Malaysian Journal of Mathematical Sciences 7(S): 87- 99 (2013)
Special Issue: The 3rd International Conference on Cryptology & Computer Security 2012 (CRYPTOLOGY2012)

MALAYSIAN JOURNAL OF MATHEMATICAL SCIENCES

Journal homepage: http://einspem.upm.edu.my/journal

An Efficient Identification Scheme in Standard Model Based on the Diophantine Equation Hard Problem

[1,2]B.C. Tea, [1,2*]M.R.K. Ariffin and [1,3]J.J. Chin

*[1]Al-Kindi Cryptography Research Laboratory,
Institute for Mathematical Research, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia*

*[2]Department of Mathematics, Faculty of Science,
Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia*

*[3]Faculty of Engineering,
Multimedia University, Cyberjaya, Malaysia*

E-mail: teaboonchian@ymail.com, rezal@putra.upm.edu.my and jjchin@mmu.edu.my

*Corresponding author

ABSTRACT

Recently the Diophantine Equation Hard Problem (DEHP) was proposed. It is utilized to design a standard identification scheme model. Since the computation involves only simple addition and multiplication steps, the efficiency and the time cost are greatly improved as compared to the existing identification schemes. In this paper, we propose a zero knowledge identification scheme based upon the DEHP. With the assumption such that DEHP is intractable, we provide the security analysis on the impersonation against non-adaptive passive attack (imp-pa) and show that our new proposed scheme is more desirable due to high efficiency in terms of time computation.

Keywords: Diophantine Equation Hard Problem, standard identification scheme model, impersonation against non-adaptive passive attack.

1. INTRODUCTION

An identification scheme, involves two parties comprising of the Prover and the Verifier where the Prover is trying to identify himself to the Verifier in such a way that no important information (private message) is relayed throughout the communication (zero knowledge). The typical identification scheme consists of three canonical moves, where the Prover sends the “commitment” to the Verifier; the Verifier will then send the “challenge” to the Prover; Prover “response” the challenge to the Verifier and finally Verifier accepts or rejects by verifying Prover’s response.

The goal of the adversary in an identification scheme is to impersonate or to attack the scheme in such a way that it behaves as a cheating prover and succeeds in identifying itself to the honest verifier. With the existence of adversary that attempts to impersonate, three common attacks are usually considered, passive, active and concurrent attacks. Hence, security against these attacks becomes a major concern in cryptography, where analysis and establishment of the identification schemes are widely researched.

Existing identification schemes are based on specific number theoretic assumptions, such as RSA assumption in Guillou-Quisquater (GQ) identification; and also Discrete Log (DLOG) assumption in Schnorr identification schemes. These schemes provide security only under impersonation against passive attack, and were developed post Fiat-Shamir. The GQ scheme, which is one of the Fiat-Shamir’s variant, utilized the hardness of RSA problem, (i.e. solving e-th root problem). Schnorr’s scheme on the other hand, relies on the Discrete Log assumption, which is the hardness of solving the discrete log problem. Bellare and Palacio in their paper proposed the Reset Lemma together with the assumption of One-More-RSA Inversion Problem (Bellare (2003)) and One-More-Discrete-Log Problem (OMDLP) (Koblitz (2008)) which successfully provides security under impersonation of active and concurrent attack of GQ and Schnorr’s schemes, respectively.

Other than the hardness problem of number theoretic assumptions, Stern (Stern (1996)) had proposed the identification scheme based on the worst-case hardness of the lattice problem, in which the author managed to provide the security against impersonation under passive attack. After a few years, with the improvement and modification made by Kawachi (2008), Stern’s identification scheme was proven to be provably secure against the concurrent attack - under the assumption of the worst-case hardness of the lattice problem.

There are also identification schemes which are established based on problems surrounding multivariate public key cryptography schemes such as in (Pointcheval (1995)) and (Pointcheval (2003)). The most recent identification scheme is by Sakumoto *et al.* in which they have proposed the identification scheme based on multivariate quadratic polynomial (Sakumoto (2011)). It is also proven to be secure by the authors. The security of their scheme relies on the intractability of the multivariate quadratic polynomial under the assumption of the existence of non-interactive commitment. This identification scheme with this assumption guarantees security under impersonation of active and passive attacks, even though the protocol is repeated in parallel. Sakumoto *et al*. also showed that their scheme is more efficient than other schemes utilizing the same multivariate function with different problems as stated in Sakumoto's one (Sakumoto (2011)).

In this paper, we propose a new identification scheme based on the Diophantine Equation Hard Problem (Ariffin (2012)). We show that our identification scheme is secure against impersonation under non-adaptive passive attacks in the standard model. Our identification scheme based on DEHP is desirable since it increases the runtime efficiency comparing other schemes as it relies only on simple mathematical operations of addition and multiplication.

The layout of the paper is as follows. In Section 2, we will first review the definition of the DEHP and provide tighter parameter selection within the definition (in comparison to the original definition). We then describe the Bivariate Function Hard Problem (BFHP) which is a 2 parameter situation for the DEHP (Ariffin (2013)). Proofs will be given on the uniqueness and intractability of the BFHP. We will also review in this section, identification schemes in the standard model, followed by the security model of the schemes. In Section 3 we propose the standard model of our identification scheme, followed by the security analysis in which proofs of security against impersonation under non-adaptive passive attack are given. In Section 4, we provide efficiency analysis and comparison of the schemes. In Section 5, the conclusion about our identification scheme is made.

2. PRELIMINARIES

2.1 Diophantine Equations Hard Problem (DEHP)

We revisited the definition by Ariffin (2012) and further enhance the definition as follows:

Definition 1

Let $Y = \sum_{i=1}^{j} A_i x_i$ be a summation where x_i are unknown integers which are m-bits, A_i is a public sequence of integers and $gcd(A_i, A_j) = 1$ where $i \neq j$ which are n-bits and at minimum $m - n = 128$. We define the DEHP is solved when Y is *prf*-solved. That is, the preferred integer set x_i^* is found from the set of all possible integers x_i such that $Y = \sum_{i=1}^{j} A_i x_i$.

Remark 1

For the purpose of this research we will take $j = 2$. Hence, we can also address it as the Bivariate Function Hard Problem (BFHP). The following is a description of the BFHP with chosen parameter structures.

Proposition 1 (Sakumoto *et al.* (2011)).

Let $F(x_1, x_2, \dots, x_n)$ be a multivariate one-way function that maps $F: \mathbb{Z}^n \to \mathbb{Z}^+_{(2^{n-1}, 2^n - 1)}$.Let $F_1$and F_2 be such functions (either identical or non-identical) such that $A_1 = F(x_1, x_2, \dots, x_n)$, $A_2 = F(y_1, y_2, \dots, y_n)$, and $gcd(A_1, A_2) = 1$. Let $u, v \in (2^{m-1}, 2^m - 1)$. Now, suppose we have the bivariate function $G(u, v) = A_1 u + A_2 v$. If at minimum $m - n - 1 = 129$, it is infeasible to determine (u, v) from $G(u, v)$. Furthermore, $(u, v)$is unique for $G(u, v)$ with high probability.

Proof.

We begin by proving that $(u, v)$is unique for each $G(u, v)$ with high probability. Assume there exists $u_1 \neq u_2$ and $v_1 \neq v_2$ such that

$$A_1 u_1 + A_2 v_1 = A_1 u_2 + A_2 v_2.$$

We will then have

$$Y = v_1 - v_2 = \frac{A_1(u_1 - u_2)}{A_2}$$

Since $gcd(A_1, A_2) = 1$and $A_2 \approx 2^n$, then the probability that Y is an integer is 2^{-n}.

Next we proceed to prove that to *prf* -solve the Diophantine equation given by $G(u, v)$ is infeasible. The general solution for $G(u, v)$ is given by

$$u = u_0 + A_2 t$$

and

$$v = v_0 - A_1 t$$

for some integer t. To find u within the stipulated interval $(2^{m-1}, 2^m - 1)$ we have to find the integer t such that $2^{m-1} < u < 2^m - 1$.
That is,

$$\frac{2^{m-1} - u_0}{A_2} < t < \frac{2^m - 1 - u_0}{A_2}.$$

Then the difference between the upper and the lower bound is approximate 2^{m-n-2}. Since$m - n - 1 = 129$, then $m - n - 2 = 128$. Hence the difference is very large and finding the correct t is infeasible. This is also the same scenario for v.■

Definition 2 (Ariffin (2013))

We say that the BFHP is hard to be *prf*-solved if for all probabilistic polynomial time algorithm there exist a negligible function $\varepsilon(n)$ such that $Pr[BFHP_{solve} = 1] \leq \varepsilon(n)$.

2.2 Identification Scheme in Standard Model

An identification scheme in a standard model consists of three probabilistic polynomial time algorithms$(KeyGen, Prove, Verify)$which are defined as follows:

1. ***KeyGen***: The Simulator S on input of security parameter1^*, generates and publishes the master public key, mpk and keeps the master secret key, msk to itself.
2. ***Prove***: An algorithm that outputs the Commitment as the initial step of identification and responses to the corresponding Challenge from the Verifier.
3. ***Verify***: A deterministic verification algorithm that first outputs challenge to the Prover and takes an input as the purported response and the public key. It outputs either 0 or 1.

2.3 Security Model of Identification Scheme

The security of the identification schemes remains on the probability of the impersonation by the adversary. In other words, after certain interactions of the adversary with the honest verifier, the adversary succeeds in the impersonation attempt and is accepted by the verifier with non-negligible probability.

In analyzing the security of the identification schemes, we consider three types of the adversaries:

1. **Passive Attacker**: The passive adversary eavesdrops on conversations between an honest prover and verifier to acquire information (usually conversation transcript).

2. **Active Attacker**: The active adversary interacts with honest prover sequentially as a cheating verifier to acquire information before attempting impersonation.

3. **Concurrent Attacker**: A special type of active adversary where it can interact with multiple provers at the same time to acquire information before attempting impersonation.

The whole process of identification schemes are based on the two-phase game, in which the impersonation attack is between an impersonator and the challenger:

1. **Setup**. The challenger takes in the security parameter and runs KeyGen. The resulting system parameters are given to the impersonator while the master secret is kept to itself.

2. **Phase 1**. In this phase, the impersonator plays the role as a cheating verifier and can issue transcript queries to the challenger. The challenger responds by sending the commitment, challenge and corresponding response to the impersonator. These queries are interleaved and asked adaptively.

3. **Phase 2**. In this phase, the impersonator now acts as a cheating prover and output a challenge which it wishes to impersonate and tries to convince the verifier to accept. Impersonator is said to win the game if it successfully convinces the verifier in accepting it.

We say that an identification scheme is (t, q_I, ε)-secure under non-adaptive passive attacks for any non-adaptive passive impersonator I who runs in time t, $Pr[I\ impersonates] < \varepsilon$, where I can makes at most q_I transcript queries.

3. THE STANDARD MODEL OF IDENTIFICATION SCHEME BASED ON DEHP / BFHP

We begin by discussing the following lemma regarding the initial solution pair for the Diophantine equation $G(u,v) = A_1u + A_2v$ which are (u_0, v_0).

Lemma 2.

The initial solution (u_0, v_0) for the Diophantine equation $G(u,v) = A_1u + A_2v$ with parameter selection as mentioned in Proposition 1, are of minimum length mn-bits.

Proof.

From $G(u,v) = A_1u + A_2v$, by the parameter selection as mentioned in Proposition 1, it is obvious that $G(u,v)$ is at minimum mn-bits. To obtain the initial solution, begin by using the Euclidean algorithm upon the Diophantine equation $A_1u + A_2v = \gcd(A_1, A_2) = 1$. Then, to obtain the initial solution for $G(u,v) = A_1u + A_2v$ multiply the initial solution obtained by using the Euclidean algorithm upon $A_1u + A_2v = 1$with $G(u,v)$. Hence, the initial solution for $G(u,v) = A_1u + A_2v$ is at least mn-bits. ■

3.1 Standard Identification Scheme against Impersonation under Non-Adaptive Passive Attack

KeyGen: The algorithm generates the private keys $\{x_i\}_{i=1}^{2} \in \mathbb{Z}_{(2^{2n-1}, 2^{2n}-1)}$, the public keys of $\{v_i\}_{i=1}^{2} \in \mathbb{Z}_{(2^{n-1}, 2^{n}-1)}$ and compute $U = \sum_{i=1}^{2} v_i x_i$. Publicize $\left(\{v_i\}_{i=1}^{2}, U\right)$ and keep $\{x_i\}_{i=1}^{2}$ secret. We will use at minimum $n = 128$.

Identification Protocol:

1. Prover P picks $\{r_i\}_{i=1}^{2} \in \mathbb{Z}_{(2^{2n-1}, 2^{2n}-1)}$ randomly and sends $R = \sum_{i=1}^{2} v_i r_i$ to the Verifier V.
2. Verifier V picks a random challenge, $c \in \{0,1\}$ and sends to Prover P.
3. Prover$P$ returns the response by computing $z_i = r_i + cx_i$for $i = 1,2$ to Verifier V.
4. Verifier V checks the bit length of all responses $\{z_i\}_{i=1}^{2}$ and accepts if all responses are within the interval $(2^{2n-1}, 2^{2n+1})$and $\sum_{i=1}^{2} v_i z_i = R + cU$.

Completeness

The following shows the completeness of the identification process:

$$\begin{aligned}\sum_{i=1}^{2} v_i z_i &= v_1 z_1 + v_2 z_2\\ &= v_1(r_1 + c x_1) + v_2(r_2 + c x_2)\\ &= v_1 r_1 + v_1 c x_1 + v_2 r_2 + v_2 c x_2\\ &= v_1 r_1 + v_2 r_2 + v_1 c x_1 + v_2 c x_2\\ &= R + cU. \blacksquare\end{aligned}$$

Remark 2

Since initial solution (u_0, v_0) for the Diophantine equation $U = \sum_{i=1}^{2} v_i x_i$ is at least $3n$-bits, then to utilize it for impersonation would be futile even though the summation $\sum_{i=1}^{2} v_i z_i = R + cU$ would still be obtained. In fact, any element within the general solution for $U = \sum_{i=1}^{2} v_i x_i$ (i.e. $x_1 = x_{1,0} + v_2 t$ and $x_2 = x_{2,0} - v_1 t$ where $t \in \mathbb{Z}$) would result in the summation $\sum_{i=1}^{2} v_i z_i = R + cU$ to be true. However, for each incorrect $t \in \mathbb{Z}$ would result in responses of $\{z_i\}_{i=1}^{2} \notin (2^{2n-1}, 2^{2n+1})$. In fact, by Proposition 1 we have proven that the preferred solution (x_1, x_2) is unique with high probability for $U = \sum_{i=1}^{2} v_i x_i$ and the corresponding t is infeasible to be obtained.

3.2 Security Analysis of Identification Scheme against Impersonation under Non-Adaptive Passive Attack

Theorem 1.

The identification scheme based on the BFHP is (t, q_I, ε)-secure against impersonation under non-adaptive passive attacks assuming the BFHP is(t', ε')-hard where

$$\varepsilon \leq \sqrt{\varepsilon'} + \frac{1}{q}$$

Proof.

To provide a proof of security of the identification scheme, we assume if there exists an Impersonator, I who can (t, q_I, ε)-break the identification scheme then there exists an algorithm (Simulator), Swho can (t', q_I, ε')-solve the BFHP. The following shows the simulation of the challenger from Simulator, S to the Impersonator, I:

1. ***SETUP.*** The Simulator, S randomly chooses public keys $\{v_i\}_{i=1}^{2}$ and $U = \sum_{i=1}^{2} v_i x_i$. It should be noticed that the Simulator, S does not

know the secrets $\{x_i\}_{i=1}^2$. S then passes all the public keys $\left(\{v_i\}_{i=1}^2, U\right)$ to the Impersonator, I.

2. ***TRANSCRIPT QUERIES.*** For any transcript queried by Impersonator I, the simulator S randomly selects $\{z_i\}_{i=1}^2 \in \mathbb{Z}_{(2^{2n-1},2^{2n+1})}$, $c \in \{0,1\}$ and returns the valid transcript to I.

$$\left\{R = \sum_{i=1}^{2} v_i z_i - cU, c, \{z_i\}_{i=1}^2\right\}$$

The correctness of the valid transcript is given below:

S randomly selects $\left(\tilde{c}, \{\tilde{z}_i\}_{i=1}^2\right)$ and computes

$$\begin{aligned} \tilde{R} &= \textstyle\sum_{i=1}^2 v_i \tilde{z}_i - \tilde{c}U \\ &= v_1(r_1 + \tilde{c}x_1) + v_2(r_2 + \tilde{c}x_2) - \tilde{c}U \\ &= v_1 r_1 + v_1 \tilde{c} x_1 + v_2 r_2 + v_2 \tilde{c} x_2 - \tilde{c}U \\ &= (v_1 r_1 + v_2 r_2) + (v_1 \tilde{c} x_1 + v_2 \tilde{c} x_2) - \tilde{c}U \\ &= R + \tilde{c}U - \tilde{c}U \blacksquare \end{aligned}$$

3. ***IMPERSONATION PHASE.*** After some time t, the Impersonator I wishes to challenge and impersonate. It is assumed that the Impersonator I plays the role of cheating prover that tries to convince the simulator, S to accept. By resetting I to the commitment phase after sending the response $\{z_{1,i}\}_{i=1}^2, \{z_{2,i}\}_{i=1}^2$, S will then able to obtain two valid transcript

$$\left(R, c_1, \{z_{1,i}\}_{i=1}^2\right) \text{and} \left(R, c_2, \{z_{2,i}\}_{i=1}^2\right).$$

Here $z_{1,i}$ and $z_{2,i}$ represent the responses sent by the Prover upon challenge c_1 and c_2 respectively. Upon receiving the valid transcripts, S will then verify the bit length of $\{z_{1,i}\}, \{z_{2,i}\} \in \mathbb{Z}_{(2^{2n-1},2^{2n+1})}$.

Extraction is then done by calculating

$$\left\{x_1 = \frac{z_{1,2} - z_{1,1}}{c_2 - c_1}, x_2 = \frac{z_{2,2} - z_{2,1}}{c_2 - c_1}\right\}$$

which outputs the solution to the BFHP problem of $U = \sum_{i=1}^2 v_i x_i$. This completes the simulation.

Remark 3

It can be easily seen that

$$\begin{aligned} x_1 &= \frac{z_{1,2}-z_{1,1}}{c_2-c_1} \\ &= \frac{(r_1+c_2x_1)-(r_1+c_1x_1)}{c_2-c_1} \\ &= \frac{c_2x_1-c_1x_1}{c_2-c_1} \blacksquare \end{aligned}$$

Remark 4

Upon the responses purported by Impersonator I, $z_i = r_i + cx_i$ with $r_i \in \mathbb{Z}_{(2^{2n-1},2^{2n})}$ and $x_i \in \mathbb{Z}_{(2^{2n-1},2^{2n})}$, the computed responses are within the interval$(2^{2n-1}, 2^{2n+1})$. Once the simulator S accepts the correctness of the responses. it will then continue the extracting process.

4. ***PROBABILITY STUDY.*** The analysis of the probability is based on the Simulator, S winning the game and solves the BFHP. Let $\varepsilon = Adv_A^{imp-pa}(n)$ be the success probability of the impersonation under passive attack and let $\varepsilon' = Adv^{BFHP}(n)$be the probability of Simulator S winning the game by solving the BFHP, by the Reset Lemma proposed by Bellare and Palacio:

$$Pr[S\ solves\ BFHP] = Pr\left[S\ computes\ \{x_i\}_{i=1}^{2}\right]$$

$$\varepsilon' \geq \left(\varepsilon - \frac{1}{q}\right)^2$$

$$\varepsilon \leq \frac{1}{q} + \sqrt{\varepsilon'}$$

$$Adv_A^{imp-pa}(n) \leq \frac{1}{q} + \sqrt{Adv^{BFHP}(n)}\ . \blacksquare$$

4. COMPARISON

The original Fiat-Shamir identification scheme utilized the square root modulo problem in designing the scheme. Besides that, current existing identification schemes, such as Guillou-Quisquater (GQ) and Schnorr's identification schemes utilized the RSA problem and Discrete Log Problem (DLP), respectively. Our identification scheme which is based upon the BFHP uses simple addition and multiplication operations, containing no pairings, hence provides efficient computing time. The following table indicates the complexity of the identification scheme of our work based on BFHP as compared to Fiat-Shamir, GQ and Schnorr's schemes:

TABLE 1: Complexity comparison of identification schemes based on 4 different hard problem assumptions.

	BFHP			**Fiat-Shamir**		
	Addition	**Multiplication**	**Exponentiation**	**Addition**	**Multiplication**	**Exponentiation**
KeyGen	k	k	0	0	0	k
Prove	$3k$	$3k+1$	0	0	k	$2k$
Verify	k	$k+2$	0	0	k	$2k$

	Guillou-Quisquater			**Schnorr**		
	Addition	**Multiplication**	**Exponentiation**	**Addition**	**Multiplication**	**Exponentiation**
KeyGen	0	0	k	0	0	k
Prove	0	k	$2k$	k	k	0
Verify	0	k	$2k$	0	k	$2k$

5. CONCLUSION

Based on the time complexity analyzed in the previous section, our zero knowledge identification scheme based on the BFHP provides better efficiency. As proposed in Section 3, this scheme utilizes a Diophantine Equation which consists of only addition and multiplication operations, with no exponentiation and pairing. This will greatly increase the speed during the identification process. We have also showed that our scheme based is provably secure against the non-adaptive passive attack, under the assumption that solving the BFHP is hard. Hence, our proposed identification scheme is more desirable than existing schemes. The identification scheme of security against impersonation under active and concurrent attacks still remains to be an open problem.

REFERENCES

Ariffin, M. R. K. 2012. A proposed IND-CCA2 Scheme for Implementation on an Asymmetric Cryptosystem Based on the Diophantine Equation Hard Problem (2012). *Proceedings of the 3rd International Conference on Cryptology and Computer Security (ISBN:978-967-394-084-4)* , pp. 193 – 197.

Ariffin, M. R. K., Asbullah, M. A., Abu, N. A. and Mahad, Z. 2013. A New Efficient Asymmetric Cryptosystem Based on the Integer Factorization Problem of $N = p^2q$. Accepted Malaysian Journal Mathematical Sciences, 2013.

Bellare, M., Fischlin, M., Goldwasser, S. and Micali, S. 2001. Identification Protocols Secure Against Reset Attacks. *Advances in Cryptology – CRYPTO '01*, Vol. 2045. Springer-Verlag: Lecture Notes in Computer Science (LNCS).

Bellare, M., Namprempre, C., Pointcheval, D. and Semanko, M. 2003.The One-More-RSA Inversion Problems and the Security of Chaum's Blind Signature Scheme. *Journal of Cryptology*. **16**:185 – 215.

Bellare, M. and Palacio, A. 2002. GQ and Schnorr Identification Schemes: Proofs of Security against Impersonation under Active and Concurrent Attacks. *Advances in Cryptology, CRYPTOLOGY '02,* Vol. 2442, pp. 162 – 177. Springer-Verlag: Lecture Notes in Computer Science (LNCS).

Canetti, R., Goldwasser, S., Goldreich, O. and Micali, S. 2000. Resettable Zero-Knowledge. *Proceedings of the 32nd Annual Symposium on the Theory of Computing, ACM.*

Chin, J. J. and Heng, S. H. 2012. Security Upgrade for a k-Resilient Identity-Based Identification Scheme in the Standard Model. *The 3rd International Conference on Cryptology and Computer Security 2012 (Cryptology 2012).*

Fiat, A. and Shamir, A. 1986. How to Prove Yourself: Practical Solutions to Identification and Signature Problem. *Advances in Cryptology, CRYPTO '86*, Vol. 263, pp. 186 – 194. Springer-Verlag: Lecture Notes in Computer Science (LNCS).

Guillou, L. and Quisquater, J. J. 1998. A Paradoxical Identity-Based Signature Scheme Resulting from Zero Knowledge.*Advances in Cryptology – CRTYPTO '88*, Vol. 403, pp. 216 – 231. Springer-Verlag: Lecture Notes in Computer Science (LNCS).

Heng, S. H. and Chin J. J. 2010. A k-Resilient Identity-Based Identification Scheme in the Standard Model. *International Journal of Cryptology Research.* **2**: 15 – 25.

Kawachi, A., Tanaka, K. and Xagawa, K. 2008. Concurrently Secure Identification Schemes Based on the Worst-Case Hardness of Lattice Problems. *ASIACRYPT 2008*, vol. 5350, pp. 372–389. Springer, Heidelberg: Lecture Notes in Computer Science (LNCS).

Koblitz, N. and Menezes, A. 2008. Another Look at Non-Standard Discrete Log and Diffie-Hellman Problems. *Journal of Mathematical Cryptology*. **2**(4): 1862–2984.

Kurosawa, K. and Heng, S. H. 2005. Identity-Based Identification without Random Oracles.*Computational Science and Its Application – ICCSA 2005,* Vol. 3481, pp. 603 – 613. Springer-Verlag: Lecture Notes in Computer Science (LNCS).

Mao, W. 2004. *Modern Cryptography: Theory and Practice*. Prentice Hall PTR, pp. 619 – 664.

Pointcheval, D. 1995. A New Identification Scheme Based on the Perceptrons Problem.*EUROCRYPT 1995*, Vol. 950, pp. 319–328. Springer-Verlag, Heidelberg: Lecture Notes in Computer Science (LNCS).

Pointcheval, D. and Poupard, G. 2003. A New NP-Complete Problem and Public-key Identification. *Des.Codes Cryptography*. 28(1): 5–31.

Sakumoto, K., Shirai, T. and Hiwatari, H. 2011. Public-Key Identification Schemes Based on Multivariate Quadratic Polynomials.*Advances in Cryptology, CRYPTO '11*, Vol. 6841, pp. 703 – 721. Springer-Verlag: Lecture Notes in Computer Science (LNCS).

Schnorr, C. P. 1989. Efficient Identification and Signature for Smart Card. *Advances in Cryptology, CRYPTO '89*, Vol. 435, pp. 239 – 252. Springer-Verlag: Lecture Notes in Computer Science (LNCS).

Shamir, A. 1984. Identity-based Cryptosystems and Signature Scheme. *Advances in Cryptology – CRYPTO '84*. Vol. 196, pp. 47 – 53. Springer-Verlag: Lecture Notes in Computer Science (LNCS).

Stern, J. 1996. A new paradigm for public key identification. *IEEE Transaction of Information Theory*. **42**(6): 749 – 765.

Stinson, D. R. 2006. *Cryptography: Theory and Practice*. Chapman & Hall/CRC, pp. 363-364.