arXiv:2003.11262 (2020)

Twin-field quantum digital signatures

Chun-Hui Zhang, 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.

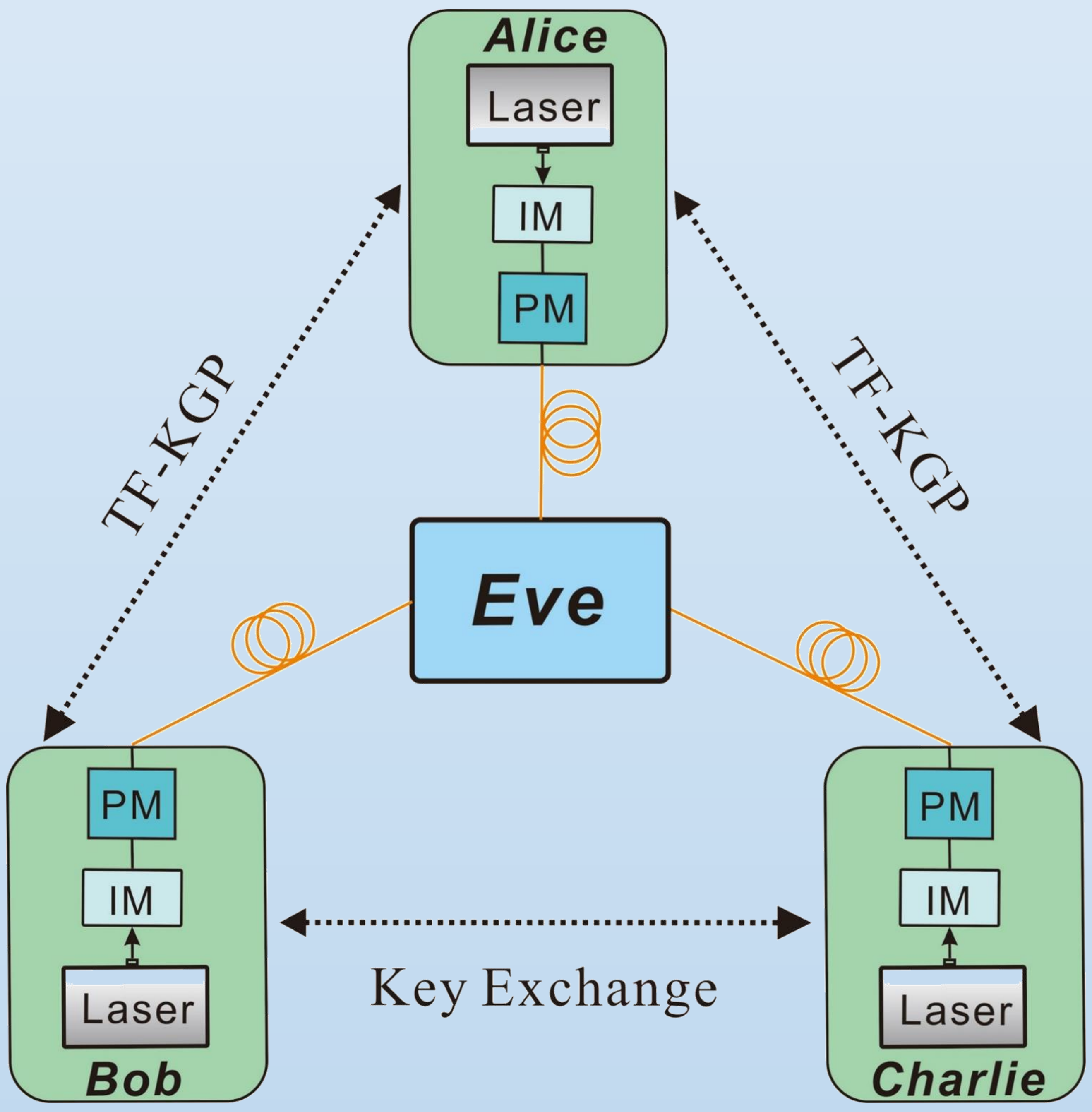

Fig. 1. Schematic of our TF-QDS protocol.

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

$$H^{\epsilon}_{\min}(U^{A}_{m,keep}|\,E) \gtrsim \underline{n}_{L,1}[1-H_2(\overline{e}_{L,1})]\,, \qquad (1)$$

where $\underline{n}_{L,1}$ and $\bar{e}_{L,1}$ 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 ε of QDS protocol is guaranteed by three probabilities and requires

$$\max\{\mathrm{P(Robust)}, \mathrm{P(Repudiation)}, \mathrm{P(Forge)}\} \leqslant \varepsilon\,. \qquad (2)$$

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

$$R = \frac{n_{pool}}{2L} \cdot \frac{1}{N}\,. \qquad (3)$$

Finite-key parameter estimation:

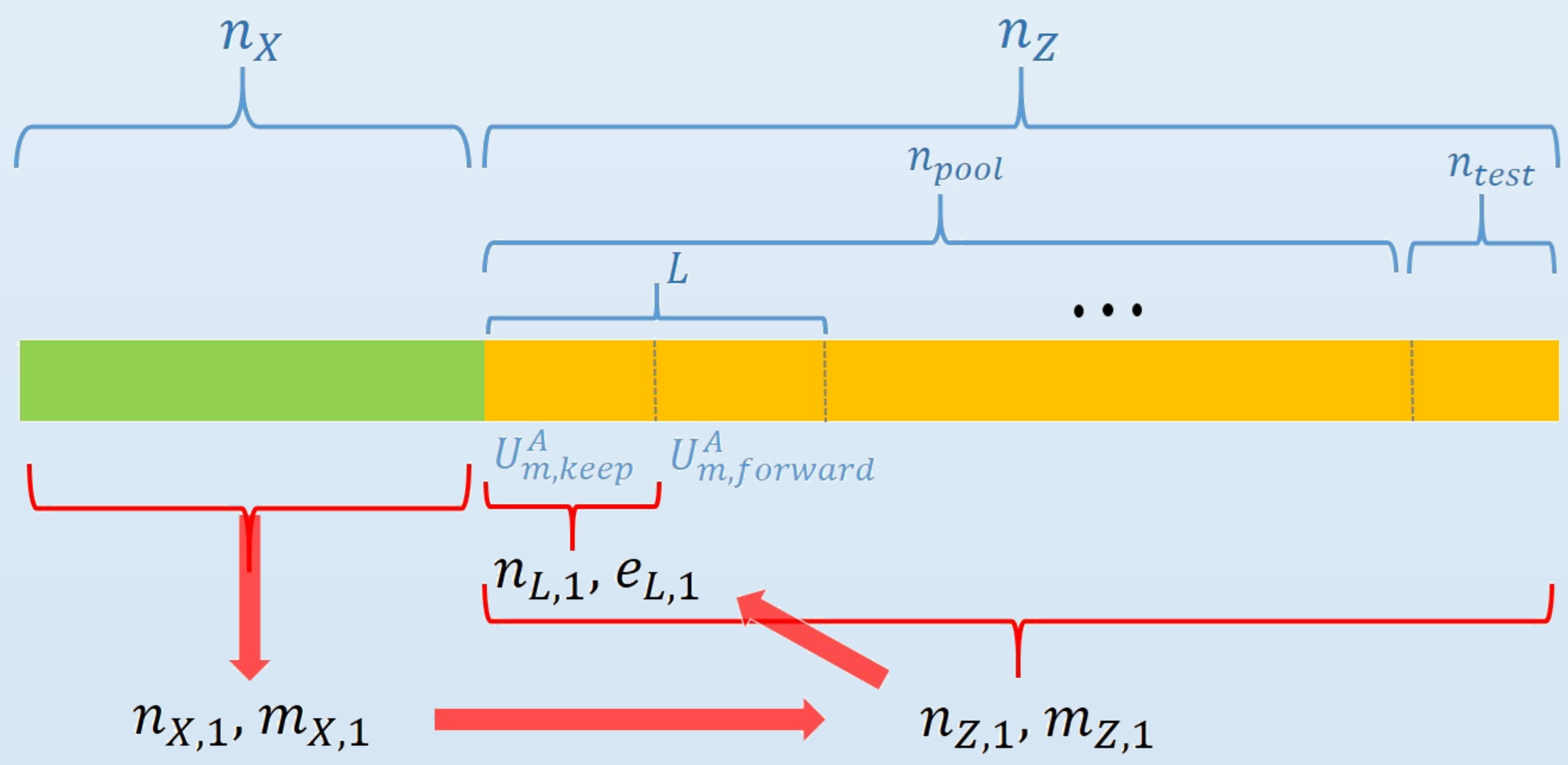

Fig. 2. The relationships of different data blocks and the route of estimating relevant parameters. n_X and n_Z are the lengths of the data on X basis and on Z basis; n_{pool} is the length of key pool and n_{test} is the length of the keys used for error test; L is the length of a basic block in n_{pool} to sign message m. $n_{X,1}$ and $m_{X,1}$ are the single-photon counts and error counts in n_X, while $n_{Z,1}$ and $m_{Z,1}$ are the quantities in n_Z; $n_{L,1}$ and $e_{L,1}$are the single-photon counts and error rate in $U^A_{m,keep}$.

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 $N = 10^{15}$.

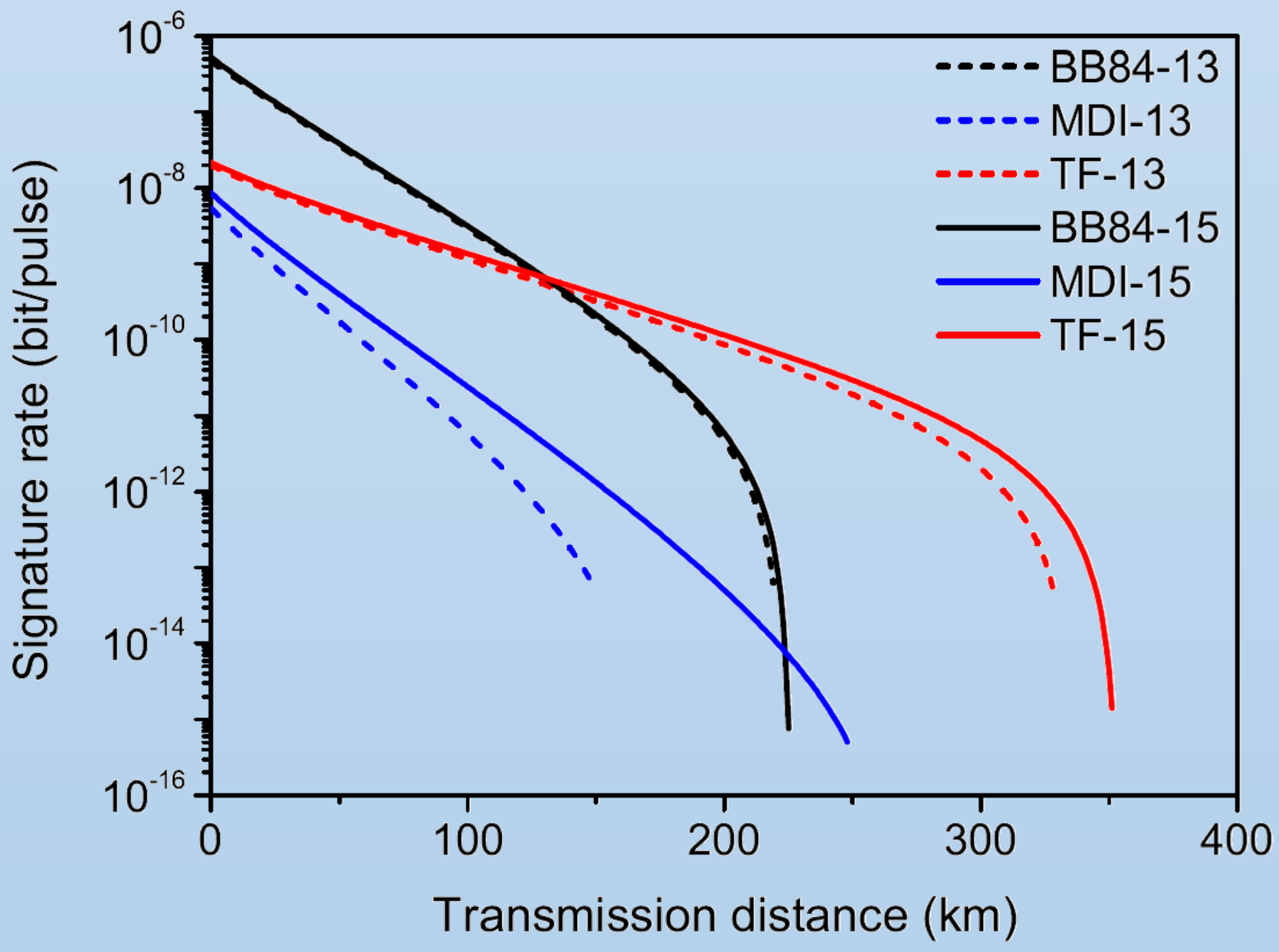

Fig. 3. The signature rates of BB84-QDS [3], MDI-QDS [4] and TF-QDS [5].

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:

[1] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Overcoming the rate-distance limit of quantum key distribution without quantum repeaters, Nature **557**, 400 (2018).
[2] X. B. Wang, Z. W. Yu, and X. L. Hu, Twin-field quantum key distribution with large misalignment error, Phys. Rev. A **98**, 062323 (2018).
[3] R. Amiri, P. Wallden, A. Kent, and E. Andersson, Secure quantum signatures using insecure quantum channels, Phys. Rev. A **93**, 032325 (2016).
[4] I. V. Puthoor, R. Amiri, P. Wallden, M. Curty, and E. Andersson, Measurement-device-independent quantum digital signatures, Phys. Rev. A **94**, 022328 (2016).
[5] C. H. Zhang, Y. T. Fan, C. M. Zhang, G. C. Guo, Q. Wang, Twin-field quantum digital signatures, arXiv:2003.11262 (2020).