Advances in Computational Research
ISSN: 0975-3273 & E-ISSN: 0975-9085, Volume 5, Issue 1, 2013, pp.-138-140.
Available online at http://www.bioinfopublication.org/jouarchive.php?opt=&jouid=BPJ0000187

HYBRID PUBLIC KEY ENCRYPTION SCHEME FOR NETWORKING

ABOUD S.J.*
Department of Information Technology, Iraqi Council of Representatives, Baghdad-Iraq
*Corresponding Author: Email- sattar_aboud@yahoo.com

Received: July 02, 2013; Accepted: July 15, 2013

Abstract- In this paper, we analyze the Akleylek, et al. scheme and their try to enhance a security of peer-to-peer network by merging El-Gamal scheme with knapsack system. We demonstrate that this combination disclose a security and causes a scheme weak to cipher-text only attack. So, in a network a hacker can use this attack and easily decrypt an encrypted message. Also, we illustrate that a receiver cannot recover an encrypted message in polynomial time. Thus, this scheme is entirely inappropriate to employ in the peer-to-peer networks. We will change this scheme to enhance security and efficiency.

Keywords- Public key encryption, cryptanalysis, ElGamal scheme, knapsack system, hybrid encryption

Citation: Aboud S.J. (2013) Hybrid Public Key Encryption Scheme for Networking. Advances in Computational Research, ISSN: 0975-3273 & E-ISSN: 0975-9085, Volume 5, Issue 1, pp.-138-140.

Introduction

The use of computer network is increased day by day. This development produces a number of nodes to increase. By increasing a customer, a server becomes full of activity and inadequate while a bandwidth is sufficient. Furthermore, because the diversity of requests is growth, server may not have information a user needed. We can conquer these problems by using peer-to-peer network. The peer-to-peer network have not central server, some powerful nodes work as servers. In a fourth generation, streams over peer-to -peer network are supported. Thus, every node can communicate with another. The most influential problem in a peer-to-peer network is security. There are some ways to make peer-to-peer networks secure. Cryptosystem has a significant role in every way. Cryptosystem is the art of keeping information secure from overhearing and other malicious behavior. Thus, cryptography is very useful in peer-to-peer schemes because it can protect message and check its integrity. Akleylek, et al. [1] presented a modified scheme for security in peer-to-peer network. In their scheme, they try to increase a security of peer-to-peer system by combining ElGamal scheme [2] with knapsack scheme. The knapsack system is NP-complete [3-6]. This difficulty cannot be clearly solved even when applying quantum computers. They use ElGamal scheme to hide private knapsack to generate the public-key. But as we illustrate, this combination disclosures a security and makes a scheme weak to encrypted cipher-text-only-attack. Thus, in a network hacker can use this attack and easily decrypt message from any challenge-cipher-text. Also, we show that this scheme is not practical. So, we attempt to modify it to increase security and efficiency.

The remainder of this article is organized as follows. In Section 2 we provide a mathematical background. In Section 3 we describe Akleylek, et al. scheme. Cryptanalysis of this scheme will be considered in Section 4. In Section 5 we revise this scheme in order to perform a good security and efficiency. Conclusion is provided in Section 6.

Materials and Methods

In this section, we provide the mathematical background and definitions which are required to show the proposed attack.

Mathematical Background

In this section we will discuss some mathematical background related to the proposed scheme.

Definition 1: Assume that the sequence of integers ($w_1,\ldots..,w_x$) and suppose an integer z. If there is a subset of W_i so that the sum equivalent to integer z. That is equal to verify if there is a set of integer ($v_1,\ldots..,v_x$) where $z=\sum_{i=1}^{x} w_i v_i$ so that $v_i \in (0,1)$ with $1 \le i \le x$ A subset sum problem is the decision problem that is NP-complete [5].

Definition 2: A set ($w_1,\ldots..,w_x$) of numbers is the super-increasing sequence, when $w_i > \sum_{j=1}^{i-1} w_j$ for every $i \ge 2$. However, the greedy algorithm to solve a subset sum problem when w_i is the super-increasing sequence. Subtract a largest number from integer Z and repeat. The following method usefully resolves a subset sum problem for super-increasing sequence in a polynomial time.

Algorithm 1: Solving the super-increasing subset sum problem.

Input: The sequence ($w_1,\ldots..,w_x$) of integer which is a sum of the subset of w_i, and an integer z.

Result: $(v_1,\ldots,v_x)$ with $v_i \in (0,1)$, where $z=\sum_{i=1}^{x} w_i v_i \cdot i := x;$

While $i \geq 1$ do
{
If $z \geq w_i$ then
{
$v_i := 1;$
$z := z - w_i;$
}
Else
{
$v_i := 0;$
$i := i - 1;$
}
} repeat
Return $(v_1, ..., v_x);$

Definition 3: The set of positive values (w_1,…..,w_x) and a number *r*are provided. If there is the subset of w_i where the result equals to *r*, specifically determine if there are values (v_1,…..,v_x) where $r = \prod_{i=1}^{x} w_i^{v_i}$ Such that $v_i \in (0,1)$ where $1 \leq i \leq x$ A subset product problem is the decision problem. As noted in [7,8], when w_i are short primes and less than *r*, the difficulty is solved in polynomial time by factoring *r*. The product can be reviewed in the following theorem.

Theorem 1: When (w_1,…..,w_x) are short primes, it can be solving a subset problem in polynomial time.

Proof: As w_i are short primes and $v_i \in (0,1)$ then:

If $\gcd(r, w_i) = w_i$ $\quad v_i = 1$

Or if $\gcd(r, w_i) = 1$ $\quad v_i = 0$

Definition 4: Assume q be prime, a primitive element $w \in Z_q^*$ and an integer $f \in Z_q^*$. Compute element *v* where $0 \leq v \leq q-2$, so that $w^v = f \bmod q$. This is the discrete logarithm problem.

The ElGamal Scheme

The ElGamal scheme is a public key scheme relied on a discrete logarithm problem. Suppose q is a prime number where a discrete logarithm problem is infeasible, and assume that $a \in Z_q^*$ is a generator. Every user chooses an arbitrary integer *w* where $1 \leq w \leq q-2$, and find $f = a^w \bmod q$. Then (q, w, f) is public key and *w* is private key. Assume that we desire to transmit the message *v* to receiver. First, we choice a random element *S* so that $1 \leq w \leq q-2$. Then we find $p_1 = w^s \bmod q$ and $p_2 = v \cdot f^s \bmod q$. We pass the encrypted message (p_1,p_2) to a receiver. The encryption process in ElGamal scheme is probabilistic, since an encrypted message relies on both a message *v* and on a random integer *S* selected by user. To decrypt message *v* from encrypted message *m*, receiver should uses a private-key *w* and find $v = p_2 (p_1^w)^{-1} \bmod q$.

Cipher Text-Only Attack

The cipher text-only attack is the situation in which a hacker attempts to determine a private key by only intercepted a cipher-text or decrypt cipher-text as a challenge. Every encryption scheme weak to this sort of attack and is considered entirely vulnerable.

Hacker knowledge: given $g_1 = (v_1, e)$ and $g_2 = (v_2, e)$.

Hacker purpose: get v_1,v_2,…..or a private key *d*.

Akleylek, et al. Scheme

In this section, we describe the Akleylek, et al. scheme. We aim to multiply the security of a proposed scheme by combing ElGamal scheme and knapsack scheme.

Key Generation

1. Every user selects the super-increasing sequence (w_1,…..,w_x), so that $w_i > \sum_{i=1}^{j-1} w_i$, with $2 \leq j \leq x$, and w_i are integer values.
2. The keys of ElGamal (q, a, w, f) scheme are computed.
3. To computing public knapsack e=(c_1,……,c_x), randomly choice integer *S* with $1 \leq s \leq q-1$ and do the following:

$$f = a^w \bmod q$$
$$z_i = a^s \bmod q$$
$$k_i = f^s \cdot w_i \bmod q$$
$$c_i = (z_i, k_i)$$
$$e = ((z_1, k_1), ..., (z_x, k_x))$$
$$d = (f, a, q, w, (w_1, ..., w_x))$$

Encryption

To encrypt *x*-bit binary message *v*=(v_1,……,v_x), user should do the following

1. Find $m = (p_1, p_2) = \prod_{i=1}^{x} (z_i, k_i)^{v_i}$ [Eq-1]
2. Send encrypted message *m* to a receiver.

Decryption

To decrypt an encrypted message *m*, a receiver finds:

$$r = p_2 (p_1^{-1})^w \bmod q$$
$$= \frac{\prod_{i=1}^{x} (k_i)^{v_i}}{\prod_{i=1}^{x} (z_i^w)^{v_i}} \bmod q$$
$$= \prod_{i=1}^{x} w_i^{v_i} \bmod q$$

Remarks

1. $k_i = f^s * w_i \bmod q = a^{s \cdot w} \cdot w_i \bmod q = (z_i^w) w^i \bmod q$.
2. Upon finding *r*, we should get message *v*=(v_1,……,v_x) from $r = w_1^{v_1} \cdot w_2^{v_2}, ..., w_x^{v_x}$
3. We have $r = \prod_{i=1}^{x} w_i^{v_i}$ with w_1,……,w_x is a super-increasing sequence.
4. From Theorem 1, if w_i are short primes, we can compute v_i from *r*, else, a problem stays NP-complete and we cannot solve this difficulty.
5. In practice, Akleylek, et al., scheme is entirely unrealistic.

Cryptanalysis of Akleylek, et al. Scheme

In this section, we illustrate that Akleylek, et al., scheme is defenseless to cipher text-only attack. However, we can find message from an encrypted message text as follows.

Assume $m = (p_1, p_2)$ is a challenge cipher text encrypted with Akleylek, et al., scheme and we aim to discover a related message. From [Eq-1], we have

$$m = (p_1, p_2)$$
$$= \prod_{i=}^{x} (z_i, k_i)^{v_i}$$
$$= (z_1, k_1)^{v_1} ... (z_x, k_x)^{v_x}$$

The element $z_i = a^s \bmod q$ of a public-key is constant for every *i*, and we can let $z_i = b$ with $1 \leq i \leq x$. We have

$$p_1 = \prod_{i=1}^{x} z_i^{v_i} = b^{\sum_{t=1}^{x} v_t} = b^y \quad \text{[Eq-2]}$$

With $y = \sum_{i=1}^{x} v_i$ is a Hamming weight of a binary message $v=(v_1, \ldots\ldots, v_x)$. From [Eq-2], we can find Hamming weight y of message $(v_1, \ldots\ldots, v_x)$. Thus, we know number of v_i with $v_i=1$. From [Eq-1], we have $p_2 = \prod_{i=1}^{x} k_i^{v_i}$. Thus, we know number of k_i and the result of them matches p_2. To find these k_i, we must obtain a y-tuple subset of $k_1, \ldots, k_x$ from public key $((*, k_1), \ldots, (*, k_x))$ so that the result of them equal to p_2. We indicate this subset by n. We can select y values of $k_1, \ldots, k_x$ in $\binom{x}{y}$ ways. Thus, we require at most $\binom{x}{y}$ bit processes to obtain such subsets. When finding these k_i, we can find an original message from $v_i = 1$ when $k_i \notin n$ else = 0. We have $\binom{x}{y} = \frac{x(x-1)\ldots(x-y+1)}{y(y-1)\ldots1} < \frac{x^y}{y!} < x^y$ Therefore, a complexity of attack is $O(x^y)$.

The Proposed Scheme

This scheme is relied on multiplicative knapsack problem. The encrypted message is found by multiplying a public key and a message is retrieved by factoring an encrypted message raised to the secret power.

Key Generation

Each user should do the following:

1. Choose a prime q.
2. Verify an integer x where $q > \prod_{i=1}^{x} q_i$ with q_i is begin from $q_1 = 2$
3. Arbitrarily select elements w,s so that $1 < w, s < q-1$
4. Find $f = a^w \bmod q$
5. Find $z_i = a^s \bmod q$
6. Find $k_i = f^s p_i \bmod q$
7. Verify $c_i = (z_i, k_i)$
8. Determine $(x, q(c_1, \ldots, c_x))$ is a public key and (f, w, a, s) is a private key.

Encryption

To encrypt *x-bit* binary message $v=(v_1, \ldots\ldots, v_x)$, we calculate:

1. $m = (p_1, p_2) = \prod_{i=1}^{x} (z_i, k_i)^{v_i} \bmod q$
2. Pass encrypted message m to a receiver.

Decryption

To decrypt message v from encrypted message m, a receiver must do the following:

1. Find $r = p_2 (p_1^{-1})^w \bmod q$
$$= \frac{\prod_{i=1}^{x} (k_i)^{v_i}}{\prod_{i=1}^{x} (z_i^w)^{v_i}} \bmod q$$
$$= \prod_{i=1}^{x} p_i^{v_i} \bmod q$$
2. While $q > \prod_{i=1}^{x} q_i$ with $v_i \in (0,1)$ therefore $\prod_{i=1}^{x} q_i^{v_i} \bmod q = \prod_{i=1}^{x} q_i^{v_i}$ and thus $r = \prod_{i=1}^{x} q_i^{v_i}$
3. Since $v_i (0,1)$ so r is a result of some distinct primes q_i.
4. By Theorem 1, we achieve that $v_i = 1$ when q_i / r else $v_i = 0$.

Result and Discussion

In the proposed scheme, we have

1. $p_1 = \prod_{i=1}^{x} z_i^{v_i} \bmod q = b^{\sum_{i=1}^{x} v_i} \bmod q = b^y \bmod q$, with $y = \sum_{i=1}^{x} v_i$ and $b = z_i = a^s \bmod q$.
2. As discrete logarithm problem is difficult. Thus, we cannot verify Hamming weight y from $p_1 = b^y \bmod q$ and so, a proposed attack is not possible in this case.

Birthday Attack

When a prime q is selected small, then x is also small. Therefore, q should be adequately large in order to avoid birthday-search over two the lists A and B of $2^{x/2}$ components to obtain a couple of sets where $\prod_{i \in A} k_i = (\prod_{i \in B} k_i)^{-1} \cdot p_2 \bmod q$

Conclusions

In this paper, we propose the hybrid public key encryption. This scheme uses ElGamal scheme in a key generation algorithm for hiding a secure knapsack secret key and to make a public knapsack key. We illustrate that this combination discloses a security and becomes a scheme vulnerable to cipher text-only attack. To prevent this attack, we calculate a cipher text mod large prime q. Furthermore, we proved that a proposed scheme is unfeasible. We adapted this scheme for enhancing security and efficiency. In this case, when individual desires to break a scheme, should find discrete logarithm problem which is intractable.

References

[1] Akleylek S., Emmungil L. and Nureyev U. (2007) *Journal of Application Computer Math*., 6(22), 258-264.

[2] ElGamal T. (1985) *IEEE Transactions on Information Theory*, 31(4), 469-472.

[3] Ronald Cramer and Victor Shoup (2004) *SIAM Journal on Computing*, 33(1), 167-226.

[4] Dennis Hofheinz and Eike Kiltz (2007) *Advances in Cryptology, Lecture Notes in Computer Science*, 4622, 553-571.

[5] Yuan Chen, Xiaofeng Chen and Hui Li (2012) *Proceedings of the Fourth International Conference on Intelligent Networking and Collaborative Systems*, 264-269.

[6] Shabnam Parveen and Priyanka Gandhi (2012) *International Journal of Engineering Research and Applications,* 2(4), 873-876.

[7] Merkle R. and Hellamn M. (1978) *IEEE Transactions on Information Theory*, 24, 525-530.

[8] Markku-Juhani Saarinen (2012) *IEEE Symposium on Security and Privacy Workshops*, 27-32.