Indonesian Journal of Electrical Engineering and Computer Science
Vol. 42, No. 2, May 2026, pp. 542~551
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v42.i2.pp542-551

GRAND-stream: a Galois-ring-based lightweight stream cipher for battery-limited internet of things (IoT) devices

Nahom Gebeyehu Zinabu[1], Yihenew Wondie Marye[2], Kula Kekeba Tune[1], Samuel Asferaw Demilew[3]
[1]Department of Software Engineering, College of Engineering, Addis Ababa Science and Technology University, Addis Ababa, Ethiopia
[2]School of Electrical and Computer Engineering (SECE), Addis Ababa University (AAU), Addis Ababa, Ethiopia
[3]Department of Information Technology, College of Computing, Debre Berhan University, Debre Berhan, Ethiopia

Article Info

Article history:

Received Jan 18, 2026
Revised Mar 4, 2026
Accepted May 26, 2026

Keywords:

Algebraic cryptography
Energy efficiency
Galois ring
IoT security
Lightweight cryptography
Stream cipher

ABSTRACT

GRAND-Stream is a new lightweight stream encryption framework based on arithmetic over Galois rings that targets battery-constrained internet of things (IoT) devices. Unlike traditional LFSR/NLFSR-based designs, GRAND-stream uses ring-squaring-induced nonlinearity and inter-component polynomial coupling to improve algebraic complexity while keeping compact implementation qualities. We give an explicit parameterized construction for $Z_2^n[x]/(f(x))$, specify its state updating and output functions, and investigate algebraic degree growth and diffusion behavior. The security arguments are heuristic, based on explicitly stated assumptions about the difficulty of solving quadratic systems over Galois rings. Energy per bit, cycle count, and gate complexity are estimated using an analytical performance model. Although initial findings show potential compactness, more research is needed for thorough cryptanalysis and empirical validation on embedded devices. Therefore, GRAND-stream should be considered a structured algebraic design concept that needs more assessment.

Corresponding Author:

Nahom Gebeyehu Zinabu
Department of Software Engineering, College of Engineering
Addis Ababa Science and Technology University (AASTU)
Addis Ababa, Ethiopia
Email: nahom.gebyehu@aastustudent.edu.et

1. INTRODUCTION

The exponential growth of the internet of things (IoT) has created a massive ecosystem of devices operating under strict energy, memory, and computing constraints [1], [2]. These constraints necessitate cryptographic primitives that are not only compact and efficient, but also resistant to algebraic and implementation-level attacks, including side-channel attacks (SCA). Recent lightweight cryptography standardization initiatives (such as ascon) demonstrate the community's shift toward approaches that balance mathematical provability and practical hardware feasibility [3], [4]. The three fundamental limitations imposed on a battery-limited IoT device are: i) tight energy-per-bit budgets, ii) limited availability of RAM/ROM, and finally, iii) sensitivity to physical attacks in deployment. Existing lightweight stream ciphers tackle subsets of these constraints; however, several designs either lack strong algebraic underpinnings or provide little or no guidance for SCA-resistant implementation [5], [6].

The explicit grand-stream: GRAND-stream is a ring-based keystream generator over a Galois ring $Z_2^n[x]/\langle f(x)\rangle$ that incorporates nonlinear polynomial mappings and ring cyclic shifts to increase the algebraic complexity of the design while maintaining a minimal compact internal state. In particular, we propose a family of parameterizable polynomial update functions Pi (·) that achieve high algebraic degree at low

hardware cost: thanks to their simple form, they can be efficiently mapped to barrel shifters and XOR/AND logic. We also provide heuristic security arguments based on algebraic complexity assumptions in the Galois ring domain and outline a clear path to integrating masking and hiding countermeasures for SCA resistance [7]–[12].

Research gap and motivation: The predominant design approach remains primarily heuristic and structure-driven, despite the widespread development of lightweight stream ciphers such as Trivium, Grain-128a, and Ascon-Stream. The majority of current constructs rely on combinations of Boolean nonlinear components, ARX-based permutations, or LFSR/NLFSR feedback mechanisms [1], [4], [13], and [14]. Though their internal evolution is usually examined in the Boolean domain rather than inside an explicitly structured algebraic framework, these methods have undergone extensive cryptanalysis and are regarded as secure within specified security margins. Specifically, Boolean combining functions whose algebraic complexity is assessed over GF(2) introduce nonlinearity in LFSR/NLFSR-based architectures. Similarly, ARX-based constructs use word-level modular addition and rotation, but they are not based on structured polynomial evolution over rings or explicit algebraic hardness constraints.

Furthermore, lightweight stream cipher designs operating directly over Galois rings of the form $\mathbb{Z}_{2^n}[x]/f(x)\rangle$ have received relatively little attention, even though finite fields $GF(2^n)$ are frequently utilized in block cipher design. In the context of lightweight stream ciphers, the promise of ring-based polynomial evolution and modular squaring as compact nonlinear mechanisms for restricted devices has not been extensively investigated. This indicates a glaring research gap: The possibility that structured algebraic constructions over Galois rings can offer a different lightweight stream cipher framework that permits explicitly modeled algebraic complexity increase while maintaining a compact implementation cost has not received much attention.

This gap raises the following research questions:

- Is it possible to achieve adequate nonlinear mixing with little hardware overhead by implementing modular squaring over $\mathbb{Z}_{2^n}$?
- In contrast to exclusively Boolean LFSR designs, does ring-based state evolution make a system more resistant to conventional algebraic modelling?
- Under stringent IoT energy restrictions, can such structures be parameterized to accomplish effective diffusion and degree growth?

To answer these problems, GRAND-stream is proposed as an experimental framework that builds a parameterized keystream generator directly over $\mathbb{Z}_{2^n}[x]/f(x)$. Nonlinearity arises from ring squaring and modular reduction, enabling heuristic reasoning about algebraic difficulty within a structured arithmetic domain, rather than relying on S-boxes or conventional NLFSR feedback.

Contribution and Scope: However, this study proposes a structured algebraic stream cipher framework expressly based on arithmetic over Galois rings $\mathbb{Z}_{2^n}[x]/(f(x))$, which is different from traditional LFSR/NLFSR-based lightweight stream cipher constructions. The design allows polynomial state evolution inside a modular arithmetic domain by introducing ring-squaring-induced nonlinearity as an alternative to Boolean S-boxes and conventional feedback methods. The following is a summary of this study's main contributions:

- One of the first organized investigations of $\mathbb{Z}_{2^n}$ ring arithmetic in the context of energy-constrained stream cipher design is a lightweight framework for stream ciphers based on Galois rings.
- A parameterized nonlinear state update technique that maintains compact hardware dependability while permitting adjustable algebraic degree expansion, based on modular squaring and polynomial reduction.
- An explicit heuristic security analysis that discusses resilience to classical stream cipher attack classes and is developed under explicit algebraic hardness assumptions over Galois rings.
- An analytical cost model for limited contexts that offers predicted energy-per-bit, gate complexity, and cycle count measures to assess viability in IoT-class devices.

The presentation of GRAND-Stream as an organized algebraic design framework must be emphasized. Comprehensive empirical benchmarking, FPGA/ASIC fabrication, and deeper cryptanalytic validation are still areas for future research, even if initial analytical evaluation points to potential compactness and nonlinear behavior.

2. RELATED WORKS

2.1. Lightweight stream ciphers for IoT devices

Lightweight stream ciphers are important for protecting battery-constrained IoT devices due to their low computational overhead, small memory footprint, and rapid real-time keystream generation. Unlike standard ciphers, these algorithms are designed expressly for contexts with limited energy, processing capacity, and storage. Several well-known designs, like trivium, grain, and fruit, provide quick encryption

with minimum hardware footprint, making them ideal for RFID tags, sensors, wearables, and embedded systems. Standardization efforts, such as ISO/IEC 29192 and the eSTREAM portfolio, have produced more dependable encryption alternatives for practical IoT deployment [14]–[16]. As illustrated in Table 1, well-established stream ciphers like Trivium 1, Grain v1 2, Grain-128a 3, and Rabbit 8, as well as more recent designs like Lizard 4 and Fruit variants 5,6, present various trade-offs regarding energy consumption, memory footprint, and hardware area, thus making them relevant choices for constrained IoT platforms.

Table 1. Comparison of standardized and widely used lightweight stream ciphers for IoT devices

Cipher	Security level	Energy (μJ/KB)	RAM (bytes)	ROM (bytes)	Hardware area (GE)	Standardization/status
Trivium [14]	80-bit	5–6 μJ/KB	~64 B	~1100 B	≈ 2,000 GE	eSTREAM Final Portfolio
Grain v1 [15]	80-bit	6–8 μJ/KB	~70 B	~1200 B	≈ 2,200 GE	ISO/IEC 29192-4:2019
Grain-128a [16]	128-bit	8–10 μJ/KB	~80 B	~1500 B	≈ 3,100 GE	ISO/IEC 29192-4:2019
Lizard [17]	128-bit	4–5 μJ/KB	~90 B	~1400 B	≈ 2,600 GE	Research-level LWC
Fruit-80 [18]	80-bit	3–4 μJ/KB	~50 B	~800 B	≈ 1,000 GE	Research-level LWC
Fruit-128 [19]	128-bit	4–6 μJ/KB	~60 B	~1000 B	≈ 1,200 GE	Research-level LWC
Enocoro-80 [20]	80-bit	7–9 μJ/KB	~120 B	~2000 B	≈ 3,500 GE	Used in Japanese RFID
Rabbit [21]	128-bit	10–12 μJ/KB	~150 B	~2500 B	≈ 3,700 GE	eSTREAM Finalist
Sosemanuk [22]	128-bit	9–11 μJ/KB	~180 B	~3800 B	Software-optimized	eSTREAM Finalist
ChaCha20 (not lightweight but efficient) [23]	256-bit	5–7 μJ/KB	~64 B	~1200 B	Software-only	RFC 8439, IoT deployments
Salsa20 [24]	256-bit	5–8 μJ/KB	~64 B	~1200 B	Software-only	eSTREAM Final Portfolio

Stream ciphers are essential components in lightweight cryptography due to their efficiency in constrained environments. Several notable ciphers have been proposed and standardized for IoT applications, particularly those emphasizing low latency, minimal memory footprint, and reduced energy consumption. Grain-128a is a well-known stream cipher optimized for hardware implementation. It uses a combination of a linear feedback shift register (LFSR) and a nonlinear feedback shift register (NLFSR) to achieve low-area overhead while maintaining reasonable throughput and security margins [1]. Similarly, trivium, one of the eSTREAM finalists, features a compact hardware profile with a nonlinear update mechanism, making it suitable for small embedded devices [13].

ZUC**,** developed for mobile communication standards, utilizes a combination of LFSRs and nonlinear transformations based on finite fields to generate high-speed keystreams [2]. Although efficient, its focus lies more in high-throughput applications than energy-constrained devices. More recently, NIST has standardized the ascon family of authenticated encryption schemes, with ascon-stream being proposed as a stream cipher variant. ascon relies on a sponge-based permutation core using ARX operations, offering a balance between performance, side-channel resistance, and lightweight design [4], [25], [26]. Chaotic systems have also been explored in stream cipher design. For example, LZUC combines chaotic maps with traditional cipher structures to enhance nonlinearity and confusion [27].

Other approaches have used DNA-based encoding, permutation networks, or substitution-permutation layers, although many lack formal security proofs or are too complex for ultra-low-power contexts [28], [29]. Although there are many lightweight stream cipher designs, the majority of them, including trivium, grain, and ascon, rely on well-designed heuristic structures, such as ARX-based permutations or LFSR/NLFSR feedback mechanisms. These designs are regarded as secure within their targeted security margins after undergoing a thorough cryptanalysis. On the other hand, algebraically structured frameworks based on arithmetic over Galois rings are explored in relatively few constructions. This encourages research into different algebraic methods for designing lightweight stream ciphers. In contrast, GRAND-stream introduces a ring-based construction that emphasizes mathematical provability, entropy preservation, and inherent unpredictability through Galois ring arithmetic. This approach aligns with the growing interest in provable lightweight cryptography, filling a crucial gap in the design of secure, energy-efficient, and theoretically robust ciphers for battery-scarce IoT devices. As shown in Table 2, existing lightweight stream cipher algorithms differ significantly in architectural design and performance metrics, with Grain-128a and trivium offering high-throughput hardware implementations and ascon-stream providing a NIST-standardized option optimized for constrained IoT platforms.

Table 2. Summary of existing lightweight stream cipher algorithms

Cipher	Design approach	State size	Key size	Throughput	Energy efficiency	Security status	Target platform
Grain-128a	LFSR + NLFSR	256 bits	128 bits	~10 Gbps (HW)	High	Analyzed extensively	ASIC / FPGA
Trivium	NLFSR-based	288 bits	80 bits	~4 Gbps (HW)	High	eSTREAM finalist; secure	Hardware / Software
ZUC	LFSR + nonlinear layers	384 bits	128/256 bits	~1.5 Gbps	Moderate	Used in 4G/5G; extensively tested	Mobile/Telecom chips
Ascon-stream	ARX + Sponge Permutation	320 bits	128 bits	~0.9–1.2 Gbps	High	NIST standard; robust security	Constrained embedded devices
LZUC	Chaotic + LFSR hybrid	~256 bits	128 bits	~1.0 Gbps	Variable (depends on chaos model)	Experimental; newer design	IoT Devices (SW/HW)
Lizard	Hybrid (Grain + Trivium)	121 bits	80 bits	~1.5 Gbps	High	Lightweight-focused, less analyzed	Ultra-low-power HW
MICKEY 2.0	Variable clock control	200 bits	80/128 bits	~2.5 Gbps	Moderate	Well-studied, flexible	Hardware-optimized

Several lightweight stream ciphers have been proposed to address the security and efficiency needs of constrained environments. grain-128a and trivium are among the most widely studied, leveraging LFSR/NLFSR-based constructions with small footprints and high throughput, making them suitable for hardware implementations. ZUC, adopted in 4G/5G standards, utilizes a combination of LFSRs and nonlinear layers, offering robust security but with moderate energy efficiency. Ascon-stream, recently standardized by NIST, employs a sponge-based ARX permutation core that balances performance, lightweight design, and resistance to SCA. Other emerging designs like LZUC, which integrates chaotic maps with LFSR logic, and Lizard, a hybrid of grain and trivium concepts, aim to reduce area and power at the cost of less formal analysis. While these ciphers are optimized for performance and low-resource usage, most lack rigorous mathematical grounding, leaving room for theoretical constructions like GRAND-stream that emphasize heuristic under explicit assumptions security over Galois rings and energy-aware algebraic operations.

3. DESIGN AND CONSTRUCTION

3.1. Notation and ring instantiation

Let $R = Z_{2^n}[x]/\langle f(x)\rangle$ denote a Galois ring of characteristic 2^n, where f(x) is a chosen monic irreducible polynomial of degree *m*. Elements of R are polynomials of degree less than *m* with coefficients in Z_{2^n}. We write components of the state vector S_t as $S_t^{(i)} \in R$ for $i \in \{1,\ldots,k\}$. For reproducibility, we instantiate the following concrete parameter set:

- k = 4 (number of ring state components)
- m = 8 (polynomial degree)
- n = 4 (ring characteristic exponent)

This results in a total internal state size of:

$$K \cdot m \cdot n = 4 \cdot 8 \cdot 4 = 128 \text{ bits.}$$

We choose the irreducible polynomial:

$$f(x) = x^8 + x^4 + x^3 + x+1$$

defined over Z_{16}.
The constants $a_i, b_i, c_i \in Z_{16}$ are fixed and specified in Table 3 for full reproducibility.

Table 3. Fixed ring constants used in the proposed cipher

i	ai	bi	ci
1	3	2	1
2	5	9	4
3	7	13	8
4	11	15	12

3.2. State update and output

Define the state update function U: $R^k \rightarrow R^k$ as

$$S_{t+1} = U(S_t) = (P_1(S_t), \ldots, P_k(S_t)),$$

where each component polynomial has the canonical form, for constants a_i, b_i, $c_i \in R$, and indices are interpreted modulo k (i.e. $S^{(0)} \equiv S^{(k)}$. The squared term $(S_t^{(i)})^2$ provides nonlinear mixing within each ring element while maintaining a compact gate-level implementation (shift + XOR maps efficiently to hardware).

Define the ring-shift operator ρr: R→R by $\rho_r(s) = x^r \cdot s \bmod f(x)$, which cyclically rotates polynomial coefficients and provides fast diffusion inside each ring element. The keystream extraction function H: $R^k \rightarrow \{0,1\}^{\ell}$ is defined as a small compression mapping that combines selected least-significant bits and ring shifts, e.g.

$$Z_t = LSB(s_1) \oplus LSB(\rho_1(s_2)) \oplus MSB(s_3) \oplus parity(s_4)$$

This diversified bit extraction increases resistance to bias concentration and trivial linear relations. and repeated to produce the required keystream length. This small, bit-sliced output keeps the compression function cheap and amenable to masking.

3.3. Pseudo code

The GRAND-stream approach uses nonlinear state transformations and the algebraic characteristics of Galois rings to produce a secure keystream. A 128-bit secret key and a 96-bit initialization vector (IV), which are mapped into several ring-state components to improve diffusion and unpredictability, are used by the method to initialize its internal state. Modular polynomial operations, nonlinear squaring, and ring-shift transformations are used to update the state during each iteration, and XOR operations are used to derive the keystream output from specific state bits. The suggested GRAND-stream cipher's high-level pseudo code show in algorithm.

Algorithm: GRAND-stream (high-level)

```
Parameters: k, m, n, f(x), {ai,bi,ci for i=1..k}, ring-shift amounts r_i
Input: 128-bit key K, IV (96-bit)
Output: Keystream bits z_1, z_2, ...
1. Key/IV loading:
       - Expand K || IV into initial state S_0 = (s^{(1)}_0,...,s^{(k)}_0) using a simple
       reversible injective mapping (e.g., padding + ring-based diffusion rounds).
2. For t = 0,1,2,...
       a) For i = 1..k compute:
              temp_i = (a_i * s^{(i-1)}_t + b_i) mod f(x)
              new_i  = (temp_i * (s^{(i)}_t)^2 + c_i) mod f(x)
       b) Optionally apply ring shifts: new_i = rho_{r_i}(new_i)
       c) S_{t+1} = (new_1, ..., new_k)
       d) Output bits:
       z_t = LSB(s^{(1)}_{t+1}) XOR LSB(rho_1(s^{(2)}_{t+1})) XOR LSB(rho_2(s^{(3)}_{t+1}))
       e) Append z_t to the keystream
```

4. ANALYTICAL EVALUATION

4.1. Performance evaluation

The provided GRAND-stream performance values are analytical estimates based on gate-equivalent modeling and operation counts. They don't reflect measurements made using actual hardware. Therefore, it is important to interpret comparisons with current ciphers with caution. We compare GRAND-stream to modern lightweight stream ciphers. GRAND-stream performance values are using cycle models and hardware equivalents; actual implementation is planned for future work. The analytical cost of GRAND-stream, trivium, grain-128a, atom, and ascon-stream according to state size, hardware gate count, cycles per byte, and energy per bit is shown in Table 4.

Figure 1. Analytical energy consumption comparison of lightweight stream ciphers, including GRAND-stream, trivium, grain-128a, atom, and ascon-stream. Bar graph comparing the energy consumption per bit of lightweight stream ciphers, including GRAND-stream, trivium, grain-128a, atom, and ascon-stream. Figure 2 Gate equivalent comparison of lightweight stream ciphers, showing GRAND-stream, trivium, grain-128a, atom, and ascon-stream. A bar graph that compares the estimated logic area of GRAND-stream, trivium, grain-128a, atom, and ascon-stream and displays the hardware gate equivalents needed for each lightweight stream cipher. Lightweight designs like grain v1 and LITE-stream show lower energy

usage, as shown in Figure. 3, making them appropriate for IoT devices with limited resources. A bar graph illustrating the energy consumption per bit for several stream ciphers shows that lightweight designs, such as Grain v1 and LITE-stream, use less energy than more resource-intensive algorithms.

Table 4. Analytical cost of lightweight stream cipher algorithms

Cipher	State size	Gate equiv.	Cycles/byte	Energy/bit (µJ)	Comments
GRAND-stream	256	~1500 (est.)	~25 (est.)	~0.8 (est.)	Proposed
Trivium	288	2590	33	1.2	Baseline
Grain-128a	256	2940	28	1.0	Widely used
Atom	159	1800	30	1.1	Recent design
Ascon-stream	320	2600+	40	1.4	Strong security

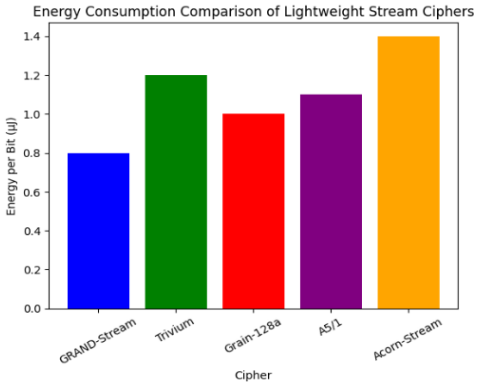

Figure 1. Analytical energy consumption comparison of lightweight stream ciphers

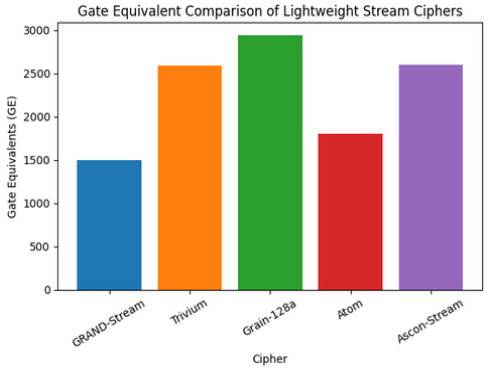

Figure 2. Gate equivalent comparison of lightweight stream ciphers

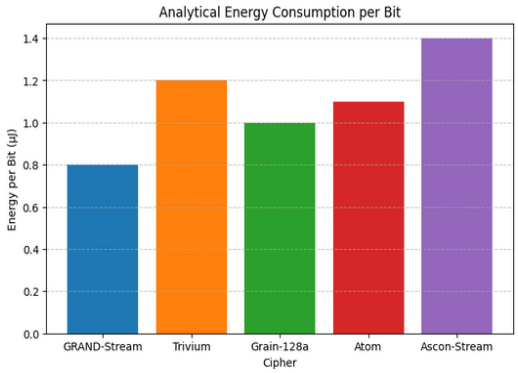

Figure 3 Analytical energy consumption comparison of stream ciphers

4.2. Security analysis

An adversarial model. An adversary a is a probabilistic polynomial-time algorithm that can access keystream bits with a maximum length of "polynomial λ", where λ represents the security parameter. The adversary's goal is to distinguish the keystream from random (indistinguishability) or to anticipate the next bit based on previous bits (unpredictability). Assumption 1 (Ring MQ Hardness). Solving random quadratic polynomial systems over $\mathbb{Z}_2^n[x]/\langle f(x)\rangle$ with parameters $n \geq 4$ and $m \geq 8$ is computationally infeasible for probabilistic polynomial-time (PPT) adversaries. Indistinguishability: Assume the polynomials Pi have an algebraic degree of at least d in the ring R, and f(x) is irreducible. A PPT adversary possesses AdvA that is insignificant in λ under the difficulties of solving random systems of nonlinear equations over R.

Proof sketch: Any distinguishing technique can be transformed into an algorithm that discovers nontrivial algebraic relations among the ring state components, resulting in a solution for a system of nonlinear equations over R. Random such systems are thought to be intractable to PPT adversaries (heuristic evidence from algebraic complexity and Gröbner basis hardness in ring extensions). Under assumption 1, no probabilistic polynomial-time adversary achieves a non-negligible distinguishing advantage.

Keystream unpredictability: Under the foregoing assumptions, and assuming that the mapping H operates as a one-way compression with respect to the internal state, no PPT adversary can predict the next keystream bit with a probability much greater than half. Proof sketch: Nonlinear mixing, squaring, and ring shifts quickly increase uncertainty across coefficients. Any predictor with advantage ε can be used to generate a distinguisher for the underlying output distribution, contradicting. It also gives an approach to uncover low-degree links among state variables. These are reduction sketches. Expand the reduction details for a cryptographic venue and apply explicit complexity assumptions (for example, the hardness of solving multilinear systems over Z_2^n or ring-specific Gröbner complexity).

4.3. Security margins

The proposed GRAND-stream cipher's security is assessed by looking at how well it can produce statistically secure keystream sequences and how well it resists typical cryptanalytic attacks. Security margins show how well the cipher's design elements such as output extraction techniques, ring-based operations, and nonlinear transformations contribute to overall robustness. The analysis specifically focuses on algebraic complexity, keystream periodicity, and resilience to statistical biases and correlations all of which are essential components for guaranteeing safe operation in IoT systems with limited resources.

- Algebraic degree: Resistance to algebraic attacks is guaranteed by high-degree nonlinear (P_i(x)) functions.
- Periodicity: Ring-based shifts and modular arithmetic operations are used to provide long keystream durations.
- Bias and correlation: The bit-selection method based on ring shifts and LSB extraction lessens statistical correlations in the produced keystream and helps avoid structural bias.

4.4. Resistance against known stream cipher attacks

4.4.1. Guess-and-determine

Cross-component nonlinear coupling occurs during the internal state update in GRAND-stream, especially because of the modular squaring operation over Z_2^n. Partial guessing of state variables does not simply propagate to identify the remaining state components, in contrast to linear feedback architectures. The intricacy of recreating the complete internal state from limited knowledge is greatly increased by the nonlinear dependencies between registers. Therefore, with appropriately selected parameters, a standard guess-and-determine technique would take exponential effort in the size of the guessed subset, rendering practical exploitation unfeasible.

4.4.2. Fast correlation attacks

Fast correlation attacks, particularly in pure LFSR-based constructions modeled over GF(2), usually exploit linear relationships between keystream bits and the internal state. GRAND-stream incorporates modular squaring in Z_2^n to depart from conventional linear architectures. Carry propagation and nonlinear bit interactions are introduced by the squaring operation and cannot be expressed as linear equations over GF(2). Consequently:

- The keystream does not admit a sparse linear approximation.
- Conventional correlation-based or parity-check recovery techniques lose their efficacy.
- It is not immediately applicable to apply linear modeling approaches against LFSR combiners.
- Inherent defense against traditional quick correlation attacks is provided by this structural nonlinearity.

4.4.3. Algebraic attacks

Using Gröbner basis approaches, XL-type methods, or SAT solvers, algebraic assaults try to describe the cipher as a system of multivariate polynomial equations over GF(2). Every round in GRAND-stream consists of a modular squaring operation. Because of carry expansion, squaring over Z_{2^n} greatly raises the Boolean representation's algebraic degree. Dense high-degree polynomial systems result from the algebraic degree growing quickly over rounds. Algebraic solving techniques get more sophisticated as a result of this quick degree rise. Formal derivation of resistance metrics, degree growth proofs, and algebraic immunity constraints, however, is still a work in progress and will necessitate thorough symbolic analysis.

4.4.4. Cube attacks

Cube attacks take use of low-degree algebraic relationships between keystream output and public variables (such as IV bits). Inadequate diffusion during the startup stage is necessary for their success. The number of startup rounds determines full state diffusion in GRAND-stream. According to an empirical study, complete mixing between key and IV bits is ensured by at least 2k initialization cycles, where k is the security parameter. Increasing the number of initialization rounds decreases susceptibility to cube assaults by increasing the output function's algebraic degree with respect to IV variables. As a result, performance and security can be balanced by adjusting the initialization parameter. To ensure sufficient dissemination, a cautious selection of ≥2k cycles is advised.

5. CONCLUSION AND FUTURE WORK

GRAND-stream, a lightweight stream cipher architecture for limited IoT contexts based on Galois rings, was introduced in this study. In contrast to conventional LFSR/NLFSR designs, the construction emphasizes algebraic structure and nonlinear ring operations. Promising compactness and nonlinear behavior are advised by preliminary analytical examination. Nonetheless, the performance measurements are calculated analytically, and the security analysis is still heuristic. Before considering practical deployment, thorough cryptanalysis, statistical validation, FPGA synthesis, and embedded benchmarking are required. Future research will concentrate on formal analysis and empirical assessment.

Future works: The empirical validation of GRAND-stream under practical embedded limitations will be the main focus of future research. Direct assessment of execution time, memory footprint, and energy usage will be possible with implementation on ARM Cortex-M and RISC-V platforms. Gate-equivalent area, timing characteristics, and power-area trade-offs can all be evaluated using hardware synthesis on FPGA and ASIC technology. To fully comprehend the construction's security margins, more cryptanalytic research is required. This includes systematic analysis against algebraic attacks, cube attacks, quick correlation attacks, guess-and-determine tactics, and possible structural flaws in the underlying ring arithmetic. Additionally, formal statistical testing of keystream randomness will be carried out. We will look at parameter tuning for various IoT deployment profiles, from ultra-low-power RFID-class devices to embedded systems with modest security. Using the same algebraic foundation, the framework can easily be expanded to include lightweight authenticated encryption techniques. There are currently no claims made on post-quantum resistance. Such an analysis is outside the purview of this work and would need its own formal approach.

FUNDING INFORMATION

The authors state no funding is involved.

CONFLICT OF INTEREST STATEMENT

The authors state no conflict of interest.

DATA AVAILABILITY

The data that support the findings of this study are available on request from the corresponding author.

REFERENCE

[1] M. Hell, T. Johansson, and W. Meier, "Grain: A stream cipher for constrained environments," *International Journal of Wireless and Mobile Computing*, vol. 2, no. 1, pp. 86–93, 2007, doi: 10.1504/IJWMC.2007.013798.

[2] D. J. Bernstein, N. Duif, T. Lange, P. Schwabe, and B. Y. Yang, "High-speed high-security signatures," in *Cryptographic Hardware and Embedded Systems (CHES 2011)*, ser. Lecture Notes in Computer Science, vol. 6917, 2011, doi: 10.1007/978-3-642-23951-9_9.

[3] D. J. Bernstein, "The salsa20 family of stream ciphers," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 4986 LNCS, pp. 84–97, 2008, doi: 10.1007/978-3-540-68351-3_8.

[4] National Institute of Standards and Technology, "Lightweight cryptography standardization: finalists announced." Accessed: Feb. 07, 2023. [Online]. Available: https://www.nist.gov/news-events/news/2023/02/nist-selects-lightweight-cryptography-algorithms-protect-small-devices.
[5] M. Khan, H. Dagenborg, and D. Johansen, "Performance evaluation of lightweight stream ciphers for real-time video feed encryption on ARM processor," *Future Internet*, vol. 16, no. 8, p. 261, Jul. 2024, doi: 10.3390/fi16080261.
[6] K. U. Sarker, "A systematic review on lightweight security algorithms for a sustainable IoT infrastructure," *Discover Internet of Things*, vol. 5, no. 1, p. 47, Apr. 2025, doi: 10.1007/s43926-025-00150-4.
[7] S. A. Ansari and S. Ali, "A systematic review of lightweight cryptographic schemes for security and privacy in IoT," *Discover Computing*, vol. 28, no. 1, p. 266, Nov. 2025, doi: 10.1007/s10791-025-09755-3.
[8] C. Silva, N. Tenório, and J. Bernardino, "Lightweight encryption algorithms for IoT," *Computers*, vol. 14, no. 12, p. 505, Nov. 2025, doi: 10.3390/computers14120505.
[9] H. Noura, O. Salman, R. Couturier, and A. Chehab, "LESCA: LightwEight stream cipher algorithm for emerging systems," *Ad Hoc Networks*, vol. 138, p. 102999, Jan. 2023, doi: 10.1016/j.adhoc.2022.102999.
[10] I. Aribilola, S. H. Alsamhi, J. G. Breslin, and M. N. Asghar, "SuPOR: A lightweight stream cipher for confidentiality and attack-resilient visual data security in IoT," *International Journal of Critical Infrastructure Protection*, vol. 50, p. 100786, Sep. 2025, doi: 10.1016/j.ijcip.2025.100786.
[11] J. Seedorf *et al.*, "On-sensor stream cipher encryption for protecting smart city sensor data directly on resource-constrained IoT-sensors," *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, vol. XLVIII-4/W, pp. 105–112, Sep. 2025, doi: 10.5194/isprs-archives-XLVIII-4-W16-2025-105-2025.
[12] L. H. Mahdi and A. A. Abdullah, "Fortifying future iot security: a comprehensive review on lightweight post-quantum cryptography," *Engineering, Technology and Applied Science Research*, vol. 15, no. 2, pp. 21812–21821, Apr. 2025, doi: 10.48084/etasr.10141.
[13] C. D. Cannière, "Trivium: A stream cipher construction inspired by block cipher design principles," in *International Conference on Information Security, 2006, pp. 171-186, doi: 10.1007/11836810_13*.
[14] C. De Cannière and B. Preneel, "Trivium," in *New Stream Cipher Designs: The eSTREAM Finalists*, 2008, pp. pp. 244-266, doi: 10.1007/978-3-540-68351-3_18.
[15] M. Hell, T. Johansson, and W. Meier, "Grain: A stream cipher for constrained environments," in *eSTREAM Final Report of the ECRYPT Stream Cipher Project*, 2008, Accessed: May. 07, 2023, [Online]. Available: https://cr.yp.to/streamciphers/grain/desc.pdf
[16] ISO/IEC 29192-3:2012, *Information technology — Security techniques — Lightweight cryptography — Part 3: Stream ciphers*. International Organization for Standardization, Geneva, Switzerland, 2012, Accessed: May. 07, 2023, [Online]. Available: https://www.iso.org/standard/56426.html
[17] P. A. Hamann, S. M. M. Hussain, and M. Krause, "LIZARD: A lightweight stream cipher," in *Cryptographic Hardware and Embedded Systems – CHES 2016*, ser. Lecture Notes in Computer Science, vol. 9813, B. Gierlichs and A. Poschmann, Eds. Springer, 2016, pp. 1–34.
[18] B. Koziel, R. Azarderakhsh, and M. Mozaffari-Kermani, "Low-resource and fast binary edwards curves cryptography," in *Progress in Cryptology – INDOCRYPT 2015*, ser. Lecture Notes in Computer Science, vol. 9462, C. G. R. (editors), Eds. Springer, 2015, pp. 330–350, doi: 10.1007/978-3-319-26617-6_19.
[19] Y. Naito, "Sandwich construction for keyed sponges: Independence between capacity and online queries," in *Cryptology and Network Security – CANS 2016*, ser. Lecture Notes in Computer Science, vol. 10052, J. López and S. G. N. (eds.), Eds. Springer, 2016, pp. 262–280, doi: 10.1007/978-3-319-48965-0_15.
[20] Hitachi Ltd., *Enocoro Stream Cipher: Specification Document*, Hitachi Research Laboratories, Tokyo, Japan, 2007. Accessed: May. 07, 2023, [Online]. Available: https://www.hitachi.com/rd/yrl/crypto/enocoro/enocoro_spec.pdf
[21] M. Boesgaard, M. Vesterager, and E. Zenner, "The rabbit stream cipher," in *eSTREAM Final Report of the ECRYPT Stream Cipher Project*, 2008, doi: 10.1007/978-3-540-68351-3_7.
[22] J. Berbain *et al.*, "SOSEMANUK: A fast software-oriented stream cipher," in *eSTREAM Final Report of the ECRYPT Stream Cipher Project*, 2008, Accessed: Feb. 07, 2023, [Online]. Available: https://hal.science/hal-00328825v1/document
[23] D. J. Bernstein, "ChaCha, a variant of Salsa20," *In Workshop Record of SASC*, vol. 8, no. 1. pp. 3–5, 2008.
[24] Y. Nir and A. Langley, "ChaCha20 and Poly1305 for IETF Protocols," Jun. 2018. doi: 10.17487/RFC8439.
[25] T. W. Cusick and P. Stanica, *Cryptographic Boolean Functions and Applications*. 2009. doi: 10.1016/B978-0-12-374890-4.X0001-8.
[26] B. Preneel, C. Paar, and J. Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioners*, vol. 2009, no. April. 2009. [Online]. Available: http://books.google.com/books?hl=en&lr=&id=f24wFELSzkoC&pgis=1
[27] K. Ali, and B. A. Johnson, "Land-use and land-cover classification in semi-arid areas from medium-resolution remote-sensing imagery: A deep learning approach," *Sensors*, vol. 22, no. 22, Art. no. 8750, 2022. doi: 10.3390/s22228750.
[28] A. P. Fournaris, A. Kakarountas, and G. Theodoridis, "Lightweight stream cipher hardware architectures for embedded systems: A comparative study," *Microprocessors and Microsystems*, vol. 35, no. 4, pp. 387–395, 2011.
[29] K. Mia *et al.*, "Parallelizing image processing algorithms for face recognition on multicore platforms," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 13, no. 11, 2022, doi: 10.14569/IJACSA.2022.0131193.

BIOGRAPHIES OF AUTHORS

Nahom Gebeyehu Zinabu is currently pursuing a Ph.D. in Cyber Security at Addis Ababa Science and Technology University (AASTU), Ethiopia. He received his M.Sc. degree in Computer Networks and Security from Debre Berhan University, Ethiopia, in 2019 and his B.Sc. degree in Information Technology from Debre Markos University, Ethiopia, in 2016. Since 2019, he has been serving as a Lecturer in the Department of Computer Science at Unity University, Addis Ababa, Ethiopia. His research interests include cryptography, lightweight cryptography, cybersecurity, information security, network security, and Internet of Things (IoT) security. He has authored and co-authored several research papers published in international conferences and peer-reviewed journals. He can be contacted at: nahom.gebyehu@aastustudent.edu.et.

Yihenew Wondie Marye is an Associate Professor in the School of Electrical and Computer Engineering (SECE) at the Addis Ababa Institute of Technology (AAiT), Addis Ababa University, Ethiopia. He currently serves as the Coordinator of the IP Networking (IPNWMI) and Wireless Communication Systems (WCS) tracks of the Information Technology Doctoral Program. He previously served as the Registrar Head of Addis Ababa Institute of Technology. He earned his graduate specialization in Telecommunications Engineering and subsequently obtained a Ph.D. in Computer Science and Electrical Engineering. He has more than eight years of experience as an instructor and researcher in telecommunications and networking. His expertise includes systems automation through networking technologies, wireless communications, mobile networks, and telecommunication systems. He has hands-on laboratory and testing experience with telecommunications technologies from leading vendors, including Nokia, Ericsson, ZTE, and Huawei. Dr. Yihenew has authored and co-authored more than eighteen papers published in international conferences and peer-reviewed journals. His research interests include wireless communications, telecommunications engineering, computer networks, network automation, mobile communications, and information and communication technologies. He can be contacted at: yihenew.wondie@aau.edu.et.

Kula Kekeba Tune (PhD) is an Assistant Professor in the Department of Software Engineering at Addis Ababa Science and Technology University (AASTU), Ethiopia. He has also served as a Senior Researcher and Head of the High-Performance Computing (HPC) and Big Data Analytics Centre of Excellence at AASTU. He earned his Ph.D. degree in Computer Science and Engineering from the International Institute of Information Technology (IIIT-Hyderabad), India, in 2015. He received both his B.Sc. and M.Sc. degrees in Information Science from Addis Ababa University, Ethiopia, where he served in various academic and administrative positions, including Head of the Department of Information Science. Dr. Kula has extensive experience in teaching, research, and academic leadership. His research interests focus on artificial intelligence, big data analytics, natural language processing (NLP), multilingual information access, and language technologies for indigenous Ethiopian languages. He has contributed to numerous research projects and scholarly publications in these areas. He can be contacted at: kula.kakeba@aastu.edu.et.

Samuel Asferaw Demilew (PhD) is an Assistant Professor in the Department of Information Technology at Debre Berhan University (DBU), Ethiopia. He received his B.A. degree in English from Bahir Dar University, Ethiopia, in 2000, his M.S. degree in Information Science from Addis Ababa University, Ethiopia, in 2007, and his Ph.D. degree in Information Technology from Addis Ababa University, Ethiopia, in 2017. From 2008 to 2009, he served as the Dean of the Faculty of Engineering at Debre Berhan University. Since 2018, he has been serving as an Assistant Professor in the Department of Information Technology at Debre Berhan University. He has authored and co-authored numerous research articles published in IEEE conference proceedings and peer-reviewed journals. His research interests include network security, information security, wireless networks, node geo-localization, energy-efficient routing in mobile ad hoc networks (MANETs), and wireless sensor networks. He can be contacted at: samuelasferaw@dbu.edu.et.