On the key exchange via cubical polynomials

Aneta Wróblewska, Vasyl Ustimenko

University of Maria Curie-Skłodowska in Lublin, Poland

11 June 2010

HUMAN CAPITAL
NATIONAL COHESION STRATEGY

EUROPEAN
SOCIAL FUND

The project is co-funded from the sources of the European Union
within the limit of the European Social Fund.

Human - The Best Inwestment

Idea

Let F_p, where p is prime, be a finite field. Affine transformations $\mathrm{x} \rightarrow A\mathrm{x} + b$, where A is invertible matrix and $b \in F_p^n$, form an affine group $AGL_n(F_p)$ acting on ${F_p}^n$. It is known that polynomial transformation of kind

$$x_1 \rightarrow g_1(x_1, \ldots, x_n), x_2 \rightarrow g_2(x_1, \ldots, x_n), \ldots, x_n \rightarrow g_n(x_1, \ldots, x_n)$$

form a symmetric group S_{p^n}.

In the simplest case F_p, affine transformations form an affine group $AGL_n(F_p)$ of order $p^n(p^n-1)(p^n-p)\dots(p^n-p^{n-1})$ in the symmetric group S_{p^n} of order $(p^n)!$. In [4] the maximality of $AGL_n(F_p)$ in S_{p^n} was proven. So we can present each permutation π as a composition of several "seed" maps of kind $\tau_1 g \tau_2$, where $\tau_1, \tau_2 \in AGL_n(F_p)$ and g is a fixed map of degree ≥ 2.

We can choose the base of ${F_p}^n$ and write each permutation $g \in S_{p^n}$ as a public rule:

$$x_1 \longrightarrow g_1(x_1, x_2, \ldots, x_n)$$

$$x_2 \longrightarrow g_2(x_1, x_2, \ldots, x_n)$$

$$\ldots$$

$$x_n \longrightarrow g_n(x_1, x_2, \ldots, x_n)$$

.

Diffie-Hellman algorithm

Let $g^k \in S_{p^n}$ be the new public rule obtained via iteration of g. We consider Diffie-Hellman algorithm for S_{p^n} for the key exchange. Correspondents Alice and Bob establish $g \in S_p^n$ via open communication channel, they choose positive integers n_A and n_B, respectively. They exchange public rules $h_A = g^{n_A}$ and $h_B = g^{n_B}$ via open channel. Finally, Alice and Bob compute common vector as ${h_B}^{n_A}$ and ${h_A}^{n_B}$, respectively.

This scheme of "symbolic Diffie-Hellman algorithm" can be secure, if:

- the order of g is "sufficiently large" (if not we have an algorithm for the cyclic group),
- adversary can not compute number n_A (or n_B) as functions from degrees for g and g^{n_A}.

Algebraic definition of the simple graph

To construct g_n we will use bipartite graph with the point set $P = F_p^n$ and line set $L = F_p^n$. Incidency of points and lines will be defined via system of algebraic equations.

Algebraic definition of the simple graph

P and L are two n-dimensional free modules of K ($K = F_p$ for the begining), where K is a commutative ring with unity.
P - *points*
L -*lines*.
If $x \in V$, then $(x) \in P$ and $[x] \in L$.

$$(p) = (p_1, p_{1,1}, p_{1,2}, p_{2,1}, p_{2,2}, p'_{2,2}, p_{2,3}, p_{3,2}, p_{3,3}, p'_{3,3}, \ldots)$$

$$[l] = [l_1, l_{1,1}, l_{1,2}, l_{2,1}, l_{2,2}, l'_{2,2}, l_{2,3}, l_{3,2}, l_{3,3}, l'_{3,3}, \ldots]$$

Incidence structure (P, L, I)

Point (p) is incident with the line $[l]$, and we write $(p)I[l]$, if the following relations between their coordinates hold:

$$l_{1,1} - p_{1,1} = l_1 p_1$$

$$l_{1,2} - p_{1,2} = l_{1,1} p_1$$

$$l_{2,1} - p_{2,1} = l_1 p_{1,1}$$

$$l_{i,i} - p_{i,i} = l_1 p_{i-1,i}$$

$$l'_{i,i} - p'_{i,i} = l_{i,i-1} p_1$$

$$l_{i,i+1} - p_{i,i+1} = l_{i,i} p_1$$

$$l_{i+1,i} - p_{i+1,i} = l_1 p'_{i,i}.$$

Rainbow like colouring

We will use a special colouring of edges. We can think that simple graph is a directed graph such that $a \longrightarrow b$ and $b \longrightarrow a$.
Let $E(\Gamma)$ be the set of arrows of k-regular graph Γ, M - set of colours and function $\pi : E \longrightarrow M$ such that for each vertex $v \in V$ and $\alpha \in M$ there exist unique neighbor $u \in V$ with property $\pi((v, u)) = \alpha$.

We say that such colouring is rainbow like, if the operator $N_a(v) := N(a, v)$ taking the neighbor u of a vertex v with arrow of colour α is bijection.
For our graph $D(k, F_p)$ the set of colours is F_p. If we have $(p) \to [l]$, where
$(p) = (p_1, p_{1,1}, p_{1,2}, p_{2,1}, p_{2,2}, p'_{2,2}, p_{2,3}, p_{3,2}, p_{3,3}, p'_{3,3}, \ldots)$
$[l] = [l_1, l_{1,1}, l_{1,2}, l_{2,1}, l_{2,2}, l'_{2,2}, l_{2,3}, l_{3,2}, l_{3,3}, l'_{3,3}, \ldots]$, the colour is $l_1 - p_1$.

Let $g = g_n = N_{\alpha_1} N_{\alpha_2} \ldots N_{\alpha_{2s}}$ where $2s$ is even constant, then $g : P \longrightarrow P$, $g \in S_{p^n}$.
$\alpha_1 \alpha_2 \ldots \alpha_{2s}$ must be irreducible, i.e. $\alpha_i \neq -\alpha_{i+1}$ for $i = 1, 2, \ldots, 2s-1$.
$g = g_n$ corresponds to the pass of length $2s$ within the graph.

To prove that order $|g_n| \to \infty$ with $n \to \infty$ we can use the concept of the family of large girth.
The **girth** of the simple graph is the length of its smallest cycle.
The infinite sequence G_i of k-regular simple graphs of increasing order v_i and girth d_i is a **family of graphs of large girth** if $d_i \geq c\log_{k-1}(v_i)$, where c is independent positive constant.
It can be shown that $d(D(n, F_p)) \geq n + 5$, and for $p \geq 5$ we have $d(D(n, F_p)) = n + 5$.

Now g^k corresponds to pass

$$(\alpha_1\alpha_2\ldots\alpha_{2s})(\alpha_1\alpha_2\ldots\alpha_{2s})\ldots(\alpha_1\alpha_2\ldots\alpha_{2s})$$

of length $2sk$, with condition $\alpha_1 \neq -\alpha_{2s}$.
If $g^k = 1$ we have a cycle. So we must have
$|g| \geq \frac{d(D(n,F_p))}{2s} = \frac{n+5}{2s}$.
The fact that for each k, g^k is cubic was proven in [8] with usage of induction.
Group generated by all g, corresponding to even sequence of colours, will be extraspecial subgroups for S_{p^n} with $c = 3$

Generalization for arbitrary finite commutative ring K

We generalize the above algorithm for the case of arbitrary finite commutative ring K with at least 3 regular elements (non zero devisors). We have to change ${F_p}^i$ for free module K^i and the family of the above mentioned simple graphs for the family of regular directed graphs with vertex set $K^i \cup K^i$ of large girth and symmetric group S_{p^i} and $AGL_i(F_p)$ for Cremona group $C(K^i)$ of all polynomial automorphisms of K^i and group of affine automorphisms of $AGL_i(K)$, respectively.

Regular directed graph

Directed graph - an irreflexive binary relation $\phi \subset V \times V$, where V is the set of vertices.
Let introduce two sets

$$id(v) = \{x \in V | (a, x) \in \phi\},$$

$$od(v) = \{x \in V | (x, a) \in \phi\}$$

as sets of inputs and outputs of vertex v. Regularity means the cardinality of these two sets (input or output degree) are the same for each vertex.

Construction of new graph - double directed graph

In the first step we connect point with line to get two sets of vertices of new graph:

$$F = \{\langle (p), [l] \rangle \mid (p) I [l]\} \quad \cong K^{n+1}$$

$$F' = \{\{[l], (p)\} \mid [l] I (p)\} \quad \cong K^{n+1}.$$

Now we define the following relation between vertices of the new graph:

$$\langle (p), [l] \rangle R \{[l'], (p')\} \quad \Leftrightarrow \quad [l] = [l'] \;\; \& \;\; p_1 - p_1' \in RegK$$

$$\{[l'], (p')\} R \langle (p), [l] \rangle \quad \Leftrightarrow \quad (p') = (p) \;\; \& \;\; l_1' - l_1 \in RegK$$

Our key will be $\alpha_1, \alpha_2, \ldots, \alpha_n$, such that $\alpha_i \in RegK$.

As a first vertex we take

$$\{[l],(p)\} = (l_1, l_{1,1}, l_{1,2}, \ldots, l_{i,j}, p_1)$$

(our variables) . Using the above relation we get get next vertex:

$$\langle (p)^{(1)}, [l]^{(2)} \rangle = (p_1, p_{1,1}^{(1)}, \ldots, p_{i,j}^{(1)}, l_1 + \alpha_1)$$

with coefficients of degree 2 or 3
Similarly we get third vertex:

$$\{[l]^{(2)}, (p)^{(3)}\} = (l_1 + \alpha_1, l_{1,1}, \ldots, l_{i,j}, p_1 + \alpha_2)$$

also with coefficients of degree 2 or 3.

Hence using the induction we got:

$$\deg p_{i,j}^{(2k+1)} = \begin{cases} 2, & (i,j) = (i,i)' \ \text{ or } \ (i,j) = (i,i+1), \\ 3, & (i,j) = (i,i) \ \text{ or } \ (i,j) = (i+1,i) \end{cases}$$

$$\deg l_{i,j}^{(2k+2)} = \begin{cases} 3, & (i,j) = (i,i)' \ \text{ or } \ (i,j) = (i,i+1), \\ 2, & (i,j) = (i,i) \ \text{ or } \ (i,j) = (i+1,i) \end{cases}$$

Hence we got extraspecial group, defined by algebraic graph acting on K^{n+1}, with $c = 3$.

Construction of new graph - triple directed graph

Now we connect three vertices of the graph to get two sets of vertices of new graph:

$$F = \{\langle (p^1), [l], (p^2)\rangle \ | \ (p^1)I[l]I(p^2)\} \quad \cong K^{n+2}$$

$$F^{'} = \{\{[l^1], (p), [l^2]\} \ | \ [l^1]I(p)I[l^2]\} \quad \cong K^{n+2}.$$

Now we define the relation between vertices of the new graph:

$$\langle (p^1), [l], (p^2)\rangle R\{[{l'}^1], (p'), [{l'}^2]\} \quad \Leftrightarrow$$

$$\Leftrightarrow \quad [l] = [{l'}^1] \ \ \& \ \ (p^2) = (p') \ \ \& \ \ {l'}^1_1 - {l'}^2_1 \in RegK$$

$$\{[l^1], (p), [l^2]\} R\langle ({p'}^1), [l'], ({p'}^2)\rangle \quad \Leftrightarrow$$

$$\Leftrightarrow \quad (p) = ({p'}^1) \ \ \& \ \ [l^2] = [l'] \ \ \& \ \ {p'}^1_1 - {p'}^2_1 \in RegK$$

We are starting from the vertex:

$$\{[l],(p),[l^1]\} = (l_1, l_{1,1}, l_{1,2}, \ldots, l_{i,j}, p_1, l_1^2)$$

Similarly as in the previous section (by the induction) in (2k) and (2k+1) vertex we get vertices with corresponding degrees:

$$\langle (p^{2k-2}),[l^{2k-1}],(p^{2k})\rangle = (p_1+\alpha_1+\ldots+\alpha_{(2k-3)}, p_{1,1},\ldots,p_{i,j},$$

$$l_1^2+\alpha_2+\ldots+\alpha_{(2k-2)}, p_1+\alpha_1+\ldots+\alpha_{(2k-1)}),$$

$$\{[l^{2k-1}],(p^{2k}),[l^{2k+1}]\} = (l_1^2+\alpha_2+\ldots+\alpha_{(2k-2)}, l_{1,1},\ldots,l_{i,j},$$

$$p_1+\alpha_1+\ldots+\alpha_{(2k-1)}, l_1^2+\alpha_2+\ldots+\alpha_{(2k)})$$

where

$$\deg p_{i,j}^{(2k)} = \begin{cases} 3, & (i,j) = (i,i)' \text{ or } (i,j) = (i,i+1), \\ 4, & (i,j) = (i,i) \text{ or } (i,j) = (i+1,i) \end{cases}$$

and

$$\deg l_{i,j}^{(2k+1)} = \begin{cases} 4, & (i,j) = (i,i)' \text{ or } (i,j) = (i,i+1), \\ 3, & (i,j) = (i,i) \text{ or } (i,j) = (i+1,i) \end{cases}$$

Hence we got extraspecial group on K^{n+2}, with $c = 4$

Construction of new graph - directed quadro graph

Different situation is when we connect four vertices to obtain a new graph.
Let define two sets of vertices:

$$F = \{\langle (p^1), [l^1], (p^2), [l^2] \rangle \ | \ (p^1) I [l^1] I (p^2) I [l^2]\} \quad \cong K^{n+3}$$

$$F' = \{\{[l^1], (p^1), [l^2], (p^2)\} \ | \ [l^1] I (p^1) I [l^2] I (p^2)\} \quad \cong K^{n+3},$$

and relation between them:

$$\langle(p^1),[l^1],(p^2),[l^2]\rangle \; R \; \{[(l')^1],((p')^1),[(l')^2],((p')^2)\} \quad \Leftrightarrow$$

$$[l^1]=[(l')^1] \;\&\; (p^2)=((p')^1) \;\&\; [l^2]=[(l')^2] \;\&\; p^1_1-(p')^2_1 \in RegK$$

$$\{[l^1],(p^1),[l^2],(p^2)\} \; R \; \langle((p')^1),[(l')^1],((p')^2),[(l')^2]\rangle \quad \Leftrightarrow$$

$$(p^1)=((p')^1) \;\&\; [l^2]=[(l')^1] \;\&\; (p^2)=((p')^2) \;\&\; l^1-(l')^2 \in RegK$$

We could start from the vertex:

$$\{[l^1],(p^1),[l^2],(p^2)\} = \left(l_1^1, l_{1,1}, l_{1,2}, \ldots, l_{i,j}, p_1^1, l_1^2, p_1^2\right)$$

After the first step we get vertex:

$$\langle (p^1),[l^2],(p^2),[l^1+\alpha_1]\rangle = \left(p_1^1, p_{1,1}, \ldots, p_{i,j}, l_1^2, p_1^2, l_1^1+\alpha_1\right),$$

with degrees 2 or 3.

By the similar calculation we get:

- the third vertex(second step):

$$\{[l^2], (p^2), [l^1 + \alpha_1], (p^1 + \alpha_2)\} =$$

$$= \left(l_1^2, l_{1,1}, l_{1,2}, \ldots, l_{i,j}, p_1^2, l_1^1 + \alpha_1, p_1^1 + \alpha_2\right),$$

with degrees 3 or 4.

- the fourth vertex (third step):

$$\langle (p^2), [l^1 + \alpha_1], (p^1 + \alpha_2), [l^2 + \alpha_3] \rangle =$$

$$= \left(p_1^2, p_{1,1}, \ldots, p_{i,j}, l_1^1 + \alpha_1, p_1^1 + \alpha_2, l_1^2 + \alpha_3\right),$$

with degrees 4 or 5.

- the fifth vertex (fourth step):

$$\{[l^1+\alpha_1],(p^1+\alpha_2),[l^2+\alpha_3],(p^2+\alpha_4)\} =$$

$$= \left(l_1^1+\alpha_1, l_{1,1}, l_{1,2}, \ldots, l_{i,j}, p_1^1+\alpha_2, l_1^2+\alpha_3, p_1^2+\alpha_4\right)$$

  with degrees 5 or 6, and so on.

This gives an information that degrees of the polynomials grows along with the growth of the length of the password - after k steps we get polynomials of degree $k-1$ or k.

Conclusion

Group G_n, generated by transformation of kind $N_{\alpha_1} \times N_{\alpha_2}$, where $\alpha_1 \neq \alpha_2$, is an extraspecial with constant $c = 3, 4$. Non trivial elements of this groups are polynomials of degree 3 (or 4 in case of triple).

The security of our key exchange based on G_n depends on the complexity of discrete logarithm problem for G_n. We hope investigate the properties of this group.

From the properties of the graph we got, that for $g = g(n) = N_{\alpha_1} N_{\alpha_2} \ldots N_{\alpha_{2s}}$ we have $\lim_{n \to \infty} |g(n)| = \infty$

Transformation $\tau_1 G_n \tau_2$, where $\tau_1, \tau_2 \in AGL_n(K)$ can be used as public rules. We have a similarity with known Imai-Matsumoto algorithm, for which J. Patarin found a cryptoanalitical solution. We hope that encryption $\tau_1 G_n \tau_2$ can be interesting problem for cryptoanalysis.

Bibliography

1 B. Bollobás, *Extremal Graph Theory*, Academic Press, London, 1978.

2 N. Koblitz, Algebraic aspects of Cryptography, in Algorithms and Computations in Mathematics, v. 3, Springer, 1998.

3 Whitfield Diffie, Martin E. Hellman, *New Directions in Cryptography*, IEEE Transactions on Information Theory, 22(6), 644-654, November 1976.

4 B. Mortimer, *Permutation groups containing affine of the same degree*, J. London Math. Soc., 15, N3, 445-455.

5 V. A. Ustimenko, *Linguistic Dynamical Systems, Graphs of Large Girth and Cryptography*, Journal of Mathematical Sciences, Springer, vol.140, N3 (2007) pp. 412-434.

6 V. A. Ustimenko, *On the extremal graph theory for directed graphs and its cryptographical applications*, in T. Shaska, W. C. Huffman, D. Joener and V. Ustimenko (editors), Advances in Coding Theory and Cryptography. Series on Coding Theory and Cryptology, World Scientific, vol. 3, (2007).

7 V. Ustimenko, *On the cryptographical properties of extremal algebraic graphs*, in "Algebraic Aspects of Digital Communications", Volume 24, NATO Science for Peace and Security Series - D: Information and Communication Security, IOS Press, July 2009.

8 A. Wroblewska, *On some properties of graph based public key*, Albanian J. Math., vol. 2, No 3 (2008), Special Issue "New Challenges of Digital Communications", Proc. of NATO Advanced Studies Institute, Vlora, 2008, pp. 229-234.

Thank you for your attention!