Graduate Program in Computer Science, Universidade Federal de Santa Catarina
INE410111 (Research Methodology in Computer Science)

Gustavo Zambonin

Optimizing the Winternitz Digital Signature Scheme with Message Randomizers

Digital signature schemes are widely used in situations requiring secure and tamper-free communication, some of which are software distribution and communications over computer networks. Predominantly used are schemes in which the underlying security argument is derived from computational hardness assumptions of problems in number theory, such as integer factorization discrete logarithm. However, with the advent of quantum computers, these problems can be solved more efficiently with the aid of Shor's algorithm [Sho97]. Ergo, such schemes will become fragile and may no longer guarantee properties required for digital signatures. The alternative is to use post-quantum cryptography, that is, algorithms that are thought to be resistant against such techniques.

There are various strategies proposed in the literature designed to produce quantum-resilient digital signatures, making use of concepts such as coding theory, lattice structures, multivariate polynomials over finite fields and cryptographic hash functions. In special, for the latter option, the robust flexibility and abundant availability of these functions in all kinds of computational systems make hash-based digital signature schemes potential candidates to replace traditional schemes. Additionally, it has been shown that one-way functions (the theoretical foundations of a hash function) are the only constructions needed to build a secure digital signature scheme [Rom90]. These reasons are strong indicators that hash-based signature schemes are presumably safe, and extremely fast in practice.

The idea of using only hashes to sign digital messages is not new. Lamport proposed [Lam79] a very simple and secure scheme to generate and verify digital signatures by the end of the seventies. It considers a pair of pseudorandom words as the private key and their hashes as the public key. The signer signs a single bit of information by choosing to distribute one string from the private key, on whether the bit is 0 or 1, as the signature. The verifier then computes the hash of this string, comparing it with part of the public key. By extending this idea to sign messages of arbitrary sizes, some drawbacks emerge, such as large sizes for key pairs and signatures.

These obstacles have been the subject of research and several improvements have been proposed since the publication of the initial design. Perhaps the most promising method is the Winternitz one time signature scheme (Wots) due to Merkle [Mer89]. This scheme is a generalization of the Lamport scheme. Unlike its predecessor, Wots allows more than one bit to be signed simultaneously through the parameter w, decreasing the size of key pairs and signatures. In fact, the lower cost of the key has been replaced with a higher processing cost, since the total number of hashes to sign a document and verify a signature depends on this parameter.

Various hash-based signature schemes have been proposed based on, or using Wots as part of the scheme. By way of illustration, organizations such as the U.S. National Institute of Standards and Technology (NIST) and the Internet Research Task Force (IRTF) have shown great interest in the research and standardization of these algorithms. The SPHINCS+ proposal [BDE+17], a variant of [BHH+15] that reduces the signature size and overall execution time, was submitted to NIST as a candidate for this process. Besides, there has been continuous activity on the development of informational documents from the IRTF [HBG+18, MCF18], featuring variant schemes derived from Wots.

Observe that the aforementioned costs for signature generation and verification are not distributed evenly, since they are derived from the result of the application of the fingerprint function to a message. Hence, these can be tailored to a faster signature generation or verification by carefully choosing a message derived from the original. We believe that the cost difference between these steps is not exploited to fit specific needs. Often, signatures are generated only once on a targeted device,

which can be properly configured to accommodate the required resources. However, the resources available for the signature verification are unlikely to be predictable in advance, since this step can be performed by any other kind of devices. For this reason, in practice, it is common to choose parameters that make it easier for a third party to verify signatures (*e.g.* the use of the public exponent 65,537 of the RSA signature scheme). Conversely, there may exist devices with constraints for signature generation.

This situation is no different with hash-based signature schemes. Several papers proposed in the literature aim to improve the performance of the verification step for WOTS, such as [CYK16, MCF18, SV08]. While these works modify the structure of the Winternitz scheme, our main proposal consists of a pre-processing of the message, keeping the scheme intact. Another advantage of our scheme is the possibility of using larger values for the parameter w, substantially reducing the size of the WOTS signature. Furthermore, these proposals focus only on the optimization of the signature verification step, whereas our method also works for hastening the creation of signatures.

We propose two methods to reduce costs for the signature generation or verification steps in WOTS. Our first method changes the checksum computation slightly, by padding unused bits with ones in the place of zeros. This can only be used to improve signature verification run times, while padding with zeros is already optimal for signature generation. Our second and main approach is based on [SV08], where we append a cryptographic nonce to a document to be signed and hash it. We repeat the process and search for hash outputs that can optimize signature generation or verification. In fact, by doing this, we do not change the underlying WOTS algorithm. We propose a fixed amount of operations before the signature is generated, so that the chosen step can be computed much faster. This is actually a trade-off choice, where improving one step results in more computations for the other. However, there is always an additional fixed cost to the signature generation. Both proposals can be applied independently or together for better results.

References

[BDE+17] D. J. Bernstein, C. Dobraunig, M. Eichlseder, S. Fluhrer, S.-L. Gazdag, A. Hülsing, P. Kampanakis, S. Kölbl, T. Lange, M. M. Lauridsen, F. Mendel, R. Niederhagen, C. Rechberger, J. Rijneveld, and P. Schwabe. SPHINCS$^+$ – Submission to the NIST post-quantum project, December 2017.

[BHH+15] 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*, volume 9056 of *Lecture Notes in Computer Science*, pages 368–397, April 2015.

[CYK16] J. P. Cruz, Y. Yatani, and Y. Kaji. Constant-sum fingerprinting for Winternitz one-time signature. In *2016 International Symposium on Information Theory and Its Applications (ISITA)*, pages 703–707, October 2016.

[HBG+18] A. Hülsing, D. Butin, S.-L. Gazdag, J. Rijneveld, and A. Mohaisen. XMSS: Extended Hash-Based Signatures. Request for Comments 8391, Internet Engineering Task Force, May 2018.

[Lam79] L. Lamport. Constructing digital signatures from a one-way function. Technical Report CSL-98, SRI International Palo Alto, October 1979.

[MCF18] D. A. McGrew, M. Curcio, and S. Fluhrer. Hash-Based Signatures. Internet-Draft draft-mcgrew-hash-sigs-11, Internet Engineering Task Force, April 2018. Work in Progress.

[Mer89] R. C. Merkle. A Certified Digital Signature. In G. Brassard, editor, *Advances in Cryptology – CRYPTO '89*, volume 435 of *Lecture Notes in Computer Science*, pages 218–238, August 1989.

[Rom90] J. Rompel. One-way Functions Are Necessary and Sufficient for Secure Signatures. In H. Ortiz, editor, *Proceedings of the Twenty-second Annual ACM Symposium on Theory of Computing*, pages 387–394, May 1990.

[Sho97] P. W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*, 26(5):1484–1509, October 1997.

[SV08] R. Steinwandt and V. I. Villányi. A one-time signature using run-length encoding. *Information Processing Letters*, 108(4):179–185, October 2008.