THE POLYNOMIAL MULTICOMPOSITION PROBLEM IN *(Z/nZ)*

Neculai Daniel Stoleru and Victor Valeriu Patriciu
Department of Mathematics and Informatics, Military Technical Academy, Caraiman Str. 116, Bucharest, Romania

Keywords: Polynomial composition, identification, key agreement.

Abstract: Generally, the public-key cryptographic schemes base their security on the difficulty of solving hard mathematical problems. The number of such problems currently known is relative reduced. Therefore the further investigation of mathematical problems with applications in cryptography is of central interest. This paper explores a new problem based on polynomial composition. We analyze the connections between the proposed problem and the RSA problem. Adjacent, we derive from it a zero – knowledge identification protocol. We show that the method allows the definition of a commutative class of polynomials. Based on this class, a "Diffie – Hellman like" key exchange protocol can be devised. .

1 INTRODUCTION

In cryptography, an asymmetric algorithm is based on a type of function first suggested by Diffie and Hellman (Diffie, Hellman, 1976) that has special properties known as *trapdoor one-way functions*. A trapdoor one-way function, if given some additional secret information, allows much easier computation of its inverse function. The one-way functions are based on *hard* mathematical problems, like factoring large composites into prime factors or the discrete logarithm problem.

Nevertheless, the number of hard mathematical problems with applications in cryptography currently known is rather reduced. Even considering the known problems of this type, there are still questionable items. As an example, the Optimal Asymmetric Encryption Padding (OAEP) has never been proven secure against the chosen ciphertext attack in the adaptive scenario (RSA, 2007).

In this context, the further research of such problems is of central interest. Similarly, finding general procedures supporting the study of a larger class of problems is also important.

The *Polynomial Composition Problem* (PCP) was first introduced in (Joye, Naccache, Porte, 2004) and can be enounced as follows:

Problem 1.
Let P and Q be two polynomials in (Z/nZ)[X]where n is an RSA modulus. Given polynomials Q and S:=Q(P), find P.

Joye et al. shown that generally the Polynomial Composition Problem is easier than the RSA problem – that is the computation of roots in Z/nZ - and gave a new version of this problem called "*Reduced Polynomial Composition Problem*" (RPCP), which can be proven to be equivalent with the RSA problem.

A number of cryptographic algorithms like the key agreement protocols based on asymmetric techniques (Menez, van Oorschot, Vanderstone, 1997) require operating in commutative groups. It is well known that generally, the polynomial composition is not commutative.

The present paper introduces a new problem called *Polynomial Multi - Composition Problem* (PMCP) based on a commutative class of polynomials.

In a proper approach, the security of the cryptographic scheme should be proven in a mathematical sense, i.e. establishing theorems claiming that illegal actions such as impersonation are as difficult as solving a specific problem, whose difficulty is well-established. Among these problems, as already mentioned, are integer factorization, or the computation of discrete logarithms in a finite group. This will also be the approach in the present paper, relating the new

Daniel Stoleru N. and Valeriu Patriciu V. (2007).
THE POLYNOMIAL MULTICOMPOSITION PROBLEM IN (Z/nZ).
In *Proceedings of the Second International Conference on Security and Cryptography*, pages 269-272
DOI: 10.5220/0002123402690272

introduced polynomial multi-composition problem to the reducible polynomial composition problem suggested in (Joye, Naccache, Porte, 2004).

Half-way between heuristic validation and formal proofs are proofs in a model where concrete objects are replaced by some ideal substitutes. Applying this paradigm to hash functions for example, yields the so-called *oracle model* described in (Bellare, Rogaway, 1993).

Using the following notation for a polynomial composed k – times with itself:

$$P^{(k)} := \underbrace{P \circ P \circ \cdots \circ P}_{k-times} = \underbrace{P(P...(P)...)}_{k-times} \qquad (1)$$

we can enounce the Polynomial Multi – Composition Problem as follows:

Problem 2.

Let P be a polynomial in (Z/nZ)[X] where n is an RSA modulus and k a big positive integer, $1 < k \leq n-1$. *Given k and the polynomial* $S := P^{(k)}$ *find* P.

We observe that choosing polynomials of type $S := P^{(k)}$ can lead to the definition of a commutative class of polynomials. For example, if we consider *P*, *Q*, *R* polynomials in Z/nZ[X] and $1 < k, l \leq n-1$ integers such that $S := P^{(k)}$ and $R := P^{(l)}$, then the polynomials *R* and *S* are commutative over Z/nZ. For any $\omega \in Z/nZ$ we have

$$\begin{aligned} S(R(\omega)) &= P^{(k)}(P^{(l)}(\omega)) \\ &= P^{(k+l)}(\omega) = P^{(l+k)}(\omega) \\ &= P^{(l)}(P^{(k)}(\omega)) \\ &= R(S(\omega)) . \end{aligned} \qquad (2)$$

This property allows us to devise a key exchange protocol based on polynomials in (Z/nZ)[X] similarly with the Diffie-Hellman key exchange protocol ((Menez, van Oorschot, Vanderstone, 1997) *Protocol* 12.47).

2 ANALYSIS OF THE POLYNOMIAL MULTI-COMPOSITION PROBLEM

In analyzing the security of the PMCP we relate the suggested problem to the *Reduced Polynomial Composition Problem* (RPCP) as given in (Joye, Naccache, Porte, 2004).

Consider a polynomial $P \in (Z/nZ)[X]$, a big integer *r*, $1 < r \leq n-1$ and the polynomial $S := P^{(k)}$. We can write:

$$S(X) = \sum_{t=0}^{p^r} c_t X^t \qquad (3)$$

where

$$c_t = \sum_{\substack{i_0+\cdots+i_p=p^r-1 \\ i_1+2i_2+\cdots pi_p=t}} \frac{(i_0+\cdots+i_p)!}{i_0!\cdots i_p!} u_0^{i_0} \cdots u_p^{i_p} \qquad (4)$$

Intuitively, the hardness of the Polynomial Multi - Composition Problem depends on how we choose the polynomial *P* in (Z/nZ)[X]. Nevertheless, generally, PMCP *cannot* be harder than the RSA Problem.

Example 1.

Consider $P(X) = u_2 X^2 + u_0$, *r* = 3 and the PMCP: "Given $S := P^{(3)}$ find *P*". Then the equations system given by relation (4) will be in this case:

$$\begin{cases} c_8 = u_2^7 \\ c_6 = 4u_0 u_2^6 \\ c_4 = 6u_0^2 u_2^5 + 2u_0 u_2^4 \\ c_2 = 4u_0^3 u_2^4 + 4u_0^2 u_2^3 \\ c_0 = u_0^4 u_2^3 + 2u_0^3 u_2^2 + u_0^2 u_2 + u_0 \end{cases} \qquad (5)$$

After some simple algebraic manipulations we obtain:

$$c_2 = \frac{c_6}{2c_8}\left(c_4 - \frac{c_6^2}{4c_8}\right) \ (mod\ \mathrm{n})$$

and analogue from the last equation in (5):

$$c_0 = \frac{c_6^3}{64c_8^3}\left(\frac{4c_8c_4}{c_6} - \frac{c_6}{2}\right) + u_0 \frac{4c_2c_8^2}{c_6^2} \ (mod\ \mathrm{n}) \qquad (6)$$

With $c_0, \ldots, c_8$ known we can determine u_0 from equation (6). Then u_2 can be determined through the direct substitution of u_0 in (5).

Consequently, we need to define a stronger problem in order to meet the usual cryptographic requirements. We introduce in the following the *Reducible Polynomial Multi – Composition Problem* (RPMCP).

Problem 3.

Let P be a polynomial in Z/nZ[X] where n is an RSA modulus and r a big integer $1 < r \leq n-1$. *Given the (deg(P) +* 1*) coefficients of* $S := P^{(k)}$ *find P.*

As proven in (Joye, Naccache, Porte, 2004) (see Theorem 1) the Reducible Polynomial Composition Problem is equivalent to the RSA Problem. We give the following result:

***Proposition* 1.** *Let P a polynomial in Z/nZ[X] where n is an RSA modulus, r a big integer* $1 < r \leq n-1$, $S := P^{(r)}$ *and* $Q := P^{(r-1)}$. *If the Polynomial Multi – Composition Problem "given S and r find P" is reducible then the Polynomial Composition Problem "given* $S := Q(P)$ *and Q find P" is also reducible.*

Proof. (Sketch) We can write the coefficients k_i of Q based on the relation (4) for $r - 1$:

$$k_i = \sum_{\substack{i_0+\cdots+i_p=p^{r-1}-1 \\ i_1+2i_2+\cdots pi_p=i}} \frac{(i_0+\cdots+i_p)!}{i_0!\cdots i_p!} u_0^{i_0}\cdots u_p^{i_p} \qquad (7)$$

for $0 \leq i \leq \deg(Q)$. Therefore, every k_i can be written as a combination of $u_0, \ldots, u_p$.

On the other hand, if the Polynomial Multi – Composition Problem is reducible, then the values of $c_0, \ldots, c_{p(p^{r-1}-1)-1}$ can be deduced from $c_{p(p^{r-1}-1)}, \ldots, c_{p^r}$ which is equivalent to deriving the values of $c_0, \ldots, c_{p(q-1)-1}$ based on $c_{p(q-1)}, \ldots, c_{pq}$ and $k_1, \ldots, k_{q-1}$ in the related Polynomial Composition Problem.

3 CRYPTOGRAPHIC APPLICATIONS

3.1 A Simple PMCP – based Identification Protocol

We suggest the following identification protocol based on PMCP:

In order to set up the system, a Trusted Third Party (TTP) selects and publishes an RSA modulus *n*. Each user chooses a polynomial *P* in (Z/nZ)[X] and some big integers *q*, *r* and *s* $1 < q, r, s \leq n-1$ such as $q + r = s$. Afterwards, the user computes

$$S := P^{(s)}, \quad Q := P^{(q)} \text{ and } R := P^{(r)} \qquad (8)$$

in (Z/nZ)[X] and registers the polynomials *S* and *Q* and the integers *q*, *r* and *s* with the TTP. *S* and *Q* represent user's public key and will be made publicly available. Nevertheless, after calculating *R*, the user will keep it secret. *P* is user's secret key.

To prove the knowledge of *P* the user executes *l* times the following protocol:

1. The prover selects a random $\omega \in Z/nZ$, evaluates $c := S(\omega)$ and sends *c* to the verifier;
2. The verifier sends to the prover a random bit *b*;
3. If $b = 0$ the prover reveals $t = \omega$ and the verifier checks $S(t) = c$;

   If $b = 1$ the prover reveals $t = R(\omega)$ and the verifier checks $Q(t) = c$.

Figure 1: A simple identification protocol.

3.2 A Diffie – Hellman Like Key Agreement Protocol based on PMCP

Based on the property (2) we can deduce that the polynomials defined as $S := P^{(k)}$ - with *k* a big integer $1 < k \leq n-1$ where *n* is an RSA modulus and $S, P \in Z/nZ[X]$ - define an abelian finite group regarding to the polynomial composition.

This property allows us to devise the following key agreement protocol:

SUMMARY: A and B each send the other one message over on open channel.
RESULT: shared secret K known to both parties A and B.

1. *One-time setup.* An RSA modulus *n*, an $\omega \in Z/nZ$ and a polynomial $P \in (Z/nZ)[X]$ are selected and published.
2. *Protocol messages.*

   $A \rightarrow B: \quad P^{(l)}(\omega) \bmod n \qquad (i)$

   $B \rightarrow A: \quad P^{(r)}(\omega) \bmod n \qquad (ii)$

3. *Protocol actions.*

Perform the following steps each time a shared key is required.

(a) A chooses a random secret *l*, $1 < l \leq n-2$, and sends B the message (*i*).
(b) B chooses a random secret *r*, $1 < r \leq n-2$, and sends A the message (*ii*).

(c) B receives $P^{(l)}(\omega)$ and computes the shared key as $K = P^{(r)}\left(P^{(l)}(\omega)\right)\bmod n$

(d) A receives $P^{(r)}(\omega)$ and computes the shared key as $K = P^{(l)}\left(P^{(r)}(\omega)\right)\bmod n$.

Note that in the set scenario, the polynomial $P \in (Z/nZ)[X]$ is known but the big integers *l* and *r* are secret. An adversary tapping the communication between A and B can catch the messages of type (*i*) and (*ii*) sent between the two parties. The adversary can also calculate $P(\omega)$ as *P* and ω are public. Nevertheless, in order to determine the values *l* and *r* and therefore to be able to determine the shared key *K*, she will have to solve a problem equivalent to the discrete logarithm problem, which is known as being hart.

4 CONCLUSIONS AND FUTURE WORK

The present paper introduced a new cryptographic primitive called Polynomial Multi – Composition Problem. We shown that this polynomial class define a commutative group towards polynomial composition. This propriety gave us the possibility to define a key exchange protocol. A zero-knowledge identification scheme based on the mentioned primitive was also presented.

It is interesting to note that the Polynomial Composition Problem gives a general framework for studying a wider class of cryptographic primitives. We believe that a deeper study of the Polynomial Composition Problem could lead to a better understanding of the actual cryptographic problems.

REFERENCES

M. Bellare and P. Rogaway, 1993, Random Oracles are Practical: A Paradigm for Designing Efficient Protocols. In Proceedings of the 1st ACM-CCS, pages 62-73. ACM Press, New York.

W. Diffie and M. Hellman, 1976, New Directions in Cryptography, IEEE Trans. Info. Theory 22(6), pages 644–654.

Marc Joye, David Naccache, and Stéphanie Porte, 2004, The Polynomial Composition Problem in (Z/nZ)[X], Article retrieved April 3, 2007 from http://citeseer.ist.psu.edu/joye04polynomial.html.

Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanderstone, 1997, *Handbook of Applied Cryptography*, CRC Press.

RSA report “Recent Results on OAEP Security, study retrieved May 27, 2007 from ”http://www.rsa.com/rsalabs/node.asp?id=2147.