THE SECURITY OF THE MCELIECE CRYPTOSYSTEM AND ITS VARIANTS

SUMMER 2010 NSERC USRA REPORT

SI RYUN SIERRA LEE

During this summer, I studied the McEliece cryptosystem with Professor Hamid Usefi. We cryptanalyze the McEliece cryptosystem and its variants which were based on made on BCH codes or GRS codes in order to reduce the size of the public key. However, these variants were not resistant to the Sidelnikov-Shestakov attack, so Berger and Loidreau proposed the cryptosystem based on subcodes of GRS Codes, which was finally resistant to the Sidelnikov-Shestakov attack.

1. Introduction

After Robert McEliece proposed public key cryptosystem based on the difficulty of decoding linear codes in Hamming matric in 1978, mathematicians have suggested the various versions of the McEliece cryptosystem such as the Niederreiter cryptosystem based on a GRS code, and the Berger-Loidreau cryptosystem based on subcodes of a GRS code. To shorten the size of public keys for code-based cryptosystem such as McEliece/Niederreiter scheme, BCH code was proposed by using its cyclicity and quasi-cyclicity. However, it turned out to be not as secure as the original McEliece's. Another alternative approach for code based cryptography was proposed: Generalized Reed Solomon Code was used instead of the Goppa code which was usually used in the McEliece Cryptosystem. Again, the use of GRS code was proven to be insecure against an attack by Sidelnikov and Shestakov. Later, Berger and Loidreau suggested a modified Niederreiter that was resistant to Sidelnikov-Shestakov attack by using the properties of GRS subcodes. Despite there are many attacks on these variants of the McEliece cryptosystem, the original scheme is still unbreakable to any structural attack.

However, Even though the McEliece system and its Niederreiter system have better encryption and decryption than asymmetric schemes

Date: September 13, 2010.

Key words and phrases. McEliece cryptosystem, Niederreiter cryptosystem, Berger-Loidreau cryptosystem, cryptanalysis, Reed-solomon codes, BCH codes.

such as RSA, they are less practical than RSA since they require very large key sizes.

Therefore, it is crucial to find a way to reduce the representation of a linear code in a secure way.

2. The McEliece PKC

R.J.McEliece constructed a public-key cryptosystem based on the existence of Goppa codes.[E]

- Private Key: a random $k \times k$ binary invertible matrix S and a random $n \times n$ permutation matrix P
- Public Key: $G' \equiv SGP$ where G is a generator matrix of the secret code C
- Encryption: the plaintext m, k-bit message, is sent to as the ciphertext $c = mG' + e$ where e is a random n - bit error vector of weight t
- Decryption: compute $cP^{-1} = mSG + eP^{-1}$, and recover mS using a fast decoding algorithm for C. The plaintext message is given by $m = (mS)S^{-1}$.

3. Conclusion

The code based cryptography, the McEliece Public Key Cryptosystem, has faster encryption and decryption than RSA, which can extend the battery life of cryptographic applications on mobile devices. However,the size of public key is too large to be practical. To enhance this drawback of the McEliece PKC cryptosystem and Niederreiter cryptosystem, many attempts to reduce the key sizes have been made. First, By using the cyclicity of BCH code,the size of public key was reduced,but it was insecure against structural attacks. Next, GRS code used, but it was insecure as well against Sidelnikov-Shestakov attack. So, Berger and Loidreau modified the Niederreiter system based on GRS code, which is resistant to Sidelnikov and Shestakov attack.

So far, nothing can compete with the McEliece cryptosystem regarding its security, so further work should focus on the cryptosystem which has a smaller size as well as long-term security is still guaranteed.

References

[E] R.J. McEliece, A public-key cryptosystem based on algebraic coding theory, *JPL DSN Progress Report*, pages 114-116, 1978.