An improved threshold ring signature scheme based on error correcting codes

Pierre-Louis Cayrel, Sidi Mohamed El Yousfi Alaoui, Gerhrad Hoffmann, and Pascal Véron

Center of Advanced Security Research Darmstadt, Germany

WAIFI 2012, Bochum

Motivation

- Quantum computers will break the most popular public-key cryptosystems (RSA, DSA, ECDSA, . . .) can be attacked in polynomial time using Shor's algorithm.

Motivation

- Quantum computers will break the most popular public-key cryptosystems (RSA, DSA, ECDSA, ...) can be attacked in polynomial time using Shor's algorithm.

- Post-quantum cryptography deals with cryptosystems that are secure against attacks by quantum computers:
  - Hash-based cryptography.
  - Code-based cryptography.
  - Lattice-based cryptography.
  - Multivariate-quadratic-equations cryptography.

Motivation

- Threshold ring signature: subset of ring members cooperatively generate a signature so that the verifier cannot identify the identity of the actual signers.

Motivation

- Threshold ring signature: subset of ring members cooperatively generate a signature so that the verifier cannot identify the identity of the actual signers.

- The first code-based threshold ring signature was proposed by Aguilar et al. in 2008, it is based on the Stern's identification scheme.

Motivation

- Threshold ring signature: subset of ring members cooperatively generate a signature so that the verifier cannot identify the identity of the actual signers.
- The first code-based threshold ring signature was proposed by Aguilar et al. in 2008, it is based on the Stern's identification scheme.
- In 2010, Cayrel et al. proposed the q-SD zero-knowledge identification scheme which has better performance than Stern's one.

Motivation

- Threshold ring signature: subset of ring members cooperatively generate a signature so that the verifier cannot identify the identity of the actual signers.
- The first code-based threshold ring signature was proposed by Aguilar et al. in 2008, it is based on the Stern's identification scheme.
- In 2010, Cayrel et al. proposed the q-SD zero-knowledge identification scheme which has better performance than Stern's one.
- Constructing a code-based threshold ring signature based on the q-SD scheme.

Table of contents

Preliminaries

Linear error-correcting code

(n, k, ω)-code over $\mathbb{F}_q$: A k-dimensional subspace of $\mathbb{F}_q^n$ that allows to correct ω errors (n, k positive integers and q prime power)

Preliminaries

Linear error-correcting code

(n, k, ω)-code over $\mathbb{F}_q$: A k-dimensional subspace of $\mathbb{F}_q^n$ that allows to correct ω errors (n, k positive integers and q prime power)

Hamming weight

The number of non-zero entries: $wt(x) = |\{i : x_i \neq 0\}|$

Preliminaries

Linear error-correcting code

(n, k, ω)-code over $\mathbb{F}_q$: A k-dimensional subspace of $\mathbb{F}_q^n$ that allows to correct ω errors (n, k positive integers and q prime power)

Hamming weight

The number of non-zero entries: $wt(x) = |\{i : x_i \neq 0\}|$

Parity check matrix

A $r \times n$ matrix H that defines a code $\mathcal{C} = \{x \in \mathbb{F}_q^n : Hx^T = 0\}$
$r = (n - k)$ is the co-dimension of $\mathcal{C}$

Security basis

q-ary Syndrome Decoding (qSD) problem

Given : $H \xleftarrow{\$} \mathbb{F}_q^{r \times n}$, $y \xleftarrow{\$} \mathbb{F}_q^r$, and an integer $\omega > 0$

Find : A word $s \in \mathbb{F}_q^n$ of weight ω s.t $Hs^T = y$

Security basis

q-ary Syndrome Decoding (qSD) problem

Given : $H \xleftarrow{\$} \mathbb{F}_q^{r \times n}$, $y \xleftarrow{\$} \mathbb{F}_q^r$, and an integer $\omega > 0$

Find : A word $s \in \mathbb{F}_q^n$ of weight ω s.t $Hs^T = y$

Theorem

The above problem is proven to be NP-complete by Barg.

Security basis

q-ary Syndrome Decoding (qSD) problem

Given : $H \xleftarrow{\$} \mathbb{F}_q^{r \times n}$, $y \xleftarrow{\$} \mathbb{F}_q^r$, and an integer $\omega > 0$

Find : A word $s \in \mathbb{F}_q^n$ of weight ω s.t $Hs^T = y$

Theorem

The above problem is proven to be NP-complete by Barg.

Attack

Best known attack: Information Set Decoding (ISD)

Security basis

q-ary Syndrome Decoding (qSD) problem

Given : $H \xleftarrow{\$} \mathbb{F}_q^{r \times n}$, $y \xleftarrow{\$} \mathbb{F}_q^r$, and an integer $\omega > 0$

Find : A word $s \in \mathbb{F}_q^n$ of weight ω s.t $Hs^T = y$

Theorem

The above problem is proven to be NP-complete by Barg.

Attack

Best known attack: Information Set Decoding (ISD)

Notation

$\mathrm{WF}_{\mathrm{ISD}}$: Workfactor of the Information Set Decoding algorithm

Special transformation

Definition

Let Σ be a permutation of $\{1, \ldots, n\}$ and $\gamma = (\gamma_1, \ldots, \gamma_n) \in \mathbb{F}_q^n$ such that $\forall i, \gamma_i \neq 0$. We define the transformation $\Pi_{\gamma,\Sigma}$ as:

$$\begin{array}{rccc} \Pi_{\gamma,\Sigma} : & \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^n \\ & (v_1, \ldots, v_n) & \mapsto & (\gamma_{\Sigma(1)} v_{\Sigma(1)}, \ldots, \gamma_{\Sigma(n)} v_{\Sigma(n)}) \end{array}$$

Special transformation

Definition

Let Σ be a permutation of $\{1, \ldots, n\}$ and $\gamma = (\gamma_1, \ldots, \gamma_n) \in \mathbb{F}_q^n$ such that $\forall i, \gamma_i \neq 0$. We define the transformation $\Pi_{\gamma,\Sigma}$ as:

$$\begin{array}{rccc} \Pi_{\gamma,\Sigma} : & \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^n \\ & (v_1, \ldots, v_n) & \mapsto & (\gamma_{\Sigma(1)} v_{\Sigma(1)}, \ldots, \gamma_{\Sigma(n)} v_{\Sigma(n)}) \end{array}$$

Remark

$\forall \alpha \in \mathbb{F}_q$, $\forall v \in \mathbb{F}_q^n$

- $\Pi_{\gamma,\Sigma}(\alpha v) = \alpha \Pi_{\gamma,\Sigma}(v)$
- $\mathrm{wt}(\Pi_{\gamma,\Sigma}(v)) = \mathrm{wt}(v)$

q-SD identification scheme

Key generation algorithm

Let κ be the security parameter

Choose n, r, ω, and q such that $\mathrm{WF}_{\mathrm{ISD}}(n, r, \omega, q) \geq 2^{\kappa}$

$H \xleftarrow{\$} \mathbb{F}_q^{r \times n}$

$s \xleftarrow{\$} \mathbb{F}_q^n$, s.t. $\mathrm{wt}(s) = \omega$

$y \leftarrow Hs^T$

Output $(\mathrm{sk}, \mathrm{pk}) = (s, (y, H, \omega))$

Protocol

Prover $\mathcal{P}$		**Verifier** $\mathcal{V}$
$(\mathrm{sk}, \mathrm{pk}) = (s, (y, H, \omega)) \longleftarrow \textsc{KeyGen}$	(h public hash function)	$\mathrm{pk} = (y, H, \omega)$
$u \xleftarrow{\$} \mathbb{F}_q^n, \Sigma \xleftarrow{\$} S_n$		
$\gamma \xleftarrow{\$} \mathbb{F}_q^{n*}$		
$c_1 \leftarrow h\left(\Sigma \|\| \gamma \|\| Hu^T\right)$		
$c_2 \leftarrow h\left(\Pi_{\gamma,\Sigma}(u) \|\| \Pi_{\gamma,\Sigma}(s)\right)$	$\xrightarrow{c_1,\, c_2}$	
	$\xleftarrow{\alpha}$	$\alpha \xleftarrow{\$} \mathbb{F}_q$
$\beta \longleftarrow \Pi_{\gamma,\Sigma}(u + \alpha s)$	$\xrightarrow{\beta}$	
	$\xleftarrow{\text{Challenge } b}$	$b \xrightarrow{\$} \{0, 1\}$
If $b = 0$:	$\xrightarrow{\Sigma,\, \gamma}$	**Check** $c_1 \stackrel{?}{=} h(\Sigma \|\| \gamma \|\| H\Pi_{\gamma,\Sigma}^{-1}(\beta)^T - \alpha y)$
Else:	$\xrightarrow{\Pi_{\gamma,\Sigma}(s)}$	**Check** $c_2 \stackrel{?}{=} h(\beta - \alpha\Pi_{\gamma,\Sigma}(s) \|\| \Pi_{\gamma,\Sigma}(s))$, $\mathrm{wt}(\Pi_{\gamma,\Sigma}(s)) \stackrel{?}{=} \omega$

CASED

q-SD identification scheme

Property

- Five-pass zero-knowledge identification protocol.
- Based on the qSD problem.
- The soundness error is close to $1/2$ for each round.
- 16, 32 rounds for $1/2^{16}, 1/2^{32}$ as impersonation resistance in accord with the norm ISO/IEC-9798-5.
- Better communication complexity.

Improved threshold ring signature scheme

Definitions

- Consider n and N two integers.

Improved threshold ring signature scheme

Definitions

- Consider n and N two integers.
- A constant (n, N)-block permutation Θ is a permutation by block which permutes together N blocks of length n block by block.
- The permutation $(3, 4, 5, 6, 1, 2)$ is a constant $(2, 3)$-block permutation.

Improved threshold ring signature scheme

Definitions

- Consider n and N two integers.
- A constant (n, N)-block permutation Θ is a permutation by block which permutes together N blocks of length n block by block.
- The permutation $(3, 4, 5, 6, 1, 2)$ is a constant $(2, 3)$-block permutation.
- A (n, N)-block permutation is a permutation which permutes also for each block the components of the block.
- The permutation $(6, 5, 4, 3, 2, 1)$ is $(2, 3)$-block permutation.

Improved threshold ring signature scheme

Idea

- Consider a ring with N members $(P_1, P_2, \ldots, P_N)$ (the signers).
- Consider a subgroup of t members which want to sign a message, among them is the particular member L (the leader).
- The t signers perform the q-SD identification protocol with the verifier through L.
  - locally each signer among the t members runs a local q-SD protocol with L.
  - at each round L collects the t answers (or commitments) of the signers, simulates the $N - t$ others, mix them with a block permutation and sends them to V.
  - V runs a global q-SD protocol with L, but with block permutations and a greater weight $t\omega$.

Improved threshold ring signature scheme

Key Generation

Each signer generates a public key H_i associated to a secret key s_i of weight ω such that $H_i s_i^T = 0$.

- Concatenation of the public matrices H_i to create a public matrix H:

$$H = \begin{pmatrix} H_1 & 0 & \cdots & 0 \\ 0 & H_2 & 0 & 0 \\ \vdots & \ddots & H_i & 0 \\ 0 & 0 & \cdots & H_N \end{pmatrix}$$

- The vector $s = (s_1, \ldots, s_N)$ is secret, s is formed of N blocks of length n and of weight ω or 0 and verifies $Hs^T = 0$ with $wt(s) = t\omega$.

Improved threshold ring signature scheme

Generalized q-SD protocol:

- **Commitment Step:**
  - Each signer P_i chooses $u_i \xleftarrow{\$} \mathbb{F}_q^n$, $\Sigma_i \xleftarrow{\$} S_n$, $\gamma_i \xleftarrow{\$} \mathbb{F}_q^{n*}$; $(1 \leq i \leq t)$
  - Each P_i constructs $c_{1,i} \leftarrow h\left(\Sigma_i || \gamma_i || H_i u_i^T\right)$ and $c_{2,i} \leftarrow h\left(\Pi_{\gamma_i,\Sigma_i}(u_i) || \Pi_{\gamma_i,\Sigma_i}(s_i)\right)$ and sends these values to Leader L
  - L fixes the secret keys s_i of the $N-t$ missing signers at 0; $(t+1 \leq i \leq N)$
  - L chooses $N-t$ values $u_i \xleftarrow{\$} \mathbb{F}_q^n$ and $N-t$ permutations $\Sigma_i \xleftarrow{\$} S_n$ and $N-t$ values $\gamma_i \xleftarrow{\$} \mathbb{F}_q^{n*}$; $(t+1 \leq i \leq N)$
  - L chooses a random constant block permutation Θ on N blocks $\{1, 2, \ldots, N\}$ in order to obtain the master commitments $C_1 \leftarrow h(\Theta || c_{1,1} || \ldots || c_{1,N})$ and $C_2 \leftarrow h(\Theta(c_{2,1}, \ldots, c_{2,N}))$
  - L sends C_1 and C_2 to the Verifier V
  - V sends the value $\alpha \xleftarrow{\$} \mathbb{F}_q$ to L who passes it to P_i ; $(1 \leq i \leq t)$
  - P_i computes $\beta_i \longleftarrow \Pi_{\gamma_i,\Sigma_i}(u_i + \alpha s_i)$; $(1 \leq i \leq t)$. L performs the same for the non signers, but with $s_i = 0$; $(t+1 \leq i \leq N)$
  - L sends $\beta' = \Theta(\beta) = \Theta(\beta_1, \cdots, \beta_N) = (\beta'_1, \cdots, \beta'_N)$ to V
- **Challenge Step**
  - V chooses $b \xleftarrow{\$} \{0, 1\}$ and sends it to L who sends it to each signer P_i.

Improved threshold ring signature scheme

Generalized q-SD protocol:

- **Answer Step**
  - Let P_i be one of the signers. The first part of this step is between each signer P_i and the leader L
    - if $b = 0$: P_i sends γ_i and Σ_i to L
    - if $b = 1$: P_i sends $\Pi_{\gamma_i,\Sigma_i}(s_i)$ to L
  - L computes the answer for V:
    - if $b = 0$ L constructs $\rho = \Theta(\Pi_{\gamma_1,\Sigma_1}, \ldots, \Pi_{\gamma_N,\Sigma_N})$ and sends it to V
    - if $b = 1$ L constructs $\rho(s) = \rho(s_1, \ldots, s_N) = (\rho_1(s_1), \ldots, \rho_N(s_N)) = \Theta(\Pi_{\gamma_1,\Sigma_1}(s_1), \ldots, \Pi_{\gamma_N,\Sigma_N}(s_N))$, and sends $\rho(s)$ to V
- **Verification Step**
  - V checks the correctness of master commitments, permutations, and Hamming weight.
    - if $b = 0$ V verifies that C_1 has been honestly calculated and that ρ is a n-permutation on N blocks
    - if $b = 1$ V verifies that C_2 has been honestly calculated and that $\rho(s)$ is formed of N blocks of length n and of weight ω or 0

Transformation to signature

- Via the extending Fiat-Shamir paradigm we transform the generalized q-SD protocol into secure threshold ring signature scheme.

Security

- Unforgeability: generalized q-SD protocol verifies the ZK proof $\Longrightarrow$ the resulting threshold ring signature is unforgeable against adaptively chosen message attacks in the random oracle model.

- Anonymity: the use of a (n, N)-block permutation block hides the identity of the signers.

Improvement

Matrix representations

- Large public key due to completely random matrix.
- Use a structured matrix to reduce storage.

Quasi-Cyclic, Quasi-dyadic Matrices

$H = (I|A) \in \mathbb{F}_q^{r \times n}$

$$A = \begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_r \\ a_r & a_1 & a_2 & \dots & a_{r-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_2 & a_3 & a_4 & \dots & a_1 \end{pmatrix}, \quad A = \begin{pmatrix} a & b & c & d \\ b & a & d & c \\ c & d & a & b \\ d & c & b & a \end{pmatrix}$$

Practical result: TRIS

Aguilar et. al scheme (28 rounds)

Matrix Type	Dim. $[n \times r]$	Weight	Setup $[ms]$	Protocol $[ms]$	Total $[ms]$	Sec
Random	704×352	76	108.539	98.662	207.200	2^{80}
Quasi-dyadic	704×352	76	811.202	474.737	1285.939	2^{80}
Quasi-cyclic	704×352	76	476.796	302.935	779.731	2^{80}

Our scheme (16 rounds)

Matrix Type	Dim. $[n \times r]$	Weight	Setup $[ms]$	Protocol $[ms]$	Total $[ms]$	Sec
Random	144×72	54	32.979	18.499	51.477	2^{80}
Quasi-dyadic	144×72	54	44.331	29.109	73.439	2^{80}
Quasi-cyclic	144×72	54	38.747	26.550	65.298	2^{80}

- $(t, N) = (50, 100)$
- C/C++ implementation with compiler gcc 4.6.2(running Debian 6.0.3)
- Intel(R) Core(TM)2 Duo CPU E8400@3.00GHz

CASED

Practical result: TRSS

Our scheme (80 rounds)

Doc. [*MiB*]	**Sig.** [*MiB*]	**Dim.** [$n \times r$]	**Weight**	**Sig** [*ms*]	**Verif** [*ms*]	**Total** [*ms*]	**Sec**
1	4	144×72	54	544	454	998	2^{80}
10	13	144×72	54	3643	3551	7194	2^{80}
25	28	144×72	54	8803	8700	17503	2^{80}

Comparison with a lattice-based threshold ring signature

For a 111 bit-security, the signature length is 45 Mbytes (lattice) and 4 Mbytes (our scheme).

Conclusion and future work

We presented a secure threshold ring signature scheme based on error-correcting codes with

- shorter signature length, smaller public key size and signature cost compared to Aguilar et al.'s scheme

- Designing other type of signature with special properties based on the q-SD identification protocol (forward signature scheme, $\cdots$)

CASED

Thanks !
Questions ?