

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

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 to 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 Multi-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 Ed25519¹ 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

¹<https://ed25519.cr.yp.to>

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

* 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].

II. PROPOSED FUTURE WORKS

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.

ACKNOWLEDGMENT

REFERENCES

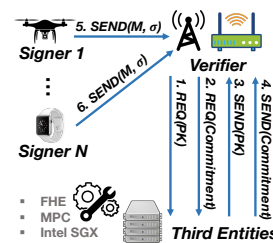


Fig. 1: High-level depiction of IoT system model