Journal of Computer Science 7 (12): 1765-1769, 2011
ISSN 1549-3636

New Cryptosystem Using Multiple Cryptographic Assumptions

E.S. Ismail and M.S. Hijazi
School of Mathematical Sciences, Faculty of Science and Technology,
University Kebangsaan Malaysia, 43600 UKM Bangi, Selangor, Malaysia

Abstract: Problem statement: A cryptosystem is a way for a sender and a receiver to communicate digitally by which the sender can send receiver any confidential or private message by first encrypting it using the receiver's public key. Upon receiving the encrypted message, the receiver can confirm the originality of the message's contents using his own secret key. Up to now, most of the existing cryptosystems were developed based on a single cryptographic assumption like factoring, discrete logarithms, quadratic residue or elliptic curve discrete logarithm. Although these schemes remain secure today, one day in a near future they may be broken if one finds a polynomial algorithm that can efficiently solve the underlying cryptographic assumption. **Approach:** By this motivation, we designed a new cryptosystem based on two cryptographic assumptions; quadratic residue and discrete logarithms. We integrated these two assumptions in our encrypting and decrypting equations so that the former depends on one public key whereas the latter depends on one corresponding secret key and two secret numbers. Each of public and secret keys in our scheme determines the assumptions we use. **Results:** The newly developed cryptosystem is shown secure against the three common considering algebraic attacks using a heuristic security technique. The efficiency performance of our scheme requires $2T_{exp}+2T_{mul}+T_{hash}$ time complexity for encryption and $T_{exp}+2T_{mul}+T_{srt}$ time complexity for decryption and this magnitude of complexity is considered minimal for multiple cryptographic assumptions-like cryptosystems. **Conclusion:** The new cryptosystem based on multiple cryptographic assumptions offers a greater security level than that schemes based on a single cryptographic assumption. The adversary has to solve the two assumptions simultaneously to recover the original message from the received corresponding encrypted message but this is very unlikely to happen.

Key words: Cryptology, cryptography, cryptosystem, cryptographic assumptions, quadratic residue, discrete logarithms, factoring attack, discrete logarithm attack, polynomial algorithm

INTRODUCTION

Many designated cryptosystems (Diffie and Hellman, 1976) in the literature were developed based on a single cryptographic assumption like algebraic geometric code (Pramod and Manju, 2010), discrete logarithms (DL) (ElGamal, 1985), factorization (FAC) (Rivest *et al*., 1978), quadratic residue (QR) (Rabin, 1979), elliptic curve discrete logarithm (ECDL) (Koblitz, 1987; Miller, 1986) problems. Some of them remain secure and are resistant to attacks. However, one day in the future, one could find a polynomial algorithm that can efficiently solve the underlying assumption hence break the corresponding cryptosystem easily. Many cryptographers realize it and start to develop a more secure cryptosystem. One of the methods to design such scheme is by using multiple cryptographic assumptions (Ismail *et al*., 2008a; Elkamchouchi *et al*., 2004; Harn, 1994; Baocang and Yupu, 2005; Ismail *et al*., 2008b; Ismail and Hijazi, 2011). The reason behind this is an adversary needs a longer period of time in order to break the multiple cryptographic assumptions-based cryptosystem since it is very unlikely for the adversary to obtain the solutions of these cryptographic assumptions simultaneously.

In this article, we proposed a new cryptosystem based on two cryptographic assumptions; quadratic residue and discrete logarithm problems. With the improved security offered, we also showed that the performance of the scheme requires acceptable numbers of operations in both encrypting and decrypting processes, which makes it very practical for real applications.

Some notations and parameters: The following notations and parameters are used to initialize the developed scheme:

Corresponding Author: E.S. Ismail, School of Mathematical Sciences, Faculty of Science and Technology, University Kebangsaan Malaysia, 43600 UKM Bangi, Selangor, Malaysia

- Two large strong random primes p and q which are safe primes and set the modulus n = pq
- A primitive element, g from H = {z : gcd(z, n)=1} of order n satisfying $g^{n-1} = 1 \bmod n$ where gcd (a,b) denotes the greatest common divisor of a and b
- A cryptographic hash-function h(.) whose output is a t-bit length and we suggest t = 128

MATERIALS AND METHODS

We propose a cryptosystem based on multiple cryptographic assumptions; quadratic residue and discrete logarithms. The scheme consists of three phases namely Initialization, Encryption and Decryption. In Initialization phase, the public and secret keys of receivers are computed. The calculated public keys will be published in a public directory and everyone including adversaries could access it while the secret keys remain secret and will be kept by the receivers.

In Encryption phase, the original message owned by a sender is first hashed using the appropriate cryptographic hash function, h(.). This function transforms an input of arbitrarily length to a fixed length of output (128 bits). The sender then gets his hashed message encrypted and this is done by first picking a secret integer randomly plus the receiver's public key. The encrypted message is then sent to the legal receiver. In Decryption phase, the receiver obtains the original message by using his own secret keys.

Initialization phase:

- Choose randomly an integer x < n from H
- Compute the number $y = g^x \bmod n$

The public key is given by y and can be accessed in the public directory and the secret key is given by x and only known to the legal receiver. Also only the receiver knows the primes factorization of n.

Encryption: Get the original message, m hashed. The sender encrypts his message h(m) of 128-bits as follows before sends receiver a pair (c_1, c_2).

- Select at random an integer c < n from H
- Disguise the message by computing

$$c_1 = h(m)^2 y^{-c} \bmod n \qquad (1a)$$

- Calculate the number:

$$c_2 = g^c \bmod n \qquad (1b)$$

In the original ElGamal, (1985) cryptosystem we compute the number c_1 in Eq. 1a without squaring the original message. In our scheme, we need this as we implementing the Rabin, (1979) cryptosystem for QR-like scheme.

Decryption: The receiver decrypts the obtained encrypted message (c_1, c_2) as below.

- Compute the following:

$$c_1(c_2)^x = h(m)^2 \bmod n \qquad (2)$$

- The receiver uses the known technique (Rabin, 1979) to extract the original message h(m) from $[h(m)^2]$ and this can be done since he knows the prime factorization of n.

A simple example: We describe an example to show the basic principle of our developed cryptosystem. Practitioners are not recommended to select keys or parameters computed in this example in practice since inappropriate parameters would make this scheme vulnerable to attacks.

Assume that p = 29 and q = 43. Then the modulus is now given by n = 1247. Next picks the number x = 37 and a primitive element, g = 17. Thus the public and secret keys of the scheme are respectively given by 1003 and 37. To encrypt the original message h(m) = 1122, the sender selects c = 3 and sends receiver

$$c_1 = 1122(1003)^{-3} = 1116 \bmod 1247$$

and

$$c_2 = 17^3 = 1172 \bmod 1247$$

The receiver once obtains (1116, 1172) recovers the original message as below:

$$(1116)1172^{37} = 661 \bmod 1247$$

and one can check easily that the quadratic residue of 661 mod 1247 is given by the original message 1122 mod 1247.

RESULTS

We discuss our results of the newly developed cryptosystem according to the following criterion.

- Verification

- Security analysis
- Efficiency performance

We start by proving the validity of our scheme then we show that our scheme is heuristically secure by considering common algebraic attacks on cryptosystem. Lastly, we describe the efficiency consideration using computational complexity of the proposed scheme.

For verification, we prove that the decrypting Eq.2 is correct. For security consideration, we use a technique from heuristic security to show that the scheme is secure. We do this by delivering the scheme to the literature for attacks. We consider three possible attacks by which an Adversary (Adv) may try to take down the new cryptosystem. We define each attack and give the corresponding analysis of why this attack would fail. For efficiency performance, we evaluate the time complexity for both phases; encryption and decryption and we calculate the communication cost for our scheme.

Verification: We validate our new cryptosystem by proving the following theorem.

Theorem: If the algorithms of Initialization and Encryption run smoothly then the decryption of the encrypted message in Decryption is correct.

Proof: The Eq.2 above is true for all encrypted message (c_1, c_2) since

$$c_1(c_2)^x = h(m)^2 y^{-c} (g^c)^x = h(m)^2 g^{-cx} (g^c)^x = h(m)^2 \bmod n$$

Security analysis: We show that our scheme is heuristically secure by considering the following three most common attacks on cryptosystem.

Direct attack: Adv wishes to obtain all secret keys using all information available from the system. Particularly, he wants to find the 3-tuples (x, p, q). In this case, Adv needs to solve QR and DL. For QR, he needs to find the primes of n and the best way to factorize the modulus n = pq is by using the number field sieve method (Lenstra *et al*., 1993). However, this method is just dependent on the size of modulus n and it is computationally infeasible to factor an integer of size 1024-bit and above. The primes p and q also must be well-chosen that they are must be strong primes (Gordon, 1984). This could resist the scheme from the special-purpose factorization algorithms attack. For DL, to resists it from various attacks one should check and confirm that the two integers (p-1)/2 and (q-1)/2 are the product of two 512-bit strong primes.

Factoring attack: Assume that the Adv has successfully solves the factoring assumption so that he knows the primes p and q. He also learns the following equation:

$$c_1 = h(m)^2 y^{-c} = h(m)^2 g^{-cx} \bmod n$$

From the equation, to recover the original message, h(m) he has to remove the term g^{-cx} from c_1. At this stage, he knows g^c and g^x but according to Diffie-Hellman problem (Diffie and Hellman, 1976) he cannot compute g^{cx}. Thus the Adv would fail.

Discrete logarithm attack: Assume that the Adv is able to solve the DL problem and thus obtain the secret integer x. He then knows that $(c_2)^x = g^{cx} \bmod n$ and tries to recover the original message h(m) from the equation

$$c_1 = h(m)^2 y^{-c} = h(m)^2 g^{-cx} \bmod n$$

Upon knowing the secret x, he manages to remove the term g^{-cx} from c_1 to obtain $h(m)^2$. Unfortunately, to get h(m) from $h(m)^2$ he must know the secret primes p and q but this is impossible since the FAC is computationally infeasible.

Efficiency performance: Next, we investigate the performance of our scheme in terms of number of keys, computational complexity and communication costs. The following notations are used to analyse the performance of the scheme.

- SK and PK denote the number of secret and public keys respectively
- T_{exp} is the time taken for a modular exponentiation
- T_{mul} is the time taken for a modular multiplication
- T_{srt} is the time taken for a modular quadratic residue computation
- T_{hash} is the time taken for performing a hash function
- |x| denotes the bit length of x

Table 1: The performance of our new cryptosystem

		Our scheme
The number of keys	SK	1
	PK	1
Computational complexity	Encryption	$2T_{exp}+2T_{mul}+T_{hash}$
	Decryption	$2T_{exp}+2T_{mul}+T_{srt}$
Communication cost	Encryption	$2\lvert n\rvert$
	Decryption	$2\lvert n\rvert$

We ignore the time complexity for modular addition or subtraction computation and we assume that the probability of the bit being selected as 0 or 1 is 0.5. The performance of our new cryptosystem is summarized in Table 1.

From Table 1, the sender performs $482T_{mul}+T_{hash}$ time complexity for encryption process and the receiver performs $242T_{mul}+T_{srt}$ time complexity for decryption process using the conversion $T_{exp}=240T_{mul}$ (Koblizt *et al*., 2000). Finally the communication costs of the scheme are given by 4|n|.

DISCUSSION

Many existing cryptosystems were developed based on a single cryptographic assumption like factoring, discrete logarithm, elliptic curve discrete logarithm and quadratic residue problems. In a near future, if an attacker finds a polynomial algorithm solving this assumption, he then can read the original message from the corresponding encrypted message and hence break the scheme.

Our new proposed cryptosystem is prevented from this situation. This is because the scheme is designed based on two cryptographic assumptions namely quadratic residue and discrete logarithms. The enemy can break this scheme only if he can solve the two problems at one time and this is happen with negligible probability. Although he manages to find a solution to one of the underlying assumption in one certain period of time, our scheme remains secure as the other assumption remains hard to solve for at least another period of time.

Our scheme next is protected from the most three common considering attacks for scheme based on two assumptions. The performance analysis shows that the developed scheme requires reasonable number of modular operations in both encryption and decryption phases and thus makes it very efficient and suitable for applications.

CONCLUSION

We developed a new cryptosystem based on two cryptographic assumptions; quadratic residue and discrete logarithms. The proposed scheme requires respectively $482T_{mul}+T_{hash}$ and $242T_{mul}+T_{srt}$ for encryption and decryption. Some possible attacks have also been considered and we showed that the scheme is secure from those attacks.

ACKNOWLEDGEMENTS

We acknowledge the financial support received from Universiti Kebangsaan Malaysia under the Research University Grant UKM-OUP-FST-2011 and the Grant UKM-DLP-2011-028.

REFERENCES

Baocang, W and H. Yupu, 2005. Public key cryptosystem based on two cryptographic assumptions. IEE Proc. Commun., 152: 861-865. DOI: 10.1049/ip-com:20045278

Diffie, W and M. Hellman, 1976. New directions in cryptography. IEEE Trans. Inform. Theory, 22: 644-654. DOI: 10.1109/TIT.1976.1055638

ElGamal, T, 1985. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. Inform. Theory, 31: 469-472. DOI: 10.1109/TIT.1985.1057074

Elkamchouchi, H.M., M.E. Nasr and R. Esmail, 2004. New public key techniques based on double discrete logarithm problem. Proceedings of the 21st National Radio Science Conference, Mar. 16-18, IEEE Xplore Press, Egypt, pp: C23-1-9. DOI: 10.1109/NRSC.2004.1321832

Gordon, J., 1984. Strong RSA keys. Elect. Lett., 20: 514-516. DOI: 10.1049/el:19840357

Harn, L., 1994. Public-key cryptosystem design based on factoring and discrete logarithms. IEE Proc., Comput. Digit. Technol., 141: 193-195. DOI: 10.1049/ip-cdt:19941040

Ismail, E. S., Hijazi, M. S. N, Hashim, I, 2008a. A New Design Public Key Encryption Scheme Based on Factoring and Discrete Logarithm Problems, IEEE International Symposium on Information Technology 2008, 1: 230-233, ISBN: 978-1-4244-2327-9. DOI 10.1109/ITSIM.2008.4631561

Ismail, E.S, N.M.F. Tahat and R.R Ahmad. 2008b. A new digital signature scheme based on factoring and discrete logarithms. J. Math. Stat., 4: 222-225. DOI: 10.3844/jmssp.2008.222.225

Ismail, E.S. and M.S.N. Hijazi, 2011. A new cryptosystem based on factoring and discrete logarithm problems. J. Math. Stat., 7: 165-168. DOI: 10.3844/jmssp.2011.165.168

Koblitz, N, 1987. Elliptic curve cryptosystems. Math. Comput., 48: 203-209. DOI: 10.1090/S0025-5718-1987-0866109-5

Koblizt, N., A. Menezes, S. Vanstone, 2000. The state of elliptic curve cryptography. Design, Codes Cryptography, 19: 173-193. DOI: 10.1023/A:1008354106356

Lenstra, A.K., H.W. Lenstra, M.S. Manesse and J.M. Pollard, 1993. The number field sieve. Dev. Number Field Sieve, 1554: 11-42. DOI: 10.1007/BFb0091537

Miller, V.S. 1986. Use of elliptic curves in cryptographys. Adv. Cryptol.-CRYPTO'85 Proc., 218: 417-426. DOI: 10.1007/3-540-39799-X_31

Pramod, K.V and C. Manju, 2010. A Cryptosystem Using the Concepts of Algebraic Geometric Code. J. Comput. Sci., 6: 244-249. DOI: 10.3844/jcssp.2010.244.249.

Rabin, M.O, 1979. Digitalized signatures and public-key functions as intractable as factorization. 1st Edn., Massachusetts Institute of Technology, Laboratory for Computer Science, Ft. Belvoir Defense Technical Information Center JAN, pp: 18.

Rivest, R.L., A. Shamir, and L. Adleman, 1978. A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM, 21: 120-126. DOI: 10.1145/359340.359342