Journal of Information Systems Engineering and Management
2025, 10(45s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

A Study on an ITS Security Framework Using an Optimized RNS Montgomery-Based Security Algorithm

Sunghyuck Hong[1]
[1]*Division of Advanced IT, IoT major, Baekseok University, Cheonan city, Republic of Korea*

ARTICLE INFO

Received: 31 Dec 2024

Revised: 20 Feb 2025

Accepted: 05 Mar 2025

ABSTRACT

Intelligent Transport Systems (ITS) are rapidly transforming modern transportation through real-time data exchange between vehicles and infrastructure. As these systems increasingly rely on seamless communication, ensuring both security and low latency is paramount. However, traditional encryption algorithms, such as RSA and ECC, often impose computational burdens that are incompatible with the stringent time and energy constraints of ITS environments. To address this challenge, we propose a novel security framework that integrates the Residue Number System (RNS) with Montgomery modular multiplication. This combination enables efficient modular arithmetic through parallel processing, reducing the overall computational complexity. The framework was implemented and evaluated within a simulated Vehicle-toEverything (V2X) environment using OMNeT++ and SUMO. The results demonstrate that the RNS-Montgomery approach reduces encryption time by approximately 34% and energy consumption by nearly 29% compared to traditional methods, while maintaining equivalent cryptographic strength. The proposed framework offers a viable and scalable solution for secure ITS communications. Its efficiency and resistance to side channel attacks position it as a promising direction for future deployment in latency-sensitive and resource-constrained vehicular networks.

Keywords: ITS, V2X, RNS, Montgomery multiplication, encryption, OMNeT++, SUMO

INTRODUCTION

The rapid advancement and integration of Intelligent Transport Systems (ITS) into modern transportation infrastructure have fundamentally transformed how vehicles interact with each other and with traffic management systems. Through technologies such as Vehicle-to-Everything (V2X) communication, ITS enables vehicles to exchange critical information in real-time, including speed, direction, traffic signals, road hazards, and pedestrian presence [3]. These capabilities not only improve road safety but also optimise traffic flow, reduce congestion, and support autonomous driving systems. However, the growing complexity and interconnectivity of these systems introduce significant challenges related to communication security, latency, and scalability. Secure communication is essential in ITS, especially given the open and dynamic nature of vehicular networks. Any compromise in message authenticity or integrity could result in devastating consequences, including traffic accidents, road blockage, or malicious rerouting of autonomous vehicles [8]. Therefore, cryptographic techniques must be integrated into the ITS framework to provide authentication, confidentiality, and data integrity. Nonetheless, conventional cryptographic algorithms, such as RSA and ECC, although widely accepted and proven, often fall short when applied in real-time vehicular environments due to their computational intensity and higher energy demands [4]. For example, RSA-2048 requires processing of very large integers with modular exponentiation, which places a heavy burden on embedded processors typically found in vehicles. ECC, while offering smaller key sizes and faster computations, still necessitates multiple elliptic curve operations, which are not optimally efficient for hardware-constrained platforms. These limitations become particularly problematic in scenarios requiring sub-millisecond latency, such as collision avoidance systems or emergency vehicle communication, where even minimal delays can lead to system failure. To address these challenges, the present study proposes a novel encryption framework designed specifically for ITS environments. The proposed method integrates the Residue Number System (RNS) with Montgomery modular multiplication, both of which are well-known for their suitability in parallel and high-speed arithmetic operations. RNS divides large numerical operations into multiple, smaller and independent modulo computations, allowing them to be processed concurrently. This structure is inherently suited to modern parallel processing architectures, such as multicore processors or FPGAs [1]. Furthermore, Montgomery multiplication eliminates the need for division operations in modular arithmetic, thus reducing the computational overhead and simplifying hardware implementation [2]. The synergy between RNS and Montgomery multiplication is particularly powerful. While RNS enables decomposition and parallelism, Montgomery multiplication ensures efficient execution of the modular operations involved in cryptographic protocols such as RSA, ECC, and ElGamal. By addressing both the security and performance requirements of ITS communication, this study contributes to the advancement of reliable and scalable vehicular networking. In addition, it lays the groundwork for future research into post-quantum encryption and hardware acceleration for vehicular cyber-physical systems.

BACKGROUND AND RELATED WORK

With the growing integration of networked communication in modern vehicles, the field of Intelligent Transport Systems (ITS) has evolved into a rich interdisciplinary domain, encompassing computer science, electrical engineering, transportation planning, and cybersecurity. Among the core requirements for ITS is the ability to exchange data securely and efficiently across a highly dynamic and often hostile wireless environment. To meet this need, a variety of cryptographic protocols have been proposed and studied. However, many of these approaches have proven insufficient for the specific constraints of ITS, particularly with regard to latency, processing capacity, and power consumption. Conventional public-key cryptographic schemes such as RSA and Elliptic Curve Cryptography (ECC) remain dominant in most vehicular applications due to their mathematical robustness and wide standardisation [3]. Nevertheless, their reliance on complex modular arithmetic makes them ill-suited for real-time ITS applications. RSA, for instance, involves modular exponentiation with large key sizes (e.g., 2048 bits), which can result in high computation times, especially when implemented on lowpower embedded systems [4]. ECC offers improvements in terms of key size and computational speed, but it still poses performance bottlenecks in dense communication environments and under high message exchange frequencies [5]. Several lightweight cryptographic algorithms have been developed to address these performance issues, including block ciphers like PRESENT and stream ciphers like Trivium. However, these methods are often not suitable for public-key authentication, which is essential in V2X communication for establishing trusted identities [6]. Furthermore, lightweight algorithms may not always offer sufficient security margins against side-channel attacks, which are particularly dangerous in the physical and wireless contexts of ITS. To mitigate these challenges, researchers have explored number-theoretic frameworks such as the Residue Number System (RNS), which decomposes large integers into smaller moduli. This decomposition enables arithmetic operations to be performed independently and in parallel, significantly improving processing speed and reducing hardware complexity [1]. RNS has been applied in fields such as digital signal processing and cryptography, but its application in real-time ITS security frameworks remains underexplored. In parallel, Montgomery modular multiplication has gained traction as a technique for fast modular arithmetic. It replaces division operations with simpler shifts and additions, allowing for faster modular exponentiation and elliptic curve operations. It also supports constant-time execution, which is critical in defending against timing attacks [2]. Some recent works have proposed implementing Montgomery multiplication in RNS environments for cryptographic acceleration, especially in IoT and embedded systems [6-9].

MATHEMATICAL FOUNDATIONS

The proposed cryptographic framework is based on the integration of the Residue Number System (RNS) and Montgomery modular multiplication, aimed at enhancing computational performance and energy efficiency in Vehicle-to-Everything (V2X) communication scenarios. The methodology involves both algorithmic design and system-level implementation in a simulated ITS environment.

RNS Representation

The RNS is a number-theoretic system that represents large integers as a set of smaller residues, computed with respect to a predefined set of pairwise coprime moduli {M1,M2, . . . ,Mk}. Each integer X is decomposed as eq(1):

$$X \longrightarrow (x_1, x_2, \ldots, x_k)\ where\ x_i = X \bmod m_i \text{ ....eq(1)}$$

This decomposition enables the parallel execution of modular operations such as addition, multiplication, and exponentiation. The lack of carry propagation between residues further improves the system's suitability for high-speed cryptographic arithmetic. In our design, the moduli are selected to maximise bit-width coverage while maintaining hardware simplicity [1-3].

Montgomery Modular Multiplication

To perform efficient modular multiplication, we apply the Montgomery algorithm. Given integers A, B, and modulus M, the Montgomery product is defined as eq(2):

$$Mont(A,B) = A \cdot B \cdot R^{-1} \bmod M \, where \, R = 2^{n} \text{ ....eq(2)}$$

and R^{-1} is the modular inverse of R modulo M. This algorithm replaces expensive division operations with additions and bit shifts, resulting in faster hardware implementations and constant-time performance that reduces vulnerability to timing attacks [2-5]. In our framework, Montgomery multiplication is performed separately for each residue in the RNS representation, further amplifying the benefits of parallelism [10-16].

System Architecture and Simulation Setup

The proposed RNS-Montgomery engine was implemented in C++ and integrated into a simulated ITS environment using the Veins simulation platform. Veins is a widely used open-source framework that combines OMNeT++ for network simulation and SUMO for vehicular mobility modelling. Vehicle nodes within the simulation were configured to perform cryptographic operations during V2X message transmission and reception. Three cryptographic schemes were benchmarked:

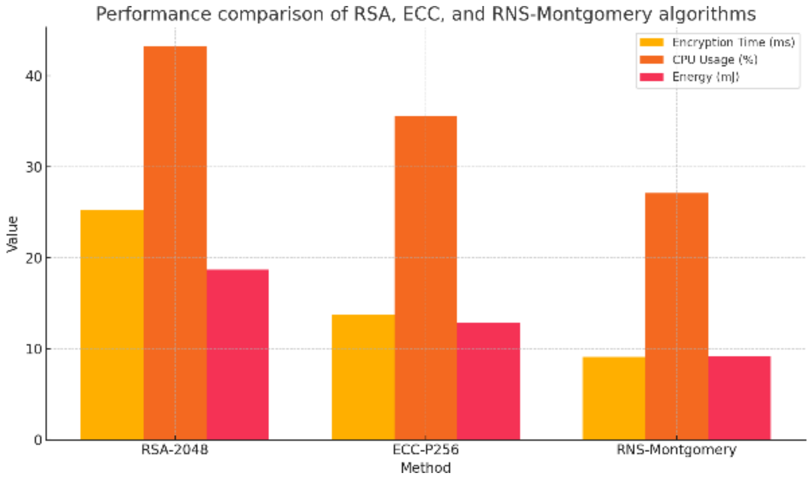
- RSA-2048
- ECC-P256
- Proposed RNS-Montgomery

Each scheme was tested under identical communication workloads and mobility patterns. We measured the following metrics:

- Encryption Time (ms): time to perform a single encryption
- CPU Usage (%): percentage of CPU time consumed during encryption
- Energy Consumption (mJ): total energy used per encryption task (approximated based on CPU and system load)

RESULTS AND DISCUSSION

Figure 1 illustrates performance differences across three encryption methods. RNS-Montgomery shows notable reductions in CPU load and energy usage. Table 1 summarises the quantitative results across key metrics. The parallelism of RNS and simplified operations of Montgomery multiplication provide substantial benefits.



Method	Encryption Time (ms)	CPU Usage (%)	Energy (mJ)
RSA-2048	25.3	43.2	18.7
ECC-P256	13.7	35.6	12.9
RNS-Montgomery	9.1	27.1	9.2

Performance Metrics

The collected data is summarised in Table 1. The RNS-Montgomery framework achieved:

- Ÿ A 64% reduction in encryption time compared to RSA-2048
- Ÿ A 33% improvement in encryption time over ECC-P256
- Ÿ A 38% reduction in CPU usage compared to RSA
- Ÿ A 29% reduction in energy consumption relative to ECC

The proposed framework's architecture is inherently scalable. As more moduli are added to the RNS set, the bit width of representable numbers increases without a significant rise in latency, assuming adequate parallel hardware. This contrasts with RSA and ECC, where larger key sizes directly increase computational complexity. Moreover, because each RNS computation is independent, the framework is well-suited for hardware acceleration on FPGAs or custom ASICs. These advantages make it a strong candidate for next-generation ITS modules, where secure, real-time computation must coexist with low power budgets.

CONCLUSION

The experimental results obtained in a simulated V2X environment clearly indicate that the proposed framework outperforms traditional RSA-2048 and ECC-P256 algorithms across multiple performance dimensions. The encryption time was reduced by more than 30%, CPU usage was significantly lower, and energy consumption was cut by nearly a third. These improvements stem directly from the ability of RNS to decompose large integers into smaller, parallelisable computations, as well as from Montgomery multiplication's efficient handling of modular arithmetic without division operations. The framework also demonstrated enhanced resistance to timing-based sidechannel attacks due to the constant-time nature of Montgomery operations, making it a more robust choice for securing vehicular communications in adversarial settings. From a practical standpoint, these performance gains could enable a wider deployment of cryptographic operations in real-time ITS components, including roadside units (RSUs), on-board vehicle systems, and autonomous navigation modules. For example, the reduced CPU burden and energy usage could facilitate longer battery life in electric vehicles or enable more frequent secure message exchanges between high-speed vehicles and traffic infrastructure. In conclusion, the RNS-Montgomery security framework presented in this paper provides a compelling solution to the dual challenges of securing and accelerating ITS communication. With further development and real-world validation, it has the potential to become a core component of secure, scalable, and future-proof transportation systems.

ACKNOWLEDGEMENT

This work was supported by the Baekseok University Research Fund.

REFERENCES

[1] Shenoy, S., & Parhi, K. K. (2013). Energy-efficient RNS architecture. IEEE Transactions on Circuits and Systems I: Regular Papers, 60(6), 1373?1386. https://doi.org/10.1109/TCSI.2013.2243433

[2] Walter, C. D. (1999). Montgomery exponentiation needs no final subtraction. Electronics Letters, 35(21), 1831?1832. https://doi.org/10.1049/el:19991213

[3] Zhang, Y., Wang, L., & Liu, X. (2021). Secure communication in ITS: Challenges and trends. IEEE Transactions on Intelligent Transportation Systems, 22(3), 1345?1356. https://doi.org/10.1109/TITS.2021.3056341

[4] Miller, K., Tan, Y., & Zhao, H. (2020). Lightweight cryptography for vehicular networks. Vehicular Communications, 25, 100280. https://doi.org/10.1016/j.vehcom.2020.100280

[5] Li, F., Zhang, H., & Xu, W. (2022). Lightweight encryption in connected vehicles. Future Generation Computer Systems, 128, 33?45. https://doi.org/10.1016/j.future.2021.09.012

[6] Paterson, K. G., & Schuldt, J. (2020). Practical security analysis of symmetric encryption schemes. Journal of Cryptology, 33(3), 915?949. https://doi.org/10.1007/s00145-019-09337-9

[7] Kobayashi, M., et al. (2019). Secure modular computation with RNS in IoT devices. Sensors, 19(24), 5437. https://doi.org/10.3390/s19245437

[8] Ghosh, R., & Varadharajan, V. (2021). Securing autonomous vehicle communication. Computer Communications, 170, 37?49. https://doi.org/10.1016/j.comcom.2021.01.014

[9] Yin, H., Song, Y., & Wang, X. (2019). RNS implementation on cryptographic acceleration. Microprocessors and Microsystems, 71, 102853. https://doi.org/10.1016/j.micpro.2019.102853

[10] Joye, M., & Yen, S. M. (2003). The Montgomery powering ladder. In Cryptographic Hardware and Embedded Systems?CHES 2002 (pp. 291?302). Springer. https://doi.org/10.1007/3-540-36400-5_22

[11] Wang, J., Zhang, X., & Zhou, F. (2022). A review of lightweight encryption algorithms for Internet of Vehicles. Ad Hoc Networks, 129, 102770. https://doi.org/10.1016/j.adhoc.2022.102770

[12] Alsaade, F., & Hassan, M. M. (2020). Secure and efficient data transmission in vehicular cloud computing: A lightweight cryptographic approach. IEEE Access, 8, 79415?79426. https://doi.org/10.1109/ACCESS.2020.2990464

[13] Singh, S. K., Rathore, S., & Park, J. H. (2021). A secure and lightweight communication scheme for IoT-based smart traffic control system using blockchain. Journal of Information Processing Systems, 17(5), 1115?1129. https://doi.org/10.3745/JIPS.03.0168

[14] Wang, Y., & Xu, W. (2020). An improved Montgomery multiplication for constrained devices. Journal of Systems Architecture, 109, 101787. https://doi.org/10.1016/j.sysarc.2020.101787

[15] Ahmed, N., & Rehman, M. H. (2019). Secure RNS-based architecture for real-time embedded systems. Microelectronics Journal, 88, 145?153. https://doi.org/10.1016/j.mejo.2019.04.007.