Lightweight Digital Signatures for Internet of Things: Current and Post-Quantum Trends and Visions

Saif E. Nouma and Attila A. Yavuz
Department of Computer Science and Engineering, University of South Florida, Tampa, FL, USA
{saifeddinenouma, attilaayavuz}@usf.edu

2023 IEEE Conference on Dependable and Secure Computing (DSC) | 979-8-3503-8211-2/23/$31.00 ©2023 IEEE | DOI: 10.1109/DSC61021.2023.10354177

***Abstract*—The Internet of Things (IoT) harbors a large number of resource-limited devices (e.g., sensors) that continuously generate and offload sensitive information (e.g., financial, health, personal). It is imperative the ensure the trustworthiness of this data with efficient cryptographic mechanisms. Digital signatures can offer scalable authentication with public verifiability and non-repudiation. However, the state-of-the-art digital signatures do not offer the desired efficiency and are not scalable for the connected resource-limited IoT devices. This is without considering long-term security features such as post-quantum security and forward security. In this paper, we summarize the main challenges to an energy-aware and efficient signature scheme. Then, we propose new scheme design improvements that uniquely embed different emerging technologies such as Mutli-Party Computation (MPC) and secure enclaves (e.g., Intel SGX) in order to secret-share confidential keys of low-end IoT devices across multiple cloud servers. We also envision building signature schemes with Fully Homomorphic Encryption (FHE) to enable verifiers to compute expensive commitments under encryption. We provide evaluation metrics that showcase the feasibility and efficiency of our designs for potential deployment on embedded devices in IoT.**

***Index Terms*—Authentication; Internet of Things; post-quantum security; embedded devices; lightweight cryptography.**

I. Introduction

Internet of Things (IoT) includes billions of connected low-end devices (e.g., RFID tags, sensors) which gather, process, and transmit vast amounts of sensitive information (e.g., financial, personal, healthcare) at large scale. Ensuring the trustworthiness of this data is of utmost importance. While symmetric key cryptography (e.g., message authentication codes) offers computational efficiency, it lacks non-repudiation which is essential for many use cases (e.g., legal cases).

Digital signatures provide authentication with public verifiability and non-repudiation which are fundamental security services to safeguard IoT devices from various attacks namely man-in-the-middle and tampering attacks. Yet, current digital signatures still do not meet the stringent requirements of IoT devices in terms of processing, memory, and bandwidth usage. This is without considering additional security guarantees such as post-quantum (PQ) and forward securities for long-term security and key-compromise resiliency, respectively.

A. Overview of State-of-the-Art Digital Signature Standards

Herein, we discuss the conventional and PQ signature standards, along with their potential hybrid constructions.

Conventional and PQ Standards. The deployed conventional signature standards are divided mainly into: *(i) factorization-based:* exemplified by the well-known RSA. Despite its fast signature verification, it suffers from large keys (e.g., 3072-bit key for 128-bit security) and costly signing. To date, there is no implementation of RSA with a 2048-bit key on a low-end 8-bit microcontroller unit (MCU). *(ii) Elliptic-Curve Discrete Logarithm Problem (ECDLP)-based:* offer faster signing and smaller key sizes. The EC-based standard Ed25519 [1] offers several software and hardware implementations for 8-bit MCUs. However, they still require expensive EC operations resulting in high energy and bandwidth usages which could drain the battery of IoT devices (e.g., medical implants). Overall, conventional signature standards still lack high signing efficiency and long-term security (e.g., PQ security).

NIST reveals the PQ signature standards, namely Falcon, Dilithium, and SPHINCS+ [3]. Dilithium provides best performance trade-off but remains more costly than conventional alternatives. To date, there is no open-source implementation of PQ signatures on 8-bit MCUs, except for BLISS, which suffer from devastating side-channel attacks [6].

Hybrid Signatures. Standardization proposals [7] advocate the important role of hybrid signatures that fuses multiple signature schemes with different hardness assumptions (e.g., conventional EC-based, PQ lattice-based) to promote cryptographic agility. However, combining signature standards will only duplicate performance slowdown rendering it more infeasible for IoTs.

Discussion: State-of-the-art signature standards are unsuitable for low-end IoT devices at scale. There is always a trade-off between security guarantees and scheme performance. Below, we discuss approaches that address these challenges.

B. Advanced Lightweight Signature Frameworks for IoTs

Several methods attempt to alleviate the burden on IoT devices by pushing it to verifiers or introducing additional assumptions (e.g., trusted hardware, non-colluding distributed servers). Below we discuss relevant works in the IoT context.

One-Time Signature (OTS): rely on one-way functions with trapdoors (e.g., cryptographic hash functions). This approach offers performance efficiency and high-security guarantees but the private/public key is valid for a single signature

979-8-3503-8211-2/23/$31.00 ©2023 IEEE

[1] https://ed25519.cr.yp.to

TABLE I: Performance evaluation of the lightweight digital signatures for IoT

Scheme	Advantages						Limitations	
	PQ Security	Side-channel Resistance	Key-compromise Resiliency	Aggregation Capability	Cryptographic Agility	Standard Compliance	Central Trusted Entity	Non-colluding Assumptions
Ed25519	×	✓	×	×	×	✓	×	×
BAF [1]	×	✓	✓	✓	×	×	×	×
ESEM [2]	×	✓	×	×	×	×	×	✓
Dilithium [3]*	✓	✓	×	×	×	✓	×	×
ANT [4]	✓	✓	✓	×	×	×	×	✓
HASES [5]	✓	✓	✓	✓	✓	✓	✓	×

* To date, the lattice-based NIST PQ Dilithium does not have a benchmark on resource-limited 8-bit MCUs thereby being considered resistant to side-channel and timing attacks. However, It has been shown that previous lattice-based signature schemes (e.g., BLISS) are prone to devastating side-channel attacks [6].

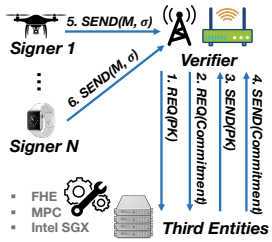

Fig. 1: High-level depiction of IoT system model

only. Several multiple-time signatures (e.g., NIST PQ standard SPHINCS+ [3]) have been proposed based on seminal OTS schemes. However, they incur additional costly computation due to the key management thereby not feasible for the IoT.

Signatures with Precomputation. achieve high signer efficiency by precomputing expensive (e.g., EC) commitments during key generation. A trivial solution is to store one-time keys w.r.t. the number of messages at the signer. This only appends a huge linear storage penalty for low-end devices. BPV technique [2] accelerates the signing process by randomly generating commitments from a constant-size table. Although it reduces the storage and computation overheads, it still incurs a storage penalty and relies on weak pseudo-random generators in resource-limited devices, making them prone to timings attacks.

Signatures with Distributed Third-Party Servers. rely on a set of non-colluding distributed servers to supply verifiers with costly one-time public keys. Examples include conventional ESEM [2] and the PQ-secure ANT [4], offering efficient signing. Yet, such techniques are limited to cases where verifiers have a stable high-bandwidth Internet. However, verifiers can be low-end or edge devices (e.g., smartphones), with limited bandwidth, thereby susceptible to delays and outages. This approach also assumes a semi-honest setting which compromises the security guarantees. Hence, it can support various wireless network security settings (e.g., [8]).

Signatures with Hardware Support. utilize a commitment constructor oracle that leverages secure hardware (e.g., HASES [5]). This oracle stores a master key, allowing the derivation of any private/public key or commitment for an IoT cluster. Hence, verifiers can request one-time public keys and commitments in advance or on demand with minimal delays. However, trusted hardware is a potential single point of failure. If compromised, all private keys within the IoT cluster would be exposed.

II. Proposed Future Works

Table I summarizes the advantages and limitations of prior proposed approaches. We aim to address the following research question: *How to achieve high-performance efficiency at low-end signers without consorting unpractical assumptions (e.g., central trusted authority) or expensive storage at verifiers?*

As depicted in Fig. 1, we now propose new research directions that cope with the above limitations and challenges.

Signatures with Distributed Root of Trust. employ distributed servers with secure hardware in order to provide verifiers with one-time commitments and public keys. Unlike previous approaches, our proposed technique avoids single-point of failures and unpractical non-colluding server assumptions. The generated public key is certified via MPC technique [9] thereby achieving distributed certificate management and malicious security against adversarial attacks.

Signatures with Fully Homomorphic Encryption (FHE). achieve high signing performance by eliminating the need for signers to communicate one-time public keys. Instead of relying on third-party entities or precomputation techniques, verifiers can utilize a master public key associated with an IoT cluster to derive the public keys of any user under encryption. While there is an extra computation involved, which can be costly, verifiers can precompute public keys or delegate the computation to a more resourceful cloud server with hardware acceleration.

Limitations. Hardware-based signature schemes have security threats, including side-channels attacks. Thus, it is crucial to recognize limitations of relying on hardware-based security. Various techniques (e.g., [10]) safeguard secure enclaves against such attacks, completing our proposed framework.

Acknowledgment

This research is supported by the Cisco Research Award (220159), and the NSF CAREER Award CNS-1917627.

References

[1] A. A. Yavuz, "Eta: efficient and tiny and authentication for heterogeneous wireless systems," in *Proc. of the sixth ACM conference on Security and privacy in wireless and mobile networks*, ser. WiSec '13, 2013, pp. 67–72.

[2] M. O. Ozmen, R. Behnia, and A. A. Yavuz, "Energy-aware digital signatures for embedded medical devices," in *7th IEEE Conference on Communications and Network Security (CNS)*, 2019.

[3] G. Alagic, D. Apon, D. Cooper, Q. Dang, T. Dang, J. Kelsey, J. Lichtinger, C. Miller, D. Moody, R. Peralta *et al.*, "Status report on the third round of the nist post-quantum cryptography standardization process," *National Institute of Standards and Technology, Gaithersburg*, 2022.

[4] R. Behnia and A. A. Yavuz, "Towards practical post-quantum signatures for resource-limited internet of things," in *Annual Computer Security Applications Conference*, 2021, pp. 119–130.

[5] S. E. Nouma, , and A. A. Yavuz, "Post-quantum forward-secure signatures with hardware-support for internet of things," ser. IEEE International Conference on Communications (ICC). IEEE, 2023, p. 1–6.

[6] S. Marzougui, N. Wisiol, P. Gersch, J. Krämer, and J.-P. Seifert, "Machine-learning side-channel attacks on the galactics constant-time implementation of bliss," in *Proceedings of the 17th International Conference on Availability, Reliability and Security*, 2022, pp. 1–11.

[7] M. Ounsworth, J. Gray, and M. Pala, "Composite Signatures For Use In Internet PKI," Internet Engineering Task Force, Internet-Draft draft-ounsworth-pq-composite-sigs-08, Mar. 2023, work in Progress.

[8] M. Grissa, A. A. Yavuz, and B. Hamdaoui, "Cuckoo filter-based location-privacy preservation in database-driven cognitive radio networks," in *Computer Networks and Information Security (WSCNIS), 2015 World Symposium on*, Sept 2015, pp. 1–7.

[9] C. Bonte, N. P. Smart, and T. Tanguy, "Thresholdizing HashEdDSA: MPC to the rescue," *Inter. Journal of Inf. Sec.*, vol. 20, no. 6, pp. 879–894, 2021.

[10] F. Lang, W. Wang, L. Meng, Q. Wang, J. Lin, and L. Song, "Informer: Protecting intel sgx from cross-core side channel threats," in *Intern. Conf. on Information and Communications Security*, 2021, pp. 310–328.