From: Kevin Carrier <kevin.carrier@ensea.fr>
Sent: Monday, July 31, 2023 9:50 AM
To: pqc-comments
Cc: pqc-forum; Jean-Pierre Tillich
Subject: Round 1 (Additional Signatures) OFFICIAL COMMENT: SDitH
Attachments: Peters_analysis_for_SDitH.pdf

Dear SDiTH, dear all,

We wish to report here that the security level of SDitH has been underestimated *at least* by about 1 to 9 bits for the parameters given in the specification document.

The reason why there is an improved attack:

A key recovery attack on SDitH is as hard as solving the d-split Syndrome Decoding problem (SD(d)). Unfortunately, the specification document of SDitH does not take into account that for the regime of parameters which is chosen, SD(d) has actually several solutions: between 31 and 748 depending on the parameters. The security analysis provided in Section 7.1 of the SDitH submission ignores this point.

The gain we report on the parameters is however less than this number of solutions because the complexity of SD(d) has been obtained in the specification document by a reduction of standard syndrome decoding (this corresponds to SD(1)) to SD(d)). This reduction is not tight in the case at hand, when there are several solutions. We wish to mention however that our complexity claims correspond to an actual attack adapting Christiane Peters' ISD [1] to the d-split problem where the complexity is computed with a formula making similar assumptions as the formula for the ISD cost given p.50 of the specification document. Full details are given here.

Results :

The complexity of solving SD(d) which is instrumental in estimating the security of SDitH is estimated apparently in the specification document of SDitH when d>1 by relying on (a) a lower bound on the complexity T(d) for solving SD(d) relying on Theorem 6.1 p.48 (b) an estimation of the complexity T(1) of the best algorithm for solving SD(1). Note that this lower bound is not tight when there is more than one solution to the SD(1) problem.

For each set of parameters of SDitH, we give
(i) the target bit security,
(ii) the estimated lower bound on T(d) following from Theorem 6.1 p.48 and the estimated cost for solving SD(1) (end of Section 7.1) in the specification document of SDitH,
(iii) the actual complexity of Peters' ISD adaptation to the SD(d) problem taking into account that there are multiple solutions.

SDitH_L1_gf256: (i) 143 bits, (ii) T(d)>=143.5 bits and T(1)=143.5 bits, (iii) 134.6 bits.
SDitH_L1_gf251: (i) 143 bits, (ii) T(d)>=143.4 bits and T(1)=143.4 bits, (iii) 133.9 bits.
SDitH_L3_gf256: (i) 207 bits, (ii) T(d)>=207.7 bits and T(1)=211.2 bits, (iii) 206.2 bits.
SDitH_L3_gf251: (i) 207 bits, (ii) T(d)>=207.6 bits and T(1)=211.1 bits, (iii) 205.0 bits.
SDitH_L5_gf256: (i) 272 bits, (ii) T(d)>=272.3 bits and T(1)=276.0 bits, (iii) 271.3 bits.
SDitH_L5_gf251: (i) 272 bits, (ii) T(d)>=272.3 bits and T(1)=276.0 bits, (iii) 269.8 bits.

Best regards,

Kevin Carrier and Jean-Pierre Tillich

[1] C. Peters. Information-set decoding for linear codes over Fq. In N. Sendrier, editor, The Third International Workshop on Post-Quantum Cryptography, PQCRYPTO 2010, pages 81–94. Springer, Heidelberg, 2010

From: Kevin Carrier <kevin.carrier@ensea.fr>
Sent: Friday, August 4, 2023 1:59 PM
To: pqc-forum; SDitH Consortium
Cc: pqc-comments
Subject: Re: [pqc-forum] Round 1 (Additional Signatures) OFFICIAL COMMENT: SDitH
Attachments: Peters_analysis_for_SDitH.pdf

Dear SDitH consortium,

First, there is indeed a typo in Equations (7) and (8) of our pdf: the factor (q-1)^w is missing. Of course, we have taken this factor into consideration in the results that we give. A corrected version of our draft is available here or in the attached file.

Concerning Theorem 6.1, we do not questions the truth of it. We only say that the inequality given in this theorem is not tight when SD(d) has many solutions. The proof in [FJR22, Appendix A] is essentially based on the probability that an SD(1) problem becomes an SD(d) problem when the positions are randomly permuted. This probability is not binom(n/d,w/d)^d/binom(n,w) but something greater when there is many solutions.

That does not imply a security loss but only that the security is underestimated when using this theorem.

Best regards,

Kévin

> Le 4 août 2023 à 17:38, Matthieu Rivain <matthieu.rivain@cryptoexperts.com> a écrit :
>
> Dear Kevin and Jean-Pierre,
>
> Thank you for your official comment. We acknowledge that our parameter generation script seems to be missing a factor that results in a misestimation of the complexity of traditional attacks (more on this below).
>
> Two aspects are at play here:
> 1) There appears to be multiple solutions in our SD instances, which lower the complexity of the best attack;
> 2) SDitH relies on the d-split variant of Syndrome Decoding.
>
> First of all, it is important to clarify that parameters for Category 1 are *not* based on the d-split variant. To be more precise, such parameters are instead based on the traditional Syndrome Decoding problem (which is the same as d-split with d=1).
>
> Regarding 1):