International Journal of Computer Networks and Communications Security

VOL.2, NO.1, JANUARY 2014, 7–14
Available online at: www.ijcncs.org
ISSN 2308-9830

Management of Confidentiality of Cryptosystems Using Linear Codes- a Bird's Eye View

Preetha Mathew K[1] and Dr Mathew Cherian[2]

[1, 2] Associate Professor, Department of Computer Science and Engineering and Principal, Cochin University College of Engineering Kuttanad, Pulincunnu, Alappuzha, Kerala, India

ABSTRACT

In this paper, we investigate the management of confidentiality in terms of security notions of McEliece cryptosystem, the first encryption scheme using linear codes, proposed on the basis of the hard problems in coding theory and its variants in the provably secure approach. The original McEliece is only a one way function. Therefore to obtain the higher notions of security, modifications on the original scheme are proposed. Li et al. in IEEE transactions on information theory (1994), proved that the security of McEliece cryptosystem and Niederreiter cryptosystem, the dual of McEliece cryptosystem are equivalent. In this paper we show that it is not true. Dolev et al. in their paper published in STOC (1991), coined the notion of non malleability which formalizes an adversary's ability to create a different cipher text y_1 for a plain text x_1 from the cipher text y which is an encryption of x. It is seen that the McEliece system is malleable and Niederreiter system is non malleable in view of the security notions existing in the provably secure scenario.

Keywords: *CCA-2 Security, CPA Security, McEliece Cryptosystem, Syndrome Decoding, Code Indistinguishability.*

1 INTRODUCTION

Confidentiality and authentication are major goals of cryptography. Confidentiality can be obtained using encryption and authentication is obtained by digital signature. One of the basis of the security of encryption is provable security. The security notions widely used in the provably secure approach for the encryption schemes are derived from the subset of the cross product of the goal to be achieved and the attack model. The goal to be achieved belongs to the set consisting of invertibility (INV), indistinguishability (IND) and non malleability (NM). The attack models fall into CPA (Chosen Plain Text attack) and CCA (Chosen Cipher Text attack). There are two variants of CCA, namely CCA-1(lunch time attack) alias non adaptive chosen cipher text attack, where the decryption oracle is provided to the attacker (adversary) for training. Once the training is over the challenge cipher text is provided. After the provision of challenge cipher text no decryption oracle is given for training so that adversary can choose other cipher text in adaptive way to identify the message. Whereas in CCA-2, the adaptive chosen cipher text attack in which the adversary is provided the decryption oracle for training before and after the challenge cipher text. Hence the adversary can take a training adaptively. The strongest notion of the security for an encryption scheme considered at present is that of indistinguishability under chosen cipher text attack (IND CCA-2).

While considering the goals, invertibility can be achieved with the help of trapdoor functions. The trap door functions are hard to invert unless one possesses some secret trapdoor information. The trap door function was conceptualized by Diffie and Hellman [5] and realized by the RSA cryptosystem Implementation by Rivest, Shamir and Adleman [18]. The adversary can observe the encryption of the single message that it wishes to crack and try to find the plain text, which is having a negligible probability of success without the trapdoor information. The drawbacks of the cryptosystems based on trapdoor functions are as follows.

- The fact that *f* is a trapdoor function does not rule out the possibility of computing *x* from *f(x)*, where *x* is of special form.
- The fact that f is a trapdoor function does not rule out the possibility of easily computing some partial information about *x* from *f(x)*.

To overcome these undesirable properties Goldwasser and Micali [10] proposed the notion of in distinguishability. It is desirable that an encryption scheme should not leak any information about the clear text from the cipher text. Dolev et al. [6] coined the notion of non malleability which formalizes an adversary's ability to create a different cipher text y' for a plain text x' from the cipher text y which is an encryption of *x*. The security proof for cryptosystem is modelled in two ways.

- Complexity-based proofs: The complexity-based approach was put forth by Diffie and Hellman [4]. They suggested that the security of a cryptographic primitive could be reduced to hardness assumptions of certain fundamental problems, such as the existence of one-way functions. The approach proved very successful, as a large number of cryptographic primitives, includeing pseudorandom generators, signatures and secure protocols were shown to exist based on general complexity assumptions, which is termed as standard model.
- Random Oracle Model: The well-known Random Oracle Model (ROM), formalised by Bellare and Rogaway [2], is one such model. In the random oracle model, one assumes that some hash function is replaced by a publicly accessible random function (the random oracle). This means that the adversary cannot compute the result of the hash function by himself: he must query the random oracle.

The differences between random oracle and standard model is as follows [12]

- In the standard model (SM), a security proof gives you a list of sufficient assumptions to guarantee security properties.
- In the ROM, no precise sufficient assumption on the hash function is provided, except one which cannot be satisfied by efficient functions. The ROM is a security model, not an assumption.

Code-based cryptography was initiated by the seminal paper due to McEliece [19], who presented a cryptosystem, based on the hardness of both the *Bounded Decoding* problem and the *Goppa Code Distinguishability* problem. Initially, the scheme did not gain sufficient acclaim, due to the large key-sizes. Therefore Niederreiter proposed a cryptosystem, that is dual of the McEliece Cryptosystem [11]. Unlike number-theoretic schemes that are weak against an attack due to Shor [21], McEliece and Niederreiter cryptosystems (when using Goppa codes) are resistant against attack proposed by Shor, thus making them strong candidates for Post-Quantum Cryptography. Also, in comparison with number-theoretic encryption schemes, code-based schemes are computationally efficient, as the underlying operations are vector-matrix multiplication and vector additions.

1.1 Related Work:

It has been proved that Niederreiter and McEliece cryptosystem have equivalent security properties [13]. The original McEliece [19] is shown as a one way function alone and not IND-CPA. To make it IND-CPA secure Nojiama et al. [15] uses concatenation a random sequence *r* to message *m* and encrypt [*r*|*m*] where *r* is of k_1 bits and m is of k_2 bits .After decryption the last k_2 bits are taken as the message. Strenzke [22] proposes the McEliece Cryptosystem in proven to be IND-CCA2 secure under the random oracle model. Rosen et al. [20] initiated the study of the one-wayness under correlated products and Freeman et al. [9] propose instantiation of lossy trapdoor functions and correlation-secure trapdoor functions. They proposed a correlation-secure trapdoor functions based on the hardness of syndrome decoding, thereby, obtaining a CCA2. Using the above concept Dowsley et al. [7] showed that a randomized version (IND-CPA secure) of the McEliece cryptosystem with *k* repetition is shown to be a IND-CCA2 secure scheme in the standard model. The construction that adhere more to the construction of Rosen and Segev [20] is given by Persichetti [17]

1.2 Our Contributions:

This paper investigates the security notion of McEliece cryptosystems and its variants and shows how that the security of McEliece and Niederreiter cryptosystems are not equivalent as shown in [13]

and also show that the semantic secure McEliece cryptosystem is also malleable.

1.3 Organization of the paper:

Section 2 provides the hardness assumptions used in the paper and the basic code-based crypto-systems (McEliece and Niederreiter). Section 3 gives the various schemes, the proof of security of each scheme, the secure parameters used. The paper is concluded in section 4.

2 PRELIMINARIES

A. Notation

If x is a vector or a string, then |x| denotes its length, while |S| represents the cardinality of the set S. The membership notation $x \in \mathbf{x}$ or $x \notin \mathbf{x}$ means x is a member of **x** or x is not a member of **x** = {x[i]: $1 \leq i \leq |x|$}. $s \in_R S$ denotes the operation of choosing an element s from a set S uniformly at random. w← A(x, y,…) represents the running of algorithm A with inputs x, y, .. and producing output w. We write w ← $A^{\mathcal{O}}$(x, y,...) for representing an algorithm A having access to oracle $\mathcal{O}$. We denote by Pr [E] as the probability that the event E occurs. Considering the decryption oracle x← D_{sk}(y) means that for i= 1 .. |Y|, x[i] ← D_{sk}(Y[i]). R(x_1,…, x_t) we write R(x,x), meaning the first argument is special and the rest are bunched into a vector x with lxl = t-1. For a matrix M, its transpose is represented by M^T and its inverse (if it exists) is represented by M^{-1}. If a and b are two strings of bits, we denote their bitwise XOR by a $\oplus$ b. Let A be a m X n_1 matrix and B be a m X n_2 matrix, the C = [A | B] is a m X (n_1 + n_2) matrix, with each row i of C being the concatenation of the ith row of A with that of B.

Since, the proposed cryptosystems are code-based, a few notations regarding coding theory are introduced. A binary linear-error correcting code of length n and dimension k or a [n, k] - code is a k-dimensional subspace of $\mathbb{F}_2^n$. The rate of a code can be calculated as $\frac{k}{n}$. A code is high-rate if $\frac{k}{n} \to 1$. If the minimum hamming distance between any two codewords is d, then the code is a [n,k,d] code. The hamming weight of a codeword x, wt(x), is the number of non-zero bits in the codeword. For $t \leq \lfloor \frac{d-1}{2} \rfloor$, the code is said to be t-error correcting if it detects and corrects errors of weight at most t. Hence, the code can also be represented as a [n,k,2t + 1] code. The generator matrix $G \in \mathbb{F}_2^{k \times n}$ of a [n, k] linear code C is a matrix of rank k whose rows span the code C. The parity-check matrix $H \in \mathbb{F}_2^{n-k \times n}$ of a [n,k] code C is a matrix satisfying $HG^T = 0$. Hence, code C can be defined as $\{mG : \forall m \in \mathbb{F}_2^k\}$ or $\{c : Hc^T = 0\}$.

B. Definition of the Security Notions

To formalize the indistinguishability and non-malleability adversary A can be considered as a pair of probabilistic algorithms A = (A1, A2). This corresponds to A running two stages. The exact purpose of each stage depends on the particular adversarial goal. For both goals the basic idea is that the first stage adversary, given the public key, seeks and outputs some test instance, and the second stage adversary is issued a challenge cipher text y generated as a probabilistic function of the test instance, in a manner depending on the goal. Adversary A is successful if she passes(depends on the goal) the challenge.

A Public-Key Encryption Scheme (PKE) is defined as follows

***Definition 1*:** A public-key encryption scheme is a triplet of algorithms (**Gen, Enc, Dec**) such that:

- **Gen** is a probabilistic polynomial time key generation algorithm which takes as input a security parameter 1^n and outputs a publickey **pk** and a secret key **sk** the public key specifies the message space M and the cipher text space **C**.
- **Enc** is a (possibly) probabilistic polynomial-time decryption algorithm which receives as input a public key **pk** and a message m∈M and outputs a cipher text c∈C.
- **Dec** is a deterministic polynomial-time decryption algorithm which takes as input a secret key sk and a ciphertext c, and outputs either message m∈ M or an error symbol ⊥
- (Soundness) For any pair of public and private keys generated by Gen and any message m ∈ M it holds that *Dec(sk,Enc(pk,m))=m* with overwhelming probability over the randomness used by Gen and Enc.

***Definition 2*:** (IND-CPA security). to a two stage adversary A = (A1,A2) against PKE we associate the following experiment $Exp^{cpa}_{PKE;A}(n)$:
(pk,sk) ← Gen(1^n)
(m0, m1, state) ← A1(pk) s.t. $|m_0| = |m_1|$
b ← (0,1)
c*← Enc(pk,mb)
b'← A2(c*,state)
if b=b' return 1 else return 0
We define the advantage of A in the experiment as

$Adv^{cpa}_{PKE,A}(n) = |Pr[Exp^{cpa}_{PKE;A}(n) = 1] - 1/2|$

The PKE is indistinguishable against chosen-plaintext attacks(IND-CPA) if for all probabilistic polynimial time (PPT) adversaries A = (A1, A2) the advantage of A in the experiment is a negligible function of n.

Definition 3**:** (IND-CCA1 security). to a two stage adversary A = (A1,A2) against PKE we associate the following experiment $Exp^{cpa}_{PKE;A}(n)$:
(pk,sk) ← Gen(1^n)
(m0, m1, state) ← $A_1^{Dec(sk,.)}$(pk) s.t. $|m_0| = |m_1|$
b ← (0,1)
c* ← Enc(pk,m_b)
b' ← A2(c*,state)
if b=b' return 1 else return 0
$Adv^{cpa}_{PKE,A}(n) = |Pr[Exp^{cpa}_{PKE;A}(n) = 1] - 1/2|$

Definition 4**:** (IND-CCA2 security). to a two –stage adversary A = (A1,A2) against PKE we associate the following experiment
$Exp^{cpa}_{PKE;A}(n)$:
(pk,sk) ← Gen(1^n)
(m0, m1, state) ← A1(pk) s.t. $|m_0| = |m_1|$b (0,1)
b ← (0,1)
c* ← Enc(pk,m_b)
b' ← $A2^{Dec(sk,.)}$(c*,state)
if b=b' return 1 else return 0
The adversary A_2 is not allowed to query Dec(sk,.) with c*.
We define the advantage of A in the experiment as
$Adv^{cpa}_{PKE,A}(n) = |Pr[Exp^{cpa}_{PKE;A}(n) = 1] - 1/2|$

We say that PKE is indistinguishable against adaptive chosen-cipher text attacks (IND-CCA2) if for all probabilist polynomial time (PPT) adversaries A= (A_1,A_2) that makes a polynomial number of oracle queries the advantage of A in the experiment is a negligible function of n.

1) *Non Malleability*: The experiment for nonmalleable CPA, CCA-1, CCA-2 can be defined as follows :

Let A = (A_1,A_2) be an adversary. In the first stage of the adversary's attack, A_1, given the public key *pk*, outputs a description of a message space, described by a sampling algorithm *M*. The message space must be *valid*, which means that it gives non-zero probability only to strings of some one particular length. In the second stage of the adversary attack, A_2 receives an encryption *y* of a random message, say *x*, drawn from *M*. the adversary then outputs a (description of a) relation R and a vector y (no component of which is y). She hopes that R(*x*, x) holds, where $x \leftarrow D_{sk}(y)$. An adversary (A_1, A_2) *is successful* if she can do this with a probability significantly more than that with which R($\tilde{x}$, x) holds for some random hidden $\tilde{x}$ ← M.

Definition 5 (NM-CPA, NM-CCA-1, NM-CCA-2): Let ∏ = (K,ϵ,D) be an encryption scheme and let (A_1,A_2) be an adversary. For atk ϵ cpa, cca1, cca2 and k ϵ N define

$$Adv^{nm-atk}_{A,\Pi}(k) \stackrel{def}{=} |Succ^{nm-atk}_{A,\Pi}(k) - Succ^{nm-atk}_{A,\Pi,\$}(k)|$$

where $Succ^{nm-atk}_{A,\Pi}(k) \stackrel{def}{=}$

$$Pr[(pk,sk) \leftarrow \mathcal{K}(1^k); (M,s) \leftarrow A_1^{\mathcal{O}_1}(pk); x \leftarrow M; y \leftarrow \epsilon_{pk}(x); (R,\mathrm{y}) \leftarrow A_2^{\mathcal{O}_2}(M,s,\mathrm{y}); \mathrm{x} \leftarrow \mathcal{D}_{sk}(y); y \notin \mathrm{y} \wedge \perp \notin \mathrm{x} \wedge R(x,\mathrm{x})]$$

and $Succ^{nm-atk}_{A,\Pi,\$}(k) \stackrel{def}{=}$

$$Pr[(pk,sk) \leftarrow \mathcal{K}(1^k); (M,s) \leftarrow A_1^{\mathcal{O}_1}(pk); x,\tilde{x} \leftarrow M; y \leftarrow \epsilon_{pk}(x); (R,\mathrm{y}) \leftarrow A_2^{\mathcal{O}_2}(M,s,\mathrm{y}); \mathrm{x} \leftarrow \mathcal{D}_{sk}(y); y \notin \mathrm{y} \wedge \perp \notin \mathrm{x} \wedge R(\tilde{x},\mathrm{x})]$$

where
if atk-cpa then $\mathcal{O}_1(.) = \epsilon$ and $\mathcal{O}_2(.) = \epsilon$
if atk-cca-1 then $\mathcal{O}_1(.) = \mathcal{D}_{sk}(.)$ and $\mathcal{O}_2(.) = \epsilon$
if atk-cca-2 then $\mathcal{O}_1(.) = \mathcal{D}_{sk}(.)$ and $\mathcal{O}_2(.) = \mathcal{D}_{sk}(.)$

We insist, above, that *M* is valid: $|x| = |x'|$ for any *x, x′* that are given non-zero probability in the message space M. We say that ∏ is secure in the sense of NM-ATK if for every polynomial *p(k)* : if A runs in time *p(k)*, outputs a (valid) message space *M* samplable in time *p(k)*, and outputs a relation R computable in time p(k), then $Adv^{nm-atk}_{A,\Pi}(.)$ is negligible. The security notion of One-time strongly unforgeable, or one-time existentially unforgeable under chosen message attack (EUF-1CMA) is as follows (based on [14]):

Definition 6**:** EUF-1CMA A signature scheme is said to secure under EUF-1CMA, if there exists no PPT algorithm *A*, which has knowledge of only the verification key vk and the public parameters and access for just one query to the signature oracle to obtain a tuple(m',σ') , outputs a valid signature (m,σ) ≠ (m',σ') with a non-negligible probability. The probability that any PPT adversary A wins the EUF- 1CMA game for a one-time signature $\mathcal{OS}$, given the verification key vk is denoted by $\mathrm{Succ}^{\mathcal{OS}}_{\mathcal{A}}(\mathsf{vk})$

C. Security assumptions

The following are some of the hard problems on which the security of the proposed cryptosystems is based.

Definition 7**: Syndrome Decoding Problem**. For some parameters [n, k, 2t + 1] given an $a \in \mathbb{F}_2^{n-k}$

and a matrix $H \in \mathbb{F}_2^{n-k \times n}$, find a vector $e \in \mathbb{F}_2^n$ with weight wt(e)≤ t such that $He^T = a$.

The advantage of a PPT algorithm D of solving the problem is denoted by $\mathsf{Adv}_{\mathcal{D}}^{\mathsf{SD}}(n)$.

Assumption 2: For any probabilistic polynomial time distinguisher *D*, $\mathsf{Adv}_{\mathcal{D}}^{\mathsf{CD}}(n,k) < \epsilon_2(n,k)$ is a negligible function if it is not a high rate goppa code, [8].

$$|Pr[\mathcal{D}(H) = 1] - Pr[\mathcal{D}(M) = 1]| < \epsilon_2(n,k)$$

Where H is the parity check matrix of the Goppa code and $M \in_R \mathbb{F}_2^{n-k \times n}$

D. McEliece Cryptosystem

McEliece cryptosystem [19] uses the hardness of syndrome decoding and code indistinguishability for its security. The scheme is given below,

- Secret Key:
  - C a binary *t* error correcting linear code.
  - a k X k non-singular matrix S,
  - a n X n permutation matrix P
- Public key: G' = SGP, where G is a generator matrix of C.
- Encryption: c→ mG'⊕ e, the message *m* is a word of length *k* and e error vector of weight *t*.
- Decryption: m → $S^{-1}\text{Decode}_G(P^{-1}c)$.

E. Neiderreiter Cryptosystem

Niederreiter's cryptosystem [11] uses the hardness of syndrome decoding for its security. The scheme is given below,

- Secret Key:
  - C a binary *t* error correcting linear code.
  - a (n - k) X (n - k) non-singular matrix Q,
  - a n X n permutation matrix P
- Public key: $\tilde{H} = QHP$, where H is a parity check matrix of C.
- Encryption: $c = \tilde{H}m^{T'}$, the message m is a word of length n and weight t.
- Decryption: $m = P^{-1}\text{Decode}_H(Q^{-1}c)$

Even though McEliece and Niederreiter cryptosystems are complementary and also not in IND-CPA, the security properties are not equivalent as Niederreiter is non-malleable and McEliece is malleable. The following will show that McEliece and Niederreiter are not in IND-CPA. For the IND-CPA experiment the adversary gives challenger two messages m_0, m_1 of the same length. The challenger flips a coin and randomly select one of the messages, encrypt it and gives to the adversary to distinguish which message has been encrypted.

Consider the McEliece system. The Challenger encrypts the message as c → m_bG'⊕ e where b ϵ 0, 1. The adversary can check wt(c⊕ m_0G') = t then the message encrypted is m_0 else it is m_1. In the case of Neiderreiter cryptosystem the checking is direct as adversary can check whether $c = \tilde{H}m_1^{T'}$ .Therefore both the cryptosystems are only one way functions or in other words the goal achieved is only invertability.

Now consider the non malleability for the McEliece system, the rows of the generator matrix form the basis for the code word *C*. The cipher text is formed by multiplying message m with a generator matrix added with a *t* error vector. Addition of the row of the generator matrix (Public key) will yield to a cipher text for m_0 in such a way that *m* and m_0 are related. A typical example is as follows *G* be a goppa generator matrix defined by

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

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

The encryption of m using McEliece encryption by adding 2 bit errors, say in the 14th and 15th bit positions is given as [1100001111110011]. Let m_0 = [1101] be another message to be encrypted using the same error vector. The encryption with G for m0 by adding a two error bits at the 14th and 15th bit positions is given as [1101010011100010]. This is equivalent to adding the row numbered 4 of the matrix G to the cipher text obtained from m using the same error vector. Since it is possible to generate a meaningful cipher text from the given cipher text with a known relation McEliece cryptosystem is malleable. There is no known relation for the creation of new syndromes from existing syndromes. Hence Neiderreiter is non-malleable. Therefore the security of McEliece system is not equivalent to that of Neiderreiter system.

3 VARIANTS OF THE MCELIECE CRYPTOSYSTEM

A. Randomized McEliece cryptosystem (IND-CPA)

The original McEliece crypto system is only a one way function that is invertible only and also

malleable. To make it IND-CPA (semantic secure) secure a randomness is added and the following scheme is shown to be IND - CPA [15].

- Secret Key:
  - C a binary *t* error correcting linear code.
  - a k X k non-singular matrix S,
  - a n X n permutation matrix P
- Public key: G' = SGP, where G is a generator matrix of C.
- Encryption: c→ [r|m]G'⊕e, the message r|m is a word of length k = k_1 + k_2 and *e* error vector of weight *t*.
- Decryption: r|m→ $S^{-1}Decode_G(P^{-1}c)$.

Even though the above system is IND-CPA it is not non-malleable (NM-CPA) because of the argument given in the previous section. That is by adding a row of generator matrix to the given cipher text yields to a cipher text corresponding to a message, whose bit is changed from the original message, only in that position as that of the row number added to the first cipher text. Also it is proved that an IND-CPA cryptosystem is not NM-CPA. But the converse is true. The proof is given by Bellare et al. [1].

B. IND-CCA1 Construction

Pass et al. gave a construction for a non-malleable encryption scheme from any semantically secure one which is a non black box construction [16]. This is improved by Choi et al. [3], and proposed a black box construction using the method of encrypting an encoding of the message with certain locally testable and self-correcting properties. If one adapt the above construction it is similar to the construction specified by Dowsley et al in constructing IND-CCA2 McEliece encryption in the standard model[7].

C. IND-CCA2 secure McEliece in random oracle model

The encryption scheme proven to be IND-CCA2 secure is considered to be the most secure system as far as encryption is concerned. The scheme is a variant of converting one way function to IND-CCA2 secure using the Fujisaki Okomoto transformation [22]. The scheme is as follows.

- The message m ϵ $\mathbb{F}_2^l$, public key G^{pub} which is a generator in the systematic form corresponding to the permuted goppa parity check matrix HP^T, where *H* is the parity check and *P* is the permutation matrix. H() is a hash function which outputs *l* bits, secret key P, g(X), which is the Goppa polynomial of degree *t*

- $Encrypt(m):$ $u_1 \in_R F_2^{k-l}, u_2 \in_R F_2^l$
  $(z_1, e) \leftarrow (u_1 || \mathbf{H}(m) || u_2) G_{pub} \oplus e$
  $z \leftarrow z_1 || \mathbf{H}(u_1) \oplus m || u_2 \oplus \mathbf{H}(e)$

- $Decrypt(z):$ $z \in F_2^{n+2l}$
  $(w, e) \leftarrow Decode_{g(x)}(P^{-1} z_1)$
  $r \leftarrow$ the first $k-l$ bits of w
  $h \leftarrow$ the bits $k-l+1, ..., k$ of w
  $m \leftarrow z_2 \oplus \mathbf{H}(r)$
  if $h = \mathbf{H}(m) || (\mathbf{H}(e) \oplus z_3)$ then
  return m
  else
  return error
  endif

As per the theorem by [1] an IND-CCA2 cryptosystem is NMCCA2 and the converse is also true. Hence the above system is IND-CCA2 as well as NM-CCA2 also. The same argument can be followed for the cryptosystem in the next section also.

D. IND-CCA2 secure McEliece in standard model

The scheme proven to be secure in the standard model is said to be practical as compared to the random oracle model. Dowsely et al.[7] proposed McEliece encryption which is IND-CCA2 secure McEliece in standard model

Public key pk = $(pk_1^0, pk_1^1, ..., pk_k^0, pk_k^1)$ and a *k*-bit string *vk* we write $pk^{vk} = (pk_1^{vk_1}, ..., pk_k^{vk_k})$. We will use the same notation for secret keys sk.

- Key Generation: Gencca2 is a probabilistic polynomial time key generation algorithm which takes as input a security parameter 1n. Gencca2 calls PKEs key generation algorithm 2k times to obtain public keys $pk_1^v, pk_1^1, ..., pk_k^v, pk_k^1$ and secret keys $sk_1^0, sk_1^1, ..., sk_k^0, sk_k^1$. It sets $pk = (pk_1^0, pk_1^1, ..., pk_k^0, pk_k^1)$, $sk = (sk_1^0, sk_1^1, ..., sk_k^0, sk_k^1)$ and outputs (pk, sk).

- Encryption: Enc_{cca2} is a probabilistic polynomial time encryption algorithm which receives as input the public key pk = $(pk_1^0, pk_1^1, ..., pk_k^0, pk_k^1)$ and a message mϵM and proceeds as follows:

  1. Executes the key generation algorithm of the signature scheme obtaining a signing key dsk and a verification key vk.

2. Compute c' = $Enc_k(pk^{vk}$,m, r) where r is random coin.
3. Computes the signature σ = Sign(dsk, c').
4. Outputs the cipher text c = (c' ,vk, σ).

Decryption: Dec_{cca2} is a deterministic polynomial time decryption algorithm which takes as input a secret key $sk = (sk_1^0, sk_1^1, ..., sk_k^0, sk_k^1)$ and a cipher text c =(c', vk, σ) and proceeds as follows:

1) If V er(c', vk, σ) = 0, outputs $\perp$ and halts.

2) It computes and outputs $m = Dec_k(sk^{vk}, c')$.

Note that if c' is an invalid cipher text (i.e. not all c_1' decrypt to the same plaintext), then Dec_{cca2} outputs ⊥ as Deck outputs ⊥.

4 CONCLUSION

In the paper, we surveyed the security properties of the McEliece cryptosystem and its variants. The scheme does not gain popularity during the time of proposal due to large key size. Now this system is identified as a candidate for developing the post quantum cryptographic protocols. It is found that McEliece cryptosystem original proposed is malleable, so also the semantically secure McEliece cryptosystem. The IND-CCA2 variant in the standard model using k repetition for the encryption hence the overhead is very huge, as the public key for the original McEliece is very large. An IND-CCA2 McEliece system without k repetition in standard model is a promising solution in developing the post quantum cryptographic systems.

5 REFERENCES

[1] Mihir Bellare, Anand Desai, David Pointcheval, and Phillip Rogaway. "Relations among notions of security for public-key encryption schemes". In CRYPTO, pages 26–45, 1998.

[2] Mihir Bellare and Phillip Rogaway. "Random oracles are practical: a paradigm for designing efficient protocols". In Proceedings of the 1st ACM conference on Computer and communications security, CCS '93, pages 62–73, New York, NY, USA, 1993. ACM.

[3] Seung Geol Choi, Dana Dachman-Soled, Tal Malkin, and Hoeteck Wee. "Black-box construction of a non-malleable encryption scheme from any semantically secure one". In TCC, pages 427–444, 2008.

[4] W. Diffie and M. Hellman. "New directions in cryptography. Information Theory", IEEE Transactions on, 22(6):644 – 654, nov 1976.

[5] Whitfield Diffie and Martin E. Hellman. "New directions in cryptography. IEEE Transactions on Information Theory", 22:644–654, 1976.

[6] Danny Dolev, Cynthia Dwork, and Moni Naor. "Non-malleable cryptography (extended abstract)". In STOC, pages 542–552, 1991.

[7] Rafael Dowsley, J¨orn M¨uller-Quade, and Anderson C. A. Nascimento. "A CCA2 secure public key encryption scheme based on the McEliece assumptions in the standard model". In Marc Fischlin, editor, CT-RSA, volume 5473 of Lecture Notes in Computer Science, pages 240–251. Springer, 2009.

[8] J.-C. Faug´ere, A Otmani, L. Perret, and J.-P. Tillich. "Algebraic Cryptanalysis of McEliece variants with compact keys – toward a complexity Analysis". In SCC '10: Proceedings of the 2nd International Conference on Symbolic Computation and Cryptography, pages 45–55, RHUL, June 2010.

[9] David Mandell Freeman, Oded Goldreich, Eike Kiltz, Alon Rosen, and Gil Segev. "More constructions of lossy and correlation-secure trapdoor functions". In Phong Q. Nguyen and David Pointcheval, editors, Public Key Cryptography, volume 6056 of Lecture Notes in Computer Science, pages 279–295. Springer, 2010.

[10] Shafi Goldwasser and Silvio Micali. Probabilistic encryption. J. Comput. Syst. Sci., 28(2):270–299, 1984.

[11] Niederreiter H. "Knapsack-type cryptosystems and algebraic coding theory". Prob Contr Inform Theor 15, pages 159 – 166, 1986.

[12] Ga¨etan Leurent and Phong Q. Nguyen. "How risky is the random-oracle model?". IACR Cryptology ePrint Archive, 2008:441, 2008.

[13] Yuan Xing Li, Robert H. Deng, and Xin mei Wang. "On the equivalence of McEliece's and Niederreiter's public-key cryptosystems". IEEE Transactions on Information Theory, 40(1):271–, 1994.

[14] Rafael Misoczki and Paulo S. L. M. Barreto. "Compact McEliece keys from Goppa Codes". In Michael J. Jacobson Jr., Vincent Rijmen, and Reihaneh Safavi-Naini, editors, Selected Areas in Cryptography, volume 5867 of Lecture Notes in Computer Science, pages 376–392. Springer, 2009.

[15] Ryo Nojima, Hideki Imai, Kazukuni Kobara, and Kirill Morozov. "Semantic security for the McEliece cryptosystem without random

oracles". Des. Codes Cryptography, 49(1-3):289–305, 2008.

[16] Rafael Pass, Abhi Shelat, and Vinod Vaikuntanathan. "Construction of a non-malleable encryption scheme from any semantically secure one". In CRYPTO, pages 271–289, 2006.

[17] Edoardo Persichetti. "On a cca2-secure variant of mceliece in the standard model". IACR Cryptology ePrint Archive, 2012, 2012.

[18] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. "A method for obtaining digital signatures and public-key cryptosystems" (reprint). Commun. ACM, 26(1):96–99, 1983.

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

[20] Alon Rosen and Gil Segev. "Chosen-ciphertext security via correlated products". In Omer Reingold, editor, TCC, volume 5444 of Lecture Notes in Computer Science, pages 419–436. Springer, 2009.

[21] Peter W. Shor. "Polynomial time algorithms for discrete logarithms and factoring on a quantum computer". In Leonard M. Adleman and Ming-Deh A. Huang, editors, ANTS, volume 877 of Lecture Notes in Computer Science, page 289. Springer, 1994.

[22] Falko Strenzke." A smart card implementation of the mceliece pkc". In Pierangela Samarati, Michael Tunstall, Joachim Posegga, Konstantinos Markantonakis, and Damien Sauveron, editors, WISTP, volume 6033 of Lecture Notes in Computer Science, pages 47–59. Springer, 2010.