Hindawi Publishing Corporation
Advances in Mathematical Physics
Volume 2016, Article ID 3162012, 7 pages
http://dx.doi.org/10.1155/2016/3162012

Research Article

A General Scheme for Information Interception in the Ping-Pong Protocol

Piotr Zawadzki[1] and Jarosław Adam Miszczak[2]

[1] *Institute of Electronics, Silesian University of Technology, Akademicka 16, 44-100 Gliwice, Poland*
[2] *Institute of Theoretical and Applied Informatics, Polish Academy of Sciences, Bałtycka 5, 44-100 Gliwice, Poland*

Correspondence should be addressed to Piotr Zawadzki; Zawadzki.Piotrus@gmail.com

Received 22 March 2016; Revised 25 May 2016; Accepted 6 June 2016

Academic Editor: Kamil Brádler

The existence of undetectable eavesdropping of dense coded information has been already demonstrated by Pavičić for the quantum direct communication based on the ping-pong paradigm. However, (a) the explicit scheme of the circuit is only given and no design rules are provided; (b) the existence of losses is implicitly assumed; (c) the attack has been formulated against qubit based protocol only and it is not clear whether it can be adapted to higher dimensional systems. These deficiencies are removed in the presented contribution. A new generic eavesdropping scheme built on a firm theoretical background is proposed. In contrast to the previous approach, it does not refer to the properties of the vacuum state, so it is fully consistent with the absence of losses assumption. Moreover, the scheme applies to the communication paradigm based on signal particles of any dimensionality. It is also shown that some well known attacks are special cases of the proposed scheme.

1. Introduction

Quantum direct communication (QDC) aims at provision of confidentiality without resorting to classic encryption. This is in contrast to quantum key distribution (QKD) technique, as no shared key is established and quantum resources take over its role. In QDC, similar to QKD, it is assumed that legitimate parties can communicate over open and authenticated classic channel.

The roots of QDC can be traced out to the QKD protocol of Long and Liu [1] that, after slight modification proposed as the two-step protocol [2], can be considered the first protocol of this kind. The ping-pong protocol [3] is another QDC scheme which is easier to implement at the price of lesser security margin and capacity. These initial works exploited the entanglement of EPR pairs to protect transmission of sensitive information. Ideas of these proposals have been further adapted to higher dimensional systems [4–7] and/or modified to enhance capacity via dense coding [8, 9]. The entanglement is a very fragile quantum resource and its handling is technically challenging. This motivated the work towards exploiting quantum uncertainty, a resource used by most QKD protocols. The first single-photon QDC protocol proposed by Deng and Long [10] has been recently demonstrated experimentally [11]. The LM05 protocol [12] is the other proposal of this kind that is worth noting. The history of the development and the review of the early QDC proposals can be found in [13].

QDC protocols offer different level of security which usually results from the tradeoff between practical feasibility and type of quantum resource available to communicating parties. QDC protocols which process particles in blocks [2, 4] can be parametrized in such a way that probability of revealing sensitive information is arbitrarily small. However, they assume that legitimate parties have long-term quantum memory. Protocols that process particles individually are quasi-secure [13–15]. Quasi-security means that before eavesdropping detection, which is inevitable for long sequences, part of the sensitive information may be revealed to the eavesdropper. QDC is a more versatile cryptographic primitive than QKD. In fact, QDC protocols can be used as engines for key agreement. Any key agreement protocol executed

in a private channel provided by a QDC protocol offering unconditional security has security comparable with QKD. Also quasi-secure QDC protocols can realize unconditionally secure QKD. However, in this case, QDC phase delivers shared sequence that is partially known to the eavesdropper. By the appropriate postprocessing, that is, privacy amplification, the eavesdropper's knowledge on the resulting sequence can be reduced to arbitrarily small value provided that his information on the initial sequence is less than mutual information of the legitimate parties. The realization of the QKD via QDC can be potentially more efficient as the basis reconciliation step, which severely plagues efficiency of many QKD protocols, can be avoided [16–18]. Protocols of this type are referred to as deterministic QKD and some of them have been recently experimentally demonstrated [19, 20].

This paper is devoted to the analysis of the (in)security of the ping-pong protocol, an entanglement based QDC scheme [3]. Quasi-security is provided only for perfect quantum channels [14] and the scheme becomes insecure when losses [21] and/or communication errors and imperfection of devices are taken into account [22]. Protocol offers capacity of single bit per protocol cycle because the authenticity of the shared EPR pair is verified only by a measurement in a single basis. This limits the available encoding to phase flips. Possible capacity enhancement via dense coding leads to undetectable information leakage as demonstrated in [2] and usage of mutually unbiased bases in control measurements is required to preserve quasi-security of the communication [8]. In our previous work, we have proved that this observation also holds for the qudit based protocol and that detection probability depends on the number of bases used in the control mode [7, 23]. Anyway, no explicit attack transformation has been given in the aforementioned papers. The present contribution is motivated by the appearance of the circuit [24] (further, it will be referred to as P-circuit) capable of undetectably intercepting information transmitted in the qubit based ping-pong protocol with the following configuration: quantum channel is perfect, legitimate parties use single basis for control measurements, and information is dense coded. In other words, the instantiation of the attack is forecasted in [2]. Although P-circuit is applicable to perfect channels, it assumes the appearance of the vacuum states in the eavesdropper's ancilla. In consequence, it does not well fit the existing analyses. Shortly after its appearance, a control mode that addresses detection of this specific circuit has been proposed [25].

We propose a generic scheme for construction of attacks that permit undetectable eavesdropping under the same assumptions: quantum channel is perfect, control measurements are executed in a single basis, and sensitive information is dense coded. Thus, our contribution can be considered as the generalization of the result given in [24]. The presented method is applicable to systems of any dimension so it can be used to construct a plethora of new transforms. Using introduced generalization, we also demonstrate the equivalence of the attack from [24] and CNOT operation. In consequence, we claim that there is no need for construction of specific control modes as in [25], because any control mode able to detect CNOT operation is also able to detect circuit proposed in [24]. We do *not* propose the attack that is undetectable by control measurements in unbiased bases. In fact, we think that the opposite is true: control measurements in mutually unbiased bases are sufficient to statistically detect coherence break of the shared entangled state and, in that way, reveal the presence of the eavesdropper [23].

The paper is organized as follows. In Section 2, we provide notation and concepts used in the text. Section 3 presents the main contribution. In particular, we provide a general bit-flip detection scheme, demonstrate its equivalence with the existing approaches, and introduce an attack on the qudit based protocol. In Section 4, we summarize the presented work.

2. Preliminaries

2.1. Ping-Pong Protocol. The communication protocol described below is a ping-pong paradigm variant analysed in [24]. Compared to the seminal version [3], it differs only in the encoding operation: the sender uses dense coding instead of phase flips. The remaining elements of the communication scenario are left intact.

Bob starts the communication process by creation of EPR pair (the assumed initial state is the same as in [3, 24] to maintain compatibility of mathematical expressions; for the qudit version of the protocol, considered in Section 3.1, it is assumed that Bob starts from the generalization of $|\Phi^+\rangle = (|0_h\rangle|0_t\rangle + |1_h\rangle|1_t\rangle)/\sqrt{2}$):

$$\left|\Psi_{\text{init}}\right\rangle = \left|\Psi^-\right\rangle = \frac{\left(\left|0_h\right\rangle\left|1_t\right\rangle - \left|1_h\right\rangle\left|0_t\right\rangle\right)}{\sqrt{2}}. \tag{1}$$

Then, he sends one of the qubits, further referred to as the signal/travel qubit, to Alice. Alice can in principle encode two classic bits μ and ν applying unitary transformation $\mathscr{A}_{\mu,\nu} = \mathscr{X}^{\mu}\mathscr{Z}^{\nu}$, where $\mathscr{X} = |1\rangle\langle 0| + |0\rangle\langle 1|$ and $\mathscr{Z} = |0\rangle\langle 0| - |1\rangle\langle 1|$ are bit-flip and phase-flip operations, respectively. The signal particle is sent back to Bob, who detects applied transformation by a collective measurement of both qubits (Figure 1).

Passive eavesdropping is impossible. Eve has access only to the travel qubit which before and after encoding looks like maximally mixed state. Unfortunately, the described communication scenario is vulnerable to the intercept-resend attack and Alice has to check whether the received qubit is genuine. As a countermeasure, Alice measures the received qubit in computational basis $(|0\rangle, |1\rangle)$ in randomly selected protocol cycles and asks Bob over authenticated classic channel to do the same with his qubit (Figure 2). Her measurement causes the collapse of the shared state (1). The perfect (anti)correlation of the outcomes is preserved only if the qubit measured by Alice is the same one that was sent by Bob. If Eve inserts fake qubit, then the measured qubits are no longer correlated and some discrepancies, which are the sign of the eavesdropping, do occur. In that way, Alice and Bob can convince themselves with confidence approaching certainty that the quantum channel is not spoofed, provided that they have executed a sufficient number of control cycles.

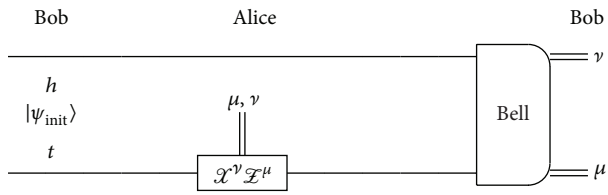

Figure 1: The schematic diagram of a message mode in the ping-pong protocol.

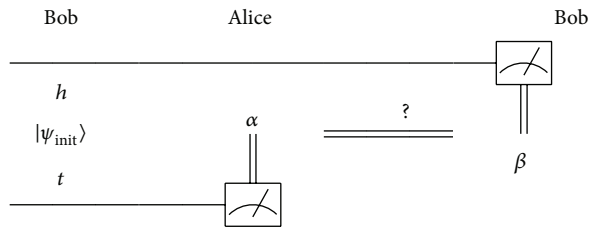

Figure 2: The schematic diagram of a control mode in the ping-pong protocol.

However, the intercept-resend attack is not the only possible way of active sensitive information interception. The signal particle that travels back and forth between legitimate parties can be the subject of any quantum action introduced by Eve (Figure 3). Introduced coupling causes the encoding operation to also modify Eve's ancilla state and Eve hopes to detect and decipher Alice's actions by its inspection. Actions of Eve, not necessarily unitary in the affected qubit's space, can be described as unitary operation $\mathcal{Q}$ acting in the space extended with two additional qubits, as follows from Stinespring's dilation theorem. The control state shared by legitimate parties then takes the form

$$|\psi_{htE}\rangle = (\mathcal{I}_h \otimes \mathcal{Q})(|\Psi_{\text{init}}\rangle \otimes |\chi_E\rangle), \tag{2}$$

where $|\chi_E\rangle$ is some initial state of Eve's ancilla. Eve presence is detected with probability

$$p_{\text{det}}(\mathcal{Q}) = \text{Tr}(\mathcal{P}_{ht}\text{Tr}_E(|\psi_{htE}\rangle\langle\psi_{htE}|)), \tag{3}$$

where projection $\mathcal{P}_{ht}$ depends on initial state and the considered case is defined as

$$\begin{aligned}\mathcal{P}_{ht} = \mathcal{I}_{ht} - |0_h\rangle\langle 0_h| \otimes |1_t\rangle\langle 1_t| - |1_h\rangle\langle 1_h| \\ \otimes |0_t\rangle\langle 0_t|.\end{aligned} \tag{4}$$

2.2. Pavičić Attack. Pavičić's attack demonstrates the violation of ping-pong protocol security when dense coding is used. The attack does not introduce errors or losses in control and message mode and it permits eavesdropping information encoded as bit-flip operation.

The P-circuit presented by Pavičić (Figure 4) is a result of a cut-and-try procedure [24, section IV] applied to Wójcik's circuit [21]. It is composed of two Hadamard gates followed by the controlled polarization beam splitter (CPBS), which is a generalization of the polarization beam splitter (PBS) concept. The PBS is a two-port gate that swaps horizontally

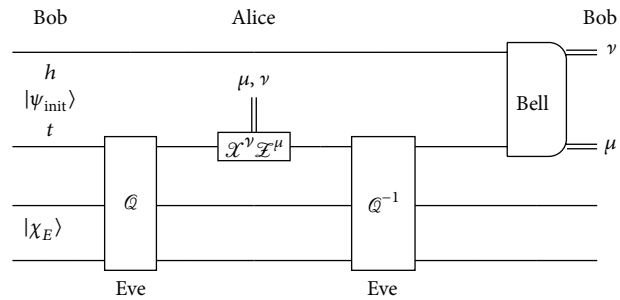

Figure 3: A schematic diagram of an individual attack.

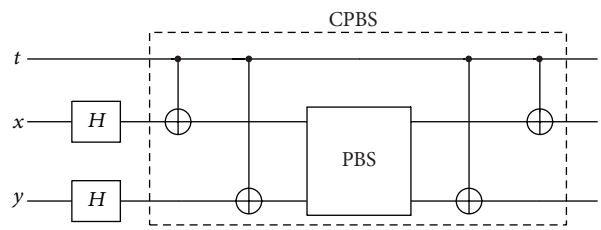

Figure 4: P-circuit $\mathcal{Q}_{txy}$ [24, eq. (2)].

polarized photons $|0_x\rangle$ ($|0_y\rangle$) entering its input to the other port $|0_y\rangle$ ($|0_x\rangle$) on output while vertically polarized ones $|1_x\rangle$ ($|1_y\rangle$) remain in their port $|1_x\rangle$ ($|1_y\rangle$); that is,

$$\begin{aligned}\text{PBS}\,|v_x\rangle\,|0_y\rangle &= |0_x\rangle\,|v_y\rangle, \\ \text{PBS}\,|v_x\rangle\,|1_y\rangle &= |v_x\rangle\,|1_y\rangle,\end{aligned} \tag{5a}$$

$$\begin{aligned}\text{PBS}\,|0_x\rangle\,|v_y\rangle &= |v_x\rangle\,|0_y\rangle, \\ \text{PBS}\,|1_x\rangle\,|v_y\rangle &= |1_x\rangle\,|v_y\rangle,\end{aligned} \tag{5b}$$

where $|v\rangle$ denotes the vacuum state. The CPBS behaves as normal PBS if control qubit is set to $|0_t\rangle$. The roles of horizontal and vertical polarization are exchanged for control qubit set to $|1_t\rangle$:

$$\begin{aligned}\text{CPBS}\,|0_t\rangle\,|v_x\rangle\,|0_y\rangle &= |0_t\rangle\,|0_x\rangle\,|v_y\rangle, \\ \text{CPBS}\,|1_t\rangle\,|v_x\rangle\,|0_y\rangle &= |1_t\rangle\,|v_x\rangle\,|0_y\rangle,\end{aligned} \tag{6a}$$

$$\begin{aligned}\text{CPBS}\,|0_t\rangle\,|0_x\rangle\,|v_y\rangle &= |0_t\rangle\,|v_x\rangle\,|0_y\rangle, \\ \text{CPBS}\,|1_t\rangle\,|0_x\rangle\,|v_y\rangle &= |1_t\rangle\,|0_x\rangle\,|v_y\rangle,\end{aligned} \tag{6b}$$

$$\begin{aligned}\text{CPBS}\,|0_t\rangle\,|v_x\rangle\,|1_y\rangle &= |0_t\rangle\,|v_x\rangle\,|1_y\rangle, \\ \text{CPBS}\,|1_t\rangle\,|v_x\rangle\,|1_y\rangle &= |1_t\rangle\,|1_x\rangle\,|v_y\rangle,\end{aligned} \tag{6c}$$

$$\begin{aligned}\text{CPBS}\,|0_t\rangle\,|1_x\rangle\,|v_y\rangle &= |0_t\rangle\,|1_x\rangle\,|v_y\rangle, \\ \text{CPBS}\,|1_t\rangle\,|1_x\rangle\,|v_y\rangle &= |1_t\rangle\,|v_x\rangle\,|1_y\rangle.\end{aligned} \tag{6d}$$

Initially, Eve's ancilla is initialized to the state $|\chi_0\rangle = |v_x\rangle|0_y\rangle$. The action of the P-circuit from Figure 4 is then described by the following formulas:

$$\begin{aligned}\mathcal{Q}_{txy}|0_t\rangle|\chi_0\rangle &= \frac{1}{\sqrt{2}}|0_t\rangle\left(|0_x\rangle|v_y\rangle + |v_x\rangle|1_y\rangle\right)\\ &= |0_t\rangle|a_E\rangle,\end{aligned} \tag{7a}$$

$$\begin{aligned}\mathcal{Q}_{txy}|1_t\rangle|\chi_0\rangle &= \frac{1}{\sqrt{2}}|1_t\rangle\left(|v_x\rangle|0_y\rangle + |1_x\rangle|v_y\rangle\right)\\ &= |1_t\rangle|d_E\rangle.\end{aligned} \tag{7b}$$

For the purpose of future analysis, let us also identify actions of the circuit under consideration onto the state $|\chi_1\rangle = |0_x\rangle|v_y\rangle$:

$$\begin{aligned}\mathcal{Q}_{txy}|0_t\rangle|\chi_1\rangle &= \frac{1}{\sqrt{2}}|0_t\rangle\left(|v_x\rangle|0_y\rangle + |1_x\rangle|v_y\rangle\right)\\ &= |0_t\rangle|d_E\rangle,\end{aligned} \tag{8a}$$

$$\begin{aligned}\mathcal{Q}_{txy}|1_t\rangle|\chi_1\rangle &= \frac{1}{\sqrt{2}}|1_t\rangle\left(|0_x\rangle|v_y\rangle + |v_x\rangle|1_y\rangle\right)\\ &= |1_t\rangle|a_E\rangle.\end{aligned} \tag{8b}$$

The control state (2) after entangling with Eve's ancilla reads

$$|\psi_{htE}\rangle = \frac{\left(|0_h\rangle|1_t\rangle|d_E\rangle + |1_h\rangle|0_t\rangle|a_E\rangle\right)}{\sqrt{2}}. \tag{9}$$

This state is further used by Alice and Bob for eavesdropping check. It is clear from (3) that the attack does not introduce errors or losses in control mode and the expected correlation of outcomes is preserved in the computational basis.

Phase Flip. The phase-flip encoding applied to the coupled state leads to

$$\begin{aligned}|\psi_{\text{phase}}\rangle &= (\mathcal{I}_h \otimes \mathcal{Z}_t)|\psi_{htE}\rangle\\ &= \frac{1}{\sqrt{2}}\left(|1_h\rangle|0_t\rangle|a_E\rangle - |0_h\rangle|1_t\rangle|d_E\rangle\right).\end{aligned} \tag{10}$$

The signal qubit is then sent back to Bob who, after disentangling on a basis of (7a) and (7b), observes

$$\begin{aligned}|\phi_{\text{phase}}\rangle &= \left(\mathcal{Q}_{txy}\right)^{-1}|\psi_{\text{phase}}\rangle\\ &= \frac{1}{\sqrt{2}}\left(|1_h\rangle|0_t\rangle - |0_h\rangle|1_t\rangle\right)|v_x\rangle|0_y\rangle\\ &= \left[(\mathcal{I}_h \otimes \mathcal{Z}_t)|\psi_{\text{init}}\rangle\right]|\chi_0\rangle.\end{aligned} \tag{11}$$

Bit Flip. The bit-flip operation transforms Alice's state to

$$\begin{aligned}|\psi_{\text{bit}}\rangle &= (\mathcal{I}_h \otimes \mathcal{X}_t)|\psi_{htE}\rangle\\ &= \frac{1}{\sqrt{2}}\left(|1_h\rangle|1_t\rangle|a_E\rangle + |0_h\rangle|0_t\rangle|d_E\rangle\right).\end{aligned} \tag{12}$$

The system state after disentangling can be deduced from (8a) and (8b):

$$\begin{aligned}|\phi_{\text{bit}}\rangle &= \left(\mathcal{Q}_{txy}\right)^{-1}|\psi_{\text{bit}}\rangle\\ &= \frac{1}{\sqrt{2}}\left(|1_h\rangle|1_t\rangle + |0_h\rangle|0_t\rangle\right)|0_x\rangle|v_y\rangle\\ &= \left[(\mathcal{I}_h \otimes \mathcal{X}_t)|\psi_{\text{init}}\rangle\right]|\chi_1\rangle.\end{aligned} \tag{13}$$

In both cases, that is, phase-flip and bit-flip encoding, the signalling subsystem behaves as if there was no coupling with the ancilla. However, Alice's bit-flip encoding modifies Eve's register ($|\chi_0\rangle \rightarrow |\chi_1\rangle$). The states $|\chi_0\rangle$ and $|\chi_1\rangle$ are orthogonal and perfectly distinguishable. In consequence, Eve can eavesdrop on bit-flip operations without introducing errors and losses in message mode as well.

3. Results

This section is devoted to the analysis of the general form of the incoherent attack shown diagrammatically in Figure 3. Each cycle of the protocol is considered to be independent of the other ones. Consequently, the effectiveness of the attack is expressed in a fraction of bits eavesdropped on per communication cycle. Throughout the analysis, it is also assumed that legitimate parties rely on control mode used in the seminal version of the protocol. They locally measure possessed particles in the computational basis and verify expected correlation via the public discussion over authenticated classic channel.

3.1. Generic Bit-Flip Detection Scheme for Qubit Based Protocol. As the control mode explores outcomes of local measurements in computational basis for intrusion detection, the map $\mathcal{Q}$ has to be of trivial form

$$\begin{aligned}\mathcal{Q}|0_t\rangle|\chi_E\rangle &\longrightarrow |0_t\rangle|a_E\rangle,\\ \mathcal{Q}|1_t\rangle|\chi_E\rangle &\longrightarrow |1_t\rangle|d_E\rangle\end{aligned} \tag{14}$$

to not induce errors and/or losses in control cycles. It follows that, under attack, Alice operates on the state

$$|\psi_{htE}\rangle = \frac{1}{\sqrt{2}}\left(|0_h\rangle|1_t\rangle|d_E\rangle - |1_h\rangle|0_t\rangle|a_E\rangle\right). \tag{15}$$

Let the entangling transformation $\mathcal{Q}$ additionally satisfy

$$\begin{aligned}\mathcal{Q}|0_t\rangle|\phi_E\rangle &\longrightarrow |0_t\rangle|d_E\rangle,\\ \mathcal{Q}|1_t\rangle|\phi_E\rangle &\longrightarrow |1_t\rangle|a_E\rangle\end{aligned} \tag{16}$$

for some state $|\phi_E\rangle \neq |\chi_E\rangle$. The process of information encoding and disentangling from the ancilla is then described by the expressions

$$\begin{aligned}&\mathcal{Q}^{-1}(\mathcal{I}_h \otimes \mathcal{I}_t \otimes \mathcal{I}_E)|\psi_{htE}\rangle\\ &\quad= \mathcal{Q}^{-1}\frac{1}{\sqrt{2}}\left(|0_h\rangle|1_t\rangle|d_E\rangle - |1_h\rangle|0_t\rangle|a_E\rangle\right)\end{aligned}$$

$$= \frac{1}{\sqrt{2}}\left(\left|0_h\right\rangle\left|1_t\right\rangle\left|\chi_E\right\rangle - \left|1_h\right\rangle\left|0_t\right\rangle\left|\chi_E\right\rangle\right)$$
$$= \left|\Psi^-\right\rangle\left|\chi_E\right\rangle, \tag{17a}$$

$$\mathcal{Q}^{-1}\left(\mathcal{I}_h \otimes \mathcal{X}_t \otimes \mathcal{I}_E\right)\left|\psi_{htE}\right\rangle$$
$$= \mathcal{Q}^{-1}\frac{1}{\sqrt{2}}\left(\left|0_h\right\rangle\left|0_t\right\rangle\left|d_E\right\rangle - \left|1_h\right\rangle\left|1_t\right\rangle\left|a_E\right\rangle\right)$$
$$= \frac{1}{\sqrt{2}}\left(\left|0_h\right\rangle\left|0_t\right\rangle\left|\phi_E\right\rangle - \left|1_h\right\rangle\left|1_t\right\rangle\left|\phi_E\right\rangle\right) \tag{17b}$$
$$= \left|\Phi^-\right\rangle\left|\phi_E\right\rangle,$$

$$\mathcal{Q}^{-1}\left(\mathcal{I}_h \otimes \mathcal{Z}_t \otimes \mathcal{I}_E\right)\left|\psi_{htE}\right\rangle$$
$$= \mathcal{Q}^{-1}\frac{-1}{\sqrt{2}}\left(\left|0_h\right\rangle\left|1_t\right\rangle\left|d_E\right\rangle + \left|1_h\right\rangle\left|0_t\right\rangle\left|a_E\right\rangle\right)$$
$$= \frac{-1}{\sqrt{2}}\left(\left|0_h\right\rangle\left|1_t\right\rangle\left|\chi_E\right\rangle + \left|1_h\right\rangle\left|0_t\right\rangle\left|\chi_E\right\rangle\right) \tag{17c}$$
$$= -\left|\Psi^+\right\rangle\left|\chi_E\right\rangle,$$

$$\mathcal{Q}^{-1}\left(\mathcal{I}_h \otimes \mathcal{X}_t\mathcal{Z}_t \otimes \mathcal{I}_E\right)\left|\psi_{htE}\right\rangle$$
$$= \mathcal{Q}^{-1}\frac{-1}{\sqrt{2}}\left(\left|0_h\right\rangle\left|0_t\right\rangle\left|d_E\right\rangle + \left|1_h\right\rangle\left|1_t\right\rangle\left|a_E\right\rangle\right)$$
$$= \frac{-1}{\sqrt{2}}\left(\left|0_h\right\rangle\left|0_t\right\rangle\left|\phi_E\right\rangle + \left|1_h\right\rangle\left|1_t\right\rangle\left|\phi_E\right\rangle\right) \tag{17d}$$
$$= -\left|\Phi^+\right\rangle\left|\phi_E\right\rangle.$$

As a result, the registers used for signalling are left untouched and decoupled but Eve's register is flipped from $|\chi_E\rangle$ to $|\phi_E\rangle$ when Alice applies bit-flip operation. In consequence, Eve can successfully decode half of the message content provided that the detection states $|\chi_E\rangle$ and $|\phi_E\rangle$ are perfectly distinguishable. It follows that any unitary coupling transformation $\mathcal{Q}$ that satisfies (14) and (16) can be used for bit-flip detection.

3.2. Equivalence of P-Circuit and CNOT Circuit. The properties of the above generic scheme and the P-circuit [24] perfectly coincide. As follows from (7a), (7b), (8a), and (8b), the states $|\chi_0\rangle = |v_x\rangle|0_y\rangle$ and $|\chi_1\rangle = |0_x\rangle|v_y\rangle$ play the role of detection states $|\chi_E\rangle$ and $|\phi_E\rangle$, respectively. It is also clear that transformation $\mathcal{Q}_{txy}$ has properties claimed in (14) and (16). Thus, the P-circuit can be considered as an instance of the generic scheme described in Section 3.1.

However, the operator $\mathcal{Q}$ satisfying (14) and (16) can be realized in many ways. It seems that CNOT operation acting on a single qubit of Eve's ancilla, $\mathcal{Q} = \mathrm{CNOT}_{tx}$, $|\chi_E\rangle = |0_x\rangle$, $|\phi_E\rangle = |1_x\rangle$, $|a_E\rangle = |0_x\rangle$, and $|d_E\rangle = |1_x\rangle$, is the simplest realization of the logic behind the attack. Such version is also practically feasible as the attacks involving probes entangled via the CNOT operation have been already proposed in the QKD context [26, 27]. As a result, both the CNOT circuit and P-circuit are equivalent in terms of provided information gain, detectability, and practical feasibility. Consequently, there is no need for the design of control modes that address P-circuit in a special manner [25].

3.3. An Attack on Qudit Based Protocol. The P-circuit has no straightforward generalization to qudit based version of the protocol. In contrast, the presented approach can be adapted with ease. Let Bob start communication process with creation of EPR pair:

$$\left|\beta_{h,t}^{(0,0)}\right\rangle = \frac{1}{\sqrt{D}}\sum_{k=0}^{D-1}\left|k_h\right\rangle\left|k_t\right\rangle, \tag{18}$$

where D is the qudit dimension. The travel qudit is then sent to Alice for encoding or control measurement. In control mode, the home and travel qubits are measured in the computational basis so the projection $\mathcal{P}_{ht}$ used in control equation (3) takes the form

$$\mathcal{P}_{ht} = \mathcal{I}_{ht} - \sum_{k=0}^{D-1}\left|k_h\right\rangle\left\langle k_h\right| \otimes \left|k_t\right\rangle\left\langle k_t\right|. \tag{19}$$

Let, by an analogy to the qubit case, $|\alpha_E^{(k)}\rangle$ and $|a_E^{(k)}\rangle$ be the sets of D orthonormal states of the ancilla system. These states will be further referred to as detection and probe states, respectively. The map used by Eve must be of the form

$$\mathcal{Q}\left|k_t\right\rangle\left|\alpha_E^{(0)}\right\rangle \longrightarrow \left|k_t\right\rangle\left|a_E^{(k)}\right\rangle, \quad k = 0, \ldots, D-1, \tag{20}$$

to not introduce errors in control measurements. Let us additionally postulate that $\mathcal{Q}$ satisfies

$$\mathcal{Q}\left|k_t\right\rangle\left|\alpha_E^{(m)}\right\rangle \longrightarrow \left|k_t\right\rangle\left|a_E^{(m+k \bmod D)}\right\rangle; \tag{21}$$

that is, $\mathcal{Q}$ advances index k positions in a set of Eve's probe states. Similarly, $\mathcal{Q}^{-1}$ decrements the index k positions:

$$\mathcal{Q}^{-1}\left|k_t\right\rangle\left|a_E^{(m)}\right\rangle \longrightarrow \left|k_t\right\rangle\left|\alpha_E^{(m-k \bmod D)}\right\rangle. \tag{22}$$

Let us recall that for qudits Alice uses

$$\mathcal{Z} = \sum_{k=0}^{D-1}\omega^k\left|k\right\rangle\left\langle k\right|,$$
$$\mathcal{X} = \sum_{k=0}^{D-1}\left|k+1 \bmod D\right\rangle\left\langle k\right|, \tag{23}$$
$$\omega = e^{j2\pi/D}$$

to encode classic μ, ν "cdits" in the following way:

$$\left|\beta_{h,t}^{(\mu,\nu)}\right\rangle = \mathcal{X}_t^{\mu}\mathcal{Z}_t^{\nu}\left|\beta_{h,t}^{(0,0)}\right\rangle$$
$$= \frac{1}{\sqrt{D}}\sum_{k=0}^{D-1}\omega^{k\nu}\left|k_h\right\rangle\left|\left(k+\mu \bmod D\right)_t\right\rangle. \tag{24}$$

Under attack, Alice applies encoding (24) to the state coupled according to rule (20):

$$\begin{aligned}|\psi_{\text{enc}}\rangle &= \mathcal{X}_t^{\mu}\mathcal{Z}_t^{\nu}\mathcal{Q}\left|\beta_{h,t}^{(0,0)}\right\rangle\left|\alpha_E^{(0)}\right\rangle \\ &= \mathcal{X}_t^{\mu}\mathcal{Z}_t^{\nu}\frac{1}{\sqrt{D}}\sum_{k=0}^{D-1}|k_h\rangle|k_t\rangle\left|a_E^{(k)}\right\rangle \\ &= \frac{1}{\sqrt{D}}\sum_{k=0}^{D-1}\omega^{k\nu}|k_h\rangle|(k+\mu \bmod D)_t\rangle\left|a_E^{(k)}\right\rangle.\end{aligned} \tag{25}$$

The travel qubit is affected by $\mathcal{Q}^{-1}$ in its way back to Bob:

$$\begin{aligned}|\phi_{\text{dec}}\rangle &= \mathcal{Q}^{-1}|\psi_{\text{enc}}\rangle = \frac{1}{\sqrt{D}} \\ &\cdot \sum_{k=0}^{D-1}\omega^{k\nu}|k_h\rangle\left(\mathcal{Q}^{-1}|(k+\mu \bmod D)_t\rangle\left|a_E^{(k)}\right\rangle\right) \\ &= \left\{\frac{1}{\sqrt{D}}\sum_{k=0}^{D-1}\omega^{k\nu}|k_h\rangle|(k+\mu \bmod D)_t\rangle\right\} \\ &\cdot \left|\alpha_E^{(-\mu \bmod D)}\right\rangle.\end{aligned} \tag{26}$$

The expression in curly braces is exactly the state that Bob expects to receive when there is no Eve (see (24)), so eavesdropping also does not affect the message. At the same time, the initial state of the ancilla is moved by μ positions within the set of detection states. As a result, Eve can unambiguously identify the value of cdit μ as long as the detection states are mutually orthogonal.

The $\mathcal{C}_X$ (controlled $\mathcal{X}$) gate seems to be the simplest instance of the attack paradigm. Let the detection and probe sets of states be the elements of the computational basis ($|\alpha_E^{(m)}\rangle = |m_E\rangle, |a_E^{(m)}\rangle = |m_E\rangle$) and the ancilla is composed of the single qudit register. The attack operation $\mathcal{Q}$ can be then implemented as

$$\begin{aligned}\mathcal{Q}|k_t\rangle\left|\alpha_E^{(m)}\right\rangle &= \mathcal{C}_X|k_t\rangle|m_E\rangle = |k_t\rangle\mathcal{X}_E^k|m_E\rangle \\ &= |k_t\rangle|(m+k \bmod D)_E\rangle.\end{aligned} \tag{27}$$

In an obvious way, requirements (21) regarding properties of $\mathcal{Q}$ are then fulfilled.

The existence of attacks able to undetectably eavesdrop on half of the dense coded information has been already forecasted in relation to qubit [2], qutrit [6], and qudit [23] based protocol. However, no explicit form of the attack transformation has been given. The presented result fills in this gap and provides some general guidelines on how to construct coupling transformation with desired properties.

3.4. Control Mode Able to Detect Bit-Flip Eavesdropping. The insecurity of the considered protocol results from inability to detect coupling $\mathcal{Q}_{ht}$ with the control measurements in a single basis. Let us consider a qubit based protocol from Section 2.1 with control mode enhanced to measurements in two bases, namely, computational basis and its dual basis, that is, eigenvectors of $\mathcal{X}$ gate. In the new control mode, Alice randomly selects measurement basis, performs measurement, and asks Bob to make local measurement in the same basis. The control state (9) in the absence of coupling takes the form

$$\begin{aligned}|\psi_{htE}\rangle &= \frac{1}{\sqrt{2}}\left(|0_h\rangle|1_t\rangle + |1_h\rangle|0_t\rangle\right)|\chi_0\rangle \\ &= \frac{1}{\sqrt{2}}\left(|+_h\rangle|+_t\rangle - |-_h\rangle|-_t\rangle\right)|\chi_0\rangle,\end{aligned} \tag{28}$$

where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$ are eigenvectors of $\mathcal{X}$. It follows that legitimate parties expect anticorrelation (correlation) of outcomes in the computational (dual) basis. Under attack undetectable in the computational basis (14), the control equation (15) takes the following form in the dual basis:

$$\begin{aligned}&|\psi_{htE}\rangle \\ &= \frac{1}{2\sqrt{2}}\left\{|+_h\rangle\left(|d_E\rangle - |a_E\rangle\right) + |-_h\rangle\left(|d_E\rangle + |a_E\rangle\right)\right\} \\ &\cdot |+_t\rangle \\ &- \frac{1}{2\sqrt{2}}\left\{|+_h\rangle\left(|d_E\rangle + |a_E\rangle\right) + |-_h\rangle\left(|d_E\rangle - |a_E\rangle\right)\right\} \\ &\cdot |-_t\rangle.\end{aligned} \tag{29}$$

Alice measurement causes the collapse to one of the states in the curly braces. It follows that Bob can obtain ± 1 outcome with equal probability, which in turn renders Eve detectability. If control bases are selected with equal probability, then bit-flip attack is detected with $p_{\text{det}} = 1/4$. The above qualitative discussion addresses bit-flip attack. The more advanced discussion on the properties of control modes based on mutually unbiased bases and in relation to attacks of any form can be found in [23].

4. Conclusion

A generic scheme that provides undetectable eavesdropping of bit-flip operations in the seminal version of the ping-pong protocol is introduced. It can be considered as a generalization of the P-circuit [24], but, in contrast, it is deduced from the very basic properties of the coupling transformation. Moreover, the proposed scheme can be realized without referring to the vacuum states so it is fully consistent with the absence of losses assumption. The CNOT gate and P-circuit are special cases of the introduced scheme so both approaches are equivalent. It follows that any control mode able to detect CNOT coupling is also able to detect the presence of the P-circuit. The control mode based on local measurements in randomly selected unbiased bases is an example of such procedure. Consequently, there is no need for special addressing of P-circuit in the security analyses. Also, the introduced scheme can be adapted to higher dimensional systems. It can be considered as the constructive proof of the existence of attacks forecasted in [2, 6, 23].

Competing Interests

The authors declare that there are no competing interests regarding the publication of this paper.

Acknowledgments

Piotr Zawadzki acknowledges the support from the statutory sources and Jarosław Adam Miszczak was supported by the Polish National Science Center (NCN) under Grant 2011/03/D/ST6/00413.

References

[1] G. L. Long and X. S. Liu, "Theoretically efficient high-capacity quantum-key-distribution scheme," *Physical Review A*, vol. 65, no. 3, Article ID 032302, 2002.

[2] F.-G. Deng, G. L. Long, and X.-S. Liu, "Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block," *Physical Review A*, vol. 68, no. 4, Article ID 042317, 6 pages, 2003.

[3] K. Boström and T. Felbinger, "Deterministic secure direct communication using entanglement," *Physical Review Letters*, vol. 89, no. 18, pp. 187902/1–187902/4, 2002.

[4] C. Wang, F. G. Deng, and G. L. Long, "Multi-step quantum secure direct communication using multi-particle Green-HorneZeilinger state," *Optics Communications*, vol. 253, no. 13, pp. 15–20, 2005.

[5] C. Wang, F. G. Deng, and G. L. Long, "Erratum to 'Multi-step quantum secure direct communication using multi-particle Green-Horne-Zeilinger state' [Opt. Commun. 253 (2005) 15–20]," *Optics Communications*, vol. 262, no. 1, p. 134, 2006.

[6] E. V. Vasiliu, "Non-coherent attack on the ping-pong protocol with completely entangled pairs of qutrits," *Quantum Information Processing*, vol. 10, no. 2, pp. 189–202, 2011.

[7] P. Zawadzki, "Security of ping-pong protocol based on pairs of completely entangled qudits," *Quantum Information Processing*, vol. 11, no. 6, pp. 1419–1430, 2012.

[8] Q.-Y. Cai and B.-W. Li, "Improving the capacity of the Boström-Felbinger protocol," *Physical Review A—Atomic, Molecular, and Optical Physics*, vol. 69, no. 5, Article ID 054301, 2004.

[9] C. Wang, F.-G. Deng, Y.-S. Li, X.-S. Liu, and G. L. Long, "Quantum secure direct communication with high-dimension quantum superdense coding," *Physical Review A*, vol. 71, no. 4, Article ID 044305, 2005.

[10] F.-G. Deng and G. L. Long, "Secure direct communication with a quantum one-time pad," *Physical Review A*, vol. 69, no. 5, Article ID 052319, 2004.

[11] J. Hu, B. Yu, M. Jing et al., Experimental quantum secure direct communication with single photons. LSA, 2016.

[12] M. Lucamarini and S. Mancini, "Secure deterministic communication without entanglement," *Physical Review Letters*, vol. 94, no. 14, Article ID 140501, 2005.

[13] G.-L. Long, F.-G. Deng, C. Wang, X.-H. Li, K. Wen, and W.-Y. Wang, "Quantum secure direct communication and deterministic secure quantum communication," *Frontiers of Physics in China*, vol. 2, no. 3, pp. 251–272, 2007.

[14] K. Boström and T. Felbinger, "On the security of the ping-pong protocol," *Physics Letters A*, vol. 372, no. 22, pp. 3953–3956, 2008.

[15] P. Zawadzki, "Improving security of the ping-pong protocol," *Quantum Information Processing*, vol. 12, no. 1, pp. 149–155, 2013.

[16] H. Lu, C.-H. F. Fung, X. Ma, and Q.-Y. Cai, "Unconditional security proof of a deterministic quantum key distribution with a two-way quantum channel," *Physical Review A—Atomic, Molecular, and Optical Physics*, vol. 84, no. 4, Article ID 042344, 2011.

[17] N. J. Beaudry, M. Lucamarini, S. Mancini, and R. Renner, "Security of two-way quantum key distribution," *Physical Review A*, vol. 88, no. 6, Article ID 062302, 2013.

[18] Y.-G. Han, Z.-Q. Yin, H.-W. Li et al., "Security of modified Ping-Pong protocol in noisy and lossy channel," *Scientific Reports*, vol. 4, article 4936, 2014.

[19] A. Cerè, M. Lucamarini, G. Di Giuseppe, and P. Tombesi, "Experimental test of two-way quantum key distribution in the presence of controlled noise," *Physical Review Letters*, vol. 96, no. 20, Article ID 200501, 2006.

[20] H. Chen, Z.-Y. Zhou, A. J. J. Zangana et al., "Experimental demonstration on the deterministic quantum key distribution based on entangled photons," *Scientific Reports*, vol. 6, Article ID 20962, 2016.

[21] A. Wójcik, "Eavesdropping on the 'ping-pong' quantum communication protocol," *Physical Review Letters*, vol. 90, no. 15, Article ID 157901, 2003.

[22] F.-G. Deng, X.-H. Li, C.-Y. Li, P. Zhou, and H.-Y. Zhou, "Eavesdropping on the 'ping-pong' quantum communication protocol freely in a noise channel," *Chinese Physics*, vol. 16, no. 2, pp. 277–281, 2007.

[23] P. Zawadzki, Z. Pucha la, and J. A. Miszczak, "Increasing the security of the ping-pong protocol by using many mutually unbiased bases," *Quantum Information Processing*, vol. 12, no. 1, pp. 569–576, 2013.

[24] M. Pavičić, "In quantum direct communication an undetectable eavesdropper can always tell Ψ from Φ Bell states in the message mode," *Physical Review A*, vol. 87, no. 4, Article ID 042326, 2013.

[25] B. Zhang, W.-X. Shi, J. Wang, and C.-J. Tang, "Quantum direct communication protocol strengthening against Pavičić's attack," *International Journal of Quantum Information*, vol. 13, no. 7, Article ID 1550052, 2015.

[26] H. E. Brandt, "Entangled eavesdropping in quantum key distribution," *Journal of Modern Optics*, vol. 53, no. 16-17, pp. 2251–2257, 2006.

[27] J. H. Shapiro, "Performance analysis for Brandt's conclusive entangling probe," *Quantum Information Processing*, vol. 5, no. 1, pp. 11–24, 2006.