Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IMPACT FACTOR: 6.199

IJCSMC, Vol. 8, Issue. 6, June 2019, pg.128 – 133

A Survey on Post Quantum Digital Signature Schemes for Blockchain

Prof. M Shanmugam Shoba

Senior Assistant Professor, Information Science & Engineering Department, NHCE, Bangalore, India

reach2shobhamahe@gmail.com / mshanmugams@newhorizonindia.edu

ABSTRACT: Blockchain has become one of the most cutting-edge technologies, which has been widely concerned and researched. Current blockchain platforms rely on digital signatures, which are vulnerable to attacks by means of quantum computers. The security of blockchains can be enhanced by using post-quantum digital signature schemes for signing transactions. Such schemes are considered to be robust against attacks with quantum computers. In this paper a survey on the existing post-quantum digital signature schemes is done.

Keywords: Blockchain, Quantum Computing, Digital Signature

I. INTRODUCTION

Blockchain is the basic technology of bitcoin and cryptocurrency. With the value appreciation and stable operation of bitcoin, blockchain is attracting more and more attention in many areas. Blockchain has the characteristics of decentralization, stability, security, and non-modifiability. It has the potential to change the network architecture.

Blockchain is a distributed database which is cryptographically protected against malicious modifications. Blockchain relies on two one-way computational technologies: cryptographic hash functions and digital signatures. Most blockchain platforms rely on the elliptic curve public-key cryptography (ECDSA) or the large integer factorization problem (RSA) to generate a digital signature. The security of these algorithms is based on the assumption of computational complexity of certain mathematical problems. A universal quantum computer would enable efficient solving of these problem.

II. LITERATURE SURVEY

A. Blockchained Post-Quantum Signatures

Inspired by the blockchain architecture and existing Merkle tree based signature schemes, In this paper they propose BPQS, an extensible post-quantum (PQ) resistant digital signature scheme best suited to blockchain and distributed ledger technologies (DLTs). One of the unique characteristics of the protocol is that it can take advantage of application-specific chain/graph structures in order to decrease key generation, signing and verification costs as well as signature size. Compared to recent improvements in the field, BPQS outperforms existing hash-based algorithms when a key is reused for reasonable numbers of signatures, while it supports a fallback mechanism to allow for a practically unlimited number of signatures if required.An open source implementation of the scheme and benchmark it was provided.

In this paper they introduced BPQS and its extensions to support {one and few}-time optimised post-quantum signatures. They have also presented the security challenges that blockchains and DLTs will soon face and why pure OTS schemes are not recommended as a quantum-resistant replacement. BPQS compares favourably even against conventional non-quantum schemes such as RSA, ECDSA and EdDSA, while it provides more reliable quantum-security estimates because of its rooting in a secure cryptographic hash function.

Among others, the main features of the BPQS protocol are:

- shorter signatures, and faster key generation, signing and verification times than the XMSS [5] and SPHINCS [23] family PQ protocols when signing for one or few times, which is usually preferred in blockchain systems to preserve anonymity,
- it is computationally comparable to non-quantum schemes. One can take advantage of the easy-to-apply multiple hash-chain WOTS parallelisation and caching to provide almost instant signing and faster verification,
- its extensibility property allows for many-time signatures, while it can also easily be customised, so it can fallback to another many-time scheme if and when required,
- when used in blockchain and DLT applications, it can take advantage of the underlying chain/graph structure by referencing a previous transaction, in which the same key is reused. This could effectively mean that each new BPQS signature simply requires the effort of an OTS scheme, because the rest of the signature path to the root is in the ledger already and can be omitted,
- it could be used as a building block to implement novel PQ schemes such as a simultaneously “Stateful and Stateless” scheme, which might benefit clustered environments, where nodes can fallback to stateless schemes when consensus is lost. Additionally, such schemes can be used for forward and backward compatibility purposes or when requiring to reuse a key between two independent and incompatible blockchains.

The main drawback of the original BPQS protocol is that the size of its signature output increases linearly with the number of signatures. However, one can mitigate this by using a combined PQ approach or by utilising existing graph structures in blockchain applications. All in all, the customisation, caching and extensibility properties of BPQS make it an ideal candidate for blockchains and it could serve as a bridging protocol between stateless, stateful and other PQ schemes.

B. A Secure Cryptocurrency Scheme Based on Post-Quantum

Blockchain has become one of the most cutting-edge technologies, which has been widely concerned and researched. However, the quantum computing attack seriously threatens the security of blockchain, and related research is still less. Targeting at this issue, in this paper, they present the definition of post-quantum blockchain (PQB) and propose a secure cryptocurrency scheme based on PQB, which can resist quantum computing attacks. First, they propose a signature scheme based on lattice problem. We use lattice basis delegation algorithm to generate secret keys with selecting a random value, and sign message by preimage sampling algorithm. In addition, they design the first-signature and last-signature in their scheme, which are defined as double-signature. It is used to reduce the correlation between the message and the signature. Second, by combining the proposed signature scheme with blockchain, they construct the PQB and propose this cryptocurrency scheme. Its security can be reduced to the lattice short integer solution (SIS) problem. At last, through analysis, the proposed cryptocurrency scheme is able to resist the quantum computing attack and its signature satisfies correctness and one-more unforgeability under the lattice SIS assumption. Furthermore, compared with previous signature schemes, the sizes of signature and secret keys are relatively shorter than that of others, which can decrease the computational complexity. These make their cryptocurrency scheme more secure and efficient.

We should actively deal with the threat of powerful parallel computing power that quantum computer has in the future. Its signature satisfies the correctness, one more unforgeability under the SIS assumption. Moreover, the sizes of signature and secret keys are shorter so that it can decrease computational complexity of the proposed cryptocurrency scheme. In addition, the security of our scheme depends on the lattice problem SIS, it is shown that cryptocurrency scheme can resist quantum computing attacks. Compared with original cryptocurrency scheme, user’s private key has the advantage of resisting quantum computing attack. In other words, cryptocurrency is more secure in this cryptocurrency scheme. It is shown that our cryptocurrency scheme is more secure and efficient. Our research will help us to protect the security of blockchain, which will be more practical under the present technical conditions. We also believe that the post-quantum blockchain is very significant for other blockchain applications in the future.

C. Blockchain: Challenges and Applications

In this paper, the authors conduct a survey of Blockchain applications using Blockchain technology and the challenges these face. Blockchain technology can also be used in various fields of business. One interesting implementation of Blockchain technology is in the healthcare system. This satisfies all stakeholders such as Hospitals, Healthcare, Health Authorities by meeting information consumer’s needs and protecting patient privacy by using Blockchain to pay fees with Bitcoin. In the paper system, if information consumers need to see a patient's health record they had to filled in a request form and sent it to the registration office for approval. After receiving approval, the information consumer will pay a copy fee to the cashier and obtain a bill of receipt. The information consumer then shows the receipt to the registration office to obtain a copy of the patient's health record. However, a patient's health records can be lost, or copies may be made for illegal purposes. The concept of an electronic health records system using Blockchain technologies is depicted in Figure1.

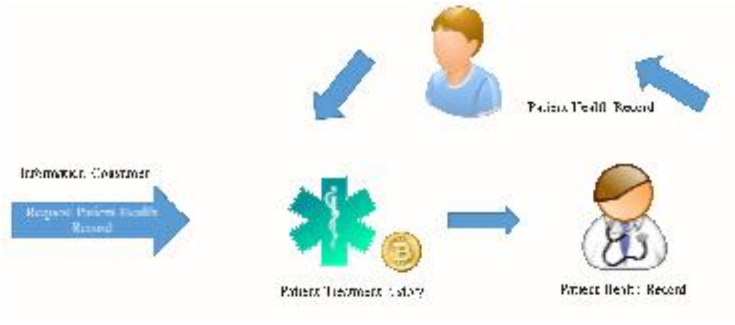

Figure1: E-health system using Blockchain

D. Introduction to Security and Privacy on the Blockchain

The blockchain has fueled one of the most enthusiastic bursts of activity in applied cryptography in years, but outstanding problems in security and privacy research must be solved for blockchain technologies to go beyond the hype and reach their full potential. At the first IEEE Privacy and Security on the Blockchain Workshop (IEEE S&B), we presented peer-reviewed papers bringing together academia and industry to analyze problems ranging from deploying newer cryptographic primitives on Bitcoin to enabling usecases like privacy-preserving file storage. We overview not only the larger problems the workshop has set out to tackle, but also outstanding unsolved issues that will require further cooperation between academia and the blockchain community.

A blockchain is simply a cryptographically verifiable list of data. One of the reasons for the enthusiasm around the blockchain is that databases do not have any cryptographic guarantees of integrity, guarantees that are necessary for any database operating in an adversarial environment. If the field of systems security and privacy-enhancing technologies has learned one lesson since the Snowden revelations, it is that all databases are likely operating in an adversarial environment. Therefore, some of the "hype" around blockchains is for good reason: For the first time in decades, the venerable database itself may be replaced by blockchains. However, there is more to blockchains than just data integrity. As exemplified by Bitcoin, the primary advantage of blockchain technologies is that the data itself can be decentralized. A distributed public ledger built with a blockchain where all users have the same data, which is necessary for high-value use-cases such as currency, is clearly privacy-invasive for many use-cases. Security and privacy on the blockchain is an emerging field that is dire need of further research.

E. Securing Smart Cities Using Blockchain Technology

A smart city uses information technology to integrate and manage physical, social, and business infrastructures in order to provide better services to its dwellers while ensuring efficient and optimal utilization of available resources. With the proliferation of technologies such as Internet of Things (IoT), cloud computing, and interconnected networks, smart cities can deliver innovative solutions and more direct interaction and collaboration between citizens and the local government. Despite a number of potential benefits, digital disruption poses many challenges related to information security and privacy. This paper proposes a security framework that integrates the blockchain technology with smart devices to provide a secure communication platform in a smart city.

Due to the heterogeneous nature of resource constrained devices, a smart city is vulnerable to a number of security attacks. It is important to identify those threats and their possible consequences in order to design an effective solution. A number of research has been conducted in this field such as Open Web Application Security Project (OWASP) enlisting common security attacks, Computer Emergency Response Teams (CERT) providing graphical representation of potential vulnerabilities, G-Cloud presenting a series of Cloud Computer Service Provider (CCSP) requirements. The following threat categories are identified for the smart cities: i) Threats on Availability- are concerned with the (unauthorised) upholding of resources, ii) Threats on Integrity- include unauthorized change to data such as manipulation and corruption of information, iii) Threats on Confidentiality- include disclose of sensitive information by unauthorized entity, iv) Threats on Authenticity- are concerned with gaining unauthorized access to resource and sensitive information, and v) Threats on Accountabilityinclude denial of transmission or reception of a message by the corresponding entity.

III. CONCLUSION

Current digital signature schemes are vulnerable and must be either replaced in current blockchains or implemented from the very beginning in new quantum-resistant ledgers designed from scratch. None of the existing digital signature schemes satisfies all the requirements of a distributed ledger system, namely small size and efficiency. We hope that future research in the area will bring smaller and more efficient schemes. Until then, its recommend maintaining agility in the architectural design and building ledgers in which changing the digital signature scheme should be relatively easy.

REFERENCES

[1]. Konstantinos Chalkias, James Brown, Mike Hearn, Tommy Lillehagen, Igor Nitto, Thomas Schroeterk, “Blockchained Post-Quantum Signatures” , International Computing Conference, IEEE, 2018.

[2]. Yu-Long Gao, Xiu-Bo Chen1, Yu-Ling Chen , Ying Sun , Xin-Xin Niu, And Yi-Xian Yang,” A Secure Cryptocurrency Scheme Based on Post-Quantum Blockchain” , IEEE Access, Volume 6, March, 2018.

[3]. Pinyaphat Tasatanattakool, Chian Techapanupreeda,” Blockchain: Challenges and Applications”, International Conference, ICOIN 2018, IEEE.

[4]. Harry Halpin,Marta Piekarsha," IntroductiontoSecurityandPrivacyontheBlockchain", 2017 IEEE European Symposium on Security and Privacy Workshops.

[5]. Kamanashis Biswas Vallipuram Muthukkumarasamy," SecuringSmartCitiesUsingBlockchainTechnology" , 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems.

[6]. Ms. V. Padmavathi ,Dr. B. Vishnu Vardhan , Dr. A. V. N. Krishna ,"Quantum Cryptography and Quantum Key Distribution Protocols: A Survey" , 6th International Computing Conference, IEEE, 2016.

[7] V. Kurochkin a, Yu.Kurochkinb*, "*PrinciplesOfThe New Quantum Cryptography Protocols Building", RFBR, grant 07-07-00263.

[8] Yi Liu, Xingtong Liu, Jian Wang, Lei Zhang and Chaojing Tang," Security analysis of electronic payment protocols based on quantum cryptography", 4th International Conference on Information Science and Control Engineering, IEEE, 2017.

[9] Mohamed Elboukhari, MostafaAzizi and Abdelmalek Azizi1," Verification Of Quantum Cryptography Protocols By Model Checking", International Journal of Network Security & Its Applications, IJNSA, 2010.

[10] Quantum Cryptography Goes a Long Way,–Katherine Kornei,katherinekornei is a freelance writer based in Portland, Oregon, November 2, 2016.

[11] W. K. Wootters and W. H. Zurek, "A Single Quantum Cannot be Cloned", Nature 299, 802-803, 1982.

[12] Bennett, C.H. and G. Brassard, "Quantum Cryptography: Public key distribution and coin tossing", Theoretical Computer Science, Elseiver, vol. 560, 2014, pp.7-11.

[13] Bennett, C. H., F.Bessette, G. Brassard, L.Salvail and J. Smolin, "Experimental quantum cryptography", Journal of Cryptology,vol. 5, no. 1, 1992, pp. 3-28.