Bulletin of Electrical Engineering and Informatics
Vol. 4, No. 2, June 2015, pp. 155~159
ISSN: 2089-3191

The Beta Cryptosystem

Chandrashekhar Meshram
Department of Mathematics, RTM Nagpur University, Nagpur, India
email: cs_meshram@rediffmail.com

Abstract

This paper, we introduce mainly the concept of beta cryptosystem, whose security is based on generalized discrete logarithm problem and integer factorization problem in the multiplicative group of finite fields. We show that the proposed public key cryptosystem based on generalized discrete logarithm problem and integer factorization problem, provides more security because of double computation comparing with the generalized discrete logarithm problem and integer factorization problem. Hence the adversary has to solve distinct discrete logarithm problems and integer factorization problem simultaneously in the multiplicative group of finite fields in order to recover a corresponding plaintext from the received cipertext. Therefore, this scheme is expected to gain a higher level of security. We next show that, the newly developed scheme is efficient with respect to encryption and decryption and the validity of this algorithm is proven by applying to message that are text and returning the original message in numerical examples.

Keywords*: Public key cryptosystem, discrete logarithm problem and Integer factorization problem*

1. Introduction

Since the Diffie-Hellman [1] seminal paper New Directions in Cryptography which introduced the concept of public key cryptography, many asymmetric cryptosystems were proposed. The new technics are based on hard mathematical problems. Among these cryptosystems, we can cite the famous RSA [2] which security relies on the impossibility of factoring a large integer. By the same way, Rabin in [3] proposed an RSA look alike cryptosystem based on the difficulty of extracting the square root modulo a large composite integer. Taking square root modulo a composite prime is equivalent to the factorization of the modulo. In another context, ElGamal introduces an efficient and simple cryptosystem in [4]. The security of the new scheme is based on discrete logarithm problem. The DLP is computationally very hard to solve when considering a prime field or the group of rational points of an elliptic curve defined over a finite field.

However, it is understood that one day in the future the IFP and DL problems could be solved and when it happens, all cryptosystem schemes that depend on one of these problems will no longer be secure. One of the strategies to surmount this situation is by designing a public key cryptosystem scheme based on multiple hard problems. Undoubtedly, the security of such schemes is longer than schemes based on a single problem. This is due to unlikely solving two hard problems simultaneously. Many public key cryptosystem have been designed based on both IFP and DLP [5-23] but to design such schemes is not an easy task since many of them have been shown insecure.

As outlined in the above, unfortunately we found that the entire existing public key cryptosystem scheme based on discrete logarithm and integer factorization cannot be regarded as secure. Therefore, we designed a new cryptosystem based on two hard problems namely; factoring and generalized discrete logarithm problems. With its guaranteed security, we also showed that the performance of the scheme requires reasonable numbers of operations in both encrypting and decrypting processes, which makes it very efficient to be implemented in the real world applications.

The remainder of this paper is organized as follows: Section 2, presented proposed beta cryptosystem. Section 3 the example for validation of beta cryptosystem. Section 4 result and consistency of algorithm. Section 5 explin the security analysis and discussion. Section 6 discussed Efficiency performance of the beta cryptosystem. Conclusion is given in the final section 7.

Received November 26, 2014; Revised January 4, 2015; Accepted January 15, 2015

2. The Beta Cryptosystem

The algorithm consists of three subalgorithms: Key generation, encryption and decryption

- Key generation: The key generation algorithm runs as follows (user 1 should do the following)

1. Generate two large random (distinct) primes p and q, each roughly of the same size
2. Compute $N = p * q$ and compute the Euler-phi function $\varphi(N) = (p-1)(q-1)$.
3. Select a random integer e, $1 \leq e \leq \varphi(N)$ such that $gcd\left(e, \varphi(N)\right) = 1$.
4. Select a random integer b such that $2 \leq b \leq \varphi(N) - 1$.
5. Choose any random element β of the multiplicative group Z_N^* and Compute $y_1 = \beta^b (mod\ N)$.
6. Use the extended Euclidean algorithm to compute the unique integer d, $1 \leq d \leq \varphi(N)$ such that $ed \equiv 1\ (mod\ N)$.

The public key is formed by (N, e, β^b) and the corresponding private key is given by (d, b, β).

- Encryption: An user 2 to encrypt a message $h\ (m)$ to user 1 should do the following:

1. Obtain public key (N, e, β^b).
2. Represent the message as $m \in [1, N-1]$.
3. Get the original message hashed and assume that the resultant becomes $h(m)$.
4. The cipher text is given by

$$C = (h\ (m)\beta^b)^e (mod\ N) \quad (1)$$

- Decryption: To recover the plaintext $h\ (m)$ from the ciphertext C, user 1 does the following:

1. Compute $y_2 = \beta^{\varphi(N)-b} (mod\ N) = \beta^{-b} (mod\ N)$.
2. Then compute $y_3 = (y_2)^e (mod\ N)$

Recover the plaintext $h\ (m)$ by computing $((y_2)^e * C)^d (mod\ N)$. (2)

3. Example

To make our construction easy to comprehend, we illustrate an example to show the basic principle of our scheme. However, practitioners are not recommended to choose such keys or parameters in practice since inappropriate parameters will make this scheme vulnerable to attacks. Let the two primes be p = 29 and q = 43 and set N = 1247 and $\varphi(N)$= 1176.

Key generation: The key generation algorithm runs as follows (user 1 should do the following)

1. Select a random integer $e = 11$, such that $gcd\ (11{,}1176) = 1$.
2. Select a random integer $b = 19$.
3. Choose any element ,$\beta = 10$of the multiplicative group Z_N^* and Compute $y_1 = \beta^b (mod\ N) = 10^{19} (mod\ 1247)$.
4. Use the extended Euclidean algorithm to compute the unique integer $d = 107$, $1 \leq d \leq \varphi(N)$ such that $11d \equiv 1\ (mod\ 1247)$.

The public key is formed by (N, e, β^b) and the corresponding private key is given by (d, b, β).

Encryption: An user 2 to encrypt a message $h\ (m)$ to user 1 should do the following:

1. Represent the message as $h\ (m) = 1122$ is represented as an integer in the interval $[1, N-1]$
2. The cipher text is given by

$$C = (h\ (m)\beta^b)^e (mod\ N) = 791$$

Decryption: To recover the plaintext M from the ciphertext C, user 1 does the following:

1. Compute $y_2 = \beta^{\varphi(N)-b} (mod\ N) = \beta^{-b} (mod\ N) = 917$.
2. Then compute $y_3 = (y_2)^e (mod\ N) = 483$.
3. Recover the plaintext $h\ (m)$ by computing $((y_2)^e * C)^d (mod\ N) = 1122$

4. Results

We discuss our results according to the following criterion:

- Consistency of the beta cryptosystem
- Security Analysis
- Efficiency of beta cryptosystem

To verify our scheme, 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 also the communication cost for our scheme.

Consistency: We validate our new scheme by proving the following theorem.
Theorem1: If the algorithms of key generation and encryption run smoothly then the decryption of the encrypted message in decryption is correct.

Prof. The Eq. 2 above is true for all encrypted message
Then, in encryption algorithm,

$$C = (h\,(m)\beta^{b})^{e}(mod\ N)$$

and decryption algorithm ,

$$y_2 = \beta^{\varphi(N)-b}(mod\ N) \quad = \beta^{-b}(mod\ N)$$

And $(y_2)^{e}(mod\ N) = (\beta^{-b})^{e} mod\ N$,

$$((y_2)^{e} * C)^{d}(mod\ N) = (\beta^{-be}(h(m))^{e}\beta^{be})^{d}(mod\ N) = (h(m))^{ed}(mod\ N) = h(m)(mod\ N).$$

5. Security Analysis

We show that our scheme is heuristically secure by considering the following three most common attacks.

- Direct attack: Adv wishes to obtain all secret keys using all information available from the system. In this case, Adv needs to solve IFP and GDLP. The best way to factorize the modulus $N = pq$, is by using the number field sieve method (Lenstra *et al*., 1990). 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. Next, to increase the security of our scheme, we must select strong primes (Gordon, 1984) to avoid attacks using special-purpose factorization algorithms. We can achieve and maintain the same security level for GDLP by selecting the modulus $N = pq$ with $\frac{p-1}{2}$ and $\frac{q-1}{2}$ respectively are product of two 512-bit strong primes.

- Factoring attack: Assume that the Adv successfully solves the factoring problem so that he knows the secret keys (β, b). With this information in hand, he learns that

$$C = (h\,(m)\beta^{b})^{e}(mod\ N)$$

From the above equation, to recover the original message M, one has to remove the term β^{b} from C and this only can be done if one knows the secret numbers (β, b). Since at this stage the GDL problem remains hard to solve then the Adv would fail.

- Discrete logarithm attack: Assume that the Adv is able to solve the GDL problem and thus obtain the secret integer b. He then knows that

$$y_2 = \beta^{\varphi(N)-b}(mod\ N) = \beta^{-b}(mod\ N)$$

and

$$(y_2)^{e}(mod\ N) = (\beta^{-b})^{e} mod\ N$$

By knowing this number the Adv tries to recover the original message M from the equation

$$C = (h\,(m)\beta^{b})^{e}(mod\ N)$$
$$= (h\,(m))^{e}\beta^{be}(mod\ N)$$

Since the exponent e is public, he manages to remove the term β^{be} from C and obtains $(h\,(m))^{e}$. Unfortunately, to read the original message he must has the secret d in hand but this is impossible since the IFP is hard to solve.

6. 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 analyses 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 and T_{mul} is the time taken for a modular multiplication
- T_{squ} is the time taken for a modular square computation and T_{srt} is the time taken for a modular square-root computation
- T_{inv} is the time taken for a modular inverse computation and T_{hash} is the time taken for performing a hash function,
- |x| denotes the bit length of x

Here we ignore the time performing modular addition or subtraction computation and we assume that the probability of the bit being selected as 0 or 1 is $\frac{1}{2}$.

The performance of our beta cryptosystem is summarized as in Table 1. From Table 1, the sender performs $721T_{mul} + T_{hash}$ time complexity for encryption and the receiver performs $481T_{mul}$ time complexity for decryption using the conversion $T_{exp} = 240T_{mul}$ [10]. Finally the communication costs or size of parameters of the scheme is 3|n|.

Table 1: The performance of our new cryptosystem

		Our beta cryptosystem
The number of keys	SK	3
	PK	3
Computational complexity	Encryption	$2T_{exp} + T_{mul} + T_{hash}$
	Decryption	$3T_{exp} + T_{mul}$
Communication cost	Encryption	2n
	Decryption	n

6.1 Discussion

Most of the designated cryptosystems are based on a single hard problem like factoring, discrete logarithm and elliptic curve discrete logarithm problems. If one day an enemy could find a polynomial algorithm solving this problem, he then can read the original message from any corresponding encrypted message.

Our new developed cryptosystem is prevented from this type of problem. This is because our scheme is designed based on two hard problems namely factoring and discrete logarithm. The enemy only can break this scheme if he can solve the two problems simultaneously and this is very unlikely to happen. If he manages to find a solution to one of the underlying hard problem, our scheme remains secure as the other problem remains hard to solve for at least another period of time.

Our scheme next is protected from the most common considering attacks for scheme based on two hard problems. The performance analysis reveals that the developed scheme requires only minimal operations in encryption and decryption phases and thus makes it very efficient.

7. Conclusion

In this present paper, we present public key encryption scheme based on integer factorization problem and generalized discrete logarithm problem in the multiplicative group of finite fields. This kind of scheme definitely provides a new scheme with a longer and higher level of security than that based integer factorization problem and generalized discrete logarithm problem and also requires minimal operations in encryption and decryption algorithms and thus

makes it is very efficient. The present paper provides the special result from the security point of view, because we face the problem of solving on integer factorization problem and generalized discrete logarithm problem at the same time in the multiplicative group of finite fields as compared to the other public key cryptosystem, where we face the difficulty of solving the traditional on integer factorization problem and generalized discrete logarithm problem in the common groups.

References

[1]. W. Diffie, M. Hellman, "New Directions in Cryptography", *IEEE Transactions On Information Theory*, vol.22, no.6, pp. 644-654, 1976.

[2]. R. L. Rivest, A. Shamir, L. Adleman., "A Method to Obtain Digital Signature and Public key Crytosystem" Commun. ACM, vol 21, pp 121-126, 1978.

[3]. M. Rabin, "Digitalized Signatures and Public Key Functions as Intractable as Factorization", 1st Edition, Massachusetts Institute of Technology, Laboratory for Computer Science, Ft. Belvoir Defense Technical Information Center, pp 18, 1979.

[4]. T. ElGamal, "A public Key Cryptosystem and a Signature Scheme based on Discrete Logarithms", *IEEE Transactions on Information Theory*, Vol 31, pp 469-472, 1985.

[5]. L.Harn, "Public key cryptosystem design based on factoring and discrete logarithms", IEE Proceeding of Computers Digital Techniques, pp: 193-195, May, 1994.

[6]. E.S. Ismail and M.S.N. Hijazi, "A New Cryptosystem Based on Factoring and Discrete Logarithm Problems" Journal of Mathematics and Statistics, vol.7 (3) , pp. 165-168, 2011.

[7]. A. Ciss, A. Y. O. Cheikh and D. Sow "A Factoring and Discrete Logarithm based Cryptosystem" Cryptography and Security (cs.CR), arXiv:1205.1212 [cs.CR].

[8]. A. Kiriyama, Y. Nakagawa, T. Takaoka and Z. Tu "A New Public-Key Cryptosystem and its Applications" Proceedings of the Eighth International Conference on Enterprise Information Systems: Databases and Information Systems Integration (ICEIS 2006), Paphos, Cyprus, May 23-27, 2006;

[9]. S. M. Kalipha, J. W. A. Sada and H. A. Hussain "New public-key cryptosystem", International Journal of Systems Science,Vol.21(1), pp. 205-215, 1990.

[10]. N. Koblizt, A. Menezes, and S. Vanstone, "The state of elliptic curve cryptography", Design, Codes Cryptography, vol. 19, pp. 173-193, 2000.

[11]. J. Gordon, Strong RSA keys, Electron. Letter, 20, No. 12 (1984), 514-516.

[12]. A.K.Lenstra and M.S. Manasse, *"Factoring by electronic mail"* Advances in CrvDtolorv - EUROCRYPT '89 Chrineer Berlin, pp. 355-371, 1990.

[13]. C. Meshram and S. Meshram "PKC Scheme Based on DDLP" *International Journal of Information & Network Security (IJINS)*, Vol.2 (2), April 2013, pp. 154-159.

[14]. C. Meshram and S. Meshram "A Public Key Cryptosystem based on IFP and DLP" International Journal of Advanced Research in Computer Science, vol.2 (5), 2011 pp. 616-619.

[15]. C. Meshram, "A Cryptosystem based on Double Generalized Discrete Logarithm Problem" *International Journal of Contemporary Mathematical Sciences*, Vol. 6(6), 2011, pp. 285 – 297.

[16]. C. Meshram and S. Agrawal, "Enhancing the security of A Public key cryptosystem based on DLP $\gamma \equiv \alpha^{a\beta b} \pmod p$" *International Journal of Research and Reviews in Computer Science* Vol.1 (4), pp.67-70, 2010.

[17]. C. Meshram and S. Agrawal, "A New Design of Public Key Encryption Scheme Based on Double Discrete Logarithm Problem" Proceedings of International Conference on Challenges and Application of Mathematics in Science and Technology (CAMIST). January 11-13, 2010, pp. 495- 502.

[18]. C..Meshram, "New PKC Technique based on DDLP in Metacyclic Group"- Proceedings of National Conference on Establishing Kinship between Mathematical Science and Society (NCKMS). October 30-31, 2009, pp. 141-147.

[19]. Z. Shi, Y. Xia and C. Yu "A Strong RFID Mutual Authentication Protocol Based on a Lightweight Public-key Cryptosystem" *TELKOMNIKA Indonesian Journal of Electrical Engineering* Vol.12(3), pp. 2320-2326, 2014.

[20]. F. Amounas and E.H. El Kinani "Construction Efficiency of the Elliptic Curve Cryptosystem using Code Computing for Amazigh Alphabet" *International Journal of Information & Network Security*, Vol.2(1), pp. 43-53, 2013..

[21]. G. C. Sheng "Multiplicative Learning with Errors and Cryptosystems" *International Journal of Information & Network Security*, Vol.3 (2), pp. 92-97, 2014.

[22]. J. Yao and T. Zhang "Biometric Cryptosystem Based Energy Attack Analysis" *TELKOMNIKA Indonesian Journal of Electrical Engineering*, Vol.10 (5), pp. 1130-1136, 2012.

[23]. T. Mantoro and A. Zakariya "Securing E-mail Communication Using Hybrid Cryptosystem on Android-based Mobile Devices" *TELKOMNIKA Indonesian Journal of Electrical Engineering*, Vol.10 (4), pp. 827-834, 2012.