IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received January 3, 2022, accepted February 10, 2022, date of publication February 15, 2022, date of current version March 1, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3151890

Generating Multi-Issued Session Key by Using Semi Quantum Key Distribution With Time-Constraint

HSING-CHUNG CHEN[1,2], **(Senior Member, IEEE), CAHYA DAMARJATI**[1,3], **EKO PRASETYO**[1,3], **(Member, IEEE), CHAO-LUNG CHOU**[4], **TZU-LIANG KUNG**[1], **AND CHIEN-ERH WENG**[5]

[1]Department of Computer Science & Information Engineering, Asia University, Wufeng, Taichung 41354, Taiwan
[2]Department of Medical Research, China Medical University Hospital, China Medical University, Taichung 110122, Taiwan
[3]Department of Information Technology, Universitas Muhammadiyah Yogyakarta, Yogyakarta 55183, Indonesia
[4]Department of Computer Science and Information Engineering, Chung Cheng Institute of Technology, National Defense University, Taoyuan 335, Taiwan
[5]Department of Telecommunication Engineering, National Kaohsiung University of Science and Technology, Kaohsiung 80778, Taiwan

Corresponding authors: Hsing-Chung Chen (cdma2000@asia.edu.tw), Tzu-Liang Kung (tlkueng@gmail.com), and Chien-Erh Weng (ceweng@nkust.edu.tw)

This work was supported in part by the Ministry of Science and Technology (MOST), Taiwan, under Grant 110-2218-E-468-001-MBK, Grant 110-2221-E-468-007, and Grant 110-2218-E-002-044; in part by the Ministry of Education under Grant I109MD040; in part by Asia University, Taiwan; in part by the China Medical University Hospital, China Medical University, Taiwan, under Grant ASIA-110-CMUH-22, Grant ASIA-108-CMUH-05, Grant ASIA-106-CMUH-04, and Grant ASIA-105-CMUH-04; in part by Asia University, Taiwan, Universitas Muhammadiyah Yogyakarta, Indonesian, under Grant 107-ASIA-UMY-02; and in part by Universitas Muhammadiyah Yogyakarta, Indonesia.

ABSTRACT Information security refers to protect the information from unauthorized access or modification. Quantum Key Distribution (QKD) is a way to generate a key preventing those malicious activities. One of QKD protocol, namely Semi-quantum key distribution (SQKD) protocol, is designed to allow two users to establish a secure secret key when either of them is limited to performing certain ''classical'' operations. It is proven to be secure from any type of attack. However, it will be a problem in the multi-session communication since the SQKD activities follow the number of the session. In this paper, we propose two modified SQKDs with time-constraint approach. Time-constraint is beneficial in QKD activity since it could generate session key between two parties within a certain time-constraint. By setting the number of session key and its time-constraint before QKD activities, many scheduled communications would be prepared well. Furthermore, BAN Logic analysis is applied to analyze the goal of the protocol, the considered assumptions, wasted phase, and the demand for data encryption. Finally, the performance analysis of the protocols is presented, and it shows a better performance compared with other certain QKDs.

INDEX TERMS Semi quantum key distribution, multi-issued session key, BAN logic.

I. INTRODUCTION

In general, cryptography is a key technology to keep communication securely between two parties, where the information is encrypted and decrypted by using the secret key that only known by the authorized parties. However, an eavesdropper may interfere the communication through some techniques. If the key distribution scheme is poorly designed, the sensitive information could be revealed by breaking the distributed key from eavesdropping or malicious attacker. Owing to this fact, many researchers proposed lots of secure key distribution protocols [1]–[7]. One of the approaches prevents eavesdroppers by using the trusted center issuing the session keys with nonce variables in current protocols.

Quantum key distribution (QKD) protocols exploit the fundamental principles of quantum mechanics and allow two parties to share a secret key with unconditional security. According to the uncertainty of measurement and the non-cloning theorem [8], any quantum system measurement will interfere with the system. Therefore, any eavesdropping on the quantum key distribution process can be detected.

The first proposed QKD protocol was so-called the BB84 protocol [9]. It uses single-photon polarization to transmit

The associate editor coordinating the review of this manuscript and approving it for publication was Wei Huang.

the qubits which are significant in its quantum superposition state. It could have both "0" and "1" states at a specific moment, which will not show the final result for each qubit until it is destroyed by measurement process. The BB84 protocol uses four polarization states based on the rectilinear basis and the diagonal basis for measuring the qubits. Subsequently, many different QKD-related protocols were proposed, *e.g.* B92 protocol [10] is a simplified version of the BB84 protocol, which uses only two polarization states instead of four polarization states; the E91 protocol [11], an entanglement-based QKD protocol, uses entangled photons in order to guarantee the security of the communication; and Quantum Secure Direct Communication (QSDC) proposed by Long and Liu [12] in 2002. QSDC provides a unique way in sending information securely [13] using quantum channel. It is improved recently by adding Single-photon-memory to increase the communication efficiency [14]. In 2022, M. Zhu *et al.* [35] proposed a code rate-compatible high-throughput hardware implementation scheme for QKD information reconciliation. However, those protocols does not be used in scheduled communication tasks that need time-constraint agreement in the process.

In general, the QKD protocol assume that all communicating parties are quantum capable. It means the quantum communication process must be made by using the fully quantum devices. At present, there are no actual full quantum computers; thus, it is unpractical to implement the quantum communications via using fully quantum devices. Recently, the semi-quantum key distribution (SQKD) protocol was introduced [15], where the SQKD protocol could be enabled in a limited quantum resource environment without losing their security. The typical structure of SQKD protocol consists of two users: a fully quantum user and a classical user (also called the semi-quantum user). The classical user could either interacts with the quantum channel by performing a 'Z' basis measurement, sending 'Z' basis qubits, or ignore the channel. Although, SQKD protocol allows to implement under the limited quantum devices, it is still proven to be completely robust scheme against eavesdropping attempts.

The main idea of one-time session key is used to encrypt or decrypt information between parties during a single communication session. In a similar way, one QKD activity could meet the demand for a session key in one certain session since each activity during a QKD procedure could generate massive binary data to be a session key. Thus, one-time pad (OTP) encryption [16] could be applied to encrypt and decrypt the quantum information. Owing to the eavesdropper presence and qubits error, QKD event might fail, where the session key for the scheduled communication would be unavailable. Moreover, the scheduled communication, one of the process automation applications, is a type of real-time data access with a fixed time for data transfer. Hence, the QKD that could generate session keys for specific sessions is necessary. Therefore, two modified SQKD protocols for multi-session communication with a time-constraint approach to reducing resource requirements are proposed in this paper. Furthermore, BAN Logic (Burrows–Abadi–Needham Logic) is also applied to analyze the trustworthiness of the two SQKD protocols, the considered assumptions, wasted phase, and the security demands for data encryption in these proposed specific designed protocols.

To comprehend such a crucial technology for the next generation QKD protocols, the contribution of this paper includes the followings.

- First, the two modified semi-QKDs with time-constraint approach is first proposed in this paper, which is helpful for many session keys between two parties within a certain time-bound.
- In addition, time-constraint is beneficial in QKD activity since it could generate session key between two parties within a certain time-constraint. By setting the number of session key and its time-constraint before QKD activities, many scheduled communications would be prepared well.
- Next, the BAN Logic is first also applied to analyze the QKD protocol.
- Most importantly, the performance of the proposed protocols is analyzed and then confirmed the truth of that better performance over some QKDs.

The rest of this paper is organized as follows. In Section 2, the related works are described. In Section 3, one of SQKD protocol is briefly explained and the notations for making easy in describing the proposed protocols are defined. The proposed protocols are presented in Section 4. Next, the analysis of the security is shown in Section 5. In addition, both the performance analysis and simulation assessment are presented clearly in Section 6. Finally, the conclusion is stated in Section 7.

II. RELATED WORKS

In 2008, Boyer *et al.* [15] proposed two SQKD protocols that allow two users to establish a secure secret key when one of them is limited for performing certain "classical" operations. Those protocols are based on Randomization and Measure-Resend approaches. In the Randomization-based model, the quantum device utilizes quantum memory in the process. It is a quantum-mechanical device functioned as a memory to store qubits for measured later. Utilizing it, this model prevents eavesdropping by randomizing the order of returned qubits. On the other hand, the Measure-Resend-based model does not utilize quantum memory. Thus, the user measures and returns (resends) the qubit immediately.

SQKD uses qubits reflection basis to detect eavesdropping activity that makes the qubits is not processed as a session key and decrease expected session key length. Shih *et al.* [17] proposed Efficient Three-Party QKD protocol utilizing quantum memory that makes all qubits processed as the key. In 2007, Hwang *et al.* [18] also proposed QKD protocols that process all qubits into a key minus user identity information without utilizing quantum memory. It used a pre-shared secret key to decide what basis will be used to measure the qubits.

However, it is critical to guarantee that the pre-shared secret key distribution is secure from eavesdropping.

Time-constraint agreements have the benefits which could avoid eavesdropping activity in the communication session and keep the computer or server device from overloading activities. Those approaches had been widely used in Internet of Things (IoTs) environments [19], [20]. Therefore, we propose a modified scheme of Boyer *et al.*'s [15] Measure-Resend SQKD model, in this paper. Even though it has been proven to achieve a good level of security, its utilization in key distribution still can be improved. Liu and Hwang [21] modified SQKD so that the protocol might work without invoking Quantum measurement. SQKD implementation with different qubits states (*e.g.,* four-particle cluster states [22], and GHZ states [23]) were performed in recent researches. In this paper, time-constraint approach that adopted from Chen *et al.* [24], [25] is applied into the processes, which could generate many certain session keys between two parties in the SQKD activities.

III. REVIEW OF BOYER ET AL.'S SQKD PROTOCOL

A SQKD protocol, namely Measured-Resend SQKD, is presented in this paper because it is not utilizing quantum memory and is the preliminary for the proposed protocols. Notation definition is described in the following to make easy understanding this protocol steps and the proposed protocols in this paper.

A. NOTATIONS

To give a proper understanding of how the protocol work, the notations is defined in Table 1. However, some symbols for security analysis are defined in later sections.

B. MEASURE-RESEND SQKD

The Measure-Resend SQKD protocol [15] is shown in Fig. 1, where Bob could measure and resend, or reflect the qubits to Alice. This protocol needs two-way quantum devices in order to finish it. The difference with Randomization-based is, it does not need quantum memory to record qubits temporarily. Before doing the SQKD activity, both parties had to defined and agreed on the threshold value. This action is necessary to decide whether the output could be used as a session key or be aborted. The architecture of this protocol is depicted in Fig. 1.

Let Alice and Bob be the two parties that want to generate a session key:

Measure-Resend SQKD

Step 1: Alice sends a large number of qubits in random basis between Z or the X.

Step 2: Bob chooses randomly whether to measure and send back it or to reflect it for each qubit arriving

Step 3 For every qubit reflected or sent back, Alice measures it directly.

Step 4: Alice publishes which were her Z bits. Bob publishes which qubits he wants to SIFT it.

TABLE 1. Notation list.

Symbols	Descriptions
↕ ,↔,⤢,⤡	Quantum bits Qubits to bit conversion: ↕ = bit 1 ↔ = bit 0 ⤡ = bit 1 ⤢ = bit 0
Bs	Basis used in the protocol. It consists of computational and hadamard basis.
Z	Rectilinear or computational basis - Alice's basis to transmit ↕ ,↔ quantum bits. - Bob's basis to measure or SIFT the received quantum bits.
X	Diagonal or hadamard basis - Alice's basis to transmit ⤢,⤡ quantum bits. - Bob's basis to reflect or CTRL quantum bits.
K	Series of converted bit from quantum bits
K'	Part of K that is used as bit test.
I	Index of INFO bits or TEST bits
SK	The generated session key
SID	Session list Identifier
A	Alice identifier
B	Bob identifier
tA	Requested time-constraint by Alice
tb	Agreed time-constraint by Bob

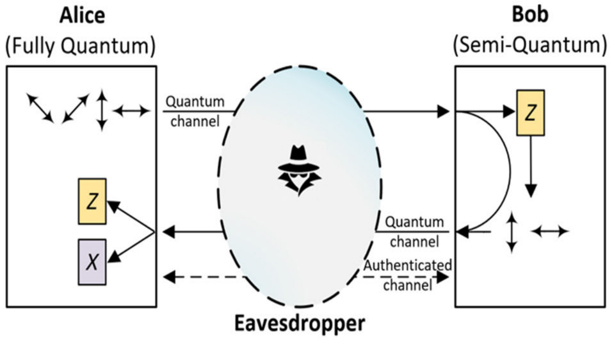

FIGURE 1. Measure-Resend SQKD architecture.

Step 5: Alice checks the error-rate of the collected reflected qubits and if either the X error-rate or the Z error-rate is higher than the predefined threshold CTRL the protocol aborts.

Step 6: Alice chooses the addresses of SIFT bits randomly to be TEST bits and publishes it. Bob publishes the value of these TEST bits. Alice checks the error-rate on the TEST bits if it is higher than the predefined threshold then the protocol aborts.

Step 7: Alice and Bob select some beginning bits of the remaining SIFT bits to be used as INFO bits. If there are no errors or eavesdropping, Alice and Bob share the same string. Otherwise, Bob's string is likely to differ from the INFO string until corrected.

Step 8: Alice publishes error-correcting code (ECC) and privacy amplification (PA) data, from which she and Bob extract the final key SK from the INFO string. □

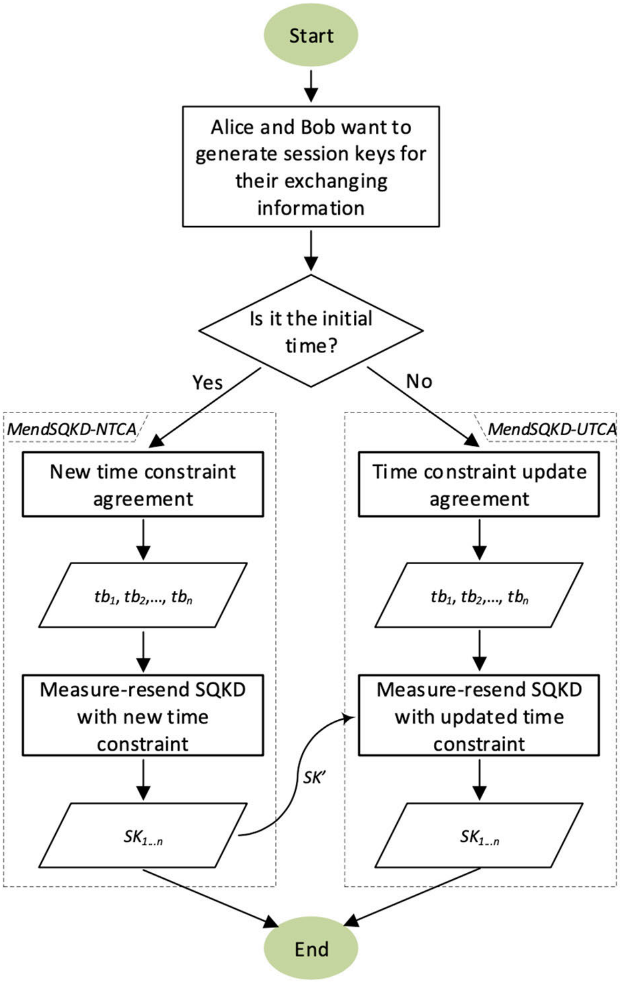
Start
Alice and Bob want to generate session keys for their exchanging information
Is it the initial time?
Yes
No
MendSQKD-NTCA
MendSQKD-UTCA
New time constraint agreement
Time constraint update agreement
tb1, tb2,..., tbn
tb1, tb2,..., tbn
Measure-resend SQKD with new time constraint
Measure-resend SQKD with updated time constraint
SK'
SK1..n
SK1..n
End

FIGURE 2. The system flowchart of *MendSQKD-NTCA* and *MendSQKD-UTCA*.

From all those steps, only qubits from Alice's Z basis and in Bob's SIFT basis that will be used as INFO or TEST bits. All qubits that in Bob's CTRL basis or being reflected, Alice expects all those bits' values are unchanged. Steps 1–3 use quantum channels for exchanging the qubits. The remaining steps use the authenticated channel for publishing information between Alice and Bob.

IV. PROPOSED SCHEME

In this section, the proposed protocols are presented in detail. It starts with the time-constraint agreement phase that followed by the proposed protocols. Time-constraint is a set of time defined by a party and proposed to the interlocutor in reaching the agreed time set for mutual and secure communication purpose. The first protocol is *MendSQKD-NTCA*. It contains *New Time-Constraint Agreement* step and *Measure-Resend SQKD With New Time-Constraint*. As shown in Fig. 2, The protocol serves Alice and Bobs Session keys need in their initial exchange information. The second protocol, *MendSQKD-UTCA*, consists of *Time-Constraint Update Agreement* and *Measure-Resend SQKD With Updated Time-Constraint*. It is used for generating session keys in continuing the exchanging information between Alice and Bob after finishing the previous session rounds. The detail description of the proposed protocols is presented in the following sub sections.

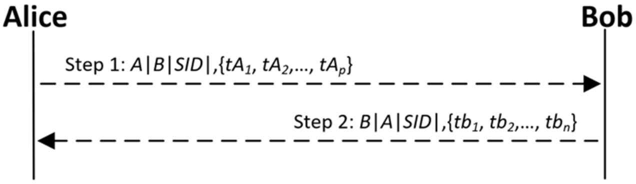
Alice
Bob
Step 1: A|B|SID|,{tA1, tA2,..., tAp}
Step 2: B|A|SID|,{tb1, tb2,..., tbn}

FIGURE 3. New time-constraint agreement between Alice and Bob.

A. NEW TIME-CONSTRAINT AGREEMENT

This phase must be accomplished before running the Measure-Resend SQKD with new time-constraint. Similar with SQKD concept, Alice is in active state in new time-constraint agreement by generating set of time-constraint while Bob is in passive state by only accepting none, part, or full of Alice's time constraint. Let Alice want to communicate with Bob in certain time-constraint sessions, Alice starts to perform this phase followed by Bob until the agreed set of time-constraint is reached as shown in Fig. 3:

New Time-Constraint Agreement

Step 1: Alice generates a set of time-constraint in accordance with the time of communication sessions that Alice proposes to Bob; SID, $\{tA_1, tA_2, \ldots, tA_p\}$, then send it to Bob.

Step 2: After Bob receives Alice's request, Bob might agree all of the time-constraint set or part of it based on his resource capability. Then, Bob sends the agreed time-constraint set SID, $\{tb_1, tb_2, \ldots, tb_n\}$ for both parties to Alice. □

B. MEASURE-RESEND SQKD WITH NEW TIME-CONSTRAINT

The modified Measure-Resend SQKD is proposed in this paper, which it could perform well with time-constraint protocol by making sure if the minimum number of generated session key $\mathcal{L}$ is satisfied. This protocol activity is illustrated in Fig. 4.

The number of n agreed time-constraint and the remaining qubits after QKD activity may affect $\mathcal{L}$. Hence, the initial random bits length must be huge enough to keep $\mathcal{L}$ satisfied. Thus, the QKD protocol will have the same steps as referred from Boyer *et al.*'s [15] SQKD protocol except for some steps. Then, *Measure-Resend SQKD With New Time-Constraint* is shown as follow:

Measure-Resend SQKD Protocol with New Time-Constraint

Step 1: Alice generates random bits $r > 8n\mathcal{L}$. Alice sends it in qubits form in random basis between Z or the X.

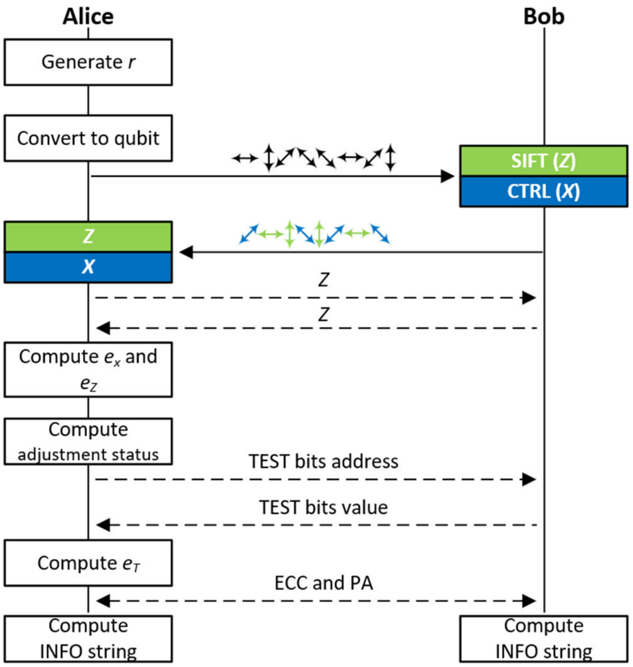

FIGURE 4. Measure-Resend SQKD with new time-constraint between Alice and Bob.

Step 5: Alice checks the error-rate of the collected reflected qubits and if either the X error-rate e_X or the Z error-rate e_Z is higher than some predefined threshold CTRL the protocol aborts. Next, Alice checks the condition $\left\lfloor \frac{number\ of\ SIFT\ bits}{n} \right\rfloor > \mathcal{L}$. If it returns false, then Alice does the adjusting operation $n = \left\lfloor \frac{n}{2} \right\rfloor$.

Step 6: Alice chooses the addresses of SIFT bits randomly to be TEST bits. Alice publishes it along with the adjustment status. Bob proceeds the adjustment status and publishes the value of these TEST bits. Alice checks the error-rate on the TEST bits e_T if it is higher than the predefined threshold then the protocol aborts.

Step 8: Alice publishes ECC and PA data, from which she and Bob extract the final key $SK_{1 \ldots n}$ from the INFO string. □

The results are set of session keys $SK_{1 \ldots n}$ from step 8 with the number of time-constraint sessions $\{tb_1, tb_2, \ldots, tb_n\}$ with n value from step 4. With that, Alice and Bob could perform scheduled communication securely. In step 5, the "division by two" operation is used to adjust the n adopted from the Additive-Increase Multiplicative-Decrease algorithm [26]. It is a feedback control algorithm that already well-known as the best congestion control for Transmission Control Protocol (TCP). Such condition and the adjusting operation are added even though the output will rarely return a false value because the initial bit length is set to occupy the pre-agreed session key needs.

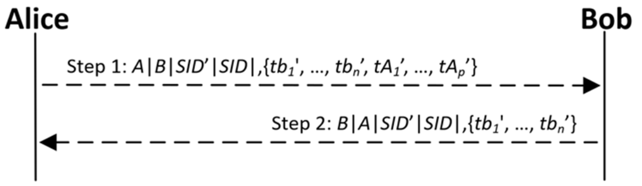
Alice
Bob
Step 1: *A*|*B*|*SID'*|*SID*|,{*tb*₁', ..., *tb*ₙ', *tA*₁', ..., *tA*ₚ'}
Step 2: *B*|*A*|*SID'*|*SID*|,{*tb*₁', ..., *tb*ₙ'}

FIGURE 5. Time-constraint update agreement between Alice and Bob.

C. TIME-CONSTRAINT UPDATE AGREEMENT

This phase is for creating other sessions because the current session communication is good in terms of security. In this phase, Alice may change the remaining time-constraint $tb'_k, tb'_{k+1}, \ldots, tb'_n$ or keep it. If Alice wants to keep it, then the value of $tb'_k, tb'_{k+1}, \ldots, tb'_n$ remain the same. As shown in Fig. 5, let Alice wants to update the session key which is starting from $tb'_{k:n}$ and add some next time-constraint $tA_{1:p}$.

Time-Constraint Update Agreement

Step 1: Alice generates a set of time-constraint in accordance with the time of the continuation communication sessions that Alice proposes to Bob. The previous set of time-constraint SID' needs to be attached so that the data will become $SID'|SID, \left\{tb'_k, tb'_{k+1}, \ldots, tb'_n, tA_1, tA_2, \ldots, tA_p\right\}$. Then, Alice sends it to Bob.

Step 2: After Bob receives Alice's request, Bob might agree all of the time-constraint set or part of it based on his resource capability. Then, Bob sends the agreed time-constraint set $SID'|SID, \{tb_1, tb_2, \ldots, tb_n\}$ for both parties to Alice. □

D. MEASURE-RESEND SQKD WITH UPDATED TIME-CONSTRAINT

A little modification from the SQKD protocol proposed by Boyer *et al.*'s [15] is made in order to improve the probability of the measured qubits, as illustrated in Fig. 6. By using the previous session key SK', Alice and Bob will have the same basis for the SQKD activity. Then, *Measure-Resend SQKD With Updated Time-Constraint* is shown as follow:

Measure-Resend SQKD With Updated Time-Constraint

Step 1: Alice generates random bits $r > 4n\mathcal{L}$. Alice uses the basis from the result of the hash computation of the last and remaining session key $H(SK')$. The binary 0 and 1 from the hash result is for Z and X respectively.

Step 2: Similar to Alice, Bob computes $H(SK')$ as the decision to chooses whether to measure and send back it or to reflect it for each qubit arriving.

Step 3: For every qubit reflected or sent back, Alice measures it directly.

Step 4: Alice checks the error-rate of the collected reflected qubits and if either the e_X or the e_Z is higher than some predefined threshold CTRL the protocol aborts. Next, Alice checks

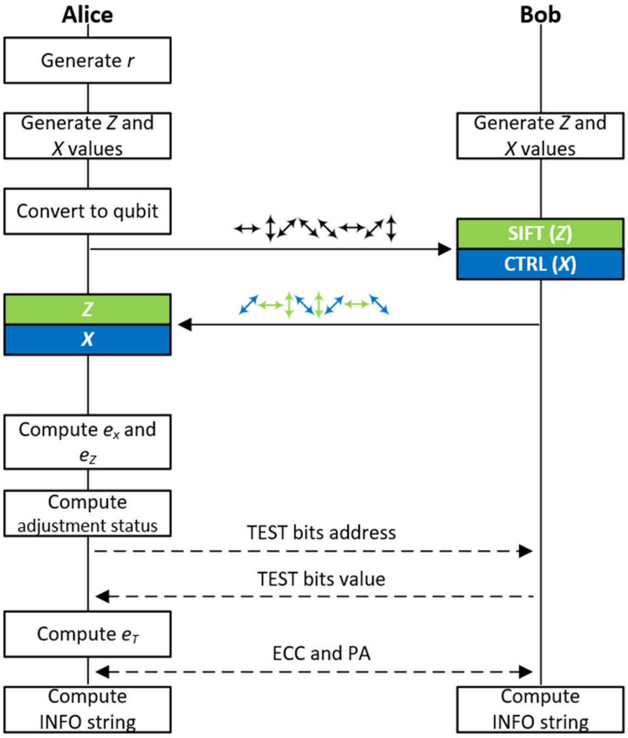

FIGURE 6. **Measure-Resend SQKD with updated time-constraint between Alice and Bob.**

$\left\lfloor \frac{number\ of\ SIFT\ bits}{n} \right\rfloor > \mathcal{L}$. If it returns false, then Alice adjusts the $n = \left\lfloor \frac{n}{2} \right\rfloor$.

Step 5: Alice chooses the addresses of SIFT bits randomly to be TEST bits. Alice publishes it along with the adjustment status. Bob proceeds the adjustment status and publishes the value of these TEST bits. Alice checks the e_T if it is higher than the predefined threshold then the protocol aborts.

Step 6: Alice and Bob select some beginning bits of the remaining SIFT bits to be used as INFO bits. If there are no errors or eavesdropping, Alice and Bob share the same string. Otherwise, Bob's string is likely to differ from the INFO string until corrected.

Step 7: Alice publishes ECC and PA data, from which she and Bob extract the final key $SK_{1\ldots n}$ from the INFO string. □

Similar to *MendSQKD-NTCA*, *MendSQKD-UTCA* final process results set of session keys $SK_{1\ldots n}$ with the number of time-constraint sessions $\{tb_1, tb_2, \ldots, tb_n\}$ with n value from step 4. With that, Alice and Bob could continue to perform scheduled communication securely with fresh session key.

V. SECURITY ANALYSES

This section provides security analyses of the proposed protocol. The analysis will be divided into typical attack and formal security analysis using BAN logic.

A. TYPICAL ATTACKS

This type of attack is always used in the security analysis of cryptography research. It consists of man-in-the-middle (MITM) attack, replay attack, and passive attack. MITM can be detected or prevented by authentication and tamper detection. But it is a different case if MITM happens at key or certificate exchange process in building the identity authenticity. At any rate, both parties can prevent MITM easily using QKD [18].

Conventional cryptography uses timestamp or nonce to defend against a replay attack. However, timestamp has a drawback in implementation. If the system is congested, the information may come late, and the solution is not trivial. A nonce is a better option. Qubits are similar to nonce because it is generated of random bits.

An Eavesdropper doing passive attack is difficult to be detected because it does not imply any change in the data. In QKD, it is trivial to detect passive attack activity. To read qubits in the quantum channel, an eavesdropper must guess the correct basis on the current passing qubit. If the guess is wrong, it will affect in qubits received by Bob. Let Alice send qubit ⤢ or ⤡, the eavesdropper reads it using Z basis, the eavesdropper will receive ↔ or ↕ with 0.5 probability.

The probability of a qubit become key from SQKD is 25%. If an eavesdropper attack, then the probability become 25% × 25% = 12.5%. In step 5 of the protocol, Alice may detect the presence of an eavesdropper using formula $P_d = 1 - \left(\frac{7}{8}\right)^{r'}$, where P_d is the probability of eavesdropper detection and r' is the TEST bits. If the predefined threshold in QKD is higher than P_d, the activity may be eavesdropped. Thus, those typical attacks basically cannot be applied in QKD. If an eavesdropper tries to attack, Alice and Bob will detect it in Step 5 of the protocol.

Besides typical attacks, an eavesdropper may attack the QKD process using two unitary operations. The first unitary operation is for every qubit delivered from Alice to Bob. The second one is for every reflected and resent qubit by Bob to Alice. Boyer *et al.* proved that their SQKD is robust from that attack [15]. The condition of eavesdropper attack also applies to MendSQKD-NTCA and MendSQKD-UTCA.

B. BAN LOGIC ANALYSIS

Burrows, Abadi, and Needham [27] proposed a security proof logic called BAN Logic to analyze key distribution protocol. It works to answer questions about; the goal of the protocol, the assumptions that needed to be considered, wasted phase, and the need for data encryption. The logic is based on the belief of a party in the truth of a formula. Since it was developed, BAN Logic has been used to analyze the security protocols [28], [29]. However, it has not been used to analyze QKD protocols. Thus, it is part of this paper novelty to present a BAN Logic analysis in SQKD. It might be possible to adapt the analysis to analyze the security of other QKD protocols formally. For the analysis of SQKD using BAN Logic, it starts

TABLE 2. BAN logic notation.

Symbol	Description
$P\mid\equiv X$	Principal P believes a statement X, or P is entitled to believe X.
$\#(X)$	Formula X is fresh.
$P\mid\Rightarrow X$	Principal P has jurisdiction over statement X.
$P\triangleleft X$	Principal P sees the statement X.
$P\mid\sim X$	Principal P once said the statement X.
(X,Y)	Formula X or Y is one part of formula (X,Y).
$\langle X\rangle_Y$	Formula X combined with the formula Y.
$P\overset{K}{\leftrightarrow}Q$	P and Q may use the shared key K to communicate. The Key K is good, in that it will never be discovered by any principal except P and Q.
$P\overset{X}{\Leftrightarrow}Q$	Formula X is secret known only to P and Q, and possibly to principals trusted by them.

with presenting the basic notation in Table 2 and the four rules of BAN Logic.

BAN Logic has four main rules as follows:

Message meaning rule:

$$R_1:\frac{A\mid\equiv A\overset{K}{\Longleftrightarrow}B,\ A\triangleleft\langle X\rangle_K}{A\mid\equiv B\mid\sim X}$$

Nonce Verification rule:

$$R_2:\frac{A\mid\equiv\#(X),\ A\mid\equiv B\mid\sim X}{A\mid\equiv B\mid\equiv X}$$

Jurisdiction rule:

$$R_4:\frac{A\mid\equiv(B\mid\Longrightarrow X),\ A\mid\equiv B\mid\equiv X}{A\mid\equiv X}$$

Fresh concatenation rules:

$$R_5:\frac{A\mid\equiv\#(X)}{A\mid\equiv\#(X,Y)}$$

Furthermore, Consensus rule is defined so that BAN Logic could be used of analyzing the security of any QKD protocols.

Consensus rule:

$$R_3:\frac{A\mid\equiv X,\ A\mid\equiv A\overset{Y}{\Longleftrightarrow}B,\ A\triangleleft Y,\ X==Y}{A\mid\equiv B\mid\sim Y}$$

Based on BAN Logic analysis criteria, MendSQKD-NTCA, MendSQKD-UTCA, and SQKD are secure if they satisfy the final goals G_1 and G_2 as follows:

$$G_1:A\mid\equiv A\overset{SK}{\leftrightarrow}B$$
$$G_2:B\mid\equiv A\overset{SK}{\leftrightarrow}B$$

From step 1, Alice sends random qubits to Bob (Message M_1):

$$M_1:A\rightarrow B:\left\langle\updownarrow,\leftrightarrow,\neswarrow,\nwsearrow\right\rangle_{Bs_A}$$

From step 2, Bob chooses to measure message M_1 or reflect it. The results are:

1) *Message M_2 (the reflected message)*:

$$M_2:B\rightarrow A:\left\langle\left\langle\updownarrow,\leftrightarrow,\neswarrow,\nwsearrow\right\rangle_{Bs'_A}\right\rangle_{X_B}$$

2) *Message M_3 (the measured message)*:

$$M_3:B\triangleleft\left\langle\left\langle\updownarrow,\leftrightarrow,\neswarrow,\nwsearrow\right\rangle_{Bs_A}\right\rangle_{Z_B}$$

where $M_1=M_2+M_3$

From step 4, Alice publishes her Z bits and Bob publishes his X bits

$$M_4:A\rightarrow B:Z_A$$
$$M_5:B\rightarrow A:X_B$$

From step 6, Alice sends test bits at $K'_A[I]$ to Bob, Bob reply with the bits value $K'_B[I]$ to Alice

$$M_6:A\rightarrow B:K'_A[I]$$
$$M_7:B\rightarrow A:K'_B[I]$$

Before the analysis begin, the preparation of some hypothesis from H_1 until H_{22} as assumptions for the initial state in each principal is written as follows:

$$H_1:Bs=X+Z;\ H_2:A\mid\Longrightarrow\left\langle\updownarrow,\leftrightarrow,\neswarrow,\nwsearrow\right\rangle_{Bs_A};$$
$$H_3:Z_A\mid\equiv\updownarrow,\leftrightarrow;\ H_4:X_A\mid\equiv\neswarrow,\nwsearrow;\ H_5:A\mid\Longrightarrow Bs_A;$$
$$H_6:A\xLeftrightarrow{\langle\updownarrow,\leftrightarrow\rangle Z_{A==B}}B\mid\Longrightarrow A\overset{K_A}{\Longleftrightarrow}B;$$
$$H_7:A\xLeftrightarrow{\langle\updownarrow,\leftrightarrow\rangle Z_{B==A}}B\mid\Longrightarrow A\overset{K_B}{\Longleftrightarrow}B;$$
$$H_8:A\mid\equiv A\xLeftrightarrow{\updownarrow,\leftrightarrow,\neswarrow,\neswarrow}B;$$
$$H_9:A\mid\equiv\#\left(\updownarrow,\leftrightarrow,\neswarrow,\nwsearrow\right);H_{10}:A\mid\equiv\#(Bs_B);$$
$$H_{11}:A\mid\equiv B\mid\Longrightarrow Bs_B;\ H_{12}:B\mid\equiv A\xLeftrightarrow{\updownarrow,\leftrightarrow,\neswarrow,\nwsearrow}B;$$
$$H_{13}:B\mid\equiv\#\left(\updownarrow,\leftrightarrow,\neswarrow,\nwsearrow\right);H_{14}:A\mid\equiv A\overset{I}{\Longleftrightarrow}B;$$
$$H_{15}:B\mid\equiv A\overset{I}{\Longleftrightarrow}B;\ H_{16}:A\mid\equiv\#\left(K'_B[I]\right);$$
$$H_{17}:B\mid\equiv\#\left(K'_A[I]\right);H_{18}:B\mid\Longrightarrow\left(K'_B[I]\right);$$
$$H_{19}:A\mid\Longrightarrow\left(K'_A[I]\right);H_{20}:A\mid\equiv B\mid\Longrightarrow\left(K'_B[I]\right);$$
$$H_{21}:B\mid\equiv A\mid\Longrightarrow\left(K'_A[I]\right);$$
$$H_{22}:A\overset{SK}{\Longleftrightarrow}B=A\overset{K}{\Longleftrightarrow}B-K'.$$

The idealized form of the proposed protocol is analysed based on the BAN logic rules and the assumptions. The main proofs are stated as follows:

S_1 is obtained by having M_5.

$$S_1:A\triangleleft X_b$$

S_2 is obtained by applying hypothesis H_1 to S_1.

$$S_2:A\triangleleft Z_b$$

S_3 is obtained by applying hypothesis H_1,H_2,H_3 to S_2.

$$S_3:A\triangleleft\langle\updownarrow,\leftrightarrow\rangle_{Z_{A==B}}$$

S_4 is obtained by having M_2.

$$S_4:A\triangleleft\left\langle\left\langle\updownarrow,\leftrightarrow,\neswarrow,\nwsearrow\right\rangle_{Bs'_A}\right\rangle_{X_B}$$

S_5 is obtained by applying hypothesis H_2 to S_1.

$$S_5 : A| \Longrightarrow \left\langle \langle \updownarrow, \leftrightarrow, \neswarrow, \nwsearrow \rangle_{Bs_A} \right\rangle_{X_B}$$

S_6 and S_7 are obtained by applying hypothesis H_2 and rule R_3 to S_4, S_5.

$$S_6 : A \mid\equiv B| \sim \left\langle \langle \updownarrow, \leftrightarrow, \neswarrow, \nwsearrow \rangle_{Bs'_A} \right\rangle_{X_B}$$
$$S_7 : A| \equiv B| \sim X_B$$

S_8 and S_9 are obtained by applying hypothesis H_1, H_{10} and rule R_2 to S_6, S_7.

$$S_8 : A \mid\equiv B| \equiv \left\langle \langle \updownarrow, \leftrightarrow, \neswarrow, \nwsearrow \rangle_{Bs'_A} \right\rangle_{X_B}$$
$$S_9 : A \mid\equiv B| \equiv X_B$$

S_{10} and S_{11} are obtained by applying hypothesis H_1, H_{11} and rule R_4 to S_8, S_9.

$$S_{10} : A| \equiv \left\langle \langle \updownarrow, \leftrightarrow, \neswarrow, \nwsearrow \rangle_{Bs'_A} \right\rangle_{X_B}$$
$$S_{11} : A| \equiv X_B$$

S_{12} is obtained by applying hypothesis H_1 to S_{11}.

$$S_{12} : A| \equiv Z_B$$

S_{13} is obtained by applying hypothesis H_1, H_5 and rule R_4 to S_3.

$$S_{13} : A| \equiv \langle \updownarrow, \leftrightarrow \rangle_{Z_{A==B}}$$

S_{14} is obtained by applying hypothesis H_6 and rule R_4 to S_{13}.

$$S_{14} : A| \equiv A \overset{K_A}{\Longleftrightarrow} B$$

S_{15} is obtained by having M_4.

$$S_{15} : B \triangleleft Z_A$$

S_{16} is obtained by combining S_{15} and M_3

$$S_{16} : B \triangleleft \langle \updownarrow, \leftrightarrow \rangle_{Z_{B==A}}$$

S_{17} is obtained by applying hypothesis H_{12} and rule R_1 to S_{16}.

$$S_{17} : B \mid\equiv A| \sim \langle \updownarrow, \leftrightarrow \rangle_{Z_{B==A}}$$

S_{18} is obtained by applying hypothesis H_{13} and rule R_2 to S_{17}.

$$S_{18} : B \mid\equiv A| \equiv \langle \updownarrow, \leftrightarrow \rangle_{Z_{B==A}}$$

S_{19} is obtained by applying hypothesis H_2 and rule R_4 to S_{18}.

$$S_{19} : B| \equiv \langle \updownarrow, \leftrightarrow \rangle_{Z_{B==A}}$$

S_{20} is obtained by applying hypothesis H_7 and rule R_4 to S_{19}.

$$S_{20} : B| \equiv A \overset{K_B}{\Longleftrightarrow} B$$

S_{21} is obtained by having M_7.

$$S_{21} : A \triangleleft K'_B\,[I]$$

S_{22} is obtained by applying hypothesis H_{14}, H_{18} and rule R_3 to S_{21}.

$$S_{22} : A \mid\equiv B| \sim K'_B\,[I]$$

S_{23} is obtained by applying hypothesis H_{16} and rule R_2 to S_{22}.

$$S_{23} : A \mid\equiv B| \equiv K'_B\,[I]$$

S_{24} is obtained by applying hypothesis H_{20} and rule R_4 to S_{23}.

$$S_{24} : A| \equiv K'_B\,[I]$$

S_{25} is obtained by having M_6.

$$S_{25} : B \triangleleft K'_A\,[I]$$

S_{26} is obtained by applying hypothesis H_{15}, H_{19} and rule R_3 to S_{25}

$$S_{26} : B \mid\equiv A| \sim K'_A\,[I]$$

S_{27} is obtained by applying hypothesis H_{17} and rule R_2 to S_{26}.

$$S_{27} : B \mid\equiv A| \equiv K'_A\,[I]$$

S_{28} is obtained by applying hypothesis H_{21} and rule R_4 to S_{27}.

$$S_{28} : B| \equiv K'_A\,[I]$$

By applying hypothesis H_{22} to S_{24} and S_{14} the predefined goal G_1 is achieved.

$$S_{29} : A| \equiv A \overset{SK}{\Longleftrightarrow} B$$

By applying hypothesis H_{22} to S_{28} and S_{20} the predefined goal G_2 is achieved.

$$S_{30} : B| \equiv A \overset{SK}{\Longleftrightarrow} B$$

From S_{29} and S_{30}, the predefined goals, G_1 and G_2, are achieved. SQKD is proven secure by BAN Logic analysis. Furthermore, any wasted phase is not arisen in the analysis. In terms of data encryption, data that is not in the quantum channel is easy to eavesdrop. However, the eavesdropper will not get any information because the data is only for discussion between parties. Thus, those data do not need any encryption process. The remaining consideration thing is the hypothesis listed in H_1 through H_{22}. It consists of logic formulas of computation in each party, freshness, and quantum channel. Computation can be proven by using math or binary operation. Freshness can be proven from its newness and randomness data. Lastly, hypotheses that are generated from quantum characteristics can be proven using previous quantum security analysis [8], [15], [30].

Consensus rule as an additional BAN rule is included in the analysis. Consensus could be used as security analysis means. In the Blockchain system [31], the transaction is done in peer to peer manner between parties. Thus, blockchain has miners that have a job to validate every transaction before putting it to the block using a consensus mechanism. It could be in the form of Proof-of-Work, Proof-of-Stake [32], or a hybrid approach. In QKD, a consensus is an agreement between parties to decide the key based on basis similarity. The qubit is proceeded further if on the same basis and is omitted if on a different basis. Thus, the rule is formulated as in R_3.

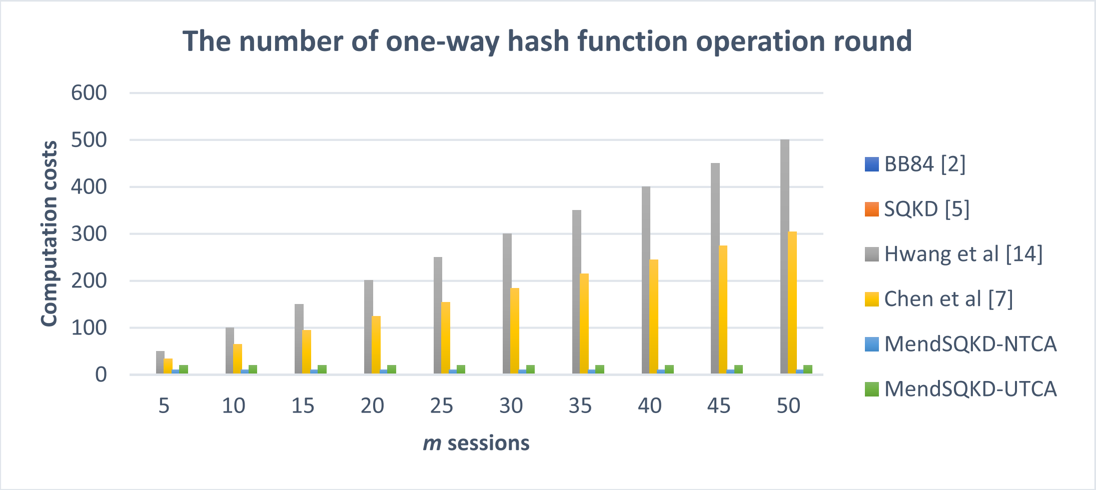

FIGURE 7. Comparison results on the number of one-way hash function operation round.

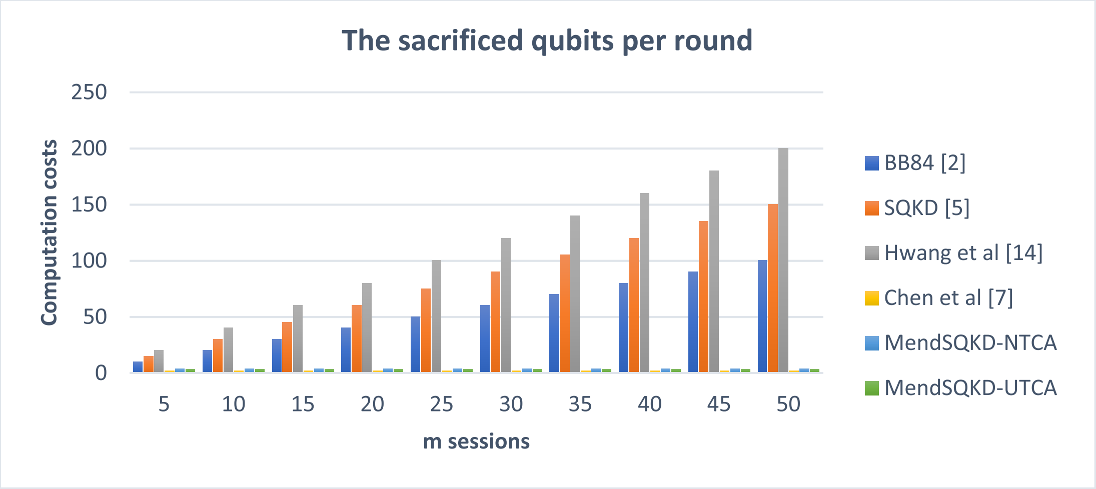

FIGURE 8. Comparison results on the sacrificed qubits per round.

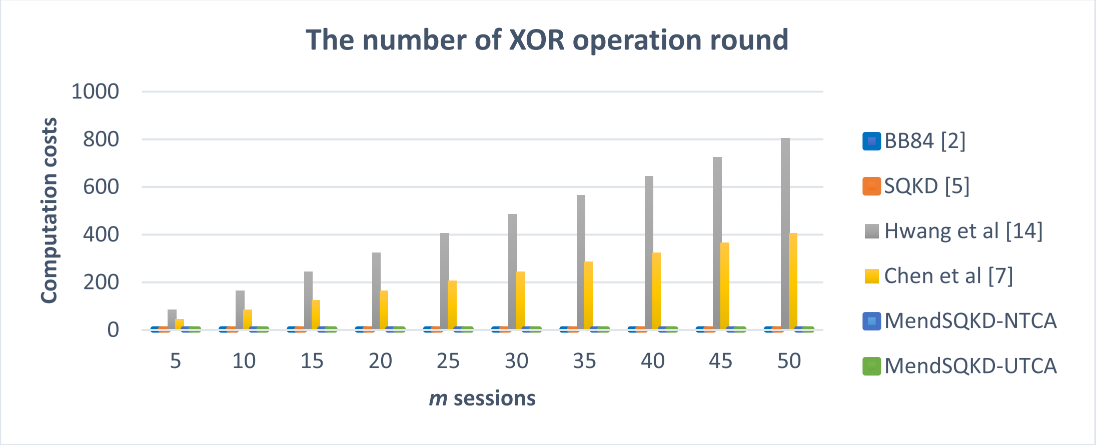

FIGURE 9. Comparison results on the number of XOR operation round.

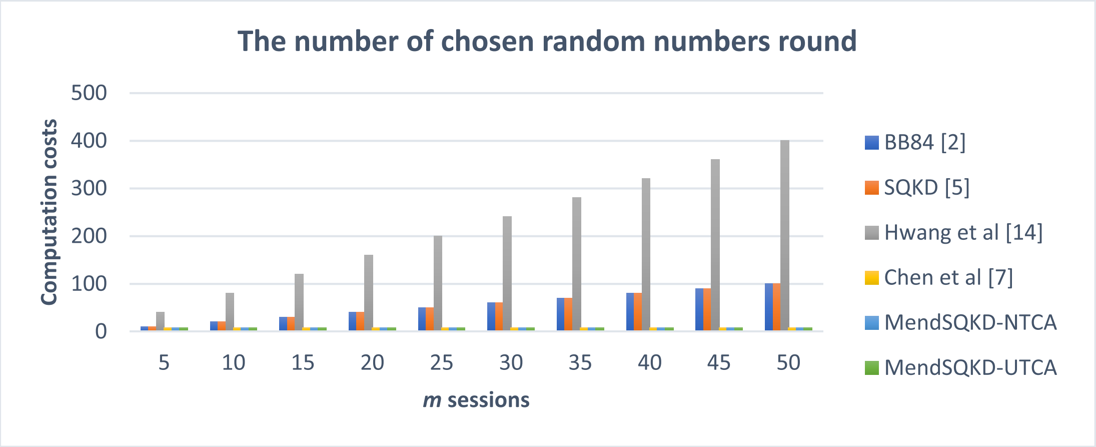

FIGURE 10. Comparison results on the number of chosen random numbers round.

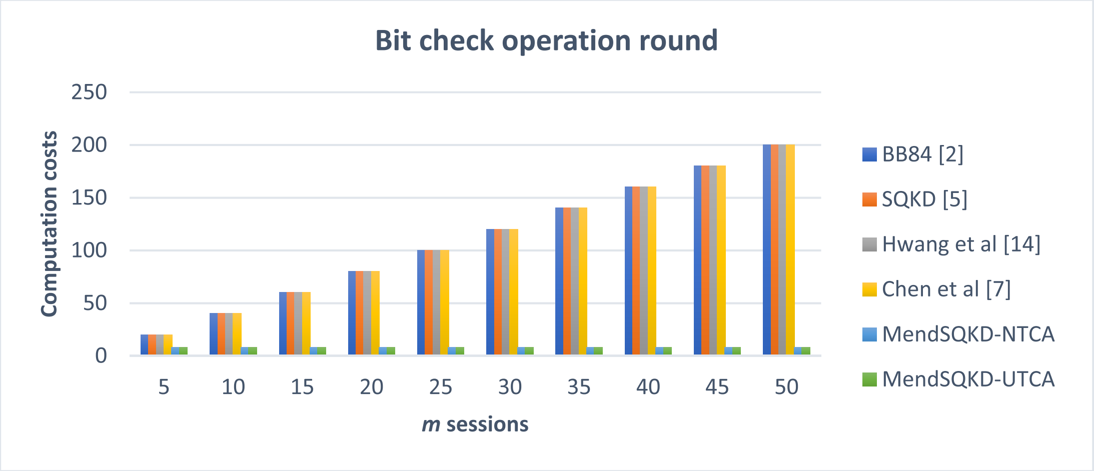

FIGURE 11. Comparison results on bit check operation round.

VI. PERFORMANCE ANALYSIS AND SIMULATION ASSESSMENT

Both MendSQKD-NTCA and MendSQKD-UTCA are analyzed in this section, then they are compared with other previous works [9], [15], [18], [25]. Originally, one QKD activity generating a key or session key. Here, the proposed protocols support efficiency by generating the multi-session key in one QKD activity. Five items of computation costs are listed as follows: The number of one-way hash function operation round, the sacrificed qubits per round, the number of XOR operation round, the number of chosen random numbers, and bit check operation round. Table 3 shows the analysis of each QKD based on those items. The results of the performance comparison based on value and the computational items are depicted in Fig. 7–11. The proposed protocols and Chen *et al.* [25] protocol could generate many session keys in one QKD so that it could outperform others. Furthermore, the proposed protocols outperform Chen *et al.* [25] protocol in all items except the sacrificed qubits per QKD round.

We also made QKD simulation for the proposed protocols in normal and eavesdropping occurrence condition using Quantum Information Toolkit in python [33]. In simulation without eavesdropping activity, 100 experiments in different given r and initial error rate are applied. The error rate simulation is used to change qubits state as given probability. Error is caused by complex noises and the limit should be defined to prevent data loss [34]. Fig. 12 shows the experiment results. In 0 error rate, it is proven that r must larger than $8n\mathcal{L}$ for MendSQKD-NTCA and larger than $4n\mathcal{L}$ for MendSQKD-UTCA to make 100% successful QKD activity. Thus, the defined protocols meet the minimum value of r. If the quantum environment has 0.0001 error rate, the device might made 97% successful QKD activity after the minimum requirement of r is fulfilled. If the error rate is higher, the chance for successful QKD become smaller. It corresponds with the Fig. 12 that QKD activity in 0.001 error rate and same r has around 70% successful probability. In simulation with eavesdropping activity, Alice always detects the

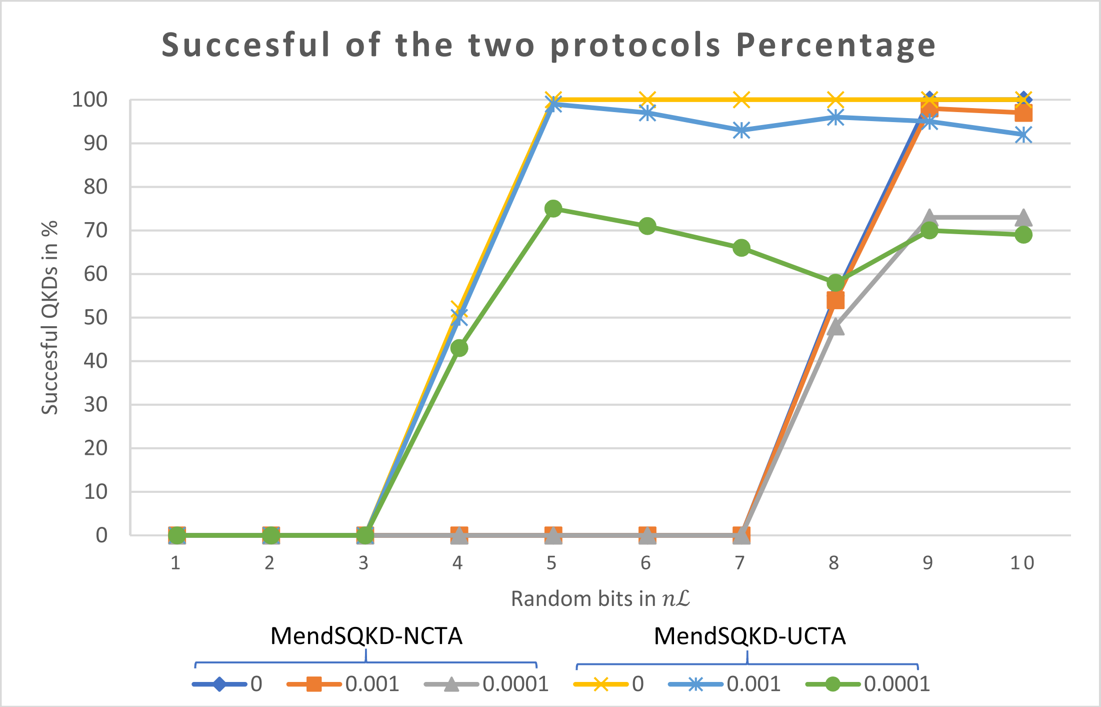

FIGURE 12. The simulation assessment with *MendSQKD-NCTA* and *MendSQKD-UCTA* varied by error rate and the number of given random bits.

TABLE 3. Performance analysis each QKD protocol.

Compared Items	Protocols	Alice	Bob	TC
The number of one-way hash function operation	BB84 [9]	0	0	none
	SQKD [15]	0	0	none
	Hwang *et al.* [18]	$4m$	$4m$	$2m$
	Chen *et al.* [25]	$4+3(m\text{-}1)$	$4+3(m\text{-}1)$	2
	MendSQKD-NTCA	0	0	none
	MendSQKD-UTCA	1	1	none
The sacrificed qubits per round	BB84 [9]	$0.5m$	$0.5m$	none
	SQKD [15]	$0.75m$	$0.75m$	none
	Hwang *et al.* [18]	0	0	0
	Chen *et al.* [25]	0	0	0
	MendSQKD-NTCA	0.75	0.75	none
	MendSQKD-UTCA	0.5	0.5	none
The number of XOR operation round	BB84 [9]	0	0	none
	SQKD [15]	0	0	none
	Hwang *et al.* [18]	$3m$	$3m$	$2m$
	Chen *et al.* [25]	$3+2(m\text{-}1)$	$3+2(m\text{-}1)$	2
	MendSQKD-NTCA	0	0	none
	MendSQKD-UTCA	0	0	none
The number of chosen random numbers	BB84 [9]	m	0	none
	SQKD [15]	m	0	none
	Hwang *et al.* [18]	m	m	$2m$
	Chen *et al.* [25]	0	0	2
	MendSQKD-NTCA	2	0	none
	MendSQKD-UTCA	2	0	none
Bit check operation round	BB84 [9]	m	m	none
	SQKD [15]	$2m$	0	none
	Hwang *et al.* [18]	m	m	0
	Chen *et al.* [25]	m	m	0
	MendSQKD-NTCA	2	0	None
	MendSQKD-UTCA	2	0	None

eavesdropping activity when checking the qubits and the basis from Bobs.

VII. CONCLUSION

In this paper, the first SQKD with time-constraint agreement protocol is proposed to generate session keys constrained with agreed time-constraint to facilitate communication in occasional and sporadic time between two parties. It contains new time-constraint agreement phase and the first proposed SQKD. This protocol has a mitigation method if the generated keys length is below predefined limit to prevent repeated QKD activity. The first protocol can generate keys from around 25% used qubits. The second SQKD with time-constraint agreement protocol is proposed to improve the generated keys into around 50% used qubits. Time-constraint update mechanism is utilized for the parties continuing the session rounds. MendSQKD-NTCA and MendSQKD-UTCA are proven secure from the prementioned attacks. BAN logics analysis is applied to prove the security requirement that needs to be considered is satisfied. In terms of performance evaluation, the proposed protocols outperform previous QKD protocols in the aforementioned comparison aspects.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

[1] K. Lim, K. M. Tuladhar, X. Wang, and W. Liu, "A scalable and secure key distribution scheme for group signature based authentication in VANET," in *Proc. IEEE 8th Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf. (UEMCON)*, New York, NY, USA, Oct. 2017, pp. 478–483, doi: 10.1109/UEMCON.2017.8249091.

[2] E. Frimpong, R. Rabbaninejad, and A. Michalas, "Arrows in a quiver: A secure certificateless group key distribution protocol for drones," in *Secure IT Systems*, vol. 13115, N. Tuveri, A. Michalas, and B. B. Brumley, Eds. Cham, Switzerland: Springer, 2021, pp. 31–48, doi: 10.1007/978-3-030-91625-1_3.

[3] K. Mahmood, X. Li, S. A. Chaudhry, H. Naqvi, S. Kumari, A. K. Sangaiah, and J. J. P. C. Rodrigues, "Pairing based anonymous and secure key agreement protocol for smart grid edge computing infrastructure," *Future Gener. Comput. Syst.*, vol. 88, pp. 491–500, Nov. 2018, doi: 10.1016/j.future.2018.06.004.

[4] G. Chai, D. Li, Z. Cao, M. Zhang, P. Huang, and G. Zeng, "Blind channel estimation for continuous-variable quantum key distribution," *Quantum Eng.*, vol. 2, no. 2, p. e37, Jun. 2020, doi: 10.1002/que2.37.

[5] H.-C. Chen, "Collaboration IoT-based RBAC with trust evaluation algorithm model for massive IoT integrated application," *Mobile Netw. Appl.*, vol. 24, no. 3, pp. 839–852, Jun. 2019, doi: 10.1007/s11036-018-1085-0.

[6] C. L. Chen, D. P. Lin, H. C. Chen, Y. Y. Deng, and C. F. Lee, "Design of a logistics system with privacy and lightweight verification," *Energies*, vol. 12, no. 16, Aug. 2019, Art. no. 3061, doi: 10.3390/en12163061.

[7] C.-L. Chen, P.-T. Huang, Y.-Y. Deng, H.-C. Chen, and Y.-C. Wang, "A secure electronic medical record authorization system for smart device application in cloud computing environments," *Hum.-centric Comput. Inf. Sci.*, vol. 10, no. 21, pp. 1–31, Dec. 2020, doi: 10.1186/s13673-020-00221-1.

[8] W. K. Wootters and W. H. Zurek, "The no-cloning theorem," *Phys. Today*, vol. 62, no. 2, pp. 76–77, Feb. 2009, doi: 10.1063/1.3086114.

[9] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," presented at the Conf. Comput., Syst. Signal Process., Bangalore, India, 1984.

[10] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Phys. Rev. Lett.*, vol. 68, no. 21, pp. 3121–3124, May 1992, doi: 10.1103/PhysRevLett.68.3121.

[11] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, pp. 661–663, Aug. 1991, doi: 10.1103/PhysRevLett.67.661.

[12] G. L. Long and X. S. Liu, "Theoretically efficient high-capacity quantum-key-distribution scheme," *Phys. Rev. A, Gen. Phys.*, vol. 65, no. 3, Feb. 2002, Art. no. 032302, doi: 10.1103/PhysRevA.65.032302.

[13] R. Qi, Z. Sun, Z. Lin, P. Niu, W. Hao, L. Song, Q. Huang, J. Gao, L. Yin, and G.-L. Long, "Implementation and security analysis of practical quantum secure direct communication," *Light: Sci. Appl.*, vol. 8, no. 1, p. 22, 2019, doi: 10.1038/s41377-019-0132-3.

[14] D. Pan, K. Li, D. Ruan, S. X. Ng, and L. Hanzo, "Single-photon-memory two-step quantum secure direct communication relying on Einstein-Podolsky-Rosen pairs," *IEEE Access*, vol. 8, pp. 121146–121161, 2020, doi: 10.1109/ACCESS.2020.3006136.

[15] M. Boyer, R. Gelles, D. Kenigsberg, and T. Mor, "Semiquantum key distribution," *Phys. Rev. A, Gen. Phys.*, vol. 79, no. 3, Mar. 2009, Art. no. 032341, doi: 10.1103/PhysRevA.79.032341.

[16] F.-G. Deng and G. L. Long, "Secure direct communication with a quantum one-time pad," *Phys. Rev. A, Gen. Phys.*, vol. 69, no. 5, May 2004, Art. no. 052319, doi: 10.1103/PhysRevA.69.052319.

[17] H. C. Shih, K. C. Lee, and T. Hwang, "New efficient three-party quantum key distribution protocols," *IEEE J. Sel. Topics Quantum Electron.*, vol. 15, no. 6, pp. 1602–1606, Nov. 2009, doi: 10.1109/JSTQE.2009.2019617.

[18] T. Hwang, K. C. Lee, and C. M. Li, "Provably secure three-party authenticated quantum key distribution protocols," *IEEE Trans. Dependable Secure Comput.*, vol. 4, no. 1, pp. 71–80, Jan. 2007, doi: 10.1109/TDSC.2007.13.

[19] H.-C. Chen, "A multi-issued tag key agreement with time constraint for homeland defense sub-department in NFC environment," *J. Netw. Comput. Appl.*, vol. 38, pp. 88–98, Feb. 2014, doi: 10.1016/j.jnca.2013.05.004.

[20] S. Sathyadevan, K. Achuthan, R. Doss, and L. Pan, "Protean authentication scheme–A time-bound dynamic keygen authentication technique for IoT edge nodes in outdoor deployments," *IEEE Access*, vol. 7, pp. 92419–92435, 2019, doi: 10.1109/ACCESS.2019.2927818.

[21] Z.-R. Liu and T. Hwang, "Mediated semi-quantum key distribution without invoking quantum measurement," *Annalen der Physik*, vol. 530, no. 4, Apr. 2018, Art. no. 1700206, doi: 10.1002/andp.201700206.

[22] N. Zhou, K. Zhu, and X. Zou, "Multi-party semi-quantum key distribution protocol with four-particle cluster states," *Annalen der Physik*, vol. 531, no. 8, Aug. 2019, Art. no. 1800520, doi: 10.1002/andp.201800520.

[23] K.-N. Zhu, N.-R. Zhou, Y.-Q. Wang, and X.-J. Wen, "Semi-quantum key distribution protocols with GHZ states," *Int. J. Theor. Phys.*, vol. 57, no. 12, pp. 3621–3631, Dec. 2018, doi: 10.1007/s10773-018-3875-3.

[24] H.-C. Chen, H.-Y. Chuang, T.-L. Kung, and Y.-F. Huang, "An enhanced three-party encrypted key exchange protocol using digital time-stamp," in *Proc. 6th Int. Conf. Netw. Comput. Adv. Inf. Manage.*, Aug. 2010, pp. 665–670, doi: 10.1109/IMIS.2011.145.

[25] H.-C. Chen, S.-Z. Lin, and T.-L. Kung, "Three-party authenticated quantum key distribution protocol with time constraint," in *Proc. 6th Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput.*, Palermo, Italy, Jul. 2012, pp. 506–511, doi: 10.1109/IMIS.2012.154.

[26] D.-M. Chiu and R. Jain, "Analysis of the increase and decrease algorithms for congestion avoidance in computer networks," *Comput. Netw. ISDN Syst.*, vol. 17, no. 1, pp. 1–14, 1989, doi: 10.1016/0169-7552(89)90019-6.

[27] J. Wessels, *Application of BAN-Logic*. CMG Finance B.V., Apr. 2001, pp. 1–23.

[28] J. Lee, S. Yu, K. Park, Y. Park, and Y. Park, "Secure three-factor authentication protocol for multi-gateway IoT environments," *Sensors*, vol. 19, no. 10, May 2019, Art. no. 2358, doi: 10.3390/s19102358.

[29] V. Odelu, A. K. Das, and A. Goswami, "A secure biometrics-based multi-server authentication protocol using smart cards," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 9, pp. 1953–1966, Sep. 2015, doi: 10.1109/TIFS.2015.2439964.

[30] W. O. Krawec, "Security proof of a semi-quantum key distribution protocol," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Hong Kong, Jun. 2015, pp. 686–690, doi: 10.1109/ISIT.2015.7282542.

[31] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," White Paper, Oct. 2008, pp. 1–9.

[32] S. King and S. Nadal, "PPcoin: Peer-to-peer crypto-currency with proof-of-stake," to be published, Aug. 2012, pp. 1–6.

[33] V. Bergholm, J. D. Biamonte, and J. D. Whitfield. *Quantum Information Toolkit*. Accessed: Oct. 24, 2020. [Online]. Available: http://qit.sourceforge.net/

[34] Y. Zhang and Q. Ni, "Design and analysis of random multiple access quantum key distribution," *Quantum Eng.*, vol. 2, no. 1, Mar. 2020, doi: 10.1002/que2.31.

[35] M. Zhu, K. Cui, S. Li, L. Kong, S. Tang, and J. Sun, "A code rate-compatible high-throughput hardware implementation scheme for QKD information reconciliation," *J. Lightw. Technol.*, early access, Feb. 8, 2022, doi: 10.1109/JLT.2022.3149567.

HSING-CHUNG CHEN (Senior Member, IEEE) received the Ph.D. degree in electronic engineering from the National Chung Cheng University, Taiwan, in 2007. From February 2008 to February 2013, he was an Assistant Professor with the Department of Computer Science and Information Engineering, Asia University, Taiwan. From February 2013 to July 2018, he was an Associate Professor with the Department of Computer Science and Information Engineering, Asia University. He was a Full Professor with the Department of Computer Science and Information Engineering, from August 2018 to July 2019. Since August 2019, he has been a Distinguished Full Professor with the Department of Computer Science and Information Engineering, Asia University. Since May 2014, he has also been the Research Consultant with the Department of Medical Research, China Medical University Hospital, China Medical University, Taichung, Taiwan. His current research interests include information and communication security, quantum cryptography, blockchain network security, artificial intelligence of things (AIoT), mobile and wireless networks protocols, medical and bio-information signal image processing, explainable artificial intelligence (XAI) and soft computing, and applied cryptography. Since February 2017, he has also been a Permanent Council Member of Taiwan Domain Names Association (Taiwan DNA), Taiwan. He had been awarded the ACM Best Paper Presentation Certificate by ICFET 2020 (ACM 2020). He had also been awarded the Best Paper Awards by BWCCA2018, MobiSec2017, and BWCCA2016, individually. He was awarded the Best Journal Paper Award by Association Algorithm & Computation Theory (AACT). He was also the Program Committee Chair of APNIC44, in September 2017, organized by the Asia-Pacific Network Information Centre (APNIC).

CAHYA DAMARJATI received the B.S. and M.S. degrees in electrical engineering from Universitas Gadjah Mada, Yogyakarta, Indonesia, in 2009 and 2015, respectively, and the Ph.D. degree in computer science and information engineering from Asia University, Taichung, Taiwan, in 2022. Since 2015, he has been an Assistant Professor with the Department of Information Technology, Universitas Muhammadiyah Yogyakarta. His research interests include information security, quantum cryptography, computer vision, and artificial intelligence.

EKO PRASETYO (Member, IEEE) received the B.S. degree in electrical engineering and the M.S. degree in engineering from Universitas Gadjah Mada Yogyakarta, in 1991 and 2011, respectively. He is currently pursuing the Ph.D. degree with the Department of Computer Science and Information Engineering, Asia University, Taiwan. He is currently a Lecturer with the Department of Information Technology, Universitas Muhammadiyah Yogyakarta. His research interests include digital learning, data mining, information security, computer vision, and artificial intelligence.

CHAO-LUNG CHOU received the Ph.D. degree in electrical and electronics engineering from the Chung Cheng Institute of Technology, National Defense University, Taiwan, in 2012. Since 2015, he has been an Assistant Professor with the Computer Science and Information Engineering Department, Chung Cheng Institute of Technology, National Defense University. His research interests include information security, image processing, machine learning, and biometrics.

TZU-LIANG KUNG received the B.S. degree in industrial administration from the National Taiwan University, in 1997, and the M.S. degree in statistics and the Ph.D. degree in computer science from the National Chiao Tung University, Taiwan, in 2001 and 2009, respectively. From 2001 to 2004, he worked as a Senior Engineer at Behavior Design Corporation, Taiwan. He is currently an Associate Professor with the Department of Computer Science and Information Engineering, Asia University, Taiwan. His research interests include multivariate data analysis, natural language processing, interconnected systems, fault-tolerant computing, algorithm design, and wireless networks.

CHIEN-ERH WENG received the M.S. degree in electrical engineering from the National Yunlin University of Science & Technology, Yunlin, Taiwan, in 2000, and the Ph.D. degree in electrical engineering from the National Chung Cheng University, Chiayi, Taiwan, in 2007. Since September 2007, he has been with the Department of Information Management, Shu-Te University, Kaohsiung, Taiwan, as an Assistant Professor, and since February 2010, he has been with the Department of Electronic Communication Engineering, National Kaohsiung Marine University, Kaohsiung, as an Assistant Professor. Since February 2020, he has been a Professor with the National Kaohsiung University of Science and Technology (NKUST). He is also the Vice Dean of Research and Development Office. He is one of the first team member finished the GWO BST and BTT train in NKUST, he also has the advanced professional license of UAV. His research interests include the fields of signal processing, data analysis, 5G/B5G communication systems, machine learning, and automatic identification systems (AIS).

• • •