Hash-based signatures for the Internet of Things

[Position Paper]

Paolo Palmieri
Department of Computer Science
University College Cork
Cork, T12 YN60 Ireland
p.palmieri@cs.ucc.ie

ABSTRACT

While numerous digital signature schemes exist in the literature, most real-world system rely on RSA-based signature schemes or on the digital signature algorithm (DSA), including its elliptic curve cryptography variant ECDSA.

In this *position paper* we review a family of alternative signature schemes, based on hash functions, and we make the case for their application in Internet of Things (IoT) settings. Hash-based signatures provide postquantum security, and only make minimal security assumptions, in general requiring only a secure cryptographic hash function. This makes them extremely flexible, as they can be implemented on top of any hash function that satisfies basic security properties. Hash-based signatures also feature numerous parameters defining aspects such as signing speed and key size, that enable trade-offs in constrained environments. Simplicity of implementation and customization make hash based signatures an attractive candidate for the IoT ecosystem, which is composed of a number of diverse, constrained devices.

Keywords

Signature schemes; Hash-based signatures; Internet of Things

1. INTRODUCTION

Hash-based signatures are signature schemes that rely exclusively on the security of hash functions, and were first introduced by Ralph Merkle in 1989 [15]. In recent years, hash-based signatures have increased in popularity, and have undergone numerous improvements [4]. In particular, modern schemes improve parameter sizes and runtimes for implementations, present security reductions, and lower the security assumptions on the underlying hash function, including resilience against collisions. There are several arguments that support the use of hash-based signatures: minimal security assumptions and resistance to quantum computers, simplicity of implementation, and extensive parameterization leading to almost complete customization. In this paper, we argument that these same characteristic also make them ideal candidates for the Internet of Things (IoT).

A first fundamental feature of hash modern hash-based signature schemes is to make make minimal security assumptions, thus reducing the attack surface and opportunities for cryptanalysis. The Extended Merkle Signature Scheme (XMSS), for instance, relies exclusively on the underlying hash function for security: it has been proven that if any secure hash function exists, then a secure implementation of XMSS is possible [3]. In practice, XMSS requires only a secure cryptographic hash function that is either second preimage resistant or pseudorandom to be secure. This effectively reduces the complexity of implementation, by eliminating reliance on multiple security components, and streamlines deployment among diverse implementations and devices, as it is often the case in IoT devices.

Hash-based signature schemes are also function-agnostic: they can be built on top of any hash function that satisfies the security requirements [4]. This inherent flexibility of hash-based signatures allows the selection of the most suitable function (in terms of efficiency) for each application scenario, which is an asset in constrained IoT settings. The same flexibility also makes them future-proof, as hash functions can be simply replaced in any implementation when vulnerabilities for the specific function emerge over time.

Future-proofness of hash-based signatures is further guaranteed by their quantum-resistant nature [5]. In practical scenarios and real-world implementations, the most common digital signature schemes are currently RSA, DSA, and ECDSA. The security of these schemes relies on trapdoor one-way functions based on the hardness of factoring integers and computing discrete logarithms, respectively. However, as shown by Shor [17], it is likely these computational problems will be solved by quantum computers in polynomial time, thus breaking the security of the trapdoor one-way functions. As functioning quantum computers may be developed over the medium term, post-quantum signature schemes are being investigated, and the Internet Engineering Task Force (IETF), the European Telecommunications Standards Institute (ETSI), and the US National Institute of Standards and Technology (NIST) have all started the standardisation process for post-quantum cryptography. The function-agnostic characteristic of hash-based signatures also makes them suitable post-quantum candidates, as there are known ways to construct efficient hash function families that display the needed security properties (such as second preimage resistance or pseudorandomness) even in the presence of quantum computers [3]. Internet of Things settings such as

DOI: 10.1145/1235

industrial applications and city monitoring, where deployment of new devices is difficult, expensive and time consuming, can benefit from the long term security offered by post-quantum cryptography.

Finally, hash-based signature implementations are highly parameterized, contrary to most other signature schemes. This is particularly true in schemes where multiple hash trees are used (as discussed in Section 2). The signature scheme parameters enable trade-offs between signing speed and key size, which can be adapted to specific implementation requirements. Therefore, parameterized hash-based signature schemes allow security in performance-constrained environments, that are common in the Internet of Things. Low-power and lightweight signatures can in fact be achieved through the selection of appropriate parameters, rather than dedicated schemes.

The minimal security assumptions, function independence, long term security and parameterization discussed above make hash based signatures an ideal candidate for implementation in several IoT scenarios. In the following, we present current hash based signing schemes (Section 2), and discuss the main challenges that need to be overcome before they can be adopted as the mainstream signing solution (Section 3).

2. HASH-BASED SIGNATURES

The basic design idea of all hash-based signatures schemes is to combine many one-time signature key pairs into a single structure using a hash tree. Hash trees are a hierarchical data structure that was proposed [14] and patented (in 1982) by Merkle [13], sometimes referred to as "Merkle tree". In a hash tree, every leaf node is labelled with the hash of a data block, and every non-leaf node is labelled with the hash of the labels of its child nodes.

One-time signatures (OTS) are the basic building block of hash-based digital signatures. One-time signatures were proposed for the first time by Leslie Lamport in 1979 [10], and derive their name from the property that each signature key pair can be used only once. Most one-time signature schemes rely on one-way functions, typically hash functions, for their security. In this sense, one-time signature schemes have similar characteristic to hash-based signature schemes. For instance, the first such scheme, proposed by Lamport in the same technical report [10], relies exclusively on the security of the underlying hash function. In order to sign a message with a Lamport signature, a hash of the message is produced. Given a hash function with output length k-bits, the private key consists of k pairs of random numbers of the same length, while the public key is the hash of all the $2k$ numbers selected as private key. The message is signed as follows: for each bit in the message hash, if the bit is 0 we select the first number in the corresponding pair in the private key, if the bit is 1 we select the second. The resulting selection of k random number is the message signature, which can be verified by hashing the message, as well as each number composing the signature, and comparing it to the hash in the public key corresponding to the message hash bit value. As evident, the entire construction is based and relies on the chosen hash function. Notable examples of one-time signature schemes also include Winternitz's OTS [2], or, more recently, W-OTS$^+$ [7].

The single-use nature of one-time signature schemes makes them impractical in real-world scenarios. Hash-based signatures solve this issue by combining a large number of one-time signature key pairs into a single structure, and constructing aggregated public and private keys from the one-time key pairs. Ralph Merkle proposed the first such scheme in 1989 [15], using a hash tree structure to combine the one-time keys. The tree uses the same hash function used by the OTS. The node at the top of the tree acts as a *global public key*. To authenticate the relation of a one-time public key to the global public key, signatures store an *authentication path*, which is the sequence of tree nodes from the one-time public key to the tree's top. The *global private key* can be constructed in a number of ways. A simple solution could be to concatenate all one-time private keys, but this would result in either a reduced number of OTS key pairs, or a very large global private key. More efficiently, a deterministic pseudorandom number generator (PNRG) can be used, following Winternitz's W-OTS construction [7]. Starting from an initial seed value, which acts as private key, both successive seeds and one-time secret keys are derived in a chain through the PRNG. This construction also provides forward secrecy, but the chain structure is inherently stateful (see Section 3). A scheme provides forward secrecy if an attacker cannot learn information about formerly used signature keys by getting hold of the current private key. Forward secrecy can be an important feature in a Internet of Things, in particular in setting where devices can be stolen, compromised or tampered with. This is a more prominent risk in urban or outdoor scenarios, where the physical security of the device cannot be guaranteed.

An efficiency limitation of the original Merkle construction is related to the hash tree height. In general, the tree must have height n in order to generate 2^n OTS. Multi Tree XMSS (styled by the authors XMSS^{MT}) [9], an improvement over the Extended Merkle Signature Scheme by Buchmann et al. [3], solved this issue by using multiple tree layers, that allow combining large numbers of OTS key pairs into a single structure.

The post-quantum security of hash-based signatures promoted research into practical schemes and their implementation. The proposed implementations have also been evaluated against side channel attacks. In particular, hash-based signatures schemes have vulnerabilities against hardware fault attacks, both in the case of natural and malicious faults. In [16], Mozaffari-Kermani et al. assess and benchmark constructions for stateless hash-based signatures on application-specific integrated circuit (ASIC). Using novel fault diagnosis methods, they propose an implementation approach that makes such hash-based constructions more reliable against natural faults, and helps protecting them against malicious faults. Similarly to the signature schemes they aim to protect, their approach is highly parameterized, and can be tailored to the resources available and for different reliability objectives.

On top of the main characteristics of hash-based signatures we presented in the introduction, modern schemes add several efficiency and security improvements such as forward secrecy and fault-attack resistance. Mainly presented as a solution to post-quantum security, we believe hash-based signatures have now reached the necessary maturity to be used in real-world applications, and in particular in a setting where their features are most useful, such as the diverse Internet of Things ecosystem. In the next section, we analyse the few main remaining challenges to widespread adoption.

3. CHALLENGES

As highlighted by Denis Butin in the article *Hash-Based Signatures: State of Play* [4], a number of challenges must be overcome before hash-based signatures can find widespread application. Butin mentions, in particular, the issues of statefulness and standardization, which are both relevant to the Internet of Things setting. In the following, we discuss progress on these topics by the cryptographic community.

Statefulness derives from the use of one-time signature key pairs. As security depends on the single, non-repeated use of each one-time key, tracking which one-time signing pairs have already been used is crucial. If one-time signing keys are used sequentially, an index and counter value must be stored in the global secret key to indicate the order in which keys can be used. Size requirements for the index depend on the tree structure, however they can be as little as 4-bytes in XMSS case [3]. The issue of state management has been recently addressed by McGrew et al. [12], who propose a hybrid stateless/stateful scheme. Stateless hash-based signature schemes have also been proposed, most notably SPHINCS by Bernstein et al. [1], and its variant SPHINCS-Simpira [6]. While such schemes were known to be possible in theory, SPHINCS was the first practical stateless scheme, achieving the level of efficiency needed for actual implementation. SPHINCS can sign hundreds of messages per second on a modern CPU, using parameters that provide 2^{128} security against quantum attacks. The figure was further improved by the optimized variant SPHINCS-Simpira.

Standardization of hash-based signatures by a recognized body such as NIST would also be beneficial to their adoption. In general, standardized schemes enjoy broader adoption; and the additional scrutiny of the schemes during the standardization process reinforces confidence in the security of the scheme. Hash based functions are currently being considered by governmental and international bodies. In particular, IETF is considering both XMSS and the Leighton-Micali schemes for standardization [11, 8].

Butin also argues that the numerous parameters that characterize hash-based signature schemes opens the way for insecure implementation choices by non-experts in the absence of guidelines. While we agree that recommended parameters should be provided by the cryptographic community, we also believe that the ability to customize signing speed and key size depending on the application scenario is a crucial asset. The flexibility and potential for case-by-case trade-offs will open the way to application in the diverse and constrained reality of the vast majority of IoT devices.

4. CONCLUSIONS

The aim of this position paper is to make the case for wider deployment of hash-based signatures in the Internet of Things. We believe that the simplicity of hash-based signature schemes, which are built and rely only on hash functions, streamlines implementation in an environment as diverse as IoT. The high level of customization and parameterization featured by hash-based signatures also facilitates deployment on resource constrained devices. Finally, hash-based signatures are future proof, thanks to their hash function-agnostic nature and quantum computing resistance.

5. REFERENCES

[1] D. J. Bernstein, D. Hopwood, A. Hülsing, T. Lange, R. Niederhagen, L. Papachristodoulou, M. Schneider, P. Schwabe, and Z. Wilcox-O'Hearn. SPHINCS: practical stateless hash-based signatures. In E. Oswald and M. Fischlin, editors, *Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I*, vol. 9056 of *Lecture Notes in Computer Science*, pp. 368–397. Springer, 2015.

[2] J. A. Buchmann, E. Dahmen, S. Ereth, A. Hülsing, and M. Rückert. On the security of the winternitz one-time signature scheme. *IJACT*, 3(1):84–96, 2013.

[3] J. A. Buchmann, E. Dahmen, and A. Hülsing. XMSS - A practical forward secure signature scheme based on minimal security assumptions. In B. Yang, editor, *Post-Quantum Cryptography - 4th International Workshop, PQCrypto 2011, Taipei, Taiwan, November 29 - December 2, 2011. Proceedings*, vol. 7071 of *Lecture Notes in Computer Science*, pp. 117–129. Springer, 2011.

[4] D. Butin. Hash-based signatures: State of play. *IEEE Security & Privacy*, 15(4):37–43, 2017.

[5] C. Cheng, R. Lu, A. Petzoldt, and T. Takagi. Securing the internet of things in a quantum world. *IEEE Communications Magazine*, 55(2):116–120, 2017.

[6] S. Gueron and N. Mouha. SPHINCS-Simpira: Fast stateless hash-based signatures with post-quantum security. *IACR Cryptology ePrint Archive*, 2017:645, 2017.

[7] A. Hülsing. W-OTS+ - shorter signatures for hash-based signature schemes. In A. Youssef, A. Nitaj, and A. E. Hassanien, editors, *Progress in Cryptology - AFRICACRYPT 2013, 6th International Conference on Cryptology in Africa, Cairo, Egypt, June 22-24, 2013. Proceedings*, vol. 7918 of *Lecture Notes in Computer Science*, pp. 173–188. Springer, 2013.

[8] A. Hülsing. Internet-draft: Xmss: Extended hash-based signatures. Technical report, Internet Engineering Task Force, 2017.

[9] A. Hülsing, L. Rausch, and J. A. Buchmann. Optimal parameters for XMSS MT. In A. Cuzzocrea, C. Kittl, D. E. Simos, E. R. Weippl, and L. Xu, editors, *Security Engineering and Intelligence Informatics - CD-ARES 2013 Workshops: MoCySEn and SeCIHD, Regensburg, Germany, September 2-6, 2013. Proceedings*, vol. 8128 of *Lecture Notes in Computer Science*, pp. 194–208. Springer, 2013.

[10] L. Lamport. Constructing digital signatures from a one-way function. Technical report, CSL-98, SRI International Computer Science Laboratory, Palo Alto (CA, USA), October 1979.

[11] D. McGrew, M. Curcio, and S. Fluhrer. Internet-draft: Hash-based signatures. Technical report, Internet Engineering Task Force, 2017.

[12] D. A. McGrew, P. Kampanakis, S. R. Fluhrer, S. Gazdag, D. Butin, and J. A. Buchmann. State management for hash-based signatures. In L. Chen, D. A. McGrew, and C. J. Mitchell, editors, *Security Standardisation Research - Third International*

Conference, SSR 2016, Gaithersburg, MD, USA, December 5-6, 2016, Proceedings, vol. 10074 of *Lecture Notes in Computer Science*, pp. 244–260. Springer, 2016.

[13] R. C. Merkle. Method of providing digital signatures, Jan 1982. US Patent 4309569, assigned to The Board Of Trustees Of The Leland Stanford Junior University.

[14] R. C. Merkle. A digital signature based on a conventional encryption function. In C. Pomerance, editor, *Advances in Cryptology - CRYPTO '87, A Conference on the Theory and Applications of Cryptographic Techniques, Santa Barbara, California, USA, August 16-20, 1987, Proceedings*, vol. 293 of *Lecture Notes in Computer Science*, pp. 369–378. Springer, 1987.

[15] R. C. Merkle. A certified digital signature. In G. Brassard, editor, *Advances in Cryptology - CRYPTO '89, 9th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 1989, Proceedings*, vol. 435 of *Lecture Notes in Computer Science*, pp. 218–238. Springer, 1989.

[16] M. Mozaffari-Kermani, R. Azarderakhsh, and A. Aghaie. Fault detection architectures for post-quantum cryptographic stateless hash-based secure signatures benchmarked on ASIC. *ACM Trans. Embedded Comput. Syst.*, 16(2):59:1–59:19, 2017.

[17] P. W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *35th Annual Symposium on Foundations of Computer Science, Santa Fe, New Mexico, USA, 20-22 November 1994*, pp. 124–134. IEEE Computer Society, 1994.