Joint Conference of 1996 International Computer Symposium
December 19~21, Kaohsiung, Taiwan, R.O.C.

Zero-Knowledge Interactive Proof Schemes Based on Subset Sum Problem

Chi-Sung Laih, Wen-Chung Kuo and M. J. Gau
Department of Electrical Engineering
National Cheng Kung University,
Tainan,Taiwan,Republic of China
E-mail:laihcs@eembox.ncku.edu.tw

Abstract

The concept of zero-knowledge interactive proof (ZKIP) scheme was first proposed by Goldwasser, Micali and Rackoff in 1985. Since then many practical ZKIP schemes have been proposed. One common feature among all these schemes is that the security of the schemes is based on factoring or discrete logarithms. In 1991, Simmons proposes an alternative practical ZKIP scheme whose security is based on subset sum problem. However, there is a very strong assumption existed in the scheme, i.e., Simmons's scheme would be secure under the assumption that an indistinguishable box is existed. Unfortunately, nobody, including Simmons, can tell us how to implement the indistinguishable box until now. In this paper, we propose a method to implement the indistinguishable box and then two concrete ZKIP protocols whose security is based on knapsack problem are proposed. It is shown that the proposed indistinguishable box is very simple, flexible and secure in the applications of ZKIP protocols.

Key words: ZKIP protocols, identification, cryptography, digital signature.

1 Introduction

In 1985, the concept of zero-knowledge interactive proof (ZKIP) scheme was first proposed by Goldwasser, Micali and Rackoff [6]. A ZKIP protocol is a protocol such that prover P can convince verifier V about the validity of the secret (or witness). P knows while V learns nothing (zero knowledge) about P's secret after the protocol is completed. Goldwasser *et al.* pointed out that a ZKIP scheme must satisfy the following conditions.

1. **Completeness:** If P and V are honest and follow the protocol, then there is a very large probability that V believes P with the secret.
2. **Soundness:** If P is dishonest and V is honest in the protocol, then there is very large probability that V does not believe P with the secret.
3. **Witness hiding:** P cannot reveal any information about his/her secret to V, i.e., V is not able to learn anything from P even if P is honest.

Since then, many ZKIP schemes have been developed by using different mathematical assumptions, e.g., discrete logarithms or factoring. Among them, Fiat and Shamir [5] proposed

the first provably and practical secure identification and signature scheme (the well-known FS scheme) whose security is based on the difficulty of computing square roots modulo a composite n when the factorization of n is unknown. A faster ZKIP scheme whose security is also based on the difficulty of factorization problem is developed by Guillow and Quisquster [7]. Here, their scheme is called GQ scheme. GQ scheme is faster than FS scheme by a factor of three in the computation required. Therefore, GQ scheme is more suitable for the applications of smart cards.

Independently, another practical ZKIP scheme based on the discrete logarithms problem had also been developed by Chaum *et al.* [2]. Chaum *et al.* presented an improved identification scheme [3] based on some generalizations of discrete logarithms problem, e.g., multiple discrete logarithms, relaxed discrete logarithms and simultaneous discrete logarithms. Later, an identification scheme based on the concept of ZKIP and ElGamal scheme [4] was developed by Beth [1]. It is also claimed that the scheme was also suitable for the applications of the smart cards.

Recently, Simmons [10] proposed a new ZKIP scheme whose security is based on another cryptographic assumption, i.e., the subset sum problem (or knapsack problem). However, Simmons gave nothing about how to implement his ZKIP scheme since there needs an indistinguishable box satisfying homomorphism under addition operations in his ZKIP protocol. In this paper, we will propose two methods to implement the indistinguishable box satisfying homomorphism under addition operations, and use the proposed boxes to implement the Simmons's ZKIP scheme.

The rest of the paper is organized as follows. In Section 2, we first review the Simmons's scheme briefly. In Section 3, a concrete implementation of Simmons's ZKIP scheme is proposed. The security analysis of the proposed ZKIP is also included. An another effective ZKIP scheme whose security is also based on the knapsack problem is also proposed in Section 4. Finally, we make some conclusions in Section 5.

2 Review of Simmons's Scheme

Before presenting our implementation, we will give a brief description on the Simmons's scheme [10] in this section.

2.1 The Subset Sum Problem

Firstly, we introduce the subset sum problem (or knapsack problem) before we discussed the Simmons's scheme. In general, subset sum problem can be defined as follows:[8]
Given a set of values, U_1, U_2, $\cdots$, U_n, S and then compute x_1, x_2, $\cdots$, x_n, $x_i \in \{0,1\}$ for all $1 \leq i \leq n$, such that

$$S = x_1U_1 + x_2U_2 + \cdots + x_nU_n.$$

It is well-known that the knapsack problem is an *NP-complete* problem, i.e., given $\underline{\mathbf{U}} = \{U_1, U_2, \cdots, U_n\}$ and S, it is computationally infeasible for anyone to compute $\underline{\mathbf{X}} = \{x_1, x_2, \cdots, x_n\}$, $x_i \in \{0,1\}$ for all $1 \leq i \leq n$, such that $S = \underline{\mathbf{X}} \cdot \underline{\mathbf{U}}$.

2.2 The Simmons's Scheme

Given a public sequence $\underline{\mathbf{A}} = \{a_1, a_2 \cdots, a_n\}$, assume P (the prover) has secret $\underline{\mathbf{X}} = \{x_1, x_2, \cdots, x_n\}$ with weight $W(\underline{\mathbf{X}}) = \frac{n}{2}$ such that P's public key S satisfying $S = \sum_i x_i a_i = \underline{\mathbf{X}} \cdot \underline{\mathbf{A}}$. Let g be an indistinguishable box satisfying $g(\underline{\mathbf{X}} \cdot \underline{\mathbf{A}}, k) = \underline{\mathbf{X}} \cdot g(\underline{\mathbf{A}}, k) = \sum_i x_i g(a_i, k)$, where k is a random number. Let Ω be the set of permutation of n elements. Obviously, the cardinality

of the set Ω is $n!$. Simmons's ZKIP protocol can be described as follows.

Simmons's ZKIP protocol

Repeat the following steps t times.

1. P randomly chooses a permutation $\pi \in \Omega$ and a random integer k, then P finds $\underline{\mathbf{A}}' = \{g(a_i, k) | a_i \in \underline{\mathbf{A}}\}$.
2. P sends $\pi(\underline{\mathbf{A}}')$ and $S' = g(S, k)$ to V (the verifier).
3. V asks P to do the following two things by $b = 0$ or $b = 1$.
   - When $b = 0$: P sends k to V, and V checks whether $g(a_i, k) \in \pi(\underline{\mathbf{A}}')$ for all $a_i \in \underline{\mathbf{A}}$ and $g(S, k) = S'$ are satisfied or not.
   - When $b = 1$: P sends $\pi(\underline{\mathbf{X}})$ to V, and V check whether $\pi(\underline{\mathbf{X}}) \cdot \pi(\underline{\mathbf{A}}') = S'$ is satisfied or not.

If the condition is hold for all t times, then V accepts that P is honest, i.e., P knows the secret $\underline{\mathbf{X}}$. Otherwise, P is an impostor. The probability that V accepts P who is an impostor is at most 2^{-t}.

3 The Implementation of Simmons's ZKIP Scheme

Although Simmons had shown that his scheme is a ZKIP scheme in [10]. However, the security of the Simmons's scheme is based on the assumption that the indistinguishable box exists. Unfortunately, nobody including Simmons can tell us how to implement the indistinguishable box, i.e., the function g such that $g(\underline{\mathbf{X}} \cdot \underline{\mathbf{A}}, k) = \sum_i x_i g(a_i, k)$ and we cannot distinguish a_i from $g(a_i, k)$ when $\underline{\mathbf{A}} = \{a_1, a_2 \cdots, a_n\}$ is given and k is unknown. Here we try to propose two concrete implementations of indistinguishable box such that above conditions are satisfied. The first proposed function is that $g(a_i, k) = (a_i k \bmod p) \bmod q$, where p and q are primes with $2n$ bits and n bits, respectively, a_i $(1 \leq i \leq n)$ are public integers with n bits and k is a random integer with $2n$ bits. Using the indistinguishable box, we will implement Simmons's ZKIP scheme as follows.

3.1 The new scheme

Let $|y|$ denote the number of bit of an integer y, Ω denote the set of permutation of n elements and $g(\cdot, \cdot)$ be the function as defined above, i.e., the indistinguishable box needed in the Simmons's ZKIP protocol. In this scheme, a random sequence $\underline{\mathbf{A}} = \{a_1, a_2, \cdots, a_n\}$, $a_i \in (1, 2^n), 1 \leq i \leq n$, is known by all users. In addition, a prime q whose length is n is public to all users. Note that it is computationally infeasible to find the subset sum problem in $\underline{\mathbf{A}}$ since the sequence $\underline{\mathbf{A}}$ does not need any assumption, e.g., superincreasing sequence needed in Merkle-Hellman scheme [9]. Let p be a prime such that $|p| = 2|q| = 2|max\{a_i\}| = 2n$, k be a random integer such that $k \in \{1, 2, \cdots, p-1\}$. Now, we describe our concrete ZKIP protocol as follows.

Suppose P has his secret $\underline{\mathbf{X}} = \{x_1, x_2, \cdots, x_n\}$, where $x_i \in \{0, 1\}$ for all i, and P has his public information $S = \sum_{i=1}^{n} x_i a_i$. P wants to prove to V that he knows the secret $\underline{\mathbf{X}}$.

Protocol 1: Repeat the following steps t times.

1. P computes $r_i = (a_i k \bmod p) \bmod q$ for all i and $\underline{\mathbf{R}} = \pi(r_1, r_2, \cdots, r_n) = \{r'_1, r'_2, \cdots, r'_n\}$, where k and p are random integers as defined above and $\pi \in \Omega$. P also calculates $Z = (Sk \bmod p) \bmod q$.
2. P sends $\underline{\mathbf{R}}$ and Z to V.
3. V gives P a challenge with $b = 0$ or $b = 1$.

4. P sends parameters k and p to V, if $b = 0$. Otherwise, P sends $\underline{\mathbf{X}}' = \pi(x_1, x_2, \cdots, x_n) = (x'_1, x'_2, \cdots, x'_n)$ to V.

5. If $b = 0$, V checks whether $(a_i k \bmod p) \bmod q \in \underline{\mathbf{R}}$ for all i and $Z = (Sk \bmod p) \bmod q$ or not. If all of them are hold, then V can confirm that P knows exact information, otherwise P is a trickster.
   If $b = 1$, then V computes $\underline{\mathbf{X}}' \cdot \underline{\mathbf{R}} \stackrel{?}{=} Z + cq$, where $0 \le c \le \frac{n}{2} - 1$. If it is satisfied , then V can be convinced that P knows the secret $\underline{\mathbf{X}} = \{x_1, x_2, \cdots, x_n\}$ exactly. Otherwise, P is a swindler.

In Lemma 1, we will explain how V can be convinced that P knows the secret $\underline{\mathbf{X}}$.

Lemma 1: If P and V follow Protocol 1, then V always accepts the proof is valid.

Proof: Now, we divide Protocol 1 into two parts to discuss the correctness of Protocol 1 with respect to $b = 0$ or $b = 1$.

- In the case of $b = 0$:
  When P replies the correct k and p to V, then it is obviously

$$(a_i k \bmod p) \bmod q \in \underline{\mathbf{R}} \quad \text{for all } i, \qquad (1)$$

$$\text{and} \quad Z = (Sk \bmod p) \bmod q. \qquad (2)$$

  If both Eq.(1) and Eq.(2) are hold, then V can confirm that P knows exact information. Otherwise, P is a trickster.

- In the case of $b = 1$:
  After V receives $\underline{\mathbf{X}}'$ from P, the V will compute

$$\begin{aligned} \underline{\mathbf{X}}' \cdot \underline{\mathbf{R}} &= \pi(x_1, x_2, \cdots, x_n) \cdot \pi(r_1, r_2, \cdots, r_n) \\ &= \sum_{i=1}^{n} x_i r_i \\ &= \sum_{i=1}^{n} x_i [(a_i k \bmod p) \bmod q] \\ &= (\sum_{i=1}^{n} a_i x_i k \bmod p) \bmod q + cq \\ &= Z + cq, \text{ where } c = \lfloor \frac{\sum_{i=1}^{n} x_i r_i}{q} \rfloor . \quad (3) \end{aligned}$$

  Since $r_i < q$ and $x_i \in \{0, 1\}$ for all $1 \le i \le n$, we have $0 \le c < \mathrm{wt}(\underline{X}) = \frac{n}{2}$, where $\mathrm{wt}(\underline{X})$ is the weight of $\underline{X}$. If Eq.(3) holds, then V can be convinced that P knows the secret $\underline{\mathbf{X}} = \{x_1, x_2, \cdots, x_n\}$ exactly. Otherwise, P is a swindler. ∎

Now, we use Example 1 to explain Protocol 1 more clearly.

Example 1: Let $\underline{\mathbf{X}} = \{1, 1, 0, 1, 0, 0\}$, $\underline{\mathbf{A}} = \{39, 17, 32, 41, 28, 50\}$, $p = 61$ and $q = 7$. Now, we follow these information to finish the Protocol 1.

Step 1. P chooses $k = 5$ and $\pi = (135246)$. Then, P computes $r_1 = 5$, $r_2 = 3$, $r_3 = 3$, $r_4 = 1$, $r_5 = 4$, $r_6 = 6$. Therefore, $\underline{\mathbf{R}} = \{6, 4, 5, 3, 3, 1\}$, $S = 97$ and $Z = (97 \times 5 \bmod 61) \bmod 7 = 2$.

Step 2. P sends $\underline{\mathbf{R}} = \{6, 4, 5, 3, 3, 1\}$ and $Z = 2$ to V.

Step 3. P sends $k = 5$, $p = 61$ and $q = 7$ to V when $b = 0$. Otherwise, P answers $\underline{\mathbf{X}}' = \{0, 0, 1, 1, 0, 1\}$ and $q = 7$ to V.

Step 4. If $b = 0$, V checks $(39 \times 5 \bmod 61) \bmod 7 = 5$, $(17 \times 5 \bmod 61) \bmod 7 = 3$, $(32 \times 5 \bmod 61) \bmod 7 = 3$, $(41 \times 5 \bmod 61) \bmod 7 = 1$, $(28 \times 5 \bmod 61) \bmod 7 = 4$, $(50 \times 5 \bmod 61) \bmod 7 = 6$. It can be checked that all $r_i \in \underline{\mathbf{R}}$ and $(97 \times 5 \bmod 61) \bmod 7 = 2 = Z$.
If $b = 1$, then V computes

$$\begin{aligned} \underline{\mathbf{X}}' \cdot \underline{\mathbf{R}} &= (0, 0, 1, 1, 0, 1) \cdot (6, 4, 5, 3, 3, 1) \\ &= 5 + 3 + 1 = 9 = 2 + 1 \times 7, \end{aligned}$$

where $0 \le c = 1 \le \frac{6}{2} - 1 = 2$. If all of them are satisfied, then V accepts P's proof.

3.2 Security of Protocol 1

The security of our scheme is based on the following two problems. One is that knapsack problem must be *NP-complete* problem and the other is that the function g must be an indistinguishable box. The former is true since we let $\underline{\mathbf{A}} = \{a_1, a_2, \cdots, a_n\}$ be a random sequence, i.e., $\underline{\mathbf{A}}$ has no any assumption like superincreasing structure [9]. The later ought to be true since given $\underline{\mathbf{R}} = \pi(r_1, r_2, \cdots, r_n)$, where $r_i = (a_i k \bmod p) \bmod q$, finding the corresponding a_i seem to be infeasible without knowing k and p. We have implemented the low-density attack proposed by Lagrias and Odlyzko [8] for breaking any low-density knapsack problem, e.g., Merkle-Hellman knapsack public key cryptosystem [9] in our laboratory. However, it is shown that it cannot be used to attack Protocol 1 successfully. Thus, we have the following conjecture.

Conjecture: Let $\underline{\mathbf{R}} = \pi(r_1, r_2, \cdots, r_n)$, where $r_i = (a_i k \bmod p) \bmod q$, $a_i \in \underline{\mathbf{A}}$,where $\underline{\mathbf{A}}, \pi, k, p,$ and q are defined as in our scheme. Then given $\underline{\mathbf{R}}$ and q, it is infeasible to find the corresponding a_i when k and p are unknown.

Although the conjecture which can resist low-density attack does not imply it is secure. However, as far as we know, there is no obvious weakness in this conjecture. Based on above conjecture, we give the following theorem to analyze the security of our scheme.

Theorem 1:

(a). If P knows $\underline{\mathbf{X}}$, then V is always able to confirm P's identity.

(b). If P does not know the secret $\underline{\mathbf{X}}$, then the probability that V will accept P's identity in this protocol is at most 2^{-t}.

(c). V cannot learn anything from P after Protocol 1 is finished even if P is honest.

Proof:

(a). It follows from Lemma 1 directly.

(b). Similar to the proof given by Simmons, if P does not know the secret $\underline{\mathbf{X}}$ then at each time in Step 4 of Protocol 1, P cannot answer V with the exact information if P cannot guess the status of b correctly. Hence, the probability that P passes each round in Protocol 1 is at most $\frac{1}{2}$ if V is honest. Since Protocol 1 contains t independent rounds, the probability that P passes Protocol 1 is at most 2^{-t}.

(c). If P is honest, then V cannot learn any information about the secret $\underline{\mathbf{X}}$ from P regardless of the status of b.

- In the case of $b = 0$:
  V will receive parameters k and p from P, then V can get the information about permutation π from Eq.(1). However, π is a random permutation which is independent of $\underline{\mathbf{X}}$. Since V does not know $\pi(\underline{\mathbf{X}})$, thus, V knows nothing about $\underline{\mathbf{X}}$ from parameters k, p and q.

- In the case of $b = 1$:
  V knows $\underline{\mathbf{X}}' = \pi(x_1, x_2, \cdots, x_n)$. However, since V does not know the permutation π unless V can solve the subset sum problem from $\underline{\mathbf{A}}$ and S or $\underline{\mathbf{R}}$, q and Z. Thus, V knows nothing about $\underline{\mathbf{X}}$ except $|\underline{\mathbf{X}}'| = |\underline{\mathbf{X}}| = \frac{n}{2}$ if solving subset sum problem in $\underline{\mathbf{A}}$ and $\underline{\mathbf{R}}$ is infeasible. But, $|\underline{\mathbf{X}}| = \frac{n}{2}$ is known by V in advance. Hence, the witness hiding is hold.

Therefore, V is not able to learn anything from P even if P is honest. ∎

4 ZKIP Scheme Based on Subset Sum Problem With Multiplicative Property

In above section, we have proposed a new ZKIP protocol based on subset sum problem by using different modulus to implement the distinguishable box in Simmons's scheme [10]. Here, another ZKIP scheme will be developed which is also based on the same cryptographic assumption with multiplicative property to replace the function of using the different modulus. The second scheme proposed in this paper uses the multiplicative property to realize the indistinguishable box needed in Simmons's scheme. Therefore, this new scheme is not only achieving the same security as Simmons's scheme but also being a practical and flexible scheme.

4.1 Notations and Setting Up Phase

Let $p_1, p_2, \cdots, p_n$ and p be large primes known by all users in the system such that $p > p_i$ for all i and Ω be the set of permutation of n elements. P computes $M = \prod_{i=1}^{n} p_i^{x_i} \bmod p$ as his public key where $\underline{X} = \{x_1, x_2, \cdots, x_n\}$, $x_i \in \{0, 1\}$ for all i, is his secret. It is assumed that P's public key M is authenticated by V in advance.

Protocol 2: Repeat the following steps t times.

1. P randomly selects an integer $r \in Z_p \backslash \{0\}$ and computes $q_i = p_i^r \bmod p$, $M' = M^r \bmod p$ for all $1 \le i \le n$, and then P sends $\underline{Q} = \{q_1', q_2', \cdots, q_n'\} = \pi(q_1, q_2, \cdots, q_n)$ and M' to V.

2. V gives P a challenge with $b = 0$ or $b = 1$.

3. P sends some required elements to V which depends on the status of b.
   - If $b = 0$, then P answers r to V.
   - If $b = 1$, then P replies $\underline{X'} = \{x_1', x_2', \cdots, x_n'\} = \pi(x_1, x_2, \cdots, x_n)$ to V.

4. If $b = 0$, V checks whether $p_i^r \bmod p \in \underline{Q}$ for all $1 \le i \le n$, and $M^r \bmod p = M'$ or not. If they are satisfied, then V accepts P's proof. If $b = 1$, V checks whether $M' \stackrel{?}{=} \prod_{i=1}^{n} (\pi(q_i))^{\pi(x_i)} \bmod p$ or not. If it is satisfied, then V accepts P's proof.

Now, we use Lemma 2 to show the completeness of Protocol 2.

Lemma 2: If P and V are honest and follow the protocol, then V will always accept the proof is valid.

Proof: Now, we divided Protocol 2 into two classes to discuss with respect to $b = 0$ or $b = 1$.

(i). P sends r to V when the challenge is "$b = 0$". It is obvious that

$$M^r \bmod p = M', \tag{4}$$

$$\text{and } p_i^r \bmod p \in \pi(q_1, q_2, \cdots, q_n) \quad \text{for all } i. \tag{5}$$

If Eq.(4) and Eq.(5) are hold, then V can corroborate that P knows the secret exactly, otherwise V assumes that P is an impostor.

(ii). If $b = 1$, then V will receive the information $\underline{X'} = \pi(x_1, x_2, \cdots, x_n)$ from P and it is obvious that

$$\begin{aligned} \underline{Q}^{\underline{X'}} &= \prod_{i=1}^{n} (\pi(q_i))^{\pi(x_i)} \bmod p \\ &= q_1'^{x_1'} \cdot q_2'^{x_2'} \cdots q_n'^{x_n'} \bmod p \\ &\stackrel{?}{=} M' \end{aligned} \tag{6}$$

If Eq.(6) hold, then V makes certain that P knows the secret, otherwise P is a cheater. ∎

We use Example 2 to further illustrate Protocol 2.

Example 2: Let $p_1 = 5, p_2 = 7, p_3 = 11, p_4 = 13, p_5 = 17, p_6 = 19$ and $p = 101$. If $\underline{\mathbf{X}} = \{1,1,0,1,0,0\}$, then $M = 5 \times 7 \times 13 = 51 \bmod 101$. Now, the Protocol 2 runs as follows.

Step 1. P chooses $r = 3$ and $\pi = (135246)$. Then, P computes $(q_1, q_2, q_3, q_4, q_5, q_6) = (24, 40, 18, 76, 65, 92)$, $\underline{\mathbf{Q}} = \{92, 65, 24, 40, 18, 76\}$, $M' = 51^3 \bmod 101 = 38$ and then sends $\underline{\mathbf{Q}}$ and M' to V.

Step 2. P sends $r = 3$ to V when $b = 0$. Otherwise, P answers $\underline{\mathbf{X}}' = \{0,0,1,1,0,1\}$ to V.

Step 3. If $b = 0$, V checks $(5^3 \bmod 101) = 24$, $(7^3 \bmod 101) = 40$, $(11^3 \bmod 101) = 18$, $(13^3 \bmod 101) = 76$, $(17^3 \bmod 101) = 65$, $(19^3 \bmod 101) = 92$ are $\in \underline{\mathbf{R}}$ and $(51^3 \bmod 101) = 38$.

If $b = 1$, then V computes

$$\underline{\mathbf{Q}}^{\underline{\mathbf{X}}'} = 24 \times 40 \times 76 \bmod 101 \stackrel{?}{=} 38.$$

If all of them are satisfied, then V accepts P's proof.

4.2 Security of Protocol 2

The security of protocol 2 is based on the following problem.

Problem 1: Given primes $p_1, p_2, \cdots, p_n$ and p and an integer M satisfying

$$M = \prod_{i=1}^{n} p_i^{x_i} \bmod p, \qquad (7)$$

where $x_i \in \{0,1\}$ for all $1 \le i \le n$. Find $\underline{\mathbf{X}} = (x_1, x_2, \cdots, x_n)$ such that Eq.(7) is hold.

Let α be a primitive root modulo p. If discrete logarithm problem over $GF(p)$ is feasible, then there exist integers $a_1, a_2, \cdots, a_n$ and s such that

$$p_i = \alpha^{a_i} \bmod p, \text{ for all } 1 \le i \le n,$$
$$\text{and } M = \alpha^s \bmod p.$$

Then Eq.(7) can be rewritten as

$$M = \alpha^s = \prod_{i=1}^{n} p_i^{x_i} \bmod p = \prod_{i=1}^{n} \alpha^{\sum_{i=1}^{n} a_i x_i} \bmod p. \qquad (8)$$

Thus, Problem 1 can be described as that given integers $a_1, a_2, \cdots, a_n$ and its subset sum s, find $\underline{\mathbf{X}} = (x_1, x_2, \cdots, x_n)$ such that $s = \sum_{i=1}^{n} a_i x_i$. Obviously, it is a subset sum problem if discrete logarithm problem over $GF(p)$ is feasible.

We propose two possible attacks on protocol 2. Both of them can not attack protocol 2 successfully.

Attack 1: An impostor P' chooses r and π randomly, then he computes Q and M' to follow the protocol 2. If the challenge given from V is $b = 0$, then P' passes the protocol this time. However, if $b = 1$, then P' faces with Problem 1, i.e., given $\underline{\mathbf{Q}}$ and M' finding $\underline{\mathbf{X}}'$ such that $\underline{\mathbf{Q}}^{\underline{\mathbf{X}}'} = M' \bmod p$.

Attack 2: An impostor P' randomly chooses $\underline{\mathbf{Q}}$, $\underline{\mathbf{X}}'$, and M' such that $\underline{\mathbf{Q}}^{\underline{\mathbf{X}}'} = M' \bmod p$ is satisfied. If the challenge is $b = 1$, then P' passes the protocol this time. However, if $b = 0$, then P' have to find an integer r such that $p_i^r \bmod p \in \underline{\mathbf{Q}}$ for all $1 \le i \le n$ and $M' = M^r \bmod p$. We conjecture that this problem should be harder than solving discrete logarithm problem over $GF(p)$.

Based on above discussions, we have the following theorem. Its proof is similar to the proof of Theorem 1 and we omit it here.

Theorem 2:

(a). If P is honest, then V is able to confirm P knows the secret.

(b). If P does not know the secret set, then any cheating by P in Protocol 2 will be detected by V with probability at least $1 - 2^{-t}$.

(c). V is not able to grasp any information about $\underline{\mathbf{X}}$ from P even if P is honest.

5 Conclusion

In this paper, we have proposed two methods to implement the indistinguishable box needed in the Simmons scheme. Using the proposed indistinguishable box, we give two concrete implementations of Simmons's ZKIP scheme whose security is based on subset sum problem. To our best knowledge, there is no such an indistinguishable box to be proposed until now. Same as the method proposed by Fiat and Shamir [5], it is easy to modify the identification schemes proposed in the paper to digital signature schemes. However, we do not intend to discuss it here.

References

[1] T. Beth, "Efficient Zero-Knowledge Identification Scheme For Smart Cards", Advances in Cryptology: *Proceedings of Eurocrypt'88* (Lecture Notes in Computer Science, Vol.330), Springer-Verlag, Berlin Heidelberg, 1988, pp. 77-84.

[2] D. Chaum, J. H. Evertse, J. van de Graff and R. Peralta, "Demonstrating Possession of Discrete Logarithm Without Revealing It", Advances in Cryptology: *Proceedings of Crypto'86* (Lecture Notes in Computer Science, Vol.218), Springer-Verlag, Berlin Heidelberg, 1987, pp. 200-212.

[3] D. Chaum, J. H. Evertse, and J. van de Graff, "An Improved Protocol for Demonstrating Possession of A Discrete Logarithms and Some Generalizations", Advances in Cryptology: *Proceedings of Eurocrypto'87* (Lecture Notes in Computer Science, Vol.263), Springer-Verlag, Berlin Heidelberg, 1988, pp. 127-141.

[4] T. ElGamal, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," *IEEE Trans. on Information Theory*, Vol.31, No.4, 1985, pp. 469-472.

[5] A. Fiat and A. Shamir, "How To Prove Yourself: Practical Solutions to Identification and Signature Problems", Advances in Cryptology: *Proceedings of Crypto'85* (Lecture Notes in Computer Science, Vol.218), Springer-Verlag, Berlin Heidelberg, 1986, pp. 186-194.

[6] S. Goldwasser, S. Micali and C. Rackoff, "The Knowledge Complexity of Interactive Proof-Systems", *17th ACM Symposium on Theory of Computation*, 1985, pp. 291-304.

[7] L. C. Guillow and J. J. Quisquater, "A Practical Zero-Knowledge Protocol Fitted to Security Microprocessor Minimizing Both Transmission and Memory", Advances in Cryptology: *Proceedings of Eurocrypt'88* (Lecture Notes in Computer Science, Vol.330), Springer-Verlag, Berlin Heidelberg, 1988, pp. 123-128.

[8] J. C. Lagarias and A. M. Odlyzko, "Solving low-density subset sum problems," *J. Assoc. Comp. Mach.*, Vol. 32, pp.229-246, 1985.

[9] R.C. Merkle and M.E. Hellman, "Hiding Information and Signatures in Trapdoor Knapsack", *IEEE Trans on Inform. Theory*, Vol.24, No. 5, pp.525-530, 1978.

[10] G. J. Simmons, "Identification of Data, Devices, Documents and Individuals", Proc. 1991 IEEE International Carnahan Conference on Security Technology, pp. 197-218.