Quadratic quasigroups in public-key cryptography

Adam Christov
e-mail: adam@christov.cz
Charles University in Prague, Departement of Algebra

Nowadays, cryptology became a part of our daily life even though most people do not realize it. One of the important categories of cryptology is the public-key cryptography (or asymmetric cryptography), which was devised by Diffie and Hellman [1]. In the public-key cryptosystem, we use a couple of different keys – a public key and a private key. The secret encrypted by the public key can be decrypted only by the corresponding private key. It provides us with the potential of establishing an encrypted connection without having to share the secret, moreover, it enables us to sign data digitally. The security of the public-key schemes, which are currently used in practice, relies on just a small number of problems. Mostly, it involves either the problem of factorization (e.g., RSA [6]), or the discrete logarithm (e.g., ECC [4]). Therefore, the research on new cryptography schemes, particularly based on other classes of problems, is of utmost importance.

In my talk I will focus on an innovative structure of a public-key scheme based on multivariate quadratic quasigroups (MQQ, [3]). It represents a special type of an MQ-scheme. In general, the MQ-schemes rely on the problem of finding a solution of a system of multivariate quadratic equations (MQ-problem, [7]). The private key in the MQ-scheme is a soluble system of n quadratic equations $\mathcal{P}(x)$ in n variables over the field $\mathbb{F}_2$, and two automorphisms of vector space $\mathbb{F}_2^n$, denoted by $\mathcal{L}_1$ and $\mathcal{L}_2$. The public key is the system of equations

$$\mathcal{P}'(x) = \mathcal{L}_2\Big(\mathcal{P}\big(\mathcal{L}_1(x)\big)\Big).$$

Therefore, finding the private key based on knowledge of the public key in the MQ-scheme relies on the complexity of decomposition of $\mathcal{P}'(x)$ into $\mathcal{L}_1$, $\mathcal{L}_2$, and $\mathcal{P}$ [7]. MQQ is based on an algorithm generating the system $\mathcal{P}(x)$ from a special kind of quasigroups, the so-called quadratic quasigroups. A cipher based on MQQ is in compare to currently used public-key ciphers much more faster, especially in encryption. There are also some disadvantages of this scheme. The public key is very large which make an implementation on low-performance devices (e.g., smartcards) more difficult. There was recently published an cryptoanalysis attack [5] which uses MutantXL algorithm to solve a system of quadratic equations. I will present some ideas how to improve this scheme to be resistant against this attack.

A quadratic quasigroup is defined as a quasigroup upon the vector space $\mathbb{F}_2^n$ with an operation which can be represented by a vector of quadratic boolean polynomials. I will show that every quadratic quasigroup can be described by means of four parameters. Two of which depend upon permutations of $\mathbb{F}_2^n$ that can be described by quadratic forms (I call them quadratic permutations). The further two parameters are a translation vector and a bilinear map. Our ability

to generate quadratic quasigroups depends, to a large extent, upon the ability to find quadratic permutations efficiently.

The property of being a quadratic quasigroup is not isotopically invariant. However, if the permutations used by an isotopy are linear and one of the quasigroups is quadratic, then the other quasigroup is quadratic as well. Under certain additional conditions this is true also in the case when the isotopy permutations are quadratic. The achieved results can be used to derive quickly many further quadratic quasigroups that are isotopic to a known quadratic loop.

Quadratic loops have only two structural invariants, i.e., a unit and a bilinear map. I will present necessary conditions for bilinear map to represent a quadratic loop. It provides a heuristic algorithm for generating these loops. They can be used for generating further quadratic quasigroups, but they are also interesting as an algebraic object.

References

[1] Diffie W., Hellman M., *New Directions in Cryptography*, IEEE Trans. Information Theory, Vol. IT-**22**,No **6**, (1976), 644654

[2] Christov A., *Diploma Thesis*
`http://artax.karlin.mff.cuni.cz/~chria3am/thesis/`

[3] Gligoroski D., Markovski S., Knapskog S.J.: *A Public Key Block Cipher Based on Multivariate Quadratic Quasigroups,* arXiv:**0808.0247v1** (2008)

[4] Koblitz N., *Elliptic curve cryptosystems*, Mathematics of Computation **48**, (1987), 203209

[5] Mohamed M.S.E., Ding J., Buchmann J., Werner F., *Algebraic Attack on the MQQ Public Key Cryptosystem*, Lecture Notes in Computer Science, ISBN **978-3-642-10432-9**, (2009) 392-401

[6] Rivest R. , Shamir A., Adleman L., *A Method for Obtaining Digital Signatures and Public Key Cryptosystems*, Comm. ACM, Vol. **21**, No. **2**, (1978), 120126

[7] Wolf C., Preneel B.: *Taxonomy of Public Key Schemes based on the problem of Multivariate Quadratic equations,* K.U.Leuvenm ESAT-COSIC, Belgium, Cryptology ePrint Archive, Report **2005/077** (2005)