Design of Signcryption system using PHOTON Hash Function on FPGA platform

Raghavendra A[1], Sai Kiran Oruganti[2]

[1]Postdoctoral Researcher, Lincoln University College, 47301, Petaling Jaya, Selangor Darul Ehsan, Malaysia

[2]Professor, Lincoln University College, 47301, Petaling Jaya, Selangor Darul Ehsan, Malaysia;

Email ID: pdf.drRaghavendra@lincoln.edu.my, saisharma@lincoln.edu.my.

Abstract: The rapid expansion of the Internet of Things (IoT), and embedded systems has raised the demand for lightweight and efficient cryptographic technologies that can provide reliable communication while using minimal hardware resources. This article describes an FPGA-based signcryption system that uses the lightweight PHOTON hash function to accomplish confidentiality, integrity, and authentication. The suggested architecture is made up of modules for key generation, encryption, and decryption that have been optimized for hardware deployment. The design was built on an Artix-7 FPGA and validated via functional simulation. Experimental findings show that message recovery and authentication are successful at a maximum operating frequency of 350.128 MHz, a throughput of 282.36 Mbps, and a total power usage of 149 milliwatts. The collected results demonstrate that the suggested architecture is suitable for resource-constrained secure interaction scenarios.

Keywords: Signcryption; PHOTON hash; Cryptography; FPGA;

Introduction

One of the most promising innovations for use in multifaceted applications is the IoT. IoT offers numerous benefits, but there are also significant issues with security, privacy, interoperability, and complexity [1]. Because signcryption systems are more efficient and less computationally expensive than the sign-then-encrypt method, they are advantageous in situations when resources are limited [2]. The best method for sending encrypted and verified data is signcryption. As a result, it may be applied to mobile device authentication as well. Three types of data are often used for authentication: (1) user-owned items, such smart cards; (2) user-known data, like passwords; and (3) user biometrics, like fingerprints. Password-based authentication is sometimes referred to as single-factor authentication. Signcryption has several potential uses in managing keys, digital government, and online retail [3].

Problem Statement: Developing IoT devices, wireless sensor networks (WSNs), and embedded systems all demand safe transmission protocols that can function under constrained area, power, and computing resource limits. Conventional systems frequently execute encryption and digital signature procedures individually, which increases hardware difficulty, latency, and energy usage. Furthermore, many existing encryption algorithms are not designed for lightweight FPGA architectures, rendering them inappropriate for low-resource scenarios. As a result, there is a need for an effective hardware design that unifies encryption and authentication into a single framework while preserving high security and minimal implementation cost. A lightweight encryption system based on the PHOTON hash function can

address these issues by minimizing resource use, power usage, and processing overhead while maintaining security.

Related Works

This section discusses the current developments in signcryption techniques. The initial FPGA deployment of Ascon-Sign for resource-constrained wireless sensor networks was described by Magyari and Chen [4], who achieved almost double the processing speed of similar architectures while lowering power usage per operation by 33%. A reliable and anonymous authentication system with fog computing and signature verification was suggested by Rajasekaran et al. [5], which reduced computational overhead by 12.04% and improved communication costs by 5.35%. A Physical Unclonable Function (PUF)-based identifying tag architecture with a lightweight authentication mechanism that is more stable and less susceptible to assaults was created by Rullo et al. [6]. Additionally, a blockchain-enabled Attribute-Based Signcryption (ABSC) architecture combined with edge computing for secured medical data handling was presented by Dou et al. [7]. Their method increased access efficiency, decreased computing load, and strengthened data security. A lightweight signcryption technique utilizing triple-truncated DES and nonlinear integrity verification was presented by Ghazal et al. [8] for Internet of Medical Things (IoMT) applications. In comparison to current systems, experimental findings showed increases of 14.12% in detection accuracy, a 13.67% decrease in service failures, and a shorter calculation time.

Method

The suggested PHOTON-based signcryption system is illustrated in Figure 1 and is made up of three primary components: Key Generation, Signcryption, and Unsigncryption. These modules together guarantee confidentiality, authentication, integrity, and non-repudiation. The architecture is optimized for FPGA implementation efficiency by using lightweight PHOTON hash algorithms for key generation and authentication.

The server and node individually create their cryptographic identities in the *Key Generation Unit*. The PHOTON hash function is used to process the Server ID (SID) and Node ID (NID) before concatenating them with other parameters like system parameter p and time information. The Master Private Key (M_{pvt}), Master Public Key (M_{pub}), Node Private Key (P_{pvt}), and Node Public Key (P_{pub}) are all produced by these processes. The signcryption and unsigncryption components then receive the created keys for safe interaction.

The *Signcryption Unit* generates digital signatures and encrypts data at the same time. First, a Linear Feedback Shift Register (LFSR) is used to create a random number λ. S and T are determined the parameters using λ and the cryptographic keys. After then, the plaintext message M is was converted to ciphertext C. An authentication digest H is created using a second PHOTON hash after an interim digest τ is calculated using the first PHOTON hash operation to guarantee message integrity. Lastly, the ciphertext and auxiliary parameters are concatenated with an authentication tag Φ to create the signcrypted output $(e = C, \Phi, T, S)$.

The *Unsigncryption Unit* receives the signcrypted tuple $(e = C, \Phi, T, S)$ from the receiver side. The identical random value λ is reproduced using the transmitted factor T, allowing the original plaintext message M to be recovered. The same two-stage PHOTON hashing technique is then used to the recovered message to produce a middle digest τ, authentication digest H, and receiver authentication

tag Φ'. A comparison is made between the received tag Φ and the produced tag Φ'. The message is properly authenticated and validated if both values match (Φ'); if not, it is denied.

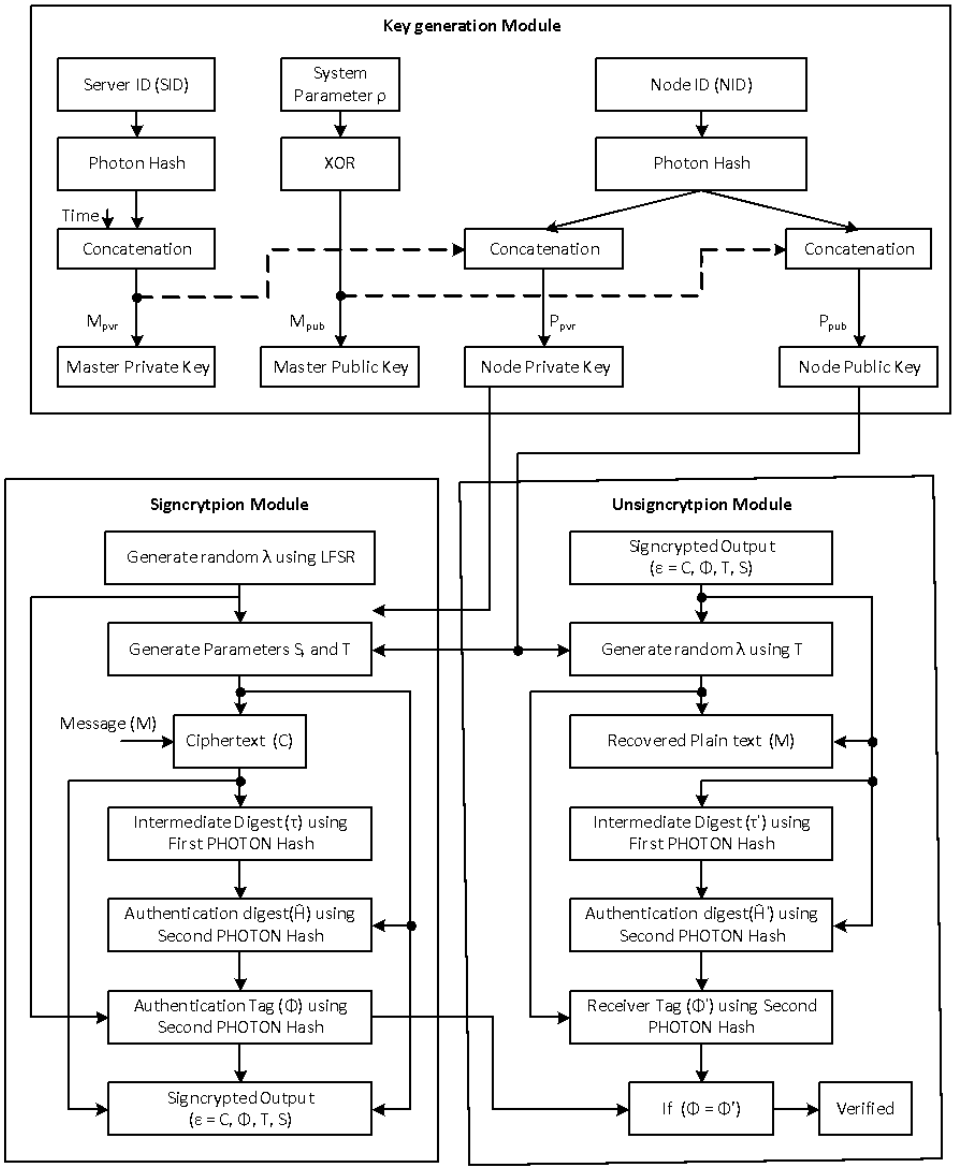

Figure 1. Hardware architecture of PHOTON-Based Signcryption System

Results

The suggested PHOTON hash-based signcryption mechanism was developed and evaluated on an Artix-7 FPGA device to ensure functionality correctness and hardware efficiency. The design combines lightweight PHOTON hash processes with encryption and decryption algorithms to deliver secure interaction with minimal resource use and high performance. Functional verification was carried out using simulation, and synthesis findings were acquired to evaluate hardware performance parameters like as area, frequency, power usage, latency, and throughput.

Figure 2 depicts the functional simulation waveform for the suggested signcryption framework. Following the assertion of the start signal, the signcryption module processes the sender and recipient identities, timestamp, plaintext message, and random parameter. The input message "abcde" is successfully encrypted, sent, and then recovered by the unsigncryption module. The recovered message is identical to the original plaintext, proving the integrity of both the encryption and decryption methods. Additionally, the validated signal is asserted following authentication tag validation to demonstrate successful integrity and authenticity verification. The done signal indicates that the signcryption-unsigncryption procedure has been completed, hence certifying the system's functioning.

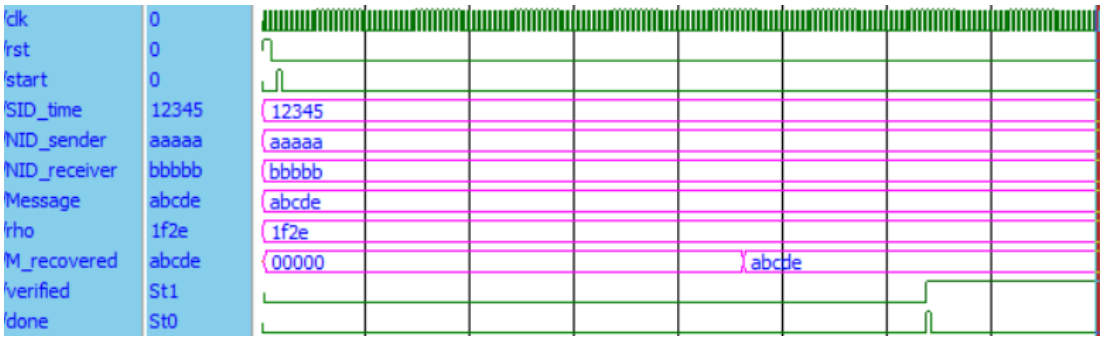

Figure 2. Simulation results of Signcryption system

Table 1 presents the hardware implementation findings for the proposed design on the Artix-7 FPGA. The design uses 604 slices, 1458 LUTs, and 457 LUT-FFs, suggesting a small hardware footprint appropriate for resource-constrained scenarios. The solution reaches a maximum running frequency of 350.128 MHz, exhibiting the power of the streamlined datapath and lightweight PHOTON hash structure. The observed static and dynamic power usages are 82 and 67 mW, respectively, for a total power usage of just 149 mW. The design consumes 124 clock cycles to execute a signcryption operation and achieves a throughput of 282.36 Mbps with an efficiency of 0.468 Mbps/Slice, demonstrating its potential to offer high-speed secure communication while maximizing hardware usage.

Table 1. Resource usage of Signcryption system using PHOTON-Hash on Artix-7 FPGA

Resources	**Usage**
Slices	604
LUTs	1458
LUT-FFs	457
Max. Frequency (MHz)	350.128
Static Power (mW)	82
Dynamic Power (mW)	67
Total Power (mW)	149
Latency (CC)	124
Throughput (Mbps)	282.36
Efficiency (Mbps/Slice)	0.468

Discussion

The obtained findings show that the suggested PHOTON-based encryption architecture strikes an appropriate balance between security, area utilization, and effectiveness. The PHOTON hash function is lightweight, reducing device complexity while ensuring reliable authentication and integrity verification. The successful simulation outcomes support the signcryption process's reliability, while the FPGA implementation findings indicate that the design functions at high frequency while using little power and using moderate resources. These features make the suggested technique ideal for FPGA-based IoT, sensor networks, and other resource-constrained integrated security initiatives that require efficient end-to-end secure interaction.

Conclusion

This paper described a lightweight FPGA-based signcryption architecture that uses the PHOTON hash function for safe transmission in resource-constrained contexts. The suggested approach combines key generation, signcryption, and unsigncryption procedures to guarantee confidentiality, integrity, and authentication, in a single framework. Functional simulation confirmed that sent communications were successfully encrypted, recovered, and authenticated. The hardware implementation using an Artix-7 FPGA shows effective resource usage, with 604 slices, 1458 LUTs, and a low power consumption of 149 mW. The architecture's highest operational frequency of 350.128 MHz and throughput of 282.36 Mbps demonstrate its applicability for high-performance embedded security programs.

References

1. A. Kumar, R. Saha, and G. Kumar, “LiSP: A Lightweight Signcryption using PHOTON hash for Internet-of-Things Infrastructure,” in *2020 IEEE International Symposium on Sustainable Energy, Signal Processing and Cyber Security (iSSSC)*, IEEE, 2020, doi: 10.1109/iSSSC50941.2020.9358905.
2. T. -H. Kim, G. Kumar, R. Saha, W. J. Buchanan, T. Devgun and R. Thomas, "LiSP-XK: Extended Light-Weight Signcryption for IoT in Resource-Constrained Environments," in *IEEE Access*, vol. 9, pp. 100972-100980, 2021, doi: 10.1109/ACCESS.2021.3097267.
3. P. Zhang, Y. Li, and H. Chi, “An elliptic curve signcryption scheme and its application,” *Wirel. Commun. Mob. Comput.*, vol. 2022, pp. 1–11, 2022, doi: 10.1155/2022/7499836.
4. Magyari and Y. Chen, “Securing the internet of things with ascon-sign,” *Internet Things (Amst.)*, vol. 28, no. 101394, p. 101394, 2024, doi: 10.1016/j.iot.2024.101394.
5. S. Rajasekaran, A. Maria, B. P. Chapa and A. R. Gondu, "FAV2G: Fog-Based Authentication Scheme for Vehicle-to-Grid Network With Verilog Implementation," in *IEEE Open Journal of the Computer Society*, vol. 6, pp. 1512-1524, 2025, doi: 10.1109/OJCS.2025.3613959.
6. Rullo *et al.*, "PUF-Based Authentication-Oriented Architecture for Identification Tags," in *IEEE Transactions on Dependable and Secure Computing*, vol. 22, no. 1, pp. 66-83, Jan.-Feb. 2025, doi: 10.1109/TDSC.2024.3387568.
7. T. Dou, Z. Zheng, W. Qiu, and C. Ge, “A secure medical data framework integrating blockchain and edge computing: An attribute-Based Signcryption approach,” *Sensors (Basel)*, vol. 25, no. 9, p. 2859, 2025, doi: 10.3390/s25092859.
8. T. M. Ghazal *et al.*, “Lightweight signcryption scheme for Securing wearable sensor observed health data sharing in internet of medical things paradigm,” *Sci. Rep.*, vol. 15, no. 1, p. 40989, 2025, doi: 10.1038/s41598-025-24687-0.