IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 25, 2018, accepted January 9, 2019, date of publication January 21, 2019, date of current version February 14, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2894101

Improved Dynamic Multi-Party Quantum Private Comparison for Next-Generation Mobile Network

HUSSEIN ABULKASIM[1,2], HANAN NASER ALSUQAIH[3], WALAA FAWZY HAMDAN[3,4], SAFWAT HAMAD[5], AHMED FAROUK[6,7], ATEFEH MASHATAN[7], AND SHOHINI GHOSE[6,8]

[1]Faculty of Science, The New Valley University, El-Kharja 72511, Egypt
[2]Faculty of Science, South Valley University, Qena 83523, Egypt
[3]Libraries, Documents and Information Department, Princess Nourah Bint Abdul Rahman University, Riyadh 11671, Saudi Arabia
[4]Libraries, Documents and Information Department, Assiut University, Assiut 71515, Egypt
[5]Department of Scientific Computing, Faculty of Computer and Information Sciences, Ain Shams University, Cairo 11566, Egypt
[6]Department of Physics and Computer Science, Wilfrid Laurier University, Waterloo, ON N2L 3C5, Canada
[7]School of Information Technology Management, Ryerson University, Toronto, ON M5B 2K3, Canada
[8]Perimeter Institute for Theoretical Physics, Waterloo, ON N2L 2Y5, Canada

Corresponding author: Ahmed Farouk (afarouk@wlu.ca)

ABSTRACT The advent of next-generation networks, such as fifth-generation cellular wireless (5G), has transformed every aspect of our lives and promised improvement for various real-life applications. Recently, Liu and Wang proposed a dynamic quantum private comparison protocol that utilizes the property of single photon, in both polarization and spatial-mode degrees of freedom. The protocol is intended to compare the private information of any two parties in n parties with the support of the other n-2 parties. However, we show that their protocol is not secure against a particular strategy of collusion attacks that leads to the problem of information leakage. Therefore, this paper suggests a security enhancement against the proposed attack strategy trying to overcome the security limitation of Liu and Wang's work. The security analysis of the suggested improvement proved that the modified protocol is secure against both the internal and external attacks, which could be used to control the various auction models for 5G services as wireless network virtualization in a secure way.

INDEX TERMS Next generation mobile network, quantum private comparison protocol, single photon in both polarization and spatial-mode degrees of freedom, collusion attack.

I. INTRODUCTION

The progress of quantum communication and cryptography has emerged in numerous fields since the first quantum key-distribution (QKD) has been published [1], since QKD is capable of achieving the unconditional security through the principles of quantum mechanics [2]–[4]. QKD or quantum cryptography is used for generating a shared secret-key between two authorized parties, e.g., Alice and Bob, who have a connection via an authenticated channel and a quantum channel [1], [5]–[10]. In the last years, the success of demonstrating QKD protocols has contributed considerably to the development of quantum devices [11]–[15]. Also, many famous branches of quantum cryptography have been developed rapidly, including quantum secure direct communication [19]–[24], quantum teleportation [16]–[18], quantum key agreement [25]–[29], quantum secret sharing [30]–[38], quantum dialogue [39]–[43], quantum private query [44], [45], quantum anonymous ranking [46], quantum anonymous voting [47], quantum oblivious transfer [48]–[51], quantum private comparison (QPC) [52], [53] and others.

QPC protocol based on Einstein–Podolsky–Rosen states has been discussed initially in [52]. The objective of QPC protocols is to allow two or more parties to decide whether their private information is identical or not, without violating data privacy. In [52], a third party (TP) is utilized to generate the initial states and announce the comparison result. Generally, TP is considered after Lo [54] pointed out that it is impossible to achieve the comparison function securely. Accordingly, the trustworthiness of the TP has been divided into three types [53], [55], [56]: (1) Dishonest TP. According to this type, all parties cannot trust TP. As a result, any multiparty QPC protocol is equal to the two party QPC protocol without TP. This situation has been proved insecure by Lo [54]. (2) Honest TP. In this case, each party only needs to perform one-time pad encryption to her/his private secret to transmit it to TP, then TP compares parties' secrets and announces the comparison result. Yet, it is arduous to find an honest TP in real life. (3) Semi-honest TP. In [53], [55], and [56], the semi-honest TP is defined into two kinds of assumptions. The first definition is that TP performs the processes of the protocol loyally, registers all the results of computations, and might try to eavesdrop on the parties' private secrets but not allowed to conspire with other parties. The second definition is that TP may misbehave on its own (sometimes called as an almost-dishonest TP) [58], yet he cannot conspire with any party. Without difficulty, the semi-honest TP is the most reasonable model. Furthermore, Sun *et al.* [57] proposed a secured QPC protocol with another adversary model where the TP is malicious, in which the TP may execute the protocol at his/her wishes for learning further information. Recently, Hung *et al.* [58] proposed a QPC protocol with two TPs, the first TP is malicious and his role is to announce the final comparison result, while the second TP monitors the first one and detect whether the first TP announces a correct comparison result or not. In 2017, Liu *et al.* [59] presented a QPC protocol with an almost-fully-dishonest TP, their protocol can carry out lower communication complexity using single-photons interference. Subsequently, many other QPC protocols have been proposed for improving both the security of QPC protocol [57], [60] and the qubit efficiency [52], [61], [62] to correctly work under noise [63], [64].

QPC protocols can be used for novel and exciting applications, including voting [80], bidding [81], and auctions [82] to meet the requirements of the rapid development of next generation mobile networks (5G) [83], [84]. Next generation mobile networks require substantive flexibility and reliability to scale up the capacity of enormous data transmission. The primary reasons for achieving this scaling are to improve the provided services to the connected users, reduction of end-to-end service discontinuation and decreasing the cost of maintenance. Therefore, the service provider (SP) has to improve resource utilization and obtain extra income simultaneously. This can achieve by implementing various auction approaches to allow SP to determine the set of their aspired resources and comparable bid amounts without distinguishing the prices of other buyers. The private comparison protocol is employed since the whole process of bidding and auction require that the submitted preferences and information be private and the SP to determine the winner without knowing the bidding details of other buyers [85].

The first multiparty quantum private comparison (MQPC) protocol allows n parties to compare whether the secret inputs of any two parties are identical or not has been investigated in [65]. Hereafter, several MQPC protocols have been proposed in [55], [58], and [66]–[71]. Recently, Liu and Wang [72] introduced an interesting dynamic MQPC protocol based on single photon in both polarization and spatial-mode-degrees of freedom (PSMDF), where two parties of $n(n \geq 4)$ parties can conclude the comparison result of their private inputs with the assistance of others $n-2$ parties and a semi-honest party. They claimed that dishonest parties could not recover any information about the others' private information. However, we have determined the incorrectness of this claim since a dishonest party can collude with another one to eavesdrop on the private information of an honest party, without being detected. Therefore, this paper proposes an enhanced secure version of the Liu-Wang protocol to prevent the attacker to gain any information about the transmitted messages.

This article is organized as follows. In Section II, a review of Liu-Wang protocol is introduced. In Section III, the cryptanalysis of Liu-Wang protocol is presented. In Section IV, the suggested improvement in Liu-Wang protocol is discussed. Finally, Section V concludes the paper.

II. REVIW OF THE LIU-WANG PROTOCOL [72]

Liu and Wang proposed a MQPC protocol for comparing the private information of $n(n \geq 4)$ parties with a semi-honest party by using a single photon state ($|\phi\rangle = |\phi\rangle_P \otimes |\phi\rangle_S$) in both PSMDF. The TP in the Liu-wang protocol performs the processes of the protocol loyally, registers all the results of computations, and might try to eavesdrop on the parties' private secrets but not allowed to conspire with other parties. Here $|\phi\rangle_P$ is the single-photon state in polarization and $|\phi\rangle_S$ is the spatial-mode degrees of freedom.

$$|\phi\rangle_P \in |H\rangle\,, |V\rangle\,, |S\rangle_P = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle),$$
$$|A\rangle_P = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)\}, \quad (1)$$

where H and V represent horizontal-polarization and vertical-polarization of the single photons, respectively. $|S\rangle_P$ and $|A\rangle_P$ are the polarization of the states S and A, respectively. Also,

$$|\phi\rangle_S \in |a_1\rangle\,, |a_2\rangle\,, |s\rangle_S = \frac{1}{\sqrt{2}}(|a_1\rangle + |a_2\rangle),$$
$$|a\rangle_S = \frac{1}{\sqrt{2}}(|a_1\rangle - |a_2\rangle)\}, \quad (2)$$

where a_1 and a_2 denote the upper spatial-mode and the lower-spatial mode of single particles, respectively. $|s\rangle_S$ and $|a\rangle_S$ are the spatial-mode degrees of freedom of the states s and a, respectively.

By assuming that the two unitary operations for each degree of freedom of single photons are the same in [20] and [21],

$$I_P = |H\rangle\langle H| + |V\rangle\langle V|\,, U_P = |V\rangle\langle H| - |H\rangle\langle V|\,,$$
$$I_S = |a_1\rangle\langle a_1| + |a_2\rangle\langle a_2|\,, U_S = |a_2\rangle\langle a_1| - |a_1\rangle\langle a_2|\,. \quad (3)$$

Using the above four unitary operations, we can obtain:

$$I_P|H\rangle = |H\rangle\,, I_P|V\rangle = |V\rangle\,,$$
$$I_P|S\rangle_P = |S\rangle_P\,, I_P|A\rangle_P = |A\rangle_P\,,$$
$$I_S|a_1\rangle = |a_1\rangle\,, I_S|a_2\rangle = |a_2\rangle\,,$$
$$I_S|S\rangle_S = |S\rangle_S\,, I_S|a\rangle_s = |a\rangle_s\,,$$

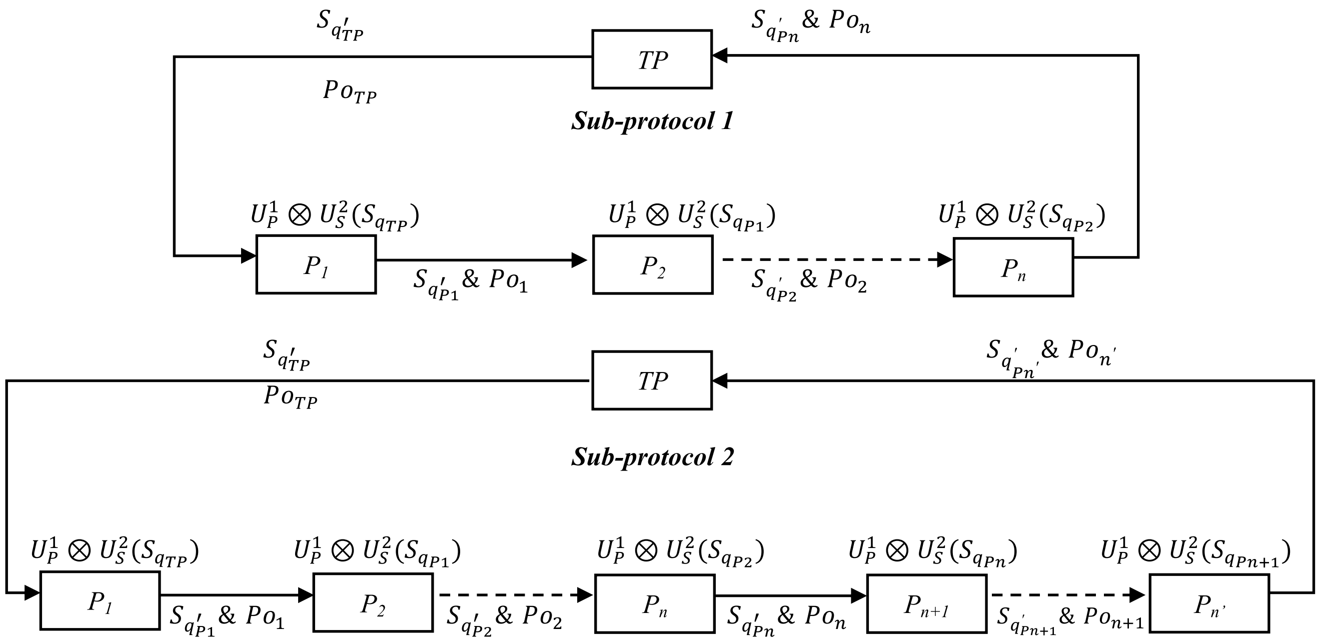

FIGURE 1. A graphical representation of the Liu-Wang protocol [72].

$$\begin{aligned} &U_P\,|H\rangle = |V\rangle\,, U_P\,|V\rangle = -\,|H\rangle\,,\\ &U_P\,|S\rangle_P = |A\rangle_P\,, U_P\,|A\rangle_P = |S\rangle_P\,,\\ &U_S\,|a_1\rangle = |a_2\rangle\,, U_S\,|a_2\rangle = -\,|a_1\rangle\,,\\ &U_S\,|S\rangle_S = -\,|a\rangle_S\,, U_S\,|a\rangle_S = |S\rangle_S\,. \end{aligned} \tag{4}$$

Now, assume that there are n parties ($n \geq 4$), $P_1, P_2, \cdots, P_n$, each party has private information M_i ($i = 1, 2, \cdots, n$) with length L. The secret messages M_i of P_i in F_{2^L} is represented by $m_1^i, m_2^i, \cdots, m_L^i$. In the Liu-Wang protocol, any two parties of n parties can compare their secrets with the assistance of other $n-2$ parties. Also, n' parties can dynamically join the protocol, before the quantum states are measured, for comparing their private information. All parties agree that I_P, I_S, $|H\rangle$, $|S\rangle_P$, $|a_1\rangle$ and $|S\rangle_S$ encode 0, and U_P, U_S, $|V\rangle$, $|A\rangle_P$, $|a_2\rangle$ and $|a\rangle_S$ encode 1, respectively. Liu-Wang protocol is divided into two sub-protocols. Firstly, sub-*protocol 1* describes how n parties get the comparison result of their secrets. Secondly, sub-*protocol 2* describes the mechanism for how n' parties can join dynamically in the private comparison protocol. Since the process of the two sub-protocols (see Fig. 1) is similar except for joining additional n' parties in the second sub-protocol, therefore, we review only the first sub-protocol as an illustrative example of the security limitation of Liu-Wang protocol as follows;

(1) $P_1(P_{2,\dots,}P_n)$ splits his binary representation of $M_1(M_2, \cdots, M_n)$ into $\lceil \frac{L}{2} \rceil$ groups $G_j^1(G_j^2, \cdots, G_j^n)$, i.e. $j = 1, 2, \dots, \lceil \frac{L}{2} \rceil$. Each group $G_j^1(G_j^2, \cdots, G_j^n)$ contains two binary bits of $M_1(M_2, \cdots, M_n)$.
If $L \bmod 2 = 1$, $P_1(P_{2,\dots,}P_n)$ adds one more "0" into the last group $G^1_{\lceil \frac{L}{2} \rceil}(G^2_{\lceil \frac{L}{2} \rceil}, \cdots, G^n_{\lceil \frac{L}{2} \rceil})$.

(2) TP generates a sequence S_{qTP} of $\lceil \frac{L}{2} \rceil$ single photons and generates L' single photons. Each photon is randomly determined from one of the eight quantum states $|\phi\rangle = |\phi\rangle_P + |\phi\rangle_S$ or $|\psi\rangle = |\psi\rangle_P + |\psi\rangle_S$, where $|\phi\rangle_P \in \{|H\rangle, |V\rangle\}$, $|\phi\rangle_S \in \{|a_1\rangle, |a_2\rangle\}$ and $|\psi\rangle_P \in \{|S\rangle_P, |A\rangle_P\}$, $|\psi\rangle_S \in \{|s\rangle_S, |a\rangle_S\}$. TP then stores the coding of sequence S_{qTP} and denotes the coding sequence by $Iv_1^1 Iv_1^2, \cdots, Iv^1_{\lceil \frac{L}{2} \rceil} Iv^2_{\lceil \frac{L}{2} \rceil}$. Afterward, TP inserts L' into S_{qTP} at random positions (Po_{TP}) and retrieves $S_{q'_{TP}}$. Finally, TP sends $S_{q'_{TP}}$ and Po_{TP} to P_1.

(3) Upon receiving $S_{q'_{TP}}$ and Po_{TP}, P_1 selects L' single photons and measures them with one of the eight bases $\{|H\rangle \otimes |a_1\rangle, |H\rangle \otimes |a_2\rangle, |V\rangle \otimes |a_1\rangle, |V\rangle \otimes |a_2\rangle, |S\rangle_P \otimes |s\rangle_S, |S\rangle_P \otimes |a\rangle_S, |A\rangle_P \otimes |s\rangle_S, |A\rangle_P \otimes |a\rangle_S\}$. According to the measurements of L' and its initial states, P_1 and TP can compute the error rate. If the error rate is higher than a specified threshold, P_1 terminates the protocol and starts again from step (1). Otherwise, P_1 continues to the next step.

(4) P_1 discards L' from $S_{q'_{TP}}$ and obtains S_{qTP}. As per his private information, P_1 applies G_j^1, $U_P^1 \otimes U_S^2$ ($U_P^1 \in \{I_P, U_P\}$, $U_S^2 \in \{I_S, U_S\}$) on the *jth* photon of sequence S_{qTP} generating a new sequence S_{qP_1} that is consistent with step (2), P_1 generates L' single photons and inserts them into S_{qP_1} producing $S_{q'_{P_1}}$. P_1 transmits $S_{q'_{P_1}}$ and the positions (Po_1) of L' to P_1.

(5) After $P_2(P_3, \cdots, P_n)$ receives $S_{q'_{P_1}}(S_{q'_{P2}}, \cdots, S_{q'_{Pn-1}})$, $P_2(P_3, \cdots, P_n)$ selects L' single photons and measures them with one of the eight bases $\{|H\rangle \otimes |a_1\rangle, |H\rangle \otimes |a_2\rangle, |V\rangle \otimes |a_1\rangle, |V\rangle \otimes |a_2\rangle, |S\rangle_P \otimes |s\rangle_S, |S\rangle_P \otimes |a\rangle_S, |A\rangle_P \otimes |s\rangle_S, |A\rangle_P \otimes |a\rangle_S\}$. According to the measurements of L' and its initial states, $P_2(P_3, \cdots, P_n)$ and *TP* can compute the error rate. If the error rate is higher than a specified threshold, P_1 terminates the protocol

TABLE 1. An example of Liu-Wang's protocol.

initial state	G_1^1	G_1^2	G_1^3	G_1^4	evolved state	$r_1^1 r_1^2$	$R_1^{1,2}$	$R_1^{1,3}$	$R_1^{2,3}$	$R_1^{1,4}$	$R_1^{2,4}$	$R_1^{3,4}$
$\|V\rangle\|a_2\rangle$	10	00	01	00	$\|H\rangle\|a_1\rangle$	00	10	11	01	10	00	01

and restarts from step (1). Otherwise, $P_2(P_3, \cdots, P_n)$ proceeds to the next step.

(6) $P_2(P_3, \cdots, P_n)$ discards L' from $S_{q'_{P_1}}(S_{q'_{P2}}, \cdots, S_{q'_{P_{n-1}}})$, and acquires $S_{qP_1}(S_{qP_2,\cdots}, S_{qP_{n-1}})$. $P_2(P_3, \cdots, P_n)$ applies, according to his private information $G_j^1(G_j^2, \cdots, G_j^n)$, $U_P^1 \otimes U_S^2$ ($U_P^1 \in \{I_P, U_P\}$, $U_S^2 \in \{I_S, U_S\}$) on the jth photon of sequence $S_{qP_1}(S_{qP_2,\cdots}, S_{qP_{n-1}})$ generating a new sequence $S_{qP_2}(S_{qP_3,\cdots}, S_{qP_n})$ that is consistent with step (2), P_n generates L' single photons and inserts them into S_{qP_n} producing $S_{q'_{P_n}}$. P_n transmits $S_{q'_{P_n}}$ and the positions (Po_n) of L' to TP.

(7) Upon receiving $S_{q'_{P_n}}$ and Po_n, TP and P_n use the same process as step (2) to determine whether the quantum channel is attacked or not. If so, they terminate the protocol and begin from step (1). Otherwise, TP measures S_{qP_n} using the correct bases and obtains the result R. The binary representation of R is $r_1^1 r_1^2 \cdots r^1_{\lceil \frac{L}{2} \rceil} r^2_{\lceil \frac{L}{2} \rceil}$.

(8) With the assistance of the TP and others $n-2$ parties, any P_k can respectively compare his secret information with P_h, here $k \in \{1, 2, \ldots, n\}$ and $h = 1, 2, \ldots, k-1, k+1, 1, \ldots, n$. For$k = 1, 2, \ldots, n$, and for $h = 1, 2, \ldots, k-1, k+1, 1, \ldots, n$: TP transfers the result R to $P_j (j \in \{1, 2, \ldots, n, \}, j \neq k, h)$. Subsequently, $n-2$ parties compute;

$$r^{1'}_{1(kh)} r^{2'}_{1(kh)} = r_1^1 r_1^2 \oplus G_1^j, \\ \cdots \\ r^{1'}_{\lceil \frac{L}{2} \rceil (kh)} r^{2'}_{\lceil \frac{L}{2} \rceil (kh)} = r^1_{\lceil \frac{L}{2} \rceil} r^2_{\lceil \frac{L}{2} \rceil} \oplus G^j_{\lceil \frac{L}{2} \rceil}. \tag{5}$$

Thenceforth, they transfer

$$r^{1'}_{1(kh)} r^{2'}_{1(kh)}, \cdots, r^{1'}_{\lceil \frac{L}{2} \rceil (kh)} r^{2'}_{\lceil \frac{L}{2} \rceil (kh)} \text{ to } TP.$$

Finally, TP computes

$$R^1_{kh} = r^{1'}_{1(kh)} r^{2'}_{1(kh)} \oplus Iv_1^{1'} Iv_1^{2'} \\ \cdots \\ R_{kh}^{\lceil \frac{L}{2} \rceil} = r^{1'}_{\lceil \frac{L}{2} \rceil (kh)} r^{2'}_{\lceil \frac{L}{2} \rceil (kh)} \oplus Iv^{1'}_{\lceil \frac{L}{2} \rceil} Iv^{2'}_{\lceil \frac{L}{2} \rceil} \tag{6}$$

For $k = 1, 2, \ldots, n$, and for $h = 1, 2, \ldots, k-1, k+1, 1, \ldots, n$: $R^1_{kh} =, \cdots, = R_{kh}^{\lceil \frac{L}{2} \rceil} = 00$, hence the private information $M_h = M_k$. Otherwise, $M_h \neq M_k$.

For example, assume there are four parties (e.g. P_1, P_2, P_3 and P_4). Each party has a private information M_i (e.g. $M_1 = \{1, 0\}, M_2 = \{0, 0\}, M_3 = \{0, 1\}, M_4 = \{0, 0\}$) and they want to compare its equality. Also, each party splits his binary representation into $\lceil \frac{L}{2} \rceil$ groups. Now, each party has only one group contains two classical bits (i.e. $G_1^1 = \{10\}, G_1^2 = \{00\}, G_1^3 = \{01\}, G_1^4 = \{00\}$).

All the parties and the TP agree that $I_P, I_S, |H\rangle, |S\rangle_P, |a_1\rangle$ and $|S\rangle_S$ encode 0, $U_P, U_S, |V\rangle, |A\rangle_P, |a_2\rangle$ and $|a\rangle_S$ encode 1. As indicating in Table 1, assume that the initial state of the TP is $|V\rangle|a_2\rangle$, and encodes 11. All parties apply the unitary operations, corresponding to their private information, to the initial state and obtain a new state; $(G_1^1 \oplus G_1^2 \oplus G_1^3 \oplus G_1^4)(|V\rangle|a_2\rangle) = U_P \otimes U_S(|V\rangle|a_2\rangle)$, $(10 \oplus 00 \oplus 01 \oplus 00)(|V\rangle|a_2\rangle) = 11(|V\rangle|a_2\rangle)$. So, we have $U_P \otimes U_S(|V\rangle|a_2\rangle) = |H\rangle|a_1\rangle$ where $U_P \otimes U_S$ encodes 11. Hence, the evolved state (i.e. $|H\rangle|a_1\rangle$) is encoded by $r_1^1 r_1^2 = 00$.

The comparison result of the private information (G_1^1 and G_1^2) of the wo parties P_1 and P_2 is denoted by $R_1^{1,2}$, where $R_1^{1,2} = r_1^1 r_1^2 \oplus G_1^3 \oplus G_1^4 \oplus 11$; here 11 encodes the initial state ($|V\rangle|a_2\rangle$). In our example, $R_1^{1,2} = 00 \oplus 01 \oplus 00 \oplus 11 = 10$, which means that G_1^1 and G_1^2 are not equal. The comparison result of the private information (G_1^1 and G_1^3) of the wo parties P_1 and P_3 is denoted by $R_1^{1,3}$, where $R_1^{1,3} = r_1^1 r_1^3 \oplus G_1^2 \oplus G_1^4 \oplus 11$; so we get $R_1^{1,3} = 00 \oplus 00 \oplus 00 \oplus 11 = 11$. Following the same computations, we get $R_1^{2,3} = 01$, $R_1^{1,4} = 10$, $R_1^{2,4} = 00$ and $R_1^{3,4} = 01$.

III. INSECRITY OF LIU-WANG'S PROTOCOL

Liu and Wang [72] showed that their protocol is secured against several types of external attacks (e.g. the intercept-resend attack and the entangle-measure attack) when performing eavesdropper checking process (or the decoy photon technique [73]) in steps (3), (5) and (7). Also, Liu and Wang showed that their protocol is safe against two cases of the participant attack: Firstly, a dishonest party tries to learn the private information of an honest party; Secondly, assume that the TP tries to discover the private information of every participant. Furthermore, participant's collusion attack is an illegal collaboration of two or more dishonest parties to cheat the private information of one or more parties. Indeed, collusion attack is one of the most powerful attacks which represents a real vulnerability to secure multiparty computation and should get more interest [74]–[77].

In this study, a new type of collusion attack can be performed on Liu-Wang's protocol by two dishonest parties to steal the private information of an honest party (see Fig. 2). Similar strategies of collusion attack have been investigated and addressed in [33], [34], and [77]–[79]. In Liu-Wang's protocol, the S_{qTP} sequence prepared by TP is transmitted among n parties $(P_1, P_2, \ldots, P_n)$. P_1 encodes his private information $G_1^1, G_2^1, \cdots, G^1_{\lceil \frac{L}{2} \rceil}$ to the sequence S_{qTP} by applying unitary operations $U_P^1 \otimes U_S^2$.

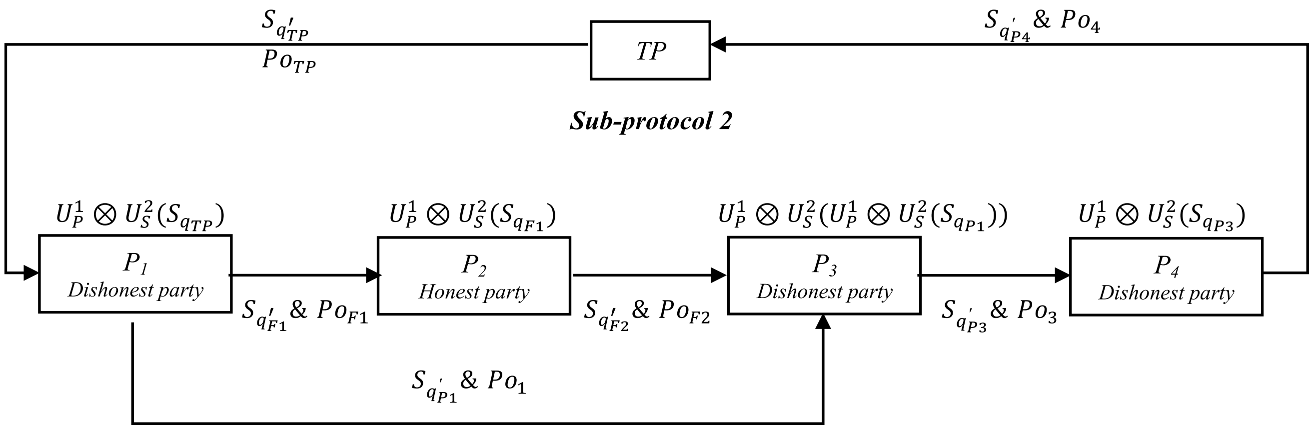

FIGURE 2. A graphical representation of the suggested collusion attack strategy on Liu-Wang's protocol for $n = 4$.

TABLE 2. Recovering the private information of P_2 by the two dishonest parties P_1 and P_3.

TP	P_1				P_2			P_1 and P_3
$\|\varphi_0\rangle$ the initial state	G_1^1	$U_P^1 \otimes U_S^2$	$U_P^1 \otimes U_S^2\|\varphi_0\rangle = \|\varphi_{P_1}\rangle$	$\|\varphi_{F_1}\rangle$ P_1's fake state	G_1^2	$U_P^1 \otimes U_S^2$	$U_P^1 \otimes U_S^2\|\varphi_{F_1}\rangle = \|\varphi_{P_2}\rangle$	Recovering G_1^2 by comparing $\|\varphi_{F_1}\rangle$ with $\|\varphi_{P_2}\rangle$
	00	$I_P \otimes I_S$	$\|H\rangle\|a_2\rangle$	$\|V\rangle\|a_2\rangle$	00	$I_P \otimes I_S$	$\|V\rangle\|a_2\rangle$	00
	01	$I_P \otimes U_S$	$-\|H\rangle\|a_1\rangle$		01	$I_P \otimes U_S$	$-\|V\rangle\|a_1\rangle$	01
	10	$U_P \otimes I_S$	$\|V\rangle\|a_2\rangle$		10	$U_P \otimes I_S$	$-\|H\rangle\|a_2\rangle$	10
	11	$U_P \otimes U_S$	$-\|V\rangle\|a_1\rangle$		11	$U_P \otimes U_S$	$\|H\rangle\|a_1\rangle$	11

Additionally, for checking the security of the quantum channel between P_1 and P_2, P_1 inserts L' single photons into $S_{q_{TP}}$. After that, P_1 transmits the new generated sequence to P_2. Moreover, $P_2, P_3, \cdots, P_n$ applies the same process as P_1 until TP receives the operated sequence from P_n. Therefore, every quantum channel is checked by the two parties themselves, and TP checks the $TP - P_1$ quantum channel and $TP - P_n$ quantum channel. The insecurity of Liu-Wang's protocol derived from that a collusion attack may be executed by two dishonest parties P_i and P_{i+2} for eavesdropping the private information of P_{i+1} (for $i = 1, 2, \cdots, n-2$) without being detected. In this situation, we consider two cases to represent the honesty of P_{i+1}.

Case 1 (P_{i+1} Is an Honest Party): By assuming that there are four parties P_1, P_2, P_3, P_4 and the two dishonest parties P_1 and P_3 may collaborate to eavesdrop on P_2's secret. The attack strategy of P_1 and P_3 is as follows (see also Table 2). Initially, P_1 prepares a fake sequence S_{q_F} of $\lceil \frac{L}{2} \rceil$ single photons and generates L' where each photon produced randomly in one of the eight quantum states indicated in step (2). Also, P_1 transmits the initial state information to P_3. According to step (3), after TP and P_1 confirm that the transmission of $S_{q_{TP}}$ is secure, P_1 holds $S_{q_{TP}}$ and inserts L' single photons into S_{q_F} producing $S_{q'_F}$. P_1 sends $S_{q'_F}$ to P_2 instead of the original sequence (later P_1 applies his unitary operation on the original $S_{q_{TP}}$ sequence). Upon receiving $S_{q'_F}$, P_1 and P_2 check the security of the quantum channel using L'. Besides, P_2 discards the measured L' single photons to retrieve S_{q_F}. After verifying the security of transmission, P_2 applies his unitary operations $U_P^1 \otimes U_S^2$ on the jth photon of S_{q_F} sequence according to G_j^2 producing $S_{q_{FP_2}}$. Actually, P_2 honestly performs his process because he ignores that he has received a fake sequence. Afterward, P_2 prepares L' single photons and inserts them into $S_{q_{FP_2}}$, producing $S_{q'_{FP_2}}$, and sends $S_{q'_{FP_2}}$ to P_3.

Upon receiving $S_{q'_{FP_2}}$, P_2 and P_3 check the security of the transmission using the L' single photons. If the transmission of $S_{q'_{FP_2}}$ is secure; P_3 discards the measured L' single photons to retrieve $S_{q_{FP_2}}$. Subsequently, P_3 starts to measure $S_{q_{FP_2}}$ with the correct initial state information which was sent by P_1 and obtains the result denoted by MR_{FP_2}. Therefore, P_1 and P_3 can easily get P_2's unitary operation (i.e. G_j^2) since they know MR_{FP_2} and the initial state information of $S_{q_{FP_2}}$. To continue the protocol without being detected, P_3 applies the recovered unitary operation of P_2 and his unitary operation on P_1's state producing a new state and sends the evolved states to next party. For example, as shown in Table 3 (a), (b), (c), or (d), P_1 sends $|H\rangle|a_2\rangle$, $-|H\rangle|a_1\rangle$, $|V\rangle|a_2\rangle$, or $-|V\rangle|a_1\rangle$ to P_3, respectively. Then, P_3 applies the recovered unitary operation of P_2 and his unitary operation on $|\varphi_{P1}\rangle$ producing $|\varphi_{P_3}\rangle$ and sends the evolved state to P_4.

Case 2 (P_{i+1} and P_{i+3} Are Dishonest Parties): In this case, the dishonest party P_{i+1} can utilize the same suggested attack strategy and collude with P_{i+3} for eavesdropping the private information of P_{i+2}. Therefore, P_{i+1} prepares a fake sequence $S_{q_{FP_{i+1}}}$ of $\lceil \frac{L}{2} \rceil$ single photons. Next, P_{i+1} transmits the fake sequence $S_{q_{FP_{i+1}}}$ and corresponding initial information to P_{i+3}. Hence, Liu-Wang's protocol is secured against our suggested attack strategy, since P_i, P_{i+2}, and all other

TABLE 3. Sections (A), (B), (C), and (D) show all the possible evolved states when P_1 sends $|H\rangle|a_2\rangle$, $-|H\rangle|a_1\rangle$, $|V\rangle|a_2\rangle$, and $-|V\rangle|a_1\rangle$ to P_3, respectively.

(A)

P_1 sends $\|\varphi_{P_1}\rangle$ to P_3	G_1^2	$U_P^1 \otimes U_S^2$	G_1^3	$U_P^1 \otimes U_S^2$	P_3		
					$G_1^2 \oplus G_1^3$	$U_P^1 \otimes U_S^2$	$U_P^1 \otimes U_S^2\|\varphi_{P1}\rangle = \|\varphi_{P_3}\rangle$
$\|H\rangle\|a_2\rangle$	00	$I_P \otimes I_S$	00	$I_P \otimes I_S$	00	$I_P \otimes I_S$	$\|H\rangle\|a_2\rangle$
	00	$I_P \otimes I_S$	01	$I_P \otimes U_S$	01	$I_P \otimes U_S$	$-\|H\rangle\|a_1\rangle$
	00	$I_P \otimes I_S$	10	$U_P \otimes I_S$	10	$U_P \otimes I_S$	$\|V\rangle\|a_2\rangle$
	00	$I_P \otimes I_S$	11	$U_P \otimes U_S$	11	$U_P \otimes U_S$	$-\|V\rangle\|a_1\rangle$
	01	$I_P \otimes U_S$	00	$I_P \otimes I_S$	01	$I_P \otimes U_S$	$-\|H\rangle\|a_1\rangle$
	01	$I_P \otimes U_S$	01	$I_P \otimes U_S$	00	$I_P \otimes I_S$	$\|H\rangle\|a_2\rangle$
	01	$I_P \otimes U_S$	10	$U_P \otimes I_S$	11	$U_P \otimes U_S$	$-\|V\rangle\|a_1\rangle$
	01	$I_P \otimes U_S$	11	$U_P \otimes U_S$	10	$U_P \otimes I_S$	$\|V\rangle\|a_2\rangle$
	10	$U_P \otimes I_S$	00	$I_P \otimes I_S$	10	$U_P \otimes I_S$	$\|V\rangle\|a_2\rangle$
	10	$U_P \otimes I_S$	01	$I_P \otimes U_S$	11	$U_P \otimes U_S$	$-\|V\rangle\|a_1\rangle$
	10	$U_P \otimes I_S$	10	$U_P \otimes I_S$	00	$I_P \otimes I_S$	$\|H\rangle\|a_2\rangle$
	10	$U_P \otimes I_S$	11	$U_P \otimes U_S$	01	$I_P \otimes U_S$	$-\|H\rangle\|a_1\rangle$
	11	$U_P \otimes U_S$	00	$I_P \otimes I_S$	11	$U_P \otimes U_S$	$-\|V\rangle\|a_1\rangle$
	11	$U_P \otimes U_S$	01	$I_P \otimes U_S$	10	$U_P \otimes I_S$	$\|V\rangle\|a_2\rangle$
	11	$U_P \otimes U_S$	10	$U_P \otimes I_S$	01	$I_P \otimes U_S$	$-\|H\rangle\|a_1\rangle$
	11	$U_P \otimes U_S$	11	$U_P \otimes U_S$	00	$I_P \otimes I_S$	$\|H\rangle\|a_2\rangle$

(B)

P_1 sends $\|\varphi_{P_1}\rangle$ to P_3	G_1^2	$U_P^1 \otimes U_S^2$	G_1^3	$U_P^1 \otimes U_S^2$	P_3		
					$G_1^2 \oplus G_1^3$	$U_P^1 \otimes U_S^2$	$U_P^1 \otimes U_S^2\|\varphi_{P1}\rangle = \|\varphi_{P_3}\rangle$
$-\|H\rangle\|a_1\rangle$	00	$I_P \otimes I_S$	00	$I_P \otimes I_S$	00	$I_P \otimes I_S$	$-\|H\rangle\|a_1\rangle$
	00	$I_P \otimes I_S$	01	$I_P \otimes U_S$	01	$I_P \otimes U_S$	$-\|H\rangle\|a_2\rangle$
	00	$I_P \otimes I_S$	10	$U_P \otimes I_S$	10	$U_P \otimes I_S$	$-\|V\rangle\|a_1\rangle$
	00	$I_P \otimes I_S$	11	$U_P \otimes U_S$	11	$U_P \otimes U_S$	$-\|V\rangle\|a_2\rangle$
	01	$I_P \otimes U_S$	00	$I_P \otimes I_S$	01	$I_P \otimes U_S$	$-\|H\rangle\|a_2\rangle$
	01	$I_P \otimes U_S$	01	$I_P \otimes U_S$	00	$I_P \otimes I_S$	$-\|H\rangle\|a_1\rangle$
	01	$I_P \otimes U_S$	10	$U_P \otimes I_S$	11	$U_P \otimes U_S$	$-\|V\rangle\|a_2\rangle$
	01	$I_P \otimes U_S$	11	$U_P \otimes U_S$	10	$U_P \otimes I_S$	$-\|V\rangle\|a_1\rangle$
	10	$U_P \otimes I_S$	00	$I_P \otimes I_S$	10	$U_P \otimes I_S$	$-\|V\rangle\|a_1\rangle$
	10	$U_P \otimes I_S$	01	$I_P \otimes U_S$	11	$U_P \otimes U_S$	$-\|V\rangle\|a_2\rangle$
	10	$U_P \otimes I_S$	10	$U_P \otimes I_S$	00	$I_P \otimes I_S$	$-\|H\rangle\|a_1\rangle$
	10	$U_P \otimes I_S$	11	$U_P \otimes U_S$	01	$I_P \otimes U_S$	$-\|H\rangle\|a_2\rangle$
	11	$U_P \otimes U_S$	00	$I_P \otimes I_S$	11	$U_P \otimes U_S$	$-\|V\rangle\|a_2\rangle$
	11	$U_P \otimes U_S$	01	$I_P \otimes U_S$	10	$U_P \otimes I_S$	$-\|V\rangle\|a_1\rangle$
	11	$U_P \otimes U_S$	10	$U_P \otimes I_S$	01	$I_P \otimes U_S$	$-\|H\rangle\|a_2\rangle$
	11	$U_P \otimes U_S$	11	$U_P \otimes U_S$	00	$I_P \otimes I_S$	$-\|H\rangle\|a_1\rangle$

(C)

P_1 sends $\|\varphi_{P_1}\rangle$ to P_3	G_1^2	$U_P^1 \otimes U_S^2$	G_1^3	$U_P^1 \otimes U_S^2$	P_3		
					$G_1^2 \oplus G_1^3$	$U_P^1 \otimes U_S^2$	$U_P^1 \otimes U_S^2\|\varphi_{P1}\rangle = \|\varphi_{P_3}\rangle$
$\|V\rangle\|a_2\rangle$	00	$I_P \otimes I_S$	00	$I_P \otimes I_S$	00	$I_P \otimes I_S$	$\|V\rangle\|a_2\rangle$
	00	$I_P \otimes I_S$	01	$I_P \otimes U_S$	01	$I_P \otimes U_S$	$-\|V\rangle\|a_1\rangle$
	00	$I_P \otimes I_S$	10	$U_P \otimes I_S$	10	$U_P \otimes I_S$	$-\|H\rangle\|a_2\rangle$
	00	$I_P \otimes I_S$	11	$U_P \otimes U_S$	11	$U_P \otimes U_S$	$\|H\rangle\|a_1\rangle$
	01	$I_P \otimes U_S$	00	$I_P \otimes I_S$	01	$I_P \otimes U_S$	$-\|V\rangle\|a_1\rangle$
	01	$I_P \otimes U_S$	01	$I_P \otimes U_S$	00	$I_P \otimes I_S$	$\|V\rangle\|a_2\rangle$
	01	$I_P \otimes U_S$	10	$U_P \otimes I_S$	11	$U_P \otimes U_S$	$\|H\rangle\|a_1\rangle$
	01	$I_P \otimes U_S$	11	$U_P \otimes U_S$	10	$U_P \otimes I_S$	$-\|H\rangle\|a_2\rangle$
	10	$U_P \otimes I_S$	00	$I_P \otimes I_S$	10	$U_P \otimes I_S$	$-\|H\rangle\|a_2\rangle$
	10	$U_P \otimes I_S$	01	$I_P \otimes U_S$	11	$U_P \otimes U_S$	$\|H\rangle\|a_1\rangle$
	10	$U_P \otimes I_S$	10	$U_P \otimes I_S$	00	$I_P \otimes I_S$	$\|V\rangle\|a_2\rangle$
	10	$U_P \otimes I_S$	11	$U_P \otimes U_S$	01	$I_P \otimes U_S$	$-\|V\rangle\|a_1\rangle$
	11	$U_P \otimes U_S$	00	$I_P \otimes I_S$	11	$U_P \otimes U_S$	$\|H\rangle\|a_1\rangle$
	11	$U_P \otimes U_S$	01	$I_P \otimes U_S$	10	$U_P \otimes I_S$	$-\|H\rangle\|a_2\rangle$
	11	$U_P \otimes U_S$	10	$U_P \otimes I_S$	01	$I_P \otimes U_S$	$-\|V\rangle\|a_1\rangle$
	11	$U_P \otimes U_S$	11	$U_P \otimes U_S$	00	$I_P \otimes I_S$	$\|V\rangle\|a_2\rangle$

TABLE 3. ***(Continued.)*** **Sections (A), (B), (C), and (D) show all the possible evolved states when P_1 sends $|H\rangle|a_2\rangle$, $-|H\rangle|a_1\rangle$, $|V\rangle|a_2\rangle$, and $-|V\rangle|a_1\rangle$ to P_3, respectively.**

(D)

P_1 sends $\|\varphi_{P_1}\rangle$ to P_3	G_1^2	$U_P^1 \otimes U_S^2$	G_1^3	$U_P^1 \otimes U_S^2$	P_3		
					$G_1^2 \oplus G_1^3$	$U_P^1 \otimes U_S^2$	$U_P^1 \otimes U_S^2\|\varphi_{P1}\rangle = \|\varphi_{P_3}\rangle$
$-\|V\rangle\|a_1\rangle$	00	$I_P \otimes I_S$	00	$I_P \otimes I_S$	00	$I_P \otimes I_S$	$-\|V\rangle\|a_1\rangle$
	00	$I_P \otimes I_S$	01	$I_P \otimes U_S$	01	$I_P \otimes U_S$	$-\|V\rangle\|a_2\rangle$
	00	$I_P \otimes I_S$	10	$U_P \otimes I_S$	10	$U_P \otimes I_S$	$\|H\rangle\|a_1\rangle$
	00	$I_P \otimes I_S$	11	$U_P \otimes U_S$	11	$U_P \otimes U_S$	$\|H\rangle\|a_2\rangle$
	01	$I_P \otimes U_S$	00	$I_P \otimes I_S$	01	$I_P \otimes U_S$	$-\|V\rangle\|a_2\rangle$
	01	$I_P \otimes U_S$	01	$I_P \otimes U_S$	00	$I_P \otimes I_S$	$-\|V\rangle\|a_1\rangle$
	01	$I_P \otimes U_S$	10	$U_P \otimes I_S$	11	$U_P \otimes U_S$	$\|H\rangle\|a_2\rangle$
	01	$I_P \otimes U_S$	11	$U_P \otimes U_S$	10	$U_P \otimes I_S$	$\|H\rangle\|a_1\rangle$
	10	$U_P \otimes I_S$	00	$I_P \otimes I_S$	10	$U_P \otimes I_S$	$\|H\rangle\|a_1\rangle$
	10	$U_P \otimes I_S$	01	$I_P \otimes U_S$	11	$U_P \otimes U_S$	$\|H\rangle\|a_2\rangle$
	10	$U_P \otimes I_S$	10	$U_P \otimes I_S$	00	$I_P \otimes I_S$	$-\|V\rangle\|a_1\rangle$
	10	$U_P \otimes I_S$	11	$U_P \otimes U_S$	01	$I_P \otimes U_S$	$-\|V\rangle\|a_2\rangle$
	11	$U_P \otimes U_S$	00	$I_P \otimes I_S$	11	$U_P \otimes U_S$	$\|H\rangle\|a_2\rangle$
	11	$U_P \otimes U_S$	01	$I_P \otimes U_S$	10	$U_P \otimes I_S$	$\|H\rangle\|a_1\rangle$
	11	$U_P \otimes U_S$	10	$U_P \otimes I_S$	01	$I_P \otimes U_S$	$-\|V\rangle\|a_2\rangle$
	11	$U_P \otimes U_S$	11	$U_P \otimes U_S$	00	$I_P \otimes I_S$	$-\|V\rangle\|a_1\rangle$

dishonest parties try to recover the private information from fake sequences of photons.

IV. LIU-WANG PROTOCOL'S IMPROVEMENT

In Liu-Wang's protocol, the prepared sequence of $\lceil \frac{L}{2} \rceil$ single photons is transmitted from TP to P_1, and the security of transmission is guaranteed by L' single photons. P_1 encodes his private information into the received sequence by performing certain unitary operations. Also, P_1 inserts new L' single photons into the received sequence and sends the operating sequence to the next party. This process continues until P_n encodes his private information and sends them to the TP. In fact, the quantum channel between every two parties is independently checked by the two parties themselves. Consequently, this process may enable a dishonest party from colluding with another dishonest party for stealing the private information of an honest party. For solving this security issue, we suggest a simple modification as follows.

Using QKD protocol [1], TP shares secret keys $K_1, K_2, \cdots, K_n$ with $P_1, P_{2,\ldots,} P_n$, respectively; and the lengths of these secret keys are the same as the private information of parties (i.e. $|K_1| = |K_2| = \cdots = |K_n| = |M_1| = |M_2| = \cdots = |M_n| = L$). $P_1(P_{2,\cdots,} P_n)$ encodes his private information $M_1(M_2, \cdots, M_n)$ with the secret keys $K_1(K_2, \cdots, K_n)$ to retrieve the encrypted information $C_1(C_2, \cdots, C_n)$, i.e., $C_i = K_i \oplus M_i$ $(i = 1, 2, \cdots, n)$. The suggested modification is performed on both steps (1*) and (8*), and the other steps will remain the same.

(1*)$P_i(TP)$ splits his binary representation of $C_i(K_i)$ into $\lceil \frac{L}{2} \rceil$ groups $GC_j^i(GK^i)$, where $i = 1, 2, \cdots, n$ and $j = 1, 2, \cdots, \lceil \frac{L}{2} \rceil$. Each group $GC_j^i(GK^i)$ contains two binary bits of $C_i(K_i)$.

If L mod $2 = 1$, then $P_i(TP)$ inserts an extra "0" into the last group $GC^i_{\lceil \frac{L}{2} \rceil}(GK^i_{\lceil \frac{L}{2} \rceil})$.

(8*) With the assistance of TP and others $n-2$ parties, any P_k can respectively compare his secret with P_h, here $k \in \{1, 2, \ldots, n\}$ and $h = 1, 2, \ldots, k-1, k+1, 1, \ldots, n$. For $k = 1, 2, \ldots, n$, and for $h = 1, 2, \ldots, k-1, k+1, 1, \ldots, n$: TP transfers the result R to $P_j (j \in \{1, 2, \ldots, n, \}, j \neq k, h)$. Subsequently, $n-2$ parties compute;

$$
\begin{aligned}
&r^{1'}_{1(kh)} r^{2'}_{1(kh)} = r^1_1 r^2_1 \oplus \bigoplus_{j \in \{1,2,\ldots n\}, j \neq h,k} GC^j_1, \\
&\cdots \\
&r^{1'}_{\lceil \frac{L}{2} \rceil (kh)} r^{2'}_{\lceil \frac{L}{2} \rceil (kh)} = r^1_{\lceil \frac{L}{2} \rceil} r^2_{\lceil \frac{L}{2} \rceil} \oplus \bigoplus_{j \in \{1,2,\ldots n\}, j \neq h,k} GC^j_{\lceil \frac{L}{2} \rceil}
\end{aligned} \tag{7}
$$

Thenceforth, they transfer

$$
r^{1'}_{1(kh)} r^{2'}_{1(kh)}, \cdots, r^{1'}_{\lceil \frac{L}{2} \rceil (kh)} r^{2'}_{\lceil \frac{L}{2} \rceil (kh)} \text{ to } TP.
$$

Finally, TP computes

$$
\begin{aligned}
R^1_{kh} &= r^{1'}_{1(kh)} r^{2'}_{1(kh)} \oplus K^{1'}_{1(k)} K^{2'}_{1(k)} \oplus K^{1'}_{1(h)} K^{2'}_{1(h)} \oplus Iv^{1'}_1 Iv^{2'}_1 \\
&\cdots \\
R^{\lceil \frac{L}{2} \rceil}_{kh} &= r^{1'}_{\lceil \frac{L}{2} \rceil (kh)} r^{2'}_{\lceil \frac{L}{2} \rceil (kh)} \oplus K^{1'}_{\lceil \frac{L}{2} \rceil (k)} K^{2'}_{\lceil \frac{L}{2} \rceil (k)} \\
&\quad \oplus K^{1'}_{\lceil \frac{L}{2} \rceil (h)} K^{2'}_{\lceil \frac{L}{2} \rceil (h)} \oplus Iv^{1'}_{\lceil \frac{L}{2} \rceil} Iv^{2'}_{\lceil \frac{L}{2} \rceil}
\end{aligned} \tag{8}
$$

For $k = 1, 2, \ldots, n$, and for $h = 1, 2, \ldots, k-1, k+1, 1, \ldots, n$: $R^1_{kh} =, \cdots, = R^{\lceil \frac{L}{2} \rceil}_{kh} = 00$, hence the private information $M_h = M_k$. Otherwise, $M_h \neq M_k$.

So, if the dishonest parties (P_i and P_{i+2}) attempt to apply the suggested attack strategy, they obtain an encrypted information of P_{i+1}, i.e. $C_{i+1} = K_{i+1} \oplus M_{i+1}$. Therefore, the dishonest parties P_i and P_{i+2} cannot retrieve any private information of P_{i+1} (for $i = 1, 2, \cdots, n-2$).

V. CONCLUSIONS

In this paper, we have investigated the security limitations of Liu and Wang quantum private comparison protocol. We have developed an improvement of Liu and Wang protocol to prevent dishonest parties from eavesdropping the private information of honest parties. Our proposed modifications show that the dishonest parties cannot retrieve any private information about the transmitted message when applying a collusion attack. This opens a new area for developing potential future secure multiparty computation applications and to improve the provided services and resource utilization of next generation mobile networks to the connected users.

REFERENCES

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theor. Comput. Sci.*, vol. 560, pp. 7–11, 2014.

[2] H.-K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," *Science*, vol. 283, no. 5410, pp. 2050–2056, Mar. 1999.

[3] D. Mayers, "Unconditional security in quantum cryptography," *J. ACM*, vol. 48, no. 3, pp. 351–406, May 2001.

[4] H. Inamori, N. Lütkenhaus, and D. Mayers, "Unconditional security of practical quantum key distribution," *Eur. Phys. J. D*, vol. 41, p. 599, Mar. 2007.

[5] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, pp. 661–663, Aug. 1991.

[6] F.-G. Deng and G.-L. Long, "Controlled order rearrangement encryption for quantum key distribution," *Phys. Rev. A, Gen. Phys.*, vol. 68, no. 4, p. 042315, 2003.

[7] K. Wen and G. L. Long, "Modified Bennett-Brassard 1984 quantum key distribution protocol with two-way classical communications," *Phys. Rev. A, Gen. Phys.*, vol. 72, no. 2, p. 022336, 2005.

[8] 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.

[9] F.-Z. Guo, F. Gao, Q.-Y. Wen, and F.-C. Zhu, "A two-step channel-encrypting quantum key distribution protocol," *Int. J. Quantum Inf.*, vol. 8, no. 6, pp. 1013–1022, 2010.

[10] C.-W. Yang, "New probabilistic quantum key distribution protocol," *Int. J. Theor. Phys.*, vol. 57, no. 12, pp. 3651–3657, 2018.

[11] F. Xu *et al.*, "Field experiment on a robust hierarchical metropolitan quantum cryptography network," *Chin. Sci. Bull.*, vol. 54, no. 17, pp. 2991–2997, 2009.

[12] M. Sasaki *et al.*, " Field test of quantum key distribution in the Tokyo QKD network," *Opt. Express*, vol. 19, no. 11, pp. 10387–10409, 2011.

[13] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, "Experimental demonstration of long-distance continuous-variable quantum key distribution," *Nature Photon.*, vol. 7, pp. 378–381, Apr. 2013.

[14] S. Wang *et al.*, "Field and long-term demonstration of a wide area quantum key distribution network," *Opt. Express*, vol. 22, no. 18, pp. 21739–21756, 2014.

[15] J. Yin *et al.*, "Satellite-based entanglement distribution over 1200 kilometers," *Science*, vol. 356, no. 6343, pp. 1140–1144, 2017.

[16] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, "Experimental quantum teleportation," *Nature*, vol. 390, pp. 575–579, Dec. 1997.

[17] X.-L. Wang *et al.*, "Quantum teleportation of multiple degrees of freedom of a single photon," *Nature*, vol. 518, pp. 516–519, Feb. 2015.

[18] M. Li, N. Zhao, N. Chen, C.-H. Zhu, and C.-X. Pei, "Quantum teleportation of five-qubit state," *Int. J. Theor. Phys.*, vol. 56, no. 9, pp. 2710–2715, 2017.

[19] F.-G. Deng and G. L. Long, "Secure direct communication with a quantum one-time pad," *Phys. Rev. A, Gen. Phys.*, vol. 69, p. 052319, May 2004.

[20] A. Farouk *et al.*, "Multi-parties quantum secure direct communication with authentication," in *Quantum Computing: An Environment for Intelligent Large Scale Real Application*. Cham, Switzerland: Springer, 2018, pp. 143–184.

[21] A. Farouk, M. Zakaria, A. Megahed, and F. A. Omara, "A generalized architecture of quantum secure direct communication for N disjointed users with authentication," *Sci. Rep.*, vol. 5, Nov. 2015, Art. no. 16080.

[22] W. Li, J. Chen, X. Wang, and C. Li, "Quantum secure direct communication achieved by using multi-entanglement," *Int. J. Theor. Phys.*, vol. 54, no. 1, pp. 100–105, 2015.

[23] D. Song, C. Long, W. Wan, J. Zhao, and S. Wang, "A quantum secure direct communication protocol based on six-qubit cluster state," in *Proc. 20th Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2018, pp. 1–2.

[24] C. Xie, L. Li, H. Situ, and J. He, "Semi-quantum secure direct communication scheme based on bell states," *Int. J. Theor. Phys.*, vol. 57, no. 6, pp. 1881–1887, 2018.

[25] M. van Dijk and A. Koppelaar, "Quantum key agreement," in *Proc. IEEE Int. Symp. Inf. Theory*, Aug. 1998, p. 350.

[26] H. Cao and W. Ma, "Multiparty quantum key agreement based on quantum search algorithm," *Sci. Rep.*, vol. 7, Mar. 2017, Art. no. 45046.

[27] B. Cai, G. Guo, S. Lin, H. Zuo, and C. Yu, "Multipartite quantum key agreement over collective noise channels," *IEEE Photon. J*, vol. 10, no. 1, Feb. 2018, Art. no. 7600211.

[28] J. He, L. Li, Y. Huang, H. Situ, and D. Qiu, "High-dimensional quantum key agreement protocol with pairs of single qudits," *Int. J. Quantum Inf.*, vol. 16, no. 3, p. 1850024, 2018.

[29] T. Cai, M. Jiang, and G. Cao, "Multi-party quantum key agreement with five-qubit brown states," *Quantum Inf. Process.*, vol. 17, p. 103, May 2018.

[30] H. Cao and W. Ma, "Verifiable threshold quantum state sharing scheme," *IEEE Access*, vol. 6, pp. 10453–10457, 2018.

[31] C. Hao and M. Wenping, "(t, n) threshold quantum state sharing scheme based on linear equations and unitary operation," *IEEE Photon. J.*, vol. 9, no. 1, Feb. 2017, Art. no. 7600207.

[32] H. Abulkasim, S. Hamad, K. E. Bahnasy, and S. Z. Rida, "Authenticated quantum secret sharing with quantum dialogue based on Bell states," *Phys. Scripta*, vol. 91, no. 8, p. 085101, 2016.

[33] G. Gao, Y. Wang, D. Wang, and L. Ye, "Comment on 'Authenticated quantum secret sharing with quantum dialogue based on Bell states,'" *Phys. Scripta*, vol. 93, no. 2, p. 027002, 2018.

[34] H. Abulkasim, S. Hamad, and A. Elhadad, "Reply to comment on 'Authenticated quantum secret sharing with quantum dialogue based on Bell states,'" *Phys. Scripta*, vol. 93, no. 2, p. 027001, 2018.

[35] H. Abulkasim, S. Hamad, A. Khalifa, and K. E. Bahnasy, "Quantum secret sharing with identity authentication based on Bell states," *Int. J. Quantum Inf.*, vol. 15, no. 4, p. 1750023, 2017.

[36] M. Sarvaghad-Moghaddam, A. Farouk, and H. Abulkasim. (2018). "Bidirectional quantum controlled teleportation by using five-qubit entangled state as a quantum channel." [Online]. Available: https://arxiv.org/abs/1806.07061

[37] J.-G. Ren *et al.*, "Ground-to-satellite quantum teleportation," *Nature*, vol. 549, pp. 70–73, Sep. 2017.

[38] G. Gao, "Notes on two multiparty quantum secret sharing schemes," *Int. J. Quantum Inf.*, vol. 16, no. 3, p. 1850030, 2018.

[39] B. A. Nguyen, "Quantum dialogue," *Phys. Lett. A*, vol. 328, no. 1, pp. 6–10, 2004.

[40] L. Gong, J. Li, and N. Zhou, "Multiparty quantum dialogue protocol based on continuous variable squeezed states," in *Proc. IEEE 17th Int. Conf. Nanotechnol. (NANO)*, Jul. 2017, pp. 36–39.

[41] H. Wang, Y. Q. Zhang, X. F. Liu, and Y. P. Hu, "Efficient quantum dialogue using entangled states and entanglement swapping without information leakage," *Quantum Inf. Process.*, vol. 15, no. 6, pp. 2593–2603, 2016.

[42] G. Gao, "Comment on 'Efficient quantum dialogue without information leakage,'" *Mod. Phys. Lett. B*, vol. 32, no. 22, p. 1875001, 2018.

[43] M.-H. Zhang, Z.-W. Cao, and J.-Y. Peng, "Fault-tolerant asymmetric quantum dialogue protocols against collective noise," *Quantum Inf. Process.*, vol. 17, p. 204, Aug. 2018.

[44] V. Giovannetti, S. Lloyd, and L. Maccone, "Quantum private queries," *Phys. Rev. Lett.*, vol. 100, no. 23, p. 230502, 2008.

[45] Y.-H. Zhou, X.-W. Bai, L.-L. Li, W.-M. Shi, and Y.-G. Yang, "A quantum private query protocol for enhancing both user and database privacy," *Commun. Theor. Phys.*, vol. 69, no. 1, p. 31, 2018.

[46] W. Huang, Q.-Y. Wen, B. Liu, Q. Su, S.-J. Qin, and F. Gao, "Quantum anonymous ranking," *Phys. Rev. A, Gen. Phys.*, vol. 89, no. 3, p. 032325, 2014.

[47] L. Jiang, G. He, D. Nie, J. Xiong, and G. Zeng, "Quantum anonymous voting for continuous variables," *Phys. Rev. A, Gen. Phys.*, vol. 85, no. 4, p. 042309, 2012.

[48] C. H. Bennett, G. Brassard, C. Crépeau, and M.-H. Skubiszewska, "Practical quantum oblivious transfer," in *Proc. Annu. Int. Cryptol. Conf.*, 1991, pp. 351–366.

[49] G. P. He and Z. D. Wang, "Oblivious transfer using quantum entanglement," *Phys. Rev. A, Gen. Phys.*, vol. 73, no. 1, p. 012331, 2006.
[50] C.-Y. Wei, X.-Q. Cai, B. Liu, T.-Y. Wang, and F. Gao, "A generic construction of quantum-oblivious-key-transfer-based private query with ideal database security and zero failure," *IEEE Trans. Comput.*, vol. 67, no. 1, pp. 2–8, Jan. 2018.
[51] K. Cheong, M.-H. Hsieh, and T. Koshiba. (2010). "Asymptotically secure quantum oblivious transfer." [Online]. Available: https://arxiv.org/abs/1004.1871
[52] Y. Yu-Guang and W. Qiao-Yan, "An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement," *J. Phys. A, Math. Theor.*, vol. 42, no. 20, p. 055305, 2009.
[53] W.-W. Zhang and K.-J. Zhang, "Cryptanalysis and improvement of the quantum private comparison protocol with semi-honest third party," *Quantum Inf. Process.*, vol. 12, no. 5, pp. 1981–1990, 2013.
[54] H.-K. Lo, "Insecurity of quantum secure computations," *Phys. Rev. A, Gen. Phys.*, vol. 56, no. 2, p. 1154, 1997.
[55] Q.-L. Wang, H.-X. Sun, and W. Huang, "Multi-party quantum private comparison protocol with n -level entangled states.," *Quantum Inf. Process.*, vol. 13, no. 11, pp. 2375–2389, 2014.
[56] X. Ting and Y. Tian-Yu, "Cryptanalysis and improvement for the quantum private comparison protocol based on triplet entangled state and single-particle measurement," *Int. J. Theor. Phys.*, vol. 56, no. 3, pp. 771–780, 2017.
[57] Z. Sun, J. Yu, P. Wang, L. Xu, and C. Wu, "Quantum private comparison with a malicious third party," *Quantum Inf. Process.*, vol. 14, no. 6, pp. 2125–2133, 2015.
[58] S.-M. Hung, S.-L. Hwang, T. Hwang, and S.-H. Kao, "Multiparty quantum private comparison with almost dishonest third parties for strangers," *Quantum Inf. Process.*, vol. 16, p. 36, Feb. 2017.
[59] B. Liu, D. Xiao, W. Huang, H.-Y. Jia, and T.-T. Song, "Quantum private comparison employing single-photon interference," *Quantum Inf. Process.*, vol. 16, p. 180, Jul. 2017.
[60] J. Gu, C.-Y. Ho, and T. Hwang, "Statistics attack on 'quantum private comparison with a malicious third party' and its improvement," *Quantum Inf. Process.*, vol. 17, p. 23, Feb. 2018.
[61] C.-H. Chang, T. Hwang, and P. Gope, "An efficient quantum private comparison of equality over collective-noise channels," *Int. J. Theor. Phys.*, vol. 55, no. 4, pp. 2125–2138, 2016.
[62] B. Liu, F. Gao, H.-Y. Jia, W. Huang, W.-W. Zhang, and Q.-Y. Wen, "Efficient quantum private comparison employing single photons and collective detection," *Quantum Inf. Process.*, vol. 12, no. 2, pp. 887–897, 2013.
[63] X.-B. Chen, Y. Su, X.-X. Niu, and Y.-X. Yang, "Efficient and feasible quantum private comparison of equality against the collective amplitude damping noise," *Quantum Inf. Process.*, vol. 13, no. 1, pp. 101–112, 2014.
[64] V. Siddhu and Arvind, "Quantum private comparison over noisy channels," *Quantum Inf. Process.*, vol. 14, no. 8, pp. 3005–3017, 2015.
[65] Y.-J. Chang, C.-W. Tsai, and T. Hwang, "Multi-user private comparison protocol using GHZ class states," *Quantum Inf. Process.*, vol. 12, no. 2, pp. 1077–1088, 2013.
[66] W. Liu, Y.-B. Wang, and X.-M. Wang, "Multi-party quantum private comparison protocol using d-dimensional basis states without entanglement swapping," *Int. J. Theor. Phys.*, vol. 53, no. 4, pp. 1085–1091, 2014.
[67] T.-Y. Ye, "Multi-party quantum private comparison protocol based on entanglement swapping of Bell entangled states," *Commun. Theor. Phys.*, vol. 66, no. 3, p. 280, 2016.
[68] J. Zhao-Xu and Y. Tian-Yu, "Multi-party quantum private comparison based on the entanglement swapping of d-level cat states and d-level Bell states," *Quantum Inf. Process.*, vol. 16, p. 177, Jul. 2017.
[69] T. Ye and Z. Ji, "Multi-user quantum private comparison with scattered preparation and one-way convergent transmission of quantum states," *Sci. China Phys., Mech. Astron.*, vol. 60, p. 090312, Sep. 2017.
[70] M.-K. Zhou, "Robust multi-party quantum private comparison protocols against the collective noise based on three-qubit entangled states," *Int. J. Theor. Phys.*, vol. 57, no. 10, pp. 2931–2937, 2018.
[71] C.-Q. Ye and T.-Y. Ye, "Multi-party quantum private comparison of size relation with d-level single-particle states," *Quantum Inf. Process.*, vol. 17, p. 252, Oct. 2018.
[72] W. Liu and Y.-B. Wang, "Dynamic multi-party quantum private comparison protocol with single photons in both polarization and spatial-mode degrees of freedom," *Int. J. Theor. Phys.*, vol. 55, no. 12, pp. 5307–5317, 2016.
[73] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Phys. Rev. Lett.*, vol. 94, no. 23, p. 230504, 2005.
[74] B. Liu, D. Xiao, H.-Y. Jia, and R.-Z. Liu, "Collusive attacks to 'circle-type' multi-party quantum key agreement protocols," *Quantum Inf. Process.*, vol. 15, no. 5, pp. 2113–2124, 2016.
[75] Y. Shuai, C. Xiu-Bo, and Y. Yi-Xian, "Attack on the enhanced multiparty quantum secret sharing," *Commun. Theor. Phys.*, vol. 58, no. 1, p. 51, 2012.
[76] J. Gu and T. Hwang, "Improvement of 'novel multiparty quantum key agreement protocol with GHZ states,"' *Int. J. Theor. Phys.*, vol. 56, no. 10, pp. 3108–3116, 2017.
[77] T.-Y. Wang, Y.-Z. Liu, C.-Y. Wei, X.-Q. Cai, and J.-F. Ma, "Security of a kind of quantum secret sharing with entangled states," *Sci. Rep.*, vol. 7, Feb. 2017, Art. no. 2485.
[78] G. Gao and Y. Wang, "Comment on 'Proactive quantum secret sharing,"' *Quantum Inf. Process.*, vol. 16, p. 74, Mar. 2017.
[79] H. Abulkasim, A. Farouk, H. Alsuqaih, W. Hamdan, S. Hamad, and S. Ghose, "Improving the security of quantum key agreement protocols with single photon in both polarization and spatial-mode degrees of freedom," *Quantum Inf. Process.*, vol. 17, no. 11, p. 316, 2018.
[80] P. Xue and X. Zhang, "A simple quantum voting scheme with multi-qubit entanglement," *Sci. Rep.*, vol. 7, Aug. 2017, Art. no. 7586.
[81] S. Muhammad, A. Tavakoli, M. Kurant, M. Pawlowski, M. Zukowski, and M. Bourennane, "Quantum bidding in Bridge," *Phys. Rev. X*, vol. 4, no. 2, p. 021047, 2014.
[82] T. Hogg, P. Harsha, and K.-Y. Chen, "Quantum auctions," *Int. J. Quantum Inf.*, vol. 5, no. 5, pp. 751–780, 2007.
[83] M. Elhoseny, A. Tharwat, and A. A. E. Farouk Hassanien, "K-coverage model based on genetic algorithm to extend WSN lifetime," *IEEE Sensors Lett.*, vol. 1, no. 4, pp. 1–4, Aug. 2017.
[84] M. Elhoseny, A. Farouk, N. Zhou, M. M. Wang, S. Abdalla, and J. Batle, "Dynamic multi-hop clustering in a wireless sensor network: Performance improvement," *Wireless Pers. Commun.*, vol. 95, no. 4, 3733–3753, 2017.
[85] U. Habiba and E. Hossain, "Auction mechanisms for virtualization in 5G cellular networks: Basics, trends, and open challenges," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2264–2293, 3rd Quart., 2018.

HUSSEIN ABULKASIM received the B.S., M.S., and Ph.D. degrees in computer science from South Valley University, in 2004, 2012, and 2016, respectively. He was a Lecturer with the College of Computer Sciences and Information Systems, Jazan University, from 2013 to 2014. He was also an Assistant Professor with the Department of Mathematics and Computer Science, Assiut University, from 2014 to 2018. He is currently an Assistant Professor with the Department of Mathematics and Computer Science, The New Valley University. His current research interests include quantum cryptography, information security, cloud security, and evolutionary computation.

HANAN NASER ALSUQAIH is currently an Assistant Professor with the Libraries and Information Department, Princess Nourah Bint Abdul Rahman University (PNU), where she is also a Scientific Researcher with the Deanship of Scientific Research. In addition, she is also the Dean of the Libraries Affairs Deanship with PNU. Her research interests include information systems, radio frequency identifications, and wireless access to the Internet. Her researches are published in many journals and international conferences in the Middle East.

WALAA FAWZY HAMDAN is currently an Assistant Professor with the Libraries and Information Department, Princess Nourah Bint Abdul Rahman University (PNU), where she is also a Scientific Researcher with the Deanship of Scientific Research. In addition, she is also the Ex-Director of Branch Libraries and is also the Ex-Director of the Arts College Library, Deanship of Library Affairs, PNU. Her research interests include information systems, radio frequency identifications, wireless access to the Internet, and bibliotherapy. Her researches are published in many journals and international conferences in the Middle East.

SAFWAT HAMAD received the bachelor's degree in 2000, the M.Sc. degree in modeling, simulation, and visualization, and the joint Ph.D. degree in high-performance computing from the Computer Science and Engineering Department, University of Connecticut, USA, and the Faculty of Computer and Information Sciences (FCIS), Ain Shams University (ASU), in 2008. He was a teaching assistant for several undergraduate courses. He is currently an Associate Professor, and he has been the Chair of the Scientific Computing Department, FCIS, ASU, Cairo, Egypt, since 2017. His main research interests include image and video processing, computational biology, machine learning, encryption, and security.

AHMED FAROUK received the M.Sc. and Ph.D. degrees from Mansoura University, in 2009 and 2015, respectively. He is currently a Postdoctoral Fellow with Wilfrid Laurier University. Also, he is one of the Top 20 Technical Co-Founders of the Quantum Machine Learning Program by the Creative Destruction Lab, University of Toronto. Furthermore, he is selected as Top 25 of InnovateTO150 Canada to showcase the best of Toronto's next generation of change makers, innovators, and entrepreneurs. He is especially well known for his seminal contributions to theories of quantum mechanics, communication and cryptography. He has published 52 papers in reputed and high-impact journals, such as *Scientific Reports* (Nature) and *Physical Review A*.

ATEFEH MASHATAN received the Ph.D. degree from the University of Waterloo. She investigates challenges and opportunities brought forward by these new technologies and how they change the threat landscape of cybersecurity. Collaborating with industry partners, she studies industry relevant research problems and proposes solutions that can be developed as a part of the industry-academic collaborations. Prior to joining Ryerson University, she was a Senior Information Security Consultant and a Solutions Architect at CIBC (Canadian Imperial Bank of Commerce), in 2012–2016, with a focus on a cryptography and enterprise architecture. Prior to that, she was a Scientific Collaborator with the Security and Cryptography Laboratory, School of Computer and Communication Sciences, Swiss Federal Institute of Technology Lausanne, Lausanne, in 2009–2012. She is currently the Director of the Cybersecurity Research Lab and an Assistant Professor with the Ted Rogers School of Information Technology Management. Her research interest includes the development of novel information security designs based on emerging technologies, such as the IoT, blockchain, and quantum computing. She is also a Certified Service-Oriented Architect with Honors. She received the Certified Information Systems Security Professional Certification from the International Information Systems Security Certification Consortium.

SHOHINI GHOSE is currently a Professor of physics and computer science with Wilfrid Laurier University and the Founding Director of the Laurier's University Research Centre for Women in Science. She is also a Theoretical Physicist who examines how the laws of quantum physics can be harnessed to transform computation and communication. She and her colleagues first experimentally demonstrated a connection between chaos theory and quantum entanglement. She is also a Researcher and an Equity, Diversity, and Inclusion Specialist with the Perimeter Institute for Theoretical Physics. She is also with the Institute for Quantum Computing, and a Fellow of the Balsillie School of International Affairs. She was a recipient of several awards, including the TED Senior Fellowship, in 2018. She is the elected Vice-President of the Canadian Association of Physicists and a Co-Editor of the *Canadian Journal of Physics*. In 2017, she was named to the Royal Society of Canada's College of New Scholars, Artists and Scientists.