

A New Efficient Threshold Ring Signature Scheme based on Coding Theory

Carlos Aguilar, Pierre-Louis Cayrel and **Philippe Gaborit**
XLIM - Limoges University, France

PQCrypto, Cincinatti, 2008

SUMMARY

- Motivation - ring signature
- Coding theory and cryptography
- Code based ring signature: a generalization of Stern scheme
- Conclusion and perspective

MOTIVATION - RING SIGNATURE

Besides the classical signature schemes like RSA, El gamal or their EC adaptation there exist many different type of signatures with interesting properties:

- blind signature
- identity based signature
- undeniable signature
- aggregate signature
- group signature
- ring signature
- ...

all based on number theory. In the PQ Crypto world very few valid signature systems exist and even less variations on signature. Of particular interest in this talk: Ring Signatures.

Group signature: introduced by Chaum and van Heyst in '91

- three different type of actors: signers, verifiers and a group manager,
- many different definition for group signature and different type of properties, in particular:

- permit to any member of a group to sign on behalf of the group anonymously
- a group manager can add member and revoke signature anonymity

Notion of group: in/out notion managed by a group manager,

entering the group = interaction with the manager.

Many applications: electronic voting, e-cash,..

Ring signature: Rivest, Shamir and Tauman, AsiaCrypt '01

Can be viewed as: Group signature with **NO** manager. A group can be formed *ad hoc*: a ring.

- permit to any member of a ring to sign on behalf of the ring anonymously
- the anonymity of the signature cannot be revealed by exterior to the group

Examples: high-ranked officials in the white house, ad-hoc networks...

More formally: 3 algorithms

- **Key-Gen** is a probabilistic polynomial algorithm that takes a security parameter(s) and returns the system, private, and public parameters.
- **Sign** is a probabilistic polynomial algorithm that takes system parameters, a private parameter (private key s_{k_i}), a list of public keys p_{k_1}, \dots, p_{k_N} of the ring, and a message M . The output of this algorithm is a ring signature σ for the message M .
- **Verify** is a deterministic algorithm that takes as input a message M , a ring signature σ , and the public keys of all the members of the corresponding ring, then outputs *True* if the ring signature is valid, or *False* otherwise.

Lot of work besides original definitions:

N number of potential signers:

signature length: $\mathcal{O}(N)$, possible to obtain a fixed length signature (but large), or in $\mathcal{O}(\sqrt{N})$.

Generalization: Threshold ring signature:

Bresson, Stern, Szydlo, **Crypto '02**

In that case: a ring of N potential signers, one wants to prove that t persons among the N have signed the message.

Full anonymity: hard to guess the t signers among the N .

BSS '02: size of signature $2^{\mathcal{O}(t)}$

Liu, Wei, Wong '03: signature length: $\mathcal{O}(N)$, complexity: $\mathcal{O}(N^2)$

CODING THEORY AND CRYPTOGRAPHY

Notation

- Code $C[n, k]$: subspace of $GF(q)^n$ of dimension k
- Weight of an element of $GF(q)^n$: number of non null coordinates
- Minimum weight of code: the minimum weight of non null vectors of the code
- Generator matrix G : a base of the code
- Dual of a code $C^\perp = \{y | x \cdot y = \sum_{i=1}^n x_i \cdot y_i = 0\}$
- H parity check matrix of C , a generator matrix of C^\perp
- $x \in C \leftrightarrow H \cdot x^t = 0$

Hard Problems

Problem:(SD) Syndrome decoding of a random code:

Instance: A $n - k \times n$ random matrix H over $GF(2)$, a non null target vector $y \in GF(2)^{(n-k)}$ and an integer ω .

Question: Is there $x \in GF(2)^n$ of weight $\leq \omega$, s.t. $Hx^t = y^t$?

Proven NP-complete by Berlekamp,McEliece and van Tilborg in 1978.

Problem: (MD) Minimum Distance:

Instance: A binary $n - k \times n$ matrix H and an integer $\omega > 0$.

Question: Is there a non zero $x \in GF(2)^n$ of weight $\leq \omega$, s.t. $Hx^t = 0$?

proven NP-complete by Vardy in 1997.

Generalization to quasi-cyclic codes Berger,Cayrel,G.,Otmani '08

Decoding a random code

Best known attacks are exponential in n the length of the code.

Attacks based on information set decoding problem:

Lee-Brickell '88, Stern '89, Leon '90, Chabaud '94,
Canteaut-Chabaud '98

For decoding t errors for a $[n, k]$ code, term in $\frac{\binom{n}{t}}{\binom{n-k}{t}}$.

for $k = n/2$, attacks in $\approx \mathcal{O}(n)2^{\frac{n}{20}}$.

Main cryptosystems

Encryption: McEliece '78, Niederreiter '86

- very efficient but large public key (quasi-cyclic codes ??)

Signature: Courtois, Finiasz, Sendrier '01

- small signature (80 bits) but very large public key (1 Mo) and rather time consuming.

- identity-based signature: Cayrel, Gaborit, Girault '07

Hash: Augot, Finiasz, Sendrier '05

PRNG: Gaborit, Laraudoux, Sendrier '07

Authentication: Stern SD protocol '93,

- Fiat-Shamir like protocol with probability of cheating $2/3$, not small public key, can be used in signature via the Fiat-Shamir paradigm

Stern authentication protocol

Zero-knowledge protocol with cheating probability $2/3$, Crypto '93

H a $(n - k) \times n$ binary matrix

Secret key: H and x a word of length n and weight w such that $w < d_{VG}(n)$.

Public key : H and s (syndrom): $s = Hx^T$

Stern Protocol:

1. P (prover) chooses randomly y of length n and a permutation σ on $\{1, \dots, n\}$. Send to V (verifier) : c_1, c_2 and c_3 such that :
 $c_1 = \langle \sigma, Hy^T \rangle$; $c_2 = \langle y; \sigma \rangle$; $c_3 = \langle (y + x).\sigma \rangle$ for $\langle arg_1, arg_2 \rangle$ the action of a hash function on the concatenation of arg_1 and arg_2 , and $arg.\sigma$ the image of arg with σ .

2. V sends to P a challenge b in $\{0, 1, 2\}$.

3. P receives b , then Three possibilities occur:

- if $b = 0$: P reveals y and σ ,
- if $b = 1$: P reveals $(y + x)$ and σ ,
- if $b = 2$: P reveals $y.\sigma$ and $x.\sigma$.

4. Three possibilities occur :

- if $b = 0$: V checks that c_1 and c_2 received are correct.
- if $b = 1$: V checks that c_1 and c_3 received are correct.

One can remark that: $Hy^T = H(y + x)^T + s$

- if $b = 2$: V checks that c_2 and c_3 received are correct.

5. Repeat steps 1, 2, 3 and 4 until the adequate security level is reached.

Zero-knowledge protocol with cheating probability at most $2/3$

Security: Random matrix:

Theoretical

- Satisfies Gilbert-Varshamov bound (existence)
- Almost all random codes are on GV (parameters)
- NP-complete problem

Practical security

Evaluation depending on the parameters of the code (d_{GV}) with best known attack (Information Set Decoding - Canteaut/Chabaud)

Advantage: no masking!

For a $[2n, n, d]$ code:

Size of keys: public matrix n^2 , x : $2n$, s : n .

Complexity: $2n^2 \times$ nb de rounds

Parameters: $n \geq 400$, H : > 200000 bits!

Improvement and variation on the protocol

Gaborit, Girault ISIT '07

Idea: use quasi-cyclic matrices, in particular double-circulant matrices

Take $H = (I|A)$ for A a random circulant matrix:

$$A = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ a_n & a_1 & a_2 & \cdots & a_{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_2 & a_3 & a_4 & \cdots & a_1 \end{pmatrix}.$$

→ new size of public key: $2n$

Security: *a priori* the same, except to a constant in n , NP-complete, GV -bound on the average (even better!).

Implementation and protection against SCA: Cayrel, Gaborit, Prouff: Cardis '08.

Variation on the scheme: MD problem

Take syndrom $= 0$, double-circulant version:

Take random $a(a_1, \dots, a_n)$ and $b(b_1, \dots, b_n)$ such that $Weight(a, b) = w$ construct $G = [A|B]$ a double circulant matrix, then $G' = [I|A^{-1}B]$ and take $H = [(A^{-1}B)^t|I]$.

One gets as secret $x = (a, b)$ of weight w with $H.x^t = 0$.

→ permits to get a 'symmetric' syndrom, so that the protocol only depends on the matrix H and not on the syndrom.

CODE BASED RING SIGNATURE: A GENERALIZATION OF STERN SCHEME

High level overview: Consider a ring with N members (P_1, P_2, \dots, P_n) (the provers), - same weight ω for their secrets, and same parameters for matrices. We consider a subgroup of t members which want to sign a message, a particular member L (the leader) among the signers and a verifier V .

Basic idea: The t provers perform globally a Stern authentication protocol with the verifier V through L (man-in-the-middle)

- locally each prover among the t runs a local Stern protocol with L
- at each round L gathers the t answers (or commitments) of the provers, simulates the $N - t$ others, mix them with a block permutation and sends them to V , conversely he sends the challenges from V to the provers.
- V runs a global Stern protocol with L (it can be seen as a classical Stern protocol but in a tensor-product way), but with block permutations and a greater weight: $t\omega$

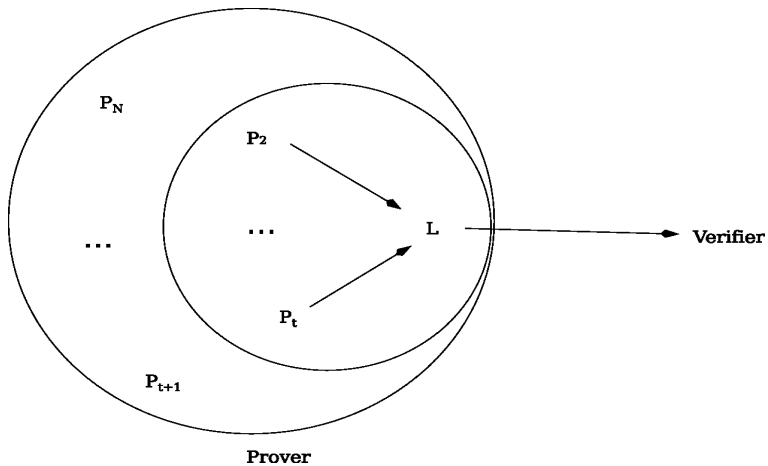


Figure: Global view

How can this work ? Each signer has a public key H_i associated to a secret s_i of weight ω with null syndrome (ie. s_i is in the code). The global protocol works because of the three following properties:

- **Concatenation of the public matrices H_i to create a large matrix H for the protocol between L and V :**

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

The weight ω and the H_i are public, the s_i such that $H_i \cdot s_i^t = 0$ are secret.
→ the large matrix H assures an interaction (even passive) between all the members of the ring

- **anonymity between the provers**

The fact that all the syndromes are taken all equal (to zero) assures a 'symmetry' between the potential provers and avoid the recovery of a particular prover through its syndrome since they are all the same.

→ same syndrome (0) limits anonymity to the use of a given matrix

- **Use of n -block permutations Π to mix the local permutations used in the local Stern protocols**

When L receives the n -length permutations from the P_i it takes them in the order $1, 2, \dots, N$ and apply on it a random permutation on the N blocks of size n .

→ block permutations permits to assure full anonymity by masking which matrices are used to compute the syndrome

1[Commitment Step]

- Each of the signers chooses $y_i \in F_2^n$ randomly and a random permutation σ_i of $\{1, 2, \dots, n\}$ and sends to L the commitments $c_{1,i}$, $c_{2,i}$ and $c_{3,i}$ such that :

$$c_{1,i} = h(\sigma_i | H_i y_i^t); \quad c_{2,i} = h(\sigma_i(y_i)); \quad c_{3,i} = h(\sigma_i(y_i \oplus s_i))$$

where $h(a_1 | \dots | a_j)$ denotes the hash of the concatenation of the sequence formed by a_1, \dots, a_j .

- L chooses $N - t$ random $y_i \in F_2^n$ and $N - t$ random permutations σ_i of $\{1, 2, \dots, n\}$
- L fixes the secret s_i of the $N - t$ missing users at 0 and computes the $N - t$ corresponding commitments by choosing random y_i and σ_i ($t + 1 \leq i \leq N$).
- L chooses a random constant n -block permutation Σ on N blocks $\{1, \dots, N\}$ in order to obtain the *master commitments*:

$$C_1 = h(\Sigma | c_{1,1} | \dots | c_{1,N}), \quad C_2 = h(\Sigma(c_{2,1}, \dots, c_{2,N})), \quad C_3 = h(\Sigma(c_{3,1}, \dots, c_{3,N}))$$

- L sends C_1 , C_2 and C_3 to V .

2 [Challenge Step] V sends a challenge $b \in \{0, 1, 2\}$ to L which sends b to the t signers.

3 [Answer Step] Let P_i be one of the t signers. The first part of the step is between each signer and L .

- Three possibilities :
 - if $b = 0$: P_i reveals y_i and σ_i .
 - if $b = 1$: P_i reveals $(y_i \oplus s_i)$ (denoted by $(y \oplus s)_i$) and σ_i .
 - if $b = 2$: P_i reveals $\sigma_i(y_i)$ (denoted by $(\sigma(y))_i$) and $\sigma_i(s_i)$ (denoted by $(\sigma(s))_i$).
- L simulates the $N - t$ others Stern's protocol with $s_i = 0$ and $t + 1 \leq i \leq N$.
- L computes the answer for V (and sends it) :
 - if $b = 0$: L constructs $y = (y_1, \dots, y_N)$ and $\Pi = \Sigma \circ \sigma$ (for $\sigma = (\sigma_1, \dots, \sigma_N)$) and reveals y and Π .
 - if $b = 1$: L constructs $y \oplus s = ((y \oplus s)_1, \dots, (y \oplus s)_N)$ and reveals $y \oplus s$ and Π .
 - if $b = 2$: L constructs $\Pi(y)$ and $\Pi(s)$ reveals them.

4[Verification Step] Three possibilities :

- if $b = 0$: V verifies that $\Pi(s)$ is a n -block permutation and that C_1, C_2 have been honestly calculated.
- if $b = 1$: V verifies that $\Pi(s)$ is a n -block permutation and that C_1, C_3 have been honestly calculated.
- if $b = 2$: V verifies that C_2, C_3 have been honestly calculated, and that the weight of $\Pi(s)$ is $t\omega$ and that $\Pi(s)$ is formed of N blocks of length n and of weight ω or 0.

5 Iterate the steps 1,2,3,4 until the expected security level is reached.

From the authentication protocol one can deduce a signature scheme via the Fiat-Shamir assumption.

Comments: $t = 1$ costs the same as $t = N/2$!

→ not too much interesting for $t = 1$ (except $N = 2$)

Security of the protocol:

Lemma

Finding a vector v of length nN such that the global weight of v is $t\omega$, the weight of v for each of the N blocks of length n is 0 or ω and such that v has a null syndrome for H , is hard under the MD assumption.

Theorem

Our scheme is a proof of knowledge, with a probability of cheating $2/3$, that the group of signers P knows a vector v of length nN such that the global weight of v is $t\omega$, the weight of v for each of the N blocks of length n is 0 or ω and such that v has a null syndrome for H . The scheme is secure under the MD assumption in the random oracle model.

Parameters

- Size of key: $\mathcal{O}(N) : \approx 400N$
- Size of signature: $\mathcal{O}(N) : 140.000 \times N$ bits
- Complexity: $N \times$ (the time of one signature)

Compares very well to other systems, except for the length of the signature $2Mo$ for $N = 100$.

Perspective and future work

In fact the approach can be generalized to linear algebra schemes where the secret satisfies $Ax^t = 0$ for A a matrix.

→ generalization to PKP (Shamir '89) , CLE ?, PPP ?

→ journal version: Aguilar, Cayrel, G., Laguillaumie

Open questions

- Better signature scheme ??
- Efficient group signature based on coding theory
- Other type of variation on signature (blind ?)