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
--

From: pqc-forum@list.nist.gov on behalf of Po-En Tseng <briantseng0320@gmail.com>
Sent: Saturday, May 4, 2024 6:48 AM
To: pqc-forum
Subject: [pqc-forum] Round 1 (Additional Signatures) OFFICIAL COMMENT: SNOVA

Dear all,
As a response to the speed comparison of signature scheme [1] in 5th PQC Standardization Conference,
we would like to share our new optimization for SNOVA and the corresponding code will be released on our website next week.

Compared to the source code submitted to NIST, there has been a significant improvement in execution efficiency.

Name	Keygen SSK	Keygen ESK	Sign SSK	Sign ESK	Verify
SNOVA_24_5_4	247467	256603	496390	317756	170479
SNOVA_25_8_3	450951	459304	733121	373797	229952
SNOVA_37_17_2	1354429	1379750	1289486	380242	206442
SNOVA_37_8_4	1696205	1742145	2610319	1191723	562304
SNOVA_49_11_3	2702573	2757368	3639863	1367077	1032828
SNOVA_56_25_2	6841311	6954716	6069886	1060334	677318
SNOVA_60_10_4	5846062	5996723	8205559	3148424	1557695
SNOVA_66_15_3	8826989	8963107	10687544	3334322	2546046
SNOVA_75_33_2	19597559	19882597	16793644	2679056	1588063

The test environment used to generate the numbers in the above table is:
•Intel(R) Core(TM) i7-8565U CPU @ 1.80GHz (Laptop CPU)
•TurboBoost and HyperThreading off
•2048 tests, number is the median (in CPU cycles).

The latest version has received an speed-up to the keygen and the sign functions.
We will continue to update our website with the latest optimization results and code.

All the best,
SNOVA team

[1] Matthias Kannwischer: pqm4: Benchmarking NIST Additional Post-Quantum Signature Schemes on Microcontrollers.

From: pqc-forum@list.nist.gov on behalf of lab pqc <pqclaborg@gmail.com>
Sent: Friday, May 10, 2024 10:16 AM
To: pqc-forum
Cc: Po-En Tseng
Subject: [pqc-forum] Re: Round 1 (Additional Signatures) OFFICIAL COMMENT: SNOVA

Dear All,

I hope this message finds you well. I am pleased to announce that the latest optimized code for the SNOVA post-quantum cryptography digital signature scheme has been updated on GitHub. This update brings some significant improvements and optimizations, which we believe will enhance the security and performance of our signature scheme.

You can find the latest code at the following link: https://github.com/pqclab-zero/SNOVA

Our team remains committed to continuously improving and optimizing our digital signature scheme to provide better security in the post-quantum era. If you have any questions or suggestions, please feel free to contact us anytime.

Thank you once again for your attention and support to our work!

Best Regards,
SNOVA TEAM