参考知乎上的文章"Paillier加密算法的推导"

https://zhuanlan.zhihu.com/p/106340045?utm_source=wechat_session&utm_medium=social&utm_oi=662336111775584256

Public-Key Cryptosystems Based on Composite Degree Residuosity Classes

合数阶剩余类

基于n次同余式以及n次剩余的问题这
个难题的求解。模的是一个合数

Pascal Paillier[1,2]

[1] GEMPLUS
Cryptography Department
34 Rue Guynemer, 92447 Issy-Les-Moulineaux
paillier@gemplus.com
[2] ENST
Computer Science Department
46, rue Barrault, 75634 Paris Cedex 13
paillier@inf.enst.fr

Abstract. This paper investigates a novel computational problem, namely the Composite Residuosity Class Problem, and its applications to public-key cryptography. We propose a new trapdoor mechanism and derive from this technique three encryption schemes : a trapdoor permutation and two homomorphic probabilistic encryption schemes computationally comparable to RSA. Our cryptosystems, based on usual modular arithmetics, are provably secure under appropriate assumptions in the standard model.

1 Background

Since the discovery of public-key cryptography by Diffie and Hellman [5], very few convincingly secure asymetric schemes have been discovered despite considerable research efforts.

We refer the reader to [26] for a thorough survey of existing public-key cryptosystems. Basically, two major species of trapdoor techniques are in use today. The first points to RSA [25] and related variants such as Rabin-Williams [24,30], LUC, Dickson's scheme or elliptic curve versions of RSA like KMOV [10]. The technique conjugates the polynomial-time extraction of roots of polynomials over a finite field with the ~~intractability of factoring large numbers~~. It is worthwhile pointing out that among cryptosystems belonging to this family, only Rabin-Williams has been proven equivalent to the factoring problem so far.

Another famous technique, related to Diffie-Hellman-type schemes (El Gamal [7], DSA, McCurley [14], etc.) combines the homomorphic properties of the modular exponentiation and the ~~intractability of extracting discrete logarithms over finite groups~~. Again, equivalence with the primitive computational problem remains open in general, unless particular circumstances are reached as described in [12].

Other proposed mechanisms generally ~~suffer from inefficiency~~, inherent security weaknesses or insufficient public scrutiny : McEliece's cryptosystem [15]

J. Stern (Ed.): EUROCRYPT'99, LNCS 1592, pp. 223–238, 1999.

based on error correcting codes, Ajtai-Dwork's scheme based on lattice problems (cryptanalyzed by Nguyen and Stern in [18]), additive and multiplicative knapsack-type systems including Merkle-Hellman [13], Chor-Rivest (broken by Vaudenay in [29]) and Naccache-Stern [17] ; finally, Matsumoto-Imai and Goubin-Patarin cryptosystems, based on multivariate polynomials, were successively cryptanalyzed in [11] and [21].

We believe, however, that the cryptographic research had unnoticeably witnessed the progressive emergence of a third class of trapdoor techniques : firstly identified as ~~*trapdoors in the discrete log*~~, they actually arise from the common algebraic setting of high degree residuosity classes. After Goldwasser-Micali's scheme [9] based on quadratic residuosity, Benaloh's homomorphic encryption function, originally designed for electronic voting and relying on prime residuosity, prefigured the first attempt to exploit the plain resources of this theory. Later, Naccache and Stern [16], and independently Okamoto and Uchiyama [19] significantly extended the encryption rate by investigating two different approaches : residuosity of smooth degree in $\mathbb{Z}^*_{pq}$ and residuosity of prime degree p in $\mathbb{Z}^*_{p^2q}$ respectively. In the meantime, other schemes like Vanstone-Zuccherato [28] on elliptic curves or Park-Won [20] explored the use of high degree residues in other settings.

In this paper, we propose a new trapdoor mechanism belonging to this family. By contrast to prime residuosity, our technique is based on *composite* residuosity classes *i.e.* of degree set to a hard-to-factor number $n = pq$ where p and q are two large prime numbers. Easy to understand, we believe that our trapdoor provides a new cryptographic building-block for conceiving public-key cryptosystems.

基于大素数分解难题的高阶剩余求解难题

In sections 2 and 3, we introduce our number-theoretic framework and investigate in this context a new computational problem (the Composite Residuosity Class Problem), which intractability will be our main assumption. Further, we derive three homomorphic encryption schemes based on this problem, including a new trapdoor permutation. Probabilistic schemes will be proven semantically secure under appropriate intractability assumptions. All our polynomial reductions are simple and stand in the standard model.

Carmichael's function

lambda = lcm(p-1, q-1) = (p-1)*(q-1)/gcd(p-1, q-1)

符号、记法

Notations. We set $n = pq$ where p and q are large primes : as usual, we will denote by $\phi(n)$ Euler's totient function and by $\lambda(n)$ Carmichael's function[1] taken on n, *i.e.* $\phi(n) = (p-1)(q-1)$ and $\lambda(n) = \mathrm{lcm}(p-1, q-1)$ in the present case. Recall that $|\mathbb{Z}^*_{n^2}| = \phi(n^2) = n\phi(n)$ and that for any $w \in \mathbb{Z}^*_{n^2}$,

$$\begin{cases} w^\lambda = 1 \bmod n \\ w^{n\lambda} = 1 \bmod n^2 \end{cases},$$

$\lambda = k\phi(n)$，ω可以看成Z_n^*中的剩余类的子集。根据欧拉定理，$\omega^{\phi(n)} \equiv 1 \, mod \, n$，则$\omega^\lambda \equiv 1 \, mod \, n$，等式 1 得证。
由上ω^λ可表示成 $1 + \mathrm{kn}$，则$\omega^{n\lambda} = (1 + kn)^n$。而$(1 + kn)^n \equiv 1 \, mod \, n^2$。所以$\omega^{n\lambda} \equiv 1 \, mod \, n^2$，等式 2 得证。

2. 对于$\omega \in \mathbb{Z}^*_{n^2}$，$\omega^\lambda = 1 \bmod n$，$\omega^{n\lambda} = 1 \bmod n^2$。因为 $\omega^{n\lambda}$ 可以表示为 $(1+kn)^n$ 的形式，而 $(1+kn)^n = 1 \bmod n^2$ 。（$\mathbb{Z}^*_{n^2}$ 中的某个元素（剩余系）是 $\mathbb{Z}^*_n$ 中的某个元素的子集，比如 $\mathbb{Z}^*_{6^2}$ 包含了 $[1]_{36}, [6+1]_{36}, [6 \times 2 + 1]_{36}, \ldots$ ，都是 $[1]_6$ 的子集。

which are due to Carmichael's theorem. We denote by RSA $[n, e]$ the (conventionally thought intractable) problem of extracting e-th roots modulo n where $n = pq$ is of unknown factorisation. The relation $P_1 \Leftarrow P_2$ (resp. $P_1 \equiv P_2$) will denote that the problem P_1 is polynomially reducible (resp. equivalent) to the problem P_2.

用 $P_1 \Leftarrow P_2$ 表示问题 P_1 与 P_2 是多项式等价的（polynomial reducible），可以理解为：有一台可以不花费时间计算 P_2 的机器（oracle），就可以在多项式时间里计算出 P_1 。

[1] we will adopt λ instead of $\lambda(n)$ for visual comfort.

2 Deciding Composite Residuosity

We begin by briefly introducing composite degree residues as a natural instance of higher degree residues, and give some basic related facts. The originality of our setting resides in using of a square number as modulus. As said before, $n = pq$ is the product of two large primes.

首先将一个平方数作为模数

Definition 1. *A number z is said to be a n-th residue modulo n^2 if there exists a number $y \in \mathbb{Z}_{n^2}^*$ such that*

$$z = y^n \bmod n^2 .$$

z被称为n次剩余

性质:

* $\sqrt[n]{z} < n$。注意到 $x^n = (x+kn)^n \bmod n^2$，因此总是能找到一个小于n 的 x。

* 对于任意两个小于 n 且不相同的 a, b，$a^n \neq b^n \bmod n^2$ 。因为$a, a+n, a+2n\ldots$

已经构成所有的n次方根。

定义：n次剩余：一个整数 z 是 n^2 的一个 n次剩余（n-th residue modulo n^2），如果存在一个整数 $y \in \mathbb{Z}_{n^2}^*$，使得$y^n = z \bmod n^2$。显然这些n次剩余的集合可以形成一个满足乘法的子群，且每个n次剩余有n个n次方根，把最小的记作 $\sqrt[n]{z}$。

每个n次剩余z有n个n次方根的解,其中最小的那个是比n小,是n次根号z

The set of n-th residues is a multiplicative subgroup of $\mathbb{Z}_{n^2}^*$ of order $\phi(n)$. Each n-th residue z has exactly n roots of degree n, among which exactly one is strictly smaller than n (namely $\sqrt[n]{z} \bmod n$). The n-th roots of unity are the numbers of the form $(1+n)^x = 1 + xn \bmod n^2$.

The problem of deciding n-th residuosity, *i.e.* distinguishing n-th residues from non n-th residues will be denoted by CR $[n]$. Observe that like the problems of deciding quadratic or higher degree residuosity, CR $[n]$ is a random-self-reducible problem that is, all of its instances are polynomially equivalent. Each case is thus an average case and the problem is either uniformly intractable or uniformly polynomial. We refer to [1,8] for detailed references on random-self-reducibility and the cryptographic significance of this feature.

intractable的反义词是polynomial,即某个问题要么是多项式时间可解的,要么是棘手的,不可解的。

本文基础是基于求解高次剩余的难题

As for prime residuosity (*cf.* [3,16]), ~~deciding n-th residuosity is believed to be computationally hard.~~ Accordingly, we will assume that :

Conjecture 2. There exists no polynomial time distinguisher for n-th residues modulo n^2, *i.e.* CR $[n]$ is intractable.

自己定义了一个难题

This intractability hypothesis will be refered to as the *Decisional Composite Residuosity Assumption* (DCRA) throughout this paper. Recall that due to the random-self-reducibility, the validity of the DCRA only depends on the choice of n.

判断某个整数 z 是否是 n^2 的n次剩余的问题记作 **CR[n]** 。我们推测 CR[n] 不存在多项式时间解法，且CR[n]关于不同的 z 的难度是一样的（最坏难度等于随机难度，称作random-self-reducible）。（局限的来说，对于n次剩余 z，判断任何一个 z 是 n次剩余 的难度是一样的，因为通过把 z 随机乘以 a^n，其中 $a \in \mathbb{Z}_n^*$，可以把 z 按照均匀分布的概率映射到任意一个n次剩余）。

3 Computing Composite Residuosity Classes

We now proceed to describe the number-theoretic framework underlying the cryptosystems introduced in sections 4, 5 and 6. Let g be some element of $\mathbb{Z}_{n^2}^*$ and denote by $\mathcal{E}_g$ the integer-valued function defined by

定义的epsilon-g这个映射具有一些较好的性质。

结合法是加法+

结合法是乘法X

$$\begin{array}{ccc} \mathbb{Z}_n \times \mathbb{Z}_n^* & \longmapsto & \mathbb{Z}_{n^2}^* \\ (x, y) & \longmapsto & g^x \cdot y^n \bmod n^2 \end{array}$$

Depending on g, $\mathcal{E}_g$ may feature some interesting properties. More specifically,

引理

Lemma 3. *If the order of g is a nonzero multiple of n then $\mathcal{E}_g$ is bijective.*

即对每对x属于Zn,y属于Zn星，epsilon g都能将其映射到唯一的z属于Zn2星与之对应。且群Zn2星的所有n2个元素(0,1,2,...,n2-1)

$\mathcal{E}_g$ 的一些性质:

* 如果 g 的阶数（满足$g^x \bmod n^2 = 1$的最小的正整数x）是 n 的正整数倍（把这些 g 的集合记作$\mathcal{B}$），则 $\mathcal{E}_g$ 是个双射。

证明：若存在 x_1, x_2，$g^{x_1}y_1^n = g^{x_2}y_2^n \bmod n^2$，那么 $g^{x_1-x_2}(\frac{y_1}{y_2})^n = 1 \bmod n^2$

（对于 $a = b \bmod n$，且 a, b 与 n 互质，两边同乘 b^{-1}，可以证明 $ab^{-1} = 1 \bmod n$）

于是 $g^{\lambda(x_1-x_2)}(\frac{y_1}{y_2})^{n\lambda} = 1 \bmod n^2$，由于根据 $\mathbb{Z}_{n^2}^*$ 的性质，$(\frac{y_1}{y_2})^{\lambda n} = 1 \bmod n^2$，因此 $g^{\lambda(x_1-x_2)} = 1 \bmod n^2$。由于 g 的阶数是 n 的正整数倍，λ 与 n 互质，所以

$x_1 = x_2$。这样有 $(\frac{y_1}{y_2})^n = 1 \bmod n^2$，因此 $\frac{y_1}{y_2}$ 的阶数 k 必有 $k|n, k|\lambda$，因此 $k = 1$，即 $y_1 = y_2 \bmod n$。因此可得不同的 (x, y) 映射到的 $\mathcal{E}_g(x, y)$ 的值也是不同的。

而我们显然可以看出，$|\mathbb{Z}_n^*||\mathbb{Z}_n| = |\mathbb{Z}_{n^2}^*|$，即函数的定义域和值域的元素个数相同。可得 $\mathcal{E}_g$ 是双射。

密文空间n乘以fai(n),明文x属于Zn, y属于Zn星(即与n互素的所有数构成的集合)

We denote by $\mathcal{B}_\alpha \subset \mathbb{Z}_{n^2}^*$ the set of elements of order $n\alpha$ and by $\mathcal{B}$ their disjoint union for $\alpha = 1, \cdots, \lambda$.

g属于Zn2星,其阶是n的倍数。B就是所有这样的g组成的集合，有lamb da个这样的g。为了保证epsilon-g是双射，g必须满足这样的性质。

我已证明fai(n2)=n*fai(n)

Proof. Since the two groups $\mathbb{Z}_n \times \mathbb{Z}_n^*$ and $\mathbb{Z}_{n^2}^*$ have the same number of elements $n\phi(n)$, we just have to prove that $\mathcal{E}_g$ is injective. Suppose that $g^{x_1}y_1^n = g^{x_2}y_2^n \bmod n^2$. It comes $g^{x_2-x_1} \cdot (y_2/y_1)^n = 1 \bmod n^2$, which implies $g^{\lambda(x_2-x_1)} = 1 \bmod n^2$. Thus $\lambda(x_2 - x_1)$ is a multiple of g's order, and then a multiple of n. Since $\gcd(\lambda, n) = 1$, $x_2 - x_1$ is necessarily a multiple of n. Consequently, $x_2 - x_1 = 0 \bmod n$ and $(y_2/y_1)^n = 1 \bmod n^2$, which leads to the unique solution $y_2/y_1 = 1$ over $\mathbb{Z}_n^*$. This means that $x_2 = x_1$ and $y_2 = y_1$. Hence, $\mathcal{E}_g$ is bijective. □

为什么是唯一解

Definition 4. *Assume that $g \in \mathcal{B}$. For $w \in \mathbb{Z}_{n^2}^*$, we call n-th residuosity class of w with respect to g the unique integer $x \in \mathbb{Z}_n$ for which there exists $y \in \mathbb{Z}_n^*$ such that*

$$\mathcal{E}_g(x, y) = w \ .$$

[[w]]g的意思是满足条件的x的剩余类

Adopting Benaloh's notations [3], the class of w is denoted $[\![w]\!]_g$. It is worthwhile noticing the following property :

当omiga是n次剩余的时候,[[w]]g=x=0。

Lemma 5. $[\![w]\!]_g = 0$ *if and only if w is a n-th residue modulo n^2. Furthermore,*

$$\forall w_1, w_2 \in \mathbb{Z}_{n^2}^* \quad [\![w_1 w_2]\!]_g = [\![w_1]\!]_g + [\![w_2]\!]_g \mod n$$

that is, the class function $w \mapsto [\![w]\!]_g$ is a homomorphism from $(\mathbb{Z}_{n^2}^*, \times)$ to $(\mathbb{Z}_n, +)$ for any $g \in \mathcal{B}$.

* 当 g 的阶数是 n 的整数倍 $\forall \omega_1, \omega_2 \in \mathbb{Z}_{n^2}^*$，$[[\omega_1\omega_2]]_g = [[\omega_1]]_g + [[\omega_2]]_g$。因为若 $x_1 = [[\omega_1]], x_2 = [[\omega_2]], x_3 = [[\omega_1\omega_2]]$，则有 $\omega_1 = g^{x_1}y_1^n, \omega_2 = g^{x_2}y_2^n, \omega_1\omega_2 = g^{x_3}y_3^n \bmod n^2$。这样可以得到 $x_3 = x_1 + x_2$，$y_3 = y_1 \cdot y_2$。但是这时候可能出现 $x_3 \geq n, y_3 \geq n$ 的情况，

给定w和g属于Zn^2星,且g的阶是n的倍数求[[w]]g的问题，定义为Class[n,g]

The *n-th Residuosity Class Problem* of base g, denoted Class$[n, g]$, is defined as the problem of computing the class function in base g : for a given $w \in \mathbb{Z}_{n^2}^*$, compute $[\![w]\!]_g$ from w. Before investigating further Class$[n, g]$'s complexity, we begin by stating the following useful observations :

因此我们可以把 $g^{x_3}y_3^n$ 写成 $g^{x_3-n}(y_3 g)^n \bmod n^2 = g^{x_3-n}(y_3 g - kn)^n \bmod n^2$。可见 $\omega \longmapsto [[\omega]]_g$ 把群 $(Z_{n^2}^*, \times)$ **同态映射**（homomorphism）到了群 $(\mathbb{Z}_n, +)$。

最坏难度等于随机难度，称作random-self-reducible

Lemma 6. *Class$[n, g]$ is random-self-reducible over $w \in \mathbb{Z}_{n^2}^*$.*

我们可以把 $\mathcal{E}_g$ 视作对 $Z_{n^2}^*$ 里面的元素的一种分解，分解成 g^x 的部分和 y^n 的部分。g^x 部分产生了 n 个与 n^2 互质的数，而 y^n 部分则可以产生 $\phi(n)$ 个与 n^2 互质的数，从这些数里任选不同的两对数分别相乘，得到的数都属于 n^2 的不同的剩余系。

Proof. Indeed, we can easily transform any $w \in \mathbb{Z}_{n^2}^*$ into a random instance $w' \in \mathbb{Z}_{n^2}^*$ with uniform distribution, by posing $w' = w\,g^\alpha\beta^n \bmod n^2$ where α and β are taken uniformly at random over $\mathbb{Z}_n$ (the event $\beta \notin \mathbb{Z}_n^*$ occurs with negligibly small probability). After $[\![w']\!]_g$ has been computed, one has simply to return $[\![w]\!]_g = [\![w']\!]_g - \alpha \bmod n$.

通过随机选取 $\alpha \in \mathbb{Z}_n, \beta \in \mathbb{Z}_n^*$，令 $\omega' = \omega g^\alpha \beta^n \bmod n^2$，可以得到 ω 被按照均匀分布随机转换成了 ω'。并且很显然有 $[[\omega]]_g = [[\omega']]_g - \alpha \bmod n$。即，计算 $[[\omega]]_g$ 和计算一个随机的 $[[\omega']]_g$ 是等价的。

Lemma 7. *Class$[n, g]$ is random-self-reducible over $g \in \mathcal{B}$, i.e.*

$$\forall g_1, g_2 \in \mathcal{B} \quad Class\,[n, g_1] \quad \equiv \quad Class\,[n, g_2] \ .$$

Proof. It can easily be shown that, for any $w \in \mathbb{Z}_{n^2}^*$ and $g_1, g_2 \in \mathcal{B}$, we have

$$[\![w]\!]_{g_1} = [\![w]\!]_{g_2} [\![g_2]\!]_{g_1} \mod n \ , \tag{1}$$

$g_1^{x_1}y_1^n = g_2^{x_2}y_2^n = \omega \bmod n^2, g_2 = g_1^{x_3}y_3^n \bmod n^2$

$\Rightarrow g_1^{x_3x_2}(y_2y_3)^n = \omega \bmod n^2 \Rightarrow x_3x_2 = x_1$

$g_1^{x_1}y_1^n = g_2, g_2^{x_2}y_2^n = g_1 \Rightarrow (g_1^{x_1}y_1^n)^{x_2}y_2^n = g_1 \Rightarrow x_1x_2 = [[g_1]]_{g_1} = 1 \bmod n$

于是有 $[[\omega]]_{g_2} = [[\omega]]_{g_1}[[g_2]]_{g_1}^{-1} \bmod n$，即进行两次 Class$[n, g_1]$。因此对不同的 g 该问题是等价的。

which yields $[\![g_1]\!]_{g_2} = [\![g_2]\!]_{g_1}^{-1} \bmod n$ and thus $[\![g_2]\!]_{g_1}$ is invertible modulo n. Suppose that we are given an oracle for Class $[n, g_1]$. Feeding g_2 and w into the oracle respectively gives $[\![g_2]\!]_{g_1}$ and $[\![w]\!]_{g_1}$, and by straightforward deduction :

推出

$$[\![w]\!]_{g_2} = [\![w]\!]_{g_1} [\![g_2]\!]_{g_1}^{-1} \bmod n .$$

□

Lemma 7 essentially means that the complexity of Class $[n, g]$ is independant from g. This enables us to look upon it as a computational problem which purely relies on n. Formally,

Definition 8. *We call Composite Residuosity Class Problem the computational problem Class* $[n]$ *defined as follows : given* $w \in \mathbb{Z}_{n^2}^*$ *and* $g \in \mathcal{B}$, *compute* $[\![w]\!]_g$.

We now proceed to find out which connections exist between the Composite Residuosity Class Problem and standard number-theoretic problems. We state first :

定义：**Composite Residuosity Class Problem：Class[n]**

给定 $\omega \in \mathbb{Z}_{n^2}^*$ 以及 $g \in \mathbb{Z}_{n^2}^*$ 且阶数是 n 的倍数，寻找 $[[\omega]]_g$。

定理9用于解密，证明了解密的困难性等价于对n进行因素分解

Theorem 9. *Class* $[n] \Leftarrow$ *Fact* $[n]$.

因素分解

用 $P_1 \Leftarrow P_2$ 表示问题 P_1 与 P_2 是多项式等价的（polynomial reducible），可以理解为：有一台可以不花费时间计算 P_2 的机器（oracle），就可以在多项式时间里计算出 P_1。

Before proving the theorem, observe that the set

$$\mathcal{S}_n = \{u < n^2 \mid u = 1 \bmod n\}$$

is a multiplicative subgroup of integers modulo n^2 over which the function L such that

乘法子群

$$\forall u \in \mathcal{S}_n \quad \mathrm{L}(u) = \frac{u-1}{n}$$

首先考虑如下集合 $\mathcal{S}_b = \{u < n^2 | u = 1 \bmod n\}$，显然它是一个乘法子群（multiplicative subgroup）。因此我们可以在这个集合上定义函数 $L(u) = \frac{u-1}{n}$。
已知$(1+n)^x \equiv 1 + xn \; mod \; n^2$
和 $(1+n)^x \equiv 1 \; mod \; n$ 。 令 $x = n$，则 $(1+n)^n \equiv 1 \; mod \; n^2$，所以$1+n$的阶整除 n，所以$1+n \in \beta$

is clearly well-defined.

Lemma 10. *For any* $w \in \mathbb{Z}_{n^2}^*$, $L(w^\lambda \bmod n^2) = \lambda [\![w]\!]_{1+n} \bmod n$.

Proof (of Lemma 10). Since $1 + n \in \mathcal{B}$, there exists a unique pair (a, b) in the set $\mathbb{Z}_n \times \mathbb{Z}_n^*$ such that $w = (1+n)^a b^n \bmod n^2$. By definition, $a = [\![w]\!]_{1+n}$. Then

$$w^\lambda = (1+n)^{a\lambda} b^{n\lambda} = (1+n)^{a\lambda} = 1 + a\lambda n \bmod n^2 ,$$

which yields the announced result.

引理7已经证明

Proof (of Theorem 9). Since $[\![g]\!]_{1+n} = [\![1+n]\!]_g^{-1} \bmod n$ is invertible, a consequence of Lemma 10 is that $\mathrm{L}(g^\lambda \bmod n^2)$ is invertible modulo n. Now, factoring n obviously leads to the knowledge of λ. Therefore, for any $g \in \mathcal{B}$ and $w \in \mathbb{Z}_{n^2}^*$, we can compute

w可以看成密文，这个公式(2)可看成解密过程

$$\frac{\mathrm{L}(w^\lambda \bmod n^2)}{\mathrm{L}(g^\lambda \bmod n^2)} = \frac{\lambda [\![w]\!]_{1+n}}{\lambda [\![g]\!]_{1+n}} = \frac{[\![w]\!]_{1+n}}{[\![g]\!]_{1+n}} = [\![w]\!]_g \bmod n , \quad (2)$$

by *virtue* of Equation 1. □

借助

给定 $\omega \in \mathbb{Z}^*_{n^2}$ 以及 $g \in \mathbb{Z}^*_{n^2}$ 且阶数是 n 的倍数，寻找 $[[\omega]]_g$。

Theorem 11. *Class* $[n] \quad \Leftarrow \quad$ *RSA* $[n, n]$.

Proof. Since all the instances of Class $[n, g]$ are computationally equivalent for $g \in \mathcal{B}$, and since $1 + n \in \mathcal{B}$, it suffices to show that

$$\text{Class}\,[n, 1+n] \quad \Leftarrow \quad \text{RSA}\,[n, n] \ .$$

Let us be given an oracle for RSA $[n, n]$. We know that $w = (1+n)^x \cdot y^n \bmod n^2$ for some $x \in \mathbb{Z}_n$ and $y \in \mathbb{Z}^*_n$. Therefore, we have $w = y^n \bmod n$ and we get y by giving $w \bmod n$ to the oracle. From now,

$$\frac{w}{y^n} = (1+n)^x = 1 + xn \bmod n^2 \ ,$$

which discloses $x = [\![w]\!]_{1+n}$ as announced.

证明：我们考虑求解 $[[\omega]]_{1+n}$。由于 $\omega = (1+n)^x y^n \bmod n^2 = y^n(1+nx) \bmod n^2$，可以得到$\omega = y^n \bmod n$。于是可以通过输入$\omega, n$ 到 RSA$[n,n]$ 得到 y，然后可以解出 x。

判断某个整数 z 是否是 n^2 的n次剩余的问题记作 **CR[n]**

Theorem 12. *Let D-Class* $[n]$ *be the decisional problem associated to Class* $[n]$ *i.e. given* $w \in \mathbb{Z}^*_{n^2}$, $g \in \mathcal{B}$ *and* $x \in \mathbb{Z}_n$, *decide whether* $x = [\![w]\!]_g$ *or not. Then*

$$\mathit{CR}\,[n] \quad \equiv \quad \mathit{D\text{-}Class}\,[n] \quad \Leftarrow \quad \mathit{Class}\,[n] \ .$$

Proof. The hierarchy D-Class $[n] \ \Leftarrow\ $ Class $[n]$ comes from the general fact that it is easier to verify a solution than to compute it. Let us prove the left-side equivalence. ($\Rightarrow$) Submit $wg^{-x} \bmod n^2$ to the oracle solving CR $[n]$. In case of n-th residuosity detection, the equality $[\![wg^{-x}]\!]_g = 0$ implies $[\![w]\!]_g = x$ by Lemma 5 and then answer "Yes". Otherwise answer "No" or "Failure" according to the oracle's response. ($\Leftarrow$) Choose an arbitrary $g \in \mathcal{B}$ ($1 + n$ will do) and submit the triple $(g, w, x = 0)$ to the oracle solving D-Class $[n]$. Return the oracle's answer without change. □

* CR$[n] \Rightarrow$ D-Class$[n]$：若 $\omega = g^x y^n \bmod n^2$，则 $\omega g^{-x} = y^n \bmod n^2$，因此把 ωg^{-x} 放入求解 CR$[n]$ 的机器中，若返回 *True*，则代表 $[[\omega]]_g = x$。若非如此，对应的 y 无法找到，ωg^{-x} 放入该机器必定返回 *False*。

To conclude, the computational hierarchy we have been looking for was

计算层次

$$\text{CR}\,[n] \ \equiv\ \text{D-Class}\,[n] \ \Leftarrow\ \text{Class}\,[n] \ \Leftarrow\ \text{RSA}\,[n,n] \ \Leftarrow\ \text{Fact}\,[n] \ , \qquad (3)$$

with serious doubts concerning a potential equivalence, excepted possibly between D-Class $[n]$ and Class $[n]$. Our second intractability hypothesis will be to assume the hardness of the Composite Residuosity Class Problem by making the following conjecture :

* D-Class$[n] \Rightarrow$ CR$[x]$：如果 ω 是n的一个n次剩余，则存在 $y^n = \omega \bmod n^2$，令 $g = n+1$，则存在 $g^0 y^n = \omega$，即把 $g = n+1, x = 0, \omega$ 放入求解 D-Class$[n]$ 的机器中会返回 *True*。反之则不存在这样的 y，因此会返回 *False*。

推测 · 猜想

Conjecture 13. There exists no probabilistic polynomial time algorithm that solves the Composite Residuosity Class Problem, *i.e.* Class $[n]$ is intractable.

我们猜测，Class$[n]$ 没有多项式时间的解法（Intractable）

By contrast to the Decisional Composite Residuosity Assumption, this conjecture will be refered to as the *Computational Composite Residuosity Assumption* (CCRA). Here again, random-self-reducibility implies that the validity of the CCRA is only conditioned by the choice of n. Obviously, if the DCRA is true then the CCRA is true as well. The converse, however, still remains a challenging open question.

4 A New Probabilistic Encryption Scheme

We now proceed to describe a public-key encryption scheme based on the Composite Residuosity Class Problem. Our methodology is quite natural : employing $\mathcal{E}_g$ for encryption and the polynomial reduction of Theorem 9 for decryption, using the factorisation as a trapdoor. 本质还是将大数分解作为陷门(难题)

Set $n = pq$ and randomly select a base $g \in \mathcal{B}$: as shown before, this can be done efficiently by checking whether

证明见最后一页

$$\gcd\left(\mathrm{L}(g^\lambda \bmod n^2), n\right) = 1\ . \tag{4}$$

Now, consider (n, g) as public parameters whilst the pair (p, q) (or equivalently λ) remains private. The cryptosystem is depicted below.

选择一个 $n = pq$，再随机选取 $g \in \mathcal{B}$。

可以通过检查 $\gcd(L(g^\lambda \bmod n^2), n) = 1$ 来有效地选取 g。因为 $\gcd(L(g^\lambda \bmod n^2), n) = 1 \Rightarrow g^\lambda = kn + 1 \bmod n^2, \gcd(k, n) = 1$

这样显然可以知道若 g 的阶数（在 $\mathbb{Z}_n^*$ 中）是 s，$g^s = 1 + kn \bmod n$ 且 $\gcd(k, n) = 1$。而且 g 在 $\mathbb{Z}_{n^2}^*$ 的阶数必须是 s 的倍数，设其为 ts，则 $g^{ts} \bmod n^2 = (1 + kn)^t \bmod n^2 = 1 + knt \bmod n^2 = 1$，于是显然有 $n|kt$。

然后我们把 (n, g) 作为公钥，λ 作为私钥。

Encryption :

plaintext $m < n$

select a random $r < n$

ciphertext $c = g^m \cdot r^n \bmod n^2$

Decryption :

ciphertext $c < n^2$

plaintext $m = \dfrac{\mathrm{L}(c^\lambda \bmod n^2)}{\mathrm{L}(g^\lambda \bmod n^2)} \bmod n$

Scheme 1. Probabilistic Encryption Scheme Based on Composite Residuosity.

The correctness of the scheme is easily verified from Equation 2, and it is straightforward that the encryption function is a trapdoor function with λ (that is, the knowledge of the factors of n) as the trapdoor secret. One-wayness is based on the computational problem discussed in the previous section.

Theorem 14. *Scheme 1 is one-way if and only if the Computational Composite Residuosity Assumption holds.*

Proof. Inverting our scheme is by definition the Composite Residuosity Class Problem. □

n次剩余

Theorem 15. *Scheme 1 is semantically secure if and only if the Decisional Composite Residuosity Assumption holds.*

Proof. Assume that m_0 and m_1 are two known messages and c the ciphertext of either m_0 or m_1. Due to Lemma 5, c is the ciphertext of m_0 if and only if $cg^{-m_0} \bmod n^2$ is a n-th residue. Therefore, a successfull chosen-plaintext attacker could decide composite residuosity, and vice-versa. 反之亦然 □

排列

5 A New One-Way Trapdoor Permutation

One-way trapdoor permutations are very rare cryptographic objects : we refer the reader to [22] for an exhaustive documentation on these. In this section, we show how to use the trapdoor technique introduced in the previous section to derive a permutation over $\mathbb{Z}^*_{n^2}$.

As before, n stands for the product of two large primes and g is chosen as in Equation 4.

Encryption :

plaintext $m < n^2$

split m into m_1, m_2 such that $m = m_1 + nm_2$

ciphertext $c = g^{m_1} {m_2}^n \bmod n^2$

Decryption :

ciphertext $c < n^2$

Step 1. $m_1 = \dfrac{\mathrm{L}(c^\lambda \bmod n^2)}{\mathrm{L}(g^\lambda \bmod n^2)} \bmod n$

Step 2. $c' = cg^{-m_1} \bmod n$

Step 3. $m_2 = c'^{n^{-1} \bmod \lambda} \bmod n$

plaintext $m = m_1 + nm_2$

Scheme 2. A Trapdoor Permutation Based on Composite Residuosity.

We first show the scheme's correctness. Clearly, Step 1 correctly retrieves $m_1 = m \bmod n$ as in Scheme 1. Step 2 is actually an unblinding phase which is necessary to recover $m_2^n \bmod n$. Step 3 is an RSA decryption with a public exponent $e = n$. The final step recombines[2] the original message m. The fact that Scheme 2 is a permutation comes from the bijectivity of $\mathcal{E}_g$. Again, trapdoorness is based on the factorisation of n. Regarding one-wayness, we state :

Theorem 16. *Scheme 2 is one-way if and only if RSA* $[n, n]$ *is hard.*

Proof. a) Since Class $[n] \Leftarrow$ RSA $[n, n]$ (Theorem 11), extracting n-th roots modulo n is sufficient to compute m_1 from $\mathcal{E}_g(m_1, m_2)$. Retrieving m_2 then requires one more additionnal extraction. Thus, inverting Scheme 2 cannot be harder than extracting n-th roots modulo n. b) Conversely, an oracle which inverts Scheme 2 allows root extraction : first query the oracle to get the two

[2] note that every public bijection $m \leftrightarrow (m_1, m_2)$ fits the scheme's structure, but euclidean division appears to be the most natural one.

w是模n的n次剩余

numbers a and b such that $1+n = g^a b^n \bmod n^2$. Now if $w = y_0^n \bmod n$, query the oracle again to obtain x and y such that $w = g^x y^n \bmod n^2$. Since $1+n \in \mathcal{B}$, we know there exists an x_0 such that $w = (1+n)^{x_0} y_0^n \bmod n^2$, wherefrom

$$w = \left(g^a b^n\right)^{x_0} y_0^n = g^{ax_0 \bmod n} \left(g^{ax_0 \operatorname{div} n} b^{x_0} y_0\right)^n \bmod n^2 .$$

By identification with $w = g^x y^n \bmod n^2$, we get $x_0 = xa^{-1} \bmod n$ and finally $y_0 = y g^{-(ax_0 \operatorname{div} n)} b^{-x_0} \bmod n$ which is the wanted value. □

Remark 17. Note that by definition of $\mathcal{E}_g$, the cryptosystem requires that $m_2 \in \mathbb{Z}_n^*$, just like in the RSA setting. The case $m_2 \notin \mathbb{Z}_n^*$ either allows to factor n or leads to the ciphertext zero for all possible values of m_1. A consequence of this fact is that our trapdoor permutation cannot be employed *ad hoc* to encrypt short messages *i.e.* messages smaller than n.

特别的

Digital Signatures. Finally, denoting by $h : \mathbb{N} \mapsto \{0,1\}^k \subset \mathbb{Z}_{n^2}^*$ a hash function see as a random oracle [2], we obtain a digital signature scheme as follows. For a given message m, the signer computes the signature (s_1, s_2) where

$$\begin{cases} s_1 = \dfrac{\mathrm{L}(h(m)^\lambda \bmod n^2)}{\mathrm{L}(g^\lambda \bmod n^2)} \bmod n \\[2ex] s_2 = \left(h(m) g^{-s_1}\right)^{1/n \bmod \lambda} \bmod n \end{cases}$$

and the verifier checks that

$$h(m) \stackrel{?}{=} g^{s_1} s_2^n \bmod n^2 .$$

推论

Corollary 18 (of Theorem 16). *In the random oracle model, an existential forgery of our signature scheme under an adaptive chosen message attack has a negligible success probability provided that RSA* $[n, n]$ *is intractable.*

Although we feel that the above trapdoor permutation remains of moderate interest due to its equivalence with RSA, the rarity of such objects is such that we find it useful to mention its existence. Moreover, the homomorphic properties of this scheme, discussed in section 8, could be of a certain utility regarding some (still unresolved) cryptographic problems.

6 Reaching Almost-Quadratic Decryption Complexity

立方的，三次的

Most popular public-key cryptosystems present a cubic decryption complexity, and this is the case for Scheme 1 as well. The fact that no faster (and still appropriately secure) designs have been proposed so far strongly motivates the search for novel trapdoor functions allowing increased decryption performances. This section introduces a slightly modified version of our main scheme (Scheme 1) which features an $\mathcal{O}\left(|n|^{2+\epsilon}\right)$ decryption complexity.

Here, the idea consists in restricting the ciphertext space $\mathbb{Z}_{n^2}^*$ to the subgroup $<g>$ of smaller order by taking advantage of the following extension of Equation 2. Assume that $g \in \mathcal{B}_\alpha$ for some $1 \le \alpha \le \lambda$. Then for any $w \in <g>$,

$$[\![w]\!]_g = \frac{\mathrm{L}(w^\alpha \bmod n^2)}{\mathrm{L}(g^\alpha \bmod n^2)} \bmod n\ . \tag{5}$$

This motivates the cryptosystem depicted below.

Encryption :

plaintext $m < n$

randomly select $r < n$

ciphertext $c = g^{m+nr} \bmod n^2$

Decryption :

ciphertext $c < n^2$

plaintext $m = \dfrac{\mathrm{L}(c^\alpha \bmod n^2)}{\mathrm{L}(g^\alpha \bmod n^2)} \bmod n$

Scheme 3. Variant with fast decryption.

Note that this time, the encryption function's trapdoorness relies on the knowledge of α (instead of λ) as secret key. The most computationally expensive operation involved in decryption is the modular exponentiation $c \to c^\alpha \bmod n^2$ which runs in complexity $\mathcal{O}\left(|n|^2|\alpha|\right)$ (to be compared to $\mathcal{O}\left(|n|^3\right)$ in Scheme 1). If g is chosen in such a way that $|\alpha| = \Omega\left(|n|^\epsilon\right)$ for some $\epsilon > 0$, then decryption will only take $\mathcal{O}\left(|n|^{2+\epsilon}\right)$ bit operations. To the best of our knowledge, Scheme 3 is the only public-key cryptosystem based on modular arithmetics whose decryption function features such a property.

Clearly, inverting the encryption function does not rely on the composite residuosity class problem, since this time the ciphertext is known to be an element of $<g>$, but on a weaker instance. More formally,

Theorem 19. *We call Partial Discrete Logarithm Problem the computational problem PDL* $[n, g]$ *defined as follows : given* $w \in <g>$, *compute* $[\![w]\!]_g$. *Then Scheme 3 is one-way if and only if PDL* $[n, g]$ *is hard.*

Theorem 20. *We call Decisional Partial Discrete Logarithm Problem the decisional problem D-PDL* $[n, g]$ *defined as follows : given* $w \in <g>$ *and* $x \in \mathbb{Z}_n$, *decide whether* $[\![w]\!]_g = x$. *Then Scheme 3 is semantically secure if and only if D-PDL* $[n, g]$ *is hard.*

The proofs are similar to those given in section 4. By opposition to the original class problems, these ones are not random-self-reducible over $g \in \mathcal{B}$ but over cyclic subgroups of $\mathcal{B}$, and present other interesting characteristics that we do not discuss here due to the lack of space. Obviously,

$$\mathrm{PDL}\,[n,g] \quad \Leftarrow \quad \mathrm{Class}\,[n] \quad \text{and} \quad \text{D-PDL}\,[n,g] \quad \Leftarrow \quad \mathrm{CR}\,[n]$$

but equivalence can be reached when g is of maximal order $n\lambda$ and n the product of two safe primes. When $g \in \mathcal{B}_\alpha$ for some $\alpha < \lambda$ such that $|\alpha| = \varOmega\left(|n|^\epsilon\right)$ for $\epsilon > 0$, we conjecture that both PDL $[n,g]$ and D-PDL $[n,g]$ are intractable.

In order to thwart Baby-Step Giant-Step attacks, we recommend the use of 160-bit prime numbers for αs in practical use. This can be managed by an appropriate key generation. In this setting, the computational load of Scheme 3 is smaller than a RSA decryption with Chinese Remaindering for $|n| \geq 1280$. Next section provides tight evaluations and performance comparisons for all the encryption schemes presented in this paper.

7 Efficiency and Implementation Aspects

In this section, we briefly analyse the main practical aspects of computations required by our cryptosystems and provide various implementation strategies for increased performance.

Key Generation. The prime factors p and q must be generated according to the usual recommandations in order to make n as hard to factor as possible. The fast variant (Scheme 3) requires additionally $\lambda = \mathrm{lcm}(p-1, q-1)$ to be a multiple of a 160-bit prime integer, which can be managed by usual DSA-prime generation or other similar techniques. The base g can be chosen randomly among elements of order divisible by n, but note that the fast variant will require a specific treatment (typically raise an element of maximal order to the power λ/α). The whole generation may be made easier by carrying out computations separately mod p^2 and mod q^2 and Chinese-remaindering g mod p^2 and g mod q^2 at the very end.

中国剩余定理

g的选择有利于加速

Encryption. Encryption requires a modular exponentiation of base g. The computation may be significantly accelerated by a judicious choice of g. As an illustrative example, taking $g = 2$ or small numbers allows an immediate speed-up factor of 1/3, provided the chosen value fulfills the requirement $g \in \mathcal{B}$ imposed by the setting. Optionally, g could even be fixed to a constant value if the key generation process includes a specific adjustment. At the same time, pre-processing techniques for exponentiating a constant base can dramatically reduce the computational cost. The second computation r^n or g^{nr} mod n^2 can also be computed in advance.

Decryption. Computing $\mathrm{L}(u)$ for $u \in \mathcal{S}_n$ may be achieved at a very low cost (only one multiplication modulo $2^{|n|}$) by precomputing n^{-1} mod $2^{|n|}$. The constant parameter 可以通过预计算某些参数的方式减少解密时间

$$\mathrm{L}(g^\lambda \bmod n^2)^{-1} \bmod n \quad \text{or} \quad \mathrm{L}(g^\alpha \bmod n^2)^{-1} \bmod n$$

can also be precomputed once for all.

用到中国剩余定理进行解密

Decryption using Chinese-remaindering. The Chinese Remainder Theorem [6] can be used to efficiently reduce the decryption workload of the three cryptosystems. To see this, one has to employ the functions L_p and L_q defined over

$$\mathcal{S}_p = \left\{x < p^2 \mid x = 1 \bmod p\right\} \quad \text{and} \quad \mathcal{S}_q = \left\{x < q^2 \mid x = 1 \bmod q\right\}$$

by

$$\mathrm{L}_p(x) = \frac{x-1}{p} \quad \text{and} \quad \mathrm{L}_q(x) = \frac{x-1}{q} \,.$$

Decryption can therefore be made faster by separately computing the message mod p and mod q and recombining modular residues afterwards :

$$\begin{aligned} m_p &= \mathrm{L}_p(c^{p-1} \bmod p^2)\, h_p \bmod p \\ m_q &= \mathrm{L}_q(c^{q-1} \bmod q^2)\, h_q \bmod q \\ m &= \mathrm{CRT}(m_p, m_q) \bmod pq \end{aligned}$$

with precomputations

$$\begin{aligned} h_p &= \mathrm{L}_p(g^{p-1} \bmod p^2)^{-1} \bmod p \quad \text{and} \\ h_q &= \mathrm{L}_q(g^{q-1} \bmod q^2)^{-1} \bmod q \,. \end{aligned}$$

where $p-1$ and $q-1$ have to be replaced by α in the fast variant.

Performance evaluations. For each $|n| = 512, \cdots, 2048$, the modular multiplication of bitsize $|n|$ is taken as the unitary operation, we assume that the execution time of a modular multiplication is quadratic in the operand size and that modular squares are computed by the same routine. Chinese remaindering, as well as random number generation for probabilistic schemes, is considered to be negligible. The RSA public exponent is taken equal to $\mathrm{F}_4 = 2^{16} + 1$. The parameter g is set to 2 in our main scheme, as well as in the trapdoor permutation. Other parameters, secret exponents or messages are assumed to contain about the same number of ones and zeroes in their binary representation.

Schemes	**Main Scheme**	**Permutation**	**Fast Variant**	**RSA**	**ElGamal**
One-wayness	Class $[n]$	RSA $[n, n]$	PDL $[n, g]$	RSA $[n, \mathrm{F}_4]$	DH $[p]$
Semantic Sec.	CR $[n]$	none	D-PDL $[n, g]$	none	D-DH $[p]$
Plaintext size	$\|n\|$	2 $\|n\|$	$\|n\|$	$\|n\|$	$\|p\|$
Ciphertext size	2 $\|n\|$	2 $\|n\|$	2 $\|n\|$	$\|n\|$	2 $\|p\|$
Encryption					
$\|n\|, \|p\| = 512$	5120	5120	4032	**17**	1536
$\|n\|, \|p\| = 768$	7680	7680	5568	**17**	2304
$\|n\|, \|p\| = 1024$	10240	10240	7104	**17**	3072
$\|n\|, \|p\| = 1536$	15360	1536	10176	**17**	4608
$\|n\|, \|p\| = 2048$	20480	20480	13248	**17**	6144
Decryption					
$\|n\|, \|p\| = 512$	768	1088	480	**192**	768
$\|n\|, \|p\| = 768$	1152	1632	480	**288**	1152
$\|n\|, \|p\| = 1024$	1536	2176	480	**384**	1536
$\|n\|, \|p\| = 1536$	2304	3264	**480**	576	2304
$\|n\|, \|p\| = 2048$	3072	4352	**480**	768	3072

These estimates are purely indicative, and do not result from an actual implementation. We did not include the potential pre-processing stages. Chinese remaindering is taken into account in cryptosystems that allow it *i.e.* all of them excepted ElGamal.

8 Properties

Before concluding, we would like to stress again the algebraic characteristics of our cryptosystems, especially those of Schemes 1 and 3.

Random-Self-Reducibility. This property actually concerns the underlying number-theoretic problems CR $[n]$ and Class $[n]$ and, to some extent, their weaker versions D-PDL $[n, g]$ and PDL $[n, g]$. Essentially, random-self-reducible problems are as hard on average as they are in the worst case : both RSA and the Discrete Log problems have this feature. Problems of that type are believed to yield good candidates for one-way functions [1].

Additive Homomorphic Properties. As already seen, the two encryption functions $m \mapsto g^m r^n \bmod n^2$ and $m \mapsto g^{m+nr} \bmod n^2$ are additively homomorphic on $\mathbb{Z}_n$. Practically, this leads to the following identities :

$$\forall m_1, m_2 \in \mathbb{Z}_n \quad \text{and} \quad k \in \mathbb{N}$$

$$\mathrm{D}(\mathrm{E}(m_1)\,\mathrm{E}(m_2) \bmod n^2) = m_1 + m_2 \bmod n$$

$$\mathrm{D}(\mathrm{E}(m)^k \bmod n^2) = km \bmod n$$

$$\mathrm{D}(\mathrm{E}(m_1)\,g^{m_2} \bmod n^2) = m_1 + m_2 \bmod n$$

$$\left.\begin{array}{l} \mathrm{D}(\mathrm{E}(m_1)^{m_2} \bmod n^2) \\ \mathrm{D}(\mathrm{E}(m_2)^{m_1} \bmod n^2) \end{array}\right\} = m_1 m_2 \bmod n \,.$$

这些性质适用于投票系统,门限密码系统,水印和秘密共享方案

These properties are known to be particularly appreciated in the design of voting protocols, threshold cryptosystems, watermarking and secret sharing schemes, to quote a few. Server-aided polynomial evaluation (see [27]) is another potential field of application.

对密文进一步加密成另一个密文后,其一次性解密结果仍可以得到原始明文,这种性质成为self-blinding

Self-Blinding. Any ciphertext can be publicly changed into another one without affecting the plaintext :

$$\forall m \in \mathbb{Z}_n \quad \text{and} \quad r \in \mathbb{N}$$

$$\mathrm{D}(\mathrm{E}(m)\,r^n \bmod n^2) = m \qquad \text{or} \qquad \mathrm{D}(\mathrm{E}(m)\,g^{nr} \bmod n^2) = m \,,$$

depending on which cryptosystem is considered. Such a property has potential applications in a wide range of cryptographic settings.

9 Further Research

本文提出了新的数论难题和相关的陷门机制基于复数阶剩余的使用。派生出三个新的密码系统

In this paper, we introduced a new number-theoretic problem and a related trapdoor mechanism based on the use of composite degree residues. We derived three new cryptosystems based on our technique, all of which are provably secure under adequate intractability assumptions.

Although we do not provide any proof of security against chosen ciphertext attacks, we believe that one could bring slight modifications to Schemes 1 and 3 to render them resistant against such attacks, at least in the random oracle model. 没有提供随机预言模型下的选择明文攻击的安全性证明

Another research topic resides in exploiting the homomorphic properties of our systems to design distributed cryptographic protocols (multi-signature, secret sharing, threshold cryptography, and so forth) or other cryptographically useful objects.

本文的同态性质还可用于设计分布式密码协议,比如多重签名,秘密共享,门限密码学

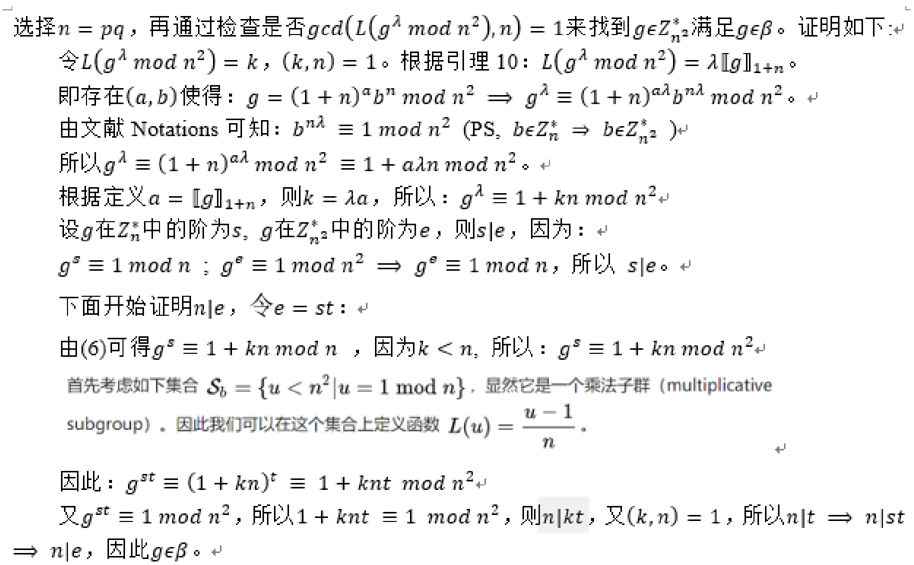
10 Acknowledgments

The author is especially grateful to David Pointcheval for his precious comments and contributions to this work. We also thank Jacques Stern and an anonymous referee for having (independently) proved that Class $[n] \Leftarrow$ RSA $[n, n]$. Finally, Dan Boneh, Jean-Sébastien Coron, Helena Handschuh and David Naccache are acknowledged for their helpful discussions and comments during the completion of this work.

References

1. D. Angluin and D. Lichtenstein, *Provable Security of Cryptosystems: A Survey*, Computer Science Department, Yale University, TR-288, 1983.
2. M. Bellare and P. Rogaway, *Random Oracles are Practical : a Paradigm for Designing Efficient Protocols*, In Proceedings of the First CCS, ACM Press, pp. 62–73, 1993.
3. J. C. Benaloh, *Verifiable Secret-Ballot Elections*, PhD Thesis, Yale University, 1988.
4. R. Cramer, R. Gennaro and B. Schoenmakers, *A Secure And Optimally Efficient Multi-Authority Election Scheme*, LNCS 1233, Proceedings of Eurocrypt'97, Springer-Verlag, pp. 103-118, 1997.
5. W. Diffie and M. Hellman, *New Directions in Cryptography*, IEEE Transaction on Information Theory, IT-22,6, pp. 644–654, 1995.
6. C. Ding, D. Pei and A. Salomaa, *Chinese Remainder Theorem - Applications in Computing, Coding, Cryptography*, World Scientific Publishing, 1996.
7. T. ElGamal, *A Public-Key Cryptosystem an a Signature Scheme Based on Discrete Logarithms*, IEEE Trans. on Information Theory, IT-31, pp. 469–472, 1985.
8. J. Feigenbaum, *Locally Random Reductions in Interactive Complexity Theory*, in Advances in Computational Complexity Theory, DIMACS Series on Discrete Mathematics and Theoretical Computer Science, vol. 13, American Mathematical Society, Providence, pp. 73–98, 1993.
9. S. Goldwasser and S. Micali, *Probabilistic Encryption*, JCSS Vol. 28 No 2, pp. 270–299, 1984.
10. K. Koyama, U. Maurer, T. Okamoto and S. Vanstone, *New Public-Key Schemes based on Elliptic Curves over the ring Zn*, LNCS 576, Proceedings of Crypto'91, Springer-Verlag, pp. 252–266, 1992.
11. T. Matsumoto and H. Imai, *Public Quadratic Polynomial-Tuples for Efficient Signature-Verification and Message-Encryption*, LNCS 330, Proceedings of Eurocrypt'88, Springer-Verlag, pp. 419–453, 1988.
12. U. Maurer and S. Wolf, *On the Complexity of Breaking the Diffie-Hellman Protocol.*
13. R. Merkle and M. Hellman, *Hiding Information and Signatures in Trapdoor Knapsacks*, IEEE Trans. on Information Theory, Vol. 24, pp. 525–530, 1978.
14. K. McCurley, *A Key Distribution System Equivalent to Factoring*, Journal of Cryptology, Vol. 1, pp. 95–105, 1988.
15. R. McEliece, *A Public-Key Cryptosystem Based on Algebraic Coding Theory*, DSN Progress Report 42-44, Jet Propulsion Laboratories, Pasadena, 1978.
16. D. Naccache and J. Stern, *A New Public-Key Cryptosystem Based on Higher Residues*, LNCS 1403, Advances in Cryptology, Proceedings of Eurocrypt'98, Springer-Verlag, pp. 308–318, 1998.

17. D. Naccache and J. Stern, *A New Public-Key Cryptosystem*, LNCS 1233, Advances in Cryptology, Proceedings of Eurocrypt'97, Springer-Verlag, pp. 27–36, 1997.
18. P. Nguyen and J. Stern, *Cryptanalysis of the Ajtai-Dwork Cryptosystem*, LNCS 1462, Proceedings of Crypto'98, Springer-Verlag, pp. 223–242, 1998.
19. T. Okamoto and S. Uchiyama, *A New Public-Key Cryptosystem as secure as Factoring*, LNCS 1403, Advances in Cryptology, Proceedings of Eurocrypt'98, Springer-Verlag, pp. 308–318, 1998.
20. S. Park and D. Won, *A Generalization of Public-Key Residue Cryptosystem*, In Proceedings of 1993 Korean-Japan Joint Workshop on Information Security and Cryptology, pp. 202–206, 1993.
21. J. Patarin, *The Oil and Vinegar Algorithm for Signatures*, presented at the Dagstuhl Workshop on Cryptography, 1997.
22. J. Patarin and L. Goubin, *Trapdoor One-Way Permutations and Multivariate Polynomials*, LNCS 1334, Proceedings of ICICS'97, Springer-Verlag, pp. 356–368, 1997.
23. R. Peralta and E. Okamoto, *Faster Factoring of Integers of a Special Form*, IEICE, Trans. Fundamentals, E79-A, Vol. 4, pp. 489–493, 1996.
24. M. Rabin, *Digital Signatures and Public-Key Encryptions as Intractable as Factorization*, MIT Technical Report No 212, 1979.
25. R. Rivest, A. Shamir and L. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Communications of the ACM, Vol. 21, No 2, pp. 120–126, 1978.
26. A. Salomaa, *Public-Key Cryptography*, Springer-Verlag, 1990.
27. T. Sander and F. Tschudin, *On Software Protection Via Function Hiding*, Proceedings of Information Hiding Workshop'98, 1998.
28. S. Vanstone and R. Zuccherato, *Elliptic Curve Cryptosystem Using Curves of Smooth Order Over the Ring Z_n*, IEEE Trans. Inf. Theory, Vol. 43, No 4, July 1997.
29. S. Vaudenay, *Cryptanalysis of the Chor-Rivest Cryptosystem*, LNCS 1462, Proceedings of Crypto'98, Springer-Verlag, pp. 243–256, 1998.
30. H. Williams, *Some Public-Key Crypto-Functions as Intractable as Factorization*, LNCS 196, Proceedings of Crypto'84, Springer-Verlag, pp. 66–70, 1985.



选择$n = pq$，再通过检查是否$gcd(L(g^\lambda \; mod \; n^2), n) = 1$来找到$g \epsilon Z_{n^2}^*$满足$g \epsilon \beta$。证明如下：

令$L(g^\lambda \; mod \; n^2) = k$，$(k, n) = 1$。根据引理 10：$L(g^\lambda \; mod \; n^2) = \lambda [\![g]\!]_{1+n}$。

即存在(a, b)使得：$g = (1+n)^a b^n \; mod \; n^2 \implies g^\lambda \equiv (1+n)^{a\lambda} b^{n\lambda} \; mod \; n^2$。

由文献 Notations 可知：$b^{n\lambda} \equiv 1 \; mod \; n^2$（PS，$b \epsilon Z_n^* \Rightarrow b \epsilon Z_{n^2}^*$）

所以$g^\lambda \equiv (1+n)^{a\lambda} \; mod \; n^2 \equiv 1 + a\lambda n \; mod \; n^2$。

根据定义$a = [\![g]\!]_{1+n}$，则$k = \lambda a$，所以：$g^\lambda \equiv 1 + kn \; mod \; n^2$

设g在Z_n^*中的阶为s，g在$Z_{n^2}^*$中的阶为e，则$s|e$，因为：

$g^s \equiv 1 \; mod \; n$；$g^e \equiv 1 \; mod \; n^2 \implies g^e \equiv 1 \; mod \; n$，所以 $s|e$。

下面开始证明$n|e$，令$e = st$：

由(6)可得$g^s \equiv 1 + kn \; mod \; n$ ，因为$k < n$，所以：$g^s \equiv 1 + kn \; mod \; n^2$

首先考虑如下集合 $\mathcal{S}_b = \{u < n^2 | u = 1 \bmod n\}$，显然它是一个乘法子群（multiplicative subgroup）。因此我们可以在这个集合上定义函数 $L(u) = \frac{u-1}{n}$。

因此：$g^{st} \equiv (1 + kn)^t \equiv 1 + knt \; mod \; n^2$

又$g^{st} \equiv 1 \; mod \; n^2$，所以$1 + knt \equiv 1 \; mod \; n^2$，则$n|kt$，又$(k, n) = 1$，所以$n|t \implies n|st \implies n|e$，因此$g \epsilon \beta$。