Finding isomorphisms between trilinear forms, slightly faster

Anand Kumar Narayanan [1]   Youming Qiao [2]   Gang Tang [2,3]

[1] SandboxAQ, Palo Alto, CA, USA.

[2] University of Technology Sydney, Ultimo, NSW, Australia.

[3] University of Birmingham, UK.

Three is a shroud!

Given two square matrices ϕ and ψ, can we tell if there is an invertible matrix A such that

$$\boxed{A} \quad \boxed{\phi} \quad \boxed{A^{-1}} = \boxed{\psi}$$

Three is a shroud!

Given two square matrices ϕ and ψ, can we tell if there is an invertible matrix A such that

$$\boxed{A} \quad \boxed{\phi} \quad \boxed{A^{-1}} = \boxed{\psi}$$

Yes, quickly!

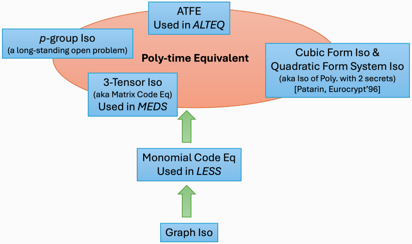
Three is a shroud!

Given two square matrices ϕ and ψ, can we tell if there is an invertible matrix A such that

$$\boxed{A}\ \boxed{\phi}\ \boxed{A^{-1}} = \boxed{\psi}$$

Yes, quickly! Jumping from two (square matrices) to three (three dimensional tensors given by a cube of numbers), is a giant leap in computational complexity.

Most such linear algebraic problems concerning three dimensional tensors (or equivalently, trilinear forms) are (NP- or VNP- or #P-)hard, with a web



of complexity theoretic reductions connecting them. Among them is the tensor isomorphism problem, on whose hardness MEDS, ALTEQ, etc. are built.

New algorithms for tensor isomorphism

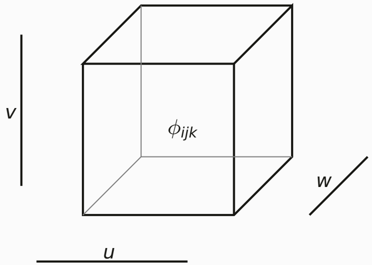
- We present algorithms to find tensor isomorphisms polynomially faster than previously known, and discuss how this informs the security/parameters of MEDS/ALTEQ.
- Meet-in-the-middle/birthday style algorithms, exploiting novel invariants to finding collisions.
- Based on our work (eprint number 368, 2024) to appear in Eurocrypt 2024, which builds on algorithms by Bouillaguet, Fouque, and Véber (Eurocrypt 2013), and Beullens (Crypto 2023).
- For the complexity theoretic reductions, average case analysis, search to decision variant reduction, etc., consult the series (ITCS 2021 I,II,III,IV) of papers by Joshua Grochow and Youming Qiao.

Trilinear forms

A trilinear form is a function

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

that is linear in each of its three arguments. Think of it as an $n \times n \times n$ cube



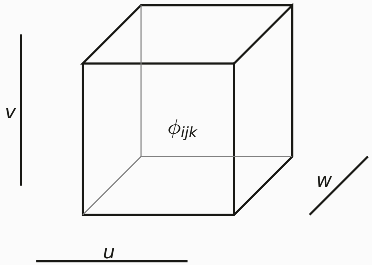
of $\mathbb{F}_q$ elements.

Trilinear forms

A trilinear form is a function

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

that is linear in each of its three arguments. Think of it as an $n \times n \times n$ cube



of $\mathbb{F}_q$ elements. It is alternating if it satisfies the anti-symmetry constraint

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

Tensor Isomorphism (Variant underlying MEDS).

Triples of invertible matrices $(A, B, C) \in GL_n(\mathbb{F}_q)^3$ act on tensors by basis change

$$((A, B, C), \phi(\star, \star, \star)) \longmapsto \phi^{A,B,C} := \phi(A\star, B\star, C\star)$$

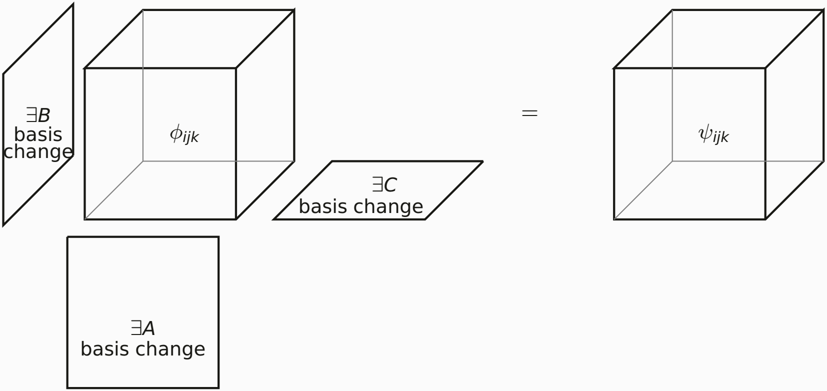
on the respective three dimensions.

Tensor Isomorphism (Variant underlying MEDS).

Triples of invertible matrices $(A, B, C) \in GL_n(\mathbb{F}_q)^3$ act on tensors by basis change

$$((A, B, C), \phi(\star, \star, \star)) \longmapsto \phi^{A,B,C} := \phi(A\star, B\star, C\star)$$

on the respective three dimensions. Two forms ϕ, ψ are isomorphic if there exists such a basis change $(A, B, C) \in GL_n(\mathbb{F}_q)^3$ taking one to the other, as pictured.



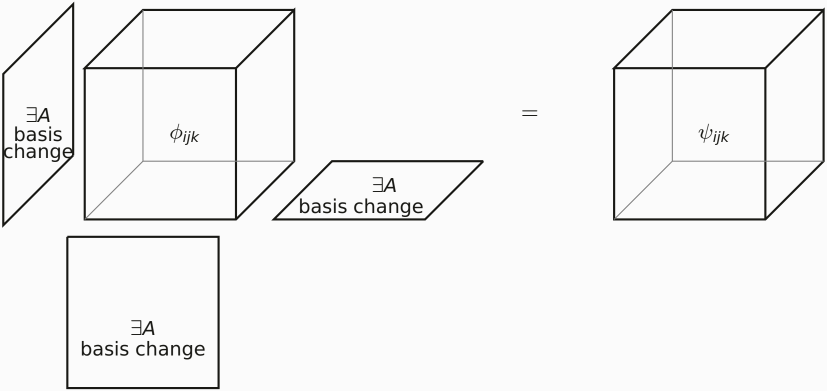
Given two isomorphic tensors, find an isomorphsim between them.

Tensor Isomorphism (Variant underlying ALTEQ).

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

$$(A, \phi(\star, \star, \star)) \longmapsto \phi^A := \phi(A\star, A\star, A\star)$$

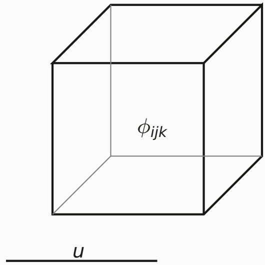
on each of the three dimensions. Two alternating trilinear forms ϕ, ψ are isomorphic if there exists such a basis change $A \in GL_n(\mathbb{F}_q)$ taking one to the other, as pictured.



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

Finding tensor isomorphism (MEDS variant)

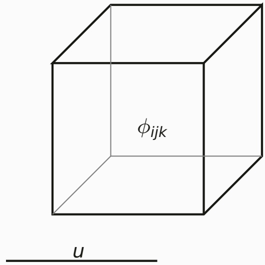
Co-rank one points are $u \in \mathbb{F}_q^n$ such that $\phi(u, \star, \star)$ is co-rank one. That is, the matrix



has rank $n - 1$.

Finding tensor isomorphism (MEDS variant)

Co-rank one points are $u \in \mathbb{F}_q^n$ such that $\phi(u, \star, \star)$ is co-rank one. That is, the matrix



has rank $n-1$. We design a fast computable invariant, pairing trilinear forms ϕ with co-rank one projective points $\hat{u} \in \mathbb{P}(\mathbb{F}_q^n)$,

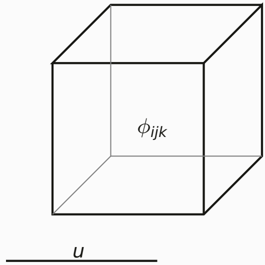
$$(\phi, \hat{u}) \longmapsto \langle \phi, \hat{u} \rangle$$

satisfying, for all $\phi, \hat{u}, A, B, C$,

$$\langle \phi, \hat{u} \rangle = \left\langle \phi^{A,B,C}, A^{-1}\hat{u} \right\rangle .$$

Finding tensor isomorphism (MEDS variant)

Co-rank one points are $u \in \mathbb{F}_q^n$ such that $\phi(u, \star, \star)$ is co-rank one. That is, the matrix



has rank $n - 1$. We design a fast computable invariant, pairing trilinear forms ϕ with co-rank one projective points $\hat{u} \in \mathbb{P}(\mathbb{F}_q^n)$,

$$(\phi, \hat{u}) \longmapsto \langle \phi, \hat{u} \rangle$$

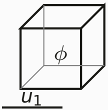
satisfying, for all $\phi, \hat{u}, A, B, C$,

$$\langle \phi, \hat{u} \rangle = \left\langle \phi^{A,B,C}, A^{-1}\hat{u} \right\rangle .$$

This invariant is distinguishing and informs a meet-in-the-middle birthday attack over the projective points, to test (and find) isomorphism.

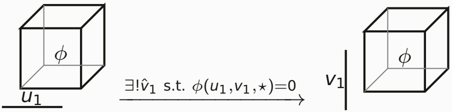
Constructing the invariant

Start with a co-rank one $\hat{u} = \hat{u}_1 \in \mathbb{P}(\mathbb{F}_q^n)$.



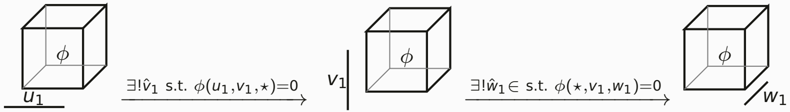
Constructing the invariant

Start with a co-rank one $\hat{u} = \hat{u}_1 \in \mathbb{P}(\mathbb{F}_q^n)$.



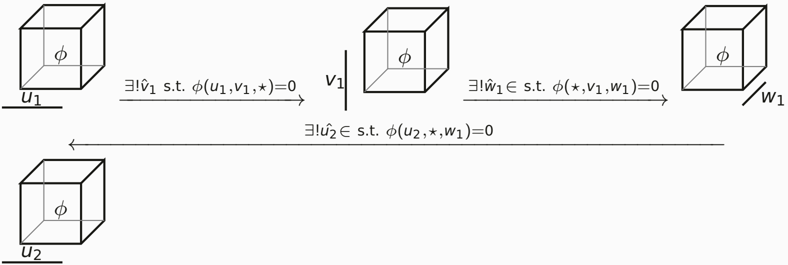
Constructing the invariant

Start with a co-rank one $\hat{u} = \hat{u}_1 \in \mathbb{P}(\mathbb{F}_q^n)$.



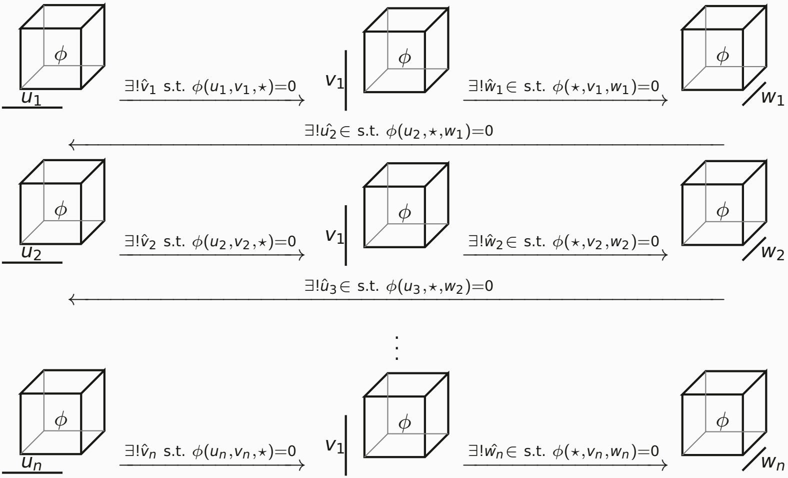
Constructing the invariant

Start with a co-rank one $\hat{u} = \hat{u}_1 \in \mathbb{P}(\mathbb{F}_q^n)$.



Constructing the invariant

Start with a co-rank one $\hat{u} = \hat{u}_1 \in \mathbb{P}(\mathbb{F}_q^n)$.



$U = \{u_1, u_2, \ldots, u_n\}$ $\quad$ $V = \{v_1, v_2, \ldots, v_n\}$ $\quad$ $W = \{w_1, w_2, \ldots, w_n\}$

Constructing the invariant

If each list U, V, W has n-linearly independent vectors, then we can construct three unique invertible matrices A_U, B_V, C_W to act. The resulting tensor

$$\langle \phi, \hat{u} \rangle := \phi^{A_U, B_V, C_W}$$

(not merely the isomorphism class) is the invariant.

Constructing the invariant

If each list U, V, W has n-linearly independent vectors, then we can construct three unique invertible matrices A_U, B_V, C_W to act. The resulting tensor

$$\langle \phi, \hat{u} \rangle := \phi^{A_U, B_V, C_W}$$

(not merely the isomorphism class) is the invariant.

If the automorphism group of ϕ is trivial (which is conjectured for random ϕ for not too small n), the invariant is distinguishing. That is,

$$\Pr_{(\hat{u}_1, \hat{u}_2)} \left(\langle \phi, \hat{u}_1 \rangle \neq \langle \phi, \hat{u}_2 \rangle \right) \approx 1.$$

Constructing the invariant

If each list U, V, W has n-linearly independent vectors, then we can construct three unique invertible matrices A_U, B_V, C_W to act. The resulting tensor

$$\langle \phi, \hat{u} \rangle := \phi^{A_U, B_V, C_W}$$

(not merely the isomorphism class) is the invariant.

If the automorphism group of ϕ is trivial (which is conjectured for random ϕ for not too small n), the invariant is distinguishing. That is,

$$\Pr_{(\hat{u}_1, \hat{u}_2)} \left(\langle \phi, \hat{u}_1 \rangle \neq \langle \phi, \hat{u}_2 \rangle \right) \approx 1.$$

Runtime

Assuming certain heuristics, the expected runtime of our algorithm is

$$O(q^{(n-2)/2} \cdot (q \cdot n^3 + n^4) \cdot (\log(q))^2).$$

Consequently, the bit security estimates of the MEDS scheme is reduced, as indicated in the table below.

parameter set	n	q	**Algebraic**	**Leon-like**	**Ours**
MEDS-I	14	4093	148.1	170.68	102.59
MEDS-III	22	4093	218.41	246.95	152.55
MEDS-V	30	2039	298.82	297.77	186.57

Remedy. Enlarging q increases the security estimate to meet the requirement. This should not affect the running times significantly, and only increase the signature size.

Finding tensor isomorphism (ALTEQ variant)

For a projective point $\hat{u}$ of large co-rank r, let $K_{\hat{u}}$ be the kernel $\ker(\phi(u, \star, \star))$. Then

$$(\phi, \hat{u}) \longmapsto \langle \phi, \hat{u} \rangle := (\phi : K_{\hat{u}} \times \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q) \bmod (GL(K) \times GL(n, q))$$

is an invariant. On the right is the isomorphism class of the restriction $\phi : K_{\hat{u}} \times \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q$ modulo $GL(K) \times GL(n, q)$.

Finding tensor isomorphism (ALTEQ variant)

For a projective point $\hat{u}$ of large co-rank r, let $K_{\hat{u}}$ be the kernel $\ker(\phi(u, \star, \star))$. Then

$$(\phi, \hat{u}) \longmapsto \langle \phi, \hat{u} \rangle := (\phi : K_{\hat{u}} \times \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q) \bmod (GL(K) \times GL(n, q))$$

is an invariant. On the right is the isomorphism class of the restriction $\phi : K_{\hat{u}} \times \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q$ modulo $GL(K) \times GL(n, q)$.

Given $(\hat{u}, \hat{u}')$ as partial information, we can test using Gröbner basis if

$$\langle \phi, \hat{u} \rangle =_? \langle \psi, \hat{u}' \rangle .$$

Algorithm.

Finding tensor isomorphism (ALTEQ variant)

For a projective point $\hat{u}$ of large co-rank r, let $K_{\hat{u}}$ be the kernel $\ker(\phi(u, \star, \star))$. Then

$$(\phi, \hat{u}) \longmapsto \langle \phi, \hat{u} \rangle := (\phi : K_{\hat{u}} \times \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q) \bmod (GL(K) \times GL(n, q))$$

is an invariant. On the right is the isomorphism class of the restriction $\phi : K_{\hat{u}} \times \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q$ modulo $GL(K) \times GL(n, q)$.

Given $(\hat{u}, \hat{u}')$ as partial information, we can test using Gröbner basis if

$$\langle \phi, \hat{u} \rangle =_? \langle \psi, \hat{u}' \rangle .$$

Algorithm. Input two alternating trilinear forms ϕ, ψ. Let the number of co-rank r points roughly be q^k.

Finding tensor isomorphism (ALTEQ variant)

For a projective point $\hat{u}$ of large co-rank r, let $K_{\hat{u}}$ be the kernel $\ker(\phi(u, \star, \star))$. Then

$$(\phi, \hat{u}) \longmapsto \langle \phi, \hat{u} \rangle := (\phi : K_{\hat{u}} \times \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q) \bmod (GL(K) \times GL(n, q))$$

is an invariant. On the right is the isomorphism class of the restriction $\phi : K_{\hat{u}} \times \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q$ modulo $GL(K) \times GL(n, q)$.

Given $(\hat{u}, \hat{u}')$ as partial information, we can test using Gröbner basis if

$$\langle \phi, \hat{u} \rangle =_? \langle \psi, \hat{u}' \rangle \, .$$

Algorithm. Input two alternating trilinear forms ϕ, ψ. Let the number of co-rank r points roughly be q^k.

- Sample a set U_ϕ of $q^{k/2}$ co-rank r points with respect to ϕ.
- Sample a set U_ψ of $q^{k/2}$ co-rank r points with respect to ψ.

Finding tensor isomorphism (ALTEQ variant)

For a projective point $\hat{u}$ of large co-rank r, let $K_{\hat{u}}$ be the kernel $\ker(\phi(u,\star,\star))$. Then

$$(\phi,\hat{u}) \longmapsto \langle \phi,\hat{u}\rangle := (\phi : K_{\hat{u}} \times \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q) \bmod (GL(K) \times GL(n,q))$$

is an invariant. On the right is the isomorphism class of the restriction $\phi : K_{\hat{u}} \times \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q$ modulo $GL(K) \times GL(n,q)$.

Given $(\hat{u},\hat{u}')$ as partial information, we can test using Gröbner basis if

$$\langle \phi,\hat{u}\rangle =_? \langle \psi,\hat{u}'\rangle .$$

Algorithm. Input two alternating trilinear forms ϕ,ψ. Let the number of co-rank r points roughly be q^k.

- Sample a set U_ϕ of $q^{k/2}$ co-rank r points with respect to ϕ.
- Sample a set U_ψ of $q^{k/2}$ co-rank r points with respect to ψ.
- Using the aforementioned Gröbner basis algorithm to test, find a collision $\langle \phi,\hat{u}\rangle =_? \langle \psi,\hat{u}'\rangle$ for some $\hat{u} \in U_\phi$ and $\hat{u}' \in U_\psi$.

Finding tensor isomorphism (ALTEQ variant)

For a projective point $\hat{u}$ of large co-rank r, let $K_{\hat{u}}$ be the kernel $\ker(\phi(u, \star, \star))$. Then

$$(\phi, \hat{u}) \longmapsto \langle \phi, \hat{u} \rangle := (\phi : K_{\hat{u}} \times \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q) \bmod (GL(K) \times GL(n, q))$$

is an invariant. On the right is the isomorphism class of the restriction $\phi : K_{\hat{u}} \times \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q$ modulo $GL(K) \times GL(n, q)$.

Given $(\hat{u}, \hat{u}')$ as partial information, we can test using Gröbner basis if

$$\langle \phi, \hat{u} \rangle =_? \langle \psi, \hat{u}' \rangle .$$

Algorithm. Input two alternating trilinear forms ϕ, ψ. Let the number of co-rank r points roughly be q^k.

- Sample a set U_ϕ of $q^{k/2}$ co-rank r points with respect to ϕ.
- Sample a set U_ψ of $q^{k/2}$ co-rank r points with respect to ψ.
- Using the aforementioned Gröbner basis algorithm to test, find a collision $\langle \phi, \hat{u} \rangle =_? \langle \psi, \hat{u}' \rangle$ for some $\hat{u} \in U_\phi$ and $\hat{u}' \in U_\psi$.

Heuristic runtime: Roughly $q^{k/2}$ times the cost to sample co-rank r points. Already taken into account in the design of ALTEQ.

Finding tensor isomorphism (ALTEQ variant)

For a projective point $\hat{u}$ of large co-rank r, let $K_{\hat{u}}$ be the kernel $\ker(\phi(u, \star, \star))$. Then

$$(\phi, \hat{u}) \longmapsto \langle \phi, \hat{u} \rangle := (\phi : K_{\hat{u}} \times \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q) \bmod (GL(K) \times GL(n, q))$$

is an invariant. On the right is the isomorphism class of the restriction $\phi : K_{\hat{u}} \times \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q$ modulo $GL(K) \times GL(n, q)$.

Given $(\hat{u}, \hat{u}')$ as partial information, we can test using Gröbner basis if

$$\langle \phi, \hat{u} \rangle =_? \langle \psi, \hat{u}' \rangle .$$

Algorithm. Input two alternating trilinear forms ϕ, ψ. Let the number of co-rank r points roughly be q^k.

- Sample a set U_ϕ of $q^{k/2}$ co-rank r points with respect to ϕ.
- Sample a set U_ψ of $q^{k/2}$ co-rank r points with respect to ψ.
- Using the aforementioned Gröbner basis algorithm to test, find a collision $\langle \phi, \hat{u} \rangle =_? \langle \psi, \hat{u}' \rangle$ for some $\hat{u} \in U_\phi$ and $\hat{u}' \in U_\psi$.

Heuristic runtime: Roughly $q^{k/2}$ times the cost to sample co-rank r points. Already taken into account in the design of ALTEQ.