Digital Signature Scheme with Message Recovery Using Knapsack-based ECC

R. Rajaram Ramasamy and M. Amutha Prabakar
(Corresponding author: R. Rajaram Ramasamy)

Department of Computer Science and Engineering, Thiagarajar College of Engineering
Thiruparankundram, Madurai, Tamil Nadu, India, 625 015, India (Email: rrajaram@tce.edu)

(Received Mar. 12, 2009; revised and accepted July 27 & Sep. 15, 2009)

Abstract

Digital signature authentication scheme provides secure communication between two users. Digital signatures guarantee end-to-end message integrity and authentication information about the origin of a message. Digital signature schemes reduce transmission costs, because the message is contained in the signature itself and no separate message and signature need be sent again. These schemes are very suitable for key exchange applications, due to the small size of the key. In this paper, we present a new digital signature scheme with message recovery based on knapsack based elliptic curve cryptography (ECC). Elliptic curve cryptosystem provides greater security compared to integer factorization system and discrete logarithm system, for any given key size and bandwidth. In our scheme, using ECC and then applying the knapsack generates the signature. Our scheme is secure against most of the current attacking mechanisms.

Keywords: Authentication, digital signature, discrete logarithm, elliptic curve cryptography, knapsack, message recovery

1 Introduction

Digital signature authentication schemes provide secure communication with minimum computational cost for real time applications, such as electronic commerce, electronic voting, etc. The sender generates the signature of a given message using his secret key; the receiver then verifies the signature by using sender's public key. The verification is done in two ways: verify the signature accompanying the clear message, or verify the signature with message recovery. In the first case the signature portion appended with the clear message is decrypted for verification. In the second case the message itself constitutes the signature, and must be decrypted to recover the original message. The second scheme hides the message from unnecessary intruders. Nyberg and Rueppel [5] proposed the signature scheme with message recovery based on discrete logarithm. In 2004, Tzeng et al. [16] proposed a new signature scheme with message recovery using the technique of self-certified public keys. Two public key signature schemes that have received widespread attention are RSA [1] and Digital Signature Algorithm [4]. RSA uses two modes of signature verification. One is the text-hashing mode and another is the message recovery mode. In the text-hashing mode, a hash value of the message is generated and appended with the clear message during transmission. The receiver then evaluates the hash value from the message and compares it with the appended hash value.

Digital Signature authenticated schemes, have the following properties.

1) **Confidentiality**. Secret information shared between sender and receiver; any outsider cannot read the information.

2) **Authentication**. The sender imprints his identity by means of the digital signature, which only the designated receiver can unravel and verify. An anonymous adversary cannot send a malicious message impersonating the genuine sender, because he does not have the necessary tools to generate the signature.

3) **Non-repudiation**. The signature firmly establishes the identity of the sender. The sender cannot deny having sent the message and the signature.

4) **Message recovery**. Upon receipt of the cipher text, the recipient decrypts it and segregates the signature and the message and verifies the authenticity of the sender. Only he will be able to do so because he alone has the necessary tools.

In this paper, we propose a new digital signature scheme with message recovery using self-certified public keys based on Elliptic Curve Discrete Logarithm Problem (ECDLP). The public key and the private key of the proposed scheme are agreed upon between the user and server through secure channel, so also the knapsack vector series a_i and n value (unique value for every user). It is computationally infeasible for the adversary to find the private key from the publicly known information.

2 Related Work

Some researches on digital signature authentication schemes based on elliptic curve discrete logarithm problem (ECDLP) are ongoing. Miller [2] and Kobitz [10] introduced the elliptic curve cryptosystem in 1980. It provides greater security than integer factorization systems and discrete logarithm systems, for given key size and bandwidth [2, 7]. Tzeng et al. [16] proposed an authenticated encryption scheme based on ECDLP . Most digital signature schemes currently available are based on well-known public key systems, such as the RSA system [1, 8, 12, 13] and the ElGamal system [3, 14]. Moreover digital signature schemes with message recovery are important for small applications. The sender generates the signature from the message. Upon receiving the cipher text containing the signature, the receiver decrypts it to recover the message, thereby establishing the identity of the sender.

In 1994, Horster et al. [6] presented an authenticated encryption scheme, which is a modified version of Nyberg and Rueppel's scheme [5]. In this scheme, only the designated verifier can retrieve the message from the signature. Hence, the scheme is regarded as a combination of the data encryption and the digital signature. The scheme requires smaller bandwidth for data communications to achieve privacy, integrity and authentication of information.

In 2004, Tzeng et al. [16] introduced a new digital signature scheme with message recovery based on ECC. They utilized the characteristic of ECC and self-certified public key, which was first proposed by Girault in 1991. Nyang et al. [17] proposed a digital signature scheme based on interactive zero knowledge proof. Chen et al. [18] proposed a digital signature scheme from identification protocol based on Elliptic Curve Cryptosystem. Dang [19] proposed a new randomized hashing digital signature scheme. Brown [20] has pointed out the conditional security analysis of the elliptic curve digital signature algorithm. Nguyen et al. [21] claims that elliptic curve digital signature algorithm is insecure, due to partially known nonces by the adversary.

Rajaram et al. [22] introduced knapsack based Elliptic Curve cryptography. Their algorithm involves a high degree of sophistication and complexity, and it is almost infeasible to attempt a brute force attack. Moreover only one parameter, namely the Knapsack vector alone needs to be kept secret.

In this paper, we have extended this algorithm for digital signature scheme with message recovery. The proposed method has two levels of authenticated encryption. First one is based on Elliptic Curve signature and second one is applying knapsack value for the signing message. The proposed method provides high security with reasonable computational cost. In this paper, Section 1 gives introduction about our scheme. Section 2 deals with other related works. Section 3 deals with the proposed new digital signature scheme-applying knapsack on ECC. In Section 4, a security analysis of the proposed scheme is presented. In Section 5 the concluding remarks are made.

3 Proposed Digital Signature Scheme With Message Recovery

In this paper, we propose a new Digital Signature scheme with message recovery based on Knapsack Based ECC. The proposed scheme is divided into three phases: Initial Phase, Signature Generation Phase, and Signature Verification Phase.

3.1 Knapsack Vector Generation

Knapsack vector values are generated using a series of vectors called a_i (this can be a common one for all the users or unique one for every user). There are several ways of generating these vector values. For example, we shall take the first value as 1, and subsequent values as multiples of n. Say

$$a_i = 1, n, n_2, n_3, ..., n_m \quad 1 \leq i \leq m.$$

Here, n may be assumed as some random integer, for example n is number less than p and k integers. Here p is a prime integer used in the modular arithmetic, k is the secret integer and m is the length of the binary bit string. Next let us explore how the signed message is subjected to Knapsack process. Say, r and s are converted as follows, which can be represented in its binary form as:

$$r = b_1, b_2, b_3, \cdots, b_m,$$

where r and s are generated as discussed in *Signature Generation Phase.*

As per the knapsack algorithm we calculate a cumulative sum R,

$$R = \sum_{i=1}^{m} a_i x_i.$$

In the final signed message version, r value is replaced by its equivalent R. Similarly s value transformed by knapsack algorithm as S.

Initial Phase: In the proposed network setup, there is a trusted authority called (SA) who is responsible for creating the system parameter. SA first selects the elliptic curve $E : y^2 = x^3 + ax + b$ defined over Z_p where p is a prime. Let $G \in E(Z_p)$ be a base point of order n which is prime. SA identifies E, p, n and G points. SA calculates $b = aG$, where $a \in [1, n-1]$ is a random number and this value is secret. Suppose a user *Alice* requires to join the system then she should register with the trusted authority through a secure channel. The user *Alice* first chooses a random number $x_{Alice} \in [1, n-1]$. Then she computes $y_{Alice} = x_{Alice}G$, and sends $(y_{Alice}, ID_{Alice}$ through a secure channel to SA, where ID_{Alice} is user Alice's identity.

Signature Generation Phase: If *Alice* wants to sign a message M, she should perform the signature procedure as follows.

Step 1. Choose a random number $k \in [1, n-1]$.

Step 2. Compute the signature (r, s) of the message M with $r = M + (kG)_x \bmod n$, and $s = k - H(r)x_{Alice} \bmod n$.

Step 3. Apply the knapsack value for the signed message:

1) $R = Knapsack(r)$ and $S = Knapsack(s)$.
2) Send a signed message $\{R, S, ID_{Alice}\}$ to user Bob.

Message Recovery Phase: After receiving $\{R, S, ID_{Alice}\}$, Bob can apply the reverse knapsack. Recover and verify the message M with $M = r - (sG + H(r)(y_{Alice})_x \bmod n$. The below given algorithms explains the signature generation and verification phase in detail.

3.2 Algorithms

Algorithms for initial phase, signature generation phase and signature verification phase explained below.

Initial Phase:

Step 1. SA is a trusted authority who selects the elliptic curve E defined over Z_p.

Step 2. Let $G \in E(Z_p)$ a base point of order n which is prime.

Step 3. Select a random number $a \in [1, n-1]$, this value is secret.

Step 4. Calculate $b = aG$,a, b are the key pairs of the trusted authority. *If user Alice wants to register with the trusted authority, she has to do the following steps.*

Step 5. User Alice selects a random number $x_{Alice} \in [1, n-1]$.

Step 6. Computes the public key $y_{Alice} = x_{Alice}G$ and send $(y_{Alice}, ID_{Alice}$ to trusted authority SA. Here ID_{Alice} is the identity of user Alice. E, Z_p, p are common for all users and key pairs $\{y_{Alice}, x_{Alice}\}$ are unique to particular user.

Signature Generation Phase:

Step 1. Alice wants to sign a message and send it to server for authentication.

Step 2. Choose a random number $k \in [1, n-1]$.

Step 3. Compute the signature (r, s) of the message M.

Step 4. $r = M + (kG)_x \bmod n$, and $s = k - H(r)x_{Alice} \bmod n$.

Step 5. $R = KnapsackValue(r)$.

Step 6. $S = KnapsackValue(s)$.

Step 7. Singed message is $\{R, S, ID_{Alice}\}$ and send it to user Bob.

Signature Verification Phase: After receiving the message $\{R, S, ID_{Alice}\}$ following steps are performed by server.

Step 1. Server knows the knapsack vector and n value, apply the reverse knapsack.

Step 2. Computes $r = ReverseKnapsackValue(R)$.

Step 3. Computes $s = ReverseKnapsackValue(S)$.

Step 4. Recover and verify the message M, $M = r - (sG + H(r)(Y_{Alice})_x \bmod n$.

4 Security Analysis

In this section, we give an analysis about our proposed scheme. A number of attacks against the proposed schemes are presented. There are two basic attacks against public-key digital signature schemes.

- Key-only Attacks: In these attacks, an adversary knows only the signer's public key.
- Message Attacks: Here an adversary is able to examine signature corresponding either to known or chosen messages. Message attacks can be further subdivided into three classes, 1) *known-message attack*, 2) *chosen-message attack*, and 3) *adaptive chosen-message attack*.

In our proposed digital signature scheme with message recovery, we consider three kinds of attacks.

Attack 1. An adversary attempts to derive the user's private key x_i from known public information (E, p, n and G point, y_i public key of user) available. We have shown this attack is not possible in our proposed scheme.

Proof. An adversary can not derive $y_{Alice} = x_{Alice}G$from known public information, because ECDLP to obtain *Alice*private key $x_{Alice's}$ is difficult. □

Attack 2. Adversary attempts to forge a digital signature to impersonate as user *Alice*.

Proof. In Attack 2, we have considered two scenarios as explained.

Table 1: Security requirement estimation for different authenticated encryption schemes

Security Requirement	Horster et al. [6]	Wu-Hus [15]	Tzeng-Hwang [16]	Nyang et al. [17]	Chen et al. [18]	Hsu-Wu [9]	Proposed Scheme
Confidentiality	No	Yes	Yes	Yes	Yes	Yes	Yes
Authentication	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Non-repudiation	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Message Recovery	No	Yes	No	No	No	No	Yes
Convertibility	Yes	No	Yes	Yes	Yes	Yes	Yes

Scenario 1: Suppose an adversary wants to create a valid signature, then he has to know the knapsack vector generation series. The n value is unique for every user and the vector generation series is unique for every user.

Scenario 2: Suppose some adversary knows the value of n and vector generation series of user *Alice*. If suppose the adversary wants to create a valid signature then he must know the value of private key x_{Alice} of user *Alice*, this is not possible in our scheme. The private key of user *Alice* is not possible using (ECDLP) to recover from the public know information (shown in Attack 1).

□

Attack 3. Suppose an adversary attempts to decrypt the message M from the digital signature R, S without knowing user *Alice's* private key $\{x_{Alice}\}$ in our proposed scheme.

Proof. In Attack 3, suppose an adversary attempts to decrypt the signed message M then he has to know two things for applying the reverse knapsack, 1) the knapsack vector generation series and 2) value for generating the knapsack values. These two things are unique for every user. So, the adversary's attempt of applying the reverse knapsack will not work. So, Attack 3 is not possible in our proposed scheme □

4.1 Security Requirement for Authenticated Encryption Scheme

According to the above description of the development of the authenticated encryption schemes, it can be inferred that an authenticated encryption scheme corresponds with the following properties: Confidentiality, Authentication, Non-repudiation, and Message recovery (explained in above section). These are the basic requirements of the authenticated encryption scheme. Any scheme, which satisfies these characteristics, can be called an authenticated encryption scheme. There is an additional requirement called *Convertibility*, which was proposed by Wu and Hsu [15] in 2002.

Convertibility. When a dispute occurs between the sender and the receiver, the authenticated encryption schemes should provide a mechanism to convert the signature to original signature that can be verified by the other third party. Table 1 illustrates the requirement estimation for proposed scheme with related schemes. We consider four related authenticated encryption schemes: Horster et al.s scheme [6], and Wu and Hus scheme [15]. In 2004, Tzeng and Hwang [22] proposed a signature scheme with elliptic curve cryptosystem. The Hsu and Wu [9] proposed a (t, n) threshold authenticated encryption scheme.

5 Performance Analysis

This section analyzes the performance all the abovementioned schemes with the proposed scheme. For convenience, we define some notations to denote the performance time.

5.1 Performance Notations

The performance notations are shown as follows.

T_{mul}	is the time for multiplication.
T_h	is the time for executing hash function.
T_{exp}	is the time for exponentiation with $\bmod P$.
T_{inv}	is the time for inversion $\bmod P$.
T_{KV}	is the time for knapsack value generation.
T_{inKV}	is the time for inverse knapsack value generation.

The T_h, T_{exp}, T_{mul}, T_{inv}, T_{KV}, T_{inKV} entail heavy computational cost. T_{ECmul} is used to indicate the time for multiplying a number by a point on the elliptic curve. T_{ECadd} is the time for the adding one point to another on the elliptic curve. Normally, it has minimum computational cost. In this performance analysis, we consider two phases to measure the performance analysis. One could dispute the computational cost over two phases, signature generation phase, and message recovery phase. The signature generation phase of Horster et al. [6] requires $T_{exp} + T_{inv} + 2T_{mul} + T_h$ and the message recovery phase needs $2T_{exp} + T_h + 3T_{mul}$. The signature generation phase of WuHus [15] requires $3T_h + T_{inv} + 2T_{mul} + 2T_{exp}$ and the message recovery phase needs $3T_h + T_{inv} + 3T_{exp}$. In the Tzeng and Hwang

Table 2: Estimated time for various operations

Operations (128 bit)	Estimated Time in ms
T_{mul}	≈ 1.527932 ms
T_h	≈ 1.513726 ms
T_{exp}	≈ 2.139810 ms
T_{inv}	≈ 2.620675 ms
T_{KV}	≈ 1.307250 ms
T_{inKV}	≈ 1.368383 ms
T_{ECmul}	≈ 44.310028 ms
T_{ECadd}	≈ 0.164062 ms

AES based on ECDLP [16], the signature scheme with message recovery, the signature generation phase needs $T_{ECmul} + T_{mul} + T_h$, and the message recovery phase has costs $2T_{ECmul} + T_{ECadd} + T_h$. In the Hsu and Wu [9] scheme, the signer generates a signature that the computational cost is $3T_{exp} + T_{mul}$, and the verifier recovers the message which needs $3T_{exp} + (2t + 1)T_{mul} + (t - 1)T_{inv}$. In the Nyang et al. [17] scheme, signature generation phase and verification phase required computational cost $2T_{exp}+T_{mul}+T_h$ and $2T_{exp}+T_{mul}+T_h$ respectively. Chen et al. [18] scheme, requires the computational cost for signature generation phase of $2T_{ECmul}+T_{ECadd}+T_{mul}+T_h$ and verification phase required $3T_{ECmul} + 2T_{ECadd} + T_h$. Table 2 illustrates the estimated time for various operations, for the implementation purpose we are taking 128-bit data.

Table 3 illustrates the computational performance analysis for different authenticated encryption schemes with the proposed scheme.

6 Conclusion

This work proposes a new digital signature scheme with message recovery using knapsack based ECC. Proposed scheme provides high security with minimum computational cost. The scheme withstands three kinds of attacks (private key derivation, forged signature generation, and digital message recovery). The proposed scheme could successfully ward off these possible attacks. To the best of our knowledge, this is the first work which proposes a new digital signature scheme with message recovery using Knapsack based ECC

References

[1] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Communications of the ACM*, vol. 21, pp. 120-126, 1978.

[2] V. Miller, "Use of elliptic curves in cryptography", *Advances in Cryptology (Crypto'85)*, LNCS 218, pp. 417-426, 1985.

[3] T. ElGamal, "A public-key cryptosystem and a signature scheme based on discrete logarithms", *IEEE Transactions on Information Theory*, vol. IT-31, pp. 469-472, July 1985.

[4] National Institute of Standards and Technology (NIST), "The digital signature standard proposed by NIST", *Communications of the ACM*, vol. 35, no. 7, pp. 34-40, 1992.

[5] K. Nyberg and R. A. Rueppel, "A new signature scheme based on the DSA giving message recovery", *ACM Computer and Communications Security*, vol. 1, pp. 58-61, 1993.

[6] P. Horster, M. Michels and H. Petersen, "Authenticated encryption schemes with low communication costs", *Electronics Letters*, vol. 30, no. 15, pp. 1212, 1994.

[7] A. Menezes and S. Vanstone, "Elliptic curve systems", *Proposed IEEE P1363 Standard*, pp. 142, 1995.

[8] C. C. Chang and M. S. Hwang, "Parallel computation of the generating keys for RSA cryptosystems", *IEE Electronics Letters*, vol. 32, no. 15, pp. 1365-1366, 1996.

[9] C. L. Hsu and T. C. Wu, "Authenticated encryption scheme with (t, n) shared verification", *IEE Proceedings - Computers and Digital Techniques*, vol. 145, no. 2, pp. 117-120, 1998.

[10] N. Koblitz, "Elliptic curve cryptosystems", *Mathematics of Computation*, vol. 48, pp. 203-209, 1987.

[11] W. J. Caelli, Ed Dawson, and S. Rea, "PKI, elliptic curve cryptography, and digital signatures", *Computers and Security*, vol. 18, no. 1, pp. 47-56, 1999.

[12] S. W. Changchien, M. S. Hwang and K. F. Hwang, "A batch verifying and detecting multiple RSA digital signatures", *International Journal of Computational and Numerical Analysis and Applications*, vol. 2, no. 3, pp. 303-307, 2002.

[13] M. S. Hwang, C. C. Lee and Y. C. Lai, "Traceability on RSA-based partially signature with low computation", *Applied Mathematics and Computation*, vol. 145, no. 2-3, pp. 465-468, 2003.

[14] M. S. Hwang, C. C. Chang and K. F. Hwang, "An ElGamal-like cryptosystem for enciphering large messages", *IEEE Transactions on Knowledge and Data Engineering*, vol. 14, no. 2, pp. 445-446, 2002.

[15] T. S. Wu and C. L. Hsu, "Convertible authenticated encryption scheme", *The journal of Systems and Software*, vol. 39, no. 3, pp. 281-282, 2002.

[16] S. F. Tzeng and M. S. Hwang, "Digital signature with message recovery and its variants based on elliptic curve discrete logarithm problem", *Computer Standards and Interface*, vol. 26, no. 2, pp. 61-71, 2004.

[17] D. Nyang and J. Song, "Knowledge proof based versatile smart card verification protocol", *ACM SIGCOMM - Computer Communication Review*, vol. 30, no. 3, pp 39-44, 2000.

Table 3: Computational cost for different authenticated encryption schemes

Schemes	Computational Cost			
	Signature Generation Phase		Signature Verification Phase	
	Time Complexity	Estimated Time for implementation in ms	Time Complexity	Estimated Time for implementation in ms
Horster et al. [6]	$T_{exp} + T_{inv} + 2T_{mul} + T_h$	$\approx$ 9.330075	$2T_{exp} + T_h + 3T_{mul}$	$\approx$10.377142
Wu-Hus [15]	$3T_h + T_{inv} + 2T_{mul} + 2T_{exp}$	$\approx$ 14.497337	$3T_h + T_{inv} + 3T_{exp}$	$\approx$ 13.581283
Tzeng-Hwang [16]	$T_{ECmul} + T_{mul} + T_h$	$\approx$ 47.351686	$2T_{ECmul} + T_{ECadd} + T_h$	$\approx$ 90.297844
Nyang et al. [17]	$2T_{exp} + T_{mul} + T_h$	$\approx$ 7.321278	$2T_{exp} + T_{mul} + T_h$	$\approx$7.321278
Chen et al. [18]	$2T_{ECmul} + T_{ECadd} + T_{mul} + T_h$	$\approx$ 91.825776	$3T_{ECmul} + 2T_{ECadd} + T_h$	$\approx$134.771934
Hsu-Wu [9]	$3T_{exp} + T_{mul}$	$\approx$ 7.947362	$3T_{exp} + (2t+1)T_{mul} + (t-1)T_{inv}$	$\approx$ 12.474339
Wu-Lin [22]	$5T_h + 2T_{inv} + 3T_{mul} + T_{ECadd} + 4T_{ECmul}$	$\approx$ 194.79795	$5T_h + T_{mul} + 2T_{ECadd} + 5T_{ECmul}$	$\approx$ 230.974826
Proposed Scheme	$T_{ECmul} + T_{mul} + T_h + T_{KV}$	$\approx$ 48.658936	$T_{ECmul} + T_{ECadd} + T_h + T_{inKV}$	$\approx$ 47.356199

[18] T. S. Chen, G. S. Huang, T. P. Liu, and Y. F. Chung, "Digital signature scheme resulted from identification protocol for elliptic curve cryptosystem", *Proceedings of IEEE TENCON'02*, pp. 192-195, 2002.

[19] Q. Dang, "Randomized hashing digital signatures", *Special Publication 800-106, National Institute of Standards and Technology*, July 2007.

[20] D. R. L. Brown, "A conditional security analysis of the elliptic curve digital signature algorithm", *The 5th Workshop on Elliptic Curve Cryptography (ECC 2001)*, Oct. 2001.

[21] P. Q. Nguyen and I. E. Shparlinksi, "The insecurity of the elliptic curve digital signature algorithm with partially known nonces", *Designs, Codes and Cryptography*, vol. 30, pp. 201-217, 2003.

[22] T. S. Wu and H. Y. Lin, "ECC based convertible authenticated encryption scheme using self-certified public key systems", *International Journal of Algebra*, vol. 2, no. 3, pp. 109-117, 2008.

[23] R. Rajaram, M. A. Prabakar, M. I. Devi, and M. Suguna, "Knapsack based ECC encryption and decryption", *International Journal of Network Security*, vol. 9, no.3, pp. 218-226, Nov. 2009.

R. Rajaram Ramasamy Dean of CSE/IT, Thiagarajar College of Engineering, has BE degree in Electrical and Electronics Engineering from Madras University in 1966. He secured the M Tech degree in Electrical Power Systems Engineering in 1971 from IIT Kharagpur, and the Ph.D. degree on Energy Optimization from Madurai Kamaraj University in 1979. He and his research scholars have published/presented more that 45 research papers in Journals and Conferences. Eight of his scholar secured the Ph.D. degree in computer science and communications areas. Two have submitted thesis and awaiting their results. Six are currently pursuing their Ph.D. research in Anna University with his guidance. His current areas of interest are Mobile Agents, Cryptography and Data Mining. He has published more than 13 text books on Computer languages and Basic Communications. He attended the International Seminar on Solar Energy at University of Waterloo, Canada during 1978. He has served the Makerere University at Uganda during 1977-1978 and University of Mosul during 1980-1981. He secured two best technical paper awards from the Institution of Engineers India and one from Indian Society for Technical Education. He has travelled to Malaysia, London, Paris, Belgium New York, Toronto, Nairobi.

M. Amutha Prabakar received the B. E. degree in Computer Science and Engineering, in 2003; the M. E. in Computer Science and Engineering, in 2005. He had worked as a lecturer in the department of Computer Science and Engineering, R. V. S. College of Engineering and Technology, India from 2004-2007. Now he is doing his Research in the area of cryptography and security under anna university - coimbatore. He worked as a Research Associate in Smart and Secure Environment Lab under IIT, Madras. Now he is working as a lecturer in department of Information Technology, Thiagarajar College of Engineering, Madurai. His current research interests include Cryptography and Security.