ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

Your Signature is Assured: Post-Quantum Cryptography

Anna N Kurian[#1], Ashly Thomas[*2]
[#] *Department of Computer Science and Engineering, St. Joseph's College of Engineering and Technology, Palai, Kerala, India.*
anna.n.kurian95@gmail.com

[*] *Department of Computer Science and Engineering, St. Joseph's College of Engineering and Technology, Palai, Kerala, India.*
ashly.thomas@sjcetpalai.ac.in

***Abstract* — Cryptographic techniques are crucial for the secure communique in cutting-edge society. As increasingly more commercial enterprise processes are performed through the internet and the necessity for efficient cryptographic answers will grow in near future. Nearly all cryptographic schemes practically used are based on difficulty of solving two problems: factoring of large complex integers and tackling the discrete logarithms. However, schemes based on these problems became unreliable when large quantum computer systems are built. In quantum computers numeric and theoretic problems which includes factorization of integers and discrete logarithms were tackled down in polynomial time. The principle reason behind is the Shor's algorithm. Therefore requires immediate alternative options for those classical public key schemes. Besides the lattice, code and hash based cryptosystems, multivariate cryptography is considered to be a most promising candidate. Besides the resistance against quantum computer attacks, the multivariate schemes are fast and needs only modest computational requirements, which makes them more appealing for the use on low-cost devices like RFID (Radio Frequency identification) chips and smart cards. The paper presents a comprehensive review on diverse signature schemes used in Multivariate Post-Quantum Cryptography literature. Moreover highlights the problems in multivariate signature scheme.**

Keywords: Cryptography, Quantum Computers, Post-Quantum Cryptography, Multivariate Public Key Signature Schemes, Low-cost devices.

I. INTRODUCTION

In the business world, the communique among trading partners needs to be remain confidential. Even private user deals with cryptography every day. Common examples are online shopping and downloading of a software application. When logging in to an electronic mail account or moving over the website of a bank, cryptographic techniques are used too. As increasingly business processes are accomplished via the internet (e.g. via cloud computing) and due to new application like e-voting and digital payment, the need for efficient cryptographic solutions will show nonetheless growth in near future. The most often used cryptographic primitives are encryption and digital signature schemes. Encryption schemes guarantee the confidentiality of information so an attacker cannot get any records approximately the content of the encrypted message. Besides that signature schemes make sure that the message genuinely comes from the sender (authentication) and that it was not changed after the signing process (data integrity). For contracts it is also vital that none of the signers forget the validity of the settlement (non- repudiation), which can also be guaranteed with the aid of a digital signature scheme.

Today, nearly all the cryptographic signature schemes practically used are primarily based on mathematical problems, specifically the factorization of large complex integers and the solving of discrete logarithms. Diverse internet and industry standards use asymmetric cryptography based fully on RSA or the Elliptic Curve Cryptography (ECC), to protect their data communication between smart cards, smart phones, computer systems, servers, or industrial control systems.

Taking an instance, with the RSA algorithm a Public-Key Encryption (PKE) scheme can be realized that permits it to send an encrypted email (e.g., with PGP/ GPG or S/MIME) to a recipient. There states no requirement that first to exchange a symmetric key though a securedchannel, the public key of the recipient is enough to achieve confidentiality.Other applicationsof asymmetric cryptography are digital signatures, which are based upon RSA or ECC. Theyare used to sign and verify information. The public key is involved to check the validity of asignature. If anyone tries to modify a digitally signed agreement or long term archives aftersigning, even with the aid of a single bit, the digital signature test fails. Both PKE and digitalsignatures are critical in Transport Layer security (TLS) protocol [1] which is the spine of securedcommunication within the inter-

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

net and utilized by browsers, smart-phones and exponentiallyon Internet of Things (IoT) devices.

However, Peter Shor's[2],[3] work, it's miles regarded that RSA and ECC are prone toattacks through quantum computer systems. A quantum computer is powerful enough toput into effect that Shor's algorithm might allow the factoring of the public key of the RSAcryptosystem in polynomial time. Moreover, the algorithm also can be tailored to breakcompletely ECC-based public keys. Another quantum algorithm proposed by Grover[4] whichcan be used to exponentially accelerate brute-force attacks on symmetric block ciphers likeAdvanced Encryption Standard(AES). But, it does not result in a whole ruin but roughly halvesof the bit-security level of symmetric algorithms. The key length of algorithms is 128-bit and thus inorder to increase the security it doubles (moving to AES-256)[5].

In this paper, we present a comprehensive survey on the emerging Multivariate Public KeyCryptographic signature schemes. We start by providing a comparison between Post-QuantumCryptography and Quantum Cryptography in section II. This is followed by variations in PostQuantum Cryptography in section III, and section IV highlights why we are choosing MultivariatePublic Key signature schemes.Various signature schemes are discussed and also states variousproblems faced by multivariate signature schemes in section V and section VI respectively. Finallysection VII concludes the paper.

II. POST-QUANTUM CRYPTOGRAPHY VERSUS QUANTUM CRYPTOGRAPHY

Quantum Cryptography (QC)[6] or to be more specific the Quantum Key Distribution (QKD),uses properties of the quantum mechanics to generate a secret key for communiqué among two parties. This secret key can then be used to encrypt a bulk amount of data using classic symmetric ciphers like AES. The security of QKD is not only based upon the computational assumption that the measurement of a quantum state (e.g., of the spin of a photon) destroys the state and that quantum states would be protected from being copied. If a passive attacker conducts a measurement to obtain the key, this attack could be easily detected by the receiver. However, QKD cannot be a universal replacement of RSA and ECC.

TABLE 1.
POST-QUANTUM CRYPTOGRAPHY VERSUS QUANTUM CRYPTOGRAPHY

Post Quantum Cryptography	Quantum Cryptography
Handles wide range over secure communication task	Only expanding a short shared secret into long shared secret
Proven to be secure	Reject conjectural systems
Does not require additional hardware	Requires additional hardware

In contrast, the Post-Quantum cryptography (PQC)[7] refers to new cryptographic algorithms executed on classical computers that are expected to be efficiently secured against attackers using quantum computers and have the same high-level behaviour as currently available ciphers. So that they can act as a universal drop-in replacement. Currently, the main concern of researchers in PQC is asymmetric cryptography (i.e., replacing RSA and ECC) as the threat of Grover's algorithm[4] to symmetric schemes can be mitigated by moving to already available 256-bit secured algorithms. Table 1 shows the comparison of Post-Quantum Cryptography and QuantumCryptography.

III. POST QUANTUM CRYPTOGRAPHY

The main goal of post-quantum cryptography (also called quantum-resistant cryptography) is to develop new cryptographic systems that are secure against both quantum and classical computers, and at the same time which can also interoperate with existing communications protocols and networks. Mainly focus moves over the public key signature schemes of post quantum cryptography. Figure 1 shows the variations in Multivariate Public Key Signature-Schemes.

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

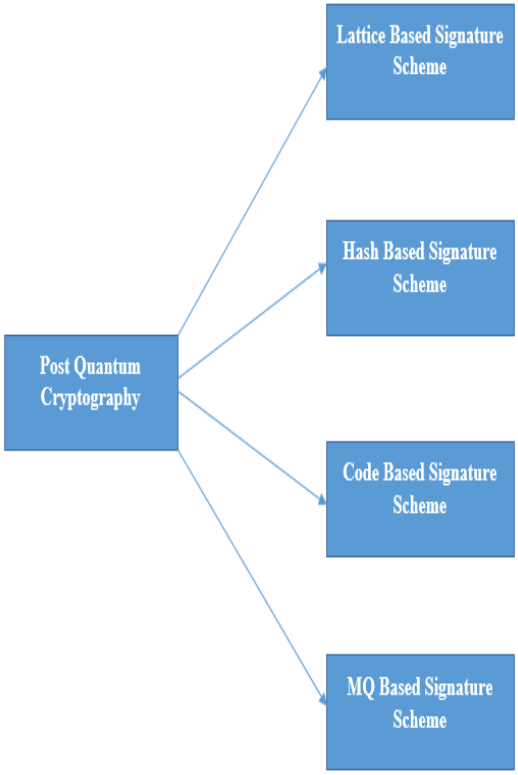

Fig. 1 Variations of Multivariate Public Key Signature Schemes

A. *Lattice based public-key signature scheme*

Lattice-based cryptographic constructions are primarily based on the presumed hardness of lattice problems, the most basic one is the shortest vector problem. The most well-known and widely studied algorithm for lattice problems is the LLL algorithm, which was developed in 1982[8].

B. *Hash Based Public Key Signature Schemes*

In hash based, the construction of cryptographic primitives based on the security of hash functions. A hash function is defined any function that is used to map data of arbitary size to data of fixed size. This signature system requires a standard cryptographic hash function H. The signer starts by generating a secret x and then computes y = H(x). The signer includes, in the signed message, a newly generated public key that is used to sign the next message. The verifier checks first the signed message, including the new public key, and then checks thesignature of the next message; finally the signature of the n^{th} message includes all the n-1 previously signed messages.

C. *Code based public-key signature scheme*

Code-based cryptography is one of the mathematical techniques that enables the construction of public-key cryptosystems which are secure against an adversary equipped with a quantum computer. The receiver's public key is a dt*n matrix K with coefficients in F2. Messages which are suitable for encryption are of n-bit strings of weight t, i.e., n-bit strings having exactly tbits and is set to be 1. To encrypt a message m, the sender just simply multiplies K by m, and produces a dt-bit ciphertext called Km. The basic problem is syndrome-decode K, which undo the multiplication done by K, if known that the input had weight t. It is easy, with aid of linear algebra, which forth backward from Km to some n-bit vector v such that Kv = Km but there exist huge number of combination for v, and finding a correct weight-t choice seems to be an extremely difficult task.

D. *Multivariate public-key signature scheme*

Solving Multivariate public-key signature scheme is an N-P Hard problem, so it is considered as a promising candidate in Post-Quantum Cryptography. Signature provides the authenticity of the message as well as shortest signature among other Post-Quantum algorithms.

IV. WHY CHOOSING MULTIVARIATE QUANTUM BASED CRYPTOGRAPHY?

The critical advantage of this signature system over hash-based signature systems is that each signature generated is short. Other multivariate-quadratic systems have even shorter signatures and, in many cases, much shorter public keys. The advantages of using Multivariate quantum based cryptography are:

- Signing and verification speed
- Modest computational requirements
- Hardness of solving the MQ-Problem.

V. SIGNATURE SCHEMES

Cryptosystems scheme are based upon the difficulty of solving systems of multivariate equations. There are various attempts to build a secure multivariate equation encryption schemes but have failed. However multivariate signature scheme particularly the rainbow could provide a secure basis for a quantum secure digital signature generation. T. Matsumoto

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

and H. Imai[9]in 1988, proposed the first MQ public-key scheme the MI scheme. The scheme introduces Small fields-Big fields into the designation of MI. The algorithm C* was broken[10], but it has a great advantage over HFE[11] scheme in terms of computation efficiency.

In Hidden Field Equations, encryption, signatures or authentications are done in an asymmetric way and is resistant against attacks, generate shorter encrypted message. IP (Isomorphisms of Polynomials)[11]are used for asymmetric authentication or signatures. IP authentications are of zero knowledge. In[11] designed a new scheme, called Oil and Vinegar" for the computationof asymmetric signatures. It is simple, can be computed very fast (both in secret and public key) and requires very little RAM usage in smartcard implementations. The main idea was to hide quadratic equations in n unknowns called oil" and v = n unknowns called vinegar" over a finite field K, with the aid of linear secret functions. This scheme was broken in [12]. A very simple variations of the original scheme where v> n (instead of v = n), called Unbalanced Oil and Vinegar" (UOV), since have more vinegar" unknowns than oil" unknowns.

In ZHFE scheme[13],the low degree of polynomial is obtained from the two high rank HFE polynomials, by a special reduction method which uses Hamming weight three polynomials produced from the two high rank HFE polynomials. In Unbalanced Oil-Vinegar Signature scheme it is easy to combine the Oil and Vinegar idea with HFE schemes[10]. The resulting scheme, then called HFEV, the length of a UOV signature can be as shorter as 192 bits and for HFEV it can be as shorter as 80 bits [14].

Rainbow [15] is one of the most important signature schemes in MPKC. It provides a strong security guarantee and a faster verification. None of the existing attacks can cause severe security threats. However, it has not been widely used because of its large key size. Therefore, reducing the size of private and public keys of Rainbow provides an important research direction. Another scheme stepwise triangular matrix which use a triangular structure for their central equations[16]. This idea was used to develop birational permutation schemes [17] over the large finite rings. But broken towards inversion attack and structural attack and is practically insecure to use.

Cyclic Rainbow[18] to reduce the public key size of Rainbow and to improve the verification speed by inserting some cyclic relations into generation of public key and accelerated the verification using the relations.

Several variants of Rainbow using sparse private keys have been proposed to reduce the size of private key and improve the signing process, e.g. Enhanced TTS[19], MB Rainbow[20], NT Rainbow[21]. The overall idea of the schemes is to use several layers of UOV trapdoors and make them as sparse as possible. It admits shorter key size and faster signing speed. However, it was broken by a variant of Rainbow-Band-Separation (RBS) attack in[21] it lacks cross-terms of Vinegar variables and Oil variables. The method of reducing private key size of Rainbow using sparse key[20],[21],survived now. Yasuda et al. proposed MB Rainbow, which divides each layer of Rainbow into smaller blocks by using diagonal matrix representations.The private key size of the MB Rainbow is smaller by 40% than that of original Rainbow and its signing speed is sped up by 40%. Then again proposed NT Rainbow, introduces some rotating relations into Vinegar-Vinegar terms of the central map of Rainbow. It can also be combined with MB Rainbow to improve Rainbow. However, the MB Rainbow is vulnerable to a variant of RBS attack and suggested parameter sets of NT Rainbow are not large enough to resist against RBS attack.

Tao et al. proposed amultivariate quadratic encryption scheme calledSimplematrix Encryption, or simply ABC Encryption [22]. Their main construction idea: embedding the polynomial matrix arithmetic inside the central trapdoor function. The inversion of trapdoor can be performed with high probability because the matrix, albeit evaluated over a single point,can be easily reconstructed from the output. With high probability, it give rise to a system of linear equations which describe the input. Then[23] a new central trapdoor formultivariate quadratic (MQ) public-key cryptosystems that allows for encryption, in contrast to time-tested MQ primitives such as Unbalanced Oil and Vinegar or Hidden Field Equations which only allow for signatures.

A new Rainbow variant called Circulant Rainbow [24], provides a new way to reduce the size of private key and improves the signing speed of Rainbow. The security parameters chosen makes Circulant Rainbow secure against all known attacks. The size of private key of Circulant Rainbow is smaller by 45% than that of original Rainbow. The implementation results predominantly reveals that Circulant Rainbow is about 3 times faster than original Rainbowand it outperforms many other signature schemes in both signing and verification speed. Table 2 presents an overview of the existing signature scheme and the attacks which broken the security of the schemes.

TABLE 2.
AN OVERVIEW OF THE EXISTING SIGNATURE SCHEMEAND THE ATTACKS WHICH BROKEN THE SECURITYOF THE SCHEMES.

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

Signature Schemes	Description	Vulnerable to Security attacks
MI Scheme	•First MQ Public key scheme. •Introduces "Small fields-Big fields". •C* Algorithm	• Linearization attack • Differential attack
HFE and IP	• Multivariate polynomials of degree two-asymmetric cryptography. • HFE-Encryption and shorter signatures • IP-Authen tication (Zero Knowledge)	• Cubic attack • Affine multiple attack • Relinearization attack • Min Rank attack
Unbalanced Oil vinegar Scheme	• v>n	• UOV attack
ZHFE Scheme	• Combine 2 HFE high rank polynomial	• UOV Reconcilation attack
Rainbow Schemes	• Strong security • Large key size	• Rainbow Band separation attack • UOV Reconcilation attack
Stepwise triangular matrix	• Birational permutation schemes over finite field. • Practical insecure	• Inversion attack • Structural attack
Cyclic Rainbow	• Reduce public key size • Improve verification speed • Cyclic relations into generation of pubic key	• Rainbow Band separation attack • UOV Reconcilation attack
Enhanced TTS	• Sparse Private keys • Use several layers of UOV trapdoors • Faster signing speed	• Rainbow Band separation attack • UOV Reconcilation attack
MB Rainbow	• Divides each layer of rainbow into smaller blocks. • Using diagonal matrix representations	• Rainbow Band separation attack • UOV Recon oncilat cilation attack
NT Rainbow	• Introduces rotating relations into vinegar-vinegar cross terms of the central map of rainbow.	• Suggested parameter can reduce RBS attack
ABC Encryption Scheme	• Simple matrix encryption • Embedding polynomial matrix arithemetic inside the central trapdoor function	• High Rank attack
Circulant Rainbow	• Improve signing speed of rainbow • Reduce private key size • Verification speed • Uses circulant matrix	• No attacks exist

VI. PROBLEMS IN MULTIVARIATE SCHEMES

A. Choice Of Parameter In Multivariate Schemes

The question of which parameter values have to be selected for cryptosystems to achieve required levels of security is one of the central concern that has not been yet answered so far.

B. Reduction Of Size Keys For Multivariate Schemes

In multivariate schemes the size of keys are in the range of 10-100 kB and is much larger than those in the classical public key cryptosystems such as RSA and ECC. The size of private key can be decreased by using a small random seed and a Pseudo Random Number Generator (PRNG), but the concern is how to reduce the public key size. By reducing size of the public key a cryptographic scheme, can reduce the data traffic by a significant factor and the size of certificates as they are used in many public key infrastructures (PKI's).

C. Development Of Multivariate Schemes With Provable Security

Another problem in multivariate cryptography is that the lack of security proofs. There are many exam-

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

ples for multivariate schemes which were considered to be secure but broken later. For example for such a scheme is the C*scheme of Matsumoto and Imai[9], which was broken by Patarin's Linearization Equations [10]. Soon after that the original scheme was modified byreplacing some of the public equations (Minus-Modification).There exist no security proofs yet.

VII. CONCLUSION

The multivariate cryptography is an asymmetric cryptographic primitives, based upon multivariate polynomials over the finite fields. Difficulty of solving cryptosystems of multivariate polynomial equations makes them NP-Hard or NP-complete which is the main reason that those schemes are regularly taken into consideration and be good promising candidate for post- quantum cryptography. The various multivariate public key signature schemes begins from MI Scheme to the variants of Rainbow schemes were evaluated. On comparing the signing efficiency of the signature schemes the circulant rainbow seems to be a better choice, but the public key size, signing and verification speed can be improved better.

REFERENCES

[1] Mohamad Badra "Securing Communications between Multiple Entities using a single TLS Session" in 2011 4th IFIP Int. Conf. on new technology, mobility and security,2011.

[2] Shor P W "Algorithms for Quantum computation: discrete logarithms and factoring" in Proc.35th Annual Symposium. Found. Computing. Sci. Nov. 1994 pp.124-134

[3] Shor P W "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer" SIAM Rev., 1999, Vol.41 pp 303-332

[4] Sakhi Z, Kabil R, Tragha A and Bennai M "Quantum cryptography based on Grovers Algorithm", 2nd Int. Conf.on the Innovative Comput. Techn. (INTECH 2012), 2012, pp 33-37.

[5] Jianyoung Huang ,Wily Susilo and Hennifer Seberry "Repeated Differential Properties of the AES-128 and AES-256 Key Schedules" IEEE 10th Conf. on trust, security and privacy in comput. and comm., 2011 pp 525-532.

[6] Fengyou Sun and Yuming Jaing "Performance guarantees in quantum key distribution networks"2017 IEEE Globecom Wrk. 2017, pp 1-6.

[7] Bernstein D J, Buchmann, and Dahmen E, "Post-Quantum Cryptography" Springer-Verlag, 2009.

[8] Lenstra A K and Lovasz L "Factoring polynomials with rational coefficients", Math. Ann. 1982, pp 4515-4534

[9] Patarin J "The Oil and Vinegar Signature Scheme", Dagsthul Wrk. on crypto. Sept.1997.

[10] Patarin J "Hidden Fields equations (HFE) and Isomorphisms of polynomials (IP): Two new families of asymmetric algorithms" in Proc. Int. Conf. Theory Appl. Crypto. Techn., Spain, 1996, pp 33-48.

[11] Kipnis A and Shamir A "Cryptanalysis of the oil and vinegar signature scheme" in Proc. Annu. Int. Cryptol. Conf. 1998,pp 257-266

[12] Porras J,Baena J, and Ding J "ZHFE, a new multivariate public key encryption scheme in Proc. 6th Int. Wrk. (PQCrypto), Oct.2014, pp 229-245.

[13] Kipnis A, J Patarin and Goubin L "Unbalanced oil and vinegar signature schemes" in Proc. Int. Conf. Theory Appl. Crypto. Technique., 1999, pp 206-222.

[14] Ding J "A new variant of the Matsumoto-Imai cryptosystem through perturbation" in Proc. Int. Wrk. Public Key Crypto., 2004, pp 305-318

[15] Ding J and Schmidt D "Rainbow, a new multivariable polynomial signature scheme" in Proc. Int. Conf. Appl. Crypto Netw. Secur., 2005 pp 164-175.

[16] Wolf C, Braeken A, and Preneel B "On the security of stepwise triangular systems" Des., Codes Crypto., 2006, pp 40285-40302

[17] Ding J,Gower J E, and Schmidt D S "Oil-Vinegar signature schemes" Multivariate Public Key Cryptosys. New York: Springer, 2006, pp 63-97

[18] Petzoldt A, Bulygin S, and Buchmann J "Cyclic Rainbow- A Multivariate signature scheme with a partially cyclic public key" in Proc. 11th Int. Conf. Crypto., Hyderabad, India, 2010, pp 33-48.

[19] Yang Y and Chen M "Building secure tame-like multivariate public-key cryptosystems: The new TTS" in Proc. Austral. Conf. Inf. Secur. Privacy, 2005, pp 518-531.

[20] Yasuda T,Ding J,Takagi T, and Sakurai K "A variant of rainbow with shorter secret key and faster signature generation" in Proc. 1st ACM Wrk. Asia Public-Key Crypto., 2013 , pp 57-62.

[21] Yasuda T, Takagi T and Sakurai K "Efficient variant of Rainbow using sparse secret keys J. Wireless Mobile Netw. Ubiquitous Comput.,Dependable , 2014, pp 5313

[22] Thomae C and Wolf C "Cryptanalysis of enhanced TTS, STS and all its variants, or: Why cross-terms are important" in Proc. 5th Intl. Conf. Crypto. Africa, 2014.

[23] Tao C, Diene A, Tang S, and Ding J "Simple matrix scheme for encryption" in Proc. PQ Crypto. 2013, pp 13231-13242

[24] Szepieniec A, Ding J, and Preneel B "Extension Field Cancellation: A new central trapdoor for multivariate quadratic systems" in Proc. Int. Wrk. Post-Quantum Crypto., 2016, pp 182-196.

[25] Zhiniang Peng, Shaohua Tang "Circulant Rainbow: A New Rainbow Variant with Shorter Private key and faster signature generation IEEE Access, 2017.

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)

Vol. 5, Special Issue 12, April 2018