Security on a Knapsack-Type Encryption Scheme Based upon Hybrid-Model Assumption

Zhengping Jin[1], Hong Zhang[2], and Zhongxian Li[3]
(Corresponding author: Zhengping Jin)

State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications[1]
Beijing 100876, China
National Computer Network Emergency Response Technical Team Coordination Center of China[2]
Beijing 100029, China
National Cybernet Security Limited, Tianjin 300384, China[3]
(Email: zhpjin@bupt.edu.cn)

(Received Apr. 17, 2016; revised and accepted June 16 & July 19, 2016)

Abstract

Provable security is a reduction that breaking the scheme is usually reduced to solving some basic hard problems, thus the foundation of the scheme's security is the assumption that it is hard to solve the based problems. Due to most existing schemes are founded on single assumption, some encryption schemes, whose security are based on multiple assumptions, have been proposed. Recently, Su and Tsai constructed a knapsack-type encryption scheme based on hybrid-model, and proved it should be more secure than schemes based on single assumption. In this paper, we find that this scheme actually cannot reach the security as claimed. By launching the known message attack, we show Su and Tsai's encryption scheme cannot provide confidentiality, for the adversary could decrypt any ciphertext in this cryptosystem if one of the assumptions does not hold.

Keywords: Confidentiality; Hybrid Problems; Knapsack Cryptosystem; Provable Security

1 Introduction

Provable security was first introduced by Goldwasser and Micali [4] in the particular context of asymmetric encryption. Its main idea comes from proofs by contradiction in Mathematics, which is a reduction as follows [14]. At first, take some goal for a scheme, such as achieving privacy via encryption. Then, make a formal adversarial model according to the adversary's ability, and define what it means for a scheme to be secure.

With this in hand, a particular scheme, based on some particular atomic primitive, can be analyzed from the point of view of meeting the definition. Eventually, one shows that the scheme works via a reduction. The reduction shows that the only way to defeat the scheme is to break the underlying atomic primitive [1, 7]. Therefore, the atomic primitive, which may be some basic mathematical problem, is the foundation of the security for intended scheme.

Since the concept of provable security was proposed, a large number of works have been made, including many delicate encryption designed and proved in formal security model [6, 8]. However, the security of most existing schemes is founded on just one cryptographic assumption, such as factoring, discrete logarithm (DL) problem [11], elliptic curve discrete logarithm problem (ECDLP) [12], etc. Though these assumptions appear reliable now, it is possible that efficient algorithms will be sooner or later developed to break one or more of them. It is unlikely that multiple cryptographic assumptions would simultaneously become easy to be solved. Thus, several cryptographic systems' security is reduced to solving multiple hard problems at the same time.

In 1994, Harn [5] first developed a public key cryptosystem based on multiple cryptographic assumptions, intractability of factoring [3] and DL problems [10]. Recently, Su and Tsai [13] presented an encryption scheme based on the linearly shift knapsack and elliptic curve cryptosystem, and claimed that it is secure based on the hardness of the linearly shifting knapsack problem and ECDLP, for one possible hope to break the proposed system might be to solve both of the problems.

In this paper, we cryptanalyze Su and Tsai's knapsack-type encryption scheme, and find it is not really secure as claimed. Concretely, with one pair of message and ciphertext in hands, the adversary could decrypt any ciphertext in this cryptosystem, if one of the assumptions, i.e. the linearly shifting knapsack problem is hard, does not hold, which consequently breaks its security based on multiple assumptions.

The rest of this paper is organized as follows. Some preliminary works are given in Section 2. Then, Su and Tsai's knapsack-type encryption scheme is recalled and our attack on its security is described in Section 3. Finally, some conclusions are drawn in Section 4.

2 Preliminaries

In this section, we briefly review some basic concepts used in this paper, including bilinear pairings, the knapsack problem, the linearly shift knapsack algorithm and the computational knapsack Diffie-Hellman problem.

2.1 Bilinear Pairings

Let $\mathbb{G}$ and $\mathbb{G}_T$ be groups of prime order q and P be a generator of $\mathbb{G}$. The map $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ is said to be an admissible bilinear pairing if the following three conditions hold true:

1) Bilinearity: for all $a, b \in \mathbb{Z}_q$, we have $e(aP, bP) = e(P, P)^{ab}$.

2) Non-degeneracy: $e(P, P) \neq 1_{\mathbb{G}_T}$.

3) Computability: e is efficiently computable.

It is noted that the map e is symmetric since $e(aP, bP) = e(P, P)^{ab} = e(bP, aP)$ and we refer reader to [2] for more details on the construction of such pairings.

2.2 Knapsack Problem

The knapsack problem is a typical problem of combinatorial optimization, and 0/1 knapsack problem is one of the most basic cases, which is presented as follows [13].

- Problem instance:
  $K = (k_1, k_2, \cdots, k_n, t)$, where $k_1, k_2, \cdots, k_n$ and t are positive integers. $k_1, k_2, \cdots, k_n$ are called sizes and t is called the target sum.

- Question:
  Is there a 0-1 vector $S = (x_1, x_2, \cdots, x_n)$ such that $\sum_{i=1}^{n} x_i k_i = t$?

It is easy to solve the knapsack problem when $(k_1, k_2, \cdots, k_n)$ is a superincreasing sequence, in which the next term of the sequence is greater than the sum of all preceding terms. However, it is assumed that the knapsack problem for the general case cannot be solved in probabilistic polynomial time (PPT).

2.3 Linearly Shift Knapsack Cryptosystem

Based on Laih et al's method [9], Su and Tsai [13] proposed the high density knapsack algorithm and the linearly shift knapsack algorithm described as follows, which are used to generate the system parameters of their encryption scheme.

- High density knapsack algorithm:

  Step 1: Let $\overline{a} = (a_1, a_2, \cdots, a_n)$ be a superincreasing sequence, and select two integers w, m satisfying $\gcd(w, m) = 1$, where $m > \sum_{i=1}^{n} a_i$.

  Step 2: Calculate the original enciphering keys $b_i \equiv a_i \times w \mod m$ for all i.

  Step 3: Compute the high density sequence $\overline{b'} = (b'_1, b'_2, \cdots, b'_n)$, where $b'_i \equiv b_i \mod w$, then $b'_i < w$ for all i.

  Step 4: Calculate $\overline{c} = (c_1, c_2, \cdots, c_n)$, where $c_i = \lfloor b_i / w \rfloor$, then $0 \leq c_i \leq v$, and compute the deciphering keys $a'_i = a_i - c_i$, where $v = \lfloor m/w \rfloor$ (here $\lfloor x \rfloor$ is a floor function, representing the largest integer value smaller than x).

- Linearly shift knapsack algorithm:

  Step 5: As high density knapsack algorithm, calculate a high density knapsack sequence $\overline{b'} = (b'_1, b'_2, \cdots, b'_n)$.

  Step 6: Choose a random binary sequence $\overline{t} = (t_1, t_2, \cdots, t_n)$, and an integer k with $0 < k < \min\{b'_i\}$ for $t_i = 1$. Then b'_i are linearly shifted by performing $e_i = b'_i - kt_i$ and $\overline{e} = (e_1, e_2, \cdots, e_n)$ which is published as the public enciphering key.

3 Chosen Plaintext Attack on Su and Tsai's Encryption Scheme

To analyze the security of Su and Tsai's encryption scheme [13], we first recall their descriptions as follows.

System setup:

The receiver Alice selects the domain parameters which are comprised of:

- The field order q.
- Two coefficients $a, b \in F_q$ that define the equation of the elliptic curve E over F_q.
- The number of points in $E(F_q)$, denoted as $\sharp E(F_q)$.
- Two field elements x_P and y_P in F_q that define a finite point $P = (x_P, y_P)$. P has a prime order q' and is called the base point.
- A one-way hash function $f()$.
- Parameters $(w, m, k, r_A, \overline{a})$ as his private keys, where $m < q', r_A \in \mathbb{Z}^*_{q'}$.
- A random binary sequence $\overline{t}$.
- Public keys $\overline{e} = (e_1, e_2, \cdots, e_n)$ and $Q_A = r_A P$.

Encryption:

To encrypt the message $\overline{x}$ to Alice, Bob picks up his secret key r_B, publishes his public key $Q_B = r_B P$ and computes the ciphertext pair message $\overline{x}$ using Alice's public keys $\overline{e} = (e_1, e_2, \cdots, e_n)$ and Q_A. The encryption phase is as follows:

- Bob encodes the plaintext message
$$\overline{x} = (x_1, \cdots, x_n),$$
where $x_i = 0$ or 1, for $i = 1, 2, \cdots, n$.
- Produces the ciphertext
$$E(\overline{x}) = ((k_1, k_2) + r_B Q_A),$$
where $k_1 = \sum_{i=1}^{n} x_i e_i, k_2 = f(Q_A, Q_B)$.
- Sends $E(\overline{x}) = ((k_1, k_2) + r_B Q_A)$ to Alice.

Decryption:

To receive the ciphertext $E(\overline{x})$, Alice computes with his secret key r_A and Bob's public information Q_B. To decrypt the knapsack value, Alice multiplies the Bob's public point using his secret key r_A and subtracts the result from $E(\overline{x})$:

$$D(E(\overline{x})) = (k_1, k_2) + r_B Q_A - r_A Q_B.$$

Before computing the knapsack value, Alice needs to verify whether k_2 is sent from Bob by checking $k_2 \overset{?}{=} f(Q_A, Q_B)$ and computing k_1 which should be the plaintext point, corresponding to the message bit is 1.

Once Alice, knowing the private key w^{-1}, can remove $k_1 = \sum\limits_{i=1}^{n} x_i e_i$ from the ciphertext, and hence retrieve the plaintext information $\overline{x}$:

Since

$$\begin{aligned} s \times w^{-1} &\equiv \left(\sum_{i=1}^{n} b_i' x_i\right) \times w^{-1} \mod m \\ &\equiv \sum_{i=1}^{n} (e_i + k t_i) x_i \times w^{-1} \\ &\equiv k_1 \times w^{-1} + k w^{-1} \times \sum_{i=1}^{n} t_i x_i \mod m \end{aligned}$$

and $0 \leqslant \sum\limits_{i=1}^{n} t_i x_i \leqslant \sum\limits_{i=1}^{n} t_i \leqslant n$, Alice can obtain the correct $s \times w^{-1} \mod m$ at most $y + 1 \leqslant n + 1$ times and get $\overline{x}$ from $s \times w^{-1}$ by his superincreasing sequence $\overline{a} = (a_1, a_2, \cdots, a_n)$, for $s \times w^{-1} = \sum\limits_{i=1}^{n} a_i x_i$. The correctness can be easily verified through normal enciphering procedures with the corresponding retrieved $\overline{x}$ by checking $\sum\limits_{i=1}^{n} x_i e_i \overset{?}{=} k_1$, as it is assumed that the system is one-to-one.

Su and Tsai [13] heuristically analyzed the security of their encryption scheme, and claimed that, one possible hope to break their cryptosystem might be to solve the linearly shifting knapsack problem and the elliptic curve cryptography system simultaneously, which is computationally infeasible for the opponents.

However, we will show that, if one adversary could only solve the linearly shifting knapsack problem but not the ECDLP, it might endanger the security of their scheme, which means it's not really secure based on hybrid-model assumption. Su and Tsai [13] defined the security of a cryptosystem that is evaluated by the amount of time needed to break it, where breaking a cryptosystem means finding the private key used to encrypt a message. However, it is also a fatal destruction for some flawed encryption schemes that any adversary can obtain the plaintext or parts of plaintext from ciphertext without the help of the private key. So what is a secure encryption scheme? It is not an easy question to answer. In fact, a widely accepted security property for encryption is the ciphertext indistinguishability [8], which is very important for maintaining the confidentiality of encrypted communications. Intuitively, if a cryptosystem possesses the property of indistinguishability, then an adversary will be unable to distinguish pairs of ciphertexts based on the message they encrypt. Furthermore, according to the adversary's capability, the security property for encryption can be divided into indistinguishability under chosen plaintext attack(IND-CPA), chosen ciphertext attack(IND-CCA1) and adaptive chosen ciphertext attack(IND-CCA2). IND-CPA is considered a basic requirement for most provably secure public key cryptosystems, though some schemes also provide stronger security that are IND-CCA1 and IND-CCA2. In the following, we show that Su and Tsai's scheme cannot provide the property of IND-CPA, to say nothing of IND-CCA1 or IND-CCA2. More exactly, with an assumed algorithm that can solve the linearly shifting knapsack problem, the adversary can decrypt any ciphertext from Bob to Alice if he successfully gets a corresponding ciphertext to his chosen message, which contradicts Su and Tsai's claim.

Once the adversary got the ciphertext for some message $\overline{x} = (x_1, \cdots, x_n)$, denoted as σ, he could calculate

$$r_B Q_A = \sigma - (k_1, k_2),$$

where $k_1 = \sum\limits_{i=1}^{n} x_i e_i, k_2 = f(Q_A, Q_B)$. Then, for arbitrary ciphertext σ^* from Bob to Alice, the adversary could compute

$$D(E(\overline{x}^*)) = \sigma^* - r_B Q_A = (k_1^*, k_2^*)$$

without any part of Alice or Bob's secret key r_A or r_B, where $\overline{x^*} = (x_1^*, \cdots, x_n^*)$ is the intended plaintext and $k_1^* = \sum\limits_{i=1}^{n} x_i^* e_i$ is its corresponding knapsack sum. Consequently, the adversary could get the plaintext $\overline{x^*}$ from k_1^* according to the assumed algorithm of solving the linearly shifting knapsack problem.

During the whole attacking process above, no algorithm concerning the ECDLP is needed, but the value related to Alice's secret key r_A is leaked in a sense. Therefore, their proposal is actually not a secure encryption scheme that couldn't be broken unless the linearly shifting knapsack problem and the ECDLP were solved simultaneously. In other words, its security is only based on the hardness of the linearly shifting knapsack problem.

4 Conclusions

We have made the cryptanalysis of Su and Tsai's knapsack-type encryption scheme based on hybrid-model problems, and launched a chosen plaintext attack to show it does not satisfy the enhanced security depends on the computational complexity of multiple assumptions. Therefore, to the best of our knowledge, it remains on its way to construct really secure encryption scheme based on hybrid-model problems.

Acknowledgments

This work is supported by NSFC (Grant Nos. 61502044, 61300181), the Fundamental Research Funds for the Central Universities (Grant No. 2015RC23).

References

[1] M. Bellare, "Practice-oriented provable-security," *Lectures on Data Security*, vol. 1561 of LNCS, pp. 1–15, 2003.

[2] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Advances in Cryptology (Crypto'01)*, vol. 2139 of LNCS, pp. 213–229, Springer-Verlag, Berlin, 2001.

[3] C. C. Chang, M. S. Hwang, "Parallel computation of the generating keys for RSA cryptosystems," *Electronics Letters*, vol. 32, no.15, pp. 1365–1366, 1996.

[4] S. Goldwasser and S. Micali, "Probabilistic encryption," *Journal of Computer and System*, vol. 28, no. 2, pp. 270–299, 1984.

[5] L. Harn, "Public-key cryptosystem design based on factoring and discrete logarithms," *IEE Proceedings - Computers and Digital Techniques*, vol. 141, pp. 193–195, 1994.

[6] Z. P. Jin, Q. Y. Wen, and H. Z. Du, "An improved semantically-secure identity-based signcryption scheme in the standard model," *Computers & Electrical Engineering*, vol. 36, no. 3, pp. 545–552, 2010.

[7] A. Kartit, H. K. Idrissi, and M. Belkhouraf, "Improved methods and principles for designing and analyzing security protocols," *International Journal of Network Security*, vol. 18, no. 3, pp. 523–528, 2016.

[8] J. Katz and Y. Lindell, *Introduction to Modern Cryptography: Principles and Protocols*, Chapman & Hall/CRC, 2007.

[9] C. S. Laih, J. Y. Lee, L. Harn, and Y. K. Su, "Linearly shift knapsack public-key cryptosystem," *IEEE Journal of Selected Areas in Communications*, vol. 7, no. 4, pp. 534–539, 1989.

[10] C. C. Lee, M. S. Hwang, L. H. Li, "A new key authentication scheme based on discrete logarithms," *Applied Mathematics and Computation*, vol. 139, no. 2, pp. 343–349, 2003.

[11] L. H. Li, S. F. Tzeng, M. S. Hwang, "Generalization of proxy signature-based on discrete logarithms," *Computers & Security*, vol. 22, no. 3, pp. 245–255, 2003.

[12] L. Liu and Z. Cao, "A note on efficient algorithms for secure outsourcing of bilinear pairings," *International Journal of Electronics and Information Engineering*, vol. 5, no. 1, pp. 30–36, 2016.

[13] P. C. Su and C. H. Tsai, "New cryptosystems design based on hybrid-mode problems," *Computers & Electrical Engineering*, vol. 35, no. 3, pp. 478–484, 2009.

[14] Y. Zhang, H. Li, X. Li, and H. Zhu, "Subliminal-free Variant of Schnorr Signature with Provable Security," *International Journal of Electronics and Information Engineering*, vol. 3, no. 1, pp. 19–30, 2015.

Biography

Zhengping Jin, received his B.S. degree in Mathematics and Applied Mathematics and his M.S. degree in Applied Mathematics from Anhui Normal University, Wuhu, Anhui, China, in 2004 and 2007, respectively, and his Ph.D. degree in Cryptography from Beijing University of Posts and Telecommunications, Beijing, China, in 2010. Currently, he is an associate professor in the State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications. His research interests include design and analysis of cryptographic protocols, and security in cloud computing.

Hong Zhang, received his B.S. degree in Automatic Control and his M.S. degree in System Engineering from Xian Jiaotong University, Xian, Shaanxi, China, in 1998 and 2001, respectively, and his Ph.D. degree in Computer Network from Institute of Computing Technology, Chinese Academy of Science, Beijing, China, in 2004. Currently, he is a senior engineer in CNCERT/CC. His research interests include cloud computing, software engineering and network security.

Zhongxian Li, received his B.S. degree in Mathematics and his M.S. degree in Number Theory from Zhengzhou University in 1984 and 1987, respectively, and his Ph.D. degree in Signal and Information Processing from Beijing University of Posts and Telecommunications, Beijing, China, in 1999. Currently, his research interests include network and information security, virtual desktop and security in cloud computing.