ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.19, No.7, July 2008, pp.1758−1765
DOI: 10.3724/SP.J.1001.2008.01758
© 2008 by *Journal of Software*. All rights reserved.

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

多一次Paillier求逆问题与并发安全的鉴别方案*

宋　焰[1,2+]

[1](中国科学院 软件研究所 计算机科学国家重点实验室,北京　100190)

[2](中国科学院 研究生院,北京　100049)

One-More Paillier Inversion and Concurrent Secure Identification

SONG Yan[1,2+]

[1](State Key Laboratory of Computer Science, Institute of Software, The Chinese Academy of Sciences, Beijing 100190, China)

[2](Graduate University, The Chinese Academy of Sciences, Beijing 100049, China)

+ Corresponding author: E-mail: songyan03@ios.cn

Song Y. One-More Paillier inversion and concurrent secure identification. *Journal of Software*, 2008,19(7): 1758−1765. http://www.jos.org.cn/1000-9825/19/1758.htm

Abstract: This paper revisits Paillier's trapdoor one-way function, focusing on the computational problem underlying its one-wayness. A new computational problem called the one-more Paillier inversion problem is formulated. It is a natural extension of Paillier inversion problem to the setting where adversaries have access to an inversion oracle and a challenge oracle. The relation between the one-more Paillier inversion problem and the one-more RSA problem introduced by Bellare, *et al*. It is shown that the one-more Paillier inversion problem is hard if and only if the one-more RSA problem is hard. Based on this, a new identification scheme is proposed. It is shown that the assumed hardness of the one-more Paillier inversion problem leads to a proof that the proposed identification scheme achieves security against concurrent impersonation attack.

Key words: trapdoor one-way function; Pallier inversion; RSA problem; hardness; identification; concurrent security

摘　要: 从计算难解性的角度重新考察Paillier的陷门单向函数,并提出多一次Paillier求逆问题这一关于Paillier求逆问题的推广问题.从计算难解性的角度考察了多一次Paillier求逆问题与Bellare等人提出的多一次RSA求逆问题之间的关系,并证明了在计算难解性的意义上,多一次Paillier求逆问题等价于多一次RSA求逆问题.以此为基础,进而提出一种新的鉴别方案,并证明在多一次Paillier求逆问题的难解性假设下这一鉴别方案具备并发安全性.

关键词: 陷门单向函数;Paillier求逆;RSA问题;难解性;鉴别方案;并发安全性

中图法分类号: TP309　　**文献标识码**: A

1　Introduction

Paillier's cryptosystem[1] belongs to the family of probabilistic encryption schemes ushered by Goldwasser and

* Supported by the National Natural Science Foundation of China under Grant No.60310213 (国家自然科学基金重大国际(地区)合作研究项目); the National Natural Science Foundation of China under Grant No.60325206 (国家自然科学基金杰出青年基金项目)

Received 2006-11-20; Accepted 2007-05-31

Micali[2] who introduce the notion of probabilistic encryption. The probabilistic encryption scheme originally proposed by Goldwasser and Micali is based on the quadratic residuosity assumption. Cohen and Fischer[3] improve the limited communications bandwidth of the Goldwasser-Micali scheme. The encryption scheme in Ref.[3] is based on the prime residuosity assumption, however the decryption procedure is inefficient since it involves a certain sort of exhaustive search. Naccache and Stern[4] suggest a variant on the Cohen-Fischer scheme, their scheme allows for high communications bandwidth, and is semantically secure under the same assumption (namely the prime residuosity assumption). Independently, Okamoto and Uchiyama[5] propose an improvement on the Cohen-Fischer scheme, using a different group structure and the semantic security of the Okamoto-Uchiyama scheme is proved under the p-subgroup assumption. Paillier[1] proposes a new candidate trapdoor one-way function and presents a new probabilistic encryption scheme based on it. The semantic security of Paillier's encryption scheme is proved under the decisional composite residuosity assumption (in contrast to the prime residuosity assumption). Paillier's encryption scheme is more efficient than the aforementioned schemes. Following Ref.[1], many related works have been done, mainly being concerned with modifications, extensions, or applications of Paillier's cryptosystem (see, e.g., Refs.[6–10]).

In this paper, we revisit Paillier's trapdoor one-way function, focusing on the computational problem underlying its one-wayness, namely the Paillier inversion problem. We formulate a new computational problem that we call the one-more Paillier inversion problem. It is a natural extension of Paillier inversion problem to the setting where adversaries gain access to an inversion oracle and a challenge oracle. We study the relation between the proposed one-more Paillier inverseon problem and the one-more RSA problem introduced by Bellare *et al*. in Ref.[11]. We show that the one-more Paillier inversion problem is hard if and only if the one-more RSA problem is hard, that is, in regard to intractability, the one-more Paillier inversion problem is equivalent to the one-more RSA inversion problem. Based on this, we next propose a new identification scheme that can be viewed as derived from a Σ-protocol (cf. Ref.[12]) for proof of knowledge of pre-image under Paillier's function. We show the assumed hardness of the one-more Paillier inversion problem leads to a proof that the proposed identification scheme is secure against concurrent impersonation attack. Compared with the known RSA-related identification schemes, the proposed identification scheme is only slightly inefficient than the well-known GQ scheme[13], but is more efficient than Okamoto's[14].

2 The One-More Paillier Inversion Problem

In this paper, we adopt the standard notations for algorithms and probability spaces (cf. Ref.[15] pp.171~173). Throughout this paper, we let positive integer k denote a *security parameter*. As done in Ref.[1], we fix an RSA-type key generator, denoted by *Key*(), in the sequel. The generator *Key*(), on input k, returns (N,e,d) consisting of a modulus N, an encryption exponent e, and the matching decryption exponent d. The modulus N is k-bit long, and is a product of two distinct odd primes; the encryption exponent e equals to N; the decryption exponent d is the multiplicative inverse of N modulo $\lambda(N)$, the least common multiple of p−1 and q−1.

2.1 The Paillier inversion problem

In this section, we review and formalize the Paillier inversion problem underlying the one-wayness of Paillier's trapdoor one-way function.

Let N=pq be an RSA-like modulus and consider the multiplicative group $\mathbb{Z}_{N^2}^*$ of units. Paillier[1] proposes a candidate trapdoor one-way function Π from $\mathbb{Z}_N \times \mathbb{Z}_N^*$ to $\mathbb{Z}_{N^2}^*$ defined by $\Pi:(x,y) \mapsto (1+N)^x y^N \bmod N^2$. Paillier actually presents this candidate trapdoor one-way function in terms of an arbitrary base g whose order modulo N^2 is a multiple of N, rather than the specific base $1+N$, which has order N modulo N^2. However, since the Paillier inversion problem is random self-reducible (cf. Ref.[1]), it follows that the hardness of the Paillier inversion problem is independent of the base g. Therefore, we formalize the Paillier inversion problem in terms of the key generator *Key*() and the function Π.

Definition 1 (**Paillier inversion problem**[1]). Let k be a security parameter and A be an adversary. Consider the following experiment associated with adversary A

```
Experiment $Exp_A(k)$
    $(N,e,d) \leftarrow Key(k)$
    $z \leftarrow \mathbb{Z}_{N^2}^*,\ (x,y) \leftarrow A(N,k,z)$
    If $z=(1+N)^x y^N \bmod N^2$ then return 1 else return 0
```

We define the inverting advantage of A by $Adv_A(k)=\Pr[Exp_A(k)=1]$. The Paillier inversion problem is said to be hard, if the function $Adv_A(k)$ is negligible in k for any adversary A with time complexity polynomial in k.

2.2 The one-more Paillier inversion problem

In this section, we propose a new computational problem related to the Paillier inversion problem, which we call the *one-more Paillier inversion problem*. This problem can be thought of as a natural extension of the Paillier inversion problem, and is analogous to the one-more extension of the RSA problem in Ref.[11].

We denote by $I()$ the *inversion oracle* which on input an element z in $\mathbb{Z}_{N^2}^*$, returns the pre-image of z under function Π. We also denoted by $C()$ the *challenge oracle* which upon query, simply returns a uniform and independent challenge element in $\mathbb{Z}_{N^2}^*$. An adversary is given oracle accesses to both the inversion oracle $I()$ and the challenge oracle $C()$, and tries to find the correct pre-images of all the challenge elements returned by $C()$, so that the number of its queries to the inversion oracle $I()$ is strictly less than the number of those challenge elements returned by the challenge oracle $C()$.

Definition 2 (**one-more Paillier inversion problem**). Let k be a security parameter. Let A be an adversary with accesses to the inversion oracle $I()$ and the challenge oracle $C()$. Consider the following experiment associated with adversary A

```
Experiment $Exp_A^{om\text{-}p}(k)$
    $(N,e,d) \leftarrow Key(k)$
    $((x_1,y_1),\ldots,(x_m,y_m)) \leftarrow A^{I(),C()}(N,\ k)$ // $m$ is the number of queries to $C()$ made by $A$
    Let $z_1,\ldots,z_m$ be the challenge elements returned by the challenge oracle $C()$
    If $z_m=(1+N)^{x_i} y_i^N \bmod N^2$ for all $1 \le i \le m$ and the number of queries to the inversion
    oracle $I()$ made by $A$ is strictly less than $m$, then return 1 else return 0
```

The advantage of A in the above experiment is defined by $Adv_A^{om\text{-}p}(k)=\Pr[Exp_A^{om\text{-}p}(k)=1]$. The *one-more Paillier inversion problem* is said to be hard if $Adv_A^{om\text{-}p}(k)$ is negligible in k for any adversary A with time complexity polynomial in k (We adopt the convention that the *time complexity* of a one-more Paillier inversion adversary A is the running time of the entire experiment $Exp_A^{om\text{-}p}(k)$, except that only one time unit is charged for each action of the two oracles).

3 The Equivalence

In this section, we investigate the relation between the one-more Pailler inversion problem and the one-more RSA problem in Ref.[11]. We show that in regard to computational intractability, these two problems are polynomially equivalent; namely, the one-more Paillier inversion problem is hard if and only if the one-more RSA problem is hard. This suggests that the new computational problem may serve as a useful primitive in designing cryptographic mechanisms, as will be demonstrated in Section 4.

Theorem 1. The one-more Paillier inversion problem is hard if and only if the one-more RSA problem is hard.

Proof: For one implication, we show that for any probabilistic polynomial time one-more Paillier inversion adversary A, there exists a probabilistic polynomial time one-more RSA inversion adversary B so that their advantage functions are related by $Adv_A^{om\text{-}p}(k) \le Adv_B^{om\text{-}rsa}(k)$, from which it follows that the one-more RSA problem is hard, if the one-more Paillier inversion problem is hard.

Recall that (Ref.[2]) the one-more RSA inversion adversary B is given oracle accesses to the RSA inversion oracle *RSAI*() (which takes an element $\tilde{z}$ in $\mathbb{Z}_N^*$, and returns the N-th root $\tilde{y}$ of $\tilde{z}$ modulo N), and to the RSA challenge oracle *RSAC*() (who returns an element chosen independently and uniformly from $\mathbb{Z}_N^*$ each time being queried). Here is the algorithm of the one-more RSA inversion adversary B: On input (N,k), run A on input (N,k), answer A's oracle queries accordingly: when A queries its challenge oracle, query *RSAC*() to get $\tilde{z}$, pick a random number x in $\mathbb{Z}_N$, compute $z=(1+N)^x\tilde{z} \bmod N^2$, and return z to A; when A queries its inversion oracle with z, query *RSAI*() with $z$mod$N$ to get $\tilde{y}$, compute $x=(z\tilde{y}^{-N}-1)/N \bmod N$, and return $(x,\tilde{y})$ to A. Until A halts with some output $((x_1,y_1),\ldots,(x_m,y_m))$, and finally return $(y_1,\ldots,y_m)$.

Notice that the challenge point z created by B is uniformly distributed in $\mathbb{Z}_{N^2}^*$. Now let $\tilde{z}_1,\ldots,\tilde{z}_m$ be the challenge points returned by the oracle RSAC(), and $z_1,\ldots,z_m$ the corresponding challenges computed by B. If A is successful, then the number of its inversion queries is strictly less than the number of its challenge queries. Moreover, for all $1\le i\le m$, the pair (x_i,y_i) is the correct pre-image of z_i under function Π. By changing modulus from N^2 to N, we see that y_i is the RSA-inverse of $\tilde{z}_i$ modulo N. In summary, the adversary B inverts all the m challenges $z_1,\ldots,z_m$ returned by *RSAC*(), but the number of its inversion queries to *RSAI*() is strictly less than m.

For the other implication, we show that for any probabilistic polynomial time one-more RSA inversion adversary B, there exists a probabilistic polynomial time one-more Paillier inversion adversary A so that their advantage functions satisfy $Adv_B^{om\text{-}rsa}(k) \le Adv_A^{om\text{-}p}(k)$, and therefore the one-more Paillier inversion problem is hard if the one-more RSA inversion problem is hard.

Recall that adversary A is given oracle accesses to an inversion oracle I() and a challenge oracle C(). Here is the algorithm of the one-more Paillier inversion adversary A: On input (N,k), invoke B with (N,k), answer B's oracle queries accordingly: when B queries its challenge oracle, query C() to obtain z, set $\tilde{z}=z \bmod N$, and return $\tilde{z}$ to B; when B queries its inversion oracle with $\tilde{z}$, query $\tilde{z}$ to I(), get back (x,y), and return y to B. Until B halts with some output $(\tilde{y}_1,\ldots,\tilde{y}_m)$. Let $z_1,\ldots,z_m$ be the challenges returned by C(). For i from 1 to m, compute $x_i=(z_i\tilde{y}_i^{-N}-1)/N \bmod N$, $y_i \leftarrow \tilde{y}_i$. Finally return $((x_1,y_1),\ldots,(x_m,y_m))$.

Now if B is successful, then the number of its inversion queries is strictly less than the number of its challenge Queries. Furthermore, for all $1\le i\le m$, $\tilde{y}_i=y_i$ is the N-th root of $\tilde{z}_i$ modulo N. It is easily verified (x_i,y_i) is the correct pre-image of z_i under function Π. Therefore, A outputs correct the pre-images of all the m challenge points $z_1,\ldots,z_m$ returned by C(), but the number of its inversion queries to I() is strictly less than m. □

4 The Concurrent Secure Identification Scheme

In this section, we present a new identification scheme, named Protocol csID, that can be viewed as derived from a Σ-protocol (cf. Ref.[12]) for proof of knowledge of pre-image under function Π (see Section 2). As a demonstration of its utility, the assumed intractability of the one-more Paillier inversion problem enables us to prove that the proposed identification scheme is secure against concurrent impersonation attack (see, e.g., Refs.[16,17] for formal definitions and further discussion). Compared with the known RSA-related identification schemes, the proposed identification scheme is only slightly inefficient than the well-known GQ scheme[13,17], but is more efficient than Okamoto's[14].

The parameter generator for the identification scheme is described as follows: On input k, first run *Key*(k) (see Section 2) to get (N,e,d). Then pick two random numbers $x\in\mathbb{Z}_N$, $y\in\mathbb{Z}_N^*$, and compute $U=(1+xN)y^N \bmod N^2$. The public key *pk* of the prover is (N,U), and the corresponding private key *sk* is (N,x,y).

In a typical execution of Protocol csID, the prover makes the first move; it picks two random numbers $r\in\mathbb{Z}_N$, $s\in\mathbb{Z}_N^*$, computes $W=(1+rN)s^N \bmod N^2$, and sends W to the verifier. The verifier responds by a random number c in $\mathbb{Z}_N$. To answer the challenge c, the prover, using its private key *sk*, computes $a=r+cx \bmod N$, $b=sy^c \bmod N$, and sends (a,b) to the verifier. The verifier accepts if and only if (a,b) is the pre-image of $WU^c \bmod N^2$ under function Π.

The following theorem relates the advantage $Adv_I^{ca}(k)$ of any concurrent impersonation adversary I attacking Protocol csID to the advantage $Adv_A^{om\text{-}p}(k)$ of a derived one-more Paillier inversion adversary A.

Theorem 2. For any concurrent impersonation adversary $I=(P,V)$ with time complexity $T()$, there exists a one-more Paillier inversion adversary A such that $Adv_I^{ca}(k)\le 1/N+\sqrt{Adv_A^{om-p}(k)}$, moreover, the time complexity of adversary A is $2T(k)+O(\ell(k)k^3)$, where $\ell(k)$ is the total number of prover instances with which the impersonation adversary I interacts during the impersonation attack.

Proof: Let N be the modulus output by the generator *Key*() on input k. Recall that the one-more Paillier inversion adversary A is given accesses to an inversion oracle $I()$ and a challenge oracle $C()$. The goal of the adversary A is to invert all elements returned by $C()$, while making strictly fewer queries to $I()$.

The algorithm of the adversary A is described schematically below. The adversary A first queries $C()$ to get a random element $U\in\mathbb{Z}_{N^2}^*$. Using this element, along with its own input (N,k), A forms a public key $pk=(N,k,U)$ for the impersonation adversary I. Then, to achieve its goal, adversary A runs V, and in every interaction of V and a prover instance, A emulates the role of the latter. To answer a query of the form (Λ,i) (meaning that V want to initiate a new instance of the prover numbered i), A queries $C()$ and forwards the answer W_i to V; to answer a query of the form (c_i,i), A queries $I()$ with $W_iU^{c_i} \bmod N^2$ and returns the answer (a_i,b_i) to V. Since the answer (a_i,b_i) returned by the inversion oracle $I()$ is the pre-image of $W_iU^{c_i} \bmod N^2$ under function Π, the pair (a_i,b_i) is precisely what prover instance i needs to produce in order to meet the challenge c_i. Now, from the perspective of V, the distribution of the resulting transcript (W_i,c_i,a_i,b_i) is identical to the distribution of transcripts resulting from a real conversation. It follows that A perfectly simulates the view of V.

Let ℓ be the number of prover instances with which V interacts. When V finishes with some piece of state information σ, adversary A has made ℓ queries to its inversion oracle $I()$ (to get the $\ell(k)$ pairs (a_i,b_i) of pre-images), and has asked for a total number $\ell(k)+1$ of challenge queries. Recall that A's goal is to invert all these $\ell(k)+1$ target points (namely, $U,W_1,\ldots,W_\ell$), while making at most $\ell(k)$ queries to the inversion oracle. So at this point, A cannot make use of its inversion oracle any more, and instead it tries to extract the pre-image (x,y) of U out of P, since in that case, the pre-image (x_i,y_i) of all the remaining numbers W_i can be computed as

$$x_i\leftarrow(a_i-c_ix)\bmod N,\ y_i\leftarrow(b_iy^{-c_i})\bmod N\ ,$$

whence inverting all the $\ell(k)+1$ challenges.

```
Adversary $A^{I(),\backslash C()}(N,k)$
  Query $C()$ to get $U$; set $pk \leftarrow (N,k,U)$, choose a random tape $\rho$ for $V$, initialize $V$ with $(pk,\rho)$, and set $\ell \leftarrow 0$
  Answer $V$'s queries as follows
    If $V$ makes a query of the form $(\Lambda,i)$, then increase $\ell$ by one, query $C()$ and forward the answer $W_i$ to $V$
    If $V$ makes a query of the form $(c_i,i)$, then query $I()$ with $W_i U^{c_i} \bmod N^2$, and forward the answer $(a_i,b_i)$ to $V$
  Until $V$ outputs some state information $\sigma$ and stops
  Set $W \leftarrow P(\Lambda,\sigma)$, $\hat{c}_1 \leftarrow \mathbb{Z}_N$, $(\hat{a}_1,\hat{b}_1) \leftarrow P(\hat{c}_1,\sigma)$. If $(1+\hat{a}_1 N)\hat{b}_1^N \equiv WU^{\hat{c}_1} (\bmod N^2)$ then set $d_1 \leftarrow 1$ else set $d_1 \leftarrow 0$
  Set $\hat{c}_2 \leftarrow \mathbb{Z}_N$, $(\hat{a}_2,\hat{b}_2) \leftarrow P(c_2,\sigma)$. If $(1+\hat{a}_2 N)\hat{b}_2^N \equiv WU^{\hat{c}_2} (\bmod N^2)$ then set $d_2 \leftarrow 1$ else set $d_2 \leftarrow 0$
  If $d_1=d_2=1$ and $\hat{c}_1 \neq \hat{c}_2$, then {set $\Delta\hat{a}=(\hat{a}_1-\hat{a}_2) \bmod N$, $\Delta\hat{b}=(\hat{b}_1/\hat{b}_2) \bmod N$, $\Delta\hat{c}=(\hat{c}_1-\hat{c}_2) \bmod N$.
    Compute integers $p$, $t$, $v$ such that $\gcd(N,\Delta\hat{c})=p=tN+v(\Delta\hat{c})$
    If $p=1$, then { set $x \leftarrow v(\Delta\hat{a}) \bmod N$, $y \leftarrow (\Delta\hat{b})^v U^t \bmod N$}
    Else {set $q \leftarrow N/p$, $\lambda \leftarrow \mathrm{lcm}(p-1,q-1)$, $y \leftarrow U^{N^{-1} \bmod \lambda} \bmod N$, $x \leftarrow (Uy^{-N}-1)/N \bmod N$}
    For $i \leftarrow 1$ to $\ell$ {set $x_i \leftarrow (a_i - c_i x) \bmod N$, $y_i \leftarrow (b_i y^{-c_i}) \bmod N$}
    Return $((x,y),(x_1,y_1),\ldots,(x_\ell,y_\ell))$}
  Else return *failure*
```

Now, adversary A executes the following procedure to compute the pre-image (x,y) of U: Run P to get its first message W, issue a random challenge $\hat{c}_1$, run P to obtain its response, and execute the verifier's checking procedure. Then, select a second random challenge $\hat{c}_2$, rewind P to get back a second response, and again evaluate the verifier's decision. If both of the decisions come out 1 and the two challenges differ, then proceed to extract the pre-image of U: Let $\Delta\hat{a}$, $\Delta\hat{b}$, $\Delta\hat{c}$ be as in the description of adversary A. By the accepting criterion of the verifier, we know that $(1+(\Delta\hat{a})N)\Delta\hat{b}^N \equiv U^{\Delta\hat{c}} (\bmod N^2)$. Using the extended Euclid's algorithm, compute integers t, v such that $d=\gcd(N,\Delta\hat{c})=tN+v(\Delta\hat{c})$. If $d=1$, then it is easily verified that $x=v(\Delta\hat{a}) \bmod N$, $y=(\Delta\hat{b})^v U^t \bmod N$ is the desired pre-image of U under function Π; if $d>1$, then noticing that $0<|\Delta\hat{c}|<N$, we can then factor the modulus N into p and q, obtain the least common multiple λ of $p-1$ and $q-1$, and compute the inverse of N modulo λ. Now, it is easy to verify that the following pair (x,y)

$$y=U^{N^{-1} \bmod \lambda} \bmod N,\ x=(U_y^{-N}-1)/N \bmod N .$$

It is the desired pre-image of U under function Π. In any case, when we successfully extract the pre-image of U, adversary A can invert all the $\ell(k)+1$ points $U,W_1,\ldots,W_\ell$, but queries its inversion oracle only $\ell(k)$ times, provided that both d_1 and d_2 equal to 1, and the two challenges $\hat{c}_1$ and $\hat{c}_2$ are different. Put differently, A succeeds if and only if both $d_1=d_2=1$ and $\hat{c}_1 \neq \hat{c}_2$. We wish to relate the probability of this event to the advantage $Adv_I^{ca}(k)$ of the impersonation attacker I.

As noted above, A simulates the view of V perfectly; hence. V behaves as it would when playing the two-phase attack game, and therefore, provides P with state information distributed identically to what P would receive in a real attack. So, the probability that the first decision d_1 evaluates to 1 is exactly $Adv_I^{ca}(k)$.

Now write π_1 for $\Pr[d_1=1|\sigma,pk]$, the probability that $d_1=1$, given that the public key produced by A is pk, and the state information output by V is σ (the probability is over the choice of the random challenge $\hat{c}_1$). Similarly, define π_2 to be $\Pr[d_1=d_2=1,\ \hat{c}_1 \neq \hat{c}_2 \mid \sigma, pk]$ (the probability is over the independent and random choices of the challenges $\hat{c}_1$ and $\hat{c}_2$). It is clear that the expectation E_1 of π_1 is $Adv_I^{ca}(k)$, and the expectation E_2 of π_2 is the probability that A succeeds as a one-more inversion adversary, namely E_2= $Adv_A^{om\text{-}p}(k)$.

It is easily verified that since $\pi_2 \geq \pi_1(\pi_1 - 1/N)$, we have

$$E_2 \geq E(\pi_1^2 - \pi_1 / N) = E(\pi_1^2) - E_1 / N \geq (E_1)^2 - E_1 / N .$$

(Here we used the fact that for any random variable X, $(EX)^2-(EX)^2=E(X-EX)^2 \geq 0$, where $E()$ denotes the mathematical expectation.) From that we see

$$E_1 - 1/2N \leq \sqrt{E_2 + (1/2N)^2} \leq \sqrt{E_2} + 1/2N,$$

as claimed.

To complete the proof, it remains to justify the claimed time complexity of adversary A. Consider the two-phase attack game defining the advantage of adversary A. By our conventions for measuring time complexity, the cost of all steps in this game prior to the execution of the next to last if the statement is at most $2T(k)$, plus the cost of computing the $\ell(k)$ queries $W_i U^{c_i} \bmod N^2$ as well as the cost of twice executing the verifier's checking procedure are easily seen to be proportional to $(\ell(k)+1)k^3$. Hence, the time complexity of A is proportional to $(\ell(k)+1)k^3$ plus $2T(k)$, as claimed. □

We can now establish the concurrent security of the proposed identification scheme, Protocol csID:

Corollary. If the one-more Paillier inversion problem is hard, then Protocol csID is secure against concurrent impersonation attack.

Proof: Let I be a concurrent impersonation adversary attacking the proposed identification scheme with polynomial time complexity. Then the one-more Paillier inversion adversary A described in the proof of Theorem 1 also has polynomial time complexity, since both $T()$ and $\ell(k)$ are polynomially bounded. The assumption that the one-more Paillier inversion problem be hard implies that $Adv_A^{om\text{-}p}(k)$ is negligible in k, and obviously $1/N$ is also negligible in k. Hence, the advantage $Adv_I^{ca}(k)$ of the concurrent impersonation adversary I is necessarily negligible in k. □

5 Conclusion

We formulate a new computational problem, called one-more Paillier inversion problem, which extends the Paillier inversion problem underlying the one-wayness of Paillier's trapdoor one-way function[1]. We investigate the relation between the proposed computational problem and the one-more extension of the RSA problem by Bellare *et al*. in Ref.[11] and prove that in regard to computational intractability, the one-more Paillier inversion problem is equivalent to the one-more RSA inversion problem. We also propose a new and efficient identification scheme which is shown to be secure against concurrent impersonation attack under the intractability assumption of the one-more Paillier inversion problem, as a demonstration of its utility as a cryptographic primitive.

References:

[1] Paillier P. Public-Key cryptosystems based on composite degree residuosity classes. In: Wiener MJ, ed. Proc. of the EUROCRYPT'99. LNCS 1592, Springer-Verlag, 1999. 223−238.

[2] Goldwasser S, Micali S. Probabilistic encryption. Journal of Computer and System Sciences, 1984,28(2):270−299.

[3] Cohen JD, Fischer M. A robust and verifiable cryptographically secure election scheme. In: Proc. of the 26th Annual IEEE Symp. on Foundations of Computer Science. IEEE, 1985. 372−382.

[4] Naccache D, Stern J. A new public key cryptosystem based on higher residues. In: Proc. of the 5th Symp. on Computer and Communications Security. ACM Press, 1998. 59−66.

[5] Okamoto T, Uchiyama S. A new public-key cryptosystem as secure as factoring. In: Nyberg K, ed. Proc. of the EUROCRYPT'98. LNCS 1403, Springer-Verlag, 1998. 308−318.

[6] Damgard I, Jurik M. A generalisation, a simplification and some applications of Paillier's probabilistic public-key system. In: Kim K, ed. Proc. of the PKC 2001. LNCS 1992, Springer-Verlag, 2001. 119−136.

[7] Catalano D, Gennaro R, Howgrave-Graham N, Nguyen PQ. Paillier's cryptosystem revisited. In: Proc. of the 8th ACM Conf. on Computer and Communications Security. ACM Press, 2001. 206−214.

[8] Galbraith SD. Elliptic curve Paillier schemes. Journal of Cryptology, 2002,15(2):129−138.

[9] Ostrovsky R, Skeith III WE. Private searching on streaming data. In: Shoup V, ed. Proc. of the CRYPTO 2005. LNCS 3621, Springer-Verlag, 2005. 223−240.

[10] Blake IF, Kolesnikov V. Conditional encrypted mapping and comparing encrypted numbers. In: Di Crescenzo G, Rubin A, eds. Proc. of the FC 2006. LNCS 4107, Springer-Verlag, 2006. 206−220.

[11] Bellare M, Namprempre C, Pointcheval D, Semanko M. The one-more-RSA inversion problems and the security of Chaum's blind signature scheme. Journal of Cryptology, 2003,16(3):185−215.

[12] Cramer R, Damgard I, Schoenmakers B. Proofs of partial knowledge and simplified design of witness hiding protocols. In: Desmedt Y, ed. Proc. of the CRYPTO'94. LNCS 839, Springer-Verlag, 1994. 174−187.

[13] Guillou L, Quisquater J. A practical zero-knowledge protocol fitted to security microprocesors minimizing both transmission and memory. In: Güther CG, ed. Proc. of the EUROCRYPT'88. LNCS 330, Springer-Verlag, 1988. 123−128.

[14] Okamoto T. Provably secure and practical identification schemes and corresponding signature schemes. In: Brickell EF, ed. Proc. of the CRYPTO'92. LNCS 740, Springer-Verlag, 1993. 31−53.

[15] Cramer R, Shoup V. Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. SIAM Journal on Computing, 2003,33(1):167−226.

[16] Bellare M, Palacio A. GQ and Schnorr identification schemes: Proofs of security against impersonation under active and concurrent attack. In: Proc. of the CRYPTO 2002. LNCS 2442, Springer-Verlag, 2002. 162−177.

[17] Bellare M, Namprempre C, Neven G. Security proofs for identity-based identification and signature schemes. In: Proc. of the EUROCRYPT 2004. LNCS 3027, Springer-Verlag, 2004. 268−286.

SONG Yan was born in 1969. He received his Ph.D. degree in 2008 at the Institute of Software, the Chinese Academy of Sciences. His research areas are ryptography, cryptographic protocols and information security.