Practical Post-Quantum Signature Schemes from Isomorphism Problems of Trilinear Forms

Gang Tang[1], Dung Hoang Duong[2], Antoine Joux[3], Thomas Plantard[4]
Youming Qiao[1], Willy Susilo[2]

[1]University of Technology Sydney
[2]University of Wollongong
[3]CISPA

[4]PayPal

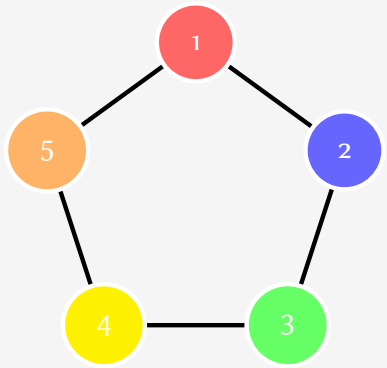
3 June, 2022

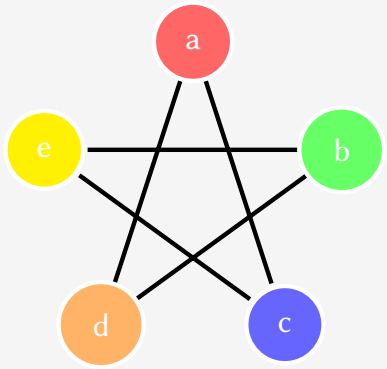
Contents

Contents

Graph isomorphism problem

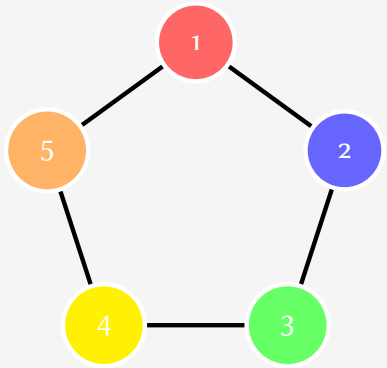
- The classical graph isomorphism problem (GraphIso) asks whether two graphs are the same up to relabelling the vertices.
- Let $G = ([n], E)$ and $H = ([n], F)$, where $[n]$ denotes $\{1, 2, \ldots, n\}$.

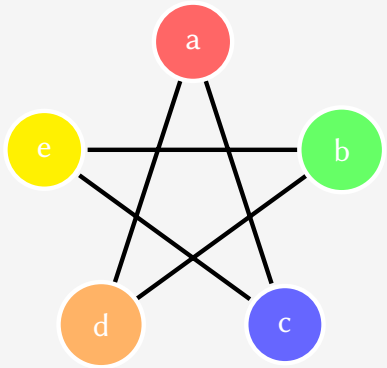




Graph isomorphism problem

- The classical graph isomorphism problem (GraphIso) asks whether two graphs are the same up to relabelling the vertices.
- Let $G = ([n], E)$ and $H = ([n], F)$, where $[n]$ denotes $\{1, 2, ..., n\}$.
- G and H are isomorphic iff. $\sigma : [n] \to [n] (\sigma \in S_n)$ st. $\sigma(E) = F$.
- $\sigma(E) = F$ means that for any $\{i, j\} \in E$ iff. $\{\sigma(i), \sigma(j)\} \in F$.





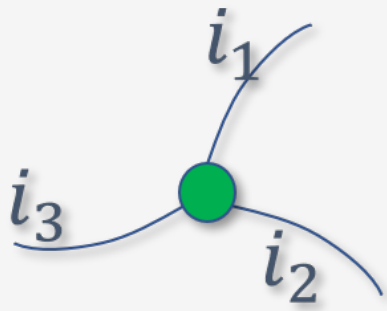
Tensors

- Tensors are multiway arrays.
- Matrices are 2-way arrays (i.e. $d = 2$).

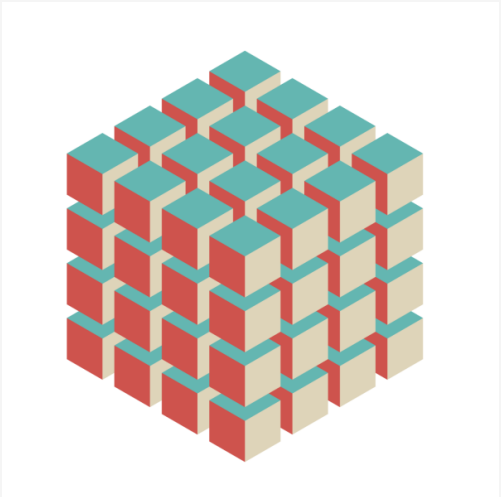
Tensors

- Tensors are multiway arrays.
- Matrices are 2-way arrays (i.e. $d = 2$).
- In this talk we focus on 3-way arrays, or 3-tensors.
- That is, $A = (a_{i,j,k})$, $a_{i,j,k} \in \mathbb{F}$, $i, j, k \in [n]$.

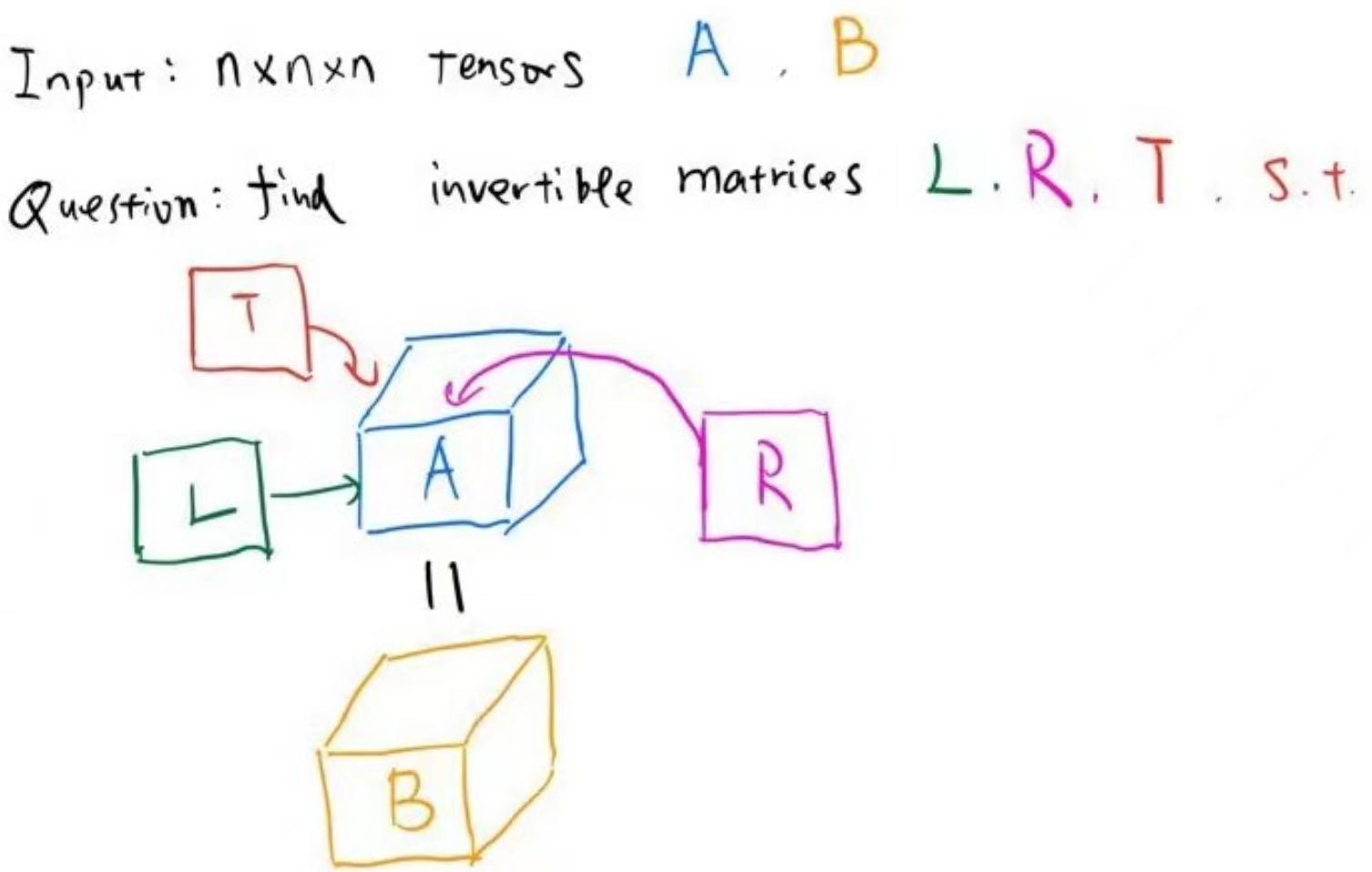
Tensors



- Tensors are multiway arrays.
- Matrices are 2-way arrays (i.e. $d = 2$).
- In this talk we focus on 3-way arrays, or 3-tensors.
- That is, $A = (a_{i,j,k})$, $a_{i,j,k} \in \mathbb{F}$, $i, j, k \in [n]$.



Tensor isomorphism



Digital signature based on isomorphism problems

- There is a digital signature design based on isomorphism problems.
  - Studied in multivariate cryptography and isogeny cryptography.

Digital signature based on isomorphism problems

- There is a digital signature design based on isomorphism problems.
  - Studied in multivariate cryptography and isogeny cryptography.
- It has a clear, 2-step, structure
  - Identification scheme based on Goldreich-Micali-Wigderson (J. ACM'91) zero-knowledge protocol for graph isomorphism.
  - Use Fiat-Shamir transformation (Crypto'86) to turn the above ID scheme to a digital signature.

Step 1: an identification scheme

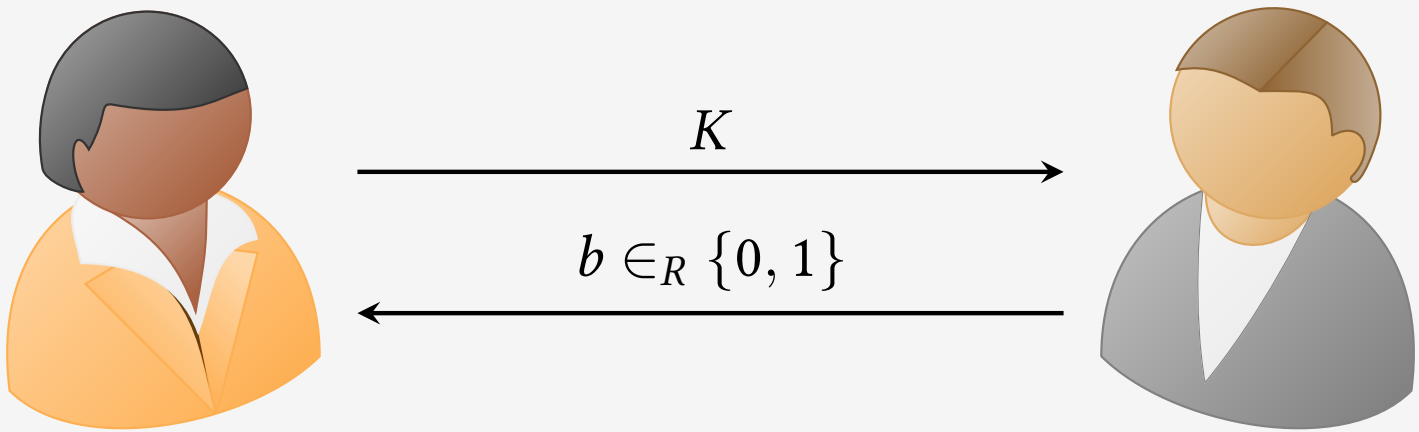
- A zero-knowledge interactive protocol for graph isomorphism.
- Two players: Prover and Verifier. They are given two graphs, G and H.
- If G and H are isomorphic, (honest) Prover knows an isomorphism.
- Prover's goal: demonstrate that she knows the isomorphism, without revealing it to Verifier.
- Verifier's goals:
  - Completeness: If G and H are isomorphic and Prover knows the isomorphism, he always accepts.
  - Soundness: If G and H are not isomorphic or Prover does not know the isomorphism, he rejects with non-negligible probability.

GMW zero-knowledge protocol for GraphIso

- Given two graphs G and H as public key, let σ be an isomorphism as secret key such that $\sigma(G) = H$.
- Alice generates a random permutation π which sends G to $K = \pi(G)$.

GMW zero-knowledge protocol for GraphIso

- Given two graphs G and H as public key, let σ be an isomorphism as secret key such that $\sigma(G) = H$.
- Alice generates a random permutation π which sends G to $K = \pi(G)$.



- If $b = 0$, Alice sends $r := \pi$ to Bob; Otherwise sends $r := \pi\sigma^{-1}$.
- If $b = 0$, Bob checks whether $r(G) = K$; Otherwise checks $r(H) = K$.

Step 2: from ID scheme to digital signature

- Fiat and Shamir proposed a method that takes an identification scheme and turns it to a digital signature.
- Key idea: use a hash function to simulate the interaction process.
- The ID scheme based on isomorphism problems fits this method.
- Security proved in:
  - The Random Oracle Access model (Pointcheval-Stern, 1996).
  - The Quantum Oracle Access model (Don-Fehr-Majenz-Schaffner, Liu-Zhandry, 2019).

GraphIso not good?

- More generally, an *isomorphism testing* problem asks whether two combinatorial or algebraic objects are essentially the same.
- Besides graphs, isomorphism testing problems for groups, algebras, lattices, and linear codes have also been studied.

GraphIso not good?

- More generally, an *isomorphism testing* problem asks whether two combinatorial or algebraic objects are essentially the same.
- Besides graphs, isomorphism testing problems for groups, algebras, lattices, and linear codes have also been studied.
- GraphIso is now an easy problem, both in theory [Babai] and in practice [McKay-Piperno].

GraphIso not good?

- More generally, an *isomorphism testing* problem asks whether two combinatorial or algebraic objects are essentially the same.
- Besides graphs, isomorphism testing problems for groups, algebras, lattices, and linear codes have also been studied.
- GraphIso is now an easy problem, both in theory [Babai] and in practice [McKay-Piperno].

Question

Can we rescue this framework (GMW+FS) to other isomorphism problems?

GMW+FS framework for the Polynomial Isomorphism

- Patarin suggested to replace graph isomorphism with polynomial isomorphism in Eurocrypt 1996.
  - In particular, he suggested the digital signature scheme as we described.
- Polynomial isomorphism is a family of problems
  - Depending on the degrees, number of polynomials, etc.
  - Some problems, such as the isomorphism of quadratic polynomials with one secret, turn out to be easy [Bouillaguet-Faugère-Fouque-Perret, Faugère-Perret, Ivanyos-Qiao].
- It gives rise to a series of works in multivariate cryptography.
  - [PGC98,GMS03,Per05,FP06,Kay11,BFFP11,MPG13,BFV13,PFM14,BFP15...].

The schemes in Isogeny-based Cryptography

- Couveignes first proposed the use of class group actions on elliptic curves in cryptography.
  - He adapted the GMW identification protocol to this action.
- Stolbunov suggested to apply the Fiat-Shamir transformation to this identification protocol to get a signature scheme.
  - However, the use of ordinary elliptic curves has issues including the subexponential-time quantum algorithm [Childs-Jao-Soukharev] and the slow performance.
- The attention then turned to supersingular elliptic curves [De Feo-Jao-Plût, Castryck-Lange-Martindale-Panne-Renes].
- This leads to some progress on signature scheme recently [Beullens-Kleinjung-Vercauteren, Kaafarani-Katsumata-Pintore, De Feo-Galbraith].

TensorIso in post-quantum cryptography

- In post-quantum cryptography, we wish to devise cryptographic protocols that are hopeful to resist attacks by quantum computers.
- This requires to utilise *limitations of quantum algorithms*.

TensorIso in post-quantum cryptography

- In post-quantum cryptography, we wish to devise cryptographic protocols that are hopeful to resist attacks by quantum computers.
- This requires to utilise *limitations of quantum algorithms*.
- A natural development of Shor's quantum algorithms for integer factorisation and discrete logarithm is the hidden subgroup problem framework.
- One key reason for utilising lattice problems in post-quantum cryptography lies in the connection with the dihedral hidden subgroup problem [Regev].
- Similarly, a key reason for utilising TensorIso lies in the connection with the hidden subgroup problem for general linear groups, for which there exists strong negative evidence for the current techniques to work [Hallgren-Moore-Rötteler-Russell-Sen].

TensorIso in post-quantum cryptography

- In post-quantum cryptography, we wish to devise cryptographic protocols that are hopeful to resist attacks by quantum computers.
- This requires to utilise *limitations of quantum algorithms*.
- A natural development of Shor's quantum algorithms for integer factorisation and discrete logarithm is the hidden subgroup problem framework.
- One key reason for utilising lattice problems in post-quantum cryptography lies in the connection with the dihedral hidden subgroup problem [Regev].
- Similarly, a key reason for utilising TensorIso lies in the connection with the hidden subgroup problem for general linear groups, for which there exists strong negative evidence for the current techniques to work [Hallgren-Moore-Rötteler-Russell-Sen].

  [Moore-Russell-Vazirani] . . . consequences of the strongest such insights we have about the limits of quantum algorithms.

Contents

Currently the best algorithms for GraphIso and TensorIso

	Graphs with n vertices	$n \times n \times n$ tensors over $\mathbb{F}_q$
Brute-force algorithms		
Worst-case algorithms		
Average-case algorithms		
Practical algorithms		

Currently the best algorithms for GraphIso and TensorIso

	Graphs with n vertices	$n \times n \times n$ tensors over $\mathbb{F}_q$
Brute-force algorithms	$n! \cdot \mathrm{poly}(n)$	
Worst-case algorithms	$n^{O((\log n)^2)}$ [Babai]	
Average-case algorithms	Linear time [Babai-Erdős-Selkow]	
Practical algorithms	$n > 10^6$ [McKay-Piperno]	

Currently the best algorithms for GraphIso and TensorIso

	Graphs with n vertices	$n \times n \times n$ tensors over $\mathbb{F}_q$
Brute-force algorithms	$n! \cdot \mathrm{poly}(n)$	$q^{n^2} \cdot \mathrm{poly}(n, \log q)$
Worst-case algorithms	$n^{O((\log n)^2)}$ [Babai]	$q^{\frac{1}{2}n^2+O(n)}$ [Li-Q]
Average-case algorithms	Linear time [Babai-Erdős-Selkow]	$q^{O(n)}$ [Li-Qiao], [Grochow-Qiao-T]
Practical algorithms	$n > 10^6$ [McKay-Piperno]	$n = 10, q = 11$ [Brooksbank-Maglione-Wilson]

If not Graph Iso, then which Iso?

Criteria for constructing a secure protocol:

- Practical complexity
- Theoretical complexity
- Well-studied

Tensor isomorphism satisfies all the above based on current evidences.

- In [Ji-Qiao-Song-Yun, TCC'19], it was proposed to use Tensor Isomorphism as the security basis for the GMW-FS framework.
- Based on advances on complexity and algorithms.
- Complexity side: [Grochow-Qiao, ITCS'21] proposed a complexity class Tensor Isomorphism.
- Algorithm side: based on many works in multivariate cryptography [Bouillaguet-Fouque-Véber] and some of works [Li-Qiao, FOCS'17]...

Contents

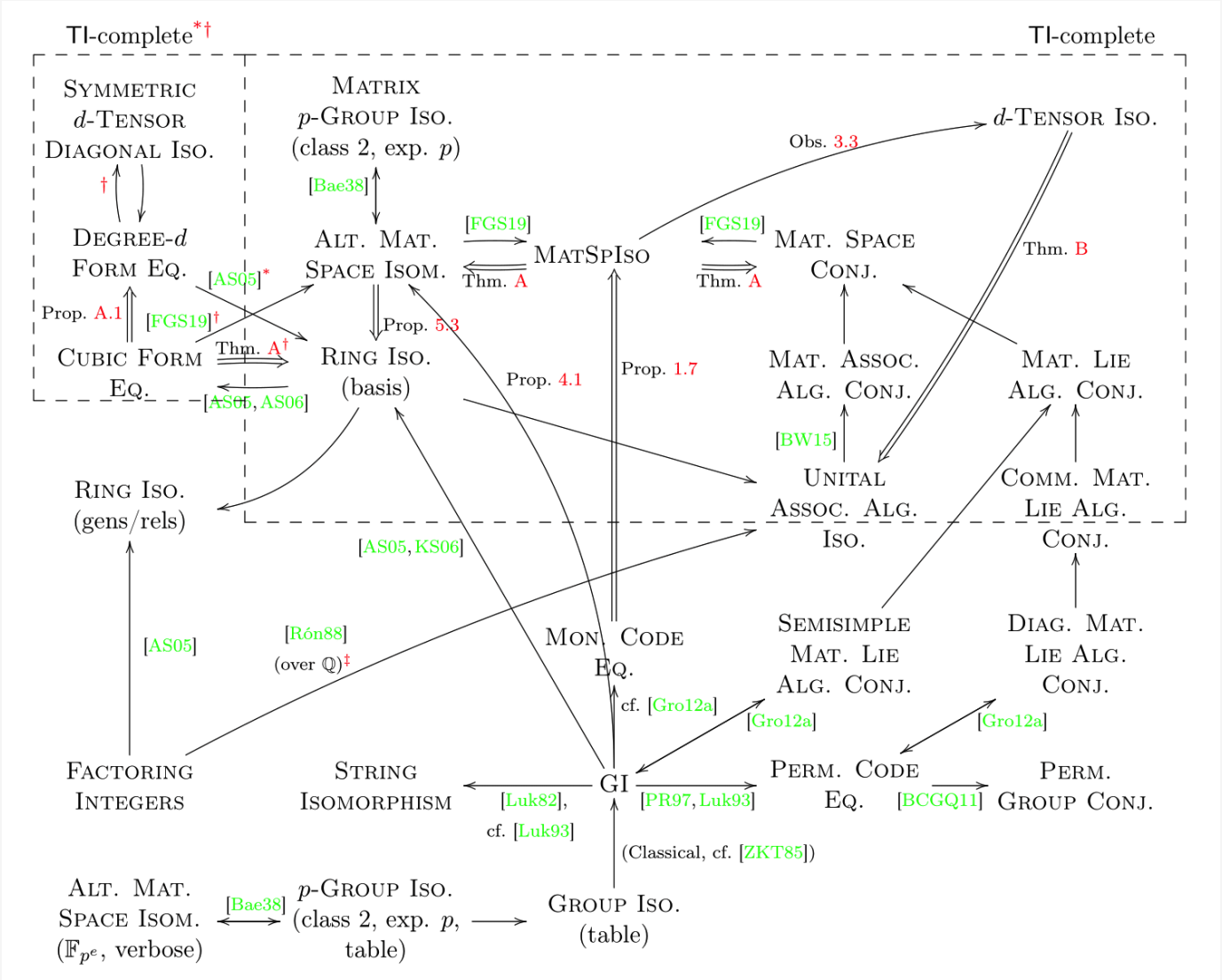
The complexity class TI-complete

Question

Can we make GMW+FS+TI practical?

- The complexity class GI-complete consists of problems that are polynomial-time equivalent to GraphIso.
- Analogously, [Grochow-Qiao] define a new complexity class TI-complete, consisting of problems that are polynomial-time equivalent to TensorIso.

The complexity class TI-complete



Alternating Trilinear Form

- Let $\mathrm{GL}(n, \mathbb{F}_q)$ be the general linear group consisting of $n \times n$ invertible matrices over $\mathbb{F}_q$
- ϕ is said to be 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 form 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.

Alternating Trilinear Form

Theorem ([Grochow-Qiao-T])

Alternating Trilinear Form Equivalence(ATFE) Problem is TI-complete (that is ATFE and TI are poly-time equivalence).

Motivations

- $n^3(\mathrm{TI}) \to \binom{n}{3}$ (ATFE).
  - i.e. $n = 9, n^3 = 729 \to \binom{n}{3} = \binom{9}{3} = 84$.

This is a big save in practice!

- A practical algorithm for ATFE [Bouillaguet-Fouque-Véber]: $q^{2/3n} \cdot poly(n \log q)$.

Attack based on Gröbner Basis

- Experimental results on Maple and Magma[1]
  - $n < 6$ very fast.
  - $n = 6, q = 5$ in about 700 seconds.
  - $n = 7, q = 5$ cannot achieve.
- Improved experimental (add more equations, guess some entries) results
  - $n < 8$ very fast.
  - Permit breaking $n = 8$.
  - $n = 9$ cannot achieve.
- It is reasonable to choose $n \geq 9$.

[1] Processor: 2.6 GHz 18-core Intel(R) Xeon(R) Gold 6132; Memory 87 GB

Parameter Choices of our Scheme

- λ denotes the security parameter.
- r denotes the number of round.
- 2^c denotes the number of alternating trilinear forms generated in each round.
- Estimations
  - $\frac{2}{3} \cdot n \cdot log_2(q) + 2\omega \cdot log_2(n) + log_2(\log_2(q)) \geq \lambda$
  - $r \cdot c \geq \lambda$
  - Here ω is the matrix multiplication exponent, and we take $\omega = 2$ for the sake of added security.
- PubKeySize $= 2^c \cdot \binom{n}{3} \cdot \lceil \log_2(q) \rceil / 8$.
- PriKeySize $= 2^c \cdot n^2 \cdot \lceil \log_2(q) \rceil / 8$.
- SigSize $= r \cdot (c + n^2 \cdot \lceil \log_2(q) \rceil) / 8$.

Benchmark of our Scheme

We have a prototype for GMW+FS+ATFE in C.

	q	n	r	c
Concrete Scheme 1	524287	9	26	5
Concrete Scheme 2	131071	10	26	5
Concrete Scheme 3	131071	10	32	4
Concrete Scheme 4	65521	11	26	5

Table: Parameters (r denotes the number of rounds, 2^c denotes the number of ATF be generated in each round.)

Benchmark of our Scheme

	Public key	Private key	Signature
Concrete Scheme 1	6384	6156	5018
Concrete Scheme 2	8160	6800	5542
Concrete Scheme 3	4080	3400	6816
Concrete Scheme 4	10560	7744	6309

Table: Output parameters for four concrete schemes based on ATFE for the 128-bit security. The sizes are measured in bytes.

	Key generation	Sign	Verify
Concrete Scheme 1	285.9	471.7	416.5
Concrete Scheme 2	383.1	660.0	578.9
Concrete Scheme 3	190.7	795.4	708.8
Concrete Scheme 4	514.0	861.1	765.2

Table: Running times (in microsecond, μs, averaged over 10^5 runs) on Linux 5.11.0-37-generic with Intel Core i7-8565U CPU (1.8GHz).

Contents

Summary

- Unlike GraphIso, ATFE seems to be a much harder problem both in theory and in practice.
- The hardness of ATFE can be explored to devise cryptographic protocols, especially in light of post-quantum cryptography.
- We propose a practical signature scheme based on ATFE.
- We analyze attacks on the Gröbner Basis.
- We choose parameters very carefully to balance and implement this scheme.

Thank you for your attention.

Questions please?