

## INTRODUCTION

Quantum key distribution (QKD) and quantum authentication (QA) have been a topic of extensive research in the last 20 years. In course of that many attacks on QKD and QA protocols have been studied. Among these, Zhang, Lee and Guo presented an attack [1] on a QKD protocol by Cabello using entanglement swapping [2]. Based on that strategy we take a look at other protocols to inspect how much information an adversary may get if he shares entanglement with either one or both parties. We will present a protocol where an adversary uses entanglement to get full information about the key without being detected.

## ENTANGLEMENT SWAPPING

Entanglement Swapping (ES) is a phenomenon where 2 or more qubits that haven't interacted in the past are brought into an entangled state. Suppose Alice and Bob share two Bell states, where Alice holds qubits 1 and 3 and Bob qubits 2 and 4. A Bell state measurement (BSM) on Alice's qubits will alter the state of Bob's qubits immediately in a way which is completely determined by Alice measurement result. Using the Bell basis it is easy to see (cf. eq. 1) that Bob's qubits are not in an arbitrary state but in a well-defined Bell state after Alice's BSM.

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

If Bob knows the initial shared states, i.e.  $|\Phi^+\rangle_{12}$  and  $|\Psi^+\rangle_{34}$ , he is able to deduce Alice's result from his own without any information from her.

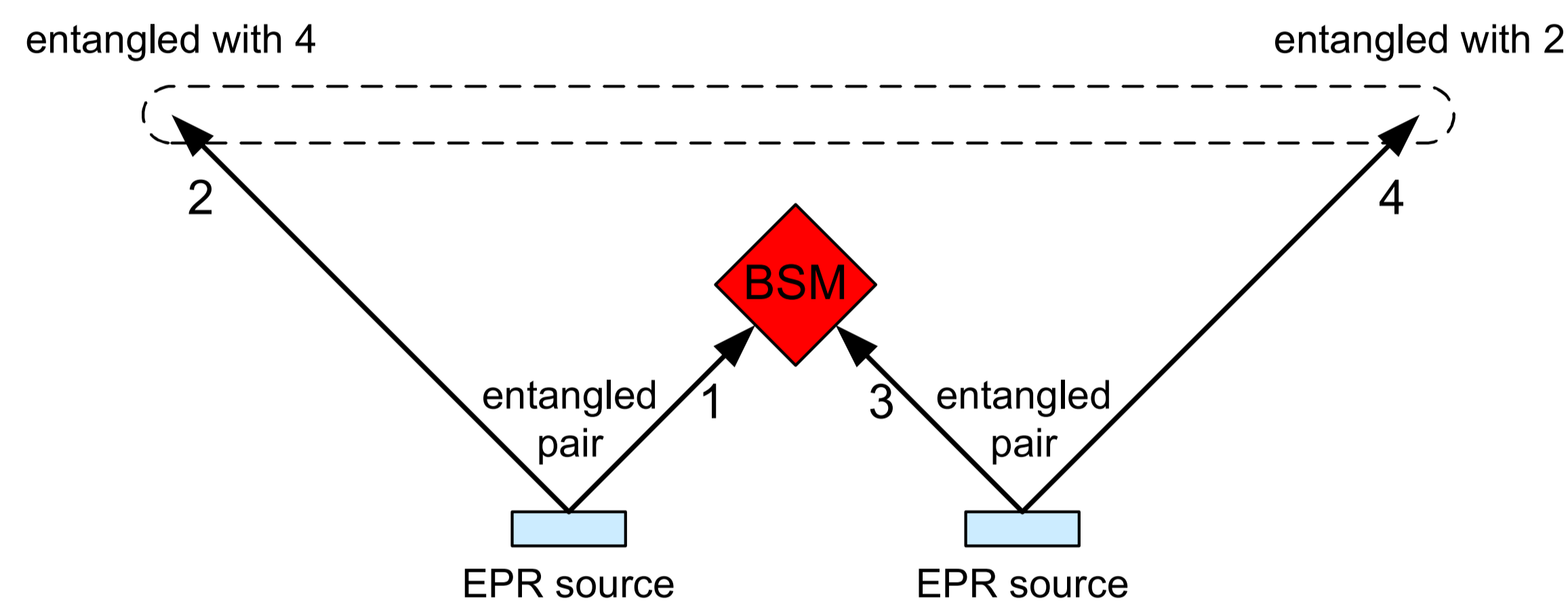


FIGURE 1: A simplified depiction of entanglementswapping (adapted from [3]). The dashed line symbolizes the final entanglement between qubits 2 and 4.

## THE CABELLO PROTOCOL

The protocol presented by Cabello in [2] is a QKD protocol based on ES. In difference to the BB84 and other protocols it sets aside the use of alternative measurements.

- Initial state:  $|\Phi^-\rangle_{12} \otimes |\Phi^+\rangle_{35} \otimes |\Phi^+\rangle_{46}$
- Alice holds qubits 1,2,3 and 5, Bob holds qubits 4 and 6
- Alice sends out qubit 2 and performs a BSM on qubits 1 and 3
- Bob receives qubit 2 and performs a BSM on qubits 2 and 4
- He sends out qubit 6 to Alice
- Alice receives qubit 6 and performs a BSM on qubits 5 and 6
- She publicly announces her result

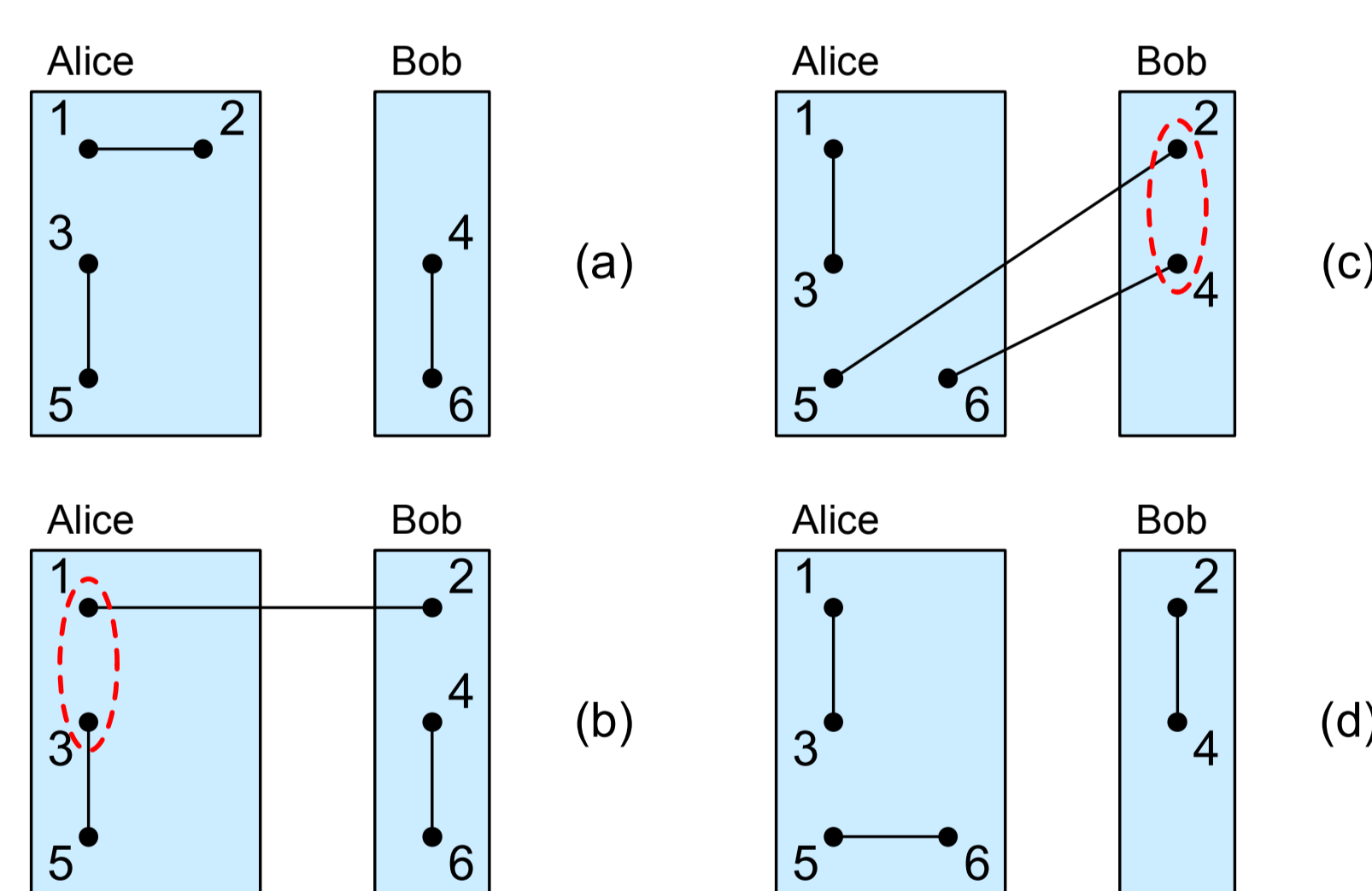


FIGURE 2: A schematic description of the Cabello protocol. A red dashed line symbolizes a BSM.

Using the public result and their respective result both parties are able to deduce the other's secret result.

## ZLG ATTACK

Eve's idea in the ZLG Attack [1] is to entangle herself with one party (Bob) and obtain information from this entanglement.

- Initial state:  $|\Phi^-\rangle_{12} \otimes |\Phi^+\rangle_{35} \otimes |\Phi^+\rangle_{46} \otimes |\Phi^+\rangle_{78}$
- Alice holds qubits 1,2,3 and 5, Bob holds qubits 4 and 6, Eve holds qubits 7 and 8
- Alice sends out qubit 2 and performs a BSM on qubits 1 and 3
- Eve intercepts qubit 2 and sends qubit 8 instead
- Bob receives qubit 8 and performs a BSM on qubits 8 and 4, then sends out qubit 6
- Eve intercepts qubit 6 and performs a BSM on qubits 6 and 7
- Depending on her result Eve applies one of the four Pauli operations (abbr. as  $\sigma_i$ ) on qubit 2 and sends it to Alice
- Alice receives qubit 2 but is convinced to have qubit 6 thus performing a BSM on qubits 5 and 2. She publicly announces her result

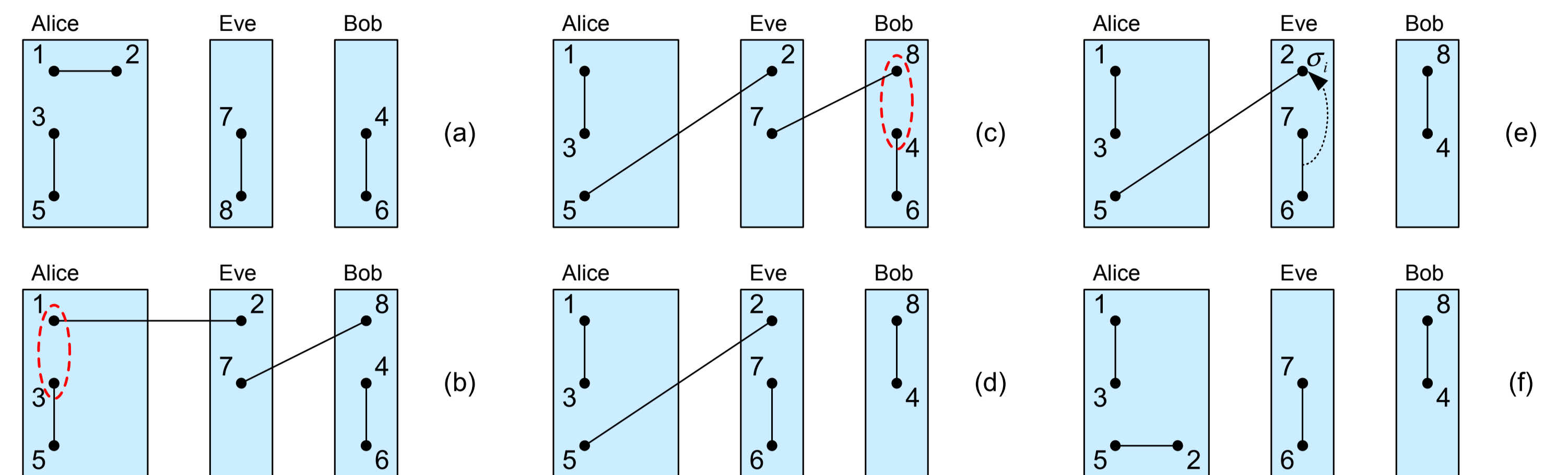


FIGURE 3: A schematic description of the ZLG attack on the Cabello protocol. A red dashed line symbolizes a BSM.

## ES-ATTACK ON THE WZT-PROTOCOL

The WZT protocol [4] uses the correlation between the qubits in a Bell state to establish a secret key. Therefore Alice changes between  $|\Phi^+\rangle_{12}$  and  $|\Phi^-\rangle_{12}$  to prevent eavesdropping. Both parties measure their qubit in the  $\{|+\rangle, |-\rangle\}$  basis.

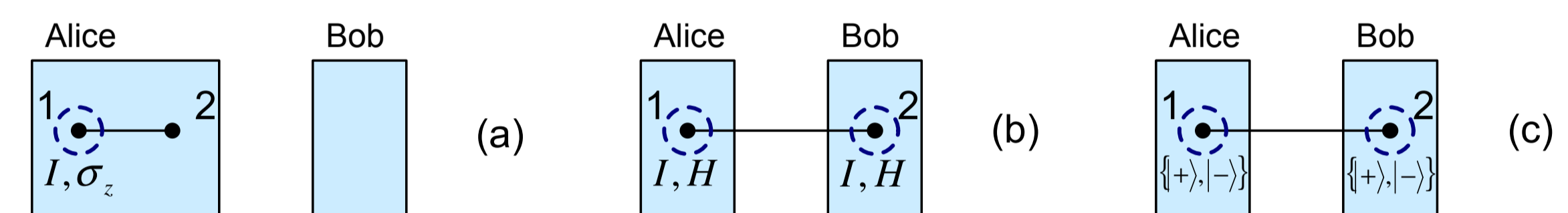


FIGURE 4: A simple illustration of the WZT protocol. A blue dashed line a local operation or measurement.

In the attack on the WZT protocol Eve uses a maximally entangled 4-qubit state  $|\delta\rangle$ , where to entangle herself with Alice and Bob. From the remaining 2 qubits in her possession she can infer the secret measurement results.

- Initial state:  $|\Phi^+\rangle_{12} \otimes \frac{1}{2}(|0000\rangle_{PQRS} + |0101\rangle_{PQRS} - |1010\rangle_{PQRS} - |1111\rangle_{PQRS})$
- Alice randomly applies  $\sigma_z$  on qubit 1 to change  $|\Phi^+\rangle_{12}$  to  $|\Phi^-\rangle_{12}$ . Then she sends out qubit 2
- Eve intercepts qubit 2 and performs a BSM on qubits 2 and P. She passes on qubit R
- Bob receives qubit R and Alice announces whether she applied  $\sigma_z$  or not
- If Alice did so, both parties apply the Hadamard operation on their qubits
- After that they measure them in the  $\{|+\rangle, |-\rangle\}$  basis

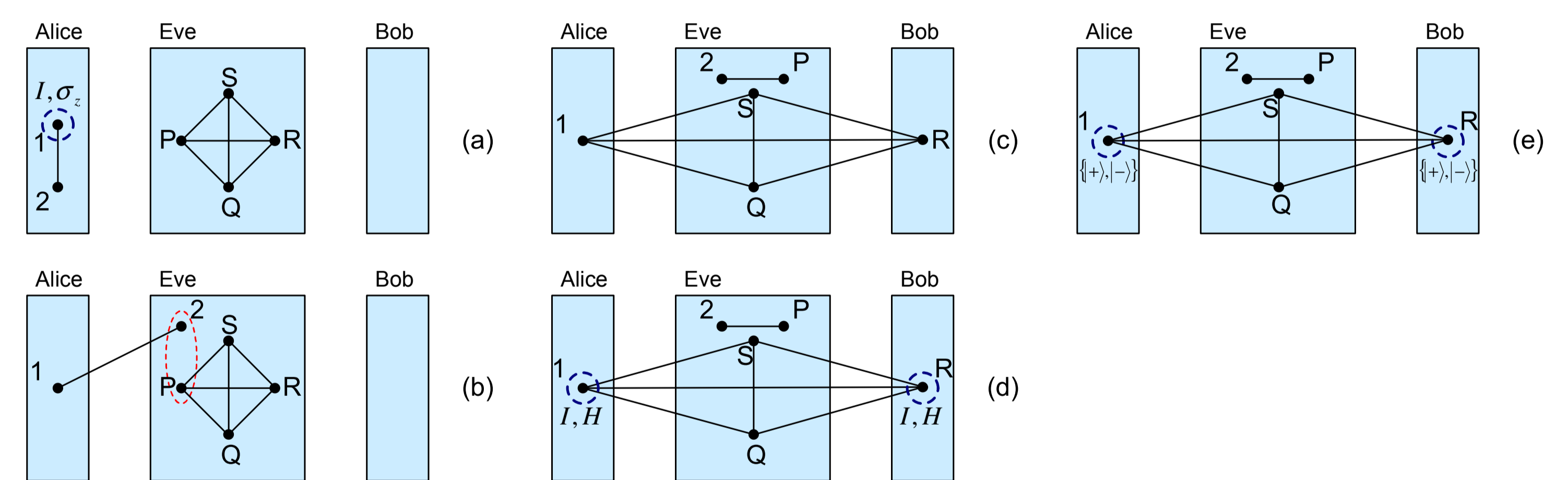


FIGURE 5: A description of Eve's attack on the WZT protocol. A red dashed line symbolizes a BSM, a blue dashed line a local operation or measurement.

Due to the entanglement of the four qubits Eve's qubits change according to Alice's and Bob's result and thus she is able to obtain their secret results without being detected.

## CONCLUSION AND OPEN QUESTIONS

As we can see there are strategies for Eve which allow her to get a secret key out of a QKD protocol without being noticed. Our further interest lies in the evaluation of several protocols to determine whether they are vulnerable to such an entanglement swapping attack and how such an attack might be prevented. Further the question arises if such kind of attacks can be formulated in a general way.

## References

- [1] Young-Sheng Zhang, Chuan-Feng Li, and Guan-Can Guo. Quantum Authentication using Entangled State. *quant-ph/0008044*, 2000.
- [2] Adan Cabello. Quantum Key Distribution without Alternative Measurements. *quant-ph/9911025 v2*, 2000.
- [3] Dirk Bouwmeester, Artur Ekert, and Anton Zeilinger. *The Physics of Quantum Information: Quantum Cryptography, Quantum Teleportation, Quantum Computation*. Springer, 2000.
- [4] Jian Wang, Quan Zhang, and Chao-jing Tang. Quantum Key Distribution Protocols using Entangled State. *quant-ph/0510208 v3*, 2005.