

Attack Strategies in Entanglement Swapping QKD Protocols

Stefan Schauer, Martin Suda
Austrian Research Centers GmbH - ARC
Donau-City-Straße 1, 1220 Wien, Austria
Stefan.Schauer@arcs.ac.at, Martin.Suda@arcs.ac.at

Abstract

We will discuss a QKD protocol based on entanglement swapping [1] and show that it is open to a special type of attack using a higher-qubit system. An adversary will be able to obtain full information about the key without being detected. Additionally, we will give some ideas on how such protocols can be secured from this kind of attack strategy.

Introduction

Entanglement Swapping [2] is a phenomenon where 2 or more qubits that haven't interacted in the past are brought into an entangled state. Alice and Bob share two Bell states where Alice holds qubits 1 and 3 and Bob qubits 2 and 4. A Bell state measurement on Alice's qubits will alter the state of Bob's qubits immediately in a way which is completely determined by Alice's measurement result:

$$|\Phi^+\rangle_{12}|\Phi^+\rangle_{34} = \frac{1}{2} \left(|\Phi^+\rangle_{13}|\Phi^+\rangle_{24} + |\Phi^-\rangle_{13}|\Phi^-\rangle_{24} + |\Psi^+\rangle_{13}|\Psi^+\rangle_{24} + |\Psi^-\rangle_{13}|\Psi^-\rangle_{24} \right)$$

Thus, if Bob knows the initial shared states he can deduce Alice's result from his own without any further information from her.

Entanglement swapping has been used in various quantum key distribution protocols. For example one protocol is presented by Li et al. [1] where Alice and Bob share n pairs of Bell states. For each pair Alice applies one of the four Pauli operations on qubit 1 and then performs a Bell state measurement on qubits 1 and 3 in her possession. Further, she calculates the state of qubits 2 and 4. Bob performs a Bell state measurement on qubits 2 and 4 and calculates the state of qubits 1 and 3 using for the case that Alice applied no Pauli operation (imaginary result). Then he asks Alice for her result and, using this information, Bob is able to deduce which Pauli operation Alice applied. Both parties publicly compare a certain number of their results to detect an eavesdropper. Using some predefined mapping of Bell states and Pauli operations onto classical bits Alice and Bob are able to generate a raw key.

Eavesdropping Strategy

In the following we want to discuss what happens if Eve also uses entanglement swapping to perform an attack on the described protocol. In fact there exists a state which allows Alice to obtain full information about Alice's and Bob's secret measurement results:

$$|\delta\rangle_{PQRSTU} = \frac{1}{2\sqrt{2}} \left(|000000\rangle_{PQRSTU} + |001101\rangle_{PQRSTU} + |010111\rangle_{PQRSTU} + |011010\rangle_{PQRSTU} + |100110\rangle_{PQRSTU} + |101011\rangle_{PQRSTU} + |110001\rangle_{PQRSTU} + |111100\rangle_{PQRSTU} \right)$$

This state has the special property that it can be rewritten in the Bell basis as

$$|\delta\rangle_{PQRSTU} = \frac{1}{2} \left(|\Phi^+\rangle_{PR} \otimes |\Phi^+\rangle_{QS} \otimes |\Phi^+\rangle_{TU} + |\Phi^-\rangle_{PR} \otimes |\Phi^-\rangle_{QS} \otimes |\Phi^-\rangle_{TU} + |\Psi^+\rangle_{PR} \otimes |\Psi^+\rangle_{QS} \otimes |\Psi^+\rangle_{TU} + |\Psi^-\rangle_{PR} \otimes |\Psi^-\rangle_{QS} \otimes |\Psi^-\rangle_{TU} \right)$$

That means, if Alice performs a Bell state measurement on qubits P and R, Bob will obtain the desired result when he measures qubits Q and S and thus Eve will stay undetected. Additionally, the two qubits at Eve's side will be in the same state as Bob's qubits, which gives Eve full information about the key.

In detail, the attack strategy can be described in the following way: Eve intercepts qubits 2 and 4 in transit between Alice and Bob and performs a Bell state measurement on qubits 2 and P and 4 and R, respectively. Afterwards, Eve passes on qubits R to Alice and Q to Bob. When Alice performs her Bell state measurement on qubits 1 and R the qubits Q and 4 in Bob's possession will be brought into a state corresponding to Alice's result. Further qubits T and U will be in the same state as qubits Q and 4. Eve performs a Bell state measurement on qubits T and U and is able to calculate Alice's result from this measurement result. When Alice and Bob publicly compare a number of their results they won't detect Eve since the correlation between their results has not been destroyed.

To secure the protocol against this kind of attack an additional random application of certain operators, e.g. the Hadamard operator H can be used. In this case, Alice randomly decides whether to apply H on qubit 1 in her possession or not before she sends any qubit to Bob. She tells Bob about her decision after

she performed her Bell state measurement and Bob applies the H operator on the respective qubits in his possession. From this equation it appears that Bob's qubits Q and S will be in a state correlated to Alice's result only with 50% probability. Thus Eve will stay undetected with probability of 75% when Alice and Bob publicly compare n of their measurement results.

Conclusion

We presented an attack strategy using entanglement swapping on the protocol by Li et al. [1] which allows an adversary to successfully eavesdrop a secret key. The adversary uses a 6-qubit state which has the special property to preserve the correlation between the measurement results of Alice and Bob. Additionally we gave an idea on how to secure a

protocol against this kind of attack. We are currently analyzing whether this attack strategy can be generalized to protocols using entanglement swapping. A detailed description of our idea has been published recently in [3].

References

- [1] C. Li, Z. Wang, C.-F. Wu, H.-S. Song, and L. Zhou, International Journal of Quantum Information 4 (2006).
- [2] M. Zukowski, Z. A., M. Horne, and A. K. Ekert, Phys. Rev. Lett. 71, 4287 (1993).
- [3] S. Schauer and M. Suda, International Journal of Quantum Information 6, 841 (2008).