Signature from One-way Functions

Cassius Puodzius

Technische Universität Darmstadt

Mar. 12, 2012

Outline

Outline of the seminar

- Motivation
- Quick introduction to One-way functions
- Attack model
- One-time signatures
  - Lamport's One-Time Signature Scheme
- ℓ-time signatures
- Full-fledged one-time signature from length-restricted one-time signature
  - Hash-and-sign paradigm
- General signature scheme from one-time signature
  - Refreshing paradigm
  - Authentication-trees
- Conclusions

Motivation

Security of Digital Signatures

Security assumptions:

- Integer factorization: *Rabin signature* [2]
- DLP: *Modified ElGamal scheme* [7]
- RSA: *RSA-PSS* [3]
- SVP: *GPV* [4]

or even:

- k-wCDHP (k-weak Computational Diffie-Hellman Problem) [9]
- k+1-IEP (k+1 inverse exponent problem) [1]
- k+1-SRP ($k + 1$ Square Roots Problem) [8]
- BISDHP (bilinear inverse-square Diffie-Hellman problem) [1]

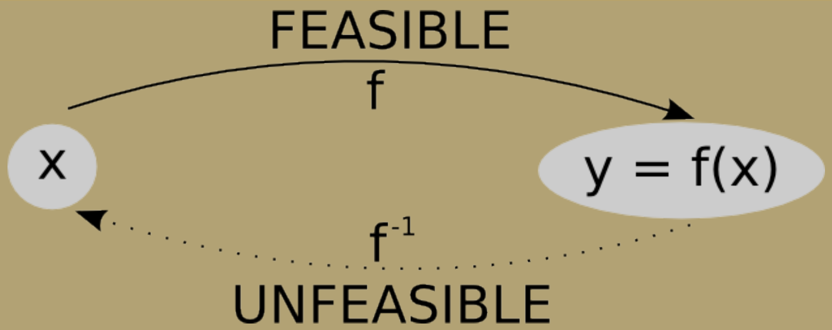
Motivation

Goal

Obtain secure digital signatures solely based on the existence of one-way functions

Quick introduction to One-way functions

Idea



Quick introduction to One-way functions

Definition

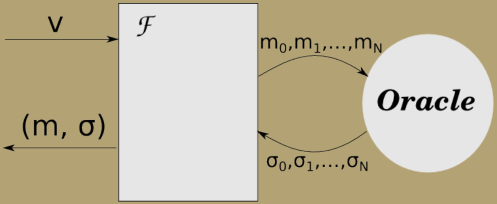
No probabilistic algorithm is able to find x given $f(x)$ in polynomial-time

Existence of OWF

- No known OWF
- Candidates: Factorization, Discrete Logarithm, Multivariate Polynomials, Learning with errors, ...

Attack model

Adaptive chosen-message attack



$m \notin \{m_0, m_1, \ldots, m_N\}$

Attack model

Existential Unforgeability

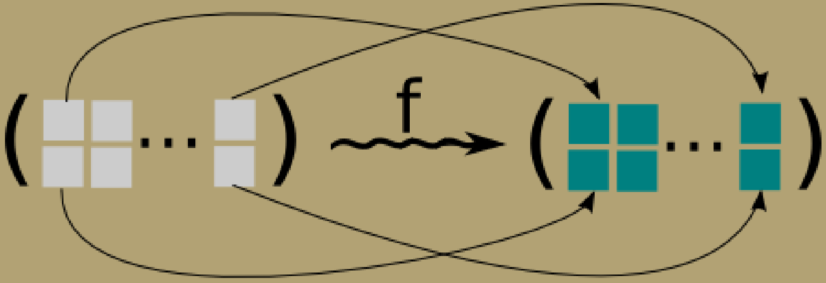
A signature scheme is secure (or unforgeable) if every feasible chosen message attack succeeds with at most negligible probability [6]

Strong Existential Unforgeability

The forger is allowed to output $m_i \in \{m_0, m_1, \ldots, m_N\}$, however $\sigma \neq \sigma_i$.

Lamport's One-Time Signature Scheme

G: Key Generation



signing-key: (…)
verification-key: (…)

Lamport's One-Time Signature Scheme

G: Key Generation

Given $f : \mathcal{D} \to \mathcal{I}$ a OWF

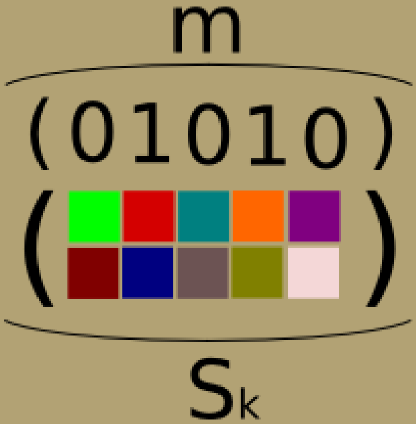
$$s_k = \begin{pmatrix} s_1^0 & \dots & s_{\ell(n)}^0 \\ s_1^1 & \dots & s_{\ell(n)}^1 \end{pmatrix} \rightsquigarrow v_k = \begin{pmatrix} v_1^0 & \dots & v_{\ell(n)}^0 \\ v_1^1 & \dots & v_{\ell(n)}^1 \end{pmatrix}$$

such that $\forall i \in \{1, \dots, \ell(n)\}$ and $\forall b \in \{0, 1\}$: $s_i^b \xleftarrow{\$} \mathcal{D}$ and $v_i^b = f(s_i^b)$

s_k: signing-key (secret)
v_k: verification-key (public)

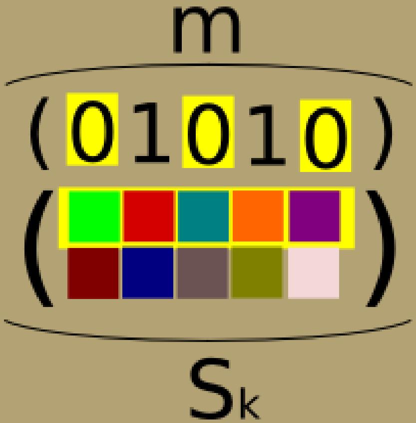
Lamport's One-Time Signature Scheme

S and V: Signature and Verification



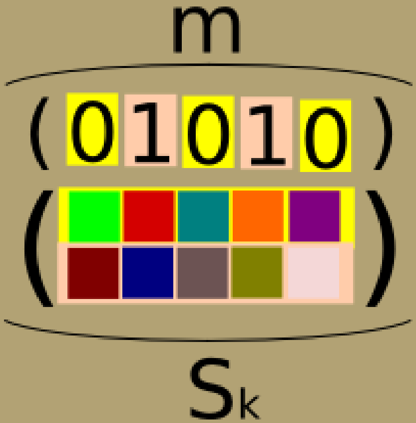
Lamport's One-Time Signature Scheme

S and V: Signature and Verification



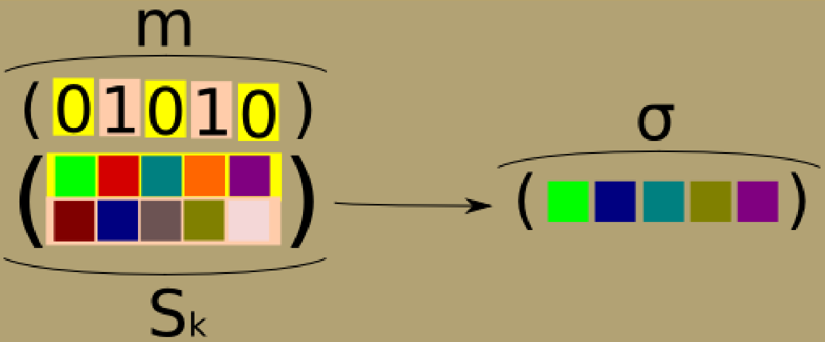
Lamport's One-Time Signature Scheme

S and V: Signature and Verification



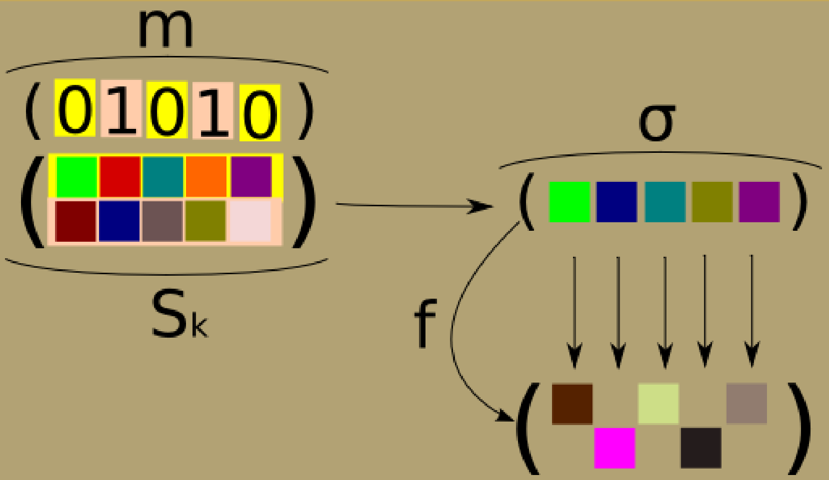
Lamport's One-Time Signature Scheme

S and V: Signature and Verification



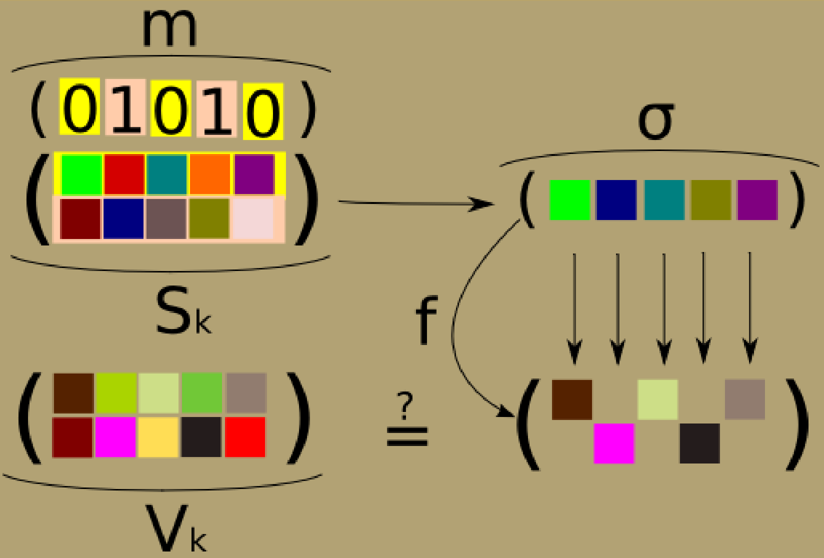
Lamport's One-Time Signature Scheme

S and V: Signature and Verification



Lamport's One-Time Signature Scheme

S and *V*: Signature and Verification



Lamport's One-Time Signature Scheme

$S(s_k, m)$: Signature

For each bit m_i of $m \in \{0,1\}^{\ell(n)}$:

$$\sigma_i = \begin{cases} s_i^0 & \text{if } m_i = 0 \\ s_i^1 & \text{if } m_i = 1 \end{cases}$$

$V(p_k, m, \sigma)$: Verification

If for all $i \in \{1, \ldots, \ell(n)\}$:

$$v_i^{m_i} = f(\sigma_i)$$

then the signature is accepted. Otherwise it is rejected.

Drawback

Lamport is a length-restricted signature

Lamport's One-Time Signature Scheme

Chosen one-message attack

The adversary can make at most one query to its Signing Oracle

Why one-time signature?

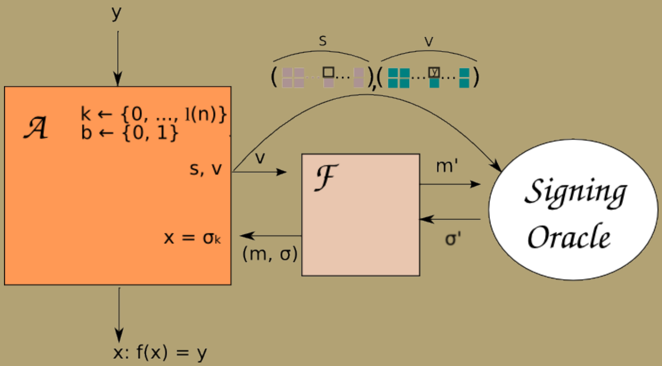
Choosing the messages $0^{\ell(n)}$ and $1^{\ell(n)}$ an attacker is able to sign any further message $m \in \{0,1\}^{\ell(n)}$

Lamport's One-Time Signature Scheme

Proposition

Lamports OTS is unforgeable under a *chosen one-message attack* assuming that f is a OWF.

Depiction of proof



Lamport's One-Time Signature Scheme

Proof - Setup

$p \stackrel{\$}{\leftarrow} \{0, \ldots, \ell(n)\}$, $b \stackrel{\$}{\leftarrow} \{0, 1\}$

$s_k = \begin{pmatrix} s_1^0 & \ldots & a_p^0 & \ldots & s_{\ell(n)}^0 \\ s_1^1 & \ldots & a_p^1 & \ldots & s_{\ell(n)}^1 \end{pmatrix} \rightsquigarrow p_k = \begin{pmatrix} v_1^0 & \ldots & b_p^0 & \ldots & v_{\ell(n)}^0 \\ v_1^1 & \ldots & b_p^1 & \ldots & v_{\ell(n)}^1 \end{pmatrix}$

where $\{s_p^0, s_p^1\} = \{\perp, s_p^{1-b}\}$ and $\{v_p^0, v_p^1\} = \{y, f(s_p^{1-b})\}$.

Proof - Emulation of Signing Oracle

When $\mathcal{F}$ demands a signature on m':

$$\sigma' \leftarrow \begin{cases} \perp & \text{if } m_p = b \Rightarrow \textit{Attack failed} \\ S_s(m) & \text{if } m_p = 1 - b \end{cases}$$

Lamport's One-Time Signature Scheme

Proof - Inversion of OWF

If $\mathcal{F}$ outputs a forgery on m_p and $m_p = b$, then:

$$x \leftarrow \sigma_p | f(x) \equiv f(\sigma_p) = y$$

Proof - Probability of success

$$\begin{aligned} Pr[Inv(y)] &\geq \underbrace{Pr[\text{Em. Signing Oracle}]}_{=1/2} \wedge \underbrace{Pr[\mathcal{F} \leftarrow \text{SUCESS}]}_{=\varepsilon} \\ &\wedge \underbrace{Pr[\text{forgery on } m_p]}_{\geq 1/\ell(n)} \wedge \underbrace{Pr[m_p = b]}_{=1/2} \\ Pr[Inv(y)] &\geq \frac{\varepsilon}{4 \cdot \ell(n)} \Rightarrow \textit{non-negligible} \end{aligned}$$

Corollary *(One-time signature)*

Corollary

If there exists any one-way function then there exists length-restricted one-time signatures as well

ℓ-time signatures

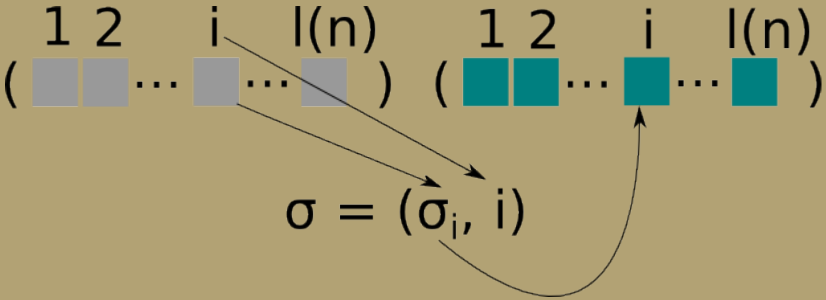
ℓ-time signature from one-time signature

For any polynomial ℓ:
ℓ one-time signature keys are generated and appended together to generate

$$sk := (sk_1, \ldots, sk_\ell) \qquad pk := (pk_1, \ldots, pk_\ell)$$

ℓ-time signatures

ℓ-time signature from one-time signature



signing-key: (⋯ ⋯)

verification-key: (⋯ ⋯)

ℓ-time signatures

ℓ-time signature from one-time signature

For $i \leq \ell$

$$\sigma_i \leftarrow \mathsf{Sign}_{sk_i}(m)$$

The signature of m is (i, σ_i).

Drawback

Stateful signature

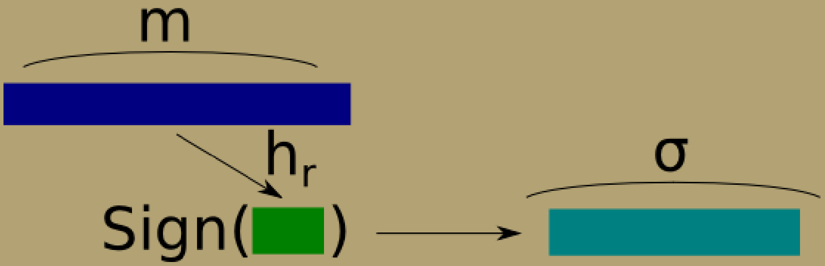
Corollary (*ℓ-time signature*)

Corollary

If there exists any one-way function then there exists length-restricted ℓ-time signature as well

Full-fledged one-time signature from length-restricted one-time signature

Hash-and-sign paradigm



$\{h_r : \{0,1\}^* \to \{0,1\}^\ell\}_{r \in \{0,1\}^*}$: *collision-free hashing collection*

Pro

Signature size depends only on the size of the signing-key

Full-fledged one-time signature from length-restricted one-time signature

Key generation with G'

On input 1^k

$$(s, v) \leftarrow G(1^k) \qquad r \leftarrow I(1^k)$$

G' outputs ((r, s), (r, v))

Signature with S'

On input a signing-key (r, s) and $m \in \{0,1\}^*$

$$\sigma \leftarrow S_s(h_r(m))$$

S' outputs σ

Verification with V'

On input a verification-key (r, v), $m \in \{0,1\}^*$ and a signature σ
V' outputs $V_v(h_r(m), \sigma)$

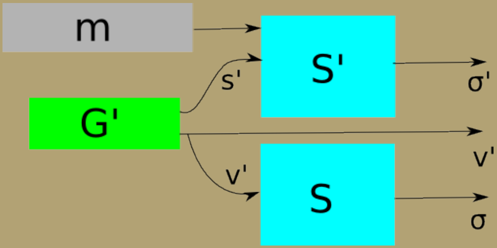
Full-fledged one-time signature from length-restricted one-time signature

Isn't collision-free hashing collection a new assumption?

Yes, but it may be replaced by a collection of Universal One-Way Hash Functions (UOWHF), which can be constructed using OWF [6].

General signature scheme from one-time signature

Refreshing paradigm



(G, S, V): signature scheme - (G', S', V'): one-time signature scheme

Refreshing paradim → general signature scheme (G", S", V"), which has G" = G

Drawback

(G, S, V) is not a one-time signature scheme

General signature scheme from one-time signature

Signing with S"

On input of a signing-key s and $m \in \{0,1\}^*$

$$\begin{aligned} (s', v') &\leftarrow G'(1^k) \\ \sigma_1 &\leftarrow S_s(v') \\ \sigma_2 &\leftarrow S'_{s'}(m) \end{aligned}$$

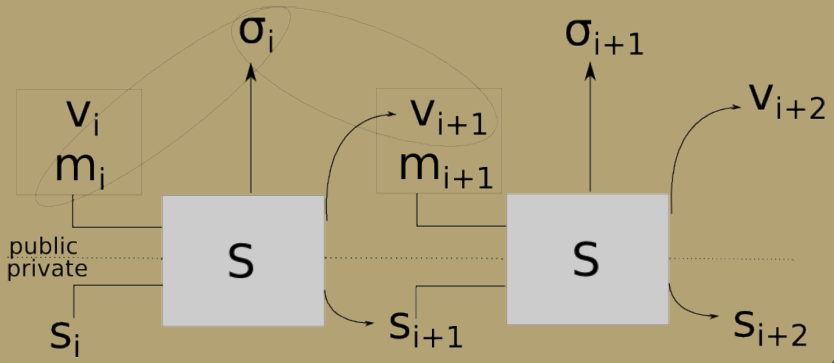
S" outputs (σ_1, v', σ_2)

Verifying with V"

On input of a verifying-key v, $m \in \{0,1\}^*$ and (σ_1, v', σ_2)
If $V_v(v', \sigma_1) = 1$ and $V'_{v'}(m, \sigma_2)$ the signature is accepted, otherwise rejected

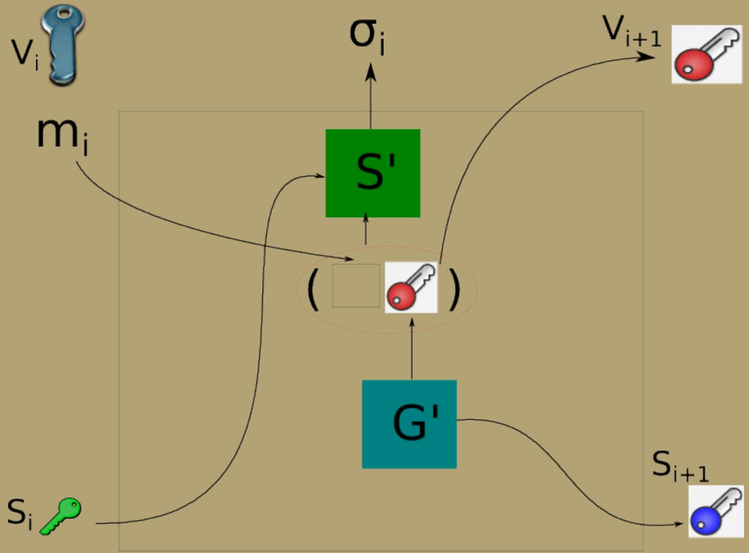
General signature scheme from one-time signature

Chain-Based signature



General signature scheme from one-time signature

Chain-Based signature



General signature scheme from one-time signature

Chain-Based signature

On input of $m_i \in \{0,1\}^*$:

$$\begin{aligned}(s_{i+1}, v_{i+1}) &\leftarrow G(1^k)\\ \sigma_i &\leftarrow S_{s_i}(m_i || v_{i+1})\end{aligned}$$

Add $(m_i,\ s_{i+1},\ v_{i+1},\ \sigma_i)$ to the current state
Signature: $\{m_j, v_{j+1}, \sigma_j\}_{j=0}$

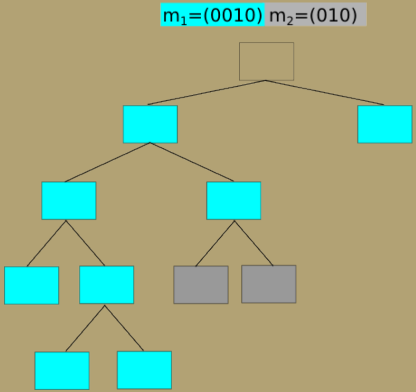
Chain-Based verification

On input of a verifying-key v_0, $m_i \in \{0,1\}^*$ and the signature $\{m_j, v_{j+1}, \sigma_j\}_{j=0}^{j=i}$:

$\mathrm{Vrfy}_{v_j}((m_j || v_{i+1}), \sigma_j) \stackrel{?}{=} ACCEPTED\ \forall j \in \{0, \cdots, i\}$

General signature scheme from one-time signature

Tree-Based signature



General signature scheme from one-time signature

Tree-Based signature

On input of $m \in \{0,1\}^N$, let μ_i be the first i bits of m (prefix):
If μ_i was never signed (while $i <= N$)

$$\begin{aligned}
(s_{\mu_i|0}, v_{\mu_i|0}) &\leftarrow G(1^k) \\
(s_{\mu_i|1}, v_{\mu_i|1}) &\leftarrow G(1^k) \\
\sigma_i &\leftarrow S_{s_i}(v_{\mu_i|0}||v_{\mu_i|1}) \\
\boxed{\mu_i|0} &\leftarrow \{s_{\mu_i|0}, v_{\mu_i|0}\} \\
\boxed{\mu_i|1} &\leftarrow \{s_{\mu_i|1}, v_{\mu_i|1}\} \\
\boxed{\mu_i} &\leftarrow S_{s_{\mu_i}}(v_{\mu_i|0}||v_{\mu_i|1})
\end{aligned}$$

$\sigma_m \leftarrow S_{s_m}(m)$

Signature: $(\{\overbrace{\sigma_j, v_{\mu_j|0}, v_{\mu_j|1}}^{auth_{\mu_j}}\}_{j=0}, \sigma_m)$

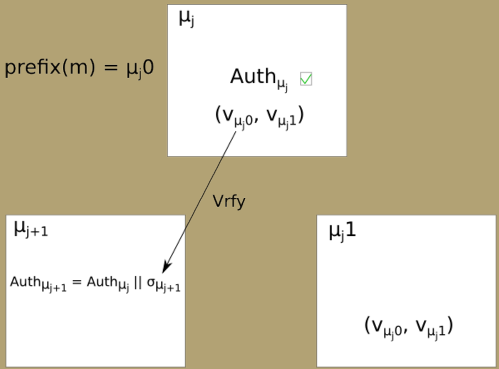
General signature scheme from one-time signature

Chain-Based verification

On input of a verifying-key v_0, $m \in \{0,1\}^N$ and the signature $(\{auth_j\}_{j=0}, \sigma_m)$:

$$\mathrm{Vrfy}_{v_{\mu_j}}(auth_{\mu_{j+1}}) \stackrel{?}{=} ACCEPTED \; \forall j \in \{0, N\}$$

$$\mathrm{Vrfy}_{v_m}(\sigma_m) \stackrel{?}{=} ACCEPTED$$

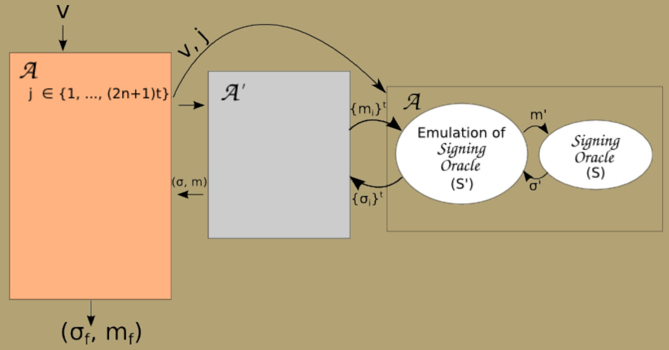


General signature scheme from one-time signature

Proposition

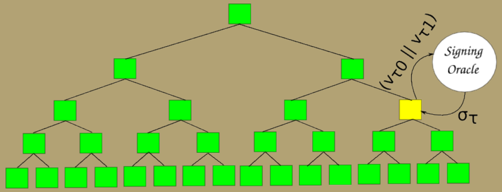
If G is a strongly unforgeable signature under a one-time chosen-message attack, then a tree-based scheme G' is strongly unforgeable signature under an adaptive chosen-message attack

Depiction of proof

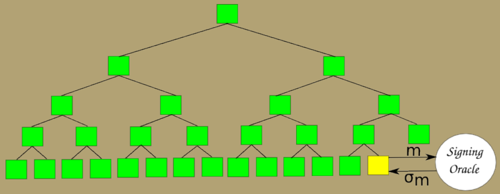


General signature scheme from one-time signature

Emulation of Oracle: Case 1



Emulation of Oracle: Case 2



General signature scheme from one-time signature

Proof - Setup

$\mathcal{A}'$ is a probabilistic *polynomial time* adversary $\Rightarrow t \leftarrow \#[\text{query}]$
$\Omega(n) = (2 \cdot poly(n) + 1)t \geq \#[(G, S, V)]$
$j \xleftarrow{\$} \{1, \cdots, \Omega(n)\}$

General signature scheme from one-time signature

Proof - Emulation of Signing Oracle (Case 1)

Node j is on the authentication path:

$$
\begin{aligned}
(s_{\mu_j|0}, v_{\mu_j|0}) &\leftarrow G(1^k) \\
(s_{\mu_j|1}, v_{\mu_j|1}) &\leftarrow G(1^k) \\
\sigma_j &\leftarrow S_{s_j}(v_{\mu_j|0}||v_{\mu_j|1})[\textit{One-time Signing Oracle}] \\
\boxed{\mu_i|0} &\leftarrow \{s_{\mu_i|0}, v_{\mu_i|0}\} \\
\boxed{\mu_i|1} &\leftarrow \{s_{\mu_i|1}, v_{\mu_i|1}\} \\
\boxed{\mu_i} &\leftarrow S_{s_{\mu_i}}(v_{\mu_i|0}||v_{\mu_i|1})
\end{aligned}
$$

Proof - Emulation of Signing Oracle (Case 2)

Node j is a leaf: $\sigma_m \leftarrow S_s(m)$ [*One-time Signing Oracle*]

General signature scheme from one-time signature

Proof - Forgery in (G, S, V)

If $\mathcal{A}'$ outputs a forgery $(m, \sigma, auth_m)$ and this forgery happens in node j, then:

$$(\sigma_f, m_f) \leftarrow \begin{cases} (\sigma_{\mu_j}, v_{\mu_{j+1}}) & \text{if } j \in Auth_m \\ (\sigma, m) & \text{if } j \notin Auth_m \end{cases}$$

Proof - Probability of success

$$Pr[(\sigma_f, m_f)] \geq \underbrace{Pr[\mathcal{A}' \leftarrow \text{SUCESS}]}_{=\varepsilon} \wedge \underbrace{Pr[\text{forgery on } j]}_{\geq 1/\Omega(n)}$$

$$Pr[(\sigma_f, m_f)] \geq \frac{\varepsilon}{\Omega(n)} \Rightarrow \textit{non-negligible}$$

Corollary (*General signature scheme from one-time signature*)

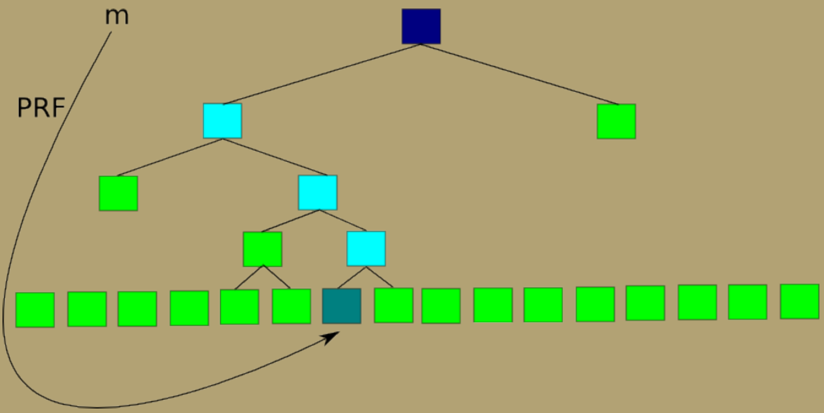
Corollary

If there exists any one-way function then there exists (stateful) general signature as well

General (stateless) signature scheme from one-time signature

Stateless Signature

Use of PRF (which can be obtained from OWF [6]):



General (stateless) signature scheme from one-time signature

Proposition

If (G, S, V) is a secure one-time signature scheme and $\{f_r : \{0,1\}^* \to \{0,1\}^{|r|}\}_{r \in \{0,1\}^*}$ is a generalized pseudorandom function ensemble then (G', S', V') constitutes a secure (general) signature scheme. [6]

Idea of the proof

Exponential growth of leaves $\to$ exponentially-vanishing probability of two signatures in the same leaf

Disregard two-times signatures $\to$ security proof similar to stateful scheme

Corollary (*General signature scheme from one-time signature*)

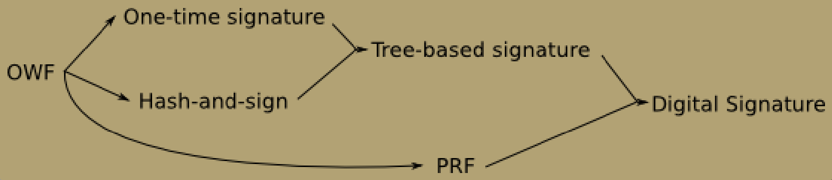
Corollary

If there exists any one-way function then there exists a general signature as well

Conclusions

Theoretical Implication

- If there exist any one-way function then there exist a general signature as well



Conclusions

So why RSA, DLP, SVP, ...?

Digital Signature			
Scheme	Assumption	S-key size (KB)	Signature Size (KB)
RSA-1024	RSA	0.62	0.13
ECDSA	DLP	0.08	0.32
GPV	SVP	6.12	13.18
Merkle-tree	OWF	41.3[a]	2.27

[a] For 2^{22} signatures[5]

The End

That's it! Questions? Remarks?

References I

Sedat Akleylek, Baris Bulent Kirlar, Omer Sever, and Zaliha Yuce.
A new short signature scheme with random oracle from bilinear pairings.

Daniel J. Bernstein.
Proving tight security for rabin/williams signatures.
In *In EUROCRYPT*, 2008.

Johannes Böck.
Rsa-pss - provably secure rsa signatures and their implementation v1.0.1, 2011.

Johannes Buchmann, Richard Lindner, Markus Rückert, and Michael Schneider.
Post-quantum cryptography: lattice signatures.
Computing, 85(1-2):105–125, 2009.

References II

- Luis Carlos and Luis Carlos Coronado Garcia.
  On the security and the efficiency of the merkle signature scheme, 2005.
- Oded Goldreich.
  Draft of chapter on signature schemes, 2003.
- David Pointcheval and Jacques Stern.
  Security Proofs for Signature Schemes.
  In Ueli Maurer, editor, *Advances in Cryptology - Proceedings of EUROCRYPT '96*, volume 1070 of *Lecture Notes in Computer Science*, pages 387–398, Saragossa, Spain, 1996. Springer.
- Fangguo Zhang, Xiaofeng Chen, Willy Susilo, and Yi Mu.
  A new short signature scheme without random oracles from bilinear pairings.
  In *IN: VIETCRYPT 2006, LNCS 4341*, pages 67–80, 2005.

References III

Fangguo Zhang, Reihaneh Safavi-naini, and Willy Susilo.
Efficient verifiably encrypted signature and partially blind signature from bilinear pairings, 2004.