A Practical Public Key Cryptosystem from Paillier and Rabin Schemes

David Galindo, Sebastià Martín, Paz Morillo and Jorge L. Villar

Dep. Matemàtica Aplicada IV. Universitat Politècnica de Catalunya
Campus Nord, c/Jordi Girona, 1-3, 08034 Barcelona
e-mail: {dgalindo,sebasm,paz,jvillar}@mat.upc.es

Abstract. We propose a practical scheme based on factoring and semantically secure (IND-CPA) in the standard model. The scheme is obtained from a modification of the so called RSA-Paillier [5] scheme. This modification is reminiscent of the ones applied by Rabin [22] and Williams [25] to the well-known RSA cryptosystem. Thanks to the special properties of such schemes, we obtain efficiency similar to that of RSA cryptosystem, provably secure encryption (since recovering plaintext from ciphertext is as hard as factoring) and indistinguishability against plaintext attacks. We also construct a new trapdoor permutation based on factoring, which has interest on its own. Semantic security of the scheme is based on an appropiate decisional assumption, named as Decisional Small 2e-Residues assumption. The robustness of this assumption is also discussed. Compared to Okamoto-Uchiyama's scheme [18], the previous IND-CPA cryptosystem in the standard model with one-wayness based on factoring, our scheme is drastically more efficient in encryption, and presents higher bandwith, achieving the same expansion factor as Paillier or El Gamal schemes. We believe the new scheme could be an interesting starting point to develop efficient IND-CCA schemes in the standard model with one-wayness based on factoring.

Keywords: public-key cryptography, semantic security, factoring, standard model.

1 Introduction

Nowadays, two main hard arithmetic problems are used in public key encryption, namely, the integer factorization problem and the discret logarithm problem. Among all public key schemes, the only ones with existing commercial realizations are RSA or Rabin-Williams schemes, related to the factoring problem, and El Gamal scheme, related to the discret logarithm problem. The hardness of these problems ensures the cryptosystems are *secure*, in the sense of the infeasibility of recovering the whole plaintext from the ciphertext. But the actual underlying goal of any encryption scheme is to guarantee that no partial information about the the plaintext is revealed from the ciphertext in a complexity-theoretic scenario. This notion is usually called *semantic security* or *indistinguishability of encryptions*. Depending on the capabilities allowed to the attacker, one

talks about indistinguishability against chosen plaintext attack (IND-CPA) or indistinguishability against chosen ciphertext attack (IND-CCA). The latter is considered as the right notion of security, although IND-CPA level is still maintained, since homomorphic cryptosystems can't achieve IND-CCA.

Up to now, we can find in the literature several settings for designing practical public-key IND-CCA schemes. The most popular is the so-called Random Oracle Model (ROM) [2], an idealized model of computation in which a cryptographic hash is considered as a *truly random* oracle accessible to both legitimate and illegitimate users. It turns out to be a very powerful primitive, and there exist several generic constructions (see [21] for instance), that provide IND-CCA schemes under standard computational assumptions. Although the ROM is a convenient setting, security proofs in this model are somewhat heuristic, since in real implementations hash functions are not truly random. This problem leads to a related approach, initiated by Canetti [4], with the aim of identifying useful and realizable properties of random oracles. There is a realization in this setting based on the factoring problem [16]. Another approach consists on building encryption schemes by means of integrating several cryptographic primitives, as symmetric cryptosystems, message authenticated codes and cryptographic hash functions. An instance in this model can be found in [1].

A different and appealing approach is used in [8] and [9]. In this setting, the security of the proposed IND-CCA schemes is only based on number-theoretic decisional assumptions. The technique used in [8] and [9] is to improve existing IND-CPA schemes under appropiate and widely accepted decisional assumptions, obtaining IND-CCA schemes based on the same assumptions and without significantly degrading their efficiency. There exist three different realizations in this setting, which are based on the Decisional Diffie-Hellman, Decision Composite Residuosity [19] and the classical Quadratic Residuosity assumptions respectively. It would be of great interest to construct IND-CCA schemes from the RSA and Rabin-Williams primitives in this model. A decisional assumption's candidate for the RSA scheme was proposed in the modification of Paillier scheme [5], although the proof of the equivalence between the one-wayness of this scheme and the RSA scheme has been presented very recently [6]. It is an open problem to study the validity of this new assumption and to develop an IND-CCA scheme from it. As far as we know, no decisional number-theoretic problem for the Rabin-Williams primitive has been proposed.

Our results

In this paper we first construct a new trapdoor permutation based on factoring, which has interest on its own. Trapdoor permutations play an important role in cryptography. Many theoretic schemes use this object as a building block, in such a way that any trapdoor permutation can be easily transformed into IND-CCA ciphering (although very impractical), signature, or authentication schemes for instance. Despite this fact, few candidate trapdoor permutations are known, and

fewer that are as secure as factoring (cf. [20]).
The new trapdoor permutation is obtained from a modification of RSA-Paillier's trapdoor permutation [5], which is reminiscent from the modifications applied by Rabin [22] and Williams [25] to RSA cryptosystem. Then, using this new function as a primitive, we design a new cryptosystem which is one-way under the intractability of factoring $n = pq$, with $p \equiv q \equiv 3 \bmod 4$, and IND-CPA under an appropiate number-theoretic decisional assumption. We summarize hereafter the main features of the proposed scheme:

- We take profit of the nice characteristics of Rabin schemes and overcome their drawbacks, by using the Rabin-Williams function to hide the randomness. More precisely, the encryption of a message $m \in \mathbb{Z}_n$ with randomness $r \in Q_n$ is defined as $E(r, m) = r^{2e} + mn \bmod n^2$, where e is an integer of small size.
- It is remarkable that the scheme allows to encrypt arbitrary messages with a very simple procedure, that does not depend further on the form of the message to be enciphered, which was the case for the previous Rabin based schemes. Besides, the efficiency is similar to that of plain RSA.
- The scheme is IND-CPA under the Decisional Small 2e-Residues assumption (DS2eR). We can also stablish a relation between the decisional assumption in RSA-Paillier scheme, the Quadratic Residuosity and the new DS2eR assumption.

Although the scheme is obtained by a simple modification of the RSA-Paillier scheme, this modification deeply influences the underlying mathematical structure. This was in turn the case of RSA-Paillier scheme respect to original Paillier scheme [19]. The main difference is that one-wayness of the new scheme is equivalent to factoring and independent of the size of the exponent e. Thus, the exponent e only affects the semantic security of the scheme.
We can also compare our scheme with the Okamoto-Uchiyama's scheme (OU) [18]. The one-wayness of OU is equivalent to factoring $n = p^2q$, whereas in our case is equivalent to factoring $n = pq$, which is the classical factoring assumption. Our scheme is drastically more efficient in ciphering, since OU presents an encryption cost proportional to the lenght of the modulus n. Besides, our scheme presents a expansion factor 2, while OU's expansion factor is 3. However, OU scheme is homomorphic and more efficient in decryption than ours.

The main drawback of our scheme is that, as well as in the previous schemes with one-wayness equivalent to factoring, there exist a chosen ciphertext attack that completely breaks the scheme. In the ROM this problem can be solved by directly applying the technique in [21]. It remains an open problem to study the validity of the DS2eR assumption and to modify our scheme to achieve IND-CCA security under the DS2eR assumption in the standard model.

2 Some previous schemes and related trapdoor permutations

In this section, we briefly recall some previous schemes and related trapdoor permutations, from which we will derive the new trapdoor permutation based on factoring, and the scheme we propose. We begin by fixing some notation.

If A is a non-empty set, then $x \leftarrow A$ denotes that x has been uniformly chosen in A, and $\texttt{negl}(\texttt{k})$ stands for a negligible function in a security parameter k. If n is an RSA modulus, i.e. $n = pq$ where p, q are different odd primes, then we denote by $\mathrm{RSA}[n, e]$ the RSA function with exponent e. The conjecture about the infeasibility of inverting the $\mathrm{RSA}[n, e]$ function on a randomly chosen input in $\mathbb{Z}_n^*$ will be referred as the $\mathrm{RSA}[n, e]$ assumption. If N is a positive integer, then Q_N stands for the set of quadratic residues modulo N. If D_1 and D_2 are two probability distributions, then $D_1 \approx D_2$ denotes that the distributions are polinomally indistinguishable [10]. It holds that if $\mathcal{A}$ is a probabilistic polynomial time (PPT) algorithm and $D_1 \approx D_2$, then $\mathcal{A}(D_1) \approx \mathcal{A}(D_2)$. Another useful property is that if g is a bijection such that g and g^{-1} can be computed in PPT, then $D_1 \approx D_2$ is equivalent to $g(D_1) \approx g(D_2)$.

Rabin function.
Let p, q be two different primes with equal length, $n = pq$. Rabin proposed in [22] a provably secure cryptosystem based on the modular squaring function

$$\begin{aligned} \mathbb{Z}_n^* &\longrightarrow Q_n \\ x &\longmapsto x^2 \bmod n\,. \end{aligned}$$

It is well known that modular squaring is a trapdoor one-way function assuming that factorisation of large numbers is infeasible. However, modular squaring is a 4 to 1 function, so a ciphertext is not uniquely decrypted. In order to avoid this drawback and to speed up the decryption algorithm (i.e. the computation of square roots modulo n), the following proposal by Blum and Williams can be considered:

Blum-Williams function.
Let p, q be (different) primes with equal length, $p \equiv q \equiv 3 \bmod 4$, $n = pq$. The squaring function restricted to Q_n, i.e.

$$\begin{aligned} \mathcal{G}_n : Q_n &\longrightarrow Q_n \\ x &\longmapsto x^2 \bmod n \end{aligned}$$

is a trapdoor one-way permutation if factoring large numbers is infeasible (see page 34 in [11]). Then, if we restrict the set of messages to Q_n, a ciphertext will be uniquely decrypted. However, this is not suitable for real applications, since it does not allow to encrypt arbitrary messages. To decrypt $c \in Q_n$ one

has to compute $\mathcal{G}_n^{-1}(c)$, i.e. the element $s \in Q_n$ such that $s^2 = c \bmod n$. Let us briefly recall how to make this computation (see [24] for a nice account on this). Assume that we know the factorisation of $n = pq$, where $p \equiv q \equiv 3 \bmod 4$. We first compute the numbers $f = c^{\frac{p+1}{4}} \bmod p$ and $g = c^{\frac{q+1}{4}} \bmod q$, which are the square roots of c modulo p and modulo q that are quadratic residues to their respective modulus. Then, by using the Chinese Remainder Theorem, we obtain an $s \in Q_n$ such that $s^2 = c \bmod n$.

Rabin-Williams function.
Let p, q be (different) primes with equal length, $p \equiv q \equiv 3 \bmod 4$, $n = pq$ and e a public RSA exponent (i.e. an integer such that $\gcd(e, \lambda(n)) = 1$, where λ denotes Carmichael's function). The map

$$\begin{aligned} \mathcal{W}_e : Q_n &\longrightarrow Q_n \\ x &\longmapsto x^{2e} \bmod n \end{aligned}$$

is also a trapdoor one-way permutation assuming that factoring large numbers is infeasible, since a perfect reduction to the Blum-Williams function inversion problem can be done as follows. Given $c = \mathcal{G}_n(x) = x^2 \bmod n$, x can be retrieved from $c^e \bmod n = x^{2e} \bmod n$ by inverting the Rabin-Williams function with some non-negligible probability.

RSA-Paillier function.
Catalano et al. proposed in [5] a mix of Paillier's scheme [19] with RSA scheme, in order to obtain an IND-CPA cryptosystem in the standard model with efficiency similar to that of RSA cryptosystem. It is based on the permutation

$$\begin{aligned} \mathcal{E}_e : \mathbb{Z}_n^* \times \mathbb{Z}_n &\longrightarrow \mathbb{Z}_{n^2}^* \\ (r, m) &\longmapsto r^e(1 + mn) \bmod n^2, \end{aligned}$$

where p, q are distinct primes with the same length, $n = pq$, and $e \in \mathbb{Z}_n$ is such that $\gcd(e, \lambda(n^2)) = 1$. The encryption scheme $\mathcal{E}_e(r, m)$ with randomness $r \in \mathbb{Z}_n^*$ is semantically secure under the *Decisional Small e-Residues* assumption [5].
Sakurai and Takagi claimed in [23] that deciphering RSA-Paillier scheme with public exponent e is actually equivalent to inverting the original RSA$[n, e]$ function. However, Catalano, Nguyen and Stern found a flaw in the proof by Takagi and Sakurai, and they proposed in [6] an alternative proof of the claim in [23]. Therefore, RSA-Paillier scheme is the first semantically secure RSA-type scheme in the standard model.

3 New trapdoor permutation based on factoring

In this section we present a new length-preserving trapdoor permutation based on factoring, i.e. a length-preserving bijection that is one-way assuming that factoring large integers is hard. It is worthwhile to remark that as well as ours,

all previous trapdoor permutations provably secure [1] are based on the factoring problem [20]. To the best of our knowledge, only two length-preserving provably secure trapdoor permutations exist, namely, the Blum-Williams permutation, and another one proposed by Gong and Harn in [12].

A new trapdoor permutation.
Let p, q be primes, $p \equiv q \equiv 3 \bmod 4$, $n = pq$, e a positive integer such that $\gcd(e, \lambda(n)) = 1$ and

$$\begin{aligned} \mathcal{F}_e : Q_n \times \mathbb{Z}_n &\longrightarrow Q_{n^2} \\ (r, m) &\longmapsto r^{2e} + mn \bmod n^2. \end{aligned}$$

Proposition 1. *$\mathcal{F}_e$ is a well-defined length-preserving bijection.*

Proof: From the Hensel-lifting, the set of quadratic residues modulo n^2 can be alternatively defined as $Q_{n^2} = \{x + yn \mid x \in Q_n \, , y \in \mathbb{Z}_n\}$. Then if $c = \mathcal{F}_e(r, m) = r^{2e} + mn \bmod n^2$, with $r \in Q_n$, $m \in \mathbb{Z}_n$, it is obvious that $c \bmod n = r^{2e} \bmod n \in Q_n$, which implies that $\mathcal{F}_e$ is well-defined.

To prove that $\mathcal{F}_e$ is bijective it suffices to show that it is injective, because, from the alternative definition of Q_{n^2}, we deduce that the sets $Q_n \times \mathbb{Z}_n$ and Q_{n^2} have the same number of elements. Let us suppose that $\mathcal{F}_e(r_0, m_0) = \mathcal{F}_e(r_1, m_1)$. Then $r_0^{2e} = r_1^{2e} \bmod n$, and since squaring and computing e-th powers modulo n, with $\gcd(e, \lambda(n)) = 1$, are bijections over Q_n, we conclude that $r_0 = r_1 \bmod n$. This implies $m_0 n = m_1 n \bmod n^2$, so $m_0 = m_1 \bmod n$.

Finally, $\mathcal{F}_e$ is length-preserving, since the natural bit representation of an arbitrary element either in $Q_n \times \mathbb{Z}_n$ or in Q_{n^2} has length $2\lceil \log_2 n \rceil$. □

In the sequel we prove that inverting $\mathcal{F}_e$ is as difficult as factoring the modulus n. We denote by $\mathcal{PRIMES}(k)$ the set of primes of length k which are congruent with 3 modulo 4.

Assumption 1 (Factoring assumption) *For every probabilistic polynomial time algorithm $\mathcal{A}$, there exists a negligible function* `negl()` *such that*

$$Pr\begin{bmatrix} p, q \leftarrow \mathcal{PRIMES}(k/2),\ n = pq, \\ \mathcal{A}(1^k, n) = (p, q) \end{bmatrix} = \mathtt{negl}(k)\,.$$

Notice that the set $\mathcal{PRIMES}(k/2)$ is a subset of the set of all primes with length $k/2$. However, there is no evidence suggesting that the factoring problem is *easier* in $\mathcal{PRIMES}(k)$ than in the whole set.

[1] We say a cryptographic scheme is provably secure if it is proven to be as secure as the underlying primitive problems (i.e., discrete logarithm or factoring problems).

Assumption 2 *$\mathcal{G}_n$ is one-way, that is, for every probabilistic polynomial time algorithm $\mathcal{A}$, there exists a negligible function* `negl()` *such that*

$$Pr\begin{bmatrix} p,q \leftarrow \mathcal{PRIMES}(k/2),\ n=pq, \\ r \leftarrow Q_n,\ c = r^2 \bmod n, \\ \mathcal{A}(1^k, n, c) = r \end{bmatrix} = \mathtt{negl}(k)\,.$$

Proposition 3 *$\mathcal{G}_n$ is one-way if and only if the Factoring Assumption holds.*
Proof: (see any basic book on cryptography, for instance [24]).

Assumption 4 *$\mathcal{F}_e$ is one-way, that is, for every probabilistic polynomial time algorithm $\mathcal{A}$, there exists a negligible function* `negl()` *such that*

$$Pr\begin{bmatrix} p,q \leftarrow \mathcal{PRIMES}(k/2),\ n=pq, \\ r \leftarrow Q_n,\ m \leftarrow \mathbb{Z}_n,\ c = \mathcal{F}_e(r,m), \\ \mathcal{A}(1^k, n, e, c) = (r,m) \end{bmatrix} = \mathtt{negl}(k)\,.$$

Proposition 5 *For all e such that $\gcd(e, \lambda(n)) = 1$, $\mathcal{F}_e$ is a trapdoor permutation if and only if the Factoring Assumption holds.*

Proof:

($\Rightarrow$) Let us suppose the Factoring Assumption does not hold. Then there exists a polynomial time algorithm that factors $n = pq$ with a non-negligible probability ε. Knowing p and q, one can compute $d \in \mathbb{Z}_n^*$ s.t. $de \equiv 1 \bmod \lambda(n)$, since $\gcd(e, \lambda(n)) = 1$. For any $c \in Q_{n^2}$ we can also compute $r = \mathcal{G}_n^{-1}(c^d \bmod n) = \mathcal{G}_n^{-1}(r^2 \bmod n)$, and $m \in \mathbb{Z}_n$ from the equality $mn = c - r^{2e} \bmod n^2$. These values are such that $\mathcal{F}_e(r,m) = c$, so we can invert $\mathcal{F}_e$ on $c \leftarrow Q_{n^2}$ with non-negligible success probability ε, which implies that $\mathcal{F}_e$ is not one-way.

($\Leftarrow$) Let us suppose that $\mathcal{F}_e$ is not one-way for a certain e such that $\gcd(e, \lambda(n)) = 1$. The goal is to show that a probabilistic polynomial time algorithm that inverts $\mathcal{F}_e$ on a random input can be transformed into another algorithm that inverts Blum-Williams permutation $\mathcal{G}_n$. Assume then we are given a security parameter k, an integer n and $c \in Q_n$ with the distributions described in assumption 2. Let $c' = c^e + mn \bmod n^2$, where $m \leftarrow \mathbb{Z}_n$. Then, since c was uniformly chosen in Q_n and the map

$$\begin{aligned} Q_n \times \mathbb{Z}_n &\longrightarrow Q_{n^2} \\ (c,m) &\longmapsto c^e + mn \bmod n^2 \end{aligned}$$

is a bijection, we deduce that c' is uniformly distributed in Q_{n^2}. Let $(r, m') = \mathcal{A}(n, c')$, where $\mathcal{A}$ is the algorithm that inverts $\mathcal{F}_e$ on a random input with a non-negligible probability ε. If $\mathcal{A}$ gives the correct answer, then $c^e + mn = r^{2e} + m'n \bmod n^2$. Reducing this equality modulo n, we have $r^{2e} = c^e \bmod n$, which is equivalent to $c = r^2 \bmod n$, since $\gcd(e, \lambda(n)) = 1$. Then $\mathcal{G}_n^{-1}(c) = r$ with probability ε. □

4 The new scheme

Using the permutation $\mathcal{F}_e$ as a primitive, we are able to develop the following encryption scheme:

Key generation. Given a security parameter ℓ, choose at random two primes p and q with $\ell/2$ bits such that $p \equiv q \equiv 3 \bmod 4$, and choose an integer $e > 2$ s.t. $\gcd(e, \lambda(n^2)) = 1$. Then the public key is PK=(n, e), where $n = pq$, and the secret key is SK=(p, q, d), where $d = e^{-1} \bmod \lambda(n)$.
Let us observe that in the definition of $\mathcal{F}_e$ in the previous section, the integer e must only satisfy the condition $\gcd(e, \lambda(n)) = 1$. Now we demand, in addition, that $e > 2$ and, since $\lambda(n^2) = n\lambda(n)$, that $\gcd(e, n) = 1$. The reason for this choice will become clearer when we study both one-wayness and semantic security of the scheme.

Encryption. To encrypt a message $m \in \mathbb{Z}_n$ we compute $c = \mathcal{F}_e(r, m)$, where r is randomly chosen in Q_n. The choice of the randomness in Q_n can be done, for instance, by selecting $s \leftarrow \mathbb{Z}_n^*$ at random, and computing $r = s^2 \bmod n$.

Decryption. To recover the message m from $c = \mathcal{F}_e(r, m)$, the randomness r is computed firstly, and, afterwards, m is easily obtained from

$$mn = c - r^{2e} \bmod n^2 \,.$$

To obtain r from c, we compute $t = RSA[n, e]^{-1}(c \bmod n) = c^d \bmod n$, and then $r = \mathcal{G}_n^{-1}(t)$, computed as explained in section 2.

5 Security analysis

In this section we discuss the security properties of the encryption scheme, namely, its one-wayness and semantic security against passive adversaries. We show the scheme is one-way under the Factoring Assumption and semantically secure under an appropiate number-theoretic decisional assumption.

5.1 One-wayness

In order to study the one-wayness of the scheme, we introduce a new computational problem which is closely related. Afterwards, we prove that the new computational problem is intractable if and only if the factoring problem is intractable. In fact, the new problem is the natural extension to our case of the questions dealed with in [23] and [6].

In [6], given an RSA modulus n and a public exponent e relatively prime to $\lambda(n)$, the following function from $\mathbb{Z}_n^*$ to $\mathbb{Z}_{n^l}^*$, for $l > 1$, is defined:

$$\textbf{Hensel-RSA}[n, e, l](r^e \bmod n) = r^e \bmod n^l \,,$$

and it is proven that the hardness of computing such a function is equivalent to the RSA $[n, e]$ assumption. With some slight modifications, the arguments in [6] can be applied to our encryption scheme. Let us consider the **Hensel-Rabin-Williams** function from Q_n to Q_{n^l} defined as

$$\textbf{Hensel-RW}[n, e, l](r^{2e} \bmod n) = r^{2e} \bmod n^l \,,$$

where $r \in Q_n$. The following proposition can then be stated

Proposition 6 *Given p, q (different) primes with equal length, $p \equiv q \equiv 3 \bmod 4$, $n = pq$ and e a public RSA exponent relatively prime to n, computing* **Hensel-RW**$[n, e, 2]$ *on a random element $w \in Q_n$ is hard if and only if the function $\mathcal{W}_e$ is one-way.*

Proof:
($\Rightarrow$) If $\mathcal{W}_e$ is not one-way, then r can be computed from $r^{2e} \bmod n$ with non-negligible probability and therefore **Hensel-RW**$[n, e, 2](r^{2e})$ is trivially computed.

($\Leftarrow$) The adversary, who wants to invert the Rabin-Williams function on a random input $r^{2e} \bmod n$, calls an oracle twice for the **Hensel-RW**$[n, e, 2]$ on inputs r^{2e} and $r^{2e}a^{2e}$, where a is randomly chosen in Q_n. Assuming that ε is the probability that the oracle gives the right answer, the adversary knows $r^{2e} \bmod n^2$ and $\mu^{2e} \bmod n^2$, where $\mu = ar \bmod n$, with probability ε^2. Then, it follows that there exists $z \in \mathbb{Z}_n$ such that

$$ar = \mu(1 + zn) \bmod n^2. \tag{1}$$

Raising this equality to the power $2e$ we obtain the equation $a^{2e}r^{2e} = \mu^{2e}(1 + 2ezn) \bmod n^2$, from which z can be computed, since the rest of values involved are known. The last step is the computation of r and μ from equation (1). This can be done by using lattice reduction techniques (see [6] for further details). □

The following lemma states the relation between computing **Hensel-RW**$[n, e, 2]$ function and the one-wayness of our scheme.

Lemma 7 *The encryption scheme described in section 4 is one-way if and only if computing* **Hensel-RW**$[n, e, 2]$ *on a random input is hard.*

Proof:

($\Rightarrow$) For a random ciphertext $c \leftarrow Q_{n^2}$, the message m is easily recovered from the **Hensel-Rabin-Williams** oracle since $mn = c-$**Hensel-RW**$[n, e, 2](c \bmod n)$.

($\Leftarrow$) To compute **Hensel-RW**$[n, e, 2]$ on $c_0 \leftarrow Q_n$, it suffices to choose $m_0 \leftarrow \mathbb{Z}_n$, and submit $c_0 + m_0 n$ to the adversary that is able to invert the proposed cryptosystem with a non-negligible probability ε. (Note that m_0 is intended to match the exact probability distribution needed for the query to the adversary.) Since

there exist uniques $r \in Q_n$ and $m \in \mathbb{Z}_n$ such that $c_0 + m_0 n = r^{2e} + mn \bmod n^2$, the adversary answers m with probability ε. Then, **Hensel-RW**$[n, e, 2](c_0) = c_0 + (m_0 - m)n \bmod n^2$. □

The above arguments lead to the following theorem.

Theorem 8 *The encryption scheme described in section 4 is one-way if and only if the Factoring Assumption holds.*

Proof: From Lemma 7 and Proposition 6, one-wayness of our scheme is equivalent to one-wayness of the Rabin-Williams function, that is in turn equivalent to the Factoring Assumption. □

At this point, we have to notice that, as the previous schemes with one-wayness based on factoring, there exists a chosen ciphertext attack that completely breaks our cryptosystem. This problem can be avoided by directly applying the construction in the random oracle model introduced by Pointcheval in [21]. Since this construction provides an IND-CCA scheme from any partial one-way function, assuming only the random oracles and the assumption under which the function is one-way, we can build the new scheme from the primitive

$$\begin{aligned} Q_n \times \mathbb{Z}_n &\longrightarrow Q_{n^2} \\ (r, m) &\longmapsto r^2 + mn \bmod n^2 \,, \end{aligned}$$

that is, taking $e = 1$. Thereby we obtain an IND-CCA scheme in the ROM based on factoring and highly efficient. This new scheme presents a *tight reduction* to the factoring problem, and it has a simpler description than some of the previous similar constructions [15, 3, 17].

5.2 Semantic security

Now we describe the number-theoretic decisional assumption on which the semantic security of the scheme is based:

Decisional Small $2e$-Residues assumption (DS2eR).
Let p, q be randomly chosen ℓ-bit long primes, with $p, q \equiv 3 \bmod 4$, $n = pq$, and let e be an integer such that $\gcd(e, pq(p-1)(q-1)) = 1$. *The following probability distributions are polinomially indistinguishable in the security parameter ℓ:*

$$\begin{aligned} D_{\text{2e-multiple}} &= (n,\ r^{2e} \bmod n^2) \text{ where } r \leftarrow Q_n, \text{ and} \\ D_{\text{random}} &= (n, c) \text{ where } c \leftarrow Q_{n^2}. \end{aligned}$$

Proposition 9 *The encryption scheme described in section 4 is semantically secure if and only if DS2eR assumption holds.*

Proof: Semantic security is equivalent to indistinguishability of encryptions, that is, for all $m_0 \in \mathbb{Z}_n$, the distributions

$$D_0 = (n,\ r^{2e} + m_0 n \mod n^2) \text{ where } r \leftarrow Q_n \quad \text{and}$$
$$D = (n,\ r^{2e} + mn \mod n^2) \text{ where } r \leftarrow Q_n,\ m \leftarrow \mathbb{Z}_n$$

are polynomially indistinguishable. It is easy to see that the map

$$\begin{aligned} Q_{n^2} &\longrightarrow Q_{n^2} \\ c &\longmapsto c - m_0 n \bmod n^2 \end{aligned}$$

is a polynomial time bijection. Then, $D_0 \approx D$ is equivalent to

$$(n, r^{2e} \bmod n^2) \approx (n, r^{2e} + m'n \mod n^2) \text{ where } r \leftarrow Q_n, m' \leftarrow \mathbb{Z}_n.$$

Note that the distribution on the left side is $D_{\text{2e-multiple}}$.
Besides, since $r^{2e} + m'n \mod n^2 = \mathcal{F}_e(r, m')$, and $\mathcal{F}_e$ is a bijection, then D and D_{random} are identically distributed. □

Once we have proved the equivalence between the semantic security of the scheme and DS2eR assumption, the question that immediately arises is the confidence we should have on this assumption. The decisional assumption in the RSA-Paillier scheme [5], named as DSeR assumption, is very similar to ours. In their case it is conjectured that it is infeasible to distinguish between a random element in $\mathbb{Z}^*_{n^2}$ and an element of the form $r^e \bmod n^2$, where $r \leftarrow \mathbb{Z}^*_n$, when the factorisation of n is unknown. As it is argued in [5], the better way we know to attack DS2eR assumption is to solve its computational version, that is, we answer the DS2eR problem by finding a solution of the equation $x^{2e} = c \bmod n^2$, with $c \in Q_{n^2}$. So we are adressed with the problem of finding small solutions of low degree polynomials. The best known way to do it is to apply the following result due to Coppersmith [7]:

Theorem 10 *Let N be an integer and let $f(x) \in \mathbb{Z}_N[x]$ be a monic polynomial of degree d. Then there is an efficient algorithm to find all $x_0 \in \mathbb{Z}$ such that $f(x_0) = 0 \bmod N$ and $|x_0| < N^{1/d}$.*

In our case, given the equation $c = x^{2e} \bmod n^2$, we must find a root $x < n$. Coppersmith's result ensures this is efficiently computable (i.e. in polynomial time) for all $|x| < n^{2/2e} = n^{1/e}$. For all values x greater than this bound, at present there is no polynomial algorithm that solves this problem when the factorization of n is unknown. Then for any $e > 2$ the assumption seems to be valid with hardness depending on the size of exponent e.

Regarding decisional assumptions DSeR and DS2eR, we can establish the following interesting link.

Proposition 11 *If both Quadratic Residuosity [13] and DSeR assumptions hold, then the DS2eR assumption also holds.*

Sketch of the proof: If the Quadratic Residuosity assumption holds, then the probability distributions D_1 and D_2 obtained from $(r^e \bmod n^2,\ r \leftarrow Q_n)$ and $(r^e \bmod n^2,\ r \leftarrow \mathbb{Z}_n)$ are indistinguishable. Moreover, DSeR assumption implies that these distributions are indistinguishable from the distribution D_3 obtained from $(c \leftarrow \mathbb{Z}_{n^2})$. Finally, squaring D_1 and D_3 we conclude that $(r^{2e} \bmod n^2,\ r \leftarrow Q_n)$ is indistinguishable from $(c^2 \bmod n^2,\ c \leftarrow \mathbb{Z}_{n^2})$, that is uniformly distributed over Q_{n^2}. □

Nevertheless, nowadays we have very little knowledge about the validity of this family of decisional assumptions, and more research is needed to evaluate their difficulty. We think this could enlighten on the design of IND-CCA encryption schemes in the standard model which one-wayness is based on the RSA or factoring problems.

Acknowledgements

We would like to thank Dario Catalano for sending us an early version of his paper [6] and the anonymous referees for their useful comments.

References

1. M. Abdalla, M. Bellare and P. Rogaway. DHAES: An Encryption Scheme Based on the Diffie-Hellman Problem. *Submission to IEEE P1363a.* (1998)
2. M. Bellare and P. Rogaway. Random Oracles are Practical: a Paradigm for Designing Efficient Protocols. *ACM CCS 93, ACM Press* (1993)
3. D. Boneh. Simplified OAEP for the RSA and Rabin Functions. *CRYPTO' 01, LNCS* **2139** 275–291 (2001).
4. R. Canetti. Towards realizing random oracles: Hash functions that hide all partial information. *CRYPTO' 97, LNCS* **1294** 455–469 (1997).
5. D. Catalano, R. Gennaro, N. Howgrave-Graham and P. Q. Nguyen. Paillier's Cryptosystem Revisited. *ACM CCS '2001 ACM Press* (2001).
6. D.Catalano, P.Q. Nguyen and J. Stern. The Hardness of Hensel Lifting: The Case of RSA and Discrete Logarithm. *To appear at Proceedings of ASIACRYPT'2002. LNCS* **2501** (2002).
7. D. Coppersmith. Finding a small root of a univariate modular equation. *EUROCRYPT '96, LNCS* **1070** 155–165 (1996).
8. R. Cramer and V. Shoup. A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Ciphertext Attack. *CRYPTO' 98, LNCS* **1462** 13–25 (1998).
9. R. Cramer and V. Shoup. Universal Hash Proofs and a Paradigm for Adaptive Chosen Ciphertext Secure Public-Key Encryption. *EUROCRYPT '2002, LNCS* **2332** 45–64 (2002).
10. O. Goldreich. Foundation of Cryptography - Basic Tools. *Cambridge University Press* (2001).
11. S. Goldwasser and M. Bellare. Lecture Notes on Cryptography. `http://www-cse.ucsd.edu/users/mihir`
12. G. Gong and L. Harn. Public-key cryptosystems based on cubic finite field extensions. *IEEE Transactions on Information Theory* **45** (7) 2601–2605 (1999)

13. S. Golwasser and S. Micali. Probabilistic encryption. *Journal of Computer and System Sciences* **28** 270–299 (1984).
14. M. Joye and J. J. Quisquater. Cryptanalysis of RSA-type cryptosystems: a visit. *Network Threats, DIMACS Series in Discr. Math. ant Th. Comp. Sci., AMS* 21–31 (1998).
15. K. Kurosawa, W. Ogata, T. Matsuo and S. Makishima. IND-CCA Public Key Schemes Equivalent to Factoring $n = pq$. *PKC' 01, LNCS* **1992** 36–47 (2001).
16. S. Müeller. On the Security of a Williams Based Public Key Encryption Scheme. *PKC' 01, LNCS* **1992** 1–18 (2001)
17. M. Nishioka, H. Satoh and K. Sakurai. Public Key Cryptosystems Based on a Modular Squaring. *ICISC'2001, LNCS* **2288** 81–102 (2001)
18. T. Okamoto and S. Uchiyama. A New Public-Key Cryptosystem as Secure as Factoring. *EUROCRYPT-98, LNCS* **1403** 308–318 (1998)
19. P. Paillier. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. *EUROCRYPT '99, LNCS* **1592** 223–238 (1999).
20. J. Patarin and L. Goubin. Trapdoor One-Way Permutations and Multivariate Polynomials. Extended version of the paper published at *ICICS' 97, LNCS* **1334** 356–368.
21. D. Pointcheval. Chosen-Ciphertext Security for any One-Way Cryptosystem. *Proc. PKC '2000 LNCS* **1751** 129–146 (2000).
22. M. O. Rabin. Digitalized signatures and public key functions as intractable as factorisation. MIT/LCS/TR-212 *MIT Laboratory for Computer Science* (1979)
23. K. Sakurai and T. Takagi. New Semantically Secure Public-Key Cryptosystems from the RSA-Primitive. *PKC 2002, LNCS* **2274** (2002).
24. H.C.A. van Tilborg. A Professional Reference and Interactive Tutorial. *Kluwer Academic Publishers SECS* **528** (1999).
25. Williams H.C. A modification of the RSA Public-Key Encryption Procedure. *IEEE Trans. Inf. Theory* Vol. IT-26, No.6, 726–729 (1980).