Public-Key Encryption Based on Matrix Diagonalization Problem

Jiande Zheng

Department of Computer Science, Xiamen University, Xiamen 361005, P. R. China

Abstract. A research on the development of a new public-key encryption scheme based on matrix diagonalization problem over a ring of algebraic integers is reported in this paper. The research is original, although it is still in its early stage. The new public key encryption algorithm has three original features that distinguish it from existing ones: (a) it works on an infinite field instead of a Galois field; (b)it recognizes the ability of adversaries to factor big integers; (c) it requires only simple (without modulus) additions and multiplications for message encryption and decryption, no high-order exponentiation is required.

1 Introduction

The idea of inventing new public key cryptographies by exploring the matrix diagonalization problem (MDP) was first suggested in [1]. The original encryption system was implemented with modulo-p addition and multiplications, where p is a big prime, which was broken due to the fact that the characteristic polynomial of the public key matrix can be factored efficiently over GF(p) using Cantor-Zassenhaus algorithm [2]. Improved public key encryption and digital signature schemes were developed later with the same idea, but with the underlying algebraic setting selected differently as Zn, the ring of integers with modulo-n addition and multiplication, where n is an RSA modulus [3][4]. The new selection links MDP to integer factorization problem (IFP). In fact, diagonalizing a 2×2 matrix over Zn is equivalent to solving a modulo-n quadratic equation, or inverting the Rabin public key function [5], which is a proven hard problem.

The purpose of this paper is to report the further research on developing an encryption scheme based on MDP over yet another algebraic setting, which is an infinite field instead of a Galois field, as is the case with almost all existing schemes. Since factoring a polynomial over the specially formulated algebraic setting is a brand new crypto problem, the complexity of which is still under study. However, we have made important progress on this aspect, which will be presented in this paper.

Zheng J. (2005).
Public-Key Encryption Based on Matrix Diagonalization Problem.
In *Proceedings of the 3rd International Workshop on Security in Information Systems*, pages 102-112
DOI: 10.5220/0002543101020112

2 The new encryption scheme

2.1 The algebraic setting

First, we choose a big composite integer, denoted n, which is a product of a large number of primes. Let p and q be two secret divisors of n, pq=n, a ring of algebraic integers, denoted Ω, can be defined as

$$\Omega = \{\sqrt{\omega_1 + \omega_2\sqrt{n}} : \omega_1 = \alpha_1^2 p + \alpha_2^2 q, \omega_2 = 2\alpha_1\alpha_2,\ \alpha_1, \alpha_2 \in R[\sqrt{s}]\} \tag{1}$$

where

$$R[\sqrt{s}] = \{z_3^{-1}(z_1 + z_2\sqrt{s}):\ z_1, z_2 \in \pm Z, z_3 \in Z^*\}, \tag{2}$$

s is an integer, $\sqrt{s}$ is an irrational number, Z stands for the ring of integers,

$$\pm Z = \{0, \pm 1, \pm 2, \pm 3, ...\},$$
$$Z^* = \{1, 2, 3, ...\}.$$

Another algebraic setting, denoted *Π*, can be defined with *Ω*,

$$\Pi = \{\pi_1 + \pi_2, \pi_1 \in \Omega, \pi_2 \in R[\sqrt{s}, \sqrt{n}]\} \tag{3}$$

where

$$R[\sqrt{s}, \sqrt{n}] = \{r_1 + r_2\sqrt{n}:\ r_1, r_2 \in R[\sqrt{s}]\} \tag{4}$$

It is easily verified that $R[\sqrt{s}, \sqrt{n}]$ is a field under normal addition and multiplication. Meanwhile, one notices that (1) can be rewritten as

$$\Omega = \{\alpha_1\sqrt{p} + \alpha_2\sqrt{q}:\ \ \alpha_1, \alpha_2 \in R[\sqrt{s}]\} \tag{5}$$

for any

$$u = u_1\sqrt{p} + u_2\sqrt{q} \in \Omega,$$
$$v = v_1\sqrt{p} + v_2\sqrt{q} \in \Omega,$$

$$w = w_1 + w_2\sqrt{n} \in \mathbf{R}[\sqrt{s},\sqrt{n}] \ ,$$

one obtains

$$\begin{aligned} uv &= (u_1\sqrt{p} + u_2\sqrt{q})(v_1\sqrt{p} + v_2\sqrt{q}) \\ &= vu = (v_1\sqrt{p} + v_2\sqrt{q})(u_1\sqrt{p} + u_2\sqrt{q}) \\ &= (u_1v_1p + u_2v_2q) + (u_1v_2 + u_2v_1)\sqrt{n} \in \mathbf{R}[\sqrt{s},\sqrt{n}], \end{aligned}$$

and

$$\begin{aligned} uw &= u(w_1 + w_2\sqrt{n}) \\ &= wu = (w_1 + w_2\sqrt{n})u \\ &= w_1u + w_2u\sqrt{n} \\ &= w_1u + w_2\sqrt{pq}(u_1\sqrt{p} + u_2\sqrt{q}) \\ &= w_1u + w_2(u_1p\sqrt{q} + u_2q\sqrt{p}) \in \Omega. \end{aligned}$$

One notices from the above discussions that Π is closed under ordinary addition and multiplication. Further more, let $\xi = \xi_1 + \xi_2 \in \Pi$, where $\xi_1 \in \Omega, \xi_2 \in R[\sqrt{s},\sqrt{n}]$, one also obtains from the above discussion

$$\xi_1^2, \xi_2^2 \in R[\sqrt{s},\sqrt{n}] \ ,$$

and

$$(\xi_1 + \xi_2)(\xi_1 - \xi_2) = \xi_1^2 - \xi_2^2 \in R[\sqrt{s},\sqrt{n}] \ ,$$

which is invertible within $R[\sqrt{s},\sqrt{n}]$, and

$$(\xi_1^2 - \xi_2^2)^{-1}(\xi_1 - \xi_2) \in R[\sqrt{s},\sqrt{n}]$$

gives the inverse of $\xi = \xi_1 + \xi_2$ in Π . So we conclude that Π is also a field under normal addition and multiplication.

There are 168 primes between 1 and 1000[6], we suggest that n be selected as 150 primes among them, so that $n < (1000)^{150} = 10^{450} < 2^{1500}$, the size of which will be comparable with that of widely used RSA modulus[7].

2.2 The keys

The private key for the encryption scheme is given by

$$\mathbf{H} = \begin{bmatrix} \lambda_1^{r-1} & \lambda_2^{r-1} & \lambda_3^{r-1} & \lambda_4^{r-1} & \ldots & \lambda_r^{r-1} \\ \lambda_1^{r-2} & \lambda_2^{r-2} & \lambda_3^{r-2} & \lambda_4^{r-2} & \ldots & \lambda_r^{r-2} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ \lambda_1^{2} & \lambda_2^{2} & \lambda_3^{2} & \lambda_4^{2} & \ldots & \lambda_r^{2} \\ \lambda_1 & \lambda_2 & \lambda_3 & \lambda_4 & \ldots & \lambda_r \\ 1 & 1 & 1 & 1 & \ldots & 1 \end{bmatrix} \qquad \textbf{(6)}$$

where

$$\begin{aligned} \lambda_1, \lambda_2, \ldots\lambda_r \in \{ & \sqrt{\omega_{11} + \omega_{12}\sqrt{s} + (\omega_{21} + \omega_{22}\sqrt{s})\sqrt{n}} + \\ & + \omega_{31} + \omega_{32}\sqrt{s} + (\omega_{41} + \omega_{42}\sqrt{s})\sqrt{n}, \\ & \omega_{1}, \omega_{12}, \omega_{21}, \omega_{22}, \omega_{31}, \omega_{32}, \omega_{41}, \omega_{42} \in Z\} \subset \mathit{\Pi}, \end{aligned}$$

r>4, while the public key is given by

$$\mathbf{A} = \begin{bmatrix} \sigma_1 & -\sigma_2 & \sigma_3 & -\sigma_4 & \ldots & (-1)^{r-1}\sigma_r \\ 1 & & & & & \\ & 1 & & & & \\ & & 1 & & & \\ & & & 1 & & \\ & & & & 1 & \end{bmatrix} \qquad \textbf{(7)}$$

where σ_1 , σ_2, ...σ_r are algebraic integers computed from λ_1, λ_2,... λ_r using the following equations:

$$\begin{aligned} &\sigma_1 = \sum_{i=1}^{r} \lambda_i, \\ &\sigma_2 = \sum_{i=1}^{r} \sum_{j=i+1}^{r} \lambda_i \lambda_j, \\ &\sigma_3 = \sum_{i=1}^{r} \sum_{j=i+1}^{r} \sum_{k=j+1}^{r} \lambda_i \lambda_j \lambda_k, \ldots \\ &\ldots\ldots \\ &\sigma_r = \lambda_1 \lambda_2 \lambda_3 \ldots \lambda_{r-1} \lambda_r. \end{aligned}$$

We have [8]

$$A = H diag(\lambda_1, \lambda_2, ...\lambda_r) H^{-1} (\bmod n) \tag{8}$$

Note that the private key can be represented by *(λ_1, λ_2,...λ_r)*, while the public key can be represented by *(σ_1 , σ_2, ...σ_r)*.

2.3 The trap-door one-way function

The following trap-door one-way function is used for message encryption in this paper:

$$f(x_1, x_2, ...x_r) = (x_1 \boldsymbol{A}^{r-1} + x_2 \boldsymbol{A}^{r-2} + ... + x_r \boldsymbol{I})^2 \boldsymbol{b},\ x_1, x_2, ...x_r \in \Pi \tag{9}$$

where $\boldsymbol{b} = [b_1 \quad b_2 \quad ... \quad b_r]^T$ is an r×1 matrix, the elements of which can be computed as $b_i = tr(\boldsymbol{A}^{r-i}),\ i = 1, 2, ...r$, so that

$$\boldsymbol{b} = \boldsymbol{H}[1 \quad 1 \quad ... \quad 1]^T \tag{10}$$

2.4 Message encryption

The encrypting process is divided into the following three steps

Step 1 Create *r* random numbers in *Ω*. These numbers, denoted $x_1, x_2, ...x_r$, can be computed from the public key as

$$\begin{aligned} &x_1 = (k_1\sigma_1 + \sigma_2 ... + \sigma_r)^{16}, \\ &x_i = (k_1\sigma_1 + k_2\sigma_2 ... + k_i\sigma_i)x_{i-1},\ i = 2, 3, ..r-1, \end{aligned} \tag{11}$$

and

$$x_r = \psi_1(x_1, x_2, ..x_{r-1}) \tag{12}$$

where $k_1, k_2, ... k_r$ are random numbers in $R[\sqrt{s}]$, ψ_1 is a publicly known one-way function, which can be made as the combination of a hash function with some arithmetic operations.

Step 2 Compute the first component of the cipher-text, denoted $\boldsymbol{y}$, which is an r×1 matrix obtainable from the public key function:

$$\boldsymbol{y} = (x_1\boldsymbol{A}^{r-1} + x_2\boldsymbol{A}^{r-2} + ... + x_r\boldsymbol{I})^2\boldsymbol{b} \tag{13}$$

Step 3 Compute the second component of the cipher-text, denoted z, which is an integer,

$$z = m\psi_2(x_1, x_2, ..x_r) \tag{14}$$

where m is the message, ψ_2 is a publicly known one-way function similar to ψ_1. The full cipher text of m is given by ($\boldsymbol{y}$, z).

2.5 Message decryption

One notices that (13) can be reduced to a univariate quadratic equation by multiplying the inverse of $\boldsymbol{H}$ on both sides of the equation. We have

$$\begin{aligned}\boldsymbol{H}^{-1}\boldsymbol{y} &= \boldsymbol{H}^{-1}(x_1\boldsymbol{A}^{r-1} + x_2\boldsymbol{A}^{r-2} + ... + x_r\boldsymbol{I})^2\boldsymbol{H}\boldsymbol{H}^{-1}\boldsymbol{b} \\ &= [x_1(\boldsymbol{H}^{-1}\boldsymbol{A}\boldsymbol{H})^{r-1} + x_2(\boldsymbol{H}^{-1}\boldsymbol{A}\boldsymbol{H})^{r-2} + ... + x_r\boldsymbol{I})^2\boldsymbol{H}^{-1}\boldsymbol{b},\end{aligned} \tag{15}$$

where

$$\boldsymbol{H}^{-1}\boldsymbol{A}\boldsymbol{H}(\bmod n) = diag(\lambda_1, \lambda_2, ...\lambda_r),$$

which is an alternative form of (8). Let $\boldsymbol{H}^{-1}\boldsymbol{y} = \begin{bmatrix}\delta_1 & \delta_2 & ... & \delta_r\end{bmatrix}^T$,

$$\mu_i = x_1\lambda_i^{r-1} + x_2\lambda_i^{r-2} + ... + x_r, \, i = 1, 2, ...r \tag{16}$$

where $\mathbf{x} = \begin{bmatrix}x_1 & x_2 & ... & x_r\end{bmatrix}^T$, and equation (15) can be reduced to

$$\begin{aligned}[\delta_1 \quad \delta_2 \quad \dots \quad \delta_r]^T &= diag\,(\mu_1^2, \mu_2^2, \dots \mu_r^2)[1 \quad 1 \quad \dots \quad 1]^T \\ &= [\mu_1^2 \quad \mu_2^2 \quad \dots \quad \mu_r^2]^T,\end{aligned}$$

which can be further rewritten as

$$\delta_i = \mu_i^2, i = 1, 2, \dots r \tag{17}$$

The above equations are readily solved, the solutions of which are given by

$$\mu_i = \pm\sqrt{\delta_i}, i = 1, 2, \dots r \tag{18}$$

Meanwhile, one obtains from (6) and (16)

$$[\mu_1 \quad \mu_2 \quad \dots \quad \mu_r] = \boldsymbol{x}^T \boldsymbol{H},$$

so we have

$$\mathbf{x}^T = [\mu_1 \quad \mu_2 \quad \dots \quad \mu_r]\mathbf{H}^{-1} \tag{19}$$

Note that 2^r possible solutions to (13) can be computed from (18) and (19), and (12) can be used to find out the correct one. The original message can then be recovered as

$$m = z[\psi_2(x_1, x_2, \dots x_r)]^{-1}.$$

3 Security of the encryption scheme

We study in this section two kinds of possible attacks on our encryption scheme. The first kind of attacks aims at recovering the secret key, while the second kind of attacks tries to crack the cipher texts.

3.1 Attacks aiming at recovering the private key

An adversary can recover ***H***, if and only if the adversary can diagonalize the corresponding public key ***A***, or factoring its characteristic polynomial

$$\phi(\lambda) = \det(\lambda \boldsymbol{I} - \boldsymbol{A}) = \lambda^{r} - \sigma_1 \lambda^{r-1} + \sigma_2 \lambda^{r-2} \ldots + (-1)^r \sigma_r \tag{\textbf{20}}$$

over *Π*. Since *Π* is an infinite field, the polynomial factoring algorithms that work well on Galois fields, such as the famous Cantor-Zassenhaus algorithm, will not work on it. According to Abel's theorem [9], it is also hard for the adversary to solve *φ(λ)=0* over *R*, the real number field, as this task is incapable of finite number of additions, multiplications and root extractions if *r>4*.

The adversary may also substitute

$$\lambda = \sqrt{\omega_{11} + \omega_{12}\sqrt{s} + (\omega_{21} + \omega_{22}\sqrt{s})\sqrt{n}} + \omega_{31} + \omega_{32}\sqrt{s} + (\omega_{41} + \omega_{42}\sqrt{s})\sqrt{n}$$

into (20) and transform *φ(λ)=0* over *Π* to

$$\begin{aligned} &\psi(\omega_1, \omega_{12}, \omega_{21}, \omega_{22}, \omega_{31}, \omega_{32}, \omega_{41}, \omega_{42}) \\ &= \phi(\sqrt{\omega_{11} + \omega_{12}\sqrt{s} + (\omega_{21} + \omega_{22}\sqrt{s})\sqrt{n}} + \omega_{31} + \omega_{32}\sqrt{s} + (\omega_{41} + \omega_{42}\sqrt{s})\sqrt{n}) \\ &= 0, \quad \omega_1, \omega_{12}, \omega_{21}, \omega_{22}, \omega_{31}, \omega_{32}, \omega_{41}, \omega_{42} \in Z, \end{aligned} \tag{\textbf{21}}$$

However, it is easily verified that (21) can not be broken into a small number of rational equations over *Z,* so this transformation can not reduce the complexity of recovering the private key.

The third method for key recovery is substituting

$$\begin{aligned} \lambda = (\alpha_{11} + \alpha_{12}\sqrt{s})\sqrt{p} + (\alpha_{21} + \alpha_{22}\sqrt{s})\sqrt{q} + \omega_{31} + \omega_{32}\sqrt{s} + (\omega_{41} + \omega_{42}\sqrt{s})\sqrt{n}, \\ \alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22}, \omega_{31}, \omega_{32}, \omega_{41}, \omega_{42} \in Z \end{aligned}$$

into (20), which will transform φ(λ)=0 over *Π* to eight polynomial equations of

$$\alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22}, \omega_{31}, \omega_{32}, \omega_{41}, \omega_{42}$$

over *Z*. This transformation makes it possible to recover the private key with existing polynomial factorization algorithms over finite fields. However *p* and *q*, the factors of *n*, should be found before the above method can be applied, and for this purpose we can not find any existing method that is more effective than enumeration. Suppose *n* is selected as a product of 150 different primes, and *p* is selected as the product of 70 prime factors of *n*, it takes maximal C_{150}^{70} tries for the adversary to find *p*. We have

$$C_{150}^{70} = 6.66 \times 10^{43} > 2^{129},$$

which is more than the number of all 128-bits symmetric keys.

3.2 Attacks aiming at cracking the cipher texts

We have studies three methods that may be used to solve (20). These methods may also be used to solve (13), in order to crack the cipher text directly. Complexity of applying the second and the third methods to (13) is the same as that of applying it to (20), while complexity of solving (13) over *R* depends heavily on that of reducing it into quartic or lower order univariate equations. The basic methods for the reduction are linear transformations, including linear eliminations and linear substitutions. We have the following proposition:

Proposition 1 Breaking (13) into univariate equations through linear transformations is as hard as finding the eigenvalues of $\boldsymbol{A}$.

Proof One may represent a scalar equation obtained from (13) through linear eliminations as

$$\boldsymbol{v}^T\boldsymbol{y} = \boldsymbol{v}^T(x_1\boldsymbol{A}^{r-1} + x_2\boldsymbol{A}^{r-2} + \ldots + x_r\boldsymbol{I})^2\boldsymbol{b},$$

where **v** is an r×1 matrix. Suppose the above equation can be turned into a univariate equation through linear substitution, there exist three scalars $\gamma_1, \gamma_2, \gamma_3$ and an r×1matrix **u**, so that $\varepsilon = \boldsymbol{u}^T\boldsymbol{x}$ satisfies

$$\boldsymbol{v}^T(x_1\boldsymbol{A}^{r-1} + x_2\boldsymbol{A}^{r-2} + \ldots + x_r\boldsymbol{I})^2\boldsymbol{b} - \boldsymbol{v}^T\boldsymbol{y} \equiv \gamma_1\varepsilon^2 + \gamma_2\varepsilon + \gamma_3 \qquad \textbf{(22)}$$

According to (8) and (10), the left side of (22) can be rewritten as

$$\begin{aligned} &\boldsymbol{v}^T(x_1\boldsymbol{A}^{r-1} + x_2\boldsymbol{A}^{r-2} + \ldots + x_r\boldsymbol{I})^2\boldsymbol{b} - \boldsymbol{v}^T\boldsymbol{y} \\ &= \boldsymbol{v}^T\boldsymbol{H}diag(\mu_1^2, \mu_2^2, \ldots\mu_r^2)\boldsymbol{H}^{-1}\boldsymbol{b} - \boldsymbol{v}^T\boldsymbol{y} \\ &= \boldsymbol{w}^T\begin{bmatrix}\mu_1^2 & \mu_2^2 & \ldots & \mu_2^2\end{bmatrix}^T - \boldsymbol{v}^T\boldsymbol{y} \\ &= w_1\mu_1^2 + w_2\mu_2^2 + \ldots + w_r\mu_r^2 - w_0, \end{aligned} \qquad \textbf{(23)}$$

where $w_0 = \boldsymbol{v}^T \boldsymbol{y}$, $\begin{bmatrix} w_1 & w_2 & \dots & w_r \end{bmatrix} = \boldsymbol{w}^T = \boldsymbol{v}^T \boldsymbol{H}$, $\|\boldsymbol{w}\| \neq 0$ since $\boldsymbol{H}$ is of full rank. Without loss of generality, we assume that $w_1 \neq 0$. Meanwhile one obtains from (19)

$$\varepsilon = \boldsymbol{u}^T \boldsymbol{x} = \boldsymbol{u}^T (\boldsymbol{H}^T)^{-1} \begin{bmatrix} \mu_1 & \mu_2 & \dots & \mu_r \end{bmatrix}^T = d_1\mu_1 + d_2\mu_2 + \dots + d_r\mu_r, \tag{24}$$

where $\begin{bmatrix} d_1 & d_2 & \dots & d_r \end{bmatrix}^T = \mathbf{H}^{-1}\mathbf{u}$. Substituting (23) and (24) into (22) gives

$$\begin{aligned} & w_1\mu_1^2 + w_2\mu_2^2 + \dots + w_r\mu_r^2 - w_0 \\ & \equiv \gamma_1(d_1\mu_1 + d_2\mu_2 + \dots + d_r\mu_r)^2 + \gamma_2(d_1\mu_1 + d_2\mu_2 + \dots + d_r\mu_r) + \gamma_3 \end{aligned} \tag{25}$$

and one obtains from the above equation

$$w_1 = \gamma_1 d_1^2, w_2 = w_3 \dots = w_r = d_2 = d_3 \dots = d_r = 0 .$$

So we have

$$\mathbf{v}^T \mathbf{H} = \begin{bmatrix} w_1 & w_2 & \dots & w_r \end{bmatrix} = \begin{bmatrix} w_1 & 0 & \dots & 0 \end{bmatrix} \tag{26}$$

which reveals the fact that $\boldsymbol{v}$ is a left eigenvector of $\boldsymbol{A}$, and an eigenvalue of $\boldsymbol{A}$ can be obtained by multiplying $\boldsymbol{A}$ with it on the left side.

In summary, obtaining a univariate equation from (13) through linear transformations is equivalent to computing an eigenvalue of $\boldsymbol{A}$. If an adversary can obtain r independent univariate equations from (13), the adversary will also be able to obtain all r eigenvalues of the public key matrix. This is the end of the proof.

4 Conclusions

Extracting irrational roots from a high-order polynomial equation has been proved to be an impossible task, while complexity of finding a secret composite factor from a big integer is decided by the number of prime factors contained in the integer, and apparently irreducible with algebraic tools. Our encryption scheme is novel since we have built a strong relationship between complexity of breaking the scheme to that of solving the above two original problems, which are different substantially from the underlying mathematical problems of existing public-key encryption schemes.

However we have not been able to reduce the cryptographic problem formulated in this paper to either of the proven hard problems mentioned above. The security topics that remained open to further research includes the complexity of reducing (13) to quartic or lower order univariate equations through nonlinear transformations and the complexity of solving (13) over R without breaking it into univariate equations.

Acknowledgements

This research is supported by National Natural Science Foundation of China under Grant 60373077.

References

1. J. D. Zheng, "A new public key cryptosystem for constrained hardware", in LNCS 2433, New York: Springer-Verlag, 2002, 334-341
2. D. Cantor, and H. Zassenhaus, "A new algorithm for factoring polynomials over finite fields", Math. Comp., 1981, 36: 587-592.
3. J. D. Zheng, "An Economical public-key crypto-device for C/S and B/S applications", Journal of Xiamen University, 2004, vol. 43(2): 141-143
4. J. D. Zheng "A fast digital signature scheme based on MDP", Journal of Computer Research and Development, 2005, 42(2) to appear
5. M O Rabin, Digital signatures and public key functions as intractable as factorization. MIT Laboratory for Computer Science, Technical Report: MIT/LCS/TR-212, 1979
6. http://www.utm.edu/research/primes/howmany.html
7. B. Schneier, Applied Cryptography, New York: John Wiley & Sons, 1996
8. T. W, Hungerford, Algebra, New York: Springer-Verlag, 1974, pp. 114-145
9. Raymond G. Ayoub, On the nonsolvability of the general polynomial, American Mathematical Monthly 89(1982), 397-401