The Journal of Open Source Software

LibSWIFFT - A fast C/C++ Library for the SWIFFT Secure Homomorphic Hash Function

Yaron Gvili[1]

1 Gvili Tech Ltd

DOI: 10.21105/joss.03040

Software

- Review
- Repository
- Archive

Editor: Daniel S. Katz

Reviewers:

- @gcdeshpande
- @jarrah42
- @henrykironde

Submitted: 14 January 2021
Published: 10 April 2021

Summary

LibSWIFFT is an open-source, production-ready C/C++ library providing SWIFFT, one of the fastest available secure hash functions that is also collision-resistant. SWIFFT also facilitates post-quantum digital signature schemes and zero-knowledge proofs of knowledge of a preimage (ZKPoKP). LibSWIFFT is optimized for short blocks of input and runs at a rate of less than 5 cycles/byte single-threaded on a modern commodity computer with AVX2. Other software providing SWIFFT, which are not claiming production-readiness as LibSWIFFT is, are the original implementation by the authors of SWIFFT (Micciancio, 2016) and the SWIFFT 8-bit (Karati & Safavi-Naini, 2018b) and 16-bit (Karati & Safavi-Naini, 2018a) AVX2 implementations for the multi-signature scheme K2SN-MSS (Karati & Safavi-Naini, 2019).

LibSWIFFT is currently intended to be used by cryptography researchers and developers. It provides clean, easy-to-use C/C++ APIs with high-performance implementations and is well-tested and well-documented. Other available implementations of the SWIFFT function do not provide all these benefits. For further details, the reader is referred to the official LibSWIFFT repository (Gvili Tech Ltd, 2021).

Statement of Need

LibSWIFFT implements the SWIFFT (Lyubashevsky et al., 2008) secure homomorphic hash function useful in constructing post-quantum protocols – ones that are resistant to attacks utilizing quantum computers. Such protocols are relevant today due to recent advances in quantum computing technology. In late 2017, NIST started a process for standardizing post-quantum cryptography (National Institute of Standards and Technology, 2017), suggesting that it believes it may not be too long before a practical quantum-computer that threatens critical security standards (including Internet ones) based on classical cryptography will become a reality. Consequently, post-quantum cryptography is becoming more relevant today and perhaps even urgent to develop.

Acknowledgements

LibSWIFFT was developed with reference to the SWIFFTX (Arbitman et al., 2008) submission to the NIST SHA-3 competition in 2008.

References

Arbitman, Y., Dogon, G., Lyubashevsky, V., Micciancio, D., Peikert, C., & Rosen, A. (2008). *SWIFFTX: A proposal for the SHA-3 standard*.

Gvili Tech Ltd. (2021). *LibSWIFFT - a fast c/c++ library for the SWIFFT secure homomorphic hash function*. https://github.com/gvilitechltd/LibSWIFFT

Karati, S., & Safavi-Naini, R. (2018a). *K2SN-MSS swifft16*. https://github.com/anon1985/K2SN-MSS/tree/master/swifft16

Karati, S., & Safavi-Naini, R. (2018b). *Swifft-avx2-8*. https://github.com/anon1985/Swifft-avx2-8

Karati, S., & Safavi-Naini, R. (2019). *K2SN-MSS: An efficient post-quantum signature (full version)*. Cryptology ePrint Archive, Report 2019/442.

Lyubashevsky, V., Micciancio, D., Peikert, C., & Rosen, A. (2008). *SWIFFT: A modest proposal for FFT hashing*. 54–72. https://doi.org/10.1007/978-3-540-71039-4_4

Micciancio, D. (2016). *SWIFFT: An efficient lattice-based cryptographic hash function*. https://github.com/micciancio/SWIFFT

National Institute of Standards and Technology. (2017). *Post-quantum cryptography*. https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization