Journal Name

Crossmark

RECEIVED
dd Month yyyy

REVISED
dd Month yyyy

PAPER

Phase coding semi-quantum key distribution system based on the Single-state protocol

Si-Ying Huang[1], Qin-Cheng Hou[1], Tian-Ming Zhao[2,*], Jin-Dong Wang[1,*], Nai-Da Mo[1], Zheng-Jun Wei[1], Ya-Fei Yu[2] and Zhi-Ming Zhang[3]

[1]Guangdong Provincial Key Laboratory of Quantum Engineering and Quantum Materials, School of Optoelectronic Science and Engineering, South China Normal University, Guangzhou 510006, China
[2]Guangdong Provincial Key Laboratory of Nanophotonic Functional Materials and Devices, School of Optoelectronic Science and Engineering, South China Normal University, Guangzhou 510006, China
[3]Center of Physics Experiments, Guangdong Technology College, Zhaoqing, 526100, China

E-mail: zhaotm@scnu.edu.cn, wangjindong@m.scnu.edu.cn

Keywords: Semi-quantum key distribution, Single-state protocol, Selective modulation

Abstract

Semi-quantum key distribution (SQKD) allows sharing random keys between a quantum user and a classical user, which significantly saves user resources, especially when using the Single-state protocol. However, the operation of the classical user, which involves measurement and resending using the Single-state protocol, presents technical difficulties in experiment and there is a security vulnerability of "tagged" attack in theory. To solve these problems, in our work, based on the Single-state protocol, we propose the "selective modulation" method and successfully implement a phase-encoded semi-quantum key distribution system. The system operates at a frequency of 100MHz and an average photon number of 0.1. The interference contrast achieved 97.45%, the average quantum bit error rate was 1.20%, and the raw key rate reached 88Kbps. Our experimental results demonstrate the feasibility and stability of the proposed phase-encoded SQKD system. Furthermore, we conducted an analysis of the "selective modulation" scheme in terms of quantum state evolution to assess the security of our system and ultimately proved that it can resist "tagged" attack. The classical user of our system requires only two optical devices and operates without relying on full quantum capabilities, thereby enhancing its application potential in quantum networks. This work validates the feasibility of SQKD experiments and provides ideas for future research on SQKD experiments and security studies.

1 Introduction

Quantum key distribution (QKD) allows the sharing of a string of random keys between legitimate users, with security guarantees provided by the principles of quantum mechanics: eavesdropping on the key distribution process will be detected. Currently, QKD has reached the stage of practical application, and its application over fiber and free space has been validated by numerous experiments [1–8]. In 2007, Boyer et al. proposed the concept of semi-quantum key distribution (SQKD) [9], and this is called the BKM07 protocol. SQKD allows one party to perform only classical operations, thereby reducing the quantum resource requirement in the key distribution process. If SQKD can reduce the requirements for quantum resources, then it will have unique application prospects and value. Since 2007, various semi-quantum key distribution protocols have been proposed [10–17]. In 2009, Boyer et al. further based on randomized SQKD protocol and measuring retransmitting the SQKD, proved their robustness [10], and Zou et al. proposed the Single-state protocol [17]. The Single-state protocol prepares only one quantum state, which holds a higher application value. Subsequently, the semi-quantum model expanded into areas such as quantum secret sharing (QSS) [18, 19], quantum secure direct communication (QSDC) [20], quantum key agreement (QKA) [21], and quantum authentication [22], evolving into semi-quantum cryptography. Regarding the security of SQKD, Boyer et al. introduced the concept of robustness [9]. In 2014, Krawec et al. pointed out that collective attacks in single-state SQKD can be regarded as restricted attacks [23]. In 2018, the security of Single-state SQKD protocols was

proven [24]. In 2022, Mi et al. conducted a security analysis on the Photon-Number Splitting (PNS) attack problem caused by multi-photon pulses in semi-quantum protocols [25]. In 2023, Dong et al. proposed a decoy state construction scheme for the four-state SQKD protocol [26].

The theoretical research of SQKD has been continuously studied since BKM07 was proposed. However, the experimental research of SQKD has faced a great challenge. SQKD requires the classical party to perform two types of classical operations: CTRL, which directly sends back photons, and SIFT, which measures and resends photons. Implementing the SIFT operation is difficult and vulnerable to the "tagged" attack, which can distinguish classical operations. This challenge has led to slow progress in SQKD experiments. In 2012, Boyer et al. proposed the Mirror protocol [11]. In 2021, Han et al. used time-phase encoding and the "selective modulation" method to implement the classical party's operations in the Mirror protocol, completing the first principal demonstration of SQKD [27]. The demonstration of the Mirror protocol prompted us to consider whether the "selective modulation" method could be applied to other protocols, such as the Single-state protocol, and to provide a security analysis of the method. In 2024, Mo et al. completed the principle verification of Single-state protocol on the free space channel by polarization dimension, and the security of "selective modulation" is proved [28]. However, the Single-state protocol on the fiber channel has not yet been verified. Therefore, we developed a phase-encoded optical system based on the Single-state protocol and verified its feasibility using the "selective modulation" method. Our system avoids the problem of measuring and retransmitting photons, maintains good stability, and improves the utilization efficiency of photons. To evaluate the security of the system, we conducted a security analysis of the "selective modulation" method in the system scheme and proved that it is resistant to "tagged" attack. Our system represents a new application of the selective modulation method in SQKD. Moreover, the security analysis has for the first time demonstrated the security of the "selective modulation" method.

The remainder of this paper is organized as follows: In Sec.2, the Single-state protocol is briefly introduced. In Sec.3, we propose the phase encoding semi-quantum key distribution based on the Single-state protocol, and then the experiment and results are described in detail in Sec.4. In Sec.5, we conducted a security analysis of the selective modulation used in this paper. We conclude in Sec.6.

2 The Single-state protocol

Since this paper focuses on the Single-state protocol, we briefly introduce it. In the Single-state protocol, Bob only needs to prepare one state, which greatly reduces the preparation difficulty of the quantum user. The protocol process is as follows: Bob prepares a quantum bit in the $|+\rangle$ state and sends it to Alice. Alice randomly chooses one of two classical operations upon receiving the quantum bit: (1) CTRL: returns the received quantum bit directly; (2) SIFT: measures the received quantum bit in Z basis, prepares the same quantum bit as her measured result, and sends it back to Bob. Bob randomly chooses to measure the returned quantum bit in either the Z basis or the X basis. Bob announces his measurement basis choice, and Alice announces her operation. As a result: If Alice chooses SIFT and Bob chooses Z-basis measurement, the resulting bits are named SIFT-Z bit. These bits contain information exchanged between Alice and Bob and can be used as the raw key. If Alice chooses CTRL and Bob chooses X-basis measurement, the resulting bits are named CTRL-X bits. Bob checks the error rate of the CTRL-X bits, and if the error rate exceeds the set threshold, the protocol is terminated. Furthermore, Alice and Bob choose a portion of the SIFT-Z bits to check the error rate. If the error rate of this portion of bits is higher than the set threshold, the protocol is terminated. Finally, Alice and Bob use the remaining SIFT-Z bits as information bits (INFO bits).

Although the Single-state protocol can reduce the difficulty of state preparation, it still requires Alice to measure and resend photons, making it susceptible to the "tagged" attack [29] and difficult to achieve in the experiment. The protocol process indicates that measurements at Alice are used only for randomly generating information bits, rather than for eavesdropping detection. This leads us to consider whether the "selective modulation" method can be employed in the Single-state protocol to mitigate the security concerns arising from measuring and resending photons. "Selective modulation" [27, 28] means that instead of using measurement and resending for SIFT operation in the classical user, the state is directly modulated, and CTRL is still directly returned. The work on this paper is based on the above considerations.

3 The phase encoding semi-quantum key distribution based on the Single-state protocol

Based on the Single-state protocol, our SQKD system employs phase encoding, in which both encoding and decoding are achieved by modulating the phase difference between two pulses. Here, we define Z basis as the phase difference between two pulses being 0 or π. Conversely, we define X basis as the phase difference between two pulses being $\frac{\pi}{2}$ or $\frac{3\pi}{2}$. Quantum states under each basis are illustrated in Fig. 1, where $|01\rangle$ and $|10\rangle$ represent photons in distinct time bins under the Fock state.

Basis	bit	State	
Z	1	$\|0\rangle = \|01\rangle + \|10\rangle$	$\Delta\varphi = 0$
Z	0	$\|1\rangle = \|01\rangle - \|10\rangle$	$\Delta\varphi = \pi$
X	0	$\|+\rangle = \|01\rangle + i\|10\rangle$	$\Delta\varphi = \frac{\pi}{2}$
X	1	$\|-\rangle = \|01\rangle - i\|10\rangle$	$\Delta\varphi = \frac{3\pi}{2}$

Figure 1. Phase encoding of the states.

The scheme of phase encoding semi-quantum key distribution is illustrated in Fig. 2. Bob prepares and sends the quantum bit $|+\rangle$ by using an asymmetric Mach-Zehnder interferometer (AMZI) and PM1. Upon receiving the quantum bit, Alice randomly selects one of two classical operations: CTRL: directly returns the received quantum bit; SIFT: selectively modulates the received quantum bit by PM2. For SIFT(0), Alice applies $\frac{\pi}{2}$ phase modulation, transforming the quantum state to $|0\rangle$. For SIFT(1), Alice applies $-\frac{\pi}{2}$ phase modulation, transforming the quantum state to $|1\rangle$. After selective modulation, Alice sends the quantum bit back to Bob. Bob randomly chooses to measure the quantum bit using either the X basis or the Z basis. When measuring in the X basis, Bob's phase modulator applies either $\frac{\pi}{2}$ or $-\frac{\pi}{2}$ phase modulation. When measuring in the Z basis, Bob set the voltage of the phase modulator to 0. When the photon reaches the polarization maintaining beam splitter (PMBS), interference occurs. Then the photon will enter different single-photon detectors based on the phase difference. The relationship between the response of the single-photon detectors and the operation of both Alice and Bob is depicted in Fig. 3. Only the cases where Alice's chosen operation and Bob's chosen basis are compatible are presented here.

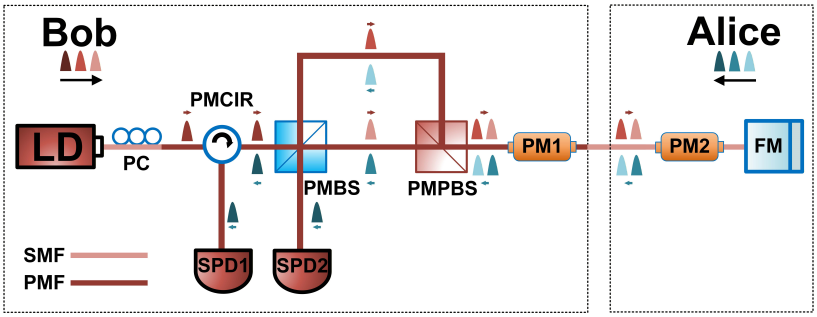

Figure 2. The scheme of phase encoding semi-quantum key distribution. LD: laser diode, PC: polarization controller, PMCIR: polarization maintaining circulator, PMBS: polarization maintaining beam splitter, PMPBS: polarization maintaining polarization beam splitter, PMs(PM1 and PM2): phase modulator, FM: faraday mirror, SPDs (SPD1 and SPD2): single-photon detectors, SMF: single mode fiber, PMF: polarization maintaining fiber. The reddish-brown envelope indicates the forward-transmitted light pulse, that is, from Bob to Alice. The blue-green envelope indicates the backward-transmitted light pulse, that is, from Alice back to Bob.

Bob sends |+>	Alice's operation	Bob's decoding base	Phase difference	Bob receives state	Response of SPDs	Function
$\pi/2$	CTRL \	X $\pi/2$	π	$\|+\rangle$	1 max 2 min	Error detection
$\pi/2$	SIFT(0) $\pi/2$	Z 0	π	$\|0\rangle$	1 max 2 min	Bit 0
$\pi/2$	SIFT(1) $-\pi/2$	Z 0	0	$\|1\rangle$	1 min 2 max	Bit 1

Figure 3. The relationship between Alice and Bob's operations and the response of the single photon detector. $\begin{matrix}\text{CTRL}\\ \backslash\end{matrix}$ indicates that Alice selects CTRL operation, while PM does not apply voltage. $\begin{matrix}\text{SIFT}(0)\\ \pi/2\end{matrix}$ indicates that Alice selects SIFT(0) operation, by changing the phase $\pi/2$ on PM. $\begin{matrix}\text{X}\\ \pi/2\end{matrix}$ indicates that Bob selects X basis, by changing the phase $\pi/2$ on PM.

4 Experiment and Results

4.1 Experimental setup

According to the previously described scheme, the experimental setup in this article is illustrated in Fig. 4. On Bob's module, the setup comprises four modules: a laser source, an AMZI, phase modulation, and detectors. In the source section, light pulses are generated by a picosecond laser diode (LD). The pulse width of the light pulses is 50ps, and the system frequency is 100MHz. The PC and the PMPBS1 are used to adjust the polarization state of the light pulses and align them with the slow axis of the polarization-maintaining fiber. In the AMZI section, the PMCIR is used to transmit the forward light pulses to the 50:50 PMBS and separate the backward light pulses to the single-photon detectors (SPDs). The PMBS, along with PMPBS2, forms the AMZI. The phase modulation section consists of two polarization-independent phase modulators (PM1, PM2), which modulate the forward and backward light pulses. A signal source (SS1) drives the phase modulators. The detection frequency of SPDs is 100 MHz. The clock synchronization of the LD, SPDs, and SS1 is achieved by a digital generator (DG).

On Alice's module, the setup consists of a polarization-independent phase modulator (PM3) and a Faraday mirror. The phase modulator is driven by SS2.

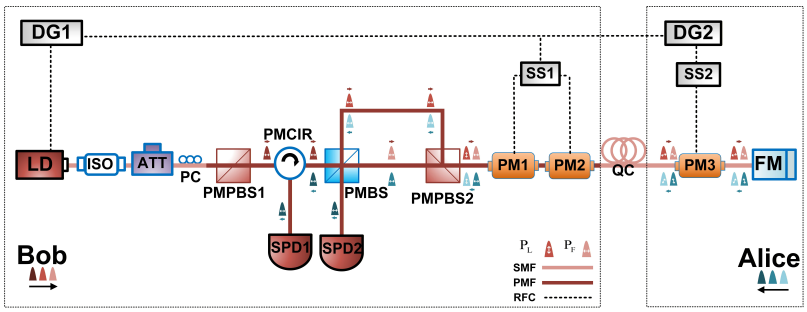

Figure 4. Experimental setup of phase encoding semi-quantum key distribution based on Single-state protocol. ATT: attenuator, QC: quantum channel, DG: digital generator, SS: signal source, RFC: radio frequency cable.

Based on the previous description, to implement classical operations in SQKD, we employ a "selective modulation" method in our scheme instead of the "original measure-and-resend" method. In the AMZI, we introduce a delay of 2.9ns between the two pulses for the arm length difference. The two light pulses are separated by AMZI and propagate along the fast axis and slow axis of the polarization-maintaining fiber respectively. For simplicity, we will refer to them as P_F and P_L. When the pulses arrive at Alice, Alice selectively modulates P_L using her phase modulator (PM3). When the pulses are reflected back to Bob, Bob modulates the pulses using his phase modulator (PM2). Due to the Faraday rotation conjugate effect, the polarization of pulse will rotate by 90°. Consequently, both P_F and P_L will return to the PMBS simultaneously and undergo interference. Finally, depending on the phase difference, the pulses will be detected by either SPD1 or SPD2.

The "selective modulation" operation is described in detail below: Bob sends light pulses. A

pulse signal with a repetition frequency of 100MHz generated by SS1, drives the phase modulator PM1. Then the PM1 consistently applies $\frac{\pi}{2}$ phase modulation on P_L. If Alice chooses CTRL, she does not drive the phase modulator, and the light pulse will be reflected to Bob directly. If Alice chooses SIFT(0), she applies $\frac{\pi}{2}$ phase modulation on P_L. In this situation, PM3 is driven by a pulse signal with a repetition frequency of 100MHz, generated from SS2. If Alice chooses SIFT(1), she applies $-\frac{\pi}{2}$ phase modulation on P_L, achieved by changing the signal polarity. In order not to disrupt the Faraday effect, Alice needs to modulate the forward and backward pulses in the same way twice. This can be achieved by controlling the length of the fiber between PM3 and FM.

When the pulses return to Bob, he randomly chooses to measure them in either the Z basis or the X basis. If Bob chooses the Z basis measurement, he drives PM2 with a voltage of 0. If Bob chooses the X measurement, he applies $\frac{\pi}{2}$ phase modulation to P_F. In this case, PM2 is driven by a pulse signal with a repetition frequency of 100MHz, generated by SS2. Here, in order to avoid the inconsistency in the detection efficiency and to balance the response counts of the two detectors, we further perform $-\frac{\pi}{2}$ phase modulation on P_f. In our system, Bob employs two phase modulators to achieve encoding and decoding functions, aiming to reduce modulation complexity. In future practical applications, through optimizing system design and improving the accuracy of electrical signals, it will be possible to achieve the aforementioned functions with only one phase modulator.

If Alice chooses the SIFT(0) operation and Bob chooses the Z basis measurement, the light pulse will reverse into PMCIR and then into SPD1 because of the interference of PMBS. If Alice chooses the SIFT(1) operation and Bob chooses the Z basis measurement, the light pulse will enter SPD2. If Alice chooses the CTRL operation and Bob chooses the X measurement, the pulse will enter SPD2.

4.2 Results and discussion

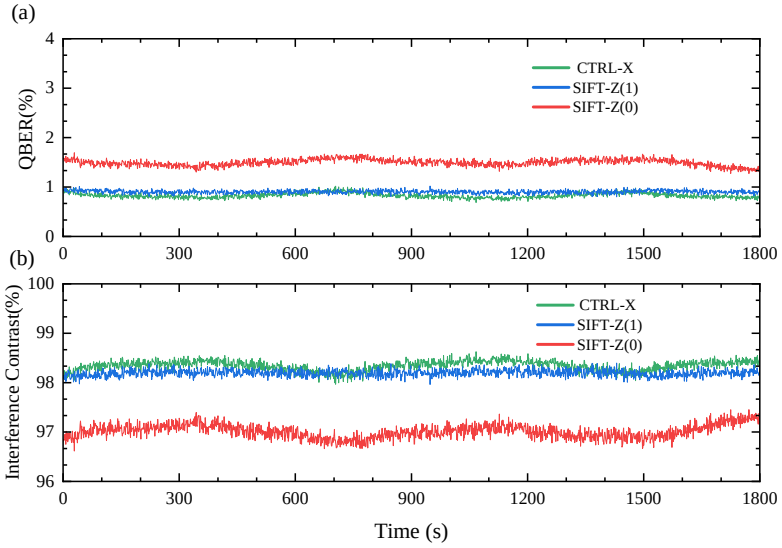

Figure 5. (a) The change of error rate within 30 minutes. (b) The change of interference contrast within 30 minutes.

According to the system design and experimental settings described earlier, to evaluate the system performance, we collected the response results of the SPDs over a 30-minute period. The overall error rate and interference contrast of each base within 30 minutes are as follows: CTRL-X: average error rate is 0.82%, interference contrast is 98.35%, and average response rate is 0.92%; SIFT-Z: average error rate is 1.20%, interference contrast is 97.45%, and average response rate is 0.90%. The change of error rate within 30 minutes is shown in Fig. 5(a), and the change of interference contrast is shown in Fig. 5(b). Overall, it is evident that the interference contrast and error rate of our system are maintained at a stable level. With an average number of photons per pulse of 0.1, the raw key rate reaches 88Kbps, representing a significant improvement over the other experimental schemes [27,28] in the field of semi-quantum key distribution. The experimental results validate the feasibility and stability of the phase encoding semi-quantum key distribution based on the Single-state protocol.

Notably, when the phase difference between light pulses is π, the response rate, error rate, and interference contrast have a slight decline compared to when the phase difference is 0. This discrepancy arises because at a phase difference of π, photons will be output from port 3 of the

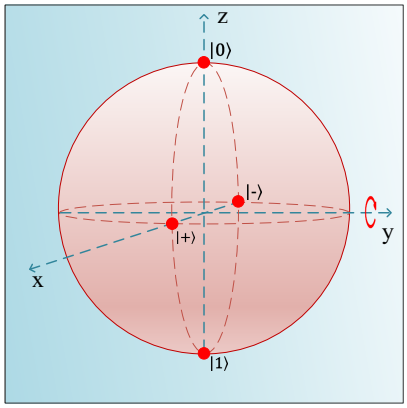

Figure 6. Quantum states on the Bloch sphere.

PMCIR, while there is a 0.39 dB attenuation from port 2 to port 3. Therefore, although detectors with similar detection efficiencies were selected for our system, the attenuation introduced by the PMCIR results in certain discrepancies in the output results at both ends, resulting in an increase in overall error rate.

5 Security proof

A security analysis is essential as this paper employs "selective modulation" instead of the original measurement-resend operation. Here, we demonstrate that if Eve attacks quantum states to obtain key information during the distribution process, errors will inevitably arise and be detected by Alice and Bob. Initially, Bob prepares the qubit state $|+\rangle_B$ and sends them one by one to Alice, sending the next quantum bit only after receiving the photon. As depicted in Fig. 1, $|+\rangle_B$ can be represented as:

$$|+\rangle_B = \frac{1+i}{2}|0\rangle_B + \frac{1-i}{2}|1\rangle_B. \tag{1}$$

It means the $|+\rangle_B$, $|0\rangle_B$ and $|1\rangle_B$ can be defined as poles on the equator of Bloch sphere (as shown in Fig. 6). To describe more clearly and without loss of generality, we rewrite Eq. (1) as follows:

$$|+\rangle_B = \frac{1}{\sqrt{2}}\left(|0\rangle_B + |1\rangle_B\right), \tag{2}$$

which does not change the relationships between each state and the subsequent analysis results.

Now, we are modeling the "selective modulation" method. When Alice performs selective modulation on the received quantum state, choosing the CTRL operation is equivalent to applying the identity operator $\hat{I}_A$ to the quantum state. When Alice chooses the SIFT operation, she randomly rotates $|+\rangle$ to either $|0\rangle$ or $|1\rangle$, corresponding to rotating the quantum state around the y-axis of the Bloch sphere counterclockwise by 90 ° or clockwise by 90 ° (Fig. 6). Therefore, the selective modulation process in this paper can be fully represented by a unitary operator corresponding to rotation around the y-axis, as shown in Eq. (3), where δ represents the angle of counterclockwise rotation around the y-axis for the quantum state:

$$\hat{R}_y(\delta) = \begin{bmatrix} \cos\frac{\delta}{2} & -\sin\frac{\delta}{2} \\ \sin\frac{\delta}{2} & \cos\frac{\delta}{2} \end{bmatrix}. \tag{3}$$

Because the classic user Alice can only perform quantum state operations on the Z basis, and only uses CTRL to return the state to the quantum user Bob in the X basis, therefore, here we define the range $\delta \in \left\{-\frac{\pi}{2}, \frac{\pi}{2}\right\}$. Thus, the selective modulation process for any quantum state in this system can be represented as:

$$\hat{S}_0 = \hat{R}_y\left(-\tfrac{\pi}{2}\right), \tag{4}$$

$$\hat{S}_1 = \hat{R}_y\left(\tfrac{\pi}{2}\right), \tag{5}$$

Where $\hat{S}_0$ represents the SIFT(0) operation, and $\hat{S}_1$ represents the SIFT(1) operation. Note that the unitary operator in Eq.(3) represents an equivalent input–output map of the SIFT process, rather than a physically implemented quantum gate by Alice. Hadamard operation realizes the mapping of bases $H|0\rangle = |+\rangle$, $H|1\rangle = |-\rangle$. But the selective modulation is $\hat{R}_y(\delta)$, $\delta \in \left\{-\frac{\pi}{2}, \frac{\pi}{2}\right\}$. Therefore, $\hat{R}_y\left(\pm\frac{\pi}{2}\right)|+\rangle = |0\rangle$ or $|1\rangle$. Alice has never mapped the Z-basis state back to the X-basis state and lacks the ability to generate $|-\rangle$ thus does not possess the complete BB84 preparation capability. So, we define Alice as a classical user.

To attack quantum states, Eve use two unitary operators $\hat{U}_F$ and $\hat{U}_R$ to perform attack on $|\phi\rangle_B$. $\hat{U}_F$ is acts on the $|\phi\rangle_B$ in forward channel and Eve's ancilla state $|\chi\rangle_E$ ($|\chi\rangle_E \in \mathcal{H}_E$,$\mathcal{H}_E$ is the two-dimensional Hilbert space corresponding to Eve's probe state). $\hat{U}_R$ is acts on the $|\phi\rangle_B$ in backwards channel and Eve's ancilla state $|\chi\rangle_E$. In forward channel, the attack $\hat{U}_F$ can be defined as follow:

$$\hat{U}_F\left(|0\rangle_B|\chi\rangle_E\right) = |0\rangle_B|\chi_{00}\rangle + |1\rangle_B|\chi_{01}\rangle, \tag{6}$$

$$\hat{U}_F\left(|1\rangle_B|\chi\rangle_E\right) = |0\rangle_B|\chi_{10}\rangle + |1\rangle_B|\chi_{11}\rangle. \tag{7}$$

Therefore, after executing the attack $\hat{U}_F$, the states held by Bob and Eve can be represented as:

$$\begin{aligned}\hat{U}_F\left(|+\rangle_B|\chi\rangle_E\right) &= \hat{U}_F\left[\tfrac{1}{\sqrt{2}}\left(|0\rangle_B + |1\rangle_B\right)|\chi\rangle_E\right] \\ &= \tfrac{1}{\sqrt{2}}\left(|0\rangle_B|\chi_{00}\rangle + |1\rangle_B|\chi_{01}\rangle + |0\rangle_B|\chi_{10}\rangle + |1\rangle_B|\chi_{11}\rangle\right).\end{aligned} \tag{8}$$

When Alice chooses the CTRL operation, the states held by Bob and Eve can still be represented as Eq.(8). When Alice chooses the SIFT(0) operation, the states held by Alice, Bob, and Eve can be represented as:

$$\begin{aligned}|\psi\rangle_{A_0B}|\chi\rangle_E &= |0\rangle_A \otimes \hat{S}_0\hat{U}_F\left(|+\rangle_B|\chi\rangle_E\right) \\ = \tfrac{1}{2}\left(|00\rangle_{AB}|\chi_{00}\rangle - |01\rangle_{AB}|\chi_{00}\rangle + |00\rangle_{AB}|\chi_{01}\rangle + |01\rangle_{AB}|\chi_{01}\rangle + |00\rangle_{AB}|\chi_{10}\rangle - |01\rangle_{AB}|\chi_{10}\rangle\right. \\ \left. + |00\rangle_{AB}|\chi_{11}\rangle + |01\rangle_{AB}|\chi_{11}\rangle\right).\end{aligned} \tag{9}$$

When Alice chooses the SIFT(1) operation, the states held by Alice, Bob, and Eve can be represented as:

$$\begin{aligned}|\psi\rangle_{A_1B}|\chi\rangle_E &= |1\rangle_A \otimes \hat{S}_1\hat{U}_F\left(|+\rangle_B|\chi\rangle_E\right) \\ = \tfrac{1}{2}\left(|10\rangle_{AB}|\chi_{00}\rangle + |11\rangle_{AB}|\chi_{00}\rangle - |10\rangle_{AB}|\chi_{01}\rangle + |11\rangle_{AB}|\chi_{01}\rangle + |10\rangle_{AB}|\chi_{10}\rangle + |11\rangle_{AB}|\chi_{10}\rangle\right. \\ \left. - |10\rangle_{AB}|\chi_{11}\rangle + |11\rangle_{AB}|\chi_{11}\rangle\right).\end{aligned} \tag{10}$$

After Alice performs selective modulation, Eve implements an attack $\hat{U}_R$ on the quantum state of the backward channel. The final quantum state of Alice 's chosen CTRL is:

$$\begin{aligned}|\psi\rangle_B|\chi_{final}\rangle_E &= \hat{U}_R\hat{U}_F\left(|+\rangle_B|\chi\rangle_E\right) \\ = \tfrac{1}{\sqrt{2}}\left(|0\rangle_B|\chi_{0000}\rangle + |1\rangle_B|\chi_{0001}\rangle + |0\rangle_B|\chi_{0110}\rangle + |1\rangle_B|\chi_{0111}\rangle + |0\rangle_B|\chi_{1000}\rangle\right. \\ \left. + |1\rangle_B|\chi_{1001}\rangle + |0\rangle_B|\chi_{1110}\rangle + |1\rangle_B|\chi_{1111}\rangle\right).\end{aligned} \tag{11}$$

If Eve introduces no errors on the CTRL-X bit, which means the measurement result state in Bob could not be $|-\rangle$, there should be:

$$|\chi_{0000}\rangle + |\chi_{0110}\rangle + |\chi_{1000}\rangle + |\chi_{1110}\rangle = |\chi_{0001}\rangle + |\chi_{0111}\rangle + |\chi_{1001}\rangle + |\chi_{1111}\rangle. \tag{12}$$

The final quantum state of Alice 's chosen SIFT(0) is:

$$\begin{aligned}\hat{U}_R\left(|\psi\rangle_{A_0B}|\chi\rangle_E\right) = \tfrac{1}{2}\left(|00\rangle_{AB}|\chi_{0000}\rangle + |01\rangle_{AB}|\chi_{0001}\rangle - |00\rangle_{AB}|\chi_{0010}\rangle - |01\rangle_{AB}|\chi_{0011}\rangle\right. \\ + |00\rangle_{AB}|\chi_{0100}\rangle + |01\rangle_{AB}|\chi_{0101}\rangle + |00\rangle_{AB}|\chi_{0110}\rangle + |01\rangle_{AB}|\chi_{0111}\rangle + |00\rangle_{BA}|\chi_{1000}\rangle + |01\rangle_{BA}|\chi_{1001}\rangle \\ \left. - |00\rangle_{BA}|\chi_{1010}\rangle - |01\rangle_{BA}|\chi_{1011}\rangle + |00\rangle_{BA}|\chi_{1100}\rangle + |01\rangle_{BA}|\chi_{1101}\rangle + |00\rangle_{BA}|\chi_{1110}\rangle + |01\rangle_{BA}|\chi_{1111}\rangle\right).\end{aligned} \tag{13}$$

The final quantum state of Alice 's chosen SIFT(1) is:

$$\begin{aligned}\hat{U}_R\left(|\psi\rangle_{A_1B}|\chi\rangle_E\right) = \tfrac{1}{2}\left(|10\rangle_{AB}|\chi_{0000}\rangle + |11\rangle_{AB}|\chi_{0001}\rangle + |10\rangle_{AB}|\chi_{0010}\rangle + |11\rangle_{AB}|\chi_{0011}\rangle\right.\\ -|10\rangle_{AB}|\chi_{0100}\rangle - |11\rangle_{AB}|\chi_{0101}\rangle + |10\rangle_{AB}|\chi_{0110}\rangle + |11\rangle_{AB}|\chi_{0111}\rangle + |10\rangle_{BA}|\chi_{1000}\rangle + |11\rangle_{BA}|\chi_{1001}\rangle\\ \left.+|10\rangle_{BA}|\chi_{1010}\rangle + |11\rangle_{BA}|\chi_{1011}\rangle - |10\rangle_{BA}|\chi_{1100}\rangle - |11\rangle_{BA}|\chi_{1101}\rangle + |10\rangle_{BA}|\chi_{1110}\rangle + |11\rangle_{BA}|\chi_{1111}\rangle\right).\end{aligned} \tag{14}$$

If Eve introduces no errors on the SIFT-Z bit, there should be:

$$\begin{aligned}&|\chi_{0000}\rangle = |\chi_{0001}\rangle = |\chi_{0010}\rangle = |\chi_{0011}\rangle = |\chi_{0100}\rangle = |\chi_{0101}\rangle = |\chi_{0110}\rangle = |\chi_{0111}\rangle\\ &= |\chi_{1000}\rangle = |\chi_{1001}\rangle = |\chi_{1010}\rangle = |\chi_{1011}\rangle = |\chi_{1100}\rangle = |\chi_{1101}\rangle = |\chi_{1110}\rangle = |\chi_{1111}\rangle = 0.\end{aligned} \tag{15}$$

Therefore, without introducing errors, Eve cannot obtain any information about the key. In the above proof, the analysis of the CTRL bit was not conducted. It can be easily proven that if Eq.(15) holds, then Eq.(12) is also satisfied simultaneously. However, this does not imply that the CTRL operation in this system can be ignored. The proof of the CTRL operation see Appendix B. All in all, if Eve attacks the quantum states during the key distribution process to obtain key information, errors would inevitably be introduced into the quantum states of both Alice and Bob, leading to detection. Thus, the design proposed in this paper, based on the "selective modulation", is completely robust against attacks targeting quantum states.

6 Conclusion

We propose a phase-encoding semi-quantum key distribution system based on the Single-state protocol. By applying the "selective modulation" method, classical users do not need to measure or retransmit the photons. We have established a semi-quantum key distribution system with a frequency of 100 MHz. Compared with previous experiments, notable enhancements are observed in experimental metrics, including an interference contrast of 97.45%, an average quantum bit error rate of 1.20%, and a raw key rate of 88Kbps, validating the feasibility and stability of our system through experimentation. The classical user of our system requires only two optical devices, significantly reducing equipment requirements and enhancing its potential for widespread application. Furthermore, we have theoretically demonstrated the security of selective modulation against marking attacks, and have shown the robustness of our system in resisting quantum state attacks. This research is a novel application of the selective modulation method in SQKD and gives a comprehensive theoretical description of the method. Additionally, the classical end design proposed in this paper is simplified, which is expected to fully leverage the potential of SQKD in quantum networks, achieving low-cost and secure key distribution.

Acknowledgments

This work was supported by Natural Science Foundation of Guangdong Province 2024A1515012427, by National Nature Science Foundation of China 62371199, 62071186, and 61771205, and by Guangdong Provincial Key Laboratory of Construction Foundation 2020B1212060066.

Data availability

The data that support the findings of this study are available from the corresponding author upon reasonable request.

Supplementary data

Appendix A: Experimental setup details

On Bob's module, the setup comprises four modules: a laser source, an AMZI, phase modulation, and detectors. In the laser source section, laser pulses are generated by a picosecond laser (LD, produced by Qasky, WT-LD100-D). The pulse width of the laser pulses is 50ps, and the system frequency is 100MHz. The isolator (ISO) is used to prevent reflected light from entering the laser. An attenuator (Att) is utilized to attenuate the average photon number per pulse of light pulses to 0.1. The PC and the PMPBS1 are employed to adjust the polarization state of the light pulses and align them with the slow axis of the polarization-maintaining fiber. In the asymmetric Mach-Zehnder interferometer section, the PMCIR is used to transmit the forward light pulses to the 50:50 PMBS and separate the backward light pulses to the detectors. The PMBS, along with

PMPBS2, forms the asymmetric Mach-Zehnder interferometer section. The phase modulation section consists of two polarization-independent phase modulators (PM1, PM2, produced by iXblue, MPZ-LN-10-P-P-FA-FA), which modulate the forward and backward light pulses. A signal source (SS1, produced by SIGLENT, SDG6052X-E) drives the phase modulators. The detector section comprises two single-photon detectors (SPD, produced by Qasky, WT-SPD300-ULN), with a detection frequency of 100MHz. SPD1 is connected to the PMCIR port3, while SPD2 is connected to PMBS. The clock synchronization between the laser, detectors, and SS is achieved using a digital generator (DG, produced by Qasky, WT-HGCG200).

On Alice's module, the setup consists of a polarization-independent phase modulator (PM3, produced by KANGGUAN, KG-SM-15-10G-PP-FP) and a Faraday mirror. The phase modulator is driven by SS (SS2, produced by SIGLENT, SDG6052X-E).

In the AMZI section, we introduce a delay of 2.9ns between the two pulses due to the arm length difference. Due to the action of PMPBS, the two light pulses will propagate along the fast axis and slow axis of the polarization-maintaining fiber, respectively. For simplicity, we will refer to them as P_F and P_L. When the pulses arrive at Alice's module, Alice selectively modulates P_L using her phase modulator. When the pulses are reflected back to Bob, Bob modulates the pulses using his phase modulator. Due to the Faraday rotation conjugate effect, the polarization of pulse will rotate by 90°. Consequently, both P_F and P_L will return to the polarization-maintaining beam splitter (PMBS) simultaneously and undergo interference. Ultimately, depending on the phase difference, the pulses will be detected by either SPD1 or SPD2.

The "selective modulation" operation in this paper is described in detail below. Bob sends light pulses. A pulse signal with a repetition frequency of 100MHz and a voltage of 2.95V, generated by SS1, drives the phase modulator PM1. Then the PM1 consistently applies $\frac{\pi}{2}$ phase modulation on P_L. If Alice chooses CTRL, she does not apply voltage to the phase modulator, and the light pulse will be reflected to Bob directly. If Alice chooses SIFT(0), she applies $\frac{\pi}{2}$ phase modulation on P_L. In this circumstance, PM3 is driven by a pulse signal with a repetition frequency of 100MHz and a voltage of 2.01V, generated from SS2. If Alice chooses SIFT(1), she applies $-\frac{\pi}{2}$ phase modulation on P_L. In this circumstance, PM3 is driven by a pulse signal with a repetition frequency of 100MHz and a voltage of -1.78V (achieved by changing the signal polarity). To maintain the Faraday effect, Alice needs to modulate the forward and backward pulses twice in the same manner, which can be ensured by controlling the length of the fiber between PM3 and FM. Due to the identical modulation twice, the required voltage for applying $\frac{\pi}{2}$ phase modulation is correspondingly reduced.

When the pulses return to Bob, he randomly chooses to measure them in either the Z basis or the X basis. If Bob chooses the Z basis measurement, he drives PM2 with a voltage of 0. If Bob chooses the X measurement, he applies $\frac{\pi}{2}$ phase modulation to P_F. In this case, PM2 is driven by a pulse signal with a repetition frequency of 100MHz and a voltage of 2.81V, generated by SS2.

The experiment employed two InGaAs/InP single-photon detectors (produced by Qasky, WT-SPD300-ULN), with a detection gate width of 1ns, a detection frequency of 100MHz, a dark count probability per gate of 3×10^{-6}, a dead time of 5ns, and an approximate detection efficiency of 20.5%.

Appendix B: Proof of the CTRL operation

Here we will demonstrate the necessity of the CTRL operation for ensuring the security of this system. We will use an example where Eve only attacks the backward channel, which can be seen as a special case of Eve implementing a two-way attack. Since Eve only attacks the backward channel, $\hat{U}_F$ can be regarded as the identity operator $\hat{I}_E$ in the previous analysis. Therefore, the states held by Bob can be represented as:

$$|\psi\rangle_B = \frac{1}{\sqrt{2}} \left(|0\rangle_B + |1\rangle_B\right). \tag{B.1}$$

When Alice chooses the SIFT(0) operation, the states held by Alice, Bob can be represented as:

$$|\psi\rangle_{A_0B} = |0\rangle_A \otimes \hat{S}_0|+\rangle_B = |00\rangle_{AB}. \tag{B.2}$$

When Alice chooses the SIFT(1) operation, the states held by Alice, Bob can be represented as:

$$|\psi\rangle_{A_1B} = |1\rangle_A \otimes \hat{S}_1|+\rangle_B = |11\rangle_{AB}. \tag{B.3}$$

After Alice performs selective modulation, Eve implements an attack $\hat{U}_R$ on the quantum state of the backward channel. The final quantum state of Alice 's chosen CTRL is:

$$\hat{U}_R \left(|\psi\rangle_B |\chi\rangle_E\right) = \tfrac{1}{\sqrt{2}} \left(|0\rangle_B |\chi_{00}\rangle + |1\rangle_B |\chi_{01}\rangle + |0\rangle_B |\chi_{10}\rangle + |1\rangle_B |\chi_{11}\rangle\right). \tag{B.4}$$

The final quantum state of Alice 's chosen SIFT(0) is:

$$\hat{U}_R\left(|\psi\rangle_{A_0B}|\chi\rangle_E\right) = \hat{U}_R\left(|00\rangle_{AB}|\chi\rangle_E\right) = |00\rangle_{AB}|\chi_{00}\rangle + |01\rangle_{AB}|\chi_{01}\rangle\,. \tag{B.5}$$

The final quantum state of Alice 's chosen SIFT(1) is:

$$\hat{U}_R\left(|\psi\rangle_{A_1B}|\chi\rangle_E\right) = \hat{U}_R|11\rangle_{AB}|\chi\rangle_E = |10\rangle_{AB}|\chi_{10}\rangle + |11\rangle_{AB}|\chi_{11}\rangle\,. \tag{B.6}$$

If Eve introduces no errors on the SIFT-Z bit, there should be:

$$|\chi_{01}\rangle = |\chi_{10}\rangle = 0. \tag{B.7}$$

Then the Eq. B.4 can be rewritten as:

$$\hat{U}_R\left(|\psi\rangle_B|\chi\rangle_E\right) = \frac{1}{\sqrt{2}}\left(|0\rangle_B|\chi_{00}\rangle + |1\rangle_B|\chi_{11}\rangle\right). \tag{B.8}$$

If Eve introduces no errors on the CTRL-X bit, there should be:

$$|\chi_{00}\rangle = |\chi_{11}\rangle\,. \tag{B.9}$$

Therefore, without introducing errors, Eve cannot obtain any information about the key. The preceding discussion highlights the necessity of the classical CTRL operation to ensure the security of SQKD.

References

[1] Bennett C H, Bessette F, Brassard G, Salvail L and Smolin J 1992 *Journal of Cryptology* **5** 3–28 ISSN 1432-1378 URL https://doi.org/10.1007/BF00191318

[2] Liao S K, Cai W Q, Liu W Y, Zhang L, Li Y, Ren J G, Yin J, Shen Q, Cao Y, Li Z P, Li F Z, Chen X W, Sun L H, Jia J J, Wu J C, Jiang X J, Wang J F, Huang Y M, Wang Q, Zhou Y L, Deng L, Xi T, Ma L, Hu T, Zhang Q, Chen Y A, Liu N L, Wang X B, Zhu Z C, Lu C Y, Shu R, Peng C Z, Wang J Y and Pan J W 2017 *Nature* **549** 43–47 ISSN 0028-0836 URL https://doi.org/10.1038/nature23655

[3] Liao S K, Yong H L, Liu C, Shentu G L, Li D D, Lin J, Dai H, Zhao S Q, Li B, Guan J Y, Chen W, Gong Y H, Li Y, Lin Z H, Pan G S, Pelc J S, Fejer M M, Zhang W Z, Liu W Y, Yin J, Ren J G, Wang X B, Zhang Q, Peng C Z and Pan J W 2017 *Nature Photonics* **11** 509–513 ISSN 1749-4885 URL https://doi.org/10.1038/nphoton.2017.116

[4] Lo H K, Curty M and Tamaki K 2014 *Nature Photonics* **8** 595–604 ISSN 1749-4885 URL https://doi.org/10.1038/nphoton.2014.149

[5] Nauerth S, Moll F, Rau M, Fuchs C, Horwath J, Frick S and Weinfurter H 2013 *Nature Photonics* **7** 382–386 ISSN 1749-4885 URL https://doi.org/10.1038/nphoton.2013.46

[6] Sasaki M, Fujiwara M, Ishizuka H, Klaus W, Wakui K, Takeoka M, Miki S, Yamashita T, Wang Z, Tanaka A, Yoshino K, Nambu Y, Takahashi S, Tajima A, Tomita A, Domeki T, Hasegawa T, Sakai Y, Kobayashi H, Asai T, Shimizu K, Tokura T, Tsurumaru T, Matsui M, Honjo T, Tamaki K, Takesue H, Tokura Y, Dynes J F, Dixon A R, Sharpe A W, Yuan Z L, Shields A J, Uchikoga S, Legré M, Robyr S, Trinkler P, Monat L, Page J B, Ribordy G, Poppe A, Allacher A, Maurhart O, Länger T, Peev M and Zeilinger A 2011 *Optics Express* **19** 10387–10409 ISSN 1094-4087 URL https://doi.org/10.1364/OE.19.010387

[7] Wang J Y, Yang B, Liao S K, Zhang L, Shen Q, Hu X F, Wu J C, Yang S J, Jiang H, Tang Y L, Zhong B, Liang H, Liu W Y, Hu Y H, Huang Y M, Qi B, Ren J G, Pan G S, Yin J, Jia J J, Chen Y A, Chen K, Peng C Z and Pan J W 2013 *Nature Photonics* **7** 387–393 ISSN 1749-4885 URL https://doi.org/10.1038/nphoton.2013.89

[8] Wang S, Yin Z Q, He D Y, Chen W, Wang R Q, Ye P, Zhou Y, Fan-Yuan G J, Wang F X, Chen W, Zhu Y G, Morozov P V, Divochiy A V, Zhou Z, Guo G C and Han Z F 2022 *Nature Photonics* **16** 154–161 ISSN 1749-4885 URL https://doi.org/10.1038/s41566-021-00928-2

[9] Boyer M, Kenigsberg D and Mor T 2007 *Physical Review Letters* **99** 1–4 ISSN 0031-9007 URL https://doi.org/10.1103/PhysRevLett.99.140501

[10] Boyer M, Gelles R, Kenigsberg D and Mor T 2009 *Physical Review A* **79** 1–12 ISSN 1050-2947 URL https://doi.org/10.1103/PhysRevA.79.032341

[11] Boyer M, Katz M, Liss R and Mor T 2017 *Physical Review A* **96** 1–6 ISSN 2469-9926 URL https://doi.org/10.1103/PhysRevA.96.062335

[12] Chen L Y, Gong L H and Zhou N R 2020 *International Journal of Theoretical Physics* **59** 1884–1896 ISSN 0020-7748 URL https://doi.org/10.1007/s10773-020-04456-7

[13] Hajji H and El Baz M 2021 *Quantum Information Processing* **20** 1–25 ISSN 1570-0755 URL https://doi.org/10.1007/s11128-020-02927-8

[14] Wang J, Zhang S, Zhang Q and Tang C J 2011 *Chinese Physics Letters* **28** 1–4 ISSN 0256-307X URL https://doi.org/10.1088/0256-307X/28/10/100301

[15] Wang K, Yang X Q, Li T Y, Lin Y Q, Hai N and Yin Z Q 2023 *Optics Express* **31** 40730–40740 ISSN 1094-4087 URL https://doi.org/10.1364/OE.506256

[16] Ye C Q, Li J, Chen X B, Tian Y and Hou Y Y 2022 *Ieee Communications Letters* **26** 1226–1230 ISSN 1089-7798 URL https://ieeexplore.ieee.org/document/9733340

[17] Zou X, Qiu D, Li L, Wu L and Li L 2009 *Physical Review A* **79** 1–7 ISSN 1050-2947 URL https://doi.org/10.1103/PhysRevA.79.052312

[18] Li L Z, Qiu D W and Mateus P 2013 *Journal of Physics a-Mathematical and Theoretical* **46** 1–10 ISSN 1751-8113 URL https://doi.org/10.1088/1751-8113/46/4/045304

[19] Wang J, Zhang S, Zhang Q and Tang C J 2012 *International Journal of Quantum Information* **10** 1–8 ISSN 0219-7499 URL https://doi.org/10.1142/S0219749912500505

[20] Wang M M, Liu J L and Gong L M 2019 *International Journal of Quantum Information* **17** 1–10 ISSN 0219-7499 URL https://doi.org/10.1142/S0219749919500242

[21] Li Y L, Bin Z S, Yan C, Wei S Z and Fan Y 2019 *Modern Physics Letters A* **34** 1–10 ISSN 0217-7323 URL https://doi.org/10.1142/S0217732319502948

[22] Wen X J, Zhao X Q, Gong L H and Zhou N R 2019 *Laser Physics Letters* **16** 1–10 ISSN 1612-2011 URL https://doi.org/10.1088/1612-202X/ab232c

[23] Krawec W O 2014 *Quantum Information Processing* **13** 2417–2436 ISSN 1570-0755 URL https://doi.org/10.1007/s11128-014-0802-2

[24] Zhang W, Qiu D W and Mateus P 2018 *Quantum Information Processing* **17** 1–21 ISSN 1570-0755 URL https://doi.org/10.1007/s11128-018-1904-z

[25] Mi S, Dong S, Hou Q, Wang J, Yu Y, Wei Z and Zhang Z 2022 *Frontiers in Physics* **10** 1–10 ISSN 2296-424X URL https://doi.org/10.3389/fphy.2022.1029552

[26] Dong S, Mi S, Hou Q C, Huang Y T, Wang J D, Yu Y F, Wei Z J, Zhang Z M and Fang J B 2023 *Epj Quantum Technology* **10** 1–15 ISSN 2662-4400 URL https://doi.org/10.1140/epjqt/s40507-023-00175-0

[27] Han S, Huang Y, Mi S, Qin X, Wang J, Yu Y, Wei Z and Zhang Z 2021 *Epj Quantum Technology* **8** 1–10 ISSN 2662-4400 URL https://doi.org/10.1140/epjqt/s40507-021-00117-8

[28] Mo N, Huang S, Wang J, Yu Y, Wei Z, Zhao T and Zhang Z 2024 *Optics Express* **32** 29291–29300 ISSN 1094-4087 URL https://doi.org/10.1364/OE.529300

[29] Tan Y G, Lu H and Cai Q Y 2009 *Physical Review Letters* **102** 1 ISSN 0031-9007 URL https://doi.org/10.1103/PhysRevLett.102.098901