Entanglement-secured single-qubit quantum secret sharing

P. Scherpelz,[*] R. Resch,[†] D. Berryrieser,[‡] and T. W. Lynn[§]
Department of Physics, Harvey Mudd College, 301 Platt Boulevard, Claremont, California 91711, USA
(Received 22 April 2011; published 2 September 2011)

In single-qubit quantum secret sharing, a secret is shared between N parties via manipulation and measurement of one qubit at a time. Each qubit is sent to all N parties in sequence; the secret is encoded in the first participant's preparation of the qubit state and the subsequent participants' choices of state rotation or measurement basis. We present a protocol for single-qubit quantum secret sharing using polarization entanglement of photon pairs produced in type-I spontaneous parametric downconversion. We investigate the protocol's security against eavesdropping attack under common experimental conditions: a lossy channel for photon transmission, and imperfect preparation of the initial qubit state. A protocol which exploits *entanglement* between photons, rather than simply polarization *correlation*, is more robustly secure. We implement the entanglement-based secret-sharing protocol with 87% secret-sharing fidelity, limited by the purity of the entangled state produced by our present apparatus. We demonstrate a photon-number splitting eavesdropping attack, which achieves no success against the entanglement-based protocol while showing the predicted rate of success against a correlation-based protocol.

DOI: 10.1103/PhysRevA.84.032303 PACS number(s): 03.67.Dd, 03.67.Hk

I. INTRODUCTION

Secret sharing is the general term for a communication task in which one participant (the sender) wants to share a message with multiple other participants (the recipients) in a way that forces the recipients to cooperate with one another to reconstruct the message. The task is relevant when recipients are considered more trustworthy as a group than individually. In the strongest version of secret sharing, the message can be fully reconstructed by the full set of $N-1$ recipients; however, any subset of $N-2$ or fewer recipients possesses zero information regarding the message. This task can be implemented classically by distributing between $N-1$ recipients $N-2$ randomly generated bit strings, or "shadows," and a final $(N-1)$th shadow string which is the bitwise sum or XOR of the other $N-2$ strings and the original message. All $N-1$ recipients together can reconstruct the message by taking the XOR of their shadows; however, any proper subset of recipients possesses no information about the message.

Classical secret sharing protocols generally do not involve the secure transmission of the shadows, leaving this task to cryptographic protocols. The emerging field of quantum cryptography hinges on the secure transmission of information encoded in quantum states. Thus by using quantum states to encode and distribute the shadows, secure communication can be built into a secret sharing protocol; quantum-state resources enhance the sharing of classical bit-string sequences. Such quantum-mechanical resources can be brought to the task of secret sharing in several distinct ways.

The original quantum secret sharing protocol, presented in 1999 [1], requires the use of a multipartite entangled state. Specifically, to share a single-bit secret between a sender and $N-1$ recipients, the N-qubit entangled state $\frac{1}{\sqrt{2}}[|0\rangle_1|0\rangle_2\cdots|0\rangle_N+|1\rangle_1|1\rangle_2\cdots|1\rangle_N]$ must be produced, and the individual qubits distributed between the participants. This quantum secret sharing protocol is in principle quite powerful. It allows participants to share secrets composed not only of bit values (0 or 1) but of complete qubits (quantum states of the form $a|0\rangle+e^{i\varphi}b|1\rangle$). The production of multipartite entangled states is unfortunately a technical challenge, requiring an experimental tour de force at each realization [2–6].

Single-qubit quantum secret sharing (SQQSS), by contrast, was first proposed and demonstrated in 2005 [7,8] using photon pairs produced by type-II spontaneous parametric downconversion (SPDC). The protocol involves the transmission of a single qubit $a|0\rangle+e^{i\varphi}b|1\rangle$ through the entire sequence of participants. The sender prepares a state with a specific value of φ and each recipient performs a simple operation to alter φ. The final participant performs a measurement on the qubit whose outcome depends on the final value of φ, and the secret—the initial φ value—can be reconstructed only when all recipients reveal their individual operations. Such a protocol uses quantum resources to allow secure sharing of a classical secret, but does not enable the more powerful sharing of a full quantum-state secret. On the other hand, SQQSS relies on physical states which can be easily produced and manipulated in the laboratory, allowing for the straightforward realization of the protocols and demonstration of their successes and vulnerabilities. The original SQQSS protocol, with proposed precautions and coding repetitions [9,10], provides security against numerous cheating attacks by a subset of recipients.

In this work, we experimentally implement two variations on the protocol of [7,8], adapted for use with type-I SPDC. One version, like the original, relies only on polarization correlation in photon pairs; the other directly exploits the quantum entanglement between photons. We note the relative

[*]Present address: Department of Physics, University of Chicago, 5720 S. Ellis Ave, Chicago, IL 60637.
[†]Present address: SLAC National Accelerator Laboratory, 2575 Sand Hill Road, Menlo Park, CA 94025-7015.
[‡]Present address: Department of Applied Physics, 348 Via Pueblo Mall, Stanford University Stanford, CA 94305-4090.
[§]lynn@hmc.edu

strengths and weaknesses of the two versions. In particular, we develop and implement a photon-number splitting (PNS) eavesdropping attack; in the presence of a lossy transmission channel and imperfect state preparation, this eavesdropping attack works against the correlation-based protocol but fails against the entanglement-secured version.

II. SINGLE-QUBIT QUANTUM SECRET SHARING SCHEMES USING TYPE-I SPDC

A. Correlation-based protocol

The SQQSS protocol relies on the secure transmission of one qubit to a number of participants sequentially. In order to prevent individual participants from cheating, however, this *signal* qubit must be produced and detected in correlation with a partner qubit, called the *idler*. In both the original version [7] and our own variation, the qubits are encoded in the polarizations of a pair of photons produced in SPDC. Thus henceforth we will refer specifically to polarization states of photons rather than to generic two-state quantum systems. Our correlation-based protocol for type-I SPDC closely follows the original treatment of [7] for the type-II case.

The sharing of a secret begins with the creation of a pair of photons in the polarization-entangled state,

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle), \tag{1}$$

where H denotes horizontal polarization and V vertical polarization of each photon. The idler photon passes through a polarizer oriented to transmit $|H\rangle$, while the signal photon passes through a chain of SQQSS participants. Taken on its own, the polarization state of the signal photon as it enters the SQQSS chain is undefined. However, the final step in the protocol is the detection of the signal and idler photons in coincidence with one another. This coincidence detection projects the signal photon, at its entry into the SQQSS chain, into the state $|H\rangle$.

The SQQSS chain is shown conceptually in Fig. 1. It begins with the sender, who uses a combination of wave plates to transform the signal photon to one of the four states,

$$\begin{aligned} |+x\rangle &= \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle), \\ |+y\rangle &= \frac{1}{\sqrt{2}}(|H\rangle + i|V\rangle), \\ |-x\rangle &= \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle), \\ |-x\rangle &= \frac{1}{\sqrt{2}}(|H\rangle - i|V\rangle). \end{aligned} \tag{2}$$

This is equivalent to the preparation of $|+x\rangle$ followed by use of a tilt-adjustable phase plate to obtain one of $|\pm x\rangle, |\pm y\rangle$, as shown in Fig. 1. The signal photon then passes to $N-1$ recipients in turn; each one uses a tilt-adjustable phase plate to apply a randomly selected phase shift $\varphi_j \in \{0, \pi/2, \pi, 3\pi/2\}$ so that after participant k, the signal photon state is

$$|\chi_k\rangle = \frac{1}{\sqrt{2}}\left[|H\rangle + \exp\left(i\sum_{j=1}^{k}\varphi_j\right)|V\rangle\right]. \tag{3}$$

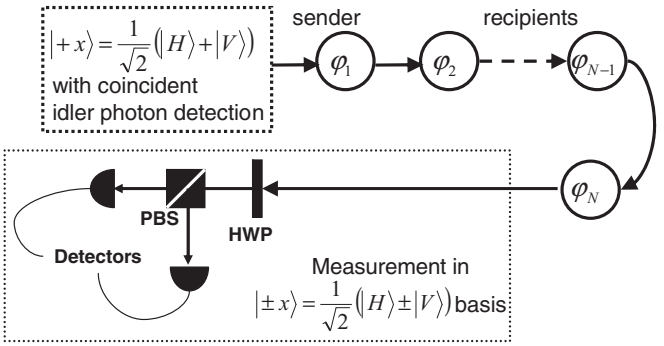

FIG. 1. A schematic of the single-qubit quantum secret sharing protocol. The qubit is initially in the state $|+x\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$, conditioned on coincident detection of the idler photon (gating). Each participant applies a relative phase shift $\varphi_j \in \{0, \pi/2, \pi, 3\pi/2\}$ to the $|V\rangle$ component. The half wave plate (HWP) and polarizing beam splitter (PBS) allow for measurement of the final state in the $|\pm x\rangle = \frac{1}{\sqrt{2}}(|H\rangle \pm |V\rangle)$ basis.

Overall, j ranges from 1 to N to account for the sender ($i = 1$) and $N-1$ recipients. The set of four possible phase shifts can be broken down into two classes:

$$\begin{aligned} \text{class } X &\Rightarrow \varphi_j \in \{0, \pi\}, \\ \text{class } Y &\Rightarrow \varphi_j \in \{\pi/2, 3\pi/2\}. \end{aligned} \tag{4}$$

The sender's choice of state preparation likewise falls into either class X, for creation of $|\pm x\rangle$, or class Y, for creation of $|\pm y\rangle$.

Thus each participant so far possesses a single "class" bit denoting which class they have chosen, but also a second "secret" bit consisting of their phase choice within that class. After N participants have applied their local operations, the initial signal photon state $|H\rangle$ is transformed to the state

$$|\chi_N\rangle = \frac{1}{\sqrt{2}}\left[|H\rangle + \exp\left(i\sum_{j=1}^{N}\varphi_j\right)|V\rangle\right]. \tag{5}$$

These phase changes are illustrated in Fig. 1.

At this point, the final participant measures the polarization of the signal photon in the $|\pm x\rangle = (1/\sqrt{2})(|H\rangle \pm |V\rangle)$ basis, conducting the measurement in coincidence with the idler photon as specified earlier. The measurer records the measurement outcome, and the physical aspect of the SQQSS is complete.

Notice that if the final state is of the form

$$|\chi_N\rangle = \frac{1}{\sqrt{2}}(|H\rangle \pm |V\rangle), \tag{6}$$

then the measurement outcome will be $|+x\rangle$ or $|-x\rangle$, each with probability 1. However, if

$$|\chi_N\rangle = \frac{1}{\sqrt{2}}(|H\rangle \pm i|V\rangle), \tag{7}$$

the final measurement result will be random.

Therefore, after the measurement is performed, the N participants publicly announce the class of the operation they applied, and the total number of class Y operations is counted. If the number of class Y operations was even, the run is valid; the $N-1$ recipients can expect to reconstruct the secret from

their shadows. If the number of class Y operations was odd, then the run is discarded; this happens half the time on average.

For valid runs, the remaining secret bit value retained by each participant regarding their applied operation constitutes that participant's shadow (or the sender's secret). The last participant also holds the record of the measurement outcome. Only if the $N-1$ recipients share their shadows can they determine the sender's secret, φ_1.

Finally, to prevent cheating, a random subset of the bits must be checked. To do this, the first N participants announce in random order their actual phase changes φ_j for a subset of runs randomly selected by the sender. The expected measurement result for each run is computed and compared to the measurement result announced by the final participant. If any recipient attempts to cheat by measuring the single-photon state and sending a newly prepared version along to subsequent participants, the bit error rate rises to at least 25%. Thus if the protocol shows an error rate of less than 25%, cheating of this form can be ruled out.

Restrictions on the order of the class announcements, along with repetitions of the protocol with coding enhancements, can be implemented to make the protocol more secure, defending even against cheaters with their own entangled-pair resources [10]. Alternately, the protocol can defend against cheating by a subset of recipients (participants 2 through N) via a simpler modification: instead of measuring the signal photon, participant N is required to transmit it back to the sender, participant 1. The sender then measures the photon in either the $|\pm x\rangle$ or $|\pm y\rangle$ basis, but all recipients announce their class choices before the sender announces the sending and measurement classes. Runs with even numbers of class X operations, *including the measurement class*, are considered valid. This protocol defends against cheating, even with entangled-pair resources, by any subset of the recipients. It privileges the trusted sender of the message, but the sender already occupies a position of trust by knowing the original secret, in many if not all possible applications.

B. Entanglement-based protocol

In both type-I protocols, the signal and idler photons are first generated as the entangled pair of Eq. (1). In the correlation-based protocol, all measurements are done in coincidence with detection of the idler photon in the state $|H\rangle$. Thus the signal photon is projected into the state $|H\rangle$ as well, and then rotated into $|\pm x\rangle$ or $|\pm y\rangle$ state afterwards by means of phase-shifting optics. As pointed out in Refs. [7,8], the polarization correlation between the signal and idler photons is crucial for the security of the protocol; a cheater or eavesdropper, who does not have access to the idler photon, therefore has no information on the initial polarization of the signal photon. Because the signal photon's initial state is ill-defined, subsequent measurements by the cheater cannot reveal information about the phase changes applied by sender or recipients.

However, while the correlation-based protocol relies on the polarization correlation between signal and idler, it does not rely explicitly on the quantum entanglement between them. This insensitivity to entanglement *per se* can be viewed as a strength of the protocol, giving robustness against imperfect entanglement in the form of a lack of coherence between the two terms in the superposition of Eq. (1). However, by failing to fully exploit the quantum entanglement in the initial resource the correlation-based protocol passes up a chance for enhanced security against eavesdropping attacks, as we demonstrate in the next section.

The entanglement-based protocol which follows makes full and explicit use of the entanglement between signal and idler in order to prepare the signal photon in the state $|+x\rangle$ before it enters the chain of SQQSS participants. Unlike a classical mixture, the initial entangled state can be rewritten as

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle) = \frac{1}{\sqrt{2}}(|+x,+x\rangle + |-x,-x\rangle). \tag{8}$$

Relying on this equality, we orient the idler polarizer to transmit only $|+x\rangle$ polarization. Detection of the signal photon in coincidence with the idler then projects the signal photon into the $|+x\rangle$ state as it enters the SQQSS chain. The sender and recipient roles remain the same as before, except that the measurement of the signal photon is now conducted in coincidence with the $|+x\rangle$-selected idler.

The success of the entanglement-based protocol depends entirely on the presence of entanglement, rather than classical correlation, between the signal and idler polarizations. To the extent that the initial state is a classical mixture of $|HH\rangle$ and $|VV\rangle$, projection of the idler photon onto $|+x\rangle$ will leave the signal photon in an uncertain polarization state rather than projecting it onto $|+x\rangle$. Thus the success rate, or fidelity, of the secret-sharing transmission is sensitive to the purity of entanglement in this protocol. However, the explicit use of entanglement makes this protocol robust against certain eavesdropping attacks and cheating strategies to which the correlation-based protocol is vulnerable. We present one such attack, a photon-number splitting exploitation of experimental asymmetries, in the next section.

III. PHOTON-NUMBER SPLITTING EAVESDROPPING ATTACK

The correlation-based SQQSS protocol, in an ideal realization, provides security against eavesdropping. However, the protocol remains vulnerable to attacks that may arise due to the imperfections of implementation. In quantum communication in general (for example, in quantum key distribution), these forms of attack have been some of the greatest obstacles to securely implementing protocols [11–13]. Such attacks include the possibility of splitting off and measuring a fraction of the photons in a pulse that is sent for each qubit (photon-number splitting), or adding photons to the channel and later extracting them for measurement (Trojan-Horse attacks) [14]. Here we focus on robustness against a photon number-splitting, or PNS, attack.

In a PNS attack, an eavesdropper takes advantage of the fact that implementations may involve transmission of pulses with the possibility of multiple photons per qubit. The eavesdropper "splits" off some of the photons, and measures the state of their polarization, while the remaining photons pass through to the intended receiver untouched. Unless the intended receiver can detect the decreased signal size, the

eavesdropper gains information about the message without alerting the participants to her presence.

There are many ways of avoiding PNS attacks in quantum key distribution, including decoy states, strong reference pulses, and differential phase shifts [15,16]. The correlation-based protocol protects against PNS by referencing the signal photon to the idler photon, which is passed through a polarizer before being detected. A PNS eavesdropper cannot discover whether her "picked-off" signal photons are coincident with the correct idler photons; thus she gains no information about the polarization state of the signal [8].

However, this protection is only completely valid in the case for which the two photons are produced with perfect symmetry in their polarization states, as in Eq. (1). Given common issues in the production of this entangled state, the photons may actually be in the state

$$|\psi_{0,\text{asymm}}\rangle = a|HH\rangle + \sqrt{1-a^2}|VV\rangle \tag{9}$$

with $a^2 \neq 1/2$. This state may be the overall two-photon state produced, or the emitted state may be symmetric but with correlations between polarization and other degrees of freedom (such as energy or spatial mode) which make it possible for an eavesdropper to filter her detection so she is dealing with an asymmetric state. In either case, the difference in the probability of detecting the signal photon in its two polarization states can give information to an eavesdropper. An eavesdropper, Eve, can gather this information by splitting off some photons, and using a beamsplitter to measure half of them in the $|\pm x\rangle$ basis and the other half in the $|\pm y\rangle$ basis.

A. Attack on correlation-based protocol

To quantify this attack, let us assume that Eve is eavesdropping on the correlation-based protocol, just after the sender has applied a phase shift to the photon. We want to find the probability that for a given $a^2 \neq 1/2$ and n photons measured by Eve, Eve can distinguish what state the sender has prepared. If she can reliably determine the qubit state, she has intercepted the secret. Eve will attempt to distinguish the qubit state by counting the number of photons detected in each of her four detectors (corresponding to measured photon state $|+x\rangle$, $|-x\rangle$, $|+y\rangle$, and $|-y\rangle$). She will then guess the bit value associated with the detector which registered the greatest number of counts. This is not the only possible algorithm for deciding which bit value Eve will guess; however, this algorithm does yield better-than-random results for Eve whenever the vulnerability $a^2 \neq 1/2$ exists.

We assume for the sake of simplicity that the sender applies 0 phase shift, and thus Eve intercepts the signal photon which is the second member of the entangled state

$$|\psi_1\rangle = a|+x,H\rangle + \sqrt{1-a^2}|-x,V\rangle. \tag{10}$$

(If the sender applies a different phase shift, the polarization states will be different, but Eve's success in identifying the correct bit does not change.) Given that the idler photon remains unmeasured, we can then find the probability that Eve measures the signal photon in either $|+x\rangle$ or $|-x\rangle$, as well as in either $|+y\rangle$ or $|-y\rangle$. If the photon goes to the $|\pm x\rangle$-basis detectors, the probability of registering $|+x\rangle$ is

$$p(|+x\rangle) = \langle\psi_1|P_{+x,s} \otimes I_i|\psi_1\rangle. \tag{11}$$

This evaluates simply to a^2, and similarly the probability of registering $|-x\rangle$ is $1-a^2$. If the photon goes to the $|\pm y\rangle$-basis detectors, the probability of measuring $|+y\rangle$ is

$$p(|+y\rangle) = \langle\psi_1|P_{+y,s} \otimes I_i|\psi_1\rangle = \frac{a^2+(1-a^2)}{2} = 1/2, \tag{12}$$

and the probability of measuring $|-y\rangle$ is likewise $1/2$. For the eavesdropper, then, for any single intercepted photon the probabilities of detection in $|+x\rangle$, $|-x\rangle$, $|+y\rangle$, and $|-y\rangle$ are $a^2/2$, $(1-a^2)/2$, $1/4$, and $1/4$, respectively.

Let us assume that n total photons can be diverted and detected by Eve. The probability of registering i counts in the $|+x\rangle$ detector, j counts in the $|-x\rangle$ detector, k counts in the $|+y\rangle$ detector, and l counts in the $|-y\rangle$ detector is

$$c_{i,j,k,l} = \frac{n!}{i!j!k!l!}\left(\frac{a^2}{2}\right)^i\left(\frac{1-a^2}{2}\right)^j\left(\frac{1}{4}\right)^k\left(\frac{1}{4}\right)^l. \tag{13}$$

Eve will successfully identify the secret if the $|+x\rangle$ detector registers the most counts ($i > j,k,l$), but also if the $|+y\rangle$ detector registers the most counts ($l > i,j,k$), since either $+$ result maps to the same secret bit value. To exactly predict Eve's success rate, however, we must also consider the possibility that two or more detectors tie for the most counts. In this case, we let Eve randomly select one of the tying detectors and base her bit-value guess on that detector. With this strategy in mind, we can assign to each outcome a probability of occurring, and a likelihood for Eve to succeed in that case.

Thus we can calculate the probability $p_{\text{Eve},n}$ for Eve to successfully identify a bit by intercepting $n = i+j+k+l$ photons to be (p_i indicates the probability that $i > j,k,l$, while $p_{i=j}$ indicates the probability that $i = j > k,l$, and so forth)

$$\begin{aligned} p_{\text{Eve},n} &= \tfrac{1}{2}[1 + p_i - p_j + p_{i=k} - p_{j=k}] \\ &\quad + \tfrac{1}{6}[p_{i=k=l} - p_{j=k=l}] \\ &\approx \tfrac{1}{2}[1 + p_i - p_j], \quad \text{for large } n. \end{aligned} \tag{14}$$

The final approximation simply neglects ties between the detectors, which become rare in the limit of large n [17]. Finally, we use Eq. (13) to evaluate the probabilities p_i, etc., in Eq. (14). A plot of Eve's predicted success rates as a function of a^2, for various numbers of "picked-off" photons per qubit, is shown in Fig. 2.

We have focused on Eve's success rate when $a^2 > 1/2$; however, if $a^2 < 1/2$ Eve will have exactly the same success rate if she systematically reverses her bit-guessing strategy. Thus Eve can be successful as long as (i) some $|HH\rangle$ vs $|VV\rangle$ asymmetry exists in the initially produced two-photon state and (ii) she is able to independently gauge the success of a small number of her guesses in order to decide whether or not to reverse her guessing strategy (a common tactic in codebreaking scenarios). If Eve can listen in on classical communications

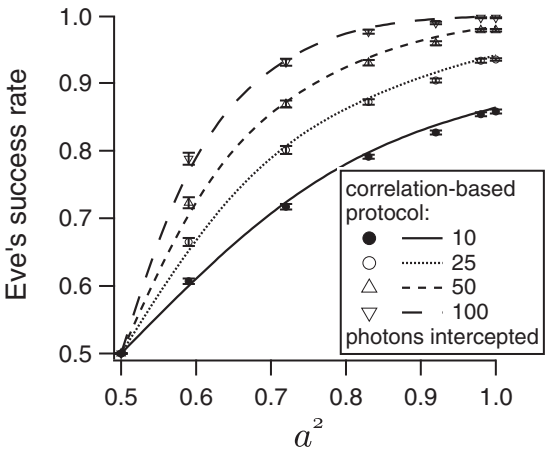

FIG. 2. Bitwise probability of successful secret identification by Eve, using a photon-number splitting attack on the correlation-based SQQSS protocol. Eve's success rate is shown as a function of a^2, the probability of $|HH\rangle$ in the emitted entangled state (as filtered by Eve's detection). Because the calculation is symmetric in a^2 and $b^2 = 1 - a^2$, $P(1-a^2) = P(a^2)$ can be used to give the probability of success for $a^2 < 0.5$. Eve's success rates are shown for $n = (10,25,50,100)$ where n is the number of photons detected in Eve's apparatus for each qubit. An eavesdropper detecting an asymmetric two-photon initial state with a good signal-to-noise ratio (points) achieves results in close agreement with theory (curves).

between the secret-sharing participants, for instance, the runs used for checking error rate should allow her to determine the correct guessing strategy.

It is clear that photon number splitting requires access to many photons. For $a^2 = 0.6$, measuring 100 photons gives Eve a theoretical 78% success rate for determining the secret bit value. The attack is especially strong when a pulse of large, indefinite photon number must be sent for each qubit.

B. Robustness of entanglement-based protocol

The correlation-based protocol for type-I SPDC is particularly vulnerable to our PNS attack because state asymmetry of the type denoted by Eq. (9) with $a^2 \neq 1/2$ is particularly common. For example, it tends to arise from unequal thicknesses or orientations of the two crystals used for SPDC, or from imprecision in the input polarization of the SPDC pump beam. The same type of asymmetric initial state arises in type-II SPDC, for example from imperfect alignment of the signal and idler paths with the positions of perfect overlap of the type-II output cones. Even in systems for which the overall state has good symmetry, more troubling is the existence of correlations between photon polarization in the H/V basis and other degrees of freedom, particularly for pulsed sources [18–20], which otherwise provide an added advantage of well-defined pulse arrival times. Correlations of this sort allow the eavesdropper to measure an effectively asymmetric state by filtering her detection on a second degree of freedom. A typical defense against this issue is to strongly prefilter the entangled state at its source, but this solution drastically reduces source brightness and secret-sharing transmission rate. Schemes have been proposed to eliminate unwanted correlations without loss of brightness [21–23], and improvements via these schemes have begun to be demonstrated experimentally [24,25]. However, it is of interest to explore an approach that improves the security of single-qubit quantum secret sharing without recourse to either a loss of brightness or these additional complications.

Asymmetry between the two terms in the initial superposition or in Eve's detected state gives rise to a bias in the signal photon's polarization state—even when observed without coincidence detection. This bias is exploited by the PNS eavesdropper. By contrast, if $a^2 \neq 1/2$ in the (possibly filtered) state but the entanglement-based protocol is followed, the single-particle state of the signal photon remains randomly distributed between $|+x\rangle$ and $|-x\rangle$ before the actions of the SQQSS participants. This can be seen quite simply by rewriting the state in the $\{|+x\rangle,|-x\rangle\}$ basis for each photon:

$$\begin{aligned}|\psi_{0,\text{asymm}}\rangle &= a|HH\rangle + \sqrt{1-a^2}|VV\rangle \\ &= \tfrac{1}{2}(a+\sqrt{1-a^2})\,(|+x,+x\rangle + |-x,-x\rangle) \\ &\quad + \tfrac{1}{2}(a-\sqrt{1-a^2})\,(|+x,-x\rangle + |-x,+x\rangle)\,. \end{aligned} \tag{15}$$

It can easily be seen from this expression that the signal photon is found in $|+x\rangle$ 50% of the time and $|-x\rangle$ 50% of the time, if no polarization information is gathered for the idler.

Indeed, if the initial entangled state were asymmetric in the x basis, there would be a parallel PNS eavesdropping attack, but asymmetries in the x basis are much less likely simply because of the physical way in which the entangled pair is produced via SPDC. Therefore the entanglement-based protocol, while it makes the fidelity of the transmission more sensitive, also provides built-in security against common exploitations by an eavesdropper.

IV. EXPERIMENTAL IMPLEMENTATION

A. Realization of correlation-based SQQSS

We now turn to implementations of both correlation-based and entanglement-based protocols with a secret sender and two recipients. An experimental schematic for the correlation-based SQQSS is shown in Fig. 3. Entangled photon pairs are produced via type-I degenerate spontaneous parametric downconversion [26] in a pair of 0.5-mm-thick BBO crystals pumped with a 50-mW cw diode laser at 405 nm. A 405-nm half wave plate and a tiltable quartz phase plate control the input pump beam polarization; these are set to prepare the initial entangled state of Eq. (1) for the signal and idler photons at 810 nm. The BBO crystals are cut at 29.15° for noncollinear downconversion, with the signal and idler at 3° from the pump beam path.

A Glan-Thompson polarizer in the idler beam path allows selective detection of $|H\rangle$ for the idler photon. An 810-nm half wave plate in the signal arm converts $|H\rangle$ to $|+x\rangle$. Now the sender and two recipients apply phase shifts $\varphi_j \in \{0,\pi/2,\pi,3\pi/2\}$. Each phase shift is accomplished using a 200-μm-thick uniaxial YVO_4 crystal. The tilt of each crystal about a vertical axis is controlled to obtain the desired phase shift. A compensation YVO_4 crystal corrects for time spreading between the polarizations. The final recipient measures the signal photon polarization in the $|\pm x\rangle$ basis

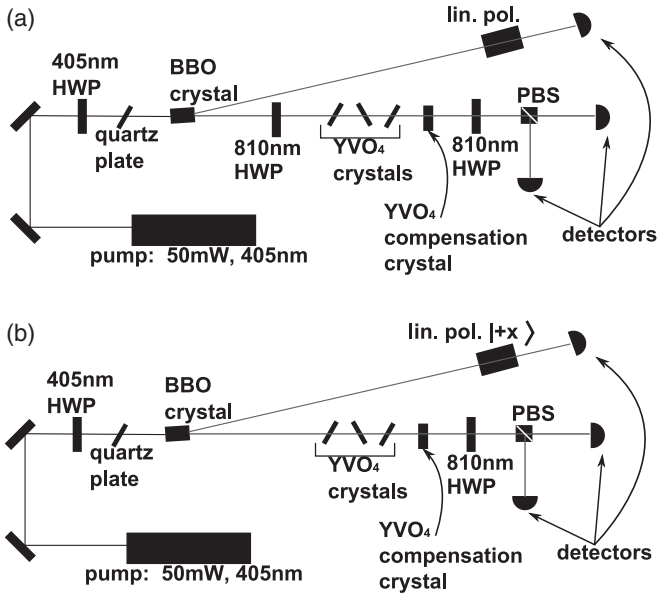

FIG. 3. (a) Experimental setup for the correlation-based protocol. The sender is composed of the first 810-nm HWP along with the first YVO_4 crystal. Additional YVO_4 crystals are the phase-shifting recipients in the protocol. The idler polarizer is set to accept horizontal polarization, which projects the signal photon into $|H\rangle$ at its entry into the SQQSS chain. (b) In the entanglement-based protocol, the idler polarizer is set to accept $|+x\rangle$ polarization, projecting the signal photon into $|+x\rangle$ at its entry into the SQQSS chain. The sender prepares the state using just the first YVO_4 crystal.

using an 810-nm half wave plate and a polarizing beamsplitter, sending signal photons into one of two detectors. Signal and idler photons are detected by coupling into multimode fibers en route to single-photon counting modules and coincidence detection with a time resolution of 4 ns. The overall efficiency of detection is approximately 2%.

B. Realization of entanglement-based SQQSS

An experimental schematic for the entanglement-based protocol is shown in Fig. 3. The polarizer in the idler arm is rotated to select $|+x\rangle$ idler polarization. The 810-nm half wave plate in the idler arm is no longer necessary, so the sender is realized entirely by the first tiltable YVO_4 phase plate. All other aspects of the setup remain unchanged from the correlation-based experiment.

To measure the rate of success in secret sharing, many runs with different secret and shadow bits were carried out using automated experiment control and data acquisition. For each run, secret and shadow bits, as well as the auxiliary class X/Y bits, were chosen randomly. The random number choices determined settings for the YVO_4 crystals, which were tilted using software-controlled motorized rotation platforms. All measurements were done by counting coincidences between the idler channel and the two signal channels over a minimum time interval of 0.1 s, limited by data acquisition techniques. Per-photon probabilities of detection were calculated, when necessary, from the observed coincidence rates.

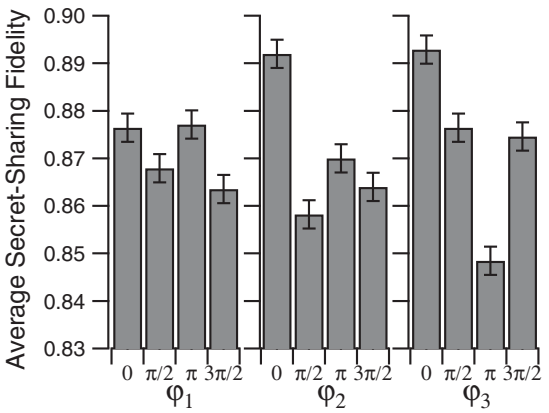

FIG. 4. Experimentally observed fidelity, or probability of "sharing" the correct qubit, using the entanglement-based protocol. Fidelity is displayed as a function of the phase-shifting angle of each YVO_4 phase plate, averaged over all settings of the other YVO_4 phase plates. The overall 13% qubit error rate is well below the 25% rate for reliable detection of cheaters. Variation of fidelity between phase plate settings matches predictions based on precision of phase plate tilting. The overall fidelity matches predictions based on phase spread in the initial two-photon entangled state.

Observed success rates for the entanglement-based protocol are shown in Fig. 4. The overall error rate of 13% is well below the 25% threshold for reliable detection of cheaters, so secret sharing has been realized in this implementation. Variations in success rate of 3–6% are observed from one set of phase plate settings to another. This variation is predicted from the limited precision of tilt angles for the YVO_4 phase plate crystals.

The imperfect 87% fidelity of secret sharing can be attributed to imperfect entanglement, or purity $P < 1$, of our entangled state produced by SPDC. For our apparatus, the BBO crystal thickness and pump laser bandwidth produce a spread in phase between $|HH\rangle$ and $|VV\rangle$ components, so that our two-photon state is only partially entangled. Separate measurements of the entangled state (see Fig. 5) indicate a purity $P = 0.78$, or entangled-state fidelity $F = 0.87$ [27], consistent with the 87% secret-sharing fidelity we measure in the experiment.

C. Eavesdropping

A maximal implementation of the photon number splitting attack is shown in Fig. 6. First, some fraction of the photons traveling through the apparatus would be picked off through the use of a polarization-preserving beamsplitter placed immediately after the first (sender) YVO_4 phase plate. The picked-off photons would be directed into Eve's polarization-analyzing detection apparatus. A 50-50 beamsplitter (BS) sends half of the intercepted photons to be measured in the $|\pm x\rangle$ basis and the other half to be measured in the $|\pm y\rangle$ basis. The measurement in the $|\pm x\rangle$ basis is done using a half wave plate, polarizing beamsplitter, and two detectors. The measurement in the $|\pm y\rangle$ basis is done using a quarter wave plate, polarizing beamsplitter, and two detectors. Eve then counts the number of photons that entered each detector and guesses a secret bit based on the detector registering the most counts.

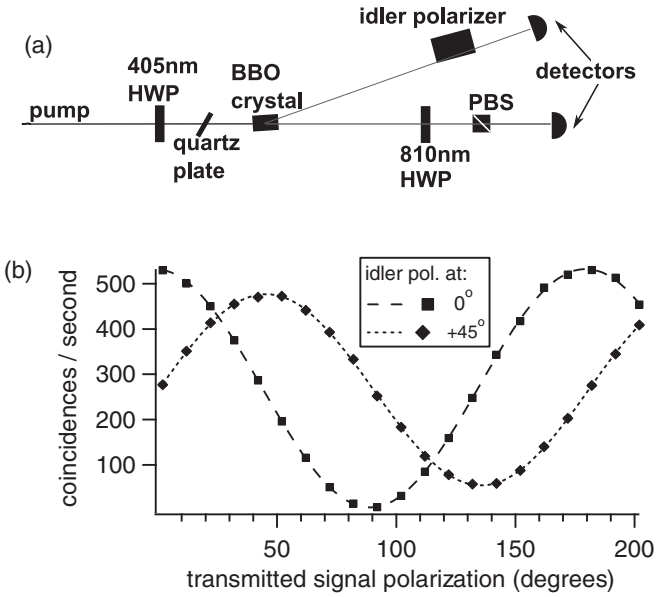

FIG. 5. (a) Schematic for measuring purity (mixedness) of two-photon entangled state, due to uncompensated spread in phase ϕ of state $\frac{1}{\sqrt{2}}(|HH\rangle + e^{i\phi}|VV\rangle)$. Coincidence counts between signal and idler photons are measured with the idler linear polarizer fixed at 0° or 45°; a half wave plate in the signal arm is rotated to change the linear polarization transmitted through the polarizing beamsplitter. (b) Coincidence counts observed. Diminished fringe visibility with the idler polarizer at 45° gives a purity of 0.78 for the two-photon state, accounting for our observed secret-sharing error rate.

To implement a photon number splitting attack experimentally, we simulated the success of the Fig. 6 eavesdropper via a simplified experimental setup. Rather than performing SQQSS detection as well as simultaneous detection in two bases by Eve, we omitted the final SQQSS measurement and conducted measurements in each of Eve's two bases at different times in the actual experiment.

The modified eavesdropping schematic is shown in Fig. 7. The 405-nm half wave plate was rotated to obtain different values of a^2. The sender's 810-nm half wave plate was present for the correlation-based protocol only. Two of the three YVO_4 crystals, left in place for convenience, were held at a constant position to introduce a phase shift of 0°. The first YVO_4 crystal was tilted to produce the four possible phase shifts introduced by the sender. An 810-nm quarter wave plate at 45° allowed measurement in the $|\pm y\rangle$ vs $|\pm x\rangle$ basis to be decided by rotation of the final 810-nm half wave plate.

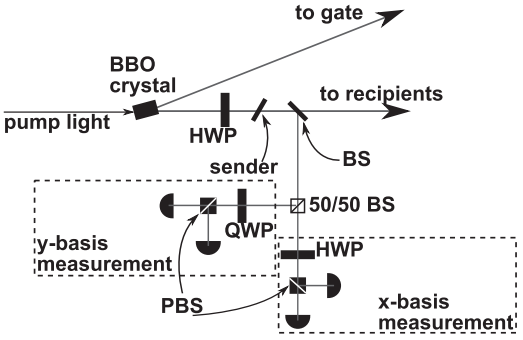

FIG. 6. Ideal eavesdropping setup for photon number splitting attack. Eve picks off a fraction of the transmitted photons and measures half of them in the $|\pm x\rangle$ basis, half of them in the $|\pm y\rangle$ basis. If the correlation-based protocol is used, Eve can exploit an imperfectly prepared initial state to determine the secret bit with better than random success.

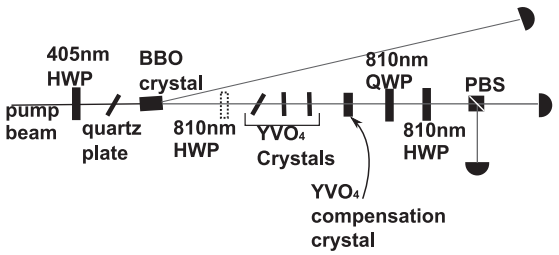

FIG. 7. Experimental setup to simulate a photon number splitting eavesdropping attack on the correlation-based protocol. The 405-nm HWP is rotated for different values of a^2 in the initial state. The last two YVO_4 crystals are held at a constant position to give a phase shift of $\varphi = 0$. For eavesdropping on the entanglement-based protocol, the first 810-nm HWP is removed. Detection is carried out in coincidence with the idler photon to improve signal-to-noise, but no idler polarizer is used to simulate an eavesdropper with no access to idler state information.

To approximate an eavesdropper with perfect signal-to-noise on her polarization analysis, we measured the signal photon in coincidence with the idler, but with no idler polarizer since the eavesdropper lacks access to the idler's polarization information. Thus the coincidence detection improved signal-to-noise problems due to background light, but otherwise faithfully simulated an eavesdropper's action.

A single run of the eavesdropping scheme consists of tilting the sender phase plate, setting the eavesdropper half wave plate to collect count rates in $|\pm x\rangle$ for 50 s, and then rotating the eavesdropper half wave plate to collect count rates in $|\pm y\rangle$ for 50 s. The observed count rates for each sender phase setting were then used as inputs to a Monte Carlo simulation of Eve's success rate for a small number of detected photons.

Observed success rates for Eve are shown here for the correlation-based measurement (Fig. 2) and likewise for the

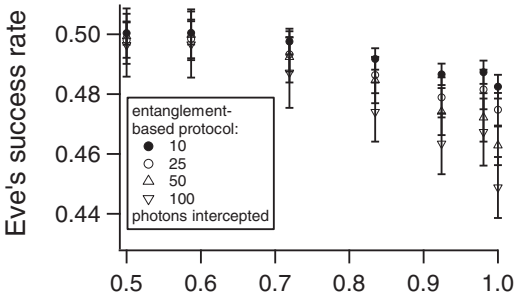

FIG. 8. A plot of the success rate of an eavesdropper detecting $n = 10, 25, 50$, or 100 photons per qubit, for the entanglement-based protocol. Note the change of vertical scale from Fig. 2. Here the eavesdropper is no longer successful despite asymmetry in the initial two-photon state. The very small deviations from 50% success can be attributed to imperfect alignment of the apparatus.

entanglement-based measurement (Fig. 8). The imperfect entangled-state purity seen in Fig. 5 does not affect eavesdropping success. Hence the experimentally inferred success rates closely follow the theoretical predictions discussed above.

V. CONCLUSIONS

We have demonstrated two SQQSS protocols using entangled photon pairs from type-I SPDC. A photon-number splitting attack on these protocols, exploiting lossy transmission and asymmetric state preparation, is demonstrated. The entanglement-based scheme is robust against this attack while the correlation-based scheme is not; this contrast illustrates the value of using quantum entanglement for security of communication.

An imperfect entangled state ($P < 1$) causes lowered fidelity of secret sharing for the entanglement-based scheme. Specifically, in this work, $P = 0.78$, input state fidelity $F = 0.87$, leads to secret-sharing fidelity of 87%. Improved purity at the $P \approx 0.95$ level should be possible in this apparatus with relatively minor modification, such as addition of a compensation BBO crystal in the pump beam to remove time/energy phase spread [28–30]. Such an improvement should lead to a secret-sharing fidelity of ≈97%, at which point imprecision in component positioning will limit the overall fidelity in practice.

To further probe the strengths and weaknesses of entanglement-secured SQQSS, other attack strategies must be developed and implemented, or a more general security analysis including both internal and external attacks must be conducted. Further work can also address scaling of SQQSS with the number of participants, and variations of SQQSS in which information is encoded in multiple entangled degrees of freedom of the photon pair.

ACKNOWLEDGMENTS

The authors thank M. Beck at Whitman College for discussions and much valuable information regarding experimental apparatus, C. Schmid for correspondence about the correlation-based SQQSS scheme in type-II downconversion, and D. K. Koh for discussions of secret-sharing security. This work was supported by Research Corporation Cottrell College Science Grant No. 10598, and by the Beckman Foundation through Harvey Mudd College. P.S. acknowledges support from the Fannie and John Hertz Foundation, R.R. acknowledges support from the Engman Foundation, and D.B. acknowledges support from the R. C. Baker Foundation.

[1] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).
[2] D. Bouwmeester, J.-W. Pan, M. Daniell, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **82**, 1345 (1999).
[3] M. Eibl, N. Kiesel, M. Bourennane, C. Kurtsiefer, and H. Weinfurter, Phys. Rev. Lett. **92**, 077901 (2004).
[4] Z. Zhao, Y.-A. Chen, A.-N. Zhang, T. Yang, H. J. Briegel, and J.-W. Pan, Nature (London) **430**, 54 (2004).
[5] H. Häffner *et al.*, Nature (London) **438**, 643 (2005).
[6] C.-Y. Lu, X.-Q. Zhou, O. Gühne, W.-B. Gao, J. Zhang, Z.-S. Yuan, A. Goebel, T. Yang, and J.-W. Pan, Nat. Phys. **3**, 91 (2007).
[7] C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Żukowski, and H. Weinfurter, Phys. Rev. Lett. **95**, 230505 (2005).
[8] C. Schmid, P. Trojek, S. Gaertner, M. Bourennane, C. Kurtsiefer, M. Żukowski, and H. Weinfurter, Fortschr. Phys. **54**, 831 (2006).
[9] C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Żukowski, and H. Weinfurter, Phys. Rev. Lett. **98**, 028902 (2007).
[10] G. P. He and Z. D. Wang, Quantum Inf. Comput. **10**, 28 (2010).
[11] D. Mayers, J. ACM **48**, 351 (2001).
[12] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
[13] H.-K. Lo and N. Lütkenhaus, Physics in Canada **63**, 191 (2007).
[14] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Phys. Rev. A **73**, 022320 (2006).
[15] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt, Phys. Rev. Lett. **98**, 010503 (2007).
[16] T. Schmitt-Manderbach *et al.*, Phys. Rev. Lett. **98**, 010504 (2007).
[17] Furthermore, this approximation always leads to a bias against Eve's true chances of success, because ties between $|+x\rangle$ and $|+y\rangle$ (which always result in the correct qubit) are more common than ties between $|-x\rangle$ and $|-y\rangle$ (which result in the incorrect qubit) as long as $a^2 > 1/2$.
[18] Y. Kim and W. Grice, Opt. Lett. **30**, 908 (2005).
[19] M. Avenhaus, M. V. Chekhova, L. A. Krivitsky, G. Leuchs, and C. Silberhorn, Phys. Rev. A **79**, 043836 (2009).
[20] H. S. Poh, C. Y. Lum, I. Marcikic, A. Lamas-Linares, and C. Kurtsiefer, Phys. Rev. A **75**, 043816 (2007).
[21] Y. Kim and W. Grice, J. Mod. Opt. **49**, 2309 (2002).
[22] R. Erdmann, D. Branning, W. Grice, and I. A. Walmsley, Phys. Rev. A **62**, 053810 (2000).
[23] D. Branning, W. P. Grice, R. Erdmann, and I. A. Walmsley, Phys. Rev. Lett. **83**, 955 (1999).
[24] H. S. Poh, J. Lim, I. Marcikic, A. Lamas-Linares, and C. Kurtsiefer, Phys. Rev. A **80**, 043815 (2009).
[25] J. F. Hodelin, G. Khoury, and D. Bouwmeester, Phys. Rev. A **74**, 013802 (2006).
[26] P. G. Kwiat, E. Waks, A. G. White, I. Appelbaum, and P. H. Eberhard, Phys. Rev. A **60**, R773 (1999).
[27] The fidelity of the experimental two-photon density matrix ρ with respect to the ideal two-photon pure state $|\Phi^+\rangle$ is defined as $\mathrm{Tr}(\sqrt{\sqrt{\rho}|\Phi^+\rangle\langle\Phi^+|\sqrt{\rho}})$, and is analogous to the state overlap for the case of two pure states.
[28] Y. Nambu, K. Usami, Y. Tsuda, K. Matsumoto, and K. Nakamura, Phys. Rev. A **66**, 033816 (2002).
[29] J. B. Altepeter, E. R. Jeffrey, and P. Kwiat, Opt. Express **13**, 8951 (2005).
[30] R. Rangarajan, M. Goggin, and P. Kwiat, Opt. Express **17**, 18920 (2009).