BLIND SIGNATURE SCHEME BASED ON CHEBYSHEV POLYNOMIALS

Maheswara Rao Valluri

Department of Information Technology, Salalah College of Technology

P.O.Box No:608, PC 211, Salalah, Sultanate of Oman

v.rao@sct.edu.om

ABSTRACT

A blind signature scheme is a cryptographic protocol to obtain a valid signature for a message from a signer such that signer's view of the protocol can't be linked to the resulting message signature pair. This paper presents blind signature scheme using Chebyshev polynomials. The security of the given scheme depends upon the intractability of the integer factorization problem and discrete logarithms of Chebyshev polynomials.

KEYWORDS

Blind signature, Chebyshev Polynomials, Digital signature, RSA, &Security

1. INTRODUCTION

The concept of blind signature was introduced by David Chaum in 1982 [2,3]. A blind signature scheme facilitates to ensure that the user's private information would not be revealed when he/she proceeds with casting or purchasing over the internet. According to Chaum who offered the concept, two parties, namely a group of requesters and a signer, are the participants of a blind signature scheme. Suppose one of the requesters asks for a blind signature from the signer, first the requester blinds a message using the blind factor and then sends the blinded message to the signer. After receiving the blinded message, the signer signs it using his/her private key and then sends the blinded signature back to the requester. Afterwards, the requester can extract the signature signed by signer by eliminating the blinding factor from the blinded signature. To verify successfully the legitimacy of the signature; one can utilize the signer's public key. The typical applications of blind signatures include e-cash, where a bank signs coins withdrawn by users, and e-voting, where an authority signs public keys that voters later use to cast their votes. Another application of blind signature scheme is anonymous credentials, where the issuing authority blindly signs a key [9, 18]. Recently, Microsoft introduced a new technology called U-prove to overcome the long standing dilemma between identity assurance and privacy which uses as a central building block blind signatures [22, 25].

The blind signature scheme is supposed to satisfy the following requirements: [3, 8, 10]:

Correctness: the correctness of the signature of a message signed through the signature scheme can be checked by anyone using signer's public key.

Blindness: the content of the message should be blind to the signature; the signer of the blind signature could not see the content of the message.

Unforgeability: only the signer can give a valid signature for the associated message.

DOI : 10.5121/ijnsa.2011.3613

Untraceability: the signer of the blind signature is unable to link the message-signature pair even when the signature has been revealed to the public.

There are many blind signature schemes have been proposed. Recently, many researchers proposed a variety of blind signature schemes [19, 20, 21]. The most widely used blind signature schemes are: RSA blind signature schemes [2], ElGamal signature scheme [5], and Schnorr Blind signature scheme [6]. RSA blind signature scheme security is based on the problem of integer factorization, while ElGamal and Schnorr blind signature schemes are based on the problem of discrete logarithm.

As Chebyshev polynomials have semi-group property in real field, a public key cryptosystem was proposed [11], on the assumption that the computation of Chebyshev polynomial in real field is a one-way function. But it was soon found the private key could be quickly recovered from the public key, using trigonometric function substitution [14, 16]. In other words, the one-way condition is not satisfied in such cryptosystem. To resist this attack, some references recommended [24, 27].

In this paper, we propose a blind signature scheme based on Chebyshev polynomials. Our scheme can meet the above requirements namely, correctness, blindness, unforgeability and untraceability. The security of the given scheme depends upon the intractability of the integer factorization problem and discrete logarithms of Chebyshev polynomials. The proposed scheme utilizes fewer numbers of bits due to inherent property of Chebysev polynomials as compared to its blind signature scheme such as RSA blind signature scheme.

The outline of this paper as follows: In section 2, the basic concept of Chebyshev polynomials and properties have been studied. In section3, the blind signature scheme has been proposed and also an example has been given. In section 4, the proposed scheme, security issues have been discussed. Finally, section 5 describes concluding remarks.

2. CHEBYSHEV POLYNOMIALS

In this section we briefly describe Chebyshev polynomials, since they represent the cornerstone on which the public key cryptosystem, described in [11, 15], key agreement protocols, described in [23] and the authentication scheme, described in [14], are built.

Definition: Let n be an integer, and let x be a variable taking value over the interval [-1, 1]. The polynomial $T_n(x):[-1,1]\rightarrow[-1,1]$ is recursively defined as

$$T_n(x)=2.x.T_{n-1}(x)-T_{n-2}(x),\ \text{for any } n\geq 2\ \text{, where } T_0(x)=1 \text{ and } T_1(x)=x\ .$$

Some examples of Chebyshev polynomials are

$$T_2(x)=2.x^2-1$$

$$T_3(x)=4.x^3-3.x$$

$$T_4(x)=8.x^4-8.x^2+1$$

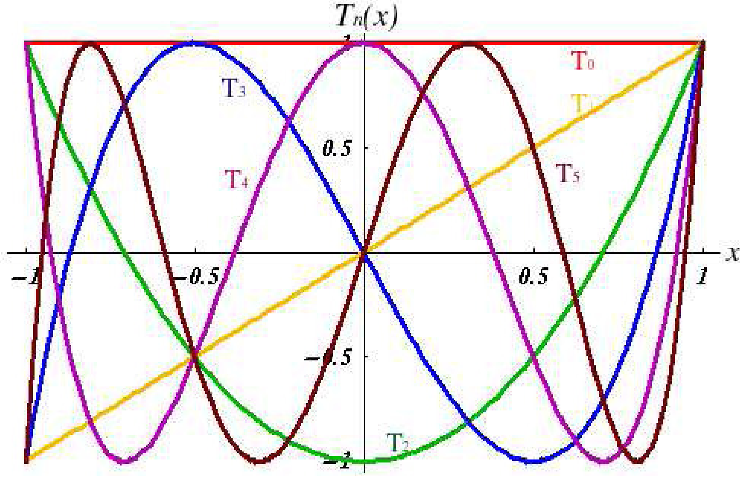

Figure 1: Graphical representation of Chebyshev polynomials:

One of the most important properties of Chebyshev polynomials is so called semi-group property which establishes that

$$T_m(T_n(x)) = T_{m.n}(x)$$

As immediate consequence of this property is that Chebyshev polynomials commute under composition

$$T_m(T_n(x)) = T_n(T_m(x)).$$

It is seen that this holds by using the classical formula [4], $T_n(x) = \cos(n\cos^{-1}(x))$ which is valid for all real 'x' in the interval [-1, 1]. Using this formula we have

$$T_m(T_n(x)) = \cos(m\cos^{-1}(\cos(n\cos^{-1}(x)))$$

$$= \cos(mn\cos^{-1}(x))$$

$$= \cos(nm\cos^{-1}(x))$$

$$= \cos(n\cos^{-1}(\cos(m\cos^{-1}(x)))$$

$$= T_n(T_m(x))$$

For $x > 1$ we can use the formula $T_n(x) = \cosh(n\cosh^{-1}(x))$ to verify the identity. Up to linear transformation the pure monomial x^n and the Chebyshev polynomial are the only classes of the polynomials that satisfy the commutative composition relation $P_n(P_m(x)) = P_m(P_n(x))$ with $P_n(x)$ a polynomial of degree n.

2.1. Binary powering for Chebyshev polynomials

We seek to generalize the binary powering algorithm, so that we can quickly compute values of the Chebyshev polynomial modulo p. We first rewrite the recurrence for Chebyshev polynomials $T_n(x) = 2.x.T_{n-1}(x) - T_{n-2}(x),$ from [1] formula 22.7.4, page 782, as a matrix equation:

$$\begin{pmatrix} T_n(x) \\ T_{n+1}(x) \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 2x \end{pmatrix} \begin{pmatrix} T_{n-1}(x) \\ T_n(x) \end{pmatrix}$$

The equation with n diminished by 1 becomes:

$$\begin{pmatrix} T_{n-1}(x) \\ T_n(x) \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 2x \end{pmatrix} \begin{pmatrix} T_{n-2}(x) \\ T_{n-1}(x) \end{pmatrix}$$

Combining the above equations yields

$$\begin{pmatrix} T_n(x) \\ T_{n+1}(x) \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 2x \end{pmatrix}^2 \begin{pmatrix} T_{n-2}(x) \\ T_{n-1}(x) \end{pmatrix}$$

We continue to replace the vector on the right side until the index is 0, yielding

$$\begin{pmatrix} T_n(x) \\ T_{n+1}(x) \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 2x \end{pmatrix}^n \begin{pmatrix} T_0(x) \\ T_1(x) \end{pmatrix}$$

As $T_0(x) = 1$ and $T_1(x) = x$, the vector on the right is just the transpose of the row vector $(1, x)$. Hence we compute the above using matrix binary powering, perform one matrix-vector product, and then extract the first element of the resulting vector to obtain $T_n(x)$. Using the classical matrix-matrix multiplication algorithm, we can do one matrix multiplication with individual elements reduced modulo p using 8 integer multiplications, 4 integer additions, and 4 integer remainder operations. As the exponent $n < p$ we use $O(\log(p))$ matrix multiplications modulo p to compute the value of the degree n Chebyshev polynomial modulo p. This calculation has been resulted that the computation would take about 4 to 8 times more C.P.U. time than the conventional Diffie-Hellman algorithm, depending on the cost of a large integer division relative to a large integer multiplication [12].

2.2. Properties of Chebyshev polynomial sequences modulo a prime

To investigate the difficulty of inverting $a = T_n(x)(\bmod p)$, with n unknown, we generate some experimental data. Choosing a small p, we can compute the sequence $T_n(a)(\bmod p)$ for n = 0, 1, 2, until we discover the period of the sequence. The result is that the period is at most p + 1 for any given input argument x = 0, 1, 2, ..., p − 1. For example , when x = 3, and p = 11, the sequence $T_n(3)$(mod11) for n = 0,1,2,3…………23 is: 1,3,6,0,5,8,10,8,5,0,6,3,1,3,6,0,5,8,10,8,5,0,6,3 which is period of 12.

Theorem 2.2.1.: Let p be an odd prime and $x \in Z$ such that $0 \le x < p$. Let k be the period of the sequence $T_n(x)(\bmod p)$ for n = 0, 1, 2, ... Let $\lambda^2 - 2x\lambda + 1$ have roots $\lambda = \alpha_1, \alpha_2$ .Then (i) k|p − 1 if the roots are in GF(p), otherwise, (ii) k|p + 1 when the roots are in GF(p2).

Proof: In [12], it has shown that one can compute $T_n(x)(\bmod p)$ by computing the n^th power of the recurrence relation matrix which has characteristic polynomial $f(\lambda) = \lambda^2 - 2x\lambda + 1$, performing one matrix-vector product modulo p, and then selecting the first element in the resulting vector. The determinant of this matrix is also equal to the co-efficient of λ^0 of $f(\lambda)$, which is 1; thus the matrix is non-singular. As the 0th power of the matrix is the identity matrix, the period k is the smallest positive integer such that the kth power of the matrix is the identity matrix. We can compute powers of a matrix by finding its Jordan canonical form, computing powers of the Jordan canonical form, then transforming back. Recall that the Jordan canonical form is either a diagonal matrix with distinct eigenvalues on the diagonal, or an upper triangular matrix with repeated eigenvalues on the diagonal; these eigenvalues are also roots of the characteristic polynomial. In the case of the characteristic polynomial has repeated roots, they both must be $\pm \bmod p$ because the only least-residue solutions of $y^2 - 1 = 0(\bmod p)$ are $y = \pm 1$. In the case that 1 is a double root, x = 1and our sequence is 1, 1, 1, ------ which has period 1. In the other case, the repeated root is -1 with x = -1; our sequence is 1, p - 1, 1, p - 1, ----- which has period 2 and is a divisor of p - 1 , as p is odd. We consider the that the distinct roots lie in GF(p) . From Fermat's theorem, $a^{p-1} = 1(\bmod p)$ for any non-zero $a < p$. The (p - 1)st power of the Jordan canonical form matrix is the identity matrix, so our sequence has period at most p - 1. If a small exponent $k < p-1$ exists such that kth power of our Jordan canonical form matrix is the identity, k must be a divisor of p - 1, because, by Lagrange's theorem for the order of a subgroups of a finite group, the period must be a divisor of p - 1. The other case is that the roots exists only in a Quadratic extension of GF(p). We can still diagonalize our matrix as long as we do our arithmetic in that quadratic extension field. First we raise our diagonal Jordan canonical form matrix to power p; such raising a number to the power p is an automorphism in the quadratic extension fields. Hence the two roots just swap position on the diagonal, as we have only one non-identity automorphism in a quadratic extension field. Then we multiply our original Jordan canonical –form matrix to complete the calculation of the (p + 1)st power .This just multiplies two pairs of conjugate roots. As the product of the conjugate roots is also co-efficient of λ^0 in the characteristic polynomial, which is 1. The (p + 1)st power is the identity matrix. Thus the period is at most (p + 1). Again by Lagrange's theorem, the period must be a divisor of (p + 1).

We recommend choosing p to be a safe prime, and check that (p+1) had large prime factor or that it is hard to factor.

2.3. The discrete log problem for Chebyshev polynomials

To make the protocol practical we require an efficient algorithm for computing $T_n(x)(\bmod p)$ for the n and p large. We call this as Chebyshev discrete log problem. We map the Chebyshev discrete log problem onto the conventional discrete log problem by recalling the hyperbolic definition of Chebyshev polynomials and solving it for n. We have the following theorem.

Theorem 2.3.1 : Let a and x be integers and p is a prime. If $a = T_m(x) \bmod p$ then m is one of the values $\log_{x+\sqrt{x^2-1}}(a+\sqrt{a^2-1})$ in which the square roots lie in the quadratic extension field $GF(P^2)$ and the logarithm is the discrete log in the field $GF(P)$ or its quadratic extension field.

Proof: $a = T_n(x) = \cosh(n\cosh^{-1}(x))$ so $n = \dfrac{\cosh^{-1}(a)}{\cosh^{-1}(x)}$. We convert this to logarithms to find $n = \dfrac{\log(a+\sqrt{a^2-1})}{\log(x+\sqrt{x^2-1})}$. Recalling the change of base formula, we write this as

$n = \log_{x+\sqrt{x^2-1}}(a+\sqrt{a^2-1})$. In the case that both the square roots $\sqrt{x^2-1}$ and $\sqrt{a^2-1}$ exists in $GF(P)$ we have a conventional discrete log problem; otherwise, at least one square root exists in the quadratic extension field $GF(P^2)$, which yields a quadratic extension fields generalization of the discrete log problem. To compute a square root in $GF(P)$ or in $GF(P^2)$ we can use $O(\log^3 p)$ the probabilistic polynomial time method of Rabin, described in [7] .

3. BLIND SIGNATURE SCHEME

3.1. Blind signature Scheme by David Chaums

Recall the Chum's blind signature scheme [2], based on RSA cryptographic algorithm. RSA based blind signature scheme is divided into five phases: initializing, blinding, signing, unblinding, and verifying. The signer first publishes the public information in the initializing phase. In the blinding phase, the requester blinds the message and sends it to the signer for requesting the signature. Then the signer signs the blinded message in the signing phase. In the unblinding phase, the requester derives the signature from the blinded signature. Finally, anyone can verify the legitimacy of signature in the verifying phase. The details of this scheme are described as follows:

Initializing phase:

The signer randomly chooses two large primes p and q, and computes $M = pq$ and $L = (p-1)(q-1)$. The signer chooses two large numbers e and d such that $0 < e < M$ and $d = \frac{1}{e}(\bmod L)$. Let (e, M) be the signer's public key and d be the signer's private key. The signer keeps (p, q, d) secure and publishes (e, M) and a one way hash function h(.) such as SHA-1 or MD5.

Blinding phase:

The requester has a message m , and he/she whishes to have it signed by the signer. The requester randomly selects an integer k such that $0 < k < M$ as the blinding factor. The requester computes and submits the number $m^* = h(m).k^e$ to the signer.

Signing phase:

After receiving m^* from the requester, the signer computes and sends back the number $s^* = m^{*d}$ to the requester.

Unblinding phase:

After receiving s^* from the signer , the requester computes $s = k^{-1}.s^*$

Verifying phase:

The s is a signature on the message m. The other users can verify the legitimacy of the signature by checking whether s^e=h(m) or $s = h(m)^d$.

3.2. Blind signature scheme based on Chebyshev polynomials

In this subsection, we propose blind signature scheme based on Chebyshev polynomials. We modify the above algorithm to use the first kind of Chebyshev polynomials $T_n(x)$ instead of monomials x^n, as follows:

Initializing phase:

The signer randomly chooses two large primes p and q, and computes $M = pq$ and $L = (p^2 - 1)(q^2 - 1)$. The signer chooses two large numbers e and d such that $0 < e < M$ and $d = \frac{1}{e} (\bmod L)$. Let (e, M) be the signer's public key and d be the signer's private key. The signer keeps (p, q, d) secure and publishes (e, M) and a one way hash function h(.) such as SHA-1 or MD5.

Blinding phase:

The requester has a message m , and he/she whishes to have it signed by the signer. The requester randomly selects an integer k such that $0 \le k \le M$ as the blinding factor. The requester computes and submits the number $m^* = h(m).T_e(k)(\bmod M)$ to the signer.

Signing phase:

After receiving m^* from the requester, the signer computes and sends back the number $s^* = T_d(m^*)(\bmod M)$ to the requester.

Unblinding phase:

After receiving s^* from the signer , the requester computes $s = \frac{s^*}{k} (\bmod M)$.

Verifying phase:

The s is a signature on the message m. The other users can verify the legitimacy of the signature by checking whether $s = T_d(m)(\bmod M)$ or $h(m) = T_e(s)(\bmod M)$.

3.3. Example for Proposed Blind signature scheme:

We now present an example with artificially small parameters by taking a bank example.

Initially Bank should do the following:

- Chooses two large primes p = 5 and q = 17 which are kept secret
- Computes the public modulus $M = 85$
- Chooses a random encryption degree e = 31
- Computes the secret modulus $L = 6912$
- Using the extended Euclidean algorithm, computes a secret decryption degree $d = 223$
- Sends to customer(requester) M and e

After receiving the above value Customer should request for the signature by computing the values as follows:

- Customer selects a random value $k = 547$
- Hashed message m=259
- Computes the blind message as $m^* = 259.T_{31}(547)(\bmod 85) = 259.37(\bmod 85) = 63$
- Sends blind message m^* to Bank for signature.

Bank should do the following:

- Receives blind message from customer and treats it as an ordinary message since the bank does not recognize the blinding. The bank computes

  $s^* = T_{223}(63)(\bmod 85) = 83$
- After computing the blind signature s^*, bank sends it to the customer as signature.

Customer should do the following to recover real signature S after receiving the blind signature s^* from the Bank.

- Computes $s = \frac{83}{547}(\bmod 85) = 4$
- Now the signature message pair is : $(s, m) = (4, 259)$
- Sends signature pair (s, m) to verifier

Verifier should do the following:

- Receives signature pair (s, m) from the customer.
- Sends signature pair (s, m) to bank.
- Bank accepts signature if (Customer signature) $S = T_{223}(259)(\bmod 85) = 4$

4. SECURITY ANALYSIS OF BLIND SIGNATURE SCHEME BASED ON CHEBYSHEV POLYNOMIALS

In this section, we examine the correctness, blindness, unforgeability and untraceability of the proposed scheme.

4.1 Correctness:

In the unblinding phase of our proposed scheme, the requester can derive the signature by computing

$$s = \frac{s^*}{k} = \frac{T_d(m^*)(\bmod M)}{k}$$

$$= \frac{T_d((h(m).T_e(k)(\bmod M))(\bmod M)}{k}$$

$$= \frac{T_d(h(m))(\bmod M)(T_d(T_e(k)(\bmod M))(\bmod M)}{k}$$

$$= \frac{T_d(h(m))(\bmod M)(T_{de}(k)(\bmod M))}{k}$$

$$= \frac{T_d(h(m))(\bmod M)(T_{k(p^2-1)(q^2-1)+1}(k)(\bmod M))}{k}$$

$$= \frac{T_d(h(m))(\bmod M)(T_1(k)(\bmod M))}{k}$$

$$= \frac{T_d(h(m))(\bmod M).k}{k}$$

$$= T_d(h(m))(\bmod M)$$

The requester computes $s = T_d(h(m))(\bmod M)$, so that $h(m) = T_e(s)(\bmod M)$.

4.2. Blindness:

Blindness is an important property in a blind signature. It is that the signer can sign a document without knowing what the document contains. In the proposed blind signature scheme,the requester picks a blinding factor k to compute the blind message $\alpha = h(m).T_e(k)(\bmod M)$ .Thus, the signer could not know the message m.

4.3. Unforgeability:

The security of our scheme is based on the difficulty of solving the factoring problem and discrete logarithmic problem of Chebyshev polynomials. It is hard to find a valid signature s on any message m to pass the verification $h(m) = T_e(s)(\bmod M)$.

4.4. Untraceability:

The security of our scheme is based on the difficulty of solving the factoring problem and discrete logarithmic problem of Chebyshev polynomials. No one can forge a valid signature pair s on message m to pass the verification $h(m) = T_e(s)(\bmod M)$.

5. CONCLUSIONS

This paper suggests a secure and efficient blind signature scheme based on Chebysev polynomials. First the properties of Chebyshev polynomial are discussed. Based on these properties blind signature scheme is introduced. This signature can be broken easily if the security parameters are not selected properly. To ensure the cryptosystem secure, few principles for parameter selection have been proposed . In the RSA based blind signature scheme, the security depends on intractability of large integer factorization problem, while the ElGmal blind signature and Schnorr blind signature based on intractability of discrete logarithmic problem. In the proposed blind signature, the security depends upon both the intractability of the integer factorization and discrete logarithms of Chebyshev polynomials. The proposed scheme utilizes fewer numbers of bits due to inherent property of Chebysev polynomials as compared to its blind signature scheme counterpart such as RSA blind signature scheme. The proposed blind signature scheme is suitably illustrated using a bank example.

ACKNOWLEDGEMENTS

Author would like to thank to the reviewers and the editors for their valuable suggestions which helped me lot to improve the article for the publication.

REFERENCES

[1] Abramowitz, M. & Stegun, A., (1965) "Handbook of Mathematical Functions", Dover publications, New York, 1965.

[2] Chaum, D., (1982) " Blind signatures for untraceable payments", *in Advances in cryptology*, CRYPTO'82,pp.199-203,1982.

[3] Chaum, D., (1983) "Blind signatures system", *in Advances in cryptology*, CRYPTO'83, pp:153-156,1983.

[4] Borowski,E.J &Borwein,J.M,(1991) "The Haper Collins Dictonary of Nathematics" *Harper Collins Publishers,* New York, 1991.

[5] Carmenisch,J.L., Piveteau,J.M. & Stadler,M.A., (1994) "Blind signature based on the discrete logarithm problem", EUROCRYPT '94, Perugia, Italy, 1994.

[6] David Pointcheval & Jaques Stern, (1996) "Provably Secure Blind Signature Schemes" , *Advances in Cryptology – Proceedings of ASIACRYPT '96, M. Y. Rhee and K. Kim Eds.Springer-Verla*g, LNCS 1163, pages 252-265, 1996.

[7] Randall K.Nichols, (1999) "ICSA guide to Cryptography", *McGraw-Hill*, New York, 1999.

[8] Chu-I Fan, Chen,W.K. & Yeh,Y.S., (2000) "Randomization enhanced Chaum's blind signature scheme *Computer communications*, Vol 23, 2000, pp 1677-1680.

[9] Stefan A.Brands., (2000), " Rethinking Public Key Infrastructures and Digital Certificates : Building in Pravacy":*.MIT Press, Cambridge,* MA, USA,2000.

[10] Zuhua Shao,(2000) "Improved user efficient blind signatures", *Electronics Letters*, Vol.36, no.16, pp.1372-1374, 2000.

[11] Kocarev.L. & Tasev.Z, (2003) "Public –Key Encryption Based on Chebyshev Maps", *Proceedings of the IEEE symposium on Circuits and Systems*, Vol 3, pp.28-31, 2003.

[12] Fee,G.J.,&Monagan,M.B., (2004) "Crytography using Chebyshev polynomials,

http://oldweb.cecm.sfu.ca/CAG/papers/cheb.pdf,pp: 1-15,2004.

[13] Xiao,D., Liao,X., Tang,G. & Chuandong,Li., (2004) " Using Chebyshev Chaotic Map to Construct Infinite Length Hash Chains" *(ISCAS 2004)*, Vol 1, PP ,11-12.

[14] Bergamo,P.,Arco,P.D.,De Santis,A. & Kocarev,L., (2005) "Security of public-key cryptosystems based on chebyshev polynomials," *Circuits and Systems I: Regular Papers, IEEE Transactions on*, vol. 52, no. 7, pp. 1382 – 1393,2005.

[15] Kocarev,L., Makraduli,J & Amato,P., (2005) "Public-Key Encryption Based on Chebyshev polynomials ", *Circuits, Systems and Signal Processing,*vol. 24, no. 5, pp. 497-517, 2005.

[16] Cheong,K. & Koshiba,T., (2007) "More on security of publickey cryptosystems based on chebyshev polynomials," *Circuits and Systems II: Express Briefs, IEEE Transactionson*, vol. 54, no. 9, pp. 795 –799, 2007.

[17] Lima, J.B. , Campello de Souza, R.M. & Panario,D., (2008) "Security of Public-Key Cryptosytem Based Cryptosystems Based on Chebyshev Polynomials over Prime Finite Fields," *Proc. IEEE Int'l Symp. Information Theory,* pp. 1843-1847, 2008.

[18] Jan Camenisch and Thomas GroB,(2008) "Efficentt attributes for anonymous credentials" *In Peng Ning, Paul F. Syverson, and Somesh Jha, editors, ACM CCS 08: 15th Conference on Computer and Communications Security, Alexandria, Virginia, USA, October 27-31, pp: 345-356, 2008.*

[19] Verma,G.K., (2008) " Blind signature schems over Braid groups" http://eprint.iacr.org/2008/027.

[20] Markus Ruckert, (2008) " Lattice-based Blind signatures", http://eprint.iacr.org/2008/322.

[21] Fuh-Gwo Jeng, Tzen-Long Chem, & Tzer-Shyong Chen, (2010) "An ECC-Based Blind Signature Scheme", *Journal of Networks,* Vol 5, No 8, 2010.

[22] Ronny Bjones, (2010) " *U-prove technology overview".* http://www.itforum.dk/downloads/Ronny_Bjones_Uprove.pdf, October 2010.

[23] Ke Qin, Mingtian Zhon, &Young Feng(2010) , "A novel multicast key exchange algorithm based on exteneded Chebyshev map, Complex,Intelligent and software intensive systems "*(CISIS), 2010, International Conference on* ,pages 643-649,2010.

[24] J.B.Lima, D.Panario, R.M. Campello de Souza, (2010) " Public –key encryption based on Chebyshev polynomials over GF(q)," *Information Processing Letters*, Volume III, Issue 2, Page 51-56,2010.

[25] Microsoft (2011), MICROSOFT U-PROVE. Microsoft u-prove ctp release 2. http://connect.microsoft.com/site642/Downloads/DownloadDetails.aspx?DownloadID=26953, March 2011.

[27] Zhihui Li, Yidong Cui, Yuehui Jin,& Huimin Xu, (2011) "Parameter Selection in Public Key Cryptosystem based on Chebyshev Polynomials over Finite Field", JOURNAL OF COMMUNICATIONS, VOL. 6, NO. 5, AUGUST 2011.

Authors:

Dr.Maheswara Rao Valluri received the M.Sc., M.Phil., Ph.D (Mathematics) from Sri Krishnadevaraya University, Anantapur, A.P., India. Currently he is working as a Faculty, Department of Information Technology, Salalah College of Technology, Salalah, Sultanate of Oman. His field of interest includes Cryptography, and Non-Associative Algebra. He has published 7 research papers and presented 8 papers in National and International conferences. Also, he is life member in Cryptology Research Society of India (CRSI), Indian Mathematical Society (IMS), Andhra Pradesh Society of Mathematical Sciences (APSMS), and Ramanujan Mathematical Society (RMS), India.