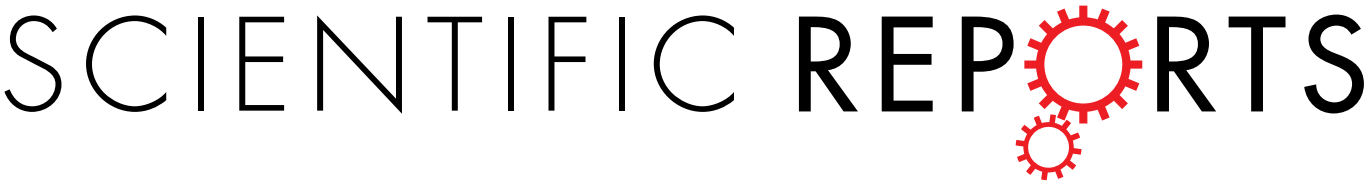

OPEN

Quantum key distribution with prepare-and-measure Bell test

Yong-gang Tan

Received: 21 March 2016
Accepted: 22 September 2016
Published: 13 October 2016

The prepare-and-measure quantum key distribution (QKD) has the merits of fast speed, high key generation rate, and easy implementation. However, the detector side channel attacks greatly undermine the security of the key bits. The eavesdropper, Eve, exploits the flaws of the detectors to obtain illegal information without violating quantum principles. It means that she can intervene in the communication without being detected. A prepare-and-measure Bell test protocol will be proposed. By randomly carrying out Bell test at the side of the information receiver, Bob, Eve's illegal information gain within the detector side channel attack can be well bounded. This protocol does not require any improvement on the detectors used in available prepare-and-measure QKD. Though we only illustrate its application in the BB84 protocol, it is applicable for any prepare-and-measure QKD.

QKD is a real-time art of generating secure key bit string between remote partners[1–3]. Its security is not based on the computational complexity, but on the correctness of physical principles[4–7]. In practical conditions where imperfectly experimental devices are used, it is proven that secure key bit string can still be generated when the tagged key bits are well restricted[8]. For example, phase-randomized weaken coherent sources are used in practical QKD. There are multi-photon pulses emitted from the source. Eve can launch the photon-number-splitting (PNS) to tag the multi-photon events[9,10]. If the amount of the tagged event can be well bounded, with decoy state technology for example, secure key bits can be generated between remote partners[11–14].

Recently, the detector side channel attacks have attracted great attention. Eve exploits the drawbacks of the detectors to control the detections. Moreover, the photons registered by the detectors may be not the ones expected by Bob, but well devised by Eve to obtained illegal information. In the fake state attack, Eve intercepts the photons from Alice and reads out the bit values on them. According to her measurement outcomes, she exploits the detection efficiency mismatches and prepares a fake state to be detected by Bob[15]. The time-shift attack uses the detection efficiency mismatches to eavesdrop on the communication without intercepting on Alice's photons[16,17]. Furthermore, the problem of information leaking from the detector side channels also exists in the blinding attack[18–20] and the phase re-mapping attack[21,22].

The detector side channel attacks do great harm to the security of QKD because Eve's illegal information gain obtained in the attacks cannot be well bounded[8]. Great improvement must be made on the detectors to avoid the detector side channel attacks[19,23–25]. It has been shown that alternative ways of measurements can be used to beat these attacks[26–32]. In this case, the security of the measurement outcomes relies on the monogamy of entanglement[33,34]. Accordingly, the experimental realization is more complex and the key generation rate is lower when compared with the prepare-and-measure QKD. An easy way to beat the detector side channel attack from the physics principle is expected.

Quantum theory is exclusive with the local hidden variable (lhv) theory[35–37]. Loophole-free Bell violation means that the lhv theory can be excluded. Or else, if no Bell violation can be obtained in the loophole-free Bell test, the quantum theory is incorrect. Recently, Bell violation is experimentally obtained with all loopholes are closed[38–40]. These significant results mean the lhvs do not exist. Based on this fact, the detector side channel attack in the prepare-and-measure QKD can be beat with a simple but efficient way. Random Bell test is required to be carried out at Bob's side to check the quantum correlations between Alice and Bob. Though this protocol is devised for the BB84 protocol[1], it is applicable to any prepare-and-measure QKD.

The prepare-and-measure Bell test

In the Bell test, a parametric-down-conversion (PDC) source is set between Alice and Bob. Entangled photon pairs are generated and distributed to them. Alice has two sets of two-channel measurement devices, A_1 and A_2. Similarly, Bob has two sets of two-channel measurement settings, B_1 and B_2. Alice and Bob randomly choose their

Physics and Information Engineering Department, Luoyang Normal College, Luoyang 471022, Henan, People's Republic of China. Correspondence and requests for materials should be addressed to Y.g.T. (email: ygtan@lynu.edu.cn)

measurement settings to measure their incoming photons. The binarily possible measurement outcomes obtained from the measurement settings are assigned with -1 and 1. Alice and Bob use their basis choices and measurement outcomes to calculate the CHSH polynomial[37]

$$S_{\mathrm{CHSH}} \equiv \langle A_1B_1 + A_1B_2 + A_2B_1 - A_2B_2\rangle. \tag{1}$$

Here $\langle A_i\rangle$, $\langle B_j\rangle$ are the average values generated on A_i and B_j, with $i, j \in \{1, 2\}$.

In local hidden variable theory and classical physics, the measurement outcomes at Alice's side cannot be affected by those at Bob's side. Similarly, the measurement outcomes at Bob's side cannot be affected by those at Alice's side, namely, the relation $\langle A_iB_j\rangle = \langle A_i\rangle\langle B_j\rangle$ obeys[41]. Because $-1 \le \langle A_i\rangle \le 1$ and $-1 \le \langle B_j\rangle \le 1$ should be satisfied, S_{CHSH} varies from -2 to 2. Quantum-mechanically, its lower bound and upper bound are $-2\sqrt{2}$ and $2\sqrt{2}$, respectively[42]. Now that the Bell violation has been obtained with loophole-free Bell test[38–40], the lhv theory does not need to be considered. If the experiment is not artificially controlled, Bell violation certifies the existence of entanglement.

Suppose that the entangled photon pair generated from the PDC source is encoded with $|\Phi^+_{AB}\rangle = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$, where the subscripts A and B denote Photon A and Photon B, respectively. After the photon pairs generated from the PDC source, Photon A is distributed to Alice, while Photon B is sent to Bob. In order to maximize the Bell violation, confinements are put on their basis choices. Without loss of any generality, one can assume that $A_1 \equiv \hat{\sigma}_z$, $A_2 \equiv \hat{\sigma}_x$, $B_1 \equiv \frac{1}{\sqrt{2}}(\hat{\sigma}_x + \hat{\sigma}_z)$, and $B_2 \equiv \frac{1}{\sqrt{2}}(\hat{\sigma}_x - \hat{\sigma}_z)$, where $\hat{\sigma}_x$ and $\hat{\sigma}_z$ are the Pauli operators. Because the state $|\Phi^+_{AB}\rangle$ is rotationally invariant in the $X-Z$ plane, one can obtain that $|\Phi^+_{AB}\rangle = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}) = \frac{1}{\sqrt{2}}(|{+}{+}\rangle_{AB} + |{-}{-}\rangle_{AB})$, with $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. In this case, it is easy to verify that $S_{\mathrm{CHSH}} = 2\sqrt{2}$.

Traditionally, the PDC source is usually set between Alice and Bob to exclude the locality loophole. Because the lhv theory is refuted, it is not necessary to care about this loophole. Alice can set the PDC source in her laboratory. When the entangled photon pair is generated, she keeps one of them and transfers the other to Bob. As there is no need to care about the locality loophole, the measurement sequences of Alice and Bob do not affect their experimental results. Alice's measurement can be implemented before that of Bob, and vise versa. If Eve does not intervene, Bell violation must be obtained.

The moment Alice measures on Photon A, the state on Photon B collapses accordingly. It means that Alice prepares the state on Photon B the moment she measures on Photon A. Because the photon pair is prepared with the state $|\Phi^+_{AB}\rangle = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$, the state on Photon B should correlate with what Alice obtains in her measurement. The same correlation can also be obtained with prepare-and-measure procedure: Suppose that single photon is generated from Alice's source. She randomly chooses the rectilinear basis $\hat{\sigma}_z$ or the diagonal basis $\hat{\sigma}_x$, together with random bit value -1 or 1, to prepare Photon B. Before Photon B is measured, its state correlates with the state chosen by Alice.

If Alice's basis choices and bit value choices on Photon B are totally random, the item $\langle A_1B_1\rangle$ in (1) can be calculated as

$$\langle A_1B_1\rangle = \frac{1}{2_B}\langle 0|B_1|0\rangle_B - \frac{1}{2_B}\langle 1|B_1|1\rangle_B. \tag{2}$$

Similarly, one can obtain

$$\begin{aligned}
\langle A_1B_2\rangle &= \frac{1}{2_B}\langle 0|B_2|0\rangle_B - \frac{1}{2_B}\langle 1|B_2|1\rangle_B,\\
\langle A_2B_1\rangle &= \frac{1}{2_B}\langle +|B_1|+\rangle_B - \frac{1}{2_B}\langle -|B_1|-\rangle_B,\\
\langle A_2B_2\rangle &= \frac{1}{2_B}\langle +|B_2|+\rangle_B - \frac{1}{2_B}\langle -|B_2|-\rangle_B.
\end{aligned} \tag{3}$$

Substituting B_1 and B_2 with $\frac{1}{\sqrt{2}}(\hat{\sigma}_x + \hat{\sigma}_z)$ and $\frac{1}{\sqrt{2}}(\hat{\sigma}_x - \hat{\sigma}_z)$, one can obtain that $\langle A_1B_1\rangle = \frac{1}{\sqrt{2}}$, $\langle A_1B_2\rangle = \frac{1}{\sqrt{2}}$, $\langle A_2B_1\rangle = \frac{1}{\sqrt{2}}$, and $\langle A_2B_2\rangle = -\frac{1}{\sqrt{2}}$. The value of the CHSH polynomial is calculated to be $S_{\mathrm{CHSH}} = 2\sqrt{2}$. It is the same as that when the entangled state $|\Phi^+_{AB}\rangle$ is used. This is because the correlations between the state on Photon B and that of Alice are the same in these two cases.

BB84 protocol with the prepare-and-measure Bell test

The BB84 protocol is a prepare-and-measure QKD protocol. Alice prepares the state on Photon B and transfers it to Bob. Bob measures it in randomly chosen basis to read its state. The states $|0\rangle_B$ and $|+\rangle_B$ are used to encode the bit value 0, while the states $|1\rangle_B$ and $|-\rangle_B$ are used to encode the bit value 1 (Here the definitions of the bit values in the quantum key distribution and those of the Bell test are different).

The prepare-and-measure BB84 protocol is characterized as follows:

(a) N single photons are generated in Alice's laboratory. She randomly chooses between the diagonal basis $A_1 = \hat{\sigma}_x$ and rectilinear basis $A_2 = \hat{\sigma}_z$ and the random bit values 0 and 1 to prepare her state on the photon. Then the photon is transferred to Bob.

(b) Bob has two modes: with probability p he chooses the signal mode and with probability $1-p$ he chooses the test mode (Only Bob himself is aware of the value of p). In the signal mode, Bob's measurement bases are randomly chosen from $B_1^s = \hat{\sigma}_z$ and $B_2^s = \hat{\sigma}_x$. In the test mode, his measurement bases are randomly chosen between $B_1^t = \frac{1}{\sqrt{2}}(\hat{\sigma}_x + \hat{\sigma}_z)$, and $B_2^t = \frac{1}{\sqrt{2}}(\hat{\sigma}_x - \hat{\sigma}_z)$.

(b′) When Bob chooses the signal mode, Alice and Bob publish their measurement bases through the public channel. They keep their measurement outcomes in the same bases as the sifted key bits.

(b″) When Bob chooses the test mode, Alice and Bob announce their basis choices and measurement outcomes through the public channel to calculate the value of S_{CHSH}.

(c) After the key distribution, Alice and Bob implement error correction (EC) and privacy amplification (PA) on their sift key bits. If secure key bits can be generated, their key distribution task is fulfilled. Or else, their task is failed.

Because Alice randomly chooses her basis and bit values on Photon B, the state on it is $\rho_B = \frac{1}{2}(|0\rangle_B\langle 0| + |1\rangle_B\langle 1|) = \frac{1}{2}(|+\rangle_B\langle +| + |-\rangle_B\langle -|)$ for any third party. The state is uniformly prepared in the conjugated bases. Eve cannot differentiate which state is prepared. If she carries out state distinguishing task on the photon, disturbance must be introduced[43,44]. Without loss of any generality, one can assume that Eve interacts on Photon B with a probe. If the interaction between the probe and Photon B can be characterized as a unitary process, one can obtain

$$\begin{aligned}
|0\rangle_A|0\rangle_B|E\rangle &\xrightarrow{U} |0\rangle_A(\sqrt{f}|0\rangle_B|0\rangle_E + \sqrt{e}|1\rangle_B)|1\rangle_E),\\
|1\rangle_A|1\rangle_B|E\rangle &\xrightarrow{U} |1\rangle_A(\sqrt{f}|1\rangle_B|0\rangle_E + \sqrt{e}|0\rangle_B)|1\rangle_E),\\
|+\rangle_A|+\rangle_B|E\rangle &\xrightarrow{U} |+\rangle_A(\sqrt{f}|+\rangle_B|+\rangle_E + \sqrt{e}|-\rangle_B)|-\rangle_E),\\
|-\rangle_A|-\rangle_B|E\rangle &\xrightarrow{U} |-\rangle_A(\sqrt{f}|-\rangle_B|+\rangle_E + \sqrt{e}|+\rangle_B)|-\rangle_E).
\end{aligned} \tag{4}$$

Here $|E\rangle$ is the blank state on Eve's probe. f and e correspond to the probability that the state on Photon B is intact and the probability that the state on Photon B is changed, respectively. It means that Eve's intervention introduces quantum bit error rate (QBER) with probability e. The amount of information for Alice and Bob used to correct the errors on their bit string is $h(e)$, with $h(x) = -x\log_2 x - (1-x)\log_2 x$ the binary entropy. In the prepare-and-measure QKD, Eve's ability to attack on the communication can be bounded with the collective attack[3,45]. In this case, the rate for Eve to tag Bob's key bits is upper bounded with[46,47]

$$I_E \leq h\left(\frac{1+\sqrt{(S_{\mathrm{CHSH}}/2)^2 - 1}}{2}\right). \tag{5}$$

After Eve's intervention, $\langle A_1B_1\rangle$ is recalculated to be

$$\langle A_1B_1\rangle = (f-e)\left(\frac{1}{2_B}\langle 0|B_1|0\rangle_B - \frac{1}{2_B}\langle 1|B_1|1\rangle_B\right). \tag{6}$$

Similarly, one has

$$\begin{aligned}
\langle A_1B_2\rangle &= (f-e)\left(\frac{1}{2_B}\langle 0|B_2|0\rangle_B - \frac{1}{2_B}\langle 1|B_2|1\rangle_B\right),\\
\langle A_2B_1\rangle &= (f-e)\left(\frac{1}{2_B}\langle +|B_1|+\rangle_B - \frac{1}{2_B}\langle -|B_1|-\rangle_B\right),\\
\langle A_2B_2\rangle &= (f-e)\left(\frac{1}{2_B}\langle +|B_2|+\rangle_B - \frac{1}{2_B}\langle -|B_2|-\rangle_B\right).
\end{aligned} \tag{7}$$

It means Alice's and Bob's states are correlated with probability f, and anti-correlated with probability e that is also known as the QBER. After Eve's intervention, $S_{\mathrm{CHSH}} = 2\sqrt{2}(f-e)$ is obtained.

Refute the detector side channel attack

In the BB84 protocol, Eve's illegal information is also bounded as[3,4,7]

$$I_E \leq h(e). \tag{8}$$

Here e is the phase error rate gained on Bob's state. Strictly speaking, phase error rate is the concept of entangled states. Because of the symmetry of BB84 protocol, however, the phase error rate is estimated from the bit error rate on the results generated from the conjugated bases[4,7]. Within the process of Eve's attack, if she can hide the bit error rates of both bases, Alice and Bob cannot find her existence. In the detector side channel attack, for instance, it is possible for Eve to intervene without introducing any bit error rate.

If Bob's detectors are imperfect, the detector side channel information leaking problem may exist. Eve can exploit the flaws of Bob's detectors to carry out the detector side channel attacks.

Theorem 1 *The detector side channel attacks can be successfully carried out if and only if Eve's information of Alice's bit value conditioned on Bob's measurement outcome is partially or totally certain.*

Proof: In the BB84 protocol, Eve interacts with Photon B to extract Alice's state on it. After Bob measuring on the incoming photons, he and Alice declare their basis choices. When considering the individual attack, Eve's information gain from Alice is bounded by her entropy decrease on her state[3]

$$I_E = H_{a\ priori} - H_{a\ posteriori}. \tag{9}$$

In the detector side channel attack, though drawbacks exist on Bob's detectors, it is indispensable to assume that no unwanted information can leak out of his laboratory. Or else, the security of QKD cannot be ensured. It means that Eve should control the information leaking from the detectors indirectly. If Alice's state on Photon B is uniformly prepared, $H_{a\ priori} = 1$ is obtained.

Consider that $H_{a\ posteriori} = \sum_r P(r)H(i|r)$, with $P(r)$ the probability Eve obtains the measurement result r, and $H(i|r)$ the information gain of i conditioned on r. If Eve does not interact with Photon B, $H_{a\ posteriori} = 1$ after Bob declaring his basis choices. Thus $I_E = 0$ and Eve cannot obtain any illegal information on Alice's state. In the detector side channel attack, r has two possible values: the registered and the unregistered, and $\sum_r P(r) = 1$ is satisfied. Whether for the registered pulses or for the unregistered pulses, Bob's measurement outcomes are controlled to be bit value biased. Bob announces Alice the values of r after his measurements. The bias of Bob's measurement outcomes is known to Eve in the detector side channel attack and $H(i|r)$ should be less than 1. Correspondingly, $H_{a\ posteriori} < 1$ and $I_E > 0$ are satisfied. In some detector side channel attacks, Eve's uncertainty on Alice's states is eliminated with the intercept-resend attack. However, only the pulses encoded with Eve's expected bit values and expected bases are forced to be detected by Bob. Or else, Alice and Bob can find Eve's presentence according to the correlations between them. In any case, Bob's measurement outcomes are partially or totally certain to Eve. Thus we end the proof.

In order to refute the detector side channel attack, Alice and Bob should estimate Eve's information gain from the attack. In practical QKD, time-windows is set for the detectors so that their dark count rate can be decreased. Thus their detection efficiencies are time-dependent. If the time windows of the two detectors are not the same, there are detection mismatches between them. This can be exploited by Eve to launch the so-called time-shift attack. Furthermore, the detector flaws may also be used by Eve to control the detectors to detect unwanted signals. Taking the blinding attack for instance, the detectors can be blinded with strong illuminations so that they are insensitive to single-photon pulses but to strong pulses. Both in the time-shift attack and in the blinding attack, Eve's *a posteriori* information on Alice's bit value is partially or even totally deterministic.

In practical Bell test with EPR pairs, the quantum channel is lossy and one has to consider the detection loophole. It means that any pulse in quantum channel cannot represent the others in violating the CHSH inequality. If the devices are inefficient, fair-sampling assumption must be made to obtain the Bell violation. If Alice and Bob can implement quantum non-demolition measurement on the photon number, they differentiate the vacuum pulses from the non-vacuum pulses. With this technique, they can remove the channel loss. Now that the lhv theory has be excluded by recent experiments, it is reasonable to assume that the movements all pulses obey the quantum principles and all photon pulses experience the same transmission situation. Thus one can sample the behaviors of some of the incoming pulses on the behalf of those of the others.

We consider the QKD with active basis choice. Bob has two detectors D_0 and D_1 to decode the key bits 0 and 1 encoded on Alice's pulses. Their detection efficiencies are assumed to be η_0 and η_1, respectively. D_0 and D_1 are manufactured to be the same so that $\eta_0 = \eta_1 = \eta$ is satisfied when there is no detector side channel attack. We assume that Bob has another detector D_t whose detection efficiency is η_t. D_t is also the same as D_0 and D_1 apart from its big time window. The time window of D_t is big enough so that its detection efficiency is stably kept within the whole time windows of both D_0 and D_1. This can be realized by keeping D_t switched on within this period of time. When Bob receives the pulses from Alice, she randomly detect them directly with D_t or decode their key bits with D_0 and D_1 in randomly chosen bases. When detector side channel attacks randomly happen on D_0 and D_1, η_0 and η_1 decrease. For Bob, the detection efficiency he can observe for D_0 and D_1 is $\eta = \frac{\eta_0 + \eta_1}{2}$. According to Eqs (2) and (3), the value of the CHSH polynomial should be normalized as

$$S_{\mathrm{CHSH}}^{\mathrm{side-channel}} = \eta/\eta_t S_{\mathrm{CHSH}}. \tag{10}$$

This relation can also be explained with the theory raised by Garg and Mermin where the photons that can be detected by D_t but are missed by D_0 and D_1 can only be assigned with the bit value 0[48]. Accordingly, the illegal information gain Eve obtained within her detector side channel attack is calculated to be

$$I_E^{\mathrm{side-channel}} \leq h\left(\frac{1 + \sqrt{(S_{\mathrm{CHSH}}^{\mathrm{side-channel}}/2)^2 - 1}}{2}\right). \tag{11}$$

The performance of the present protocol

In practical QKD, instead of single-photon source, weaken coherent sources are used for Alice to encode her key bits. Compared with single-photon source, multi-photon pulses exist. It is proven that Eve can exploit the multi-photon pulses to launch the so-called PNS attack. Thus decoy states are usually added in practical QKD protocol to beat this attack[12–14]. We consider the practical decoy state protocol raised by Ma *et al.* where a signal source, a weaker decoy source and a vacuum decoy source are used[14]. The intensities of the signal source and the

weaker decoy source are μ and ν, respectively. After randomization of the phase, the photon number distributions of the sources obey

$$\begin{aligned} P_\mu(i) &= \frac{\mu^i}{i!}e^{-\mu}, \\ P_\nu(i) &= \frac{\nu^i}{i!}e^{-\nu}. \end{aligned} \tag{12}$$

Here i is the photon number in the pulses.

Alice randomly chooses the signal source and the decoy sources to encode her bit values and transfers them to Bob. When Bob takes the pulses from Alice, with probability p he chooses the signal mode that he measures the incoming pulses randomly in $B_1^s = \hat{\sigma}_z$ and $B_2^s = \hat{\sigma}_x$ to extract the key bits on them. With probability p', he chooses the test mode that his measurement bases are randomly chosen between $B_1^t = \frac{1}{\sqrt{2}}(\hat{\sigma}_x + \hat{\sigma}_z)$, and $B_2^t = \frac{1}{\sqrt{2}}(\hat{\sigma}_x - \hat{\sigma}_z)$. With probability $1-p-p'$, however, Bob directly measures Alice's pulses in his detector D_t. The gains on the detectors D_0/D_1, and D_t write

$$\begin{aligned} Q_\mu^\eta &= Y_0 + 1 - e^{\eta\mu}, \qquad Q_\nu^\eta = Y_0 + 1 - e^{\eta\nu}, \\ Q_\mu^{\eta_t} &= Y_0' + 1 - e^{\eta_t\mu}, \qquad Q_\nu^{\eta_t} = Y_0' + 1 - e^{\eta_t\nu}. \end{aligned} \tag{13}$$

Here Y_0 and Y_0' are the dark counts on D_0/D_1 and D_t that can be estimated from the vacuum decoy state. After Bob's measurements, Alice announces Bob her state choices with which Bob can calculate the values of η and η_t.

After the EC and PA, the final key generation rate is

$$R \geq Q_1^\nu(1 - I_E^{\text{side-channel}}) - f(E_\nu)Q_\nu^\eta h(E_\nu), \tag{14}$$

where Q_1^ν is the gain on the untagged pulses of the weaker decoy source, $f(E_\nu)$ is error correction efficiency, and E_ν is the total QBER on the sifted key bits generated from the decoy source. Here we choose the weaker decoy source for key generation because the multi-photon pulses affect the value of the CHSH polynomial greatly. Numerical results shows that no Bell violation can be obtained when the intensity of the signal source is greater than 0.659 even if D_0 and D_1 have perfect detection efficiency. The fraction of the multi-photon pulses in the decoy source is comparably small, however, thus we assume Alice and Bob use it to generate the key bits.

We will give some numerical simulations on the performance of the QKD with prepare-and-measure Bell test. We will use the setup parameters from the QKD experiment completed by Gobby, Yuan and Shields (GYS)[49] that has also been taken used for numerical simulation in ref. 14. Namely, the transferring coefficient is $\beta = 0.21\text{d}B/km$, the detector's detection efficiency is $\eta_B = 4.5\%$, the misalignment coefficient is $e_d = 3.3\%$, and the dark count rate $Y_0 = 1.7 \times 10^{-6}$. The intensities of the signal pulses, weaker decoy pulses and vacuum pulses are 0.48, 0.1 and 0, respectively. One thing should be pointed out that we will not consider the contribution of the misalignment to the value of the CHSH polynomial.

Firstly, we want to show the performances of the present protocol under the blinding attack and the time-shift attack. For blinding attack, Eve controls the basis of Bob. When Bob's basis choices coincide with hers, there are efficient registers on his measurement settings. Or else, no clicking event happens. Thus one can obtain $\eta_t = 2\eta$, and the value of CHSH polynomial is $\sqrt{2}$ for perfect single-photon source. It means that no secure key bits can be generated between Alice and Bob. For the time-shift attack, the CHSH inequality after the time-shift attack is calculated to be $\frac{\sqrt{2}(\eta_0+\eta_1)}{\eta_t}$. In this attack, however, Eve's illegal information gain is calculated to be $I_E^{\text{time-shift}} = 1 - h(r/(r+1))$, with $r = \min\left\{\frac{\eta_0}{\eta_1}, \frac{\eta_1}{\eta_0}\right\}$. For simplicity of discussion, one can assume that $\eta_0 < \eta_1$. It is apparent that the big the value $\Delta = \eta_t - \frac{1}{2}(\eta_0 + \eta_1)$ is, the more key bits should be sacrificed for PA. The amount of information Alice and Bob should sacrifice for PA is $I_E^{\text{side-channel}} = h\left(\frac{1+\sqrt{(1+r)^2/2-1}}{2}\right)$.

From Fig. 1, it is apparent that the amount of information (dash line) Alice and Bob sacrificed for PA is greater than that (solid line) Eve obtained in her time-shift attack. Thus the present protocol is secure under the time-shift attack. The value of r begins from 0.414 because $\sqrt{(1+r)^2/2 - 1}$ required that $r \geq \sqrt{2} - 1 \approx 0.414$. When $r \leq \sqrt{2} - 1$, however, one can obtain $S_{\text{CHSH}} \leq 2$. It means that the classical bound of the CHSH inequality cannot be violated and no secure key bit can be generated. We can also compare the key generation rate of the present protocol with that of the practical decoy state QKD[14]. In Fig. 2, one can see that the key generation rate of the present protocol is small than that in ref. 14. This is because we generate the key bits from the weaker decoy state whose intensity is smaller than that of the signal state. Furthermore, the transmission distance of the present protocol can reach about 103 km (solid line). This distance is also shorter than that in ref. 14 (dash line).

Discussion and Conclusion

In this paper, the QKD protocol with prepare-and-measure Bell test has been proposed. Though the security of the present protocol is based on Bell's theorem, it is different with the DI-QKD protocol[46,47] and the Ekert91 protocol[2]. First, there is no need to care about the detection efficiency. In the present protocol, only the registered photons are used to calculate the CHSH polynomial. Second, entanglement is not required in the present protocol. The protocol is implemented in a prepare-and-measure way. Furthermore, the Bell test in the present protocol is only carried out at Bob's side. Our protocol is also different with the detection device-independent

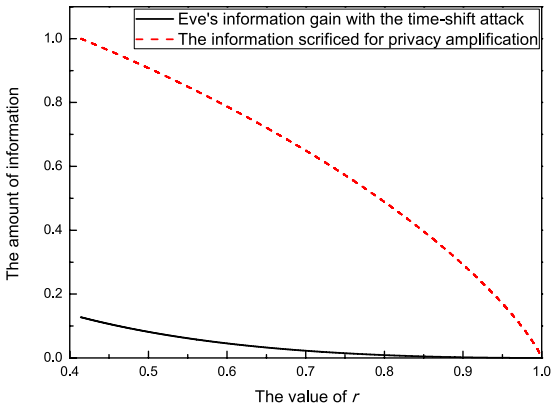

Figure 1. The solid line represents Eve's information gain within her time-shift attack. The dash line represents the amount of information Alice and Bob should sacrifice for PA after Eve's time-shift attack.

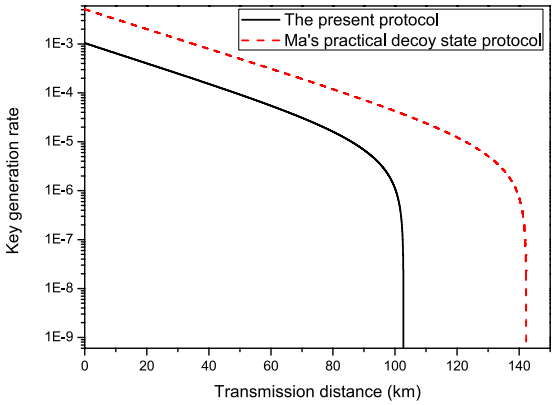

Figure 2. The solid line represents the relation between the key generation rate and the transmission distance of the present protocol. The dash line characterize the relation between the key generation rate and the transmission distance in ref. 14.

QKD protocols of the ref. 50. In the detection device-independent protocols, Alice and Bob have characterized sources but uncharacterized detectors. In the present protocol, however, Bob's detectors are partially characterized. We assume that the detectors have the same attributions. Furthermore, Bob can control the time window of the testing detector.

References

1. Bennett, C. H. Quantum cryptography: Public key distribution and coin tossing. *Proceedings of the International Conference on Computer System and Signal Processing, IEEE*, **1984,** 175–179 (1984).
2. Ekert, A. K. Quantum cryptography based on Bells theorem. *Phys. Rev. Lett.* **67,** 661 (1991).
3. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74,** 145 (2002).
4. Lo, H.-K. & Chau, H. F. Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **283,** 2050–2056 (1999).
5. Mayers, D. Unconditional security in quantum cryptography. *Journal of the ACM* (*JACM*) **48,** 351–406 (2001).
6. Biham, E., Boyer, M., Boykin, P. O., Mor, T. & Roychowdhury, V. A proof of the security of quantum key distribution. *J. Cryptol.* **19,** 381–439 (2006).
7. Shor, P. W. & Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **85,** 441 (2000).
8. Gottesman, D., Lo, H.-K., Ltkenhaus, N. & Preskill, J. Security of quantum key distribution with imperfect devices. *Proceedings of the Information Theory, 2004. ISIT 2004. Proceedings. International Symposium on, IEEE*, 2004, 136.
9. Huttner, B., Imoto, N., Gisin, N. & Mor, T. Quantum cryptography with coherent states. *Phys. Rev. A* **51,** 1863 (1995).
10. Lütkenhaus, N. & Jahma, M. Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack. *New Journal of Physics* **4,** 44 (2002).
11. Hwang, W.-Y. Quantum key distribution with high loss: toward global secure communication. *Phys. Rev. Lett.* **91,** 057901 (2003).
12. Lo, H.-K., Ma, X. & Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **94,** 230504 (2005).
13. Wang, X.-B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **94,** 230503 (2005).
14. Ma, X., Qi, B., Zhao, Y. & Lo, H.-K. Practical decoy state for quantum key distribution. *Phys. Rev. A* **72,** 012326 (2005).
15. Makarov, V. & Hjelme, D. R. Faked states attack on quantum cryptosystems. *J. Mod. Optic.* **52,** 691–705 (2005).
16. Qi, B., Fung, C.-H. F., Lo, H.-K. & Ma, X. Time-shift attack in practical quantum cryptosystems. *Quantum Information and Computation* **7,** 073 (2007).
17. Zhao, Y., Fung, C.-H. F., Qi, B., Chen, C. & Lo, H.-K. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems. *Phys. Rev. A* **78,** 042333 (2008).
18. Makarov, V. Controlling passively quenched single photon detectors by bright light. *New Journal of Physics* **11,** 065003 (2009).

19. Lydersen, L. *et al.* Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature photonics* **4,** 686–689 (2010).
20. Gerhardt, I. *et al.* Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nature communications* **2,** 349 (2011).
21. Fung, C.-H. F., Qi, B., Tamaki, K. & Lo, H.-K. Phase-remapping attack in practical quantum-key-distribution systems. *Phys. Rev. A* **75,** 032314 (2007).
22. Xu, F., Qi, B. & Lo, H.-K. Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. *New Journal of Physics* **12,** 113026 (2010).
23. Yuan, Z., Dynes, J. & Shields, A. Avoiding the blinding attack in QKD. *Nature Photonics* **4,** 800–801 (2010).
24. Lydersen, L. *et al.* Avoiding the blinding attack in QKD. *Nature Photonics* **4,** 801–801 (2010).
25. Zhang, J., Itzler, M. A., Zbinden, H. & Pan, J.-W. Advances in InGaAs/InP single-photon detector systems for quantum communication. *Light: Science & Applications* **4,** e286 (2015).
26. Biham, E., Huttner, B. & Mor, T. Quantum cryptographic network based on quantum memories. *Phys. Rev. A* **54,** 2651 (1996).
27. Inamori, H. Security of practical time-reversed EPR quantum key distribution. *Algorithmica.* **34,** 340–365 (2002).
28. Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108,** 130503 (2012).
29. Braunstein, S. L. & Pirandola, S. Side-channel-free quantum key distribution. *Phys. Rev. Lett.* **108,** 130502 (2012).
30. Ma, X., Fung, C.-H. F. & Razavi, M. Statistical fluctuation analysis for measurement-device-independent quantum key distribution. *Phys. Rev. A* **86,** 052305 (2012).
31. Ma, X. & Razavi, M. Alternative schemes for measurement-device-independent quantum key distribution. *Phys. Rev. A* **86,** 062319 (2012).
32. Xu, F., Curty, M., Qi, B. & Lo, H.-K. Practical aspects of measurement-device-independent quantum key distribution. *New Journal of Physics* **15,** 113007 (2013).
33. Wootters, W. K. Entanglement of formation of an arbitrary state of two qubits. *Phys. Rev. Lett.* **80,** 2245 (1998).
34. Coffman, V., Kundu, J. & Wootters, W. K. Distributed entanglement. *Phys. Rev. A* **61,** 052306 (2000).
35. Einstein, A., Podolsky, B. & Rosen, N. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.* **47,** 777 (1935).
36. Bell, J. S. On the einstein podolsky rosen paradox [M] (1964).
37. Clauser, J. F., Horne, M. A., Shimony, A. & Holt, R. A. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.* **23,** 880 (1969).
38. Hensen, B. *et al.* Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature* **526,** 682–686 (2015).
39. Giustina, M. *et al.* Significant-loophole-free test of Bells theorem with entangled photons. *Phys. Rev. Lett.* **115,** 250401 (2015).
40. Shalm, L. K. *et al.* Strong loophole-free test of local realism. *Phys. Rev. Lett.* **115,** 250402 (2015).
41. Barrett, J., Hardy, L. & Kent, A. No signaling and quantum key distribution. *Phys. Rev. Lett.* **95,** 010503 (2005).
42. Cirel'son, B. S. Quantum generalizations of Bell's inequality. *Lett. Math. Phys.* **4,** 93–100 (1980).
43. Ivanovic, I. D. How to differentiate between non-orthogonal states. *Phys. Lett. A* **123,** 257–259 (1987).
44. Peres, A. How to differentiate between non-orthogonal states. *Phys. Lett. A* **128,** 19 (1988).
45. Renner, R. Security of quantum key distribution. *International Journal of Quantum Information* **6,** 1–127 (2008).
46. Acn, A. *et al.* Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.* **98,** 230501 (2007).
47. Pironio, S. *et al.* Device-independent quantum key distribution secure against collective attacks. *New Journal of Physics* **11,** 045021 (2009).
48. Garg, A. & Mermin, N. D. Detector inefficiencies in the Einstein-Podolsky-Rosen experiment. *Phys. Rev. D* **35,** 3831 (1987).
49. Gobby, C., Yuan, Z. & Shields, A. Quantum key distribution over 122 km of standard telecom fiber. *Appl. Phys. Lett.* **84,** 3762–3764 (2004).
50. Ma, X. & Lütkenhaus, N. Improved data post-processing in quantum key distribution and application to loss thresholds in device independent QKD. *Quantum Information and Computation* **12,** 203 (2012).

Acknowledgements

This work is supported by MOST 2013CB922003 of the National Key Basic Research Program of China, and NSFC under Grant No. 61378011. Tan thanks Qing-yu Cai for helpful discussion and partial preparation of the paper.

Author Contributions

Y.-g.T. wrote the paper.

Additional Information

Competing financial interests: The author declares no competing financial interests.

How to cite this article: Tan, Y.-g. Quantum key distribution with prepare-and-measure Bell test. *Sci. Rep.* **6**, 35032; doi: 10.1038/srep35032 (2016).