McEliece As An Alternative Cryptosystem

Djatnika (13502016)[1], Riko Boestari (13502027)[2], Leonardo Z Tomarere (13502028)[3]

Laboratorium Ilmu dan Rekayasa Komputasi
Departemen Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if12016@students.if.itb.ac.id[1], if12027@students.if.itb.ac.id[2], if12028@students.if.itb.ac.id[3]

Abstract

Since the concept of public-key cryptography appeared in 1977, searching for secure public-key cryptosystems and identification schemes has been one of the most active areas in the field of cryptology. Many public-key ciphers emerged just after the invention of RSA and their underlying problems were as varied as computing a discrete logarithm, solving a knapsack problem, inverting some polynomial equations over a finite field. But the development of some cryptanalysis methods has finally made most of them insecure. However the class of public-key ciphers and identification schemes based on error-correcting codes still resists cryptanalysis. One of the most famous of these systems is McEliece cipher. It is at the moment one of the few alternatives to the common public-key algorithms based on number theory. This public-key cipher is particularly interesting since it runs much faster than any algorithm relying on number theory. Therefore, we try to review McEliece cryptosystem in this paper: its description, strengths, drawbacks, security, and usage in digital signature.

Keywords: public-key cryptography, cryptosystem, cryptology, public-key cipher, cryptanalysis method, error-correcting codes, McEliece, number theory, digital signature.

1. Introduction

The McEliece cryptosystem is an asymmetric key algorithm developed in 1978 by Robert McEliece. The algorithm has never gained much acceptance in the cryptographic community like RSA. This cryptosystem is similar to the Merkle-Hellman Knapsack cryptosystem in that it takes an easy case of an NP-problem and disguises it to look like the hard instance of the problem. In this cryptosystem, the problem that is used is drawn from the theory of error-correcting codes.

Syndrome decoding of linear codes (when considered as a decision problem) is an NP-complete problem if the number of errors is not bounded. However, there are classes of linear codes which have very fast decoding algorithms. The basic idea of the McEliece system is to take one of these linear codes and disguise it so that Oscar, when trying to decrypt a message, is forced to use syndrome decoding, while Bob, who set up the system, can remove the disguise and use the fast decoding algorithm. McEliece suggested using **Goppa Codes**, which are linear codes with a fast decoding algorithm, in the system,

but any linear code with a good decoding algorithm can be used.

2. Error Correction and Detection

In computer science and information theory, the issue of error correction and detection has great practical importance. Error detection is the ability to detect errors that are made due to noise or other impairments in the course of the transmission from the transmitter to the receiver. Error correction has the additional feature that enables localization of the errors and correcting them.

Error correction schemes permit error localization but also give the possibility of correcting errors that have been introduced. Error correction and detection schemes find use in implementations of reliable data transfer over noisy transmission links, data storage media (including dynamic RAM, compact discs), and other applications where the integrity of data is important.

3. The McEliece Public-Key Cryptosystem

McEliece consists of three algorithms: a probabilistic key generation algorithm which produces a public and a private key, a probabilistic encryption algorithm, and a deterministic decryption algorithm.

All users in a McEliece deployment share a set of common security parameters: n, t, k. Recommended values for these parameters are n=1024, t=38, k=644.

Keygeneration Algorithm

- Users select a binary (n,k)-linear code C capable of correcting t errors. This code must possess an efficient decoding algorithm.
- Alice generates a kxn generator matrix G for the code C.
- Select a random kxk binary non-singular matrix S.
- Select a random nxn permutation matrix P.
- Compute kxn matrix G'=SGP.
- Alice's public key is (G', t); her private key is (S, G, P).

Message Encryption

Suppose Bob wishes to send a message m to Alice whose public key is (G', t):

- Encode the message as a binary string of length k.
- Compute the vector c'=mG'.
- Generate a random n-bit vector z containing at most t ones.
- Compute the cipher text as c = c' + z

Message Decryption

- Compute the inverse of P, P^{-1}.
- Compute $c'=cP^{-1}$.
- Use the decoding algorithm for the code C to c' to m'.
- Compute $m=m'S^{-1}$.

4. Strengths

1. McEliece is strong against cryptanalysis. Attempts have been made to cryptanalyze McEliece, but none have been successful.
2. This public-key cipher runs much faster than any algorithm relying on number theory.

5. Drawbacks

There are two major concerns with the McEliece cryptosystem:

1. The size of the public key (G') is quite large. Using the Goppa code with parameters suggested by McEliece, the public key would consist of 2^{19} bits. This will certainly cause implementation problems.
2. The encrypted message is much longer than the plaintext message. This increase of the bandwidth makes the system more prone to transmission errors.

5. McEliece Cryptosystem Security

The McEliece cryptosystem is considered to be fairly secure. Attempts have been made to cryptanalyze McEliece, but none have been successful. However, the algorithm is never used in practice because of the massive keys and because the cipher text is twice as large as the plaintext. The similarity between this algorithm and the knapsack problem (which has been proven insecure) also worries some.

In 1986, Rao and Nam proposed a variant of the system using only one matrix to disguise the problem and the following year Struik and Tilburg showed how to break the Rao-Nam system. Up till now, many people have contributed in modifying McEliece cryptosystem to strengthen its security without increasing the size of the public key. This greatly strengthens the system against the decoding attacks.

6. Usage of McEliece Cryptosystem in Digital Signature

It is widely believed that code-based do not allow practical digital signatures. McEliece is considered can not be used for authentication or signature schemes because the encryption algorithm is not one-to-one and the total algorithm is truly asymmetric (encryption and decryption do not commute). The problem open for more than 20 years have been recently solved by Matthieu Finiasz, Nicolas Sendrier, and Nicolas Courtois. McEliece instead gives the shortest signatures ever known: 87 bits and for the binary workfactor of 2^{85}, signing time of 30 seconds and verification time of about 1 second. For information, the shortest signature scheme previously known was Quartz with 128 bits.

In their journal, "How to achieve a McEliece-based Digital Signature Scheme", Nicolas Courtois, Matthieu Finiasz, and Nicolas Sendrier proposed schemes that have tight security proofs in random oracle model. They are based on the well known hard syndrome decoding problem that after some years of research is still exponential. The table below summarizes the concrete security of their schemes (McEliece Digital Signature) compared to some other known signature schemes.

base cryptosystem	RSA	ElGamal	EC	HFE	McEliece/Niederreiter		
signature scheme	RSA	DSA	ECDSA	Quartz	CFS1	CFS2	CFS3
data size(s)	1024	160/1024	160	100	144		

security						
structural problem	factoring	DL(p)	Nechaev group?	HFEv-	Goppa $\stackrel{?}{=}$ PRCode	
best structural attack	$\mathbf{2^{102}}$	2^{102}	∞	$> 2^{97}$	2^{119}	
inversion problem	RSAP	DL(q)	EC DL	MQ	SD	
best inversion attack	2^{102}	$\mathbf{2^{80}}$	$\mathbf{2^{80}}$	2^{100}	$\mathbf{2^{83}}$	

efficiency							
signature length	1024	320	321	128	132	119	**81**
public key [kbytes]	0.2	0.1	0.1	71	1152		
signature time 1 GHz	9 ms	1.5 ms	5 ms	15 s	$10-30$ s		
verification time 1 GHz	9 ms	2 ms	6 ms	40 ms	$< 1\ \mu$s	< 1 ms	≈ 1s

The proposed McEliece-based signature schemes have unique features that will make it an exclusive choice for some applications while excluding other. On one hand, we have seen that both key size and signing cost will remain high, but will evolve favorably with technology. On the other hand the signature length and verification cost will always remain extremely small.

7. Conclusion

1. McEliece cryptosystem is an asymmetric key algorithm developed in 1978 by Robert McEliece. The algorithm uses Goppa codes, which are a type of error-correcting code. The algorithm disguises a Goppa code made from the plaintext as a general linear code. Goppa codes are easy to decode, but distinguishing them from a general linear code is hard. This is McEliece's hard problem.
2. McEliece algorithm has never gained much acceptance in the cryptographic community like RSA since it creates very large public key. But with technology evolve, this is not a big problem anymore.
3. McEliece cipher runs much faster than any algorithm relying on number theory. One of its implementation in cryptology is digital signature. McEliece-based signature gives the shortest signatures ever known: 87 bits and for the binary workfactor of 2^{85}, signing time of 30 seconds and verification time of about 1 second [7].

8. References

[1] *McEliece Cryptosystem*, http://en.wikipedia.org, diakses tanggal 27 Desember 2005 pukul 11:00 WIB.

[2] *The New McEliece-based Signature Scheme CFS*, http://eprint.iacr.org/2001/010/, diakses tanggal 27 Desember 2005 pukul 11:00 WIB.

[3] *Public-key Cryptosystems Based On Error-correcting Codes*, http://www-rocq.inria.fr/, diakses tanggal 27 Desember 2005 pukul 11:00 WIB.

[4] *What is McEliece Cryptosystem?*, http://www.x5.net/faqs/crypto/, diakses tanggal 27 Desember 2005 pukul 11:00 WIB.

[5] Alfred J. Menezes, Scott A. Vanstone, A. J. Menezes and Paul C. van Oorschot, Handbook of Applied Cryptography.

[6] *Error Correction and Detection*, http://en.wikipedia.org/wiki/Error-correcting_code, diakses tanggal 27 Desember 2005 pukul 11:00 WIB.

[7] Matthieu, Finiasz. *How to achieve a McEliece-based Digital Signature Scheme*. 2004. Toulon University, France.

[8] C. McFarlane and Y. Sauls. 2005. *McEliece's Cryptosystem*.