ALTEQ: Digital Signatures from Alternating Trilinear Form Equivalence

Markus Bläser[1], Dung Hoang Duong[2], Anand Kumar Narayanan[3], Thomas Plantard[4] Youming Qiao[5], Arnaud Sipasseuth[6], **Gang Tang**[5]

[1]Saarland University
[2]University of Wollongong
[3]SandboxAQ
[4]Bell Labs
[5]University of Technology Sydney
[6]KDDI Research

7 Sep, 2023

Alternating Trilinear Form

- 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 $\phi \circ A = \phi(A^t(u), A^t(v), A^t(w))$.

Alternating Trilinear Form

- 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 $\phi \circ A = \phi(A^t(u), A^t(v), A^t(w))$.

Definition (Alternating Trilinear Form Equivalence (ATFE))

Given two alternating trilinear forms ϕ and ψ, whether there exists $A \in \mathrm{GL}(n, \mathbb{F}_q)$ such that $\phi = \psi \circ A$, and computes one such A if it exists.

The complexity class TI-complete

- Recently, [Grochow-Qiao] define a new complexity class TI-complete, consisting of problems that are polynomial-time equivalent to TensorIso.
- Alternating Trilinear Form Equivalence (ATFE) problem is TI-complete [Grochow-Qiao-Tang].

The complexity class TI-complete

- Recently, [Grochow-Qiao] define a new complexity class TI-complete, consisting of problems that are polynomial-time equivalent to TensorIso.
- Alternating Trilinear Form Equivalence (ATFE) problem is TI-complete [Grochow-Qiao-Tang].
- More, Matrix Code Equivalence problem is TI-complete and Linear Code Monomial Equivalence can be reduced to ATFE [Grochow-Qiao, Growchow-Qiao-Tang].
  - Based on these two problems, two signature schemes are proposed as the NIST candidates: MEDS and LESS.
- Interestingly,these problems are of particular relevance!

Digital signature based on ATFE

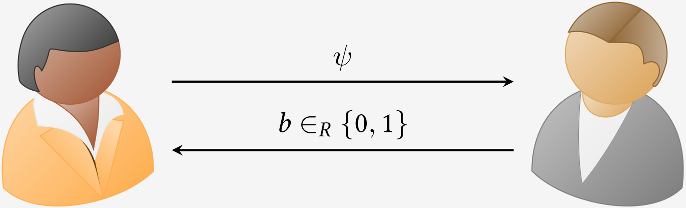
- It has a clear, 2-step, structure
  - Identification scheme based on Goldreich-Micali-Wigderson (J. ACM'91) zero-knowledge protocol.
  - Use Fiat-Shamir transformation (Crypto'86) to turn the above ID scheme to a digital signature.

GMW zero-knowledge protocol for ATFE

- Given two ATFs ϕ_0 and ϕ_1 as public key, let A be an equivalence as secret key such that $\phi_0 \circ A = \phi_1$.
- Alice generates a random equivalence B which sends ϕ_0 to ψ.

GMW zero-knowledge protocol for ATFE

- Given two ATFs ϕ_0 and ϕ_1 as public key, let A be an equivalence as secret key such that $\phi_0 \circ A = \phi_1$.
- Alice generates a random equivalence B which sends ϕ_0 to ψ.



Alice: ϕ_0, ϕ_1

Bob: ϕ_0, ϕ_1

- If $b = 0$, Alice sends $r := B$ to Bob; Otherwise sends $r := A^{-1}B$.
- If $b = 0$, Bob checks whether $\phi_0 \circ r = \psi$; Otherwise checks $\phi_1 \circ r = \psi$.

Digital signature based on ATFE

- It's well-known GMW ZK protocol is complete, 2-special sound and HVZK.

Digital signature based on ATFE

- It's well-known GMW ZK protocol is complete, 2-special sound and HVZK.
- Reduce the soundness error by $r = \lambda$ repetitions.
- Optimization by the following method:
  - Larger challenge space
    - Public key include C ATFs instead of 2 ATFs, then reduce soundness error to $1/C$.
  - Unbalanced challange space
    - Respond a seed instead of a matrix for the fixed positions.

Digital signature based on ATFE

- It's well-known GMW ZK protocol is complete, 2-special sound and HVZK.
- Reduce the soundness error by $r = \lambda$ repetitions.
- Optimization by the following method:
  - Larger challenge space
    - Public key include C ATFs instead of 2 ATFs, then reduce soundness error to $1/C$.
  - Unbalanced challange space
    - Respond a seed instead of a matrix for the fixed positions.
- Apply Fiat-Shamir transformation: use a hash function to simulate the interaction process.

Algorithms and complexity of ATFE problem

- The direct Gröbner basis attack
- There are there modellings as follows:

Algorithms and complexity of ATFE problem

- The direct Gröbner basis attack
- There are there modellings as follows:
  - The direct cubic modelling.
    $\phi_2(u, v, w) = \phi_1(A^t(u), A^t(v), A^t(w))$

Algorithms and complexity of ATFE problem

- The direct Gröbner basis attack
- There are there modellings as follows:
  - The direct cubic modelling.
    $\phi_2(u, v, w) = \phi_1(A^t(u), A^t(v), A^t(w))$
  - The quadratic with inverse modelling.
    $AB = BA = I_n$
    $\phi_2(u, v, B^t(w)) = \phi_1(A^t(u), A^t(v), w)$
    $\phi_2(u, B^t(v), B^t(w)) = \phi_1(A^t(u), v, w)$

Algorithms and complexity of ATFE problem

- The direct Gröbner basis attack
- There are there modellings as follows:
  - The direct cubic modelling.
    $\phi_2(u, v, w) = \phi_1(A^t(u), A^t(v), A^t(w))$
  - The quadratic with inverse modelling.
    $AB = BA = I_n$
    $\phi_2(u, v, B^t(w)) = \phi_1(A^t(u), A^t(v), w)$
    $\phi_2(u, B^t(v), B^t(w)) = \phi_1(A^t(u), v, w)$
  - The quadratic dual modelling [Ran-Samardjiska-Trimoska].
    - Let $(X_1, \ldots, X_n)$ and $(Y_1, \ldots, Y_n)$ represent the ATF ϕ_1 and ϕ_2 respectively, where X_i, Y_i are n by n matrices.
    - Let $l = \binom{n}{2} - n$ and $B_1, \ldots, B_l$ be a basis of linear space $\{D \in \Lambda(n, q) \mid \mathrm{Tr}(Y_i D^t) = 0\}$.
    - For $i \in [n], j \in [l]$, set $\mathrm{Tr}(A^t X_i A B_j^t) = 0$.
    - Add some cubic equations to remove invalid solutions.

Algorithms and complexity of ATFE problem

- The direct Gröbner basis attack
- There are there modellings as follows:
  - The direct cubic modelling.
    $\phi_2(u, v, w) = \phi_1(A^t(u), A^t(v), A^t(w))$
  - The quadratic with inverse modelling.
    $AB = BA = I_n$
    $\phi_2(u, v, B^t(w)) = \phi_1(A^t(u), A^t(v), w)$
    $\phi_2(u, B^t(v), B^t(w)) = \phi_1(A^t(u), v, w)$
  - The quadratic dual modelling [Ran-Samardjiska-Trimoska].
    - Let $(X_1, \ldots, X_n)$ and $(Y_1, \ldots, Y_n)$ represent the ATF ϕ_1 and ϕ_2 respectively, where X_i, Y_i are n by n matrices.
    - Let $l = \binom{n}{2} - n$ and $B_1, \ldots, B_l$ be a basis of linear space $\{D \in \Lambda(n, q) \mid \mathrm{Tr}(Y_i D^t) = 0\}$.
    - For $i \in [n], j \in [l]$, set $\mathrm{Tr}(A^t X_i A B_j^t) = 0$.
    - Add some cubic equations to remove invalid solutions.
    - This modelling is interesting, but based on an assumption which we are still working on understanding.

Algorithms and complexity of ATFE problem

- The graph-theoretic algorithms
- $\mathbf{a} \in \mathbb{F}_q^n$ be a vertex. $(\mathbf{a}, \mathbf{b})$ be a edge iff $\phi_{\mathbf{a},\mathbf{b}} = \phi(\mathbf{a}, \mathbf{b}, w) = 0$.

Algorithms and complexity of ATFE problem

- The graph-theoretic algorithms
- $\mathbf{a} \in \mathbb{F}_q^n$ be a vertex. $(\mathbf{a}, \mathbf{b})$ be a edge iff $\phi_{\mathbf{a},\mathbf{b}} = \phi(\mathbf{a}, \mathbf{b}, w) = 0$.
  - $O(q^{2/3n})$ by brute force sampling and then find collision.[Bouillaguet-Fouque-Véber].
  - $O(q^k)$ by graph walking for sampling and then find collision, when n is odd $k = n - 7$ otherwise $k = n - 4$ [Beullens].
  - $O(q^{k/2})$ by graph walking or Min-Rank for sampling and then birthday paradox [Narayanan-Qiao-Tang].

Parameter Choices

- λ denotes the security parameter.
- r denotes the number of round.
- C denotes the number of alternating trilinear forms in public key.
- K is the parameter from unbalanced challenge.
- Choose n by the direct Gröbner Basis attack.
- Choose q by the graph-theoretic algorithm.
- $\text{PubKeySize} = (C \cdot \binom{n}{3} \cdot \lceil \log_2(q) \rceil + \lambda)/8.$
- $\text{PriKeySize} = \lambda/8.$
- $\text{SigSize} = ((r - K + 2) \cdot \lambda + K \cdot n^2 \cdot \lceil \log_2(q) \rceil)/8.$

Benchmark

NIST Cat.	n	q	r	K	C	PK(KB)	Sig(KB)
1	13	$2^{32}-5$	84	22	7	8.0	15.9
3	20	$2^{32}-5$	201	28	7	31.9	49.0
5	25	$2^{32}-5$	119	48	8	73.67	122.3

Table: Key and Signature Sizes for Balanced-ALTEQ

NIST Cat.	n	q	r	K	C	PK(KB)	Sig(KB)
1	13	$2^{32}-5$	16	14	458	52.4	9.5
3	20	$2^{32}-5$	39	20	229	104.4	32.5
5	25	$2^{32}-5$	67	25	227	208.8	63.9

Table: Key and Signature Sizes for ShortSig-ALTEQ

Benchmark

- We test our code on a laptop with the following configurations:
  - Processor: 12th Gen Intel(R) Core(TM) i7-1270P, 2.2GHz, 12 cores, 18MB L3 Cache.
- Balanced, Cat. 1, Keygen:0.39 Mcycles, Sign: 2.8 Mcycles, Verify: 4.2 Mcycles.
- ShortSig, Cat. 1, Keygen:26.3 Mcycles, Sign: 0.73 Mcycles, Verify: 1.77 Mcycles.

Benchmark

- We test our code on a laptop with the following configurations:
  - Processor: 12th Gen Intel(R) Core(TM) i7-1270P, 2.2GHz, 12 cores, 18MB L3 Cache.
- Balanced, Cat. 1, Keygen:0.39 Mcycles, Sign: 2.8 Mcycles, Verify: 4.2 Mcycles.
- ShortSig, Cat. 1, Keygen:26.3 Mcycles, Sign: 0.73 Mcycles, Verify: 1.77 Mcycles.
- There is ample room for improvement in our implementation:
  - This or Next week (for verification time): about 2x speed up (for Balanced) and 4x speed-up (for ShortSig) of NIST Cat. 1 parameter set.
  - Next step: implement 64-bit arithmetic, AVX512...

Thank you for your attention.

Questions please?