Encoding-Free ElGamal-Type Encryption Schemes on Elliptic Curves

Marc Joye[1(✉)] and Benoît Libert[2]

[1] NXP Semiconductors (USA), San Jose, USA
marc.joye@nxp.com
[2] CNRS, Laboratoire LIP (CNRS, ENSL, U. Lyon, Inria, UCBL), ENS de Lyon, Lyon, France

Abstract. At PKC 2006, Chevallier-Mames, Paillier, and Pointcheval proposed a very elegant technique over cyclic subgroups of $\mathbb{F}_p^*$ eliminating the need to encode the message as a group element in the ElGamal encryption scheme. Unfortunately, it is unclear how to adapt their scheme over elliptic curves. In a previous attempt, Virat suggested an adaptation of ElGamal to elliptic curves over the ring of dual numbers as a way to address the message encoding issue. Advantageously the resulting cryptosystem does not require encoding messages as points on an elliptic curve prior to their encryption. Unfortunately, it only provides one-wayness and, in particular, it is not (and was not claimed to be) semantically secure.

This paper revisits Virat's cryptosystem and extends the Chevallier-Mames *et al.*'s technique to the elliptic curve setting. We consider elliptic curves over the ring $\mathbb{Z}/p^2\mathbb{Z}$ and define the underlying class function. This yields complexity assumptions whereupon we build new ElGamal-type encryption schemes. The so-obtained schemes are shown to be semantically secure and make use of a very simple message encoding: messages being encrypted are viewed as elements in the range $[0, p-1]$. Further, our schemes come equipped with a partial ring-homomorphism property: anyone can add a constant to an encrypted message –or– multiply an encrypted message by a constant. This can prove helpful as a blinding method in a number of applications. Finally, in addition to practicability, the proposed schemes also offer better performance in terms of speed, memory, and bandwidth.

Keywords: Public-key encryption · ElGamal encryption · Elliptic curves · Class function · Standard model

1 Introduction

Encryption is one of the most fundamental cryptographic primitives. It allows parties to exchange data privately. In the *asymmetric* setting, a (certified) public encryption key is made publicly available and the matching decryption key is kept private. Anyone can encrypt messages with the public key but only the intended recipient (possessing the private key) is able to decrypt ciphertexts. We refer the reader to Appendix A for background on public-key encryption.

H. Handschuh (Ed.): CT-RSA 2017, LNCS 10159, pp. 19–35, 2017.
DOI: 10.1007/978-3-319-52153-4_2

ElGamal Encryption. The classical ElGamal public-key encryption scheme [12] readily extends to any group $\mathbb{G}$ wherein computing discrete logarithms is assumed to be intractable. In order to avoid sub-group attacks using the Pohlig-Hellman algorithm [25], the underlying group is usually restricted to a prime-order group $\mathbb{G} = \langle g \rangle$; see also [4]. We let q denote the order of $\mathbb{G}$.

The description of $\mathbb{G}$ and the generator g are made public. A random element $y = g^x \in \mathbb{G}$ is drawn for some randomly chosen $x \xleftarrow{R} \mathbb{Z}/q\mathbb{Z}$. The public-key/private-key pair is defined by (pk, sk) with $pk = \{\mathbb{G}, q, g\}$ and $sk = \{x\}$; the message space is $\mathcal{M} = \mathbb{G}$. The encryption of a message $m \in \mathbb{G}$ is given by the pair (c_1, c_2) where

$$c_1 = g^r \quad \text{and} \quad c_2 = m\, y^r$$

for a random integer $r \xleftarrow{R} \mathbb{Z}/q\mathbb{Z}$. Given the ciphertext $C = (c_1, c_2) \in \mathbb{G} \times \mathbb{G}$, message m is then recovered thanks to secret key x as $m = c_2/{c_1}^x$.

As described above, the ElGamal scheme is known to meet the IND-CPA security notion under the decisional Diffie-Hellman (DDH) assumption [29]. Loosely speaking, the *DDH assumption* states that no efficient algorithm can distinguish between the distributions (g, g^a, g^b, g^{ab}) and (g, g^a, g^b, g^c) where $a, b, c \xleftarrow{R} \mathbb{Z}/q\mathbb{Z}$.

Message Encoding. Elliptic curve cryptography [22,24] benefits from the absence of sub-exponential algorithms to solve the underlying hard problem, the elliptic curve discrete logarithm problem. Elliptic curve cryptosystems therefore feature smaller key sizes, which results in significant gains in speed and memory. When applied to elliptic curves over a finite field, ElGamal encryption compels to express the plaintext message m as a point on an elliptic curve or, more precisely, as a point on a prime-order subgroup $\mathbb{G}$ thereof. This requires an injective encoding function mapping the message space to $\mathbb{G}$. Such encodings are provided in [2,14,15] for certain elliptic curves. Unfortunately they do not apply to prime-order elliptic curves as those recommended in most cryptographic standards.

Another option is to leverage the property that any element $w \in \mathbb{G} = \langle g \rangle$ is uniquely represented as $w = g^t$ for some $t \in \mathbb{Z}/q\mathbb{Z}$. This leads to the 'exponent' ElGamal scheme (see e.g. [10]). A message $m \subseteq \mathbb{Z}/q\mathbb{Z}$ is encoded as g^m. The corresponding ciphertext then becomes (c_1, c_2) with $c_1 = g^r$ and $c_2 = g^m\, y^r$ for some $r \xleftarrow{R} \mathbb{Z}/q\mathbb{Z}$. Unfortunately, decryption now involves the computation of a discrete logarithm in $\mathbb{G}$: m is the discrete logarithm of ${c_2}/{c_1}^x$ w.r.t. base g. Since discrete logarithms are supposed to be hard in $\mathbb{G}$, this limits the message space to a small subset of $\mathbb{Z}/q\mathbb{Z}$ so that discrete logarithms can be solved through, e.g., exhaustive search or Pollard's lambda method [26].

Yet another option is to modify the scheme by introducing a hash function. The resulting scheme is referred to as the hash-ElGamal scheme. In more details, let $h : \mathbb{G} \to \{0,1\}^\ell, w \mapsto h(w)$ be a hash function that maps group elements to ℓ-bit strings. The message space is defined as $\mathcal{M} = \{0,1\}^\ell$. The encryption of a message $m \in \mathcal{M}$ is given by (c_1, c_2) with $c_1 = g^r$ and $c_2 = m \oplus h(y^r)$. This variant elegantly solves the encoding problem. On the downside, unless one is willing to model h as a random oracle, the security analysis requires either additional assumptions on h – which should behave as a computationally

secure (a.k.a. entropy-smoothing [27]) key derivation function – or larger key sizes [3,17,18]. Indeed, as observed in [18, Appendix A], using an information-theoretically secure key derivation function, the Leftover Hash Lemma [20,21] would require y^r to come from a distribution with about 300 bits of min-entropy in order to produce a 128-bit symmetric encryption key.

To overcome the message-encoding issue, Virat came with a different approach in [30]. Her idea consists in working with an elliptic curve over the ring $\mathbb{F}_p[\varepsilon]$, namely the ring of dual numbers over the prime field $\mathbb{F}_p$. Doing so, the message space becomes $\mathbb{F}_p$; i.e., messages are now viewed as integers in the set $\{0, \ldots, p-1\}$ rather than points on an elliptic curve.

Homomorphism Property. Malleability of ciphertexts is usually seen as an undesirable property. It proves nevertheless very useful in certain applications. Examples include electronic voting, electronic commerce or, more generally, privacy-preserving computations. The basic ElGamal scheme satisfies a homomorphism property with respect to the group law in $\mathbb{G}$. Namely, if $\cdot$ denotes the group law in $\mathbb{G}$ then given the ElGamal encryption of messages $m_1, m_2 \in \mathbb{G}$, anyone can derive the encryption of $m_1 \cdot m_2$. Indeed, letting $C_1 = (c_{1,1}, c_{1,2})$ and $C_2 = (c_{2,1}, c_{2,2})$ the respective encryption of m_1 and m_2, with $c_{i,1} = g^{r_i}$ and $c_{i,2} = m_i\, y^{r_i}$ $(i \in \{1,2\})$, it is easily checked that

$$C_3 = (c_{1,1} \cdot c_{2,1}, c_{2,1} \cdot c_{2,2})$$

is the encryption of message $m_3 = m_1 \cdot m_2 \in \mathbb{G}$. For elliptic-curve ElGamal, including Virat's cryptosystem, this translates into the encryption of the (elliptic-curve) addition of two points. When the exponent variant is used, composing two ciphertexts yields the encryption of a message $m_3 = m_1 + m_2 \pmod q$, where messages m_1 and m_2 are viewed as elements in a small subset of $\mathbb{Z}/q\mathbb{Z}$.

Hash ElGamal is only *partially* homomorphic, w.r.t. the XOR operator. Given the encryption of a message m, anyone can compute the encryption of a message $m' = m \oplus K$ for any chosen value $K \in \{0,1\}^\ell$. If $C = (c_1, c_2)$ with $c_1 = g^r$ and $c_2 = m \oplus h(y^r)$ then $C' = (c_1, c_2')$ with $c_2' = K \oplus c_2$ is the hash-ElGamal encryption of m'. This holds true, regardless of the underlying group. In particular, this is verified for elliptic curves.

Our Contribution. Compared to the classical elliptic-curve ElGamal encryption scheme, there are several drawbacks in Virat's cryptosystem. First it is computationally more demanding. Second it leads to an increased ciphertext expansion ratio. This is particularly damaging for elliptic curve cryptosystems as they are primarily designed to reduce the bandwidth. Third and more importantly, the security of the scheme is rather weak. It is only shown to be one-way; in particular, it does *not* provide semantic security.

We propose in this paper new ElGamal-type cryptosystems that enjoy the same advantage as Virat's cryptosystem (namely, no message encoding as points on elliptic curves) but without its drawbacks. In an earlier work, Chevallier-Mames *et al.* [9] astutely observe that certain mathematical properties of integers modulo p^2, where p is a prime number, allow getting rid of the message

encoding from the classical ElGamal cryptosystem. Unfortunately, the solution of [9] is not known to be readily instantiable over elliptic curve subgroups. As a consequence, the Chevallier-Mames *et al.* [9] system loses the benefit of shorter keys enabled by elliptic curve cryptography. In this work, we solve a problem left open by Chevallier-Mames *et al.* [9] and provide an adaptation of their scheme [9] to the elliptic curve setting. The resulting encryption schemes features the same ciphertext expansion ratio as [9] and retains the partial homomorphism properties (additive or multiplicative). We prove that they are semantically secure in the standard model under a natural hardness assumption. We also describe a chosen-ciphertext secure extension of these schemes.

2 Encoding-Free ElGamal Schemes

2.1 Virat's Cryptosystem

Let $\mathbb{K}$ be a finite field of characteristic $p \neq 2, 3$. The *ring of dual numbers of* $\mathbb{K}$ is $\mathbb{K}[\varepsilon]$ with $\varepsilon^2 = 0$.

Consider the elliptic curve E over $\mathbb{K}[\varepsilon]$ given by the Weierstraß equation

$$E : y^2 = x^3 + ax + b \tag{1}$$

with $a, b \in \mathbb{K}[\varepsilon]$ and $4a^3+27b^2 \neq 0$. The set of points $(x, y) \in \mathbb{K}[\varepsilon]\times\mathbb{K}[\varepsilon]$ satisfying this equation together with the points at infinity, $\boldsymbol{O}_k = (k\varepsilon : 1 : 0)$ with $k \in \mathbb{K}$, form an Abelian group under the chord-and-tangent rule. Explicit addition formulæ are provided in [31, Table 2.1]. This group is denoted by $E(\mathbb{K}[\varepsilon])$ and its order by $\#E(\mathbb{K}[\varepsilon])$. Since $E(\mathbb{K}[\varepsilon])$ contains the p-torsion subgroup formed by the points at infinity, its order is a multiple of p.

Virat's cryptosystem relies on elliptic curves over $\mathbb{F}_p[\varepsilon]$ for some prime $p > 3$. Hence let E be an elliptic curve over $\mathbb{F}_p[\varepsilon]$ as per Eq. (1) of order pq for some prime $q \neq p$, and let $\hat{\boldsymbol{P}}$ be a generator of $E(\mathbb{F}_p[\varepsilon])$.

$\mathsf{KeyGen}(1^\lambda)$. On input security parameter λ, generate a cyclic group $E(\mathbb{F}_p[\varepsilon]) = \langle\hat{\boldsymbol{P}}\rangle$ of order pq as above. Next, choose a random integer $x \xleftarrow{R} \mathbb{Z}/q\mathbb{Z}$ and compute $\boldsymbol{Y} = [xp]\hat{\boldsymbol{P}}$.

The public key is $pk = \{E(\mathbb{F}_p[\varepsilon]), q, \hat{\boldsymbol{P}}, \boldsymbol{Y}\}$ and the private key is $sk = \{x\}$.

$\mathsf{Encrypt}(pk, m)$. The encryption of a message $m \in \mathbb{F}_p$ is given as follows:

1. Choose a random integer $r \xleftarrow{R} \mathbb{Z}/q\mathbb{Z}$;
2. Choose a random finite point $(x_0, y_0) \xleftarrow{R} E(\mathbb{F}_p)$;
3. Define $\hat{\boldsymbol{M}} = (x_0 + m\varepsilon, y_0 + y_1\varepsilon)$ where y_1 is the unique solution in $\mathbb{F}_p$ such that $\hat{\boldsymbol{M}} \in E(\mathbb{F}_p[\varepsilon])$;
4. Compute the points $\boldsymbol{C_1} = [rp]\hat{\boldsymbol{P}}$ and $\hat{\boldsymbol{C}}_\mathbf{2} = \hat{\boldsymbol{M}} + [r]\boldsymbol{Y}$;
5. Output the ciphertext $C = (\boldsymbol{C_1}, \hat{\boldsymbol{C}}_\mathbf{2})$.

$\mathsf{Decrypt}(sk, C)$. The decryption of $C = (\boldsymbol{C_1}, \hat{\boldsymbol{C}}_\mathbf{2})$ is obtained as $\hat{\boldsymbol{M}} = \hat{\boldsymbol{C}}_\mathbf{2} - [x]\boldsymbol{C_1}$ using secret key x, which in turn yields the value of m.

In a variant, Virat suggests to define the elliptic curve E over $\mathbb{F}_p[\varepsilon]$ but with curve parameters $a, b \in \mathbb{F}_p$. It is then shown that the scheme is one-way under the computational Diffie-Hellman assumption in $E(\mathbb{F}_p)$ [30, Theorem 6.4].

Given the x-coordinate of a finite point in $E(\mathbb{F}_p[\varepsilon])$, there are two possible values for its y-coordinate. So $2|p|+1$ bits suffice to represent $\boldsymbol{C_1}$ or $\hat{\boldsymbol{C}}_{\boldsymbol{2}}$, leading to a ciphertext expansion ratio of $4 \div 1$ [30, Sect. 5.2].

Remark 1. When the curve parameters $a, b \in \mathbb{F}_p$, Lemma 1 in [1] implies that for every finite point $\hat{\boldsymbol{P}} = (x_0 + x_1\varepsilon, y_0 + y_1\varepsilon) \in E(\mathbb{F}_p[\varepsilon])$ there exists a unique $k \in \mathbb{F}_p$ such that $\hat{\boldsymbol{P}} = \boldsymbol{P} + \boldsymbol{O}_k$ with $\boldsymbol{P} = (x_0, y_0) \in E(\mathbb{F}_p)$. It thus turns out that $[p]\hat{\boldsymbol{P}} = [p]\boldsymbol{P} + [p](k\varepsilon : 1 : 0) = [p]\boldsymbol{P} \in E(\mathbb{F}_p)$. In this case, it is interesting to define the public key as $pk = \{E(\mathbb{F}_p[\varepsilon]), q, \boldsymbol{Q}, \boldsymbol{Y}\}$ where $\boldsymbol{Q} = [p]\hat{\boldsymbol{P}} \in E(\mathbb{F}_p)$ and to evaluate $\boldsymbol{C_1}$ as $\boldsymbol{C_1} = [r]\boldsymbol{Q} \in E(\mathbb{F}_p)$. The ciphertext expansion ratio then drops to $3 \div 1$ using a compressed point representation (i.e., $\boldsymbol{C_1}$ is represented with $|p|+1$ bits and $\hat{\boldsymbol{C}}_{\boldsymbol{2}}$ with $2|p|+1$ bits).

2.2 The Chevallier-Mames–Paillier–Pointcheval Scheme

The scheme of Chevallier-Mames *et al.* [9] is based on the class function over cyclic subgroups of $\mathbb{F}_p^*$. Specifically, for primes p and q such that $q \mid p-1$, given a cyclic subgroup $\langle g \rangle \subseteq \mathbb{F}_p^*$ of order q, the class of $w = g^a \bmod p$ (w.r.t. $\hat{g}$) is denoted by $[\![w]\!]$ and is defined as the unique integer in $\mathbb{Z}/p\mathbb{Z}$ such that

$$\hat{g}^{\mathrm{CRT}([\![w]\!],a)} \bmod p^2 = w$$

for some $\hat{g} \in (\mathbb{Z}/p^2\mathbb{Z})^*$ of order pq and such that $\hat{g} \equiv g \pmod p$, and where $\mathrm{CRT}([\![w]\!], a)$ is an integer such that

$$\mathrm{CRT}([\![w]\!], a) \equiv [\![w]\!] \pmod p \quad \text{and} \quad \mathrm{CRT}([\![w]\!], a) \equiv a \pmod q;$$

see [9, Sect. 4.1]. For example, if $\hat{g} = \big(1 - k\,p\big)\, g^p \bmod p^2$ with $k := \frac{(p-1)}{q}$ then

$$[\![w]\!] = \frac{(w^q \bmod p^2) - 1}{p} \bmod p.$$

Proof. Observe that $\hat{g} \equiv g^p \equiv g \pmod p$ as required. Remark also that, as elements in $(\mathbb{Z}/p^2\mathbb{Z})^*$, $1 - k\,p \pmod{p^2}$ is of order p and $g^p \pmod{p^2}$ is of order q. Hence, it follows that $w \equiv \hat{g}^{\mathrm{CRT}([\![w]\!],a)} \equiv (1-k\,p)^{[\![w]\!]}\,(g^p)^a \pmod{p^2}$ and thus $w^q \equiv (1-k\,p)^{[\![w]\!]\,q} \equiv 1 - (k\,[\![w]\!]\,q)p \equiv 1 + [\![w]\!]\,p \pmod{p^2}$. □

Equipped with such an efficiently computable class function, the encryption scheme of Chevallier-Mames *et al.* goes as follows.

$\mathsf{KeyGen}(1^\lambda)$. On input security parameter λ, generate a prime p and an element $g \in \mathbb{F}_p^*$ of large prime order q. Next, compute $y = g^x \bmod p$ for some random integer $x \xleftarrow{R} \mathbb{Z}/q\mathbb{Z}$. The public key is $pk = \{\mathbb{F}_p^*, q, g, y\}$ and the private key is $sk = \{x\}$.

Encrypt(pk, m). The encryption of $m \in \mathbb{Z}/p\mathbb{Z}$ is given by the following algorithm:
1. Choose a random $r \xleftarrow{R} \mathbb{Z}/q\mathbb{Z}$. Compute $c_1 = g^r \bmod p$ and $d = y^r \bmod p$;
2. Define $c_2 = m + [\![d]\!] \pmod p$;
3. Output the ciphertext $C = (c_1, c_2)$.

Decrypt(sk, C). $C = (c_1, c_2)$ is decrypted as $m = c_2 - [\![{c_1}^x \bmod p]\!] \pmod p$ using the private key $sk = x$.

3 New Cryptosystems

Rather than considering elliptic curves over the ring $\mathbb{F}_p[\varepsilon]$, we work with elliptic curves defined over the ring $\mathbb{Z}/p^2\mathbb{Z}$. Borrowing the terminology of [9], this allows us to define a class function whereupon new ElGamal-type cryptosystems are derived. See also [16] for another family of cryptosystems making use of elliptic curves defined over a ring.

3.1 Class Function on Elliptic Curves

Since $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \subset \mathbb{Z}/p^2\mathbb{Z}$, we can view an elliptic curve given by a Weierstraß equation (with curve parameters $a, b \in \mathbb{F}_p$) over the ring $\mathbb{Z}/p^2\mathbb{Z}$. In order to deal with the points at infinity, we regard the projective form

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

The set of points on this elliptic curve over $\mathbb{Z}/p^2\mathbb{Z}$ is denoted by $E(\mathbb{Z}/p^2\mathbb{Z})$. The subset of points that reduce to $\boldsymbol{O} = (0 : 1 : 0)$ modulo p is denoted by $E_1(\mathbb{Z}/p^2\mathbb{Z})$; see [28, Sect. 2].

Proposition 1. *Using the previous notations, we have*

$$E_1(\mathbb{Z}/p^2\mathbb{Z}) = \{(\alpha p : 1 : 0) \mid 0 \leq \alpha \leq p-1\}.$$

Proof. By definition, we have $E_1(\mathbb{Z}/p^2\mathbb{Z}) = \{(X : Y : Z) \in E(\mathbb{Z}/p^2\mathbb{Z}) \mid (X : Y : Z) \equiv (0 : 1 : 0) \pmod p\}$. Since $Y \equiv 1 \pmod p$ we obviously have $Y \not\equiv 0 \pmod{p^2}$ and so we can write $E_1(\mathbb{Z}/p^2\mathbb{Z}) = \{(\frac{X}{Y} : 1 : \frac{Z}{Y}) \in E(\mathbb{Z}/p^2\mathbb{Z}) \mid (X : Y : Z) \equiv (0 : 1 : 0) \pmod p\} = \{(\alpha p : 1 : \gamma p) \in E(\mathbb{Z}/p^2\mathbb{Z}) \mid 0 \leq \alpha, \gamma \leq p-1\}$. Plugging $(\alpha p : 1 : \gamma p)$ into the Weierstraß equation yields $\gamma p = 0 \pmod{p^2} \iff \gamma = 0 \pmod p$. We therefore get $E_1(\mathbb{Z}/p^2\mathbb{Z}) = \{(\alpha p : 1 : 0) \mid 0 \leq \alpha \leq p-1\}$. □

The theory of formal groups [28, Proposition IV.3.2] implies that $E_1(\mathbb{Z}/p^2\mathbb{Z})$ is a group isomorphic to the additive group $(\mathbb{Z}/p\mathbb{Z})^+$. We have

$$\Gamma : E_1(\mathbb{Z}/p^2\mathbb{Z}) \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})^+, (\alpha p : 1 : 0) \longmapsto \alpha.$$

Hence, the sum of two elements $(\alpha_1 p : 1 : 0)$ and $(\alpha_2 p : 1 : 0)$ in $E_1(\mathbb{Z}/p^2\mathbb{Z})$ is given by $(\alpha_3 p : 1 : 0)$ with $\alpha_3 = (\alpha_1 + \alpha_2) \bmod p$. This also implies that $E_1(\mathbb{Z}/p^2\mathbb{Z})$ is a cyclic group of order p. Letting $\boldsymbol{U} = (p : 1 : 0)$, we can write $E_1(\mathbb{Z}/p^2\mathbb{Z}) = \langle \boldsymbol{U} \rangle$.

Given a finite point $\boldsymbol{P} = (x, y) \in E(\mathbb{F}_p)$, with $y \neq 0$, we define

$$\Delta(\boldsymbol{P}) = \frac{(x^3 + ax + b - y^2) \bmod p^2}{p} \quad \text{and} \quad \psi(\boldsymbol{P}) = \frac{\Delta(\boldsymbol{P})}{2y} \bmod p.$$

[In the definition of $\Delta(\boldsymbol{P})$, point $\boldsymbol{P}$ is lifted; i.e., its coordinates x and y are viewed as integers.]

This gives rise to the map

$$\Psi : E(\mathbb{F}_p) \to E(\mathbb{Z}/p^2\mathbb{Z}), \begin{cases} \boldsymbol{O} \mapsto \boldsymbol{O} \\ (x, y) \mapsto (x, y + \psi(\boldsymbol{P})p). \end{cases}$$

To ease the notation, we will sometimes write $\tilde{\boldsymbol{P}}$ for $\Psi(\boldsymbol{P})$.

We assume that E is not an anomalous curve (i.e., $\#E(\mathbb{F}_p) \neq p$) and we let $q = \mathrm{ord}_E(\boldsymbol{P})$ denote the order of point $\boldsymbol{P} \in E(\mathbb{F}_p)$. We define $\boldsymbol{V} = [p]\tilde{\boldsymbol{P}}$. Clearly, we have that $\boldsymbol{V}$ is of order q.

Consider now the subgroups $\mathbb{G} = \langle \boldsymbol{P} \rangle \subseteq E(\mathbb{F}_p)$ of order q and $\hat{\mathbb{G}} = \langle \boldsymbol{U}, \boldsymbol{V} \rangle \subseteq E(\mathbb{Z}/p^2\mathbb{Z})$ of order pq. Any element $\boldsymbol{Q} \in \hat{\mathbb{G}}$ can uniquely be written as

$$\boldsymbol{Q} = [\beta]\boldsymbol{U} + [\alpha]\boldsymbol{V} \quad \text{for some } \alpha \ \in \mathbb{Z}/q\mathbb{Z} \text{ and } \beta \in \mathbb{Z}/p\mathbb{Z}. \tag{2}$$

We call integer β the *class of* $\boldsymbol{Q}$ and write $\beta = [\![\boldsymbol{Q}]\!]$. The crucial observation is that $\Psi(\mathbb{G}) \subseteq \hat{\mathbb{G}}$. As a consequence, to any element $\boldsymbol{Q} \in \mathbb{G}$, we similarly define its class as $[\![\tilde{\boldsymbol{Q}}]\!]$. To ease the notation, we will sometimes omit the tilde and simply write $[\![\boldsymbol{Q}]\!]$.

It is worth noticing that computing the class is easy. By definition, from the unique decomposition of a point $\boldsymbol{Q} \in \hat{\mathbb{G}}$ as $\boldsymbol{Q} = [\beta]\boldsymbol{U} + [\alpha]\boldsymbol{V}$ with $\beta = [\![\boldsymbol{Q}]\!]$, it immediately follows that $[q]\boldsymbol{Q} = [q\beta]\boldsymbol{U} = (q\beta p : 1 : 0)$ and thus

$$[\![\boldsymbol{Q}]\!] = \frac{\Gamma([q]\boldsymbol{Q})}{q} \bmod p. \tag{3}$$

3.2 An Additive Cryptosystem

With the above setting, we can now describe our first cryptosystem. The message space is $\mathbb{Z}/p\mathbb{Z}$ for some prime p.

$\mathsf{KeyGen}(1^\lambda)$. On input security parameter λ, generate an elliptic curve E over the prime field $\mathbb{F}_p$ and a point $\boldsymbol{P} \in E(\mathbb{F}_p)$ of large prime order q. Next, compute the point $\boldsymbol{Y} = [x]\boldsymbol{P} \in E(\mathbb{F}_p)$ for some random integer $x \xleftarrow{R} \mathbb{Z}/q\mathbb{Z}$.
The public key is $pk = \{E(\mathbb{F}_p), q, \boldsymbol{P}, \boldsymbol{Y}\}$ and the private key is $sk = \{x\}$.

$\mathsf{Encrypt}(pk, m)$. The encryption of a message $m \in \mathbb{Z}/p\mathbb{Z}$ is given by the following algorithm:

1. Choose a random integer $r \xleftarrow{R} \mathbb{Z}/q\mathbb{Z}$;
2. Compute in $E(\mathbb{F}_p)$ the points $\boldsymbol{C_1} = [r]\boldsymbol{P}$ and $\boldsymbol{C_2} = [r]\boldsymbol{Y}$;
3. Compute $\beta = [\![\tilde{\boldsymbol{C}}_{\boldsymbol{2}}]\!]$;

4. Define $c_2 = m + \beta \pmod p$;
5. Output the ciphertext $C = (\boldsymbol{C_1}, c_2)$.

$\mathsf{Decrypt}(sk, C)$. The decryption of $C = (\boldsymbol{C_1}, c_2)$ is obtained as $m = c_2 - [\![\Psi([x]\boldsymbol{C_1})]\!] \pmod p$ using the secret key x.

The above cryptosystem presents a number of advantages. First, the ciphertexts are very compact. In their basic version, they feature a $3 \div 1$ ciphertext expansion ratio. This ratio can even be reduced to only $2 \div 1$ by using a compressed representation for $\boldsymbol{C_1}$. Second, as will be shown in Sect. 4, it meets the standard IND-CPA security level in the standard model (while Virat's cryptosystem only satisfies one-wayness). Third, the proposed cryptosystem is to some extent malleable. More precisely, if $(\boldsymbol{C_1}, c_2)$ denotes the [additive] encryption of a message m then $(\boldsymbol{C_1}, c_2 + K \pmod p)$ is the encryption of message $m + K \pmod p$ for any $K \in \mathbb{Z}/p\mathbb{Z}$. Fourth, encryption is very fast. In an on-line/off-line mode [13], the encryption of a message m only requires a mere addition modulo p. Fifth, in contrast to classical ElGamal on elliptic curves over $\mathbb{F}_p$, no prior encoding of the message as a point on an elliptic curve is required.

3.3 A Multiplicative Cryptosystem

The previous cryptosystem is additive. As $\mathbb{Z}/p\mathbb{Z}$ is equipped with both addition and multiplication, we can define a multiplicative cryptosystem by replacing Step 3.2 in the encryption process accordingly.

$\mathsf{KeyGen}(1^\lambda)$ Idem.

$\mathsf{Encrypt}(pk, m)$. The encryption of a message $m \in \mathbb{Z}/p\mathbb{Z}$ is given by the following algorithm:

1. Choose a random integer $r \xleftarrow{R} \mathbb{Z}/q\mathbb{Z}$;
2. Compute in $E(\mathbb{F}_p)$ the points $\boldsymbol{C_1} = [r]\boldsymbol{P}$ and $\boldsymbol{C_2} = [r]\boldsymbol{Y}$;
3. Compute $\beta = [\![\tilde{\boldsymbol{C}}_{\boldsymbol{2}}]\!]$;
4. Define $c_2 = m \cdot \beta \pmod p$;
5. Output the ciphertext $C = (\boldsymbol{C_1}, c_2)$.

$\mathsf{Decrypt}(sk, C)$. The decryption of $C = (\boldsymbol{C_1}, c_2)$ is obtained as $m = c_2 / [\![\Psi([x]\boldsymbol{C_1})]\!] \pmod p$ using the secret key x.

This multiplicative variant shares the advantages as its additive counterpart. The difference resides in that it is partially homomorphic w.r.t. multiplication; that is, if $(\boldsymbol{C_1}, c_2)$ is the [multiplicative] encryption of a message m then $(\boldsymbol{C_1}, c_2 \cdot K \pmod p)$ is the encryption of message $m \cdot K \pmod p$.

4 Security Analysis

4.1 Complexity Assumptions

Let $E(\mathbb{F}_p)$ be an elliptic curve over the prime field $\mathbb{F}_p$ and let $\mathbb{G} \subseteq E(\mathbb{F}_p)$ a cyclic subgroup thereof. Let also $\boldsymbol{P}$ be a generator of $\mathbb{G}$ and $\tilde{\boldsymbol{P}} = \Psi(\boldsymbol{P}) \in E(\mathbb{Z}/p^2\mathbb{Z})$.

We remind that the class of a point $\boldsymbol{Q} \in \mathbb{G}$ (w.r.t. $\boldsymbol{P}$), denoted $[\![\boldsymbol{Q}]\!]$, is the unique integer $\beta \in \mathbb{Z}/p\mathbb{Z}$ such that $\Psi(\boldsymbol{Q}) = [\beta]\boldsymbol{U} + [\alpha]\boldsymbol{V}$ where $\boldsymbol{U} = (p : 1 : 0)$ and $\boldsymbol{V} = [p]\tilde{\boldsymbol{P}}$.

Given $\boldsymbol{P}$ and $[a]\boldsymbol{P}, [b]\boldsymbol{P} \xleftarrow{R} \mathbb{G} = \langle \boldsymbol{P} \rangle \subseteq E(\mathbb{F}_p)$, the *elliptic curve class computational Diffie-Hellman (Class-CDH) problem* is to compute the class of $[ab]\boldsymbol{P}$; i.e., $[\![[ab]\boldsymbol{P}]\!]$. Likewise, the *elliptic curve class decisional Diffie-Hellman (Class-DDH) problem* is to distinguish between the two distributions $(\boldsymbol{P}, [a]\boldsymbol{P}, [b]\boldsymbol{P}, [\![[ab]\boldsymbol{P}]\!])$ and $(\boldsymbol{P}, [a]\boldsymbol{P}, [b]\boldsymbol{P}, \vartheta)$ for $a, b \xleftarrow{R} [0, \#\mathbb{G})$ and $\vartheta \xleftarrow{R} \mathbb{Z}/p\mathbb{Z}$. We assume that these two problems are hard.

More formally, define an instance-generating algorithm $\mathcal{G}$ taking as input a security parameter λ and returning (the description of) a cyclic group $\mathbb{G} \subseteq E(\mathbb{F}_p)$, its order $q = \#\mathbb{G}$, and a generator $\boldsymbol{P}$, as above. We consider the following experiment for an adversary $\mathcal{A}$.

$\mathsf{Class}_{\mathcal{A},\mathcal{G}}(\lambda)$:

1. Run $\mathcal{G}(1^\lambda)$ and obtain $(E(\mathbb{F}_p), q, \boldsymbol{P})$;
2. Choose $a, b \xleftarrow{R} \mathbb{Z}/q\mathbb{Z}$ and compute $[a]\boldsymbol{P}$ and $[b]\boldsymbol{P}$;
3. $\mathcal{A}$ is given $(E(\mathbb{F}_p), q, \boldsymbol{P}, [a]\boldsymbol{P}, [b]\boldsymbol{P})$ and outputs $\beta' \in \mathbb{Z}/p\mathbb{Z}$;
4. The output of the experiment is 1 if $\beta' = [\![\boldsymbol{C}]\!]$ where $\boldsymbol{C} = [ab]\boldsymbol{P} \in E(\mathbb{F}_p)$, and 0 otherwise.

Definition 1. *The* Class-CDH assumption *says that for any probabilistic polynomial-time adversary $\mathcal{A}$ there exists a negligible function* negl *such that*

$$\Pr\big[\mathsf{Class}_{\mathcal{A},\mathcal{G}}(\lambda) = 1\big] \leq \mathrm{negl}(\lambda).$$

Definition 2. *The* Class-DDH assumption *says that for any probabilistic polynomial-time adversary $\mathcal{A}$ there exists a negligible function* negl *such that*

$$\Big|\Pr\Big[\mathcal{A}\big(E(\mathbb{F}_p), q, \boldsymbol{P}, [a]\boldsymbol{P}, [b]\boldsymbol{P}, [\![[ab]\boldsymbol{P}]\!]\big) = 1\Big] - \Pr\Big[\mathcal{A}\big(E(\mathbb{F}_p), q, \boldsymbol{P}, [a]\boldsymbol{P}, [b]\boldsymbol{P}, \vartheta\big) = 1\Big]\Big| \leq \mathrm{negl}(\lambda)\,,$$

where the probabilities are taken over the experiment of running $(E(\mathbb{F}_p), q, \boldsymbol{P}) \leftarrow \mathcal{G}(1^\lambda)$ and choosing $a, b \xleftarrow{R} \mathbb{Z}/q\mathbb{Z}$ and $\vartheta \xleftarrow{R} \mathbb{Z}/p\mathbb{Z}$.

4.2 Semantic Security

Clearly the one-wayness of our cryptosystems is equivalent to the Class-CDH assumption.

We show below that the proposed cryptosystems are semantically secure under the Class-DDH assumption. We state:

Theorem 1. *The schemes of Sects. 3.2 and 3.3 are* IND-CPA *under the Class-DDH assumption.*

Proof. In order to deal with the two cryptosystems at the same time, we write the second part of the ciphertext, c_2, as $c_2 = m \star \beta \pmod p$ where $\star$ stands for addition modulo p or multiplication modulo p.

The goal is to construct a distinguisher $\mathcal{D}$ against the Class-DDH problem from an IND-CPA attacker $\mathcal{A}$ against the scheme. Consider the following algorithm $\mathcal{D}$ receiving as challenge the Class Diffie-Hellman triplet $([a]\boldsymbol{P}, [b]\boldsymbol{P}, \beta)$ for $(E(\mathbb{F}_p), q, \boldsymbol{P}) \leftarrow \mathcal{G}(1^\lambda)$, where either $\beta = [\![[ab]\boldsymbol{P}]\!]$ or $\beta = \vartheta$, with $a, b \xleftarrow{R} \mathbb{Z}/q\mathbb{Z}$ and $\vartheta \xleftarrow{R} \mathbb{Z}/p\mathbb{Z}$:

1. Set $\boldsymbol{Y} = [a]\boldsymbol{P}$ and define $pk = \{E(\mathbb{F}_p, q, \boldsymbol{P}, \boldsymbol{Y}\}$;
2. Call $\mathcal{A}(pk)$ and receive two messages m_0 and m_1 in $\mathbb{Z}/p\mathbb{Z}$;
3. Choose a bit b at random and define $C = ([a]\boldsymbol{P}, m_b \star \beta)$;
4. Return ciphertext C to $\mathcal{A}$ and obtain its output bit b';
5. Output 1 if $b' = b$, and 0 otherwise.

When $\beta = [\![[ab]\boldsymbol{P}]\!]$, C is a faithful ciphertext for message m_b. On the contrary, when $\beta = \vartheta$, C appears as a random value, independent of m_b. As a result, if $\epsilon(\lambda)$ denotes the probability that $\mathcal{A}$ wins the IND-CPA game, this means that

$$\Pr\big[\mathcal{D}\big(E(\mathbb{F}_p), q, \boldsymbol{P}, [a]\boldsymbol{P}, [b]\boldsymbol{P}, [\![[ab]\boldsymbol{P}]\!]\big) = 1\big] = \epsilon(\lambda)$$

and

$$\Pr\big[\mathcal{D}\big(E(\mathbb{F}_p), q, \boldsymbol{P}, [a]\boldsymbol{P}, [b]\boldsymbol{P}, \vartheta\big) = 1\big] = \frac{1}{2}.$$

But the Class-DDH assumption says that their difference should be a negligible function in λ, that is, $\big|\epsilon(\lambda) - \frac{1}{2}\big| \leq \mathrm{negl}(\lambda)$. □

5 Extension

5.1 Chameleon Hash Functions

Chameleon hash functions [23] are hash functions associated with a pair (hk, tk) of hashing/trapdoor keys. The name chameleon refers to the ability for the owner of the trapdoor key to modify the input without changing the output.

A chameleon hash function is defined by a tuple of three algorithms: $(\mathsf{CMKg}, \mathsf{CMhash}, \mathsf{CMswitch})$. The key-generation algorithm CMKg, given a security parameter λ, outputs a key pair $(hk, tk) \leftarrow \mathsf{CMKg}(1^\lambda)$. The hashing algorithm outputs $y = \mathsf{CMhash}(hk, m, r)$ given the public key hk, a message m and random coins $r \in \mathcal{R}_{hash}$. On input of m, r, m' and the trapdoor key tk, the switching algorithm $r' \leftarrow \mathsf{CMswitch}(tk, m, r, m')$ outputs $r' \in \mathcal{R}_{hash}$ such that

$$\mathsf{CMhash}(hk, m, r) = \mathsf{CMhash}(hk, m', r').$$

Collision-resistance mandates that it be infeasible to find pairs $(m', r') \neq (m, r)$ such that $\mathsf{CMhash}(hk, m, r) = \mathsf{CMhash}(hk, m', r')$ without knowing tk. Uniformity guarantees that the distribution of hashes is independent of the message m, in particular, for all hk and m, m', the distributions

$$\{r \leftarrow \mathcal{R}_{hash} \colon \mathsf{CMhash}(hk, m, r)\} \quad \text{and} \quad \{r \leftarrow \mathcal{R}_{hash} \colon \mathsf{CMhash}(hk, m', r)\}$$

are identical.

5.2 A Chosen-Ciphertext-Secure Construction

In this section, we describe an IND-CCA2-secure extension of our schemes which builds on the approach of Cash, Kiltz and Shoup [7] in its security analysis. We present below the additive variant. The multiplicative variant proceeds similarly.

$\mathsf{KeyGen}(1^\lambda)$. On input security parameter λ, generate an elliptic curve E over the prime field $\mathbb{F}_p$ and a point $\boldsymbol{P} \in E(\mathbb{F}_p)$ of large prime order q. Then, do the following.

1. Choose $y_0, y_1, z_0, z_1 \xleftarrow{R} \mathbb{Z}/q\mathbb{Z}$ and compute points $\boldsymbol{Y_0}, \boldsymbol{Y_1}, \boldsymbol{Z_0}, \boldsymbol{Z_1} \in E(\mathbb{F}_p)$ as

$$\boldsymbol{Y_0} = [y_0]\boldsymbol{P}, \qquad \boldsymbol{Y_1} = [y_1]\boldsymbol{P},$$
$$\boldsymbol{Z_0} = [z_0]\boldsymbol{P}, \qquad \boldsymbol{Z_1} = [z_1]\boldsymbol{P}.$$

2. Choose a chameleon hash function $\mathsf{CMH} = (\mathsf{CMKg}, \mathsf{CMhash}, \mathsf{CMswitch})$ that ranges over $\mathbb{Z}/q\mathbb{Z}$, with a key pair $(hk, tk) \leftarrow \mathsf{CMKg}(1^\lambda)$. We denote by $\mathcal{R}_{hash}$ the randomness space of the hashing algorithm.

The public key is $pk = \{E(\mathbb{F}_p), q, \boldsymbol{P}, \boldsymbol{Y_0}, \boldsymbol{Y_1}, \boldsymbol{Z_0}, \boldsymbol{Z_1}, hk\}$ and the matching private key is $sk = \{y_0, y_1, z_0, z_1\}$.

$\mathsf{Encrypt}(pk, m)$. To encrypt a message $m \in \mathbb{Z}/p\mathbb{Z}$, do the following.

1. Choose $r \xleftarrow{R} \mathbb{Z}/q\mathbb{Z}$ as well as $s \xleftarrow{R} \mathcal{R}_{hash}$;
2. Compute in $E(\mathbb{F}_p)$, $\boldsymbol{C_0} = [r]\boldsymbol{Y_0}$ and $\boldsymbol{C_1} = [r]\boldsymbol{P}$;
3. Compute $\beta = [\![\tilde{\boldsymbol{C}}_{\boldsymbol{0}}]\!]$ and $c_0 = m + \beta \pmod p$;
4. Compute $t = \mathsf{CMhash}(hk, (c_0, \boldsymbol{C_1}), s_{hash}) \in \mathbb{Z}/q\mathbb{Z}$;
5. Compute

$$\boldsymbol{C_2} = [rt]\boldsymbol{Y_0} + [r]\boldsymbol{Z_0}, \qquad \boldsymbol{C_3} = [rt]\boldsymbol{Y_1} + [r]\boldsymbol{Z_1};$$

6. Output the ciphertext $C = (c_0, \boldsymbol{C_1}, \boldsymbol{C_2}, \boldsymbol{C_3}, s_{hash})$.

$\mathsf{Decrypt}(sk, C)$. Given the ciphertext $C = (c_0, \boldsymbol{C_1}, \boldsymbol{C_2}, \boldsymbol{C_3}, s_{hash})$ and the private key $sk = (y_0, y_1, z_0, z_1)$, conduct the following steps.

1. Compute $t = \mathsf{CMhash}(hk, (c_0, \boldsymbol{C_1}), s_{hash}) \in \mathbb{Z}/q\mathbb{Z}$;
2. Return $\perp$ if $\boldsymbol{C_2} \neq [ty_0 + z_0]\boldsymbol{C_1}$ or $\boldsymbol{C_3} \neq [ty_1 + z_1]\boldsymbol{C_1}$;
3. Compute $\boldsymbol{C_0} = [y_0]\boldsymbol{C_1}$ and return $m = c_0 - \beta \bmod p$, where $\beta = [\![\tilde{\boldsymbol{C}}_{\boldsymbol{0}}]\!]$.

The above description follows a method suggested in [32] in that it makes use of a chameleon hash function to authenticate the message-carrying part c_0 of the ciphertext. We note that, instead of a chameleon hash function, the scheme could also use a strongly unforgeable one-time signature as in the Canetti-Halevi-Katz methodology [6]. However, this would incur longer ciphertexts. If we want to minimize the ciphertext overhead, the Boyen-Mei-Waters technique [5] can be used to eliminate the randomness s_{hash} of the chameleon hash function at the expense of introducing $O(\lambda)$ additional elliptic curve points in the public key.

Theorem 2. *The scheme is* IND-CCA*2-secure under the Class-DDH assumption, provided that the chameleon hash function is collision-resistant.*

Proof. The proof proceeds with a sequence of games. For each i, we denote by S_i the event that the adversary wins in Game i.

Game 0: This is the real game. In this game, the adversary $\mathcal{A}$ is given the public key pk and the challenger $\mathcal{B}$ answers all decryption queries by faithfully running the decryption algorithm. In the challenge phase, $\mathcal{A}$ chooses two distinct messages $m_0, m_1 \in \mathbb{Z}/p\mathbb{Z}$ and obtains a challenge ciphertext $C^\star = (c_0{}^\star, \boldsymbol{C_1}{}^\star, \boldsymbol{C_2}{}^\star, \boldsymbol{C_3}{}^\star, s^\star_{hash})$ which encrypts m_d, for some random bit $d \stackrel{R}{\leftarrow} \{0,1\}$. In the second phase, the adversary $\mathcal{A}$ is granted further access to the decryption oracle. At the end of the game, $\mathcal{A}$ outputs a bit $d' \in \{0,1\}$ and we denote by S_0 the event that $d' = d$.

Game 1: This game is identical to Game 0 but the challenger $\mathcal{B}$ rejects all pre-challenge decryption queries $C = (c_0, \boldsymbol{C_1}, \boldsymbol{C_2}, \boldsymbol{C_3}, s_{hash})$ such that $\boldsymbol{C_1} = \boldsymbol{C_1}{}^\star$. Since $\boldsymbol{C_1}{}^\star$ is uniformly distributed in $\langle \boldsymbol{P} \rangle$ and independent of $\mathcal{A}$'s view before the challenge phase, the probability that $\mathcal{B}$ rejects a ciphertext that would not have been rejected in Game 0 is at most q_{dec}/q, where q_{dec} is the number of decryption queries. We have $|\Pr[S_1] - \Pr[S_0]| \leq q_{dec}/q$.

Game 2: In this game, the challenger $\mathcal{B}$ aborts if it realizes that, before or after the challenge phase, $\mathcal{A}$ has made a decryption query $C = (c_0, \boldsymbol{C_1}, \boldsymbol{C_2}, \boldsymbol{C_3}, s_{hash})$ such that

$$t = \mathsf{CMhash}(hk, (c_0, \boldsymbol{C_1}), s_{hash}) = \mathsf{CMhash}(hk, (c_0{}^\star, \boldsymbol{C_1}{}^\star), s^\star_{hash}) = t^\star.$$

Clearly, the latter event would contradict the collision-resistance property of the chameleon hash function. Moreover, Game 2 and Game 1 proceed identically until the latter event occurs, so that we obtain the inequality $|\Pr[S_2] - \Pr[S_1]| \leq \mathbf{Adv}^{\text{CM-Hash}}(\lambda)$.

Game 3: This game is identical to Game 2 with the sole difference that the challenger $\mathcal{B}$ automatically rejects all post-challenge decryption queries of the form $C = (c_0{}^\star, \boldsymbol{C_1}{}^\star, \boldsymbol{C_2}, \boldsymbol{C_3}, s_{hash})$, where $(\boldsymbol{C_2}, \boldsymbol{C_3}) \neq (\boldsymbol{C_2}{}^\star, \boldsymbol{C_3}{}^\star)$. This change is only conceptual since these ciphertexts would be rejected in Game 2 as well. We thus have $\Pr[S_3] = \Pr[S_2]$.

Game 4: In this game, we modify the generation of the public key. At the outset of the game, $\mathcal{B}$ chooses a random value $t^\star \in \mathbb{Z}/q\mathbb{Z}$ in the range of the hashing algorithm CMhash, by hashing a random string R' using a random $s'_{hash} \stackrel{R}{\leftarrow} \mathcal{R}_{hash}$. It also picks $\gamma, \omega \stackrel{R}{\leftarrow} \mathbb{Z}/q\mathbb{Z}$ and sets $\boldsymbol{Y_1} = [\gamma]\boldsymbol{P} + [\omega]\boldsymbol{Y_0}$. It also picks $\gamma_0, \gamma_1 \stackrel{R}{\leftarrow} \mathbb{Z}/q\mathbb{Z}$ and sets

$$\boldsymbol{Z}_0 = [-t^\star]\boldsymbol{Y_0} + [\gamma_0]\boldsymbol{P}\,, \qquad \boldsymbol{Z}_1 = [-t^\star]\boldsymbol{Y}_1 + [\gamma_1]\boldsymbol{P}\,,$$

which implicitly defines the private key as $y_1 = \gamma + \omega y_0$, $z_0 = -t^\star y_0 + \gamma_0$ and $z_1 = -t^\star y_1 + \gamma_1$. In the challenge phase, $\mathcal{B}$ computes the challenge as

$$\boldsymbol{C_1}{}^\star = [r^\star]\boldsymbol{P}\,, \qquad \boldsymbol{C_2}{}^\star = [\gamma_0]\boldsymbol{C_1}{}^\star\,, \qquad \boldsymbol{C_3}{}^\star = [\gamma_1]\boldsymbol{C}^\star_1$$

while m_d is blinded as $c_0{}^\star = m_d + \beta^\star \pmod p$, where $\beta^\star = [\![\tilde{\boldsymbol{C_0}}{}^\star]\!]$, where $\boldsymbol{C_0}{}^\star = [y_0]\boldsymbol{C_1}{}^\star$. Finally, $\mathcal{B}$ uses the trapdoor key tk of the chameleon hash

function to obtain $s^{\star}_{hash} = \mathsf{CMswitch}(tk, (R', s'_{hash}), (c_0{}^{\star}, \boldsymbol{C_1}{}^{\star}))$ such that $t^{\star} = \mathsf{CMhash}(hk, (c_0^{\star}, \boldsymbol{C_1}{}^{\star}), s^{\star}_{hash})$.

In Game 4, we remark that the public key pk and the challenge ciphertext $C^{\star} = (c_0{}^{\star}, \boldsymbol{C_1}{}^{\star}, \boldsymbol{C_2}{}^{\star}, \boldsymbol{C_3}{}^{\star}, s^{\star}_{hash})$ both have the same distribution as in Game 3, so that $\mathcal{A}$'s view has not changed. We have $\Pr[S_4] = \Pr[S_3]$.

Game 5: In this game, we modify the decryption oracle. Namely, at each decryption query $C = \big(c_0, \boldsymbol{C_1}, \boldsymbol{C_2}, \boldsymbol{C_3}, s_{hash}\big)$, the challenger $\mathcal{B}$ computes the chameleon hash value $t = \mathsf{CMhash}(hk, (c_0, \boldsymbol{C_1}), s_{hash})$ as well as

$$\boldsymbol{W_1} = [(t - t^{\star})^{-1} \bmod q]\big(\boldsymbol{C_2} - [\gamma_0]\boldsymbol{C_1}\big)$$
$$\boldsymbol{W_2} = [(t - t^{\star})^{-1} \bmod q]\big(\boldsymbol{C_3} - [\gamma_1]\boldsymbol{C_1}\big)$$

At this point, $\mathcal{B}$ returns $\perp$ if $\boldsymbol{W_2} \neq [\gamma]\boldsymbol{C_1} + [\omega]\boldsymbol{W_1}$. Otherwise, $\mathcal{B}$ computes $\tilde{\boldsymbol{W_1}} = \Psi(\boldsymbol{W_1})$, obtains $\beta = [\![\tilde{\boldsymbol{W_1}}]\!]$ and returns $m = c_0 - \beta \pmod p$.

It is easy to see that, in the adversary's view, Game 5 is identical to Game 4 until the event F_5 that $\mathcal{B}$ fails to reject a ciphertext that would have been rejected in Game 4. Using the same arguments as in [7,11], we can prove that $\Pr[F_5] \leq q_{dec}/q$. Specifically, event F_5 can only occur for a decryption query on an invalid ciphertext $C = (c_0, \boldsymbol{C_1}, \boldsymbol{C_2}, \boldsymbol{C_3}, s_{hash})$ where

$$\boldsymbol{C_1} = [r]\boldsymbol{P}\,, \qquad \boldsymbol{C_2} = [r + r']([t]\boldsymbol{Y_0} + \boldsymbol{Z_0})\,, \qquad \boldsymbol{C_3} = [r + r'']([t]\boldsymbol{Y_1} + \boldsymbol{Z_1})$$

and either $r' \neq 0$ or $r'' \neq 0$. This implies that $\boldsymbol{W_1} = [r + r_1]\boldsymbol{Y_0}$ and $\boldsymbol{W_2} = [r + r_2]\boldsymbol{Y_1}$, where $r_1 \neq 0$ (resp. $r_2 \neq 0$) if and only if $r' \neq 0$ (resp. $r'' \neq 0$). It is easy to see that, if $r_2 = 0$ and $r_1 \neq 0$ or $r_1 = 0$ and $r_2 \neq 0$, the equality $\boldsymbol{W_2} = [\gamma]\boldsymbol{C_1} + [\omega]\boldsymbol{W_1}$ never holds and we thus assume that $r_1 \neq 0$ and $r_2 \neq 0$. However, in this case $[\gamma]\boldsymbol{C_1} + [\omega]\boldsymbol{W_1}$ can be written $[r]\boldsymbol{Y_1} + [\omega r_1]\boldsymbol{Y_0}$, which is the sum of an information-theoretically fixed value $[r]\boldsymbol{Y_1}$ and another term $[\omega r_1]\boldsymbol{Y_0}$ that is completely undetermined in $\mathcal{A}$'s view: indeed, for a fixed $\boldsymbol{Y_1} = [\gamma]\boldsymbol{P} + [\omega]\boldsymbol{Y_0}$, we have q equally likely candidates for ω at the first decryption query such that $r' \neq 0$ or $r'' \neq 0$. For this query, we can only have the equality $\boldsymbol{W_2} = [\gamma]\boldsymbol{C_1} + [\omega]\boldsymbol{W_1}$ by pure chance, with probability $1/q$. Throughout the game, each invalid decryption query allows an unbounded adversary to eliminate one candidate for ω. Hence, after i queries, the adversary is left with a probability of $1/(q - i)$ of inferring the right ω. In the worst case, this probability is smaller than $1/(q - q_{dec})$ for a given decryption query. A union bound over all decryption queries gives the inequality $|\Pr[S_5] - \Pr[S_4]| \leq \Pr[F_5] \leq q_{dec}/(q - q_{dec})$. We remark that the private exponents (y_0, y_1, z_0, z_1) are not used any longer in Game 5 and we thus rely on the Class-DDH assumption to move to Game 6.

Game 6: This game is like Game 5 with the difference that, in the challenge ciphertext $C^{\star} = (c_0{}^{\star}, \boldsymbol{C_1}{}^{\star}, \boldsymbol{C_2}{}^{\star}, \boldsymbol{C_3}{}^{\star}, s^{\star}_{hash})$, $c_0{}^{\star}$ is chosen as a uniformly random element of $\mathbb{Z}/p\mathbb{Z}$. Under the Class-DDH assumption, this change should not be noticeable to $\mathcal{A}$ and we can write $|\Pr[S_6] - \Pr[S_5]| \leq \mathbf{Adv}^{\text{Class-DDH}}(\lambda)$.

In Game 6, we easily see that $\Pr[S_6] = 1/2$ since the challenge ciphertext can be seen as an encryption of a random message of $\mathbb{Z}/p\mathbb{Z}$, which is completely independent of m_0 and m_1. When counting probabilities throughout the sequence of

games, we find that $|\Pr[S_0] - 1/2|$ is bounded by a sum of negligible functions under the aforementioned assumptions. □

Acknowledgments. We thank Frederik Vercauteren for useful discussions and Antoine Joux for comments on an earlier version of this work. The second author's work has been supported in part by the "Programme Avenir Lyon Saint-Etienne de l'Université de Lyon" in the framework of the programme "Investissements d'Avenir" (ANR-11-IDEX-0007) and by the French ANR ALAMBIC project (ANR-16-CE39-0006).

A Appendix

A.1 Public-Key Encryption

A *public-key encryption scheme* consists of three algorithms: ($\mathsf{KeyGen}, \mathsf{Encrypt}, \mathsf{Decrypt}$).

Key generation. The key generation algorithm KeyGen is a randomized algorithm that takes on input some security parameter λ and returns a matching pair of public key and secret key for some user: $(pk, sk) \xleftarrow{R} \mathsf{KeyGen}(1^\lambda)$.

Encryption. Let $\mathcal{M}$ be the message space. The encryption algorithm $\mathsf{Encrypt}$ is a randomized algorithm that takes on input a public key pk and a plaintext $m \in \mathcal{M}$, and returns a ciphertext C. We write $C \leftarrow \mathsf{Encrypt}(pk, m)$.

Decryption. The decryption algorithm $\mathsf{Decrypt}$ takes on input secret key sk (matching pk) and a ciphertext C, and returns the corresponding plaintext m or a symbol $\perp$ indicating that the ciphertext is invalid. We write $m \leftarrow \mathsf{Decrypt}(sk, C)$ if C is a valid ciphertext and $\perp \leftarrow \mathsf{Decrypt}(sk, C)$ if it is not.

It is required that $\mathsf{Decrypt}\big(sk, \mathsf{Encrypt}(pk, m)\big) = m$ for any message $m \in \mathcal{M}$.

A.2 Security Notions

Beyond the basic property of one-wayness, data privacy in a public-key encryption scheme is captured by the notion of *semantic security*: An adversary should not learn any information whatsoever about a plaintext given its encryption beyond the length of the plaintext. This notion is known to be equivalent to the (easier to deal with) notion of *indistinguishability of encryptions* [19]. Furthermore, since the encryption key is public, an adversary can always encrypt messages of its choice; in other words, the adversary can mount chosen-plaintext attacks. It is therefore customary to let $\mathsf{IND\text{-}CPA}$ denote the security notion achieved by a semantically secure public-key encryption scheme.

The advantage of an adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ in the $\mathsf{IND\text{-}CPA}$ experiment is defined as

$$\left| \Pr_{b \xleftarrow{R} \{0,1\}} \left[\begin{array}{l} (pk, sk) \leftarrow \mathsf{KeyGen}(1^\lambda), (m_0, m_1, s) \leftarrow \mathcal{A}_1(pk), \\ C^\star \leftarrow \mathsf{Encrypt}(pk, m_b) \ : \ \mathcal{A}_2(m_0, m_1, s, C^\star) = b \end{array} \right] - \frac{1}{2} \right| \qquad (*)$$

where the probability is taken over the random coins of the experiment according to the distribution induced by $\mathsf{KeyGen}(1^\lambda)$ as well as the ones of the adversary, and $m_0, m_1 \in \mathcal{M}$. An encryption is IND-CPA if the advantage of any polynomial-time adversary $\mathcal{A}$ is negligible a a function of λ.

The IND-CPA security notion offers an adequate security level in the presence of a *passive* adversary. The "right" security level against *active* attacks is that of IND-CCA2 security, or *security against chosen-ciphertext attacks*. The definition of the adversary's advantage as given by (*) extends to the IND-CCA2 model but the adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ is now given an adaptive access to a decryption oracle to which it can submit any ciphertext of its choice with the exception that $\mathcal{A}_2$ may not query the decryption oracle on challenge ciphertext $C^\star$.

A.3 Consistent Lifting Problem

In this section, we extend the results of [8] to the elliptic curve setting.

Let $E(\mathbb{F}_p)$ be an elliptic curve over the prime field $\mathbb{F}_p$ and let $\mathbb{G} \subseteq E(\mathbb{F}_p)$ be a cyclic subgroup thereof. Let also $\boldsymbol{P}$ be a generator of $\mathbb{G}$ (i.e., $\mathbb{G} = \langle \boldsymbol{P} \rangle$) and $\tilde{\boldsymbol{P}} = \Psi(\boldsymbol{P}) \in E(\mathbb{Z}/p^2\mathbb{Z})$.

Given $\boldsymbol{P}$ and $\boldsymbol{Q} := [a]\boldsymbol{P} \xleftarrow{R} \mathbb{G}$, the *elliptic curve consistent lifting (ECCL) problem* is to compute $\boldsymbol{Q'} := [a]\tilde{\boldsymbol{P}}$. It is easily seen that this problem is equivalent to the discrete logarithm problem in $\mathbb{G}$. Indeed, given access to an ECCL solver, on input $\boldsymbol{Q}$, we receive $\boldsymbol{Q'}$ and then can obtain $\bar{a} := a \bmod p$ as $\bar{a} = \frac{[\![\boldsymbol{Q'}]\!]}{[\![\tilde{\boldsymbol{P}}]\!]} \bmod p$. From Hasse's theorem, we know that $a = \bar{a}$ or $a = \bar{a}+p$; this can be easily decided by checking if $\boldsymbol{Q} = [\bar{a}]\boldsymbol{P}$ or $\boldsymbol{Q} = [\bar{a}+p]\boldsymbol{P}$. The other direction is straightforward. Given access to an ECDL solver, on input $\boldsymbol{Q}$, we obtain a and then can compute $\boldsymbol{Q'} = [a]\tilde{\boldsymbol{P}}$ where $\tilde{\boldsymbol{P}} = \Psi(\boldsymbol{P})$.

References

1. Belding, J.V.: A Weil pairing on the p-torsion of ordinary elliptic curves over $K[\epsilon]$. J. Number Theory **128**(6), 1874–1888 (2008)
2. Bernstein, D.J., Hamburg, M., Krasnova, A., Lange, T.: Elligator: elliptic-curve points indistinguishable from uniform random strings. In: ACM-CCS 2013, pp. 425–438. ACM Press (2013)
3. Boneh, D.: The decision Diffie-Hellman problem. In: Buhler, J.P. (ed.) ANTS 1998. LNCS, vol. 1423, pp. 48–63. Springer, Heidelberg (1998). doi:10.1007/BFb0054851
4. Boneh, D., Joux, A., Nguyen, P.Q.: Why textbook ElGamal and RSA encryption are insecure. In: Okamoto, T. (ed.) ASIACRYPT 2000. LNCS, vol. 1976, pp. 30–43. Springer, Heidelberg (2000). doi:10.1007/3-540-44448-3_3
5. Boyen, X., Mei, Q., Waters, B.: Direct chosen ciphertext security from identity based techniques. In: ACM-CCS 2005, pp. 320–329. ACM Press (2005)
6. Canetti, R., Halevi, S., Katz, J.: Chosen-ciphertext security from identity-based encryption. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 207–222. Springer, Heidelberg (2004). doi:10.1007/978-3-540-24676-3_13

7. Cash, D., Kiltz, E., Shoup, V.: The twin Diffie-Hellman problem and applications. In: Smart, N. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 127–145. Springer, Heidelberg (2008). doi:10.1007/978-3-540-78967-3_8
8. Catalano, D., Nguyen, P.Q., Stern, J.: The hardness of hensel lifting: the case of RSA and discrete logarithm. In: Zheng, Y. (ed.) ASIACRYPT 2002. LNCS, vol. 2501, pp. 299–310. Springer, Heidelberg (2002). doi:10.1007/3-540-36178-2_19
9. Chevallier-Mames, B., Paillier, P., Pointcheval, D.: Encoding-free ElGamal encryption without random oracles. In: Yung, M., Dodis, Y., Kiayias, A., Malkin, T. (eds.) PKC 2006. LNCS, vol. 3958, pp. 91–104. Springer, Heidelberg (2006). doi:10.1007/11745853_7
10. Cramer, R., Gennaro, R., Schoenmakers, B.: A secure and optimally efficient multi-authority election scheme. In: Fumy, W. (ed.) EUROCRYPT 1997. LNCS, vol. 1233, pp. 103–118. Springer, Heidelberg (1997). doi:10.1007/3-540-69053-0_9
11. Cramer, R., Shoup, V.: A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In: Krawczyk, H. (ed.) CRYPTO 1998. LNCS, vol. 1462, pp. 13–25. Springer, Heidelberg (1998). doi:10.1007/BFb0055717
12. ElGamal, T.: A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. Inf. Theory **31**(4), 469–472 (1985)
13. Even, S., Goldreich, O., Micali, S.: On-line/off-line digital schemes. J. Cryptol. **9**(1), 35–67 (1996)
14. Farashahi, R.R.: Hashing into Hessian curves. In: Nitaj, A., Pointcheval, D. (eds.) AFRICACRYPT 2011. LNCS, vol. 6737, pp. 278–289. Springer, Heidelberg (2011). doi:10.1007/978-3-642-21969-6_17
15. Fouque, P.-A., Joux, A., Tibouchi, M.: Injective encodings to elliptic curves. In: Boyd, C., Simpson, L. (eds.) ACISP 2013. LNCS, vol. 7959, pp. 203–218. Springer, Heidelberg (2013). doi:10.1007/978-3-642-39059-3_14
16. Galbraith, S.D.: Elliptic curve Paillier schemes. J. Cryptol. **15**(2), 129–138 (2002)
17. Gennaro, R., Krawczyk, H., Rabin, T.: Secure hashed Diffie-Hellman over non-DDH groups. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 361–381. Springer, Heidelberg (2004). doi:10.1007/978-3-540-24676-3_22
18. Gennaro, R., Shoup, V.: A note on an encryption scheme of Kurosawa and Desmedt. Cryptology ePrint Archive, Report 2004/194 (2004)
19. Goldwasser, S., Micali, S.: Probabilistic encryption. J. Comput. Syst. Sci. **28**(2), 270–299 (1984)
20. Håstad, J., Impagliazzo, R., Levin, L.A., Luby, M.: A pseudorandom generator from any one-way function. SIAM J. Comput. **28**(4), 1364–1396 (1999)
21. Impagliazzo, R., Levin, L.A., Luby, M.: A pseudorandom generator from any one-way function. In STOC 1989, pp. 12–24. ACM Press (1989)
22. Koblitz, N.: Elliptic curve cryptosystems. Math. Comput. **48**, 203–209 (1987)
23. Krawczyk, H., Rabin, T.: Chameleon signatures. In: NDSS 2000. The Internet Society (2000)
24. Miller, V.S.: Use of elliptic curves in cryptography. In: Williams, H.C. (ed.) CRYPTO 1985. LNCS, vol. 218, pp. 417–426. Springer, Heidelberg (1986). doi:10.1007/3-540-39799-X_31
25. Pohlig, S.C., Hellman, M.E.: An improved algorithm for computing logarithms over GF(p) and its cryptographic significance. IEEE Trans. Inf. Theory **24**(1), 106–110 (1978)
26. Pollard, J.M.: Monte Carlo methods for index computation mod p. Math. Comput. **32**, 918–924 (1978)

27. Shoup, V., Sequences of games: a tool for taming complexity in security proofs. Cryptology ePrint Archive Report, 2004/332 (2004)
28. Silverman, J.H.: The Theory of Elliptic Curves, GTM 106. Springer-Verlag, Heidelberg (1986)
29. Tsiounis, Y., Yung, M.: On the security of ElGamal based encryption. In: Imai, H., Zheng, Y. (eds.) PKC 1998. LNCS, vol. 1431, pp. 117–134. Springer, Heidelberg (1998). doi:10.1007/BFb0054019
30. Virat, M.: A cryptosystem "à la" ElGamal on an elliptic curve over $\mathbb{F}_p[\varepsilon]$. In: WEWoRC 2005, LNI 74, pp. 32–44. Gesellschaft für Informatik e.V (2005)
31. Virat, M.: Courbes elliptiques sur un anneau et applications cryptographiques. Ph.D. thesis, Université de Nice-Sophia Antipolis (2009)
32. Zhang, R.: Tweaking TBE/IBE to PKE transforms with chameleon hash functions. In: Katz, J., Yung, M. (eds.) ACNS 2007. LNCS, vol. 4521, pp. 323–339. Springer, Heidelberg (2007). doi:10.1007/978-3-540-72738-5_21

http://www.springer.com/978-3-319-52152-7

Topics in Cryptology – CT-RSA 2017
The Cryptographers' Track at the RSA Conference 2017, San Francisco, CA, USA, February 14–17, 2017, Proceedings
Handschuh, H. (Ed.)
2017, XIII, 452 p. 78 illus., Softcover
ISBN: 978-3-319-52152-7