A new Post-Quantum Signature from Alternating Trilinear Forms

Giuseppe D'Alconzo

Commutative algebra applied to coding theory, cryptography and algebraic combinatorics

April 27, 2022

Contents

Post-quantum Digital Signatures

Current situation for the NIST's post quantum call for signatures:

	Signature	*Assumption*
Fin.	CRYSTALS-DILITHIUM	Lattices (MLWE)
	FALCON	Lattices (NTRU)
	Rainbow*	Multivariate
Alt.	SPHINCS+	Hash functions
	GeMSS	Multivariate
	Picnic	MPC/NIZK/Symmetric prim.

*Broken for lower levels of security.

The need for other assumptions

- Rainbow is “broken”.

> **Breaking Rainbow Takes a Weekend on a Laptop**
> Ward Beullens
> Concretely, given a Rainbow public key for the SL 1 parameters of the second-round submission, our attack returns the corresponding secret key after on average 53 hours (one weekend) of computation time on a standard laptop.

- The other two finalists are both lattices-based: different assumptions are needed.
- There are new (not-so-practical) signatures on linear codes.
- Isogenies: CSI-FiSh and SeaSign are close to be practical.

New Assumptions

New hardness assumptions can be carried by Hard Homogeneous Space. An example is given by isogeny-based cryptography, such as CSIDH.

- The POLYNOMIAL ISOMORPHISM problem can be seen in this setting.
- We introduce another problem: ALTERNATING TRILINEAR FORM EQUIVALENCE (ATFE).

Alternating Trilinear Forms

Alternating Trilinear Form

A map $\phi : (\mathbb{F})^n \times (\mathbb{F})^n \times (\mathbb{F})^n \to \mathbb{F}$ is *trilinear* if it is linear in each of its 3 arguments. It is *alternating* if it evaluates to 0 whenever two inputs are equal. The set of alternating trilinear forms over $(\mathbb{F}_q)^n$ is denoted with ATF(n, q)

We can define the action of GL(n, q) over ATF(n, q) in the following way:

$$A \star \phi = \phi \circ A$$

and we have $(\phi \circ A)(x, y, z) = \phi(A^t(x), A^t(y), A^t(z))$.

Given ϕ, ψ in ATF(n, q), we write $\phi \sim \psi$ if there exists A in GL(n, q) such that $\phi = \psi \circ A$.

Main Problem and Variants

The decision problem ALTERNATING TRILINEAR FORM EQUIVALENCE (ATFE) is the following:

- **Input**: two alternating trilinear forms ϕ and ψ.
- **Output**: "Yes" if $\phi \sim \psi$ and "No" otherwise.

The promised search problem psATFE is the following:

- **Input**: two alternating trilinear forms ϕ and ψ such that $\phi \sim \psi$.
- **Output**: some A such that $\phi = \psi \circ A$.

Multiple psATFE

The signature scheme is based on a generalization of psATFE:

The promised search version of ATFE for m instances is denoted with m-psATFE and is the following problem:

- **Input**: m alternating trilinear forms $\phi_1, \ldots, \phi_m$ such that $\phi_i \sim \phi_j$ for every (i, j).
- **Output**: some A and a pair (i, j), with $i \neq j$, such that $\phi_i = \phi_j \circ A$.

Why ATFE?

To answer this question, we need to introduce the following problem.

The decision problem $d-$TENSOR ISOMORPHISM over the field $\mathbb{F}$ is the following:

- **Input**: two d-tensors in $\mathbb{F}$, of sides length $n_1, \ldots, n_d$, $A = (a_{i_1,\ldots,i_d})$ and $B = (b_{i_1,\ldots,i_d})$.
- **Output**: "Yes" if there exist $P_1 \in \mathrm{GL}(n_1, \mathbb{F}), \ldots, P_d \in \mathrm{GL}(n_d, \mathbb{F})$ such that for all $i_1, \ldots, i_d$

$$a_{i_1,\ldots,i_d} = \sum_{j_1,\ldots,j_d} b_{j_1,\ldots,j_d} (P_1)_{i_1 j_1} \cdots (P_d)_{i_d j_d}$$

and "No" otherwise.

The class TI

In [Grochow and Qiao, 2021], the following definitions are given.

For any field $\mathbb{F}$, the class $\mathrm{TI}_{\mathbb{F}}$ contains problems that are polynomial-time reducible to d-Tensor Isomorphism over $\mathbb{F}$ for some d.
A problem is said $\mathrm{TI}_{\mathbb{F}}$-complete if it is in $\mathrm{TI}_{\mathbb{F}}$ and d − Tensor Isomorphism for any d reduces to it.

In the same flavour of SAT and $3-\mathrm{SAT}$, the problem 3 − Tensor Isomorphism is $\mathrm{TI}_{\mathbb{F}}$-complete.

Theorem [Grochow et al., 2020]

Alternating Trilinear Form Eq. is $\mathrm{TI}_{\mathbb{F}}$-complete.

Why TI?

The class TI is of large interest for many reasons:

1. TI-complete problems are *hard-on-average*:
   - the worst case is hard as the average case $\implies$ useful for cryptography;
   - they cannot be NP-hard unless the polynomial hierarchy collapses;
   - they are at least as hard as Graph Isomorphism and Code Equivalence.
2. Many problems from different areas:
   - d – Tensor Isomorphism from quantum information;
   - Tensor Congruence from machine learning;
   - Polynomial Isomorphism from cryptography;
   - Group Isomorphism for certain groups from computational algebra;
   - many other like Algebra Isomorphism.

Structure of TI

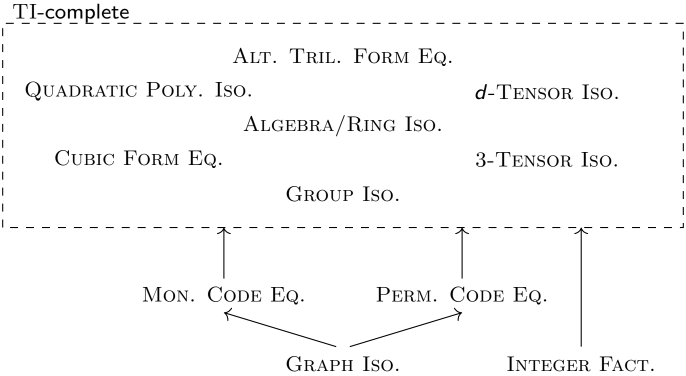

Figure: Structure of TI (see [Grochow and Qiao, 2021, Grochow et al., 2020]).

Effort from different areas $\implies$ well-studied problems.

Assumptions on Group Actions

We generalize the Decisional Diffie-Hellman Assumption for group actions.

Pseudorandom Action

Let $(G, S, \star)$ be the action of G over S through $\star : (G, S) \to S$.
Define the following distributions over $S \times S$:

1. the *random* distribution is the uniform one over $S \times S$;
2. the *pseudorandom* distribution picks uniformly $x \in S$ and $g \in G$ and returns $(x, g \star x)$.

The action is *pseudorandom* if the two distributions above cannot be distinguished efficiently.

Hardness Assumption

It is assumed that (post-quantum) pseudorandom group actions exist:

1. the class group action from CSIDH or
2. the group action on 3-tensor used in [Ji et al., 2019] to design a digital signature.

Pseudorandom Assumption

The group action of $\mathrm{GL}(n, q)$ over $\mathrm{ATF}(n, q)$ underlying ATFE is pseudorandom.

Representations of ATF

Let e_i^* be the canonical linear form. We can construct an alternating trilinear form $e_i^* \wedge e_j^* \wedge e_k^*$, where, given $(x, y, z) \in (\mathbb{F}_q)^n \times (\mathbb{F}_q)^n \times (\mathbb{F}_q)^n$, we have

$$\left(e_i^* \wedge e_j^* \wedge e_k^*\right)(x, y, z) = \det \begin{pmatrix} x_i & y_i & z_i \\ x_j & y_j & z_j \\ x_k & y_k & z_k \end{pmatrix}$$

An element ϕ in $\mathrm{ATF}(n, q)$ can be represented as

$$\phi = \sum_{1 \leq i < j < k \leq n} c_{i,j,k}\, e_i^* \wedge e_j^* \wedge e_k^*.$$

We need $\binom{n}{3}$ elements of $\mathbb{F}_q$.

How $\mathrm{GL}(n,q)$ acts

Let $A = (a_{i,j})$ in $\mathrm{GL}(n,q)$. We have

$$\left(e_i^* \wedge e_j^* \wedge e_k^*\right) \circ A = \sum_{1 \le r < s < t \le n} d_{r,s,t}\, e_r^* \wedge e_s^* \wedge e_t^*,$$

where

$$d_{r,s,t} = \det \begin{pmatrix} a_{i,r} & a_{i,s} & a_{i,t} \\ a_{j,r} & a_{j,s} & a_{j,t} \\ a_{k,r} & a_{k,s} & a_{k,t} \end{pmatrix}.$$

We extend this action linearly over $\mathrm{ATF}(n,q)$.

The Σ-protocol

The signature scheme in [Tang et al., 2022] is built applying the Fiat-Shamir transform to a Σ-protocol based on C-psATFE.
Let $\phi_C \in \mathrm{ATF}(n, q)$ and $\phi_i = \phi_C \circ A_i$ for randomly chosen $A_i \in \mathrm{GL}(n, q)$, for every $i = 1, \dots, C-1$.
Set $sk = \{A_i\}_{i=1,\dots,C-1}$ and $pk = \{\phi_i\}_{i=1,\dots,C-1}$.

Alice(sk, ϕ_C)		**Bob**(pk, ϕ_C)
Picks $B \in \mathrm{GL}(n, q)$.	$\psi = \phi_C \circ B$ $\longrightarrow$	
	b $\longleftarrow$	Picks $b \in \{1, \dots, C-1\}$.
Set $D = A_b^{-1} B$	D $\longrightarrow$	Checks if $\psi = \phi_b \circ D$.

Key Generation Algorithm

Algorithm 1: Key generation.

Input: The variable number $n \in \mathbb{N}$, a prime power q, the alternating trilinear form number $C = 2^c$.

Output: Public key: C alternating trilinear forms $\phi_i \in \mathrm{ATF}(n, q)$ such that $\phi_i \sim \phi_j$ for any $i, j \in [C]$.

Private key: C matrices $A_1, \ldots, A_C$, such that $\phi_i \circ A_i = \phi_C$.

Randomly sample an alternating trilinear form $\phi_C : \mathbb{F}_q^n \times \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$.

Randomly sample $C - 1$ invertible matrices, $A_1, \ldots, A_{C-1} \in \mathrm{GL}(n, q)$.

For every $i \in [C-1]$, $\phi_i \leftarrow \phi_C \circ A_i$.

For every $i \in [C-1]$, $A_i \leftarrow A_i^{-1}$.

$A_C \leftarrow I_n$.

return *Public key:* $\phi_1, \phi_2, \ldots, \phi_C$. *Private Key:* $A_1, \ldots, A_C$.

Signing Algorithm

Algorithm 2: Signing procedure.

Input: The public key $\phi_1, \dots, \phi_C \in \mathrm{ATF}(n,q)$. The private key $A_1, \dots, A_C \in \mathrm{GL}(n,q)$. $r \in \mathbb{N}$, $C = 2^c$. The message M. A hash function $H : \{0,1\}^* \to \{0,1\}^\ell$, with the promise that $\lfloor \ell/c \rfloor \geq r$.

Output: The signature S on M.

for $i \in [r]$ **do**
  Randomly sample $B_i \in \mathrm{GL}(n,q)$.
  $\psi_i \leftarrow \phi_C \circ B_i$.
end
Compute $L = H(\mathrm{M}|\psi_1|\dots|\psi_r) \in \{0,1\}^\ell$.
/* For the next step we need $\lfloor \ell/c \rfloor \geq r$. */
Slice L into $\lfloor \ell/c \rfloor$ bit strings in $\{0,1\}^c$, and set $b_1, \dots, b_r \in [C]$ to be the integer represented by the first r bit strings.
for $i \in [r]$ **do**
  $D_i \leftarrow A_{b_i} B_i$. ; // Note that $\phi_{b_i} \circ D_i = \psi_i$.
end
return $S = (b_1, \dots, b_r, D_1, \dots, D_r)$.

Verify Algorithm

Algorithm 3: Verification procedure.

Input: The public key $\phi_1, \ldots, \phi_C \in \mathrm{ATF}(n, q)$. The signature $S = (b_1, \ldots, b_r, D_1, \ldots, D_r)$, $b_i \in [C]$, $D_i \in \mathrm{GL}(n, q)$. The message M. The A hash function $H : \{0,1\}^* \to \{0,1\}^\ell$, with the promise that $\lfloor \ell/c \rfloor \geq r$.

Output: "Yes" if S is a valid signature for M. "No" otherwise.

for $i \in [r]$ **do**
  Compute $\psi_i = \phi_{b_i} \circ D_i$.
end
Compute $L' = H(\mathrm{M}|\psi_1| \ldots |\psi_r) \in \{0,1\}^\ell$.
`/* For the next step we need` $\lfloor \ell/c \rfloor \geq r$. `*/`
Slice L' into $\lfloor \ell/c \rfloor$ bit strings in $\{0,1\}^c$, and set $b'_1, \ldots, b'_r \in [C]$ to be the integer represented by the first r bit strings.
if *for every* $i \in [r]$, $b_i = b'_i$ **then**
  return *Yes*
else
  return *No*

Security of the Digital Signature Scheme

Theorem [Tang et al., 2022]

The previous signature scheme based on ATFE is EUF-CMA secure in the Random Oracle Model (ROM) under the hardness of the C-psATFE problem.

Equivalently, the scheme is EUF-CMA in the ROM secure under the assumption that the group action underlying ATFE is pseudorandom.

Attacks

The cryptanalysis of the signature consist of solving the psATFE problem.

- **Brute force**: $|\mathrm{GL}(n,q)| = O(q^{n^2})$.
- **Average-time**: in [Grochow et al., 2020] is presented an algorithm for psATFE running in $\sim q^{4n}$ that solves the fraction $1 - \frac{1}{q^{\Omega(n)}}$ of all instances.
- **Gröbner bases**: solving a polynomial system to find A in $\mathrm{GL}(n,q)$.

Setting up the system

Given two alternating trilinear forms ϕ and ψ, we want to find A such that $\psi = \phi \circ A$.
We want to solve the system

$$(*) = \begin{cases} XY = I_n \\ \phi(X^t(u), X^t(v), w) = \psi(u, v, Y^t(w)) \end{cases}$$

where X and Y are $n \times n$ matrices representing A, while the second equation formulates $\phi(X^t(u), X^t(v), X^t(w)) = \psi(u, v, w)$ avoiding cubic terms.

We have a system of $\binom{n}{3} + n^2$ quadratic equations in $2n^2$ variables.

A First Estimation

Under some assumptions (used for equivalent problems), we can estimate the degree of regularity of the ideal generated by $(*)$.

- we assume that polynomials in $(*)$ forms a *semi-regular sequence* (defined in [Bardet et al., 2005]);
- given $m = N\alpha(n)$ quadratic polynomials in N variables, we assume that the estimation of the degree of regularity from [Bardet et al., 2005] applies even if α is not constant.

We obtain that the degree of regularity is asymptotically $3n$. Then, since in our case $N = 2n^2$, the F5 algorithm has complexity

$$O(2^{6\omega n \log_2(n)})$$

where ω is the matrix multiplication exponent.

Using Partial Information

If we assume that the first column of A is known, we can achieve a significant speed-up.

- The knowledge of the first column of X implies constrains on Y and reduces the number of variables to $2(n^2 - n)$.
- Experiments in this setting show that maxGBdeg of the ideal generated by $(*)$ is 3 for each n up to 13.

The polynomial system with partial information can be solved in time

$$O(n^{2\omega} \log_2(q)).$$

How to find such partial information?

Heuristic Complexity

Let $\phi, \psi \in \mathrm{ATF}(n, q)$ such that $\psi = \phi \circ A$.

- For any $\varphi \in \mathrm{ATF}(n, q)$ and $u \in (\mathbb{F}_q)^n$, we define the bilinear form
$$\varphi_u(y, z) = \varphi(u, y, z).$$
- For a fixed r, the size of the set $R_{\varphi,r} = \{u \mid \mathrm{rk}(\varphi_u) = r\}$ is an isomorphism invariant.
- The *birthday attack* can be used to find *partial information* in the space $R_{\phi,r} \times R_{\psi,r}$, having size $O(q^{4n/3})$.
- After $O(q^{2n/3})$ samples, we find, with constant probability u and v in $(\mathbb{F}_q)^n$ such that $Au = v$.

We have an heuristic algorithm that solves psATFE in

$$O(q^{2n/3} n^{2\omega} \log_2(q)).$$

Recap on attacks

1. Upper bound for the F5 algorithm:

$$O(2^{6\omega n \log_2(n)}).$$

2. Average-time:

$$O(q^{4n}).$$

3. Partial information and birthday attack:

$$O(q^{2n/3} n^{2\omega} \log_2(q)).$$

4. Reduction to minRank Problem: slower than partial information for practical instances.

Post-quantum considerations

- The Shor's quantum algorithm can solve the Hidden Subgroup Problem (HSP) in polynomial time for certain instances.
- A reduction from psATFE to HSP is known, but the instance obtained is non-abelian.
- There are no practical algorithm for non-abelian HSP, even in the quantum setting.
- This is the same argument used for lattice-based cryptosystems.

Security in the QROM

The security of the signature in [Tang et al., 2022] is shown in the ROM. What can we say about the Quantum ROM (QROM)?

- The security of the Fiat-Shamir transform in the QROM is non trivial and it is only assumed.
- Different properties for the Σ-protocol are required. For example the *collapsing property* [Liu and Zhandry, 2019].
- It can be achieved asking that the following problem is hard: given $\phi, \psi \in \mathrm{ATF}(n, q)$, to find $A, B \in \mathrm{GL}(n, q)$ such that

$$\phi = \psi \circ A = \psi \circ B.$$

This is linked to find automorphisms of a given alternating trilinear form (ATFA).

Params, Sizes and Times

	Parameters					Size in Byte			Time in μs		
	n	q	r	c	λ	Public key	Private key	Signature	Set-Up	Sign	Verify
Option 1	9	524287	26	5	128	6384	6156	5018	285.9	471.7	416.5
Option 2	10	131071	26	5	128	8160	6800	5542	383.1	660.0	578.9
Option 3	10	131071	32	4	128	4080	3400	6816	190.7	795.4	708.8
Option 4	11	65521	26	5	128	10560	7744	6309	514.0	861.1	765.2

Figure: Proposed parameters, sizes and timings for 128 bits of security

- NIST's finalists run in the range $100\mu s - 1000\mu s$.
- The public key and signature sizes of Dilithium are 1312 and 2420 B, while for Falcon-512 we have 897 and 666 B.
- Isogeny-based schemes have smaller sizes (204 and 64 B) but slower algorithms: $2500ms$ for signing and $50ms$ for verifying.

Conclusions

- We have seen a new signature scheme, using new assumptions (ATFE).
- The class TI is itself interesting, both in Complexity Theory and in Cryptography.
- The signature scheme has practical times and close to practical sizes. It can be a potential alternative candidate for the NIST's call.

Thank you for your attention!

References I

Bardet, M., Faugere, J.-C., Salvy, B., and Yang, B.-Y. (2005).
Asymptotic behaviour of the degree of regularity of semi-regular polynomial systems.
In *Proc. of MEGA*, volume 5, pages 2–2.

Grochow, J. A. and Qiao, Y. (2021).
On the complexity of isomorphism problems for tensors, groups, and polynomials i: Tensor isomorphism-completeness.
In *12th Innovations in Theoretical Computer Science Conference (ITCS 2021)*. Schloss Dagstuhl-Leibniz-Zentrum für Informatik.

References II

Grochow, J. A., Qiao, Y., and Tang, G. (2020).
Average-case algorithms for testing isomorphism of polynomials, algebras, and multilinear forms.
arXiv preprint arXiv:2012.01085.

Ji, Z., Qiao, Y., Song, F., and Yun, A. (2019).
General linear group action on tensors: A candidate for post-quantum cryptography.
In *Theory of Cryptography Conference*, pages 251–281. Springer.

Liu, Q. and Zhandry, M. (2019).
Revisiting post-quantum fiat-shamir.
In *Annual International Cryptology Conference*, pages 326–355. Springer.

References III

Tang, G., Duong, D. H., Joux, A., Plantard, T., Qiao, Y., and Susilo, W. (2022).
Practical post-quantum signature schemes from isomorphism problems of trilinear forms.
Cryptology ePrint Archive.