Improved Dynamic Multiparty Quantum Private Comparison for Next Generation Mobile Network

H. Abulkasim, H. Alsuqaih, W. Hamdan, A. Farouk, S. Hamad, A. Mashatan, and S. Ghose
Cybersecurity Research Lab, Ted Rogers School of Information Technology Management, Ryerson University

Introduction

Background: Recently, a multiparty quantum private comparison (QPC) protocol was proposed by **Liu and Wang (2017),** that can be used to control various auction models for 5G services.

Problem: We showed the protocol is **insecure against a particular strategy of collusion attacks** that leads to information leakage.

Solution: We suggested a **security enhancement** against the proposed attack strategy.

Background

Research Question: **What are the most secure procedures** that should be followed to avoid collusion attacks?

Objective: To describe the **current potential collusion attack strategies** and suggest **secure procedures** to address them.

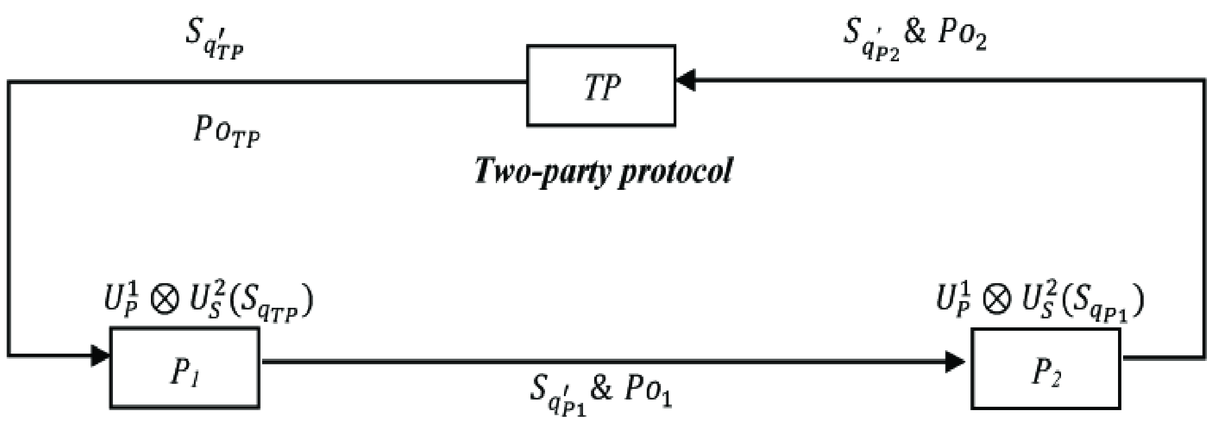

Figure 1 : Liu and Wang's (2017) QPC Protocol

Methodology

Unlike two-party QPC protocols, multiparty QPC protocols are susceptible to a powerful participant attack known as **collusion attack**.

This work :

- Cryptanalyzes Liu and Wang's (2017) QPC protocol.
- Identifies the security issues in Liu and Wang's (2017) protocol based on computational operations.
- Suggests necessary procedures to design a secure multiparty QPC protocol.

Results

The security analysis of Liu and Wang's (2017) protocol demonstrated that:

- Two dishonest participants can steal the private information from an honest one.

We also put forward a modified version of Liu and Wang's (2017) protocol in which:

- The third party (**TP**) pre-shares a random key with the participants to encrypt their private information.
- Or TP inserts additional decoy photons.

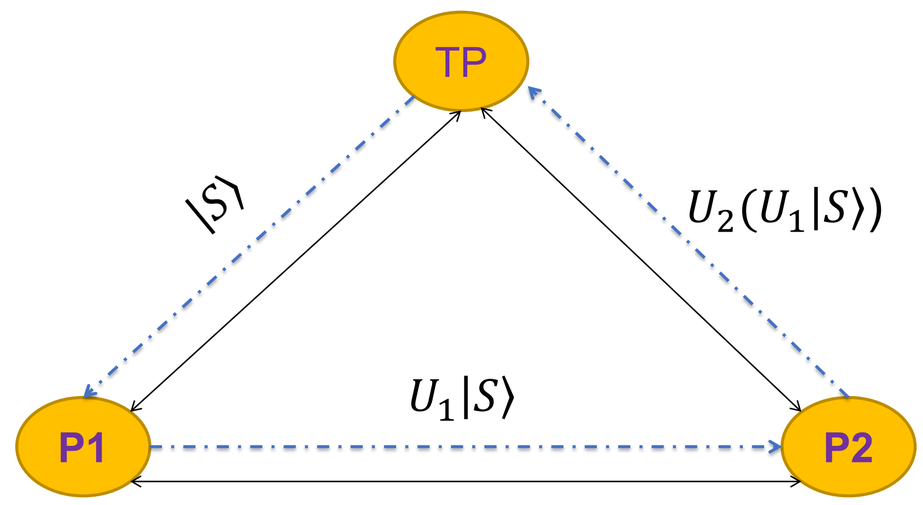

Figure 2 : Two-party QPC Protocol

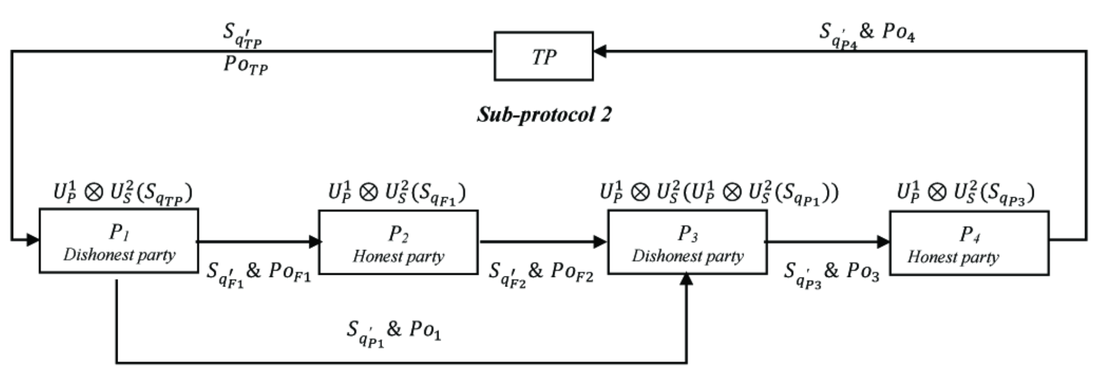

Figure 3 : The Suggested Attack Strategy on Liu-Wang's (2017) Protocol

Discussions

- Cryptanalysis is an essential ingredient in quantum cryptography
- In circular multiparty QPC protocols, more attention should be paid to collusion attack.
- We proposed a general solution to address the security issues in circular multiparty QPC protocols.

Implications

- Checking the security of communication among parties by the parties themselves is not sufficient to protect parties' privacy.
- It is recommended that both the TP and other participants collaborate to check the security of quantum channels to avoid collusion attacks.

References

1. *Yang, Y.G., Wen, Q.Y.: An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement. J. Phys. A Math. Theor. 42(5), 055305 (2009)*

2. *Liu, Wen, and Yong-Bin Wang. "Dynamic multi-party quantum private comparison protocol with single photons in both polarization and spatial-mode degrees of freedom." Int. J. Theo. Phy. 55.12 (2017): 5307-5317.*

Ryerson University
TED ROGERS SCHOOL Information Technology Management
WILFRID LAURIER UNIVERSITY LAURIER Inspiring Lives.
NSERC CRSNG
CYBERSECURITY RESEARCH LAB
www.ryerson.ca/crl