

Securing micro transactions in the Internet of Things with cryptography primitives

Sukhvinder Singh Dari *

Symbiosis Law School Nagpur

Symbiosis International (Deemed University)

Pune

Maharashtra

India

Dharmesh Dhabliya [†]

Department of Information Technology

Vishwakarma Institute of Information Technology

Pune

Maharashtra

India

Anishkumar Dhablia [§]

Engineering Manager

Altimetrik India Pvt Ltd.

Pune

Maharashtra

India

Shreyas Dingankar [‡]

Institute of Management & Entrepreneurship Development

Bharati Vidyapeeth (Deemed to be University)

Pune

Maharashtra

India

* E-mail: sukhvinder.dari@gmail.com (Corresponding Author)

† E-mail: dharmesh.dhabliya@viit.ac.in

§ E-mail: anishdhablia@gmail.com

‡ E-mail: shreyas.dingankar@bharativedyapeeth.edu

M. Jahir Pasha [@]

*Department of Computer Science and Engineering
G.Pulllaiah College of Engineering and Technology
Kurnool
Andhra Pradesh
India*

Samir N. Ajani [#]

*Department of Computer Science and Engineering (Data Science)
Shri Ramdeobaba College of Engineering and Management
Nagpur
Maharashtra
India*

Abstract

The growing number of IoT devices, microtransaction security in the Internet of Things (IoT) is a critical issue. In order to improve the security of microtransactions in Internet of Things ecosystems, this article investigates the usage of cryptographic primitives. Strong safeguards against possible risks including data manipulation, eavesdropping, and unauthorized access are provided by cryptography, which provides a foundation for guaranteeing the confidentiality, integrity, and validity of transaction data. We address the special problems of power and processing limits by delving into the implementation of lightweight cryptography algorithms and protocols designed for resource-constrained IoT devices. Our goal is to create a trust framework that guarantees the security and privacy of data exchange by incorporating cryptographic primitives into IoT microtransactions. By encouraging trust and dependability in microtransactions, which are essential to the future of networked smart devices, our research helps to build a more secure and robust Internet of Things environment.

Subject Classification: Primary 93A30, Secondary 49K15.

Keywords: Cryptographic primitives, Internet of Things, Security, Microtransaction, Key management.

1. Introduction

The ever-growing array of networked gadgets that are improving our daily lives and changing a variety of businesses has led to the exponential expansion of the Internet of Things, or IoT. The resource limitations that are frequently present in Internet of Things devices are one of the main

[@] E-mail: jahir4444@gmail.com

[#] E-mail: samir.ajani@gmail.com

issues we address. Because the processing and memory capacity of these devices, such sensors and actuators, is usually constrained, traditional cryptographic solutions are not feasible [1]. We investigate lightweight cryptography methods and protocols designed specifically for Internet of Things devices to address this problem. Strong security is intended to be provided with the least amount of computational and energy overhead possible thanks to these cryptographic primitives.

The crucial problem of protecting microtransactions in an Internet of Things (IoT) environment has been tackled by a plethora of earlier publications, frequently making use of cryptographic primitives and algorithms. The research [2] conducted a noteworthy study that examined IoT security generally and emphasized the importance of secure data exchange. Furthermore, [4] explored how blockchain technology might be used for safe IoT microtransactions, emphasizing how distributed ledgers can improve trust and transparency. This idea is directly relevant to our work, as we look into cryptographic primitives that can support or function in addition to blockchain-based solutions. Additionally, [5] research from 2020 looked at privacy and security issues with IoT microtransactions. They covered a range of encryption methods and key management approaches, highlighting the significance of cryptography in protecting transactions in Internet of Things networks.

2. Cryptography Primitives in IoT

2.1 Introduction to cryptographic primitives

The fundamental building blocks of cryptography are known as cryptographic primitives. In many applications, secure communication, data protection, and authentication are built on these fundamental mathematical concepts and methods [6]. Digital signatures, hashing, encryption, and key exchange protocols are examples of cryptographic primitives. They are crucial to protecting sensitive data in the digital era because they guarantee the secrecy, integrity, and authenticity of data. For the purpose of creating safe systems, whether they be for protecting online transactions or facilitating privacy in the Internet of Things (IoT), it is essential to comprehend and apply cryptographic primitives as shown in Figure 1 and Table 1.

2.2 Lightweight cryptography for resource-constrained IoT devices

The lightweight cryptography, a specialized area of cryptographic research, is to create encryption and security solutions that are appropriate

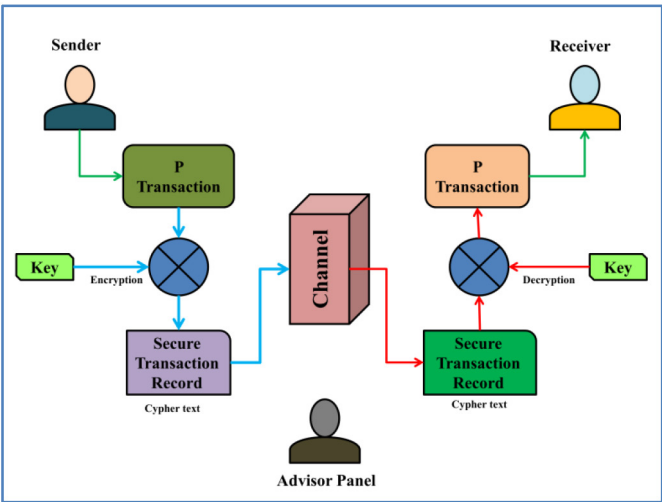


Figure 1
Representation Architecture of Microtransaction using cryptographic primitives

for Internet of Things (IoT) devices with little resources [11]. Because IoT devices frequently have low amounts of RAM, computing power, and energy, typical encryption techniques are not suitable for these kinds of settings. Lightweight cryptography designs algorithms with low computational and memory requirements while preserving robust cryptographic features in an effort to achieve a balance between security and resource efficiency.

Table 1
Different IoT device with specification in microtransaction

IoT Device	Power	Memory Used	Technology	Security	Communication Bandwidth
Smart Wearables [7]	Low	Low	Bluetooth LE	Medium	Moderate
RFID Tags [8]	Ultra-Low	Very Low	NFC	Low	Low
Environmental Sensors [9]	Low	Low	MQTT	Medium	Low
Industrial Sensors [10]	Low	Low	CoAP	High	Moderate

2.3 Key management and encryption techniques for IoT microtransactions

Encryption and key management strategies are essential for guaranteeing the safety of microtransactions in the Internet of Things (IoT) network as presented in Table 2. It is essential to use the right cryptographic techniques in the context of the Internet of Things, where devices with limited resources are common. Elliptic curve cryptography (ECC) is frequently used to achieve a trade-off between security and efficiency since it offers strong security at lower key lengths, which makes it perfect for IoT devices with limited resources.

Table 2
Encryption techniques suitable for IoT

Technique	Description
Symmetric Key Encryption [11]	Utilizes a single common key for decryption as well as encryption. Its efficiency makes it appropriate for devices with limited resources.
Asymmetric Key Encryption [6]	Uses a set of public and private keys, which increases resource requirements but provides secure communication and authentication.
Elliptic Curve Cryptography (ECC) [2]	Strong security with lower key lengths makes it ideal for devices with low memory and processing capacity.
Lightweight Cryptographic Algorithms [4]	Developed with internet of things devices in mind, providing a balance between resource efficiency and security.

3. Implementing Cryptographic Primitives in IoT Microtransactions

3.1 Cryptographic algorithms

- i. SECP256K1 (Elliptic Curve Digital Signature Algorithm):

A popular digital signature algorithm for elliptic curves, SECP256K1 (ECDSA) is utilized in many different applications, such as Internet of Things microtransactions. The following is a detailed mathematical model that illustrates how ECDSA functions in the context of IoT microtransactions for message signing and verification as Presented in Figure 2:

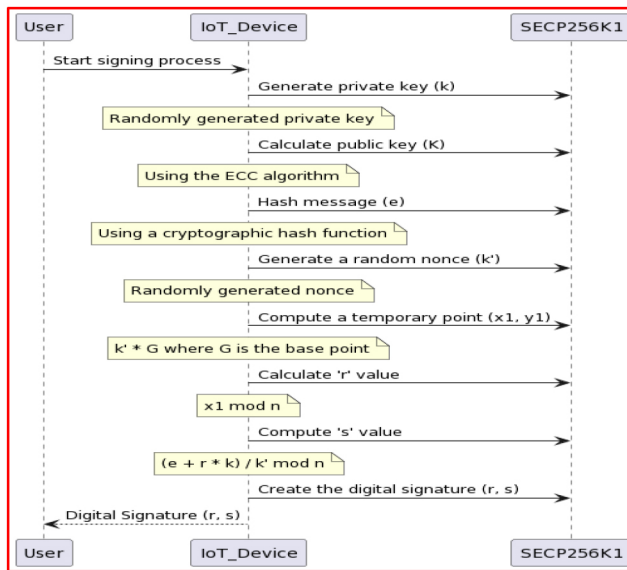


Figure 2

Flowchart of Elliptic Curve Digital Signature Algorithm (SECP256K1)

Key Generation:

- Select a random private key (k) as an integer between 1 and $n-1$, where n is the elliptic curve's order.
- Calculate the matching public key (K) using the formula $K = k * G$, where G is the elliptic curve's base.
- Typically, the public key (K) is shown as two coordinates (x, y) .

Message Signing:

- Apply a cryptographic hash function (like SHA-256) to the message (M) to get the message hash (e).
- Select a random nonce (k') that falls between the private key's range.
- Find a temporary elliptic curve point by computing: $(k' * G) = (x1, y1)$.
- Determine the 'r' value by taking the modulo n x-coordinate of $(x1, y1)$.
- Ascertain the value of "s" by computing $s = (e + r * k) / k' \pmod{n}$.
- The procedure of signing results in the signature (r, s) .

Message Verification:

- Acquire the signature (r, s) and the public key (K).
- Determine the received message's message hash (e).
- Check to see if r and s fall inside the range $[1, n-1]$.
- Find the value of $s^{-1} \pmod{n}$, which is the inverse of s .
- The values $u_1 = e * s^{-1} \pmod{n}$ and $u_2 = r * s^{-1} \pmod{n}$ should be calculated.
- Use the formula $(x_1, y_1) = u_1 * G + u_2 * K$ to find a temporary point on the elliptic curve.
- The signature is legitimate if the computed point (x_1, y_1) agrees with the signature's ' r ' value. If not, it isn't valid.

3.2 Integration of cryptographic primitives into IoT devices

Ensuring the security and privacy of data and transactions within the Internet of Things (IoT) ecosystem requires the integration of cryptographic primitives into IoT devices. These fundamentals, such authentication methods and encryption, are essential for defending against a range of security risks. IoT devices frequently operate in contexts with limited processing power and memory, so it's critical to carefully choose and apply cryptographic solutions that balance efficiency and strong security.

These algorithms are ideal for devices with constrained resources because they are developed to reduce computational overhead. Furthermore, since safe key exchange and storage are essential to Internet of Things security, key management techniques must be taken into account while implementing cryptographic primitives.

4. Evaluation and Performance considerations with trade-offs

ECC (SECP256K1) provides a robust security foundation with comparatively low computational overhead, making it an energy-efficient option for Internet of Things devices with limited resources. Additionally, it uses less memory, which is crucial for gadgets with constrained storage as shown in Table 3. Its short latency also guarantees effective communication. Its adaptation to different algorithms and flexibility are minimal, nevertheless. CoAP-PSK is a popular choice for IoT devices with limited resources since it offers robust security with little memory usage and computational cost. Its great degree of flexibility and low latency enable quick communication in a variety of situations. It achieves equilibrium between resource efficiency and security.

Table 3
Performance consideration of different security algorithm and it tradeoff for IoT

Consideration / Trade-off	ECC (SECP256K1)	MQTT-TLS	CoAP-PSK
Computational Overhead	Low	Moderate	Low
Memory Usage	Low	Moderate	Low
Energy Consumption	Low	Moderate	Low
Latency	Low	Moderate	Low
Algorithm Flexibility	Moderate	High	High

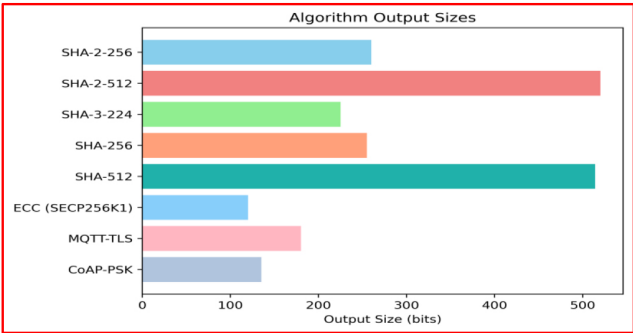


Figure 3
Comparative analysis of output for different method

ECC (SECP256K1) is a good choice for Internet of Things devices with limited resources because of its ability to handle cryptographic operations efficiently, as seen by its comparatively short processing times as shown in Figure 3. Higher processing times are seen in MQTT-TLS, which is indicative of its more robust security measures. The trade-offs between resource efficiency and security is highlighted by these findings, as shown in Table 4.

Table 4
Result for different input size for Security algorithm and it tradeoff for IoT

Input Size (KB)	ECC (SECP256K1) Time (ms)	MQTT-TLS Time (ms)	CoAP-PSK Time (ms)
10	2.12 ms	4.14 ms	3.08 ms
40	8.10 ms	15.20 ms	10.25 ms
80	16.05 ms	30.46 ms	20.74 ms
120	24.47 ms	45.11 ms	30.23 ms

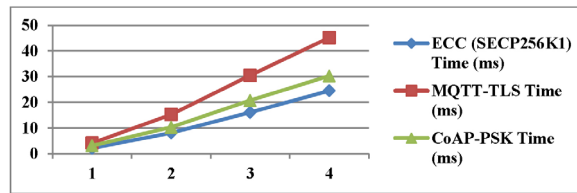


Figure 4

Performance comparison of algorithm for microtransaction for different Input data

IoT developers must choose the best cryptographic solutions based on the capabilities and security requirements of their device. While MQTT-TLS and CoAP-PSK offer improved security at the cost of higher resource consumption, ECC is efficient yet can be desirable in scenarios where computational resources are few as shown in Figure 4. Informed decision-making based on these trade-offs is necessary to guarantee the effectiveness and security of Internet of Things systems.

5. Conclusion

The importance of cryptographic primitives in improving the security of microtransactions has been highlighted by this research. Examples of these primitives include lightweight algorithms designed for IoT devices with limited resources. It is now clear that choosing the best cryptographic algorithm requires careful consideration of trade-offs between performance and other factors. ECC (SECP256K1) and CoAP-PSK provide effective yet strong security for IoT devices with limited resources, balancing data protection with energy and memory conservation. Furthermore, careful consideration of elements like key management, communication protocols, and performance trade-offs is necessary when integrating cryptographic primitives into Internet of Things devices. Establishing trust and guaranteeing the confidentiality and validity of microtransactions in the Internet of Things (IoT) environment depend heavily on the effective deployment of cryptographic technologies.

References

- [1] H. Bi, Y. Chen and X. Zhu, "A Multipath Routing for Payment Channel Networks for Internet of Things Microtransactions," in *IEEE Internet of Things Journal*, vol. 9, no. 20, pp. 19670-19681, 15 Oct.15 (2022), doi: 10.1109/JIOT.2022.3167098.

- [2] Z. Zhang, D. Zhu and B. Mi, "C-DAG: Community-assisted DAG mechanism with high throughput and eventual consistency", *Proc. Int. Conf. Wireless Algorithms Syst. Appl.*, pp. 113-121 (2020).
- [3] A. Singh, K. Click, R. M. Parizi, Q. Zhang, A. Dehghantanha and K.-K. R. Choo, "Sidechain technologies in blockchain networks: An examination and state-of-the-art review", *J. Netw. Comput. Appl.*, vol. 149, Jan. (2020).
- [4] J. Zhang, Y. Ye, W. Wu and X. Luo, "Boros: Secure and efficient off-blockchain transactions via payment channel hub", *IEEE Trans. Dependable Secure Comput.*, Dec. (2021).
- [5] Y. Ye, Z. Ren, X. Luo, J. Zhang and W. Wu, "Garou: An efficient and secure off-blockchain multi-party payment hub", *IEEE Trans. Netw. Service Manag.*, vol. 18, no. 4, pp. 4450-4461, Dec. (2021).
- [6] S. Roos, P. Moreno-Sanchez, A. Kate and I. Goldberg, "Settling payments fast and private: Efficient decentralized routing for path-based transactions", *arXiv:1709.05748*(2017).
- [7] D. Strugar, R. Hussain, M. Mazzara, V. Rivera, J. Young Lee and R. Mustafin, "On M2M Micropayments: A Case Study of Electric Autonomous Vehicles," 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada (2018).
- [8] Y. Yuan and F.-Y. Wang, "Towards blockchain-based intelligent transportation systems", *Intelligent Transportation Systems (ITSC) 2016 IEEE 19th International Conference on.* IEEE, pp. 2663-2668 (2016).
- [9] U. Hunkeler, H. L. Truong and A. Stanford-Clark, "Mqtt-s: A publish/subscribe protocol for wireless sensor networks", *Communication Systems Software and Middleware and Workshops 2008. COMSWARE 2008. 3rd International Conference on*, pp. 791-798, Jan (2008).
- [10] K. W. E. Cheng, B. P. Divakar, H. Wu, K. Ding and H. F. Ho, "Battery-management system (bms) and soc development for electrical vehicles", *IEEE Transactions on Vehicular Technology*, vol. 60, no. 1, pp. 76-88, Jan (2011).
- [11] C. Tang, C. Li, X. Yu, Z. Zheng and Z. Chen, "Cooperative mining in blockchain networks with zero-determinant strategies", *IEEE Trans. Cybern.*, vol. 50, no. 10, pp. 4544-4549, Oct. (2019).