INSTITUTE OF PHYSICS PUBLISHING JOURNAL OF OPTICS B: QUANTUM AND SEMICLASSICAL OPTICS

J. Opt. B: Quantum Semiclass. Opt. **6** (2004) 63–68 PII: S1464-4266(04)58455-0

Secret-message sharing via direct transmission

Kamil Brádler[1] **and Miloslav Dušek**[2]

[1] Department of Chemical Physics and Optics, Charles University, Ke Karlovu 3, 121 16 Prague 2, Czech Republic
[2] Department of Optics, Palacký University, 17. listopadu 50, 772 00 Olomouc, Czech Republic

Received 8 January 2003, accepted for publication 10 October 2003
Published 3 November 2003
Online at stacks.iop.org/JOptB/6/63 (DOI: 10.1088/1464-4266/6/1/011)

Abstract
Two new protocols for secret-information splitting among many participants are proposed. One of them uses only bipartite entangled states (Bell states) and the other one multi-partite entangled states. We prove their security against the family of rather general intercept–resend attacks and discuss the possibility of an experimental realization.

Keywords: secret sharing, quantum cryptography, entanglement

1. Introduction

In their concurrent 1979 papers [1, 2] Blakely and Shamir presented a method for splitting secret information called secret sharing. They showed how to divide a sequence of bits into n pieces reconstructible from any $k \leqslant n$ pieces. The keystone of secret sharing is the impossibility of the reconstruction of the sequence from any $k-1$ pieces. Such a scheme was called the (k, n) threshold scheme.

Later, a generalization of secret sharing on the area of quantum information was also considered. On the one hand, a quantum state serves as an intermediary for distribution of classical information. The Hillery *et al* paper [3] devoted to this topic first deeply studied the possibility of using GHZ states for classical information splitting. Security aspects were analysed at length and the study showed that an eavesdropper's actions would lead to his or her disclosure. A link between eavesdropping in this scheme and the violation of one type of Bell inequality was revealed in [4]. The authors of [5] dealt with the possibility of using pseudo-GHZ states for secret sharing. On the other hand, the secret alone can be in the form of an unknown quantum state. Progress in this direction was made in [6] where the authors gave a construction of a quantum threshold scheme and discussed the role of the no-cloning theorem. Close connection between quantum secret sharing and error-correcting codes was discussed in [7]. The way to share a secret in the form of a continuous-variable quantum state was investigated in [8].

All quantum cryptographic protocols derived from the original BB84 protocol [9] are essentially indeterministic. This means that not every photon is a carrier of a key bit. There also exist several proposals of deterministic (direct) protocols. A pioneering contribution on this topic was first proposed in [10, 11]. These protocols do not need to establish a secret key. The principle can be explained in the following way: first, the cipher is sent through a quantum channel and later, if no eavesdropper is detected, the key is transmitted classically. Recently, another scheme for direct communication has been devised [12]. The principle is similar but this protocol employs four different entangled states (Bell states). One of two entangled particles always goes from the sender (Alice) to the recipient (Bob) and back again. To be more specific, Alice generates one of four Bell states and sends one 'travel qubit' (TB) from every pair to Bob. This enables her to encode two bits of the message. Bob chooses at random one of four Pauli operations (including identity) and applies it on TB. Then he sends TB back to Alice. Bob's operation changes the original Bell state to some another Bell state (the set of four Bell states is closed with respect to the Pauli transformations). Then, Alice performs measurement in the Bell basis on both particles. If she is assured that no eavesdropper (Eve) was present she announces the results of her measurement publicly (it is supposed that Eve cannot manipulate the public channel). In such a case, Bob is the only person who knows the operations performed on the TBs and thus he is the only one who is able to determine the original Bell states prepared by Alice. Eve can apply the following attack: she cuts the quantum channel, stores Alice's TB and sends TB from her own Bell state towards Bob. When she gets this TB back she deduces Bob's operation and performs the same operation on the stored TB. Then she sends it back to Alice. She would stay undisclosed. Therefore, beside the above-described procedure, Alice and

Bob must switch to a 'correlation' (test) measurement (CM) from time to time in order to reveal such intrusions. At random instants Bobs decides to hold TB. Then Alice and Bob make measurements on their qubits in one of two conjugated bases. Bob announces his result and Alice verifies the expected correlation.

It is worth mentioning that the random selection of one of two conjugated bases is not necessary. There is no difference whether Eve knows the basis or not. The continuous eavesdropping causes 50% error rate on average (which is better than the 25% stated in [12]). The reason is that the man-in-the-middle attack erases any correlation between Alice's and Bob's results.

In the present paper we propose two distinct protocols for the direct quantum distribution of a message among N parties. Direct quantum distribution means that no key is established. We show the way for deterministic secret-message sharing. The only way to uncover the message sent by Alice is cooperation of recipients. Our schemes are based on the Boström protocol transferred into the secret-sharing context. Further, we discuss a general family of intercept–resend attacks (IR attacks) on the proposed schemes and bring in security analysis. Another possible attack on legal participants' Pauli operations is also considered.

The paper is organized as follows. In section 2 we introduce two proposed schemes ('ring' and 'star') explained on the simplest nontrivial case of three participants. Both arrangements are followed by the detailed security analysis. We classify two basic ways of eavesdropping: internal (someone from the legitimate participants cheats) and external (Eve). Then, in section 3 we generalize the secret-sharing protocols for N participants and $M < N$ cheaters. We conclude with the discussion on the feasibility of an experimental realization in section 4. The reader can find some detailed calculations in the appendix.

The following terminology is used: an n-dimensional standard basis is the set of 2^n different states obtained by the sequence of Pauli transformations σ_X from the state $|0\rangle^{\otimes n}$. Similarly, if we denote the state $1/\sqrt{2}(|0\rangle^{\otimes n} + |1\rangle^{\otimes n})$ as the nGHZ (generalized GHZ) state, then the nGHZ basis is the set of 2^n different maximally entangled states created with the help of Pauli operations from the nGHZ state. Solely in the next section, by GHZ states are meant 3GHZ states.

2. Secret sharing for tripartite system

2.1. Ring arrangement

The first way to distribute information between two recipients is the following: Alice, Bob, and Charlie constitute a ring or loop (see figure 1(a)). Alice has four Bell states at her disposal:

$$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_{\mathrm{A}}|1\rangle_{\mathrm{BC}} \pm |1\rangle_{\mathrm{A}}|0\rangle_{\mathrm{BC}}),$$
$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_{\mathrm{A}}|0\rangle_{\mathrm{BC}} \pm |1\rangle_{\mathrm{A}}|1\rangle_{\mathrm{BC}}). \quad (1)$$

She chooses one of them and sends a qubit to Bob at first. Bob applies at random one of four Pauli transformations, $\{\mathbb{I}, \sigma_X, \sigma_Y, \sigma_Z\}$, and sends the particle towards Charlie.

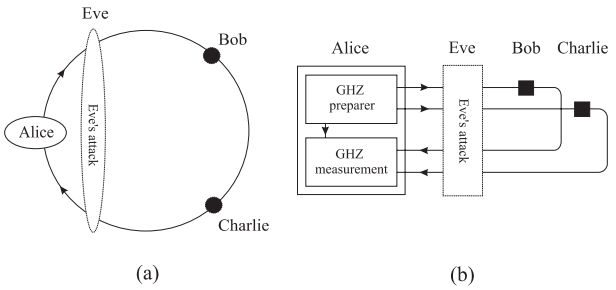

Figure 1. Ring and star arrangement for a direct tripartite secret sharing with an external attack. Eve is also listening to traffic on a public channel.

Analogously, Charlie applies a random Pauli transformation. When it is completed he sends the qubit back to Alice. The qubit makes a sight-seeing tour along the route A $\rightarrow$ B $\rightarrow$ C $\rightarrow$ A. Then Alice performs measurement in Bell basis (1) on both particles and proceeds in the same way as in the above-recapitulated two-party protocol. Also, in this tripartite protocol the participants must realize CM from time to time. This is the way to detect Eve's activities. Let us describe it in short. When a qubit arrives at Bob's side Bob does not apply a Pauli operation but he performs a measurement on the qubit in a standard basis $\{|0\rangle, |1\rangle\}$. He announces the result on the public channel. Alice then measures her qubit in the same basis and compares the results. The second alternative is that CM is performed by Charlie (i.e., Charlie decides to stop the qubit and makes the measurement). Charlie's result is also published. But in this case, Alice needs to know Bob's operation, too. When Bob reveals it she is able to test the correctness of measured correlations (she knows the original Bell state).

How is this protocol immune against an external attack? To be able to uncover the information sent by Alice, Eve needs to determine the total transformation resulting from Bob's and Charlie's operations. Therefore she intercepts the qubit on the edge A–B and substitutes it by a qubit from her own Bell state. On the edge C–A she catches the transformed qubit and makes a Bell measurement on 'her' pair of particles. Then she knows the overall transformation performed by Bob and Charlie. She applies this transformation to the original qubit and sends the qubit back to Alice. However, Eve's intervention causes discrepancies in the results of CMs. The error rate is the same no matter whether CM is performed by Charlie or Bob and it is equal to $1/2$ because Alice's and Bob's (Charlie's) results are completely uncorrelated after the intervention. The probability that Bob (Charlie) gets the 'wrong' result with respect to Alice's is $1/2$.

The case with a spy inside is more interesting. It is not difficult to realize that CM performed by a cheater (and Alice) cannot expose him because in such a case the situation is under his control. So, let us analyse the case when CM is performed by a honest party. First suppose that Charlie cheats. He 'bypasses' Bob and instead of the original qubit he sends him a faked qubit (a part of Charlie's own Bell state) in order to read out Bob's operation. Then he applies any operation on the original qubit and returns it to Alice. If Bob and Alice perform CM they notice 50% error rate on average. This is the consequence of Charlie's intervention, that causes Alice's

and Bob's results to be uncorrelated. If the average numbers of CMs realized by Bob and by Charlie are the same then the total error rate is 1/4 (on average). The situation when Bob cheats leads to the same result. Bob substitutes Charlie's qubit with a 'Bell fake'. After Alice and Charlie have performed CM, Alice waits for the declaration of Bob's fictitious transformation, in this case. But there is no way for Bob to change (*ex post*) the reality that the results of CM are uncorrelated. Again, the overall error rate is equal to 1/4. We can see that if the rate of CMs is the same for both Bob and Charlie the error rate is independent of the position of a cheater. Of course all the three parties must agree in advance that from N sent qubits some N_1 have to be used for CMs.

2.2. Star arrangement

The second way of the distribution of secret information is based on multi-partite entanglement. Alice uses one of eight three-particle maximally entangled states (GHZ states) of the form

$$|\Phi\rangle_{klm} = \frac{1}{\sqrt{2}}(|0, l, m\rangle + (-1)^k |1, l \oplus 1, m \oplus 1\rangle), \qquad (2)$$

where the convention is used that $|j, l, m\rangle = |j\rangle_{\mathrm{A}} |l\rangle_{\mathrm{B}} |m\rangle_{\mathrm{C}}$; $k, l, m \in \{0, 1\}$; $x \oplus y = (x + y) \bmod 2$. She sends corresponding qubits towards Bob and Charlie (see figure 1(b)). They perform Pauli transformations randomly and independently and return the qubits to Alice. When the qubits are back Alice makes a measurement in the GHZ basis (2)—she reads out the transformed GHZ state. Finally, Alice announces the resulting state. To decode Alice's message (i.e., the GHZ states chosen by Alice) Bob and Charlie have to come together and share the knowledge on their single qubit operations. To avoid IR attacks Bob and Charlie have to perform CMs. This means that either of them may order stopping qubits and making one-particle measurements in the standard basis. The results are announced on the public channel for Alice's security analysis. The instants of CMs must be random and the probability of performing CM must be the same both for Bob and Charlie.

Let us focus on several features of the states of the form (2) before we come to the security analysis. First, it is known that $\mathrm{Tr}_{\mathrm{AB}} |\Phi\rangle\langle\Phi| = \mathrm{Tr}_{\mathrm{AC}} |\Phi\rangle\langle\Phi| \propto \mathbb{I}$ for all states (2). The unit trace over Alice and Bob or Charlie assures that neither Charlie nor Bob is able to extract the information (Alice's state) alone.

Second, we see that $\mathrm{Tr}_{\mathrm{A}} |\Phi\rangle\langle\Phi| \not\propto \mathbb{I}$ for any state (2). What is really important is the fact that the trace over Alice leads to two different results for two different sets of GHZ states. A direct measurement on the density matrix coming from Alice enables Eve to distinguish two groups (let us call them 'families') of four GHZ states (that with $l = m$ and $l \neq m$)—see the appendix. This implies that Eve could obtain some information about Alice's message. Hence Alice may not use all the states (2) for encoding the message. She is forced to encode information within only one family (even publicly known). Thus, she can send only two bits of information in one run. The restriction to one fixed family must be part of the protocol.

A final note is devoted to the algebra used. Bob and Charlie can assemble 16 operators of the type $\Pi^{\mathrm{BC}}_{rs} = \sigma^{\mathrm{B}}_r \otimes \sigma^{\mathrm{C}}_s$ where $r, s \in \{0, 1, 2, 3\}$ which are mapped onto $\{I, X, Y, Z\}$. However, because

$$\sigma^{\mathrm{B}}_r \otimes \sigma^{\mathrm{C}}_s |\Psi\rangle_{klm} = \mathrm{e}^{\mathrm{i}\phi} \sigma^{\mathrm{B}}_{3-r} \otimes \sigma^{\mathrm{C}}_{3-s} |\Psi\rangle_{klm}, \qquad (3)$$

where ϕ is an unimportant global phase factor, there are only eight different transformations of Alice's states. The set of GHZ states is closed with respect to these operations.

Now, let us analyse the security of the protocol against existent intrusions. As in the case of the ring arrangement we consider two types of attack. First, we will study an external attack (Eve is an intruder and Bob and Charlie are honest). Eve's strategy for an IR eavesdropping is apparent. She just stores the qubits from Alice in a quantum memory and resends her own GHZ state. Eve cannot manipulate qubits more sophistically (POVM etc) because the states from the particular family have the same partial trace.

After storing the qubits, Eve sends qubits from her own GHZ state towards Bob and Charlie. They perform random Pauli operations and send the qubits back. Applying their local operations they transform Eve's original state into another GHZ state. So, if Eve makes a measurement in the GHZ basis (2) she can learn the joint transformation of Bob and Charlie. Then she just properly transforms Alice's state. The way to detect this attack is to perform CMs as described next. To illustrate an eavesdropping let us consider that Alice prepares the state $|\Phi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$. In the case of CM she awaits result $|000\rangle$ or $|111\rangle$, both with the probability one-half. After Eve's attack Alice's particle is no longer entangled either with Bob's or Charlie's photon. Results of their measurements are uncorrelated. In order to stay henceforth undisclosed Eve would have to assure the right correlations at CM. But she does not know the state generated by Alice. This means that she sends a state of the form $|\Phi\rangle_{\mathrm{fake}} = \frac{1}{\sqrt{2}}(|x00\rangle \pm |\bar{x}11\rangle)$. The probability that Alice measures $|0\rangle$ and Bob and Charlie measure $|00\rangle$ is 1/4. The same holds for $|1\rangle$ and $|11\rangle$ respectively. The error rate in this case is equal to 1/2 and has the same value for all combinations of GHZ states sent by Alice and Eve[3].

What about the enemy within? Suppose, e.g., that Charlie is a cheater. He has access to all quantum channels as Eve has and he wants to acquire all information without cooperation with Bob. An attack consists in substitution of a qubit from an original GHZ state prepared by Alice that aims to Bob by a qubit from Charlie's own Bell state. This enables Charlie to find out Bob's operation. Both recipients (Bob and Charlie) decide equiprobably to perform CM. Of course, if Charlie is a cheater then once he decides to execute CM he will not substitute Bob's qubit. Simply, Charlie does not disclose himself. His attack affects just CMs ordered by Bob. The error rate is thus equal to 1/4 only (in about a half of Bob's CMs Charlie hits the correct result). The error rate is less than in the case of an external eavesdropper. To avoid this 'security attenuation' the following modification of the protocol is required: Alice prepares her GHZ state as before. But, when Bob and Charlie receive the qubits they must ask Alice what

[3] Eve could moreover rotate particular qubits in every GHZ state but it can be shown that she cannot decrease the overall error rate in this way. Next, even a simplified version of this attack is known. Eve can separately deceive Bob and Charlie. Instead of a faked GHZ state Eve can send two (generally different) Bell states to Bob and Charlie.

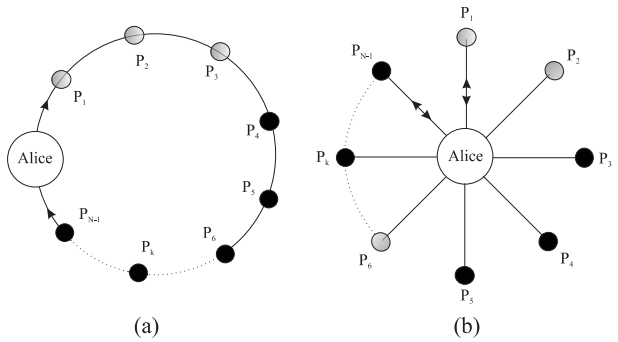

Figure 2. Schematic depiction of ring (a) and star (b) arrangement for direct N-partite secret sharing. There are $M = 3$ spies inside (shaded).

to do with them. This communication proceeds on the public channel. Alice either orders execution of Pauli transformations or execution of CM. Now, the enemy inside cannot use the advantage of the choice of CM. He does not know when Alice will order CM. Therefore, for this modified protocol the error rate is equal to $1/2$ even for the eavesdropping by a dishonest recipient.

3. Secret sharing for N-partite system

3.1. Generalized ring arrangement

Now we generalize the previous arrangements for N partners (see figure 2). Let us have $N-1$ participants on a chain plus Alice (see figure 2(a)) and start with the external type of attack. Eve stops and stores a qubit coming from Alice and sends a faked qubit from her own Bell state. Behind the last participant Eve picks the qubit up. Then she measures in the Bell basis and reveals the overall transformation. Finally, Eve executes such a transformation on Alice's qubit and sends it back to Alice. Again, the only way of detection of such an attack is CM. This means that one of the participants decides to stop the qubit and performs measurement in the standard basis. The result is announced on the public channel and Alice performs the same measurement. If the participant who orders CM is not in the first position on the chain Alice needs the Pauli operations of all previous participants. Then, the measurement results are compared and the correctness is verified. Eve's probability of success is equal to $1/2$. This implies an error rate of $1/2$. This value is independent either of the number of participants or of the position of the chosen participant in the chain.

At first sight the situation is a little bit more complicated in the case of generalized internal attack. M cheaters from $N-1$ participants can be deployed in many ways. Fortunately, it makes no difference which position is occupied by honest and dishonest participants. Bad boys 'overbridge' every legal user and tap their Pauli operations. Now, we are able to derive the formula for the error rate when M spies are present among $N-1$ participants

$$\epsilon = \frac{N-1-M}{2(N-1)}. \tag{4}$$

This stems from the fact that if CM is ordered by a honest party the probability of disclosing bad boys is equal to $1/2$.

Table 1. Dependence of the number of states (5) and operations (6) on the number of partners.

Partners	States	Operations
2	4	4
3	8	16
⋮	⋮	⋮
N	2^N	$4^{(N-1)}$

The probability of ordering CM by a honest party is $\frac{N-1-M}{(N-1)}$. For $N = 3$, $M = 1$ we get an error rate of 25% as should be.

3.2. Generalized star arrangement

Alice uses maximally entangled states of the form

$$|\Phi(k_1,\ldots,k_N)\rangle = \frac{1}{\sqrt{2}}\Bigg[|0\rangle_1 \bigotimes_{i=2}^{N} |0\oplus k_i\rangle_i + \mathrm{e}^{\mathrm{i}\pi k_1}\,|1\rangle_1 \bigotimes_{i=2}^{N} |1\oplus k_i\rangle_i\Bigg]. \tag{5}$$

The protocol alone is the same as in the tripartite version. The only difference now is that Alice sends $N-1$ qubits (instead of two qubits) from the state (5) towards $N-1$ participants (see figure 2(b)). Operations applied by recipients,

$$\Pi^{N-1} = \sigma^1 \otimes \cdots \otimes \sigma^{N-1}, \tag{6}$$

transform any state from this set to some other one. However, independently of the rapidly growing number of operators (6) with increasing N (see table 1), many of them have the same effect (up to a global phase factor) on states (5). To be specific, we observe that the number of different transformations is always equal to the number of states, i.e. 2^N.

Again, irrespective of the number of participants Alice can safely send only two bits of information at once. This is due to another feature of the states (5). If we trace over one qubit (e.g. Alice's one) in all 2^N states we obtain $2^N/4$ different density matrices (i.e., $2^N/4$ different families of states). This means that four different states have the same reduced density matrix. To avoid the leakage of information Alice may encode only 'four digits' from an arbitrary family, i.e. two bits of information. The arrangement is the same as in the three-participant case: the family of chosen states in our protocol is fixed and publicly known. One can see that Eve is certainly able to make up a unitary gate which discriminates families of an arbitrary nGHZ state (generalized version of the family discriminator presented in the appendix).

External IR attack. For successful eavesdropping Eve should tap the wires going to all $(N-1)$ receivers (they are considered to be honest). She retains qubits sent by Alice and substitutes these original qubits with faked qubits stemming either from own generalized nGHZ state of the form (5) or from $N-1$ generally different Bell states (technologically simpler solution for her). Recipients perform Pauli operations and send the qubits back. All qubits are caught by Eve who makes a measurement in the nGHZ basis and compares sent and received states. This way she deduces the overall

transformation. Finally, she applies the same transformation on original Alice's qubits and sends them to Alice.

CMs are executed in the same way as in the three-party protocol. If any of the partners decides to perform CM (measurement on an 'own' qubit in the standard basis) other participants do the same as well. Under the above described circumstances the resulting error rate $\epsilon = 1/2$ for arbitrary N. The growing number of partners leaves the error rate constant.

Internal IR attack. The strategy of cheaters in the case of an internal IR attack is the following. Suppose that M of $N-1$ receivers can cheat. These criminals survey the other quantum channels and they are able to fob off their own qubits in suitable states. They store qubits coming from Alice and send qubits from their own nGHZ (now $N-M$-partite) state to $N-1-M$ remaining recipients. The next scenario is the same as before: all (honest) parties carry out Pauli transformations. Spies find out the collective transformation made by the honest users (by measurement in the corresponding nGHZ basis) and apply the same transformation on original Alice's qubits.

As in the three-participant illustration, it is necessary to distinguish situations when CM is ordered by Alice and when it is ordered by some of the recipients. In the first case the error rate is $1/2$ because the cheaters do not know when CM is ordered.

If CM is not ordered by Alice but by recipients the situation is different. CM is ordered equiprobably by honest and dishonest users and the overall error rate is equal to

$$\epsilon = 1 - \left[\frac{M}{N-1}1 + \frac{N-1-M}{N-1}\frac{1}{2}\right] = \frac{N-1-M}{2(N-1)}. \quad (7)$$

This expression is quite accidentally the same as in equation (4). But now the situation is entirely dissimilar. In contrast to the ring arrangement now every user owns one qubit from the generalized nGHZ state and thus every one can order CM. We suppose that M cheaters cooperate together (they act like 'one man'). When they decide to order CM they do not substitute Alice's qubits by qubits from a faked nGHZ state. This means that they are overall successful with probability equal to $\frac{M}{N-1}$. Even if CM is ordered by some of the honest recipients at the same time as the intruders they cannot be detected. In the opposite case when CM is ordered by some of the $N-1-M$ well-mannered users but not by any intruder then the probability of the cheaters' success is equal to $\frac{N-1-M}{N-1}\frac{1}{2}$.[4]

Other than IR attack. We claimed that Eve's best strategy is IR attack and that any other information within a fixed family is inaccessible to her. In this context we should prove that any measurement by Eve on the qubits returning from recipients (after their operations have been applied) cannot give her any useful information (if she does not affect qubits on their route to recipients). Applying the family discrimination (described in the appendix) Eve could measure the family of the state modified by recipients without disturbing the state (this family is different, in general, from the original one). By comparing her measurement result with the known family of Alice's original state she could therefore get certain information on the Pauli operations used by recipients. But this information is not complete. It just enables Eve to discriminate a few classes of operations but it gives her no chance to deduce the state sent by Alice from Alice's announced final-measurement result. The key point is that this information does not contain the knowledge on the changes of mutual phases in the total state as well as the exact knowledge which particular qubits were flipped.

[4] Note that in the case of the ring arrangement it does not matter whether CM is ordered by Alice or by recipients.

4. Experimental realization

We have proposed two arrangements that differ in several respects. One aspect is the feasibility of experimental realization. In recent years, great progress in the generation of multi-partite entangled states was made [13–18]. But it is still impossible to compare the experimental feasibility of these techniques with Bell state generation and detection. Therefore in the following we will only focus on the ring arrangement where the Bell states are used.

If we are interested only in the linear optical implementation it is known that it is possible deterministically to detect only two of four Bell states [19, 20]. This represents an important practical obstacle. Allowing auxiliary photons, the discrimination of all Bell states with the probability arbitrarily close to one is possible by means of linear optics [21] but the scheme is still unfeasible for experimental realization with contemporary technology.

In the sections above we have described the quantum-cryptographic protocols under perfect (i.e., unrealistic) conditions. We did not take into account errors in the transmission or detector inefficiencies. The lost particles do not represent a problem: Alice simply repeats the last transmission step. No information can leak. More difficulties stem from errors caused by decoherence, misalignment, etc. It was said that at the end of the transmission Alice decides whether to publicly announce measured states or not. Her decision acts up to the measured error rate. However, Alice cannot distinguish the technological error rate and errors caused by Eve's activities. Here one may ask: if Alice measures error rate ϵ' how much information was a contingent attacker able to gain?[5] Let N be the overall number of sent bits, $N_1 \leqslant N$ the number of CMs and $K \leqslant N$ the number of Eve's IR attacks. Then, $K_1 = K\frac{N_1}{N}$ is the number of attacks detectable with the help of CM and the measured error rate has the form $\epsilon' = \frac{K_1}{N_1}\epsilon$ where ϵ is the error rate for the continuous eavesdropping calculated above. If we put these two fractions together we find that

$$K = \frac{\epsilon'}{\epsilon}N, \quad (8)$$

where ϵ' is the measured error rate. So, if there was an eavesdropper Alice would be able to calculate how much information has leaked.

5. Conclusion

We have described two distinct schemes (the 'ring' and the 'star') for N-partite secret sharing in the spirit of direct

[5] Of course, Alice can always decide not to announce the measured states.

◯	Alice or arb. user
E	$\frac{1}{2}$
I	$\frac{N-1-M}{2(N-1)}$

✵	Alice	arbitrary user
E	$\frac{1}{2}$	
I	$\frac{1}{2}$	$\frac{N-1-M}{2(N-1)}$

Figure 3. Eavesdropping gives rise to a detectable error rate. In the case of the star arrangement the error rate is different if the CM is ordered by a sender (Alice) or by the recipients. E/I means external/internal type of attack.

message transmission. The security of these two sharing schemes against the family of intercept–resend attacks has been analysed. The summary of our results is given in two tables in figure 3. We have assumed two models of attack: first, the external type of attack, and second, the internal one with M treacherous recipients who want to reconstruct the message without cooperation with the honest ones. The two proposed topological arrangements for the secret-sharing procedure differ in one important aspect. From the viewpoint of technological requirements and a possible practical realization the ring arrangement is more feasible even for sharing among many partners. The fact that using multipartite entanglement in the case of the star arrangements does not bring better values of error rates is slightly startling.

Acknowledgments

This research was supported under the project LN00A015 of the Ministry of Education of the Czech Republic. KB is very indebted for the support of the Josef Hlávka foundation.

Appendix

We argued that Eve would be able to distinguish deterministically the family of the 3GHZ states generated by Alice without affecting them. Here is the recipe to 'separate' two families of eight 3GHZ states of the form (2). Let us define a specific unitary operation acting on states from both families. For the first family we have

$$(\mathbb{1}_{\mathrm{A}} \otimes U_{\mathrm{BCE}})\left(\frac{1}{\sqrt{2}}(|x00\rangle_{\mathrm{ABC}} \pm |\bar{x}11\rangle_{\mathrm{ABC}}) \otimes |0\rangle_{\mathrm{E}}\right) = \frac{1}{\sqrt{2}}(|x00\rangle_{\mathrm{ABC}} \pm |\bar{x}11\rangle_{\mathrm{ABC}}) \otimes |1\rangle_{\mathrm{E}} \quad (9)$$

and for the second family the action is

$$(\mathbb{1}_{\mathrm{A}} \otimes U_{\mathrm{BCE}})\left(\frac{1}{\sqrt{2}}(|x01\rangle_{\mathrm{ABC}} \pm |\bar{x}10\rangle_{\mathrm{ABC}}) \otimes |0\rangle_{\mathrm{E}}\right) = \frac{1}{\sqrt{2}}(|x01\rangle_{\mathrm{ABC}} \pm |\bar{x}10\rangle_{\mathrm{ABC}}) \otimes |0\rangle_{\mathrm{E}}\,. \quad (10)$$

The operator U_{BCE} has the form

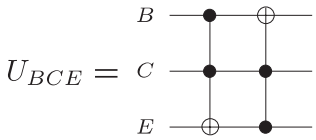

Figure A.1. The circuit corresponding to unitary operation (11).

$$U_{\mathrm{BCE}} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \quad (11)$$

and is acting on both Bob's and Charlie's qubits and Eve's ancilla in the state $|0\rangle_{\mathrm{E}}$. The gate U_{BCE} can be realized by two Toffoli gates as depicted in figure A.1. Clearly, Alice's qubit stays untouchable. If Eve projectively measures on her ancilla she is able to distinguish the two families. The gate serves as a 'family discriminator'. It is possible to enhance such a type of measurement to higher dimension for nGHZ states of the form (5).

References

[1] Blakely G 1979 *Proc. AFIPS* **48** 313
[2] Shamir A 1979 *Comm. ACM* **22** 612
[3] Hillery M *et al* 1999 *Phys. Rev.* A **59** 1829 (*Preprint* quant-ph/9806063)
[4] Scarani V and Gisin N 2002 *Phys. Rev.* A **65** 012311 (*Preprint* quant-ph/0104016)
[5] Tittel W *et al* 2001 *Phys. Rev.* A **63** 042301
[6] Cleve R *et al* 1999 *Phys. Rev. Lett.* **83** 648
[7] Gottesman D 2000 *Phys. Rev.* A **61** 042311 (*Preprint* quant-ph/9910067)
[8] Tyc T *et al* 2002 *Phys. Rev.* A **65** 042310
[9] Bennet C H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing (Bangalore)* (New York: IEEE) p 175
[10] Beige A *et al* 2002 *J. Phys. A: Math. Gen.* **35** L407 (*Preprint* quant-ph/0101066)
[11] Beige A *et al* 2002 *Acta Phys. Pol.* **101** 357 (*Preprint* quant-ph/0111106)
[12] Boström K 2002 *Preprint* quant-ph/0203064
[13] Bouwmeester D 1999 *Phys. Rev. Lett.* **82** 1345 (*Preprint* quant-ph/9810035)
[14] Pan J-W *et al* 2001 *Phys. Rev. Lett.* **86** 4435 (*Preprint* quant-ph/0104047)
[15] Mair A 2001 *Nature* **412** 313 (*Preprint* quant-ph/0104070)
[16] Fiurášek J 2002 *Phys. Rev.* A **65** 053818 (*Preprint* quant-ph/0110138)
[17] Eibl M 2003 *Preprint* quant-ph/0302042
[18] Fiurášek J *et al* 2003 *Preprint* quant-ph/0304005
[19] Weinfurter H 1994 *Europhys. Lett.* **25** 559
[20] Calsamiglia J and Lütkenhaus N 2001 *Appl. Phys.* B **72** 67 (*Preprint* quant-ph/0007058)
[21] Dušek M 2001 *Opt. Commun.* **199** 161