Encoding-Free ElGamal Encryption Without Random Oracles

Benoît Chevallier-Mames[1,2], Pascal Paillier[3], and David Pointcheval[2]

[1] Gemplus, Security Technology Department,
La Vigie, Avenue du Jujubier, ZI Athélia IV,
F-13705 La Ciotat Cedex, France
benoit.chevallier-mames@gemplus.com

[2] École Normale Supérieure,
Département d'Informatique, 45 rue d'Ulm,
F-75230 Paris 05, France
david.pointcheval@ens.fr

[3] Gemplus, Security Technology Department,
34 rue Guynemer,
F-92447 Issy-les-Moulineaux, France
pascal.paillier@gemplus.com

Abstract. ElGamal encryption is the most extensively used alternative to RSA. Easily adaptable to many kinds of cryptographic groups, ElGamal encryption enjoys homomorphic properties while remaining semantically secure providing that the DDH assumption holds on the chosen group. Its practical use, unfortunately, is intricate: plaintexts have to be encoded into group elements before encryption, thereby requiring awkward and ad hoc conversions which strongly limit the number of plaintext bits or may partially destroy homomorphicity. Getting rid of the group encoding (*e.g.*, with a hash function) is known to ruin the standard model security of the system.

This paper introduces a new alternative to group encodings and hash functions which remains *fully compatible* with standard model security properties. Partially homomorphic in customizable ways, our encryptions are comparable to plain ElGamal in efficiency, and boost the encryption ratio from about 13 for classical parameters to the optimal value of 2.

Keywords: Cryptography, ElGamal encryption, Diffie-Hellman, Residuosity classes, Group encodings.

1 Introduction

Since the discovery of public-key cryptography [7], very few practical cryptosystems have been suggested that sustain a strong evidence of security in the standard model.

FACTORING VS. DISCRETE-LOG ENCRYPTION SCHEMES. In brief, there exist two main families of provably secure cryptosystems. The first family relates to integer factoring (Rabin [21], RSA [22], Naccache-Stern [16], Okamoto-Uchiyama [18], Paillier [19]). The others are based on the discrete logarithm or the Diffie-Hellman problems. Within this family, ElGamal encryption [8] is certainly the most extensively used for cryptographic applications.

Cryptosystems belonging to the first family support the encryption of messages without prior formatting in the sense that any fixed-size integer is a proper input of the encryption algorithm. However, all known discrete-log-based encryption schemes which feature standard-model security such as Cramer-Shoup encryption [5], are restricted to encrypt group elements.

This drawback, often overlooked, seems inherent to the nature of these cryptosystems. Variants and alternate designs either drastically degrade bandwidth and efficiency, or imply extra (and possibly questionable) assumptions in their security analysis.

Historically, the first designs suggested to work in the largest possible subgroup over which the encryption takes place. By virtue of the fact that invoking the DDH assumption requires to use a prime order subgroup (or at least a subgroup which order does not have small factors), the subgroup of quadratic residues in $\mathbb{Z}_p^*$ appears as the best choice in this respect. However, one then has to perform operations in the group of order $q = (p-1)/2$ which implies exponentiations with large exponents.

A standard lesser evil consists in applying a hash function to the Diffie-Hellman session key before masking the plaintext. The price to pay then amounts to making stronger assumptions, such as the Hash Diffie-Hellman assumption [1, 12] or the random oracle model [2].

OUR CONTRIBUTIONS. This paper introduces a novel encryption technique that does not require message encoding before encryption and enjoys strong security against chosen-plaintext attacks without any extra assumption *i.e.*, the security of our cryptosystems stands in the standard model. One-wayness and indistinguishability rely on the use of new specifically introduced integer-theoretic problems which we call the (computational/decision) Class Diffie-Hellman problems (CCDH, resp. DCDH).

Most interestingly, we provide a proof that CCDH is in fact *equivalent* to CDH, meaning that the one-wayness of our schemes is identical to the one of ElGamal encryption while providing an optimal encryption ratio of 2 instead of 13. The study of DCDH, however, remains a challenging open problem.

In terms of performance, the encryption and decryption procedures are equivalent to respectively 6 and 5 exponentiations in a subgroup of prime order q with *e.g.*, $\log q = 160$. No group encoding is required before encryption. Finally the ciphertext size is identical to an ElGamal ciphertext, although the encryption ratio reaches its optimum level: one may encrypt 1024-bit strings into a 2048-bit ciphertext while still relying on a 160-bit subgroup.

Our cryptosystems also provide a weak form of additive or multiplicative homomorphic property, in the sense that one can add a constant or multiply by a constant an encrypted value. However, one cannot re-randomize encryptions. This amounts to say that if two ciphertexts were created using this property (with the same random coins), every one may recover the difference or the ratio between the plaintexts, without any private material.

Our encryption schemes are based on the mathematical properties of integers modulo p^2 where p is a prime number. Interestingly, one would note that homomorphicity has often been achieved by relying on the properties of special moduli: Okamoto and Uchiyama [18] use properties of integers modulo $n = p^2q$, while Paillier [19] and Bresson, Catalano and Pointcheval [3] rather employ moduli of the form n^2. Damgård and Jurik [6] use operations modulo n^s for $s > 2$. In all of these schemes, however, various forms of RSA moduli constitute basic scheme parameters and the trapdoor technique relates to factoring rather than to discrete-log problems. Our work, by opposition, makes exclusive use of prime-order groups.

Outline of the paper. Our work is divided as follows. Section 2 reviews standard definitions and security notions for public-key encryption. Section 3 briefly recalls ElGamal encryption and variants thereof. In Section 4, we introduce the Class Diffie-Hellman problems, then proceed to define and comment on our encryption schemes. Their security is further discussed in Section 5. We finally provide extensions to $\mathbb{Z}_{p^k}$ in Section 6.

2 Preliminaries

2.1 Public-Key Encryption

We identify a public-key encryption scheme S to a tuple of probabilistic algorithms $\mathsf{S} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ defined as follows:

Key Generation. Given a security parameter k, $\mathcal{K}(1^k)$ produces a pair $(\mathsf{pk}, \mathsf{sk})$ of public and private keys.

Encryption. Given a message m and a public key pk, $\mathcal{E}_{\mathsf{pk}}(m)$ produces a ciphertext c. If the procedure is probabilistic, we write $c = \mathcal{E}_{\mathsf{pk}}(m; r)$ where r denotes the randomness used by $\mathcal{E}$.

Decryption. Given a ciphertext c and a private key sk, $\mathcal{D}_{\mathsf{sk}}(c)$ returns a plaintext m or possibly $\perp$ if the ciphertexts is invalid.

2.2 Security Notions for Encryption Schemes

One-Wayness. A most important security notion that one would expect from an encryption scheme to fulfil is the property of *one-wayness* (OW): an attacker should not be able to recover the plaintext matching a given ciphertext. We capture this notion more formally by saying that for any adversary $\mathcal{A}$, succeeding in inverting the effects of $\mathcal{E}$ on a ciphertext c should occur with negligible probability. $\mathcal{A}$ is said to (k, ε, τ)-break OW when

$$\mathsf{Succ}_{\mathsf{S}}^{\mathsf{ow}}(\mathcal{A}) = \Pr_{m,r}[(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathcal{K}(1^k) \; : \; \mathcal{A}(\mathsf{pk}, \mathcal{E}_{\mathsf{pk}}(m; r)) = m] \geq \varepsilon \; ,$$

where the probability is taken over the random coins of the experiment and the ones of the adversary, and $\mathcal{A}$ halts after τ elementary steps. An encryption scheme is said to be one-way if no probabilistic algorithm (k, ε, τ)-breaks OW for $\tau \leq \mathsf{poly}(k)$ and $\varepsilon \geq 1/\mathsf{poly}(k)$.

Semantic Security. The notion of *semantic security* (IND) [13], *a.k.a.*, *indistinguishability of encryptions* captures a strong notion of privacy. Here, the attacker should not learn any information whatsoever about a plaintext given its encryption. The adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ is said to (k, ε, τ)-break IND when

$$\mathsf{Adv}_{\mathsf{S}}^{\mathsf{ind}}(\mathcal{A}) = 2 \times \Pr_{b,r}\left[\begin{array}{l}(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathcal{K}(1^k), (m_0, m_1, s) \leftarrow \mathcal{A}_1(\mathsf{pk}), \\ c = \mathcal{E}_{\mathsf{pk}}(m_b; r) \; : \; \mathcal{A}_2(m_0, m_1, s, c) = b\end{array}\right] - 1 \geq \varepsilon,$$

where again the probability is taken over the random coins of the experiment as well as the ones the adversary. $\mathcal{A}$ must run in at most τ steps and it is imposed that $|m_0| = |m_1|$. An encryption scheme is said to be semantically secure or indistinguishable if no probabilistic algorithm can (k, ε, τ)-break IND for $\tau \leq \mathsf{poly}(k)$ and $\varepsilon \geq 1/\mathsf{poly}(k)$.

2.3 Computational Assumptions

We now briefly recall the definition of the discrete-log and related problems needed for the sake of this work. In what follows, $\mathbb{G}$ denotes an abelian group (denoted multiplicatively) of prime order q. We also consider a generator g of $\mathbb{G} = \langle g \rangle$.

Definition 1 (Discrete Logarithm – DL). *Given $g^x \in \mathbb{G}$ where $x \leftarrow \mathbb{Z}_q$, compute x.*

Definition 2 (Computational Diffie-Hellman – CDH). *Given $g^x \in \mathbb{G}$ and $g^y \in \mathbb{G}$ for $x, y \leftarrow \mathbb{Z}_q$, compute $g^{xy} \in \mathbb{G}$.*

Definition 3 (Decision Diffie-Hellman – DDH). *Let us consider the two distributions $D = (g^x, g^y, g^{xy})$ and $R = (g^x, g^x, g^z)$ for randomly distributed $x, y, z \leftarrow \mathbb{Z}_q$. Distinguish D from R.*

It is easily seen that $\mathsf{DDH} \Leftarrow \mathsf{CDH} \Leftarrow \mathsf{DL}$ where $\Leftarrow$ denotes polynomial reduction between computational problems. In most cryptographic applications, the structure of the group $\mathbb{G}$ is chosen in such a way that these three computational problems seem intractable. A typical example is to choose $\mathbb{G} \subseteq \mathbb{F}_p^*$ where q divides $(p-1)$ where classically, p is a 1024-bit prime and q a 160-bit prime. Another widely used family of groups is elliptic curves over large prime fields [15, 14].

3 The ElGamal Cryptosystem

ElGamal encryption was introduced by T. ElGamal in 1985 [8]. The algebraic framework requires a cryptographic group $\mathbb{G}$ of order q given with some generator g.

One generates a public-private key pair by randomly selecting $x \leftarrow \mathbb{Z}_q$ and computing $y = g^x$. The public key is then y while the private key is x. In order to encrypt a message m, one randomly selects $r \leftarrow \mathbb{Z}_q$ and computes $u = g^r$ and $v = y^r m$. The ciphertext is $c = (u, v)$. Using the private key x, the ciphertext $c = (u, v)$ can be decrypted as $m = v \cdot u^{-x}$.

The key point here resides in the definition of the message space $\mathcal{M}$. As defined originally in [8], the group $\mathbb{G}$ was chosen to be the set of integers modulo a large prime p (*i.e.*, $\mathbb{G} = \mathbb{Z}_p$), q was set to $p-1$ and $\mathcal{M}$ was identified to $\mathbb{Z}_p^*$. Unfortunately, using this definition, the cryptosystem is not indistinguishable: given a ciphertext $c = (u, v)$, an attacker can well decide with non negligible probability whether c encrypts a given message m_0. To this end, the attacker computes $v' = v \cdot m_0^{-1}$, and then computes $a = u^{(p-1)/2}$ and $b = v'^{(p-1)/2}$. If only one of the elements a or b is equal to 1, the adversary knows that c does not encrypt m_0. This simple attack actually checks the parity of the logarithms of u and v' with respect to g and y respectively: if $c = (u, v)$ encrypts m_0, it is needed that these parities be identical.

This attack against indistinguishability shows that the order of the group $\mathbb{G}$ must be relatively prime to any small integer (the attack described just above can be extended trivially for any small divisor of q), and most preferably, the order of group $\mathbb{G}$ must be chosen to be prime.

Description. Unfortunately, the above constraint translates into a restriction on the message space $\mathcal{M}$: it has to be embedded into the group $\mathbb{G}$. Hence, before encryption takes place, the message must be *encoded* into a group element, and this group encoding must be efficiently invertible in order to allow the original message to be recovered during the decryption process. Such an encoding may be time-consuming, and may also partially or totally destroy the inherent homomorphic property of the system. Also, using a group encoding remains incompatible with the optimization which consists in working in a small subgroup of $\mathbb{Z}_p^*$ of prime order q where q is a 160-bit prime, a setting in which group exponentiations are much faster.

Set up: Let p be an ℓ_p-bit prime and q an ℓ_q-bit prime so that q divides $(p-1)$. Let $\mathbb{G}$ be the subgroup of $\mathbb{Z}_p^*$ of order q, and g be a generator of $\mathbb{G}$. Let Ω be a one-to-one encoding map from $\mathbb{Z}_q$ onto $\mathbb{G}$.

Key generation: The private key is $x \leftarrow \mathbb{Z}_q$. The corresponding public key is $y = g^x$.

Encryption: To encrypt a message $m \in \mathbb{Z}_q$, one encodes m by computing $\omega = \Omega(m)$, randomly selects $r \leftarrow \mathbb{Z}_q$ and computes $(u, v) = (g^r, y^r \omega)$. The ciphertext is $c = (u, v)$.

Decryption: To decrypt a ciphertext $c = (u, v)$, one computes $\omega = v \cdot u^{-x}$ and recovers the original plaintext $m = \Omega^{-1}(\omega)$.

This cryptosystem is known to be one-way under the CDH assumption, and indistinguishability holds under the DDH assumption. These security notions are reached in the context of chosen-plaintext attacks, in the standard model.

3.1 The Hash-ElGamal Cryptosystem

In order to overcome the issue of group encoding, a hash variant of ElGamal encryption was suggested.

Set up: Let p be an ℓ_p-bit prime and q an ℓ_q-bit prime so that q divides $(p-1)$. Let $\mathbb{G}$ be the subgroup of order q of $\mathbb{Z}_p^*$, and g be a generator of $\mathbb{G}$. Let $\mathcal{H} : \mathbb{G} \to \{0,1\}^{\ell_m}$ be a hash function.

Key generation: The private key is again $x \leftarrow \mathbb{Z}_q$. The corresponding public key is $y = g^x$.

Encryption: To encrypt a message $m \in \{0,1\}^{\ell_m}$, one randomly selects $r \leftarrow \mathbb{Z}_q$ and computes $(u, v) = (g^r, \mathcal{H}(y^r) \oplus m)$. The ciphertext is $c = (u, v)$.

Decryption: To decrypt a ciphertext $c = (u, v)$, one computes $m = \mathcal{H}(u^x) \oplus v$.

This cryptosystem features one-wayness and indistinguishability under chosen plaintext attacks under the sole CDH assumption. The security proof, however, stands in the random oracle model. Alternatively, under the DDH assumption, one can apply a randomness extractor in place of the random oracle, in order to generate a truly random mask. But this either requires large groups, or drastically reduces the size of the mask [4].

4 Encoding-Free ElGamal Encryption

We now proceed to describe our new technique for encoding-free ElGamal encryption. Our cryptosystems enjoy performances similar to plain ElGamal but do not require group encoding, nor randomness extractors. Furthermore, their security holds in the standard model under new intractability assumptions that we introduce below. We start by providing definitions as well as the mathematical facts underlying our proposal.

4.1 The Class Function

Let p and q be prime numbers such that $q \mid p-1$. Let g be an integer of order pq modulo p^2 and $\mathbb{G} = \langle g \rangle$ the group formed by all elements of order pq modulo p^2. Hence $\mathbb{G}_p = \langle g \bmod p \rangle$ is the subgroup of order q in $\mathbb{Z}_p^*$. By the Chinese Remainder Theorem, there is a canonical mapping between $\mathbb{Z}_p \times \mathbb{Z}_q$ and $\mathbb{Z}_{pq}$. For any $x \in \mathbb{Z}_p$ and $y \in \mathbb{Z}_q$, $\langle x, y \rangle$ stands for the unique integer modulo pq such that $\langle x, y \rangle = x \bmod p$ and $\langle x, y \rangle = y \bmod q$.

Definition 4 (Class of an element of $\mathbb{G}$). *Each and every element w of $\mathbb{G}$ can be written as $w = g^{\langle x,\, y\rangle} \bmod p^2$ for a unique $x \in \mathbb{Z}_p$ and a unique $y \in \mathbb{Z}_q$. The integer $x = [\![w]\!]$ is said to be the* class *of w with respect to g.*

It is easily seen that if $w = g^{\langle x,\, y\rangle} \bmod p^2$, then $w = g^y \bmod p$. In other words, y is the discrete log of $w \bmod p$ with respect to $g \bmod p$. This means that, unless extracting discrete logs over $\mathbb{G}_p$ is easy, y cannot be easily computed from w. It appears, however, that computing the class of elements of $\mathbb{G}$ can be done publicly and efficiently.

Lemma 1. *Define over $\mathbb{G}$ the function $\mathcal{L}(w) = (w^q - 1 \bmod p^2)/p$. The class of $w = g^{\langle x,\, y\rangle} \bmod p^2$ can be computed as $x = \mathcal{L}(w)\mathcal{L}(g)^{-1} \bmod p$.*

This property is well-known and we refer the reader to [18, 19] for a proper proof. Now let a be an integer modulo q and consider $w = g^a \bmod p$. Since w can also be viewed as an element of $\mathbb{G}$, there exist integers x, y such that $w = g^{\langle x,\, y\rangle} \bmod p^2$. However, $g^{\langle x,\, y\rangle} = g^y \bmod p$ and therefore $y = a$ by unicity of y. It appears that the value of x can be recovered as a function of a:

Lemma 2. *Let us define*

$$\mathsf{Upper}(g^a) = \frac{g^a \bmod p^2 - g^a \bmod p}{p}$$

and

$$\Delta(g^a) = \frac{q}{\mathcal{L}(g)} \cdot \frac{\mathsf{Upper}(g^a)}{g^a} \bmod p\ .$$

Then

$$[\![g^a \bmod p]\!] = a - \Delta(g^a) \bmod p\ .$$

Proof. Noting $g^a = A + p \cdot \bar{A} \bmod p^2$ for $A, \bar{A} \in \mathbb{Z}_p$ with $A \neq 0$, and using the identity $1 + p \cdot \mathcal{L}(g) = g^{\langle q,\, 0\rangle} \bmod p^2$, we have

$$g^a = A\left(1 + p \cdot \frac{\bar{A}}{A}\right) = A\,(1+p)^{\frac{\bar{A}}{A}} = A \cdot g^{\langle \frac{q}{\mathcal{L}(g)} \frac{\bar{A}}{A},\, 0\rangle} \bmod p^2\ .$$

Taking the class of the left and right terms, we get $a \cdot [\![g]\!] = [\![A]\!] + \Delta(g^a)$ which leads to the above using the trivial fact that $[\![g]\!] = 1$. □

Lemma 3. *The mapping $a \to [\![g^a \bmod p]\!]$ is random self-reducible.*

Proof. Assume we want $[\![A]\!]$ for some given $A = g^a \bmod p$. We make use of the fact that for any $r \in \mathbb{Z}_q$, we have

$$[\![A^r \bmod p]\!] = [\![A^r \bmod p^2]\!] - \Delta(A^r) = r \cdot [\![A]\!] - \Delta(A^r) \bmod p\ .$$

If r is drawn uniformly at random from $\mathbb{Z}_q^*$, $A^r \bmod p$ is a random element of $\mathbb{G}_p$. Knowing $[\![A^r \bmod p]\!]$ and r, $[\![A]\!]$ is easily recovered as

$$[\![A]\!] = r^{-1}\left([\![A^r \bmod p]\!] + \Delta(A^r)\right) \bmod p\ .$$

□

4.2 The Class Diffie-Hellman Problems

We now turn to defining the computational problems over which we base the encryption schemes suggested in the forthcoming sections.

Definition 5 (Computational Class Diffie-Hellman). *Let $\mathbb{G}_p = \langle g \bmod p\rangle$ be defined as above. Given group elements $g^a \bmod p$ and $g^b \bmod p$, compute $[\![g^{ab} \bmod p]\!]$.*

Definition 6 (Decision Class Diffie-Hellman). *Distinguish the two distributions $D = (g^a \bmod p, g^b \bmod p, [\![g^{ab} \bmod p]\!])$ and $R = (g^a \bmod p, g^b \bmod p, z)$ for $a, b \leftarrow \mathbb{Z}_q$ and $z \leftarrow \mathbb{Z}_p$.*

We denote these problems CCDH and DCDH throughout the paper. As we shall now see, CCDH is in fact closely related to CDH.

Theorem 1. CCDH *and* CDH *are equivalent.*

Proof. $[\mathsf{CCDH} \Leftarrow \mathsf{CDH}]$. Assume we are given a probabilistic algorithm $\mathcal{A}$ such that $\mathcal{A}(g^a \bmod p, g^b \bmod p)$ outputs $g^{ab} \bmod p$ with probability ε and time bound τ, the success probability being taken over the random variables of $\mathcal{A}$ and the random selections $a, b \leftarrow \mathbb{Z}_q$. Given $A, B \leftarrow \mathbb{G}_p$, we run $\mathcal{A}(A, B)$ to get $\mathsf{DH}(A, B)$ and deduce $[\![\mathsf{DH}(A, B)]\!]$, thereby succeeding in solving CCDH with probability ε and no more than $\tau + \mathsf{poly}(\log p)$ steps.

$[\mathsf{CDH} \Leftarrow \mathsf{CCDH}]$. Assume there exists a probabilistic algorithm $\mathcal{A}$ which solves CCDH. By virtue of Lemma 3, we may assume that the input distribution of $\mathcal{A}$ need not be uniform and that the success probability of $\mathcal{A}$ is overwhelming. We build a reduction algorithm $\mathcal{B}$ that computes $C = \mathsf{DH}(A, B)$ for arbitrary elements $A, B \leftarrow \mathbb{G}_p$. $\mathcal{B}$ first runs $\mathcal{A}(A, B)$ to get $[\![C]\!]$. $\mathcal{B}$ now sets $A' = Ag \bmod p$ and runs $\mathcal{A}$ again to get $[\![C']\!] = \mathcal{A}(A', B)$ where $C' = \mathsf{DH}(A', B) = BC \bmod p$. We must have

$$[\![C']\!] = [\![BC \bmod p]\!] = [\![BC \bmod p^2]\!] - \Delta(BC) = [\![B]\!] + [\![C]\!] - \Delta(BC)$$

wherefrom $\Delta(BC) = [\![B]\!] + [\![C]\!] - [\![C']\!] \bmod p$. Since

$$BC = C' + p \cdot \mathsf{Upper}(BC) = C' \left(1 + p \cdot \frac{\mathcal{L}(g)}{q} \cdot \Delta(BC)\right) \bmod p^2 \ ,$$

$\mathcal{B}$ now remains with the problem of finding a solution to the modular equation

$$\frac{C}{C'} = B^{-1} \left(1 + p \cdot \frac{\mathcal{L}(g)}{q} \cdot \Big([\![B]\!] + [\![C]\!] - [\![C']\!]\Big)\right) \bmod p^2 \qquad (1)$$

where the unknowns are $C, C' \in \mathbb{Z}_p$. Setting the right-hand term to $\mu < p^2$, $\mathcal{B}$ applies the extended Euclidean algorithm to μ and p^2 in order to find small solutions $C, C' < p$ satisfying $C/C' = \mu \bmod p^2$. The validity of C is easily checked by making sure that $C'C^{-1} \bmod p$ is equal to B. This stage finishes with probability one in time bounded by $\log^3 p$ resulting in that $C = \mathsf{DH}(A, B)$ is found with no more than two calls to $\mathcal{A}$ and polynomial extra time. □

So far, the study of DCDH remains a challenging open question. In particular, the relations between DCDH and DDH are somewhat unclear. Although we do not provide evidence of that fact, we suspect these two problems to be extremely closely connected. We will make the assumption that DCDH is intractable throughout the rest of this paper.

4.3 Encoding-Free Additive Encryption

As discussed above, our goal is to render ElGamal encryption truly practical by getting rid of intricate group encoding mechanisms while maintaining a security level in the standard model (in opposition to Hash-ElGamal encryption for instance). The basic idea, instead of embedding the message into a group element, consists in converting the session key output by the Diffie-Hellman exchange[1] into an integer modulo p using the class function.

Set up: Let p an ℓ_p-bit prime and q an ℓ_q-bit prime divisor of $p-1$. Let g be a generator of the subgroup $\mathbb{G}_p$ of order q of $\mathbb{Z}_p^*$.

Key generation: The private key is a random number $x \in \mathbb{Z}_q$. The corresponding public key is $y = g^x \bmod p$.

Encryption: To encrypt a message $m \in \mathbb{Z}_p$, one picks a random $r \in \mathbb{Z}_q$ and computes $u = g^r \bmod p$ and $v = [\![y^r \bmod p]\!] + m \bmod p$. The ciphertext is $c = (u, v)$.

Decryption: To decrypt a ciphertext $c = (u, v)$, one simply computes $m = v - [\![u^x \bmod p]\!] \bmod p$.

4.4 Encoding-Free Multiplicative Encryption

Since the message and the class of $g^{xy} \bmod p$ are both integers modulo p, encryption may also be performed using modular multiplication instead of modular addition.

Set up: Let p an ℓ_p-bit prime and q an ℓ_q-bit prime divisor of $p-1$. Let g be a generator of the subgroup $\mathbb{G}_p$ of order q of $\mathbb{Z}_p^*$.

Key generation: The private key is a random number $x \in \mathbb{Z}_q$. The corresponding public key is $y = g^x \bmod p$.

Encryption: To encrypt a message $m \in \mathbb{Z}_p^*$, one picks a random $r \in \mathbb{Z}_q$ and computes $u = g^r \bmod p$ and $v = [\![y^r \bmod p]\!] \cdot m \bmod p$. The ciphertext is $c = (u, v)$.

Decryption: To decrypt a ciphertext $c = (u, v)$, one simply computes $m = v[\![u^x \bmod p]\!]^{-1} \bmod p$.

[1] ElGamal encryption can indeed be viewed as a Diffie-Hellman key exchange where the publication of the public-key y plays the role of the first pass.

4.5 Properties of our encryption schemes

NO CONVERSION. Our encryption schemes do not require any conversion: the message space is *really* the ring $\mathbb{Z}_p$ (or the multiplicative subgroup $\mathbb{Z}_p^*$ in the multiplicative version.) Therefore, any string of bitlength lesser than k, where $p > 2^k$, can be encrypted directly. This is a strong property since we may have q much smaller than p without impact on the encryption and decryption procedures.

EFFICIENCY. It is easily seen that ciphertexts have a similar size as with ElGamal encryption. The bandwidth is exactly $\frac{1}{2}$ (*i.e.*, the encryption ratio is exactly 2), by opposition to ElGamal encryption for which the bandwidth is $\frac{q}{2p}$. We recall that for $p = 1024$ and $q = 160$, the bandwidth of ElGamal is close to $\frac{1}{13}$).

From the viewpoint of computational performances, it appears that in addition to the two exponentiations that are inherent to ElGamal encryption, we require an additional exponentiation in $\mathbb{Z}_{p^2}$ with a ℓ_q-bit exponent. This amounts to four times the execution time of the same exponentiation in $\mathbb{Z}_p$. Totaling everything, we need 6 exponentiations vs. 2 exponentiations in ElGamal. However, no encoding is needed, which are basically done with exponentiations.

When decrypting an ElGamal encryption, an exponentiation of ℓ_q bits in $\mathbb{Z}_p$ is required, as well as a group decoding. In our schemes, however, we require an exponentiation in $\mathbb{Z}_{p^2}$ with an exponent of size ℓ_q and another exponentiation with an exponent of size ℓ_q. Finally, we require 5 exponentiations to be compared to the single exponentiation needed in ElGamal. Once again, no inverse of the encoding is needed.

MULTIPLICATIVE OR ADDITIVE HOMOMORPHISM. Last but not least, our schemes feature a partial homomorphic property over the ring of integers modulo p. We mean for instance that one could add some constant to an encrypted plaintext without needing the private key. Although these properties do forbid resistance against chosen-ciphertext attacks, these are perceived as most desirable in many cryptographic applications such as electronic voting, and we expect to see applications of our work in this regard. However, our schemes do not allow to re-randomize a ciphertext per se.

5 Security Analysis

We now proceed to assessing the security of our schemes. Obviously, one cannot prevent chosen-ciphertext attacks due to the partial malleability described above. However, generic conversions do exist to convert CPA-secure schemes into CCA-secure schemes (in the random oracle model)[9–11, 20, 17] when the context of use demands CCA security.

ONE-WAYNESS. Focusing on the additive version of our encoding-free encryption scheme, we state:

Theorem 2. *Let $\mathcal{A}$ be an adversary which can invert our cryptosystem with success probability ε under a chosen-plaintext attack within time τ. Then the Computational Class Diffie-Hellman problem can be solved with success probability ε within time similar to τ.*

Proof. Given a Computational Class Diffie-Hellman instance $(g, y = g^x \bmod p, w = g^s \bmod p)$, our goal is to compute $z = [\![g^{xs} \bmod p]\!]$. To this aim, we use the $\mathsf{OW}-\mathsf{CPA}$ attacker $\mathcal{A}$ against our scheme, where g is the public generator, and set the public key to y. We submit to $\mathcal{A}$ the ciphertext $(u, v) = (w, a)$ for a randomly chosen $a \in \mathbb{Z}_p$. This is a truly random ciphertext of a random message, for which we have set $r = s$, and so $\mathcal{A}$ succeeds with probability ε to find the corresponding plaintext m. If $\mathcal{A}$ succeeds, we thus learn $[\![g^{xs} \bmod p]\!]$, our expected result $z = a - m \bmod p$. □

It is easily seen that the same theorem holds for the multiplicative encryption scheme. One would simply note that the message space in this latter version is $\mathbb{Z}_p^*$, and not $\mathbb{Z}_p$, as one needs to compute the inverse $m^{-1} \bmod p$ to deduce z from a and m.

Indistinguishability. About indistinguishability, we state a similar result:

Theorem 3. *Let $\mathcal{A}$ be an adversary breaking the indistinguishability of our cryptosystem with advantage ε under a chosen-plaintext attack within time τ. Then the Decisional Class Diffie-Hellman problem can be solved with advantage $\varepsilon/2$ within time similar to τ.*

Proof. Assume we are given an instance $(g, y = g^x \bmod p, w = g^s \bmod p, z)$ of the Decisional Class Diffie-Hellman problem in $\mathbb{Z}_p$, and want to decide whether z is randomly selected in $\mathbb{Z}_p$ or whether $z = [\![g^{xs} \bmod p]\!]$.

As above, we make use an $\mathsf{IND}-\mathsf{CPA}$ attacker $\mathcal{A}$ against our scheme, where g is the public generator, and set the public key to y. We let the adversary to choose two messages m_0 and m_1, pick a random bit b, and encrypt m_b as $(u, v) = (w, z + m_b \bmod p)$. Finally, we send this ciphertext to the $\mathcal{A}$ as the challenge ciphertext.

Clearly, if $z = [\![g^{xs} \bmod p]\!]$, c is a valid ciphertext of m_b, where we set $r = s$, and consequently the attacker $\mathcal{A}$ can guess the value b with advantage ε. On the contrary, if z is a random element of $\mathbb{Z}_p$, $z' = z + m_b \bmod p$ is also a random element of $\mathbb{Z}_p$, thereby making the ciphertext independent from the message m_b. The advantage of $\mathcal{A}$ is then necessarily zero.

Hence, to solve our decisional problem, we reply True if the guess of $\mathcal{A}$ is correct, otherwise a random bit is replied. Our reduction solves DCDH with advantage at least $\varepsilon/2$. □

6 Generalization to $\mathbb{Z}_{p^k}$

As the scheme suggested by Damgård-Jurik [6] is a generalization of Paillier encryption, we may generalize our systems using $\mathbb{Z}_{p^k}$ for any integer $k > 2$.

For any integer $k > 2$, we denote naturally $\mathcal{L}_k$ the function defined by $X \mapsto \frac{X^{q-1} \bmod p^k}{p}$, and let the class of w as $[\![w]\!]_k = \mathcal{L}_k(w)\mathcal{L}_k(g)^{-1} \bmod p^{k-1}$. Then the generalization of our technique to $\mathbb{Z}_{p^k}$ is as follows:

Set up: Let p an ℓ_p-bit prime and q an ℓ_q-bit prime divisor of $(p-1)$. Let g be a generator of the subgroup $\mathbb{G}_p$ of order q of $\mathbb{Z}_p$.

Key generation: The private key is a random number $x \in \mathbb{Z}_q$. The corresponding public key is $y = g^x \bmod p$.

Encryption: To encrypt a message $m \in \mathbb{Z}_{p^{k-1}}$, one picks a random $r \in \mathbb{Z}_q$ and computes $u = g^r \bmod p$ and $v = [\![y^r \bmod p]\!]_k + m \bmod p^{k-1}$. The ciphertext is $c = (u, v)$.

Decryption: To decrypt a ciphertext $c = (u, v)$, one simply computes

$$m = v - [\![u^x \bmod p]\!]_k \bmod p^{k-1}.$$

We may equally well use modular multiplication instead of addition of course. In these cryptosystems, the encryption bandwidth is equal to $\frac{k-1}{k}$, and therefore can be made nearly optimal. Furthermore, the property of partial malleability is still a feature of the scheme. Regarding security, one refer the reader to [6] for proofs that the generalizations of CCDH and DCDH are equivalent to their version for $k = 2$. We then adapt the proof of the scheme in $\mathbb{Z}_{p^2}$ to show that the one-wayness and that indistinguishability of the generalized schemes are identical to the extended versions of CCDH and DCDH.

7 Conclusion and Open Issues

In this paper, we have proposed new cryptosystems based on new computational problems related to the Diffie-Hellman problems. Encryption does not require messages to be converted into group elements by opposition to all known discrete-log-based cryptosystem proven secure in the standard model.

Our cryptosystems feature a better encryption ratio (decreased by a factor 6.5 for common parameters), an identical ciphertext size, and remain comparable in speed with ElGamal encryption. Their security in the standard model under chosen-plaintext attacks is based on the CDH assumption for one-wayness, and on the assumption that the Decision Class Diffie-Hellman for indistinguishability.

Our encryption schemes are partially homomorphic, either additively or multiplicatively. To the best of our knowledge, this gives the only example of an additive encryption (even if partial) featuring standard-model security in the discrete-log setting.

An open research area would be to find a discrete-log-based cryptosystem that would provide a *fully* additive or multiplicative homomorphism. Another independent but challenging topic would be to provide a more accurate study on the connections between DCDH and DDH.

Acknowledgements

The first author would like to thank Jean-François Dhem and Philippe Proust, as well as his colleague Eric Brier for fruitful and enjoying discussions about the difficulty of the DCDH problem.

This work was funded in part by the European project ECRYPT and in part by the French RNRT project CRYPTO^{++}.

References

1. M. Abdalla, M. Bellare, and P. Rogaway. DHAES: An Encryption Scheme Based on the Diffie-Hellman Problem. Submission to IEEE P1363a. September 1998. Available from `http://grouper.ieee.org/groups/1363/`.
2. M. Bellare and P. Rogaway. Optimal Asymmetric Encryption – How to Encrypt with RSA. In *Eurocrypt '94*, LNCS 950, pages 92–111. Springer-Verlag, Berlin, 1995.
3. E. Bresson, D. Catalano, and D. Pointcheval. A Simple Public-Key Cryptosystem with a Double Trapdoor Decryption Mechanism and its Applications. In *Asiacrypt '03*, LNCS 2894, pages 37–54. Springer-Verlag, Berlin, 2003.
4. O. Chevassut, P.-A. Fouque, P. Gaudry, and D. Pointcheval. The Twist-Augmented Technique for Key Exchange. In *PKC '06*, LNCS. Springer-Verlag, Berlin, 2006.
5. R. Cramer and V. Shoup. A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Ciphertext Attack. In *Crypto '98*, LNCS 1462, pages 13–25. Springer-Verlag, Berlin, 1998.
6. I. Damgård and M. Jurik. A Generalisation, a Simplification and Some Applications of Paillier's Probabilistic Public-Key System. In *PKC '01*, LNCS 1992, pages 119–137. Springer-Verlag, Berlin, 2001.
7. W. Diffie and M. E. Hellman. New Directions in Cryptography. *IEEE Transactions on Information Theory*, IT–22(6):644–654, November 1976.
8. T. El Gamal. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. *IEEE Transactions on Information Theory*, IT–31(4):469–472, July 1985.
9. E. Fujisaki and T. Okamoto. How to Enhance the Security of Public-Key Encryption at Minimum Cost. In *PKC '99*, LNCS 1560, pages 53–68. Springer-Verlag, Berlin, 1999.
10. E. Fujisaki and T. Okamoto. Secure Integration of Asymmetric and Symmetric Encryption Schemes. In *Crypto '99*, LNCS 1666, pages 537–554. Springer-Verlag, Berlin, 1999.
11. E. Fujisaki and T. Okamoto. How to Enhance the Security of Public-Key Encryption at Minimum Cost. *IEICE Transaction of Fundamentals of Electronic Communications and Computer Science*, E83-A(1):24–32, January 2000.
12. R. Gennaro, H. Krawczyk, and T. Rabin. Secure Hashed Diffie-Hellman over Non-DDH Groups. In *Eurocrypt '04*, LNCS 3027, pages 361–381. Springer-Verlag, Berlin, 2004.
13. S. Goldwasser and S. Micali. Probabilistic Encryption. *Journal of Computer and System Sciences*, 28:270–299, 1984.
14. N. Koblitz. Elliptic Curve Cryptosystems. *Mathematics of Computation*, 48(177):203–209, January 1987.

15. V. Miller. Uses of Elliptic Curves in Cryptography. In *Crypto '85*, LNCS 218, pages 417–426. Springer-Verlag, Berlin, 1986.
16. D. Naccache and J. Stern. A New Public-Key Cryptosystem. In *Eurocrypt '97*, LNCS 1233, pages 27–36. Springer-Verlag, Berlin, 1997.
17. T. Okamoto and D. Pointcheval. REACT: Rapid Enhanced-security Asymmetric Cryptosystem Transform. In *CT – RSA '01*, LNCS 2020, pages 159–175. Springer-Verlag, Berlin, 2001.
18. T. Okamoto and S. Uchiyama. A New Public Key Cryptosystem as Secure as Factoring. In *Eurocrypt '98*, LNCS 1403, pages 308–318. Springer-Verlag, Berlin, 1998.
19. P. Paillier. Public-Key Cryptosystems Based on Composite-Degree Residuosity Classes. In *Eurocrypt '99*, LNCS 1592, pages 223–238. Springer-Verlag, Berlin, 1999.
20. D. Pointcheval. Chosen-Ciphertext Security for any One-Way Cryptosystem. In *PKC '00*, LNCS 1751, pages 129–146. Springer-Verlag, Berlin, 2000.
21. M. O. Rabin. Digitalized Signatures and Public Key Functions as Intractible as Factorization. Technical Report MIT/LCS/TR-212, Massachusetts Institute of Technology – Laboratory for Computer Science, January 1979.
22. R. Rivest, A. Shamir, and L. Adleman. A Method for Obtaining Digital Signatures and Public Key Cryptosystems. *Communications of the ACM*, 21(2):120–126, February 1978.