New results on algebraic constructions of Extremal Graph Theory and implementations of new algorithms of Postquantum Cryptography

Tymoteusz Chojecki
UMCS Lublin, Poland,
V. Ustimenko
University of London (Royal Holloway), UK
Michał Klisowski
UMCS Lublin, Poland,

Content

- Introduction
- Graphs
- Symmetric Cipher
- Public Key
- Statistical analysis

Motivation

NIST 2017 (National Institute of Standards and Technology) tender starts the standardisation process of possible Post-Quantum Public keys aimed for purposes to be

- (i) encryption tools
- (ii) tools for digital signatures.

In July 2020 the Third round of the competition was started. In the category of **Multivariate Cryptography** (MC) remaining candidates are easy to observe. For the task (i) multivariate algorithm were not selected at all, last multivariate candidate **"Rainbow Like Unbalanced Oil and Vinegar"** (RUOV) was investigated for task (ii) but some cryptoanalitic intruments to deal with ROUV were found. In July 2022 first four winners of NIST standarisation competition were chosen. They all are lattice based algorithms.

$A(n, q)$ graph

We use $A(n, q) = A(n, F_q)$ **graphs**. In fact $A(n, K)$ defined over arbitrary commutative ring K. Bipartite graph with the point set $P = K^n$ and line set $L = K^n$. $(p) = (p_1, p_2, \ldots, p_n) \in P$ and $[l] = [l_1, l_2, \ldots, l_n] \in L$. $(p)I[l]$

$$
\begin{aligned}
p_2 - l_2 &= l_1 p_1, \\
p_3 - l_3 &= p_1 l_2, \\
p_4 - l_4 &= l_1 p_3, \\
p_5 - l_5 &= p_1 l_4, \\
&\ldots, \\
p_n - l_n &= p_1 l_{n-1}
\end{aligned}
$$

$p_n - l_n = l_1 p_{n-1}$ for even n.

Small world graphs

$A(n, F_q)$, $n \geq 2, q > 2$ form a family of **small world graphs**, because their **diameter** is bounded by linear function in variable n. In fact, we conjecture that **diameter** of graph $A(n, F_q)$ is bounded by $2n + 2$.
The **girth** of the graph is at least $[n/2]$. Our **computer simulations** shows that theoretical bound can be improved in future.

Girth and diameter

Table: Girth and Diam for $A(n, F_3)$

n	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
Girth	8	12	12	12	12	16	16	16	16	20	20	20
Diam	8	12	13	16	18	20	20					

n	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**
Girth	20	24	24	24	26	30	30	32	32	36	36	36

Table: Girth and Diam for $A(n, F_4)$

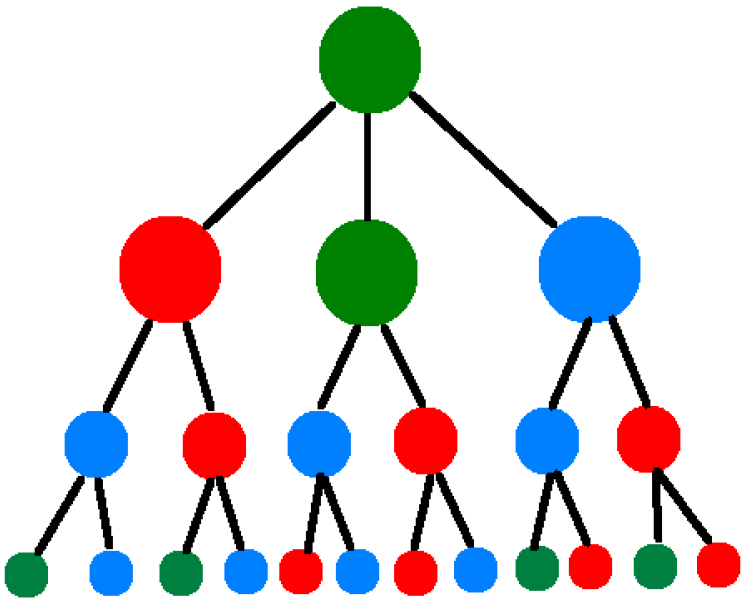
n	**3**	**4**	**5**	**6**	**7**	**8**	**9**
Girth	8	10	12	12	14	16	18
Diam	6	8	10	12	14	16	

Table: Girth and Diam for $A(n, F_5)$

n	**3**	**4**	**5**	**6**	**7**
Girth	8	8	10	12	12
Diam	6	8	10	12	14

Colors $A(n, 2)$

First coordinates $p_1 = \rho((p))$ and $l_1 = \rho([l])$ – **colors**. Each vertex v has a unique neighbor $Na(v)$ of selected color.



Walks

Walk of length $2k$ from vertex $(0, 0, \ldots)$ will be given by the sequence of colors of its elements $w = (b_1, a_1, b_2, a_2, \ldots, b_k, a_k)$. **Path** if $0 \neq a_1, a_i \neq a_{i+1}$ and $b_i \neq b_{i+1}$ for $i = 1, 2, \ldots, k-1$. Let $B_P(K)$ be a **semigroup of all walks** with composition. One can identify empty string with the unity of $B_P(K)$.

Motivation

Noteworthy that all multivariate NIST candidates were presented by multivariate rule of degree bounded by small constant (2 or 3). In particular, RUOV is given by system of quadratic polynomial equations. We think that NIST outcomes motivate investigations of alternating options in MC oriented on encryption tools:

- (a) to work with encryption transformations of plaintext space $(F_q)^n$ of **linear degree** cn, where $c > 0$ is a constant as instruments of stream ciphers or public keys,
- (b) to use protocols of **Noncommutative Cryptography** with platforms of multivariate transformations.

Both approaches as well as combination of (b) and (a) will be used in our talk.

Introduction

We will use special extremal graphs to generate highly nonlinear automorphisms of $F_q[x_1, x_2, \ldots, x_n]$. They are connected with the problem of approximation of **k -regular tree T_k** , $k > 2$ by elements of the family of k-regular graphs of **increasing order and increasing girth** (minimal length of cycle in the graph).

Introduction

We use family of **graphs** $A(n, q)$, $n = 2, 3, \dots$ q , $q > 2$, prime, to make symmetric cipher which use password tuple, length t to form cubic transformation E induced by the path in the graph of length t. Two other parts of the password encode two linear transformations T_1 and T_2 of plaintext space $V = (F_q)^n$. The encryption map is a composition of kind $T_1 E T_2$. Execution of E takes $O(nt)$. If t is less that half of the girth and T_1, T_2 are fixed linear transformations, than **different paths produce distinct ciphertexts**.

Introduction

Cubical nature of encryption/decryption transformations means that adversary can conduct costly linearization attacks via the interception of n^3 pairs of kind plaintext - corresponding ciphertext. It allows him/her to restore E in time $O(n^{10})$. We can modify this symmetric cipher to make it **resistant to linearization attack**.

Introduction

- 1) We use the group of cubical transformations, as above, as a platform of Noncommutative Cryptography. **Noncommutative cryptography** is rapidly grown part of **Post Quantum Cryptography**.
- 2) Using **noncommutative modification of Diffie-Hellman protocol** we obtain a cryptosystem with Perspective to be used in Postquantum Era.
- 3) We modify presented below symmetric cipher via usage of highly nonlinear (**"unbounded degree"**) transformation to make it resistant against the linearization attack.

Walks

Consider $A(n, K[x_1, x_2, \ldots, x_n])$. From each element from $B_P(K)$ we consider a walk $\Delta(w)$ in $A(n, K[x_1, x_2, \ldots, x_n])$ with starting point $(x_1, x_2, \ldots, x_n)$, where x_i are generic elements of $K[x_1, x_2, \ldots, x_n]$ and special colors
$x_1 + b_1, x_1 + a_1, \ldots, x_1 + b_k, x_1 + a_k$.
Let $p' = dest(\Delta(w))$ be a **destination**, i.e. a final point of this walk. Has coordinates
$(x_1 + a_k, f_1(x_1, x_2), f_2(x_1, x_2, x_3), \ldots, f_{n-1}(x_1, x_2, \ldots, x_n))$, f_i are elements of $K[x_1, x_2, \ldots, x_n]$.

Transformation

The map ${}^n\eta(w)$ of $P = K^n$: $x_1 \to x_1 + a_k, x_2 \to f_1(x_1, x_2), x_3 \to f_2(x_1, x_2, x_3), \ldots, x_n \to f_{n-1}(x_1, x_2, \ldots, x_n)$. This transformation is bijective map of K^n to itself. It is an element of affine Cremona group $CG(K^n) = Aut(K[x_1, x_2, \ldots, x_n])$ acting naturally on K^n. We denote the image of ${}^n\eta(B_P(K))$ as the **group** $GA(n, K)$. Elements of this group are used to gather with linear transformations T_1, T_2 in presented below symmetric cipher.

Platform

Theorem

The **maximal degree** of multivariate transformation g from $GA(n, K)$ equals 3.

It means that subgroup G of kind $TGA(n, K)T^{-1}$, where T is an element of affine general linear group $AGL_n(K)$, can be used efficiently as a **platform for the implementation of protocols** of Noncommutative Cryptography.
But the inverse $g \in G$ is also a cubical map. This fact means that standard form of G of kind $x_i \to f_i(x_1, x_2, \ldots, x_n)$, $i = 1, 2, \ldots, n$ where cubical f_i are given via their list of monomial terms **could not serve as public rule**.

Unbounded degree

The following **construction** will provide us the modification of high degree of the symmetric cipher.
For the task 3), **we change the alphabet** of construction of $B_P(K)$ for the commutative ring $K[x]$. Let $CS_n(K)$ be a semigroup of endomorphisms of $K[x_1, x_2, \ldots, x_n]$.
We define ${}^n\eta$ of $B_P(K[x]) \to CS_n(K)$ moving $(f_1, f_2, \ldots, f_k)$ into the transformation $(x_1, x_2, \ldots, x_n)$ of $I = A(n, K[x_1, x_2, \ldots, x_n])$ to the destination point v_k of the walk $(x_1, x_2, \ldots, x_n)Iv_1Iv_2I \ldots Iv_k$ where $\rho(v_i) = f_i(x_1)$, $i = 1, 2, \ldots, k$.

Unbounded degree

We will use transformation of kind $T_1{}^n\eta(u)T_2$ as an encryption instruments. The following Lemma guarantee us that this is **resistant to the linearization attack**.

Lemma

Let $n > k$ and $u = (f_1, f_2, \ldots, f_k)$ be an element of $B_P(K[x])$. Assume that $deg(f_1) \geq 1$, $deg(f_2) \geq 1, deg(f_i - f_{i+2}) \geq 1$ for $i = 1, 2, \ldots, k-2$. Then **degree of** ${}^n\eta(u)$ **at least** k.

Computer execution time of encryption

We present the **computer execution time of encryption** of T_1ET_2 in the case $K = F_p, p = 127, k = 50, 100, 1000$ and size of plaintext is 10 Kb, 20Kb and 40Kb in table

File size	10Kb	20Kb	40Kb
k=50	1,75s	3,41s	6,72s
k=100	3,31s	6,74s	12,8s
k=1000	32,72s	65,21s	125,1s

Twisted Diffie-Hellman protocol (TD-H)

Let S be an abstract semigroup which has some invertible elements.

Alice and Bob share element $g \in S$ and pair of invertible elements $h, h^{-1} \in S$. Alice takes k_A and r_A and forms $g_A = h^{-r_A} g^{k_A} h^{r_A}$. Bob takes k_B and r_B and forms $g_B = h^{-r_B} g^{k_B} h^{r_B}$. They exchange g_A and g_B and **compute collision element** X as ${}^A g = h^{-r_A} g_B^{k_A} h^{r_A}$ and ${}^B g = h^{-r_B} g_A^{k_B} h^{r_B}$ respectively.

We implemented this protocol using $S = TGA(n, q)T^{-1}$.

Correspondents can execute this protocol and share the tuple $Z$of $t = o(n^4)$ coefficients of X.

Cryptosystem

Consider the expansion of the TD-H protocol to a **cryptosystem** with the trust interval.
Alice selects transformations T_1 and T_2 and element u from $B_P(K)$ corresponding to some pass. She computes element ${}^n\eta(u) = E$ and $G = T_1 E T_2$, she sends $G + X$ to Bob. He uses G as an **encryption tool**. Alice decrypts in time $O(n^2)$ because of her knowledge of T_1, E, T_2 and their inverses. The natural question is the following one.

Trust Interval

How long correspondents can use encryption map G?
Cryptanalytical studies gives the following answer. Alice and Bob have to keep the **TRUST INTERVAL** of size $n^3/2$. It is justified by investigation of linearization attacks where adversary has to intercept n^3 pairs of kind plaintext/ciphertext.
So, Alice and Bob have to **count exchanged messages up to $n^3/2$ files**. If counter indicates $[n^3/2]$ they have to start a new session of the protocol.

Algorithm

We use polynomials over F_q, $q = 2m$ filed.

- Our starting point is $Start = [x_1, x_2, \ldots, x_n]$, n is the size of plain text.
- Using some password we generate two invertible linear transformation T_1, T_2
- We apply $II = T_1(Start) = [y_1, y_2, \ldots, y_n]$,
- We choose some password $w = (b_1, a_1 \ldots, b_k, a_k)$ representing path in our $A(n, K[x_1, \ldots, x_n])$ graph. We apply transformation ${}^n\eta(w)$ to point II and obtain point III.
- We change color of III from $y_1 + a_k$ into $(y_1)^2 + a_k$. $(2m - 1$ is relatively prime with 2)
- We apply T_2 and obtain $IV = T_2(III)$.

Public key

Our point $IV = [f_1(x_1, x_2, \ldots, x_n), \ldots, f_n(x_1, x_2, \ldots, x_n)]$. List of all coefficents of $f_1, \ldots, f_n$ in lexicographic order form public key. In order to decode you only need to reverse T_1 and T_2, calculate square root and reverse path to w.

implementation

I use Python 3.6 and Sage to implements this algorithm. I use polynomials over filed $\mathbb{F}_{2^{32}}$.

Table: Case I. Without changing into square, First coordinate linear transformation. Number of nonzero coefficients

n	length of w				
	16	32	64	128	256
16	4679	4679	4679	4679	4679
32	52570	59873	59873	59873	59873
64	490837	729991	847099	847109	847109
128	4214042	7165704	10829396	12705549	12705549

Table: Case II. Changing into square, First coordinate linear transformation. Number of nonzero coefficients

n	length of w				
	16	32	64	128	256
16	4679	4679	4679	4679	4679
32	52570	59873	59873	59873	59873
64	490906	729992	847109	847109	847109
128	4214042	7165704	10829396	12705549	12705549

Table: Case III. Changing into square, Full linear transformation. Number of nonzero coefficients

n	length of w				
	16	32	64	128	256
16	15504	15504	15504	15504	15504
32	209440	209440	209440	209440	209440
64	3065920	3065905	3065920	3065920	3065920
128	46866560	46866560	46866560	46866560	46866560

Thank you for your attention :)