Second round modifications of the lattice-based signature scheme qTESLA

Sedat Akleylek, Erdem Alkim, Paulo S. L. M. Barreto, Nina Bindel, Johannes Buchmann, Edward Eaton, Gus Gutoski, Juliane Krämer, Patrick Longa, Harun Polat, Jefferson E. Ricardini, and Gustavo Zanon

This is the outline of the modifications introduced in the new submission of the lattice-based signature scheme qTESLA to the second round of NIST's post-quantum standardization project.

New parameter sets. qTESLA 's original parameters were chosen provably secure, according to our security proof. This approach is conservative and provides a high-level of assurance. However, it requires larger keys and signature sizes. For added flexibility and efficiency, we include an additional methodology to generate parameter sets, namely, a heuristic approach in which corresponding R-LWE parameters provide an R-LWE instance of a certain hardness, without taking into account the security reduction. This approach features high-speed execution and a small memory footprint while requiring relatively compact keys and signatures. This addition motivates describing qTESLA more generically using $k \geq 1$ R-LWE samples.

In summary, we propose the following parameter sets:

Provably-secure qTESLA ($k \geq 1$ R-LWE samples):

- qTESLA-p-I (NIST's level 1)
- qTESLA-p-III (NIST's level 3)

Heuristic qTESLA ($k = 1$ R-LWE sample):

- qTESLA-I and qTESLA-I-s (NIST's level 1)
- qTESLA-II and qTESLA-II-s (NIST's level 2)
- qTESLA-III and qTESLA-III-s (NIST's level 3)
- qTESLA-V and qTESLA-V-s (NIST's level 5)

- `qTESLA-V-size` and `qTESLA-V-size-s` (NIST's level 5, for size)

The options with `-s` correspond to a variant using a *public key splitting* technique to reduce the public key size (see below).

Additional ring structure. To improve further `qTESLA`'s parameterization flexibility, in addition to using the popular ring $\mathcal{R}_q = \mathbb{Z}_q[x]/\langle \Phi_n(x) \rangle = \mathbb{Z}_q[x]/\langle x^n + 1 \rangle$, with q prime and the dimension n a power of two, we add support for the cyclotomic ring $\mathcal{R}_q = \mathbb{Z}_q[z]/\langle \Phi_{2^\ell 9}(z) \rangle$, with dimension $n = 2^{\ell-1} \cdot 6$. This required small modifications in the rejection bounds of the signature scheme. Parameter sets `qTESLA-II` and `qTESLA-V-size` (and, hence, `qTESLA-II-s` and `qTESLA-V-size-s`) are instantiated in this alternative setting.

Prevention of implementation attacks. In light of recent research that shows the vulnerability of signature schemes such as `qTESLA` and Dilithium [3] to devastating and easy-to-carry out fault attacks (see [1]), we have modified the scheme from a deterministic signature generation to a probabilistic one. The modification includes the use of a fixed-randomness, a fresh random value and the hash of the message to derive the polynomial y. This simple modification fully prevents the fault attack above, prevents fixed-randomness attacks such as [2], and introduces a first layer of protection against side-channel and fault attacks in general. We note that this change does not impact our security reduction.

In addition, the new reference and optimized implementations are written in constant-time, fixing a few issues on this regard in the originally submitted implementations.

Full portability. In this submission, we include a new portable and efficient CDT-based Gaussian sampler that gets by without floating point operations. This new sampler requires integer instructions only, enabling the deployment of key generation on platforms without a floating point unit.

AVX2-optimized implementations. We provide new AVX2-optimized implementations for the parameter sets `qTESLA-I`, `qTESLA-III`, and `qTESLA-V`, and their variants with smaller public keys `qTESLA-I-s`, `qTESLA-III-s`, and `qTESLA-V-s`.

Security reduction in the quantum random oracle model. We have refined our conjecture that is used in the security reduction of `qTESLA`. Moreover, we give a more detailed explanation why the conjecture should hold true for `qTESLA`'s instantiation. In addition, we include a script which can be used to understand the conjecture. The script samples the relevant elements of the ring to try and search for a possible counterexample

to the conjecture. Our experiments support the statement conjectured since no counter example occurs.

Public key splitting. We describe a qTESLA variant that features significantly smaller public keys at the expense of slightly larger signatures. This is achieved using a simplified version of the compression technique proposed in Ducas *et al.* [3]. We showcase the technique with the heuristic parameter sets, but it can be easily extended to the provably-secure case.

Other minor corrections of the implementation and supporting documentation. We have corrected typos throughout the specification document, and provided more efficient implementations of the different internal functions. These changes include

- Improved explanation of the realization of the different functions.
- Updated correctness proof.
- Introduced hash function $\mathsf{G} : \{0,1\}^* \rightarrow \{0,1\}^{512}$ that maps a message to a 512-bit string. See Algorithms 7 and 8.
- Modified expression for hash function H in Algorithms 7 and 8 to match function definition in Algorithm 13.

References

[1] Leon Groot Bruinderink and Peter Pessl. Differential fault attacks on deterministic lattice signatures. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2018(3):21–43, 2018. https://tches.iacr.org/index.php/TCHES/article/view/7267.

[2] H.M. Cantero, S. Peter, Bushing, and Segher. Console hacking 2010 – PS3 epic fail. 27th Chaos Communication Congress, 2010. https://www.cs.cmu.edu/~dst/GeoHot/1780_27c3_console_hacking_2010.pdf.

[3] Vadim Lyubashevsky, Leo Ducas, Eike Kiltz, Tancrede Lepoint, Peter Schwabe, Gregor Seiler, and Damien Stehle. Crystals-dilithium. Technical report, National Institute of Standards and Technology, 2017. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions.