The Korean Institute of Communications and Information Sciences

Available online at www.sciencedirect.com

ScienceDirect

ICT Express 7 (2021) 316–321

www.elsevier.com/locate/icte

A new key protocol design for cryptocurrency wallet

Soonhwa Sung

Creative Fusion Education Department, Chungbuk National university, Cheongju, Republic of Korea

Received 26 February 2021; received in revised form 22 June 2021; accepted 2 August 2021
Available online 24 August 2021

Abstract

The majority of hacking accidents in cryptocurrency occur when the information of a cryptocurrency wallet is stolen. Since the cryptocurrency wallet is simply used for a key storage, when connecting to a transaction network, it is vulnerable for a key theft. Blockchain is not traceable, but it should communicate to applicate data of blockchain. To communicate to applicate data of blockchain, this study proposes a key protocol design to secure cryptocurrency transactions for user privacy of cryptocurrency to resolve the drawback of decentralized exchange.

The key protocol includes a session key for a blockchain data structure and the Federated Byzantine Agreement (FBA) for the key-exchange agreement among users. In F-measure model, the values of Key Cluster Mode, Test Session key Mode and Original Session key Mode resulted in True Positive Ratio greater than 0.5 and False Positive Ratio lesser than 0.5. Therefore, the key protocol model has optimal security. In addition, computation costs of the protocol improve by compared with former studies. It may be played an important role in the cryptocurrency hacking accident and supported robust cryptocurrency market The study guarantees the security of cryptocurrency users without decentralized exchange, and it is scalable to other areas by using secure distributed networks.

Keywords: Cryptocurrency wallet; Key protocol; Blockchain

1. Introduction

Blockchain, the technology at the foundation of Bitcoin and other cryptocurrencies, has been considered as innovative potentials to transform most industries [1].

A blockchain's peer-to-peer system provides verifiable ledger maintenance without a centralized authority. Thus, it addresses not only a single point-of-failure but also a single point-of-trust [2].

Despite the functional features of blockchain [3], recent reports have highlighted the security risks associated with blockchain technology [4–8].

The security of blockchain systems is important for potential users with regard to their acceptability [9].

As blockchains are not proper for high capacity data-storing, an additional location for data storage is required. The storage for data also needs additional security. In this process, as a matter of high-demanding security, blockchains simply add complicated layers that could secure the data.

Therefore, this study proposes a method to enhance the security of the cryptocurrency wallets. Blockchain is not traceable, but it should communicate to applicate data of blockchain. The study suggests a key protocol for the cryptocurrency wallet. The proposal can replace the conventional key storage scheme with a session key agreement that follows a multilateral protocol. The key exchange agreement among users is enabled by the Federated Byzantine Agreement (FBA) protocol, while the session key is encoded in the blockchain data structure.

This study contains Section 2 Related Works, Section 3 Cryptocurrency Wallet Key Protocol Design, Section 4 Analysis, and Section 5 Conclusion.

2. Related works

Cryptocurrency has been mentioned often as a replacement of currency, which ensures the integrity of transaction along with the low maintenance cost [10]. However, the vulnerability of security still exists during a crypto mining process based on the blockchain [11–13]. In a commercial content for distributed applications in the Internet environment, a self-recovery key mechanism is useful to protect highly sensitive

E-mail address: shsung@cbnu.ac.kr.

Peer review under responsibility of The Korean Institute of Communications and Information Sciences (KICS).

https://doi.org/10.1016/j.icte.2021.08.002

information. However, the key mechanism cannot recover the session key only with one's own security. The studies [14–21] proposed that the key mechanism can allow group users to recover a lost session key and to reduce communication overhead from *O(tj)* to *O(t+j)* without any additional increment in the storage cost as compared to the previous approaches, where j is the current session number and t is the maximum number of compromised group members that may collude.

However, the limitations of the studies are that hash chain-based mechanisms are unable to resist colluded attacks. That is, if the revoked users competed with newly subscribed users, it would not be safe because they could recover all of the included session keys. Although Wang et al. [22] proposed a group key distribution including self-recovery characteristics in wireless networks where resources are limited, this paper does not qualify forward security and include the collusion resistance. Chen et al. [23] suggested a self-healing group key distribution based on unidirectional hash chains containing collusion resistance. The distribution is divided into different groups according to the time the users join the group. It can recover the session key from the session in which the legitimate user joined the last session. However, this study refers to the violation of forward security because the revoked user can recover the private security of other legitimate users who are able to recover the session key of the current session.

Therefore, this paper proposes a key protocol that can be adapted to the block chain network as well as the complete forward security of the session key to protect the cryptocurrency wallet.

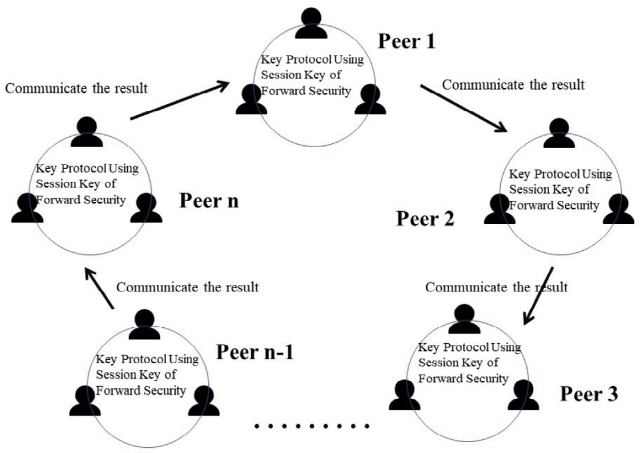
Peer 1
Key Protocol Using Session Key of Forward Security
Communicate the result
Communicate the result
Key Protocol Using Session Key of Forward Security
Peer n
Key Protocol Using Session Key of Forward Security
Peer 2
Communicate the result
Communicate the result
Key Protocol Using Session Key of Forward Security
Peer n-1
Key Protocol Using Session Key of Forward Security
Peer 3
Key Protocol Using Session Key of Forward Security
....

Fig. 1. The proposed key protocol mechanism.

Table 1
Notation for test session keys.

Abbreviation	Description
$\hat{A}$	Party *A*
$\hat{B}$	Party *B*
$\hat{C}$	Party *C*
X	Ephemeral public key of $\hat{A}$
Y	Ephemeral public key of $\hat{B}$
Z	Ephemeral public key of $\hat{C}$
$r\hat{A}$	Ephemeral private key of $\hat{A}$
$r\hat{B}$	Ephemeral private key of $\hat{B}$
$r\hat{C}$	Ephemeral private key of $\hat{C}$

3. Cryptocurrency wallet key protocol design

The key protocol includes the session key that ensures the cryptocurrency wallet key from being stolen and a preparation in case of the collusion.

3.1. Key protocol mechanism

This key protocol is a protocol to protect a cryptocurrency wallet key. The overall protocol mechanism is shown in Fig. 1. A peer is composed of numerous parties, and each party includes at least three persons. Each peer must proceed with the key protocol using a session key based on the forward security for valid users. This protocol contains a test session key protocol and an original session key agreement protocol for secure key management.

In Fig. 1, Peer 1 proceeds with the key protocol with the session key of the forward security and Peer 2 proceeds with the key protocol with the session key of the forward security. Peer 1 communicates with the protocol which is connected to Peer 2, then Peer 2 communicates with the protocol which is sequentially connected to Peer 3, and the peer n communicates in the same way accordingly. Meanwhile, if there is an unauthorized user, the protocol is automatically terminated. This process confirms whether a peer is legitimate persons who can execute cryptocurrency transactions. The peer interacts with many parties using the FBA in order to tolerate possible faults. A party operates a key protocol with the session key based on the forward security for valid communications of block chain. The session key is managed by a key cluster in the peer. The key cluster in a peer communicates with another key cluster in another peer using the key result of FBA. Each peer has only one key cluster. Therefore, before a party operates the key protocol, a peer sustains secure communications with the FBA for active parties.

3.2. Key protocol using session key of forward security

The key protocol supports that the key cluster in a peer operates the key-exchange agreement by the FBA and manages the session key. The key cluster includes the session of a test session and an original session. Due to the separation of the session keys, the process is divided into the test session and the original session. The suggested session key consists of a long-term key and an ephemeral key. The long-term key is in charge of the original session, and the short-term key is in charge of the test session.

In the suggested session, the users who have the session key and the users who agreed to the session key would participate in a multilateral communication. If it fails to conclude the block agreement, all the session data will be deleted in the memory storage and then the session will terminate without establishing the session key. Tables 1 and 2 are a notation description for the multilateral session key process of the

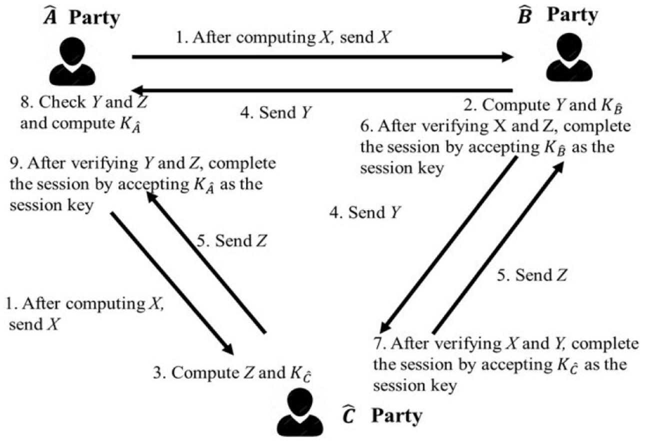
Â Party
B̂ Party
Ĉ Party
1. After computing X, send X
8. Check Y and Z and compute $K_{\hat{A}}$
4. Send Y
2. Compute Y and $K_{\hat{B}}$
6. After verifying X and Z, complete the session by accepting $K_{\hat{B}}$ as the session key
9. After verifying Y and Z, complete the session by accepting $K_{\hat{A}}$ as the session key
4. Send Y
5. Send Z
5. Send Z
1. After computing X, send X
3. Compute Z and $K_{\hat{C}}$
7. After verifying X and Y, complete the session by accepting $K_{\hat{C}}$ as the session key

Fig. 2. Test session key exchange protocol for cryptocurrency wallet.

block chain. The protocol also consists of the test session key exchange protocol of Fig. 2 and the original session key agreement protocol of Fig. 3.

Test session

1. Activate session s = $(\hat{A}, i)$ with $\hat{B}$, $\hat{C}$, and $\hat{A}$ calculates $X = g^{f_I(r\widehat{A},\mathrm{a},\Omega)}$ by choosing a short term secret key. Then $\hat{A}$ sends X to $\hat{B}$ and $\hat{C}$. ($i = 1...q$: query phase).
2. $\hat{B}$ chooses a short term secret key and calculates $Y = g^{fR(r\hat{B},b,\Omega)}$ and $K_{\hat{B}} = F_R(f_R(\mathrm{r}\hat{B}, b, \Omega), b, X, \Omega)$.
3. $\hat{C}$ chooses a short term secret key and calculates $Z = g^{fR(r\hat{C},c,\Omega)}$ and $K_{\hat{C}} = F_R(f_R(\mathrm{r}\hat{C}, c, \Omega), c, Y, \Omega)$.
4. $\hat{B}$ sends Y to $\hat{A}$ and $\hat{C}$.
5. $\hat{C}$ sends Z to $\hat{A}$ and $\hat{B}$.
6. $\hat{B}$ confirms X, Z and receives $K_{\hat{B}}$ using the session key, completing the session.
7. $\hat{C}$ confirms X, Y and receives $K_{\hat{C}}$ using the session key, completing the session.
8. $\hat{A}$ checks Y, Z and calculates $K_{\hat{A}} = F_I(f_I(\mathrm{r}\hat{A}, a, \Omega), a, Y, \Omega)$.
9. $\hat{A}$ checks Y, Z and receives $K_{\hat{A}}$ using the session key, completing the session.
10. Each $\hat{A}$, $\hat{B}$, $\hat{C}$ confirms the hash function: H (session key value plus transaction session key tree root value) less than TV (Target Value). (H: Hash function) If it satisfied, it proceeds with the next step and if not, the session process will be stopped.

Original session

1. $\hat{A}$ has a pair of long term key(a, A) and a pair of agreement key $(pk\hat{A}, sk\hat{A})$. $\hat{B}$ has a pair of long term key(b, B) and a pair of agreement key $(pk\hat{B}, sk\hat{B})$. $\hat{C}$ has a pair of long term key(c, C) and a pair of agreement key $(pk\hat{C}, sk\hat{C})$.
2. $\hat{A}$ agrees with X using $sk\hat{A}$ and X, and sends X to $\hat{B}$ and $\hat{C}$.
3. $\hat{B}$ agrees with Y using $sk\hat{B}$ and Y, and sends Y to $\hat{A}$ and $\hat{C}$.

Table 2
Notation for original session keys.

Abbreviation	Description
A	Long-term private key of A $(A = g^a)$
a	Long-term private key of $\hat{A}$ $(a \in z_p)$
B	Long-term public key of B $(B = g^b)$
b	Long-term private key of $\hat{B}$
C	Long-term public key of C $(C = g^c)$
c	Long-term private key of $\hat{C}$
g	Generator
$pk\hat{A}$	Agreement public key of $\hat{A}$
$pk\hat{B}$	Agreement public key of $\hat{B}$
$pk\hat{C}$	Agreement public key of $\hat{C}$
$sk\hat{A}$	Agreement secret key of $\hat{A}$
$sk\hat{B}$	Agreement secret key of $\hat{B}$
$sk\hat{C}$	Agreement secret key of $\hat{C}$

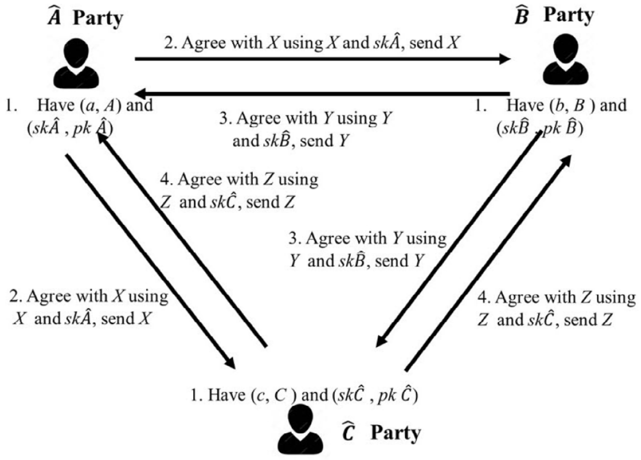
Â Party
B̂ Party
Ĉ Party
2. Agree with X using X and skÂ, send X
1. Have (a, A) and (skÂ , pk Â)
3. Agree with Y using Y and skB̂, send Y
1. Have (b, B) and (skB̂ , pk B̂)
4. Agree with Z using Z and skĈ, send Z
3. Agree with Y using Y and skB̂, send Y
2. Agree with X using X and skÂ, send X
4. Agree with Z using Z and skĈ, send Z
1. Have (c, C) and (skĈ , pk Ĉ)

Fig. 3. Original session key agreement protocol for cryptocurrency wallet.

4. $\hat{C}$ agrees with Z using $sk\hat{C}$ and Z, and sends Z to $\hat{A}$ and $\hat{B}$.

4. Analysis

4.1. Security analysis of the key protocol

The assumption of the scheme states that a ledger exists and only analyzes the key protocol design for transactions of cryptocurrency. Security information of the key protocol is added to the block body of the block chain as a transaction session key tree root. Corresponding to the Proof of Stake (PoS), the information of the secret key in the sessions is attached to the block body of the block chain in one transaction. The key protocol communicates with each user of a peer, and each user of a peer communicates with another peer by the key cluster. The key cluster of a peer exchanges the session keys by operating multiparty computations using the FBA. In Fig. 4, once the key cluster in a peer processes the session keys for all the users in a peer, the protocol sends the secret key information of the key cluster to the key cluster in another peer. The key protocol security is a hybrid of the FBA and the *forward secrecy*. The security analysis

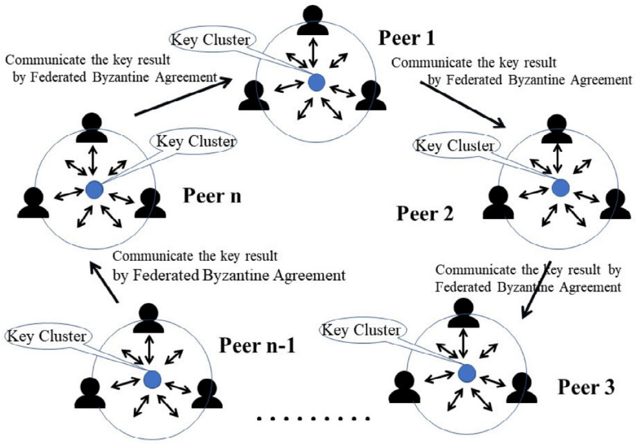
Key Cluster
Peer 1
Communicate the key result
by Federated Byzantine Agreement
Communicate the key result
by Federated Byzantine Agreement
Key Cluster
Peer n
Key Cluster
Peer 2
Communicate the key result
by Federated Byzantine Agreement
Communicate the key result by
Federated Byzantine Agreement
Key Cluster
Peer n-1
Key Cluster
Peer 3
....

Fig. 4. Security mechanism of the key protocol.

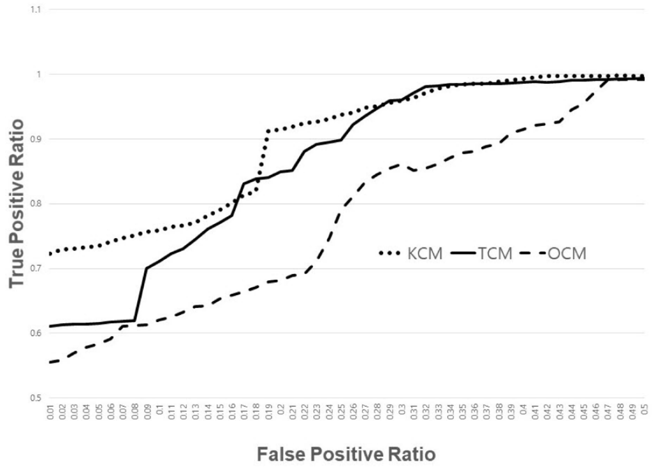

Fig. 5. Comparing Receiver Operating Characteristic (ROC). Curves for the Key Protocol Security.

assumes botnet attacks on peer to peer users. Botnets can be defined as networks of compromised computers, which can be remotely controlled by the attacker. The simulation of systems supposes that the system state is represented through the messages transferred between processes, these messages are only available to the interacting processes creating a global de-synchronization. To make understanding peer-to-peer protocol source code easy, this study uses OverSim. OverSim is an open-source overlay and peer-to-peer network simulation framework for the OMNeT++ simulation environment. The study uses a simulation obtained from OverSim [24] for analyzing botnet behavior [25] and applies to a F-measuremodel. Fig. 5 expresses the evaluation of F-measure model for the key protocol. Receiver Operating Characteristic (ROC)analysis provides tools to select possibly optimal models. In ROC curve of Fig. 5, the values of Key Cluster Mode (KCM), Test Session key Mode (TSM) and Original Session key Mode (OSM) resulted in True Positive Ratio (TPR) greater than 0.5 and False Positive Ratio(FPR) lesser than 0.5. Therefore, the key protocol model has optimal security.

Table 3
Comparison of computation costs.

Scheme	Computation cost
[28] M. Just et al.	$11T_{me} + 3T_{ecm} + 2\ T_{eca} + 5\ T_{senc}/T_{sdec}$
[29] E. Bresson et al.	$12\ T_{me} + 4\ T_{senc}/T_{sdec}$
[30] D. Pointcheval et al.	$13T_{me} + 6\ T_{ecm} + 2T_{eca} + 6\ T_{senc}/T_{sdec}$
[31] Eduarda S.V. et al.	$13T_h + 10\ T_{me} + 8T_{senc}/T_{sdec}$
Proposed scheme	$9T_{me} + 4T_{ecm} + T_{eca} + 9T_h$

4.2. Computation efficiency

To compare the computation costs, the current research followed the experiment environment of [24]. Time stamp, arbitrary value, and sequence number were set to 32 bits. In [25], since 160 bits ECC cryptographic system provides the security that 1024 bits RSA cryptographic uses, the session key will use 1024 bits. In Table 3, given T_h is one-way hash function, T_{ecm} is ECC point multiplication, T_{eca} is ECC point addition, T_{senc} is Symmetric encryption, T_{sdec} is Symmetric decryption, and T_{me} is Modular exponentiation. The communication costs were compared. There have been research studies introduced with regard to improving computation efficiency. In [26], a digital signature key computation which verifies only the participating users is required. Since the Diffie–Hellman computation can confirm the key, it takes longer than the mutual authentication using Diffie–Hellman group key verification in [27]. In [27], the group key authentication cost is efficient, but it is not suitable for the block chain where it needs to save the transaction history and prove the work. [28] requires a polynomial reduction in key size with the number of signer mutual authentication. It is inefficient not only in security due to the combination of polynomial time and key size for a blind signature, but also in calculation cost.

In [29], a pairing-based key for public key efficiency is constructed, but there is a problem to be considered from a theoretical and practical point of view. In addition, it cannot arbitrarily generate a secret key algorithm and nor deal with publicly public keys. Furthermore, it contains an issue in which [31] generally involves randomized private key generation algorithms, making it difficult to work backwards.

The key protocol can prevent theft of wallet information by session key contract instead of storing the key in the wallet. It has optimal security by statistic verification and protects privacy of investors without decentralized exchange. However, the key protocol design to secure cryptocurrency transactions is worried about conflicts of interest which users register and withdraw in cryptocurrency transactions because it supports decentralized massive networks.

The method expresses statistic verification for security of the protocol and does not verify practical security of the decentralized protocol because it supports decentralized massive networks. In addition, it is difficult to verify network evaluation because it has decentralized massive networks.

5. Conclusion

The paper proposes a new blockchain key that is able to tolerate the Byzantine faults and can be used to work correctly in an asynchronous system such as the Internet. Most hacking-related cryptocurrency incidents occur when the information of the wallet is stolen. The cryptocurrency wallet does not store the currency, but the key that has access to the account does. Thus, the study suggests the key protocol that can prevent the wallet information theft by the session key agreement instead of the key storage in a wallet. This multilateral protocol is processed by the session key authentication that uses the key sessions and by the cluster key in a peer that works multiparty computations by utilizing the FBA based on blockchain technology. The key protocol plays a major role in the cryptocurrency wallet and it uses the forward security session key and the FBA of the blockchain. The keys prevent the collusion between the miners and the data receivers who use the blockchain. The protocol ultimately does not violate the forward security. Additionally, it protects the users' privacy because of a key agreement. Currently, many investors are concerned with cryptocurrency, but they worry about its security because it goes through decentralized exchange of blockchain market. Without decentralized exchange, the proposed protocol is processed by the session key authentication that uses the key sessions and by the cluster key in a peer that works multiparty computations by utilizing the FBA based on blockchain technology. Blockchain is not traceable, but it should communicate to applicate data of blockchain. To communicate to applicate data of blockchain, this study proposes a key protocol for user privacy of cryptocurrency to resolve the drawback of decentralized exchange. It may be played an important role in the cryptocurrency hacking accident and supported robust cryptocurrency market. The study is also scalable to other areas using secure distributed networks.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Available: https://arxiv.org/pdf/1711.03936.pdf.

[2] M. Corallo, et al., Enabling Blockchain Innovations with Pegged Sidechains, Oct. 2014, pp. 1–25.

[3] S. Underwood, Blockchain beyond bitcoin, Commu. ACM 59 (11) (2016) 15–17, Available: http://doi.acm.org/10.1145/2994581.

[4] E.F. Jesus, V.R.L. Chicarino, C.V.N. de Albuquerque, A.A. de A. Rocha, A survey of how to use blockchain to secure internet of things and the stalker attack, Secur. Commun. Netw. 2018 (2018) 1–27, http://dx.doi.org/10.1155/2018/9675050, 9675050.

[5] X. Li, P. Jiang, T. Chen, X. Luo, Q. Wen, A survey on the security of blockchain systems, 2017, 9675050, http://dx.doi.org/10.1016/j.future.2017.08.020.

[6] I.-C. Lin, T.-C. Liao, A survey of blockchain security issues and challenges, I.J. Network Secur. 19 (5) (2017) 653–659.

[7] N. Atzei, M. Bartoletti, T. Cimoli, A survey of attacks on ethereum smart contracts sok, in: The 6th Int. Conf. on Principles of Security and Trust, 2017, pp. 164–186, http://dx.doi.org/10.1007/978-3-662-54455-6_8.

[8] M.C.K. Khalilov, A. Levi, A survey on anonymity and privacy in bitcoin-like digital cash systems, IEEE Commun. Surv. Tutor. 20 (3) (2018) 2543–2585, http://dx.doi.org/10.1109/COMST.2018.2818623.

[9] M. Pilkington, Blockchain Technology: Principles and Applications, Research HandBook on Digital Transformations, 2016, pp. 225–253, http://dx.doi.org/10.4337/9781784717766.00019.

[10] Frank Holmes, As Banknotes Disappear Will Bitcoin Take Its Place?, US Global Investors, Apr. 2018.

[11] B. Georg, Merkle Signature Schemes, Merkle Trees and their Cryptanalysi S, Ruhr-University Bochum, 2013, Retrieved Nov. 2013.

[12] D. Yaga, P. Mell, N. Roby, K. Scarfone, Blockchain technology overview, in: Report NISTIR 8202, NIST, Oct. 2018, http://dx.doi.org/10.6028/NIST.IR.8202.

[13] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, Oct. 2008, Available : http://bitcoin.org/bitcoin.pdf.

[14] R. Dutta, Y.D. Wu, S. Mukhopadhyay, Constant storage self-healing key distribution with revocation in wireless sensor network, in: IEEE Int. Conf. Communications (ICC07), 2007, pp. 1323-1328.

[15] R. Dutta, S. Mukhopadhyay, Improved self-healing key distribution with revocation in wireless sensor network, in: Wireless Communications and Networking Conf. (WCNC), Mar. 2007, pp. 2963-2968.

[16] R. Dutta, S. Mukhopadhyay, Designing scalable self-healing key distribution schemes with revocation capability, in: Int. Symposium on Parallel and Distributed Processing and Applications, 2007, pp. 419-430.

[17] R. Dutta, S. Mukhopadhyay, S. Emmanuel, Low bandwidth self-healing key distribution for broadcast encryption, in: Asia Int. Conf. on Modeling and Simulation (ICOMS), Kuala Lum pur, Malaysia, 13C15, 2008, pp. 867-872.

[18] R. Dutta, E.C. Chang, S. Mukhopadhyay, Self-healing key distribution with revocation for wireless sensor networks using one way key chains, in: Int. Conf. on Applied Cryptography and Network Security (ACNS), Springer Berlin Heidelberg, 2007, pp. 385–400.

[19] S. Han, B. Tian, M. He, E. Chang, Threshold self-healing key distribution with sponsorization for infrastructureless wireless networks, IEEE Trans. Wireless Commun. 8 (4) (2009) 1876–1887.

[20] F. Kausar, S. Hussain, P. JH, A. Masood, Secure group communication with self-healing and rekeying in wireless sensor networks, in: Int. Conf on Mobile Ad-Hoc and Sensor Networks, vol. 4864, Springer-Verlag, 2007, pp. 737–748.

[21] Y. Yang, J. Zhou, R.H. Deng, F. Bao, Computationally Secure Hierarchical Self-Healing Key Distribution for Heterogeneous Wireless Sensor Networks, in: Lecture Notes in Computer Science, 2009, pp. 135–149.

[22] Q. Wang, H. Chen, L. Xie, K. Wang, Access-polynomial-based self-healing group key distribution scheme for resource-constrained wireless networks, Secur. Commun. Netw. 5 (12) (2012) 1363–1374.

[23] H. H. Chen, L. Xie, Improved one-way hash chain and revocation polynomial-based self-healing group key distribution schemes in resource-constrained wireless networks, Sensors 14 (12) (2014) 24358–24380.

[24] Available : http://www.oversim.org/.

[25] Information security R & D data challenge, Mobile malware, Available : https://www.kisis.or.kr/kisis/subIndex/282.do, 2019.

[26] D. He, N. Kumar, J.H. Lee, R.S. Sherratt, Enhanced three factor security protocol for consumer USB mass storage devices, IEEE Trans. Consum. Electron. 60 (1) (2014) 30–37.

[27] R.L. Rivest, M.E. Hellman, J.C. Anderson, J.W. Lyons, Responses to NIST's proposal, Commun. ACM 35 (7) (1992) 50–52.

[28] M. Just, S. Vaudenay, Authenticated multi-party key agreement, in: Proc. of Asiacrypt'96, in: LNCS 1163, Springer, 1997, pp. 36–49.

[29] E. Bresson, O. Chevassut, D. Pointcheval, Provably authenticated group diffie–hellman key exchange-the dynamic case, in: Proc. of Asiacrypt'01, in: LNCS 2248, Springer, 2001, pp. 290–309.

[30] D. Pointcheval, J. Stern, Security arguments for digital signaturesand blind signatures, J. Cryptol. 13 (3) (2000) 361–396.

[31] E.S.V. Freire, D. Hofheinz, E. Kiltz, K.G. Paterson, Non-interactive polynomial-based self-healing group key distribution schemes in resource-constrained wireless networks, Sensors 14 (12) (2014) 24358–24380.

Soonhwa Sung received the Ph.D. degree in 2005 from the Department of Computer Engineering, Chungnam National University, Daejeon, Republic of Korea. From 2000 to 2005, she was teaching in the Department of Computer Web Informations, Daeduk College, Daejeon, Republic of Korea. From 2006 to 2019, she was teaching and researching in the Department of Computer Engineering, Chungnam National University, Daejeon, Republic of Korea. Currently, she is visiting professor in Chungbuk National University, Cheongju, Republic of Korea. In addition, she is a IEEE member, a ACM member, a life member of the Korean Institute of Information Scientists and Engineers (KIISE), the Korea Information Processing Society (KIPS), and the Korean Society Internet Information (KSII), Republic of Korea.

Her research interests include mobile payment system, user authentication, future internet with blockchain.