Journal of Applied Mathematics & Bioinformatics, vol.3, no.1, 2013, 1-15
ISSN: 1792-6602 (print), 1792-6939 (online)
Scienpress Ltd, 2013

On the Cryptographic Long Term Security

Dimitrios Poulakis[1]

Abstract

In this note we deal with the problem of long-term cryptographic security. We discuss briefly the methods of multiple encryption and signature, and the future influence of Quantum, DNA and Chaos methods in cryptography. Moreover, we propose an encryption and a signature scheme based on the problems of integer factorization and discrete logarithm suitable for applications needing long-term security.

Mathematics Subject Classification: 94A60
Keywords: Long-Term Security; Public-Key Cryptography; Symmetric Encryption; Multiple Encryption; Multiple Signature; Quantum Cryptography; DNA Cryptography; Chaos Cryptography

[1] Aristotle University of Thessaloniki, Department of Mathematics, Thessaloniki 54124, Greece, e-mail: poulakis@math.autj.gr

Article Info: *Received* : November 1, 2012. *Revised* : January 30, 2013
Published online : March 30, 2013

1 Introduction

Cryptography serves as the foundation for most IT security solutions. It has been used to verify the authenticity of updates for computer operating systems, such as Windows XP, to protect financial transactions and other Web-based applications, to protect the privacy and authenticity of health cards, etc.

Many applications of the IT need long term cryptographic security. Some examples are digital signatures for contracts, encryption of sensitive medical data (for instance, according to German laws authentic medical data must remain accessible for at least 30 years) and encryption in archival storage systems (in such systems data lifetimes are measured in decades).

Today's cryptography provides strong tools only for short term security. Cryptographic primitives that we currently use for encryption, as RSA, ECC and AES, are adequate to achieve short term security (5, 10 or 15 years). Similarly, digital signatures that we use today as RSA, DSA, ECDSA, etc do not guarantee the desired long-term security.

In this short note we discuss briefly the problem of long term cryptographic security and we propose two cryptographic schemes which can be used for the fulfillment of this task. The paper is organized as follows. We recall the methods of multiple encryption and signature we use today for enhancing the security in Section 2. In Section 3 we deal with the methods of non-conventional cryptography. In Section 4 and 5 we describe an encryption and a signature scheme based on the problems of integer factorization and discrete logarithm in such way that if any of these problems is broken, the others will still be valid and hence the scheme will be protected, and so are adequate for applications which need long-term cryptographic security.

2 Multiple Encryption and Signatures

A practical partial solution to this problem of the long term confidentiality can be provided by Multiple Encryption, which encrypts a message several times with different keys or algorithms. The idea was first seen in "product cipher" and in "cascade cipher" [46]. Recall that the distinction between these two types of multiple encryption is that the keys of the component cipher of

the first need not be statistically independent, whereas they are in the second. Multiple encryptions has been applied to many communication systems in order to enhance security; they are basic components for designing other cryptographic applications as broadcast encryption, threshold encryption, MIX-net etc.

If the encryption algorithms are different with independent keys, then the resulting cipher is at least as difficult to break as the first encryption algorithm [34]. The security of multiple symmetric encryptions has be discussed in several papers (see for instance [38]). Security definitions and generic constructions for multiple encryption schemes based on asymmetric key encryptions are proposed recently in [49, 14, 18]. Although the multiple encryption is used to enhance security, there is no proof that the time needed to break a such system is longer than the time needed to break the stronger component encryption scheme.

In order to achieve the goal of long-term security for the signatures, Maseberg [33] suggested the use of more than one sufficiently independent signature schemes. Thus, if one of them is broken, then it can be replaced by a new secure one. Afterward the document has to be re-signed. Maseberg has proposed protocols that support multiple signatures including the update management in the case of a break. Thus, every message has at least two signatures which take more space and has to be re-signed with a new system in the case of a break.

The above idea of efficient replacement of insecure primitives by secure ones has adoptet by Buchmann, May and Volmer [11] who have designed and implemented the open source crypto library Flexi-Provider [17] that support the Java Cryptographic Architecture and implements current and alternative cryptography.

3 Quantum, DNA and Chaos

In this section we discuss the influence of Quantum, DNA and Chaos based techniques to the contemporary cryptography.

Quantum Computing. In 1994, Shor [47] proposed polynomial quantum

algorithms for integer factorization and the computation of discrete logarithms. So, in case of the construction of efficient quantum computers all widely used public-key cryptography will be insecure.

In 1997, Bennet, Bernstein, Brassard and Vazirani proved that quantum computers cannot provide an exponential speedup of search algorithms, and so current symmetric encryption and hash functions will be resistant to attacks based on quantum computing [5]. Thus, in the presence of large scale quantum computers we have to examine alternatives to the currently used public key cryptographic primitives.

The following public-key cryptographic primitives are believed to be resistant to quantum computing based attacks [6, 13]:

1. The NTRU family of cryptographic schemes [22, 23, 24] whose security is relied on two NP-hard problems related to lattices: The shortest vector problem and the closest vector problem. In moderate large dimensions the two problems are far from being feasible in both the quantum and classical computation models.

2. The McEliece encryption scheme [36, 16] whose security is relied on the decoding problem for certain classes of error-correcting codes which in large dimensions is infeasible and there is no quantum algorithm that enhance the speed of classical algorithms.

3. Merkle's hash-tree public-key signature scheme, building upon a one-message-signature of Lamport and Diffie [38].

4. Multivariate-quadratic-equations schemes whose security is relied on the difficulty of solving systems of multivariate quadratic equations over finite fields [40]. The solution of a such system requires the computation of its Gröbner basis. Actually, there is no quantum algorithm that improve significantly the performance of classical ones.

On the other hand, QC provides primitives for key agreements whose security relies on the laws of quantum mechanics and information theory and not on the difficulty of certain computational problems. Such primitives are the protocols BB84 [4] and E91 [15]. Actually, quantum computing is not yet sufficiently efficient and many basic cryptographic primitives cannot be realized.

DNA Computing. DNA cryptography uses DNA as the computational tool exploiting the extreme complexity and randomness in the DNA structure for coding and decoding. DNA computing has a high level computational ability and is capable of storing huge amounts of data.

Several encryption schemes have been proposed based on DNA computing; more precisely there are some propositions for encryption schemes based on DNA binary strands [31], the technology of DNA synthesis, PCR amplification and DNA digital coding [12], etc.

Classical algorithms as One-Time-Pad, IDEA, RSA, etc has been connected with DNA computing techniques [20, 45, 26]. On the other hand, a number of proposals have been submitted for breaking conventional cryptosystems by DNA computing, as DES, RSA, NTRU, IDEA and ECC (over the finite fields $GF(2^n)$) [8, 3, 50, 21, 32].

The main problems of the present DNA computing is the lack of the related theoretical basis, the difficulty of realization and the cost of application. Thus, it is not able to construct real intimidation to the security of the current cryptography or to apply in practice the proposed cryptographic schemes based on it.

Chaos. Chaos theory is the mathematical study of nonlinear dynamical systems. It has many potential applications in a digital communication system: compression, encryption and modulation. Chaotic encryption makes use of chaotic systems which are known to be very sensitive to initial conditions and have very random behavior. In the last two decades many chaos-based encryption methods have been proposed (for instance, see [25, 29, 30, 44, 39]). In general they are two approaches in the use of chaotic systems in cryptography. The first one is the generation of pseudo-random sequences while the second is the used of plaintext as initial state and the cipher text follows from the orbit being generated. These two approaches correspond to stream and block ciphers, respectively. A review of attacks on chaos-based ciphers and recommendations about security in given in [1]. Chaos-based schemes have also being proposed for hashing, key-exchange protocols, etc.

Security and performance of almost all proposed chaos-based methods are not analyzed in terms of the techniques developed in the conventional cryptography. Most of the proposed methods generate cryptographically weak and slower algorithms than the corresponding conventional ones. Since chaos-based

cryptographic algorithms use dynamical systems defined on the real numbers, they are difficult for practical realization and circuit implementation. For the above reasons, although, at theoretical level, it seems that chaotic systems are ideal candidates for cryptographic primitives, at the practical level, the impact that this research has made on cryptography is rather marginal. It seems that much work must be done in order chaos-based cryptography reaches the same standard of security and speed of conventional cryptography

4 An Encryption Scheme

In this section we describe briefly an encryption scheme proposed in [42] based on the integer factorization problem and the discrete logarithm problem. If any of these problems is broken, the other will still be valid and hence the encrypted message will be protected. Thus, this encryption scheme is suitable for applications requiring long term security.

Bases of $\mathbb{Z}_n^*$. Let n be an integer > 0. For every $x \in \mathbb{Z}$, we denote by $\mathrm{ord}_n(x)$ the order of $x \pmod n$ and by ϕ the Euler's totient function. Suppose that n is odd and $n = p_1^{a_1} \cdots p_k^{a_k}$ its prime factorization. Then there exist $g_1, \ldots, g_k \in \mathbb{Z}$ with $\mathrm{ord}_n(g_i) = \phi(p_i^{a_i})$ $(i = 1, \ldots, k)$ such that for every $x \in \mathbb{Z}$ with $\gcd(x, n) = 1$ there are uniquely determined $n_1, \ldots, n_k \in \mathbb{Z}$ with $0 \leq n_i < \phi(p_i^{a_i})$ satisfying $x \equiv g_1^{n_1} \cdots g_k^{n_k} \pmod n$. We call the set $\{g_1, \ldots, g_k\}$ a *basis* of $\mathbb{Z}_n^*$.

Public and private key generation. A user $\mathcal{A}$, who wants to create a public and a private key, selects two large primes p and q of almost equal length such that the factorization of $n = pq$ is infeasible and $\delta = \gcd(p-1, q-1)$ is quite large. He also finds a basis $g_p, g_q \in \{1, \ldots, n-1\}$ of $\mathbb{Z}_n^*$. Next, $\mathcal{A}$ selects $c_p \in \{0, \ldots, p-2\}$, $c_q \in \{0, \ldots, q-2\}$, $b \in \{0, \ldots, \phi(n)-1\}$ and computes $\gamma_p = g_p^{c_p} \bmod n$, $\gamma_q = g_q^{c_q} \bmod n$, $y_p = \gamma_p^b \bmod n$, $y_q = \gamma_q^b \bmod n$. Finally, he selects $e, d \in \{1, \ldots, \phi(n)-1\}$ such that $ed \equiv 1 \pmod{\phi(n)}$. (In [42] a typographic error has replaced $\phi(n)$ by n). The public key of $\mathcal{A}$ is $(n, e, \gamma_p, \gamma_q, y_p, y_q)$ and its private key (p, q, d, b).

Encryption. The plaintext space is the set P of integers x satisfying $1 \leq x \leq n-1$ and $\gcd(x, n) = 1$. Suppose that another user $\mathcal{B}$ wants to send a message $m \in P$ to $\mathcal{A}$ using his public key. He selects (secret) integers

$k \in \{1, \ldots, n-1\}$ with $\gcd(k, n) = 1$, $z_p, z_q \in \{0, \ldots, n-1\}$ and computes $B = k^e \bmod n$, $C = \gamma_p^{z_p}\gamma_q^{z_q} \bmod n$, and $D = y_p^{z_p} y_q^{z_q}(k+1)^e m \bmod n$. $\mathcal{B}$ sends to $\mathcal{A}$ the encrypted message (B, C, D).

Decryption. For the decryption of the message (B, C, D), $\mathcal{A}$ computes $k = B^d \bmod n$, $M = (k+1)^{-e} D \bmod n$, and $N = C^{-b} M \bmod n$. Since $N \equiv m \pmod n$ and $0 < m, N < n-1$, it follows $N = m$.

Security. The computation of the secret key from the private requires the factorization of n (provided that d is large enough) and the computation of b from $y_p = \gamma_p^b \bmod n$, $y_q = \gamma_q^b \bmod n$. An attacker who knows p, q but not b, and the encrypted message (B, C, D) is able to recover m if he can calculate z_p and z_q from C.

If there is an oracle O that given a public key $(n, e, \gamma_p, \gamma_q, y_p, y_q)$ for our cryptosystem and a ciphertext v, gives the corresponding plaintext u for v, then it can also break the DRSA [41] and ElGamal cryptosystems. Note that the DRSA Encryption Scheme, which is a version of the RSA, is semantically secure against chosen plaintext attacks and the semantic security of the ElGamal cryptosystem (with messages from a subgroup) is equivalent to the Decision Diffie-Helman problem [48, Theorems 1 and 2]. Finally, note that our scheme is more efficient from the trivial use of the two above schemes.

5 A Signature Scheme

In this section we present an signature scheme based on the integer factorization problem and the discrete logarithm problem for elliptic curves. If any of these problems is broken, the other will still be valid and hence the signature will be protected. In this case, the signature should be regenerated with a new system, without the chain of valid signatures being broken. So, this scheme is suitable for applications requiring long-term security and provides a more efficient solution than that in Section 2. For all details and proofs one can see [43].

Public and private key generation. A user $\mathcal{A}$, who wants to create a public and a private key selects two primes p_1, p_2 such that the factorization of $n = p_1 p_2$ is infeasible, an elliptic curve E over a finite field $\mathbb{F}_q$ with a point $P \in E(\mathbb{F}_q)$ having $\mathrm{ord}(P) = n$ and an efficiently computable pairing

e_n such that $e_n(P,P)$ is a primitive n-th root of 1. Furthermore, he selects $g \in \{1,\ldots,n-1\}$ with $\gcd(g,n)=1$ and $a,b \in \{1,\ldots,\phi(n)-1\}$, and computes $Q = g^a P$, $r = g^b \pmod n$ and $R = g^{a-ab}P$; Finally, he chooses two hash functions, $H : \{0,1\}^* \rightarrow < P >$, where $< P >$ is the subgroup of $E(\mathbb{F}_q)$ generated by P, and $h : \{0,1\}^* \rightarrow \{0,\ldots,n-1\}$. $\mathcal{A}$ publishes the elliptic curve E, the pairing e_n and the hash functions h and H. The public key of $\mathcal{A}$ is (g,P,Q,R,r,n) and his private key (a,b,p_1,p_2).

Signature generation. $\mathcal{A}$ wants to sign a message $m \in \{0,1\}^*$. Then he computes $S = g^{ab}H(m)$ and $s = bh(m) + a - ab \bmod \phi(n)$. Let $x(S)$ be the x-coordinate of S. The signature of m is the couple $(x(S),s)$.

Verification. Suppose that (x,s) is the signature of m. The receiver determines y such that $\Sigma = (x,y)$ is a point of $E(\mathbb{F}_q)$. He accepts the signature if and only if $e_n(\pm g^s\Sigma, P) = e_n(r^{h(m)}H(m), Q)$ and $g^s P = r^{h(m)}R$.

Security. For the determination of a and b from the public key, an attacker has to compute at least a discrete logarithm in the group $< P >$ and two logarithms modulo n. Note that an algorithm which computes the discrete logarithm modulo n implies an algorithm which breaks the Composite Diffie-Hellman key distribution scheme for n and any such algorithm can be used to factorize n [35, 7]. Furthermore, if there is an oracle $\mathcal{O}$ such that given a public key of our scheme and a message m provides a signature for m, then we can construct an algorithm for the factorization of n which and to solve the computational problem co-Diffie-Hellman for the subgroups of orders p_1 and p_2 of $< P >$ [9].

The Elliptic Curve and the Pairing. A practical method for the construction of an elliptic curve having a point of order n is as follows. We draw at random a prime number p_1 of a given size l; next we draw at random a number p_2 of size l and we repeat $p_2 = \text{NextPrime}(p_2)$ until $p = 4p_1p_2 - 1$ is prime. Then the elliptic curve $E : y^2 = x^3 + ax$, where $-a$ is not a square in $\mathbb{F}_p$, is supersingular and so $|E(\mathbb{F}_p)| = p+1 = 4p_1p_2$. Hence there is $P \in E(\mathbb{F}_p)$ with $\text{ord}(P) = p_1p_2$.
If ϵ is one of the Weil, Tate, eta, ate, omega pairings on $E[n]$, then we use the distorsion map $\psi(Q) = \psi(x,y) = (-x, iy)$ with $i^2 = -1$ and so, we have the pairing with the desired properties: $e(P,Q) = \epsilon(P,\psi(Q))$. In [43] we give another deterministic algorithm for the construction of a such curve running in polynomial time and a new map to point function.

6 Conclusion

The method we use today in order to enhance security in many applications is multiple encryption. Since no proof exists that the time needed to break a such system is considerably longer than the time needed to break the stronger component encryption scheme, it cannot actually used as solution to the problem of long term confidentiality. Thus the long-term confidentiality of encrypted data has turned out to be one of the most challenging open problems.

The method of multiple signature can provide a solution of the problem of long-term security for digital signatures. Since every message has more than one signature, we need more space in order to store a signed message. Of course, another drawback of the method is that the document has to be re-signed in case where a valid signature is broken.

Quantum and DNA computing are in the development phase and it requires a lot of work and research to reach an established stage. Thus, at the present, they do not consist a real threat to the security of conventional cryptography. To prepare for the future and unexpected attacks coming from Quantum and DNA computing, the designers of cryptographic primitives suitable for applications requiring long-term security have to bear in mind these two methods. On the other hand, since these methods are not yet sufficiently efficient, many basic cryptographic primitives of Quantum and DNA Cryptography cannot actually be realized. Finally, note that the research on Chaos cryptography is still at the initial stage, and since there are many problems to be solved, it is not able to provide efficient cryptographic primitive comparable with the conventional ones.

In addition to the aforementioned schemes, a number of additional approaches have been proposed based on algebraic problems, as for instance encryption and signature schemes based on problems of combinatorial group theory [2, 27, 28]. It is not clear when these or other problems will be well understood in order to provide practical public-key cryptographic primitives with reliable security.

As a solution of the problem of long term security we propose the construction of primitives which are based on two or more hard problems in such way that if any of these problems is broken, the others will still be valid and

hence the cryptographic scheme will be protected. Following this idea we have presented two such primitives. An encryption scheme which is based on the problems of integer factorization and integer logarithm problem, and a signature scheme relied on the problems of integer factorization and discrete logarithm of elliptic curves. Of course, a drawback of these schemes is that are not secure under the presence of quantum or DNA computers.

References

[1] G. Alvarez and S. Li, Some basic cryptographic requirements for chaos-based cryptosystems, *Int. J. Bifur. Chaos*, **16**, (2009), 2129–2151.

[2] I. Anshel, M. Anshel and D. Goldfeld, An algebraic method for public key cryptography, *Mathematical Research Letters*, **6**, (1999), 1–5.

[3] D. Beaver, Factoring: The DNA solution. In *4th International Conference on the Theory and Applications of Cryptology*, Wollongong, Australia, Springer-Verlag, (1994), 419–423.

[4] C. H. Bennett and G. Brassard, Quantum Cryptography: Public key distribution and coin tossing, *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, (1984), p. 175.

[5] C. Bennett, E. Bernstein, G. Brassard and U. Vazirani, Strengths and weaknesses of quantum computation, *Special Issue on Quantum Computation of the Siam Journal of Computing*, (Oct., 1997).

[6] D. J. Bernstein, J. Buchmann, E. Dahmen (Eds.), *Post-Quantum Cryptography*, Springer, 2009.

[7] E. Biham, D. Boneh and O. Reingold, Breaking generalized Diffie-Hellman is no easier than factoring, *Information Processing Letters*, **70**, (1999), 83–87.

[8] D. Boneh, C. Dunworth and R. Lipton, Breaking DES using a molecular computer, in *Proceedings of DIMACS workshop on DNA computing*, (1995), 37–65.

[9] D. Boneh, B. Lynn and H. Shacham, Short Signatures from the Weil Pairing, *Lecture Notes in Computer Science*, **2248**, (2001), 514–532.

[10] R. Bróker, Constructing Supersingular Elliptic Curves, *Journal of Combinatorics and Number Theory*, **1**(3), (2009), 269–273.

[11] J. Buchmann, A. May and U. Vollmer, Perspectives for cryptographic long term security, *Communications of the ACM*, **49**(9), (2006), 50–55.

[12] G.Z. Cui, L.M. Qin, and Y.F. Wang, An encruption scheme using DNA technology. In *IEEE 3rd International Conference on BioInspired Computing: Theories and Applications (BICTA08),* Adelaid, SA, Australia, (2008), 37–42.

[13] E. Dahmen, *Post-quantum signatures for today*, TU Darmstadt, Dissertation, 2009.

[14] Y. Dodis and J. Katz, *Chosen-Ciphertext Security of Multiple Encryption.* In: Kilian, J. (ed.) TCC 2005. LNCS, **3378**, 188–209, Springer, Heidelberg, 2005.

[15] A. K. Ekert, Quantum cryptography based on Bell's Theorem, *Phys. Rev. Lett.*, **67**, (1991), 661–663.

[16] D. Engelbert, R. Overbeck, and A. Schmidt, A Summary of McEliece-Type Cryptosystems and their Security, *J. Math. Crypt.*, **1**, (2007), 151–199.

[17] FlexiProvider-A toolkit for the Java Cryptographic Architecture (JCA/JCE); www.flexiprovider.de.

[18] A. Fujioka, Y. Okamoto and T. Saito, *Security of Sequential Multiple Encryption.* In: Abdalla, M., Barreto, P.S.L.M. (eds.) LATINCRYPT. LNCS, **6212**, pp. 20–39, 2010.

[19] S. D. Galbraith and V. Rotger, Easy Decision Diffie-Hellman Groups, *LMS J. Comput. Math.*, **7**, (2004), 201–218.

[20] A. Gehani, T.H LaBean, J.H. Reif, DNA-based cryptography, In *5th DIMACS Series in Discrete Mathematics and Theoretical Computer Science, MIT*, **54**, (1999), 233–249.

[21] X.T. Geng, Research on Molecular Algorithms in Block Cipher and Graph Theory, A Dissertation for the Degree of Doctor, Huazhong University of Science and Technology, (2008).

[22] J. Hopffstein, N. Howgrave-Graham, J. Pipher, J. H. Silverman and W. Whyte. NTRUSign: Digital signatures using the NTRU lattice. In *Topics in Cryptology-CT-RSA 2003, The Cryptographers' Track at the RSA Conference 2003*, (2003), 122–140.

[23] J. Hopffstein, N. Howgrave-Graham, J. Pipher, J. H. Silverman and W. Whyte. NTRUEncrypt and NTRUSign: Efficient public key algorithms for a post-quantum world. In *PQCrypto 2006: International Workshop on Post-Quantum Cryptography,* May 2006, 141–158.

[24] J. Hopffstein, J. Pipher and J. H. Silverman. NTRU: A ring-based public-key cryptosystem. In *Algorithmic Number Theory (ANTS-III): Proceedings of the Third International Symposium on the Algorithmic Number Theory,* June 1998, 267–288.

[25] G. Jakimoski and L. Kocarev, Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps, *IEEE Trans. on Circuits and Systems, Part I*, **48**(2), (2001), 163–169.

[26] S. V. Kartalopoulos, DNA-inspired cryptographic method in optical communications, authentication and data mimicking. In *Military Communications Conference 2005*, MILCOM 2005, IEEE.

[27] K. H. Ko, S. J. Lee, J. H. Chean, J. W. Han, J. S. Kang and C. Park, *New public-key cryptosystem using braid groups.* In *Advances in Cryptology-CRYPTO 2000 (Mihir Bellare, ed.)* LNCS 1880, Springer-Verlag, 2000, 163–183.

[28] K. H. Ko, D. H. Choi, M. S. Cho, and J. W. Lee, New signature scheme using conjugacy problem, http://eprint.iacr.org/2002/ 168/, 2002.

[29] L. Kocarev and G. Jakimoski, Unpredictable Pseudo-Random Bits Generated by Chaotic Maps, *IEEE Trans. on Circuits and Systems, Part I*, **50**(1), (2003), 123–126.

[30] L. Kocarev, M. Sterjev, A. Fekete and Vattay, Public-Key Encryption with Chaos, *CHAOS*, **14**(4), (2004) 1078–1084.

[31] A. Leier, C. Richter, W. Banzhaf and H. Rauhe, Cryptography with DNA binary strands, *BioSystems, Elsevier Science*, **57**(1), (2000), 13–22.

[32] K. Li, S. Zou and J. Xv, Fast parallel molecular algorithms for DNA-based computations: Solving the elliptic discrete logarithm problem over $GF(2^n)$, *Journal of Biomedicine and Biotechnology, Hindawi*, (2008), 1–10.

[33] J. S. Maseberg, Fail-safe konzept fur public-key infrastrukturen, Thesis, Technische Universitat Darmstadt 2002.

[34] U. M. Maurer and J. L. Massey, Cascade Cipher: The Important to be First, *J. Cryptology,* **6**, 1, (1993) 55–61.

[35] K. S. McCurley, A key distibution system equivalent to factoring, *J. Cryptology*, **1**, (1988), 95–105.

[36] R. J. McEliece, A public-key cryptosystem based on algebraic coding theory. *Deep space Network Progress Report*, **42-44**, Jet Propulsion Laboratory, California Institute of Technology, (1978), 114–116.

[37] R. C. Merkle, A certified digital signature. In *Advances in Cryptology-CRYPTO'89, 9th Annual International Cryptology Conference*, (1989), 218–238.

[38] R. C. Merkle and M. E. Hellman, On the Security of Multiple Encryption, *ACM Commun.*, **24**(7), (1981), 465–467.

[39] Mislovatry, E. Klein, I. Kanter and W. Kinzel, Public Channel Cryptography by Synchronization of Neural Networks and Chaotic Maps, *Phys. Rev. Lett.*, **91**, (2003), 118701.

[40] J. Patarin, Cryptoanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt'88, In *Advances in Cryptology-CRYPTO'95*, LNCS, **963**, Springer 1995, 248–261.

[41] D. Pointcheval, New public key cryptosystems based on the dependent-RSA problems. In *Advances in Cryptology - EUROCRYPT '99. Proceedings. Berlin: Springer. Lect. Notes Comput. Sci.* **1592** (1999) 239–254.

[42] D. Poulakis, A public key encryption scheme based on factoring and discrete logarithm, *Journal of Discrete Mathematical Sciences and Cryptography,* **12**, 6, (2009) 745–752.

[43] D. Poulakis and R. Rolland, A Digital Signature Scheme for Long-Term Security, Cryptology ePrint Archive: Report 2012/134, 2012, http://eprint.iacr.org/2012/134.pdf.

[44] K. Prasadh, K. Ramar and Gnanajeyaraman, Public key cryptostems based on chaotic Chebyshev polynomials, *Journal of Engineering and Technology Research,* **1**(7), (2009) 122–128.

[45] P. Rakheja, Integrating DNA Computing in International Data Encryption Algorithm (IDEA), *International Journal of Computer Applications*, (0975-8887), **26**(3), (July, 2011).

[46] C. E. Shannon, Communication Theory of Secrecy Systems, *Bell System Technical Journal*, **28**, (1949) 656–715.

[47] P. W. Shor, Algorithms for quantum computation: Discrete logarithms and factoring, In *Proceedings of 35th Symposium on Foundations of Computer Science*, (1994), 124–134.

[48] Y. Tsiounis and M. Yung, On the security of ElGamal based encryption. Imai, Hideki (ed.) et al., Public key cryptography. 1st international workshop on practice and theory in public key cryptography, PKC '98, *Proceedings*, Berlin, Springer, *Lect. Notes Comput. Sci.*, **1431**, (1998), 117–134.

[49] R. Zhang, G. Hanaoka, J. Shikata and H. Imai, *On the Security of Multiple Encryption or CCA-security+CCA-security = CCA-security*? In : Bao, F., Deng, R., H., Zhou, J. (Eds) PKC 2004, LNCS 2947, 364–374, Springer Heidelberg, 2004.

[50] X. Zhang, Breaking the NTRU public key cryptosystem using self-assembly of DNA tilings, *Chinese Journal of Computers*, **12**, (2008), 2129–2137.