

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

Katja Schmidt-Samoa¹ and Tsuyoshi Takagi²

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