Smaller SLH-DSA

September 25th, 2025

Quynh Dang
Cryptographic Technology Group

Tuesday, October 3rd, 2023

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Outline

- **FIPS 205: SLH-DSA**
  - Searches and Evaluations of Smaller SLH-DSA Options
- **The Option for Certificate, Software and Firmware Signings**
  - 2^24 Signatures per Signing Key at Level 1 Security
  - 2^24 Signatures per Signing Key at Level 3 Security
  - 2^24 Signatures per Signing Key at Level 5 Security
- **Is there a strong demand for 2^30 limit options ?**
  - 2^30 Limit with Comparable Signing in FIPS 205 Options
- **2^16-Signature Limit per Key for Certificate Signing ?**
  - 2^16 Limit with Comparable Signing in FIPS 205 Options
  - 2^16 Limit with Slow Sign and Fast Verify Options

Questions/Comments

Our Current Plan

- We plan to standardize 2^24-signature limit **rls128cs1, rls192cs1, rls256cs1**
  - **For certificate, software and firmware signings.**

- We need more input from the community about the demand of 2^30 and 2^16 limits
  - Let us know if the 2^24 options above would have unacceptable performance for your systems.

- We don’t plan to standardize them now:
  - Lower limits come with higher security risks when misuse happens
  - Minimize the number of parameter sets

Let us know if you think differently

FIPS 205

- FIPS 205 [**1**] has12 parameter sets.
- The smallest one: **SLH-DSA-SHA2-128s**
  - Signature is 7,856 bytes.
  - Signing takes 2.2 million hash calls, about 644,740,090 cycles, about 0.2 seconds [**2**].
    on a 3.1 GHz Intel Xeon E3-1220 CPU (Haswell)
- Too large for many applications.
- 2^64 signatures per key not needed for many use cases.
- Reduce the number of signature limit and/or increasing the signing time leads to smaller signature and/or faster verify options.

➢ We plan to standardize new parameter sets.

[1] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.205.pdf
[2] https://sphincs.org/data/sphincs+-r3.1-specification.pdf

Searches and Evaluations of Smaller SLH-DSA Options

- "A note on SPHINCS+ parameter sets" by Stefan Kölbl and Jade Philipoom [3].
- "Smaller SPHINCS$^+$" by Scott Fluhrer and Quynh Dang [4].
- Work done by Chris Fenner, his team, others and NIST, see the discussion [5].

[3] https://csrc.nist.gov/csrc/media/Events/2024/fifth-pqc-standardization-conference/documents/papers/a-note-on-sphincs-plus-parameter-sets.pdf

[4] https://eprint.iacr.org/archive/2024/018/1737032157.pdf

[5] https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/MW4PR09MB10059280AD24C92B4EA8C0E96F3C92%40MW4PR09MB10059.namprd09.prod.outlook.com?utm_medium=email&utm_source=footer

The Option for Certificate, Software and Firmware Signings

- For certificate, software and firmware signings, generally fast verify is more important than fast signing.

- A small signature, fast verify and conservative in security one seems ideal.

2^24 Signatures per Signing Key at Level 1 Security

Some small signature options at 2^20 and 2^24 limits at Level 1.

Id	n	h	d	h’	a	k	lg(w)	m
Level1-a	16	21	1	21	25	6	3	22
Level1-b	16	21	1	21	23	6	4	21
rls128cs1	16	22	1	22	24	6	2	21

Note: Level1-b: 128 bits of security at 2^20.

2^24 Signatures per Signing Key at Level 1 Security cont.

Id	Bit-security/#sigs	pk	sig	-bytes -%	Sign in #hashes	Verify in # hashes %	#Sigs at 112 bits
Level1-a	128/2^24	32	3488	-368 -9.54%	1266679808	465 49.5%	26.93
Level1-b	117.97/2^24	32	3216	-640 -16.6%	1329594368	448 44%	25.16
rls128cs1	128/2^24	32	3856	0	1451229184	311	27.25

2^24 Signatures per Signing Key at Level 1 Security cont.

-rls128cs1's signing time ≈ 664 times of the **SLH-DSA-SHA2-128s**' signing time in the normal method.

-The scale reduces to 138 times when the one-time signature tree is cached. If **SLH-DSA-SHA2-128s** takes 0.1 seconds for signing, rls128cs1 would take 13.8 seconds for signing. 2^24 = 16,777,216 would take about 64,312 hours ≈ 2,679.69 days ≈ 223.3 months.

-Best overuse safety among the 3 choices.

Id	Bit-security/#sigs	pk	sig	-bytes -%	Sign in #hashes	Verify in # hashes/%	#Sigs at 112 bits
Level1-a	128/2^24	32	3488	-368 -9.54%	1266679808	465 49.5%	26.93
Level1-b	117.97/2^24	32	3216	-640 -16.6%	1329594368	448 44%	25.16
rls128cs1	128/2^24	32	3856	0	1451229184	311	27.25

2^24 Signatures per Signing Key at Level 3 Security

Id	n	h	d	h’	a	k	lg(w)	m
Level3-a	24	20	1	20	23	9	4	29
Level3-b	24	21	1	21	23	9	4	29
rls192cs1	24	21	1	21	25	9	3	32
Level3-c	24	21	1	21	25	9	2	32
Level3-d	24	21	1	21	23	10	4	32

2^24 Signatures per Signing Key at Level 3 Security cont.

Id	Bit-sec/#sigs	pk	sig	bytes %	sign	Verify %	#Sigs at 128/ 112 Bit-sec
Level3-a	(168.46/2^24), (192/2^20.13)	48	6912	-840 -10.8%	1084227584	647 23%	28.76 30.55
Level3-b	(175.69/2^24), (192/2^21.12)	48	6936	-816 -10.5%	1329594368	648 23%	29.76 31.55
rls192cs1	192/2^24	48	7752	0	1451229184	526	31.77 33.55
Level3-c	192/2^24	48	8568	816 10.5%	1757413376	460 -12.5%	31.77 33.55
Level3-d	192/2^24	48	7512	-240 -3 %	1967128576	672 27.7%	31.19 32.79

Note: "#Sigs at" is # of sigs in power of 2.

Note: Verify is in number of hash calls. "%" is increase or decrease comparing with the target.

2^24 Signatures per Signing Key at Level 5 Security

Id	n	h	d	h’	a	k	lg(w)	m
Level5-a	32	21	1	21	20	14	4	38
Level5-b	32	21	1	21	22	14	4	42
rls256cs1	32	21	1	21	25	12	2	41

2^24 Signatures per Signing Key at Level 5 Security cont.

Id	pk	sig	Size reduction in bytes %	sign	Verify %	Bit-sec/#sigs
Level5-a	64	12256	-2688 -18%	2296381440	854 41.8%	(256/2^20), (192/2^27.17)
Level5-b	64	13152	-1792 -12%	2428502016	882 46.5%	(256/2^24), (192/2^29.26)
rls256cs1	64	14944	0	2327838720	602	(256/2^24), (192/2^29.98)

Is there a strong demand for 2^30 limit options ?

- When each signature is used per update and per recipient and the signing times of the 2^24 limit options are considered not acceptable, then 2^30 limit options with fast enough signing time would be better.

- We urge the community to confirm that such use case is common.

Level 1 2^30 Comparable Signing in FIPS 205

ID	n	h	d	h'	a	k	lg_w	m	Sec cat.	Pk bytes	Sig bytes	% Size	Sign time	Verify time	Sigs at Level 112	Overuse safety
1	16	32	4	8	14	10	6	22	1	32	4464	100%	2066421	3260	33.97	15
2	16	36	6	6	13	10	8	22	1	32	4560	102%	2015987	14008	36.24	75
3	16	30	3	10	13	12	4	25	1	32	4864	108%	2021364	1043	33.10	8

Selection set (128, 112, 2^{30}, 2,200,000)

Note: “sigs at level…” is # of sigs in power of 2.

Level 3 2^30 Comparable Signing in FIPS 205

ID	n	h	d	h'	a	k	lg_w	m	Sec cat.	Pk bytes	Sig bytes	% size	Sign time	Verify time	Sigs at level 128	Overuse safety
1	24	32	4	8	15	14	6	31	3	48	9432	100%	3606513	4614	37.70	207
2	24	30	5	6	15	15	8	33	3	48	9624	102%	3605103	16917	36.36	82
3	24	36	6	6	14	14	8	30	3	48	9672	102%	3244783	20222	40.55	1499
4	24	30	3	10	13	18	4	35	3	48	10464	110%	2955246	1511	35.70	51
5	24	30	3	10	14	17	4	35	3	48	10536	111%	3348463	1514	36.35	81
6	24	36	4	9	15	13	4	31	3	48	10776	114%	2953202	1882	40.92	1937

Selection set (192, 128, 2^{30}, 3,800,000)

Level 5 2^30 Comparable Signing in FIPS 205

ID	n	h	d	h'	a	k	lg_w	m	Sec cat.	Pk bytes	Sig bytes	% size	Sign time	Verify time	Sigs at level 192	Overuse safety
1	32	32	4	8	13	23	6	42	5	64	17120	100%	3516392	6120	36.08	67
2	32	35	5	7	13	22	7	41	5	64	17248	100%	3736808	12830	38.57	380
3	32	36	6	6	12	23	8	40	5	64	17280	100%	3625702	26455	38.57	380
4	32	35	5	7	15	18	6	39	5	64	17568	102%	3613932	7530	38.78	439
5	32	36	6	6	12	24	8	41	5	64	17696	103%	3637989	26468	39.10	548
6	32	36	6	6	15	18	7	39	5	64	17888	104%	3687147	15308	39.78	879

Selection set (256, 192, 2^{30}, 3,800,000)

2^16-Signature Limit per Key for Certificate Signing ?

- 2^16 = 65,536
- With smaller signatures and similar signing times in FIPS 205.
- With slow signing times and fast verifies to reduce the size significantly.

Level 1 2^16 Comparable Signing in FIPS 205

ID	n	h	d	h'	a	k	lg_w	m	Sec cat.	Pk bytes	Sig bytes	% size	Sign time	Verify time	Sigs at level 112	Overuse safety
1	16	21	3	7	13	10	8	20	1	32	3456	100%	2015990	7078	21.24	37
2	16	24	3	8	9	14	7	19	1	32	3648	105%	2087410	4201	21.39	41
3	16	21	3	7	15	9	7	20	1	32	3664	106%	1917687	4202	22.69	103
4	16	21	3	7	13	11	8	21	1	32	3680	106%	2040565	7092	22.92	121
5	16	18	2	9	15	9	4	21	1	32	3728	107%	1460216	726	19.69	12
6	16	20	2	10	12	11	4	21	1	32	3744	108%	1286134	727	20.12	17

Selection set (128, 112, 2^{16}, 2,200,000)

Note: “sigs at…” is # of sigs in power of 2.

Level 3 2^16 Comparable Signing in FIPS 205

ID	n	h	d	h'	a	k	lg_w	m	Sec cat.	Pk bytes	Sig bytes	% size	Sign time	Verify time	Sigs at level 128	Overuse safety
1	24	18	2	9	15	14	6	31	3	48	7464	100%	3606515	2422	23.70	207
2	24	18	3	6	15	14	8	30	3	48	7704	103%	2654578	10231	23.70	207
3	24	18	2	9	16	13	4	30	3	48	8208	109%	3393524	1059	24.04	263

Selection set (192, 128, 2^{16}, 3,800,000)

Level 5 2^16 Comparable Signing in FIPS 205

ID	n	h	d	h'	a	k	lg_w	m	Sec cat.	Pk bytes	Sig bytes	% size	Sign time	Verify time	Sigs at Level 192	Overuse safety
1	32	18	3	6	15	19	8	39	5	64	13600	100%	3539309	13383	22.49	89
2	32	20	2	10	14	20	4	39	5	64	14560	107%	3182573	1396	23.81	224

Selection set (256, 192, 2^{16}, 3,800,000)

Level 1 2^16 Slow Sign and Fast Verify

ID	n	h	d	h'	a	k	lg_w	m	Sec cat.	Pk bytes	Sig bytes	% size	Sign time	Verify time	Sigs at level 112	Overuse safety
1	16	21	1	21	25	5	2	19	1	32	3520	117%	1077936128	290	23.15	142
2	16	21	1	21	25	5	3	19	1	32	3168	105%	1279262720	338	23.15	142
3	16	20	1	20	21	6	4	19	1	32	3008	100%	627048448	435	21.68	51
4	16	21	1	21	21	6	4	19	1	32	3024	100%	1216348160	436	22.68	102

Selection set (128, 112, 2^{16}, 1,500,000,000)

Level 3 2^16 Slow Sign and Fast Verify

ID	n	h	d	h'	a	k	lg_w	m	Sec cat.	Pk bytes	Sig bytes	% size	Sign time	Verify time	Sigs at level 128	Overuse safety
1	24	20	1	20	24	8	2	27	3	48	7728	118%	828375040	425	27.98	4039
2	24	20	1	20	24	8	3	27	3	48	6912	105%	966787072	491	27.98	4039
3	24	20	1	20	24	8	4	27	3	48	6528	100%	1260388352	631	27.98	4039

Selection set (192, 128, 2^16, 1,500,000,000)

Level 5 2^16 Slow Sign and Fast Verify

ID	n	h	d	h'	a	k	lg_w	m	Sec cat.	Pk bytes	Sig bytes	% size	Sign time	Verify time	Sigs at level 192	Overuse safety
1	32	19	1	19	24	11	2	36	5	64	13696	118%	833617920	563	25.47	709
2	32	19	1	19	24	11	3	36	5	64	12320	106%	932184064	657	25.47	709
3	32	19	1	19	24	11	4	36	5	64	11584	100%	1116733440	833	25.47	709

Selection set (256, 192, 2^{16}, 2,500,000,000)

Our Current Plan

- We plan to standardize **rls128cs1, rls192cs1, rls256cs1 for certificate, software and firmware signings.**

- We need more input from the community about the demand of 2^30 and 2^16 limits
  - Let us know if the 2^24 options above would have unacceptable performance for your systems.

- We don’t plan to standardize them now:
  - Lower limits come with higher security risks when misuse happens
  - Minimize the number of parameter sets

Let us know if you think differently

Questions/Comments

Open for questions and comments.

We encourage you to share comments/input at pqc-forum@list.nist.gov (a public forum).

Contacts

NIST PQC standardization
www.nist.gov/pqcrypto

Extra Slides

Level 5 2^30 Comparable Signing in FIPS 205

ID	n	h	d	h'	a	k	lg_w	m	Sec cat.	Pk bytes	Sig bytes	% size	Sign time	Verify time	Sigs at level 192	Overuse safety
1	32	32	4	8	13	23	6	42	5	64	17120	100%	3516392	6120	36.08	67
2	32	35	5	7	13	22	7	41	5	64	17248	100%	3736808	12830	38.57	380
3	32	36	6	6	12	23	8	40	5	64	17280	100%	3625702	26455	38.57	380
4	32	35	5	7	15	18	6	39	5	64	17568	102%	3613932	7530	38.78	439
5	32	36	6	6	12	24	8	41	5	64	17696	103%	3637989	26468	39.10	548
6	32	36	6	6	15	18	7	39	5	64	17888	104%	3687147	15308	39.78	879
7	32	40	5	8	10	27	6	39	5	64	18016	105%	3771875	7544	40.85	1845
8	32	36	6	6	12	25	8	43	5	64	18112	105%	3650276	26481	39.56	754
9	32	36	6	6	12	26	8	44	5	64	18528	108%	3662563	26494	39.96	995
10	32	36	6	6	12	27	8	46	5	64	18944	110%	3674850	26507	40.32	1278
11	32	30	3	10	12	28	4	47	5	64	19072	111%	3643364	2007	34.65	25
12	32	36	4	9	13	21	4	41	5	64	19168	111%	2715626	2480	38.98	504
13	32	36	4	9	14	20	4	41	5	64	19360	113%	3182571	2486	39.81	897
14	32	36	4	9	14	21	4	43	5	64	19840	115%	3231722	2501	40.40	1351

Selection set (256, 192, 2^{30}, 3,800,000)

Level 1 2^16 Comparable Signing in FIPS 205

ID	n	h	d	h'	a	k	lg_w	m	Sec cat.	Pk bytes	Sig bytes	% size	Sign time	Verify time	Sigs at level 112	Overuse safety
1	16	21	3	7	13	10	8	20	1	32	3456	100%	2015990	7078	21.24	37
2	16	24	3	8	9	14	7	19	1	32	3648	105%	2087410	4201	21.39	41
3	16	21	3	7	15	9	7	20	1	32	3664	106%	1917687	4202	22.69	103
4	16	21	3	7	13	11	8	21	1	32	3680	106%	2040565	7092	22.92	121
5	16	18	2	9	15	9	4	21	1	32	3728	107%	1460216	726	19.69	12
6	16	20	2	10	12	11	4	21	1	32	3744	108%	1286134	727	20.12	17
7	16	20	2	10	15	9	4	21	1	32	3760	108%	2035704	728	21.69	51
8	16	20	2	10	14	10	4	22	1	32	3856	111%	1642487	734	21.97	62
9	16	20	2	10	15	10	4	23	1	32	4016	116%	2134007	744	23.37	165

Selection set (128, 112, 2^{16}, 2,200,000)

Note: “sigs at…” is # of sigs in power of 2.

Back-up Slides

Small Options in FIPS 205

SHL-DSA	Sign: Hashes	Verify: Hashes
128s	2,186,222	2214
192s	3,767,275	3183
256s	3,280,869	4692

2^50-Signature Limit Per Key Level 1

ID	n	h	d	h'	a	k	lg_w	m	sec cat.	pk bytes	sig bytes	% size	sign time	verify time	sigs at level 112	overuse safety
1	16	49	7	7	14	11	6	27	1	32	6128	100%	1918705	5599	52.35	5
2	16	56	8	7	14	9	6	24	1	32	6144	100%	2017266	6345	55.92	60
3	16	55	11	5	13	10	8	25	1	32	6304	102%	1868462	25552	55.24	37
4	16	54	6	9	12	11	4	25	1	32	6528	106%	1861618	1885	54.12	17
5	16	54	6	9	13	11	4	26	1	32	6704	109%	1996786	1896	55.92	60

Table 1: Selection set (128, 112, 2^{50}, 2,200,000)

128s, signature size: 7,856. 7,856 – 6,128 = 1,728 (22%).

2^50-Signature Limit Per Key Level 3

ID	n	h	d	h'	a	k	lg_w	m	sec cat.	pk bytes	sig bytes	% size	sign time	verify time	sigs at level 128	overuse safety
1	24	49	7	7	12	21	7	39	3	48	12792	100%	3700455	13771	54.69	25
2	24	56	8	7	15	13	6	33	3	48	12888	100%	3508206	8978	60.92	1937
3	24	50	10	5	15	15	8	36	3	48	13224	103%	3605098	33582	56.36	82
4	24	54	6	9	13	16	4	34	3	48	14040	109%	2906093	2734	58.68	410

Table 2: Selection set $(192, 128, 2^{50}, 3{,}800{,}000)$

192s, signature size: 16,224. 16,224 - 12,792 = 3,432 (21%)

2^50-Signature Limit Per Key Level 5

ID	n	h	d	h'	a	k	lg_w	m	sec cat.	pk bytes	sig bytes	% size	sign time	verify time	sigs at level 128	overuse safety
1	24	49	7	7	12	21	7	39	3	48	12792	100%	3700455	13771	54.69	25
2	24	56	8	7	15	13	6	33	3	48	12888	100%	3508206	8978	60.92	1937
3	24	50	10	5	15	15	8	36	3	48	13224	103%	3605098	33582	56.36	82
4	24	54	6	9	13	16	4	34	3	48	14040	109%	2906093	2734	58.68	410

Table 2: Selection set $(192, 128, 2^{50}, 3{,}800{,}000)$

256s, signature size: 29,792. 29,792 – 22,720 = 7,072 (23.7%)