Eurasia Journal of Science and Technology	ISSN: 2663-1024	Volume 4, Issue 1, pp 53-60	JUN 2022

A SCALAR OPERATION BASED ENDOMORPHISM SPARSE METHOD FOR SOLVING HYPERSINGULAR ELLIPTIC CURVE LADDER FOR INTERNET OF THINGS DEVICE SECURITY AUTHENTICATION

Jin Lu[1*]
Guangdong Key Laboratory of Big Data Intelligence for Vocational Education, Shenzhen Polytechnic, Shenzhen 518055, Guangdong, China;
Corresponding Author's Email: lujin0808@szpt.edu.cn

Abstract
At present, RSA, ECC and other asymmetric encryption algorithms are mainly used in the authentication of the Internet of Things gateway, but due to the limited amount of computation of embedded devices and the inability to resist quantum attacks, the traditional encryption algorithms are difficult to meet the security needs of the existing Internet of Things authentication, so it is urgent to develop a lightweight encryption algorithm that can resist quantum attacks. In this paper, we propose a lightweight SIKE encryption algorithm for security authentication of Internet of Things devices based on the latest release of NIST's key exchange algorithm based on hypersingular endomorphisms (SIKE algorithm), which is optimized by solving the ladder of hypersingular elliptic curves with sparse hSomomorphisms and double-channel exchange of random prime numbers. The simulation results show that the computational overhead of the algorithm can be reduced by 40% in the prime number solving stage, by 32% in the key exchange stage, and by more than 28% in ASIC implementation circuit area (taking logic gate as an example), and the final FOM value can be more than 300.
Keyword: Internet of Things, SIKE; Safety Certification, Supersingular elliptic curves

1. Introduction

At present, the Internet of Things system is mainly composed of lightweight embedded devices, which have limited computing power, communication bandwidth and storage space. At the same time, IOT sensing devices are often scattered in unmanned areas or insecure physical environments, and these nodes are likely to be physically destroyed or captured. If an attacker captures a node device, he can carry out traditional attacks or even quantum attacks on the device. Therefore, the data security, network communication and access interface of the whole Internet of Things system need data encryption, usually using RSA, ECC and other asymmetric encryption algorithms. Although the above algorithm can ensure the reliability of encryption, for lightweight devices such as the Internet of Things, its computational complexity will reduce the transmission speed of the gateway interface. With the rapid development of Internet of Things technology, the research and application of tailored cryptographic algorithms have provided sufficient security guarantee for resource-constrained devices such as Internet of Things gateways. However, due to the different emphasis of many algorithms in optimization, there are also great differences in the performance of security balance, cost and efficiency, and few algorithms can really be applied to Internet of Things devices. According to the characteristics of the existing Internet of Things devices, considering the application environment and usage scenarios, the encryption algorithms that can be applied in the Internet of Things devices include AES cryptography, stream cryptography, public key cryptography and post-quantum cryptography, covering two mainstream algorithms of symmetric encryption and asymmetric encryption.

AES is a group symmetric encryption algorithm, whose plaintext is usually 128 bits with a fixed length of 16 bytes, and the encrypted or decrypted data is divided into 16 byte groups. According to the different encryption length, AES encryption algorithm can be divided into AES-128, AES-192 and AES-256. The key lengths are 128, 192, and 256 bits. At present, the lightweight AES encryption algorithm applied in Internet of Things devices is mainly based on the original encryption by cutting the main operations CBC and ECB to integrate resources and reduce the consumption of hardware resources. Because AES encryption algorithm is mainly used to resist quantum attacks by increasing the key length, it can not be applied to Internet of Things applications such as identity authentication, resulting in its limited application.

HC-128, HC-256, SNOW2.0, SEEPENT and other algorithms are mainly based on the sequence key implementation of eSTERAM, which has lower requirements for software and hardware, and is very suitable for platforms with limited computing resources such as the Internet of Things. At present, the industry mainly focuses on the structural improvement of basic operation units such as cascade operation, shift and Xor of stream ciphers to achieve lightweight optimization. However, the important problem of

stream cipher is that its anti-attack type is poor, and the data and key stored in the same channel are easy to be cracked, so it is not suitable for the Internet of Things gateway devices with large amount of data.

Asymmetric encryption algorithms include RSA and ECC algorithms, which are mainly based on mathematical methods such as prime number decomposition, discrete logarithm solution, elliptic curve solution and so on. The RSA encryption algorithm is based on the difficulty of factoring the maximum integer, and its reliability is determined by the difficulty of factoring the maximum integer, and the key length is distributed in the range of 1024-15360, which is a highly reliable algorithm, but because of the limitation of the principle of RSA encryption algorithm itself, it is difficult to optimize its lightweight. It has not been applied to the gateway equipment of the Internet of Things for the time being. The ECC encryption algorithm, namely the elliptic curve encryption algorithm, is mainly realized by utilizing the computational difficulty of the elliptic discrete logarithm on the Abel addition group formed by the rational points on the elliptic curve. The lightweight optimization of ECC encryption algorithm mainly focuses on operations such as scalar sparsity, curve heterogeneity and endomorphism acceleration, which has been successfully applied to Internet of Things modules such as RFID. However, in the face of the attack of quantum computer, ECC encryption algorithm also shows the characteristics of poor anti-attack ability.

In the face of the attack threat of quantum computer, the traditional encryption algorithms such as ECC and RSA do not have the corresponding anti-attack ability, so it is urgent to study new encryption algorithms. At present, the post-quantum encryption algorithm is generally recognized as a cryptosystem that can resist the attack of quantum computer. Its implementation principle is different from the traditional large number decomposition and other problems, mainly the discrete logarithm of supersingular curves and other problems, including lattice-based cryptography, multivariate cryptography, hash-based cryptography, code-based cryptography and supersingular endomorphic cryptography. Among many post-quantum encryption algorithms, SIKE algorithm is widely used in the Internet of Things and other fields because of its short key length and fast solving process. In the research on the application of post-quantum encryption algorithm, Anton Stolbunov first proposed the Diffie-Hellman key exchange algorithm, which is mainly based on the extremely difficult operation of traditional elliptic curve, and its anti-quantum attack is very low[4]. In order to solve this problem, Anton Stolbunov proposed a post-quantum encryption algorithm, and Andrew Childs proposed a corresponding quantum domain side attack method to crack the algorithm[5]. Based on the post-quantum encryption algorithm proposed by Anton, David Jao replaces the traditional elliptic curve encryption algorithm with the supersingular elliptic curve encryption algorithm to solve the problem of side attack on the quantum domain, and realizes the post-quantum encryption in a real sense. Compared with the traditional elliptic encryption curve algorithm, the supersingular elliptic encryption curve has a magnitude from $O(\sqrt[4]{p}) \to O(\sqrt[6]{p})$ The difficulty of cracking is greatly increased(11). In the optimization of the post-quantum algorithm, Saarinen and James respectively optimize the approximate solution through the eigenvalue domain and the scalar sparsity, so that it can achieve asymmetric encryption(12)in a limited computational area. Pony proposed a hybrid public key cryptosystem based on Rabin, which is suitable for the lightweight Internet of Things plaorm(13)for authentication tags such as RFID. Brian proposed a FPGA-based post-quantum supersingular elliptic curve encryption algorithm circuit, and optimized the scalar multiplication, point multiplication and other modules to achieve lightweight optimization to meet the circuit characteristics of FPGA. Pessl proposed a post-quantum encryption algorithm for digital signature, which is anti-quantum attack(14)compared with the traditional encryption algorithm.

Based on the above review, it can be seen that the application of post-quantum encryption algorithm in the security related fields of the Internet of Things is still in its infancy, especially in the application of post-quantum encryption algorithm such as supersingular elliptic encryption curve, which needs to be improved and further studied. However, there are two problems in the application of the above quantum algorithm in the Internet of Things devices. First, the existing optimization process mainly focuses on the optimization of basic operation units, including scalar multiplication, dot multiplication module and other basic units to achieve bottom-up optimization, but there is no detailed consideration for the optimization of the overall key exchange and curve solution, which leads to the unchanged operation route after the overall optimization. The optimization effect is limited. At the same time, the traditional encryption algorithm applied in the related devices of the Internet of Things can not resist quantum attacks, and the overall security is not high. Therefore, according to the characteristics of the existing Internet of Things devices, it is particularly important to select the appropriate post-quantum encryption algorithm for lightweight optimization, so that it can meet the security requirements of the Internet of Things against quantum attacks under limited computing resources.

This paper focuses on the research of lightweight SIKE encryption algorithm applied to the security authentication of Internet of Things devices, and proposes an optimization method for solving supersingular elliptic curve ladder based on scalar operation endomorphism sparsity, aiming at solving the difficult problem of solving the curve in the authentication process of Internet of Things with limited computing resources. According to the characteristics of discrete curve solving, we first label the leaf nodes, label the key nodes, and then traverse the tree in a depth-first manner, and output the node labels when they are encountered. Secondly, the output of the optimized structure tree will be simplified from

the original { 4,3,2,2,2,1 } to { 3,1,1,1,1,1 }, so as to achieve a more simplified higher-order endomorphism solution structure. In order to optimize the solution level of supersingular elliptic curve data encryption, facing the full binary fast scalar tree structure, the adhesion degree between levels is gradually broken and sparsified. Because the elliptic curve follows the Homer criterion, the linearization method is needed to deal with it. In the process of linear processing, the loop is broken to achieve a more compact variable endomorphism operation in the part of the leaf nodes in a non-adjacent sparse way. In addition, in order to solve the problem of low key exchange efficiency in the supersingular elliptic encryption curve algorithm, a key exchange method of the supersingular endomorphic key exchange algorithm based on the double-channel exchange of random prime numbers is proposed, that is, the definition of mutual operation points is carried out on the initialization curve, and two groups of random prime number coefficients are introduced. m_A 、 m_B And n_A 、 n_B The computation cost of the characteristic point coefficients can be greatly reduced by approximate solution, and the whole key exchange process is completed by two-channel computation instead of six-channel computation exchange.

2. Proposed method

$$E(\mathrm{F}_P) \ : \ \mathrm{B}y^2 = x^3 + Ax^2 + x \quad (1)$$

Where X, y, A a $\in F_p$ 。Through the above operations, we can know all the $E(F_p)$ It is a finite additive group, and its whole operation is realized by group operation, which follows the normalized prime number solution, that is, the curve discrete solution is realized by using the prime number singularity

Based on the above initialization curve, the high-order singularity solution will be carried out. $E_0 = E$, $R_0 = R$, define the function as

$$E_{\mathrm{i}+1} = E_i / \langle \ell^{e-i-1} R_i \rangle \phi_i : E_i \text{->} E_{i+1} R_{\mathrm{i}+1} = \phi_i(R_{\mathrm{i}}) \quad (3)$$

At present, supersingular elliptic encryption curves are usually used. ℓ The case of = 6 proceeds. From the architecture of supersingular curves of order 6, we can see that R is a whole supersingular elliptic

2.1Key exchange pre-distribution

The existing SIKE algorithm mainly focuses on scalar multiplication over feature 2 or 3, especially in the process of public key exchange, using these two scalar curves to operate each other at the same time, so as to achieve the effect of anti-quantum attack. The key exchange process of supersingular elliptic encryption curves is essentially the mutual operation of known definition points on the initialization curves (curves of characteristic 2 and characteristic 3, respectively).

Define two points based on feature 2 as P_2 、 Q_2 ,

2.2 Introduction to the supersingular endomorphic key exchange algorithm (SIKE)

Based on the ECC algorithm, the SIKE algorithm is realized by adding an anti-quantum attack module, and the core algorithm is solving the supersingular elliptic curve. The existing SIKE algorithm, from the perspective of traditional encryption, mainly includes two processes, one is the solving process of high-order endomorphism based on discrete curves, and the other is the pre-distribution process of key exchange.

2.3Solving process of higher order endomorphism based on discrete curves

The SIKE algorithm is based on the finite field of prime numbers, and realizes the encryption and decryption of data by solving the endomorphism of the logarithm discrete curve. The main implementation process is as follows: define the finite field as F_{q} , a supersingular elliptic curve is set to $E(F_p)$, the singular point is R , the supersingular endomorphism function is ϕ , the prime field order is ℓ , j Is a curve invariant. The solution process refers to the procedure in Eq. F_p The set of singular points on all supersingular curves over solves:

R. $E(F_p)$ To $E / \langle R \rangle$ The conversion of. For different parameters, the supersingular elliptic curve will form a set of different related curves, the initial curve is a special case of the supersingular elliptic curve, that is, B = 1, A = 6, where the curve invariant is j = 287 496, while $E_0 = (2^{e2}3^{e3})^2$ 。

$$E_0(\mathrm{F}_p) : \ y^2 = x^3 + 6x^2 + x \quad (2)$$

curve. $E(F_{\mathrm{q}})$ At a point on, Q = is realized by the operation $E / \langle R \rangle$ Operation, where K is a prime number. The operation here is usually floating-point fast scalar multiplication, which is the core module of the whole supersingular elliptic curve, and is also the place where the main computation of the whole supersingular elliptic curve encryption and decryption is concentrated. Except for scalar multiplication, other algorithms can be ignored.

here $P_2 \in E_0(\mathrm{F}_{P^2})$, $Q_2 \in E_0(\mathrm{F}_{P^2})$ 。 Both of the above points exist in a discrete set of primes. 2^{e2} And form a combination of $\{P_2, Q_2\}$ belongs to $E_0[2^{e2}]$。

The two points defined based on feature 3 are P_3 、 Q_3 , here $P_3 \in E_0(\mathrm{F}_{P^2}) \setminus E_0(\mathrm{F}_P)$, $Q_3 \in E_0(\mathrm{F}_P)$ Both of the above points exist in the set of discrete primes. 3^{e3} And form the combination $\{P_3, Q_3\}$

belongs to $E_0[3^{e3}]$。

In the specific key distribution process, Alice imports the function of the private key based on feature 2 as follows: sk_2 , while Bob obtains the private key based on feature 3 sk_3 。 sk_2 、 sk_3 The two functions are obtained respectively by E_A 、 E_B The hyperbola performs the key distribution operation.

2.4 Optimization algorithm for ladder solution of supersingular elliptic curves based on scalar operation endomorphism sparsity

In order to solve the problem of curve solving in the authentication process of the Internet of Things with limited computing resources, according to the above analysis of the supersingular elliptic curve encryption algorithm, this paper proposes a ladder solving optimization algorithm of supersingular elliptic curve based on scalar operation endomorphism sparsity, which improves the running speed and resource consumption. According to the characteristics of discrete curve solving, we first label the leaf nodes, label the key nodes, and then traverse the tree in a depth-first manner, and output the node labels when they are encountered. The output of the optimized structure tree will be simplified from the original { 4,3,2,2,2,1 } to { 3,1,1,1,1,1 }, so as to achieve a more simplified higher-order endomorphism solution structure.

As shown in Figure 3 below, the number of layers for solving the supersingular elliptic curve data encryption is optimized. In the face of the full binary fast scalar tree structure, the degree of adhesion between layers is gradually broken and thinned. Because the elliptic curve follows the Homer criterion, the linearization method is used to deal with it. In the process of linear processing, a more compact variable endomorphism operation is realized in a non-adjacent sparse way in the part of the leaf node by breaking the loop. The specific implementation steps are as follows:

The first order is R_0 As a starting point and as an initial leaf node, cannot be thinned out. Calculated here ℓ , and get $\phi_0 : E \to E_0$;

The second order is ℓR_0 And R_1 Linear optimization is performed for the order value, and its output value is the discrete center point of the third order; here The output value of the third order can be thinned, ℓR_0 And R_1 As a leaf node. And calculate synchronously ℓ^2 , get $\phi_1 : E \to E_1$;

The third order is $\ell^2 R_0$ And R_2 Linear optimization is performed for the order value and the center value of the second order, and the output values are two discrete center nodes of the fourth order. Here, since the central node of the second order is optimized, only the order value is retained here as well $\ell^2 R_0$ And R_2 As a leaf node. And calculate synchronously ℓ^3 , get $\phi_2 : E \to E_2$;

The fourth order is $\ell^3 R_0$ And R_3 Linear optimization is performed for the order value and the discrete center value of the third order, and the output values are three discrete center points of the fifth order. Again, here only $\ell^3 R_0$ And R_3 As a leaf node. And calculate synchronously ℓ^4 , get $\phi_3 : E \to E_3$;

The fifth order follows $\ell^4 R_0$ And R_4 The current optimization is carried out for the order value and the discrete central value of the fourth order. In order to ensure the integrity of the final output node, according to the depth-first principle, the left and right discrete points of the fifth order are retained as leaf nodes for solution, which are retained here. $\ell^4 R_0$ And R_4 And two discrete points of the fifth order as leaf nodes. Synchronous calculation ℓ^5 , get $\phi_4 : E \to E_4$;

The sixth order is the final output set of the whole endomorphism solving structure, which is obtained by calculation. $\ell^4 R_0 \to \ell^4 R_1$ 、 $\ell^3 R_0 \to \ell^3 R_2$ 、 $R_4 \to \ell R_4$ 、 $R_3 \to \ell^2 R_3$, here with $\ell^5 R_0$ 、 $\ell^4 R_1$ 、 $\ell^3 R_2$ 、 $\ell^2 R_3$ 、 ℓR_4 、 R_5 Is the final output point and forms an endomorphism solving set.

The above six steps are the endomorphism sparse method based on scalar operation. After the lightweight optimization of the sparse method, the computational complexity of the whole discrete curve is reduced from 2^{21} Reduce to 2^{17} The computing speed and the implementation area are greatly improved.

2.5 Key exchange method of supersingular endomorphic key exchange algorithm based on two-channel exchange of random prime numbers

In order to solve the problem of low key exchange efficiency in SIKE algorithm, this paper also proposes a key exchange method of supersingular elliptic curve encryption algorithm based on random prime channel exchange. The key exchange operation based on Diffie-Hellman scheme mainly uses six-way key data processing to solve the problem, and its computational

$$\mathrm{sk}_2: \quad E_A \xleftarrow{\Phi_A} E_0 / \langle([\mathrm{sk}_2]P_2 + Q_2)\rangle \quad (4)$$

$$\mathrm{sk}_3: \quad E_B \xleftarrow{\Phi_B} E_0 / \langle([\mathrm{sk}_3]P_3 + Q_3)\rangle \quad (5)$$

After the above calculation, Ailce obtained by exchanging through 6 channels E_{AB} Bob gets E_{BA} 。

$$E_{AB} \xleftarrow{\Phi_{AB}} E_B / \langle([\mathrm{sk}_2]\Phi_B(P_2) + \Phi_B(Q_2))\rangle \quad (6)$$

$$E_{BA} \xleftarrow{\Phi_{BA}} E_A / \langle([\mathrm{sk}_3]\Phi_A(P_3) + \Phi_A(Q_3))\rangle \quad (7)$$

complexity mainly focuses on the two processes of point doubling operation and data exchange, that is, the iteration of the protocol and the exchange of intermediate data are used to realize the operation. Therefore, this paper optimizes the solving process of key exchange, simplifies the solving process of starting point mutual operation and the exchange process respectively, and proposes the following key exchange process.

In order to simplify the exchange process, the definition of the mutual operation point is directly

$$P_2 = [3^{e_3}](i+c, \sqrt{f(i+c)}) \quad (8)$$

$$Q_2 = [3^{e_3}](i+c, \sqrt{f(i+c)}) \quad (9)$$

$$P_3 = [2^{e_2-1}](c, \sqrt{f(c)}) \quad (10)$$

$$Q_3 = [2^{e_2-1}](c, \sqrt{f(c)}) \quad (11)$$

Here $P_2 \in E_0(\mathrm{F}_{P^2})$, $Q_2 \in E_0(\mathrm{F}_{P^2})$, $P_3 \in E_0(\mathrm{F}_{P^2}) \setminus E_0(\mathrm{F}_P)$, $Q_3 \in E_0(\mathrm{F}_P)$. The four points obtained directly by the initialization formula P_2 、 Q_2 、 P_3 、 Q_3 The key will be distributed through the mutual operation as a public parameter of the SIKE encryption algorithm.

$$\phi : E \to E / \langle R \rangle \quad (12)$$

$$R = \langle [m]P + [n]Q \rangle \quad (13)$$

$$\phi_A: \ E_0 \to E_A = E_0 / \langle [m_A]P_2 + [n_A]Q_2 \rangle \quad (14)$$

$$\phi_B: \ E_0 \to E_B = E_0 / \langle [m_B]P_3 + [n_B]Q_3 \rangle \quad (15)$$

Obtained through the above calculation ϕ_A 、 ϕ_B , and get R_{AB} 、 R_{BA} , and the intermediate state is obtained by the mutual operation of the formulas 14 and 15 $\phi_A^{'}$ 、 $\phi_B^{'}$;

$$R_{AB} = \langle [m_A]\phi_B(P_2) + [n_A]\phi_B(Q_2) \rangle \quad (16)$$

$$R_{BA} = \langle [m_B]\phi_A(P_3) + [n_B]\phi_A(Q_3) \rangle \quad (17)$$

$$\phi_A^{'} : E_B \to E_{AB} \quad (18)$$

$$\phi_B^{'} : E_A \to E_{BA} \quad (19)$$

Finally, through the exchange of two channels, we can get E_{AB} 、 E_{BA} 。

$$E_{AB} = E_B / \langle ([m_A]\phi_B(P_2) + [n_A]\phi_B(Q_2)) \rangle \quad (20)$$

$$E_{BA} = E_A / \langle ([m_B]\phi_A(P_3) + [n_B]\phi_A(Q_3)) \rangle \quad (21)$$

After the above exchange function solving process is optimized, on the premise of reducing certain security, the key exchange complexity of the (SIKE) algorithm is greatly reduced, the overall efficiency can be greatly improved, and the anti-quantum computing attack can be realized on the premise of ensuring the limited computing capacity of the existing Internet of Things gateway.

carried out on the initialization curve. Initialize the curve $E_0(\mathrm{F}_p): \ y^2 = x^3 + 6x^2 + x$ The calculation of the above four points directly adopts the initialization curve function, namely $f = x^3 + 6x^2 + x$ The equation is used to solve the characteristic points, where C is the smallest non-negative integer in the set of prime numbers, and the specific formula for calculating the four points is as follows.

Through the optimization of the above parameters, the key distribution process will be further simplified. A key exchange process based on prime channel at any time is proposed. The optimization of point doubling operation is realized by exchanging parameters, which is different from that obtained by exponential operation proposed in formulas 4 and 5 sk_2 、 sk_3 Two functions, directly by introducing two sets of random prime coefficients m_A 、 m_B And n_A 、 n_B This is an important innovation of this project, which can greatly reduce the computational cost of characteristic point coefficients. Solve approximately by random prime coefficients, as calculated by higher endomorphisms in the previous section ϕ_A 、 ϕ_B To implement the exchange; the solve calculation function is shown below :

3 Experimental process and results

The Supersingular elliptic curve encryption optimization algorithm based on scalar operation endomorphism sparsity and random prime number channel exchange proposed in this paper is mainly designed for Internet of Things device gateway authentication, in order to confirm the feasibility of the theoretical method and the practicability of the specific application. A complete verification test is carried out from six steps of algorithm verification, resource evaluation, prototype verification, performance comparison and case test. All experiments were performed on a workstation equipped with an intel I9-10900k, 64GB memory, 2 * RTX3090, 1 T pcie3.0 SSD. The specific experimental process is as follows:

Algorithm design. The algorithm design of ladder solution optimization of supersingular elliptic curve based on scalar operation endomorphism sparsity is carried out, and the key exchange method of supersingular endomorphism key exchange algorithm based on random prime number double-channel exchange is realized. The implementation of the optimization of supersingular elliptic curve ladder solving based on scalar operation endomorphism sparsity is as follows.

Algorithm : Computing degree 6 Isogeny Using Optimum Computational Strategy
1 .Input: Starting curve E, kernel generator point R corresponding to le isogeny map, computational strategy {s1, s2, . . . , se−1} and a list of points (P1, P2, . . .) Result: Image curve $E \to E/\langle R \rangle$ corresponding to isogeny map (-) of degree le, the list of image points (-(P1), -(P2), . . .) on E0 2. if e == 1 (empty strategy) then 3. $E \to E/\langle R \rangle$ (Compute degree l isogeny) 4 .Return E0, (-l(P1), -l(P2), . . .) 5 .end 6 .n = s1 7. Left = s2, . . . , se−n and Right = se−n+1, . . . , se−1 8 .T = [ln]R 9 .Compute E, (U, P1, P2, . . .)= Recurse on E, T, (R, P1, P2, . . .) with strategy Left 10. Compute E, (P1, P2, . . .)= Recurse on E, U, (P1, P2, . . .) with strategy Right

Data simulation. Based on the above algorithm, the corresponding model is designed, and the simulation is verified by Matlab tool, and the waveform is compared with modelsim to confirm that the optimization effect is in line with expectations. In the course of the experiment, the algorithm will be corrected according to the waveform, and the problems of the existing algorithm will be solved by online debug to ensure that it is consistent with the expected optimization effect.

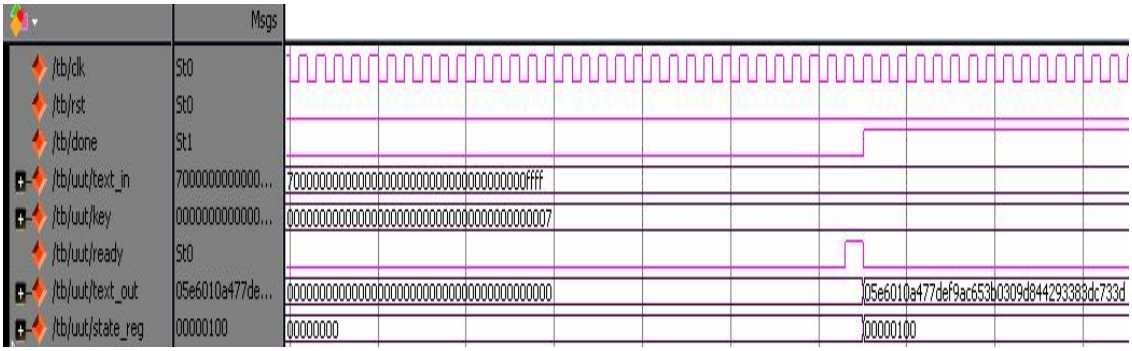

Fig. 1 Simulation of two-channel key exchange process based on random prime number

Prototype verification, the entire prototype verification platform will be oriented to the application scenario of this project, namely, the Internet of Things gateway security encryption application, prototype verification development platform. The algorithm proposed in this paper is implemented by FPGA, using workstation as the simulation data center, using PC as the simulation terminal of the Internet of Things, and the gateway module is implemented by ARM on SOC, which constitutes a preliminary simulation and verification platform. However, at present, the platform can only verify the function, and lacks the necessary encryption attack platform to analyze the security.

Performance comparison: After the functional prototype verification is completed on the FPGA platform, the post-quantum encryption algorithms such as AES, ECC, SIKE algorithm and SIDH algorithm are selected for functional comparison, and the number of resource gates, DSP, RAM, ROM and other basic ASIC units are used as reference for comparison.

After the prototype simulation and resource comparison, a real Internet of Things platform will be built for example testing. Through 5G and other ultra-high-speed data transmission, the instance platform will add embedded units to the gateway application devices corresponding to the Internet of Things devices, run encryption algorithms, and conduct instance testing through the corresponding authentication platform. Through the experiment, the FOM index (FOM = throughput/ares spuared), which is commonly used in the lightweight optimization process of the algorithm, is evaluated, and the FOM value proposed in this paper can reach more than 300.

4 Conclusion

In order to solve the problems of limited computing resources and the inability to resist quantum attacks faced by the security of intelligent Internet of Things gateway devices, this paper investigates the post-quantum encryption algorithm, and proposes that the post-quantum encryption algorithm with the shortest key, that is, the super-singular endomorphic key exchange algorithm (SIKE algorithm), can be applied to the Internet of Things gateway authentication after being lightweight. In the optimization process of the SIKE algorithm, it is known through analysis that the existing algorithm can be optimized in the two parts of solving the high-order endomorphic discrete curve and exchanging the key, so the optimization of the algorithm is realized by solving

the ladder optimization of the homomorphic sparse supersingular elliptic curve and exchanging the double channels of random prime numbers, which has achieved the purpose of optimizing the lightweight encryption algorithm.

Funding

This work is partially supported by Shenzhen Education Science "14TH FIVE-YEAR PLAN"2021 Subject: Research on online learning emotion analysis and intelligent tutoring based on collaborative perception of multi-modal education data(ybzz21015), Key technology research and innovative application demonstration of intelligent education(2019KZDZX1048), Guangdong Key Laboratory of Big Data Intelligence for Vocational Education(2019GKSYS001), Shenzhen Vocational Education Research Center Jointly Established by the Ministry and the Province(6022240004Q).

Reference

[1] Koziel Brian et al. Post-Quantum Cryptography on FPGA Based on Isogenies on Elliptic Curves[J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2017, 64(1) : 86-99.

[2] Pessl P , Bruinderink L G , Yarom Y . To BLISS-B or not to be: Attacking strongSwan's Implementation of Post-Quantum Signatures[C]// the 2017 ACM SIGSAC Conference. ACM, 2017.

[3] Majot A , Yampolskiy R . Global catastrophic risk and security implications of quantum computers[J]. Futures, 2015, 72:S0016328715000294.

[4] Anton Stolbunov. Constructing public-key cryptographic schemes based on class group action on a set of isogenous elliptic curves. Advances in Mathematics of Communications, 4(2):215–235, 2010

[5] Andrew Childs, David Jao, and Vladimir Soukharev. Constructing elliptic curve isogenies in quantum subexponential time. Journal of Mathematical Cryptology, 8(1):1–29, 2014

[6]David Jao and Luca De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In International Workshop on Post-Quantum Cryptography, pages 19–34. Springer, 2011

[7] Cheng C , Lu R , Petzoldt A , et al. Securing the Internet of Things in a Quantum World[J]. IEEE Communications Magazine, 2017, 55(2):116-120.

[8] Joye M , Yen S M . Optimal left-to-right binary signed-digit recoding[J]. IEEE Transactions on Computers, 2000, 49(7):740-748.

[9] Saarinen M J O . Ring-LWE Ciphertext Compression and Error Correction: Tools for Lightweight Post-Quantum Cryptography[C]// Acm International Workshop on Iot Privacy. ACM, 2017.

[10] Basu Roy D , Mukhopadhyay D . [IEEE 2018 IEEE Computer Society Annual Symposium on VLSI (ISVLSI) - Hong Kong (2018.7.8-2018.7.11)] 2018 IEEE Computer Society Annual Symposium on VLSI (ISVLSI) - Minimalistic Perspective to Public Key Implementations on FPGA[C]// 2018:381-386.

[11] Fan J , Hsieh M H , Chen H , et al. Construction and Performance of Quantum Burst Error Correction Codes for Correlated Errors[J]. 2018.

[12] Roetteler M , Naehrig M , Svore K M , et al. Quantum resource estimates for computing elliptic curve discrete logarithms[J]. 2017.

[13] Oliveira B D , Fábio. On Privacy-Preserving Protocols for Smart Metering Systems || Selected Privacy-Preserving Protocols[J]. 2017, 10.1007/978-3-319-40718-0(Chapter 6):61-100.

[14] Solat S . Security of Electronic Payment Systems: A Comprehensive Survey[J]. 2017.

[15]Bonilla L L , Carpio A . Control challenges in semiconductor nanostructure devices[C]// European Control Conference Cdc-ecc 05 IEEE Conference on Decision & Control. IEEE, 2020.

[16] Yi H , Nie Z . High-speed hardware architecture for implementations of multivariate signature generations on FPGAs[J]. EURASIP Journal on Wireless Communications and Networking, 2018, 2018(1):93.

[17] Sasikaladevi N , Geetha K , Srinivas K N V . A multi-tier security system (SAIL) for protecting audio signals from malicious exploits[J]. International Journal of Speech Technology, 2018, 21(3):1-14.

[18] Yi H , Nie Z . Side-channel security analysis of UOV signature for cloud-based Internet of Things[J]. Future Generation Computer Systems, 2018:S0167739X18304151.

[19] Boneh D , Eskandarian S , Fisch B . Post-quantum EPID Signatures from Symmetric Primitives: The Cryptographers' Track at the RSA Conference 2019, San Francisco, CA, USA, March 4–8, 2019, Proceedings[C]// 2019.

[20] Bobrysheva J , Zapechnikov S . Post-Quantum Security of Communication and Messaging Protocols: Achievements, Challenges and New Perspectives[C]// 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). IEEE, 2019.

[21] Chacón, Iván Blanco. Ring Learning With Errors: A crossroads between postquantum cryptography, machine learning and number theory[J]. 2019.

[22] Dong X , Zheng L I , Wang X . Quantum cryptanalysis on some generalized Feistel schemes[J]. Science China(Information Sciences), 2019, 62(02):180-191.

[23] Li Y , Unruh D . Quantum Relational Hoare Logic with Expectations[J]. Proceedings of the ACM on Programming Languages, 2019.

[24] Jo Y , Bae K , Son W . Enhanced Bell state measurement for efficient

measurement-device-independent quantum key distribution using 3-dimensional quantum states[J]. Scientific reports, 2019, 9(1):687.

[25] Cai J , Jiang H , Zhang P , et al. An Efficient Strong Designated Verifier Signature Based on R-SIS Assumption[J]. IEEE Access, 2019, PP(99):1-1.

[26] Abusukhon A, Anwar M N, Mohammad Z, et al. A hybrid network security algorithm based on Diffie Hellman and Text-to-Image Encryption algorithm[J]. 2019, 22(5):1-17.

[27] Mizuide T, Takayasu A, Takagi T. Tight Reductions for Diffie-Hellman Variants in the Algebraic Group Model[C]// Cryptographers' Track at the RSA Conference. 2019.

[28] Bobrysheva J, Zapechnikov S. Post-Quantum Security of Communication and Messaging Protocols: Achievements, Challenges and New Perspectives[C]// 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). 2019.

[29] Huang Y, Bo C, Ma X. Research on the status and problems of psychological teaching in colleges and universities based on Diffie–Hellman key exchange algorithm[J]. Cluster Computing, 2018(2):1-7.

[30] Abusukhon A, Anwar M N, Mohammad Z, et al. A hybrid network security algorithm based on Diffie Hellman and Text-to-Image Encryption algorithm[J]. 2019, 22(5):1-17.

[31] Karati A, Islam S H, Karuppiah M. Provably Secure and Lightweight Certificateless Signature Scheme for IIoT Environments[J]. IEEE Transactions on Industrial Informatics, 2018, PP(99):1-1.

[32] Bai Y. Research on the effect of psychological stress intervention in music students based on Diffie–Hellman key exchange algorithm[J]. Cluster Computing, 2018(2):1-7.

[33] Dongyoung Roh, I-Yeol Kim, Sang Geun Hahn. The l -th power Diffie–Hellman problem and the l -th root Diffie–Hellman problem[J]. Applicable Algebra in Engineering Communication & Computing, 2018, 29(2):1-17.

[34] Sakai Y, Attrapadung N, Hanaoka G. Practical attribute-based signature schemes for circuits from bilinear map[J]. Iet Information Security, 2018, 12(3):184-193.

[35] Muir J , Stinson D . Minimality and other properties of the width-[J]. Mathematics of Computation, 2006, 75(253):369-384.

[36] Saarinen M J O . The BlueJay Ultra-Lightweight Hybrid Cryptosystem[C]// Security and Privacy Workshops (SPW), 2012 IEEE Symposium on. IEEE, 2012.

[37] David Jao and Luca De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In International Workshop on Post-Quantum Cryptography, pages 19–34. Springer, 2011