Two Generic Constructions of Probabilistic Cryptosystems and Their Applications

Guilhem Castagnos
GREYC, Ensicaen,
Boulevard Maréchal Juin, BP 5186, 14032 Caen cedex, France
guilhem.castagnos@info.unicaen.fr

Abstract. In this paper, we build, in a generic way, two asymmetric cryptosystems with a careful study of their security. We present first an additively homomorphic scheme which generalizes, among others, the Paillier cryptosystem, and then, another scheme, built from a deterministic trapdoor function. Both schemes are proved semantically secure against chosen plaintext attacks in the standard security model and modify versions can be proved secure against adaptive chosen ciphertext attacks.

By implementing these constructions with quotients of $\mathbb{Z}$, elliptic curves and quadratic fields quotients we get some cryptosystems yet described in the past few years and provide variants that achieve higher levels of security than the original schemes. In particular, using quadratic fields quotients, we show that it is possible to build a new scheme secure against adaptive chosen ciphertext attacks in the standard security model.

Keywords: Probabilistic Encryption, Homomorphic Scheme, Generic Construction, Paillier Cryptosystem, Quadratic Fields, IND-CPA and IND-CCA2 security, Standard Model.

1 Introduction

In 1984, Goldwasser and Micali have designed the first probabilistic cryptosystem and defined the adequate notion of security for this type of scheme: the notion of semantic security. After this system, based on quadratic residuosity, many probabilistic schemes built from the same principle have been proposed: chronologically by Benaloh (Ben88), Naccache and Stern (NS98), Okamoto and Uchiyama (OU98) and at last, the most achieved system have been proposed by Paillier (Pai99) and then generalized by Damgård and Jurik (cf. DJ01), allowing to encrypt larger messages. All these schemes use quotients of $\mathbb{Z}$, their one-wayness is based on factoring and their semantic security is based on the hardness of distinguishing some powers. Moreover, these schemes are additively homomorphic, i.e., if we got a multiplicative group structure on the ciphertexts set and an additive one on the plaintexts set, then, if $c_i$ is a valid encryption of $m_i$, with $i \in \{1,2\}$, $c_1 c_2$ is a valid ciphertext of $m_1 + m_2$. This property has many...
applications, for example the systems of Paillier and Damgård and Jurik can be used to design electronic vote systems (cf. [BFP+01, Jur03]), for Private Information Retrieval (cf. [Lip05]), or for building Mix-nets (cf. [NSNK06, Jur03]). At the present time, the Paillier and Damgård-Jurik cryptosystems are almost the only schemes that are additively homomorphic and practical. The system of Paillier has also been adapted in elliptic curves over $\mathbb{Z}/n^2\mathbb{Z}$ by Galbraith in [Gal02]. Another finite group, simpler than elliptic curves over finite ring can be used to adapt this system: the group of norm 1 quadratic integers modulo $n$, where $n$ is an RSA integer (this adaptation was only briefly sketched in [Cas07]).

A fast and non-homomorphic variant of the Paillier scheme has been proposed by Catalano, Gennaro et al. in [CGH+01], and later adapted in elliptic curves by Galindo, Martín et al. (cf. [GMMV03]) and again in quadratic fields quotients in [Cas07]. These schemes can also be seen like probabilistic variants of deterministic trapdoor functions: respectively RSA, KMOV (cf. [KMOV92]) and LUC (cf. [SL93]).

In this paper, we propose two generic constructions that capture the ideas of all these schemes. In section 2, we show how to build a generic homomorphic encryption trapdoor whose semantic security is based on the hardness of the problem of distinguishing $k^{th}$ powers of a group, for a well-chosen integer $k$. Note that this construction is essentially known as it is a direct generalization of the Paillier scheme. We include it here for completeness as a formal exposition is not known by the author. Then, in section 3, we modify the previous construction in order to get more efficient schemes. This will result in a method to build a probabilistic trapdoor function from a deterministic trapdoor function which satisfies some properties.

For each construction, we do a careful study of both one-wayness and semantic security. For the first one, we begin with a scheme secure against chosen-plaintext attacks (the homomorphic schemes can not be secure against chosen-ciphertext attacks because of their obvious malleability) and then we show that we can modify this construction to use universal hash proof systems (cf. [CS02]) in order to build an IND-CCA2 scheme in the standard model. The second construction can be viewed as a simple way to transform a deterministic trapdoor function into an encryption primitive IND-CPA secure in the standard model against a decision problem relative to the properties of the deterministic trapdoor function used. We also present a variant IND-CCA2 secure in the random oracle model by using standard techniques.

In section 4, we apply these generic constructions in quotients of $\mathbb{Z}$, elliptic curves and quadratic fields quotients. By doing this, we will see that a large number of probabilistic schemes proposed these last years can be considered as applications of the generic constructions. This study also leads to an historical treatment of probabilistic encryption based on factoring. With quadratic fields quotients, the application of the generic construction of section 2 leads to a concise but detailed description of the practical homomorphic cryptosystem only briefly sketched at the end of [Cas07]. Moreover, we will show that this scheme can be transformed to build an IND-CCA2 secure cryptosystem in the standard model.