
From: pqc-forum@list.nist.gov on behalf of Wessel van Woerden
<wesselvanwoerden@gmail.com>
Sent: Thursday, July 20, 2023 7:34 AM
To: pqc-forum
Cc: Felicitas Hörmann
Subject: [pqc-forum] Round 1 (Additional Signatures) OFFICIAL COMMENT: FuLeeca

Dear FuLeeca Team,

The FuLeeca scheme is a hash-and-sign scheme based on quasi-cyclic codes with the Lee metric. The secret key consists of a quasi-cyclic generator matrix G of a length n and dimension $n/2$ linear code over F_p with $p=65521$.

Signatures are codewords of small Lee weight, and messages are bound to this by some sort of parity-count condition. Following the specification we work with row vectors here. Looking at the signing procedure each signature (low-weight codeword) v is in fact a small linear combination of the rows of G , i.e., $v = x * G \bmod p$ for some small integer vector x .

We observe however experimentally that with the current parameters the coefficients of $x * G$ (without modulo) are already well within the range $[-(p-1)/2, (p-1)/2]$. E.g., experimentally the coefficients of v are in the range $[-5000, 5000]$ for all the three variants. This implies that we have a real equality $v = x * G$, and therefore, signatures leak the \mathbb{Z} -span of (the rows of) G , which thus reveals the rank $n/2$ lattice $L(G)$ in \mathbb{Z}^n . In fact, it is enough to only consider the first $n/2$ coefficients of each vector of v , and therefore recover the lattice $L(G')$ where $G=(G' | G'')$.

We thus ignore the Lee metric and move to lattices with the standard Euclidean metric. The $n/2$ shortest vectors of the lattice $L(G')$ are precisely the rows of the secret key G' . The gap between the norm of these shortest vectors, and the Gaussian Heuristic of the lattice $L(G')$ is of order $O(\sqrt{n})$, i.e., on a concrete example generated by the FuLeeca1 parameters with $n/2=659$ we obtain $gh/\lambda_1=4.722$.

So the recovery of G' is an unusual SVP instance in an $n/2$ dimensional lattice with gap $O(\sqrt{n})$. Asymptotically this can be broken by BKZ with blocksize $\beta=n/4+o(n)$. Concretely, for the FuLeeca1 parameters a quick estimate gives that BKZ recovers G' with blocksize less than 310, which is significantly below the security level 1. We expect a similar reduction in security for the other variants.

Some additional comments:

- The signature vectors themselves are quite short (shorter than what one would get by BKZ-310), which could reduce the blocksize even further.
- The lattice $L(G')$ is in fact a circulant lattice. Firstly, due to this structure 2 signatures can be enough to recover the full lattice span. Secondly, this extra structure might make the attack classically sub-exponential $\exp(O(\sqrt{n}))$ or quantum-polynomial-time by known ideal-lattice attacks.
- Given the leakage of the signature procedure, and the similarity of the Lee metric to the Euclidean one, we expect a more advanced learning attack à la [Nguyen-Regev,2006] on GGH to also apply to this scheme.

Best regards,

Felicitas Hörmann and Wessel van Woerden

--

You received this message because you are subscribed to the Google Groups "pqc-forum" group.

