Security Using Identity Based Cryptography

Dr. Purvi Ramanuj [#1]

[#]*Department of Information Technology, Gujarat technological University*

[1]purviramanuj@yahoo.com

Abstract: In today's world, lots of transactions are carried out online and huge data is getting transmitted via various applications using computer networks. Many security solutions are already available and vast research efforts are being carried out worldwide. Elliptic curve cryptography has been proven a highly secure method for network security. Biometrics can be blended with identity-based cryptography for enhanced security and efficiency. A comprehensive key generation scheme is presented as a robust security solution. The scheme is not dependent on the type of network being used.

Key Words: **Identity based Security, Key management, Key generation, Fingerprint, ECC**

I. INTRODUCTION

Now a days everything and everywhere is on the internet, there exists a demand for standardization. For the same, various academicians and professionals have collaborated and are working on basic guidelines, standard process and policies on various security essentials like passwords, antivirus software, firewalls, encryption software, legal liability, training, and awareness imparting etc.

Various corporations, financial institutes, hospitals, social media, government departments and other institutes have huge data about their customers, employees, vendors etc. This information is very critical for the business to function and even a small leakage can destroy goodwill of the organization. It may lead to many legal and criminal actions.

Cryptography is widely used for providing security to networks and data transmission. All algorithm of cryptography depends on the piece of information called key. As algorithms are known to all, security highly depends on the key used for encryption and decryption. The key is a variable which changes its value frequently and is employed using an appropriate algorithm on a message which can be a string or block. On application, the key will transform such data into some complex – not an easily understandable form which is called encrypted data. Also, a key can recover the original data from an encrypted data which is known as decryption.

Research is going on to generate key easily and securely. After generation of a key, it is distributed to each node. There should be some mechanism which revokes a key in case of compromised keys. This process is called as the key revocation. Revoked nodes should also be given a new key. This is called the renewal of key. In many mechanisms, there is a provision of renewal of key after a predefined time.

II. REVIEW OF LITERATURE

In today's world, Security has emerged as an extremely important parameter for any kind of network. There exist different types of networks like mobile ad hoc network, wireless sensor network, vehicular ad hoc network, etc. In all types of network and in all types of communication, security is very important. Also, the level of security required differs from application to application. Such different security levels and varied applications made this issue more complicated for end users and interesting for researchers.

Various cryptographic algorithms which provide security are discussed.

A. Identity based key management system

Shamir (1) presented a novel solution to the problem of secret sharing among nodes. He devised an idea of sharing secret data D by dividing among n nodes in n pieces in such a way that it can be reconstructed by any t pieces. Even knowledge of t – 1 will not be able to reconstruct the data D. Shamir called it as (t, n) threshold scheme. He used polynomial interpolation and divided secret D into n pieces and each piece is the value of the polynomial at that point. Thus any t pieces can reconstruct D using Lagrange

interpolation. He suggested for modular arithmetic and not real arithmetic. This scheme was later on used by many researchers for construction distributed PKG to enhance security.
Various identity based key management scheme are available in the literature. Key management includes generation of the key and distributing the same safely and later on safekeeping and renewal of generated keys. A comparative study of some of the important schemes is presented here.

1) Khalili-Katz-Arbaugh's Id based key management (2)

This scheme emphasized on key distribution and threshold cryptography. It introduced the concept of distributed PKG. A set of n nodes required to perform the function of PKG. Such nodes are known as threshold PKG. The master Private key is provided to all nodes of a network in such a way that no any node can generate a master private key on its own but at least t nodes are required to complete this function. It is known as (t, n) threshold scheme. Node's identity is its public key. It assumed that node identity is recorded into hardware and can't be altered. Private Key is generated by at least t nodes collectively. Each of these t nodes shall provide a part of node's private key on successful authentication. A node combines these parts and gets its private key. Such a distributed function provides enhanced security against single point failure. For a successful attack, it requires one has to compromise at least t nodes. The value of selected t can be calibrated to suit the need for the application and required security.
This scheme does not address other aspects of key management namely key revocation and key renewal. No specification about how keys are generated. An attacker with false identity i.e. an attacker which has inbuilt an identity in such a way that it looks like an original node, can be a threat to the network. To get the private key by a new entrant, it requires safe and secured communication with at least t nodes.

2) Deng-Mukharji-Agrawal's scheme (3)

This scheme is divided into two parts:

- Private key generation in distributed way
- Identity based authentication

In the first phase, the master key is generated for key generator nodes. Each node's public and private key is calculated and sent in a secure way. In the second phase, identity based authentication is provided. Authentication is ascertained end to end. On successful authentication, a secret key is exchanged between nodes and communication takes place using such shared key. The scheme uses IP Address as identity.
In this scheme during key generation phase, network's master key is generated. Also, each node is provided with a pair of public and private keys. End to end authentication is provided through the presented authentication scheme which is based on node's identity. Also, the communication among nodes is confidential. On successful authentication only, a session key is exchanged and future communication takes place using this session key.
A node joining the network must demand its private key from t PKG nodes. Each node shall provide a part of node's private key and the receiving node on combining all these parts gets its private key. Such transmission of private key parts happens in a secure way. The requesting node generates the temporary public key. The secret part of the key is sent to the node encrypted with such public key.
In this scheme also, false identity poses a problem and may hamper the operation of the network. It is also silent on key revocation and renewal. Scheme for authority-less MANETs, so it is less applicable to single-authority network

3) IDAKE - Identity based authentication and key exchange (4)

There are two main variants of this scheme: Basic IDAKE and fully self-organized IDAKE. It uses symmetric cryptography and pairing based keys. The trusted Third party initializes all devices before they join the network. The public key is Qi = H1 (Idi ‖ 'expiry date'). They are first to introduce key revocation and key renewing mechanisms for IBC schemes.
Both the variants employ pairing based keys and symmetric cryptography. The scheme is divided into following six sub-algorithms:
Setup generates a long-term private key of PKG and public parameters of the network.
Extract generates participating nodes' public key – as identity and computes private key.
Distribute, the private key is provided to nodes, when two nodes want to communicate.
Compute algorithm provides a symmetric paired key which will be used for encryption of data.
Key Renewal will play its part when a key's lifetime is expired or it is revoked during operation.

Key Revocation is activated when a node is found to be compromised. Various rule-based observations are carried out like neighborhood watch and accusation scheme to perform this operation.
In basic mode, PKG performs pre-initialization activities like the setup, extract, and distribution of keys algorithm. In the second mode that is running system phase, nodes themselves perform various activities like computation of shared keys, key renewal, and key revocation. In this scheme, the attack can be easily performed because of single point failure.
In fully self-organized version, all tasks are performed by network nodes using (t, n) threshold scheme. This algorithm is silent on the way in which nodes distributes private keys.
In both, the variant resource requirement and complexity of computations depends on how key renewal and key revocation algorithms are designed.

4) Identity Based key management scheme – IKM (5)

This scheme is a combination of threshold cryptography and key management using identity. It Proves IKM has advantages over Certificate based cryptographic scheme. Public and private keys of the nodes are formed using their identity and a network-wide common element. PKG issues a random number salt to each node with an efficient hash function h such as SHA-1. Use of common network element facilitates fast and efficient key update through a broadcast message. On the other hand, ID-based element helps in maintaining the secrecy of nodes.
The key **pre-distribution** happens in network initialization where PKG provides keying material and system parameters to each node. PKG also hand over it's working to a set of distributed PKGs, which are called d-PKGs. The private key is computed by (t,n) threshold cryptography. For **key revocation,** during normal network operation mode, each node monitors another node for any malicious activity. If any suspected activity is observed then that node sends a signed message to d-PKG. A node is declared malicious when a number of accusations reported at d-PKG against it reach its defined revocation threshold limit. In this scheme, nodes update their public and private keys at defined intervals. A revoked node is not able to renew its key on its own and hence gets separated from the network

B. Comparison of different Id based key management system

Table I lists various key features of the above discussed ID-based key management schemes.

TABLE I
Key Features of Identity Based Key Management Schemes

	Khalili – Katz – Arbaugh	**Deng Mukherjee Agrawal**	**Basic – IDAKE**	**Dist. – IDAKE**	**IKM**
(t,n)	Yes	Yes	No	Yes	Yes
PKG	Internal	Internal	External	Internal	Internal
Key Renewal / Revocation	No	No	Yes	Yes	Yes
Private Key Distribution	Safe Channel	Temporary Key	Before N/W formation	Not clear	N/W Initialization

Apart from these key management schemes, there are other various identity based security schemes. These schemes are presented in Table II These schemes helped in designing final prototype of the proposed scheme. In (6) author used a fingerprint as a biometric attribute and generated identity based key pairs. Such keys were used for securely transferring secret key between nodes. On the other hand, (7) employed email address as identity. RSA algorithm was used for key generation. In this scheme, the concept of distributed PKG was not used and hence it is susceptible to single point breakdown.

TABLE II
Comparison of Key generation schemes

Author	**Main Contribution**	**Key Generation**	**Weakness**
Subhas Barman et al(6)	Biometrics-based authentication and secret key sharing	Fingerprint biometrics	Securely sending user identity to KDC. Pre-registration with KDC
Sachin Tripathi et al(7)	RSA based key generation using identity & hash function	Email address	Single point breakdown
Bohio – Miri(8)	Identity based group key generation	Not specified	Online server required for escrow free system. Universal forgery attack
Smart(9)	ID-based key agreement using Weil pairing with key confirmation	ID based	Key escrow problem
MQV(11)	Authenticated key agreement using ephemeral key pair	PKI based	Leaks private session information
Yasser(10)	Use of iris signature as ID with ECC for generation of ECC parameters	Iris data	Private Key not generated from iris. Key revocation and renewal not addressed

Bohio – Miri (8) introduced group based key generation but not clearly mentioned on which identity was used for key generation. Key escrow problem was addressed but online server access was required for the same. Smart (9) used Weil pairing for identity key generation but it is suffering from key escrow problem. MQV (11) introduced a novel concept of ephemeral key pairs for communication between threshold nodes and new joining nodes. Generated key share is transferred using such temporary keys. It still suffers from leakage of private session information. Yasser (10) used iris data as identity and for generation elliptic curve parameters. It was a nice practical implementation of elliptic curve cryptography using biometrics as identity. The scheme is silent on key revocation and key renewal.

Discussion: From the comparison, it is clear that Threshold based scheme eliminates the possibility of one point failure which is a desirable feature. Similarly internal or distributed PKG also helps in providing security. Also, private key distribution is a critical aspect but no one else except Khalili – Katz – Arbaugh have addressed it. Each scheme addresses different issues but also lacking on other. Key renewal and revocation are not addressed in Khalili – Katz – Arbaugh and Deng – Mukherjee – Agrawal. Broadly it is concluded that all these schemes have their benefits and shortcomings.

III. PROPOSED SCHEME

A. *Introduction*

A comprehensive solution of key management is presented in the proposed scheme. It focuses on two major portions of key management. They are key generation and key revocation. Key generation phase generates a secure cryptographic key using Elliptic curve cryptography, RSA, and fingerprint of the individual. This is a novel scheme which gives two level of security.

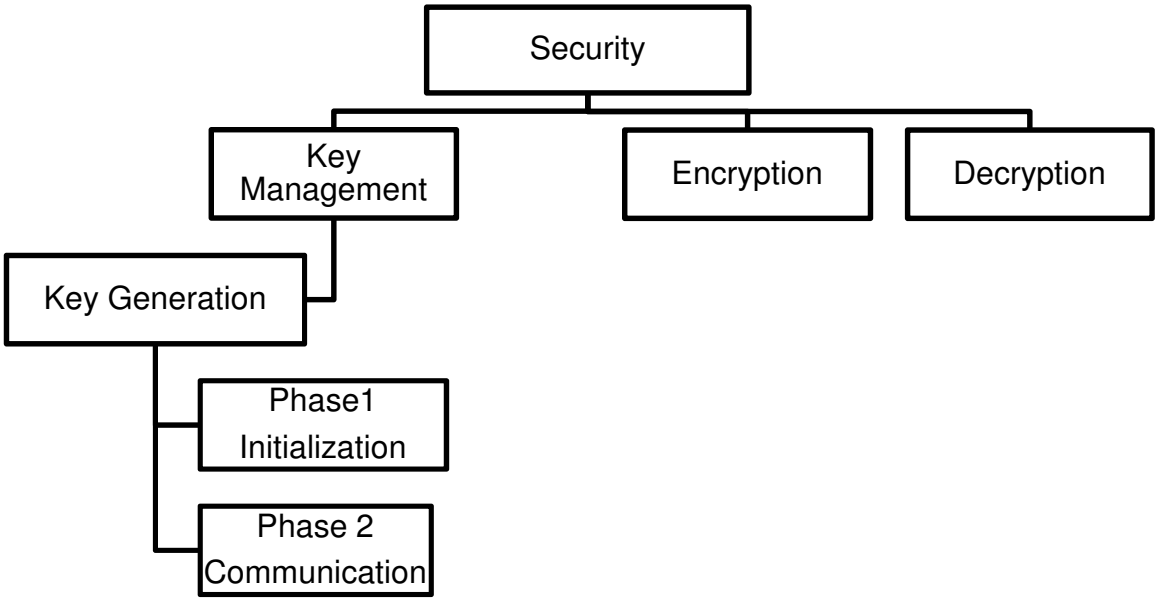


Figure: 1: Proposed Scheme

B. *Key generation*

The fingerprint of each person is unique. This is the most important feature which is used in the proposed scheme. The scheme is designed to achieve a high level of security using fingerprint signature generated from individual finger impression so as to produce the domain parameters of the elliptic curve, or to produce private keys. The fingerprint is one of the most reliable and most used biometric features. The signature is unique and can not to be produced by another individual. Generally, in elliptic curve cryptography schemes, a random value of parameters a and b are chosen. In the proposed scheme, fingerprint data and private key generated using RSA are used respectively for these parameters.

There are two stages of the key generation process. This provides two level of security. The first stage uses RSA algorithm, which is one of best trapdoor functions used since last several years. RSA uses the mechanism of multiplication and factorization concept. As multiplication of prime numbers is very easy but factorization is very difficult, RSA was known to be best and easy algorithm for years.

The second level uses ECC, Elliptic curve cryptography, which is the best performing algorithm nowadays. An Elliptic curve cryptography includes a prime number as a maximum, a curve equation, a private key which is a random number, and a public key which is generated multiplying private key with a generator point G on the curve. Computing the private key from the public key in this kind of cryptosystem is called the elliptic curve discrete logarithm function. This turns out to be a Trapdoor Function.

C. *Working Module*

The operation of the proposed scheme is described in this section. The scheme has following two phases:

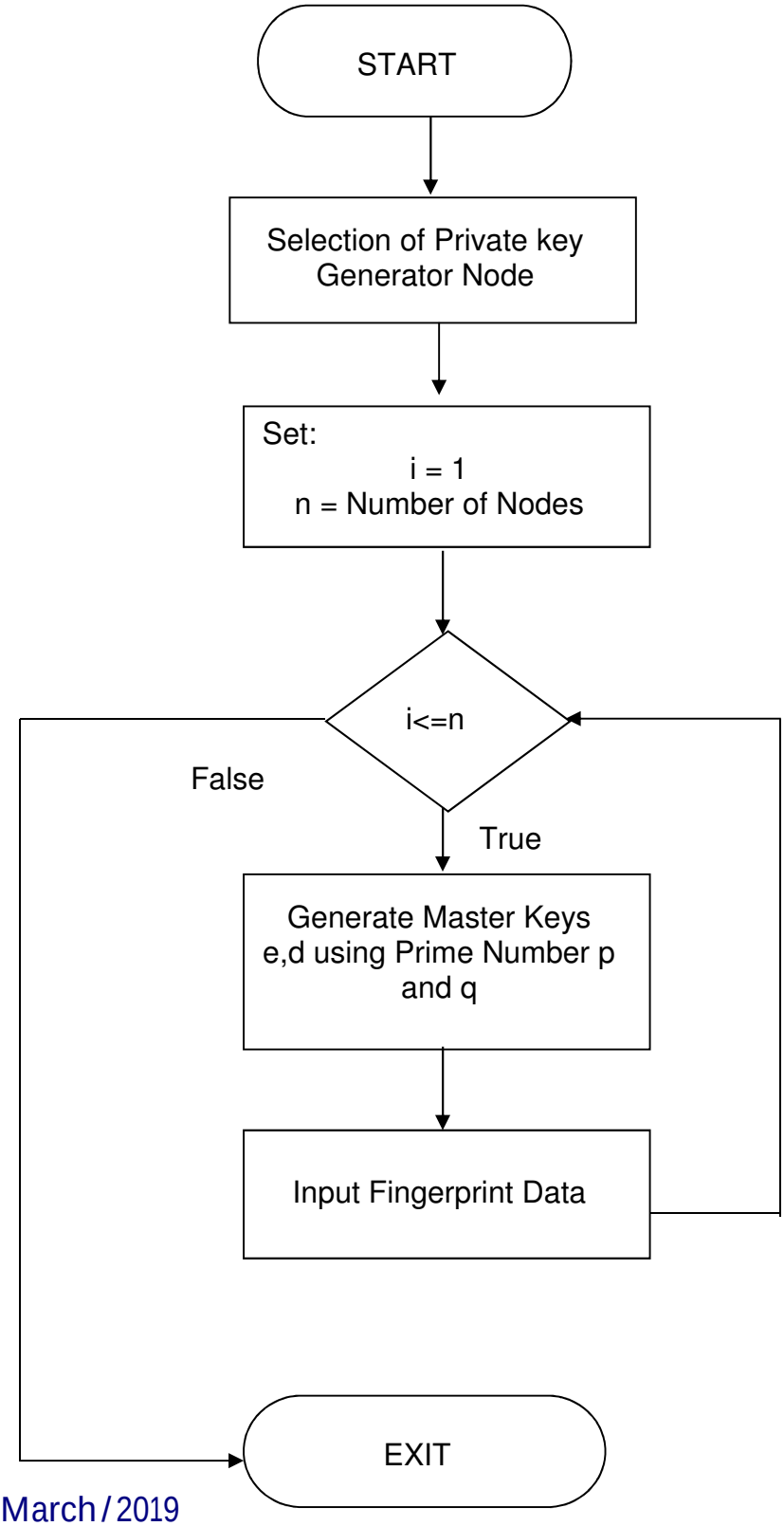
- Initialization
- Communication

In initialization phase Private Key Generator – PKG generates its own master private and public key using RSA algorithm. Also, fingerprint information is provided by each node to PKG. In communication phase, actual messages are transmitted between nodes.

Phase 1: Initialization

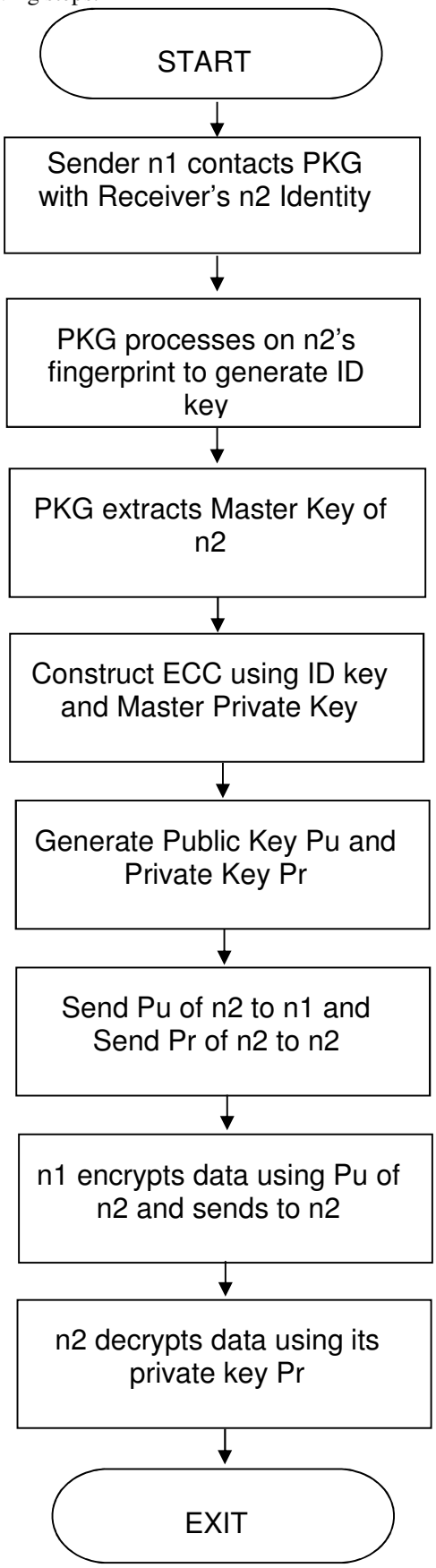
Before starting a network, this is an initial phase. Any node from the participating node can work as private key generator known as PKG. Following steps are executed for generation of the public key and private key by PKG.

Flowchart shown below:



Phase 2: Communication

Whenever any node wants to communicate with another node, it should have the public key of receiving node to encrypt the message. To get the Public key of the receiver, Sender node sends a request to PKG. The process can be defined in following steps.



Process shown in flowchart as above

In this section, the proposed methodology of generation of cryptographic key and modification in key revocation scheme is shown. The concepts used are an identity-based key generation, fingerprint, RSA, and ECC. Proposed scheme provides two level securities using RSA and ECC algorithm and Identity-based encryption simplicity mechanism.

IV. CONCLUSION

From the presented literature review, the need for robust security solution was identified. In today's world security is the key concern. Various identity based key management solutions are found in the literature. They are the best choice among various other schemes for providing security. It is also very obvious that different applications require different levels of security and hence there is a pressing need for a solution which is flexible enough and scalable for providing different levels of security.

Various research papers are available which uses biometrics for cryptographic operations. But only a few were found employing biometric trait to be used as elliptic curve generation parameters. It is observed that a perfect blend of biometric and elliptic curve cryptography is required to provide robust security. Enhancement in security level can be performed by the double-layered security of RSA and Identity based cryptography.

REFERENCES

[1] A. Shamir, "How to share a secret," Communications of the ACM, vol. 22, no. 11, 1979

[2] Hongmei Deng, Anindo Mukherjee, Dharma P. Agrawal, Threshold and Identity-based Key Management and Authentication for Wireless Ad Hoc Networks, Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04) Volume 2, p.107, April 05-07, 2004

[3] K. Hoeper and G. Gong, "Bootstrapping Security in Mobile Ad Hoc Networks Using Identity-Based Schemes with Key Revocation," tech. rep., Centre for Applied Cryptographic Research, Univ. of Waterloo, 2006

[4] M. Boujelben, H. Youssef, R. Mzid, and M. Abid, "IKM—An identity based key management scheme for heterogeneous sensor networks," J. Commun., vol. 6, no. 2, pp. 185–197, Apr. 2011

[5] S. Barman, S. Chattopadhyay, D. Smanta,"An Approach to Cryptographic Key Distribution Through Fingerprint Based Key Distribution Center", Advances in Computing, Communications and Informatics, 2014, pp: 1629 – 1635

[6] S. Tripathi, G.P. Biswas, and S. Kisan, "Cryptographic keys generation using identity," in Proc. 3rd International Conference on Advances in Recent Technologies in Communication and Computing (ARTCom 2011),2011, pp. 148-15l

[7] M. J. Bohio and A. Miri, "Efficient Identity-Based Security Schemes for Ad Hoc Network Routing Protocols," Ad Hoc Networks, vol. 2, no. 3, 2004, pp. 309–17

[8] N.P. Smart. An identity based authenticated key agreement protocol based on the Weil pairing. Electronics Letters, 38(13):630–632, 2002

[9] Yasser Salem Mohamed Ali, "Implementation of Elliptic Curve Cryptography using biometric features to enhance security services", Master of Comp.Science, Thesis, pp.17-38,July 2009

[10] Alfred J. Menezes, Minghua Qu & Scott A. Vanstone, Some new key agreement protocols providing mutual implicit authentication, pp. 22-32, Selected Areas in Cryptology – SAC '95