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 $\mathbf{Z}$, 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 $\mathbf{Z}$, 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 $\mathbf{Z}/n^2\mathbf{Z}$ 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 $\mathbf{Z}$, 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.

Notations: In all the paper, G will denote a finite multiplicative abelian group, k a nonnegative integer and g an element of G of order k. We will denote $|G|$ the order of the group G. Let G^k be the subgroup of k^{th} power of G. We will suppose that $k \,\big|\, |G|$ and denote $\lambda := |G|/k$. Moreover, we will suppose that λ and k are coprime. Given a group element h, $\langle h \rangle$ will denote the group generated by h.

Given an integer i, $|i|_2$ will denote the size of i in bits, *i. e.*, $|i|_2 := \lfloor \log_2 k \rfloor + 1$.

We will denote by n an RSA integer, *i. e.*, n will be the product of two distinct odd primes p and q, large enough, such that the factorization of n is infeasible in reasonable time (*i. e.*, $|n|_2 \geq 1024$).

For two algorithmic problems A and B, we will denote $A \overset{\mathcal{P}}{\Longleftarrow} B$ whenever A is polynomial-time reducible to B, and $A \overset{\mathcal{P}}{\Longleftrightarrow} B$ whenever the two problems are polynomial-time equivalent.

2 Additively Homomorphic Trapdoor Function

Let us first state a straightforward result of group theory.

Theorem 1. *Let G be a finite multiplicative abelian group, k a nonnegative integer such that k divides $|G|$ and that k and $\lambda := |G|/k$ are coprime, then*

1. *the order of G^k is λ;*
2. *the order of the quotient group G/G^k is k;*
3. *$G^k = \left\{x \in G,\ x^\lambda = 1\right\}$;*
4. *If g is an element of G of order k then G/G^k is cyclic and $G/G^k = \langle \pi(g) \rangle$ where π denotes the canonic surjection $\pi : G \to G/G^k$.*

Proof (sketch). We use the decomposition of G in a direct sum of cyclic groups, and the fact that in a cyclic group of order n, the equation $x^k = 1$ has zero or $\gcd(n, k)$ roots. As a consequence, there are k k^{th} roots of unity in G and the kernel of the map $x \mapsto x^k$ has order k. This proves 1. and 2.; to prove 3. and 4., one uses the fact that λ and k are coprime. □

From this theorem, one can also deduce that G^λ has order k and that G^λ is actually the subgroup of k^{th} roots of unity of G. Note that g will be a generator of G^λ, *i. e.*, $G^\lambda = \langle g \rangle$. One can see that there is an isomorphism:

$$G^\lambda \times G^k \xrightarrow{\sim} G.$$

The evaluation of this isomorphism if easy: one simply multiply the two elements. The decomposition of an element of G in a product of a k^{th} root of unity by a k^{th} power is less obvious, unless one knows the values of λ and k. As these integers are coprime, there exists μ and ν such that $\mu\lambda + \nu k = 1$ and $c = \left(c^\mu\right)^\lambda \left(c^\nu\right)^k$. In the following, we are going to use this isomorphism to build the trapdoor function. Before that, we define a decision problem.

Definition 1. *We will call the decision residuosity problem of degree k in G, and will denote* $\mathrm{Res}_{G,k,g}$*, the following problem: Given c an element of G and g an element of order k*[1]*, decide whether $c \in G^k$ or not.*

We want to build an homomorphic encryption whose semantic security is based on the difficulty of the decision residuosity problem of degree k in G. This construction will generalize, among others, the system of Paillier (cf. [Pai99]) where $G = \left(\mathbf{Z}/n^2\mathbf{Z}\right)^\times$ with n an RSA integer and $k = n$.

Public Key The group G, the integer k and the element g will be public. Plaintext messages will be the elements of $\mathbf{Z}/k\mathbf{Z}$. We will suppose known an efficient algorithm to generate random elements of G^k, and an efficient algorithm to compute the discrete logarithm to base g in $\langle g \rangle$.

Encryption Primitive

$$\mathcal{E}_{G,k,g} \ : \ \begin{cases} \mathbf{Z}/k\mathbf{Z} \longrightarrow G \\ m \quad \longmapsto g^m \rho \end{cases}$$

where ρ is a random element of G^k.

According to Theorem 1, 4., if π denotes the canonic surjection $\pi : G \to G/G^k$, $\pi(g)$ is a generator of the quotient group G/G^k. So if $c \in G$ is an encryption of $m \in \mathbf{Z}/k\mathbf{Z}$, we will have

$$m = \log_{\pi(g)} \left(\pi(c)\right).$$

As a consequence, the decryption function associated to $\mathcal{E}_{G,k,g}$ will be a surjective morphism from $(G, \times)$ to $(\mathbf{Z}/k\mathbf{Z}, +)$, and a cryptosystem based on the $\mathcal{E}_{G,k,g}$ primitive will be additively homomorphic. As the scheme is homomorphic, it also enjoys the "self-blinding" property: given c an encryption of m, one can produce another valid ciphertext c' of m by computing $c' := c\rho'$, where ρ' is a random element of G^k.

Private Key and Decryption Algorithm The integer λ is a trapdoor for the $\mathcal{E}_{G,k,g}$ function. Let $c \leftarrow \mathcal{E}_{G,k,g}(m)$. There exists an element $\rho \in G^k$ such that $c = g^m\rho$. According to Theorem 1, 3., $c^\lambda = g^{m\lambda}$. Thanks to the public algorithm for the discrete logarithm problem in $\langle g \rangle$, we can recover $m\lambda$ in the ring $\mathbf{Z}/k\mathbf{Z}$, and them m, as λ and k are coprime.

One-Wayness Let us define a new computational problem.

[1] This condition is technical, in order to prove the equivalence in Theorem 3. We will see that in practice, (cf. section 4), given G and k, it will be easy to find an element of order k in G.

Definition 2. *Given c an element of G we will call the residuosity class of degree k of c the element m of $\mathbf{Z}/k\mathbf{Z}$ such that $m = \log_{\pi(g)}\left(\pi(c)\right)$. We will denote* $\mathrm{Class}_{G,k,g}$*, the problem of computing the residuosity class of degree k of elements of G.*

A scheme built from the $\mathcal{E}_{G,k,g}$ function will be one-way if and only if the $\mathrm{Class}_{G,k,g}$ problem is hard. It is easy to see that this problem is random self-reducible (so all the instances of the problem have the same complexity) and does not depend of the choice of the element g of order k, thanks to the properties of the discrete logarithm.

In the decryption algorithm, we have seen that one can decrypt an encryption $c = g^m\rho$ of m thanks to the knowledge of λ. It is also possible to decrypt c by computing the element x of G such that $x^k \equiv c \pmod{G^\lambda}$. Note that x is indeed unique modulo $G^\lambda = \langle g\rangle$, the subgroup of k^{th} roots of unity. As

$$m = \log_{\pi(g)}\left(\pi(c)\right) = \log_{\pi(g)}\left(\pi(c/x^k)\right),$$

and as c/x^k is an element of $G^\lambda = \langle g\rangle$, one can recover m by computing the discrete logarithm of c/x^k to base g in $\langle g\rangle$. As a consequence of the existence of this decryption process, we define another computational problem in order to analyse the $\mathrm{Class}_{G,k,g}$ problem.

Definition 3. *We will denote* $\text{C–RSA}_{G,k}$*, the following problem: Given c an element of G, find x such that $x^k \equiv c \pmod{G^\lambda}$.*

Remark 1. If one knows how to manipulate the elements of G/G^λ and to lift them in G, the $\text{C–RSA}_{G,k}$ problem is equivalent to the problem of the local inversion of the automorphism $x \mapsto x^k$ of G/G^λ, which is a generalization of the RSA function (G/G^λ has order λ which is prime to the exponent k).

If one knows λ, *i. e.*, the order of G, one can solve the $\text{C–RSA}_{G,k}$ problem: given $c \in G$, the element

$$x := c^{k^{-1} \mod \lambda}$$

verifies $x^k \equiv c \pmod{G^\lambda}$. As a consequence, we can state the following theorem which generalizes Theorem 1 and 2 of [Pai99].

Theorem 2. *Let G be a finite multiplicative abelian group, k a nonnegative integer such that k divides $|G|$ and that k and $|G|/k$ are coprime, and let g be an element of G of order k. We have the following reductions:*

$$\mathrm{Class}_{G,k,g} \overset{\mathcal{P}}{\Longleftarrow} \left(\text{C–RSA}_{G,k} \wedge \mathrm{Dlog}_{\langle g\rangle}\right) \overset{\mathcal{P}}{\Longleftarrow} \left(\mathrm{Order}_G \wedge \mathrm{Dlog}_{\langle g\rangle}\right).$$

where $\mathrm{Dlog}_{\langle g\rangle}$ *denotes the discrete logarithm problem in $\langle g\rangle$ and* Order_G *the problem of computing $|G|$.*

Remark 2. The problem $\mathrm{Dlog}_{\langle g\rangle}$ appears in the previous theorem for completeness, but in practice, as we said earlier, we will hope that this problem is easy in order to be able to decrypt efficiently.

Semantic Security

Theorem 3. *Let G be a finite multiplicative abelian group, k a nonnegative integer such that k divides $|G|$ and that k and $|G|/k$ are coprime, and let g be an element of G of order k. An encryption scheme built from the $\mathcal{E}_{G,k,g}$ primitive is semantically secure against Chosen-Plaintext Attacks if and only there exists no polynomial algorithm to solve the decision residuosity problem of degree k in G.*

Proof. To prove that a scheme is semantically secure, one can use the "real or random property": *i. e.*, prove that no polynomial time algorithm can distinguish an encryption of a chosen message, m, from an encryption of a random message. In our construction, an encryption of a random message is a random element of G. So we have to distinguish a random element of G from an encryption of m. As the scheme is homomorphic, this is equivalent to distinguish encryption of 0 in G, that is an element of G^k, in G. □

Generation of random elements of G^k To generate random elements of G^k, one can just take at random elements of G and raise them to the power of k. If one can work in the quotient group G/G^λ and lift the elements of this group in G, one can also use the isomorphism $G/G^\lambda \to G^k$, $x \mapsto x^k$. The encryption function becomes:

$$\mathcal{E}'_{G,k,g} \; : \; \begin{cases} \mathbf{Z}/k\mathbf{Z} \times G/G^\lambda & \xrightarrow{\sim} & G \\ (m \quad , \quad \rho) & \longmapsto & g^m \rho^k \end{cases}$$

It is trivial to see that $\mathcal{E}'_{G,k,g}$ is a group isomorphism.

Remark 3. If one can not generate random elements of G or random elements of G/G^λ, a solution to generate elements of G^k is to publish an element ρ of G^k of high order and to generate others k^{th} powers by raising ρ to a random power. Note that in this case, the semantic security of the scheme relies on a slightly different problem: the decision problem of distinguishing the elements of $\langle \rho \rangle$ in G.

IND-CCA2 variant in the standard model The system of Paillier, generalized by the previous construction, has been used in [CS02] to build an IND-CCA2 cryptosystem in the standard security model by an application of a general framework built from a subset membership problem and some projective hash families. Our construction with the decision residuosity problem can be easily adapted to fit the framework of [CS02] with only one extra hypothesis. We refer the reader to [CS02] for definitions.

Suppose that the group G is cyclic. Denote $\mathcal{H} = \mathrm{Hom}(G, G)$. Then, from the example 7.4.2 in [CS02], one can prove that the group system $\mathbf{G} := (\mathcal{H}, G, G^k, G)$ is diverse and that the projective hash family derived from $\mathbf{G}$ is $1/\tilde{p}$-universal where $\tilde{p}$ is the smallest prime dividing λ (Theorem 2 of [CS02]). With this, we get

an $1/\tilde{p}$-universal hash proof system (UHPFS). Following the general construction of [CS02], from this UHPFS, one can build a scheme that is IND-CCA2 secure in the standard model, providing that $\tilde{p}$ is sufficiently large, and assuming the hardness of the decision residuosity problem.

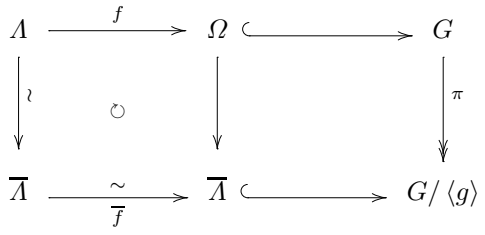
3 Non-homomorphic Trapdoor Function

In this section, we change the previous construction in order to reduce the encryption and decryption costs. The idea is to replace the most costly step of the encryption process: the evaluation of the function $x \mapsto x^k$. This exponentiation will be replaced by a function f, cheaper to evaluate. This idea corresponds to the scheme of [CGH$^+$01], which uses a function built from the RSA function. By doing this, we will loose the homomorphic property.

We have to build the function f in order to still have an efficient way to decrypt. In the previous section, we saw that if was possible to decrypt by inverting the automorphism $x \mapsto x^k$ of $G/\langle g \rangle$. We are going to replace this automorphism by a known determinist trapdoor function $\overline{f}$, permutation of a subset of $G/\langle g \rangle$. The function f will be built from $\overline{f}$. As a consequence, the construction of this section will enable oneself to build a probabilistic trapdoor function from a determinist one.

Construction of f We suppose that we know a trapdoor permutation $\overline{f}$ of a subset $\overline{\Lambda}$ of $G/\langle g \rangle$. In this section, π will denote the canonical surjection $G \to G/\langle g \rangle$. We suppose that π is computable at low cost for anyone who knows G and g.

We define $\Omega := \pi^{-1}(\overline{\Lambda})$ and Λ, a subset of Ω such that Λ be a representative set of $\overline{\Lambda}$, *i. e.*, $\pi(\Lambda) = \pi(\Omega) = \overline{\Lambda}$ and π is a bijection from Λ to $\overline{\Lambda}$. We suppose that it is easy to find the unique representative of a class of $\overline{\Lambda}$ in Λ. Let f be a function from Λ to Ω such that the following diagram commutes:



Public Key The group G, the integer k and the element g will be public. Plaintext messages will be the elements of $\mathbf{Z}/k\mathbf{Z}$. We will suppose known an efficient algorithm that returns random elements of Λ, an efficient algorithm to evaluate the function f, and an efficient algorithm to compute the discrete logarithm to base g in $\langle g \rangle$.

Encryption Primitive

$$\mathcal{E}_{G,f,g} \ : \ \begin{cases} \mathbf{Z}/k\mathbf{Z} \times \Lambda \longrightarrow \quad \Omega \\ (m \quad , \ \rho) \longmapsto g^m f(\rho) \end{cases}$$

It is easy to see that $\mathcal{E}_{G,f,g}$ is well defined as $\langle g \rangle f(\Lambda) = \Omega$ and bijective: suppose that $g^{m_1} f(\rho_1) = g^{m_2} f(\rho_2)$ then $\pi\big(f(\rho_1)\big) = \pi\big(f(\rho_2)\big)$. As $\pi \circ f = \overline{f} \circ \pi$, $\pi \circ f$ is bijective so $\rho_1 = \rho_2$. As a consequence, $m_1 = m_2$ in $\mathbf{Z}/k\mathbf{Z}$.

Private Key and Decryption Algorithm The private key is the trapdoor that allows to invert $\overline{f}$. Let $c \in \Omega$ be a ciphertext. To decrypt c, we have to recover $m \in \mathbf{Z}/k\mathbf{Z}$ such that there exists $\rho \in \Lambda$ such that $c = g^m f(\rho)$. We have $\pi(c) = \pi \circ f(\rho) = \overline{f} \circ \pi(\rho)$. With the private key we recover $\pi(\rho)$ and then its representative $\rho \in \Lambda$. Then, by computing $c/f(\rho)$ we get g^m and then m thanks to the algorithm for the discrete logarithm problem in $\langle g \rangle$.

One-Wayness Let us give the definition of the problem on which relies the one-wayness of a scheme built from the $\mathcal{E}_{G,f,g}$ primitive.

Definition 4. *We will denote* $\mathrm{Class}_{G,f,g}$ *the following problem: given* c *an element of* Ω*, find* $m \in \mathbf{Z}/k\mathbf{Z}$ *such that there exists* ρ *in* Λ *such that* $c = g^m f(\rho)$*.*

Now we define two others problems and we give a theorem that links the three problems.

Definition 5. *We will denote* $\mathrm{Hensel}_{G,g}{-}f$ *the following problem: given* $\overline{c}$ *an element of* $\overline{\Lambda} = \pi(\Omega)$*, find the element* c *of* Ω *such that* $c = f(\rho)$ *where* ρ *is the element of* Λ *such that* $\overline{c} = \pi(f(\rho))$*. We will denote* $\mathrm{Inv}-\overline{f}$ *the problem of local inversion of the trapdoor* $\overline{f}$*,* i. e.*, given* $\overline{c}$ *an element of* $\overline{\Lambda}$*, find* $\overline{\rho}$ *in* $\overline{\Lambda}$ *such that* $\overline{c} = \overline{f}\,(\overline{\rho})$*.*

Theorem 4. *Let* G *be a finite multiplicative abelian group,* k *a nonnegative integer,* g *an element of* G *of order* k*,* $\overline{\Lambda}$ *a subset of* $G/\langle g \rangle$*,* Λ *a representative set of* $\overline{\Lambda}$ *in* G *and* $\overline{f}$ *a trapdoor permutation of* $\overline{\Lambda}$*. We denote* π *the canonic surjection from* G *to* $G/\langle g \rangle$ *and* f *a function from* Λ *to* $\Omega := \pi^{-1}(\overline{\Lambda})$ *such that* $\pi \circ f = \overline{f} \circ \pi$*. We have the following relations:*

$$\mathrm{Class}_{G,f,g} \overset{\mathcal{P}}{\Longleftrightarrow} \Big(\mathrm{Hensel}_{G,g}{-}f \ \wedge \ \mathrm{Dlog}_{\langle g \rangle}\Big) \overset{\mathcal{P}}{\Longleftarrow} \Big(\mathrm{Inv}-\overline{f} \ \wedge \ \mathrm{Dlog}_{\langle g \rangle}\Big)$$

where $\mathrm{Dlog}_{\langle g \rangle}$ *denotes the discrete logarithm problem in* $\langle g \rangle$*.*

Proof. We prove the left equivalence, the reduction on the right will follow from the decryption algorithm. Suppose that we have two oracles that solve respectively the $\mathrm{Hensel}_{G,g}{-}f$ and $\mathrm{Dlog}_{\langle g \rangle}$ problems. Let c be an element of Ω. We want to recover $m \in \mathbf{Z}/k\mathbf{Z}$ in the decomposition $c = g^m f(\rho)$ with $\rho \in \Lambda$. We have $\pi(c) = \pi\big(f(\rho)\big)$. We give $\pi(c)$ to the oracle for the $\mathrm{Hensel}_{G,g}{-}f$ problem.

We get the element c' of Ω such that $c' = f(\rho)$. Given c/c', the oracle for the $\mathrm{Dlog}_{\langle g \rangle}$ problem returns m.

For the opposite way, we have an oracle that solve the $\mathrm{Class}_{G,f,g}$ problem. If g' is an element of $\langle g \rangle$, we take a random element ρ in Λ. By giving $g'f(\rho)$ to the oracle, we get m, the discrete logarithm of g' to base g. Suppose now that we have an element $\overline{c}$, of $\overline{\Lambda}$, for which we want to solve the $\mathrm{Hensel}_{G,g}{-}f$ problem. We take m' at random in $\mathbf{Z}/k\mathbf{Z}$. We denote c the element of Λ such that $\pi(c) = \overline{c}$. We give $g^{m'}c \in \Omega$ to the oracle (note that it is a random query for the oracle). We then get from the oracle the element m of $\mathbf{Z}/k\mathbf{Z}$ such that $g^{m'}c = g^m f(\rho)$ with ρ element of Λ. As $\pi(g^{m'}c) = \overline{c} = \pi\big(f(\rho)\big)$, the element $g^{m'-m}c$ is a correct answer to the $\mathrm{Hensel}_{G,g}{-}f$ problem. □

Remark 4. This theorem establishes that the security of a system built from the $\mathcal{E}_{G,f,g}$ primitive relies on the security of the trapdoor $\overline{f}$. For the Catalano *et al.* scheme, (cf. [CGH+01] and section 4), an instance of this construction in which $\overline{f}$ is the classic RSA function, the result of [CNS02] states that the equivalence actually holds. Unfortunately, the proof of this result uses intrinsic properties of the RSA function and can not be exploited for the generalized case.

Semantic Security

Definition 6. *Let us denote* $\mathrm{Res}_{G,f,g}$*, the problem of distinguishing the elements of* $f(\Lambda)$ *in* Ω*.*

Theorem 5. *An encryption scheme built from the* $\mathcal{E}_{G,f,g}$ *primitive is semantically secure against Chosen-Plaintext Attacks if and only there exists no polynomial algorithm that solve the decision* $\mathrm{Res}_{G,f,g}$ *problem.*

Proof. A scheme built from the construction of the previous section, and a scheme built from $\mathcal{E}_{G,f,g}$ shares a similar property:

$$(c \leftarrow \mathcal{E}_{G,f,g}(m)) \iff \left(\frac{c}{g^m} \in f(\Lambda)\right).$$

As a consequence, the proof of Theorem 3 can be easily adapted. □

IND-CCA2 variant in the ROM Using standard techniques, one can modify the $\mathcal{E}_{G,f,g}$ primitive to make it resistant against adaptive chosen-ciphertext attacks in the random oracle model. One can simply add $h(m, \rho)$ to the ciphertext, where h is an hash function viewed like a random oracle. One can also use the Fujisaki-Okamoto conversion (cf. [FO99]) in order to reduce the ciphertexts size.

4 Applications

We will use the constructions of sections 2 and 3 in algebraic groups over $(\mathbf{Z}/n^s\mathbf{Z})^\times$ where s is a nonnegative integer. RSA integers will allow to use the

group order as a trapdoor. This would lead to an historical of probabilistic cryptography based on factoring.

The idea of working modulo n^s with $s > 1$ is due to Paillier (cf. [Pai99]) and Damgård and Jurik (cf. [DJ01]) for the case $s > 2$. As we shall see in the following, this enables oneself to meet the hypothesis of the generic construction: the subgroup of n^{th} roots of unity of the group considered will be the kernel of the reduction modulo n, and its elements will be easy to describe. As a consequence, we will exhibit an element g of order n such that the discrete logarithm problem in $\langle g \rangle$ is easy.

4.1 Schemes in Quotients of Z

The first probabilistic cryptosystem, proposed by Goldwasser and Micali in 1984 (cf. [GM84]) is very similar to the generic construction explained in section 2. Its semantic security is based on a well-known problem, the quadratic residuosity problem (*i. e.*, $k = 2$), but its expansion is awful as one bit is encrypted with $|n|_2$ bits.

$G = (\mathbf{Z}/n\mathbf{Z})^\times$, k prime, $k \mid \varphi(n)$, Benaloh (88) The cryptosystem of Goldwasser-Micali has been generalized by Benaloh in [Ben88]. The group G is now $(\mathbf{Z}/n\mathbf{Z})^\times$, the integer k is an odd prime such that k divides $\varphi(n)$ and k does not divide $\lambda := \varphi(n)/k$. Let g be an element of order k, to encrypt an element $m \in \mathbf{Z}/k\mathbf{Z}$, one uses the encryption primitive $\mathcal{E}_{G,k,g}$ defined in section 2: an encryption of m is $g^m r^k$ where r is a random element of $(\mathbf{Z}/n\mathbf{Z})^\times$. The drawback of this system is that k has to be small because there is no particular algorithm for computing discrete logarithms in $\langle g \rangle$. As a consequence, the expansion of the system, $|n|_2 \,/\, |k|_2$ remains high.

$G = (\mathbf{Z}/n\mathbf{Z})^\times$, k smooth, $k \mid \varphi(n)$, Naccache-Stern (98) Naccache and Stern have improved in [NS98] the previous system. They still use $G = (\mathbf{Z}/n\mathbf{Z})^\times$ but k is chosen smooth. This leads to a more efficient algorithm for computing discrete logarithms in $\langle g \rangle$ by using the Pohlig-Hellman algorithm. Naccache and Stern state that the expansion can be reduced to 4.

Okamoto and Uchiyama have proposed in [OU98] to work modulo $n = p^2 q$. The following system is an improvement of their proposal.

$G = \left(\mathbf{Z}/n^2\mathbf{Z}\right)^\times$, $k = n$, Paillier (99) The system of Paillier (cf. [Pai99]) corresponds to an application of the $\mathcal{E}_{G,k,g}$ encryption function with $G = \left(\mathbf{Z}/n^2\mathbf{Z}\right)^\times$, and $k = n$. If we suppose that $\gcd(n, \varphi(n)) = 1$, as $|G| = n\varphi(n)$, k divides $|G|$ and k is prime to $\lambda := |G| \,/ k = \varphi(n)$. One can see that the subgroup G^λ of G, the subgroup of n^{th} roots of unity, is the kernel of the surjective homomorphism: $\left(\mathbf{Z}/n^2\mathbf{Z}\right)^\times \to (\mathbf{Z}/n\mathbf{Z})^\times$. As a consequence, this subgroup is a cyclic group of

order n, generated by $g :\equiv 1+n \pmod{n^2}$. Moreover, the discrete logarithm problem in $\langle g \rangle$ is trivial as for all $i \in \mathbf{Z}/n\mathbf{Z}$, $g^i \equiv 1+in \pmod{n^2}$. To encrypt, one can use the isomorphism $\mathcal{E}'_{G,k,g}$ defined in section 2. The encryption function is thus the isomorphism:

$$\begin{cases} \mathbf{Z}/n\mathbf{Z} \times (\mathbf{Z}/n\mathbf{Z})^\times & \xrightarrow{\sim} & \left(\mathbf{Z}/n^2\mathbf{Z}\right)^\times \\ (m \ , \ r) & \longmapsto & g^m r^n \end{cases}$$

where m is the plaintext and r a random element. The trapdoor is $\varphi(n)$, *i. e.*, the factorization of n, and the decryption algorithm is the application of the generic algorithm described in section 2. The expansion of this system is 2.

An IND-CCA2 variant of this scheme has been designed by Cramer and Shoup in [CS02]. As previously said, this variant can also be obtained from the construction of section 2, if the group G is cyclic. One can have a cyclic group by choosing Sophie Germain primes for p and q: with this choice there exists a cyclic group of order $n\varphi(n)/2$ in $\left(\mathbf{Z}/n^2\mathbf{Z}\right)^\times$, isomorphic to $\mathbf{Z}/n\mathbf{Z} \times (\mathbf{Z}/n\mathbf{Z})^+$, where $(\mathbf{Z}/n\mathbf{Z})^+$ is the subgroup of elements of $\left(\mathbf{Z}/n^2\mathbf{Z}\right)^\times$ that have a positive Jacobi symbol (see [CS02] subsection 8.2 for details).

Damgård and Jurik have proposed in [DJ01] a generalization of the Paillier cryptosystem. They work in the group $G = \left(\mathbf{Z}/n^{s+1}\mathbf{Z}\right)^\times$ with $s > 1$ and $k = n^s$. One obtains a system that allows oneself to encrypt messages of arbitrary length (by increasing s). This can have many applications (cf. [DJ01,Jur03]). The expansion of this scheme is $1 + 1/s$.

***G* = $(\mathbf{Z}/n^2\mathbf{Z})^\times$, $\overline{f}$ = *RSA*, Catalano *et al.* (01)** In [CGH+01], Catalano, Gennaro *et al.* have proposed a probabilistic encryption scheme presented like a fast variant of the Paillier cryptosystem. With the help of the generic construction of section 3, one can also see this scheme as a probabilistic version of the RSA cryptosystem. Let $G = \left(\mathbf{Z}/n^2\mathbf{Z}\right)^\times$, and $g \equiv 1+n \pmod{n^2}$. The quotient group $G/\langle g \rangle$ is isomorphic to $(\mathbf{Z}/n\mathbf{Z})^\times$. We denote respectively Ω and Λ, the sets of elements of G and $G/\langle g \rangle$, *i. e.*,

$$\Omega := \left\{ r \in \mathbf{N},\, 0 < r < n^2,\, \gcd(r,n) = 1 \right\},$$

and

$$\Lambda := \left\{ r \in \mathbf{N},\, 0 < r < n,\, \gcd(r,n) = 1 \right\}.$$

With the notation of section 3, one actually has $\overline{\Lambda} := \Lambda$, and the set Λ is a representative set of the classes of Ω modulo n. Let e be an integer prime to $\varphi(n)$, the RSA function, $\overline{f} : x \mapsto (x^e \bmod n)$ is a permutation of Λ. This function is lifted from Λ to Ω by considering $f : x \mapsto (x^e \bmod n^2)$, so that $\pi \circ f = \overline{f} \circ \pi$. To encrypt, we use the $\mathcal{E}_{G,f,g}$ primitive and we obtain the following encryption function:

$$\begin{cases} \mathbf{Z}/n\mathbf{Z} \times \Lambda & \longrightarrow & \Omega \\ (m \quad , \ r) & \longmapsto & g^m r^e \bmod n^2 \end{cases}$$

where m is the plaintext and r a random element. The decryption is done has described in section 3: one reduces the ciphertext modulo n and recover r by inverting the RSA function, thanks to the knowledge of d, the inverse of e modulo $\varphi(n)$, the trapdoor of the function $\overline{f}$.

Remark 5. The previous scheme can be generalized by taking $G = \left(\mathbf{Z}/n^{s+1}\mathbf{Z}\right)^{\times}$ with $s > 1$, in order to decrease the expansion. One has to redefine the set Ω accordingly and to lift $\overline{f}$ in $f : x \mapsto x^e \bmod n^{s+1}$.

One can apply the non-homomorphic construction of section 3, with all the known trapdoor functions of $\mathbf{Z}/n\mathbf{Z}$, *e. g.*, Demytko's (cf. [Dem94]) or LUC (cf. [SL93]). Note that with the LUC function, one gets a scheme already proposed in [Cas07].

4.2 Schemes in Elliptic Curves over $\mathbf{Z}/n^{s+1}\mathbf{Z}$

Both constructions can be applied in elliptic curves. This leads respectively to the systems of Galbraith (cf. [Gal02]) and Galindo, Martín *et al.* (cf. [GMMV03]).

$G = E/(\mathbf{Z}/n^{s+1}\mathbf{Z})$, $k = n^s$, Galbraith (02) In [Gal02], Galbraith has adapted the Damgård and Jurik scheme (and hence the Paillier scheme) in elliptic curves. This homomorphic scheme can also be viewed as an application of the $\mathcal{E}_{G,k,g}$ primitive of section 2. The group G is the group of points of an elliptic curve over $\mathbf{Z}/n^{s+1}\mathbf{Z}$, *i. e.*, the set of elements $(X : Y : Z)$ of $\mathbf{P}^2(\mathbf{Z}/n^{s+1}\mathbf{Z})$ such that

$$Y^2Z = X^3 + aXZ^2 + bZ^3,$$

where a and b are two elements of $\mathbf{Z}/n^{s+1}\mathbf{Z}$ such that $4a^3 + 27b^2$ is invertible. We denote this group $E_{a,b}/(\mathbf{Z}/n^{s+1}\mathbf{Z})$ (See [Gal02] for more details on elliptic curves over rings).

One can prove that the order of this group is $n^s\,|E_{a,b}/(\mathbf{Z}/n\mathbf{Z})|$. By taking $k = n^s$, and supposing that n^s is prime to $\lambda := |E_{a,b}/(\mathbf{Z}/n\mathbf{Z})|$, one can apply the generic construction. The tricky part of this adaptation is to find an element g of G of order n^s such that the discrete logarithm problem is easy in $\langle g\rangle$. Once again, we look for g in the kernel of the reduction modulo n from $E_{a,b}/(\mathbf{Z}/n^{s+1}\mathbf{Z})$ to $E_{a,b}/(\mathbf{Z}/n\mathbf{Z})$. One can see that the element $g := (n : 1 : n^3 + an^7 + bn^9 + \cdots)$ is of order n^s and that discrete logarithms are easy to compute in $\langle g\rangle$ (again see [Gal02] for details on this element g, on the subgroup $\langle g\rangle$ and how to compute the group law in this subgroup and in G).

To encrypt a message m of $\mathbf{Z}/n^s\mathbf{Z}$, one use the $\mathcal{E}_{G,k,g}$ primitive of section 2: a ciphertext for m is a point of the form $m.g + P$ where P is a random "$n^{s^{\text{th}}}$ power". To produce a such P, as it is difficult to produce an element of the curve without knowing the factorization of n, one can not take a random element of G or of $E_{a,b}/(\mathbf{Z}/n\mathbf{Z})$ and take it to the "power" n^s. Hence, we use the method exposed in Remark 3: a $n^{s^{\text{th}}}$ power is part of the public key.

A drawback of this scheme is its cost as one has to do costly scalar multiplications in elliptic curve over a huge base ring (as the security is based on factorization and not on the discrete logarithm problem, we can not reduce the size of this ring).

***G = E/(Z/n²Z), $\overline{f}$ = KMOV*, Galindo *et al.* (03)** In [GMMV03], Galindo, Martín *et al.* have proposed a non-homomorphic scheme based on the KMOV trapdoor permutation (cf. [KMOV92]). This scheme is not a direct adaptation of the generic construction of section 3 as the KMOV function is not a permutation of a subset of a group. Indeed, the KMOV function is a permutation of the set

$$\left\{(x,y) \in \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z},\ \left(y^2 - x^3\right) \in (\mathbf{Z}/n\mathbf{Z})^\times\right\},$$

and maps (x,y) to $e.(x,y)$, where the scalar multiplication is performed on the elliptic curve $E_{0,y^2-x^3}/(\mathbf{Z}/n\mathbf{Z})$ where e is prime to $(p+1)(q+1)$ and p and q are chosen congruent to 2 modulo 3 (it is hard to take points on a fixed curve without knowing p and q). So, one has to apply the generic construction with a group G that depends on the plaintext message. One define *ad hoc* subsets Λ and Ω of $\mathbf{Z}/n^2\mathbf{Z}$ and lift the KMOV function from Λ to Ω by computing $e.(x,y)$ in a curve modulo n^2. See [GMMV03] for more details.

Again, one can generalize this scheme by working modulo n^s with $s > 2$.

4.3 Additively Homomorphic Scheme in Quadratic Fields Quotients

In this subsection, we apply the generic construction of section 2 in another finite group, not widely used in cryptography, the group of norm 1 elements of a quadratic field modulo n. We will obtain the system only briefly sketched at the end of [Cas07].

Definition 7. *Let Δ be a non-square integer, and a an odd integer prime to Δ. We will denote $(\mathcal{O}_\Delta/a\mathcal{O}_\Delta)^\wedge$ the group of norm one elements of $\mathcal{O}_\Delta/a\mathcal{O}_\Delta$, where $\mathcal{O}_\Delta$ denotes the ring of integers of $\mathbf{Q}(\sqrt{\Delta})$. We will denote $\varphi_\Delta(a)$ the order of the group $(\mathcal{O}_\Delta/a\mathcal{O}_\Delta)^\wedge$.*

We refer the reader to [Cas07] for the basic properties of this group. We only recall that exponentiation can be efficiently computed in this group by using the Lucas sequence, and that if n is prime to Δ, then for $s > 1$, the order of $\left(\mathcal{O}_\Delta/n^{s+1}\mathcal{O}_\Delta\right)^\wedge$ is

$$\varphi_\Delta(n^{s+1}) = n^s\,\varphi_\Delta(n) = n^s\left(p - \left(\frac{\Delta}{p}\right)\right)\left(q - \left(\frac{\Delta}{q}\right)\right),$$

where $\left(\frac{\Delta}{p}\right)$ denotes the well-known Legendre symbol. Moreover, note that the group $(\mathcal{O}_\Delta/p^s\mathcal{O}_\Delta)^\wedge$ is cyclic (the same holds modulo q^s).

$\boldsymbol{G = \left(\mathcal{O}_\Delta/n^2\mathcal{O}_\Delta\right)^\wedge,\ k = n,}$ We apply the construction of section 2 with $G = \left(\mathcal{O}_\Delta/n^2\mathcal{O}_\Delta\right)^\wedge$, where Δ is a non-square integer prime to n. The order of G is $n\,\varphi_\Delta(n)$, so we set $k = n$ and $\lambda = \varphi_\Delta(n)$ and suppose that k and Λ are coprime.

Element of order n: As previously seen, we look for an element of order n in the kernel of the reduction modulo n from $\left(\mathcal{O}_\Delta/n^2\mathcal{O}_\Delta\right)^\wedge$ to $(\mathcal{O}_\Delta/n\mathcal{O}_\Delta)^\wedge$. This reduction is surjective by the Hensel Lemma. The element $g \equiv 1 + n\sqrt{\Delta} \pmod{n^2}$ is a generator of this kernel and g is indeed of order n as $g^r \equiv 1+nr\sqrt{\Delta} \pmod{n^2}$ for all integer r. As a consequence of this expression of g^r, the discrete logarithm problem in $\langle g\rangle$ is easy.

k^{th} powers generation: To simplify, we suppose that Δ is neither a square modulo p nor modulo q. It is easy to see that the map $\alpha \mapsto \alpha/\overline{\alpha}$ from $(\mathcal{O}_\Delta/n\mathcal{O}_\Delta)^\times$ to $(\mathcal{O}_\Delta/n\mathcal{O}_\Delta)^\wedge$ is surjective and that its kernel is $(\mathbf{Z}/n\mathbf{Z})^\times$. As a consequence, the map

$$\Psi : r \mapsto \frac{r+\sqrt{\Delta}}{r-\sqrt{\Delta}} = \frac{r^2+\Delta}{r^2-\Delta} + \frac{2r}{r^2-\Delta}\sqrt{\Delta},$$

from $\mathbf{Z}/n\mathbf{Z}$ to $(\mathcal{O}_\Delta/n\mathcal{O}_\Delta)^\wedge$ is well-defined, injective and is almost surjective (we only miss 1 and elements that allow to factor n (elements different from 1 and that are congruent to 1 modulo p or 1 modulo q). Moreover, the map $\beta \mapsto \beta^n$ from $(\mathcal{O}_\Delta/n\mathcal{O}_\Delta)^\wedge$ to G^n is an isomorphism. As a consequence, the map

$$\mathbf{Z}/n\mathbf{Z} \to G^n : r \mapsto \Psi(r)^n,$$

is still injective and almost surjective.

Encryption function: The encryption function is

$$\begin{cases} \mathbf{Z}/n\mathbf{Z} \times (\mathbf{Z}/n\mathbf{Z})^\times & \longrightarrow & G \\ (m\ ,\ r) & \longmapsto & g^m\Psi(r)^n \end{cases}$$

where m is the plaintext and r a random element, and the public key is (n, Δ) where $n = pq$ is an RSA integer, Δ is a non-square integer, prime to n and Δ is neither a square modulo p nor modulo q.

Decryption algorithm: The trapdoor is $\lambda = \varphi_\Delta(n)$. The decryption algorithm is the same as the generic one. Note that it can be sped up by using Chinese remaindering (this is true for all the others schemes presented in this paper).

Security: The one-wayness of the scheme is based on the $\text{Class}_{G,k,g}$ problem and the reductions of Theorem 2 hold. The semantic security is based on the the difficulty of distinguishing the elements of G^n in G (As the map $r \mapsto \Psi(r)^n$ is injective and almost surjective, almost all the element of G^n can be produced. The ones that are not produced are either easy to distinguish or allow to factor n).

Expansion: The cryptosystem expansion is 4, *a priori*, but can be reduced to 3. One defines a lifting L of the elements of $(\mathcal{O}_\Delta/n\mathcal{O}_\Delta)^\wedge$ in $\left(\mathcal{O}_\Delta/n^2\mathcal{O}_\Delta\right)^\wedge$. Then, an element α of $\left(\mathcal{O}_\Delta/n^2\mathcal{O}_\Delta\right)^\wedge$ is represented by the couple $(k, \alpha \bmod n) \in \mathbf{Z}/n\mathbf{Z} \times (\mathcal{O}_\Delta/n\mathcal{O}_\Delta)^\wedge$ with k such that $\alpha = (1+n\sqrt{\Delta})^k\, L(\alpha \bmod n)$. Note that the computation of this representation (by using the Hensel Lemmma) only costs a few multiplications and one inversion. This method can also be applied for the system of Galbraith.

Comparison with others additively homomorphic systems: In the following table, we compare this system with the Paillier and Galbraith schemes. The unity of complexity is the cost of a multiplication modulo n. We use the following estimations: a multiplication modulo n^2 costs as much as 3 multiplications modulo n (by using radix n representation), a multiplication modulo p^2 costs as much as a multiplication modulo n and three multiplications modulo p as much as a multiplication modulo n. An inversion modulo n costs as much as 10 multiplications modulo n. We have used Chinese remaindering for all the schemes.

Cryptosystem	Paillier	Galbraith	QF scheme
Group	$\left(\mathbf{Z}/n^2\mathbf{Z}\right)^\times$	$E/(\mathbf{Z}/n^2\mathbf{Z})$	$\left(\mathcal{O}_\Delta/n^2\mathcal{O}_\Delta\right)^\wedge$
Encryption	$\frac{9}{2}\left\|n\right\|_2 + 1$	$35\left\|n\right\|_2 + 3$	$9\left\|n\right\|_2 + 20$
Decryption	$\frac{3}{2}\left\|n\right\|_2 + \frac{5}{3}$	$21\left\|n\right\|_2 + \frac{5}{3}$	$3\left\|n\right\|_2 + \frac{4}{3}$

We see that the scheme in quadratic fields is much more faster than the system that uses elliptic curves, thanks to efficient exponentiation using Lucas sequences. This scheme complexity is not far from the Paillier cryptosystem (the factor two is inherited from the respective costs of exponentiation in $\mathbf{Z}/n^2\mathbf{Z}$ and in $\left(\mathcal{O}_\Delta/n^2\mathcal{O}_\Delta\right)^\wedge$). As a result, this scheme is still practical.

If all the schemes are based on factorization, from Theorem 2, we see that the intermediate problems on which the one-wayness of the schemes are based are not the same. For Paillier, it is the RSA_n problem *i. e.*, the inversion of the map $x \mapsto x^n$ in $(\mathbf{Z}/n\mathbf{Z})^\times$. For the presented scheme, it is the adaptation of this problem in $(\mathcal{O}_\Delta/n\mathcal{O}_\Delta)^\wedge$, *i. e.*, the inversion of the map $\alpha \mapsto \alpha^n$. We do not know if one problem is easier than the other (as the only known way to solve them is to factor n), but this scheme brings some diversity as the Paillier scheme is almost the only practical additively homomorphic scheme known. Another advantage of this scheme is that one has more choice for the public key than for the Paillier scheme: one can choose freely the modulus n *and* the discriminant Δ.

Generalization: This scheme can also be generalized by working modulo n^{s+1} with $s > 1$ in order to encrypt messages of $\mathbf{Z}/n^s\mathbf{Z}$. One has only to find an element g of order n^s and an efficient algorithm for the discrete logarithm problem.

One can see that the following element:

$$g := n\sqrt{\Delta} + 1 + \frac{1}{2}\Delta n^2 - \frac{1}{2^3}\Delta^2 n^4 + \frac{1}{2^4}\Delta^3 n^6 - \frac{5}{2^7}\Delta^4 n^8 + \cdots$$

obtained by successive applications of the Hensel Lemma is indeed of order n^s. Given g^k, one can still compute the discrete logarithm k at low cost, by computing recursively $k \mod n^2$, $k \mod n^4, \ldots$

IND-CCA2 *variant of this scheme:* Similarly to the Paillier cryptosystem, one can design a variant that is IND-CCA2 in the standard model. A cyclic group is obtained in the same way, by using primes p and q such that $(p - (\Delta/p))/2$ and $(q - (\Delta/q))/2$ are both primes. Then, one obtains a subgroup of order $n\,\varphi_\Delta(n)/2$. Note that some optimisations used by Cramer and Shoup in [CS02] to get compact ciphertexts for the adaptation of the Paillier scheme can also be done here as $\left(\mathcal{O}_\Delta/n^2\mathcal{O}_\Delta\right)^\wedge$ is very similar to $\left(\mathbf{Z}/n^2\mathbf{Z}\right)^\times$.

5 Conclusion

We have proposed two generic constructions that generalize many probabilistic cryptosystems already proposed. This process helps to capture the ideas behind these schemes. In particular, we have seen that the efficient homomorphic cryptosystem proposed in the group of norm 1 elements of a quadratic field is very similar to the Paillier scheme and can serve to construct an IND-CCA2 secure system in the standard model, which is a rare object. We hope that these generic constructions will help to propose new probabilistic cryptosystems. One possible domain of application could be class groups of quadratic orders such as those used in the NICE cryptosystem (cf. [PT00]).

References

[Ben88] J.C. Benaloh. *Verifiable Secret-Ballot Elections*. PhD thesis, Yale University, 1988.

[BFP+01] O. Baudron, P. Fouque, D. Pointcheval, G. Poupard, and J. Stern. Practical multi-candidate election system. In *Proc. of PODC' 01*, 2001.

[Cas07] G. Castagnos. An efficient probabilistic public-key cryptosystem over quadratic fields quotients. *Finite Fields Appl.*, 13(3):563–576, 2007.

[CGH+01] D. Catalano, R. Gennaro, N. Howgrave-Graham, and P. Q. Nguyen. Paillier's cryptosystem revisited. In *Proceedings of the 8th ACM Conference on Computer and Communications Security*, pages 206–214, 2001.

[CNS02] Dario Catalano, Phong Q. Nguyen, and Jacques Stern. The Hardness of Hensel Lifting: The Case of RSA and Discrete Logarithm. In *Advances in Cryptology* - ASIACRYPT *2002*, pages 299–310, 2002.

[CS02] Ronald Cramer and Victor Shoup. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In *EUROCRYPT '02: Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques*, pages 45–64, London, UK, 2002. Springer-Verlag.

[Dem94] N. Demytko. A New Elliptic Curve Based Analogue of RSA. In T. Helleseth, editor, *Advances in Cryptology* - EUROCRYPT *'93*, volume 765 of *Lect. Notes Comput. Sci.*, pages 40–49. Springer, 1994.

[DJ01] I. Damgård and M. J. Jurik. A Generalisation, a Simplification and some Applications of Paillier's Probabilistic Public-Key System. In *PKC' 01*, volume 1992 of *LNSC series*, 2001.

[FO99] E. Fujisaki and T. Okamoto. How to Enhance the Security of Public-Key Encryption at Minimum Cost. In *PKC '99*, volume 1560 of *Lecture Notes in Computer Science*, page 634. Springer-Verlag, 1999.

[Gal02] Steven D. Galbraith. Elliptic Curve Paillier Schemes. *Journal of Cryptology*, 15 (2): pages 129–138, 2002.

[GM84] S. Goldwasser and S. Micali. Probabilistic Encryption. *J. Comput. Syst. Sci.*, 28:270–299, 1984.

[GMMV03] D. Galindo, S. Martín, P. Morillo, and J.L. Villar. An Efficient Semantically Secure Elliptic Curve Cryptosystem Based on KMOV. In *Proc. of WCC' 03*, pages 213–221, 2003.

[Jur03] Mads Jurik. *Extensions to the Paillier Cryptosystem with Applications to Cryptological Protocols*. PhD thesis, Aarhus University, 2003.

[KMOV92] K. Koyama, U. M. Maurer, T. Okamoto, and S. A. Vanstone. New Public-Key Schemes Based on Elliptic Curves over the Ring Z_n. In J. Feigenbaum, editor, *Advances in Cryptology* - CRYPTO *'91*, volume 576 of *Lect. Notes Comput. Sci.*, pages 252–266. Springer, 1992.

[Lip05] H. Lipmaa. An Oblivious Transfer Protocol with Log-Squared Communication. In *In The 8th Information Security Conference (ISC'05)*, volume 3650 of *Lecture Notes in Computer Science*, pages 314–328, 2005.

[NS98] D. Naccache and J. Stern. A New Public Key Cryptosystem Based on Higher Residues. In *Proceedings of the Third ACM Conference on Computer and Communications Security*, pages 59–66, 1998.

[NSNK06] Lan Nguyen, Rei Safavi-Naini, and Kaoru Kurosawa. Verifiable shuffles: a formal model and a Paillier-based three-round construction with provable security. *Int. J. Inf. Secur.*, 5(4):241–255, 2006.

[OU98] T. Okamoto and S. Uchiyama. A New Public Key Cryptosystem as Secure as Factoring. In *Proc. of Eurocrypt' 98*, pages 308–318, 1998.

[Pai99] P. Paillier. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. In J. Stern, editor, *Advances in Cryptology* - EUROCRYPT *'99*, volume 1592 of *Lect. Notes Comput. Sci.*, pages 223–238. Springer, 1999.

[PT00] S. Paulus and Takagi T. A new public-key cryptosystem over quadratic orders with quadratic decryption time. *Journal of Cryptology*, 13:263–272, 2000.

[SL93] Peter Smith and Michael J. J. Lennon. LUC: A New Public Key System. In *Proc. of the Ninth IFIP Int. Symp. on Computer Security (1993)*, pages 103–117, 1993.