chapter 10

Noise-Immune Quantum Key Distribution

Z.D. Walton, A.V. Sergienko, B.E.A. Saleh, and M.C. Teich
Boston University

Contents

Abstract

We review quantum key distribution schemes that are noise-immune (require no alignment). For both polarization and time-bin qubits, we present three noise-immune schemes: round-trip, one-way, and symmetric. In the round-trip schemes, the signal travels back and forth between the legitimate users (Alice and Bob); in the one-way schemes, the signal travels only from Alice to Bob; in the symmetric schemes, a central source sends signals to Alice and Bob. The primary benefit of the symmetric configuration is that both Alice and Bob may have passive setups (neither Alice nor Bob is required to make active changes for each run of the protocol). We show that all the schemes can be implemented with existing technology.

Z. D. Walton, A. V. Sergienko, B. E. A. Saleh, and M. C. Teich, "Noise-Immune Quantum Key Distr bution," in Quantum Communications and Cryptography, edited by A. V. Sergienko (CRC Press, Boca Raton, 2006), ch. 10, pp. 211-224.

10.1 Introduction

Of all the capabilities afforded by quantum information science [1], quantum key distribution (QKD; for a review, see Reference [2]) currently shows the most promise for practical implementation. Accordingly, there has been a concerted effort to develop QKD schemes that mitigate the technical challenges associated with existing approaches. Among the successes in this effort are the development of noise-immune (alignment-free) schemes for polarization [3] and time-bin [4–7] qubits. A further advance is the development of a symmetric scheme for time-bin qubits in which neither Alice nor Bob is required to make active changes to their setups [8]. Here we use the term symmetric to describe QKD schemes in which a central source distributes some number of photons to both Alice and Bob, so that they share entanglement. This is in contrast to round-trip and one-way configurations, in which the photons move according to Bob→Alice→Bob, and Alice→Bob, respectively. Here we show that symmetry and noise-immunity can be combined in a single implementation, for both polarization and time-bin qubits. Beginning with polarization-coded QKD, we first present a round-trip scheme in which noise-immunity is achieved by sampling the channel birefringence twice (once on the way from Bob to Alice and once on the way back). Second, we show how Klyshko's "advanced wave interpretation" (AWI) [9] can be used to transform this round-trip scheme into a one-way scheme imbued with passive detection. Third, we apply the AWI again to obtain a symmetric noise-immune scheme in which both Alice and Bob have passive setups. We then repeat these three steps for time-bin-coded QKD. For each scheme, we present a feasible implementation that relies only on current technology.

10.2 Noise-Immune Polarization-Coded Schemes

10.2.1 Round-Trip Noise-Immune Polarization-Coded QKD

The left column of Figure 10.1 shows the space-time diagrams of three noise-immune polarization-coded QKD schemes. For polarization qubits, noise-immune means that the scheme is immune to channel birefringence. The first scheme [Figure 10.1(A)] requires a round trip and is active (both Alice and Bob are required to make changes to their respective setups). The scheme runs as follows. Bob randomly chooses between polarization states $|V\rangle$ and $|H\rangle + |V\rangle$ (here, and for the rest of this chapter, we suppress normalization factors) and sends a single photon in that state to Alice. Alice uses a Faraday mirror to reflect that single photon back, and she also sends along an auxiliary unpolarized photon. Alice encodes a single bit by controlling the time ordering of the two photons she sends to Bob. Bob then measures each photon in the basis associated with the state of the initial photon he sent. Without knowing which state Bob sent to Alice, Eve cannot deterministically learn

Z. D. Walton, A. V. Sergienko, B. E. A. Saleh, and M. C. Teich, "Noise-Immune Quantum Key Distr bution," in Quantum Communications and Cryptography, edited by A. V. Sergienko (CRC Press, Boca Raton, 2006), ch. 10, pp. 211-224.

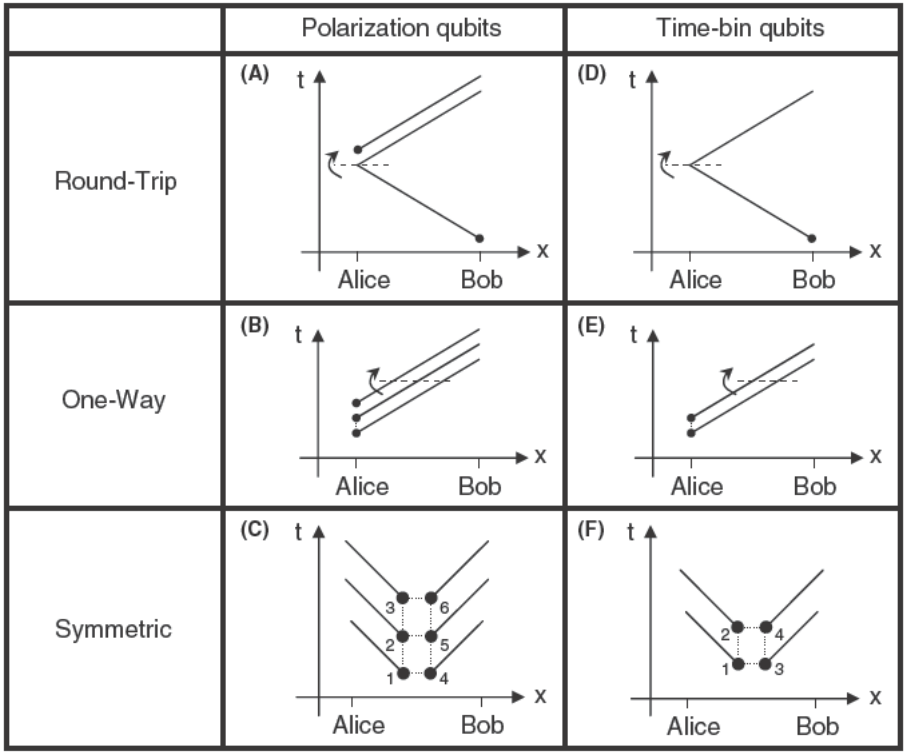


Figure 10.1 Space-time diagrams of six noise-immune QKD schemes organized by encoding (polarization or time-bin) and signal flow (round-trip, one-way, and symmetric). The dashed lines and curved arrows show how the advanced wave interpretation relates the round-trip schemes [(A) and (B)] to the one-way schemes [(B) and (C)], and the one-way schemes to the symmetric schemes [(C) and (F)]. The dotted lines connecting photons indicate entanglement. The photon labels in (C) and (F) are used later in this chapter.

Alice's bit setting. From Bob's point of view, the scheme is equivalent to Bennett's two-state protocol [10], since he is attempting to distinguish probabilistically between two nonorthogonal states. The noise-immune feature is derived from the unique property of the Faraday rotator: whatever the polarization transformation along the line from Bob to Alice, the photon that Alice reflects will arrive in Bob's laboratory in a polarization state orthogonal to its original state [11]. For example, if Bob sent $|V\rangle$, then either the first or the second photon he receives from Alice will be in the state $|H\rangle$. Thus if he measures one photon in state $|V\rangle$ and the other in state $|H\rangle$, he knows the value of Alice's bit. Any other detection pattern is ambiguous, and Alice and Bob discard these cases.

The AWI was originally conceived as a method for generating one-photon experiments from two-photon experiments. However, we may reverse this procedure and determine which two-photon state embodies the action of

Z. D. Walton, A. V. Sergienko, B. E. A. Saleh, and M. C. Teich, "Noise-Immune Quantum Key Distr bution," in Quantum Communications and Cryptography, edited by A. V. Sergienko (CRC Press, Boca Raton, 2006), ch. 10, pp. 211-224.

Alice's Faraday rotator. Using Faraday rotation as an example, the AWI associates the single-photon transformation

$$H_{\text{in}} \rightarrow V_{\text{out}} \qquad V_{\text{in}} \rightarrow H_{\text{out}} \tag{10.1}$$

with the two-photon state

$$|H_{\text{in}} V_{\text{out}}\rangle + |V_{\text{in}} H_{\text{out}}\rangle. \tag{10.2}$$

In going from Equation (10.1) to Equation (10.2), the propagation direction for H_{in} and V_{in} is reversed. To preserve the handedness of the coordinate system, one of the transverse directions must be reversed as well. This may be accomplished by replacing V_{in} with $-V_{\text{in}}$. Thus we see that the AWI associates Faraday rotation with the polarization singlet state $|HV\rangle - |VH\rangle$.

10.2.2 *One-Way Noise-Immune Polarization-Coded QKD*

We arrive at the one-way scheme of Figure 10.1(B) by "folding" the input arm of the Faraday rotator of Figure 10.1(A) along the dashed line, thereby replacing a round-trip single-photon space-time diagram with a one-way, two-photon space-time diagram (the dotted line connecting the two photons indicates entanglement). What follows is a passive-detection version of the three-photon scheme presented in Reference [3]. Alice sends three photons to Bob, with the first two (case 1), the last two (case 2), or the first and last (case 3) in the singlet state and the other photon unpolarized. Bob makes his measurements using the passive setup shown on the right side of Figure 10.2. By appropriate postselection, this setup effectively makes a random choice of two out of the three photons and brings them together on a nonpolarizing beam splitter, which serves to distinguish the singlet state from the other three Bell states [12]. Ignoring the first Mach–Zehnder interferometer (with relative

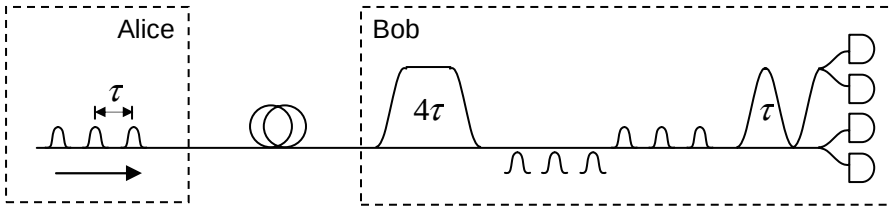


Figure 10.2 A schematic of one-way noise-immune polarization-coded QKD [see Figure 10.1(B)]. Alice sends three photons to Bob, with the first two (case 1), the last two (case 2), or the first and last (case 3) in the singlet state and the other photon unpolarized. The delay in Bob's first and second interferometer are 4τ and τ, respectively. Bob's apparatus effectively makes a random choice of two out of the three photons and brings them together on a nonpolarizing beam splitter, which serves to distinguish the singlet state from the other three Bell states [12]. The operation of the protocol is described in the text.

Z. D. Walton, A. V. Sergienko, B. E. A. Saleh, and M. C. Teich, "Noise-Immune Quantum Key Distr bution," in Quantum Communications and Cryptography, edited by A. V. Sergienko (CRC Press, Boca Raton, 2006), ch. 10, pp. 211-224.

delay 4τ) for the moment, we see that the second interferometer (with relative delay τ) enables the first two, or the last two, photons to meet at the second beam splitter of this interferometer. If these two photons are in the singlet state, they will leave by opposite ports. The contrapositive is also true: if they leave by the same port (and are detected by one of the pairs of detectors on each output port), then one can infer that they were not in the singlet state. Returning to the first interferometer, we see that this interferometer provides an opportunity for the first and last photons to be analyzed in a similar way. Thus Bob's apparatus probabilistically chooses a pair out of the three photons sent by Alice and determines whether the pair is in the singlet state or in some orthogonal state [22]. Based on his detections, Bob can rule out at most one of the three cases corresponding to Alice's possible signal states. Therefore, after Bob has made his detection, Alice announces whether the run was a "data run" (cases 1 or 2), or a "test run" (case 3). The data runs are used to share key material, and the test runs are used to monitor the eavesdropper. The scheme is noise-immune because the singlet state is immune to collective rotation.

10.2.3 *Symmetric Noise-Immune Polarization-Coded QKD*

We can apply the AWI one more time to get a six-photon symmetric scheme [Figure 10.1(C)] from the three-photon one-way scheme by folding along the dotted line in Figure 10.1(B). As indicated in Figure 10.1(C), this would yield a six-photon entangled state. It is currently not practical to create such a state; however, we can still implement the scheme using three pairs of entangled photons in the state

$$|\Phi^+\rangle_{14}|\Phi^+\rangle_{25}|\Phi^+\rangle_{36}, \tag{10.3}$$

where $|\Phi^+\rangle = |HH\rangle + |VV\rangle$. The execution of the protocol is similar to the one-way polarization protocol, except that instead of randomly choosing a three-photon state and sending it to Bob, Alice uses the the apparatus depicted in Figure 10.3 to choose randomly which pair of photons is in the singlet state. For example, if Alice obtains a triple coincidence that indicates that photons

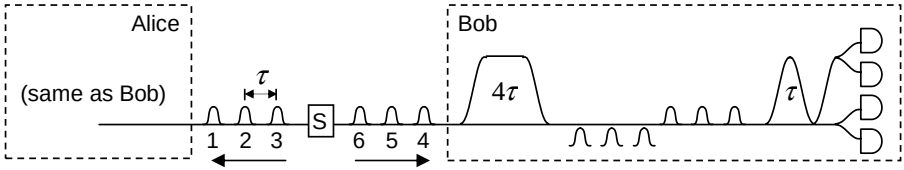


Figure 10.3 A schematic of symmetric noise-immune polarization-coded QKD [see Figure 10.1(C)]. A central source (S) emits three entangled pairs, so that Alice and Bob each get one from each pair. The scheme works much the same as the one-way scheme of Figure 10.2, except that Alice's apparatus makes a passive choice of the signal state that Bob receives, as described in the text.

Z. D. Walton, A. V. Sergienko, B. E. A. Saleh, and M. C. Teich, "Noise-Immune Quantum Key Distr bution," in Quantum Communications and Cryptography, edited by A. V. Sergienko (CRC Press, Boca Raton, 2006), ch. 10, pp. 211-224.

1 and 2 were in the singlet state, then she knows that photons 4 and 5 are also in the singlet state. This effect can be seen as an application of entanglement swapping [13]. A similar argument works for the other two possible photon pairs on Alice's side. Thus, on these occasions, she effectively prepares for Bob one of the three signal states from the one-way scheme of Figure 10.1(B). The protocol then runs exactly as that of Figure 10.1(B). The security of the scheme derives from the fact that only a triple of maximally entangled photon pairs will produce the correlations that Alice and Bob measure. Therefore the source can be controlled by the adversary without compromising security.

10.3 Noise-Immune Time-Bin-Coded Schemes

10.3.1 Round-Trip Noise-Immune Time-Bin-Coded QKD

Figure 10.4 contains a schematic and space-time diagram of round-trip noise-immune time-bin-coded QKD (originally introduced as plug-and-play quantum cryptography [4]). The protocol begins with Bob launching a strong

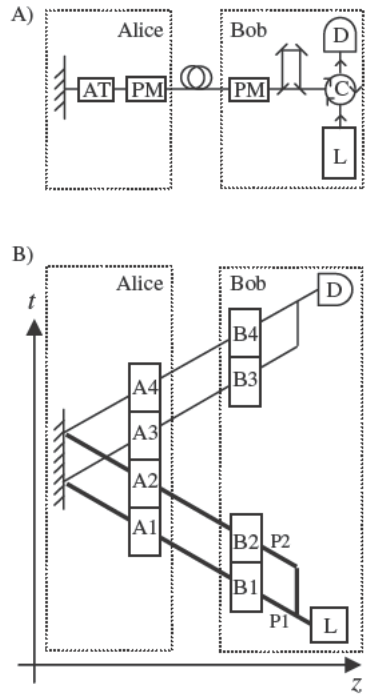


Figure 10.4 Schematic (A) and space-time diagram (B) for round-trip noise-immune time-bin-coded QKD. L is a source of laser pulses, C is a circulator, AT is an attenuator, and PM is a phase modulator.

Z. D. Walton, A. V. Sergienko, B. E. A. Saleh, and M. C. Teich, "Noise-Immune Quantum Key Distr bution," in Quantum Communications and Cryptography, edited by A. V. Sergienko (CRC Press, Boca Raton, 2006), ch. 10, pp. 211-224.

pulse from a laser (L) into a Mach–Zehnder interferometer via a circulator (C). This interferometer splits the pulse into an advanced amplitude (P1) and a retarded amplitude (P2). The amplitudes travel through phase modulators (PM) on Bob's side and Alice's side, and are then attenuated (AT) to the single photon level and reflected by Alice back to Bob. Although both P1 and P2 will again be split at Bob's Mach–Zehnder interferometer, by gating his detector appropriately, Bob can postselect those cases in which P1 takes the long path and P2 takes the short path on the return trip. Thus the interfering amplitudes experience identical delays on their round trip, ensuring insensitivity to drift in Bob's interferometer.

The role of the phase modulators can be readily understood by examining the space-time diagram of this protocol [see Figure 10.4(B)]. The eight boxes (A1–A4, B1–B4) refer to the phase settings on the two modulators as the two amplitudes pass through each of them twice. For example, B2 refers to the phase acquired by the delayed amplitude of the pulse that Bob sends to Alice, while B4 refers to the phase acquired by the same amplitude as it travels back from Alice to Bob. It should be understood that B1–B4 refer to settings of the same physical phase shifter at different times (and similarly for A1–A4). The probability of a detection at Bob's detector is given by

$$P_{\mathrm{d}} \propto 1 + \cos[(\mathrm{B2} - \mathrm{B1}) + (\mathrm{A2} - \mathrm{A1}) + (\mathrm{A4} - \mathrm{A3}) + (\mathrm{B4} - \mathrm{B3})]. \qquad (10.4)$$

From this expression we see that only the relative phase between the phase modulator settings affects the probability of detection. Thus, by setting $\mathrm{B1} = \mathrm{B2}$ and $\mathrm{A1} = \mathrm{A2}$, Alice and Bob can implement the interferometric version of BB84 [14] by encoding their cryptographic key in the difference settings $\Delta\phi_A \equiv \mathrm{A4} - \mathrm{A3}$ and $\Delta\phi_B \equiv \mathrm{B4} - \mathrm{B3}$. Since the resulting expression

$$P_{\mathrm{d}} \propto 1 + \cos(\Delta\phi_A + \Delta\phi_B) \qquad (10.5)$$

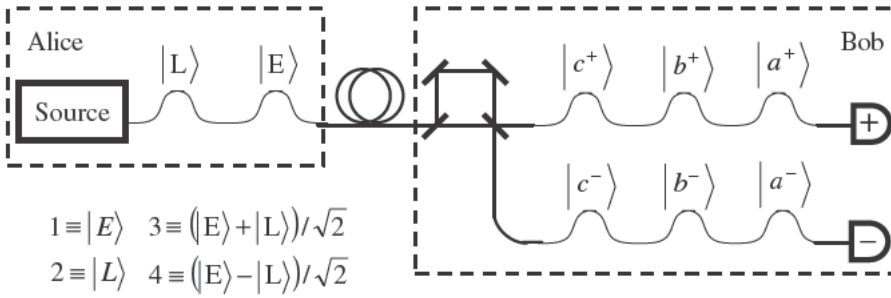
is independent of the time delay in Bob's interferometer and the absolute phase settings in either modulator, Alice and Bob are able to achieve high-visibility interference without initial calibration or active compensation of drift.

10.3.2 *One-Way Noise-Immune Time-Bin-Coded QKD*

In this section, we describe a one-way noise-immune time-bin-coded QKD scheme. The scheme also allows for Bob's apparatus to be passive. Before presenting the full scheme, we review a non-noise-immune QKD scheme that motivates the technique used to combine noise-immunity and passive detection.

The two-photon quantum key distribution scheme described in Reference [8] has the remarkable property that both Alice and Bob use passive detection (i.e., they are not required to switch between conjugate measurement bases). In Reference [2], Gisin et al. suggest applying the AWI to generate an associated one-photon scheme. We present a specific implementation of this one-photon scheme here to show that it achieves passive detection by enlarging the Hilbert space (see Figure 10.5). Let the advanced and delayed

Z. D. Walton, A. V. Sergienko, B. E. A. Saleh, and M. C. Teich, "Noise-Immune Quantum Key Distr bution," in Quantum Communications and Cryptography, edited by A. V. Sergienko (CRC Press, Boca Raton, 2006), ch. 10, pp. 211-224.



		Time of Detection		
		$\|a^{\pm}\rangle$	$\|b^{\pm}\rangle$	$\|c^{\pm}\rangle$
Detector	+	{2,3,4}	{1,2,4}	{1,3,4}
	−	{2,3,4}	{1,2,3}	{1,3,4}

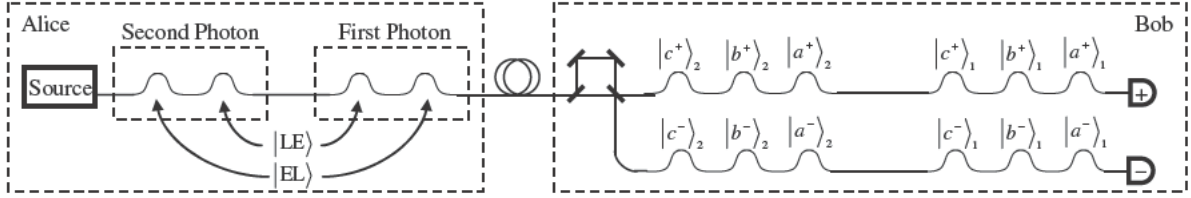
Figure 10.5 A single-photon implementation of BB84 suggested in Reference [2]. The kets |E⟩ and |L⟩ correspond respectively to an advanced (early) and a delayed (late) single-photon wavepacket. Alice sends one of the four states listed below the diagram of the apparatus. The chart indicates which of Alice's states are consistent with a given measurement event at Bob's side. As described in the text, Bob's apparatus does not require active change of measurement basis.

single-photon wavepackets be associated with the poles of the Poincaré sphere. The four states required for BB84 are typically taken from the equator, since a single Mach–Zehnder interferometer can be used to generate any of the equatorial states. Instead, we imagine using two antipodal points on the equator and the poles themselves. Bob analyzes the signal from Alice with a Mach–Zehnder interferometer, recording which detector fired (one of two possibilities) at which time (one of three possibilities). When Bob's detection is in the first or third time positions, he can reliably distinguish between the pole states based on the time of detection. When his detection is in the second time position, he can reliably distinguish between the equatorial states based on which detector fired. Thus Bob is no longer obliged to make an active change to his apparatus to effect the requisite change of basis [23].

To see how this passive detection is derived from enlargement of the Hilbert space, consider the quantum state of Alice's signal after Bob's Mach–Zehnder interferometer. Alice's four states of one qubit are mapped onto four mutually nonorthogonal states of a six-state quantum system (see Figure 10.5). Thus by mapping a two-state quantum system into a six-state quantum system, Bob is able to perform his part of the BB84 protocol with a fixed-basis measurement in the six-state Hilbert space [24].

Next we present a scheme that combines passive detection with one-way noise-immunity (see Figure 10.6). This scheme follows from that presented

Z. D. Walton, A. V. Sergienko, B. E. A. Saleh, and M. C. Teich, "Noise-Immune Quantum Key Distr bution," in Quantum Communications and Cryptography, edited by A. V. Sergienko (CRC Press, Boca Raton, 2006), ch. 10, pp. 211-224.



$1 \equiv |EL\rangle$
$2 \equiv |LE\rangle$
$3 \equiv (|EL\rangle + |LE\rangle)/\sqrt{2}$
$4 \equiv (|EL\rangle - |LE\rangle)/\sqrt{2}$

(+,–)→ Detector "+" fired for the first photon and detector "–" fired for the second photon.

Time of Det. of Second Photon	Time of Detection of First Photon: $\|c^{\pm}\rangle_1$	$\|b^{\pm}\rangle_1$	$\|a^{\pm}\rangle_1$
$\|c^{\pm}\rangle_2$	(+,+) { } (–,+) { }	(+,+){1,3,4} (–,+){1,3,4}	(+,+){1,3,4} (–,+){1,3,4}
	(+,–) { } (–,–) { }	(+,–){1,3,4} (–,–){1,3,4}	(+,–){1,3,4} (–,–){1,3,4}
$\|b^{\pm}\rangle_2$	(+,+){2,3,4} (–,+){2,3,4}	(+,+){1,2,3} (–,+){1,2,4}	(+,+){1,3,4} (–,+){1,3,4}
	(+,–){2,3,4} (–,–){2,3,4}	(+,–){1,2,4} (–,–){1,2,3}	(+,–){1,3,4} (–,–){1,3,4}
$\|a^{\pm}\rangle_2$	(+,+){2,3,4} (–,+){2,3,4}	(+,+){2,3,4} (–,+){2,3,4}	(+,+) { } (–,+) { }
	(+,–){2,3,4} (–,–){2,3,4}	(+,–){2,3,4} (–,–){2,3,4}	(+,–) { } (–,–) { }

Figure 10.6 A schematic of one-way noise-immune time-bin-coded QKD [see Figure 10.1(E)]. Two time-bin qubits are sent from Alice to Bob in one of the four quantum states on the left of the figure. The chart on the right uses two levels of structure to describe the detection pattern at Bob's side. The coarse structure is defined by the bold lines. Each of the nine bold-lined rectangles corresponds to a specification of the joint time of detection of the two photons. The fine structure is defined by the thin lines. Each of the four thin-lined rectangles within a bold-lined rectangle corresponds to a specification of which detector fired for each of the two photons (this coding is illustrated by an example at the bottom left of the figure). The numbers in the curly brackets in each thin-lined rectangle indicate which (if any) of the four quantum states on the left are consistent with the corresponding detection pattern.

Z. D. Walton, A. V. Sergienko, B. E. A. Saleh, and M. C. Teich, "Noise-Immune Quantum Key Distr bution," in Quantum Communications and Cryptography, edited by A. V. Sergienko (CRC Press, Boca Raton, 2006), ch. 10, pp. 211-224.

in Reference [6], just as the preceding single-photon scheme follows from the traditional phase-coding implementation. Let the states $|1\rangle$ and $|2\rangle$ in Figure 10.6 be associated with the poles of the Poincaré sphere. Instead of using equatorial states and forcing Bob to postselect those cases for which the advanced (delayed) amplitudes take the long (short) path, we use two equatorial points ($|3\rangle$ and $|4\rangle$) and the poles themselves to make up Alice's four signal states. Signal states that are consistent with a given joint detection are presented in the chart. As seen in Figure 10.5, each photon can lead to six different detection events. Thus, since the new protocol involves two photons, there are 36 possible detection events (see Figure 10.6).

The protocol operates as follows. As in BB84, Alice and Bob publicly agree on an association of each of the four signal states (see Figure 10.6) with logical values 0 or 1 (i.e., $1 \rightarrow 0$, $2 \rightarrow 1$, $3 \rightarrow 0$, $4 \rightarrow 1$). For each run of the experiment, Alice randomly chooses one of the four signal states and sends it to Bob. When Bob detects both photons in their respective middle time slots, he has effectively measured in the {3, 4} basis (the "phase" basis). When Bob detects both photons in their early time slots, or both photons in their late time slots, he has effectively measured in the {1, 2} basis (the "time" basis) [25]. After the quantum transmission, Alice and Bob publicly announce their bases. On the occasions when their bases match, Bob is able to infer the state that Alice sent, based on his detection pattern using the chart in Figure 10.6. As in single-qubit BB84, the occasions in which their bases do not match are discarded. The scheme achieves passive detection (Bob is not required to make any active changes to his apparatus) and noise-immunity (the phase delay in Bob's interferometer does not affect any measured probabilities). The intrinsic efficiency of the scheme is 1/4, compared to 1/2 for single-qubit BB84.

A proposed implementation for the source employed in Figure 10.6 is presented in Figure 10.7. First, a pair of noncollinear, polarization-entangled photons is produced via type-II spontaneous parametric down-conversion from a nonlinear crystal pumped by a brief pulse [26]. Second, the modulating element M performs one of four functions (filters one of the two polarization modes, or introduces one of two relative phases between the two polarization modes), based on Alice's choice of signal states. Third, the two

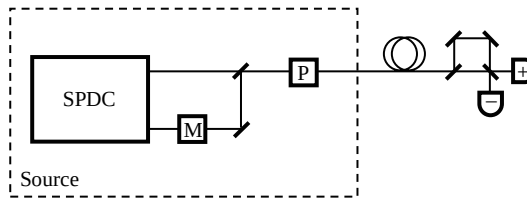


Figure 10.7 A proposed implementation for the source employed in Figure 10.6. SPDC is a nonlinear crystal pumped by a brief pulse to produce a noncollinear, polarization-entangled two-photon state via spontaneous parametric down-conversion. The action of elements M and P is described in the text.

Z. D. Walton, A. V. Sergienko, B. E. A. Saleh, and M. C. Teich, "Noise-Immune Quantum Key Distr bution," in Quantum Communications and Cryptography, edited by A. V. Sergienko (CRC Press, Boca Raton, 2006), ch. 10, pp. 211-224.

beams are combined with a relative temporal delay that matches the temporal delay that Bob will subsequently introduce with his Mach–Zehnder interferometer. This stage converts the photon pair from a pair of spatially defined polarization-entangled qubits to a pair of polarization-defined time-bin-entangled qubits. Finally, the element labeled P (for polarization) delays and rotates one of the polarization modes by a duration much greater than the delay of the third step, so that the delayed portion of the state is in the same polarization mode as the nondelayed portion. Thus the two photons sent from Alice to Bob have the wavepacket structure illustrated at the top of Figure 10.6.

There are two noteworthy aspects of the configuration in Figure 10.7. First, the technique introduced in Reference [8] for creating time-bin-entangled photons pairs only leads to superpositions of the correlated possibilities (i.e., $|\mathrm{EE}\rangle$ and $|\mathrm{LL}\rangle$). The source presented in Figure 10.7 enables arbitrary superpositions of the anticorrelated possibilities (i.e., $|\mathrm{EL}\rangle$ and $|\mathrm{LE}\rangle$). Furthermore, the correlated states can easily be created from this source by rotating the polarization axes at element M in Figure 10.7. In this way, all four time-bin-entangled Bell states can be conveniently generated with this source. Second, the interference in Bob's interferometer results from the indistinguishability of photon amplitudes that were initially in the same polarization mode. This is in contrast to configurations in which photon amplitudes from different polarization modes are made indistinguishable by use of a polarization analyzer. Thus the reduction in visibility that has come to be associated with extremely brief pump pulses [15] will not be present in this scheme. Note that a symmetrization method has been developed to restore visibility for experiments using polarization-entangled photons created by such a short pulse pump [16,17].

10.3.3 *Symmetric Noise-Immune Time-Bin-Coded QKD*

In the symmetric time-bin scheme of Figure 10.1(F), the source produces a four-photon entangled state. As it is currently not practical to create such a state, we achieve the same result in Figure 10.8 by using two entangled pairs in the state

$$(|EE\rangle_{13} + |LL\rangle_{13})(|EE\rangle_{24} + |LL\rangle_{24}), \tag{10.6}$$

where E and L stand for early and late, respectively. The source apparatus consists of three switches, while Alice and Bob simply have Mach–Zehnder interferometers. The switches in the source behave as follows. The first switch (SW1) directs photon 1 along the lower path and photon 2 along the upper path. The action of the second switch (SW2) is indicated by the labels t and r, which stand for transmit and reflect, respectively. Thus for the early amplitude of photon 1 and the late amplitude of photon 2, SW2 reflects; otherwise it transmits. The third switch (SW3) directs the photons 5 and 6 onto the same output fiber. By postselecting only those occasions when one photon is found in the positions labeled 5 and 6, Alice effectively creates the

Z. D. Walton, A. V. Sergienko, B. E. A. Saleh, and M. C. Teich, "Noise-Immune Quantum Key Distr bution," in Quantum Communications and Cryptography, edited by A. V. Sergienko (CRC Press, Boca Raton, 2006), ch. 10, pp. 211-224.

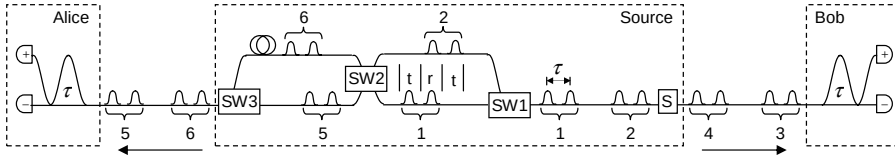


Figure 10.8 A schematic of symmetric noise-immune time-bin-coded QKD [see Figure 10.1(F)]. A central source (S) emits two separately entangled photon pairs [see Equation (10.6)]. One photon from each pair is sent to Bob. The other two photons are sent through a series of three switches. The first switch (SW1) directs photon 1 along the lower path and photon 2 along the upper path. The action of the second switch (SW2) is indicated by the labels t and r, which stand for transmit and reflect, respectively. The third switch (SW3) directs photons 5 and 6 onto the same output fiber. By postselecting the cases in which one photon is in position 5 and one photon is in position 6, Alice effectively creates the four-photon entangled state in Equation (10.7). This state is then analyzed by Alice and Bob with their Mach–Zehnder interferometers, each of which has a delay equal to τ. The protocol used to establish a shared key is described in the text.

four-photon entangled state

$$|ELLE\rangle_{5634} + |LEEL\rangle_{5634}. \tag{10.7}$$

When all the amplitudes follow the pattern ($E \rightarrow$long path, $L \rightarrow$ short path) in Alice's and Bob's Mach–Zehnder interferometers, Alice and Bob announce that they have measured in the phase basis, and they use the chart in Figure 10.9 to infer the bit value. When one photon on each side does not

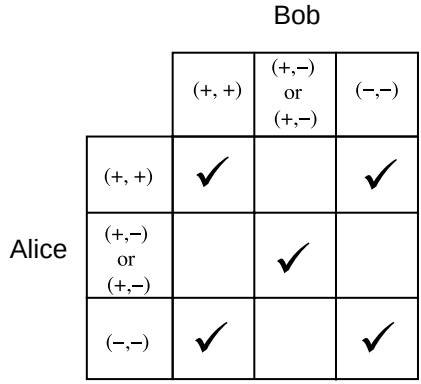


Figure 10.9 Possible joint detection patterns for the scheme of Figure 10.8. The expression $(+, -)$ indicates that the $+$ detector fired for the first photon and the $-$ detector for the second. Given that the source produces the state in Equation (10.6), when all the amplitudes follow the pattern ($E \rightarrow$ long, $L \rightarrow$ short) in Alice's and Bob's Mach–Zehnder interferometers, the unchecked joint detection patterns do not occur because of destructive interference. Thus Alice and Bob may use a publicly known encoding (e.g., $\{(+, +), (-, -)\} \rightarrow 0$, $\{(+, -), (-, +)\} \rightarrow 1$) to agree on a secret key bit.

Z. D. Walton, A. V. Sergienko, B. E. A. Saleh, and M. C. Teich, "Noise-Immune Quantum Key Distr bution," in Quantum Communications and Cryptography, edited by A. V. Sergienko (CRC Press, Boca Raton, 2006), ch. 10, pp. 211-224.

follow the pattern ($E \rightarrow$ long, $L \rightarrow$ short), Alice and Bob announce that they have measured in the time basis. On these occasions, they each know which of the superposed terms in Equation (10.7) was realized, and they use this knowledge to establish a shared bit. The scheme is noise-immune because on the phase-basis occasions, each leg of the two Mach–Zehnder interferometers is traversed by one of the four photons. Thus the relative phase along the two paths of each interferometer factors out and does not affect the measured results. The scheme is passive because neither Alice nor Bob is required to make active changes to their apparatus.

The security of the scheme derives from the fact that only the state in Equation (10.6) will produce the correlations that Alice and Bob measure. Therefore the source can be controlled by the adversary without compromising security. This technique can be viewed as the time-bin analog of the polarization based entanglement distillation experiment described in Reference [18].

10.4 Discussion

We have presented round-trip, one-way, and symmetric noise-immune QKD schemes that can be implemented with existing technology for both polarization and time-bin qubits. The noise-immunity of the schemes makes active compensation of interferometric drift and channel birefringence unnecessary. The round-trip methods are the simplest, since they do not involve entanglement. However, the bidirectional flow of signals leaves an opportunity for an eavesdropper to compromise the security of the link by sending signals into the apparatus of Alice and/or Bob and measuring the state of the reflected signal. The one-way schemes remove this security concern at the cost of requiring a multi-photon entangled state. A further advantage of the one-way schemes presented here is that they do not require Bob to make active changes to his apparatus. Finally, the symmetric schemes presented here achieve noise-immunity while requiring neither Bob nor Alice to make active changes to his/her apparatus. The cost of this simplicity is a doubling of the number of photons involved in each run of the protocol.

It is interesting to observe that discoveries in the field of quantum information (entanglement swapping and entanglement distillation) can be naturally related to other areas of quantum information theory (quantum error correction and decoherence-free subpaces) via the AWI, as demonstrated in Figure 10.1. Since the central goal of quantum computation is a "folding in time" of a classical computation, the AWI may yield insight into the mechanisms behind the speed-up achieved by certain quantum computation algorithms.

References

1. M.A. Nielsen and I.L. Chuang, *Quantum Computing and Quantum Information*, Cambridge University Press, Cambridge, 2000.
2. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Rev. Mod. Phys.*, 74, 145, 2002.

Z. D. Walton, A. V. Sergienko, B. E. A. Saleh, and M. C. Teich, "Noise-Immune Quantum Key Distr bution," in Quantum Communications and Cryptography, edited by A. V. Sergienko (CRC Press, Boca Raton, 2006), ch. 10, pp. 211-224.

3. J.-C. Boileau, D. Gottesman, R. Laflamme, D. Poulin, and R. Spekkens, quant-ph/0306199, 2003.
4. A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, *Appl. Phys. Lett.*, 70, 793, 1997.
5. D.S. Bethune and W.P. Risk, *IQEC'98 Digest of Postdeadline Papers,* 12–2, 1998.
6. Z. Walton, A.F. Abouraddy, A.V. Sergienko, B.E.A. Saleh, and M.C. Teich, *Phys. Rev.* A, 67, 062309, 2003.
7. Z. Walton, A.F. Abouraddy, A.V. Sergienko, B.E.A. Saleh, and M.C. Teich, *Phys. Rev. Lett.*, 91, 087901, 2003.
8. J. Brendel, N. Gisin, W. Tittel, and H. Zbinden, *Phys. Rev. Lett.,* 82, 2594, 1999.
9. A.V. Belinsky and D.N. Klyshko, *Laser Phys.* (Moscow), 2, 112, 1992.
10. C.H. Bennett, *Phys. Rev. Lett.,* 68, 3121, 1992.
11. M. Martinelli, *Opt. Comm.,* 72, 341, 1989.
12. S.L. Braunstein and A. Mann, *Phys. Rev.* A, 51, R1727, 1995.
13. M. Zukowski, A. Zeilinger, M.A. Horne, and A.K. Ekert, *Phys. Rev. Lett.,* 71, 4287, 1993.
14. C.H. Bennett and G. Brassard, *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing,* 175–179, 1984.
15. T.E. Keller and M.H. Rubin, *Phys. Rev.* A, 56, 1534, 1997.
16. F. De Martini, G. Di Giuseppe, and S. Pádua, *Phys. Rev. Lett.,* 87, 150401, 2001.
17. Y.-H. Kim and W.P. Grice, *J. Mod. Optics,* 49, 2309, 2002.
18. T. Yamamoto, M. Koashi, S.K. Ozdemir, and N. Imoto, *Nature,* 421, 343, 2003.
19. H. Bechmann-Pasquinucci and W. Tittel, *Phys. Rev.* A, 61, 62308, 2000.
20. K. Inoue, E. Waks, and Y. Yamamoto, *Phys. Rev. Lett.,* 89, 37902, 2002.
21. W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, *Phys. Rev. Lett.*, 84, 4737, 2000.
22. One can always convert an active-detection scheme to a passive-detection scheme by using a beam splitter to probabilistically send the received photon(s) to one of some number of separate detection setups. A drawback of this approach is that the number of optical elements required is increased. The passive schemes described in this chapter, like that in Reference [8], are "intrinsically passive," in that they achieve passive operation without increasing the number of optical elements required.
23. The idea of using pole states is explored in Reference [19]; however, that paper does not mention the possibility of passive detection.
24. A similar idea is presented in Reference [20]. In that paper, Alice uses four states of a three-state quantum system, and Bob achieves passive detection by mapping Alice's three-state quantum system into an eight-state quantum system.
25. On the occasions when Bob's detection pattern is (early, middle), (middle, early), (middle, late), or (late, middle), he has also effectively measured in the time basis. However, to simplify the analysis by making the probability of successful bit-sharing independent of the basis in which Alice sent, we consider only the extreme cases (early, early) and (late, late) as valid time-basis detections.
26. A femtosecond pump pulse is typically desired for experiments involving the simultaneous creation of multiple down-converted photon pairs [16]. Our implementation does not require such a brief pump pulse and will work with a picosecond laser, such as that used in Reference [21].

Z. D. Walton, A. V. Sergienko, B. E. A. Saleh, and M. C. Teich, "Noise-Immune Quantum Key Distr bution," in Quantum Communications and Cryptography, edited by A. V. Sergienko (CRC Press, Boca Raton, 2006), ch. 10, pp. 211-224.