Algebraic Cryptanalysis of a Quantum Money Scheme
The Noise-Free Case

Marta Conde Pena[1] Jean-Charles Faugère[2,3,4] Ludovic Perret[3,2,4]

[1]Spanish National Research Council (CSIC)

[2]Sorbonne Universités, UPMC Univ Paris 06

[3]INRIA

[4]CNRS

Contents

Cash from a Classical vs Quantum Perspective

Classical Physics

In principle, it is impossible to make money uncopyable.

No-cloning Theorem in Quantum Mechanics

- An unknown quantum state cannot be cloned.
  - Can this be used to make unforgeable cash?

Quantum Money

S. Wiesner.
"Conjugate Coding".
ACM SIGACT News, 15(1):78–88, 1983.

Wiesner's Idea for Quantum Money

A quantum banknote has a serial number and t photons.

No Forging

- Probability of successful forging exponentially small on t.

A Step Forward: Public-key Quantum Money

- Ideally, anyone should be able to verify the validity of money.
  - **Public-key quantum money.**

E. Farhi et al.
"Quantum Money from Knots".
ITCS 2012.

S. Aaronson and P. Christiano.
"Quantum Money from Hidden Subspaces".
STOC 2012.

Quantum Money Scheme of Aaronson-Christiano

- Security under a classical (non-quantum) hardness assumption.

Hardness Assumption

Hidden Subspaces Problem (HSP_q)

Input :

- $p_1, \ldots, p_m, q_1, \ldots, q_m \in \mathbb{F}_q[x_1, \ldots, x_n]$ of degree d.
- $d \geq 3$.
- $n \leq m \leq 2n$.

Find : $n/2$-dimensional subspace $A \subset \mathbb{F}_q{}^n$ s.t

$$p_i(A) = 0 \text{ and } q_i(A^{\perp}) = 0 \ \forall i \in \{1, \ldots, m\}.$$

- Secret key: A.
- Public key: $p_1, \ldots, p_m, q_1, \ldots, q_m$.
  - The subspace and the polynomials are chosen uniformly at random from the appropriate sets.

Security of the Scheme

Aaronson-Christiano (STOC 2012)

- Their scheme relies on HSP_2.

Open Question (STOC'2012)

Extension of the scheme to $\mathbb{F}_q$ for any $q \neq 2$.

Challenge

- Is HSP_q really a hard problem?

Contributions

Our Contributions

- Randomized polynomial-time algorithm for HSP_q, $q > d$.
- Heuristic randomized polynomial-time algorithm for HSP_2.
- Experimentally verified and efficient in practice.

Technique

Algebraic cryptanalysis using Gröbner bases.

- We solve the challenge and master the complexity of solving.

Algebraic Cryptanalysis

1. Solution of a problem $\leftrightarrow$ Solution of a multivariate polynomial system.
2. Solve the system in practice and/or control the complexity of solving.

Our Case (HSP_q)

- Algebraic modeling that allows to master the complexity.
  - Similar modeling to the one used for IP in

J.-C. Faugère, L. Perret.
"Polynomial Equivalence Problems: Algorithmic and Theoretical Aspects".
EUROCRYPT 2006.

Gröbner Bases

F_5 Algorithm (J.-C.Faugère, 2002)

Computation of a Gröbner basis of $\langle f_1, \dots, f_r \rangle \subset \mathbb{F}_q[x_1, \dots, x_n]$ equivalent to succesive reductions to row echelon form of

$$M_{\tilde{d}} = \begin{array}{cc} k_i \text{ monomials of degree } \tilde{d} & \begin{array}{ccc} k_1 \succ & \dots \succ & k_\ell \end{array} \\ \begin{array}{c} t_1 f_{i_1} \\ t_2 f_{i_2} \\ \dots \end{array} & \begin{pmatrix} \dots & \dots & \dots \\ \dots & \dots & \dots \\ \dots & \dots & \dots \end{pmatrix} \end{array}, \quad \deg(t_j f_{i_j}) \leq \tilde{d}.$$

until for big enough $\tilde{d} = d_{reg}$, the row echelon form of $M_{d_{reg}}$ contains a GB.

Gröbner Bases

F_5 Algorithm (J.-C.Faugère, 2002)

Computation of a Gröbner basis of $\langle f_1, \ldots, f_r \rangle \subset \mathbb{F}_q[x_1, \ldots, x_n]$ equivalent to succesive reductions to row echelon form of

$$M_{\tilde{d}} = \begin{array}{cc} k_i \text{ monomials of degree } \tilde{d} & k_1 \succ \quad \ldots \succ \quad k_\ell \\ \begin{array}{c} t_1 f_{i_1} \\ t_2 f_{i_2} \\ \ldots \end{array} & \begin{pmatrix} \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots \end{pmatrix} \end{array}, \quad \deg(t_j f_{i_j}) \leq \tilde{d}.$$

until for big enough $\tilde{d} = d_{reg}$, the row echelon form of $M_{d_{reg}}$ contains a GB.

Complexity Analysis

- Complexity of $\mathcal{O}(n^{\omega d_{reg}})$, $2 \leq \omega \leq 3$ linear algebra constant.
- d_{reg} difficult to estimate in general.
  - In our case we can bound it.

Contents

First Approach

Toy Example

$(p_1 = x_1x_2 + x_1 + x_2x_4 + x_4, p_2, p_3, p_4, q_1, \ldots, q_4)$, $A = \begin{pmatrix} a_{1,1} & \ldots & a_{1,4} \\ a_{2,1} & \ldots & a_{2,4} \end{pmatrix}$ matrix of size 2×4. Let (y_1, y_2) be formal variables over $\mathbb{F}_2$.

$$p_1\left((y_1, y_2)A\right) = 0 = \left(a_{1,1}a_{2,2} + a_{2,1}a_{1,2} + a_{1,2}a_{2,4} + a_{2,2}a_{1,4}\right) y_1y_2 +$$
$$+\left(a_{1,1}a_{1,2} + a_{1,2}a_{1,4} + a_{1,1} + a_{1,4}\right) y_1 + \left(a_{2,1}a_{2,2} + a_{2,2}a_{2,4} + a_{2,1} + a_{2,4}\right) y_2 =$$

First Approach

Toy Example

$(p_1 = x_1x_2 + x_1 + x_2x_4 + x_4, p_2, p_3, p_4, q_1, \dots, q_4)$, $A = \begin{pmatrix} a_{1,1} & \dots & a_{1,4} \\ a_{2,1} & \dots & a_{2,4} \end{pmatrix}$ matrix of size 2×4. Let (y_1, y_2) be formal variables over $\mathbb{F}_2$.

$$p_1\left((y_1, y_2)A\right) = 0 = \left(a_{1,1}a_{2,2} + a_{2,1}a_{1,2} + a_{1,2}a_{2,4} + a_{2,2}a_{1,4}\right)y_1y_2 +$$
$$+\left(a_{1,1}a_{1,2} + a_{1,2}a_{1,4} + a_{1,1} + a_{1,4}\right)y_1 + \left(a_{2,1}a_{2,2} + a_{2,2}a_{2,4} + a_{2,1} + a_{2,4}\right)y_2 =$$
$$\mathrm{Coeff}(p_1, y_1y_2)y_1y_2 + \mathrm{Coeff}(p_1, y_1)y_1 + \mathrm{Coeff}(p_1, y_2)y_2$$
$$\implies \mathrm{Coeff}(p_1, y_1y_2) = \mathrm{Coeff}(p_1, y_1) = \mathrm{Coeff}(p_1, y_2) = 0.$$

First Approach

Toy Example

$(p_1 = x_1x_2 + x_1 + x_2x_4 + x_4, p_2, p_3, p_4, q_1, \dots, q_4)$, $A = \begin{pmatrix} a_{1,1} & \dots & a_{1,4} \\ a_{2,1} & \dots & a_{2,4} \end{pmatrix}$ matrix of size 2×4. Let (y_1, y_2) be formal variables over $\mathbb{F}_2$.

$$\begin{gathered} p_1\left((y_1, y_2)A\right) = 0 = \left(a_{1,1}a_{2,2} + a_{2,1}a_{1,2} + a_{1,2}a_{2,4} + a_{2,2}a_{1,4}\right) y_1y_2 + \\ +\left(a_{1,1}a_{1,2}+a_{1,2}a_{1,4}+a_{1,1}+a_{1,4}\right) y_1 + \left(a_{2,1}a_{2,2}+a_{2,2}a_{2,4}+a_{2,1}+a_{2,4}\right) y_2 = \\ \mathrm{Coeff}(p_1, y_1y_2)y_1y_2 + \mathrm{Coeff}(p_1, y_1)y_1 + \mathrm{Coeff}(p_1, y_2)y_2 \\ \implies \quad \mathrm{Coeff}(p_1, y_1y_2) = \mathrm{Coeff}(p_1, y_1) = \mathrm{Coeff}(p_1, y_2) = 0. \end{gathered}$$

Naive Model

$\forall i \in \{1, \dots, m\}, \forall t \in \mathrm{M}\left(\mathbb{F}_q[y_1, \dots, y_{n/2}]\right)$,

$$\mathrm{SysNaive}_{\mathrm{HSP}_q} = \begin{cases} \mathrm{Coeff}(p_i, t) = 0, \\ \mathrm{Coeff}(q_i, t) = 0. \end{cases}$$

Optimizing the Model

Key Observation

If A is a solution of HSP_q, for any $S \in \mathrm{GL}_{n/2}(\mathbb{F}_q)$, SA is also a solution.

Naive Model Has Many Equivalent Solutions.

Not optimal.

Canonical Form of the Solution of HSP_q

With probability

$$\gamma_q(n/2) = \prod_{i=1}^{n/2}\left(1 - \frac{1}{q^i}\right) \approx 1 - \frac{1}{q} \ ,$$

A admits a basis in systematic form

$$(I|G), \quad G = (g_{i,j}) \text{ is an } n/2 \times n/2 \text{ matrix.}$$

Our Model

Optimizing the Model

Naive system with A in systematic form.

Our Model

$\forall i \in \{1, \ldots, m\}, \forall t \in \mathrm{M}\left(\mathbb{F}_q[y_1, \ldots, y_{n/2}]\right)$,

$$\mathrm{Sys}_{\mathrm{HSP}_q} = \begin{cases} \mathrm{Coeff}(p_i, t) = 0, \\ \mathrm{Coeff}(q_i, t) = 0. \end{cases}$$

Contents

HSP_q, with $q > d$

Linear Equations

For all $i \in \{1, \ldots, m\}, j \in \{1, \ldots, n\}$, denoting by

$$p_i{}^{(1)} = \sum_{j=1}^{n} \lambda_{i,j}^{p} x_j, \;\; q_i{}^{(1)} = \sum_{j=1}^{n} \lambda_{i,j}^{q} x_j, \quad \lambda_{i,j}^{p}, \lambda_{i,j}^{q} \in \mathbb{F}_q \;\; ,$$

$\forall i \in \{1, \ldots, m\}, \forall k \in \{1, \ldots, n/2\}$, the following equations are linear:

$$\mathrm{Coeff}(p_i, y_k) = \lambda_{i,k}^{p} + \sum_{j=1}^{n/2} \lambda_{i,j+n/2}^{p} g_{k,j},$$

$$\mathrm{Coeff}(q_i, y_k) = \lambda_{i,k+n/2}^{q} - \sum_{j=1}^{n/2} \lambda_{i,j}^{q} g_{j,k}.$$

HSP$_q$, with $q > d$

Matrix of Coefficients of Size $mn \times n^2/4$ Has the Following Shape

$$\begin{pmatrix}
\lambda^p_{i,n/2+1} & \dots & \lambda^p_{i,n} & 0 & \dots & 0 & \dots & 0 & \dots & 0 \\
0 & \dots & 0 & \lambda^p_{i,n/2+1} & \dots & \lambda^p_{i,n} & \dots & 0 & \dots & 0 \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
0 & \dots & 0 & 0 & \dots & 0 & \dots & \lambda^p_{i,n/2+1} & \dots & \lambda^p_{i,n} \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
-\lambda^q_{j,1} & \dots & 0 & -\lambda^q_{j,2} & \dots & 0 & \dots & -\lambda^q_{j,n/2} & \dots & 0 \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
0 & \dots & -\lambda^q_{j,1} & 0 & \dots & -\lambda^q_{j,2} & \dots & 0 & \dots & -\lambda^q_{j,n/2} \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots
\end{pmatrix}$$

Full Rank of the Coefficient Matrix with Overwhelming Probability

The probability is $\frac{\gamma_q(m)}{\gamma_q(m-n/2)}$, m number of p_i's.

Randomized Polynomial-time Algorithm for HSP_q

Input: $p_1, \ldots, p_m, q_1, \ldots, q_m \in \mathbb{F}_q[x_1, \ldots, x_n]$ of degree $d \geq 3$, $n \leq m \leq 2n$.

1. Construct the linear system

$$\{\mathrm{Coeff}(p_i, y_k), \mathrm{Coeff}(q_i, y_k) \ , \quad \forall i \in \{1, \ldots, m\}, \forall j \in \{1, \ldots, n/2\}\}.$$

2. Solve it.

Return this solution.

- $\boxed{\text{Complexity } \mathcal{O}(n^{2\omega}),\ 2 \leq \omega \leq 3 \text{ linear algebra constant.}}$
- Success probability

$$\frac{\gamma_q(n/2)\gamma_q(m)}{\gamma_q(m - n/2)} \ .$$

Some Benchmarks for HSP_q, $q > d$

Table : Experiments performed for $m = n$ with MAGMA v.19

n	# Variables	#Eqs	q	Exh. search	Time $d=3$	Time $d=4$
12	36	1992	$2^{16}+1$	$\mathcal{O}\left(2^{576}\right)$	0.00s	0.00s
20	100	11400	$2^{16}+1$	$\mathcal{O}\left(2^{1600}\right)$	0.02s	0.02s

HSP_q for big q is insecure!

HSP_2

- No linear equations: all equations are of degree d with overwhelming probability.
  - Reductions modulo the field equations.

Sys_{HSP_2} Very Overdetermined Non-Linear System

- The number of equations is at least

$$2n\left[\binom{n/2}{1}+\ldots+\binom{n/2}{d}\right] \gg n^2/4.$$

- Behaviour when computing a Gröbner basis?

Some Benchmarks for HSP_2

Table : Experiments performed for $m = n$ with MAGMA v.19

$d = 3$					
n	# Variables	#Eqs	d_{reg}	Exh. search	Time
14	49	1764	4	$\mathcal{O}\left(2^{49}\right)$	136s
16	64	2944	4	$\mathcal{O}\left(2^{49}\right)$	2.30min
18	81	4644	4	$\mathcal{O}\left(2^{81}\right)$	2h20

$d = 4$					
n	# Variables	#Eqs	d_{reg}	Exh. search	Time
12	36	1344	5	$\mathcal{O}\left(2^{36}\right)$	38s
14	49	2744	5	$\mathcal{O}\left(2^{49}\right)$	66min

HSP_2

Structural Symmetries in Our Model

If we order in increasing lexicographic order the monomials of degree d $m_i \in \mathbb{F}_2\left[x_{n/2+1}, \ldots, x_n\right]$, $m^\perp{}_i \in \mathbb{F}_2\left[x_1, \ldots, x_{n/2}\right]$, and $t_i \in \mathbb{F}_2\left[y_1, \ldots, y_{n/2}\right]$, then

$$\mathrm{Coeff}\big(m_i, t_j\big)^{(d)} = \mathrm{Coeff}\big(m^\perp{}_j, t_i\big)^{(d)} \ .$$

HSP_2

Structural Symmetries in Our Model

If we order in increasing lexicographic order the monomials of degree d $m_i \in \mathbb{F}_2\left[x_{n/2+1},\ldots,x_n\right]$, $m^{\perp}{}_i \in \mathbb{F}_2\left[x_1,\ldots,x_{n/2}\right]$, and $t_i \in \mathbb{F}_2\left[y_1,\ldots,y_{n/2}\right]$, then

$$\mathrm{Coeff}\left(m_i, t_j\right)^{(d)} = \mathrm{Coeff}\left(m^{\perp}{}_j, t_i\right)^{(d)} \ .$$

Low Degree Equations

$$\mathrm{Coeff}(p, t_j)+\mathrm{Coeff}(q, t_i)+\sum_{\{k\neq i|\alpha_k\neq 0\}}\mathrm{Coeff}(q, t_k)+\sum_{\{\ell\neq j|\beta_\ell\neq 0\}}\mathrm{Coeff}(p, t_\ell)=0$$

is of degree $d-1$ and is a linear combination of the equations of $\mathrm{Sys}_{\mathsf{HSP}_2}$.

HSP_2

Behaviour of $\mathrm{Sys}_{\mathrm{HSP}_2}$

- Degree falls not typically occurring in a random system of equations.
- Heuristically the degree of regularity is bounded by $d+1$.

Heuristic Randomized Polynomial-time Algorithm for HSP_2

Input: $p_1, \ldots, p_m, q_1, \ldots, q_m \in \mathbb{F}_q[\mathbf{x}]$ of degree $d \geq 3$, $n \leq m \leq 2n$.

1. Compute a Gröbner basis J of $\mathrm{Sys}_{\mathrm{HSP}_2}$.

Return the variety of J.

- $\boxed{\text{Complexity } \mathcal{O}(n^{2\omega(d+1)}),\ 2 \leq \omega \leq 3 \text{ linear algebra constant.}}$
- Success probability $\gamma_2(n/2)$.

Contents

Conclusions and Open Problems

Conclusions

- HSP_q for big q is easy.
    - Randomized polynomial-time algorithm for HSP_q for big q.
- HSP_2 conjectured to be easy.
    - Heuristic randomized polynomial-time algorithm for HSP_2.

Open Problems

1. Noise-free version if the polynomials are not random but more structured (e.g., homogeneous of degree d)?
2. Noisy version?