DOI: 10.26314/GARR-Conf25-proceedings-22

The 'encrypted cable': FPGA implementation of secure communication based on cryptographic algorithms

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

Abstract. The "Encrypted Cable", a secure and high-speed communication system for public communication networks, is proposed as a solution for encrypted data exchange between nodes in a smart grid. Encryption and decryption are performed on an FPGA using the QP-Dyn cryptographic algorithm. The proposed system achieves an intrinsic throughput of 750 MB/s and has been successfully tested in encrypted transmissions between ENEA sites in Casaccia and Portici.

Keywords. Smart grid, Cyber security, Cryptography, FPGA

Introduction

In modern smart grids, both the energy distribution network and its associated data communication network are extensive and highly branched. Ensuring secure data transmission and management is essential—from individual devices, such as smart meters installed in apartments, to entire buildings and neighborhoods [Fouda 2011]. These smart meters, capable of bidirectional data exchange, may be located in private residences or connected to charging stations for electric vehicles [Cheng 2024]. Encrypting transmitted data is crucial to prevent unauthorized access and safeguard user privacy.

Various types of encryption algorithms exist, typically categorized into three main classes: symmetric, asymmetric, and those based on hash functions [Alenezi 2020]. These algorithms serve to protect data from theft, tampering, and unauthorized processing by entities responsible for managing smart meter data. Encryption requirements vary across the hierarchy of the network architecture. While individual smart meters—often constrained in terms of computational resources—operate within private networks, higher-level systems must handle significantly larger volumes of data. Although these upper levels generally have greater processing power, they often depend on public networks, which are inherently less secure.

1. Encryption algorithm choice

This research focuses on the development and hardware implementation of cryptographic algorithms optimized for deployment on programmable logic devices, particularly targeting the upper levels of the smart grid network hierarchy. A preliminary analysis was con-

Conferenza GARR 2025 - Frontiere Digitali Selected Papers
Bari, 13-15 maggio 2025 - ISBN: 978-88-946629-4-8 - Creative Commons CC-BY

ducted to identify algorithms offering the best performance for this context.
In [Abood 2017], symmetric and asymmetric encryption algorithms suitable for secure data transmission in smart grids were compared in terms of encryption/decryption times and the estimated time required to break the encryption for short plaintexts. Among them, the asymmetric RSA algorithm with a 1024-bit key [Rivest 1978] was found to be the slowest, while the Advanced Encryption Standard (AES) [Daemen 2002] demonstrated both the highest security and fastest execution. Additionally, in [Alenezi 2020], common symmetric algorithms were evaluated based on throughput, encryption time, and CPU usage for varying text sizes. AES, RC4, and RC6 yielded the best performance overall; however, only AES showed high resistance to known cryptographic attacks, as noted in [George 2023].
Based on performance and security benchmarks, AES emerges as the most suitable candidate for data encryption in smart grids. However, secure communication in this context often requires additional cryptographic operations, given the hierarchical architecture comprising at least three levels: from smart meters (lowest level), to one or more data aggregation centers, up to the highest level (e.g., the power operator, PO), which is also responsible for key management and distribution. Asymmetric encryption is often employed at this top level to ensure secure key distribution. For instance, the protocol described in [Uludag 2015] uses the Diffie-Hellman algorithm for key exchange, AES-256 for data encryption, and SHA-256 for digital signatures. Consequently, while AES is optimal for primary encryption tasks, it must often be supported by auxiliary cryptographic mechanisms to ensure complete security.
In addition to AES, the QP-Dyn algorithm [Abundo 1992][Accardi 2011] has also been considered. QP-Dyn is a symmetric encryption algorithm based on the chaotic behavior of a class of deterministic dynamical systems known as Anosov systems. These systems produce very long periodic orbits that pass standard randomness tests, despite not being fully chaotic, as their orbits cannot originate from irrational initial points.
A comparative study [Italiano 2009] evaluating encryption algorithms for mobile applications showed that QP-Dyn generates longer secret keys more quickly than conventional algorithms. Specifically, when comparing its stream cipher version to AES in Cipher Feedback mode (AES-CFB), QP-Dyn—with a 279-bit key—outperformed AES-CFB with a 256-bit key for input sizes greater than 256 bytes. Although AES in block cipher mode (its standard configuration) remains faster overall, the performance gap is minimal (<60 ms) for blocks smaller than 512 bytes.

2. Hardware implementation and transmission tests

Secure communication between two users—referred to as the "encrypted cable"—was implemented using the VITIS environment [Amd 2023], enabling encrypted data exchange via the AXI-Stream interface. The data (e.g., from a smart meter) are streamed from memory to a QP-Dyn encoder. The encrypted data is then sent back to memory, with overall latency primarily determined by memory access times.
The QP-Dyn algorithm is implemented using dynamical systems modeled as a matrix M

of size d × d. Starting from an initial state $S_0 = [S_{0,1} \dots S_{0,d}]$, the system generates an orbit S_0, S_1, ... through the recurrence relation

$$S_{i+1,j} = (\Sigma^{d}_{k=1} M_{j,k}\, S_{i,k}) \bmod p \qquad j=1,2,\dots,d \qquad (1)$$

The parameter p is typically a large number. In this implementation, two independent dynamical systems M_A and M_B with d = 4 were used. Secret keys K_A and K_B were derived at each iteration i from the states $S_{i,A}$ and $S_{i,B}$, respectively, using a Key Generating Function (KGF), and combined via an XOR operation. KGF constructs the encryption key by concatenating the words derived from $S_{i,j}$ (j=1,2,...,d) removing all leading zeros up to and including the first 1.

The modulo p operations are efficiently handled using Barrett's algorithm [Barrett 1986] which avoids division operations.

Figure 1 shows a schematic of the QP-Dyn architecture. The "Dynamic System" block implements equation (1); on even cycles, it computes the evolution of system M_A, while M_B is updated on odd cycles.

The XOR operation on KGF outputs generates the final key

$$K_i = K_{i,A} \text{ XOR } K_{i,B}$$

which is used to encode the input word via a bitwise XOR.

The initial states $S_{0,A}$ and $S_{0,B}$, which are parameters of the encryption algorithm, are loaded during the first two clock cycles via the multiplexer input selected by the condition i≤1.

Once synthesized on an AMD ALVEO U280 board, the "encrypted cable" was deployed between two nodes of the ENEA network: an encryption node at the Casaccia site and a decryption node at the Portici site. The design was synthesized with a target clock frequency of 100 MHz.

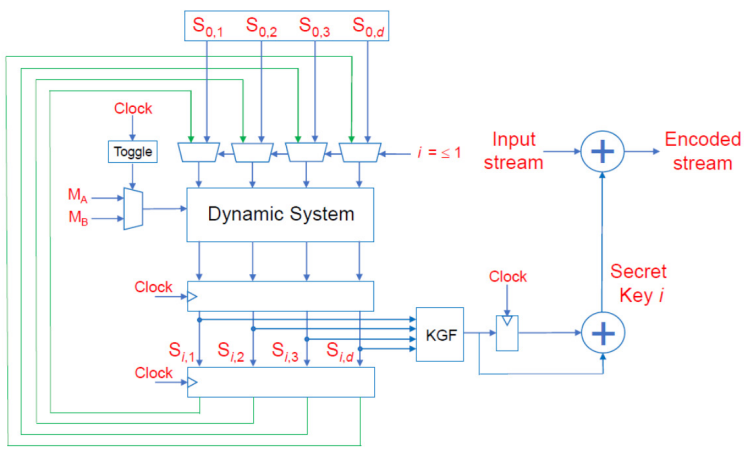

Fig. 1
QP-Dyn algorithm implemented with two dynamic systems MA and MB

The synthesis results are summarized in Figure 2, demonstrating the low hardware resource utilization of the QP-Dyn implementation.
The system was validated through a series of tests: first on a single node hosting both transmitter and receiver on two U280 boards, and then in a real-world deployment between the ENEA Casaccia and Portici sites. The first test evaluated the intrinsic throughput of the "encrypted cable", considering only encryption, decryption, and memory transfers, and yielded a performance of 750 MB/s.

Name	LUT	LUTAsMem	REG	BRAM	URAM	DSP
Platform	194876 [14.95%]	23758 [3.95%]	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 [1.60%]
Unused Resources	1099964 [99.20%]	577448 [99.89%]	2322342 [99.73%]	1682 [99.76%]	960 [100.00%]	8890 [98.40%]
Memory2Stream	1308 [0.12%]	277 [0.05%]	1510 [0.05%]	2 [0.12%]	0 [0.00%]	0 [0.00%]
Memory2Stream_1	1308 [0.12%]	277 [0.05%]	1510 [0.05%]	2 [0.12%]	0 [0.00%]	0 [0.00%]
Stream2Memory	1194 [0.11%]	367 [0.06%]	1913 [0.06%]	2 [0.12%]	0 [0.00%]	0 [0.00%]
Stream2Memory_1	1194 [0.11%]	367 [0.06%]	1913 [0.06%]	2 [0.12%]	0 [0.00%]	0 [0.00%]
krnl_qp_dyn	6338 [0.57%]	0 [0.00%]	2928 [0.13%]	0 [0.00%]	0 [0.00%]	124 [1.38%]
krnl_qp_dyn_1	6338 [0.57%]	0 [0.00%]	2928 [0.13%]	0 [0.00%]	0 [0.00%]	124 [1.38%]

Fig. 2 Synthesis results on the ALVEO U280 board

The inter-site test, on the other hand, reported a throughput of 60 MB/s, limited by the available bandwidth of the communication channel between the two locations.

3. Conclusions

We presented an FPGA implementation of the QP-Dyn encryption algorithm, which generates pseudo-random numbers using a dynamical system. These numbers are used as ciphering keys for point-to-point encrypted communication within the context of energy smart grids.

References

Abood, O. G. et al. (2017). Investigation of cryptography algorithms used for security and privacy protection in smart grid. In 2017 Nineteenth International Middle East Power Systems Conference (MEPCON) (pp. 644-649). IEEE.
Abundo, M. et al. (1992). Hyperbolic automorphisms of tori and pseudo-random sequences. Calcolo, 29, 213-240.
Accardi, L. et al. (2011). The Qp-Dyn Algorithms (Vol. 8, pp. 1-15). Singapore: World Scientific Publishing Co. Pte. Ltd.
Alenezi, M. N. et al. (2020). Symmetric encryption algorithms: Review and evaluation study. International Journal of Communication Networks and Information Security, 12(2), 256-272.
Amd: UG 1399 - Vitis High-Level Synthesis User Guide. 2023.
Cheng, R. et al. (2024). LLRA: A Lightweight Leakage-Resilient Authentication Key Exchange Scheme for Smart Meters. IEEE Transactions on Smart Grid.
Daemen, J., & Rijmen, V. (2002). The design of Rijndael (Vol. 2). New York: Springer-verlag.
Fouda, M. M et al. (2011). A lightweight message authentication scheme for smart grid communications. IEEE Transactions on Smart grid, 2(4), 675-685.
George, D. J., & Thomas, T. (2023). A Comparative Study of Symmetric Key Algorithms. International Journal of Computer Science and Mobile Computing, Vol.12 Issue.6, June-

2023, pg. 71-75.
Guan, D. J. (2003). Montgomery algorithm for modular multiplication. Departement of Computer Science, National Sun Yar-Sen University, Taiwan.
Italiano, G. F. et al. (2009, August). Benchmarking for the QP cryptographic suite.
MontgomeryBarrett, P. L. (19865). Modular multiplication without trial division. Mathematics of computation, 44(170), 519-521. Implementing the Rivest Shamir and Adleman Public Key Encryption Algorithm on a Standard Digital Signal Processor. Advances in Cryptology – CRYPTO' 86. Lecture Notes in Computer Science. Vol. 263. pp. 311–323.
Rivest, R. L. et al. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120-126.
Uludag, S. et al. (2015). Secure and scalable data collection with time minimization in the smart grid. IEEE Transactions on Smart Grid, 7(1), 43-54.

Authors

Antonio Mastrandrea antonio.mastrandrea@uniroma1.it

Antonio Mastrandrea received the master's(Laurea) degree (cum laude) in electronics engineering and the Ph.D. degree, from the Sapienza University of Rome, Rome, Italy, in 2010 and 2014,respectively. He is a Research Assistant with the Department of Information Engineering, Electronics and Telecommunications, Sapienza University of Rome. His current research interests include digital system-on-chip architectures and nano-CMOS circuits oriented to high-speed computation.

Paolo Palazzari paolo.palazzari@enea.it

Paolo Palazzari (M.Eng. 1989, Ph.D. 1994) has been a researcher at ENEA since 1996. He founded ENEA's first spin-off, Ylichron srl, developing the HCE High-Level Synthesis tool. From 2010 to 2018 he was detached to PLDA Italia as CTO, contributing to the development of the QuickPlay High-Level Synthesis flow. Since 2018 he has returned to ENEA as a senior researcher, focusing on FPGA algorithm development using High-Level Synthesis tools.

Pasquale Tommasino pasquale.tommasino@uniroma1.it

Pasquale Tommasino is a researcher at the Department of Information, Electronics and Telecommunications Engineering of the University "La Sapienza" of Rome. His research activity focuses mainly on the design of integrated circuits for communication applications in the microwave and millimetre wave field, in its different aspects of methodology, modelling and development of circuit topologies, and also on issues concerning spectral analysis and processing of radar and communication signals.