ALTEQ : 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 [5,7]

[1]Saarland University, Germany [2]University of Wollongong, Australia [3]SandboxAQ, USA [4]Nokia Bell Labs, USA [5]University of Technology Sydney, Australia [6]KDDI Research, Japan [7]University of Birmingham, UK

ALTEQ = GMW Σ-protocol based on ATFE + Fiat-Shamir.

The ALTEQ signature scheme is founded on the hardness of finding isomorphisms between alternating trilinear forms modulo the general linear group acting by base change. The Goldreich–Micali–Wigderson (GMW) motif tailored to this group action builds a Σ-protocol identification scheme, whose soundness and zero-knowledge rely on this hardness. Then, the Fiat-Shamir transform removes the interaction from the Σ-protocol to yield a signature scheme.

Alternating Trilinear Form Equivalence Problem (ATFE)

Let $\mathbb{F}_q$ denote the finite field with q elements. An alternating trilinear form ϕ is a function

$$\phi : \mathbb{F}_q^n \times \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q$$
$$(u, v, w) \longmapsto \sum_i \sum_j \sum_k \phi_{ijk} u_i v_j w_k$$

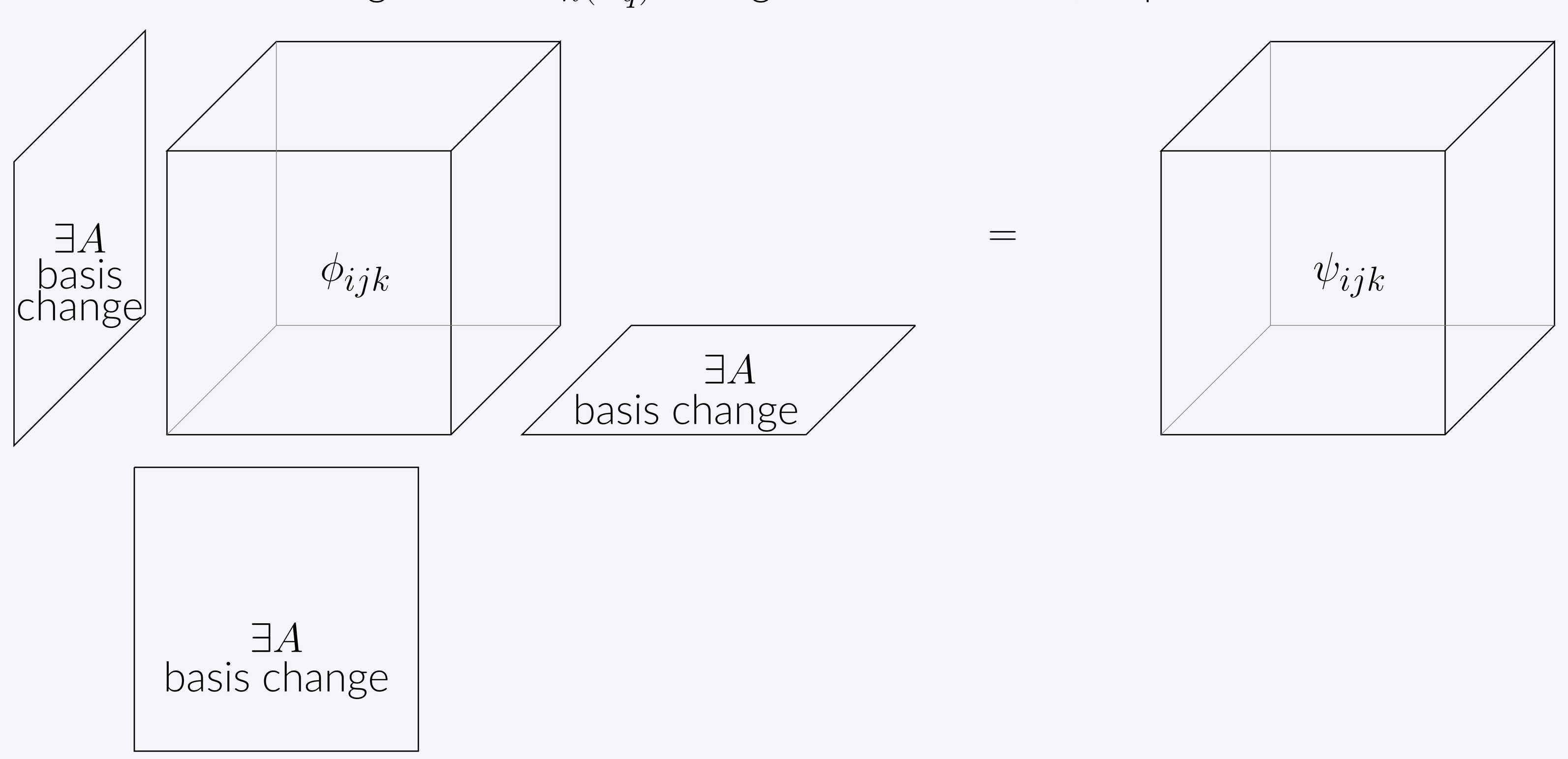
that is linear in each of its three arguments, satisfying the anti-symmetry constraint

$$\phi(u, u, w) = \phi(u, v, v) = \phi(w, v, w) = 0, \forall u, v, w \in \mathbb{F}_q^n.$$

Invertible matrices $A \in GL_n(\mathbb{F}_q)$ act on alternating tensors by the same basis change

$$(A, \phi(\star, \star, \star)) \longmapsto \phi(A^T\star, A^T\star, A^T\star)$$

on each of the three dimensions. Two alternating trilinear forms ϕ, ψ are isomorphic if there exists such a basis change $A \in GL_n(\mathbb{F}_q)$ taking one to the other, as pictured below.



ATFE (decision version)

Given two alternating tensors, decide if they are isomorphic.

ATFE (promise search version)

Given two isomorphic alternating tensors, find an isomorphism between them.

ATFE (pseudorandom version)

Distinguish the following two distributions:

- Random distribution: two randomly sampled alternating tensors.
- Pseudorandom distribution: two randomly sampled alternating tensors in the same orbit.

Tensor Isomorphism Complexity Class

The Tensor Isomorphism (TI) complexity class was introduced in [4] to capture the complexity of several isomorphism problems for algebraic structures, such as tensors, groups, and polynomials. The following relations between isomorphism problems are shown in [4, 5].

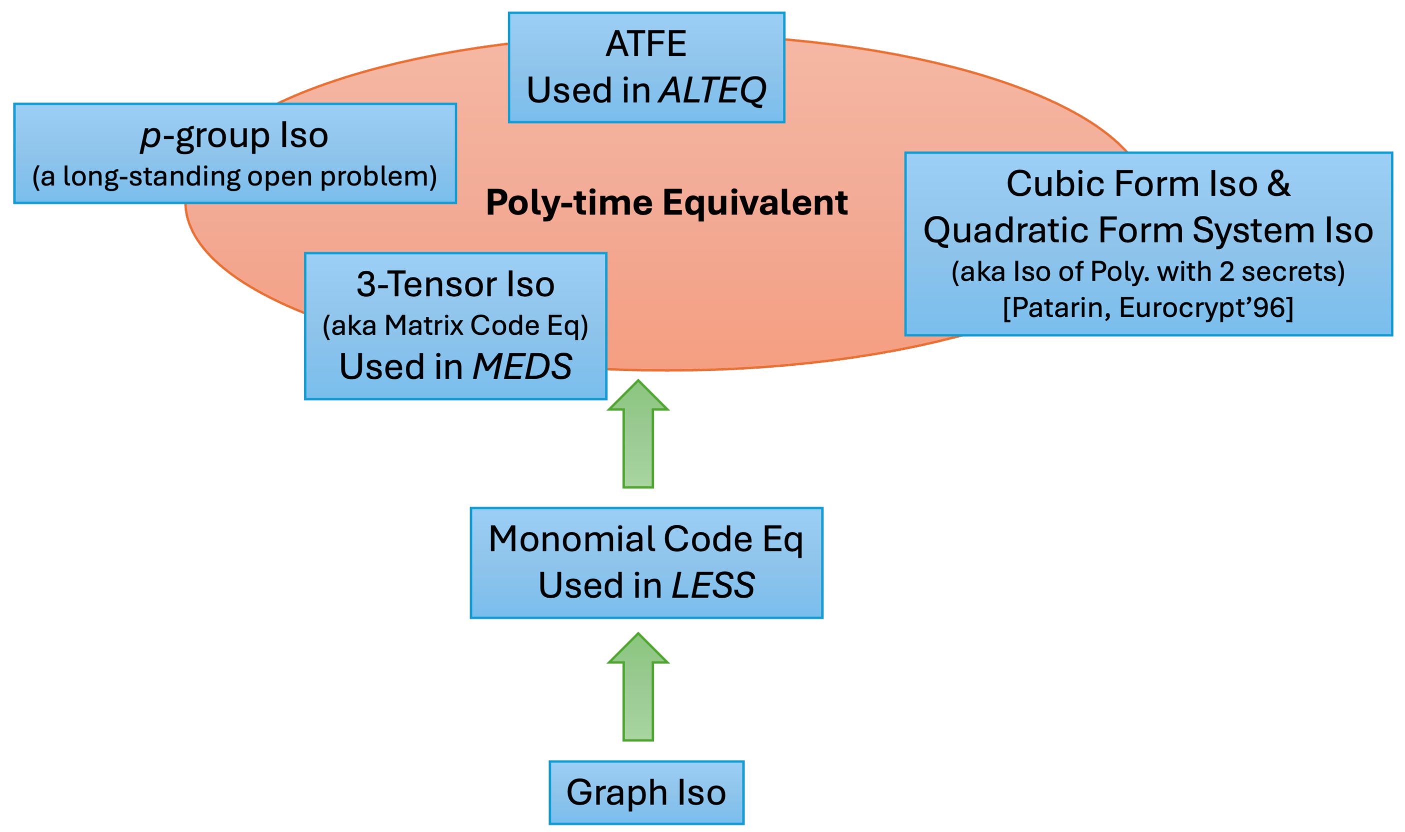


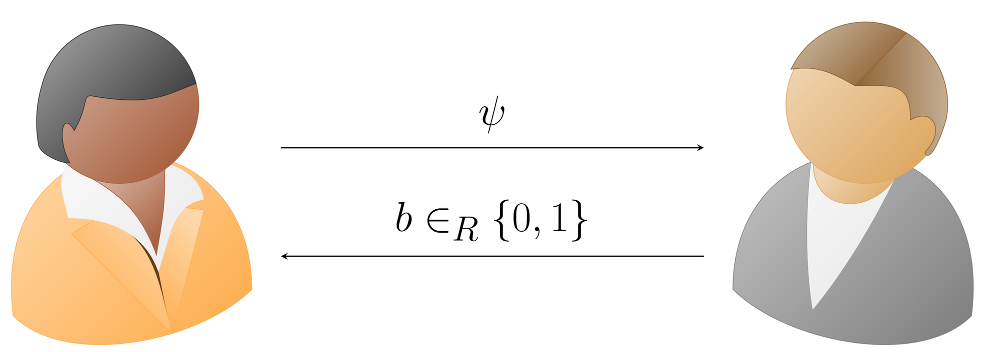
Figure 1. Complexity

Protocol

Secret key: a invertible matrix $A \in \mathrm{GL}(n, \mathbb{F}_q)$.

Public key: two alternating trilinear form ϕ_0 and ϕ_1 such that $\phi_0 \circ A = \phi_1$.

1. Alice samples a random matrix $B \in \mathrm{GL}(n, \mathbb{F}_q)$ which transforms ϕ_0 to $\psi = \phi_0 \circ B$.
2. Bob flips a random coin $b \in_R \{0, 1\}$.



Alice: ϕ_0, ϕ_1 Bob: ϕ_0, ϕ_1

3. Based on b, the protocol goes into one of the following.
   - If $b = 0$, Alice sends $r := B$ to Bob; otherwise sends $r := A^{-1}B$.
   - If $b = 1$, Bob verifies whether $\phi_0 \circ r = \psi$; otherwise verifies whether $\phi_1 \circ r = \psi$.

Before applying Fiat-Shamir, need to reduce the soundness error by repeating λ times in parallel.

The protocol can be improved with the following optimizations:

1. **Larger challenge space:** reducing the soundness error from 1/2 to $1/2^C$; public key size C factor increases.
2. **Unbalanced challenge space:** reducing the signature size by replacing partial responses with seeds; the round number r increases.

Parameters & Performance

- Processor: Intel Xeon E-2288G 3.7GHz 8 cores 16MB L3 Cache HT Enabled (Max Turbo Freq. 5.0GHz, Min 4.7GHz).
- Memory: 64GB.
- Operating system: Red Hat Enterprise Linux 8.6 (Ootpa).
- Compiler: gcc version 8.5.0 20210514 (Red Hat 8.5.0-10).

Parameter set	Parameters (n, q, r, K, C)	Private key Size (Bytes)	Public key Size (Bytes)	Signature Size (Bytes)	Public key + signature Size (Bytes)
I	$(18, 2^{24} - 3, 159, 21, 4)$	32	9824	22684	32508
III	$(27, 2^{21} - 9, 342, 28, 4)$	48	30761	61214	91975

Table 1. Key and Signature Sizes for Balanced-**ALTEQ**

Parameter set	Parameters (n, q, r, K, C)	Private key Size (Bytes)	Public key Size (Bytes)	Signature Size (Bytes)
I	$(18, 2^{24} - 3, 130, 8, 1960)$	32	4798112	9792
III	$(27, 2^{21} - 9, 250, 12, 1420)$	48	10902986	28772

Table 2. Key and Signature Sizes for ShortSig-**ALTEQ**

parameter set		Key gen	Sign	Verify	Sign+verify
I	cycles	1038786	10979754	9939474	20919228
	time (ms)	0.306	3.126	2.818	5.944
III	cycles	6586317	101706473	98377696	200084169
	time (ms)	1.820	28.333	27.412	55.745

Table 3. Performance of Balanced-**ALTEQ**

parameter set		Key gen	Sign	Verify
I	cycles	103829839	9147687	12340116
	time (ms)	33.323	2.579	3.350
III	cycles	368025726	78018518	85334976
	time (ms)	97.706	20.895	22.736

Table 4. Performance of ShortSig-**ALTEQ**

Ongoing Improvements

- [3] introduces a technique that could reduce the signature size by 1/3 to 1/2.
- An ongoing project indicates that using quadrilinear forms (or 4-tensors) could thwart some of the main cryptanalytic attack approaches and lead to smaller signature sizes.

References

[1] Ward Beullens. Graph-theoretic algorithms for the alternating trilinear form equivalence problem. CRYPTO, 2023.

[2] Markus Bläser, Zhili Chen, Dung Hoang Duong, Antoine Joux, Ngoc Tuong Nguyen, Thomas Plantard, Youming Qiao, Willy Susilo, and Gang Tang. On digital signatures based on isomorphism problems: Qrom security and ring signatures. PQCrypto, 2024.

[3] Tung Chou, Ruben Niederhagen, Lars Ran, and Simona Samardjiska. Reducing signature size of matrix-code-based signature schemes. Cryptology ePrint Archive, 2024/495, 2024.

[4] Joshua A. Grochow and Youming Qiao. On the complexity of isomorphism problems for tensors, groups, and polynomials i: Tensor isomorphism-completeness. SIAM J. Comput., 2023.

[5] Joshua A. Grochow, Youming Qiao, and Gang Tang. Average-case algorithms for testing isomorphism of polynomials, algebras, and multilinear forms. STACS, 2021.

[6] Anand Kumar Narayanan, Youming Qiao, and Gang Tang. Algorithms for matrix code and alternating trilinear form equivalences via new isomorphism invariants. EUROCRYPT, 2024.