CONFERENZA GARR 2025
FRONTIERE DIGITALI

FPGA implementation of the 'encrypted cable'

Antonio Mastrandrea[1], Paolo Palazzari[2], *Pasquale Tommasino*[1]

[1]Dept. of Information Engineering, Electronics and Telecommunications, Sapienza University of Rome

[2]ENEA, ICT-HPC Division, Casaccia Research Center, Rome

Secure communication in Smart Grids

- Secure data transmission in Smart Grids, both for management and accounting purposes, requires data encryption

- Transmission of encrypted data prevents data from being stolen or tampered for fraudulent purposes

Encryption algorithms

- Several performance comparisons in technical literature indicate that AES is a good candidate for encrypting data within a smart grid

- The QP-Dyn algorithm, a symmetric encryption algorithm based on the chaotic properties of a class of deterministic dynamical systems (Anosov systems), can also be considered

- The QP-Dyn algorithm generates longer secret keys in less time. QP-Dyn with 279-bit key outperforms AES-256 in Cipher Feedback mode for text sizes exceeding 256 bytes

Encryption algorithms

- The dynamical systems in QP-Dyn are described by a 4 x 4 integer matrix M

- These systems feature very long periodic ‘orbits’ that pass common randomness tests despite not being properly chaotic (the starting point cannot be un irrational number)

- Each point of the orbit is produced, starting from the initial state S_0, through the recurrence

$$S_{n+1}=M\,S_n$$

- Modulo *p* arithmetic is used (*p* is a large prime number)

Hardware implementation

- In the present implementation two independent QP-Dyn systems have been considered; the keys generated at each iteration are XORed together

- Modulo *p* multiplications are efficiently implemented using Montgomery's algorithm

Name	LUT	LUTAsMem	REG	BRAM	URAM	DSP
Platform	194876 [14.95%]	22868 [3.81%]	278667 [10.69%]	330 [16.37%]	0 [0.00%]	10 [0.11%]
User Budget	1108804 [100.00%]	578092 [100.00%]	2328693 [100.00%]	1686 [100.00%]	960 [100.00%]	9014 [100.00%]
Used Resources	8840 [0.80%]	644 [0.11%]	6351 [0.27%]	4 [0.24%]	0 [0.00%]	124 [1.38%]
Unused Resources	1099964 [99.20%]	577448 [99.89%]	2322342 [99.73%]	1682 [99.76%]	960 [100.00%]	8890 [98.62%]
Memory2Stream	1308 [0.12%]	277 [0.05%]	1510 [0.06%]	2 [0.12%]	0 [0.00%]	0 [0.00%]
Memory2Stream_1	1308 [0.12%]	277 [0.05%]	1510 [0.06%]	2 [0.12%]	0 [0.00%]	0 [0.00%]
Stream2Memory	1194 [0.11%]	367 [0.06%]	1913 [0.08%]	2 [0.12%]	0 [0.00%]	0 [0.00%]
Stream2Memory_1	1194 [0.11%]	367 [0.06%]	1913 [0.08%]	2 [0.12%]	0 [0.00%]	0 [0.00%]
rtl_QPDYN_NEW	6338 [0.57%]	0 [0.00%]	2928 [0.13%]	0 [0.00%]	0 [0.00%]	124 [1.38%]
rtl_QPDYN_NEW_1	6338 [0.57%]	0 [0.00%]	2928 [0.13%]	0 [0.00%]	0 [0.00%]	124 [1.38%]

Hardware implementation

- Secure communication between two users (the ‘encrypted cable’) exchanging QP-DYN encrypted data through the AXI-Stream interface has been implemented on FPGA using the VITIS development flow

- The ‘encrypted cable’ was deployed and tested between two nodes (Casaccia and Portici) of the ENEA network. Both nodes host ALVEO U280 FPGA boards

Encryption performance

- The intrinsic throughput of the ‘encrypted cable’ was measured between two connected U280 boards: it is **750 MB/s**
- Using the current communication infrastructure, the throughput shown by the cable is determined by the actual BW available between the sites
- The introduction of the encryption/decryption layer does not limit the channel BW and the latency added by the layer (few μs) does not significantly impact the channel latency

Thanks for your attention!

- The work was performed in the framework of:

Piano Triennale della ricerca di sistema del settore elettrico nazionale per il triennio 2022-2024 - Progetto 2.1 "Progetto integrato cyber security dei sistemi energetici"

- Contact emails: antonio.mastrandrea@uniroma1.it

paolo.palazzari@enea.it

pasquale.tommasino@uniroma1.it