IMPROVED AND FORMAL PROPOSAL FOR DEVICE INDEPENDENT QUANTUM PRIVATE QUERY

Jyotirmoy Basak[1], Kaushik Chakraborty[2], Arpita Maitra[3], Subhamoy Maitra[1]

[1]Indian Statistical Institute, Kolkata, India. [2]The University of Edinburgh, UK.
[3]TCG Centre for Research and Education in Science and Technology, Kolkata.

QCRYPT 2021

Introduction

- 1 out of N Oblivious Transfer (OT)
  - Distrustful quantum cryptographic scheme.
  - Client queries to a database and knows only intended bits (known as Database Security).
  - Server should not know any information about client's query (known as User Privacy).
- Private information retrieval (PIR)
  - Database query technique which guarantees only user privacy.
  - Symmetric private information retrieval (SPIR) takes PIR further by additionally offering database privacy.
- Quantum Private Query (QPQ)
  - Conceptually a probabilistic version of OT or SPIR with weaker security.
  - Client is allowed to know the non-intended bits with negligible probability.
  - User privacy is preserved in a cheat-sensitive way.

QPQ vs SPIR vs OT

- Impossible to design information theoretic secure OT both in quantum as well as classical setting.
- Information theoretic secure SPIR can be designed in a distributed database setting [1].
- Due to weaker security requirement, information theoretic secure QPQ can be designed in a single database setting [2,3].

Contributions

1. Propose a novel QPQ scheme with full Device Independent (DI) certification.
   - We exploit the self-testing mechanism of EPR pairs along with the proper self-testing mechanism of projective measurement [4] and POVM measurement device to certify full DI.
2. In our scheme, we replace the usual projective measurement at client's side with optimal POVM measurement.
   - Client can obtain maximum raw key bits with certainty and (possibly) retrieve the maximum number of data bits in a single query.
3. We provide (for the first time in this domain) a general security analysis considering all the attacks that preserve the correctness condition.
   - Provide an upper bound on the cheating probabilities for both dishonest server as well as dishonest client.

QPQ vs QKD

- The parties trust each other in QKD but not in QPQ.
- Every party knows all the bits of the shared key in QKD but not in QPQ.

QKD Based QPQ Schemes

- Key Generation:
  - The server and the client share entangled states to generate a shared raw key among themselves such that the server knows all the key bits but the client knows only some of the bits.
- Private Query:
  - Server encrypts the whole database with the shared key and send it to client.
  - The client decrypts the intended bits using her known key bits.

Security Issues

The security is guaranteed based on the following definitions-

- Correctness: In honest Bob and honest Alice scenario (considering no channel noise), the probability that Alice can correctly retrieve the expected number of raw key bits is very high.
- Device Independent Security: In honest Bob and honest Alice scenario (considering no channel noise), if the input-output statistics of an unknown device satisfies a predefined value then it guarantees that the device is noiseless.
- Data Privacy: The expected number of data bits ($D_{\mathcal{A}^*}$) that dishonest Alice ($\mathcal{A}^*$) can guess in a single query from the N-bit database X is upper bounded by τN (where τ is negligible in N) i.e.,

$$\max_{\mathcal{A}^*}[E_R(D_{\mathcal{A}^*}|\text{Bob does not abort})] \leq \tau N$$

- User Privacy: If the honest Alice wants to have access to $x_{i_1}, \ldots, x_{i_l}$ bits of the N-bit database X and $\mathcal{I}_l = \{i_1, \ldots, i_l\}$ denotes the corresponding indices set, then the expected number of bits ($\mathcal{I}_{\mathcal{B}^*}$) guessed by the dishonest Bob ($\mathcal{B}^*$) from the set $\mathcal{I}_l$ is upper bounded by δl (where δ is negligible in l) i.e.,

$$\max_{\mathcal{B}*}[E_{R'}(\mathcal{I}_{\mathcal{B}^*}|\text{Alice does not abort})] \leq \delta l$$

Possible Future Works

- Remove the *i.i.d* assumptions.
- To check whether the DI testing can be done in less number of phases using less number of samples.
- Analyze the performance of this scheme considering channel noise.

Proposed DI-QPQ Scheme

Full DI schemes certify the functionality of all the devices involved in a scheme without imposing any trustful assumptions on them.

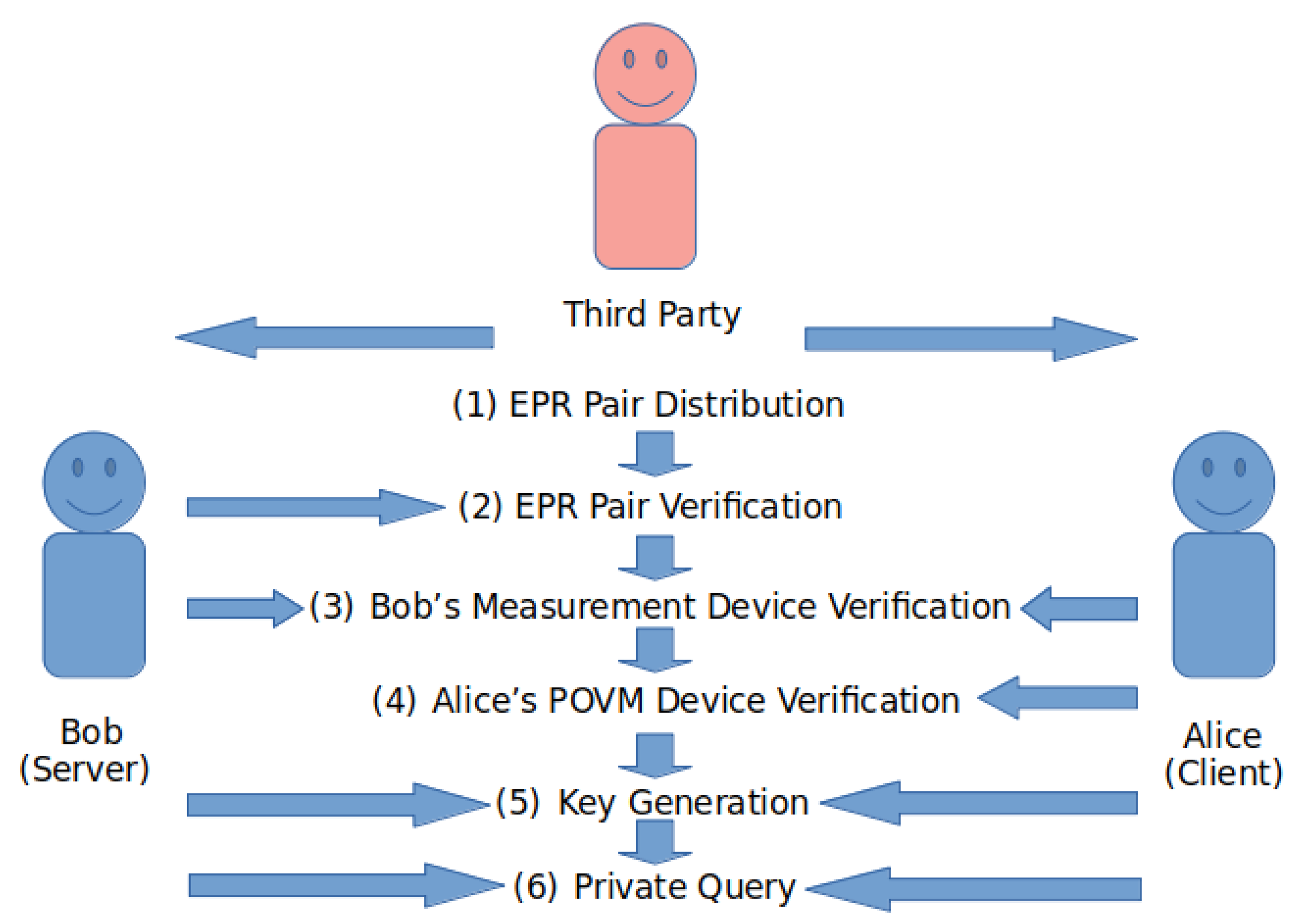

Fig. 1: Schematic diagram of our proposed DI-QPQ scheme

[1]. Y. Gertner, Y. Ishai, E. Kushilevitz, and T. Malkin, *Journal of Computer and System Sciences*, 60, 3, 592–629, 2000.
[2]. V. Giovannetti, S. Lloyd, L. Maccone, *Physical review letters*, 100, 23, 230502, 2008.
[3]. A. Maitra, G. Paul, S. Roy, *Phys. Rev. A*, 95, 4, 042344, 2017.
[4]. J. Kaniewski, *Phys. Rev. A*, 95, 6, 062323, 2017.