Radboud University

Rare structures in tensor graphs

Bermuda triangles for cryptosystems based on the Tensor Isomorphism problem

Lars Ran and Simona Samardjiska

December 10, Asiacrypt 2024

Motivation

Two tensor-based schemes In NIST's additional call for signatures:

Motivation

Two tensor-based schemes In NIST's additional call for signatures:

ALTEQ

Motivation

Two tensor-based schemes In NIST's additional call for signatures:

ALTEQ

They rely on the hardness of the tensor isomorphism problem

Tensors

Tensors

In this work, tensors are 3-dimensional $n \times m \times k$ arrays over a finite field $\mathbb{F}_q$

Tensors

In this work, tensors are 3-dimensional $n \times m \times k$ arrays over a finite field $\mathbb{F}_q$

We take the trilinear forms perspective

$$\mathcal{C} : \mathbb{F}_q^n \times \mathbb{F}_q^m \times \mathbb{F}_q^k \to \mathbb{F}_q$$

Tensors

In this work, tensors are 3-dimensional $n \times m \times k$ arrays over a finite field $\mathbb{F}_q$

We take the trilinear forms perspective

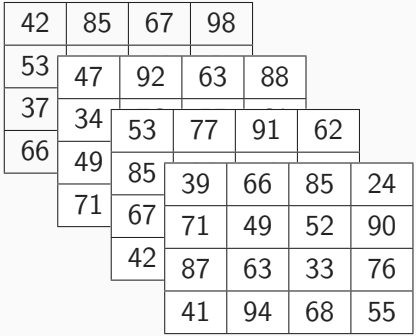
$$\mathcal{C} : \mathbb{F}_q^n \times \mathbb{F}_q^m \times \mathbb{F}_q^k \to \mathbb{F}_q$$

Fix bases $\mathbf{e}_1, \mathbf{e}_2, \ldots$ of $\mathbb{F}_q^n, \mathbb{F}_q^m$, and $\mathbb{F}_q^k$
A tensor is determined by its values on the basis vectors

$$\mathcal{C}_{ijl} := \mathcal{C}(\mathbf{e}_i, \mathbf{e}_j, \mathbf{e}_l) \quad \forall i, j, l.$$

An example

A tensor $\mathcal{C} : \mathbb{F}_{101}^4 \times \mathbb{F}_{101}^4 \times \mathbb{F}_{101}^4 \to \mathbb{F}_{101}$:



Tensor transformations

We can transform tensors by applying linear transformations to its arguments

Tensor transformations

We can transform tensors by applying linear transformations to its arguments

$(\mathbf{A}, \mathbf{B}, \mathbf{T}) \in \mathrm{GL}_n(q) \times \mathrm{GL}_m(q) \times \mathrm{GL}_k(q)$ maps a tensor $\mathcal{C}$ to a tensor $\mathcal{D}$ given by

$$\mathcal{D}(\mathbf{x}, \mathbf{y}, \mathbf{z}) = \mathcal{C}(\mathbf{Ax}, \mathbf{By}, \mathbf{Tz})$$

Tensor transformations

We can transform tensors by applying linear transformations to its arguments

$(\mathbf{A}, \mathbf{B}, \mathbf{T}) \in \mathrm{GL}_n(q) \times \mathrm{GL}_m(q) \times \mathrm{GL}_k(q)$ maps a tensor $\mathcal{C}$ to a tensor $\mathcal{D}$ given by

$$\mathcal{D}(\mathbf{x}, \mathbf{y}, \mathbf{z}) = \mathcal{C}(\mathbf{Ax}, \mathbf{By}, \mathbf{Tz})$$

This is a group action of $\mathrm{GL}_n(q) \times \mathrm{GL}_m(q) \times \mathrm{GL}_k(q)$ on the space of tensors

Tensor transformations

We can transform tensors by applying linear transformations to its arguments

$(\mathbf{A}, \mathbf{B}, \mathbf{T}) \in \mathrm{GL}_n(q) \times \mathrm{GL}_m(q) \times \mathrm{GL}_k(q)$ maps a tensor $\mathcal{C}$ to a tensor $\mathcal{D}$ given by

$$\mathcal{D}(\mathbf{x}, \mathbf{y}, \mathbf{z}) = \mathcal{C}(\mathbf{Ax}, \mathbf{By}, \mathbf{Tz})$$

This is a group action of $\mathrm{GL}_n(q) \times \mathrm{GL}_m(q) \times \mathrm{GL}_k(q)$ on the space of tensors

Two tensors are isomorphic if they are in the same orbit

3-TI (n, m, k, q)

Let $\mathcal{C}, \mathcal{D}$ be two $n \times m \times k$ tensors over $\mathbb{F}_q$. The 3-TI problem asks to find, if any exists, a triplet of matrices $\mathbf{A}, \mathbf{B}, \mathbf{T} \in \mathrm{GL}_n(q) \times \mathrm{GL}_m(q) \times \mathrm{GL}_k(q)$ such that:

$$\mathcal{C}(\mathbf{Ax}, \mathbf{By}, \mathbf{Tz}) = \mathcal{D}(\mathbf{x}, \mathbf{y}, \mathbf{z}) \qquad \forall\, \mathbf{x} \in \mathbb{F}_q^n, \mathbf{y} \in \mathbb{F}_q^m, \mathbf{z} \in \mathbb{F}_q^k$$

Variants

We can consider just a subset of structured tensors, for example, alternating tensors

Variants

We can consider just a subset of structured tensors, for example, alternating tensors

Alternating trilinear forms are $n \times n \times n$ tensors ϕ such that

$$\phi(\mathbf{x}, \mathbf{x}, -) = \phi(\mathbf{x}, -, \mathbf{x}) = \phi(-, \mathbf{x}, \mathbf{x}) = \mathbf{0}$$
$$\phi(\mathbf{x}, \mathbf{y}, -) = -\phi(\mathbf{y}, \mathbf{x}, -) \quad \text{and} \quad \phi(\mathbf{x}, -, \mathbf{z}) = -\phi(\mathbf{z}, -, \mathbf{x})$$

Variants

We can consider just a subset of structured tensors, for example, alternating tensors

Alternating trilinear forms are $n \times n \times n$ tensors ϕ such that

$$\phi(\mathbf{x}, \mathbf{x}, -) = \phi(\mathbf{x}, -, \mathbf{x}) = \phi(-, \mathbf{x}, \mathbf{x}) = \mathbf{0}$$
$$\phi(\mathbf{x}, \mathbf{y}, -) = -\phi(\mathbf{y}, \mathbf{x}, -) \quad \text{and} \quad \phi(\mathbf{x}, -, \mathbf{z}) = -\phi(\mathbf{z}, -, \mathbf{x})$$

This imposes additional constraints on transformations $\mathbf{A}, \mathbf{B}, \mathbf{T}$

The TI variants

	Tensor constraint $\forall\ i, j, k$	**Matrix constraint (induced)**	**Equivalent problem**	**Used in**
Unstructured	-	-	MCE	MEDS
Alternating	$\mathcal{C}_{ijk} = -\mathcal{C}_{jik}$ $\mathcal{C}_{ijk} = -\mathcal{C}_{kji}$	$\mathbf{A} = \mathbf{B} = \mathbf{T}$	ATFE	ALTEQ

The TI variants (extended)

	Tensor constraint $\forall\ i,j,k$	**Matrix constraint (induced)**	**Equivalent problem**
Unstructured	-	-	MCE
Alternating	$\mathcal{C}_{ijk} = -\mathcal{C}_{jik}$ $\mathcal{C}_{ijk} = -\mathcal{C}_{kji}$	$\mathbf{A} = \mathbf{B} = \mathbf{T}$	ATFE
Symmetric	$\mathcal{C}_{ijk} = \mathcal{C}_{jik}$ $\mathcal{C}_{ijk} = \mathcal{C}_{kji}$	$\mathbf{A} = \mathbf{B} = \mathbf{T}$	Cubic-IP
Partial Symmetric	$\mathcal{C}_{ijk} = \mathcal{C}_{jik}$	$\mathbf{A} = \mathbf{B}$	QMLE

Algorithms for solving TI

Overview

Prior work:

- Algebraic modeling
- Collision-based
- Graph-based

Overview

Prior work:

- Algebraic modeling
- Collision-based
- Graph-based

This work:

- Subgraph collision

Collisions

Elements $\mathbf{x}, \mathbf{x}' \in \mathbb{F}_q^n$ are a collision for $\mathbf{A}$ when

$$\mathbf{A}\mathbf{x} = \mathbf{x}'$$

This provides us linear relations for $\mathbf{A}$

Collisions

Elements $\mathbf{x}, \mathbf{x}' \in \mathbb{F}_q^n$ are a collision for $\mathbf{A}$ when

$$\mathbf{A}\mathbf{x} = \mathbf{x}'$$

This provides us linear relations for $\mathbf{A}$

Also yields quadratic equations

$$\mathcal{C}(\mathbf{x}', \mathbf{B}\mathbf{y}, \mathbf{T}\mathbf{z}) = \mathcal{D}(\mathbf{x}, \mathbf{y}, \mathbf{z})$$

Two Collisions

From two collisions $(\mathbf{x}_1, \mathbf{x}'_1)$ and $(\mathbf{x}_2, \mathbf{x}'_2)$ for $\mathbf{A}$ we obtain

$$\mathcal{C}(\mathbf{x}'_1, \mathbf{B}\mathbf{y}, \mathbf{z}) = \mathcal{D}(\mathbf{x}_1, \mathbf{y}, \mathbf{T}^{-1}\mathbf{z})$$
$$\mathcal{C}(\mathbf{x}'_2, \mathbf{B}\mathbf{y}, \mathbf{z}) = \mathcal{D}(\mathbf{x}_2, \mathbf{y}, \mathbf{T}^{-1}\mathbf{z})$$

Two Collisions

From two collisions $(\mathbf{x}_1, \mathbf{x}'_1)$ and $(\mathbf{x}_2, \mathbf{x}'_2)$ for $\mathbf{A}$ we obtain

$$\mathcal{C}(\mathbf{x}'_1, \mathbf{B}\mathbf{y}, \mathbf{z}) = \mathcal{D}(\mathbf{x}_1, \mathbf{y}, \mathbf{T}^{-1}\mathbf{z})$$
$$\mathcal{C}(\mathbf{x}'_2, \mathbf{B}\mathbf{y}, \mathbf{z}) = \mathcal{D}(\mathbf{x}_2, \mathbf{y}, \mathbf{T}^{-1}\mathbf{z})$$

This yields $2mk$ linear equations in $m^2 + k^2$ variables

The tensor-graph

To each $n \times m \times k$ tensor $\mathcal{C}$ over $\mathbb{F}_q$, we can associate a graph

The tensor-graph

To each $n \times m \times k$ tensor $\mathcal{C}$ over $\mathbb{F}_q$, we can associate a graph

$$\begin{aligned}
\mathcal{V}_{\mathcal{C}} =& \mathbb{P}(\mathbb{F}_q^n) \cup \mathbb{P}(\mathbb{F}_q^m) \cup \mathbb{P}(\mathbb{F}_q^k) \\
\mathcal{E}_{\mathcal{C}} =& \{(\mathbf{x}, \mathbf{y}) \in \mathbb{P}(\mathbb{F}_q^n) \times \mathbb{P}(\mathbb{F}_q^m) \mid \mathcal{C}(\mathbf{x}, \mathbf{y}, -) = \mathbf{0}\} \\
& \cup \{(\mathbf{x}, \mathbf{z}) \in \mathbb{P}(\mathbb{F}_q^n) \times \mathbb{P}(\mathbb{F}_q^k) \mid \mathcal{C}(\mathbf{x}, -, \mathbf{z}) = \mathbf{0}\} \\
& \cup \{(\mathbf{y}, \mathbf{z}) \in \mathbb{P}(\mathbb{F}_q^m) \times \mathbb{P}(\mathbb{F}_q^k) \mid \mathcal{C}(-, \mathbf{y}, \mathbf{z}) = \mathbf{0}\}
\end{aligned}$$

The tensor-graph

To each $n \times m \times k$ tensor $\mathcal{C}$ over $\mathbb{F}_q$, we can associate a graph

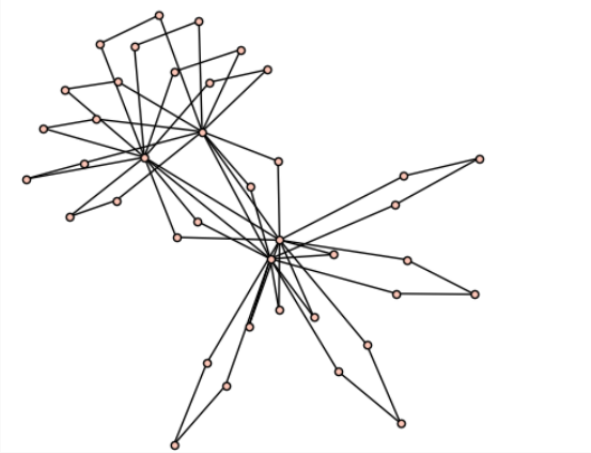
$$\begin{aligned}
\mathcal{V}_{\mathcal{C}} =& \mathbb{P}(\mathbb{F}_q^n) \cup \mathbb{P}(\mathbb{F}_q^m) \cup \mathbb{P}(\mathbb{F}_q^k) \\
\mathcal{E}_{\mathcal{C}} =& \{(\mathbf{x}, \mathbf{y}) \in \mathbb{P}(\mathbb{F}_q^n) \times \mathbb{P}(\mathbb{F}_q^m) \mid \mathcal{C}(\mathbf{x}, \mathbf{y}, -) = \mathbf{0}\} \\
& \cup \{(\mathbf{x}, \mathbf{z}) \in \mathbb{P}(\mathbb{F}_q^n) \times \mathbb{P}(\mathbb{F}_q^k) \mid \mathcal{C}(\mathbf{x}, -, \mathbf{z}) = \mathbf{0}\} \\
& \cup \{(\mathbf{y}, \mathbf{z}) \in \mathbb{P}(\mathbb{F}_q^m) \times \mathbb{P}(\mathbb{F}_q^k) \mid \mathcal{C}(-, \mathbf{y}, \mathbf{z}) = \mathbf{0}\}
\end{aligned}$$

Note:

- This is a tripartite graph
- It has $q^{n-1} + q^{m-1} + q^{k-1}$ vertices!

Tensor graph: an example

$$\mathcal{C} : \mathbb{F}_5^3 \times \mathbb{F}_5^3 \times \mathbb{F}_5^3 \to \mathbb{F}_5$$



Tensor-graph isomorphism

A tensor isomorphism $(\mathbf{A}, \mathbf{B}, \mathbf{T}) : \mathcal{C} \to \mathcal{D}$ induces a graph isomorphism

$$\mathcal{V}_{\mathcal{D}} \to \mathcal{V}_{\mathcal{C}}$$

$$v \mapsto \begin{cases} \mathbf{A}v & \text{if } v \in \mathbb{P}(\mathbb{F}_q^n) \\ \mathbf{B}v & \text{if } v \in \mathbb{P}(\mathbb{F}_q^m) \\ \mathbf{T}v & \text{if } v \in \mathbb{P}(\mathbb{F}_q^k) \end{cases}$$

Tensor-graph isomorphism

A tensor isomorphism $(\mathbf{A}, \mathbf{B}, \mathbf{T}) : \mathcal{C} \to \mathcal{D}$ induces a graph isomorphism

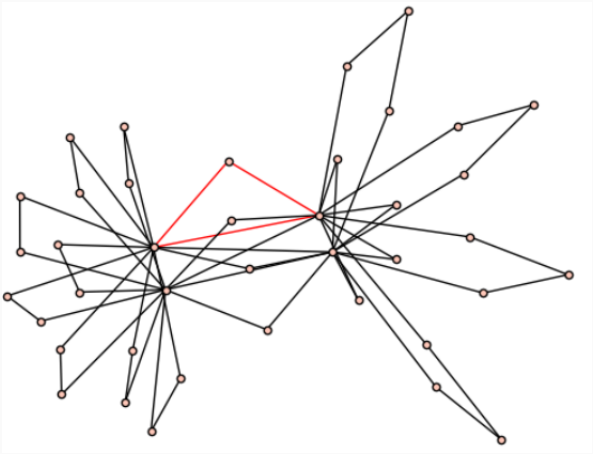
$$\mathcal{V}_{\mathcal{D}} \to \mathcal{V}_{\mathcal{C}}$$

$$v \mapsto \begin{cases} \mathbf{A}v & \text{if } v \in \mathbb{P}(\mathbb{F}_q^n) \\ \mathbf{B}v & \text{if } v \in \mathbb{P}(\mathbb{F}_q^m) \\ \mathbf{T}v & \text{if } v \in \mathbb{P}(\mathbb{F}_q^k) \end{cases}$$

$$\mathbf{0} = \mathcal{D}(\mathbf{x}, \mathbf{y}, -) = \mathcal{C}(\mathbf{A}\mathbf{x}, \mathbf{B}\mathbf{y}, -)$$

A new invariant: Triangles

Example



Definition

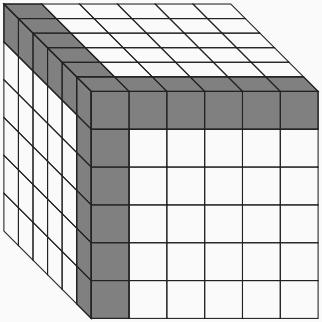
Let $\mathcal{C}$ be a $n \times m \times k$ tensor over $\mathbb{F}_q$.

A *triangle* for $\mathcal{C}$ is a triplet $(\mathbf{u}, \mathbf{v}, \mathbf{w}) \in \mathbb{P}(\mathbb{F}_q^n) \times \mathbb{P}(\mathbb{F}_q^m) \times \mathbb{P}(\mathbb{F}_q^k)$ such that

$$\mathcal{C}(\mathbf{u}, \mathbf{v}, -) = \mathcal{C}(\mathbf{u}, -, \mathbf{w}) = \mathcal{C}(-, \mathbf{v}, \mathbf{w}) = \mathbf{0}.$$

Probability of triangle (e_1, e_1, e_1)

For a tensor $6 \times 6 \times 6$ tensor $\mathcal{C}$, the coefficients in the gray positions should be zero for $(\mathbf{e}_1, \mathbf{e}_1, \mathbf{e}_1)$ to be a triangle.



Probability of any triangle

Intuitively:

- $(n-1)+(m-1)+(k-1)$ degrees of freedom
- $n+m+k-2$ constraints (gray cells)

Probability of any triangle

Intuitively:

- $(n-1)+(m-1)+(k-1)$ degrees of freedom
- $n+m+k-2$ constraints (gray cells)

Rigorously:

$$\frac{1}{q} - \mathcal{O}(q^{-2}) \leq \mathbb{P}_{\mathcal{C}}(\mathcal{C} \text{ has a unique triangle}) \leq \frac{1}{q} + \mathcal{O}(q^{-2})$$

Using the new invariant

Overview of the algorithm

(1) Find a triangle for $\mathcal{C}$ if it exists (probability $1/q$)

(2) If so, find the triangle for $\mathcal{D}$

(3) Add the 3-point collision to the algebraic model

(4) Solve!

An algebraic approach

We work in the polynomial ring $\mathbb{F}_q[x_2, \ldots, x_n, y_2, \ldots, y_m, z_2, \ldots, z_k]$ and denote

$$\mathbf{x} = [1, x_2, \ldots, x_n] \qquad \mathbf{y} = [1, y_2, \ldots, y_m] \qquad \mathbf{z} = [1, z_2, \ldots, z_k]$$

We work in the polynomial ring $\mathbb{F}_q[x_2, \ldots, x_n, y_2, \ldots, y_m, z_2, \ldots, z_k]$ and denote

$$\mathbf{x} = [1, x_2, \ldots, x_n] \qquad \mathbf{y} = [1, y_2, \ldots, y_m] \qquad \mathbf{z} = [1, z_2, \ldots, z_k]$$

Then look for solutions of the following system:

$$\begin{cases} \mathcal{C}(\mathbf{x}, \mathbf{y}, \mathbf{e}_i) = 0 & \text{for } 1 \leq i \leq k \\ \mathcal{C}(\mathbf{x}, \mathbf{e}_i, \mathbf{z}) = 0 & \text{for } 1 \leq i \leq m \\ \mathcal{C}(\mathbf{e}_i, \mathbf{y}, \mathbf{z}) = 0 & \text{for } 1 \leq i \leq n \end{cases}$$

An algebraic approach

We work in the polynomial ring $\mathbb{F}_q[x_2, \ldots, x_n, y_2, \ldots, y_m, z_2, \ldots, z_k]$ and denote

$$\mathbf{x} = [1, x_2, \ldots, x_n] \qquad \mathbf{y} = [1, y_2, \ldots, y_m] \qquad \mathbf{z} = [1, z_2, \ldots, z_k]$$

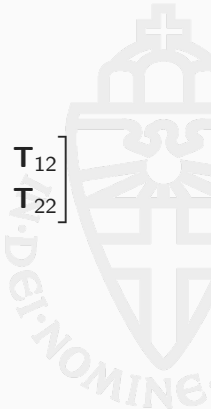
Then look for solutions of the following system:

$$\begin{cases} \mathcal{C}(\mathbf{x}, \mathbf{y}, \mathbf{e}_i) = 0 & \text{for } 1 \leq i \leq k \\ \mathcal{C}(\mathbf{x}, \mathbf{e}_i, \mathbf{z}) = 0 & \text{for } 1 \leq i \leq m \\ \mathcal{C}(\mathbf{e}_i, \mathbf{y}, \mathbf{z}) = 0 & \text{for } 1 \leq i \leq n \end{cases}$$

Solve this using tri-graded XL

The 3-point collision yields the following constraints on $\mathbf{A}, \mathbf{B}, \mathbf{T}$:

$$\mathbf{A} = \begin{bmatrix} \lambda & \mathbf{A}_{12} \\ \mathbf{0}_{(n-1)\times 1} & \mathbf{A}_{22} \end{bmatrix} \qquad \mathbf{B} = \begin{bmatrix} 1 & \mathbf{B}_{12} \\ \mathbf{0}_{(n-1)\times 1} & \mathbf{B}_{22} \end{bmatrix} \qquad \mathbf{T} = \begin{bmatrix} 1 & \mathbf{T}_{12} \\ \mathbf{0}_{(n-1)\times 1} & \mathbf{T}_{22} \end{bmatrix}$$

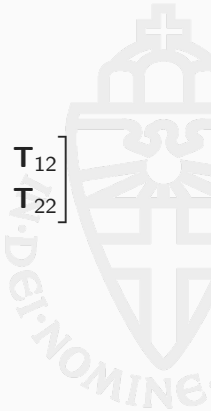


Using triangles

The 3-point collision yields the following constraints on $\mathbf{A}, \mathbf{B}, \mathbf{T}$:

$$\mathbf{A} = \begin{bmatrix} \lambda & \mathbf{A}_{12} \\ \mathbf{0}_{(n-1)\times 1} & \mathbf{A}_{22} \end{bmatrix} \qquad \mathbf{B} = \begin{bmatrix} 1 & \mathbf{B}_{12} \\ \mathbf{0}_{(n-1)\times 1} & \mathbf{B}_{22} \end{bmatrix} \qquad \mathbf{T} = \begin{bmatrix} 1 & \mathbf{T}_{12} \\ \mathbf{0}_{(n-1)\times 1} & \mathbf{T}_{22} \end{bmatrix}$$

Empirically, the resulting system was linearizable in degree 2



Triangles for ATFE

What is a triangle

Our previous definition no longer works

Recall $\phi(\mathbf{x}, \mathbf{x}, -) = \phi(\mathbf{x}, -, \mathbf{x}) = \phi(-, \mathbf{x}, \mathbf{x}) = \mathbf{0}$

Any triple $(\mathbf{v}, \mathbf{v}, \mathbf{v})$ would be a triangle!

What is a triangle

Our previous definition no longer works

Recall $\phi(\mathbf{x}, \mathbf{x}, -) = \phi(\mathbf{x}, -, \mathbf{x}) = \phi(-, \mathbf{x}, \mathbf{x}) = \mathbf{0}$

Any triple $(\mathbf{v}, \mathbf{v}, \mathbf{v})$ would be a triangle!

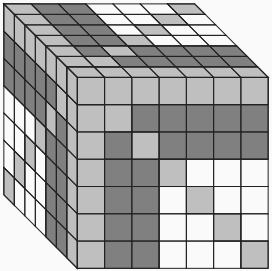
Definition

Let ϕ be an alternating trilinear form over $\mathbb{F}_q$.
A triangle for ϕ is a 3-dimensional subspace $T \in \mathbb{F}_q^n$ such that

$$\phi(\mathbf{v}, \mathbf{w}, -) = 0 \quad \forall\, \mathbf{v}, \mathbf{w} \in T.$$

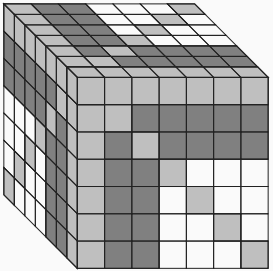
Probability of triangle $\langle e_1, e_2, e_3 \rangle$

For an ATF ϕ, the coefficients in the dark gray positions should be zero for $\langle \mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3 \rangle$ to be a triangle. The coefficients in the light gray positions are zero by alternatingness



Probability of triangle $\langle e_1, e_2, e_3 \rangle$

For an ATF ϕ, the coefficients in the dark gray positions should be zero for $\langle \mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3 \rangle$ to be a triangle. The coefficients in the light gray positions are zero by alternatingness



For sufficiently high n (≥ 9) we again have

$$\frac{1}{q} - \mathcal{O}(q^{-2}) \leq \mathbb{P}_\phi(\phi \text{ has a unique triangle}) \leq \frac{1}{q} + \mathcal{O}(q^{-2})$$

Finding the triangle algebraically

Work in the ring $\mathbb{F}_q[x_4, \ldots, x_n, y_4, \ldots, y_n, z_4, \ldots, z_n]$ and denote

$$\mathbf{x} = [1, 0, 0, x_4, \ldots, x_n] \qquad \mathbf{y} = [0, 1, 0, y_4, \ldots, y_n] \qquad \mathbf{z} = [0, 0, 1, z_4, \ldots, z_n]$$

Finding the triangle algebraically

Work in the ring $\mathbb{F}_q[x_4, \ldots, x_n, y_4, \ldots, y_n, z_4, \ldots, z_n]$ and denote

$$\mathbf{x} = [1, 0, 0, x_4, \ldots, x_n] \qquad \mathbf{y} = [0, 1, 0, y_4, \ldots, y_n] \qquad \mathbf{z} = [0, 0, 1, z_4, \ldots, z_n]$$

Now, our system for finding a triangle looks as follows:

$$\begin{cases} \phi(\mathbf{x}, \mathbf{y}, \mathbf{e}_i) = 0 \\ \phi(\mathbf{y}, \mathbf{z}, \mathbf{e}_i) = 0 \\ \phi(\mathbf{z}, \mathbf{x}, \mathbf{e}_i) = 0 \end{cases} \qquad \forall 1 \leq i \leq n$$

We solve using tri-graded XL again

Better than predicted

		Actual		Predicted	
n	Time	Memory	d_{solv}	$\mathbf{d}_{reg}$	$\mathbf{d}_{ff}$
12	29 s	96 MB	4	11	8
13	490 s	850 MB	4	12	9
14	30 h	29 GB	5	13	10

Using the triangle

This is no longer a 3-point collision!

Using the triangle

This is no longer a 3-point collision!

For the alternating variant we get the following constraint on $\mathbf{A}$ instead:

$$\mathbf{A} = \begin{bmatrix} \mathbf{A}_{11} & \mathbf{A}_{12} \\ \mathbf{0}_{(n-3)\times 3} & \mathbf{A}_{22} \end{bmatrix}$$

Solving this system took at most 3 hours for all security levels

Complexity results

MEDS

The $\log_2$ complexity estimates for solving MCE (with probability $1/q$) in field operations. The parameters are taken from the MEDS specifications. We use the solving degree as an estimator here.

	n	q	Specs	Best previous[1]	**This work** (prob $1/q$)
Level I	14	4093	147	95	90
Level III	22	4093	217	145	143
Level V	30	2039	276	180	197

[1] "Algorithms for matrix code and alternating trilinear form equivalences via new isomorphism invariants." by A. K. Narayanan, Y. Qiao, and G. Tang

The $\log_2$ complexity for solving ATFE (with probability $1/q$) in field operations. The parameters are taken from the ALTEQ specifications. We use the solving degree as an estimator here. In all cases $q = 2^{32} - 5$.

	n	Specs	Best previous[2]	**This work** (prob $1/q$)	practical
Level I	13	143	120	62	**1501 s**
Level III	20	219	165	108	
Level V	25	276	203	141	

[2] "Algebraic algorithm for the alternating trilinear form equivalence problem." by L. Ran, S. Samardjiska, and M. Trimoska

Thanks for listening!

Bonus slides

MCE:

$$\mathcal{H}(r,s,t) = \frac{(1-rs)^k(1-rt)^m(1-st)^n(1-rst)^{-2}}{(1-r)^{n-1}(1-s)^{m-1}(1-t)^{k-1}}$$

ATFE:

$$\mathcal{S}(r,s,t) = (1-r^2s)(1-rs^2)(1-s^2t)(1-st^2)(1-t^2r)(1-tr^2)(1-rst)^2$$

$$\mathcal{H}(r,s,t) = \frac{(1-rs)^n(1-rt)^n(1-st)^n}{(1-r)^{n-2}(1-s)^{n-2}(1-t)^{n-2}} \cdot \mathcal{S}^{-1}$$

Tri-degree experiments MCE

	Tri-degree						
(n, m, k)	(1, 1, 1)	(2, 1, 1)	(3, 1, 1)	(2, 2, 1)	(4, 1, 1)	(3, 2, 1)	(2, 2, 2)
(7,7,7)	2	61	336	772	1141	—	—
(8,8,8)	2	78	504	1174	1960	6356	11601
(9,9,9)	2	97	720	1694	3156	10512	
(8,7,7)	2	63	399	882	1540	4599/4620	7969/8064
(9,8,8)	2	80	584	1316	2544	7896	13907

Tri-degree experiments ATFE

	Tri-degree								
n	(2, 2, 0)	(2, 1, 1)	(4, 1, 0)	(3, 2, 0)	(3, 1, 1)	(2, 2, 1)	(5, 1, 0)	(4, 2, 0)	(3, 3, 0)
12	86	184	55	803	1726	4002	220/221	4281/4282	7241/7242
13	100	213	66	1032	2207	5140	286/287	6018/6019	10319/10320
14	115	244	78	1300	2768	6472	364	8231	14277
15	131	277	91	1610	3415	8013	455	10999	
16	148	312	105	1965	4154	9778	560		
17	166	349	120	2368	4991				
18	185	388	136	2822	5932				
19	205	429	153	3330					
20	226	472	171	3895					