On public-key cryptosystem MST_3 and its realization

Tran van Trung, University of Duisburg-Essen
Joint work with Pavol Svaba

We are concerned with the new public-key cryptosystem MST_3 based on non-abelian finite groups. To begin with, we describe the concept of covers and logarithmic signatures for finite groups. A *cover* $\alpha = [A_1, \ldots, A_s]$ of type $(r_1, \ldots, r_s)$, $s \geq 2$ for a subset H of a finite group G can be viewed as an ordered collection of subsets A_i of G with $|A_i| = r_i$ such that each element $h \in H$ can be expressed in at least one way as a product of the form

$$h = g_1 \cdot g_2 \cdots g_{s-1} \cdot g_s \tag{1}$$

for $g_i \in A_i$. If every $h \in H$ can be expressed in exactly one way, then α is called a *logarithmic signature* for H. If $H = G$ then α is called a cover (resp. logarithmic signature) for G. A cover α is called *tame* if the factorization in (1) can be achieved in time polynomial with the *width* $w = \lceil \log |H| \rceil$ of H, it is called *wild* otherwise. There are instances for α and G showing that the factorization in (1) is intractable [1]. The transversal logarithmic signatures obtained from the coset representatives of a chain of subgroups of G are examples of tame logarithmic signatures. Any cover α for G induces a surjective mapping

$$\breve{\alpha} \quad : \quad Z_m \to G$$

where $m = \prod_{i=1}^{s} r_i$. If α is a logarithmic signature for G, then $\breve{\alpha}$ is a bijection. The mapping $\breve{\alpha}$ is efficiently computed by a mixed radix representation of the integers in Z_m.

Given an element $g \in G$, to determine any element $x \in \breve{\alpha}^{-1}(g)$ it is necessary to obtain any one of the possible factorizations of type (1). This is possible if and only if α is tame. For this reason it is conceivable that $\breve{\alpha}$ is a one way function if α is a wild cover. Therefore we make use of the following cryptographic hypothesis that if α is a random cover for a "large" subset H of G, then finding a factorization in (1) is an intractable problem.

The usage of covers and logarithmic signatures for non-abelian finite groups in public-key cryptography was first introduced in [1]. In that paper the cryptosystem MST_1 is proposed on the basis of wild logarithmic signatures and the MST_2 on random covers. The recent developed public-key cryptosystem called MST_3 [2] exploits logarithmic signatures and covers for non-abelian groups. The main idea of the generic version of MST_3 can be described as follows: Beginning with a random cover α for a subset of a non-abelian group G one obtains a random cover $\tilde{\alpha}$ by using a so-called two-sided transform. Then, using $\tilde{\alpha}$ and a tame logarithmic signature β for the center of G one constructs a random cover γ for a second subset of G. Now make α and γ public and keep β and the information used in transforming α to $\tilde{\alpha}$ secret. This secret forms the trapdoor for the system.

For a realization of MST_3 the Suzuki 2-groups of order q^2, $q = 2^m$, have been proposed [2]. Specially the matrix form representation of the Suzuki 2-groups enables an efficient implementation of MST_3. The important fact about using these groups, however, is that they allow us to rigorously carry out the analysis of two conceivable attacks on the system, a direct and a chosen plaintext attack. As a result a lower bound for the work effort required in terms of the size of the Suzuki 2-groups is obtained [2]. In [3] a further analysis of the realization provides a stronger lower bound and in particular we show that the transversal logarithmic signatures are unfit to use in this realization.

In this talk we present two approaches to improve the system MST_3. The basic idea of the methods consists in integrating the logarithmic signature β into a random cover for the center of G and the latter is used to create public-key γ. The methods show that restriction on the properties of the logarithmic signatures is no longer required. Consequently, the transversal logarithmic signatures, for instance, can be used in these improved versions of MST_3. We then determine the complexity for the lower bounds of the above mentioned attacks on the new versions with the Suzuki 2-groups. We will report experimental results of an implementation of the improved

versions. Finally, we discuss the choice of suitable parameters for an efficient realization of the system and its practical usage.

References

[1] S. S. Magliveras, D. R. Stinson and Tran van Trung, *New approaches to designing public key cryptosystems using one-way functions and trapdoors in finite groups*, J. Cryptology, **15** (2002), 285–297.

[2] W. Lempken, S. S. Magliveras, Tran van Trung, W. Wei, *A public key cryptosystem based on non-abelian finite groups*, submitted to J. Cryptology.

[3] S. S. Magliveras, P. Svaba, Tran van Trung, P. Zajac, *On the security of a realization of cryptosystem* MST_3, Preprint.