Bull. Korean Math. Soc. **47** (2010), No. 1, pp. 63–71
DOI 10.4134/BKMS.2010.47.1.063

IMPERSONATION ATTACK ON THE STRONG IDENTIFICATION BASED ON A HARD-ON-AVERAGE PROBLEM

Bonwook Koo, Daesung Kwon, Jooyoung Lee, and Jung Hwan Song

Abstract. In this paper, we analyze a zero-knowledge identification scheme presented in [1], which is based on an average-case hard problem, called *distributional matrix representability problem*. On the contrary to the soundness property claimed in [1], we show that a simple impersonation attack is feasible.

1. Introduction

Zero-knowledge proof is an interactive method for one party to convince another of knowledge of a secret without revealing any information on the secret. It has been used in authentication systems where a prover wants to prove her identity to a verifier via some secret information, but does not want the verifier or a wiretapper to learn anything about the secret. The zero-knowledge proof must satisfy completeness, soundness, and zero-knowledge property. Completeness is satisfied if an honest verifier always verifies an honest prover. Soundness is satisfied if no cheating prover can convince an honest verifier of knowledge of the secret. Zero-knowledge property stipulates that no cheating verifier learns any information on the secret except the fact that the prover knows the secret. Zero-knowledge proofs was introduced in the seminal paper of Goldwasser, Micali, and Rackoff [3] and realized as Fiat-Shamir scheme and Schnorr's scheme [2, 6]. They are based on well known problems in number theory such like integer factoring problem and discrete logarithm problem. Since there are no proofs on the hardness of these problems, cryptographers have published alternative schemes based on NP-complete problems in combinatorics, coding theory, graph theory, and so on.

NP-complete problems are widely used as basis of cryptographic protocols. However, most of NP-complete problems allow for efficient solvers on random instances, making useless their worst-case difficulty. For this reason, Levin et al. introduced a notion of *average-case complexity* which deals with distributional

Received September 12, 2008; Revised June 30, 2009.
2000 *Mathematics Subject Classification.* Primary 94A60, 94A62, 94A15.
Key words and phrases. cryptography, authentication, zero-knowledge identification.

problems assuming that instances are chosen from a certain distribution [5]. A pair of a decision problem and a distribution of instances is called a *distributional NP problem*, if some non-deterministic polynomial time algorithm solves the problem on random instances chosen from the distribution. A *distributional NP-complete problem* is similarly defined. It can be regarded as analogous to an NP-complete problem in worst-case analysis.

In [1], the author presented a new identification scheme based on the hardness of *distributional matrix representability problem*, which is known to be distributional NP-complete, and claimed that the success probability of impersonating an honest prover is not greater than 2^{-m}, where m is the number of rounds in a session. However, in this paper, we show that a simple impersonation attack is feasible with success probability almost one! Our attack suggests that the security proof of the identification scheme is flawed. In the next section, we briefly review the scheme and the underlying problem. In Section 3, our impersonation attack is illustrated with a toy example.

2. Caballero-Gil's identification scheme

2.1. Underlying problem

A distributional decision problem is a pair of a decision problem and a probability distribution of instances. In the matrix representability problem with security parameters r and k, an instance consists of a square integral matrix M of order r, a set $\mathcal{P} = \{M_1, M_2, \ldots, M_k\}$ of k distinct square integral matrices of order r, and a positive integer n. Each instance is chosen uniformly at random. The problem is to decide if matrix M can be represented as a product of n matrices in $\mathcal{P}$. For $r = 20$, the matrix representability problem has been proved as distributional NP-complete [7]. (So we assume $r = 20$ throughout this paper.) Now the Caballero-Gil's identification scheme is based on the search version of the matrix representability problem.

2.2. Identification scheme

Caballero-Gil's identification scheme involves two parties: a *prover* Alice and a *verifier* Bob. That is, Alice wants to prove herself to Bob. In the preparation steps, *Trusted Authority*(TA) generates and publishes a set $\mathcal{P} = \{M_1, \ldots, M_k\}$ of k invertible $r \times r$ matrices of integer entries. (The set $\mathcal{P}$ is commonly used for every user in the system.) Then Alice chooses a private (ordered) subset

$$\mathcal{P}_A = \{M_{i_1}, \ldots, M_{i_n}\} \subset \mathcal{P},$$

and computes her public information $M_A = \prod_{j=1}^{n} M_{i_j}$, where n is a system parameter. Now each session of Caballero-Gil's scheme consists of m rounds, and each round is executed as follows. Note that integers m and t in the following description are system parameters.

(1) (*Commit*) Alice chooses an integral vector v of size r and an integer x between 2 and 2^n uniformly at random, and sends Bob $2k$ witness

vectors $\{M_i v, M_i^T v\}_{i=1,\ldots,k}$ in a random order and a witness integer $v^T {M_A}^x v$.

(2) (*Challenge*) Bob randomly selects a bit $e \in \{0,1\}$, and depending on its value, requests to Alice:
   (a) (*Decommit*) vector v and integer x if $e = 0$.
   (b) (*Proof*) vectors $M_{i_1}^T v$, $M_{i_n} v$ and $r \times r$ *integral* matrix $M_{A_1} = {M_{i_1}}^{-1} \cdot {M_A}^x \cdot {M_{i_n}}^{-1}$ if $e = 1$.

(3) (*Response*) Alice responds to the challenge.

(4) (*Verification*) Depending on the selected challenge, Bob checks that:
   (a) if $e = 0$, the witness information is correct.
   (b) if $e = 1$, the witness integer $v^T {M_A}^x v$ is obtained from the product of $v^T M_{i_1}$, M_{A_1}, and $M_{i_n} v$. Then Bob runs the following steps recursively for $j = 2, \ldots, t$:
      b1. (*Commit*) Alice sends Bob a witness integer $v^T {M_{A_{j-1}}}^x v$.
      b2. (*Proof*) Alice indicates to Bob two vectors $M_{i_j}^T v$ and $M_{i_{n-j+1}} v$, and sends him $r \times r$ *integral* matrix $M_{A_j} = M_{i_j}^{-1} \cdot {M_{A_{j-1}}}^x \cdot M_{i_{n-j+1}}^{-1}$.
      b3. (*Verification*) Bob checks that the witness integer $v^T {M_{A_{j-1}}}^x v$ is obtained from the product of $v^T M_{i_j}$, M_{A_j} and $M_{i_{n-j+1}} v$.

3. Impersonation attack

The soundness of this scheme depends on the difficulty of finding matrices $M_{i_j}^T v$, $M_{i_{n-j+1}} v$ and M_{A_j} such that $v^T {M_{A_{j-1}}}^x v = v^T M_{i_j} M_{A_j} M_{i_{n-j+1}} v$ without knowing the private subset $\mathcal{P}_A$. However, one can generate valid responses without knowledge of $\mathcal{P}_A$.

3.1. Attack scenario

In order for an adversary Oscar to impersonate Alice to Bob, Oscar does the followings for each round.

(1) (*Commit*) Oscar randomly chooses an integral vector v of size r, an integer x between 2 and 2^n and a set of indices $\{i_1, \ldots, i_n\}$ from $\{1, \ldots, k\}$. Then Oscar sends Bob $2k$ witness vectors $\{M_i^T v, M_i v\}_{i=1,\ldots,k}$ in any order and a witness integer $v^T {M_A}^x v$. Note that Oscar is able to compute the witness vectors and the witness integer from public information $\mathcal{P}$ and M_A.

(2) (*Challenge*) Bob randomly selects a bit $e \in \{0,1\}$, and depending on its value, requests to Oscar:
   (a) (*Decommit*) vector v and integer x if $e = 0$.
   (b) (*Proof*) vectors $M_{i_1}^T v$, $M_{i_n} v$ and $r \times r$ integral matrix $M_{A_1} = {M_{i_1}}^{-1} \cdot {M_A}^x \cdot {M_{i_n}}^{-1}$ if $e = 1$.

(3) (*Response*) Oscar responds to the challenge as follows.

(a) if $e = 0$, Oscar responds with v and x that he chose.
(b) if $e = 1$, Oscar finds an integral matrix H_1 satisfying

$$v^T M_{i_1} \cdot H_1 \cdot M_{i_n} v = v^T {M_A}^x v, \tag{1}$$

and responds with $M_{i_1}^T v$, $M_{i_n} v$ and H_1. Finding H_1 satisfying equality (1) is only a slight difficulty of our attack, and we discuss a method of finding such a matrix in the following section.

(4) (*Verification*) Depending on the selected challenge, Bob checks that:
(a) if $e = 0$, the witness information is correct.
(b) if $e = 1$, the witness integer $v^T {M_A}^x v$ is obtained from the product of $v^T M_{i_1}$, H_1, and $M_{i_n} v$. (It is obvious from (1).) Then Bob runs the following steps recursively for $j = 2, \ldots, t$:
b1. (*Commit*) Oscar chooses a random integral matrix H_j, computes an integer

$$z_j = v^T M_{i_j} \cdot H_j \cdot M_{i_{n-j+1}} v, \tag{2}$$

and sends Bob the integer z_j as the witness integer.
b2. (*Proof*) Oscar indicates to Bob two vectors $M_{i_j}^T v$ and $M_{i_{n-j+1}} v$, and sends him the integral matrix H_j.
b3. (*Verification*) Bob checks that the witness integer z_j is obtained from the product of $v^T M_{i_j}$, H_j, and $M_{i_{n-j+1}} v$. (It is obvious from (2).)

3.2. Finding the matrix H_1

The success probability of our attack depends on Oscar's ability to find a matrix H_1 satisfying equality (1). Simplifying notations, we want to find an $r \times r$ integral matrix H satisfying $u^T H w = y$ for a given integer y and given integral vectors u and w. As an additional condition, we require that H is invertible and its determinant is divided by the determinant of M_A since otherwise Bob would be able to check if the matrix H is faithfully computed. However, we note that this step is not specified in the original description of the scheme.

Let $H = (h_{ij})$, $u = (u_1, \ldots, u_r)$ and $w = (w_1, \ldots, w_r)$. Then a simple computation shows

$$u^T H w = \sum_{1 \le i,j \le r} u_i w_j h_{ij} = y. \tag{3}$$

For simplicity, we will find h_{ij} satisfying the following conditions.

(1) $h_{ij} = 0$ if $i > j$,
(2) $h_{ij} = 1$ if $i = j < r$,
(3) $h_{ij} = \det(M_A)$ if $i = j = r$.

Then, equation (3) is rewritten as follows.

$$u^T H w = u_r w_r \det(M_A) + \sum_{i=1}^{r-1} u_i w_i + \sum_{1 \le i < j < r} u_i w_j h_{ij} = y. \tag{4}$$

Since we know u, w, and M_A, equation (4) is simplified as

$$\sum_{1 \le i < j < r} u_i w_j h_{ij} = Y \tag{5}$$

for a constant Y.

By re-indexing the coefficients and the variables, we see that finding an integer solution to equation (5) is equivalent to finding an integer solution $(x_1, x_2, \ldots, x_t)$ to an equation of the following form,

$$a_1 x_1 + a_2 x_2 + \cdots + a_t x_t \ = \ Y, \tag{6}$$

where every coefficient is integral and $t = \frac{r(r-1)}{2}$. If there exists $i^* \in \{1, \ldots, t\}$ such that $a_{i^*} \neq 0$ divides Y, then $x_{i^*} = Y/a_{i^*}$ and $x_i = 0$ for $i \neq i^*$ would be a trivial solution to (6). Also, if there exists a co-prime pair (a_i, a_j), then we would be able to find an integer solution by the *extended Euclidean algorithm*. In general, a condition for equation (6) to have integer solutions can be derived from Bézout's identity.

Lemma 3.1 ((Bézout's identity) [4])**.** *If a and b are nonzero integers with the greatest common divisor d, then there exist integers x and y such that*

$$ax + by = d. \tag{7}$$

Moreover, for any integers $a_1, a_2, \ldots, a_n$ with the greatest common divisor g, there exist integers $x_1, x_2, \ldots, x_n$ such that

$$a_1 x_1 + a_2 x_2 + \cdots + a_n x_n = g. \tag{8}$$

Since the integers satisfying (8) can be found by iteratively applying the extended Euclidean algorithm, Bézout's identity implies that we could solve equation (6) if $\gcd(a_1, a_2, \ldots, a_t) = 1$. Now we estimate the probability P that $\gcd(a_1, a_2, \ldots, a_t) = 1$ under the assumption that the coefficients a_i's are distributed uniformly at random within the interval $[1, N]$ for a sufficiently large N. Let p_d denote the probability that d is a divisor of all a_i, $i = 1, 2, \ldots, t$. Then it is easy to show that $p_d = 1/d^t$. Since $\gcd(a_1, a_2, \ldots, a_t) = 1$ if and only if there is no common divisor $d \in [2, N]$ for $\{a_1, a_2, \ldots, a_t\}$, we obtain the following inequality.

$$P \ge 1 - \sum_{d=2}^{N} p_d = 1 - \sum_{d=2}^{N} \frac{1}{d^t}. \tag{9}$$

A straightforward computation shows

$$\begin{aligned} P &\geq 1 - \left(\frac{1}{2^t} + \frac{1}{3^t} + \cdots + \frac{1}{N^t}\right) \\ &= 1 - \left(\frac{1}{N^t}\left(\frac{1}{(2/N)^t} + \cdots + \frac{1}{(N/N)^t}\right)\right) \\ &\geq 1 - \frac{1}{N^{t-1}} \int_{1/N}^{1} \frac{1}{x^t} dx \\ &= 1 - \frac{1}{t-1} \cdot \left(1 - \frac{1}{N^{t-1}}\right) \\ &\geq 1 - \frac{1}{t-1}. \end{aligned} \tag{10}$$

For example, let $r = 20$. Then $t = \frac{r(r-1)}{2} = 190$, and the probability P that equation (6) has a solution is estimated by $P \geq 1 - 1/189 \approx 0.9947$.

3.3. Example

In this section, we illustrate our impersonation attack for the first round of the scheme with a small example. Let

$$\mathcal{P} = \{M_1, M_2, M_3, M_4, M_5, M_6, M_7, M_8\},$$

and

$$M_1 = \begin{pmatrix} -1 & -2 & -5 & 2 \\ -3 & 2 & 2 & -3 \\ 1 & -3 & 6 & 1 \\ 2 & 0 & 3 & 3 \end{pmatrix}, M_2 = \begin{pmatrix} -4 & -1 & -1 & 0 \\ 2 & 0 & 3 & 3 \\ 0 & 5 & -1 & 2 \\ -2 & -3 & 1 & 0 \end{pmatrix},$$

$$M_3 = \begin{pmatrix} 2 & -4 & 3 & 3 \\ 0 & 1 & -7 & 2 \\ -1 & 5 & 1 & 0 \\ 1 & 0 & 4 & 5 \end{pmatrix}, M_4 = \begin{pmatrix} -2 & 0 & -3 & 5 \\ 0 & 1 & 4 & -1 \\ 4 & 3 & 0 & 4 \\ 1 & -1 & 2 & 0 \end{pmatrix},$$

$$M_5 = \begin{pmatrix} -1 & -4 & -1 & 3 \\ 0 & 5 & -3 & -1 \\ 6 & -2 & 0 & 1 \\ 3 & 1 & 4 & -4 \end{pmatrix}, M_6 = \begin{pmatrix} -2 & 0 & 5 & -2 \\ 0 & -4 & 0 & 3 \\ 2 & -2 & -1 & 1 \\ -6 & 3 & 4 & -2 \end{pmatrix},$$

$$M_7 = \begin{pmatrix} 2 & 1 & 0 & 1 \\ -3 & 2 & 4 & -3 \\ 1 & 2 & 2 & 0 \\ 0 & -4 & -1 & 3 \end{pmatrix}, M_8 = \begin{pmatrix} -1 & 0 & 2 & -8 \\ 2 & 3 & -3 & 0 \\ 0 & 6 & 4 & -1 \\ 4 & -2 & 3 & -5 \end{pmatrix}.$$

If Alice's private subset is $\mathcal{P}_A = \{M_7, M_2, M_5\}$, then the corresponding public information would be

$$M_A = \begin{pmatrix} 29 & 6 & 35 & -29 \\ 32 & 82 & -62 & -20 \\ 48 & 49 & 13 & -46 \\ -76 & -12 & 0 & 20 \end{pmatrix},$$

with $\det(M_A) = -1344$.

In the first commit step of the scheme, Oscar chooses $v = (0, 0, 1, 0)^T$, $x = 2$ and $(i_1, i_2, i_3) = (1, 2, 3)$. Then Oscar sends Bob a witness integer

$$y = v^T {M_A}^x v = -1189,$$

and the witness vectors associated with M_1, M_2, and M_3. Suppose that Bob selects $e = 1$ in the challenge step. Then Oscar computes $u = M_1 v = (1, -3, 6, 1)^T$ and $w = M_3 v = (3, -7, 1, 4)^T$, and finds an integral matrix H_1 satisfying $u^T H_1 w = y$ by solving the following equation.

$$(11)\quad \begin{pmatrix} 1, & -3, & 6, & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & x_1 & x_2 & x_3 \\ 0 & 1 & x_4 & x_5 \\ 0 & 0 & 1 & x_6 \\ 0 & 0 & 0 & -1344 \end{pmatrix} \cdot \begin{pmatrix} 3 \\ -7 \\ 1 \\ 4 \end{pmatrix} = -1189.$$

Solving equation (11) is equivalent to solving the following equation.

$$(12)\qquad -7x_1 + x_2 + 4x_3 - 3x_4 - 12x_5 + 24x_6 = 5346.$$

We have a trivial integer solution $(x_1, x_2, x_3, x_4, x_5, x_6) = (0, 5346, 0, 0, 0, 0)$ to equation (12). Now the response made by Oscar would be $u = (1, -3, 6, 1)^T$, $w = (3, -7, 1, 4)^T$ and

$$H_1 = \begin{pmatrix} 1 & 0 & 5346 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1344 \end{pmatrix}.$$

In the verification step, Bob checks that

$$u^T H_1 w = y = -1189.$$

For the subroutines, Oscar is able to impersonate Alice in a much simpler way. For $j = 2$, Oscar arbitrarily chooses

$$H_2 = \begin{pmatrix} 1 & 5 & -2 & 3 \\ 0 & 3 & 2 & -1 \\ 4 & 2 & -1 & 7 \\ 5 & 9 & 6 & 1 \end{pmatrix},$$

and computes

$$z_2 = v^T M_2 \cdot H_2 \cdot M_2 v = 24.$$

In the commit step, Oscar sends z_2 to Bob as a witness integer. In the proof step, Oscar indicates to Bob two vectors $u = v^T M_2 = (0, 5, -1, 2)^T$ and $w = M_2 v = (-1, 3, -1, 1)^T$ and sends the matrix H_2 to Bob. Then Bob checks that

$$u^T H_2 w = 24.$$

In a similar way, Oscar is able to successfully impersonate Alice for the subsequent subroutines with $j = 3, \ldots, t$.

4. Conclusion

In this paper, we analyzed an identification scheme presented in [1], which is based on a distributional NP-complete problem. On the contrary to the claimed soundness property, we showed that a simple impersonation attack is feasible except with negligible probability.

References

[1] P. Caballero-Gil, *Strong identification based on a hard-on-average problem*, IEICE Transection Fundamentals Vol. **E88-A** (2005), no. 5, 1117–1121.
[2] A. Fiat and A. Shamir, *How to prove yourself: practical solutions to identification and signature problems*, Advances in cryptology—CRYPTO '86 (Santa Barbara, Calif., 1986), 186–194, Lecture Notes in Comput. Sci., 263, Springer, Berlin, 1987.
[3] S. Goldwasser, S. Micali, and C. Rackoff, *The knowledge complexity of interactive proof systems*, SIAM J. Comput. **18** (1989), no. 1, 186–208.
[4] G. A. Jones and J. M. Jones, *Elementary Number Theory*, Springer Undergraduate Mathematics Series. Springer-Verlag London, Ltd., London, 1998.
[5] L. Levin, *Average case complete problems*, SIAM J. Comput. **15** (1986), no. 1, 285–286.
[6] C. P. Schnorr, *Efficient identification and signatures for smart cards*, Advances in cryptology—CRYPTO '89 (Santa Barbara, CA, 1989), 239–252, Lecture Notes in Comput. Sci., 435, Springer, New York, 1990.
[7] R. Venkatesan and S. Rajagopalan, *Average case intractability of matrix and diophantine problems (extended abstract)*, In Proceedings of the 24th Annual Symposium on Theory of Computing, ACM Press, pp. 632–642, 1992.

Bonwook Koo
The Attached Institute of ETRI
P.O.Box 1, Yuseong-Gu, Deajeon, Korea
E-mail address: bwkoo@ensec.re.kr

Daesung Kwon
The Attached Institute of ETRI
P.O.Box 1, Yuseong-Gu, Deajeon, Korea
E-mail address: ds_kwon@ensec.re.kr

Jooyoung Lee
The Attached Institute of ETRI
P.O.Box 1, Yuseong-Gu, Deajeon, Korea
E-mail address: jlee05@ensec.re.kr

Jung Hwan Song
Department of Mathematics
Hanyang University
Seoul 133-791, Korea
E-mail address: camp123@hanyang.ac.kr