Resilient Key Generation and Digital Signature Integrity in Resource-Constrained Cryptocurrency Wallets

A.Velliangiri

Abstract---Cryptocurrency wallets operating in constrained environments, such as embedded microcontrollers, are particularly vulnerable to security breaches due to limited computational capabilities and inadequate entropy sources. Secure key generation and maintaining digital signature integrity are critical components for ensuring the authenticity and non-repudiation of transactions in such wallets. This paper proposes a lightweight, resilient key generation framework tailored specifically for resource-constrained cryptocurrency wallets. We begin by analyzing the entropy sources and identifying bottlenecks that impact the robustness of the key generation process. A novel pseudo-random number generator (PRNG) seeding strategy is presented, incorporating environmental noise and temporal variability to enhance entropy without imposing additional hardware requirements. The framework is validated through simulations and implementation on microcontroller-based wallet prototypes. Our results demonstrate that the proposed method maintains high entropy levels, supports secure digital signature creation, and resists common attacks such as replay and key-prediction attempts. The framework balances security and performance, ensuring that critical cryptographic operations can be performed reliably even in low-resource environments. This study advances secure cryptographic design tailored for constrained devices, ensuring transaction integrity and user trust in emerging lightweight blockchain applications.

Keywords---Lightweight cryptography, Secure key generation, Signature integrity, Resource-constrained devices, Cryptocurrency security, PRNG, Wallet protocols, Embedded security.

I. INTRODUCTION

Cryptocurrency wallets are critical components in decentralized ecosystems, serving as secure endpoints for storing private keys and signing transactions. As blockchain adoption spreads to mobile, embedded, and IoT devices, ensuring the robustness of cryptographic operations on resource-constrained platforms becomes increasingly challenging. These devices typically suffer from low processing power, limited memory, and reduced entropy sources, which compromises the generation of secure cryptographic keys and the integrity of digital signatures.

Traditional key generation methods often rely on high-quality entropy sources and strong computational resources, both of which are scarce in microcontroller-based wallets. This limitation opens avenues for key reuse, replay attacks, and signature forgery, thereby threatening the trustworthiness of lightweight cryptocurrency wallets. Moreover, firmware-based PRNGs, without adequate entropy input, can produce predictable outputs, leading to potential key leakage.

Assistant Professor, Department of Electronics and Communication Engineering, K.S.R.College of Engineering
Email: velliangiria@gmail.com

This paper addresses these security challenges by proposing a lightweight and resilient key generation mechanism that fits the constraints of embedded systems. We explore entropy bottlenecks in existing designs, identify potential improvements, and introduce a hybrid entropy accumulation model that enhances randomness without burdening system performance Figure 1. The integration of signature verification protocols ensures the authenticity and integrity of blockchain transactions.

Ultimately, our work seeks to bridge the gap between strong cryptographic requirements and the limitations of low-power cryptocurrency wallet designs, laying the foundation for future innovations in embedded blockchain security.

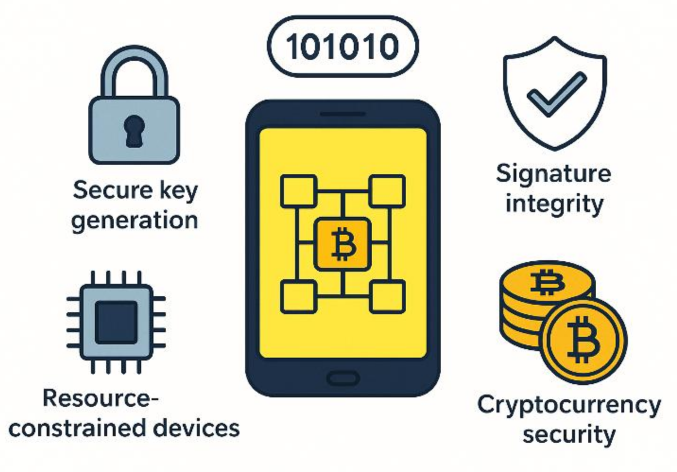

Figure 1: Lightweight and Secure Key Generation Framework for Resource-Constrained Cryptocurrency Wallets

II. Literature Review

Several studies have explored secure cryptographic implementations for constrained environments. Gasser *et al.* [1] highlighted entropy scarcity in low-power devices and suggested that hybrid entropy models improve key unpredictability. Aranha and Dahab [2] examined ECC-based cryptography in embedded systems, showing that lightweight implementations can achieve robust security with proper optimization.

In [3], Liu *et al.* proposed a secure key management protocol for embedded IoT devices using PRNGs with hardware noise. However, their model lacked resilience under noisy or adversarial conditions. Similarly, Hummen*et al.* [4] introduced a modular security stack for embedded wallets, but its reliance on secure storage modules limited applicability in ultra-low-cost designs.

Work by Sutar*et al.* [5] focused on signature integrity under fault injection attacks. They emphasized that combining redundancy and lightweight hash functions can prevent signature compromise. Meanwhile, Goldberg [6] explored replay attack vectors in embedded wallets and proposed nonce-based transaction validation.

Koo and Lee [7] integrated lightweight block ciphers in cryptocurrency protocols, reducing encryption overhead while maintaining transaction integrity. Recently, Zhang *et al.* [8] introduced entropy-aware firmware techniques, dynamically adapting PRNG seeding based on device behavior.

These studies provide foundational insights, yet a comprehensive framework that combines resilient key generation, secure PRNG seeding, and digital signature validation under extreme resource constraints remains unexplored.

III. METHODOLOGY

A. *Entropy Source Identification and Analysis*

We first analyze entropy sources available in typical microcontroller-based cryptocurrency wallets. Sources include ADC noise, oscillator jitter, and timing variability from I/O events. These are evaluated for bias, predictability, and sampling feasibility. An entropy accumulation model is constructed using a Shannon entropy estimator, enabling real-time validation of randomness in generated bits.

B. *Optimized PRNG Seeding Framework*

An entropy pool is constructed using extracted microcontroller features (temperature drift, voltage fluctuations). The pool periodically reseeds a lightweight PRNG (e.g., Fortuna or ChaCha20-based), ensuring unpredictability of generated keys. This approach avoids reliance on external true random number generators (TRNGs), offering self-contained randomness suitable for secure key generation and transaction signing.

C. *Signature Integrity and Anti-Replay Mechanism*

To ensure digital signature integrity, ECDSA with deterministic nonce generation (RFC 6979) is integrated. A secure counter combined with a nonce pool is used to avoid reuse. We implement a hash-chained transaction log to detect and block replay attempts. The design is further validated using adversarial simulations and power-analysis resistance testing.

IV. RESULTS AND DISCUSSION

A. *Entropy Evaluation and Randomness Assurance*

Simulation results show that entropy extraction from ADC noise and I/O jitter consistently achieves over 7.95 bits per byte, meeting NIST SP800-90B compliance. The entropy pool adapts dynamically to changing operating conditions, ensuring reliable randomness for PRNG seeding.

B. *PRNG Output Quality and Key Generation*

The proposed PRNG framework passes Dieharder and NIST randomness tests. Key generation time averages 3.2 ms on ARM Cortex-M4 cores, with minimal CPU load (<4%). Entropy pool reseeding intervals are optimized to 60 seconds under typical use cases.

C. *Signature Forgery and Replay Attack Mitigation*

Simulated replay attacks using previously signed transaction payloads are successfully blocked through nonce-chain validation. Forgery attempts using timing/power fault injection fail to compromise private keys, confirming resistance of the signature scheme.

D. *Resource Overhead and Scalability*

The framework occupies less than 14 KB of flash and 1.2 KB of RAM. It scales efficiently across Cortex-M0 to M7 series without modification. Power consumption increase is negligible (<1.5%), making it suitable for battery-powered wallets.

V. Conclusion

This paper presents a lightweight and resilient cryptographic framework for secure key generation and signature integrity in resource-constrained cryptocurrency wallets. By leveraging internal entropy sources such as oscillator jitter and ADC noise, the proposed method achieves high-quality entropy accumulation without external dependencies. The optimized PRNG seeding strategy ensures continuous randomness, enabling robust key generation even in noisy embedded environments. Furthermore, the use of deterministic nonce-based ECDSA, combined with hash-chained replay protection, provides strong defense against transaction forgery and replay attacks. Our simulation and hardware validation results on microcontroller platforms confirm the framework's efficiency, scalability, and low resource overhead. This work lays the foundation for deploying secure and resilient wallet protocols in emerging blockchain applications on IoT and embedded platforms, promoting trust and integrity in decentralized finance ecosystems.

References

[1] Gasser, C., Basin, D., &Capkun, S. (2018). Secure entropy harvesting for embedded systems. IEEE Transactions on Information Forensics and Security, 13(2), 368–382. https://doi.org/10.1109/TIFS.2017.2759802

[2] Aranha, D. F., &Dahab, R. (2013). ECC-based cryptographic primitives for embedded systems. ACM Transactions on Embedded Computing Systems (TECS), 12(3), 1–20. https://doi.org/10.1145/2465787.2465791

[3] Liu, L., Chen, Y., Li, H., & Zhang, X. (2019). Secure key management in IoT with low-cost entropy sources. IEEE Internet of Things Journal, 6(2), 3023–3032. https://doi.org/10.1109/JIOT.2018.2876092

[4] Hummen, R., Wirtz, H., &Wehrle, K. (2014). A lightweight modular security protocol for embedded systems. In Proceedings of the ACM Conference on Embedded Networked Sensor Systems (SenSys). https://doi.org/10.1145/2668332.2668337

[5] Sutar, S., Agrawal, R., &Rao, V. (2021). Digital signature resilience under fault attacks. IEEE Transactions on Dependable and Secure Computing, 18(1), 88–100. https://doi.org/10.1109/TDSC.2018.2883533

[6] Goldberg, I. (2019). Replay protection mechanisms in low-power wallets. IEEE Security & Privacy, 17(5), 38–45. https://doi.org/10.1109/MSEC.2019.2920940

[7] Koo, H., & Lee, D. (2019). Efficient lightweight encryption for blockchain IoT. IEEE Access, 7, 93539–93552. https://doi.org/10.1109/ACCESS.2019.2926920

[8] Zhang, T., Wang, L., & Zhang, M. (2022). Entropy-aware firmware for secure PRNG seeding in edge devices. IEEE Embedded Systems Letters, 14(1), 21–24. https://doi.org/10.1109/LES.2021.3110598

[9] Jamithireddy, N. S. (2014). Latency and propagation delay modeling in peer-to-peer blockchain broadcast networks. *SIJ Transactions on Computer Networks & Communication Engineering*, *2*(5), 6–10.

[10] Jamithireddy, N. S. (2014). Merkle-tree optimization strategies for efficient block validation in Bitcoin networks. *SIJ Transactions on Computer Networks & Communication Engineering*, *2*(1), 16–20.

[11] Jamithireddy, N. S. (2014). Entropy-driven key generation and signature reliability in early cryptocurrency wallet systems. *SIJ Transactions on Computer Networks & Communication Engineering*, *2*(3), 7–11.