Future Generation Computer Systems 30 (2014) 91–97

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Towards provably secure proxy signature scheme based on Isomorphisms of Polynomials[☆]

Shaohua Tang[*], Lingling Xu

School of Computer Science and Engineering, South China University of Technology, Guangzhou 510640, China

HIGHLIGHTS

- We propose a proxy signature scheme based on IP (Isomorphism of Polynomials) problem.
- An attractive advantage is to potentially resist attacks of quantum computers.
- Our scheme is proven strictly to be secure through a formal security proof.
- This is a valuable attempt to explore the provable security in the area of MPKC.
- Our scheme is implemented in C/C++ and the performance shows that it is efficient.

ARTICLE INFO

Article history:
Received 29 December 2012
Received in revised form
2 May 2013
Accepted 6 June 2013
Available online 19 June 2013

Keywords:
Post-Quantum Cryptography
Multivariate Public Key Cryptography
Isomorphism of Polynomials
Proxy signature
Provable security

ABSTRACT

Proxy signatures are important cryptosystems that are widely adopted in different applications. Most of the proxy signature schemes so far are based on the hardness of integer factoring, discrete logarithm, and/or elliptic curve. However, Peter Shor proved that the emerging quantum computers can solve the problem of prime factorization and discrete logarithm in polynomial time, which threatens the security of current RSA, ElGamal, ECC, and the proxy signature schemes based on these problems. We propose a proxy signature scheme based on the problem of Isomorphism of Polynomials (IP) which belongs to a major category of Multivariate Public Key Cryptography (MPKC). The most attractive advantage of our scheme should be its feature to potentially resist the future quantum computing attacks. A formal security proof is also given, which shows that our scheme can reach *Existential Unforgeability under an Adaptive Chosen Message Attack with Proxy Key Exposure* assuming that the underlying IP signature is *Existential Unforgeability under an Adaptive Chosen Message Attack*. It is a valuable attempt to explore the provable security in the area of MPKCs. The scheme is implemented in C/C++ programming language, and the performance shows that the scheme is efficient. The parameters we choose can let the security level of our implementation up to $2^{86.59}$.

1. Introduction

A proxy signature protocol allows an entity, called original signer or delegator, to delegate another entity, called a proxy signer, to sign messages on behalf of the original signer. The first efficient proxy signature was introduced in [1,2]. The types of delegation can be classified into full delegation, delegation by warrant, partial delegation and partial delegation with warrant [3]. A considerable number of proxy signature schemes have been constructed for each of these delegation types, as shown in [4]. Proxy signatures have found numerous practical applications, particularly in distributed computing where delegation of rights is quite common, for example, grid computing, mobile agent applications, and mobile communications. The basic proxy signature has been extended to own various features, for example, threshold proxy signatures [5], blind proxy signatures [6], anonymous proxy signatures [7], etc.

Almost all the proxy signature schemes so far are based on the difficulty problem of integer factoring, discrete logarithm, and/or elliptic curve. However, Peter Shor [8] proved that the emerging quantum computers can solve the problem of prime factorization and discrete logarithm in polynomial-time, which threatens the security of current RSA, ElGamal, DSA, ECC, and proxy signature schemes based on these problems.

In order to resist the attacks of quantum computing, the Post-Quantum Cryptography has attracted cryptographers' intensive attentions. Some cryptosystems, such as hash-based cryptography,

[☆] The material in this paper was presented in part at the 6-th International Conference on Network and System Security (NSS'2012) [25], Nov 2012.

[*] Corresponding author. Tel.: +86 2087114942.
E-mail addresses: csshtang@scut.edu.cn, shtang@IEEE.org (S. Tang), csllxu@scut.edu.cn (L. Xu).

0167-739X/$ – see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.future.2013.06.003

coding-based cryptography, lattice-based cryptography, and Multivariate Public Key Cryptography (MPKC), belong to the area of Post-Quantum Cryptography [9].

The security of MPKC is based on the hardness of solving a set of multivariate polynomial equations over a finite field, which is proven to be an NP-hard problem [10], and quantum computers do not appear to have any advantages when dealing with this NP-hard problems. A lot of research has already been focused on MPKCs, for example, a group signature based on MPKC was proposed in [11], a fast hardware implementation of MPKC was presented in [12], etc. Cryptosystem based on the problem of Isomorphism of Polynomials (IP) is a major category of MPKC. Therefore, our proposed proxy signature scheme based on IP problem has the potential advantage of resisting the attacks of future quantum computers.

1.1. Our contribution

After the introduction of the problem of Isomorphism of Polynomials, we simplify Patarin's signature algorithm [13] based on IP problem to become a compact and workable digital signature scheme that we call IP signature.

Then we propose a proxy signature scheme based on IP signature, which includes the stages of initialization, delegation and proxy key generation, generation of proxy signature, and verification of proxy signature.

After that, we present a strict security proof for our proxy signature scheme under the assumption that the underlying IP signature is secure. More concretely, if we assume that the underlying IP signature is *Existential Unforgeability under an Adaptive Chosen Message Attack* (euf-cma), then our proxy signature scheme is *Existential Unforgeability under an Adaptive Chosen Message Attack with Proxy Key Exposure* (ps-uf-pke).

Finally, we implement the scheme in C/C++ programming language. The performance shows that our scheme can run efficiently, and our chosen parameters can let the security level of the implementation up to $2^{86.59}$.

1.2. Organization

The rest of the paper is organized as follows. In Section 2, we introduce the problem of Isomorphisms of Polynomials and IP signature scheme. In Section 3, we present the security model in which we will prove our proxy signature scheme. Then the proposed proxy signature scheme based on IP signature is described in Section 4. We present the security proof of our scheme in Section 5. The implementation and performance of our scheme are described in Section 6. Finally, the conclusion is summarized in Section 7.

2. Preliminaries

Some basic building blocks adopted by our scheme are introduced in this section, which includes the problem of Isomorphism of Polynomials (IP), the signature algorithm based on IP, and the procedure to verify the IP signature.

2.1. Problem of Isomorphism of Polynomials

The problem of Isomorphism of Polynomials was introduced in [13]. It is a fundamental problem of multivariate public key cryptography, since it is related to the hardness of key recovery of such cryptosystems. The concept of IP is briefly described as follows. For more details, we refer the reader to [13].

Let K be a finite field, and all the arithmetic operations hereafter are over this field. Let n and u be positive integers. Let A be a set of u quadratic equations with n variables $x_1, \ldots, x_n$ that give y values from x values:

$$y_k = \sum_i \sum_j \gamma_{ijk} x_i x_j + \sum_i \mu_{ik} x_i + \delta_k, \quad \text{for } k = 1, \ldots, u. \tag{1}$$

Let B be a set of u quadratic equations with n variables $x'_1, \ldots, x'_n$ that give y' values from x' values:

$$y'_k = \sum_i \sum_j \gamma'_{ijk} x'_i x'_j + \sum_i \mu'_{ik} x'_i + \delta'_k, \quad \text{for } k = 1, \ldots, u. \tag{2}$$

Let S be a bijective affine transformation of variables $y_1, \ldots, y_u$, which is defined by

$$S(y_1, \ldots, y_u) = (y'_1, \ldots, y'_u); \tag{3}$$

and T be a bijective affine transformation of variables $x'_1, \ldots, x'_n$, which is defined by

$$T(x'_1, \ldots, x'_n) = (x_1, \ldots, x_n). \tag{4}$$

If there exists such transformation pair (S, T) which satisfies $B = S \circ A \circ T$, then we call A and B are *"isomorphic"*, and the bijective affine transformation pair (S, T) is an *"isomorphism"* from A to B.

Definition 1 (*IP Problem*). The *Problem of Isomorphism of Polynomials* (abbreviated *IP problem*) is the problem to find an isomorphism (S, T) from A to B, where A and B are two public sets of u quadratic equations, and A and B are isomorphic.

2.2. Security of IP problem and MPKCs

2.2.1. Provable security of MPKCs

In the aspect of provable security of MPKCs, a lot of researchers have paid intensive attention on it, which is to prove that a given MPKC is indeed secure with some reasonable theoretical assumptions. Some security models, for example random oracle model and standard model, can be adopted to formally prove the security of traditional cryptosystems based on integer factoring, discrete logarithm, and/or elliptic curve. However, these security models cannot be directly applied to MPKCs. Even though there have been some works related to this area, for example [14–17], there is still little essential progress in this topic. Therefore, the most common ways to analyze the security of MPKCs are to launch the existing effective attacks against the targeted MPKC to test its ability to resist these attacks.

2.2.2. Security of IP problem

Cryptosystems based on IP problem belong to a major category of Multivariate Public Key Cryptosystems (MPKCs). Many researchers have been devoting their efforts to solve the IP problem in an efficient way. The "To and Fro" technique proposed in [18] is a significant approach to solve the IP problem, which assumes the ability to invert the polynomial systems, and has an exponential complexity. Moreover, the authors gave an upper bound on the theoretical complexity of IP problem. But [15] pointed out that the proof in [18] is not complete. They gave an upper bound on the theoretical complexity of "IP-like" problems, and presented a new algorithm to solve IP problem when S and T are linear mappings. An improved algorithm proposed in [19] integrates some new techniques, and claims to get the best result on the state of the art.

An important special case of IP is the IP problem with one secret (IP1S for short). Although most of the algorithms for IP can be applied to IP1S almost directly, several more efficient algorithms are proposed to solve IP1S problem.

The algorithm to solve IP1S proposed in [20] conducts an exhaustive search to find the solutions of an algebraic system of equations. Later, Levy-dit-Vehel and Perret improved it by using the Gröbner basis computation in [21]. Perret presented a new approach for solving IP1S using the Jacobian matrix in [22], and