An FPGA-Based Controller for B92 QKD Systems Featuring Synchronized Secret Key Extraction

Sreeja R R[1], Kamala J[1], Sahaana Kanagesan[1], AR Aruna[1], Sivasubramanian S[2]

[1]*Department of ECE, College of Engineering Guindy, Anna University, Chennai-600025, India*

[2]*Primebridge Consultancy and Services, Sivagangai, India*

This research presents a high-speed FPGA-based hardware realization of a Quantum Key Distribution (QKD) controller utilizing the B92 protocol. Unlike software-centric models, this architecture executes real-time secret key synchronization and encryption entirely in hardware to minimize latency [1]. The system employs two FPGA nodes, Alice and Bob, communicating via an SPI bus. Each node independently generates 64-bit pseudo-random numbers using Linear Feedback Shift Registers (LFSR). Through hardware-level bitwise comparison logic, Bob identifies matching bits from Alice's transmitted stream to assemble a synchronized 64-bit secure key, effectively discarding mismatches to ensure key integrity. The core innovation is a unique dual-layer encryption engine. Level 1 utilizes the 64-bit synchronized key for primary data protection. Level 2 introduces a secondary non-linear layer by extracting a 58-bit secret key and a 6-bit pointer from the original key. Validated on the Xilinx Basys 3 platform, the design achieves an efficient power profile of 4.201 W [2]. This modular approach provides a scalable foundation for practical free-space QKD systems and secure hardware training kits, bridging the gap between theoretical quantum protocols and real-world hardware constraints [3].

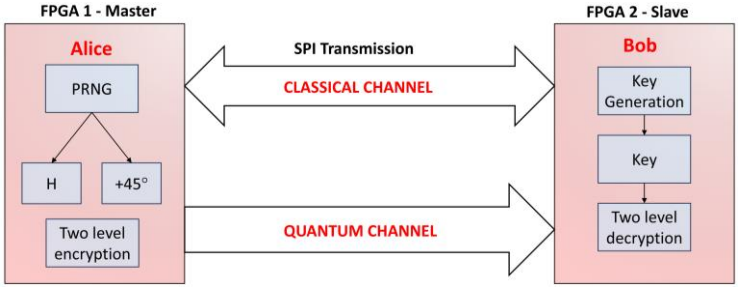

Fig. 1: *FPGA based QKD Controller with B92 Protocol.*

References

[1] A. Stanco, F. B. L. Santagiustina, L. Calderaro, M. Avesani, T. Bertapelle, D. Dequal, G. Vallone, and P. Villoresi, IEEE Trans. Quantum Eng. 3, 1 (2022).

[2] Y. Abbas and A. Abdullah, IOP Conf. Ser.: Mater. Sci. Eng. 1076, 012043 (2021).

[3] M. Canale, D. Bacco, S. Calimani, F. Renna, N. Laurenti, G. Vallone, and P. Villoresi, Proc. of conference, edited by N. P. Editor (ACM, 2011), p. 1.