Unique Signature with Short Output from CDH Assumption

Shiuan-Tzuo Shen, Amir Rezapour and Wen-Guey Tzeng

國立交通大學
National Chiao Tung University

outline

- Introduction
- Contribution
- Unique Signature Scheme
- Efficiency
- Security Proof
- Conclusion

Introduction

- Each message would have only "*one*" possible signature.
- *EUF-CMA* AND *SUF-CMA*.
  - Adversary cannot even produce a valid signature for an earlier signed message.

Introduction

- There is no reason to verify a signature on the same message twice.
- Above all:
  - Selective-identity CPA-secure IBE → adaptive CCA-secure IBE scheme. [CHK06]
  - VRF (Verifiable Random Function)
  - Non-interactive zero-knowledge proofs
  - micropayment schemes
  - Verifiable transaction escrow schemes, …

Contribution

- Unique signature scheme with
  - a *weaker assumption (CDH)*
  - a signature of only "*one*" group element.
- In order to give a non-negligible lower bound to our reduction:
  I. We design a dynamic pattern for signature.
  II. The combination of secret exponents is determined by the hash of message.
  III. The forgery has a specific pattern.

Contribution

- Malicious signer resistance.
  - Upper bound for hash outputs → in the same signature.
  - Equivalent set.
- H-F-H
  - To evaluate the output, a malicious signer has to decide his public key first.
  - H-F-H structure is one-way.
  - Double hash layers.

Unique Signature Scheme

- $Setup(1^k) \rightarrow \pi$.
  - Let q be a k-bit prime, $\mathbb{G}$ and $\mathbb{G}_{\mathbb{T}}$ be two multiplicative cyclic groups of prime order q.
  - $H: \{0,1\}^* \rightarrow \{0,1\}^{n+t-1}$ be a cryptographic hash function.
  - $F: \{0,1\}^{n+t-1+n_0} \rightarrow \{0,1\}^{n+t-1+n_0}$ be a one-way permutation.

$$\pi = (k, n_0, n, q, \mathbb{G}, \mathbb{G}_{\mathbb{T}}, g, \hat{e}, H, F)$$

Unique Signature Scheme (cont.)

- $KeyGen(\pi) \rightarrow (sk, pk)$.
  - A signer randomly chooses $2n$ exponents $a_{i,j} \in_R \mathbb{Z}_q^*$ and computes $A_{i,j} = g^{a_{i,j}}$, where i $\in \mathbb{Z}_n$ and j $\in \mathbb{Z}_2$.
  - These exponents have to satisfy the two requirements:
    1. All $a_{i,j}$ are distinct → every $A_{i,j}$ is unique
    2. For every $h \in \{1,2, \ldots, \frac{n-1}{2}\}$, every i $\in \mathbb{Z}_n$, and every j, j′ $\in \mathbb{Z}_2$, we have $a_{i,j} + a_{[i+2h],j'} \neq 0 \rightarrow A_{i,j} \times A_{[i+2h],j'} \neq 1$.

$$sk = \{(a_{0,0}, a_{0,1}), (a_{1,0}, a_{1,1}), \ldots, (a_{n-1,0}, a_{n-1,1})\}$$
$$pk = \{(A_{0,0}, A_{0,1}), (A_{1,0}, A_{1,1}), \ldots, (A_{n-1,0}, A_{n-1,1})\}$$

Unique Signature Scheme (cont.)

- $Sign(\pi, sk, pk, m) \rightarrow \sigma$
  - To sign a message $m \in \{0,1\}^{n_0}$, a signer generates the signature σ as follows:
    1. $x = H(pk \parallel m)$.
    2. $y = F(x \parallel m)$.
    3. $z = H(y)$.
    4. Let $h = LSB_{t-1}(z) + 1$. Use his secret key sk:

$$\sigma = \prod_{i=0}^{n-1} g^{a_{i,z(i)} a_{[i+h],z([i+h])}}$$

Unique Signature Scheme (cont.)

- $Verify(\pi, pk, m, \sigma) \rightarrow \{Yes, No\}$
  1. $x = H(pk \parallel m)$.
  2. $y = F(x \parallel m)$.
  3. $z = H(y)$.
  4. Let $h = LSB_{t-1}(z) + 1$. Use signer's public key pk:

$$\hat{e}(\sigma, g) = \prod_{i=0}^{n-1} \hat{e}\left(A_{i,z(i)}, A_{[i+h],z([i+h])}\right)$$

Unique Signature Scheme (cont.)

- ***Consistency:*** If the signature σ is well-formed, then we have:

$$\hat{e}(\sigma, g) = \hat{e}\left(\prod_{i=0}^{n-1} g^{a_{i,z(i)}a_{[i+h],z([i+h])}}, g\right)$$

$$= \prod_{i=0}^{n-1} \hat{e}\left(g^{a_i,z(i)}, g^{[i+h],z([i+h])}\right)$$

$$= \prod_{i=0}^{n-1} \hat{e}\left(A_{i,z(i)}, A_{[i+h],z([i+h])}\right)$$

Unique Signature Scheme (cont.)

- ***Uniqueness:*** If there are two signatures (σ_1, σ_2) for the same message m under a secret-public key pair (sk, pk).
  - Since σ_1 and σ_2 share the same
    - $x = H(pk \parallel m)$,
    - $y = F(x \parallel m)$
    - $z = H(y)$
    - and $h = LSB_{t-1}(z) + 1$.

$$\hat{e}(\sigma_1, g) = \prod_{i=0}^{n-1} \hat{e}\left(A_{i,z(i)}, A_{[i+h],z([i+h])}\right) = \hat{e}(\sigma_2, g)$$

Thus, it must be $\sigma_1 = \sigma_2$ unless g is not a generator.

Efficiency

- ***Sign:*** $2Hash + Perm + (n-1)Add_{\mathbb{Z}_q} + nMul_{\mathbb{Z}_q} + Exp_{\mathbb{G}}$
- ***Verify:*** $2Hash + Perm + (n+1)Pair + (n-1)Mul_{\mathbb{G}_{\mathbb{T}}}$

Scheme	Assumption	SK (bits)	PK (bits)	Output (bits)
Micali et. al.	RSA	k	$(2k^2+1)k+t$	k
Jager	l-CDH	$2nk$	$(2n+2)\ell$	$n\ell$
Lysyanskaya	l-CDH	$2nk$	$2n\ell$	$n\ell$
Dodis et. al.	l-DHI	k	ℓ	ℓ
BLS	CDH	k	ℓ	ℓ
Ours	CDH	$2nk$	$2n\ell$	ℓ

Security Proof

- **Theorem 1.**
  - If the (t, ϵ)-CDH secure,
  - Our signature $(t - q_h t_h - q_s t_s, q_s, 2e(n - 1)\varepsilon)$ strongly existential unforgeability.

Security Proof (cont.)

CDH(g, g^a, g^b)

Setup

I. Choose $h^* \in \{1,2,\dots,\frac{n-1}{2}\}$

II. $i^* \in_R \mathbb{Z}_n$ and $\mathrm{b}_{i^*}, \mathrm{b}_{[i^*+h^*]} \in \mathbb{Z}_2$

$\mathcal{O}_H$

Maintain a table $\boldsymbol{T}_{\mathrm{H}} = \{(\mathrm{m}, \mathrm{H}(\mathrm{m}))\}$
Choose $x \in_R \{0,1\}^{n+t-1}$ and $H(m) = x$

$\mathcal{O}_S$

Combine the secret exponents and compute σ_{m_i}

$h^* = h, z(i^*) = b_{i^*}, z([i^*+h^*]) = \mathrm{b}_{[i^*+h^*]}$

$pk = \{(A_{0,0}, A_{0,1}), (A_{i^*,\mathrm{b}'_{i^*}}, g^a), \dots, (g^b, A_{[i^*+h^*],\mathrm{b}'_{[i^*+h^*]}}), (A_{n-1,0}, A_{n-1,1})\}$

q_h

$m \in \{0,1\}^*$

$H(m) = x$

q_s

$m_i \in \{0,1\}^{n_0}$

σ_{m_i}

(m^*, σ^*)

Security Proof (cont.)

- **Theorem 2.**
  - Min-entropy
  - $\left(t_S\ , \varepsilon_H\ + \frac{t_S\ (t_S - 1)}{2} \times 2^{\left(\frac{1}{3} - c\right)n} + \ 2\varepsilon_F\ + \ t_S \times 2^{-cn-t+1}\right)$ malicious signer resistance.

Conclusion

- We proposed a unique signature scheme on groups equipped with bilinear map.
- Our unique signature scheme produces a signature of only one group element.
- The security of the proposed scheme is based on the CDH assumption in the random oracle model.

Thank you for your attention!

- ePrint: *https://eprint.iacr.org/2015/830*