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

- Unique signature (VUF), is a function from the message space to the signature space under the given public key.
- This particular property ensures that each message would have only "*one*" possible signature.
- From the security perspective, unique signature is not only *EUF-CMA*, but also *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.
  - For instance, if one has verified a signature on one particular message, it is unnecessary to verify the message again unless the signature is changed.
  - A very efficient signer can generate many signatures for one particular message. This may simply lead to overload a verifier to verify many signatures on the same message.
- Above all:
  - Constructing an adaptive CCA-secure IBE encryption scheme from a selective-identity CPA-secure IBE scheme.
  - VRF (Verifiable Random Function)
  - Non-interactive zero-knowledge proofs, micropayment schemes, verifiable transaction escrow schemes, compact e-cash, adaptive oblivious transfer protocols,…

Contribution

- The primary objective of this study is to find a unique signature scheme with a *weaker assumption (CDH)* and 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 contains the solution of the *CDH* problem has a specific pattern.

Contribution

- Malicious signer resistance.
  - Find an upper bound for the number of hash outputs which result in the same signature.
  - We proposed the notion of the equivalent set for a signature and show that the size of an equivalent set is in a negligible proportion.
- H-F-H
  - To evaluate the output, a malicious signer has to decide his public key first.
  - H-F-H structure is one-way. Therefore, a malicious signer cannot compute a message from an equivalent set.
  - The design of double hash layers makes a malicious signer hard to find a candidate for the hash function.

Definitions

- Bilinear Map. Let $\mathbb{G}$ and $\mathbb{G}_{\mathbb{T}}$ be two multiplicative cyclic groups of prime order q. Let g be a generator of $\mathbb{G}$. A map $\hat{e}: \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_{\mathbb{T}}$ is called an admissible bilinear map if it satisfies the following properties:
  - Bilinearity: for all $u, v \in \mathbb{G}$ and $x, y \in \mathbb{Z}_q$, we have $\hat{e}(u^x, v^y) = \hat{e}(u, v)^{xy}$.
  - Non-degeneracy: we have $\hat{e}(g, g) \neq \mathbf{1}$, where $\mathbf{1}$ is the identity element of $\mathbb{G}_{\mathbb{T}}$.
  - Computability: there is a polynomial-time algorithm to compute $\hat{e}(u, v)\ \forall\, u, v \in \mathbb{G}$.

Unique Signature Scheme

- $Setup(1^k) \rightarrow \pi.$
  - Let k be the security parameter, and n_0 be the message length, where $n_0 = \ poly(k)$.
  - Let n be $2t+1$, and $[x]$ denote $[x]_n = x \ mod \ n$, where $t \in \mathbb{N}$ and $n = \theta(n_0)$.
  - 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.

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

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

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. For every $i, i' \in \mathbb{Z}_n$ and every $j, j' \in \mathbb{Z}_2$, we have $a_{i,j} = a_{i',j'}$ iff. $(i, j) = (i', j')$. It can be verified without knowing the exponents by checking whether 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 $a_{i,j} + a_{[i+2h],j'} \neq 0$. It can be verified without knowing the exponents by checking whether every $A_{i,j} \times A_{[i+2h],j'} \neq 1$.

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

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

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

Unique Signature Scheme (cont.)

- $Sign(\pi, sk, pk, m) \rightarrow \sigma$
  - To sign a message $m \in \{0,1\}^{n_0}$ of n_0 bits, a signer generates the signature σ as follows:
    1. Use his public key pk and the cryptographic hash function H to compute $x = H(pk \parallel m)$.
    2. Use the one-way permutation F to compute $y = F(x \parallel m)$.
    3. Use the cryptographic hash function H to compute $z = H(y)$.
    4. Let $h = LSB_{t-1}(z) + 1$, where $LSB_{t-1}(z)$ is the least $t-1$ significant bits of z. Use his secret key sk:

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

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

Unique Signature Scheme (cont.)

- $Verify(\pi, pk, m, \sigma) \rightarrow \{Yes, No\}$
  - Suppose that the signer's public key pk is well-formed. A verifier verifies a message-signature pair (m, σ) of the signer as follows:
    1. Use the cryptographic hash function H and signer's pk to compute $x = H(pk \parallel m)$.
    2. Use the one-way permutation F to compute $y = F(x \parallel m)$.
    3. Use the cryptographic hash function H to compute $z = H(y)$.
    4. Let $h = LSB_{t-1}(z) + 1$, where $LSB_{t-1}(z)$ is the least $t - 1$ significant bits of z. Use signer's public key pk:

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

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

Unique Signature Scheme (cont.)

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

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

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

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

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

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

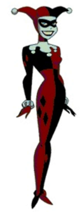
Security Proof

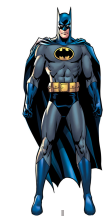
- **Theorem 1.**
  - Let k be the security parameter.
  - Let $\mathcal{O}_S$ be the signing oracle of the unique signature scheme. Suppose that an adversary queries at most q_s messages to $\mathcal{O}_S$, and each query is handled in time t_s.
  - Let $\mathcal{O}_H$ be the random oracle of hash function H, where $n = 2t + 1 \in poly(k)$ and $n \geq \frac{q_s+3}{2}$. Suppose that an adversary queries at most q_h messages to $\mathcal{O}_H$, and each query is handled in time t_h.
  - If the (t, ϵ)-CDH assumption holds, the unique signature scheme achieves $(t - q_h t_h - q_s t_s, q_s, 2e(n - 1)\varepsilon)$ strongly existential unforgeability, where e is the Euler's number.

Shiuan-Tzuo Shen, Amir Rezapour and Wen-Guey Tzeng
26. November 2015

Security Proof (cont.)

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





Setup

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

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

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

$\mathcal{O}_H$

Maintain a table $\boldsymbol{T}_{\mathrm{H}} = \{(\mathrm{m}, \mathrm{H}(\mathrm{m}))\}$

Choose $x \in_R \{0,1\}^{n+t-1}$ and $H(m) = x$

q_h

$\mathrm{H}(m), m \in \{0,1\}^*$

x

$\mathcal{O}_S$

As long as signing the queried message doesn't contain both instance of input challenge, compute the combination of known exponents to compute the signature σ_{m_i}

q_s

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

σ_{m_i}

(m^*, σ^*)

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

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

Security Proof (cont.)

- **Theorem 2.**
  - Let k be the security parameter.
  - Let c be a positive real number, where $1/3 < c < 1$.
  - Let t_S be the execution time of a malicious signer S, where $t_S \in poly(k)$.
  - Suppose that hash function H is (t_H, ε_H) collision resistant.
  - Suppose that one-way permutation F is (t_F, ε_F) one-way.
  - If we choose $\epsilon_H \le 1 - e^{-\frac{t_S(t_S-1)}{2} \times 2^{-cn-t+1}}$, the unique signature scheme achieves $\left(t_S, \varepsilon_H + \frac{t_S(t_S-1)}{2} \times 2^{\left(\frac{1}{3}-c\right)n} + 2\varepsilon_F + t_S \times 2^{-cn-t+1}\right)$ 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 computational Diffie-Hellman assumption in the random oracle model.

Thank you for your attention!

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