Paillier's Cryptosystem Modulo p^2q and Its Applications to Trapdoor Commitment Schemes

Katja Schmidt-Samoa[1] and Tsuyoshi Takagi[2]

[1] Technische Universität Darmstadt, Fachbereich Informatik,
Hochschulstr. 10, D-64289 Darmstadt, Germany
samoa@informatik.tu-darmstadt.de
[2] Future University – Hakodate, School of Systems Information Science,
116-2 Kamedanakano-cho Hakodate, Hokkaido, 041-8655, Japan
takagi@fun.ac.jp

Abstract. In 1998/99, T. Okamoto and S. Uchiyama on the one hand and P. Paillier on the other hand introduced homomorphic encryption schemes semantically secure against passive adversaries (IND-CPA). Both schemes follow in the footsteps of Goldwasser-Micali, Benaloh-Fischer and Naccache-Stern cryptosystems, and yield their improvements above the latter by changing the group structure. Paillier's scheme works in the group $\mathbb{Z}_{n^2}^{\times}$ where n is an RSA modulus, whilst Okamoto-Uchiyama is located in the group $\mathbb{Z}_n^{\times}$ for n of p^2q type. The new schemes attracted much attention because of their rich mathematical structure. It is notable that Okamoto-Uchiyama is one-way under the p^2q factoring assumption, whilst there is no reduction known from the one-wayness of Paillier's scheme to a standard computational assumption.

In this paper we point out that the combination of both techniques yields a new scheme that inherits all the nice properties of Paillier's scheme and that is one-way under the p^2q factoring assumption. The one-wayness is based on a new trapdoor one-way function which might be of independent interest. In addition, we show how to construct trapdoor commitment schemes with practical applications based on our new scheme and on the trapdoor function. Among other things, we propose a trapdoor commitment scheme that perfectly meets the requirements to construct Shamir-Tauman on-line/off-line signatures.

Keywords: homomorphic encryption, trapdoor commitments, trapdoor hash families, on-line/off-line signatures, chameleon signatures

1 Introduction

In their seminal paper from 1984 Goldwasser and Micali introduced the notion of semantic security and presented the first cryptosystem meeting this requirements [GM84]. Their proposed cryptosystem is additively homomorphic and probabilistic but suffers from a very limited bandwidth (the encryption is performed bit-wise). Over the intervening years this scheme has been improved several times, where the most notable ameliorations came from Benaloh-Fischer

E. Dawson and S. Vaudenay (Eds.): Mycrypt 2005, LNCS 3715, pp. 296–313, 2005.

[CF85] and Naccache-Stern [NS98]. However, the actual breakthrough in the field of semantically secure additive homomorphic encryption has been achieved by Okamoto-Uchiyama and Paillier with a different approach. Namely, their idea was to change the group structure from $\mathbb{Z}_n^\times$ with a RSA modulus n to $\mathbb{Z}_n^\times$ with $n = p^2q$ (Okamoto-Uchiyama [OU98]), resp. $\mathbb{Z}_{n^2}^\times$ (Paillier [Pai99]). Both works gained recognition not only for presenting practical solutions to homomorphic encryption, but also for pointing out the rich mathematical structure of the groups $\mathbb{Z}_n^\times$ with $n = p^2q$ resp. $\mathbb{Z}_{n^2}^\times, n = pq$. Whilst the assumptions on which semantic security relies seems to be comparable for both schemes (*p-subgroup assumption* versus *decisional composite residuosity assumption*), this is not the case for one-wayness: Okamoto-Uchiyama's cryptosystem can be proven one-way if factoring integers p^2q is hard, but for Paillier's scheme no reduction to a standard intractability assumption has been observed yet[1].

Our Contributions. Our first contribution is the development of a factorization-based variant of Paillier's homomorphic encryption scheme. Our concept is to study Paillier's original encryption function in a different group, *i.e.* instead of $\mathbb{Z}_{n^2}^\times$ with an RSA modulus n we consider the group $\mathbb{Z}_{n^2}^\times$ with the Okamoto-Uchiyama modulus $n = p^2q$. Based on the analysis of a new trapdoor one-way function which we introduce in Sect. 2.2, we are able to show that the proposed cryptosystem is one-way under the p^2q factorization assumption. Moreover, the new scheme inherits all the nice properties of Paillier's original one, such as semantic security, additively homomorphic property and efficiency. Unfortunately, the new scheme inherits the most serious drawback of Okamoto-Uchiyama's cryptosystem, too, namely it is vulnerable to a simple chosen ciphertext attack (in general this seems to be the flip-side of the coin regarding factorization-based one-wayness, see *e.g.* textbook Rabin). Of course, there are standard techniques to overcome this problem, for instance the clever use of hash functions, but all in all we feel that this part of the paper is predominantly of theoretical value.

In the rest of the paper we develop practical applications of our novel scheme and the underlying one-way function. More precisely, we introduce two new trapdoor commitments intended as building blocks for Shamir-Tauman on-line/off-line signatures [ST01] and chameleon signatures [KR00]. In the case of on-line/off-line signatures our proposed trapdoor commitment scheme to the best of our knowledge is the first one to yield a highly efficient and perfectly powerful construction at the same time. In addition, we propose the first factorization-based trapdoor commitment that can be used to construct on-line/off-line chameleon signatures, therefore improving the RSA(n, n)-based construction from [CGHGN01]. For a more detailed motivation and comparison see Sect. 4. As the first part of the paper is indeed of theoretical interest, but achieves no significant improvement in homomorphic encryption, we regard our new trapdoor commitment schemes as our main contribution.

[1] In [Pai99], Paillier based the one-wayness of his scheme on the *composite residuosity assumption*, but this assumption is merely a paraphrase of the designated one-wayness property.