On digital signatures based on group actions: QROM security and ring signatures

Markus Bläser[1], Zhili Chen[2], Dung Hoang Duong[3], Antoine Joux[4], Tuong Nguyen[3], Thomas Plantard[5] Youming Qiao[2], Willy Susilo[3], **Gang Tang**[2,6]

[1]Saarland University
[2]University of Technology Sydney
[3]University of Wollongong
[4]CISPA
[5]Nokia Bell Labs
[6] University of Birmingham

13 Jun, 2024

Contents

Gang Tang |
[1]Saarland University [2]University of Technology Sydney [3]University of Wollongong [4]CISPA [5]Nokia Bell Labs [6] University of Birmingham |

Contents

Our results

Our contributions can be classified into two sets

- GMW-FS design based on abstract group actions.
  - distill properties for group actions to be secure in the quantum random oracle model (QROM).
  - the ring signature construction of Beullens-Katsumata-Pintore (Asiacrypt'20) with abstract group actions.
- based on concrete setting: alternating trilinear form equivalence (ATFE).
  - demonstrates its QROM security.
  - implements the ring signature scheme.

Contents

Group action and notions

Definition (Group action)

A group G acts on a set X if there exists a map $\star : G \times X \to X$ such that:

- identity: let id be the identity element of G, then $\forall x \in X,\ \mathrm{id} \star x = x$.
- compatibility: $\forall g, h \in G, x \in X, gh \star x = g \star (h \star x)$.

Definition (Orbit)

For $x \in X$, the *orbit* of x is $\mathcal{O}_x = \{y \in X \mid \exists g \in G, y = g \star x\}$.

Definition (Stabilizer group)

For $x \in X$, the *stabilizer group* under $\star$ is $\mathrm{Stab}(x) = \{g \in G \mid g \star x = x\}$.
An element in $\mathrm{Stab}(x)$ is called an automorphism of x.

By the orbit-stabilizer theorem, $|\mathcal{O}_x| \cdot |\mathrm{Stab}(x)| = |G|$.

Group actions and notions

Definition (Group action - stabilizer problem)

Given an element $x \leftarrow\!\!\$\, X$, the problem asks to find some $g \in G, g \neq \mathrm{id}$ such that $g \star x = x$.

Definition (One-way assumption)

For $x \leftarrow\!\!\$\, X, y \leftarrow\!\!\$\, \mathcal{O}(x)$, there is no probabilistic or quantum polynomial-time algorithm that returns $g \in G$ such that $g \star x = y$.

Definition (Pseudorandom assumption)

There is no probabilistic or quantum polynomial-time algorithm that can distinguish the following two distributions with nonnegligible probability:

- The random distribution: $(x, y) \in X \times X$, where $x, y \leftarrow\!\!\$\, X$. The pseudorandom distribution: $(x, y) \in X \times X, x \leftarrow\!\!\$\, X, y \leftarrow\!\!\$\, \mathcal{O}(x)$.

Contents

The GMW-FS digital signature design

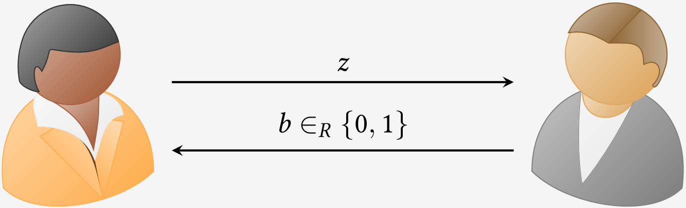
- It has a clear, 2-step, structure
  - Identification scheme based on Goldreich-Micali-Wigderson (J. ACM'91) zero-knowledge protocol for group actions.
  - Use Fiat-Shamir transformation (Crypto'86) to turn the above ID scheme to a digital signature.

GMW zero-knowledge protocol for group actions

- Given two set elements x and y as public key, let g be a group element as secret key such that $g \star x = y$.
- Alice samples a random group element h which sends x to $z = h \star x$.

GMW zero-knowledge protocol for group actions

- Given two set elements x and y as public key, let g be a group element as secret key such that $g \star x = y$.
- Alice samples a random group element h which sends x to $z = h \star x$.



Alice: x, y Bob: x, y

- If $b = 0$, Alice sends $r := h$ to Bob; Otherwise sends $r := hg^{-1}$.
- If $b = 0$, Bob checks whether $r \star x = z$; Otherwise checks $r \star y = z$.

Step 2: from ID scheme to digital signature

- Fiat and Shamir proposed a method that takes an identification scheme and turns it to a digital signature.
- Key idea: use a hash function to simulate the interaction process.

Step 2: from ID scheme to digital signature

- Fiat and Shamir proposed a method that takes an identification scheme and turns it to a digital signature.
- Key idea: use a hash function to simulate the interaction process.
- Security proved in:
  - The Random Oracle Model (Pointcheval-Stern, 1996).
  - The Quantum Random Oracle Model (Don-Fehr-Majenz-Schaffner, Liu-Zhandry, 2019).

Some group actions based PQC candidates

- NIST call for additional PQ signature: MEDS, LESS, ALTEQ.
- MEDS: matrix code equivalence.
- LESS: linear code equivalence.
- ALTEQ: alternating trilinear form equivalence.
- Matrix code equivalence is polynomially equivalent to alternating trilinear form equivalence and linear code equivalence can be reduced to these two problems [Grochow-Qiao, Growchow-Qiao-Tang].
- Group actions here are not transitive.

Contents

Security in the QROM

Definition (Perfect unique response)

A Σ-protocol has *perfect unique response*, if there is no two valid transcripts (a, c, r) and (a, c, r'), where $r \neq r'$.

Definition (Computationally unique response)

A Σ-protocol has *computationally unique response*, if any poly-time quantum adversary produces two valid transcripts (a, c, r) and (a, c, r') with negligible probability, where $r \neq r'$.

- It's straightforward to give a security proof in QROM for group action + GMW +FS signatures: assume perfect unique response and one-wayness.
- Tight security proof [Kaafarani-Katsumata-Pintore, PKC'20]: assume computationally unique response and pseudorandom property.

Security in the QROM

Lemma (Perfect unique response)

A group action based GMW protocol supports perfect unique response if and only if the stabilizer group is trivial.

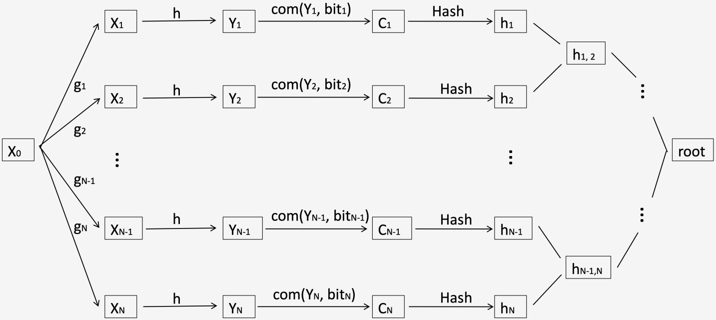
Lemma (Computationally unique response)

A group action based GMW protocol supports computationally unique response if and only if no poly-time quantum algorithm can solve the stabilizer problem.

Ring signature

The Beullens-Katsumata-Pintore design

- statement: $X_0, \dots, X_N \in X$, witness: $g_1, \dots, g_N \in G$, where $X_I = g_I \star X_0$ for $I \in \{1, \dots, N\}$.



- If challenge 0, respond $\mathsf{rsp} = (hg_I, \mathsf{path}, \mathsf{bit}_I)$, otherwise $\mathsf{rsp} = (h, \mathsf{bit}_1, \dots, \mathsf{bit}_N)$

Contents

A candidate: Alternating Trilinear Form Equivalence

- Let $\mathrm{GL}(n, \mathbb{F}_q)$ be the general linear group consisting of $n \times n$ invertible matrices over $\mathbb{F}_q$
- $\phi : \mathbb{F}_q^n \times \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$ is trilinear if it is linear in all the three arguments.
- We say that a trilinear form $\phi : \mathbb{F}_q^n \times \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$ is alternating, if whenever two arguments of ϕ are equal, ϕ evaluates to zero.
- A natural group action of $A \in \mathrm{GL}(n, \mathbb{F}_q)$ on the alternating trilinear form ϕ sends $\phi(u, v, w)$ to $A \star \phi = \phi(A(u), A(v), A(w))$.

A candidate: Alternating Trilinear Form Equivalence

- Let $\mathrm{GL}(n, \mathbb{F}_q)$ be the general linear group consisting of $n \times n$ invertible matrices over $\mathbb{F}_q$
- $\phi : \mathbb{F}_q^n \times \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$ is trilinear if it is linear in all the three arguments.
- We say that a trilinear form $\phi : \mathbb{F}_q^n \times \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$ is alternating, if whenever two arguments of ϕ are equal, ϕ evaluates to zero.
- A natural group action of $A \in \mathrm{GL}(n, \mathbb{F}_q)$ on the alternating trilinear form ϕ sends $\phi(u, v, w)$ to $A \star \phi = \phi(A(u), A(v), A(w))$.

Definition (Alternating Trilinear Form Equivalence (ATFE) problem)

Given two alternating trilinear forms ϕ and ψ, the problem asks whether there exists $A \in \mathrm{GL}(n, \mathbb{F}_q)$ such that $\phi = A \star \psi$.

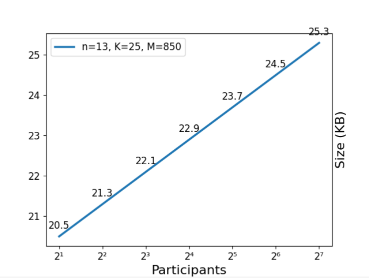
The QROM security of the ATFE-GMW-FS scheme

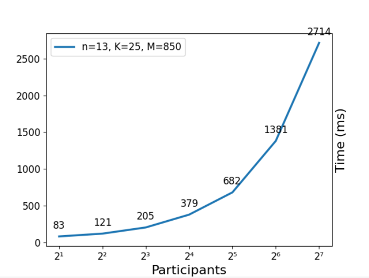
To decide whether the stabilizer group is trivial or not is a difficult algorithmic problem.

- Let A and B be two n by n variable matrices. set up a system of polynomial equations expressing the following:
  - $\phi(A(u), A(v), A(w)) = \phi(u, v, w)$ and $\phi(u, v, w) = \phi(B(u), B(v), B(w))$.
  - $\phi(A(u), v, w) = \phi(u, B(v), B(w))$ and $\phi(A(u), A(v), w) = \phi(u, v, B(w))$.
  - $AB = I$ and $BA = I$.

  Guess one row for A, and use the Gröbner basis algorithm. This algorithm running in time $q^n \cdot \text{poly}(n, \log q)$. we made progress by running experiments for small parameters.
- For $q = 2$ and $n = 10, 11$, all 100 samples return trivial stabilizer groups.
- For $q = 3$ and $n = 10, 11$, all 10 samples return trivial stabilizer groups.

Performance of the ring signatures





Parameters				Size in Bytes				
				R				
n	q	M	K	2^1	2^3	2^6	2^{12}	2^{21}
13	$2^{32}-5$	850	25	20.5	22.1	24.5	29.3	36.5

Table: The signature size (KB) of the ring signature.

Open questions

- Our ring signature obtained from OR-Sigma protocol is proven securely only in ROM. As far as we are aware, whether it is secure in QROM is still an open problem.
- Rigorous proof for trivial stabilizer group.

Thank you for your attention.

Questions please?