On Eulerian Transformations and Postquantum Access Control Protocol-Based Algorithms

Vasyl Ustimenko[1,2] and Oleksandr Pustovit[2]

[1] *University of Marie Curie-Sklodowska in Lublin, 5 Plac Marii Curie-Skłodowskiej, Lublin, 20-031, Poland*
[2] *Institute of Telecommunications and the Global Information Space, 13 Chokolivsky bul., Kyiv, 02000, Ukraine*

Abstract

The paper is dedicated to applications of Noncomutative Cryptography to access control algorithms for Information Systems. The example of usage of the protocol based on multivariate transformations to access control tasks is given. The platforms for such protocols are subsemigroups of affine Cremona semigroup acting on affine space of dimension *n* with Multicomposition property, i.e. ability to make computation of the composition of *n* elements from subsemigroup in polynomial time *T*(*n*).The implementation of the algorithm is given in the case of platform of Eulerian transformations. The modification of main algorithm is based on the idea of combination of Eulerian Transformations with elements of affine Cremona group of bounded degree and polynomial density.

Keywords

Access control, noncommutative cryptography, multivariate cryptography, multicomposition property, Eulerian transformations, one-time pad.

1. Introduction

Protocol based approach to control access to information systems in information space is a very popular one. With the appearance of the first samples of quantum computers it is very important to investigate potential of this approach. We study new postquantum resistant multivariate protocols which can substitute unresistable to quantum computer based attacks Diffie-Hellman algorithm. Current state of research in Postquantum Multivariate Cryptography is presented on the web page of the future Satellite Conference “Mathematical Aspects of Post Quantum Cryptography” of the Mathematical Congress 2022 (see https://icm2022.org/satellites). One of the sixth main directions of the Post Quantum Cryptography is Multivariate Cryptography for which affine Cremona semigroup named after Luigi Cremona [1] and its multivariate transformations are the main instruments to create cryptographical algorithms. These transformations are induced by endomorphisms of polynomial ring $K[x_1, x_2,..., x_n]$ over commutative ring *K*. The case $K=F_q$ of finite field is very popular in classical Multivariate Cryptography. We discover large subgroups of $CS_n(K)$, $n=2,3,\ldots$ with the Multicomposition property (MCP) which means possibility to compute the composition of *N* arbitrary chosen elements of $CS_n(K)$ in polynomial time $T(n)$. We assume that each element of $CS_n(K)$ is given in its standard polynomial form $x_i \to f_i(x_1, x_2,..., x_n)$, $i=1,2,\ldots n$.

2. On Multivariate Protocols of Noncommutative CRYPTOGRAPHY and Access Control

Tahoma protocol was introduced in [2]. It uses two semigroups $S_n<SC_n(K)$ and $S_m<CS_m(K)$, $m<n$ with the MPC property. We assume that there is homomorphism $\varphi_{n,m} : S_n \to S_m$.

CPITS-II-2021: Cybersecurity Providing in Information and Telecommunication Systems, October 26, 2021, Kyiv, Ukraine
EMAIL: vasulustimenko@yahoo.pl (V. Ustimenko); sanyk_set@ukr.net (O. Pustovit)
ORCID: 0000-0002-2138-2357 (V. Ustimenko); 0000-0002-3232-1787 (O. Pustovit)

At the entrance of protocol we have elements $g_1, g_2,..., g_k$, $k \geq 2$ from $CS_n(K)$ conjugated with elements $g'_1, g'_2,..., g'_k$ from S_n together with elements $h_1, h_2,..., h_k$ from S_m conjugated with $\varphi(g'_1), \varphi(g'_2),..., \varphi(g'_k)$.

Alice sends pair (g_i, h_i), $i=1, 2,...,k$ to Bob.

Bob selects sequences $w(1)=(i(1,1), i(2,1), ..., i(l(1),1)$, $w(2)=(i(1,2), i(2,2), ..., i(l(2),2),$, …., $w(s)=(i(1,s), i(2,s), ..., i(l(s),s)$ of elements from $\{1,2,...,k\}$

He sends $g(j)=g_{i(1,j)}g_{i(2,j)}$, ... $g_{i(l(j),j)}$, $j=1,2,...,s$ to Alice. Bob keeps $z(j)=h_{i(1,j)}h_{i(2,j)}$, ... $h_{i(l(j),j)}$, $j=1,2,...,s$ in his private storage.

Alice restores $z(j)$ because of her knowledge on the input data. Postquantum security of the protocol rests on the problem of decomposition of $w(i)$ into generators g_i .

Access control algorithm.

Alice (administrator of information system) forms pseudorandom or genuine random system $(p_1, p_2,...,p_m)$ from K^m and word w in the alphabet $z(1)$, $z(2),...,z(s)$. Alice sets password as $w(p)$. Bob enters $w(p)$ and gets access to the system.

Algorithm is implemented with various platforms S_n, S_m and homomorphism between them (see [3–5]).

3. Case of Eulerian Platform

Let us consider the case when S_n and S_m are subsemigroups of semigroups $ES_n(K)$ and $ES_m(K)$ of Eulerian transformations, i.e. transformations moving each variable x_i into monomial term $q_i x_1^{\alpha(i,1)} x_2^{\alpha(i,2)} ... x_n^{\alpha(i,n)}$ $(t=n$ or $t=m)$ where q_i are regular elements of K and $a(i,j)$ from Z_d ,$d=|K^*|$. These transformations were used for the development of public key algorithms [6, 7] and key exchange protocols [8] and key generation algorithm of one time pad encryption [9].

For simplicity we assume that algorithm has two outputs $z(1)$ and $z(2)$ with coefficients q_i, $a(i,j)$ and q'_i, $a'(i,j)$ respectively. Alice and Bob use generator of pseudorandom sequence $(r_1, r_2 ,...,r_m)=r$ where r_i, are from K^*.

They form formal word w of kind $z(1)^{\alpha(1)} z(2)^{\alpha(2)} z(1)^{\alpha(3)}$ … or $z(2)^{b(1)} z(1)^{b(2)} z(2)^{b(3)}$ … of length k, $k=O(1)$ and use $w(r)$ as entrance password.

It is clear that the execution time of the protocol is $O(n^3)$ which is the time to compute the composition of the elements from $ES_n(K)$.

The computation of the entrance password costs $O(m^2)$ because Alice and Bob use publicly known decomposition of w into hidden $z(1)$ and $z(2)$.

Assume that Alice and Bob use word w without change and the adversary is able to intercept some pairs $(r, w(r))$ where unknown w is of kind $x_i \rightarrow y_i$ $x_1^{y(i,1)} x_2^{y(i,2)} … x_m^{y(i,m)}$, $i=1,2, ..., n$ .The word depends on m^2+m unknowns. So Alice and Bob can use unchanged word safely $<m+1$ times.

With this restrictions the only option for adversary is to break postquantum safe protocol. So Alice and Bob can use various words w during practically unlimited time. Noteworthy that they can change the size of parameter m via new session of the protocol with the same or new platform.

Alternative usage. In this case correspondents can use the protocol with several outputs for the generation of password for "multiplicative" one time pad with plainspace $(K^*)^m$ and encryption function $(x_1 , x_2 ,..., x_m) \rightarrow (x_1p_1, x_2p_2 , ..., x_mp_m)$ where $p=(p_1, p_2 ,..., p_m)$ is the password.

They form password via described above process of generation pairs (w , r) and setting $p=w(r)$. Password has to be used only one time.

Noteworthy that in the case $K=F_q$ correspondents can use plainspace K^n and additive one time pad with encryption function $(x_1 , x_2 ,..., x_m) \rightarrow (x_1 + p_1, x_2 + p_2 , ..., x_m + p_m)$.

4. An Example of Implementation

Let us consider an Eulerian semigroup $ES_n(K)$, which is a subsemigroup of $CS_n(K)$ of transformations of kind $x_i \rightarrow t_i(x_1,x_2,...,x_n)$, where t_i are monomial terms in $K[x_1,x_2,...,x_n]$. Let $LE_n(K)$ be a subsemigroup of $ES_n(K)$ of kind

$x_1 \rightarrow q_1 x_1^{a(1,1)}$

L: $x_2 \to q_2 a_{21} x_1^{a(2,1)} x_2^{a(2,2)}$

$\ldots$

$x_n \to q_n a_{n1} x_1^{a(n,1)} x_2^{a(n,2})\ldots x_n^{a(n,n)}$

where q_i are regular element of K

together with subgroups $UE_n(K)$ of transformations of kind

$x_1 \to q_1 x_1^{a(1,1)} x_2^{a(1,2)} \ldots x_n^{a(1,n)}$

U: $x_2 \to q_2 x_1^{a(2,1)} x_2^{a(2,2)} \ldots x_{n-1}^{a(2,n-1)}$

$\ldots$

$x_n \to q_n x_1^{a(n,1)}$

Notice that in the case of finite K map L is invertible transformation of $(K^*)^n$ if $a(1,1), a(2,2),\ldots, a(n,n)$ are mutually prime with $d=|K^*|$. Similarly U induces a bijection of K^* if $a(n,1), a(n-1,1),\ldots,a(1,1)$ are mutualy prime with d.

Assume that $m<n$. We consider a parabolic semigroup $P_{n,m}(K)$ of all transformations of kind

$x_1 \to q_1 x_1^{a(1,1)} x_2^{a(1,2)} \ldots x_m^{a(1,m)}$

$x_2 \to q_2 x_1^{a(2,1)} x_2^{a(2,2)} \ldots x_m^{a(2,m)}$

$\ldots$

$x_m \to q_m\, x_1^{a(m,1)} x_2^{a(m,2)} \ldots x_m^{a(n,m)}$

$x_{m+1} \to q_{m+1} x_1^{a(m+1,1)} x_2^{a(m+1,2)} \ldots x_m^{a(m+1,n)}$

$x_{m+2} \to q_{m+2} x_1^{a(m+2,1)}\, x_2 a^{(m+2,2)} \ldots\, x_m^{a(m+2,n)}$

$\ldots$

$x_n \to q_n x_1^{a(n,1)}\, x_2^{a(n,2)} \ldots x_n^{a(n,n)}$

Let $\varphi_{n,m}(g)$ be the restriction of $g \epsilon P_{n,m}(K)$ onto variables $x_1, x_2,\ldots,x_m$. It is easy to see that $\varphi_{n,m}$ is a homomorphism of $P_{n,m}(K)$ onto $ES_m(K)$. We consider a special case of Tahoma protocol presented in [2].

Alice takes transformations $p_1, p_2,\ldots, p_t \epsilon P_{n,m}(K)$ with pseudorandom coefficient for p_i given by list ${}^iq_1, {}^iq_2,\ldots, {}^iq_n$, from K^* and ${}^ia(i,j)$ from Z_d., $d=|K^*|$. Alice takes $L \epsilon LE_n(K)$ given by coefficients $b(i,j), i\leq j, q_i \epsilon K^*, i=1,2,\ldots,n$ and $U \epsilon UE_n(K)$ with coefficients $c(i,j), j\leq i$ and $q_i' \epsilon K^*, i=1,2,\ldots,n$. We assume that $b(1,1), b(2,2),\ldots, b(n,n)$ and $c(1,n), c(2,n),\ldots, c(n,n)$ are mutually prime with $d=|K^*|$.

Alice forms elements $p_1, p_2,\ldots, p_t$ $a_i=ULp_iU^{-1}L^{-1}$, $i=1,2,\ldots n$ where U^{-1} and L^{-1} are inverse automorphisms for U and L from $AutK[x_1,x_2,\ldots,x_n]$. She computes $b_i=\varphi(p_i)$ and takes automorphism $U' \epsilon UE_m(K)$ and $L' \epsilon LEm(K)$.

Alice computes $b_i=U'L'\varphi(p_i)(U'L')^{-1}$, where $U'\epsilon UE_m(K), L'\epsilon UL_m(K)$ and sends pairs (a_i,b_i) to Bob.

Bob takes sequences ${}^rj(1,r)$, ${}^rj(2,r),\ldots$, ${}^rj(l(r),r)\epsilon\{1,2,\ldots,t\}$, r $\epsilon\{1,2,\ldots, k\}$ and forms $w_r=a_{j(1,r)}a_{j(2,r)}\ldots a_{j(l\circledR, r)}$ and $w_r'= b_{j(1, r)}b_{j(2,r)}\ldots b_{j(l\circledR, r)}$. He sends w_r to Alice and keeps w_r' for himself.

Alice restores w'_r via computation of $L^{-1}(U')^{-1}w_r'LU=v$, $\varphi(v)$ and $U'L'\varphi(v)(U'L')^{-1}$. $z_r=w'_r$ are collision elements (outputs) of the protocol. The complexity of algorithm is established by the complexity of composition of two elements from $ES_n(K)$ which is $O(n^3)$.

The protocol can be used for the presented access control algorithm. Correspondents can use strings $(r_1,r_2,\ldots,r_m)\epsilon(K^*)^n$ to form entrance password to the system.

5. Algorithm Modification

Assume that z_r is given by the rule

$x_1 \to {}^rq_1 x_1^{\,a(1,1,r)} x_2^{a(1,2,r)} \ldots x_m^{\,a(1,m,r)}$

$x_2 \to {}^rq_2 x_2^{a(2,1,r)}\, x_2^{a(2,2,r)} \ldots\, x_m^{\,a(2,m,r)}$ $\ldots$

$\ldots$

$x_n \to {}^rq_m x_m^{\,a(m,1.r)} x_2^{a(m,2,r)} \ldots\, x_n^{\,a(m,m,r)}$ $\ldots$

We form z_r via consideration of

$g_1(r)={}^rq_1{}^rq_1x_1^{a(1,1,r)}+{}^rq_1{}^rq_2x_2^{a(1,2,r)}+{}^rq_1{}^rq_mx_m^{a(1,m,r)}$

$g_2(r)={}^rq_2{}^rq_1x_1^{a(1,1,r)}+{}^rq_2{}^rq_2x_2^{a(1,2,r)}+{}^rq_2{}^rq_mx_m^{a(1,m,r)}$

$\ldots$

$g_{m,}(r)={}^rq_m{}^rq_1x_1^{a(m,1,r)}+{}^rq_m{}^rq_2x_2^{a(m,2,r)}+{}^rq_1{}^rq_mx_m^{a(m,m,r)}$

and the map

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

We define $G_{i(1)i(2)\ldots i(k)}$ as the rule

$x_1 \to g_1(i(1))g_1(i(2))\ldots g_1(i(k))$,
$x_2 \to g_2(i(1))g_2(i(2))\ldots g_2(i(k))$,
…
$x_m \to g_m(i(1))g_m(i(2))\ldots g_m(i(k))$.

5.1. Modified Access Control Algorithm Based on Protocol

Alice and Bob selects two strings $(j(1), j(2),\ldots j(k(1)))\epsilon\{1,2,\ldots,t\}^{k(1)}$ and $(i(1), i(2),\ldots i(k(2)) \epsilon\{1,2,\ldots,t\}^{k(2)}$.

They form composition $Z_{j(1),j(2),\ldots,j(k(1))}$ of $Z_{j(1)}, Z_{j(2)}, \ldots, Z_{j(k(1))}$ from $ES_m(K)$ and compose it with $G_{i(1)i(2)\ldots i(k(2))}$ $\epsilon CS_m(K)$. They will use this composition C=$C(j(1),j(2),\ldots j(k(1)),i(1),i(2),\ldots,i(k(2))$ of $Z_{j(1),j(2),\ldots,j(k(1))}$ and $G_{i(1)i(2)\ldots i(k(2))}$ in affine Cremona group formally, i. e. without computation of the standard form.

In fact they create string $r=(r_1,r_2,\ldots,r_m)\epsilon(K^*)^m$ and compute $C=C(r)$ with the usage of decomposition C into Z= $Z_{j(1),j(2),\ldots,j(k(1))}$ and G= $G_{i(1)i(2)\ldots i(k)}$ and given above formula in the definitions of Z and G.

Notice that standard forms C are of degree αm for some constant α, the density of C, i.e total number of monomials in its standard form is $O(m^{k(2)+1})$. So the task of adversary to interpolate C via interceptions of pairs of kind r, $c(r)$ is impossible task.

So the only option for adversary is to break the suggested above postquantum protocol.

5.2. On the Symbiotic Combination with One Time Pad

Classical one time pad over additive group K^+ of the ring K is encryption function on the plainspace K^n given by the rule $(x_1,x_2,\ldots x_m \to (x_1,x_2,\ldots x_m)+(p_1,p_2,\ldots,p_m)= (y_1,y_2,\ldots,y_m)$ where password $(p_1,p_2,\ldots,p_m)$ and ciphertext $(y_1,y_2,\ldots,y_m)$.

Alice and Bob can use it via generation of passwords $C(j(1),j(2),\ldots j(k(1)),i(1),i(2),\ldots,i(k(2))(r)$ generated via suggested above protocol based scheme.

Complexity remarks

1) The complexity of protocol is $O(m^3)$
2) The computation of $Z(i)$ in the point $(r_1,r_2,\ldots,r_m)$ takes $O(m^2)$
3) Generation of $g(m)$ takes $O(m^2)$

The complexity of algorithm is $O(m^2(k(1)))+O(m^2(k(2)))$. Suggestion: correspondents can select $k(1)$ and $k(2)$ of size $O(m)$. Then complexity of entire algorithm is $O(m^3)$.

The algorithm is implemented in the cases of finite fields and arithmetical rings of residues modulo q. $q>2$.

6. Conclusion

The paper gives an example of application of protocols of Noncommutative Cryptography (see [10–23]) to the problems of Access Control for Information Systems.

The general scheme can be the following one. Alice and Bob use protocol based on the input (IAS) and output algebraic systems (OAS) given by some generators $a_1, a_2,\ldots, a_n$ and $b_1, b_2, \ldots, b_m$ respectively. Correspondents elaborate in a secure way some elements $c_1, c_2,\ldots, c_t$ which generates the special subsystem (RIS) of OIS. They take element $w=w(c_1, c_2,\ldots,c_t)$ which is known function from hidden generators c_i.

Finally they use some ‘’deformation rule” d to form entrance password $d(w)$ for some Information System IS.

For the selection of appropriate protocol recent cryptanalytical results [24–26] can be used. Flexibility of the method allows generalization for the case of multiuser mode.

Descriptions of cryptographical problems in access control technology and alternative solutions reader can find in [27, 28].

7. References

[1] Max Noether, Luigi Cremona, Mathematische Annalen 59, 1904, 1–19.

[2] V. Ustimenko, On new symbolic key exchange protocols and cryptosystems based on hidden tame homomorphism, Dopovidi NAS of Ukraine, no 10, 26–36, 2018.

[3] V. Ustimenko, M. Klisowski, On Noncommutative Cryptography with cubical multivariate maps of predictable density, in: Intelligent Computing, Proceedings of the 2019 Computing Conference, Volume 2, Part of Advances in Intelligent Systems and Computing (AISC, volume 998), pp. 654-674.

[4] V. Ustimenko, M. Klisowski, On Noncommutative Cryptography and homomorphism of stable cubical multivariate transformation groups of infinite dimensional affine spaces, Cryptology ePrint Archive, 593, 2019.

[5] V. Ustimenko, On the usage of postquantum protocols defined in terms of transformation semigroups and their homomophisms, Theoretical and Applied Cybersecurity, National Technical University of Ukraine "Igor Sikorsky Kiev Polytechnic Institute", vol. 1, no. 2, 32–44, 2020.

[6] V. Ustimenko, On new multivariate cryptosystems based on hidden Eulerian equations, Reports of Nath. Acad of Sci, Ukraine, 5, 17-24, 2017.

[7] V. Ustimenko, On new multivariate cryptosystems based on hidden Eulerian equations over finite fields, ePrint Archive, 093, 2017.

[8] V. Ustimenko, On semigroups of multiplicative Cremona transformations and new solutions of Post Quantum Cryptography, IACR Cryptol, ePrint Arch, 133, 2019.

[9] V. Ustimenko, O. Pustovit, New Cryptosystems of Noncommutative Cryptography based on Eulerian Semigroups of Multivariate Transformations, CPITS 2021, 18-26.

[10] D. N. Moldovyan, N. A. Moldovyan, A New Hard Problem over Non-commutative Finite Groups for Cryptographic Protocols, International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ACNS 2010: Computer Network Security pp 183-194.

[11] L. Sakalauskas, P. Tvarijonas, A. Raulynaitis, Key Agreement Protocol (KAP) Using Conjugacy and Discrete Logarithm Problem in Group Representation Level, INFORMATICA, 2007, vol. 18, No 1, 115-124.

[12] V. Shpilrain, A. Ushakov, The conjugacy search problem in public key cryptography: unnecessary and insufficient,Applicable Algebra in Engineering, Communication and Computing, August 2006, vol. 17, iss. 3–4, 285–289.

[13] Delaram Kahrobaei, Bilal Khan, A non-commutative generalization of ElGamal key exchange using polycyclic groups, In IEEE GLOBECOM 2006 - 2006 Global Telecommunications Conference [4150920] https://doi.org/10.1109/GLOCOM.2006.lications

[14] A. Myasnikov, V. Shpilrain, A. Ushakov, Group-based Cryptography. Berlin: Birkhäuser Verlag, 2008.

[15] A. G. Myasnikov; Vladimir Shpilrain and Alexander Ush akov (2011), Noncommutative Cryptography and Complexity of Group-theoretic Problems, American Mathematical Society

[16] Zhenfu Cao (2012). New Directions of Modern Cryptography. Boca Raton: CRC Press, Taylor & Francis Group. ISBN 978-1-4665-0140-9.

[17] G. Maze, C. Monico, J. Rosenthal, Public key cryptography based on semigroup actions. Adv. Math. Commun. 1(4), 489–507, 2007.

[18] P. H. Kropholler, et al., Properties of certain semigroups and their potential as platforms for cryptosystems, Semigroup Forum, 81: 172–186, 2010.

[19] J. A. Lopez Ramos, et al., Group key management based on semigroup actions, Journal of Algebra and its applications, vol. 16(08):1750148, 2017.

[20] G. Kumar, H. Saini, Novel Noncommutative Cryptography Scheme Using Extra Special Group, Security and Communication Networks ,Volume 2017, Article ID 9036382, 21 pages, https://doi.org/10.1155/2017/9036382.

[21] A. Bessalov, et al., Analysis of 2-isogeny properties of generalized form Edwards curves, in: Proceedings of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems, July 7, 2020, vol. 2746, pp. 1–13.

[22] A. Bessalov, V. Sokolov, P. Skladannyi, Modeling of 3- and 5-isogenies of supersingular Edwards curves, in: Proceedings of the 2nd International Workshop on Modern Machine Learning Technologies and Data Science, June 2–3, 2020, no. I, vol. 2631, pp. 30–39.

[23] A. Bessalov, et al., Computing of odd degree isogenies on supersingular twisted edwards curves, in: Proceedings of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems, January 28, 2021 vol. 2923, 1–11.

[24] V. Roman'kov, An improved version of the AAG cryptographic protocol, Groups, Complex., Cryptol, 11, No. 1 (2019), 35-42.

[25] A. Ben-Zvi, A. Kalka, B. Tsaban, Cryptanalysis via algebraic span, in: Shacham H. and Boldyreva A. (eds.) Advances in Cryptology, CRYPTO 2018. 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part I, Vol. 10991, 255{274, Springer, Cham (2018).

[26] B. Tsaban, Polynomial-time solutions of computational problems in noncommutative-algebraic cryptography, J. Cryptol., 28, no. 3, 601-622, 2015.

[27] S. Contiu, et al., IBBE-SGX: cryptographic group access control using trusted execution environments. In 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2018, Luxembourg City, Luxembourg, June 25-28, 2018, 207–218, 2018.2222

[28] J. Kim, S. Nepal, A Cryptographically Enforced Access Control with a Flexible User Revocation on Untrusted Cloud Storage Data Science and Engineering, vol. 1, 149–160 (2016)