NEW DIRECTIONS IN FORGING MULTIVARIATE SIGNATURE SCHEMES

By

NURUL AMIERA SAKINAH BINTI ABDUL JAMAL

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Degree of Master of Science

August 2023

IPM 2023 10

DEDICATION

Dedicated to me. It’s me.
Hi, I’m the problem, it’s me.

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Master of Science

NEW DIRECTIONS IN FORGING MULTIVARIATE SIGNATURE SCHEMES

By

NURUL AMIERA SAKINAH BINTI ABDUL JAMAL

August 2023

Chair : Professor Muhammad Rezal Kamel Ariffin, PhD
Institute : Mathematical Research

Quantum computer is a revolution in the realm of cryptography, as it can break conventional cryptographic hard problems such as RSA and DLP. Transitioning to post-quantum cryptography requires new hard problems that resist to quantum computer attacks, such as the multivariate quadratic problem (MQP). MQP is a hard problem in multivariate cryptography, where one needs to find a solution to a system of multivariate quadratic equations. This thesis focuses on attacking MQP under four distinct cases. In these scenarios, the rogue certificate authority (RCA) intervenes during the key generation of multivariate public key cryptosystems (MPKC). The first case considers polynomials in MQP can be expressed as multiples of other polynomials within the same system. By inheriting these characteristics, MQP can be resolved by finding a solution to only one polynomial from MQP system of equations. The second case considers polynomials in MQP can be expressed as additions of two other polynomials within the same system. The second case of MQP is solvable by finding a solution to any two polynomials within the same MQP system of equations. The first and second cases are vulnerable to forgery due to the potential for RCA to generate weak public keys with characteristics inherited from both cases. Therefore, two strategies to identify the generated weak public key by RCA are laid out for the users. The assumption in the third case is, after generating the public-private key pair the RCA computes one solution vector, prior handing over the key pair to the owner. An adversary who receives the solution vector can produce a valid forged signature for any message. The fourth case assumes that the public key system is constructed from slightly modified secret keys based on quadratic factorisation formula. By substituting one designated value for the first variable, one can solve the whole public key system. This forgery mechanism allows an adversary to produce many forged signatures for any message. To identify the forged signatures of the third and fourth cases is still an open question. The forgery mechanisms that are based on the four cases are executed on two significant multivariate signature schemes, namely UOV and Rainbow. We show that UOV signature scheme is vulnerable in all four cases since the form of secret central map is easy to satisfy. Whereas Rainbow signature scheme is safe from forgery in the

first, second and fourth cases. It is only vulnerable to the third case as the forgery strategy does not involve any amendment on either the public key or the private key.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Master Sains

HALA TUJU BAHARU PEMALSUAN DALAM SKEMA-SKEMA TANDATANGAN PELBAGAI-PENGUBAHSUAI

Oleh

NURUL AMIERA SAKINAH BINTI ABDUL JAMAL

Ogos 2023

Pengerusi : Professor Muhammad Rezal Kamel Ariffin, PhD
Institut : Penyelidikan Matematik

Komputer kuantum adalah suatu revolusi dalam dunia kriptografi, kerana ia boleh menyelesaikan masalah kriptografi konvensional yang sukar seperti RSA dan DLP. Peralihan kepada kriptografi pasca-kuantum memerlukan masalah-masalah sukar yang baru yang ampuh terhadap serangan komputer kuantum, seperti masalah kuadratik pelbagai-pembolehubah (MKP). MKP adalah masalah yang sukar dalam kriptografi pelbagai-pembolehubah, di mana seseorang perlu mencari penyelesaian bagi sebuah sistem persamaan kuadratik pelbagai-pembolehubah. Tesis ini memfokuskan penyelesaian MKP di bawah empat kes berbeza. Senario tersebut melibatkan campur tangan dari penguatkuasa sijil yang jahat (PSJ) ketika menjana kunci untuk sistem kriptografi kekunci awam pelbagai-pembolehubah. Kes pertama mempertimbangkan keadaan di mana polinomial dalam MKP boleh ditulis dalam bentuk gandaan polinomial lain dalam sistem yang sama. Apabila polinomial tersebut mempunyai kriteria seperti ini, MKP dapat diselesaikan dengan mencari penyelesaian hanya pada satu polinomial dari sistem persamaan MKP. Kes kedua mempertimbangkan polinomial dalam MKP boleh ditulis dalam bentuk hasil tambah dua polinomial lain dalam sistem yang sama. Kes MKP kedua boleh diselesaikan dengan mencari penyelesaian kepada sebarang dua polinomial dalam sistem persamaan MKP yang sama. Kes pertama dan kedua rentan terhadap pemalsuan kerana kemungkinan RCA akan menghasilkan kunci awam yang lemah yang mempunyai ciri-ciri daripada kedua-dua kes tersebut. Oleh itu, dua strategi untuk mengenal pasti kunci awam yang lemah yang dihasilkan oleh RCA diperkenalkan untuk pengguna. Andaian dalam kes ketiga adalah, sebelum PSJ tersebut menyerahkan sepasang kunci awam-rahsia yang dijana kepada pengguna, mereka mempunyai satu vektor penyelesian. Seorang musuh yang menerima vektor penyelesaian tersebut daripada PSJ boleh menggunakannya untuk menghasilkan tandatangan palsu untuk sebarang mesej. Kes keempat mengandaikan bahawa system kekunci awam dibina daripada kekunci rahsia yang telah diubahsuai berdasarkan

formula pemfaktoran kuadratik. Dengan menggantikan satu nilai yang ditentukan untuk pembolehubah pertama, seseorang dapat menyelesaikan keseluruhan sistem kekunci awam. Mekanisma pemalsuan ini membenarkan seseorang musuh untuk menghasilkan banyak tandatangan untuk sebarang mesej. Untuk mengenalpasti tandatangan palsu yang dihasilkan daripada sistem ini pula masih menjadi suatu tanda tanya. Mekanisma pemalsuan berdasarkan keempat-empat kes tersebut dijalankan ke atas dua skema tandatangan pelbagai-pembolehubah yang penting, iaitu UOV dan Rainbow. Kami tunjukkan bahawa skema tandatangan UOV adalah tidak selamat dalam keempat-empat kes kerana bentuk peta pusat senang untuk dipenuhi. Manakala, skema tandatangan Rainbow selamat daripada pemalsuan bagi kes pertama, kedua dan keempat. Ianya menjadi tidak selamat di bawah kes ketiga kerana strategi pemalsuan tersebut tidak melibatkan pengubahsuaian ke atas mana-mana kunci awam atau kunci rahsia.

ACKNOWLEDGEMENTS

Alhamdulillah.

All the praises and thanks are to Allah, *Ar-Rahman Ar-Rahim*. Thank you Allah for lighting up my way, for giving me the strength and give me patience. Alhamdulillah, for I am able to complete my Master with remarkable knowledge.

I would like to express my heartfelt thanks to my supervisor, Prof. Dr. Muhammad Rezal Kamel Ariffin, for his invaluable guidance, support, and encouragement throughout my research. His expertise and knowledge in Mathematical Cryptography were instrumental in shaping the direction of my work and developing my skills as a researcher. I really appreciate for the available opportunities to engage with professionals in the related field of my study. Thanks to them, I am able to have a better vision of my career path.

I would like to express my deepest gratitude to my parents Abdul Jamal Bin Arifin and Kamariah Binti Abdullah for their unwavering love, prayers and motivation not only throughout my academic journey, but my whole life. Thank you for trying to understand every difficult processes and steps that I took to complete my Master. I am grateful to them for always giving their best support both physically and mentally. I am forever grateful to my family, Kaklong, Angah, Icha and Akeef for making my life colorful and wonderful with you tremendous love and chaos.

I would like to extend my heartfelt thanks to my friends. Kak Ella, the one whom I always talk about almost everything, who buys me delicious food, and encourages me. She is a friend, a sister and like a mother to me. My besties, Tommy, Donut, Hurin, Sehoh and Hawe, I am endlessly grateful for your attention and time that you spend for me. The laughter and the memories we shared are a source of comfort and joy when going through hard times. My special thanks goes to my annoying companion who always make time for me.

I want to express my gratitude to Universiti Putra Malaysia for their investment in my education through Graduate Research Fellowship (GRF) scheme. I am grateful to the warm-hearted INSPEM's staff for the kind assistance in administrative processes pertaining to my studies.

Incessantly grateful.

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfillment of the requirement for the degree of Master of Science. The members of the Supervisory Committee were as follows:

Muhammad Rezal Bin Kamel Ariffin, PhD
Professor
Institute for Mathematical Research
Universiti Putra Malaysia
(Chairman)

Siti Hasana Binti Sapar, PhD
Associate Professor
Faculty of Science
Universiti Putra Malaysia
(Member)

ZALILAH MOHD SHARIFF, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 9 November 2023

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ALGORITHMS

LIST OF ABBREVIATIONS

DES	Data Encryption Standard
AES	Advanced Encryption Standard
KEM	Key Encapsulation Mechanism
CA	Certificate Authority
RCA	Rogue Certificate Authority
IFP	Integer Factorization Problem
DLP	Discrete Log Problem
NIST	National Institute of Standards and Technology
MQP	Multivariate Quadratic Problem
RSA	Rivest Shamir Adleman
MPKC	Multivariate Public Key Cryptosystems
NP-hard	Non-deterministic polynomial-time hard
3SAT	3-Satisfiability
UOV	Unbalanced Oil and Vinegar
IPP	Isomorphism of Polynomials Problem
IP1S	Isomorphism of Polynomials with One Secret
IP2S	Isomorphism of Polynomials with Two Secrets
EIP	Extended Isomorphism of Polynomials

DSFM1	Digital Signature Forgery Mechanism 1
DSFM2	Digital Signature Forgery Mechanism 2
DSFM3	Digital Signature Forgery Mechanism 3
char $\mathbb{F}_q$	characteristic of $\mathbb{F}_q$

Greek Symbol

$\mathbb{Z}$	Integers

Subscripts

$\mathbb{F}_q$	A finite field with q elements
$\mathbb{Z}_q$	The set of integers less than q

CHAPTER 1

INTRODUCTION

1.1 The Art of Secrecy

Secret writing falls into two methodologies, namely steganography and cryptography. Steganography aims to hide a message or information in various ways, such as embedding the message into a picture without altering its meaning. Whereas cryptography does not hide the message, it uses mathematical techniques to transform plaintext into ciphertext, making it appear as unreadable text. A different mathematical technique is required to recover the original form.

Cryptography enables users to openly distribute processed information without the need to hide it in any manners. The intended recipient must possess the secret knowledge on how to unseal the information. In short, cryptography ensures secure data transfer between two entities who want to communicate without third-party interference. Practically, most secret conversations today happen in the realm of internet, involving encryption and decryption of data.

Secret writing falls into two methodologies, namely steganography and cryptography. Steganography aims to hide a message or information in various ways, such as embedding the message into a picture without altering its meaning. Whereas cryptography does not hide the message, it uses mathematical techniques to transform plaintext into ciphertext, making it appear as unreadable text. A different mathematical technique is required to recover the original form.

Cryptography enables users to openly distribute processed information without the need to hide it in any manners. The intended recipient must possess the secret knowledge on how to unseal the information. In short, cryptography ensures secure data transfer between two entities who want to communicate without third-party interference. Practically, most secret conversations today happen in the realm of internet, involving encryption and decryption of data.

Cryptology is the study of mathematical cryptography, which aims to achieve four specific goals in securing the exchange of information against malicious threats. Firstly, cryptography should ensure confidentiality, ensuring that the message's contents are known only to the sender and the intended recipient, even when transferred through insecure channels like the internet. Secondly, it should ensure authenticity, allowing users to validate the identities of entities present in ongoing communication; otherwise, a foe might pretend to be an ally in order to

gain confidential information from its target. Thirdly, cryptography must ensure data integrity to prevent unwanted alterations by outsiders during information transmission, preserving the message's contents. Lastly, it should support non-repudiation, preventing any entities involved in the communication from denying their actions of sending and receiving data.

1.2 Symmetric Encryption

There are two main operations in cryptography, namely encryption and decryption. Encrypting a message transforms original state of data or plaintext into a ciphertext. Meanwhile, decrypting ciphertext will recover plaintext. Both encryption and decryption require an encryption-decryption key and an encryption-decryption mechanism, which involve well-defined mathematical algorithms.

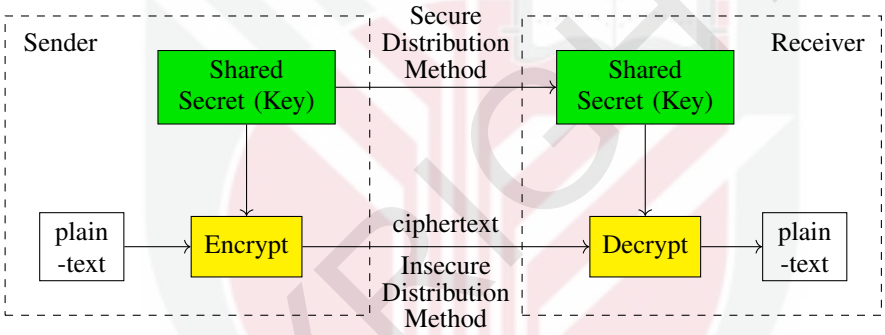

Figure 1.1: Symmetric Encryption

In symmetric encryption, the secret key to encrypt and decrypt is identical. Therefore, all parties wishing to communicate securely must share the same key. Key distribution problem arises as more people involve in the confidential conversation and the key distribution distance becomes impractical. Among famous traditional symmetric cryptography are stream ciphers and block ciphers. Examples of stream cipher are Caesar cipher and Vigenère cipher whereas Hill cipher and playfair cipher are among block cipher. Modern symmetric cryptography, such as Data Encryption Standard (DES) and Advanced Encryption Standard (AES), encapsulates their symmetric keys using asymmetric algorithms. Key encapsulation mechanism (KEM) makes encryption of long messages faster via symmetric encryption, and the exchange of symmetric keys becomes more efficient via asymmetric algorithm.

1.3 Public Key Cryptography

Two significant applications in public key cryptography are public key encryption and digital signature. The keys used for encryption and decryption, or signing and verification are not identical. One of them can be publicly announced and another one should be kept secret.

1.3.1 Public Key Encryption

Asymmetric encryption, or public key encryption, follows a different approach in terms of key generation. One way function, which is easy to compute but hard to reverse, is a fundamental component in asymmetric encryption. One uses an encryption key to compute the one function and uses a different key to reverse the computation. Hence, individuals can publish their encryption keys on the internet, allowing anyone worldwide to send messages encrypted with the public key. The only thing the sender must keep secret is decryption key. Decryption key is generated corresponding to the public encryption key. In other words, decryption key is a secret trapdoor information to one-way function that makes the computation for its inverse becomes relatively easy.

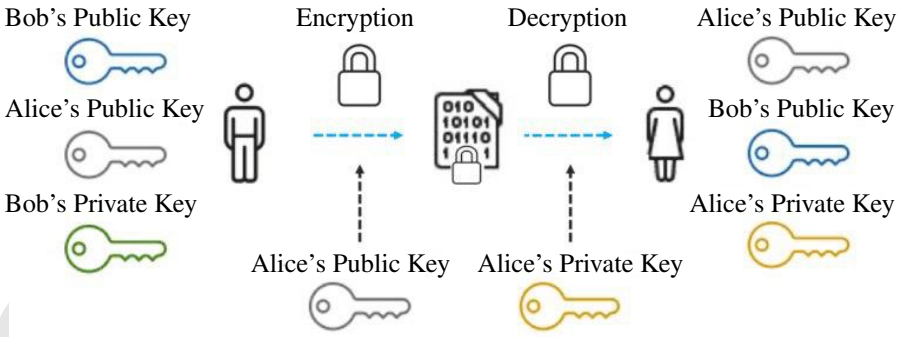

Figure 1.2: Asymmetric Encryption

1.3.2 Digital Signature

Confidentiality of data information can be achieved by encryption either with symmetric or asymmetric encryption. Encryption protects information content from being read by an adversary unless the adversary successfully gains the knowledge of trapdoor information. Other cryptographic requisites: authenticity, integrity and non-repudiation are provided through digital signature.

Two major components in digital signature are signing and validating. Both signing and validating processes of a digital document are mathematical procedures that can prove the identity of entities in communication, prevent entities from denying their actions, as well as preserving the contents of the document. The holder of public key and private key are switched; the sender will sign the document using his or her private key and the verification key is publicize. An adversary will attempt to forge a signature that can pass through verification process, in other words, produce a valid signature by any means.

1.4 Rogue Certificate Authority (RCA)

A certificate authority (CA) is responsible for generating public-private key pairs and serves as a trusted third parties who validates the identity of entities who receive public key certificates issued by CAs. An adversary might target the CA to obtain an equivalent key pair of anyone by impersonating the person so that the CA is tricked and issues the certificate to the adversary. On the darker side, as defined by Dong et al. (2016) a rogue certificate authority (RCA) could join hands with the adversary to generate weak key pairs where the weaknesses are only known to the RCA, thus making forgery easier. Despite inheriting weaknesses, the key pairs appear and work perfectly fine and satisfy security requirements, making it challenging for users to detect rogueness in the certificates.

1.5 Post-Quantum Cryptography

1994 remarked the biggest possible threat on traditional cryptography as Peter Shor, an american mathematician proved that hard problems such as Integer Factorization Problem (IFP) and Discrete Log Problem (DLP) are solvable in polynomial time in the presence of quantum computers.

An algorithm to find prime factors of integers by quantum computation was submitted by Shor (1999) and is widely known as Shor's algorithm. The ability of a quantum computer being in superposition makes solving IFP and DLP feasible. As a result, public-key cryptosystems such as RSA (Rivest et al., 1978), classical Diffie-Hellman key exchange (Hellman, 1976) and Elliptic Curve Diffie-Hellman key exchange (Barker et al., 2017) are at risk.

In continuation to the events, cryptographers aim to study for new hard problems that are resistant to quantum computers. Post-quantum cryptography candidates include multivariate cryptography, hash-based cryptography, lattice-based cryptography and

code-based cryptography. The National Institute of Standards and Technology (NIST) also takes part in preparing for the post-quantum computing era. An announcement by NIST (2016) was made globally requesting for public key post-quantum cryptographic algorithms nominations. The proposed algorithms need to go through continuous evaluations and standardization by NIST. Up till November 2022, Classic McEliece (Albrecht et al., 2020), CRYSTALS-Kyber (Bos et al., 2018), NTRU (Chen et al., 2019) and SABER (D'Anvers et al., 2018) are the finalists for encryption algorithms that have passed the Third Round and become the finalist candidates for Round 4. Meanwhile, the finalists for digital signature algorithms in Round 3 are CRYSTALS-DILITHIUM (Ducas et al., 2018), FALCON (Fouque et al., 2018) and Rainbow (Ding and Schmidt, 2005). The intersection attack and the rectangular MinRank attack on Rainbow signature scheme were proposed by Beullens (2021) can highly reduce the key recovery cost causing the failure of parameter sets to meet the security requirements. Beullens completely broke the Rainbow signature scheme when he presented another key recover attack in Beullens (2022). Despite the attacks, Rainbow is still qualified to be the candidate for Round 4 after Cartor et al. (2022) suggested to add an internal perturbation in the scheme.

1.6 Problem Statement

MQP for underdetermined system is utilised in digital signature so it is important to study its security in order to prevent forgery. The existing algorithms to solve underdetermined MQP only run in polynomial time under the finite fields with even characteristics. The algorithm by Miura et al. (2013) has a narrow applicable range and runs in exponential time for odd finite fields. If there exists a polynomial time algorithm for solving underdetermined MQP given any number of equations and variables, producing a valid forged signature is an easy task.

1.7 Research Objectives

The objectives of this research are:

1. to solve MQP in polynomial time for even and odd finite fields,
2. to extend the applicable range for all type of classes: underdetermined system, determined system and over determined system,
3. to design a forgery strategy upon multivariate signature schemes.

1.8 Research Methodologies

1. We study the behaviour of multivariate quadratic polynomials under two cases:
   (a) when polynomials in $\mathscr{P}$ can be written into multiple of other equations,
   (b) when polynomials in $\mathscr{P}$ can be written into addition of two other equations.

   Based on these conditions, we observe the patterns of solutions and able to solve MQP in polynomial time. Our attacks work for any number of equations and variables.

2. We design four forgery strategies: DSFM1, DSFM2, DSFM3 and a forgery via quadratic structures. Then, the forgery strategies were implemented on UOV and Rainbow signature schemes. We are able to show that both schemes are vulnerable to our attacks in the presence of RCA. Additionally, one of the forgery mechanisms does not require the RCA to generate weak public keys i.e. polynomials in $\mathscr{P}$ are totally random.

1.9 Thesis Outline

This thesis consists of seven chapters and is laid out as follows.

Chapter 1 provides insight into the motivation behind this research by explaining crucial topics in cryptography, including symmetric encryption, public key cryptography, rogue certificate authority, and post-quantum cryptography. Additionally, this chapter highlights the problem statement and research objectives.

Chapter 2 explains the fundamentals of multivariate cryptography, including mathematical expressions, hard problems, the general workflow of multivariate cryptosystems as well as two important multivariate signature schemes in this research, namely UOV and Rainbow.

Chapter 3 recalls pivotal researches related to solving the hard problem of multivariate cryptography, specifically the multivariate quadratic problem (MQP). The complexities and applicable ranges proposed in these research studies are compared. Based on the studies, the research problem is formulated, with the aim of developing more efficient strategies.

Chapter 4 presents a collection of useful theorems and lemmas essential for solving MQP. Two strategies for solving MQP in polynomial time are introduced under specific conditions, where the system $\mathscr{P}$ can be expressed as $p^{(j)} = k_j p^{(1)}$ or

$p^{(j)} = p^{(i)} + p^{(h)}$. Subsequently, three forgery mechanisms for multivariate signature schemes, namely DSFM1, DSFM2, and DSFM3, are discussed. DSFM3 works without having to generate weak public key. Additionally, two strategies are provided for users to identify public keys generated via DSFM1 and DSFM2.

Chapter 5 extends the results from Chapter 4 by attacking two well-known signature schemes in multivariate cryptography, UOV and Rainbow, via DSFM1, DSFM2 and DSFM3. The research demonstrates that UOV is vulnearable to all three forgery mechanisms, while Rainbow is only susceptible to DSFM3. Additionally, the explanation on how the structure of the Rainbow central map prevents the RCA from generating weak public key via DSFM1 and DSFM2 is given at the end of this chapter.

Chapter 6 highlights the potential of utilising the quadratic factorisation formula for forgery in multivariate signature schemes. MQP with the underlying mathematical operation, is easy to solve. Furthermore, the private and public keys generated from these mathematical elements are found to be applicable to UOV since the key pairs satisfy the key security requirements of UOV.

Chapter 7 serves as the concluding chapter, summarising the research work and contributions. Finally, it offers insights into potential future research directions.

REFERENCES

Albrecht, M. R., Bernstein, D. J., Chou, T., Cid, C., Gilcher, J., Lange, T., Maram V., von Maurich, I., Misoczki, R., Niederhagen, R., et al. (2020). Classic mceliece, *NIST Post-Quantum Cryptography Standardization Project (Round 3)*.

Barker, E., Chen, L., Keller, S., Roginsky, A., Vassilev, A., and Davis, R. (2017). Recommendation for pair-wise key-establishment schemes using discrete logarithm cryptography. Technical report, National Institute of Standards and Technology.

Beullens, W. (2021). Improved cryptanalysis of uov and rainbow. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 348–373. Springer.

Beullens, W. (2022). Breaking rainbow takes a weekend on a laptop. *Cryptology ePrint Archive.*

Billet, O. and Gilbert, H. (2006). Cryptanalysis of rainbow. *In Security and Cryptography for Networks: 5th International Conference, SCN 2006, Maiori, Italy, September 6-8, 2006. Proceedings 5*, pages 336–347. Springer.

Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., Schwabe, P., Seiler, G., and Stehlé, D. (2018). Crystals-kyber: a cca-secure module-lattice-based kem. In *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 353–367. IEEE.

Cartor, R., Cartor, M., Lewis, M., and Smith-Tone, D. (2022). Iprainbow. In *International Conference on Post-Quantum Cryptography*, pages 170–184. Springer.

Chen, A. I.-T., Chen, C.-H. O., Chen, M.-S., Cheng, C.-M., and Yang, B.-Y. (2008). Practical-sized instances of multivariate pkcs: Rainbow, tts, and ℓic-derivatives. In *International Workshop on Post-Quantum Cryptography*, pages 95–108. Springer.

Chen, A. I.-T., Chen, M.-S., Chen, T.-R., Cheng, C.-M., Ding, J., Kuo, E. L.-H., Lee, F. Y.-S., and Yang, B.-Y. (2009). Sse implementation of multivariate pkcs on modern x86 cpus. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 33–48. Springer

Chen, C., Danba, O., Hoffstein, J., Hülsing, A., Rijneveld, J., Schanck, J. M., Schwabe, P., Whyte, W., and Zhang, Z. (2019). Algorithm specifications and supporting documentation. *Brown University and Onboard security company, Wilmington USA*.

Cheng, C.-M., Hashimoto, Y., Miura, H., and Takagi, T. (2014). A polynomial-time algorithm for solving a class of underdetermined multivariate quadratic equations over fields of odd characteristics. In *International Workshop on Post-Quantum Cryptography*, pages 40–58. Springer.

Ding, J. and Petzoldt, A. (2017). Current state of multivariate cryptography. *IEEE Security & Privacy*, 15(4):28–36.

Ding, J., Petzoldt, A., and Schmidt, D. S. (2020). Multivariate cryptography. In *Multivariate Public Key Cryptosystems*, pages 7–23. Springer.

Ding, J. and Schmidt, D. (2005). Rainbow, a new multivariable polynomial signature scheme. In *International conference on applied cryptography and network security*, pages 164–175. Springer.

Ding, J., Yang, B.-Y., Chen, C.-H. O., Chen, M.-S., and Cheng, C.-M. (2008). New differential-algebraic attacks and reparametrization of rainbow. In *International Conference on Applied Cryptography and Network Security*, pages 242–257. Springer.

Dong, Z., Kane, K., and Camp, L. J. (2016). Detection of rogue certificates from trusted certificate authorities using deep neural networks. ACM *Transactions on Privacy and Security (TOPS)*, 19(2):1–31.

Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., and Stehlé, D. (2018). Crystals-dilithium: A lattice-based digital signature scheme. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pages 238–268.

D'Anvers, J.-P., Karmakar, A., Sinha Roy, S., and Vercauteren, F. (2018). Saber: Module-lwr based key exchange, cpa-secure encryption and cca-secure kem. In *International Conference on Cryptology in Africa*, pages 282–305. Springer.

Fouque, P.-A., Hoffstein, J., Kirchner, P., Lyubashevsky, V., Pornin, T., Prest, T., Ricosset, T., Seiler, G., Whyte, W., Zhang, Z., et al. (2018). Falcon: Fast-fourier lattice-based compact signatures over ntru. *Submission to the NIST's post-quantum cryptography standardization process*, 36(5):1–75.

Furue, H., Kiyomura, Y., Nagasawa, T., and Takagi, T. (2022). A new fault attack on uov multivariate signature scheme. In *International Conference on Post-Quantum Cryptography*, pages 124–143. Springer.

Furue, H., Nakamura, S., and Takagi, T. (2021). Improving thomae-wolf algorithm for solving underdetermined multivariate quadratic polynomial problem. In *International Conference on Post-Quantum Cryptography*, pages 65–78. Springer.

Garey, M. R. and Johnson, D. S. (1979). Computers and intractability. *A Guide to the Theory of NP-Completeness*.

Hellman, M. (1976). New directions in cryptography. *IEEE transactions on Information Theory*, 22(6):644–654

Huang, H. and Bao, W. (2015). Algorithm for solving massively underdefined systems of multivariate quadratic equations over finite fields. *arXiv preprint arXiv:1507.03674.*

Kipnis, A., Patarin, J., and Goubin, L. (1999). Unbalanced oil and vinegar signature schemes. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 206–222. Springer.

Miura, H., Hashimoto, Y., and Takagi, T. (2013). Extended algorithm for solving underdefined multivariate quadratic equations. In *Post-Quantum Cryptography: 5th International Workshop, PQCrypto 2013, Limoges, France, June 4-7, 2013. Proceedings 5*, pages 118–135. Springer.

NIST, Computer Security Division, I. T. L. (2016). Public-key post-quantum cryptographic algorithms: Nominations.

Rivest, R. L., Shamir, A., and Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126.

Ruiz, A. L., Morales, E. C., Roure, L. P., and Ríos, A. G. (2014). *Algebraic circuits.* Springer.

Shor, P. W. (1999). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332.

Thomae, E. and Wolf, C. (2012). Solving underdetermined systems of multivariate quadratic equations revisited. In *International Workshop on Public Key Cryptography*, pages 156–171. Springer.

Wolf, C. (2002). *"Hidden Field Equations" (HFE)-Variations and Attacks*. PhD thesis, Verlag nicht ermittelbar.

Yang, B.-Y., Cheng, C.-M., Chen, B.-R., and Chen, J.-M. (2006). Implementing minimized multivariate pkc on low-resource embedded systems. In *International Conference on Security in Pervasive Computing*, pages 73–88. Springer.