Future Generation Computer Systems 52 (2015) 116–124

Contents lists available at ScienceDirect

Future Generation Computer Systems

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

Efficient hardware implementation of PMI+ for low-resource devices in mobile cloud computing☆

Shaohua Tang [a,*], Bo Lv [a], Guomin Chen [a], Zhiniang Peng [a], Adama Diene [b], Xiaofeng Chen [c]

[a] School of Computer Science and Engineering, South China University of Technology, China
[b] Department of Mathematical Sciences, United Arab Emirates University, United Arab Emirates
[c] School of Telecommunications Engineering, Xidian University, China

HIGHLIGHTS

- We design a hardware to implement MQ asymmetric cipher PMI+ for low-resource devices.
- Basic arithmetic units are implemented in optimized and full parallel.
- Our design can complete a large power operation in 16 clock cycles.
- Our hardware can complete an encryption operation of PMI+ within 497 clock cycles, and a decryption operation within 438 clock cycles.
- Our design has a good performance in cycle-area products.

ARTICLE INFO

Article history:
Received 30 June 2014
Received in revised form
12 October 2014
Accepted 14 November 2014
Available online 24 November 2014

Keywords:
Multivariate Quadratic (MQ) public key algorithm
PMI+ encryption and decryption
Hardware implementation
Mobile cloud computing
Low-resource devices
Optimized large power operation

ABSTRACT

With rapid development of cloud computing, security issues have gained more and more attention, especially in mobile cloud computing environment. Smart phones and other mobile devices provide a lot of convenience to us, but due to its intrinsic low-resource limitation, it also causes many security problems. In this paper, we design a hardware that can efficiently implement PMI+, which is a Multivariate Quadratic (MQ) asymmetric cipher, for low-resource devices in mobile cloud computing. Our main contributions are that, firstly, hardware architectures of encryption and decryption of PMI+ are developed, and descriptions of corresponding hardware algorithm are proposed; secondly, basic arithmetic units are implemented with higher efficiency that multiplication, squaring, vector dot product and power operation are implemented in full parallel; and thirdly, optimized implementations for core modules, including optimized large power operation, are achieved. The encryption and decryption hardware of PMI+ is efficiently realized on FPGA by the above optimization and improvement. It is verified by experiments that the designed hardware can complete an encryption operation within 497 clock cycles, and the clock frequency can be up to 145.60 MHz, and the designed hardware can complete a decryption operation within 438 clock cycles wherein the clock frequency can be up to 132.21 MHz. Our experiment results also confirm that our design can be deployed in low-resource devices as thin client of mobile cloud computing.

1. Introduction

Security is one of the most significant barriers to faster and more widespread adoption of cloud computing, which has become the focus that many researchers care [1–6]. Thin client technology has been widely used in cloud computing. However, due to the limitation of resources, computation and data processing are usually performed in the clouds. It is not hard to predict that connecting mobile devices to the cloud will become mainstream in the coming days. When users use cloud applications or cloud services, data transmission is engaged. In order to preserve the privacy of sensitive data, mobile device itself requires not only basic security handling capacity and defense capabilities, but also public key cryptographic processing capabilities. Public key cryptography has played an important role in modern communication and computer networks. The public key cryptography, which is used widely, mainly includes RSA that is based on integer factorization problem, ElGamal that is based on discrete logarithm problem, and elliptic curve cryptography, etc. In order to adapt various

☆ The material in this paper was presented in part at the 10th International Conference on Information Security Practice and Experience (ISPEC'2014) (Tang et al., (2014) [38]), May 2014.

* Corresponding author.
E-mail addresses: csshtang@scut.edu.cn, shtang@IEEE.org (S. Tang).

http://dx.doi.org/10.1016/j.future.2014.11.014
0167-739X/

occasions, many efficient hardware implementations are proposed by researchers [7–17]. However, traditional public key cryptography, such as RSA, is not suitable for low-resource mobile devices, because of its large amount of calculation and high power requirements.

The quantum algorithm of P. Shor is able to solve the integer factorization and discrete logarithm problem in polynomial time, including a computation problem in elliptic curve field. As a result, it directly threatens classical cryptosystems based on hard problems of number theory, and which helps to drive the development of post quantum cryptography. The post quantum cryptography can be divided into four categories: signature schemes based on hash function [18], lattice-based public key cryptosystem [19], public key cryptosystem based on error correcting code [20] and multivariate public key cryptosystem [21]. The research for post quantum cryptography is growing rapidly and many hardware and embedded system implementations of the post quantum cryptography appear in order to adapt various occasions [22–29].

MPKCs have advantages in low-resource devices with its low-power and high speed computation. PMI+ [30] is one kind of multivariate public key cryptosystem, and is a variant of MI [31]. Ding enhanced the security of MI by adding an internal perturbation to the central map of MI in 2004, to produce a new variant of the MI cryptosystem which is called PMI cryptosystem [32]. However, the PMI cryptosystem has been broken by differential cryptanalysis by Fouque et al. [33] in 2005. Ding introduced a new external perturbation to the central mapping of MI [30] in 2006, to produce PMI+ cryptosystem whose security has been greatly improved. In this paper, we design an efficient PMI+ hardware implementation which works fine for low-resource devices under mobile cloud computing environment.

The material in this paper was presented in part at the 10th International Conference on Information Security Practice and Experience (ISPEC'2014) (Tang et al., (2014) [38]), May 2014.

1.1. Our contribution

In this paper, we design a hardware that can efficiently implement PMI+ for low-resource devices in mobile cloud computing.

Firstly, hardware architectures of encryption and decryption of PMI+ are developed, and descriptions of corresponding hardware algorithm are proposed.

Secondly, basic arithmetic units are implemented with higher efficiency that multiplication, squaring, vector dot product and power operation are implemented in full parallel, wherein compared with a full parallel multiplier, a full parallel squarer takes up about one-twentieth of the logical units and has shorter latency.

Thirdly, we implement an optimized large power operation which, compared with the general power operation, has the ability to reduce 4288 cycles at most in one process of decryption, with an obvious optimization. The encryption and decryption hardware of PMI+ is efficiently realized on FPGA by the above optimization and improvement.

Our experiments verify that if parameters are selected as $(n, q, \theta, r, a) = (84, 2, 4, 6, 14)$, the length of a plaintext block is 84 bits and the length of a ciphertext block is 98 bits. Our designed hardware can complete an encryption operation within 497 clock cycles or 3.42 μs, wherein the clock frequency can be up to 145.60 MHz, and our designed hardware can complete a decryption operation within 438 clock cycles or 3.31 μs, wherein the clock frequency can be up to 132.21 MHz.

1.2. Organization

The rest of this paper is organized as follows. The theory of PMI+ scheme, including principles of encryption and decryption algorithms, and the choice of parameters, is briefly introduced in Section 2. Section 3 primarily focuses on hardware design and implementation of PMI+, including hardware structure design, algorithm description, and implementation of basic arithmetic units and hardware core modules. Our experimental results, performance, and comparisons with other public key crypto systems are given in detail in Section 4. Section 5 is the conclusion of this paper, which summarizes the main contributions of this paper and proposes further research directions.

2. Preliminaries

We describe the basic theory of the encryption and decryption of PMI+ [30] in this section. The basic idea of PMI+ is adding an internal perturbation and an external perturbation to the central map of MI scheme to resist linearization equation attack and differential attack. The ciphertext encrypted by PMI+ encryption scheme is unique, and it can be used to construct a multivariate public key signature scheme.

2.1. Notations for PMI+

Let k be a finite field of characteristic two and cardinality q, K be an extension of degree n over k. Let $\varphi : K \to k^n$ defined by $\varphi(a_0 + a_1x + \cdots + a_{n-1}x^{n-1}) = (a_0, a_1, \ldots, a_{n-1})$.

Fix θ so that $\gcd(q^\theta + 1, q^n - 1) = 1$ and define $\tilde{F} : K \to K$ by $\tilde{F}(X) = X^{1+q^\theta}$. Then F is invertible and $\tilde{F}^{-1}(X) = X^t$, where $t(1 + q^\theta) \equiv 1 \bmod (q^n - 1)$.

Define the map $F' : k^n \to k^n$ by $F'(x_1, \ldots, x_n) = \varphi \circ \tilde{F} \circ \varphi^{-1}(x_1, \ldots, x_n)$.

Fix a small integer r and randomly choose r invertible affine linear functions $z_1, \ldots, z_r$, written as $z_j(x_1, \ldots, x_n) = \sum_{i=1}^{n} \alpha_{ij}x_i + \beta_j$, for $j = 1, \ldots, r$. This defines a map $Z : k^n \to k^r$ by $Z(x_1, \ldots, x_n) = (z_1, \ldots, z_r)$. The map Z is the source of the internal perturbation.

Randomly choose n quadratic polynomials $\hat{f}_1, \ldots, \hat{f}_n \in k[z_1, \ldots, z_r]$. The $\hat{f}_i$ define a map $\hat{F} : k^r \to k^n$ by $\hat{F}(z_1, \ldots, z_r) = (\hat{f}_1, \ldots, \hat{f}_n)$. Let P be the set consisting of the pairs (λ, μ), where λ is a point that belongs to the image of $\hat{F}$ and μ is the set of pre-images of λ under $\hat{F}$.

Define an internal perturbation map by $F^*(x_1, \ldots, x_n) = \hat{F} \circ Z(x_1, \ldots, x_n) = (f_1^*, \ldots, f_n^*)$. Define a map by $F(x_1, \ldots, x_n) = (F' + F^*)(x_1, \ldots, x_n)$.

Randomly choose a non-linear equations on $x_1, \ldots, x_n$ for the central map F as external perturbation. Randomly choose an invertible affine map L_1 in $n + a$ dimensional vector space k^{n+a}, randomly choose an invertible affine map L_2 in n dimensional vector space k^n, and $\bar{F}(x_1, \ldots, x_n) = L_1 \circ F \circ L_2(x_1, \ldots, x_n)$ is a public key of PMI+, and the private key includes the central map F', the map $\hat{F}$, Z, L_1^{-1} and L_2^{-1}.

2.2. PMI + encryption

For a given plaintext block $(x_1, \ldots, x_n)$, when encrypting the plaintext, it only needs to apply the plaintext into the public key polynomials

$$\begin{aligned} y_1 &= \bar{f}_1(x_1, x_2, \ldots, x_n), \\ &\ldots \\ y_{n+a} &= \bar{f}_{n+a}(x_1, x_2, \ldots, x_n), \end{aligned} \tag{1}$$

to calculate the evaluation of $n + a$ quadratic polynomials that a ciphertext $(y_1, \ldots, y_{n+a})$ can be acquired.

2.3. PMI + decryption

The decryption algorithm of PMI+ is more complicated. For a given ciphertext block $(y_1, \ldots, y_{n+a})$, the decryption of the