International Journal of Emerging Engineering Research and Technology
Volume 3, Issue 9, September 2015, PP 8-12
ISSN 2349-4395 (Print) & ISSN 2349-4409 (Online)

Mechansuim to Eliminate Composite Residuosity Class Problem by Using Modular Arithmetic for Public-Key Cryptography

Mukkamalla Snehapriya[1], Bullarao Domathoti[2], Putta Nageswara Ra[3]

[1]PG Scholar, Dept of CSE, Swetha institute of Technology & Science, Tirupati, AP, India.
[2]Assistant Professor, Dept of CSE, Swetha institute of Technology & Science, Tirupati, AP, India.
[3]Associate Professor, Dept of CSE, Swetha institute of Technology & Science, Tirupati, AP, India.

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 arithmetic, are provably secure under appropriate assumptions in the standard model.

Keywords: Paillier Cryptosystems, Trapdoor Mechanism, Residuosity Class Problem.

INTRODUCTION

Since the discovery of public-key cryptography by Diffie and Hellman, very few convincingly secure asymmetric schemes have been discovered despite considerable research efforts. We refer the reader to 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 and related variants such as Rabin-William, LUC, Dickson's scheme or elliptic curve versions of RSA like KMOV. 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 combines the homomorphism 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. Other proposed mechanisms generally suffer from inefficiency, inherent security weaknesses or insufficient public scrutiny: McEliece's cryptosystem based on error correcting codes, Ajtai-Dwork's scheme based on lattice problems (cryptanalyzed by Nguyen and Stern), additive and multiplicative knapsack-type systems including Merkle-Hellman, Chor-Rivest (brokenby Vaudenay) and Naccache-Stern; finally, Matsumoto-Imai and Goubin-Patarin cryptosystems, based on multivariate polynomials, were successively crypt analyzed. 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 based on quadratic residuosity, Benaloh's homomorphic encryption function, originally designed for electronic voting and relying on prime residuosity, pregured the first attempt to exploit the plain resources of this theory. Later, Naccache and Stern, and independently Okamoto and Uchiyama [19] significantly extended the encryption rate by investigating two different approaches: residuosity of smooth degree in Z*pq and residuosity of prime degree p in Z*p2qrespectively. In the meantime, other schemes like Vanstone-Zuccherato on elliptic curves or Park-Won 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

**Address for correspondence*

building-block for conceiving public-key cryptosystems. **Notations:** We set n = pq where p and q are large primes: as usual, we will denote by ϕ (n) Euler's to tient function and by λ(n) Carmichael's function1 taken on n, i.e. ϕ (n) = (p-1)(q -1) and λ(n) = lcm(p -1, q -1) in the present case. Recall that |Z*n2| = ϕ (n2) = n ϕ (n) and that for any w ϵ Z*n2

$$w^{\lambda} = 1 \bmod n \tag{1}$$

$$w^{n\lambda} = 1 \bmod n^2 , \tag{2}$$

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 factorization. The relation P1 <= P2 (resp. P1 ≡ P2) will denote that the problem P1 is polynomials reducible (resp. equivalent) to the problem P2.

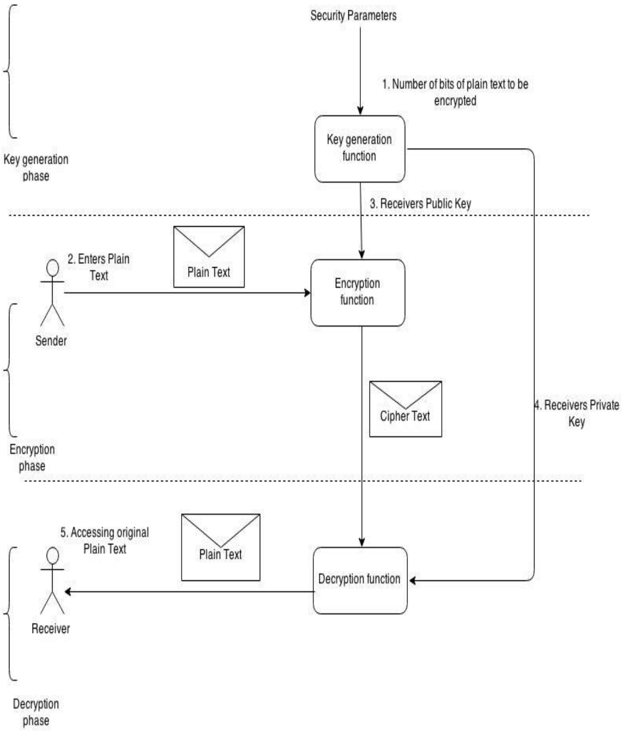

Fig1. *The overview of the System*

DECIDING COMPOSITE RESIDUOSITY

We begin by brief 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.

Definition 1. A number z is said to be a n-th residue modulo n2 if there exists a number y ϵ Z*n2 such that

$$z = y^n \bmod n^2. \tag{3}$$

The set of n-th residues is a multiplicative subgroup of Z*n2 of order ϕ (n).Each n-th residue z has exactly n roots of degree n, among which exactly one is strictly smaller than n (namely mod n). The n-th roots of unity are the numbers of the form (1 + n)x = 1 + xn mod n2. 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 polynomials 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. As for prime residuosity (cf. [3, 16]), deciding n-th residuosity is believed to be computationally hard. Accordingly, we will assume that:

Conjecture 1: There exists no polynomial time distinguisher for n-th residues modulo n2, i.e. CR[n] is intractable. This intractability hypothesis will be referred 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.

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 Z*n2and denote by εg the integer-valued function defined by

$$Z_n \times Z^*_n \rightarrow Z^*_n{}^2(x, y) \rightarrow g^x . y^n \bmod n^2 \qquad (4)$$

Depending on g, εg may feature some interesting properties. **Dentition 2:** Assume that g є B. For w є Z*n2, we call n-th residuosity class of w with respect to g the unique integer x є Zn for which there exists y єZ*n such that

$$\varepsilon_g(x, y) = w \qquad (5)$$

Adopting Benaloh's notations [3], the class of w is denoted [w]g. Our second intractability hypothesis will be to assume the hardness of the Composite Residuosity Class Problem by making the following conjecture:

Conjecture 2: There exists no probabilistic polynomial time algorithm solving the Composite Residuosity Class Problem, i.e. Class [n] is intractable. By contrast to the Decisional Composite Residuosity Assumption, this conjecture will be referred 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.

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 εg for encryption and the polynomial reduction of Theorem 1 for decryption, using the factorization as a trapdoor. Set n = pq and randomly select a base g є B: as shown before, this can be done efficiently by checking whether

$$\gcd\left(L(g^{\lambda} \bmod n^2), n\right) = 1 \qquad (6)$$

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

Scheme1. Probabilistic Encryption Scheme Based on Composite Residuosity. The correctness of the scheme is easily verified, and it is straightforward that the encryption function is a trapdoor function with λ as the trapdoor secret. One-wayness is based on the computational problem discussed in the previous section.

Encryption:

plaintext $m < n^2$

split m into m1, m2 such that $m = m1 + nm2$

ciphertext $c = g^{m1} m2^{n} \bmod n^2$

Decryption:

ciphertext $c < n^2$

Step 1. $m1 = \frac{L(c\lambda \bmod n2)}{L(g\lambda \bmod n2)} \bmod n$

Step 2. $C` = cg^{-m1} \bmod n$

Step 3. $m2 = c`^{n-1 \bmod \lambda} \bmod n$

plaintext $m = m1 + nm2$

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 Z*n2 .As before, n stands for the product of two large primes and g is chosen as in Equation.

Scheme 2: A Trapdoor Permutation Based on Composite Residuosity. We first show the scheme's correctness. Clearly, Step 1 correctly retrievesm1 = m mod n as in Scheme 1. Step 2 is actually an unbinding phase which is necessary to recover mn2mod n. Step 3 is an RSA decryption with a public exponent e = n. The final step recombines the original message m. The fact that Scheme 2 is a permutation comes from the objectivity of εg. Again, trapdoorness is based on the factorization of n. Regarding one-wayness, we state:

Digital Signatures: Finally, denoting by h: IN {0, 1}k Z*n2 a hash function see as a random oracle, we obtain a digital signature scheme as follows. For a given message m, the signer computes the signature (s1, s2) where

$$\begin{cases} s1 = \frac{L(h(m)\lambda modn2)}{L(g\lambda modn2)} modn \\ s2 = (h(m)g - s1)\,1/nmod\lambda modn \end{cases} \qquad (7)$$

and the verifier checks that h(m) =gs1sn2mod n2.

Encryption:

plaintext m < n

select a random r < n

ciphertext $c = g^{m}.r^{n} \bmod n^{2}$

Decryption:

ciphertext c < n2

plaintext $m = \frac{L(c \bmod n2)}{L(g \bmod n2)} \bmod n$

REACHING ALMOST-QUADRATIC DECRYPTION COMPLEXITY

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 O(|n|2+ϵ) decryption complexity. Here, the idea consists in restricting the cipher text space Z*n2 to the subgroup <g > of smaller order by taking advantage of the following extension of Equation 2. Assume that g ϵ Bα for some 1α λ. Then for any w ϵ <g>,

$$[w]_{g} = \frac{L(w\alpha modn2)}{L(g\alpha modn2)} \bmod n. \qquad (8)$$

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 < n2

plaintext $m = \frac{L(c\alpha \bmod n2)}{L(g\alpha \bmod n2)} \bmod n$

Scheme 3: Variant with fast decryption. Note that this time; the encryption function's trapdoorness relies on the knowledge of as secret key. The most computationally expensive operation involved in decryption is the modular exponentiation c ->cα mod n2which runs in complexity O(|n|2| α|)(to be compared to O(|n|3) in Scheme 1). If g is chosen in such a way that | α|=(|n|ϵ) for some ϵ> 0, then decryption will only take O(|n|2+ϵ) bit operations. To the best of our knowledge, Scheme 3 is the only public-key cryptosystem based on modular arithmetic 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 cipher text is known to be an element of <g>, but on a weaker instance. In order to thwart Baby-Step Giant-Step attacks, we recommend the use of 160-bit prime numbers for s in practical use. This can be managed by an appropriate key generation. In this setting, the computational load of Scheme 3is smaller than a RSA decryption with Chinese Remaindering for |n| 1280.Next section provides tight evaluations and performance comparisons for all the encryption schemes presented in this paper.

CONCLUSION

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.

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 Ecient Protocols, In Proceedings of the First CCS, ACM Press, pp. 62{73,1993.

[3] J. C. Benaloh, Veriable Secret-Ballot Elections, PhD Thesis, Yale University, 1988.

[4] R. Cramer, R. Gennaro and B. Schoenmakers, A Secure And Optimally E-cient 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 Scientic 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.

AUTHOR'S BIOGRAPHY

Mukkamalla Snehapriya has received her B.Tech in Computer Science and Engineering from sri raghavendra institute of science and technology, Nellore affiliated to JNTU, Anantapur in 2012 and pursuing M.Tech degree in Computer Science and Engineering in Swetha institute of Technology & Science, Tirupati, Affiliated to JNT University, Nellore, A.P affiliated to JNTU, Anatapur in (2013-2015).

Bullarao Domathoti is working as assistant professor in in the Computer Science & Engineering Department, College of Swetha institute of Technology & Science, Tirupati, Affiliated to JNT University. He received Master of technology of Information Technology degree in 2012 from JNTUK. Kakinada, India, His research interests are Computer Networks (wireless Networks), HCI, Algorithms, Information security, social networks, Datamining, web 2.0 etc.

Putta Nageswara Rao, Associate professor, dept of CSE, Sits, Jntua, Tirupati, Ap, India.