This is Not an Attack on Wave

Thomas Debris-Alazard[1,2], Nicolas Sendrier[2], and Jean-Pierre Tillich[2]

[1] Sorbonne Universités, UPMC Univ Paris 06
[2] Inria, Paris
{thomas.debris,nicolas.sendrier,jean-pierre.tillich}@inria.fr

Abstract. Very recently, a preprint "Cryptanalysis of the Wave Signature Scheme", eprint 2018/1111, appeared claiming to break Wave "Wave: A New Code-Based Signature Scheme", eprint 2018/996. We explain here why this claim is incorrect.

Wave [3] is a new digital signature scheme which is proven EUF-CMA secure under two computational assumptions:

1. Hardness of multiple target decoding, DOOM [5],
2. Indistinguishability of generalized (U,U+V) codes.

The proof uses the GPV approach [4]. In particular it is proven in Theorem 1 of [3] that the Wave signature function produces words uniformly distributed in S_w the set of ternary words of length n and Hamming weight exactly w. With this property, no amount of signatures, coming from a genuine Wave signature oracle, can reveal any information on the secret.

We will refer to *rejection sampling* to describe the features introduced in Algorithm 3 and 4 of [3], and which ensure the uniform distribution of the signatures.

What the preprint [1] basically does is:

(1) implement a degraded Wave scheme by stripping off its rejection sampling,
(2) collect signatures produced by the degraded signature function,
(3) recover the secret key from the collected signatures,
(4) in addition, there is a claim in the paragraph "*** Update" p. 3 (version 3) that the attack does not depend on the rejection sampling.

The claim (4) is incorrect since the attack only exploits statistical correlations between pairs of positions in signatures. This bias of $(U, U+V)$ decoders was previously identified (see [2] p. 23, §5.1), and is provably removed in Wave by rejection sampling.

Ignoring the features which remove the bias, and then using this bias to recover the secret key is pointless and is by no mean a valid attack on Wave.

References

1. Paulo S. L. M. Barreto and Edoardo Persichetti. Cryptanalysis of the wave signature scheme. Cryptology ePrint Archive, Report 2018/1111, 2018. https://eprint.iacr.org/2018/1111.
2. Thomas Debris-Alazard, Nicolas Sendrier, and Jean-Pierre Tillich. A new signature scheme based on $(U|U+V)$ codes. preprint, June 2017. arXiv:1706.08065v1.
3. Thomas Debris-Alazard, Nicolas Sendrier, and Jean-Pierre Tillich. Wave: A new code-based signature scheme. Cryptology ePrint Archive, Report 2018/996, October 2018. https://eprint.iacr.org/2018/996.
4. Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the fortieth annual ACM symposium on Theory of computing*, pages 197–206. ACM, 2008.
5. Nicolas Sendrier. Decoding one out of many. In *Post-Quantum Cryptography 2011*, volume 7071 of *LNCS*, pages 51–67, 2011.