Surveys in Mathematics and its Applications

ISSN 1842-6298 (electronic), 1843-7265 (print)
Volume **5** (2010), 73 – 82

A FUZZY COMMITMENT SCHEME WITH MCELIECE'S CIPHER

Deo Brat Ojha and Ajay Sharma

Abstract. In this paper an attempt has been made to explain a fuzzy commitment scheme with McEliece scheme. The efficiency and security of this cryptosystem is comparatively better than any other cryptosystem. This scheme is one of the interesting candidates for post quantum cryptography. Hence our interest to deal with this system with fuzzy commitment scheme. The concept itself is illustrated with the help of a simple situation and the validation of mathematical experimental verification is provided.

1 Introduction

In cryptography, a commitment scheme or a bit commitment scheme is a method that allows a user to commit to a value while keeping it hidden and preserving the user's ability to reveal the committed value later. A useful way to visualize a commitment scheme is to think of the sender as putting the value in a locked box, and giving the box to the receiver. The value in the box is hidden from the receiver, who cannot open the lock (without the help of the sender), but since the receiver has the box, the value inside cannot be changed. Commitment schemes are important to a variety of cryptographic protocols, especially zero-knowledge proofs and secure computation.

Bit-commitment from any one-way function: One can create a bit-commitment scheme from any one-way function. The scheme relies on the fact that every one-way function can be modified to possess a computationally hard-core predicate. Let w be a one-way function, with j a hard-core predicate. Then to commit to a bit e Alice picks a random input t and sends the triple $(j, w(t), e + j(t))$ to Bob, where $+$ denotes XOR, i.e. addition $modulo 2$. To decommit Alice simply sends t to Bob. This scheme is concealing because for Bob to recover e he must recover $j(t)$. Since j is a computationally hard-core predicate, recovering $j(t)$ from $w(t)$ with probability greater than one-half is as hard as inverting w.

2010 Mathematics Subject Classification: 94A60; 94B40; 11T71.
Keywords: Cryptography; Error Correcting Codes; Fuzzy logic and Commitment scheme; McEliece scheme.

The scheme bindingness depends greatly on whether or not w is injective. For more knowledge readers may see [12, 13, 14].

McEliece proposed the first public-key cryptosystem (the McEliece Scheme) based on algebraic coding theory in 1978 [1]. The idea behind McEliece public-key cryptosystem is based on the fact that the decoding problem of an arbitrary linear code is an NP-hard problem [2].The McEliece scheme has the advantage of high speed encryption and decryption and this system employs probabilistic encryption [3, 4], which is better than other type of deterministic encryption [5, 6] in preventing the elimination of any information leaked through public-key cryptography.

It is point of remark [15] that the security comparison is made here for classical attackers.

The picture changes drastically to the advantage of the McEliece system if we consider two systems to offer the same level of security if breaking them requires quantum computers with the same number of qubits. Protocols are essentially a set of rules associated with a process or a scheme defining the process. Commitment protocols were first introduced by Blum [7].

Efficiency and security of the McEliece cryptosystem vs RSA crypttosystem

Table No.1 [15]:		Work factor (binary operations)		
System	Size public key (bytes)	Encryption/ Block size	Decryption/ Block size	Best Attack
McEliece [1024 · 524 · 101]	$67,072$	2^{9}	$2^{13.25}$	2^{65}
RSA 362-bit Modulus	46	2^{17}	2^{17}	2^{68}
McEliece [2048 · 1025 · 187]	$262,400$	2^{10}	$2^{14.5}$	2^{107}
RSA 1024-bit Modulus	256	2^{20}	2^{20}	2^{110}
RSA 2048-bit Modulus	512	2^{22}	2^{22}	2^{145}
McEliece [4096 · 2056 · 341]	$1,052,672$	2^{11}	$2^{15.5}$	2^{187}
RSA4096-bit Modulus	1024	2^{24}	2^{24}	2^{194}

Moreover in the conventional commitment schemes, opening key are required to enable the sender to prove the commitment. However there could be many instances where the transmission involves noise or minor errors arising purely because of the factors over which neither sender nor the receiver have any control , which creates uncertainties. Fuzzy commitment scheme was first introduced by Juels and

Martin [8]. The new property "fuzziness" in the open phase to allow, acceptance of the commitment using corrupted opening key that is close to the original one in appropriate metric or distance.

We combine well-known techniques from the areas of error-correcting codes and cryptography to achieve a improve type of cryptographic primitive. Fuzzy commitment scheme is both concealing and binding: it is infeasible for an attacker to learn the committed value, and also for the committer to decommit a value in more than one way. In a conventional scheme, a commitment must be opened using a unique witness, which acts, essentially, as a decryption key. , it accepts a witness that is close to the original encrypting witness in a suitable metric, but not necessarily identical. This characteristic of fuzzy commitment scheme makes it useful for various applications. Also in which the probability that data will be associate with random noise during communication is very high. Because the scheme is tolerant of error, it is capable of protecting data just as conventional cryptographic techniques.

2 Preliminaries

2.1 Crisp Commitment Schemes

In a commitment scheme, one party Alice(sender) aim to entrust a concealed message m to the second party Bob(receiver) , intuitively a commitment scheme may be seen as the digital equivalent of a sealed envelope.

If Alice wants to commit to some message m she just puts it into the sealed envelope, so that whenever Alice wants to reveal the message to Bob , she opens the envelope. First of all the digital envelope should hide the message from : Bob should be able to learn m from the commitment. Second, the digital envelope should be binding , meaning with this that Alice can not change her mind about m, and by checking the opening of the commitment one can verify that the obtained value is actually the one Alice had in mind originally.

2.2 The McEliece public-Key Cryptosystem

Secret Key: W is a random $(k \times k)$ nonsingular matrix over $GF(2)$, called the scrambling matrix, T is a $(k \times n)$ generator matrix of binary Goppa code T with the capability of correcting an n-bit random error vector of weight less than or equal to a, and Q is a random $(n \times n)$ permutation matrix.

Public Key: $V = WTQ$

Encryption: $c = mV + e$, where m is a n -bit message, c is n -bit ciphertext, and e is an n -bit random error vector of weight a.

Decryption: The receiver first calculates

$$c\prime = cQ^{-1} = mWT + eQ^{-1},$$

where Q^{-1} is the inverse of Q. Because the weight of eQ^{-1} is the same as the weight of e, the receiver uses the decoding algorithm of the original code T to obtain $m\prime = mW$. Finally, the receiver recovers m by computing $m = m\prime W^{-1}$, where W^{-1} is the inverse of W.

Definition 1. *A metric space is a set C with a distance function*

$$dist : C \times C \to \mathbb{R}^+ = [0, \infty)\,,$$

which obeys the usual properties (symmetric, triangle inequalities, zero distance between equal points).

Definition 2. *Let $C\{0,1\}^n$ be a code set which consists of a set of code words c_i of length n. The distance metric between any two code words c_i and c_j in C is defined by*

$$dist\,(c_i, c_j) = \sum_{r=1}^{n} |c_{ir} - c_{jr}|\,, \quad c_i, c_j \in C.$$

This is known as Hamming distance [9].

Definition 3. *An error correction function f for a code C is defined as*

$$f\,(c_i) = \{c_j\,|dist\,(c_i, c_j) \;\text{ is the minimum, over } C\backslash\{c_i\}\}\,.$$

Here, $c_j = f\,(c_i)$ is called the nearest neighbor of c_i.

Definition 4. *The measurement of nearness between two code words c and c' is defined by*

$$nearness(c, c') = dist(c, c')/n,$$

it is obvious that $0 \leq nearness(c, c\prime) \leq 1$.

Definition 5. *The fuzzy membership function for a codeword c' to be equal to a given c is defined as [10]*

$$FUZZ\,(c') = \begin{cases} 0 & \text{if } nearness(c, c') = z \leq z_0 < 1, \\ z & \text{otherwise.} \end{cases}$$

3 Fuzzy Commitment Scheme with McEliece scheme

First select secret key W is a random $(k \times k)$ nonsingular matrix over $GF(2)$ called the scrambling matrix, T is a $(k \times n)$ generator matrix of a binary Goppa code T with the capability of correcting n –bit random error vector of weight less than or equal to a, and Q is a random $(n \times n)$ permutation matrix.

Public Key: $V = WTQ$

A tuple $\{P, H, M, f\}$ where $M \subseteq \{0,1\}^k$ is a message set which consider as a code, P is a set of individuals, generally with three elements A as the committing party, B as the party to which commitment is made and TC as the trusted party, f is error correction function and $H = \{t_i, a_i\}$ are called the events occurring at times t_i, $i = 0, 1, 2$, as per algorithm a_i, $i = 0, 1, 2$. The scheme always culminates in either acceptance or rejection by A and B.

In the setup phase , the environment is setup initially and public commitment key CK generated, according to the algorithm $setupalg(a_0)$ and published to the parties A and B at time t_0. During the commit phase, Alice commits to a message $m \in M$ then she finds $g : m \rightarrow mV$.

Encryption: $E = mV + e$, where m is the k -bit message, E is an n -bit cipher text and e is an n -bit random error vector of weight a.

According to the algorithms $commitalge_1$ into string c i.e. her commitment

$$c = commitalg(XOR, g(m), E),$$

then after Alice sends c to Bob, which Bob will receive as $t(c)$, where t is the transmission function which includes noise.

In the open phase, Alice sends the procedure for revealing the hidden commitment at time t_2 and Bob use this.

So Alice discloses the procedure $g(m)$ and E to Bob to open the commitment.

$openlg(e2)$: Bob constructs $c\prime$ using $commitalg$, message $t(m)$ and opening key i.e.

$$c\prime = commitalg(XOR, t(g(m)), t(E))$$

and checks whether the result is same as the received commitment $t(c)$.

Fuzzy decision making

$$\begin{aligned} &\text{If } \left(nearness\left(t\left(c\right), f\left(c'\right)\right) \leq Z_0\right) \\ &\quad \text{Then A is bound to act as in } m \\ &\quad \text{Else he is free not to act as } m. \end{aligned}$$

Then after acceptance, Bob calculates $f\left(c'\right)\left(WTQ\right)^{-1}$ and finally gets the message.

4 Our Process for simple Illustration

Secret Key: W is a random (4×4) nonsingular matrix over $GF(2)$, called the scrambling matrix, T is a (4×7) generator matrix of binary Goppa code T with the capability of correcting an 7-bit random error vector of weight less than or equal to a, and Q is a random (7×7) permutation matrix.

Public Key: $V = WTQ$

Encryption: Let $g : m \to mV$, where m is a 4-bit message. Then after for the sake of secrecy add error e, which is a 7-bit random error vector of weight a. then $E = g(m) + e$, E is a 7-bit ciphertext.

Now commitment

$$c = commitalg(CK, g(m), E).$$

Decryption : The receiver first calculates $c\prime = commitalg(CK, t(g(m)), t(E))$, where t is the transmission function. The receiver checks the $dist(t(c), c') \neq 0$, then apply Error Correction function f to $c\prime$ and finds $f(c\prime)$. Then after apply

Fuzzy decision making:

If$(nearness\,(t\,(c)\,, f\,(c') \leq Z_0))$

Then A is bound to act as in m

Else he is free not to act as m.

Then receiver uses the decoding algorithm of the original code T to obtain $m\prime = mWTQ$.

Finally, the receiver recovers m by computing $m = m\prime\,(WTQ)^{-1}$, where $(WTQ)^{-1}$ is the inverse of WTQ.

5 A Simple Illustration

Let

$$D = \{Alice, Bob\}$$

i.,e. we consider a situation where there is not trusted party.

Message Space: Let

$$M = \{0000, 1011, 0101, 1110, 1010, 1100, 1111\} \subset \{0,1\}^4.$$

Message : Let $m = 1011$.

Encoding function: Let

$$W = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

and

$$T = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$Q = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Now

$$g(m) = mWTQ = 0100101.$$

Set up phase: At time t_0, it is agreed between all that

$$\begin{aligned} CK &\cong XOR \\ f &\cong \text{nearest neighbour in } \{g(m)\}. \\ Z_0 &= 0.20. \end{aligned}$$

Commit phase: At time t_1
Alice committed to her message $m = 1011$. She knows that

$$g(m) = g(1011) = 0100101.$$

For the sake of secrecy she adds error and make

$$E = g(m) + e = 1011010$$

at random.

Then her commitment

$$c = commitalg(CK, g(m), E) = g(m)XORE = 1111111.$$

Alice sends c to Bob, which Bob will receive as $t(c)$, where t is the transmission function.

Let the transmitted value $t(c) = 1011111$, which includes noise.

Open Phase: At time t_2
Alice discloses the procedure $g(m)$ and E to Bob to open the commitment.
Suppose Bob gets $t(g(m)) = 1100101$ and $t(E) = 1011010$.
Bob compute

$$c\prime = commitalg(CK, t(g(m)), t(E)) = t(g(m))XORt(E) = 0111111.$$

Bob check the that $dist(t(c), c') = 2$, he will realize that there is an error occurs during the transmission.

Bob apply the error correction function f to $c\prime : f(c') = 1111111$

(the nearest neighbour of $c\prime = 0111111$ is 1111111.
Then Bob will compute nearness

$$(t(c), f(c')) = dist(t(c), f(c'))/n = 0.14$$

Since $0.14 \leq Z_0 = 0.20$.
Then

$$FUZZ(f(c' = 0111111)) = 0.$$

Bob accepted

$$t(c) = f(c') = 1111111.$$

Finally Bob calculate

$$f\left(c'\right)(WTQ)^{-1} = 1011.$$

6 Concluding Remarks

In this paper, we used McEliece scheme. As we know that if $n \in N$ and let $F = \{0, 1\}$ be the field of two elements, consider F-vector space F^N then a decoding problem having $n, k \in N$, $k \leq n$, an (n, k) - code C, and $y \in F^N$, to find $x \in C$ such that $dist(x, y)$ is minimum. For $y = 0$ the decoding problem is the minimum weight problem if $x \neq 0$. Berlekamp, McEliece, and Van Tilborg [2] show that the minimum weight problem is NP-complete. Linear codes can be used for error correction. A message $m \in F^K$ is encoded as $z = mC$.

The encoded message z is transmitted. It is possible that during the transmission some bits of z are changed. The receiver receives the incorrect message y.

He solves the decoding problem, that is, he calculates $x \in C$ such that $dist(x, y)$ is minimum. If the error is not too big, that is, $dist\,(z, y) < \frac{1}{2d}$, where d is the minimum distance of any two distinct code words, then x is equal to the original message z. Linear codes are also used for encryption, for example in the McEliece cryptosystem [2], to encrypt a message it is encoded and an error vector of fixed weight a is added. Decryption requires the solution of the decoding problem. In order for error correction to be efficient, the decoding problem must be efficiently solvable. Also, coding theory based cryptosystems can only be secure if decoding is hard without the knowledge of a secret. This is both true for binary Goppa codes. Decryption of a coding theory based cryptosystem means solving a decoding problem for which the weight of the error vector is known. If we have no special knowledge about the linear code such as a generating polynomial of a Goppa code, then generic methods for decoding can be used. The efficiency and security of McEliece cryptosystem comparatively better than the RSA cryptosystem also [11, 15]. Hence our approach is more appropriate than previous literature of fuzzy commitment schemes.

Acknowledgment. We are most grateful and deeply indebted to anonymous reviewer for their valuable comments and feedback towards completion of this work.

References

[1] R.J. McEliece, *A public-key cryptosystem based on algebraic coding theory*, Jet Propulsion Laboratory DSN Progress Report, **42–44** (1978), 114–116.

[2] E. R. Berlekemp, R. J. McEliece and H. C. A.van Tilborg, *On the inherent intractability of certain coding problems*, IEEE Transactions on Information Theory **24** (1978) No.5, 384-386. MR0495180(58 #13912). Zbl 0377.94018.

[3] M. Blum and S.Goldwasser, *An efficient probabilistic public-key encryption scheme which hides all partial information.* Advances in cryptology (Santa Barbara, Calif., 1984), 289–299, Lecture Notes in Comput. Sci., **196**, Springer, Berlin, 1985. MR0820024 (87e:94029). Zbl 0602.94010.

[4] S.Goldwasser and S. Micali, *Probabilistic encryption & how to play mental poker keeping secret all partial information*, Annual ACM Symposium on Theory of Computing, Proceedings of the fourteenth annual ACM symposium on Theory of computing, 1982, 365 - 377.

[5] R.L.Rivest, A.Shamir, and L.M.Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Communications of the ACM **21** (1978) No.2, 120-126. MR0700103 (83m:94003). Zbl 0368.94005.

[6] M.O. Rabin, *Digital signatures and public-key functions as intractable as factorization*, MIT Lab. For Computer Science, Technical Report, MIT/LCS/TR-212,1979.

[7] M. Blum, *Coin flipping by telephone*, Advances in Cryptology : A Report on CRYPTO'81, 1981, 11-15.

[8] A. Juels and M.Wattenberg, *A fuzzy commitment scheme*, In Proceedings of the 6th ACM Conference on Computer and Communication Security, November 1999, 28-36.

[9] V. Pless, *Introduction to theory of Error Correcting Codes*, Wiley , New York 1982.

[10] A. A. Al-saggaf and H. S. Acharya, *A Fuzzy Commitment Scheme*, IEEE International Conference on Advances in Computer Vision and Information Technology 28-30 November 2007 – India.

[11] A. Canteaut and N. Sendrier, *Cryptanalysis of the original McEliece Cryptosystem, Advances in Cryptology*, -ASIACRYPT '98 Proceedings, Springer-Verlag, 1998, 187–199. MR1727918 (2000i:94042). Zbl 0930.94028 .

[12] M. Alabbadi and S.B. Wicker, *A digital signature scheme based on linear errorcorrecting block codes*, In Josef Pieprzyk and Reihanah Safavi-Naini, editors, Asiacrypt '94, 238–248. Springer-Verlag, 1994. LNCS No. 917.

[13] V. Guruswami and M. Sudan, *Improved decoding of reed-solomon and algebraicgeometric codes*, In FOCS '98, 28–39. IEEE Computer Society, 1998.

[14] W. W. Peterson, *Encoding and error-correction procedures for Bose-Chaudhuri codes*, (Russian. English original) [J] Kibern. Sb. **6**, 25-54 (1963); translation from IRE Trans. Inform. Theory IT-6, 459-470 (1960). MR0118576(22 #9349). Zbl 0171.17501.

[15] J. Buchmann, C. Coronado, M. Doring, D. Engelbert, C. Udwig, R. Overbeck, A. Schmidt, U. Vollmer and R.-P. Weinmann, *Post- Quantum Signatures*, http://eprint.iacr.org/2004/297.pdf.

Deo Brat Ojha
Department of Mathematics,
Raj Kumar Goel Institute of Technology,
Ghaziabad, India.
e-mail: ojhdb@yahoo.co.in

Ajay Sharma
Department of Information Technology,
Raj Kumar Goel Institute of Technology,
Ghaziabad, India.
e-mail: ajaypulastya@gmail.com