Code-Based Cryptosystems Using Generalized Concatenated Codes

Karim Ishak, Sven Müelich, Sven Puchinger, Martin Bossert

Ulm University, Germany,
{karim.ishak, sven.mueelich, sven.puchinger, martin.bossert}@uni-ulm.de

Public-key cryptosystems nowadays are mostly based on number theoretic problems like factorization (RSA) and the discrete logarithm problem (Elgamal). However, such systems can be broken with quantum computers by applying Shor's algorithms [1] for solving both problems, factorization and discrete logarithm, in polynomial time. Hence there is a need for post-quantum cryptography, i.e., methods resisting quantum computers. Code-based cryptography, introduced by McEliece in 1978 [2], is one of these candidates. In the original work, the McEliece cryptosystem uses Goppa codes. Ongoing research work is investigating other classes of codes for use in this cryptosystem.

Code-based cryptosystems based on Ordinary Concatenated (OC) codes were suggested by Nicolas Sendrier in [3]. OC codes are characterized by a lower decoding complexity than non-concatenated codes. However, in order to reach the same level of security as the original cryptosystem, systems based on OC codes require larger key sizes than the ones based on Goppa codes. Generalized Concatenated (GC) codes also have the advantage of low decoding complexity at the cost of possessing larger key sizes. As explained in [4], comparing a GC and an OC code with the same number of codewords, a GC code has a larger minimum distance. On the other hand, when they both have the same minimum distance, a GC code has more codewords.

In [3, 5], it is shown that the structure of a randomly permuted OC code could be discovered. A cryptosystem using OC codes, can then be attacked through obtaining the structure of the inner and outer codes from the public generator matrix. The attack consists of three main steps. The first step is based on identifying the positions of the inner code blocks. The second step orders the positions of the elements of the inner code blocks with respect to each other. Finally, in the third step, a generator matrix for an equivalent inner code is obtained. Moreover, a generator matrix of a π-equivalent outer code is also obtained, where π symbolizes the Frobenius field automorphism and also any power of π results in a field automorphism. After obtaining the structures of the inner and outer codes, already known attacks could be applied to each of them in order to break the whole system.

In this work, code-based cryptosystems using GC codes are analyzed in light of Sendrier's attack [3, 5]. If a GC code could be converted to an OC code, the attack would be directly applicable. However, it is mentioned in [6] that this conversion in general leads to a nonlinear outer code of the OC code. We show that this conversion always leads to a nonlinear outer code of the OC code if the outer codes of the GC code are not all exactly the same, i.e, do not contain the same set of codewords.

Sendrier's attack is only partially applicable in a direct way to systems using GC codes. The first part of the attack can be applied just as for the case of OC codes but with corresponding conditions for the case of GC codes. The second step of the attack also works straightforwardly. A generator matrix of an equivalent inner code could also be obtained. However, the part of the third step of the attack, which is responsible for obtaining a π-equivalent outer code, is not directly applicable. We present a non-structural alternative to this third step that works for both OC and GC codes. Its applicability is based on the corresponding work factor. For the code parameters suggested by Sendrier in [3], the attack results in a work factor that is considered to be insecure. This attack is applied after the first and second steps of Sendrier's attack and after obtaining the generator matrix of an equivalent inner code. It is non-structural because it does not obtain a certain structure for the outer code. However, it is able to reconstruct the message. This non-structural attack is mainly based on the information set decoding attack which is mentioned in [2].

Sendrier's attack on cryptosystems using GC codes is restricted to certain constraints, similar to OC codes. We investigate the possibilities of choosing GC codes that might resist the attack, e.g., when the dual distance of the inner code is greater than or equal to the minimum of the minimum distances of the outer codes. In this case, the first step of Sendrier's attack is not guaranteed to work. Our work aims to provide an idea which GC codes might be suited for McEliece cryptosystems.

References

[1] Peter W. Shor, *Algorithms for Quantum Computation: Discrete Logarithms and Factoring*, 35th Annual Symposium on Foundations of Computer Science, 1994 Proceedings. pp. 124–134, IEEE (1994).

[2] Robert J. McEliece, *A Public-Key Cryptosystem Based On Algebraic Coding Theory*, DSN progress report. 42(44), pp. 114-116 (1978).

[3] Nicolas Sendrier, *On the Structure of Randomly Permuted Concatenated Code*, research report, RR-2460 <inria-00074216> (1995).

[4] Martin Bossert, *Channel Coding for Telecommunications*, John Wiley & Sons, Inc. (1999).

[5] Nicolas Sendrier, *On the Concatenated Structure of a Linear Code*, Applicable Algebra in Engineering, Communication and Computing. 9(3), pp. 221-242, Springer (1998).

[6] Hervé Chabanne and Nicolas Sendrier, *On the concatenated structures of a [49, 18, 12] binary abelian code*, Discrete mathematics. 112(1), pp. 245-248, Elsevier (1993).