Middle-East Journal of Scientific Research 5 (6): 445-448, 2010
ISSN 1990-9233

Application of Coding Theory in Fuzzy Commitment Scheme

[1]*Ajay Sharma* and [2]*Deo Brat Ojha*

[1]Research Scholar of Singhania University, Jhunjhunu, Rajasthan, India
[2]R.K.G.I.T., Ghaziabad, U.P. India

Abstract: In this paper attempt has been made to explain a fuzzy commitment scheme on an algebraic coding theory based public key cryptosystem which relay on the difficulty of decoding and proposed by McEliece in 1978. Here we present a fuzzy commitment scheme which avoids hash function and use the high speed and probabilistic encryption/decryption of McEliece cryptosystem to enhance the efficiency of fuzzy commitment scheme.

Key Words: Error correcting code · Fuzzy logic · Commitment scheme · McEliece cryptosystem · Hash function

INTRODUCTION

In cryptography, commitment schemes are an essentials ingredient of many cryptographic protocols. A commitment scheme is a method that allows a user to commit a value while keeping it hidden and preserving the user's ability to reveal the committed later [1]. Parties which perform according to the prescribed rule and aimed to achieve the protocol objective are called "Honest" [1, 2]. Fuzzy commitment scheme was introduce first by Juels and martin but fuzziness was added in it later by Juels and Watfenberg in 1999 [1].

McEliece proposed the first public-key cryptosystem (the McEliece Scheme) based on algebraic coding theory in 1978 [3] . The idea behind this public-key cryptosystem is based on the fact that the decoding problem of an arbitrary linear code is an NP- hard problem [4]. The McEliece has the advantage of high speed encryption and decryption and this system employs probabilistic encryption [5, 6], which is better than other type of deterministic encryption [7, 8] in preventing the elimination of any information leaked through public-key cryptography.

Linear codes are also used for encryption, for example in the McEliece cryptosystem [3], to encrypt a message it is encoded and an error vector of fixed weight α 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, [9]. This cryptosystem can not be used for authentication because the encryption is not one to one and total algorithm is truly asymmetric.

Most commitment schemes in the literature are based on hash functions [10, 15], which cause them to share two shortcomings:

- The hash functions used should be strongly collision free. However, this property can only be empirically checked. It actually turns out that some schemes are inadvertently based on weakly collision-free hash functions.
- Hash functions alone cannot offer non-repudiability.

Here in this paper we tried to enhance the fuzzy commitment scheme by using code base cryptosystem like based on Goppa Code. The rest of the paper is organized as follows: In section 2 We present a brief introduction of crisp commitment schemes, McEliece public key cryptosystem and defined some used term in the rest of the paper. In section 3, we give our new proposed scheme. In section 4 we analyze the security of proposed approach.

Corresponding Author: Ajay Sharma, Research Scholar of Singhania University, Jhunjhunu, Rajasthan, India, E-mail: ajaypulast@rediffmail.com.

Preliminaries

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 [12, 13].

The McEliece Public-key Cryptosystem: For each irreducible polynomial g (x) over GF (2^m) of degree t, there exists a binary irreducible Goppa code of length n = 2^m and dimension k ≥ n - m τ, capable of correcting any pattern of t or fewer errors. As it is a linear code, it can be described by its $k \times n$ generator matrix G. With the aid of a regular $k \times k$ matrix S and an $n \times n$ permutation matrix P, a new generator matrix G' is constructed that hides the structure of G:

$$G' = S . G . P$$

The public key consists of $G'$and the matrices S and P together with g (x) are the secret key. The new matrix G' is the generator matrix of another linear code, that is assumed to be difficult to decode if the trapdoor information is not known. The encryption operation consists of multiplication of the k-bit message vector by G' and the modulo 2 addition of an error vector e with Hamming weight τ:

$$c = m . G' \oplus e:$$

The First step of the decryption is the computation of cP^{-1}. Subsequently the decoding scheme makes it possible to recover m . S from $cP^{-1} = (m . S . G) \oplus (e .P^{-1})$:

The message m is finally constructed by a multiplication with S^{-1} [3, 14].

Definition: A metric space is a set C with a distance function dist : $C \times C \rightarrow R^+ = [0,\infty)$, which obeys the usual properties(symmetric, triangle inequalities, zero distance between equal points).

Definition : 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 $dist(c_i, c_j) = \sum_{r=1}^{n} |c_{ir} - c_{jr}| \qquad c_i, c_j \in C$, This is known as Hamming distance [11].

Definition: An error correction function f for a code C is defined as $f(c_i)$ = {c_j / dist (c_i,c_j) is the minimum, over C - {c_i}}. Here, $c_j = f\ (c_i)$ is called the nearest neighbor of c_i [1].

Definition: The measurement of nearness between two code words c and $ć$ is defined by nearness (c, $ć$) = *dist* (c, $ć$) / n, it is obvious that 0 ≤ nearness (c, $ć$) ≤1 [2].

Definition: The fuzzy membership function for a codeword $ć$ to be equal to a given c is defined as [8].

$$\begin{aligned} FUZZ(c') &= 0 \qquad && if\ nearness(c,c') = z \le z_0 < 1 \\ &= z && otherwise \end{aligned}$$

The Proposed Scheme: The scheme consists of three phase: first setup phase, second commitment phase and third opening/verifying phase.

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

$CK \cong XOR$
$f \cong$ nearest neighbour in {$h(m)$}.
Z_0 = 0.20
Id_A = Identifier

It is assumed that McEliece public key (P_A) is duly certified and public. It can be described by its $k \times n$ generator matrix G. With the aid of a regular $k \times k$ matrix S and an $n \times n$ permutation matrix P, a new generator matrix G' is constructed that hides the structure of G:

$$G' = S . G . P$$

The public key consists of $G'$and the matrices S and P together with g(x) are the private key(S_A).

Here, the root cause for using Id_A as we stated in introduction section that This cryptosystem can not be used for authentication because the encryption is not one to one and total algorithm is truly asymmetric.

Commitment phase: At time t_1

- Alice chooses message m (k bit vector) in the form of bitstring to which she wish to commit.
- Alice generates a secret pseudo q-bit random vector r.
- Alice has a identifier Id_A of p-bit random vector.
- Alice concatenate her identifier Id_A with secret pseudo q-bit random vector r which give us a vector R=$Id_A \| r$.

Here $h(m) = mP_A$ where $h(m) \subseteq GF(2^n)$,

Encryption: $C = mP_A \oplus e$, where $e = g(R)$, here g is an invertible function which maps R in to an n-bit error vector of weight τ.

According to the algorithms *commita* lg (e_1) into string *c* i.e. her commitment
c = *commita* lg (*XOR*, *h*(*m*),*C*) then after Alice sends *c* to Bob, which Bob will receive as $t_f\,(c)$, where *t* is the transmission function which includes noise .

Open Phase: Alice sends the procedure for revealing the hidden commitment at time t_2 and Bob use this, So Alice discloses the procedure *h*(*m*) and *C* to Bob to open the commitment.

*opena*lg (e_2): Bob constructs *ć* using *commita* lg, message $t_f(m)$ and opening key
i.e *ć* = *commita* lg (*XOR*, *t*(*h*(*m*)), *t*(*C*)) and checks whether the result is same as the received commitment *t*(*c*).
Fuzzy decision making

$$If\,(nearness\,(t_f(c), f(\acute{c})) \le Z_0)$$

Then *A* is bound to act as in *m*
Else he is free not to act as *m*.

Then after acceptance, Bob decrypt the massage as first m can be recovered by using the decryption algorithm in the original scheme. In the meantime, the value *g*(*R*) can also be obtained. Then the receiver computes $R = g^{-1}$ (g(R)), where g^{-1} is the inverse of *g*. finally Bob calculates $f(\acute{c})(SGP)^{-1}$ and finally get the message. Here Bob get the Id_A from the R to know the authenticity of the sender.

Security Analysis: Using a public key cryptosystem to construct a commitment is a way to achieving non-repudiability and authentication, a property which can not be offered by hash functions alone.

Here we know that a commitment scheme is secure if the binding and hiding properties are both satisfies.

- Is the proposed scheme in section 3 is computationally binding.

Is it possible that Alice find a way to commit a value and later another value to Bob without being detected? In order to cheat successfully, Alice has to find a pair as $c_1 = c_2$.

Here 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.
Hence after opening the commitment

$$C_1 = C_2$$
$$m_1P_A \oplus e_1 = m_2P_A \oplus e_2$$

Here $m_1 \neq m_2$ and $e_1 \neq e_2$
So by this
$C_1 \neq C_2$, here Alice has no way to cheat, i.e., the proposed scheme is computationally binding.

- The proposed scheme in section 3 is information theoretically hiding.

Is it possible that Bob find a way to practice fraud i.e., extract Alice commitment before the open phase. Before open phase, Bob knows only *c* but in open phase Alice discloses the procedure *g*(*m*) and *C* (which reveal the S,G,P) to Bob to open the commitment.

Under these assumption infect, Bob has no chance to practice fraud no matter how powerful computation ability possesses, i.e., the proposed scheme is information theoretically binding.

CONCLUSION

By using McEliece in fuzzy commitment scheme error vector *e* used to enhance the security of the function hiding, particularly against matrix factorization attacks. The main feature of this approach is randomness of the error vector concatenate with identifier, here identifier provide the authenticity with randomness, so we can not obtain any information about the positions in which the error occurs. Thus the information rate is increasing and information leakage rate decreasing by using this approach. To provide better security, it is suggested that data compression technique be applied before encryption.

REFERENCES

1. Juels, A. and M. Wattenberg, 1999. A fuzzy commitment scheme, In Proceedings of the 6th ACM Conference on Computer and Communication Security, pp: 28-36.
2. Blum, M., 1982. Coin flipping by telephone: a protocol for solving impossible problems, Proc. IEEE Computer Conference, pp: 133-137.
3. McEliece, R.J., 1978. A public-key cryptosystem based on algebraic coding theory, DSN Progress Report, 42-44: 114-116.
4. Berlekemp, E.R., R.J. McEliece and H.C.A. VanTilborg, 1978. On the inherent intractability of certain coding problems, IEEE Transactions on Information Theory, 24(5): 384-386.
5. Blum, M. and S. Goldwasser, 1985. An efficient probabilistic public-key encryption scheme which hides all partial information, Advances in Cryptology-CRYPTO'84, Lecture notes in computer science (Springer-Verlag): 289-299.
6. Goldwasser, S. and S. Micali, 1982. Probabilistic encryption and how to play mental pocker keeping secret all partial information, in Proceeding of the 14th ACM Symposium on the theory of computing, pp: 272-299.
7. Rivest, R.L. A. Shamir and L.M. Adleman, 1978. A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM, 21(2): 120-126.
8. Rabin, M.O., 1979. Digital signatures and public-key functions as intractable as factorization, MIT Lab. For Computer Science, Technical Report, MIT/LCS/TR-212.
9. Canteaut and N. Sendrier, 1998. Cryptanalysis of the original McEliece Cryptosystem, Advances in Cryptology-ASIACRYPT' 98Proceedings, Springer-Verlag, pp: 187-199.
10. Halevi, S. and S. Micali, 1996. Practical and provably secure commitment schemes from collision free hashing, in Proceedings on Advances in Cryptology -CRYPTO,LNCS 1109, Springer, pp: 201-215.
11. Pless, V., 1982. Introduction to theory of Error Correcting Codes, Wiley, New York.
12. Alawi A. Al-saggaf and H.S. Acharya, 2009. A generalized Framework for Crisp Commitment Schemes eprint.iacr.org/.
13. Alawi A. Al-saggaf and H.S. Acharya, 2007. Mathematics Of Bit-Commitment Schemes, Bulletin of the Marathwada Mathematical Society, 8(1): 08-15.
14. Berlekemp, E.R., R.J. McEliece and H.C.A. VanTilborg, 1978. On the inherent intractability of certain coding problems,"IEEE Transactions on Information Theory, 24(5): 384-386.
15. Preneel, B., 1999. The state of cryptographic hash functions, in Lectures on Data Security: ModernCryptology in Theory and Practice, LNCS 1561, Berlin: Springer, pp. 158-192.