J Med Syst (2019) 43: 276
https://doi.org/10.1007/s10916-019-1320-7

MOBILE & WIRELESS HEALTH

A Rainbow-Based Authentical Scheme for Securing Smart Connected Health Systems

Haibo Yi[1] · Jianqiang Li[2] · Qiuzhen Lin[2] · Huihui Wang[3] · Houbing Song[4] · Zhong Ming[2] · Zhe Nie[1]

Received: 1 October 2018 / Accepted: 1 May 2019 / Published online: 6 July 2019

Abstract
Smart Connected Health Systems (SCHSs) belong to health systems that provide services of health care remotely. They provide the doctors with access to electronic medical records with the aid of medical sensors, smart wearable devices and smart medical instruments. Although SCHSs have many applications in the area of health care, securing massive amount of valuable and sensitive data of the patients and preserving the privacy are challenging. User authentication based on public key cryptographic techniques is playing a crucial role in SCHSs for protecting the privacy of patients. However, quantum computers will break such techniques. Rainbow signature is one of the candidates of the next generation of cryptographic algorithms which can resist attacks on quantum computers. However, it is vulnerable to Differential Power Analysis (DPA) attacks, which is based on information gained from the cryptographic implementations. We present techniques to exploit the countermeasures to protect Rainbow against DPA attacks. We propose a variant of Rainbow with resistance to DPA attacks. First, we take a random vector to randomize the power consumption of private keys during computing the first affine transformation; Second, random variables are adopted during computing central map transformation; Third, we take two random vectors during computing the second affine transformation to randomize the power consumption of private keys. We analyze the efficiency and implement the scheme on hardware. Compared with the related implementations, our scheme is efficient and suitable for signature generations on hardware. Besides, we propose a secure authentical scheme based on the implementation for protecting record of patients in SCHSs.

Keywords Smart connected health system (SCHS) · Rainbow · Differential power analysis (DPA) · Authentication · Multivariate cryptography

Introduction

Health systems are organization of resources, people and institutions that deliver services of health care to meet the health needs of target populations [1–3]. Among health systems, Smart Connected Health Systems (SCHSs) connect smart medical devices, electronic medical records and medical cloud that provide services of health care remotely [4–6]. They can monitor the patients' conditions and provide the doctors with access to electronic medical records with the aid of medical sensors, smart wearable devices and smart medical instruments [7–9]. SCHSs improve both convenience and efficiency since doctors and patients are no longer required to be present at the same place [10].

Although SCHSs have many life-critical, context-aware, and intelligent medical applications in the area of health care, securing massive amount of valuable and sensitive data of the patients and preserving the privacy of the patients are challenging [11–13]. In order to protect the data of the patients and preserve the privacy of the patients in SCHSs, the user authentication is playing a crucial role [14–16]. Generally, the authentical schemes for SCHSs are based on passwords or biometric keys on smart cards, etc. Many authentical schemes based on public key cryptographic techniques have been proposed for SCHSs.

The most popular public key cryptographic systems used in SCHSs are Rivest-Shamir-Adleman (RSA) [17], Digital Signature Algorithm (DSA) [18] and Elliptic Curve Digital Signature Algorithm (ECDSA) [19]. However, Quantum

This article is part of the Topical Collection on *Mobile & Wireless Health*

✉ Jianqiang Li
lijq@szu.edu.cn

Extended author information available on the last page of the article.

computers will break such systems by using Shor's algorithm for factoring and computing discrete logarithms [20]. Shor's algorithm was proposed by Peter Shor in 1994, which is a quantum algorithm for integer factorization. Fortunately, there are lattice-based cryptography [21], hash-based cryptography [22], code-based cryptography [23] and multivariate cryptography [24]. They are candidates of the next generation of cryptographic algorithms which can resist attacks on quantum computers.

Rainbow signature is one of the most promising candidates in the area of post-quantum algorithms, which belongs to multivariate cryptography [25]. The theoretical basis for the constructions of Rainbow cryptographic systems is the proven theorem, i.e., solving a set of multivariate polynomial equations. The importance of Rainbow signature scheme lies in the applications as a more efficient and secure public key authentication system [26–37]. Rainbow is very suitable for hardware implementations [24]. S. Balasubramanian et al. implemented Rainbow signature on FPGA in 2008 [38]. S. Tang et al. speeded up Rainbow signature generations in 2011 [39]. Implementation of Rainbow is proven to be more efficient than RSA and elliptic curves on hardware [40].

Motivations. K. Okeya et al. proposed a Differential Power Analysis (DPA) attack on SFLASH signature in 2014 [41] and we proposed a DPA attack on Rainbow in 2018 [42]. The results from [41, 42] showed that Rainbow signature is vulnerable to DPA attacks. DPA belongs to side channel attacks, which is based on information gained from the cryptographic implementations. DPA attacks can provide detailed information of cryptographic systems by observing the power consumption. The countermeasures are typically costly for cryptographic implementations.

Our contributions. We present techniques to exploit countermeasures to protect Rainbow signature against DPA attacks. We propose a variant of Rainbow with resistance to DPA attacks. First, we take a random vector to randomize the power consumption of private keys during computing the first affine transformation; Second, random variables are adopted during computing central map transformation; Third, we take two random vectors during computing the second affine transformation to randomize the power consumption of private keys. We analyze the efficiency and implement the scheme on hardware. In addition, we also show that the implementation can be used for a secure authentical scheme to protect privacy of patients in SCHSs.

Organization. Section "Preliminary" introduces Rainbow signature schemes and DPA attacks to Rainbow. Section "A secure rainbow-based authentical scheme with resistance to DPA" presents a secure Rainbow-based authentical scheme with resistance to DPA. Section "Efficient implementation and performance evaluation" presents efficient implementations on hardware and results are evaluated. Section "Conclusions" summarizes our design.

Preliminary

Rainbow signature generation

Rainbow was proposed by J. Ding and D. Schmidt in 2005 [25]. It is an extended version of UOV. The central map transformation is the main operation in Rainbow. It is composed with two invertible affine transformations. Notations used in this paper are illustrated in Table 1.

(1) L_1: the first invertible affine transformation. The form of invertible affine transformation is $L_1(x) = Ax + B$, where A is a matrix, B is a vector. Besides, the input and output are vectors.
(2) F: the central map transformation. The form of the central map transformation is a set of multivariate quadratic equations with the form of $F(x) = y$.
(3) L_2: the second invertible affine transformation. The form of invertible affine transformation is $L_2(x) = Cx + D$, where C is a matrix, D is a vector. Besides, the input and output are vectors.
(4) K: a finite field. Finite field is a field with finite elements. $GF(2^n)$ and $GF(p)$ are two popular choices for many applications.
(5) y: the message of Rainbow.
(6) x: the signature of Rainbow.

Correspondingly, the private key of Rainbow is three transformations, i.e., L_1, F and L_2, and Rainbow's public key is $L_1 \circ F \circ L_2$. y is a vector with the form of $y(y_0, y_1, ..., y_{m-1})$, where $y_0, y_1, ..., y_{m-1} \subset K$. $x(x_0, x_1, ..., x_{n-1})$ is a vector, where $x_0, x_1, ..., x_{n-1} \subset K$.

The Rainbow signature generation flowchart is depicted in Fig. 1.

The following equation is to sign Rainbow's message $y(y_0, y_1, ..., y_{m-1}) \subset K$.

$$F \circ L_2(x_0, x_1, ..., x_{n-1}) = L_1^{-1}(y_0, y_1, ..., y_{m-1}). \quad (1)$$

First, in order to solve (1), it is required to compute the invertible affine transformation L_1.

$$\bar{y} = L_1^{-1}(y_0, y_1, ..., y_{m-1}). \quad (2)$$

Second, based on the computation result of (2), the central map transformation F is computed.

$$\bar{x} = F^{-1}(\bar{y}_0, \bar{y}_1, ..., \bar{y}_{m-1}). \quad (3)$$

Table 1 Rainbow signature schemes

Finite field	Message size	Signature size	Private key	Public key	Rainbow Message	Rainbow Signature
K	m	n	L_1, L_2, F	$L_1 \circ F \circ L_2$	$y_0, y_1, ..., y_{m-1}$	$x_0, x_1, ..., x_{n-1}$

Third, based on the computation result of (3), the invertible affine transformation L_2 is computed.

$$x = {L_2}^{-1}(\bar{x}_0, \bar{x}_1, ..., \bar{x}_{n-1}). \tag{4}$$

Finally, we generate the signature x.

DPA attacks to rainbow

The recent research on DPA attacks to Rainbow showed that the invertible affine transformations in Rainbow are vulnerable to DPA, as shown in Fig. 2.

DPA attack to Rainbow will be effective if there exists intermediate variables during the Rainbow signature generation which are correlated to mathematical operations depending on private keys and on known data of input or output. Private keys from the first invertible affine transformation are correlated to known input data and the private keys from the second invertible affine transformation are correlated to known output data. We choose the value of intermediate variables and guess the private key. According to such values and the known data of input or output, the set of power consumption curves partitioned. By computing and comparing simple statistic on the partitioned curves at individual points in time, private keys are reconstructed.

First invertible affine transformation is computed as follows.

$$\bar{y} = L_1^{-1}(y_0, y_1, ..., y_{m-1}). \tag{5}$$

The private keys from the first invertible affine transformation are variables in K of a matrix and a vector. a and b denote the matrix and the vector, respectively. They are involved in the following computations.

$$\bar{y} = ay + b. \tag{6}$$

It can be observed from (6) that the private keys a and b are correlated to known input y.

The second invertible affine transformation is computed as follows.

$$x = {L_2}^{-1}(\bar{x}_0, \bar{x}_1, ..., \bar{x}_{n-1}). \tag{7}$$

The private keys from the second invertible affine transformation are variables in K of a matrix and a vector. We use c and d to denote the matrix and the vector, respectively. They are involved in the following computations.

$$x = c\bar{x} + d. \tag{8}$$

It can be observed from (8) that the private keys c and d are correlated to known output x.

The correct guess of the private keys leads to a significant difference between the computed average power consumption curves.

A secure rainbow-based authentical scheme with resistance to DPA

Overview of the scheme

SCHSs use smart cards, sensors and other hardware, which are vulnerable to DPA attacks. We propose a secure authentical scheme based on a variant of Rainbow signature with resistance to DPA.

First, we present techniques to exploit countermeasures for protecting Rainbow signature against DPA attacks. We propose a variant of Rainbow with resistance to DPA attacks. We take a random vector to randomize the power consumption of private keys during computing the first affine transformation; Then, random variables are adopted during computing central map transformation;

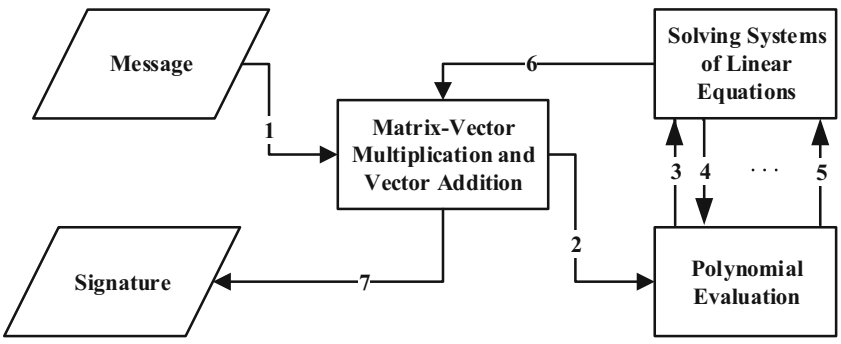

Fig. 1 The flowchart of rainbow signature generation

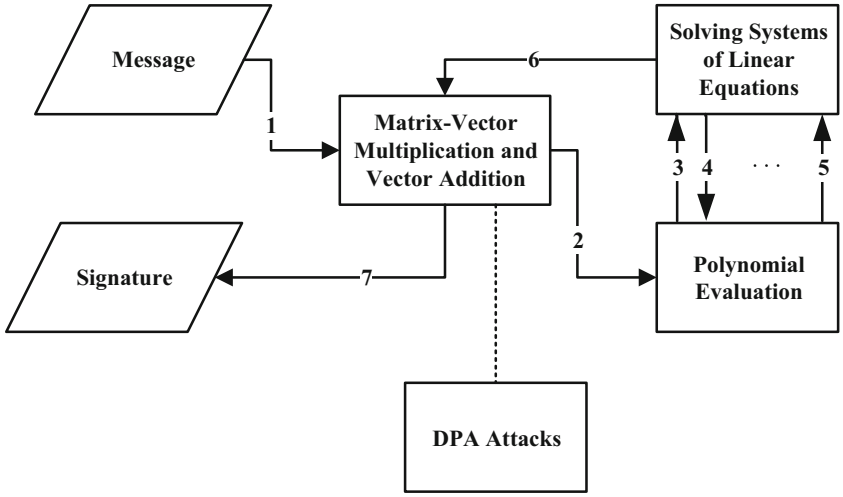

Fig. 2 DPA attacks to rainbow signature generation

Finally, we take two random vectors during computing the second affine transformation to randomize the power consumption of private keys. The Rainbow signature scheme with resistance to DPA is illustrated in Fig. 3. We ensure that random variables are involved in computations during the first invertible affine transformation, central map transformation and the second invertible affine transformation.

Second, we propose a secure authentical scheme based on our algorithm for obtaining record of patients, which is depicted in Fig. 4. We illustrate the scheme as follows.

Doctor A wants to obtain the record of Patient V. A generates a random value R_1 and uses his AES' key K_A to encrypt V and R_1, i.e., $E = AES(R_1 + V, K_A)$. He uses his private key of Rainbow to generate a signature of E and his ID ID_A, i.e $S = Rainbow(E + ID_A, P_A)$. Then he sends S, ID_A to the center of health system.

The center uses the public key of Doctor A to verify S, i.e., $M = Rainbow^{-1}(S, P'_A)$. Then, suppose that $M = E' + ID'_A$. If $ID'_A == ID_A$, the center uses the secret key K_A to decrypt E', i.e., $M' = AES^{-1}(E', K_A)$. Suppose that $M' = R_1 + V$. The center obtains the record of patient V, i.e $RecV$. Then, the center uses AES' key K_A of A to encrypt $RecV$ and R_1, i.e., $E = AES(RecV + R_1, K_A)$. The center uses his private key P_C to generate a Rainbow signature of E and his ID ID_C, i.e $S = Rainbow(E + ID_C, P_C)$. Then he sends S, ID_C to Doctor A.

Doctor A uses the public key of the center to verify S, i.e., $M = Rainbow^{-1}(S, P'_C)$. Suppose that $M = E' + ID'_C$. If $ID'_C == ID_C$, A uses the secret key K_A to decrypt E', i.e., $M' = AES^{-1}(E', K_A)$. Suppose that $E' = RecV' + R'_1$. If $R'_1 == R_1$, $RecV'$ is the record of patient V.

The first invertible affine transformation

The following equation is to sign Rainbow's message $y(y_0, y_1, ..., y_{m-1}) \subset K$.

$$\bar{y} = L_1^{-1}(y_0, y_1, ..., y_{m-1}). \tag{9}$$

Since the message is known to the attackers, it is vulnerable to DPA attacks. In order to deal with the issue, we take a

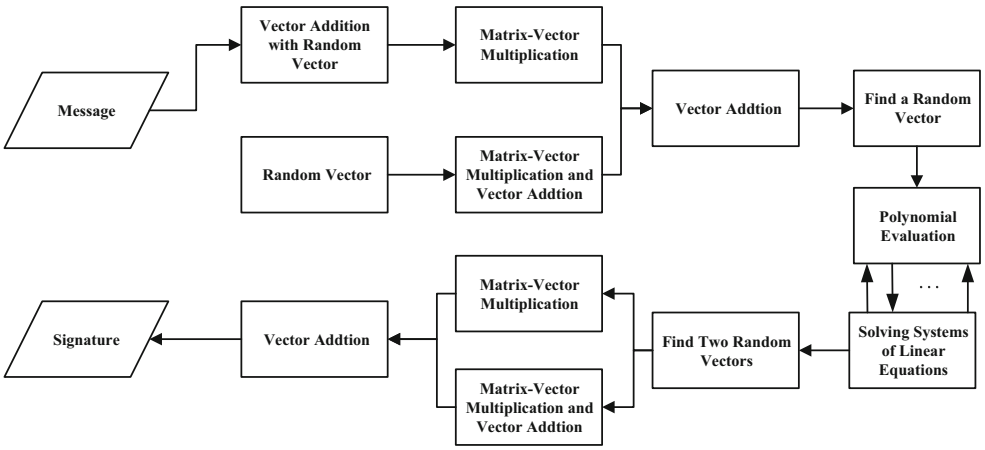

Fig. 3 A secure rainbow signature scheme with resistance to DPA

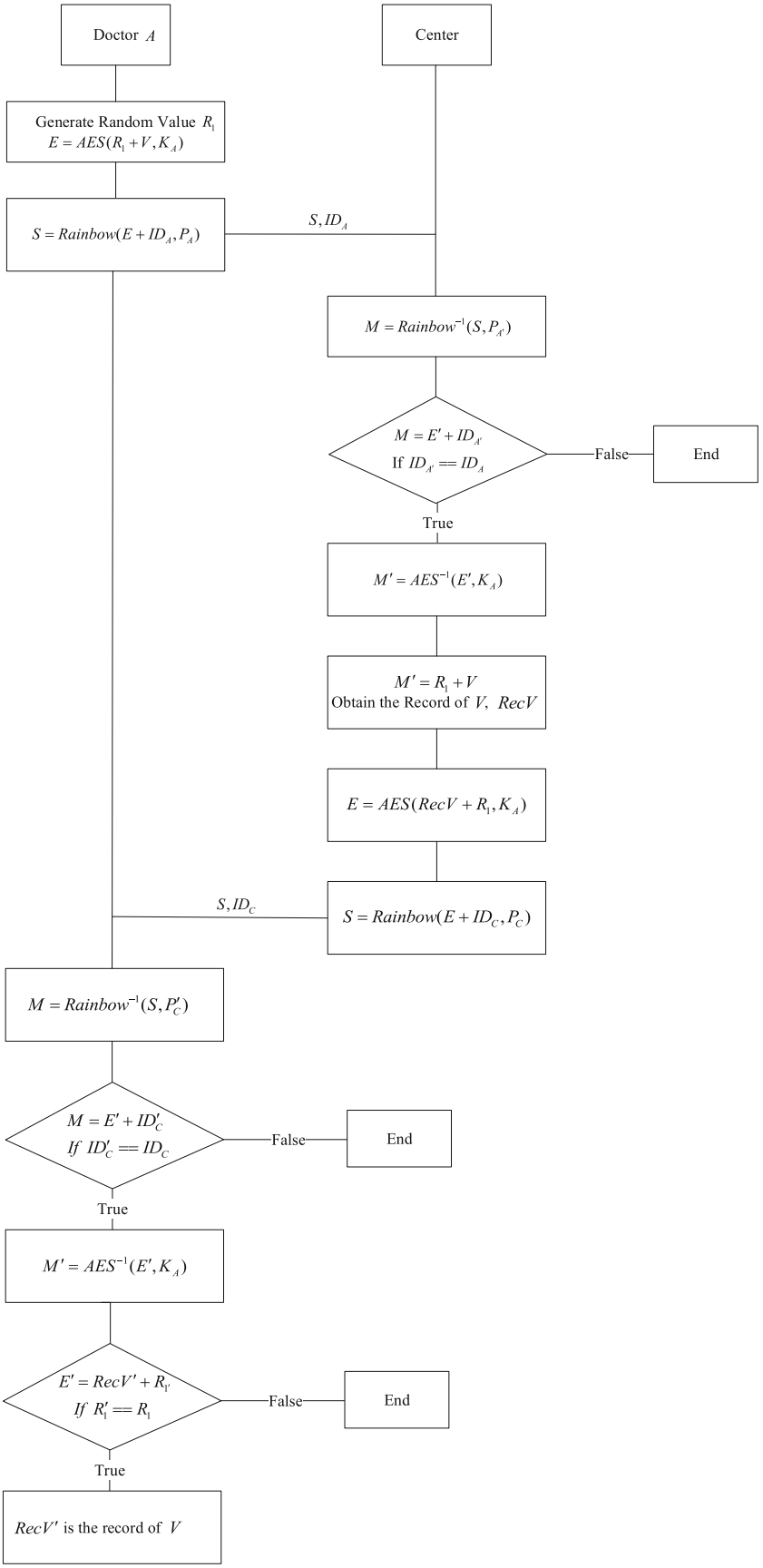

Fig. 4 A secure authentical scheme based on our algorithm for obtaining record of patients

vector $y'(y'_0, y'_1, ..., y'_{m-1}) \subset K$ with random values. The elements are generated by a random number generator.

Then, we compute a vector addition in finite field K.

$$y'' = y' + y. \tag{10}$$

$y''(y''_0, y''_1, ..., y''_{m-1}) \subset K$ is random during each signature generation of Rainbow. The elements of y'' are in finite field K.

Next, the following equation is computed via multiplication of matrix and vector and addition between vectors in finite field K.

$$\bar{y}' = ay' + b. \tag{11}$$

In (11), a is a $m \times m$ matrix of key and b is a m vector of key. Since y' is random during each signature generation of Rainbow, the power consumption curves are random.

Then, we compute a matrix-vector multiplication in finite field K.

$$\bar{y}'' = ay''. \tag{12}$$

In (12), a is a key-matrix with the size of $m \times m$. Since y'' is random during each signature generation of Rainbow, the power consumption curves are random.

Finally, we compute a vector addition in finite field K.

$$\bar{y} = \bar{y}' + \bar{y}''. \tag{13}$$

Equation (13) equals to the following computation.

$$\bar{y} = Ay + b. \tag{14}$$

The first invertible affine transformation with DPA resistance includes three vector additions and two matrix-vector multiplications in finite field K.

Central map transformation

Based on the computation result of (13), the central map transformation F is computed.

$$\bar{x} = F^{-1}(\bar{y}_0, \bar{y}_1, ..., \bar{y}_{m-1}). \tag{15}$$

Elements in $\bar{x}$ are divided into Vinegar variables (Denoted by V_i) and Oil variables (Denoted by O_i). F includes m multivariate polynomial equations with the following form.

$$\bar{y}_k = \sum \alpha_{ij} V_i O_j + \sum \beta_i O_i + \sum \chi_{ij} V_i V_j + \sum \delta_i V_i + \Delta. \tag{16}$$

$\alpha, \beta, \chi, \delta, \Delta$ are private keys.

Generally, the m multivariate polynomial equations are divided into multiple layers as Rainbow is a multi-layer construction. Here, we suggest that two-layer construction is efficient.

For the Vinegar variables on the first layer, we choose random values. Thus, the private key $\alpha, \beta, \chi, \delta, \Delta$ related computations have random power consumption curves. Then, we substitute them into the equations of the first layer. They are transformed into the following form on the unknown Oil variables.

$$\sum \varepsilon_i O_i = \phi. \tag{17}$$

Then, we solve the equations of (17).

For Vinegar variables on second layer, variables from the upper layer are substituted into the equations of the current layer. They are transformed into the following form on the unknown Oil variables.

$$\sum \varepsilon_i O_i = \phi. \tag{18}$$

Then, we solve equations of (18).

After that, variables in $\bar{x}$ are solved.

The second invertible affine transformation

Based on the computation result of (17) and (18), it is required to compute the invertible affine transformation L_2.

$$x = {L_2}^{-1}(\bar{x}_0, \bar{x}_1, ..., \bar{x}_{n-1}). \tag{19}$$

Since the signature x is known to the attackers, it is vulnerable to DPA attacks. So as to deal with this issue, we take two random vectors $\bar{x}' \subset K$ and $\bar{x}'' \subset K$.

First, vector $\bar{x}'$ is generated by a random number generator.

Then, we make sure that $\bar{x}''$ and $\bar{x}'$ have the following relation.

$$\bar{x} = \bar{x}' + \bar{x}''. \tag{20}$$

Next, we compute a matrix-vector multiplication in finite field K.

$$x' = c\bar{x}'. \tag{21}$$

In (21), c is a $n \times n$ matrix of key. Since the vector $\bar{x}'$ is random for each signature generation of Rainbow, the power consumption curves are random.

Then, we compute a multiplication of matrix and vector and an addition between vectors in finite field K.

$$x'' = c\bar{x}'' + d. \tag{22}$$

In (22), c is a $n \times n$ matrix of key and d is a n vector of key. Since vector $\bar{x}''$ is random for each signature generation of Rainbow, the power consumption curves are random.

Finally, we compute a vector addition in finite field K.

$$x = x' + x''. \tag{23}$$

Equation (23) equals to the following computation.

$$x = c\bar{x} + d. \tag{24}$$

The second invertible affine transformation with DPA resistance includes three vector additions and two matrix-vector multiplications in finite field K.

Table 2 Implementation results of rainbow scheme

Signature Scheme	Message Size	Signature Size	Time Frequency	Clock Cycle	Executing Time	Gate Equivalents
Rainbow(17,13,13)	26 Bytes	43 Bytes	50 MHz	242	4.9 us	30000

Efficient implementation and performance evaluation

Here, we choose Rainbow(17,13,13) in $GF((2^4)^2)$ for efficient implementation and comparison. The operations of the new scheme include solving systems of linear equations, multiplication of matrix and vector and addition between vectors based on multiplication and inversion in a finite field.

Overall performance

Since SCHSs use sensor, smart card and other hardware to provide services of health care, we implement the Rainbow scheme on hardware. In order to prove that the designs of Rainbow(17,13,13) are efficient on hardware, designs of Rainbow scheme for $GF((2^4)^2)$ have been implemented on ASICs. We present the experimental results in Tables 2 and 3.

Tables 2 and 3 show that Rainbow implementation includes 26×26 and 43×43 invertible affine transformations, evaluations of 26 MQ polynomials and solving two 13×13 equation systems. Table 3 summarizes the performance, which shows that it takes only 4840 ns and 242 clock cycles for each signature generation.

Performance comparison

The work in [39, 43–45] are believed to be the latest public key cryptographic techniques on hardware. Comparisons with these systems are depicted in Table 4, which show that our design is much efficient than implementations of RSA and ECC. Besides, the work in [39] is an original implementation without DPA countermeasures. Compared with such work, our implementation with countermeasure is 20% slower.

Application

The implementation can be used to build a Rainbow-based authentical scheme for protecting record of patients in SCHSs. We suppose that Patient V's medical record is secure and stored in the cloud (The center). Doctor A is authorized to read his record. The process is protected by the Rainbow-based authentical scheme with AES encryption and decryption.

(1) Doctor A generates a random value R_1;
(2) Doctor A uses his AES' key K_A to encrypt V and R_1, i.e., $E = AES(R_1 + V, K_A)$.
(3) Doctor A uses his private key of Rainbow P_A to generate a signature of E and his ID ID_A, i.e $S = Rainbow(E + ID_A, P_A)$.
(4) Doctor A sends S, ID_A to the center of health system.
(5) The center uses the public key of Doctor A to verify S, i.e., $M = Rainbow^{-1}(S, P'_A)$.
(6) Suppose that $M = E' + ID'_A$. If $ID'_A == ID_A$, the center uses the secret key K_A to decrypt E', i.e., $M' = AES^{-1}(E', K_A)$.
(7) Suppose that $M' = R_1 + V$. The center obtains the record of patient V, i.e $RecV$.
(8) The center uses AES' key K_A of A to encrypt $RecV$ and R_1, i.e., $E = AES(RecV + R_1, K_A)$.
(9) The center uses his private key P_C to generate a Rainbow signature of E and his ID ID_C, i.e $S = Rainbow(E + ID_C, P_C)$.
(10) The center sends S, ID_C to Doctor A.

Table 3 Execution time of the implementation in clock cycles

Steps	Components	Clock cycles
1	${L_1}^{-1}$ transformation	28
2	The first round of 13 polynomial evaluations	65
3	The first round of solving system of linear equations	13
4	The second round of 13 polynomial evaluations	78
5	The second round of solving system of linear equations	13
6	${L_2}^{-1}$ transformation	45
	Total	242

Table 4 Comparison on Public Key Cryptographic Systems

Signature scheme	Clock cycle	Executing time (us)
RSA with resistance [43]	–	518330
ECC with resistance [44]	–	7290
enTTS [45]	5418	216.72
Rainbow [39]	198	3.96
This work	242	4.84

(11) Doctor A uses the public key of the center to verify S, i.e., $M = Rainbow^{-1}(S, P'_C)$.
(12) Suppose that $M = E' + ID'_C$. If $ID'_C == ID_C$, A uses the secret key K_A to decrypt E', i.e., $M' = AES^{-1}(E', K_A)$.
(13) Suppose that $E' = RecV' + R'_1$. If $R'_1 == R_1$, $RecV'$ is the record of patient V.

Conclusions

We propose a variant of Rainbow with resistance to DPA attacks. First, we take a random vector to randomize the power consumption of private keys during computing the first affine transformation; Second, random variables are adopted during computing central map transformation; Third, we take two random vectors during computing the second affine transformation to randomize the power consumption of private keys. We analyze the efficiency and implement the scheme on hardware. The comparison results with the related implementations show that our scheme is efficient and suitable for the signature of the post-quantum applications. In addition, we also show that the implementation can be used for a secure authentical scheme to protect privacy of patients in SCHSs.

The most popular public key cryptographic systems used in SCHSs are RSA, DSA and ECDSA. However, they are not secure under quantum computer attacks. Thus, the proposed signature scheme is one of the promising candidates for building secure and efficient SCHSs. In addition, it can be further used in many areas, such network security, cloud security and IoT security.

Acknowledgments This study was funded by the Joint Funds of the National Natural Science Foundation of China under Key Program Grant (No. U1713212), Natural Science Foundation of Guangdong Province, China (No. 2018A030310030), Foundation for Distinguished Young Talents in Higher Education of Guangdong, China (No. 2017GkQNCX059), Special funds for Shenzhen Strategic Emerging Industries and Future Industrial Development (No. 20170502142224600), Shenzhen Science and Technology Program under Grant (No. JCYJ20170306144219159), Science and Technology Program of Shenzhen Polytechnic (No. 601722K20018).

Compliance with Ethical Standards

Conflict of interests All authors declare that they have no conflict of interest. This article does not contain any studies with human participants or animals performed by any of the authors.

References

1. Ghaffar, A., Langlois, E. V., Rasanathan, K. et al., Strengthening health systems through embedded research[J]. *Bull. World Health Organ.* 95(2):87–87, 2017.
2. Kutzin, J., and Sparkes, S. P., Health systems strengthening, universal health coverage, health security and resilience[J]. *Bull. World Health Organ.* 94(1):2, 2016.
3. Kieny, M. P., Bekedam, H., Dovlo, D. et al., Strengthening health systems for universal health coverage and sustainable development[J]. *Bull. World Health Organ.* 95(7):537–539, 2017.
4. Lin, C., Song, Z., Song, H. et al., Differential privacy preserving in big data analytics for connected Health[J]. *J. Med. Syst.* 40(4):97, 2016.
5. Vlahugjorgievska, E., Koceski, S., Kulev, I. et al., Connected-Health Algorithm: Development and Evaluation.[J]. *J. Med. Syst.* 40(4):1–7, 2016.
6. Rantos, K., Fysarakis, K., Manifavas, C. et al., Policy-Controlled Authenticated Access to LLN-Connected Healthcare Resources[J]. *IEEE Syst. J.* PP(99):1–11, 2018.
7. Bloss, R., Embedded medical sensors, an emerging technology to monitor hearts, brains, nerves and addressing other medical applications for improved patient care[J]. *Sens. Rev.* 36(2):115–119, 2016.
8. Vasiliev, A., Varfolomeev, A., Volkov, I. et al., Reducing humidity response of gas sensors for medical applications: use of spark discharge synthesis of metal oxide nanoparticles[J]. Sensors, 18(8), 2018.
9. Polsky, R., Narayan, R., and Miller, P., Microneedle-Based Sensors for medical Diagnosis[J]. *J. Mater. Chem. B* 4(8):1379–1383, 2016.
10. Ullah, S., Pedrycz, W., Karagiannidis, G. K. et al., Guest editorial special issue on communications technologies and infrastructures for smart e-health systems[J]. *IEEE Syst. J.* 12(1):16–19, 2018.
11. Huang, H., Gong, T., Ye, N. et al., Private and secured medical data transmission and analysis for wireless sensing healthcare System[J]. *IEEE Trans. Ind. Inf.* 13(3):1227–1237, 2017.
12. Zhang, L., Zhang, Y., Tang, S. et al., Privacy protection for E-Health systems by means of dynamic authentication and Three-Factor key Agreement[J]. *IEEE Trans. Ind. Electron.* 65(3):2795–2805, 2017.
13. Sharma, S., Chen, K., and Sheth, A., Towards practical privacy-preserving analytics for iot and cloud based healthcare systems[J]. *IEEE Internet Comput.* PP(99):1–1, 2018.
14. Fontaine, J., Zheng, K., Van, D. V. C. et al., Evaluation of a proximity card authentication system for health care settings[J]. *Int. J. Med. Inform.* 92:1–7, 2016.
15. Mohit, P., Amin, R., Karati, A. et al., A standard mutual authentication protocol for cloud computing based health care System[J]. *J. Med. Syst.* 41(4):1–13, 2017.
16. Kumar, V., Jangirala, S., and Ahmad, M., An efficient mutual authentication framework for healthcare system in cloud Computing[J]. *J. Med. Syst.* 42(8):142, 2018.
17. Brown, D. R., and Breaking, RSA, May be as difficult as Factoring[J]. *J. Cryptol.* 29(1):220–241, 2016.

18. Sharma, G., Bala, S., and Verma, A. K., PF-IBS Pairing-Free Identity based digital signature algorithm for wireless sensor Networks[J]. *Wirel. Pers. Commun.* 97(2):1–12, 2017.
19. Barenghi, A., Bertoni, G. M., Breveglieri, L. et al., A Fault-Based secret key retrieval method for ECDSA: Analysis and Countermeasure[J]. *ACM J. Emerg. Technol. Comput. Syst.* 13(1):8, 2016.
20. Bernstein, D. J., and Lange, T., Post-quantum cryptography[J]. *Nature* 549(7671):188, 2017.
21. Howe, J., Khalid, A., Rafferty, C. et al., On practical discrete gaussian samplers for lattice-based cryptography[J]. *IEEE Trans. Comput.* PP(99):322–334, 2018.
22. Butin, D., Hash-Based signatures: State of Play[J]. *IEEE Secur. Priv.* 15(4):37–43, 2017.
23. Sendrier, N., Code-Based cryptography: State of the art and Perspectives[J]. *IEEE Secur. Priv.* 15(4):44–50, 2017.
24. Ding, J., and Petzoldt, A., Current state of multivariate Cryptography[J]. *IEEE Secur. Priv.* 15(4):28–36, 2017.
25. Ding, J., and Schmidt, D., Rainbow, a new multivariable polynomial signature Scheme[J]. *Applied Cryptography & Network Security* 3531:164–175, 2005.
26. Billet, O., and Gilbert, H., Cryptanalysis of rainbow[C]. In: International Conference on Security and Cryptography for Networks, Springer, pp 336–347, 2006.
27. Ding, J., Yang, B. Y., Chen, C. H. O. et al., *New Differential-Algebraic Attacks and Reparametrization of Rainbow[M], applied cryptography and network security*, pp. 242–257. Berlin: Springer, 2008.
28. Petzoldt, A., Bulygin, S., Buchmann, J., and CyclicRainbow, C, A Multivariate Signature Scheme with a Partially Cyclic Public Key[C]. In: Progress in Cryptology - Indocrypt 2010 - , International Conference on Cryptology in India, Hyderabad, India, December 12-15, 2010. Proceedings. DBLP, pp 33–48, 2010.
29. Petzoldt, A., Bulygin, S., and Buchmann, J., Selecting parameters for the rainbow signature Scheme[C]. In: International Conference on Post-Quantum Cryptography, Springer, pp 218–240, 2010.
30. Yasuda, T., Sakurai, K., and Takagi, T., Reducing the key size of rainbow using non-commutative rings[J]. *Lect. Notes Comput. Sci* 7178:68–83, 2012.
31. Thomae, E., *Quo Vadis Quaternion? Cryptanalysis of Rainbow over Non-commutative Rings[M]// Security and Cryptography for Networks*, pp. 361–373. Berlin: Springer, 2012.
32. Petzoldt, A., Bulygin, S., and Buchmann, J., *Fast Verification for Improved Versions of the UOV and Rainbow Signature Schemes[M]// Post-Quantum Cryptography*, pp. 188–202. Berlin: Springer, 2013.
33. Yasuda, T., Takagi, T., and Sakurai, K., Efficient Variant of Rainbow without Triangular Matrix Representation[C]. In: Information and Communication Technology - EurAsia Conference, pp 532–541, 2014.
34. Yasuda, T., Takagi, T., and Sakurai, K., Efficient variant of Rainbow using sparse secret keys. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* 5:3–13, 2014.
35. Yasuda, T., and Sakurai, K., *A Multivariate Encryption Scheme with Rainbow[M]// Information and Communications Security*. Berlin: Springer International Publishing, 2015.
36. Mohamed, M. S. E., Petzoldt A., and RingRainbow, C., An efficient multivariate ring signature scheme[C]. In: *International Conference on Cryptology in Africa*, pp. 3–20. Cham: Springer, 2017.
37. Peng, Z., and Tang S., Circulant Rainbow: A new rainbow variant with shorter private key and faster signature Generation[J]. *IEEE Access* 5(99):11877–11886, 2017.
38. Balasubramanian, S., Bogdanov, A., Rupp, A. et al., Fast multivariate signature generation in hardware: The case of Rainbow[C]. In: International Symposium on Field-Programmable Custom Computing Machines, IEEE, pp 281–282, 2008.
39. Tang, S., Yi, H., Ding, J. et al., *High-speed Hardware Implementation of Rainbow Signature on FPGAs[m], Post-Quantum Cryptography*, pp. 228–243. Berlin: Springer, 2011.
40. Yi, H., Under quantum computer attack: Is rainbow a replacement of RSA and elliptic curves on Hardware?[J]. *Security & Communication Networks* 2018:1–9, 2018.
41. Okeya, K., Takagi, T., and Vuillaume, C., On the importance of protecting δ in SFLASH against side channel attacks. In: *International Conference on Coding and Computing (ITCC 2004)*, pp. 560–568. Washington: IEEE, 2004.
42. Yi, H., and Nie, Z., On the security of MQ cryptographic systems for constructing secure Internet of medical things[J]. Personal & Ubiquitous Computing, pp 1–7, 2018.
43. Mahanta, H. J., and Khan, A. K., Securing RSA against power analysis attacks through non-uniform exponent partitioning with randomisation[J]. *IET Inf. Secur.* 12(1):25–33, 2018.
44. Liu, Z., Liu, D., and Zou, X., An efficient and flexible hardware implementation of the dual-field elliptic curve cryptographic processor[J]. *IEEE Trans. Ind. Electron.* PP(99):1–1, 2017.
45. Yi, H., and Li, W., On the importance of checking multivariate public key cryptography for side-channel attacks: the case of enTTS scheme[J]. *Comput. J.* 60(8):1–13, 2017.

Affiliations

Haibo Yi[1] · Jianqiang Li[2] · Qiuzhen Lin[2] · Huihui Wang[3] · Houbing Song[4] · Zhong Ming[2] · Zhe Nie[1]

Haibo Yi
haiboyi@szpt.edu.cn

Qiuzhen Lin
qiuzhlin@szu.edu.cn

Huihui Wang
hwang1@ju.edu

Houbing Song
Houbing.Song@erau.edu

Zhong Ming
mingz@szu.edu.cn

Zhe Nie
niezhe@szpt.edu.cn

1 School of Computer Engineering, Shenzhen Polytechnic, Shenzhen, People's Republic of China

2 College of Computer Science and Software Engineering, Shenzhen University, Shenzhen, People's Republic of China

3 Department of Engineering, Jacksonville University, Jacksonville, FL, 32211 USA

4 Department of Electrical, Computer, Software, and Systems Engineering, Embry-Riddle Aeronautical University, Daytona Beach, FL 32114 USA