Chair of
Applied Cryptography

FRIEDRICH-ALEXANDER
UNIVERSITÄT
ERLANGEN-NÜRNBERG

FACULTY OF ENGINEERING

A Family of FDH Signature Schemes Based on the Quadratic Residuosity Assumption

Giuseppe Ateniese[1], **Katharina Fech**[2], Bernardo Magri[2]
[1]Stevens Institute of Technology
[2]Friedrich-Alexander-Universität Erlangen-Nürnberg

Overview

1. (Unique) signatures
2. Tight proofs
3. State of the art
4. Unique scheme
5. Efficiency
6. Deterministic scheme

Signatures

$$m, \sigma$$

$$(\mathsf{vk}, \mathsf{sk}) \leftarrow \mathsf{KGen}(1^\kappa)$$
$$\sigma \leftarrow \mathsf{Sign}(\mathsf{sk}, m)$$

$$b := \mathsf{Vrfy}(\mathsf{vk}, (m, \sigma))$$

Signatures

m, σ

$(\mathsf{vk}, \mathsf{sk}) \leftarrow \mathsf{KGen}(1^\kappa)$
$\sigma \leftarrow \mathsf{Sign}(\mathsf{sk}, m)$

$b := \mathsf{Vrfy}(\mathsf{vk}, (m, \sigma))$

Definition: $\Pi = (\mathsf{KGen}, \mathsf{Sign}, \mathsf{Vrfy})$ is (t, q, ε)-existentially unforgeable under chosen-message attacks if for all adversaries A running in time t it holds

$$\mathbb{P}\left[\mathsf{Vrfy}(\mathsf{vk}, (m^*, \sigma^*)) = 1 \wedge m^* \notin \mathcal{Q} : \begin{array}{c}(\mathsf{vk}, \mathsf{sk}) \leftarrow \mathsf{KGen}(1^\kappa); \\ (m^*, \sigma^*) \leftarrow \mathsf{A}^{\mathsf{Sign}(\mathsf{sk}, \cdot)}(\mathsf{vk})\end{array}\right] \leq \varepsilon,$$

where $\mathcal{Q} = \{m_1, \ldots, m_q\}$ is the set of queries to the signing oracle.

Unique Signatures

Definition: Π satisfies uniqueness if there exists only a *single* value $\sigma = \mathsf{Sign}(\mathsf{sk}, m)$ $\forall \mathsf{vk}$ of $(\mathsf{vk}, \mathsf{sk}) \leftarrow \mathsf{KGen}(1^\kappa)$ and $\forall\, m$ such that

$$\mathsf{Vrfy}(\mathsf{vk}, (m, \mathsf{Sign}(\mathsf{sk}, m))) = 1.$$

Unique Signatures

Definition: Π satisfies uniqueness if there exists only a *single* value $\sigma = \mathsf{Sign}(\mathsf{sk}, m)$ $\forall \mathsf{vk}$ of $(\mathsf{vk}, \mathsf{sk}) \leftarrow \mathsf{KGen}(1^\kappa)$ and $\forall\, m$ such that

$$\mathsf{Vrfy}(\mathsf{vk}, (m, \mathsf{Sign}(\mathsf{sk}, m))) = 1.$$

- Derandomized signature schemes
- Deterministic signature schemes

Advantage of Unique Signatures

Advantage of Unique Signatures

- Resistant against subversion attacks (Ateniese, Magri, Venturi CCS' 15)

Advantage of Unique Signatures

- Resistant against subversion attacks (Ateniese, Magri, Venturi CCS' 15)
- No randomness needed for signing

Advantage of Unique Signatures

- Resistant against subversion attacks (Ateniese, Magri, Venturi CCS' 15)
- No randomness needed for signing
- Efficient and easy to implement

Tight Proofs

- Degree of polynomials of running-time and success probability in reductions relevant for practical applications
- Loss is a small constant in tight reductions.

State of the Art

Hash-then-sign signature schemes in the ROM

	Assumption	Unique?	Tight?
Derandomized Rabin-Williams (EC' 08)	Factoring	✗	✓
Absolute Principal Rabin-Williams (PKC' 14)	2-Φ/4-Hiding	✓	✓
RSA-FDH (EC' 12)	Φ-Hiding	✓	✓
BLS (JoC' 04)	CDH	✓	✗
Katz-Wang (CCS' 03)	RSA	✗	✓
Our unique scheme	Quadratic Residuosity	✓	✓
Our deterministic scheme	Quadratic Residuosity	✗	✓

Unique Scheme

- Inspired by a lossy trapdoor function from Freeman et. al (JoC' 13)

- $\mathbb{J}_n$: set of all $x \in \mathbb{Z}_n^*$ with Jacobi symbol 1
  $\overline{\mathbb{J}}_n$: set of all $x \in \mathbb{Z}_n^*$ with Jacobi symbol -1
  $\mathbb{QR}_n$: set of all quadratic residues of $\mathbb{Z}_n^*$

- Define $h, j : \mathbb{Z}_n \to \{0,1\}$ as

$$h(x) = \begin{cases} 1, \text{ if } x > n/2, \\ 0, \text{ otherwise,} \end{cases}$$

$$j(x) = \begin{cases} 1, \text{ if } x \in \overline{\mathbb{J}}_n, \\ 0, \text{ otherwise.} \end{cases}$$

Unique Scheme

$\Pi_u = (\mathsf{KGen}, \mathsf{Sign}, \mathsf{Vrfy})$

$\mathsf{KGen}(1^\kappa)$

Sample a κ-bit Williams integer $n := pq$

// i. e. primes p, q such that $p \equiv 3 \mod 8, \quad q \equiv 7 \mod 8$

$s \leftarrow\!\!\$\, \mathbb{J}_n \setminus \mathbb{QR}_n$

return $\mathsf{vk} := (n, s), \quad \mathsf{sk} := (p, q)$

n Williams integer $\Rightarrow 2 \in \overline{\mathbb{J}}_n$

Unique Scheme

Sign(sk, m)

$b := 0$

$x := \mathsf{H}(m)$ // $\mathsf{H} : \{0,1\}^* \to \mathbb{Z}_n^*$ hash function

$x' := x \cdot 2^{j(x)} \mod n$

if $x' \notin \mathbb{QR}_n$ **do**

$b := 1$

$x' := x' \cdot s \mod n$

$\sigma := y$ with $y^2 \equiv x' \mod n$,
$j(y) = j(x)$,
$h(y) = b$

return σ

$$h(x) = \begin{cases} 1, \text{ if } x > n/2, \\ 0, \text{ otherwise,} \end{cases} \qquad j(x) = \begin{cases} 1, \text{ if } x \in \overline{\mathbb{J}}_n, \\ 0, \text{ otherwise.} \end{cases}$$

Unique Scheme

Sign(sk, m)

$b := 0$

$x := \mathsf{H}(m)$ // $\mathsf{H} : \{0,1\}^* \to \mathbb{Z}_n^*$ hash function

$x' := x \cdot 2^{j(x)} \mod n$

if $x' \notin \mathbb{QR}_n$ **do**

$b := 1$

$x' := x' \cdot s \mod n$

$\sigma := y$ with $y^2 \equiv x' \mod n$,
$j(y) = j(x)$,
$h(y) = b$

return σ

	$\mathbb{QR}_n$	$\overline{\mathbb{QR}}_n$
$\mathbb{J}_n$	?	?
$\overline{\mathbb{J}}_n$	?	?

$$h(x) = \begin{cases} 1, \text{ if } x > n/2, \\ 0, \text{ otherwise,} \end{cases} \qquad j(x) = \begin{cases} 1, \text{ if } x \in \overline{\mathbb{J}}_n, \\ 0, \text{ otherwise.} \end{cases}$$

Unique Scheme

Sign(sk, m)

$b := 0$

$x := \mathsf{H}(m)$ // $\mathsf{H} : \{0,1\}^* \to \mathbb{Z}_n^*$ hash function

$x' := x \cdot 2^{j(x)} \mod n$

if $x' \notin \mathbb{QR}_n$ **do**

$b := 1$

$x' := x' \cdot s \mod n$

$\sigma := y$ with $y^2 \equiv x' \mod n$,

$j(y) = j(x)$,

$h(y) = b$

return σ

	$\mathbb{QR}_n$	$\overline{\mathbb{QR}}_n$
$\mathbb{J}_n$	?	?
$\overline{\mathbb{J}}_n$		

$$h(x) = \begin{cases} 1, \text{ if } x > n/2, \\ 0, \text{ otherwise,} \end{cases} \qquad j(x) = \begin{cases} 1, \text{ if } x \in \overline{\mathbb{J}}_n, \\ 0, \text{ otherwise.} \end{cases}$$

Unique Scheme

Sign(sk, m)

$b := 0$

$x := \mathsf{H}(m)$ // $\mathsf{H} : \{0,1\}^* \to \mathbb{Z}_n^*$ hash function

$x' := x \cdot 2^{j(x)} \mod n$

if $x' \notin \mathbb{QR}_n$ **do**

$b := 1$

$x' := x' \cdot s \mod n$

$\sigma := y$ with $y^2 \equiv x' \mod n$,

$j(y) = j(x)$,

$h(y) = b$

return σ

	$\mathbb{QR}_n$	$\overline{\mathbb{QR}}_n$
$\mathbb{J}_n$	✓	
$\overline{\mathbb{J}}_n$		

$$h(x) = \begin{cases} 1, \text{ if } x > n/2, \\ 0, \text{ otherwise,} \end{cases} \qquad j(x) = \begin{cases} 1, \text{ if } x \in \overline{\mathbb{J}}_n, \\ 0, \text{ otherwise.} \end{cases}$$

Unique Scheme

Sign(sk, m)

$b := 0$

$x := \mathsf{H}(m)$ // $\mathsf{H} : \{0,1\}^* \to \mathbb{Z}_n^*$ hash function

$x' := x \cdot 2^{j(x)} \mod n$

if $x' \notin \mathbb{QR}_n$ **do**

$b := 1$

$x' := x' \cdot s \mod n$

$\sigma := y$ with $y^2 \equiv x' \mod n$,

$j(y) = j(x)$,

$h(y) = b$

return σ

$$h(x) = \begin{cases} 1, \text{ if } x > n/2, \\ 0, \text{ otherwise,} \end{cases} \qquad j(x) = \begin{cases} 1, \text{ if } x \in \overline{\mathbb{J}}_n, \\ 0, \text{ otherwise.} \end{cases}$$

Unique Scheme

Sign(sk, m)

$b := 0$

$x := \mathsf{H}(m)$ // $\mathsf{H} : \{0,1\}^* \to \mathbb{Z}_n^*$ hash function

$x' := x \cdot 2^{j(x)} \mod n$

if $x' \notin \mathbb{QR}_n$ **do**

$b := 1$

$x' := x' \cdot s \mod n$

$\sigma := y$ with $y^2 \equiv x' \mod n$,

$j(y) = j(x)$,

$h(y) = b$

return σ

y_1, y_2, y_3, y_4: square roots of $x \mod n$

i	$j(y_i)$	$h(y_i)$
1	0	0
2	1	0
3	0	1
4	1	1

$$h(x) = \begin{cases} 1, \text{ if } x > n/2, \\ 0, \text{ otherwise,} \end{cases} \qquad j(x) = \begin{cases} 1, \text{ if } x \in \overline{\mathbb{J}}_n, \\ 0, \text{ otherwise.} \end{cases}$$

Unique Scheme

$\mathsf{Sign}(\mathsf{sk}, m)$

$b := 0$

$x := \mathsf{H}(m)$

$x' := x \cdot 2^{j(x)} \mod n$

if $x' \notin \mathbb{QR}_n$ **do**

$b := 1$

$x' := x' \cdot s \mod n$

$\sigma := y$ with $y^2 \equiv x' \mod n$,

$j(y) = j(x)$,

$h(y) = b$

return σ

$\mathsf{Vrfy}(\mathsf{vk} = (n, s), (m, \sigma))$

if $\sigma \notin \{1, \ldots, n-1\}$

return 0

else

return $\mathsf{H}(m) = \sigma^2 \cdot 2^{-j(\sigma)} \cdot s^{-h(\sigma)} \mod n$

Unique Scheme

Due to the results of Seurin (PKC' 14) and Kakvi, Kiltz (EC' 12):

Theorem: If the Quadratic Residuosity assumption is $(t_{QR}, \varepsilon_{QR})$-hard, then for any q_h, q_s the unique signature scheme Π_u is $(t, q_h, q_s, \varepsilon)$-existentially unforgeable under chosen-message attacks in the random oracle model with

$$t = t_{QR} - q_h \cdot \mathcal{O}(\kappa^2) \quad \text{and} \quad \varepsilon = 3 \cdot \varepsilon_{QR}.$$

Efficiency

- Comparable to Rabin-Williams family
- Unique scheme requires computation of a Jacobi symbol

Efficiency

- Comparable to Rabin-Williams family
- Unique scheme requires computation of a Jacobi symbol
- Deterministic scheme for even faster verification
  (*does not* require computation of the Jacobi symbol)

Deterministic Scheme

$\Pi_d = (\mathsf{KGen}', \mathsf{Sign}', \mathsf{Vrfy}')$, where KGen' and Sign' are the same as KGen and Sign in Π_u

$\mathsf{Vrfy}'(\mathsf{vk} = (n, s), (m, \sigma))$

if $\sigma \notin \{1, \ldots, n-1\}$
  return 0
else return
  $(\mathsf{H}(m) = \sigma^2 \cdot s^{-h(\sigma)} \mod n) \vee (\mathsf{H}(m) = \sigma^2 \cdot s^{-h(\sigma)} \cdot 2^{-1} \mod n)$

Thank you!

Katharina Fech

Friedrich-Alexander-Universität Erlangen-Nürnberg
Nuremberg Campus of Technology
Chair of Applied Cryptography
Fürther Straße 246C
90429 Nürnberg, Germany

katharina.fech@fau.de