Implementation challenges of Photon-Beetle, a NIST Standardization Finalist

CARLOS ANDRES LARA-NINO AND PIERRE ANTOINE TISSOT[*],

Univ Lyon, UJM-Saint-Etienne, CNRS. Laboratoire Hubert Curien UMR 5516, F-42023, France.

Ten lightweight authenticated ciphers have been selected as finalists of the Lightweight Cryptography Standardization process by NIST. These algorithms provide authenticated encryption and hashing through different design approaches, offering varying tradeoffs between performance and implementation complexity. As the final round of the standardization process draws to the end, the focus of the evaluation has shifted towards bench-marking these finalists using different hardware targets. Low-cost FPGAs stand out in this regard. Despite implementation results for multiple finalists being reported, several algorithms still remain unattended. That is the case of Photon-Beetle, which to the best of our knowledge, has not been implemented before in hardware. In this talk, we discuss the implementation challenges associated with this algorithm. We first propose an unified low-area architecture for the implementation of Photon-Beetle with focus on the 32-bit rate variant. Our design performs data encryption, decryption, and hashing through an unified datapath. Then, we review the security of this architecture against side-channel attacks and propose a threshold implementation. Lastly, we propose modifications to the algorithm which can improve the efficiency and security of its implementation.

[*] Authors appear in alphabetical order.

Author's address: Carlos Andres LARA-NINO and Pierre Antoine TISSOT,
Univ Lyon, UJM-Saint-Etienne, CNRS. Laboratoire Hubert Curien UMR 5516, F-42023, 18 rue Benoit Lauras 42000, 18 rue du Professeur Benoît Lauras 42000, Saint-Étienne, France., carlos.lara@univ-st-etienne.fr, pierre.antoine.tissot@univ-st-etienne.fr.