Twin-field quantum digital signatures

Chun-Hui Wang, Yu-Teng Fan, Chun-Mei Zhang, Guang-Can Guo, Qin Wang*,
Institute of quantum information and technology, Nanjing University of Posts and Telecommunications, Nanjing, 210003, China
*qinw@njupt.edu.cn Web: quantum.njupt.edu.cn

Abstract: Inspired by the twin-field quantum key distribution [1], we first propose a twin-field quantum digital signature (TF-QDS) protocol, which is secure against all detection side-channel attacks, and present a corresponding security analysis. In its distribution stage, a specific key generation protocol (KGP), the sending-or-not-sending (SNS) twin-field protocol [2], has been adopted. Besides, after implementing full parameter optimization, the results show that TF-QDS exhibits outstanding performance compared with the other two typical protocols, BB84-QDS [3] and MDI-QDS [4].

Theory:
A schematic diagram of our TF-QDS is illustrated in Fig. 1. In distribution stage, the pairs Alice-Bob and Alice-Charlie perform TF-KGP separately through Eve to generate keys, and then Bob and Charlie randomly choose half keys to exchange with a secret channel to Alice. In messaging stage, Alice’s signature is sent to Bob for authentication, and forwarded to Charlie for further verification.

In TF-KGP, we employ the SNS protocol [2] to generate sifted keys. The min-entropy resulting from single-photon components in the half of keys kept by Bob or Charlie ($U^A_{m,keep}$) at the presence of Eve is

$$\tilde{H}_E^*(U^A_{m,keep} | E) \geq n_{L,1} \{1 - H_2(\tilde{r}_{L,1})\},$$

where $n_{L,1}$ and $\tilde{r}_{L,1}$ respectively represent the lower bound of single-photon counts and upper bound of single-photon error rate; $H_2(\cdot)$ is the binary Shannon entropy function.

The security level $\varepsilon$ of QDS protocol is guaranteed by three probabilities and requires

$$\max\{P_{\text{Robust}}, P_{\text{Repudiation}}, P_{\text{Forge}}\} \leq \varepsilon.$$  

Besides, we propose a simple model, signature rate $R$, to evaluate the performance of a QDS protocol as

$$R = \frac{n_{\text{pool}}}{N},$$

Finite-key parameter estimation:

![Finite-key parameter estimation diagram](image)

Results:
The comparisons of signature rates between BB84-QDS [3], MDI-QDS [4] and our TF-QDS [5] at the security level $\varepsilon = 10^{-5}$ and total pulses $N = 10^{13}$ or $N = 10^{15}$.

![Signature rate comparison](image)

Conclusion:
We propose a TF-QDS protocol, and develop a uniform framework on evaluating the signature performance for all QDS protocols, demonstrating that our present protocol shows outstanding security and practicality among all existing QDS protocols.

References: