GRAPH BASED SECURE COMMUNICATION WITH ONTOLOGICAL INSTRUMENTS OF KNOWLEDGE BASE PORTAL.

VASYL USTIMENKO AND TYMOTEUSZ CHOJECKI

Keywords: Ontological extraction, Noncommutative Cryptography, Multivariate Cryptography, families of graphs of large girth, graph based cryptography.

We suggest the scheme of usage of protected knowledge base portal B for secure communication of base administrator (Alice) and public user (Bob).

Assume that the information in B is presented in binary alphabet. So we can identify characters of this alphabet with elements of finite field F_{256}. Portal has a search engine. So we can assume that the size of the information through the portal is practically unlimited. The ontological instruments like extraction of key words together with graph presented relation of them are available.

Assume that some secure tools are used to protect the entrance of B. To enter the system user need a password which is a tupple E of length n. We suggest the following access control scheme. Alice and Bob use twisted Diffie - Hellman protocol of Noncommutative Cryptography based on the cubical group $GA(n, F_q), q = 256$ of transformation of vector space $(F_q)^n$ (see author's abstract on CECC 2022 and further references). So, they elaborate multivariate map of kind

$x_1 \to f_1(x_1, x_2, \ldots, x_n), x_2 \to f_1(x_1, x_2, \ldots, x_n), \ldots, x_n \to f_n(x_1, x_2, \ldots, x_n)$. where f_i are written via the list of their monomial terms ordered in lexicographical order. The security of this protocol rests on the Conjugacy Power Problem for the group of automorphisms of $F_q[x_1, x_2, \ldots, x_n]$. This problem is on the list of hard problems of Post Quantum Cryptography.

Assume that f_i contains linear form $a(i,1)x_1 + a(i,2)x_2 ... + a(i,n)x_n$. Alice and Bob use vector $E = (f_1(a(1,1), a(1,2), \ldots, a(1,n)), f_2(a(2,1), a(2,2), \ldots, a(2,n)), \ldots,$ $f_n(a(n,1), a(n,2), \ldots, a(n,n))$ to enter the system. Administrator Alice sets E for user Bob and he enters the base B.

Thus, they can use graph based stream cipher C (see [1]) to work with potentially infinite text from $(F_q)^m, m = n^a, a > 1$. The tupple password which encode two sparse linear transfor-mation and vector of length m has length $3m - 2$.Alice selects the file D from B and mark the position of the file in file directory of B. After Bob and Alice use ontological instruments of B to extract file P of 'key words' from D of size $3n^a - 2$ and use stream cipher C for the information exchange. Linearisation attack require the interception of n^{3a} pairs plaintext-ciphertext. So, after the exchange $1/2n^{3a}$ messages Alice has select other piece D' of information from B for creation of new password P' for cipher C. The scheme is implemented in Ukraine for users of "Taras Shevchenko knowledge portal". Recently we modify stream cipher C to make it resistant to linearisation attacks. The modification will be presented in the talk. Its combinations with other protocols of Noncommutative Cryptography one of the authors will present in his plenary talk at satellite ICM-2022 conference 'Mathematical Aspects of Postquantum Cryptography' (on line event, September, 2022).

References

[1] V. Ustimenko, CRYPTIM: Graphs as Tools for Symmetric Encryption, in Lecture Notes in Computer Science, Springer, 2001, v. 2227, 278-287

Vasyl Ustimenko: University of Maria Curie Sklodowska, Lublin 20-036, Poland;, University of London (Royal Holloway), UK
E-mail address: vasylustimenko@yahoo.pl

Tymoteusz Chojecki: Institute of Mathematics, UMCS, pl. Marii Curie-Skłodowskiej 1, 20-031, Lublin, Poland.
E-mail address: tymoteusz.chojecki@umcs.pl