One-More Extension of Paillier Inversion Problem and Concurrent Secure Identification

Yan Song[1,2]

[1] State Key Lab. of Computer Science, Institute of Software,
Chinese Academy of Sciences, P.O.Box 8718, 100080 Beijing, China
[2] Graduate University of Chinese Academy of Sciences, Beijing, China
songyan03@ios.cn

Abstract. In this paper, we revisit Paillier's trapdoor one-way function [15], focusing on the computational problem underlying its one-wayness. We formulate a new computational problem that we call *one-more Paillier inversion problem*. It is a natural extension of Paillier inversion problem to the setting where adversaries have access to an inversion oracle and a challenge oracle. We study the relation between the proposed problem and the one-more RSA inversion problem introduced by Bellare *et al.* in [2]; we prove that the one-more Paillier inversion problem is hard if and only if the one-more RSA inversion problem is hard. Then we propose a new identification scheme; we show 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. Compared with the known RSA-related identification schemes, the proposed identification scheme is only slightly inefficient than the best known GQ scheme, but is more efficient than Okamoto's.

1 Introduction

Paillier's cryptosystem [15] is an important member of a family of public-key, probabilistic encryption schemes utilizing a discrete logarithm trapdoor technique modulo a hard-to-factor integer. This family begins when Goldwasser and Micali [10] introduce the notion of probabilistic encryption. The probabilistic encryption scheme of Goldwasser and Micali is based on the quadratic residuosity assumption. Cohen and Fischer [5] improve the limited communications bandwidth of the Goldwasser-Micali scheme; their encryption scheme is based on the prime residuosity assumption. However, the decryption procedure is inefficient since it involves a certain exhaustive search. Naccache and Stern [12] suggest a variant on the Cohen-Fischer scheme; their scheme allows for high communications bandwidth and is proved to be semantically secure under the same assumption, namely the prime residuosity assumption. Independently, Okamoto and Uchiyama [14] propose an improvement on the Cohen-Fischer scheme, this time using a different group structure; the semantic security of the Okamoto-Uchiyama scheme is proved under the p-subgroup assumption. Paillier [15] proposes a new candidate trapdoor one-way function on which he builds a new

J. Lopez, P. Samarati, and J.L. Ferrer (Eds.): EuroPKI 2007, LNCS 4582, pp. 65–77, 2007.

encryption scheme; the semantic security of Paillier's encryption scheme is proved under the decisional composite residuosity assumption (in contrast to the prime residuosity assumption), and is more efficient than the aforementioned schemes. Following [15], many related works have been done, mainly concerned with modifications, extensions or applications of Paillier's cryptosystem; see, for example, [7,4,9].

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 [15]. We formulate a new computational problem that we call *one-more Paillier inversion problem*. It is a natural extension of Paillier inversion problem to the setting where adversaries have access to an inversion oracle and a challenge oracle. We study the relation between the proposed problem and the one-more RSA inversion problem introduced by Bellare *et al.* in [2]. We prove that the one-more Paillier inversion problem is hard if and only if the one-more RSA inversion problem is hard; that is, in regard to intractability the one-more Paillier inversion problem is equivalent to the one-more RSA inversion problem. We then propose a new identification scheme derived from a Σ-protocol 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 best known GQ scheme [11], but is more efficient than Okamoto's [13].

2 The One-More Paillier Inversion Problem

In Section 2.1, we review the Paillier inversion problem underlying the one-wayness of Paillier's trapdoor one-way function ([15]). In Section 2.2, we formulate the *one-more Paillier inversion problem*, which is analogous to the one-more RSA inversion problem in [2].

Throughout this paper, we let positive integer k denote the *security parameter*. An RSA-type *modulus generator* is a probabilistic, polynomial time algorithm that on input 1^k returns an RSA-type modulus N, which is k-bit long (namely $2^{k-1} \leq N < 2^k$), and is a product of two distinct odd primes. For an RSA-type modulus N, we denote by $\mathbb{Z}_N$ the ring of integers modulo N, and by $\mathbb{Z}_N^*$ the multiplicative group of units (namely invertible elements in $\mathbb{Z}_N$).

An RSA-type *key generator* is a probabilistic, polynomial time algorithm that on input 1^k returns a triple (N, e, d), where the first component $N = pq$ is a k-bit long modulus that is the product of two distinct odd primes p and q, the second component e is an encryption exponent, and the third component d is the matching decryption exponent.

As done in [15], we fix an RSA-type key generator that will be referred to as $\mathcal{K}$ throughout. The generator $\mathcal{K}$ on input 1^k returns 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