From: Lorenz Panny <l.s.panny@tue.nl>
Sent: Monday, July 17, 2023 2:04 PM
To: pqc-comments
Cc: pqc-forum
Subject: Round 1 (Additional Signatures) OFFICIAL COMMENT: Xifrat1-Sign.I

Dear all,

here's a Sage script that quickly computes secret keys from public keys in the Xifrat1-Sign.I submission:

https://yx7.cc/files/xifrat-attack.sage

On a 24-core machine, one run of the script takes about 4 minutes.
It currently hardcodes the public key from the first KAT.

The attack is based on the machinery from ePrint 2021/583: We can rewrite the quasigroup multiplication x*y as C + Ax + By, where + is an abelian group and A,B are commuting automorphisms. Since all mixing functions used in the construction are affine-linear maps with respect to this +, the system connecting the secret with the public key is linear in the secrets, and we can reduce to linear algebra. In this particular case, the group is actually isomorphic to $\mathbb{F}_2^4$, rendering the implementation of the attack particularly easy, but the general case works similarly.

Best,
Lorenz