From: pqc-forum@list.nist.gov on behalf of Hiroki Furue <furue-hiroki261@g.ecc.u-tokyo.ac.jp>
Sent: Monday, August 28, 2023 9:18 PM
To: pqc-forum
Subject: [pqc-forum] Round 1 (Additional Signatures) OFFICIAL COMMENT: VOX

Dear all,

This message argues that the parameters chosen by the designers of VOX have to be revised to satisfy the claimed security level.

In IWSEC 2023, we show that the rectangular MinRank attack proposed for Rainbow by Beullens is applicable to two variants of UOV, MAYO and QR-UOV. In [FI23], we confirmed that the proposed parameters of MAYO and QR-UOV are secure against the rectangular MinRank attack.

We here consider applying the rectangular MinRank attack to VOX. The public and secret keys of VOX are constructed by mixing random quadratic polynomials and UOV polynomials with the quotient ring structure used in QR-UOV. As mentioned in Section 5 in [FI23], for the public key with c*v vinegar-variables, c*o oil-variables, and c*o equations over F_q (c: a factor of the QR structure), we can apply the key recovery attacks on the public key with v vinegar-variables, o oil-variables and c*o equations over F_{q^c} utilizing the QR-structure. After transforming the public key of VOX, we apply the rectangular MinRank attack and recover the oil space by finding a matrix with rank t+v in a space of given v+1 $c*o \times v+o$ matrices.

For the proposed lv1, 3, 5 parameters of VOX, by using the support minors method, we estimate that one vector of the oil space can be recovered by 2^39, 2^42, 2^41 operations, respectively. After obtaining one vector of the oil space over F_{q^c}, we can recover the secret key T and S completely by solving some linear systems.

The reason that our attack can be applied to VOX is that the parameters satisfy t+v<v+o, and thus one has to choose parameters satisfying t>=o to make the scheme secure.

Note that we confirmed that the proposed parameters of QR-UOV and MAYO are secure against this rectangular MinRank attack in [FI23].

Best regards,
Hiroki Furue and Yasuhiko Ikematsu

[FI23] Hiroki Furue and Yasuhiko Ikematsu: A New Security Analysis Against MAYO and QR-UOV Using Rectangular MinRank Attack. IWSEC 2023.
https://link.springer.com/chapter/10.1007/978-3-031-41326-1_6
--

From: pqc-forum@list.nist.gov on behalf of Hao Guo <guoh22@mails.tsinghua.edu.cn>
Sent: Thursday, September 7, 2023 5:00 PM
To: pqc-forum
Cc: Hiroki Furue
Subject: [pqc-forum] Re: Round 1 (Additional Signatures) OFFICIAL COMMENT: VOX

Dear Hiroki, Yasuhiko and all,

We hope to draw your attention to the fact that:

1. The matrix deformation technique described in [FI23] and [INT22] first appeared in [TPD21], where the authors used this trick to perform MinRank attack and break HFEv-.
2. Similar techniques have also been considered in §4.2.4, "MinRank Attack", of TUOV specification file.

Best regards,
Hao Guo

[FI23] Hiroki Furue and Yasuhiko Ikematsu: A New Security Analysis Against MAYO and QR-UOV Using Rectangular MinRank Attack. IWSEC 2023.
https://link.springer.com/chapter/10.1007/978-3-031-41326-1_6
[INT22] Ikematsu, Y., Nakamura, S., Takagi, T.: Recent progress in the security evaluation of multivariate public-key cryptography. IET Inf. Secur. 17(2), 210–226 (2022)
https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/ise2.12092
[TPD21] Tao, C., Petzoldt, A., Ding, J.: Efficient key recovery for all HFE signature variants. In: Malkin, T., Peikert, C. (eds.) CRYPTO 2021.
https://link.springer.com/chapter/10.1007/978-3-030-84242-0_4

在 2023 年 8 月 29 日星期二 UTC+8 09:17:34<Hiroki Furue> 写道：

> Dear all,
>
> This message argues that the parameters chosen by the designers of VOX have to be revised to satisfy the claimed security level.
>
> In IWSEC 2023, we show that the rectangular MinRank attack proposed for Rainbow by Beullens is applicable to two variants of UOV, MAYO and QR-UOV. In [FI23], we confirmed that the proposed parameters of MAYO and QR-UOV are secure against the rectangular MinRank attack.
>
> We here consider applying the rectangular MinRank attack to VOX. The public and secret keys of VOX are constructed by mixing random quadratic polynomials and UOV polynomials with the quotient ring structure used in QR-UOV. As mentioned in Section 5 in [FI23], for the public key with c*v vinegar-variables, c*o oil-variables, and c*o equations over F_q (c: a factor of the QR structure), we can apply the key recovery attacks on the public