On Delegatability of Four Designated Verifier Signatures

Yong Li[1] Helger Lipmaa[23] Dingyi Pei[1]

[1]State Key Laboratory of Information Security
Graduate School of Chinese Academy of Sciences
li.yong9@gmail.com

[2]Cybernetica AS, Estonia
[3]Institute of Computer Science, University of Tartu, Estonia

ICICS 2005, 10, December 2005, Beijing

Overview

Overview

Overview

Overview

Overview

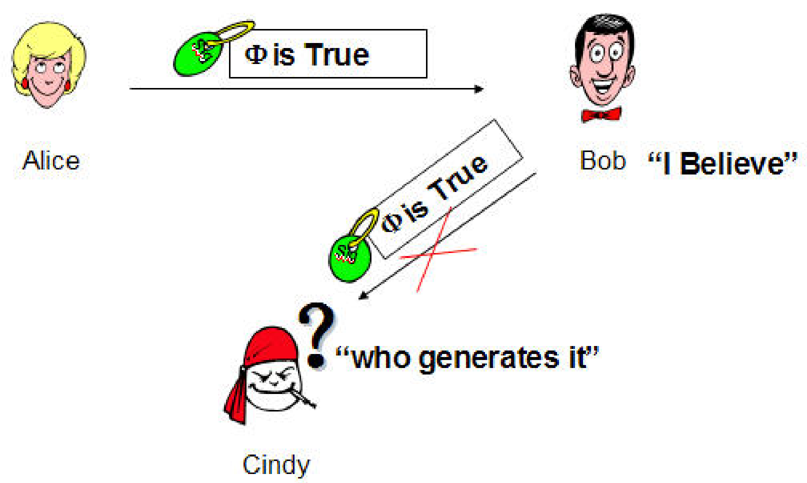
Designated Verifier Proof

Goal: solve the conflict between authenticity and privacy

First Proposed

- Designated Verifier Proof
  Jakobsson, Sako, and Impagliazzo [JSI96]
- Private Signature and Proof
  Chaum [Cha96]

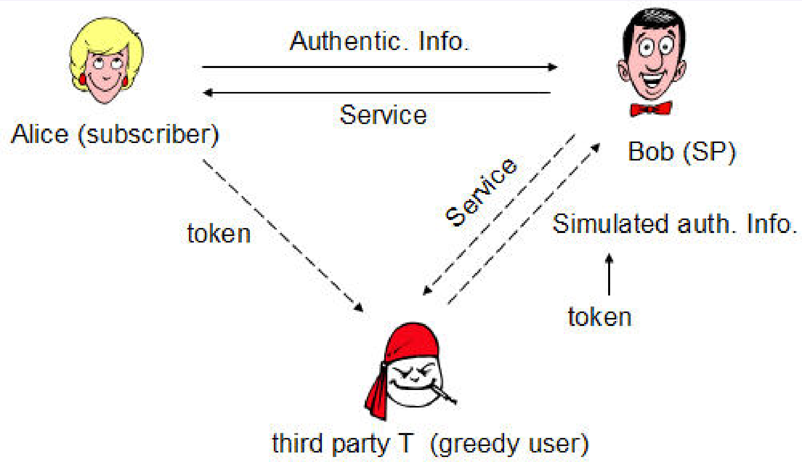
Basic idea (E-service Scenario)



Attack history

- First attack on [JSI96]
  Guilin Wang , ePrint 2003/243
- Helger Lipmaa, Guilin Wang, Feng Bao [LWB05]

Delegatable & Non-delegatability



Delegatable schemes ([LWB05] result)

1. Saeednia-Kremer-Markowitch, ICISC 2003, [SKM03]
2. Steinfeld-Bull-Wang-Pieprzyk, Asiacrypt 2003, [SBWP03]
3. Steinfeld-Wang-Pieprzyk, PKC 2004, [SWP04]
4. Laguillaumie-Vergnaud, SCN 2004, [LV04a]

Question?

Are there other DVS schemes and its variants also have delegatable weakness?

Bilinear pairing

Definition

Let $\mathbb{G}$ be a cyclic additive group generated by P, whose order is a prime q, and let $\mathbb{H}$ be a cyclic multiplicative group of the same order q. A *bilinear pairing* is a map $\langle \cdot, \cdot \rangle : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{H}$ with the following properties:

- **Bilinearity:** $\langle aP, bQ \rangle = \langle P, Q \rangle^{ab}$ for all $P, Q \in \mathbb{G}$ and $a, b \in \mathbb{Z}_q^*$;
- **Non-degeneracy:** There exist $P, Q \in \mathbb{G}$ such that $\langle P, Q \rangle \neq 1$;
- **Computability:** There is an efficient algorithm to compute $\langle P, Q \rangle$ for all $P, Q \in \mathbb{G}$.

Formal Definition of n-DVS

Notions:

- S: signer
- $D_1, \ldots, D_n$: n designated verifiers.
- $\mathrm{PK}_{\vec{D}}$: $(\mathrm{PK}_{D_1}, \ldots, \mathrm{PK}_{D_n})$.
- $\mathrm{SK}_{\vec{D}}$: $(\mathrm{SK}_{D_1}, \ldots, \mathrm{SK}_{D_n})$.
- $\mathrm{Simul}_{\mathrm{PK}_S, \mathrm{PK}_{\vec{D}}, \mathrm{SK}_{\vec{D}}}$: $(\mathrm{Simul}_{\mathrm{PK}_S, \mathrm{PK}_{\vec{D}}, \mathrm{SK}_{D_1}}, \ldots, \mathrm{Simul}_{\mathrm{PK}_S, \mathrm{PK}_{\vec{D}}, \mathrm{SK}_{D_n}})$

Formal Definition of n-DVS

- Setup is a probabilistic algorithm that outputs the public parameter *param*;
- KeyGen(*param*) is a probabilistic algorithm that takes the public parameters as an input and outputs a secret/public key-pair $(\mathsf{SK}, \mathsf{PK})$;
- $\mathsf{Sign}_{\mathsf{SK}_S, \mathsf{PK}_{\vec{D}}}(m)$ takes as inputs signer's secret key, designated verifiers' public keys, a message $m \in \mathcal{M}$ and a possible random string, and outputs a signature σ;

Formal Definition of n-DVS (cont.)

- For $i \in [1, n]$, $\mathsf{Simul}_{\mathsf{PK}_S, \mathsf{PK}_{\vec{D}}, \mathsf{SK}_{D_i}}(m)$ takes as inputs signer's public key, designated verifiers' public keys, secret key of one designated verifier, a message $m \in \mathcal{M}$ and a possible random string, and outputs a signature σ;
- $\mathsf{Verify}_{\mathsf{PK}_S, \mathsf{PK}_{\vec{D}}}(m, \sigma)$ is a deterministic algorithm that takes as inputs a signing public key PK_S, public keys of all designated verifiers D_i, $i \in [1, n]$, a message $m \in \mathcal{M}$ and a candidate signature σ, and returns accept or reject;

n-DVS variations

- *strong n-DVS*: verification algorithm also takes an SK_{D_i}, $i \in [1, n]$, as an input
- designated multi verifier signature scheme: verification can be performed only by the coalition of all n designated verifiers.
- universal DVS: conventional signature+ designation algorithm.
- ID-based DVS: ID info. $\longrightarrow$ public key.

Security requirements

- Unforgeability
- Non-transferability
- Non-delegatability

Other four DVS schemes

1. Susilo-Zhang-Mu, ACISP 2004, [SZM04]
2. Ng-Susilo-Mu, SNDS 2005, [NSM05]
3. Zhang-Furikawa-Imai, ACNS 2005, [ZFI05]
4. Laguillaumie-Vergnaud, ICICS 2004, [LV04b]

SZM04 scheme (ID-based strong DVS)

- Setup: master key $s \in \mathbb{Z}_q$, $P_{pub} \leftarrow sP$. $H_{\mathbb{G}} : \{0,1\}^* \rightarrow \mathbb{G}$, $H_q : \{0,1\}^* \rightarrow \mathbb{Z}_q$.
  $params = (q, \mathbb{G}, \mathbb{H}, \langle \cdot, \cdot \rangle, P, P_{pub}, H_{\mathbb{G}}, H_q)$.
- KeyGen($param$): $\mathsf{PK}_S \leftarrow H_{\mathbb{G}}(\mathsf{ID}_S)$ and $\mathsf{PK}_D \leftarrow H_{\mathbb{G}}(\mathsf{ID}_D)$. secret keys are $\mathsf{SK}_S \leftarrow s \cdot \mathsf{PK}_S$ and $\mathsf{SK}_D \leftarrow s \cdot \mathsf{PK}_D$.
- $\mathsf{Sign}_{\mathsf{SK}_S, \mathsf{PK}_D}(m)$: $k \leftarrow \mathbb{Z}_q$, $t \leftarrow \mathbb{Z}_q^*$, S computes $c \leftarrow \langle \mathsf{PK}_D, P \rangle^k$, $r \leftarrow H_q(m, c)$, $T \leftarrow t^{-1}kP - r \cdot \mathsf{SK}_S$. The signature is (T, r, t).
- $\mathsf{Simul}_{\mathsf{PK}_S, \mathsf{SK}_D}(m)$: D generates random $R \in \mathbb{G}$ and $a \in \mathbb{Z}_q^*$, and computes $c \leftarrow \langle R, \mathsf{PK}_D \rangle \cdot \langle \mathsf{PK}_S, \mathsf{SK}_D \rangle^a$, $r \leftarrow H_q(m, c)$, $t \leftarrow r^{-1}a \mod q$, $T \leftarrow t^{-1}R$. The simulated signature is (T, r, t).
- $\mathsf{Verify}_{\mathsf{PK}_S, \mathsf{SK}_D}(m, \sigma)$: $H_q(m, (\langle T, \mathsf{PK}_D \rangle \cdot \langle \mathsf{PK}_S, \mathsf{SK}_D \rangle^r)^t) = r$.

Attack on SZM04

First attack. S or D leaking $\langle \mathrm{SK}_S, \mathrm{PK}_D \rangle$ or $\langle \mathrm{PK}_S, \mathrm{SK}_D \rangle$.
Second attack. S discloses $(k, k \cdot \mathrm{SK}_S)$ to T, where $k \leftarrow \mathbb{Z}_q^*$.
Given $\tilde{m}$ and arbitrary designated verifier D, T chooses $R \leftarrow \mathbb{G}$, $a \leftarrow \mathbb{Z}_q^*$ and computes

$$\tilde{c} \leftarrow \langle R, \mathrm{PK}_D \rangle \cdot \langle k \cdot \mathrm{SK}_S, \mathrm{PK}_D \rangle^{a(k^{-1}+1)},$$
$$\tilde{r} \leftarrow H_q(\tilde{m}, \tilde{c}),$$
$$\tilde{t} \leftarrow \tilde{r}^{-1} a \mod q,$$
$$\tilde{T} \leftarrow \tilde{t}^{-1} R + \tilde{r} k \cdot \mathrm{SK}_S.$$

The simulated signature is $(\tilde{T}, \tilde{r}, \tilde{t})$.
D can verify whether $H_q(\tilde{m}, (\langle \tilde{T}, \mathrm{PK}_D \rangle \cdot \langle \mathrm{PK}_S, \mathrm{SK}_D \rangle^{\tilde{r}})^{\tilde{t}}) = \tilde{r}$.

NSM05 scheme (UDMVS)

- Setup: $|\mathbb{G}| = |\mathbb{H}| = q$, $\langle \cdot, \cdot \rangle : \mathbb{G} \times \mathbb{G} \to \mathbb{H}$, $H_{\mathbb{G}} : \{0,1\}^* \to \mathbb{G}$. $param = (q, \mathbb{G}, \mathbb{H}, \langle \cdot, \cdot \rangle, P, H_{\mathbb{G}})$.
- KeyGen($param$): $\mathsf{SK} \leftarrow \mathbb{Z}_q^*$, $\mathsf{PK} \leftarrow \mathsf{SK} \cdot P$.
- $\mathsf{Sign}_{\mathsf{SK}_S, \mathsf{PK}_{\vec{D}}}(m)$: $\hat{\sigma} \leftarrow \mathsf{SK}_S \cdot H_{\mathbb{G}}(m)$, $\sigma \leftarrow \langle \hat{\sigma}, \sum_{i=1}^{n} \mathsf{PK}_{D_i} \rangle$. Return σ.
- $\mathsf{Verify}_{\mathsf{PK}_S, \mathsf{PK}_{\vec{D}}, \mathsf{SK}_{\vec{D}}}(m, \sigma)$: Each D_i does the following: compute $\tilde{\sigma}_i \leftarrow \mathsf{SK}_{D_i} \cdot H_{\mathbb{G}}(m)$ and send it to other $n-1$ verifiers.
  After receiving all $\tilde{\sigma}_j$, $j \neq i$, validate all $\tilde{\sigma}_j$ by verifying that $\langle P, \tilde{\sigma}_j \rangle = \langle \mathsf{PK}_j, H_{\mathbb{G}}(m) \rangle$ for $j \neq i, j \in [1, n]$.
  Return reject if any of the verifications fails. Return accept if $\sigma = \prod_{i=1}^{n} \langle \tilde{\sigma}_i, \mathsf{PK}_S \rangle$, or reject otherwise.

Attack on NSM05 scheme

Denote $P_{sum} := \sum_{i=1}^{n} \mathrm{PK}_{D_i}$. If signer leaks $\mathrm{SK}_S \cdot P_{sum}$ to T, then T can compute

$$\sigma \leftarrow \langle H_{\mathbb{G}}(m), \mathrm{SK}_S \cdot P_{sum} \rangle = \langle \mathrm{SK}_S \cdot H_{\mathbb{G}}(m), P_{sum} \rangle = \langle \hat{\sigma}, P_{sum} \rangle \ .$$

After receiving (m, σ), each verifier i computes $\tilde{\sigma}_i \leftarrow \mathrm{SK}_{D_i} \cdot H_{\mathbb{G}}(m)$, and verifies that $\langle P, \tilde{\sigma}_j \rangle = \langle \mathrm{PK}_j, H_{\mathbb{G}}(m) \rangle$ for $j \neq i, j \in [1, n]$.

$$\begin{aligned} \sigma &= \langle H_{\mathbb{G}}(m), \mathrm{SK}_S \cdot P_{sum} \rangle = \langle \mathrm{SK}_S \cdot H_{\mathbb{G}}(m), P_{sum} \rangle = \langle \hat{\sigma}, P_{sum} \rangle \\ &= \prod_{i=1}^{n} \langle \hat{\sigma}, \mathrm{SK}_{D_i} \cdot P \rangle = \prod_{i=1}^{n} \langle \mathrm{SK}_S \cdot H_{\mathbb{G}}(m), \mathrm{SK}_{D_i} \cdot P \rangle \\ &= \prod_{i=1}^{n} \langle \mathrm{SK}_{D_i} \cdot H_{\mathbb{G}}(m), \mathrm{SK}_S \cdot P \rangle = \prod_{i=1}^{n} \langle \tilde{\sigma}_i, \mathrm{PK}_S \rangle \ . \end{aligned}$$

Attack on NSM05 scheme (cont.)

Notes.

- all verifiers can cooperate by leaking $\sum \mathrm{SK}_{D_i} \cdot \mathrm{PK}_S = \mathrm{SK}_S \cdot P_{sum}$.
- “simple” UDMVS scheme based on UDVS [SBWP03] is delegatable.
- MDVS scheme in [NSM05] is delegatable.

ZFI05 scheme (UDVS. simplified)

- Setup: $|\mathbb{G}| = |\mathbb{H}| = q$, $\langle\cdot,\cdot\rangle : \mathbb{G} \times \mathbb{H} \to \mathbb{H}$, isomorphism $\psi : \mathbb{H} \to \mathbb{G}$. Here, $\mathbb{G}$ is multiplicative. Random generator $g_2 \in \mathbb{H}$, compute $g_1 = \psi(g_2) \in \mathbb{G}$.
  $param = (q, \mathbb{G}, \mathbb{H}, \langle\cdot,\cdot\rangle, \psi, g_1, g_2)$.
- KeyGen($param$): $x, y \leftarrow \mathbb{Z}_q^*$, $u \leftarrow g_2^x$, $v \leftarrow g_2^y$. PK $\leftarrow (u, v)$, SK $\leftarrow (x, y)$.
- $\mathrm{Sign}_{\mathrm{SK}_S,\mathrm{PK}_D}(m)$: $r \leftarrow \mathbb{Z}_q^*$. If $x_S + r + y_S m \equiv 0 \mod q$, restart. Compute $\sigma' \leftarrow g_1^{1/(x_S+r+y_S m)} \in \mathbb{G}$, $h \leftarrow g_2^r$, $d \leftarrow \langle u_D, v_D^r \rangle \in \mathbb{H}$. Return $\sigma \leftarrow (\sigma', h, d)$.

ZFI05 scheme (cont.)

- $\mathsf{Simul}_{\mathsf{PK}_S,\mathsf{SK}_D}(m)$: $s \in \mathbb{Z}_q^*$ and compute $\sigma' \leftarrow g_2^s$, $h \leftarrow g_2^{1/s} u_S^{-1} v_S^{-m}$ and $d \leftarrow \langle g_1, h\rangle^{x_D y_D}$. Return $\sigma \leftarrow (\sigma', h, d)$.
- $\mathsf{Verify}_{\mathsf{PK}_S,\mathsf{SK}_D}(\sigma', h, d)$: Output accept if $\langle g_1, g_2\rangle = \langle \sigma', u_S \cdot h \cdot v_S^m\rangle$ and $d = \langle u_D, h^{y_D}\rangle$. Otherwise, output reject.

Attack on ZFI05 scheme

Designated verifier can compute d as $d \leftarrow \langle g_1^{x_D y_D}, h \rangle$ in simulation algorithm.
The scheme is delegatable by the verifier. (reveal $g_1^{x_D y_D}$)

LV04b scheme (MDVS, 2-DVS)

- Setup: $param = (q, \mathbb{G}, \mathbb{H}, \langle\cdot,\cdot\rangle, P, H_{\mathbb{G}})$.
- KeyGen($param$): $\mathrm{SK} \leftarrow \mathbb{Z}_q^*$, $\mathrm{PK} \leftarrow \mathrm{SK} \cdot P$.
- $\mathrm{Sign}_{\mathrm{SK}_S, \mathrm{PK}_{D_1}, \mathrm{PK}_{D_2}}(m)$: $m \in \{0,1\}^*$, S picks $(r, \ell) \in \mathbb{Z}_q^* \times \mathbb{Z}_q^*$, computes

$$u \leftarrow \langle \mathrm{PK}_{D_1}, \mathrm{PK}_{D_2} \rangle^{\mathrm{SK}_S},$$
$$Q_1 \leftarrow \mathrm{SK}_S{}^{-1}(H_{\mathbb{G}}(m, u^{\ell}) - r(\mathrm{PK}_{D_1} + \mathrm{PK}_{D_2})),$$
$$Q_2 \leftarrow rP$$

The signature is $\sigma = (Q_1, Q_2, \ell)$.
- $\mathrm{Verify}_{\mathrm{PK}_S, \mathrm{PK}_{\vec{D}}, \mathrm{SK}_{D_i}}(m, Q_1, Q_2, \ell)$: $D_i (i \in \{1, 2\})$ computes $u \leftarrow \langle \mathrm{PK}_S, \mathrm{PK}_{D_{3-i}} \rangle^{\mathrm{SK}_{D_i}}$. Test whether $\langle Q_1, \mathrm{PK}_S \rangle \cdot \langle Q_2, \mathrm{PK}_{D_1} + \mathrm{PK}_{D_2} \rangle \stackrel{?}{=} \langle H_{\mathbb{G}}(m, u^{\ell}), P \rangle$.

Attack on LV04b scheme

Suppose D_1 and D_2 collude to leak $\mathrm{SK}_{D_1} + \mathrm{SK}_{D_2}$ to T. Then T picks $\tilde{r}, \tilde{\ell} \leftarrow \mathbb{Z}_q^*$, computes

$$\tilde{M} \leftarrow H_{\mathbb{G}}(m, \tilde{\ell}),$$
$$\tilde{Q}_1 \leftarrow \tilde{r}P,$$
$$\tilde{Q}_2 \leftarrow (\mathrm{SK}_{D_1} + \mathrm{SK}_{D_2})^{-1}(\tilde{M} - \tilde{r} \cdot \mathrm{PK}_S).$$

The simulated signature is $\tilde{\sigma} \leftarrow (\tilde{Q}_1, \tilde{Q}_2, \tilde{\ell})$.

Attack on LV04b scheme (cont.)

Verification accepts since

$$
\begin{aligned}
&\langle \tilde{Q}_1, \mathrm{PK}_S \rangle \cdot \langle \tilde{Q}_2, \mathrm{PK}_{D_1} + \mathrm{PK}_{D_2} \rangle \\
&\quad = \langle \tilde{r}P, \mathrm{PK}_S \rangle \cdot \langle (\mathrm{SK}_{D_1} + \mathrm{SK}_{D_2})^{-1}(\tilde{M} - \tilde{r} \cdot \mathrm{PK}_S), \mathrm{SK}_{D_1} P + \mathrm{SK}_{D_2} \cdot P \rangle \\
&\quad = \langle \tilde{r}P, \mathrm{PK}_S \rangle \cdot \langle (\mathrm{SK}_{D_1} + \mathrm{SK}_{D_2})^{-1}(\tilde{M} - \tilde{r} \cdot \mathrm{PK}_S), P \rangle^{\mathrm{SK}_{D_1} + \mathrm{SK}_{D_2}} \\
&\quad = \langle \tilde{r}P, \mathrm{PK}_S \rangle \cdot \langle \tilde{M} - \tilde{r} \cdot \mathrm{PK}_S, P \rangle \\
&\quad = \langle \tilde{M}, P \rangle \cdot \langle \tilde{r} \cdot \mathrm{PK}_S, P \rangle \cdot \langle -\tilde{r} \cdot \mathrm{PK}_S, P \rangle \\
&\quad = \langle \tilde{M}, P \rangle \ .
\end{aligned}
$$

Attack on LV04b scheme (cont.)

Notes.

- The above attack can also be treated as two-party simulation algorithm if D_1 and D_2 execute it themselves.
- require that two parties D_1 and D_2 compute $\mathrm{SK}_{D_1} + \mathrm{SK}_{D_2}$ together.
- third party can simulate the signature of *any* signer w.r.t. a fixed designated verifier or a fixed pair of designated verifiers. (LV04b , ZFI05 scheme)

Attack I & II

Attack I

Either the signer or one of the designated verifiers can delegate the signing rights to a third party T without disclosing his or her secret key.

Attack II

Attack I & II

Attack I

Either the signer or one of the designated verifiers can delegate the signing rights to a third party T without disclosing his or her secret key.

Attack II

Attack I & II

Attack I

Either the signer or one of the designated verifiers can delegate the signing rights to a third party T without disclosing his or her secret key.

Attack I & II

Attack I

Either the signer or one of the designated verifiers can delegate the signing rights to a third party T without disclosing his or her secret key.

Attack II

One of the designated verifiers (or even only the coalition of all verifiers) can delegate the signing right to a third party without disclosing his or her secret key, while the signer cannot do it.

Attack I & II

Attack I

Either the signer or one of the designated verifiers can delegate the signing rights to a third party T without disclosing his or her secret key.

Attack II

One of the designated verifiers (or even only the coalition of all verifiers) can delegate the signing right to a third party without disclosing his or her secret key, while the signer cannot do it.

Attack I & II

Attack I

Either the signer or one of the designated verifiers can delegate the signing rights to a third party T without disclosing his or her secret key.

Attack II

One of the designated verifiers (or even only the coalition of all verifiers) can delegate the signing right to a third party without disclosing his or her secret key, while the signer cannot do it.

Verifier-only delegatability

Definition

(informally) n-DVS scheme Δ is *verifier-only* delegatability if it is delegatable but it cannot be delegated by the signer without leaking signer's secret key.

Summary

- Formal definition of *n*-DVS.
- Attacks on four DVS schemes. (all DVS schemes based on bilinear maps are delegatable.)
- More varied delegation attacks:
  - *fixed* signer w.r.t. *fixed* designated verifiers,
  - *any* signer w.r.t. *fixed* designated verifiers,
  - *fixed* signer w.r.t. *any* designated verifiers.
- New weaker notion of delegatability

Thank You!

Q & A