From: 王立中 <lcwang@gms.ndhu.edu.tw>
Sent: Friday, January 19, 2024 3:38 AM
To: pqc-comments
Cc: briantseng0320@gmail.com
Subject: Round 1 (Additional Signatures) OFFICIAL COMMENT: SNOVA

Dear all,

We wish to inform you of the revised selection of SNOVA parameters for l=2.

For Security Level I:
(v, o, q, l) = (28, 17, 16, 2) ==> (37, 17, 16, 2)

For Security Level III:
(v, o, q, l) = (43, 25, 16, 2) ==> (56, 25, 16, 2)

For Security Level V:
(v, o, q, l) = (61, 33, 16, 2) ==> (75, 33, 16, 2)

In light of the preprint by Yasuhiko Ikematsu and Rika Akiyama, it has been noted that the SNOVA scheme exhibits a (q, lv, lo) UOV structure concerning key recovery. Consequently, a modification to the security analysis of SNOVA is essential, and the parameters for l=2 do not meet the NIST security level. However, parameters for l=3 and l=4 remain secure, satisfying the v>2o condition. The inadequacy of vinegar variables in the previous parameters for l=2 necessitates an increase to meet security requirements.

Stay tuned for the forthcoming updated security analysis of SNOVA.

Our heartfelt gratitude extends to Yasuhiko Ikematsu and Rika Akiyama for sharing their preprint and insights. Additionally, we appreciate Gilles Macario-Rat for providing us with similar insights.

Best regards,

SNOVA Team

From: pqc-forum@list.nist.gov on behalf of Po-En Tseng <briantseng0320@gmail.com>
Sent: Monday, January 22, 2024 1:20 AM
To: pqc-forum
Subject: [pqc-forum] Round 1 (Additional Signatures) OFFICIAL COMMENT: SNOVA

Dear all,

We wish to inform you of the revised selection of SNOVA parameters for l=2.

For Security Level I:
(v, o, q, l) = (28, 17, 16, 2) ==> (37, 17, 16, 2)

For Security Level III:
(v, o, q, l) = (43, 25, 16, 2) ==> (56, 25, 16, 2)

For Security Level V:
(v, o, q, l) = (61, 33, 16, 2) ==> (75, 33, 16, 2)

In light of the preprint by Yasuhiko Ikematsu and Rika Akiyama, it has been noted that the SNOVA scheme exhibits a (q, lv, lo) UOV structure concerning key recovery. Consequently, a modification to the security analysis of SNOVA is essential, and the parameters for l=2 do not meet the NIST security level. However, parameters for l=3 and l=4 remain secure, satisfying the v>2o condition. The inadequacy of vinegar variables in the previous parameters for l=2 necessitates an increase to meet security requirements.

Stay tuned for the forthcoming updated security analysis of SNOVA.

Our heartfelt gratitude extends to Yasuhiko Ikematsu and Rika Akiyama for sharing their preprint and insights. Additionally, we appreciate Gilles Macario-Rat for providing us with similar insights.

Best regards,

SNOVA Team

--

From: pqc-forum@list.nist.gov on behalf of Ikematsu Yasuhiko <ikematsu.academic@gmail.com>
Sent: Friday, January 26, 2024 8:50 PM
To: pqc-forum
Cc: Po-En Tseng
Subject: [pqc-forum] Re: Round 1 (Additional Signatures) OFFICIAL COMMENT: SNOVA

Dear all,

Our preprint can be found here.
https://eprint.iacr.org/2024/096

Best regards,
Yasuhiko Ikematsu

2024 年 1 月 22 日月曜日 15:19:36 UTC+9 Po-En Tseng:

> Dear all,
>
> We wish to inform you of the revised selection of SNOVA parameters for l=2.
>
> For Security Level I:
> (v, o, q, l) = (28, 17, 16, 2) ==> (37, 17, 16, 2)
>
> For Security Level III:
> (v, o, q, l) = (43, 25, 16, 2) ==> (56, 25, 16, 2)
>
> For Security Level V:
> (v, o, q, l) = (61, 33, 16, 2) ==> (75, 33, 16, 2)
>
> In light of the preprint by Yasuhiko Ikematsu and Rika Akiyama, it has been noted that the SNOVA scheme exhibits a (q, lv, lo) UOV structure concerning key recovery. Consequently, a modification to the security analysis of SNOVA is essential, and the parameters for l=2 do not meet the NIST security level. However, parameters for l=3 and l=4 remain secure, satisfying the v>2o condition. The inadequacy of vinegar variables in the previous parameters for l=2 necessitates an increase to meet security requirements.
>
> Stay tuned for the forthcoming updated security analysis of SNOVA.
>
> Our heartfelt gratitude extends to Yasuhiko Ikematsu and Rika Akiyama for sharing their preprint and insights. Additionally, we appreciate Gilles Macario-Rat for providing us with similar insights.
>
> Best regards,
>
> SNOVA Team

From: pqc-forum@list.nist.gov on behalf of Po-En Tseng <briantseng0320@gmail.com>
Sent: Sunday, February 25, 2024 2:43 AM
To: pqc-forum
Subject: [pqc-forum] Round 1 (Additional Signatures) OFFICIAL COMMENT: SNOVA

Dear all,

The updated security analysis of SNOVA can be found here.
https://eprint.iacr.org/2022/1742

Best regards,

SNOVA Team
--