computing* (*IFIP/ SEC 2005*), pp. 425-4413. Springer, 2005.
- Willy Susilo, Yi Mu. On the Security of Nominative Signatures. In: *Information Security and Privacy* (ACISP 2005), LNCS 3574, pp. 329-335. Springer-Verlag, 2005. BibTeX
- Guilin Wang. Designated-Verifier Proxy Signature Schemes. In: *Security and Privacy in the Age of Ubiquitous Computing* (*IFIP/ SEC 2005*), pp. 409-423. Springer, 2005.

- Rui Zhang II, Jun Furukawa, Hideki Imai. Short Signature and Universal Designated Verifier Signature Without Random Oracles. In: *Applied Cryptography and Network Security* (*ACNS 2005*), LNCS 3531, pp. 483-498. Springer-Verlag, 2005. BibTeX

10.11Přehled literatury k tzv. Threshold signature

[1] K. Itakura and K. Nakamura, “A publ ic key cryptosystem suitable for digital multisignatures,” *NEC Research & Development*, 71:1-8, 1983.

[2] L. Harn, “Group-oriented (t,n) threshold digital signature scheme and digital multisignature,” *IEE Proc. Computers and Digital Techniques*, 141(5), 1994.

[3] C. Li, T. Hwang and N. Lee, “Threshold-multisignature schemes where suspected forgery implies traceability of adversarial shareholders,” *Eurocrypt 94*, 1994.

[4] P. Horster, M. Michels and H. Petersen, “Meta-multisignatures schemes based on the discrete logarithm problem,” *IFIP/Sec* 1995.

[5] T. Okamoto, “Adi gital multisignature schema using bijective public-key cryptosystems,”

ACM Transaction on Computer Systems, 6(4): 432-441, 1988.

[6] K. Ohta and T. Okamoto, “Ad igital multisignature scheme based on the Fiat-Shamir scheme”, *Asiacrypt 91*, 1991.

[7] K. Ohta and T. Okamoto, “Multi-signature scheme secure against active insider attacks”, *IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences*, E82-A(1):21-31, 1999.

[8] S. Micali, K. Ohta and L. Reyzin, “Accountable-subgroup multisignatures,” *ACM Conference on Computer and Communications Security*, 2001.

[9] D. Boneh, C. Gentry, B. Lynn and H. Shacham, “Aggregate signatures from bilinear maps,” Manuscript.

[10] D. Boneh, B. Lynn and H. Shacham, “Short signatures from theWeil pairing,” *Asiacrypt 01*, 2001.

[11] A. Lysyanskaya, “Unique signatures and verifiable random functions from the DH-DDH separation”, *Crypto 02*, 2002.

[12] A. Boldyreva “Threshold signatures, multisignatures and blind signatures based on the Gap-Diffie-Hellman-group signature scheme,” Full version of this paper. Available at http://www-cse.ucsd.edu/users/aboldyre/.

[11] D. Chaum, “Blind signatures for untreaceable payments,” *Crypto 82*, 1982.

[12] C. Boyd, “Digital multisignatures,” *Cryptography and Coding*, 1986

[13] Y. Desmedt, “Society and group oriented cryptography,” *Crypto 87*, 1987.

[14] Y. Desmedt and Y. Frankel, “Threshold cryptosystems,” *Crypto 89*, 1989.

[15] A. Shamir, “How to share a secret,” *Communications of the ACM,* 22:612-613, (1979).

[16] Y. Desmedt, “Threshold cryptography,”, *European Transactions on Telecommunications*,5(4), 1994.

[17] J.Hrubý , Elektronické volby v ČR?, Crypto-World 2006, ISSN 1801-2140,16(2006).

[18] A. Nicolosi and D. Mazieres. Secure acknowledgement of multicast messages in open peer-to-peer networks. In *3rd International Workshop on Peer-to-Peer Systems (IPTPS ’04)*, San Diego, CA, February 2004.

[19]A. Boldyreva. Efficient threshold signatures, multisignatures and blind signatures based on the gap-diffie-hellman-group signature scheme. In *Public Key Cryptography 2003*, 2003.

11.Abecední rejstřík