# An Efficient SKM Framework for Data Authentication and its Application to the Adhoc Networks

Suma Christal Mary
Research Scholar,
Department of CSE,
Kalasalingam University,
Anand Nagar,
Krishnankoil-626 190

Pallikonda Rajasekaran
Associate Professor,
Department of ICE,
Kalasalingam University,
Anand Nagar,
Krishnankoil-626 190

Chrisbin Jeeva
Assistant Professor,
Department of MCA,
PSN College of Engg and Technology,
Palayamkottai,
Thirunelveli-627152

## ABSTRACT

The Internet and various other forms of electronic communication is such an essential thing to move up with this periodic global world and indulging security is another gradient to climb defeating those black hats. One essential aspect for secure communications is that of cryptography. In previous approaches RSA and ECC algorithms plays a vital role however both algorithms are lacking of mathematical problems monotonously. In our proposed approach a novel protocol called Shared Key Management (SKM) is employed. In this approach McEliece algorithm is embedded with Dispense Key designed for key generation and for the key distribution. This scheme is highly scalable with respect to memory moreover number of keys are drastically reduced. Experimental results are being encountered that our proposed approach increases its efficiency in terms of memory and execution time for performing both encryption and decryption. As a result this algorithm is providing a high-performance platform to execute key generation, key distribution encryption and decryption scenarios.

## 1. INTRODUCTION

Computers are used by millions of people for many purposes such as Banking, Shopping, Tax returns, Protesting Military, Student records. Privacy is a crucial issue in many of these applications. Security is the way to persuade that inquisitive people cannot read or secretly modify messages which is intended for other recipients.

The number of complications encountered with security problems in network includes secrecy, authentication, and Non-repudiation and Data integrity too includes distinct security features comprising secured commerce, payments to private communications and protecting passwords. The unique trait of secure communications is the cryptography. Apprehensive use of internet, progressing cyber crime prefers a challenging field to IT security. The primitive solution to this defect is the cryptography, which reinforces on privacy, confidentiality and identity, providing the fundamentals for trusted e-commerce and secure communications.

The determining factor of a cryptographic algorithm or cipher is *a key* that decides its functional output or else no result is produced. A key in encryption influences the particular transformation of plaintext into cipher text and vice versa during decryption. Moreover finds its applications in other cryptographic algorithms as digital signature schemes and message authentication codes. By the concept of a Brute force attack, the key must be long enough to break. The key significantly maintained secret, should be of at least, a length of 80 bits for strong security, with symmetric encryption also finds its applications in other cryptographic algorithms as digital signature schemes and message authentication codes. Algorithms with 128-bit keys are considered very strong. Our proposed approach tries to overcome this confront.

Other security primitives are built, key management is an essential. No other key management schemes are suitable for ad-hoc networks. They are unknown network topology, an arbitrary is non functional or changing network topology is non tolerant or link failures in addition to inefficient also. Key pre-distribution schemes are the only practical option for scenarios where the network topology is unknown prior to deployment suggested by the recent research on distributed sensor networks. All of the existing key pre-distribution schemes rely on trusted third parties rendering them inapplicable in many ad-hoc networking scenarios in addition to restrict them from wide-spread use in ad-hoc networks.

Distributed Key distribution scheme is introduced in addition to construct the first distributed key distribution scheme prototype to realize fully distributed and self organized key pre-distribution without relying on any infrastructure support. The main limitation of the previous schemes overcomes the key distribution of the distribution scheme's need for trusted third parties in order to establish routing infrastructure .The underlying networks are more over can be easily applied to the ad-hoc networking scenarios where key pre-distribution schemes are previously inapplicable. Key for communicating privacy shared problems; integrity in addition authenticity can't be generated. A network to bootstrap a secure communications infrastructure shouldn't allow a key distribution scheme. It is providing secrecy, preferably entity in addition to message authentication. The addition of new nodes, rather the revolution of old nodes shouldn't be allowed by the shared scheme. The deficiency of a central administration is the drawback of shared scheme. Privacy, authenticity in addition to integrity are the most security requirements that are addressed by building upon a solid key management framework.

Node mobility and Unreliable communication pose an unreal threat over network nodes. In certificate based schemes, certificate exchange provides noticeable expense in resource limited environments, which leads to a self-contained key management scheme, allowing a mobile node to carry the authentication information. The theory is based on, the mobile devices ensuring secure communication with the server before they are disposed to the action. Once they are dispatched, the remedial authentication is only by their local information. The basic limitation on using PKC is its computational complexity. The concept exposes a self-contained public key management scheme which includes all necessary cryptographic keys in individual nodes before they're aligned. Thus it favors zero communication overhead for authentication, for the nodes with other party ID's.

In our approach the key distribution applied for the shared key distribution is applied based on the Dispense Key approach where the number of keys generated are reduced hugely.

The security of these primitives is prerequisite by a secure key management scheme in addition to secure infrastructure in ad-hoc networks. Security services having no responsibility such as defining the policies for network more over predistribution of keys to all the participants. Their high computational complexity is not applicable to the shared scheme. Low computational complexity in addition to high degree of security is afforded by the security protocol. As the nodes can be turned off or stolen by intruders limited with physical security is provided. Arises the bottle neck, the number of nodes are required to recreate the key. Trying to communicate, the key are not found in the range of communication node.

Our paper is spontaneously ordered as follows. We start with section 2 with a brief review of related works. In section 3 the background intrinsic terms needed to know before implementing the proposed approach. Section 3 presents the proposed system elaborately. Experimental results are conferred in section 4. Finally section 5 concludes the paper.

## 2. RELATED WORK

An effectual way of shielding perceptive information while storing on media or transmitted through communicational links is termed as cryptography. There are several methods and techniques are available in Cryptography.

A substitution cipher is one of the method in which letters are replaced by other letters; On knowing the order of the cipher alphabet someone can decipher the alphabets used. A Letter-Substitution Ciphers is described in [1]. This approach suffers with the problem of absolute synchronization between sender and receiver additionally the numbers of keys are restricted.

Elliptic Curve Cryptography (ECC) is a public key cryptography. In public key cryptography each user or the device taking part in the communication generally have a pair of keys, a public key and a private key, and a set of operations associated with the keys to do the cryptographic operations. In [5] a brief preface is specified regarding the elliptic curve cryptography (ECC), its implementation procedure on considering the digital signature (ECDSA) and key agreement (ECDH) algorithms. Furthermore a short discussion is made concerning the implementation of ECC on two restricted fields such as prime field and binary field. A synopsis of ECC implementation on different coordinate systems called the projective coordinate systems is being endowed. In this approach the calculation of discrete logarithms is a quite typical one to put into operation.

An outlook of various cryptographic applications which are derived from the proposal of R.J. McEliece for the sake of using the error correcting codes for cryptographic purposes in [2] are offered by D. Engelbert, R. Overbeck, and A. Schmidt. Daniel J. Bernstein, Tanja Lange, and Christiane Peters has put forward new-fangled parameters for the McEliece and Niederreiter cryptosystems[3] thus greatly attaining standard levels of security against all known attacks. These improved attacks are taken as values for new parameters along with the current introduction of list decoding for binary Goppa codes; and the possibility of choosing code lengths that are not a power of 2. Thus resultantly the public-key sizes are significantly much smaller than previous parameter supplemented for the security purpose. The added a new advantage for McElice. This is also included implicitly in our proposed approach.

An ancient public-key cryptosystems ever designed is the McEliece cryptosystem. Based on linear error-correcting codes, it is the first ever public key cryptosystem developed. This system gains an added advantage because of having very fast encryption and decryption functions. The chief thing to be highly concentrated is that it requires a very large public key which makes it very complicated to use in many real time circumstances. The most probable situation is to advantageously use quasi-cyclic codes since it is characterizes to be rich in compact. Finally [4] affords a novel technique to reduce the Key Length in McEliece Cryptosystem. Encryption is carried on representing it as a number M, and raising M to a publicly specified power e, then enchanting the remainder while the result is alienated by the widely specified product n, of two large secret prime numbers p and q. The Decryption process is very similar; the only difference is a secret power d is used. All those public key cryptosystem rely on computational complexity of different mathematical problems

There are many security aspects concatenated with wireless adhoc networks. Some of them are as follows. As per in [8], [9], [10], [11], [12], [13] wireless sensor networks use symmetric key techniques for secure communication. The main advantage of symmetric key techniques is its computational and energy efficiency. In symmetric key techniques, secret keys are pre-distributed among nodes before their deployment. To use small memory size to establish secure communication among a large number of nodes and achieve good resilience is the biggest challenge of the key distribution scheme.

However, with a centralized server, security service for critical applications may suffer from low availability and poor scalability due to the low reliability and poor connectivity of ad-hoc networks. Furthermore, a single point failure of centralized server is able to paralyze the whole network, which makes the network extremely vulnerable to compromises and denial-of-service attacks. In order to improve resilience to break-ins in wireless ad-hoc networks, Zhou and Haas tailor has offered the certificate-based approaches to ad-hoc networks and present a distributed public-key management scheme for ad-hoc networks [7], where multiple distributed certificate authorities are used.

Due to the lack of support for authentication and confidentiality [9] , it is not suitable in critical applications over wireless ad-hoc networks. Pairwise key distribution schemes [10-12] are able to bolster authentication. But applying distribution keys leads to produce a large of number of keys which is a major challenge.

## 3. BACKGROUND

On the basis of number of keys involved for encryption and decryption, the cryptographic algorithms can be classified.

### Secret Key Cryptography (SKC)

In SKC it employs a single key for both encryption and decryption (hence also known as symmetric encryption). Here the key used at the sender is to encrypt the plain text used by the receiver in order to decrypt the received cipher text, thus the key is known secret, to both the sender and the receiver. The limitation met is the key distribution. The marked SKC scheme used today is DES. DES is related to block-ciphering in which it exercises a 56-bit key that functions on 64-bit blocks. The prime catalyst of DES is 3DES and DESX.

### Public Key Cryptography (PKC)

PKC enclose one key for encryption and another for decryption, both keys being mathematically related (hence involving pair of keys also known as asymmetric cryptography).One key encrypts the plaintext and the other decrypts the ciphertext.

The fundamental is that, it does not mind on which key is applied first, but both keys are required for the working process. In PKC, the public key is acquainted to the needs of owner while the private key is screened from the other users. Public-key cryptography algorithms are for private key exchange of encrypting message or a digital signature includes: RSA Encryption and Diffe-Hellman.

## 4. RSA ENCRYPTION

The RSA cryptosystem, introduced by Rivest, Shamir, and Adlement in 1977, is known for its security on the difficulty of solving the factors dividing large integers. Since the advent of Internet, the base of cryptography depends primarily on the RSA public key system. The constraint of RSA lies in the level of protection, being worn out by developing efficient methods.

### Quantum Cryptography

Quantum Cryptography, modern algorithm-based cryptography, are designed to provide secure communications over unsecured networks i.e., it can be used for interception-proof data transmission over transmission links that are accessible to the public and makes eavesdropping theoretically impossible. In the quantum cryptography the communications are carried out by replacing a digital one or zero signal to each of photon, which is often called as "grains of light". In quantum cryptography communications, the information taken by the photons is instantly broken if the communication is eavesdropped, thereby making it possible to know the interceptions made and making it impossible for the third party to be crypto-analyzed ,also the information transmitted are only the type of measurements and not their result.

### Linear Codes

A Linear Code *C(n,k )* over a field F is ventured in a vector subspace of $F^n$ with dimension *K.n* ,which is called the length of the code *C.* The minimum distance (C) is found having the hamming distance *d(x,y)* which is being calculated by the formulae $d:=min\{d(x,y)|x,y \in C, x\neq y\}$, Moreover *(n,k,d)* is judged as the parameter of *C.*

## 5. PROPOSED SYSTEMIZATION

Initially with an intention to provide secure communications in wired and wireless networks Key Management system is used. Initially the nodes are clustered stochastically and the leader nodes are elected. The cluster will be comprised of leader accompanying with neighboring hop nodes. The leader node in the cluster is responsive to create the possible keys for exchanging. The key pairs (Private and Public Key) are generated by leader node and will distribute the same key pairs to the neighbor hops belonging to the same group. The distribution process will be carried on by having the mutual understanding between the leaders in the respective groups. The following sections discusses regarding Encryption and decryption techniques while sharing.

## 4.1 Shared Key Management (SKM) Protocol

Originally the data is converted into ASCII format. There are certain steps in implementing this protocol. It includes the subsequent circumstances.

## 4.2 Key Generation

A key is [a tool to protect the small information] than an encryption algorithm, and quite easier to change if it is encompassed with the mutual agreement. A key which is often to protect (it's typically a small piece of information. Resultantly the hard-hitting strategy lies in proving the security to an encryption system in protecting the key. The key generation is carried out using Hamming Codes. These are widely used in computing, telecommunication, and other applications. The hamming code used in our approach is of n X k dimension. The generated matrix is called Hamming Matrix which is denoted as G.

When computer data is moved or stored a set of error-correction called hamming codes are used to detect and correct bit errors that can occur. Similar to further error-correction code, the hamming codes are devised with the concept of adding parity bits. It is because that when they are added to data, the data validation can be checked on after reading and after undergoing data transmission. Thus this parity bit adding process endeavors an added advantage to these error-correction code. It not only identifies a single bit error in the data unit, but also confirms its performance in locating the data unit. Suppose the leader node chooses this matrix for as [n, k, d] code.For Instance consider a linear code of length 7, dimension 4, and minimum distance 3. It is called the Hamming [7, 4, 3] code. This type of sharing is called dual sharing. It is a general type of linear code constructed by using an algebraic curve X over a finite field Fq

1. Assume a matrix S having k X k dimensions. That matrix is termed as a private between the nodes. The private may be varying by interchanging this matrix.
2. Assume another matrix P having n X n dimensions
3. Compute G'=G *S*P
4. This matrix is called Public Key matrix.

   Therefore the respective keys are estimated

## 4.3 Encryption & Decryption Process

This employs the procedure of McEliece algorithm.

1. Consider a plain text X also embedded with the weight vector e.
2. The cipher text is computed to be
3. Y= x*G + e
4. Calculate approximately $y_1$=y $*P^{-1}$
5. This gives the encrypted text.

The decryption process is carried out having the

1. The decryption process is carried out having $y_1$ by extracting the first four components of $X_1$ . which is represented by $X_0$
2. The corresponding nodes will calculate x=$S^{-1}$ * X

3. Finally x gives the plain text.

Thus the encryption and decryption process along with key generation is carried out having McElice Algorithm. Key distribution is given by the Dispense Key Approach.

## 4.4 Dispense Key Approach

In Dispense Key, assume a group of agents in an incident network, who want to exchange correspondence securely among each other in pair-wise. Consider a key pool *K* that consists of a set of private-public key pairs, which is maintained by an off-line trusted server. Each key pair consists of two mathematically related keys.

The i-th key pair in the key pool is represented by ($k_{ipriv}$ , $k_{ipub}$). To support secure communication in the group, each member is loaded with all public keys of the group and assigned a distinct subset of private keys. Let IPriv denote a subset of private keys held by Alice, and IPub represents Alice's corresponding public key subset. If Bob wants to send a secret message to Alice, he needs to know KPub, where $k_{ipriv}$ the anonymous designator. Bob is able to pass the secret message to Alice, using the public keys KPub to encrypt the message. The message can be opened only by Alice, who has the private key set $k_{ipriv}$ , but others do not.

Consider an example of a small group with 10 nodes. In Dispense Key, 5 distinct public-private key pairs are needed to build pair-wise secure communication channels among 10 nodes. They are ($k_{1priv}$; $k_{1pub}$), ($k_{2\mathrm{Priv}}$; $k_{2pub}$), ($k_{3priv}$; $k_{3pub}$), ($k_{4priv}$; $k_{4pub}$), ($k_{5priv}$; $k_{5pub}$).

Leader node keeps 5 public keys and 2 private keys. Each node keeps a predetermined subset of private keys, and no one else has all the private keys in that subset for a public-private key pair, multiple copies of the private key can be held by different users. In the given scenario, each private key has 4 copies. A message is encrypted by multiple public keys, and it can only be read by a node who has the corresponding private keys.

If leader node 1 encrypts a message *m* by public keys $k_{2pub}$ and $k_{5pub}$ as *Enc*(*Enc*(*m*; $k_{2pub}$); $k_{5\ pub}$),then only user 7 can decrypt it with private keys $k_{2priv}$ and $k_{5priv}$. In this way the pair wise keys are generated.

## 5. EXPERIMENTAL RESULTS

The experiment is conducted having several nodes. The algorithms namely AES, DES, RSA are implemented with McElise. The result reveals that McElice is having good throughput when concentrated on Encryption and Decryption scenarios. Figure 1 expels execution time for performing encryption as well as comparison is made for the four approaches. It is that McElice is exploited with less execution time with the other approaches. Same circumstances are prevailing for figure 2 , figure 3 ,figure 4 which exemplifies McElice is providing less execution time for decryption , memory usage is also reduced with respect to both circumstances(Encryption, Decryption).

In our experiment the dimensions of Hamming matrix is of the fixed form which is taken to be 7 X 4 . This dimension in order to bring maintain the accuracy. Moreover primary key is taken by interchanging of S matrix for those corresponding nodes.

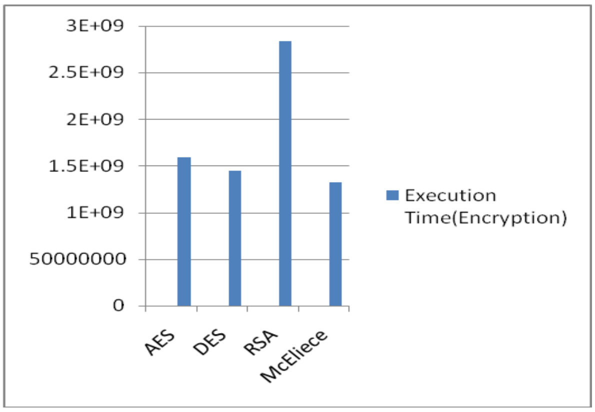

**Figure 1: Execution Time (Encryption) Comparison**

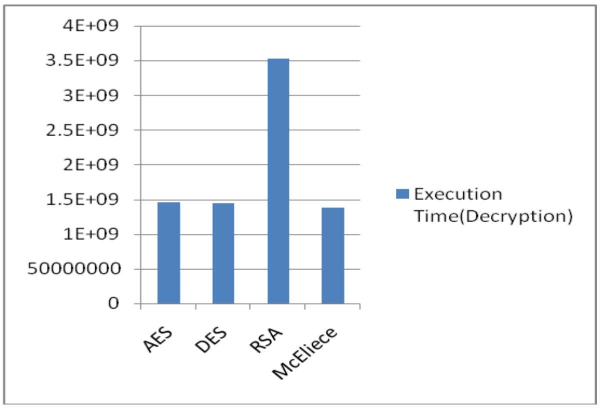

**Figure 2: Execution Time(Decryption) Comparison**

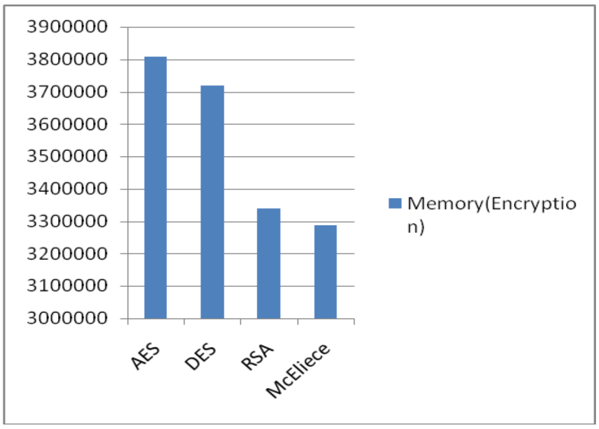

**Figure 3: Memory (Encryption) Comparison**

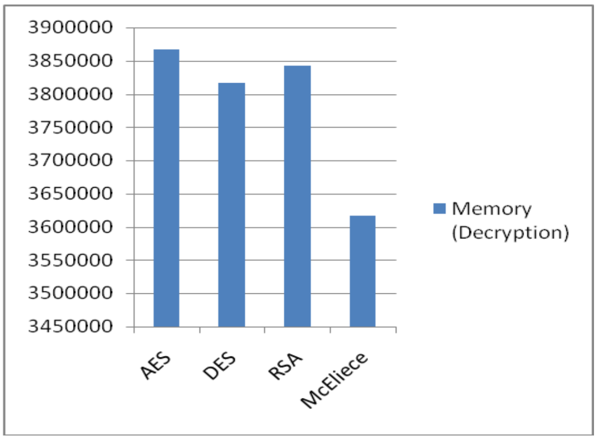

**Figure 4: Memory (Decryption) Comparison**

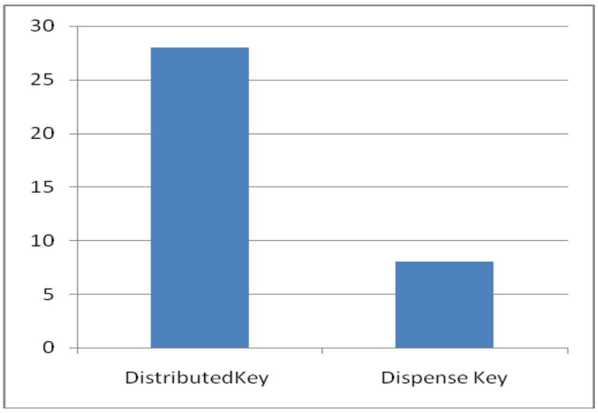

**Figure 5: Comparison between Distributed and Dispense Key**

Moreover when proposing the Dispense Key approach the key management circumstances are very effective. For instance we have considered some nodes which are clustered initially. The leader node is elected and the corresponding virtual group nodes are constituted by the nodes. It is observed that totally 14 key pairs are formed but the used keys are only 8. In the previous approach which uses distributed scheme the neighboring nodes will create their individual keys in which the numbers of keys are very large with respect to the neighboring nodes say total key pairs are 14 out of that deployed keys are 28. This experimentation is portrayed in figure 5. Resultantly the numbers of keys are reduced in our proposed system. It is known that due to the portability the wireless device constitutes having limited bandwidth, memory and processing power. Consequently the proposed approach SKM is adaptable for all the throughput constraints. These circumstances are depicted in Figure 6.

## 6. CONCLUSION

Our Proposed approach SKM where McElice ensembled with Dispense Key approach tends to be effective in both key generation and its management. As the key size is very large in McElice approach, it provides a secure authentication mechanism. On considering the scalability in terms of number of nodes and the memory space, we have outfitted our system comprising of its flexibility, and affordability with respect to public-private key pairs framing, which designates the nodes to be united with more than one key pair to encrypt and decrypt messages. The storage space for traditional self-contained public key management schemes is of O(n) order. With this combinatorial framework we expect better scalability and still reducing time delay constraints than traditional broadcast authentication schemes. This will be investigated deeply in future work.

## 7. REFERENCE

[1] "An Exact A* Method for Deciphering Letter-Substitution Ciphers" - Eric Corlett and Gerald Penn, Jul 2010

[2] "A Summary of McEliece-Type Cryptosystems and Their Security" - D. Engelbert, R. Overbeck, and A. Schmidt , 2006

[3]"Attacking and defending the McEliece cryptosystem" - Daniel J. Bernstein, Tanja Lange, and Christiane Peters, Aug 2008

[4]"Reducing Key Length of the McEliece Cryptosystem" - Thierry P. Berger, Pierre-Louis Cayrel, Philippe Gaborit, and Ayoub Otmani,2009

[5]"Elliptic Curve Cryptography" - An implementation Guide , Anoop MS, anoopms@tataelxsi.co.in

[6] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Comm. ACM, vol. 21, pp. 120-126, 1978.

[7]"Securing Ad-hoc Networks. IEEE Network Magazine " - L. Zhou and Z. J. Haas , Nov. 1999.

[8] S.A. Camtepe and B. Yener, Combinatorial design of key distribution mechanisms for wireless sensor networks. In Proceedings of 9th European Symposium On Research in Computer Security (ESORICS 04), 2004.

[9] H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. In IEEE Symposium on Research in Security and Privacy, pages 197-213, 2003.

[10] W. Du, J. Deng, Y. S. Han, and P. K. Varshney. A pairwise key predistribution scheme for wireless sensor networks. In Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS), pages 42-51, Washington, DC, USA, October 27-31 2003.

[11] D. Liu and P. Ning. Establishing pairwise keys in distributed sensor networks. In Proceedings of 10th ACM Conference on Computer and Communications Security (CCS'03), pages 52-61, October 2003.

[12]F. Delgosha and F. Fekri. Threshold Key-Establishment in Distributed Sensor Networks Using a Multivariate Scheme.In Proceedings of 25th IEEE INFOCOM, April 2006.

[13] P. Traynor, H. Choi, G. Cao, S. Zhu, T. La Porta. Establishing Pair-Wise Keys in Heterogeneous Sensor Networks. In Proceedings of 25th IEEE INFOCOM, April 2006

[14] D. J. Bernstein, T. Lange, and C. Peters, "Attacking and defending the McEliece cryptosystem," Post-Quantum Cryptography, LNCS, vol. 5299, pp. 31–46, 2008.

[15] K. Kobara and H. Imai, "Semantically Secure McEliece Public-Key Cryptosystems-Conversions for McEliece PKC," Lecture Notes in Computer Science, pp. 19–35, 2001.

[16] S. Balasubramanian et. al., "Fast Multivariate Signature Generation in Hardware: The Case of Rainbow," 19th IEEE Int. Conf. on Application-specific Systems, Architectures and Processors ASAP 2008, 2008.

[17] D.J. Bernstein, T. Lange, and C. Peters, "Attacking and Defending the McEliece Cryptosystem," Post-Quantum Cryptography, pp. 31- 46, Springer, 2008.

[18]J. Buchmann, Introduction to Cryptography (Undergraduate Texts in Mathematics). Springer, 2004.

[19]D. Engelbert, R. Overbeck, and A. Schmidt, "A Summary of McEliece-Type Cryptosystems and Their Security," Math. Cryptology, vol. 1, pp. 151-191, 2007.

[20] D.J. Bernstein, J. Buchmann, and E. Damen, Post-Quantum Cryptography. Springer, 2009.