IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 22, Issue 4, Ser. III (Jul. – Aug. 2020), PP 33-37
www.iosrjournals.org

Survey on Quantum Resist Public Key Algorithms Compatible for Java Card

Hithaishi P[1], Vinay Prasad M S[2]
Electronics & Communication Department, JSS Science &Technological University, India
Electronics & Communication Department, JSS Science &Technological University, India

Abstract
Public key cryptography is now a vital element of our global communication digital infrastructure.Most of our important communication protocols depend on primary cryptographic functionalities for secure communicationThe invention of quantum machines are likely to be applied to unravel certain challenges when compared with classical computer systems, which has stimulated good curiosity about quantum computing.Quantum computer systems are now being developed are capable of breaking much of the current public key system, undermining the privacy and protection of digital internet communications and post-quantum encryption, aiming at building systems that are immune to, and adaptable to, existing communication systems, protocols and networks.Java Cards that happen to be utilized extensively in enormous applications Presently, algorithms that are used for public key cryptography in Java Cards are prone to quantum attacks. Public key algorithms that are quantum safe will come under Post quantum cryptography. This paper surveys quantum resistant algorithms that could be new alternative to current standard scheme for public key identification to employ Quantum safe Security in Java Cards.

Keywords: *Java Cards, Quantum Computer, Public key cryptography , Post Quantum Cryptography .*

Date of Submission: 17-08-2020 Date of Acceptance: 03-09-2020

I. Introduction

1.1 Quantum Computer

A quantum computer is a computing technology used to perform data operations using specific quantum mechanical properties, such as superposition and entanglement.Data is stored as bits on a standard computer, on a quantum computer it is stored as qubits. Potential quantum Machine development is capable of solving problems we don't want to solve. Cryptography is focused on complex mathematical problems, including large numbers.Standard equations can be solved by quantum computers in a short space of time. The efficiency of the Integer factorization of quantum computers is presumed to be computationally impracticable with an ordinary large computer[12].

Using Shor's algorithm to find its factor, an quantum computer effectively resolves this problem. This technology will allow a quantum computer to crack cryptographic structures currently in use, and Quantum computers promise advantages whenit comes to solving computationally complicated problems that classical computers cannot solve[13].Computer scientists as well as quantum physicists have been debating the use of quantum mechanics for computational purposes for years. The two algorithms most commonly developed are Shor 's algorithm, and Grover 's algorithm.

1.2 Java Card

Java Card is an advanced, Java and Virtual Machine-based smart card programming platform. The main development challenge for Java Card technologies is to fit Java device functionality into a smart card while maintaining enough space for applications[2][3].The approach is to include the subset of the Java language features and to use a distributed model to implement the virtual machine. Java cards have the tremendous ability to implement cryptographic algorithms within their embedded chip and calculate the keys internally[12].Java-cards do have built-in, self-programmable memory for special use ofmicro - controller. Together, these features make the cost of a malicious attack much greater than the benefits[11].

Supported Java Features	**Unsupported Java features**
primitive data types: Boolean, byte, short	primitive data types: long, double, float
One-dimensional arrays	Characters and strings
packages, classes, interfaces, and exceptions	Multidimensional arrays

inheritance, virtual methods, overloading	Dynamic class loading
dynamic object creation	Security manager
access scope	Garbage collection and finalization
binding rules	Threads
int keyword	Object serialization
32-bit integer data type	Object cloning

Table:1*List Java features supported and un-Supported on Java-Card*

II. Public Key Cryptosystem on Java Cards

The RSA and elliptic curves are two main cryptographic Public-Key algorithms deployed on the Java Card. RSA uses modulo numbers for operations of large integer numbers. RSA security hinges on key size[11].Security keys of at least 768 bits can currently be used on timely fashion. Given that elliptic curve mathematical model is more complicated than the one used in the RSA scheme, studies suggest elliptic-based cryptosystems can use smaller key sizes to achieve an equivalent degree of safety.It is important to assess that the elliptic curves of 163-bit correspond to 1024-bit RSA, while the elliptic curves of 223-bit conform to 2048-bit RSA. Signing with elliptic curves is six times better for these bit-lengths but testing an RSA signature is seven times faster[10]. Shorter keys also mean lower requirements on memory.

Current co-processors of smart cards can do 1024-bit computations, and some can also do 2048-bit computations. Using technologies like the Chinese Remainder Theorem (CRT) these chips can work up to 4096 bits on operands of the size. Verification of a signature is much faster than signing.

III. Impact of Quantum Attack on Java Cards

Quantum computers have the ability to crack current encryption algorithms used to protect all Java cards and most other Cryptographic systems Upon arrival all current algorithms including RSA and ECC will be challenged. While covered, this will have an effect on Internet standards as well as smart cards, industrial control systems on servers, online banking and more.Key techniques for establishing an authenticated session between two parties on the commercially available card chip for implementing post-quantum public key scheme. The problems would include limited chip size and insufficient memory space to store and execute such a complicated algorithm, as well as the processing speed.Post-quantum cryptography will have a degree of protection equal to that of RSA and ECC in the present computing environment in a world of quantum computers. In addition, key lengths must be longer than the RSA 2048 bits or 256 bits norm of the ECC in order to resist the quantum calculation.

3.1 Attacks on Public key Cryptosystemon Java Card

All Asymmetric key techniques utilized currentlytoday are based on the Factorization and Discrete Logarithm mathematical problems.

RSA cryptosystem is based on the factorization process, RSA is used primarily for the cryptographic exchange of end-node messages and is often used in conjunction with symmetric algorithms where the symmetric algorithm is used for the encryption and decryption of raw data.RSA becomes potentially vulnerable when Quantum Computers implement a rapid factorization algorithm or when computational power is significantly increased.

Diffie-Hellmanand Elliptic Curve Cryptography (ECC) are based on Discrete Logarithmic Problem. The complexity of breaking such cryptosystems is based on evaluating the integer r in the equation the $g^r = x \bmod p$.Pervasive use of ECC cryptosystems such as ECDH and ECDSA leads to hypothetically vulnerable to quantum computingThe problem with the discrete logarithm structure is that it's very difficult to calculate when the variables are significantly large. [17].

Public Key Cryptography	Purpose	Size	Quantum Attack
RSA	encryption	128-bit	Broken (Shor's)
DH& DSA	Key Exchange	128-bit	Broken (Shor's)
ECDH& ECDSA	Key Exchange	128-bit	Broken (Shor's)

Table:2*Attacks on Public key Cryptography*

Large-number factorization and discrete logarithm problem have a common theoretical framework from the implementation point of view, and it can easily be cracked with Shor algorithm[14].Kirsch and Chow mentioned the idea to use a revised Shor algorithm to decrypt ECC-encoded data[43].

In comparison, they observed that the ECC's relatively small key size makes it more vulnerable to quantum attacks compared to the RSA[32]. Proos and Zalka have shown that a 1000-qubit quantum computer could split 160-bit elliptic curves, while a 2000-qubit quantum computer will mostly need for a 1024-bit RSA factorization[31].

The amount of qubits needed to break a cryptosystem is proportional with the implemented algorithm. Shor 's algorithm may lead to the downfall of modern asymmetric cryptography, since it is built on either large prime integer factorization or a discrete logarithm problem[14].Vazirani presented a detailed review of Shor 's algorithm and demonstrated that a new overlay can set up initiating from twoarbitrary integer inoverlay state and executing a series of Fourier transformations to give us two entities that will satisfy a high probability equation[30].By using this equation we can determine the unknown "exponent" value r in the discrete logarithm problems.

IV. Standard Quantum Resist Algorithms

The implementations that are researched are as follows:

- Multivariate Public-Key Cryptography
- Lattice-based cryptography
- Code based cryptography
- Super singular elliptic curve isogeny cryptography

4.1 Multivariate Public-Key Cryptography

Multivariate schemes provide alternative problem other than factoring and discrete logarithmic problem. multivariate key strength is its fundamental mathematical principle in solving a sequence of multivariate quadratic (MQ) polynomial equations in a finite field known as an NP-hard problem[7][33].

The Oil and Vinegar signature scheme proposed by Kipnis and Patarin in 1999 The Rainbow signing scheme introduced by Ding and SchmidtCould be called a multi-layer UOV variant, convincing algorithms for digital signatures[27].The SRP encryption algorithm by Yasuda et al is yet another possible candidate for a multivariate polynomial-based public-key encryption scheme[36]. The system combines several multivariate schemes to one, avoiding several of the known multivariate schemes vulnerabilities, the key sizes are relatively large

Multivariate schemes provide vast advantages over other post-quantum cryptosystems.Multivariate schemes only involve basic mathematical calculations in small finite areas, and can therefore be applied effectively to low-cost devices such as Java cards and RFID chips, which allows multivariate cryptosystem relevant to protection on the Internet of Things.The biggest disadvantages of multivariate schemes are the high key size. The public key size of MPKC's is typically around 100 kB, and much larger than those of standard schemes such as RSA and lattice based cryptosystems.

4.2 Lattice-based cryptography

Lattice based cryptographic schemes are built on lattices. Structures based on lattices are immune to attacks on both traditional and qubits computers[26]. This has proposed several solutions to designing public key encryption system depends on the hardness of the lattice problems.It also relies on another encryption method, called Fully Homo-morphic Encryption (FHE).This encryption method helps in performing calculations on a document without uncovering sensitive data to malware [34].

Ajtai and Dwork have described and graded a public-key cryptosystem based on hidden hyperplane hardness, Ajtai-Dwork cryptosystem is of theoretical significance only. In his later work, Ajtai introduced a more robust version of the cryptosystem distinguished by cryptographic keys and ciphertext sizes of $Oe(n^2)$ and Oe(n) [4].In modern lattice cryptography, almost all methods are derived from the idea of Short Integer Solution (SIS) and Error Learning (LWE) two typical computational Techniques. Regev presented the average-case problem known as Learning with errors Problem. Ring-LWE is more commonly referred to as Learning with Errors over Rings, and is simply a larger lattice problem with errors (LWE) devoted to polynomial rings over finite fields.It is based upon arithmetic polynomial with coefficients selected from a finite field[35].

Public-key, cryptography based on the Lattice is extremely intriguing. At the one hand the programs seem very easy to incorporate. If schemes are chosen in ideal lattices that depend on hard issues, then there is very small, at least asymptotic, storage space and computing time available.

4.2 Code based cryptography

Code-based cryptographic system, where the basic algorithm (the simple one-way function) uses code C for error correction. This approach works by adding an error to a term of C, or computing a parity check matrix of C [15].The public-key encryption scheme McEliece and its variations are the current candidates for the scheme for post-quantum encryption. The first cryptographic algorithm based on coding theory was the

public-key encryption method, adopted by McEliece in 1978.Almost all asymmetric cryptographic programs subsequently implemented based on coding theory have a certain limitation over its large memory needs.

Niederreiter suggested a PKC-type knapsack based on codes corrected by mistake.Niederreiter, and others,Estimated generalized Reed-Solomon codes as permissible cryptography codes that were intended to demand lesser key sizes than Goppa codes[38]. However, 1992 observed Sidelnikov and Shestakov prove that Niederreiter 's attempt to use GRS codes was unsafe[40]. With its original version, McEliece cryptosystem remains unbroken,Encryption and decryption in McEliece scheme can be performed very quickly. But the keys are tall in contrast.Incomparison to the McEliece cryptosystem, Niederreiter suggested encoding the text into the error vector rather than representing it as a codeword.

For these schemes the only significant issue is the key size. The key size would be of one megabyte at a high level of Security requirement. In order to enable more compression, some newer code-based systems implemented more framework into public keys, but all of these proposals were compromised.The original McEliece / Niederreiter systems are the one of the public-key-encryption systems for post-quantum cryptography that have given enough survey to suggest for implementation .

4.3 Super singular elliptic curve isogeny cryptography

Among the most widely used cryptographic algorithms for the public key, the Diffie-Hellman key exchange (ECDH) elliptic curve is vulnerable to attacks using quantum computers.Isogenic cryptography provides the closest quantum-safe primitives to the ECDH [25].Two parties in SIDH wish to reach agreement on a key. The form is similar to that of Diffie-Hellman, the key difference being that a type of relation between elliptic curves, called isogeny, replaces the scalar multiplication. Because of calculating the image of a point P under two separate functions, the parties also measure the image of the entire elliptic curve under the two different functions Both parties begin with the same elliptical curve E.

The above algorithms are focused on the hard problem of finding isogeny between elliptic curves. Terms of two elliptic curves it has been considered incredibly difficult to locate an isogeny from one elliptic curve to the other. Relative to other quantum-safe protocols, isogeny-based algorithms are considered to have substantially smaller key sizes.SIKEp751, for example, needs public keys of about 400 bytes to achieve 124-bit quantum protection SIDH differs from ECDH by substituting isogeny's for scalar multiplication. Combining quantum-safe algorithms with an proven classical algorithm is often suggested [41][42].There is a hybrid algorithm explicitly for added security which combines SIDH with the closely monitored ECDH. This can be done easily, since both use elliptic curves. Compared with other post-quantum algorithms, because of its small key sizes, SIDH appears to be well suited for implementing on memory constrained devices. On the other hand, SIDH is computationally complex, leading presumably to long calculation times.

V. Conclusion

Java card is an extremely restricted computational resource capable of safely running applets, the idea of migrating the security system from current algorithms to quantum resistant algorithms due to the extensive use of the java card needed work on cryptographic algorithms immune to quantum attacks.Post Quantum cryptography plays a crucial role in the implementation of Java Card quantum resistance algorithms. from the above-mentioned Post Quantum Algorithms survey, cryptography based on the Lattice is considered secure against quantum computer attacks. Error learning (ring-LWE) cryptosystem, one of the lattice-based cryptosystem variants, has high performance , reliability and good functionality that enables us to implement PQC,encryption scheme using matrices are advisable for the implementation in Java card, In java card messages are represented either as binary data or bit stream. Ring-LWE methods uses bit-wise encryption method which is best suitable for Public Key Encryption and Digital signature in Java Card.

References

[1]. Johannes, Buchmann ,Denis Butin, Florian G¨opfert, and Albrecht Petzoldt,"Post-Quantum Cryptography: State of the Art", Springer Heidelberg LNCS 9100, pp. 88–108, (2016)

[2]. Songyan Liu,Zhigang Mao&Yizheng Ye "Implementation of Java card Virtual Machine"Journal of Computer Science and Technology volume 15, pages591–596 2000

[3]. ShardhaPorwal,HimanshuMittal"An Efficient Memory Management Technique For Smart Card Operating System" International Journal OF Computers & Technology 5(2):124-129 · June 2006

[4]. Ajtai, M.: "Generating hard instances of lattice problems" Annual ACM Symposium on Theory of Computing, STOC 1996, pp. 99–108. (1996)

[5]. Daniel J, bernstein1 , Tanja Lange : "Post-quantum cryptography" ,Springer Nature VOL 549, September (2017)

[6]. Lily Chen Stephen Jordan Yi-Kai Liu Dustin Moody Rene Peralta, Ray Perlner, Daniel Smith-Tone : "Report on Post-Quantum Cryptography", NISTIR 8105 , April(2016)

[7]. Jintai Dingand Bo-Yin Yang : "Multivariate Public Key Cryptography"

[8]. Raphael Overbeck and Nicolas Sendrier : "Code-based cryptography"

[9]. Douglas Stebila1and Michele Mosca, : "Post-Quantum Key Exchange for the Internet and the Open Quantum Safe Project" *NISTIR 8309*,July (2019)

[10]. Zhang Peng and Jia Jian Fang : " Comparing and Implementation of Public Key Cryptography Algorithms on Smart Card"ICCASM ,(2010)
[11]. David Naccache and David M'Ra¨ıhi " Cryptographic Smart Cards " IEEE Micro 16(3):14–24, (1996)
[12]. Padamvathi, B. V. Vardhan and A. V. N. Krishna, "Quantum Cryptography and Quantum Key Distribution Protocols: A Survey," 2016 IEEE 6th International Conference on Advanced Computing (IACC), Bhimavaram, 2016, pp. 556-562, doi: 10.1109/IACC.2016.109.
[13]. N. Imoto, "Quantum cryptography," Technical Digest. CLEO/Pacific Rim '99. Pacific Rim Conference on Lasers and Electro-Optics (Cat. No.99TH8464), Seoul, South Korea, 1999, pp. 9-10 vol.1, doi: 10.1109/CLEOPR.1999.811587.
[14]. S. P. Jordan and Y. Liu, "Quantum Cryptanalysis: Shor, Grover, and Beyond," in IEEE Security & Privacy, vol. 16, no. 5, pp. 14-21, September/October 2018, doi: 10.1109/MSP.2018.3761719.
[15]. M. Baldi, "Post-Quantum Cryptographic Schemes Based on Codes," 2017 International Conference on High Performance Computing & Simulation (HPCS), Genoa, 2017, pp. 908-910, doi: 10.1109/HPCS.2017.151.
[16]. Johan Borst, Brat Preneel,Vincent Rijmen : " Cryptography on Smart Cards" Computer Networks 36 423-435 (2001)
[17]. Gayoso Martinez and L. Hernandez Encinas : "Developing ECC Applications in Java Card" IEEE(2013)
[18]. Vasileios Mavroeidis, Kamer Vishi, Mateusz D. Zych, AudunJøsang : "The Impact of Quantum Computing on Present Cryptography", IJACSA Vol. 9, No. 3, 2018
[19]. LIU Songyan,MAOZhigang,YEYizheng: "Implementation of Java Card Virtual Machine " J. Computer Science & Technology .Vol.15 No.6 Nov. 2000
[20]. Ebo van der Laan, Erik Poll, Joost Rijneveld , Joeri de Ruiter, Peter Schwabe, and Jan Verschuren1: "Is Java Card ready for hash-based signatures" ICT-645622 project 13114 June,(2018)
[21]. Logan O. Mailloux, Charlton D. Lewis II, Casey Riggs, and Michael R. Grimaila,"Post-Quantum Cryptography" IEEE Computer Society 1520-9202/16,(2016)
[22]. Jintai Ding and Albrecht Petzoldt : "Current State of Multivariate Cryptography" IEEE Security and Privacy Magazine,January (2017)
[23]. Daniel R. Simon "On the Power of Quantum Computation" IEEE (1994)
[24]. Martin E. Hellman : "An Overview of Public Key Cryptography"
[25]. Cong Peng ,Peng Cheng Laboratory : "Jianhua Chen Isogeny-Based Cryptography: A Promising Post-Quantum Technique",IEEE Computer Society December 2019
[26]. Hamid Nejatollahi,NikilDutt, Sandip ,Ray,Regazzoni,AlariIndranil Banerjee,RosaiCammorota:"Post-quantumLattice-basedCryptographyImplementationsASurvey"ACMComputingSurveys,Vol.1,No.1,Article1.January(2018)
[27]. Le Van LuyenAn, "Improved Identity-Based Multivariate Signature Scheme Based on Rainbow"Cryptography(2019)
[28]. Ryan Amiri, Erika Andersson: "Unconditionally Secure Quantum Signatures",Entropy ISSN 1099-4300,(2015)
[29]. John Proos, Christof Zalka:"Shor's discrete logarithm quantum algorithm for elliptic curves", QIC 3 (No. 4) (2003)
[30]. Xie, H., Yang, L. Using Bernstein–Vazirani algorithm to attack block ciphers. *Des. Codes Cryptogr.* **87,** 1161–1182 (2019).
[31]. John Proos, Christof Zalka "Shor's discrete logarithm quantum algorithm for elliptic curves" Quantum Information & Computation 3 (No. 4) (2003) pp.317-344
[32]. Zach Kirsch,Ming Chow "Quantum Computing: The Risk to Existing Encryption Methods"Computer Systems Security Computer Science 116 (December 15, 2015)
[33]. JOUR,Khokhar, Umar M,YiHaibo "Under Quantum Computer Attack: Is Rainbow a Replacement of RSA and Elliptic Curves on Hardware?"Security and Communication Networks Hindawi(2018)
[34]. Gentry C., Sahai A., Waters B. (2013) Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asyptotically-Faster, Attribute-Based. In: Canetti R., Garay J.A. (eds) Advances in Cryptology – CRYPTO 2013. CRYPTO 2013. Lecture Notes in Computer Science, vol 8042. Springer, Berlin, Heidelberg.
[35]. Oded,Regev "The Learning with Errors Problem" Citeseer (2010)
[36]. Yasuda, T., and Sakurai, K. A multivariate encryption scheme with Ranbow. In ICICS 2015, vol. 9543 of Lecture Notes in Compu. Sci. Springer, 2016, pp. 222 236.
[37]. R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory", DSN Progress Report, pp. 114-116, 1978.
[38]. SendrierN.Niederreiter Encryption Scheme. In: van Tilborg H.C.A., Jajodia S. (eds) Encyclopedia of Cryptography and Security. Springer, Boston, (2011)
[39]. V. D. Goppa, "A new class of linear correcting codes", *Probl. Pered. Info.*, vol. 6, no. 3, pp. 24-30, 1970.
[40]. V. M. Sidelnikov S. O. Shestakov "On the insecurity of cryptosystems based on generalized Reed-Solomon codes. Discrete Math. Appl., 2:439–444, (1992).
[41]. L. De Feo, D. Jao and J. Plût, "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies", J. Math. Cryptol., vol. 8, no. 3, pp. 209-247, 2014.
[42]. Rostovtsev and A. Stolbunov, "Public-key cryptosystem based on isogenies", *IACR Cryptol. ePrint Archive*, vol. 2006.
[43]. Z. Kirsch, "Quantum Computing: The Risk to Existing Encryption Methods," Ph.D. dissertation, Tufts University, Massachusetts, 2015.

Hithaishi P, et. al. "Survey on Quantum Resist Public Key Algorithms Compatible for Java Card." *IOSR Journal of Computer Engineering (IOSR-JCE)*, 22(4), 2020, pp. 33-37.