Smaller Sphincs+

or, Honey, I Shrunk the Signatures

Scott Fluhrer[1] Quynh Dang[2]

[1] Cisco Systems
[2] National Institute of Standards and Technology, USA
January 5, 2024

1 Introduction

NIST has released the draft specification of SLH-DSA (also known as Sphincs+). When NIST released its original call for proposals for the Postquantum Process, they specified that signature systems would need to be usable at full security for 2^{64} signatures per private key. Hence, the parameter sets specified in SLH-DSA is tuned to have full security after that many signatures. However, it has been noted that in many cases, we don't have need for that many signatures, and that parameter sets tuned for fewer signatures would be shorter and more efficient to process. This paper examines such possible alternative parameter sets.

1.1 Terminology note

When we refer to the Sphincs+ parameter sets specified in the Draft FIPS 205 [1], we will refer to the system as SLH-DSA. When we refer to a more general parameter set, we will refer to the system as Sphincs+.

2 Background of Sphincs

A hash based signature is a signature scheme that relies solely on the strength of an underlying hash function. In this system, the signer has a number of hash preimages, and when he generates a signature, he reveals several of those preimages (which the verifier can validate). Because the signer has a finite number of hash preimages, there is always a bound on the number of signatures he can safely generate. However, this bound can practically be made quite large.

One advancement was the Sphincs [2] signature system, which had 41 kilobyte signatures, and had a practical (if slow) signature generation time. It could safely generate 2^{50} signatures from a single private key at 256 bits of security (NIST Level 5).

The digital signature system worked by having a tree structure based on hashes with 256 bit outputs. At the top, there is a 60-level hypertree of Merkle trees. At the bottom of the hypertree, there are 2^{60} HORST few time signature structures. Each such HORST structure could safely sign several messages.

When signing a message, the signer would select a random HORST structure, use it to sign the message, and then sign the HORST root with the authentication path through the hypertree.

3 Sphincs+ overview

Sphincs+ is a refinement and generalization of the Sphincs structure.

Sphincs+ relies on a tree structure based on hashes with n bit outputs. At the top, there is an h level hypertree of Merkle trees. The h levels are made up of d layers, each of which consists of a h/d-height Merkle tree, and each leaf

of the Merkle tree is a one time signature. At the bottom of the hypertree, there are 2^h one-time signatures. Below that, there are 2^h FORS structures, and each one-time signature signs the root of one of the FORS structures. Each FORS structure consists of k sets, each of which consists of $t = 2^a$ private key values. These sets use an a-level Merkle tree to allow the authentication of these private values. The k roots of the Merkle trees are hashed together to form the root of the FORS structure.

To verify a Sphincs+ signature, the verifier takes the message and a value R found in the signature, and hashes them together. This hash is used to select one of the 2^h FORS structures, and for each of the k sets within that FORS, one of the t private values. For each of these private values, the verifier takes the value in the signature, and hashes it. It then takes the a-level authentication path found in the signature to derive an intermediate root for this set. Once all the intermediate roots for the sets have been computed, those are hashed together to form the root for the FORS structure. The verifier then uses the one-time signature (also found in the signature) to process this root. It then processes upwards through the hypertree to compute the ultimate root. This root of the hypertree is compared to the expected root value in the public key. If the two compare the same, the signature is accepted as valid.

There are several parameters that can be adjusted to specify the Sphincs+ parameter set:

- n: the length of each hash in bits.
- h: the height of the hypertree.
- d: the number of layers within the hypertree.
- w: the Winternitz parameter to use within the one-time signatures.
- k: the number of sets within a FORS.
- a: the $2^a = t$ private values within each FORS set.

4 Sphincs+ usage limitations

There are a number of ways to attack a Sphincs+ signature system, such as side channel attacks to recover an internal secret and fault attacks (which cause the signer to use a single internal one-time signature to sign two different values). However, if we assume a correctly running black-box signer, there are effectively two attack strategies available to the attacker. The first attack strategy is to find a hash preimage or second preimage against the underlying hash function, and use that to generate a forgery. Because we only use the hash functions (see [3] [4]) which have the expected preimage and second-preimage resistance strength of 2^n bits, the expected effort required for this attack is 2^n hash evaluations.

The second attack strategy is to piece together a valid signature for a new message from hashes found in previously published valid signatures. If we go through the Sphincs+ structure, we find that the only opportunity for this lies within the FORS structure. Each valid signature reveals k private key values from k sets within a FORS structure. If the adversary finds a message that hashes to a FORS and k values that are all revealed somewhere in the valid signatures in that FORS, he can combine them to form a valid signature for that message.

If p is the probability that a new message hashes to k values (one in each of the k t-element sets) that all appear somewhere in the known valid signatures, then the expected effort taken by this process is p^{-1} hashes.

If the hash length is n bits (and so the attack effort for former attack is 2^n hashes), then we want the latter attack to take at least as much effort , that is $p^{-1} \geq 2^n$ or $p \leq 2^{-n}$.

This is the process the adversary would use to perform this attack: he selects a message (and randomizer R value), and hashes them into a hypertree leaf (which specifies the FORS) and k FORS leaves. He then goes through his pile of valid signatures, finds the ones that specify the same FORS, and from the ones he has, see if all k FORS

leaves appears within them. If all k FORS leaves do appear, then he has all the leaf preimages and authentication paths he needs, and so can generate a signature for the message he picked.

When computing the probability of success of this process, we first need to consider "of the valid signatures that the attacker has, how many specify the same FORS as this message". We model the process of hashing a message to a hypertree leaf as a random process; if the hypertree height is h, then the probability of a specific valid signature hashing to the same hypertree leaf is 2^{-h}. Each valid signature can be modeled as selecting a hypertree leaf independently, and so if he has 2^m valid signatures, with m large, then the probability distribution of the number of valid signatures that hash to that specific hypertree leaf is quite close to a Poisson distribution with mean $\lambda = 2^{m-h}$. That is, the probability of the adversary having exactly g valid signatures that hash to that hypertree leaf is approximately $\lambda^g e^{-\lambda}/g!$.

The next step is "if the adversary has exactly g valid signatures for that FORS, what is the probability that all k private values that he needs appear somewhere within those valid signatures?". If we model the hash of a message to FORS leaves as a random process, this probability is $(1–(1–t^{-1})^g)^k$ (where each of the k FORS sets consists of t private values).

If we combine those two results, it gives us the probability of the attacker being able to generate a forgery to the selected message with a single query as:

$$p = \sum_{g=0}^{2^m} \frac{\lambda^g e^{-\lambda}}{g!} \cdot (1–(1–t^{-1})^g)^k \tag{1}$$

We note that once g is several multiples of the mean λ, the terms drop off exponentially fast (because the $\lambda^g e^{-\lambda}/g!$ term drops by a factor of λ/g for each term and the $(1–(1–t^{-1})^g)^k$ term is upwards bounded by 1), and so this can be efficiently evaluated.

We say that a Sphincs+ parameter set is 'tuned' to 2^m signatures if $p \approx 2^{-n}$; that is, if the adversary has 2^m signatures available to him, then the expected work effort for either attack strategy is approximately the same.

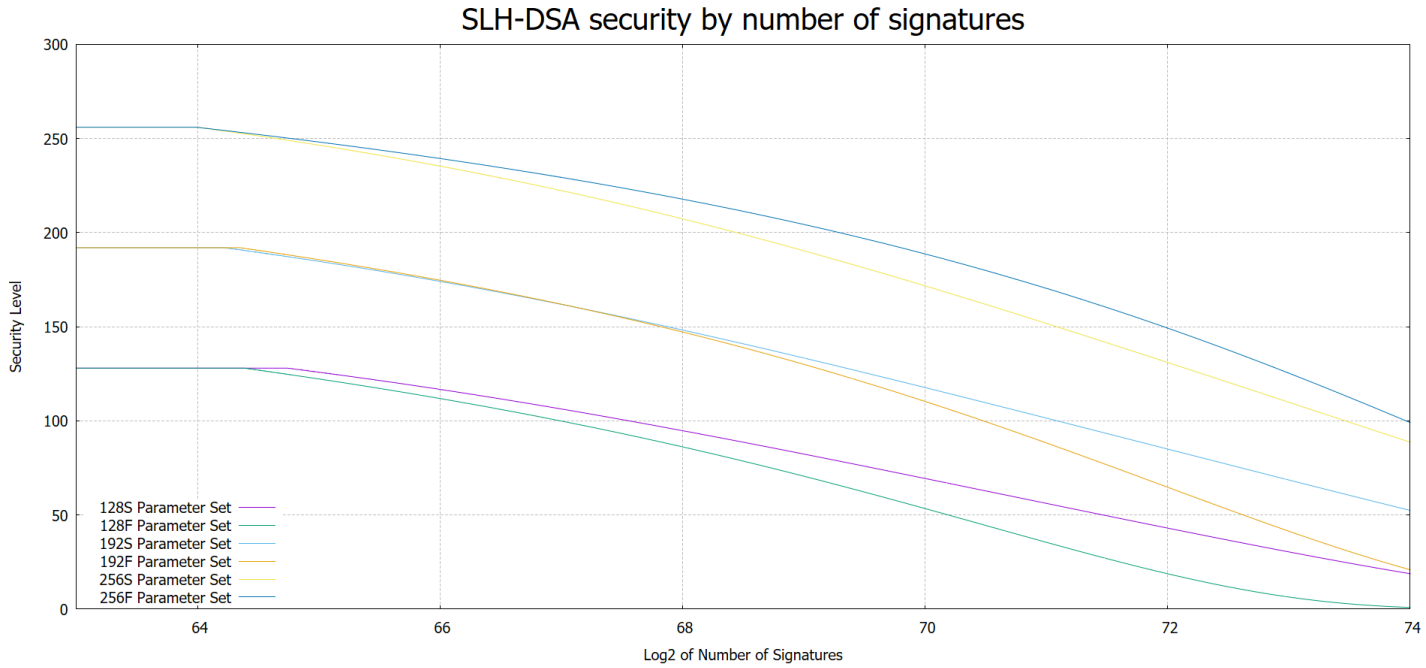
5 Overuse

We can then consider what happens if we 'overuse' a parameter set, that is, generate more signatures than it is tuned for. Unlike a one-time-signature (where 'overuse' would be using the same private key to generate two different signatures), the security of Sphincs+ doesn't drop off drastically under overuse, but instead is rather more gradual. For a given parameter set, when m increases, the attacker's success probability increases, meaning the security strength goes down. For example, if p is around 2^{-80}, the security strength is only 80 bits.

For example, we can consider how the current SLH-DSA parameter sets fare under overuse conditions. The below figure 5 shows how they behave under various overuse conditions (as computed using Equation 1). Since the choice of the hash function does not affect the security under overuse, we leave that as unspecified. For example, 128S stands for both SLH-DSA-SHA2-128s and SLH-DSA-SHAKE-128s parameter sets and 192F stands for both SLH-DSA-SHA2-192f and SLH-DSA-SHAKE-192f parameter sets, see [1] .

If we examine this graph, we note several things. First, there remains quite a bit of security strength even with moderate overuse. For example, if we look at the 256F parameter sets, they retain about 100 bits of security strength even after 2^{74} signatures, that is, 1,000 times more than they were designed for. In addition, while the security strength of all the parameters drop, they do not drop at the same rate. For example, at 2^{74} signatures, both 128S and 192F have about the same security strength.

We also noticed that the 128S and 192S parameter sets' security strengths degrade slower than their counter-part 128F and 192F parameter sets' do respectively. However, the order is reversed for the 256S and 256F parameter



sets.

Of course, practically speaking, no one will ever generate anywhere close to 2^{64} signatures for one private key, much less go over that. So, considering overuse for the SLH-DSA parameter sets is an academic exercise. However, when we consider parameter sets with lower usage limits, it is plausible that they might be misused by going over their tuned limits. Hence it is important to consider how they behave on moderate overuse.

6 Small Parameter Sets

When we consider how a Sphincs+ parameter set works, there are a number of desirable properties they may have, and to some extent, we need to select a trade-off between them. These properties[1] that are involved in the trade-offs include:

- The target security level
- The number of signatures the parameter set is tuned for
- The fall-off behavior when the parameter set is overused
- Signature generation time
- Signature verification time
- Signature size

We consider overuse behavior to be important, because (unlike the parameter sets defined in SLH-DSA) the signature limits are sufficiently small that it is plausible that the parameter set will be misused by signing more messages than expected, and thus we would prefer to reduce the damage in that case.

We did a computerized search of the various potential parameter sets, with security levels 128 bits and 192 bits; with the tuned number of signatures being $2^{20}, 2^{30}, 2^{40}$ and 2^{50}, and signature generation times of 100,000, 1,000,000,

[1]We don't list key generation time. The bulk of the computation done during the key generation process consists of building the top level merkle tree, and hence it is always faster than signature generation (which also effectively rebuilds that merkle tree as one of its tasks). Hence, if signature generation is 'fast enough', so is key generation.

10,000,000 and 100,000,000 hashes. If our implementation is able to compute a hash in one microsecond, then this corresponds signature generation times of 0.1, 1, 10 and 100 seconds[2][3]. Even though taking 100 seconds to generate a signature may seem excessive, the processing within Sphincs+ signature generation is parallizable, and some implementations may be able to use that to accelerate the signing processs (perhaps using AVX instructions or multithreading).

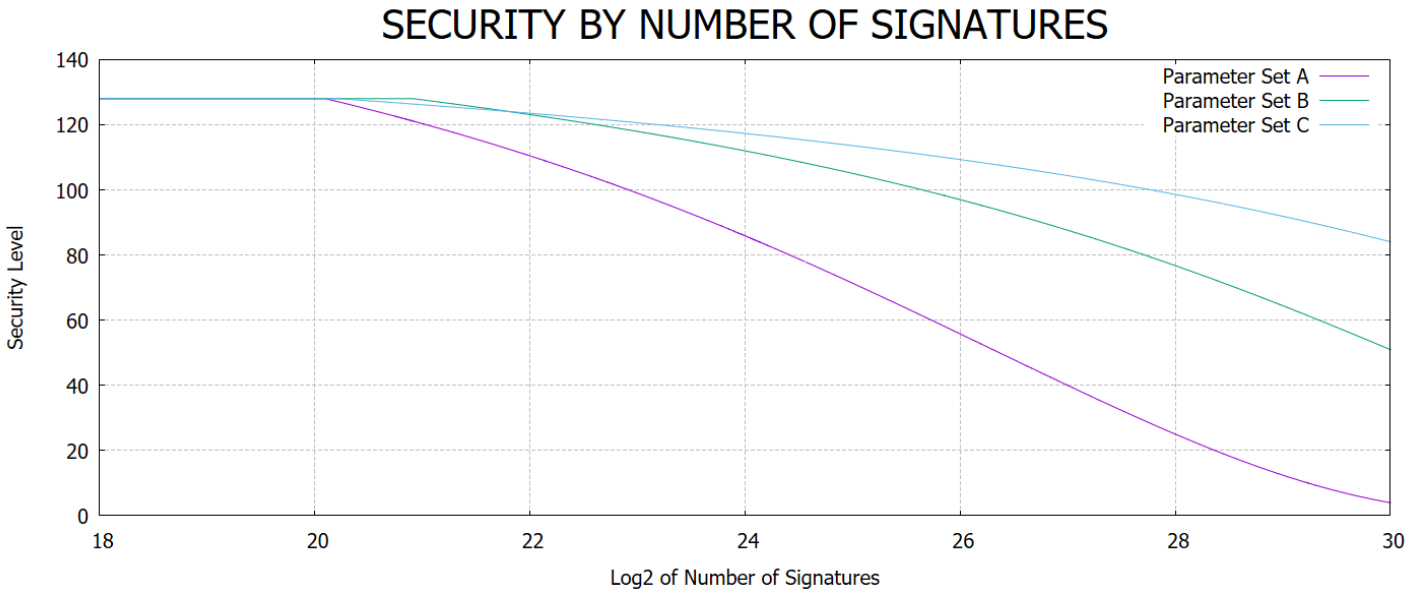
For each parameter set, we list how many signatures can be generated and still retain a lesser security level (112 bits for parameter sets tuned to Level 1 security; 128 bits for parameter sets tuned to Level 3 security). This is here to display information on how well the parameter sets behave under overuse. For the parameter sets we recommend, we also show a graph displaying their security falloffs during overuse.

6.1 Initial comments about overuse of small parameter sets

For an initial example, we will consider three parameter sets that all have Level 1 security, tuned for 2^{20} signatures. They all take approximately 100,000 hashes to generate a signature[4]. They vary somewhat in verification time and signature size; these parameter sets are:

- Set A - n=16 h=20 d=4 a=9 k=19 w=16 - Signature size = 5616
- Set B - n=16 h=25 d=5 a=8 k=18 w=16 - Signature size = 5808
- Set C - n=16 h=28 d=7 a=10 k=13 w=16 - Signature size = 6672

Just looking at the signature size, Set A would look superior, however we can also consider the fall-off behavior.



As we can see from the graph, Set A loses its security relatively quickly on overuse. However, Set B loses it rather more slowly (still retaining 100 bits of security after 2^{25} signatures), and Set C loses it even slower still.

We look for parameter sets whose signature sizes are smaller than the smallest signature size in SLH-DSA, which is 7,856 bytes for security Level 1 and 16,224 for security Level 3. To facilitate the discussions in this paper, we call those numbers the *bound-size* and the *192-size* respectively.

[2]This is a bit of a simplification; in practice, we compute hashes of strings of differing lengths, which means that just counting hash computations doesn't give a precise reflection of the time taken. On the other hand, the ratio of differing length hashes is approximately the same for different parameter sets, and so this is still a useful for comparing parameter sets.

[3]Computing hashes take up the bulk of the time during the signature generation process.

[4]Hence if we can compute about a million hashes per second, they all take about 0.1 second to generate a signature.

As discussed above, there are 6 factors in choosing a parameter set for any particular use case, each of which has a number of plausible settings. However, a standard should not have so many parameter sets. Therefore, for most cases, under a selection set of (security level, retained lesser security level, maximum number of signatures, the upper bound of hash operations for signing), we are going to pick 2 parameter sets to recommend for standardization consideration: one with the smallest signature and the other with the lowest risk of degrading to below its retained lesser security level. For example, a selection set: (128, 112, 2^{20}, 100,000) means we search for parameter sets offering 128 bits of security, the retained lesser security at 112 bits, the maximum number of signatures a signing key is allowed to generate before its security strength starts to fall below 128 bits, signing times are not more than 100,000 hash operations.

When a parameter set A losses its retained lesser security level faster than a parameter set B, we may just say that B has "less risk" than A or A has "more risk" than B.

In addition, we are going to search for a third parameter set which does not have either one of the 2 properties above, but has either one of the 2 properties below.

1) It has noticeably lower risk than the smallest signature parameter set has and its signature size is marginally larger than the latter.
2) Its risk is marginally larger than the lowest risk parameter set, but its signature size is noticeably smaller than the latter.

Of course, this is a subjective matter for what "marginally" and "noticeably" mean. So, we'll need to look at specific instances in order to have sound opinions.

To generate the raw list of parameter sets for us to consider, we went through the possible combinations exhaustively and selected the parameter sets that had the required security level at the minimum number of signatures (as well as requiring fewer hash computations to generate a signature than our bound), sorted them by signature size, and scanned them (in increasing signature size order). We then selected the parameter sets which were "better" than any of the ones previously found, where "better" is either "better overuse characteristic" or "better W value[5]"

To determine the overuse characteristics, we computed the number of signatures it would take to reduce the security to a lesser security level (112 bits for Level 1 security parameter sets, 128 bits for Level 3 security parameter sets); the more signatures can be generated before reducing security to that lesser security level, the better (safer).

We then went through the lists of parameter sets manually, and selected ones which appeared to us to be attractive.

6.2 Level 1 security at 2^{20} signatures

Here are the search results for parameter sets tuned for Level 1 security after 2^{20} signatures, and an upper bound of 100,000 hash operations during the signing process. This selection set is (128, 112, 2^{20}, 100,000).

ID	h	d	a	k	w	SigSize	Sign Time	Verify Time	Sigs/level 112
A-1	20	4	9	19	16	5616	91369	1336	21.85
A-2	20	4	9	20	16	5776	92392	1346	22.32
A-3	25	5	8	18	16	5808	99113	1594	24.00
A-4	25	5	8	19	16	5952	99624	1603	24.74
A-5	24	6	8	21	32	6112	96933	2909	24.86
A-6	24	6	8	22	32	6256	97444	2918	25.31
A-7	25	5	7	24	16	6288	96035	1624	24.85

[5]W=16 is considered the best, because that's what SLH-DSA uses, hence making plugging in these parameter sets into an existing SLH-DSA implementation the easiest; W=4 or W=256 is second best (because it makes the mapping of the hash to digit conversion simple), and other W values the worst (because digit values will span bytes at times).

A-8	24	6	10	15	16	6400	84651	1877	25.08
A-9	24	6	8	23	32	6400	97955	2927	25.69
A-10	25	5	7	25	16	6416	96290	1632	25.24
A-11	25	5	7	26	16	6544	96545	1640	25.59
A-12	24	6	8	24	32	6544	98466	2936	26.03
A-13	24	6	10	16	16	6576	86698	1888	25.85
A-14	28	7	10	13	16	6672	89548	2140	26.76
A-15	28	7	9	15	16	6784	78282	2147	26.79
A-16	28	7	10	14	16	6848	91595	2151	28.09
A-17	28	7	10	15	16	7024	93642	2162	29.08
A-18	28	7	10	16	16	7200	95689	2173	29.85
A-19	32	8	10	13	16	7296	98539	2425	30.76

Table 1: Selection set (128, 112, 2^{20}, 100,000)

The 'Sigs/level 112' is the logarithm (to the base of 2) of the number of signatures that can be generated and retain a security level of 112 bits.

For example, the parameter set listed on top has 112 bits of security after approximately $2^{21.85}$ signatures. It is intended to show how the parameter set handles moderate overuse.

Sign Time and Verify Time is the number of hashes computed during signature generation and verification. Now, in practice, not all hash computations are the same, as some hashes have larger inputs than others, however in practice, that does not affect the relative numbers appreciably.

The first parameter set A-1 (20, 4, 9, 19,16) is $(7,856 - 5,616 =)$ 2,240 bytes smaller than the *bound-size*. This is a roughly 29% improvement in the signature size. However, it has the largest risk of overuse among the parameter sets As while having the biggest signature size improvement.

On the other hand, the last parameter set A-19 (32,8,10,13,16) has the lowest risk of overuse, but has the least improvement in signature size. The improvement is less than 300 bytes from the *bound-size*.

A-1 and A-19 are recommended for standardization consideration.

Even the best of the above parameter sets has a signature size of 5,616 bytes, this may be too larrge for for many applications. So, we are going to look at how we can shrink the signature size by spending more time during signature generation.

Now, we are going to list the search result for an upper bound on the signer time of 1,000,000 hashes in the table below. This selection set is (128, 112, 2^{20}, 1,000,000).

ID	h	d	a	k	w	SigSize	Sign Time	Verify Time	Sigs/level 112
B-1	21	3	13	11	64	3968	770802	2484	22.92
B-2	24	4	12	11	128	4032	778737	5549	24.12
B-3	25	5	13	10	256	4096	901425	11692	25.24
B-4	24	4	13	11	128	4208	868849	5560	25.92
B-5	28	4	13	10	64	4240	951282	3246	28.24
B-6	18	2	14	12	16	4304	968690	762	22.37
B-7	30	6	12	10	256	4304	967024	13992	27.86
B-8	24	3	12	11	16	4368	521714	1012	24.12
B-9	27	3	10	13	16	4416	889840	1015	25.76
B-10	27	3	12	11	16	4416	953330	1015	27.12

B-11	32	4	10	12	32	4432	944112	1962	28.82
B-12	32	4	11	11	32	4432	964593	1962	29.62
B-13	30	5	12	11	128	4464	950896	6900	30.12
B-14	30	6	10	13	256	4512	911725	14005	28.76
B-15	30	6	12	11	256	4512	975215	14005	30.12
B-16	27	3	11	13	16	4624	916464	1028	27.99
B-17	27	3	12	12	16	4624	961521	1028	28.59
B-18	32	4	13	9	16	4784	722931	1284	29.48
B-19	27	3	12	13	16	4832	969712	1041	29.65
B-20	32	4	12	10	16	4848	657394	1288	29.86
B-21	32	4	14	9	16	4928	870387	1293	31.92

Table 2: Selection set (128, 112, 2^{20}, 1,000,000)

In comparison to the previous A parameter sets' signatures, these are considerably smaller. In addition, with this amount of computation available during signature generation, the setting w=32 and above becomes viable; this reduces the signature size somewhat. However, this comes at a cost of significantly increasing the signature verification time. Hence, we included both w=16 and w=256 options, as well as intermediate options when appropriate.

The parameter set B-1 (21,3,13,11,64) has the smallest signature size which is 3,968 bytes and the parameter set B-21 (32,4,14,9,16) has the largest signature size, 4,928 bytes.

The signature size reductions of B-1 and B-21 from the *bound-size* are $(7,856 - 3,968)/7,856$ ($\approx 50\%$) and $(7,856 - 4.928)/7,856$ ($\approx 37\%$), respectively. The former parameter set has a large signature size reduction, while the latter has a noticeable but smaller reduction. However, the latter has significantly lower risk of overuse than the former by the factor of $2^{31.92-22.92} = 2^9$.

B-1 and B-21 are recommended for standardization consideration.

We now consider the same situation, except for an upper bound on the signing time of 10,000,000 hash function evaluations. Below is the parameter sets under this selection set: (128, 112, 2^{20}, 10,000,000).

ID	h	d	a	k	w	SigSize	Sign Time	Verify Time	Sigs/level 112
C-1	24	3	16	8	256	3440	4589045	7077	24.90
C-2	27	3	14	9	256	3472	7375860	7079	26.92
C-3	27	3	16	8	256	3488	8129525	7080	27.90
C-4	30	3	15	8	128	3552	8787957	4195	28.94
C-5	27	3	15	9	256	3616	7670772	7088	28.69
C-6	27	3	17	8	256	3616	9178101	7088	29.42
C-7	30	3	14	9	128	3664	8558580	4202	29.92
C-8	30	3	16	8	128	3680	9312245	4203	30.90
C-9	24	2	16	8	16	3696	5652470	724	24.90
C-10	32	4	13	9	256	3696	4868083	9380	29.48
C-11	32	4	17	7	256	3696	6555637	9380	31.21
C-12	26	2	14	9	16	3712	9502709	725	25.92
C-13	26	2	13	10	16	3792	9371636	730	26.24
C-14	24	2	17	8	16	3824	6701046	732	26.42
C-15	26	2	15	9	16	3856	9797621	734	27.69
C-16	24	2	18	8	16	3952	8798198	740	27.70
C-17	26	2	14	10	16	3952	9535476	740	27.97
C-18	24	2	17	9	16	4112	6963189	750	28.32

C-19	26	2	15	10	16	4112	9863156	750	29.37
C-20	33	3	13	9	16	4240	3600372	1004	30.48

Table 3: Selection set (128, 112, 2^{20}, 10,000,000)

When we are able to spend this amount of time during the signature generation process, parameter sets with small signatures tend to have a comparatively large hypertree and large FORS sets; both tend to lend themselves to superior overuse characteristics.

As we can see, parameter set C-1 (24,3,16,8,256) has the smallest signature size in the table. C-1 is also 528 (3968-3440) bytes smaller than the smallest signature (B-1) in the previous table. C-1 also has lower risk than B-1 by a factor of $2^{24.9-22.92} = 2^{1.98}$.

The second parameter set C-2(27,3,14,9,256) has the second smallest signature size which is only 32 bytes larger than C-1. However, C-2 has a meaningful reduction in the overuse risk from the C-1. The risk reduction is $2^{26.92-24.9} = 2^{2.02}$ times. In addition, it has a smaller combined signature plus public key size (3,504 = 3472 + 32) than the smallest option in *Draft FIPS 204, Module-Lattice-Based Digital Signature Standard (ML-DSA)* [5]. This smallest option is the parameter set ML-DSA-44, which has a combined signature and public key size of 3,732 (1312 + 2420) bytes.

The parameter set C-9 is only $3696 - 3472 = 224$ bytes larger than C-2 in signature size, but the former's Verify Time is only around 10% of C-2's verification time, however C-9 has worse overuse characteristics.

The parameter set C-11 has the lowest risk. Its signature size is only 256 bytes ($3696 - 3472 = 224$) larger than C-2's signature size, but its overuse risk is significantly smaller than C-2's and the factor of the risk reduction is $2^{31.21-26.92} = 2^{4.29}$ times.

C-2, C-9 and C-11 are recommended for standardization consideration.

Now, searching for the parameter sets with 100,000,000 hash evaluations, we get:

ID	h	d	a	k	w	SigSize	Sign Time	Verify Time	Sigs/level 112
D-1	24	2	21	6	256	3088	62930936	4768	25.68
D-2	26	2	18	7	256	3136	79200248	4771	27.05
D-3	26	2	21	6	128	3216	69238776	2850	27.68
D-4	26	2	19	7	256	3248	82870264	4778	28.50
D-5	28	2	18	7	128	3264	91815928	2853	29.05
D-6	28	2	21	6	64	3344	75563000	1700	29.68
D-7	26	2	20	7	256	3360	90210296	4785	29.74
D-8	30	3	20	6	256	3376	26744824	7073	30.10
D-9	17	1	20	8	16	3536	90439672	468	22.92
D-10	24	2	21	6	16	3632	29769720	720	25.68
D-11	30	2	17	7	16	3632	38666232	720	29.21
D-12	30	2	20	6	16	3632	49414136	720	30.10

Table 4: Selection set (128, 112, 2^{20}, 100,000,000)

We first note that all the parameter sets listed here have a combined public key size plus signature size of 3,120 to 3,664 bytes, which is again smaller than the smallest option in ML-DSA.

We also note that parameter set D-8 has signatures that are only 282 bytes longer than D-1's signatures, and D-8 has considerably better overuse properties (as well as being comparatively cheap to generate for this group).

D-1 and D-8 are recommended for standardization consideration.

Figure 1 illustrates the security degradation behaviors of the recommended parameter sets that can sign 2^{20} signatures with 128 bits of security strength.

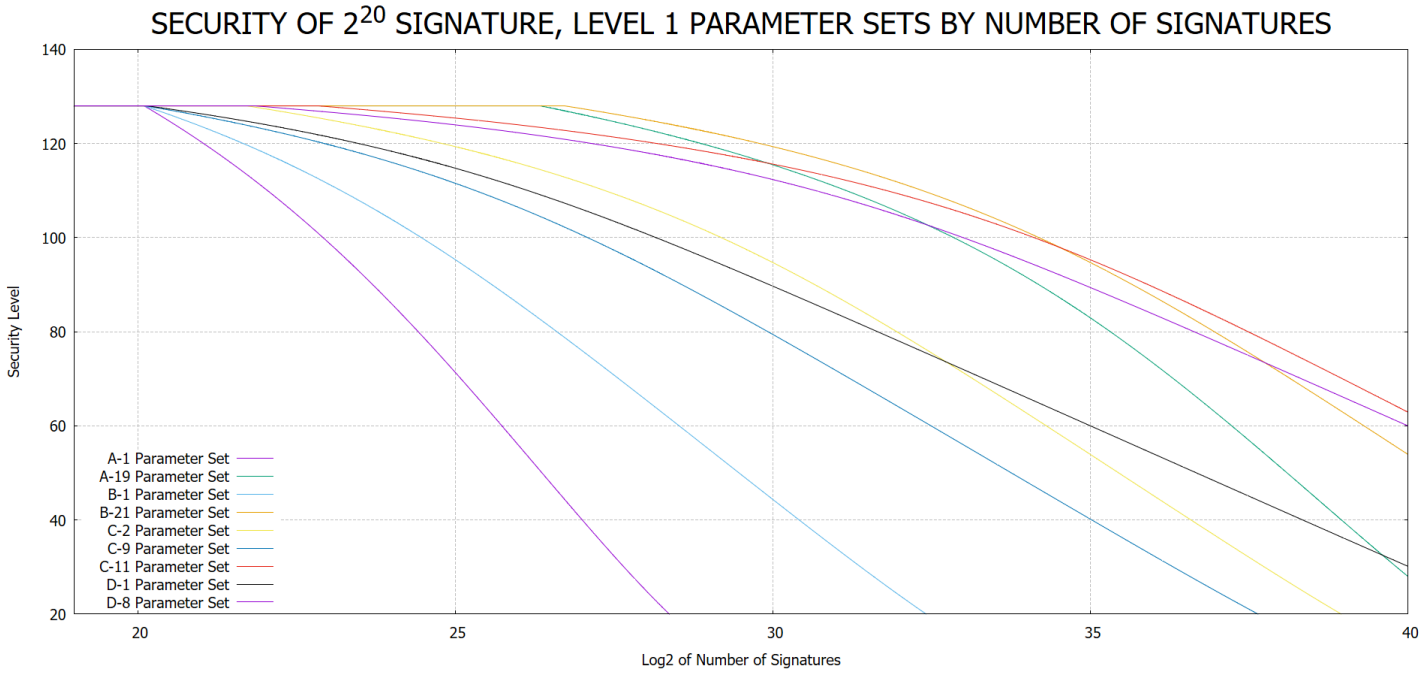


Figure 1: Recommended Parameter Sets

6.3 Parameter sets targeting 2^{30} signatures

Below is the parameter sets under selection set: (128, 112, 2^{30}, 1,000,000). The parameter sets we found are below.

ID	h	d	a	k	w	SigSize	Sign Time	Verify Time	Sigs/level 112
E-1	32	4	11	13	32	4816	972783	1986	32.99
E-2	30	6	12	13	256	4928	991597	14031	32.65
E-3	32	4	10	15	32	4960	950253	1995	33.08
E-4	32	4	11	14	32	5008	976878	1998	33.99
E-5	35	5	13	10	32	5056	738545	2422	35.24
E-6	36	6	14	9	64	5056	885489	4787	35.92
E-7	30	6	11	15	256	5104	946539	14042	32.76
E-8	30	6	12	14	256	5136	999788	14044	33.47
E-9	36	6	13	10	64	5136	754416	4792	36.24
E-10	32	4	14	10	16	5168	903154	1308	33.97
E-11	35	5	14	10	32	5216	902385	2432	36.97
E-12	36	6	14	10	64	5296	918256	4802	37.97
E-13	36	9	14	9	256	5344	958734	20918	35.92
E-14	42	7	13	9	64	5392	836464	5553	39.48
E-15	32	4	14	11	16	5408	935921	1323	35.35
E-16	36	9	13	10	256	5424	827661	20923	36.24
E-17	42	7	12	10	64	5456	770927	5557	39.86
E-18	40	8	14	9	128	5504	983535	10937	39.92

E-19	40	5	12	10	16	5536	801265	1577	37.86
E-20	42	7	14	9	64	5536	983920	5562	41.92
E-21	36	9	14	10	256	5584	991501	20933	37.97
E-22	40	5	13	10	16	5696	883185	1587	40.24

Table 5: Selection set (128, 112, 2^{30}, 1,000,000)

The parameter set E-1 (32,4,11,13,32) has the smallest signature size from the table even though it does not have the biggest overuse risk. The parameter set E-20(42,7,14,9,64) has the lowest overuse risk. E-1's signature size is (5536 - 4816 =)720 bytes smaller than E-20's. But, the overuse risk of E-20 is significantly lower than E-1's by a factor of $2^{41.24-32.99} = 2^{8.25}$.

E-1 and E-20 are recommended for standardization consideration.

To search for smaller parameter sets, we increased the upper bound to 10,000,000 hash operations to generate a signature. Below are several of such parameter sets under the selection set (128, 112, 2^{30}, 10,000,000).

ID	h	d	a	k	w	SigSize	Sign Time	Verify Time	Sigs/level 112
F-1	36	4	14	9	256	3904	9736179	9393	35.92
F-2	36	4	13	10	256	3984	9605106	9398	36.24
F-3	36	4	18	7	128	4064	9179125	5551	37.05
F-4	40	5	17	7	256	4112	7735796	11693	39.21
F-5	40	5	18	7	256	4224	9570804	11700	41.05
F-6	36	3	14	9	16	4432	7200756	1016	35.92
F-7	36	3	16	8	16	4448	7954421	1017	36.90
F-8	36	3	15	9	16	4576	7495668	1025	37.69
F-9	36	3	17	8	16	4576	9002997	1025	38.42
F-10	36	3	16	9	16	4720	8085492	1034	39.10
F-11	36	3	15	10	16	4832	7561203	1041	39.37
F-12	36	3	17	9	16	4864	9265140	1043	40.32

Table 6: Selection set (128, 112, 2^{30}, 10,000,000)

There are parameter sets in this table which have noticeable reductions in signature sizes and overuse risks over the parameter sets D-i$_s$ and E-i$_s$. For example, the parameter set F-1 (36,4,14,9,256)'s signature size is (4816 - 3904 =) 912 bytes smaller than the signature of the parameter set E-1 (32,4,11,13,32) which has the smallest signature among all parameter sets D-i$_s$ and E-i$_s$. F-1 also has a significant reduction in overuse risk from E-1 by the factor of $2^{35.92-32.99} = 2^{2.93}$.

One can also choose parameter sets which have even much lower overuse risks, but larger signature sizes. One of such parameter sets is the parameter set F-5 (40,5,18,7,256) which has the lowest overuse risk, but is only 320 (4224-3904) bytes larger than F-1's signature size.

F-5 is an excellent parameter set since it has the lowest overuse risk, but has the 5th smallest signature among 12 F-i$_s$ parameter sets.

F-1 and F-5 are recommended for standardization consideration.

To search for smaller parameter sets, we increased the upper bound to 100,000,000 hash operations to generate a signature. Below are several of such parameter sets under the selection set (128, 112, 2^{30}, 100,000,000).

ID	h	d	a	k	w	SigSize	Sign Time	Verify Time	Sigs/level 112
G-1	36	3	21	6	256	3568	81813496	7085	37.68
G-2	39	3	20	6	128	3664	78692344	4202	39.10
G-3	36	3	19	7	256	3696	63987704	7093	38.50
G-4	39	3	21	6	128	3760	91275256	4208	40.68
G-5	36	3	20	7	256	3808	71327736	7100	39.74
G-6	40	4	20	6	256	3824	31465462	9388	40.10
G-7	32	2	19	7	16	3888	81002488	736	34.50
G-8	32	2	20	7	16	4000	88342520	743	35.74
G-9	30	2	22	7	16	4192	95551480	755	35.93
G-10	32	2	19	8	16	4208	82051064	756	36.85
G-11	39	3	20	6	16	4336	26394616	1010	39.10
G-12	45	3	19	6	16	4336	61538296	1010	43.02

Table 7: Selection set (128, 112, 2^{30}, 100,000,000)

G-1 has the smallest signatures, and relatively decent overuse properties. G-4 has somewhat larger signatures (by 192 bytes) and somewhat better overuse properties.

G-1 and G-4 are recommended for standardization consideration.

Figure 2 illustrates the security degradation behaviors of the recommended parameter sets that can sign 2^{30} signatures with 128 bits of security strength.

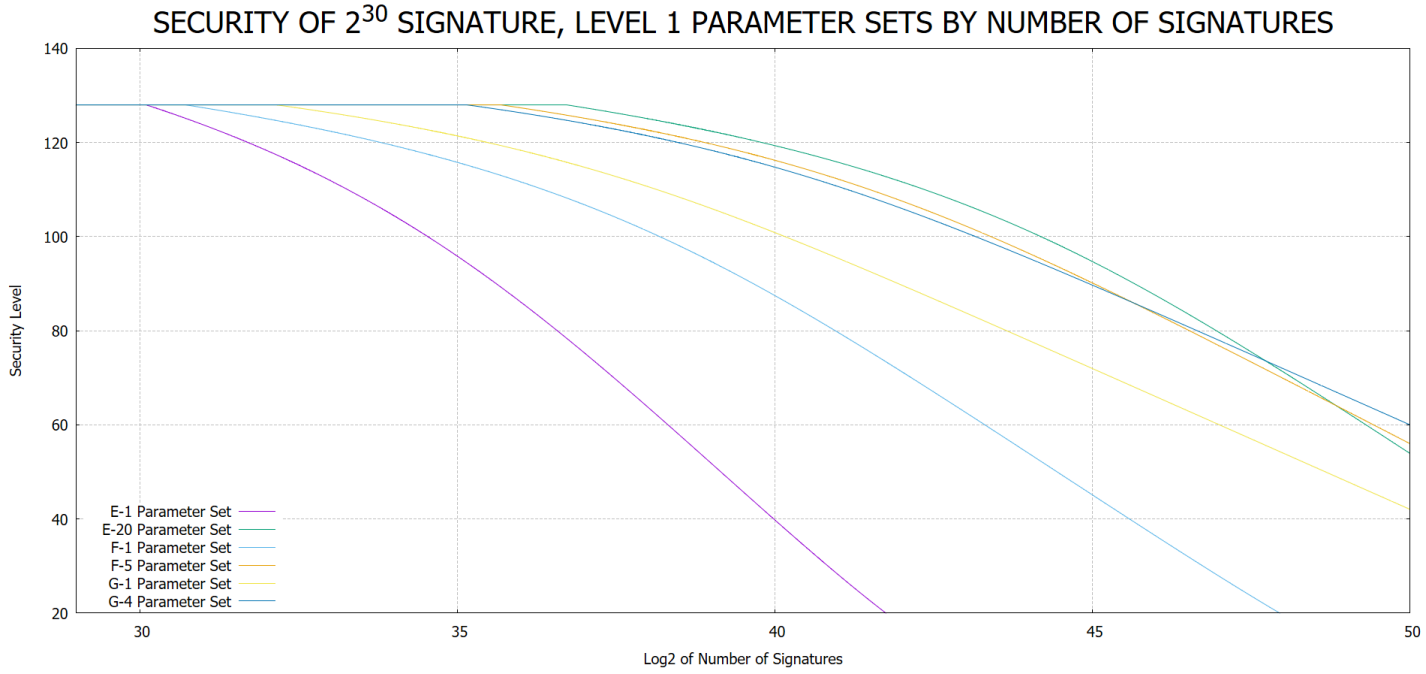


Figure 2: Recommended Parameter Sets

6.4 Parameter sets targeting 2^{40} signatures

Increasing the number of signatures to 2^{40}, we set the number of hashes to 1,000,000 and many parameter sets which have smaller signature sizes than the *bound-size*. Below are several of such parameter sets under the selection set (128, 112, 2^{40}, 1,000,000).

ID	h	d	a	k	w	SigSize	Sign Time	Verify Time	Sigs/level 112
H-1	42	7	13	11	64	5840	869230	5581	43.92
H-2	45	9	13	10	128	6000	938541	12292	45.24
H-3	49	7	11	11	32	6048	849646	3326	46.62
H-4	48	8	13	10	64	6096	951278	6342	48.24
H-5	40	5	13	12	16	6144	915951	1615	43.10
H-6	44	11	12	11	256	6176	901450	25544	44.12
H-7	49	7	13	10	32	6176	968431	3334	49.24
H-8	48	8	13	11	64	6320	967661	6356	49.92
H-9	44	11	13	11	256	6352	991562	25555	45.92
H-10	40	5	12	14	16	6368	834029	1629	43.47
H-11	40	5	13	13	16	6368	932334	1629	44.00
H-12	48	6	9	14	16	6384	877548	1876	45.39
H-13	49	7	13	11	32	6400	984814	3348	50.92
H-14	48	6	10	13	16	6432	889837	1879	46.76
H-15	48	6	12	11	16	6432	953327	1879	48.12
H-16	48	6	11	13	16	6640	916461	1892	48.99
H-17	48	6	12	12	16	6640	961518	1892	49.59
H-18	48	6	11	14	16	6832	920556	1904	49.99
H-19	48	6	12	13	16	6848	969709	1905	50.65

Table 8: Selection set (128, 112, 2^{40}, 1,000,000)

All of the parameter sets H-i$_s$ have smaller signatures than the *bound-size*. The biggest and smallest signature size reductions are 2,016 (7,856 - 5,840) and 1008 (7,856 - 6848) bytes which come with the parameter sets H-1 (42,7,13,11,64) and H-19 (48,6,12,13,16) respectively. H-1 is about 1,000 bytes smaller than H-19, but H-19 has a much smaller risk than H-1 by the factor of $2^{50.65-43.92} = 2^{6.73}$.

Signatures being around 6,000 bytes are not small enough for many applications.

The parameter set I-i$_s$ in the table below have smaller signature sizes than the parameter set H-i$_s$. I-i$_s$ have an upper bound of 10,000,000 hash operations for signing process and they were generated according to the selection set (128, 112, 2^{40}, 10,000,000).

ID	h	d	a	k	w	SigSize	Sign Time	Verify Time	Sigs/level 112
I-1	40	5	16	9	256	4544	7080434	11720	43.10
I-2	45	5	16	8	128	4592	7934963	6908	45.90
I-3	40	5	15	10	256	4656	6556145	11727	43.37
I-4	48	6	14	9	256	4672	7375857	14015	47.92
I-5	48	6	16	8	256	4688	8129522	14016	48.90
I-6	50	5	17	7	64	4752	9709556	4023	49.21
I-7	48	6	15	9	256	4816	7670769	14024	49.69
I-8	48	6	17	8	256	4816	9178098	14024	50.42
I-9	44	4	16	8	16	5136	5652468	1306	44.90
I-10	48	4	14	9	16	5184	9502707	1309	47.92
I-11	48	4	13	10	16	5264	9371634	1314	48.24
I-12	48	4	15	9	16	5328	9797619	1318	49.69
I-13	48	4	14	10	16	5424	9535474	1324	49.97
I-14	48	4	15	10	16	5584	9863154	1334	51.37

Table 9: Selection set (128, 112, 2^{40}, 10,000,000)

I-1 is the smallest signature. Interestingly, I-1 is 1,296 (5840 - 4544) bytes smaller than H-1 even though I-1 has higher security risk than H-1's by a small factor of $2^{43.92-43.10} = 2^{0.82}$.

Another interesting parameter set is I-14 which has the lowest security risk among all H and I parameter sets and it is smaller than all signatures from H parameter sets.

I-1 and I-14 are recommended for standardization consideration.

Increasing the number of hashes to 100,000,000, we found the parameter sets below:

ID	h	d	a	k	w	SigSize	Sign Time	Verify Time	Sigs/level 112
J-1	44	4	21	6	256	3984	62930936	9398	45.68
J-2	48	4	18	7	256	4064	79200248	9403	49.05
J-3	48	4	19	7	256	4176	82870264	9410	50.50
J-4	45	3	21	6	16	4528	80412664	1022	46.68
J-5	45	3	19	7	16	4656	62586872	1030	47.50
J-6	45	3	20	7	16	4768	69926904	1037	48.74
J-7	45	3	21	7	16	4880	84606968	1044	49.87
J-8	56	4	19	6	16	5072	43122680	1302	54.02

Table 10: Selection set (128, 112, 2^{40}, 100,000,000)

J-1 has the smallest signatures, while J-3 has better overuse properties. Even though J-8 has outstanding overuse properties, its relatively large signature size makes it unattractive.

J-1 and J-3 are recommended for standardization consideration.

Figure 3 illustrates the security degradation behaviors of the recommended parameter sets that can sign 2^{40} signatures with 128 bits of security strength.

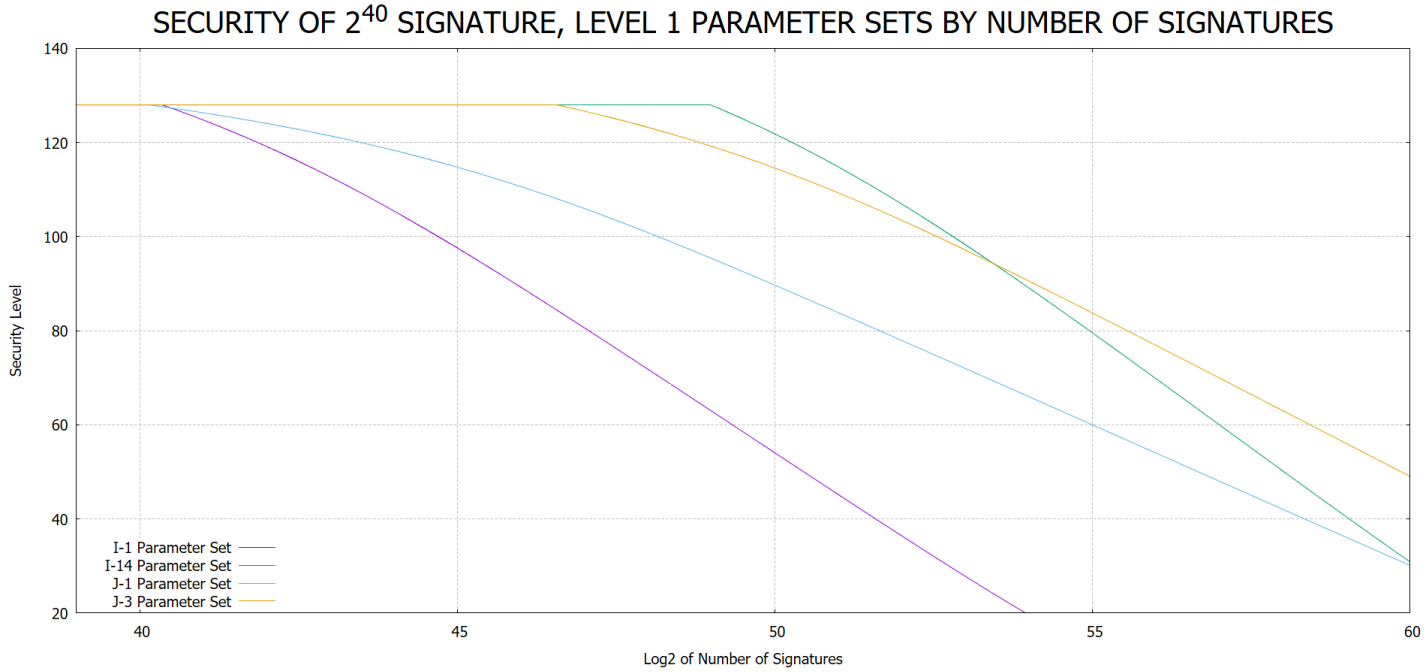


Figure 3: Recommended Parameter Sets

6.5 Parameter sets targeting 2^{50} signatures

To increase the maximum number of signatures per a signing key is a way to search for safer parameter sets. On the other hand, that also increases the signature size. Therefore, such parameter sets tend to have less signature size reductions.

K-i parameter sets in the table below were produced when we set the hash operation limit for signing to 1,000,000. The selection set was (128, 112, 2^{50}, 1,000,000).

ID	h	d	a	k	w	SigSize	Sign Time	Verify Time	Sigs/level 112
K-1	54	9	12	11	64	6624	975980	7120	54.12
K-2	56	8	10	13	32	6784	946155	3793	54.76
K-3	56	8	11	12	32	6800	968684	3794	55.63
K-4	56	8	10	14	32	6960	948202	3804	56.09
K-5	56	8	11	13	32	6992	972779	3806	56.99
K-6	60	10	9	14	64	7056	998632	7892	57.39
K-7	56	8	11	14	32	7184	976874	3818	57.99
K-8	60	10	9	15	64	7216	999655	7902	58.79
K-9	52	13	10	15	256	7232	989572	30184	53.08
K-10	48	6	12	15	16	7264	986091	1931	52.13
K-11	49	7	14	11	16	7360	863982	2183	52.35
K-12	52	13	10	16	256	7408	991619	30195	53.85
K-13	60	10	8	18	64	7408	993508	7914	59.00
K-14	48	6	12	16	16	7472	994282	1944	52.69
K-15	56	8	14	9	16	7552	870383	2441	55.92
K-16	60	10	8	19	64	7552	994019	7923	59.74
K-17	60	10	14	9	32	7616	869613	4687	59.92
K-18	56	8	13	10	16	7632	739310	2446	56.24
K-19	60	10	13	10	32	7696	738540	4692	60.24
K-20	56	8	14	10	16	7792	903150	2456	57.97
K-21	56	8	14	11	16	8032	935917	2471	59.35
K-22	63	9	13	9	16	8080	794862	2720	60.48

Table 11: Selection set (128, 112, 2^{50}, 1,000,000)

The smallest signature parameter set is K-1 whose signatures are 1,232 (7,856 - 6,624) bytes smaller than the *bound-size* and that is about 15% reduction. But, its risk of security degradation to below 112 bits is significantly larger than the smallest signature parameter sets' risks in draft FIPS 205. However, this parameter set might be good for some applications where the signature size reduction is impactful for performance. For parameter sets K-1, K-2, K-3, K-4, K-5, K-6, K-7, K-8, the signature gets bigger the overuse risk gets smaller.

It depends on a specific use case, which parameter set is most desirable. However, if we got to choose one to recommend: that would be K-1 since it has the smallest signature and 2^{50} signatures per key seems safe for most cases.

As seen, there were no parameter sets which had great signature size reductions produced under the selection set (128, 112, 2^{50}, 1,000,000), we tried with the selection set (128, 112, 2^{50}, 10,000,000). L-i$_s$ in the table below are several parameter sets that we found.

ID	h	d	a	k	w	SigSize	Sign Time	Verify Time	Sigs/level 112
L-1	54	6	16	8	128	5072	9312242	8262	54.90

L-2	56	7	14	9	256	5088	8556016	16328	55.92
L-3	56	7	16	8	256	5104	9309681	16329	56.90
L-4	56	7	15	9	256	5232	8850928	16337	57.69
L-5	56	7	14	10	256	5328	8588783	16343	57.97
L-6	60	6	15	8	64	5328	9973746	4804	58.94
L-7	64	8	13	9	256	5360	9588719	18632	61.48
L-8	55	5	18	7	16	5824	9424884	1595	56.05
L-9	55	5	15	9	16	6000	6344690	1606	56.69
L-10	55	5	17	8	16	6000	7852019	1606	57.42
L-11	55	5	18	8	16	6128	9949171	1614	58.70
L-12	55	5	17	9	16	6288	8114162	1624	59.32
L-13	55	5	16	10	16	6416	7065585	1632	59.58
L-14	66	6	13	9	16	6448	7053297	1880	63.48

Table 12: Selection set (128, 112, 2^{50}, 10,000,000)

The parameter set L-1's signature size is 2,784 (7,856 - 5072) bytes smaller than the *bound-size*. This is more than 35% reduction in size.

Another attractive parameter set is L-14 because its risk of security degradation to below 112 bits is extremely low and significantly lower than L-1's and its signature size is 1,408 (7,856 - 6,448) bytes smaller than the *bound-size*.

Many L parameter sets are good for consideration. There are trade-offs between SigSize, Sign Time, Verify Time and Sigs/level 112. One downside of these parameter sets is their slow signature generation operation.

L-1 and L-14 are recommended for consideration.

When we set the hash limit to 100,000,000, we get the following:

ID	h	d	a	k	w	SigSize	Sign Time	Verify Time	Sigs/level 112
M-1	60	5	17	7	256	4432	96247800	11713	59.21
M-2	60	5	18	7	256	4544	98082808	11720	61.05
M-3	60	4	17	7	16	5232	75497464	1312	59.21
M-4	60	4	20	6	16	5232	86245368	1312	60.10

Table 13: Selection set (128, 112, 2^{50}, 100,000,000)

M-1 has the smallest signature and relatively good overuse properties.
M-1 is recommended for standardization consideration.

Figure 4 illustrates the security degradation behaviors of the recommended parameter sets that can sign 2^{50} signatures with 128 bits of security strength.

6.6 Parameter sets with 192 bits of security

Similarly, we searched for parameter sets with 192 bits of security (which is NIST level 3) at different maximum numbers of signatures. However, instead of finding the bounds on total number of signatures per a signing key for the retention of 112 bits of security, we found the bounds for the retention of 128 bits of security. That means that when overuse happens, at what bound of the total number of generated signatures per a key pair of a particular parameter set still retains 128 bits of security.

The smallest signature parameter sets at 192-bit security level in FIPS 205 are SLH-DSA-SHA2-192s and SLH-DSA-SHAKE-192s and their signature size is 16,224 bytes. Again, we call this signature size, the *192-size* in this

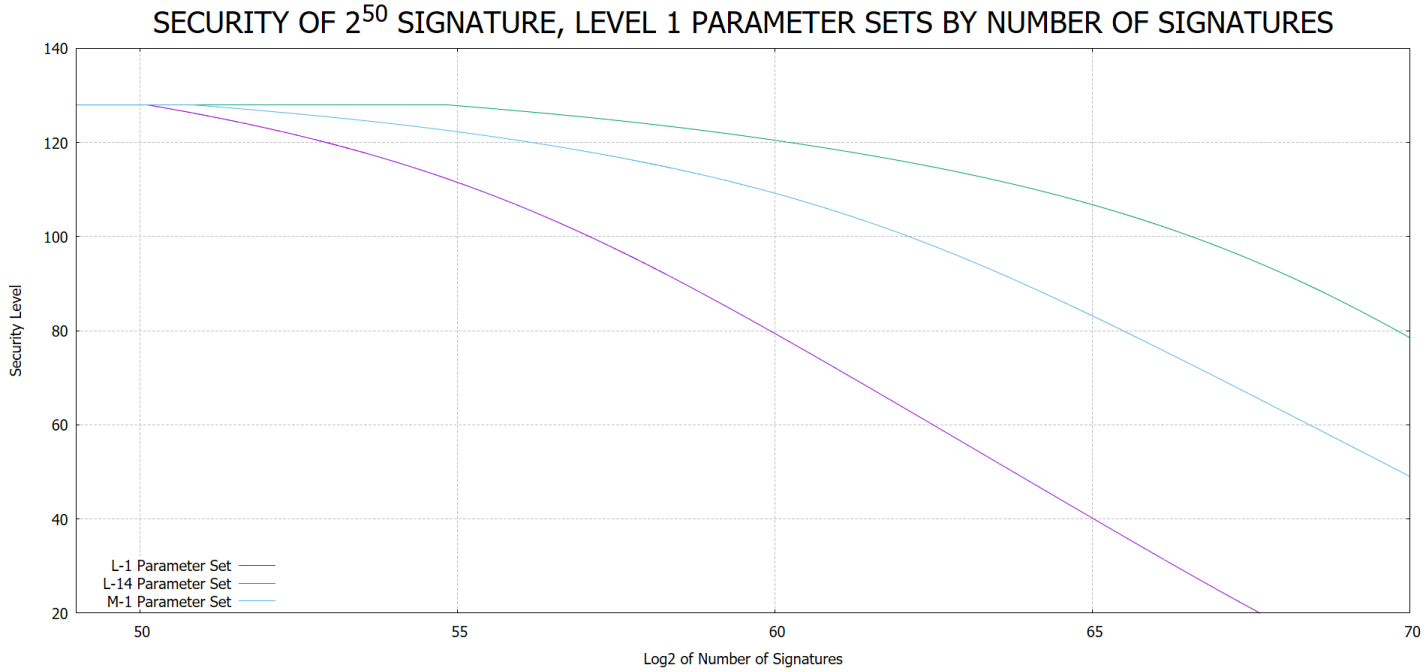


Figure 4: Recommended Parameter Sets

document to facilitate for easy discussions.

6.7 Level 3 security at 2^{20} signatures

We are now going to consider parameter sets under the selection set (192, 128, 2^{20}, 1,000,000). They are the N-i$_s$ in the table below.

ID	h	d	a	k	w	SigSize	Sign Time	Verify Time	Sigs/level 128
N-1	21	3	12	19	64	8904	991978	3537	25.95
N-2	24	4	13	16	64	9240	819692	4606	28.68
N-3	25	5	12	17	128	9528	753962	9853	29.00
N-4	24	4	13	17	64	9576	836075	4620	29.23
N-5	25	5	13	16	128	9600	876843	9856	29.68
N-6	20	4	11	23	256	9624	946405	13614	25.11
N-7	24	3	13	16	16	9648	890349	1477	28.68
N-8	28	4	12	16	32	9720	820204	2930	31.39
N-9	24	3	13	17	16	9984	906732	1491	29.23
N-10	28	7	12	16	256	10056	876745	23541	31.39
N-11	24	3	13	18	16	10320	923115	1505	29.70
N-12	28	4	12	16	16	10584	549868	1874	31.39

Table 14: Selection set (192, 128, 2^{20}, 1,000,000)

Interestingly, N-8, N-10 and N-12 have the same risk level of falling below 128 bits of security (because they share the same h, a, k parameters). But N-8 has the smallest signature size among them. N-1 has the smallest signature size, but its risk is significantly higher than N-8's.

N-1 and N-8 are recommended for standardization consideration.

Let's see how much reduction in signature sizes when using the upper bound of 10,000,000 hash function evaluations for a signing. O-i$_s$ are the parameter sets that we found under the selection set (192, 128, 2^{20}, 10,000,000)

ID	h	d	a	k	w	SigSize	Sign Time	Verify Time	Sigs/level 128
O-1	22	2	15	14	64	7560	9838576	2426	27.70
O-2	24	3	17	12	256	7656	8259057	10229	30.24
O-3	24	2	17	12	16	8232	9846770	1060	30.24

Table 15: Selection set (192, 128, 2^{20}, 10,000,000)

O-2 has smaller signature size than O-3 while they both have the same overuse risk. Therefore, O-1 and O-2 are recommended for standardization consideration.

When we increase the hash limit to 100,000,000, we get the following:

ID	h	d	a	k	w	SigSize	Sign Time	Verify Time	Sigs/level 128
P-1	24	2	18	11	256	6864	60309492	6893	30.28
P-2	26	2	21	9	16	7848	51150840	1044	32.73

Table 16: Selection set (192, 128, 2^{20}, 100,000,000)

P-1 has the best signature size, and decent overuse characteristics. P-2 has lower risk than P-1. However, the overuse risk of P-1 is very small for its 2^{20} signature limit. Therefore, in our view, P-1 is a better choice because its signature is about 1,000 bytes smaller than P-2's signature.

P-1 is recommended for standardization consideration.

Figure 5 illustrates the security degradation behaviors of the recommended parameter sets that can sign 2^{20} signatures with 192 bits of security strength.

6.8 Level 3 security at 2^{30} signatures

Now, searching under the Selection set (192, 128, 2^{30}, 1,000,000), we found the parameter sets Q-i$_s$ below.

ID	h	d	a	k	w	SigSize	Sign Time	Verify Time	Sigs/level 128
Q-1	30	5	13	18	64	10872	991849	5729	35.70
Q-2	36	6	12	17	64	11088	975593	6793	40.00
Q-3	32	4	12	19	16	11616	993257	1917	36.95
Q-4	36	9	9	24	256	12264	983295	30239	38.59
Q-5	35	5	12	17	16	12288	662762	2303	39.00
Q-6	35	5	13	16	16	12360	785643	2306	39.68
Q-7	35	5	13	17	16	12696	802026	2320	40.23

Table 17: Selection set (192, 128, 2^{30}, 1,000,000)

Q-2's signature size is about 300 bytes larger than Q-1's, but Q-2's risk of security degradation to below 128 bits is a factor of $2^{4.3}$ times smaller than Q-1's.

Q-1 and Q-2 are recommended for standardization consideration.

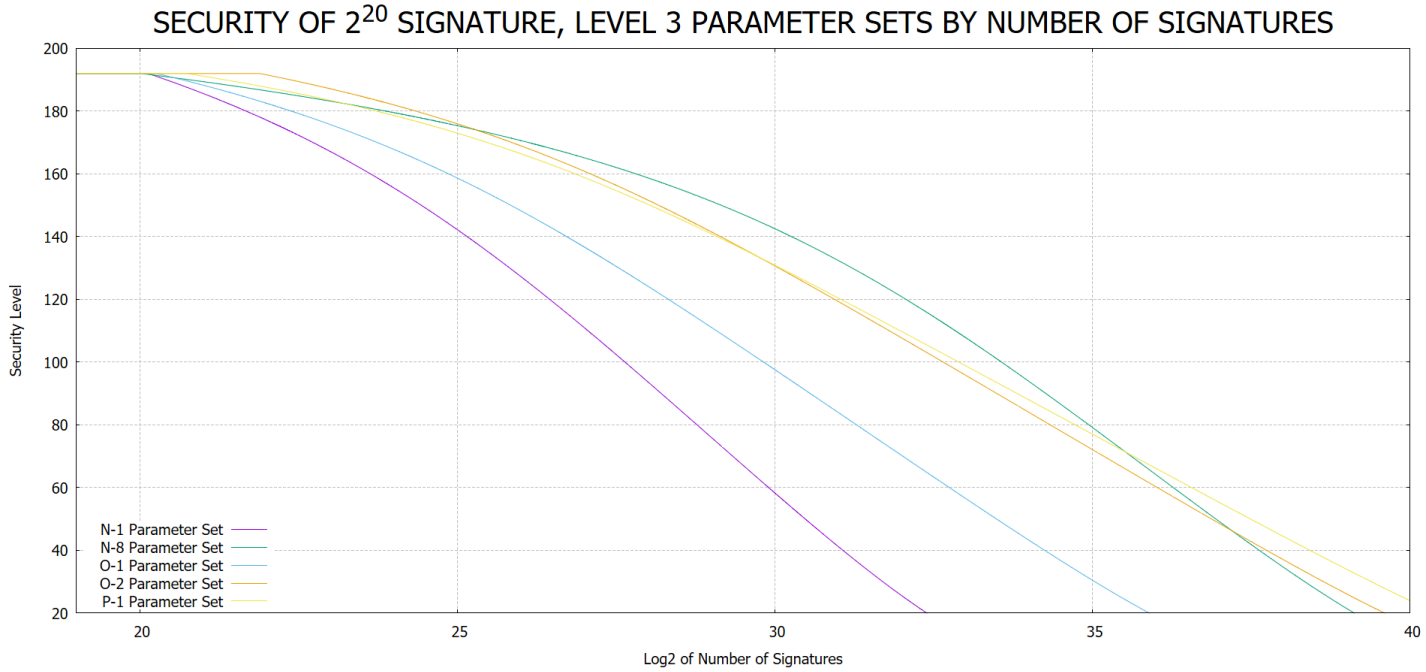


Figure 5: Recommended Parameter Sets

Now, searching under the Selection set (192, 128, 2^{30}, 10,000,000), we found the parameter sets R-i$_s$ below.

ID	h	d	a	k	w	SigSize	Sign Time	Verify Time	Sigs/level 128
R-1	32	4	16	13	256	8592	8521711	13571	38.04
R-2	36	4	16	12	128	8664	9441264	7926	41.14
R-3	32	4	16	14	256	9000	8652782	13588	38.78
R-4	40	5	12	16	256	9096	8653291	16895	43.39
R-5	33	3	17	12	16	9672	8171505	1478	39.24
R-6	33	3	17	13	16	10104	8433648	1496	40.09

Table 18: Selection set (192, 128, 2^{30}, 10,000,000)

R-2's signature size is only 72 bytes larger than R-1's signature size, but R-2's risk is the smallest risk in this category and a factor of $2^{3.1}$ times smaller than R-1's risk.

R-2 is recommended for standardization consideration.

Under the Selection Set (192, 128, 2^{30}, 100,000,000), we found the parameter sets below.

ID	h	d	a	k	w	SigSize	Sign Time	Verify Time	Sigs/level 128
S-1	36	3	19	10	256	7560	92299256	10225	42.11
S-2	30	2	21	10	16	8472	95551480	1070	38.18
S-3	30	2	20	11	16	8736	76677104	1081	38.34
S-4	30	2	21	11	16	9000	99745776	1092	39.35
S-5	36	3	21	9	16	9312	47800308	1463	42.73

Table 19: Selection set (192, 128, 2^{30}, 100,000,000)

S-1 has the smallest signatures and very good overuse characteristics; other than fast verify times, the other parameter sets don't have enough to justify their larger signatures.

S-1 is recommended for standardization consideration.

Figure 6 illustrates the security degradation behaviors of the recommended parameter sets that can sign 2^{30} signatures with 192 bits of security strength.

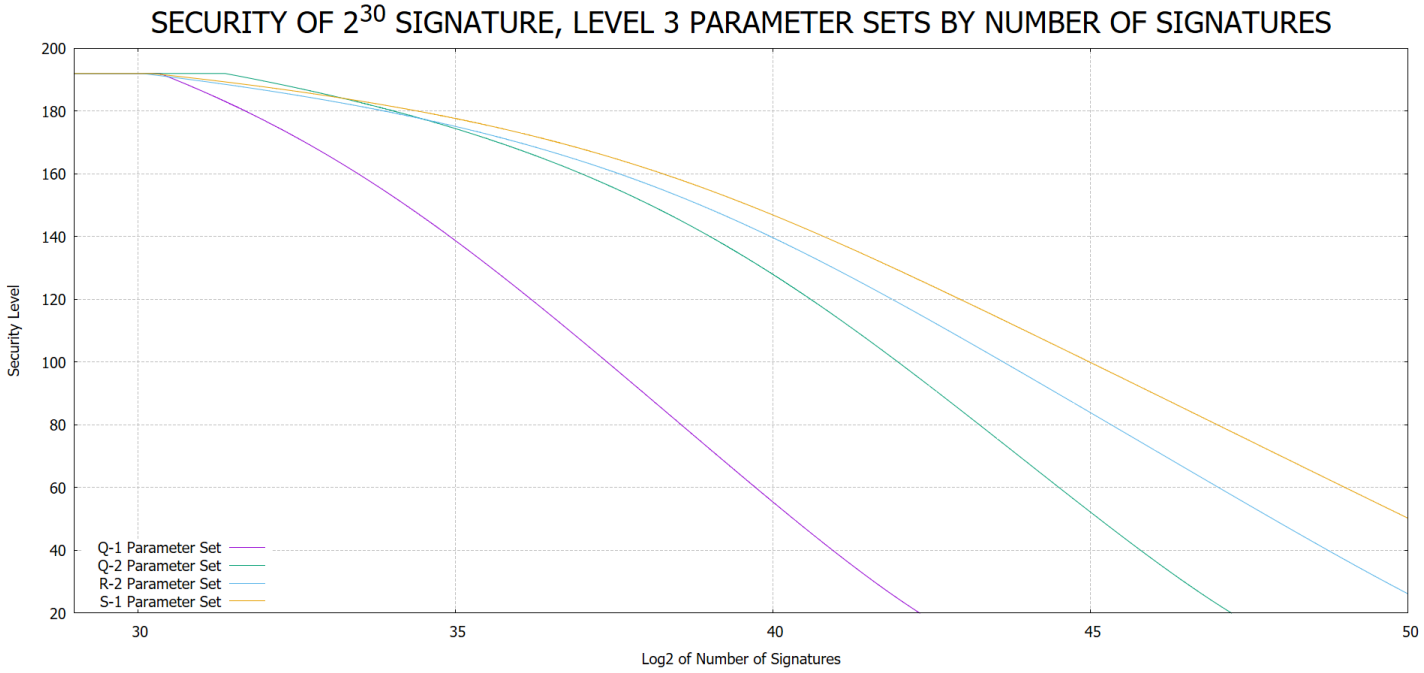


Figure 6: Recommended Parameter Sets

6.9 Level 3 security at 2^{40} signatures

Now, searching under the Selection set (192, 128, 2^{40}, 1,000,000), we found the parameter sets T-i$_s$ below.

ID	h	d	a	k	w	SigSize	Sign Time	Verify Time	Sigs/level 128
T-1	40	8	13	18	64	13560	852454	9006	45.70
T-2	45	9	12	17	64	13752	766502	10069	49.00
T-3	45	9	13	16	64	13824	889383	10072	49.68
T-4	42	6	13	17	16	14088	906729	2736	47.23
T-5	45	9	13	17	64	14160	905766	10086	50.23
T-6	42	6	13	18	16	14424	923112	2750	47.70
T-7	49	7	12	16	16	14760	863977	3122	52.39

Table 20: Selection set (192, 128, 2^{40}, 1,000,000)

T-1 has the smallest signature size and T-7 has the smallest risk of security degradation to below 128 bits. Therefore, they are recommended for standardization consideration.

Now, searching under the Selection set (192, 128, 2^{40}, 10,000,000), we found the parameter sets U-i$_s$ below.

ID	h	d	a	k	w	SigSize	Sign Time	Verify Time	Sigs/level 128
U-1	40	5	15	15	256	9864	9505260	16927	46.36
U-2	45	5	12	17	128	10008	9974762	9873	49.00
U-3	42	6	16	13	256	10080	6817261	20239	48.04
U-4	48	6	17	11	128	10248	8784879	11774	53.19
U-5	49	7	17	11	256	10320	8849134	23552	54.19
U-6	44	4	17	12	16	11160	9846768	1898	50.24

Table 21: Selection set (192, 128, 2^{40}, 10,000,000)

U-1 and U-5 are recommended for standardization recommendation based on having smallest signature size and smallest risk respectively.

When increasing the number of hashes to 100,000,000, we get the following parameter sets:

ID	h	d	a	k	w	SigSize	Sign Time	Verify Time	Sigs/level 128
V-1	44	4	18	11	256	8592	60309488	13571	50.28
V-2	45	3	18	11	16	9792	86179832	1483	51.28

Table 22: Selection set (192, 128, 2^{40}, 100,000,000)

V-1 has the smallest signatures and very good overuse characteristics. V-2 has lower risk than V-1. However, the overuse risk of V-1 is very small for its 2^{40} signature limit. Therefore, in our view, V-1 is a better choice because its signature is 1,200 bytes smaller than V-2's signature. V-1 is recommended for consideration.

Figure 7 illustrates the security degradation behaviors of the recommended parameter sets that can sign 2^{40} signatures with 192 bits of security strength.

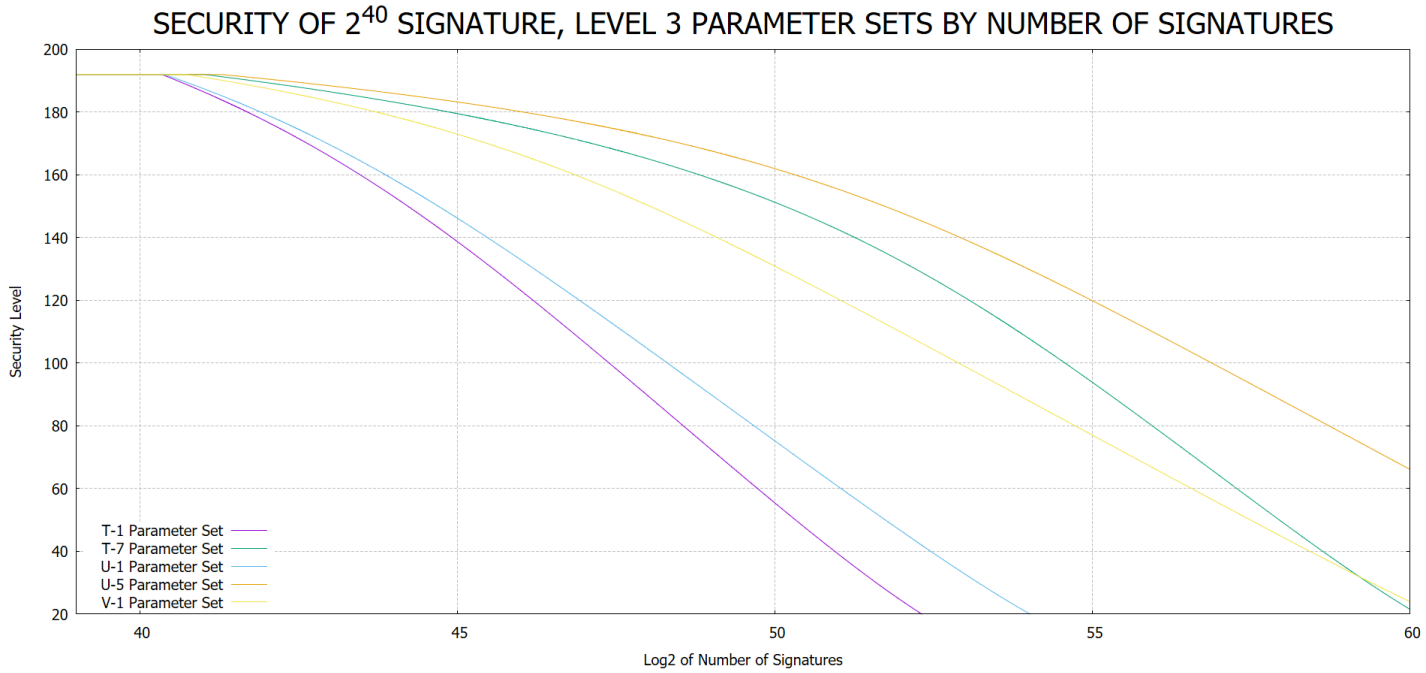


Figure 7: Recommended Parameter Sets

6.10 Level 3 security at 2^{50} signatures

Now, searching under the Selection set (192, 128, 2^{50}, 1,000,000), we found the parameter sets W-i$_s$ below.

ID	h	d	a	k	w	SigSize	Sign Time	Verify Time	Sigs/level 128
W-1	50	10	13	18	64	15432	991844	11194	55.70
W-2	55	11	12	17	64	15624	905892	12257	59.00
W-3	55	11	12	18	64	15936	914083	12270	59.51
W-4	55	11	12	19	64	16248	922274	12283	59.95
W-5	60	12	12	16	64	16248	967396	13338	63.39
W-6	49	7	12	21	16	16320	904932	3187	54.69
W-7	56	8	12	17	16	16464	976871	3551	60.00

Table 23: Selection set (192, 128, 2^{50}, 1,000,000)

Only W-1, W-2 and W-3 have smaller signature sizes than the *192-size*, but with small percentages in the signature reductions. We don't think they are good choices for consideration.

Now, searching under the Selection set (192, 128, 2^{50}, 10,000,000), we found the parameter sets X-i$_s$ below.

ID	h	d	a	k	w	SigSize	Sign Time	Verify Time	Sigs/level 128
X-1	56	8	16	12	256	11256	8390636	26894	61.14
X-2	55	5	12	17	16	12768	8515562	2323	59.00
X-3	55	5	13	16	16	12840	8638443	2326	59.68
X-4	55	5	15	14	16	12840	9293805	2326	60.70

Table 24: Selection set (192, 128, 2^{50}, 10,000,000)

X-1 has the smallest signature size and the lowest risk. The downside is its verification time which is about 10 times the other 3 parameter sets' verification times.

X-1 is recommended for standardization consideration. If X-1's verification time is not acceptable, X-4 is the recommended one for consideration.

Increasing the hash limit to 100,000,000, we found the parameter sets below:

ID	h	d	a	k	w	SigSize	Sign Time	Verify Time	Sigs/level 128
Y-1	55	5	18	11	256	9480	73945072	16911	61.28
Y-2	56	4	21	9	16	11016	91357168	1892	62.73

Table 25: Selection set (192, 128, 2^{50}, 100,000,000)

Y-1 has the smallest signatures and very good overuse characteristics. Y-2 has lower risk than Y-1, but not much. In addition, the overuse risk of Y-1 is very small for its 2^{50} signature limit. Therefore, in our view, Y-1 is a better choice because its signature is 1,536 bytes smaller than Y-2's signature. Y-1 is recommended for consideration.

Figure 8 illustrates the security degradation behaviors of the recommended parameter sets that can sign 2^{50} signatures with 192 bits of security strength.

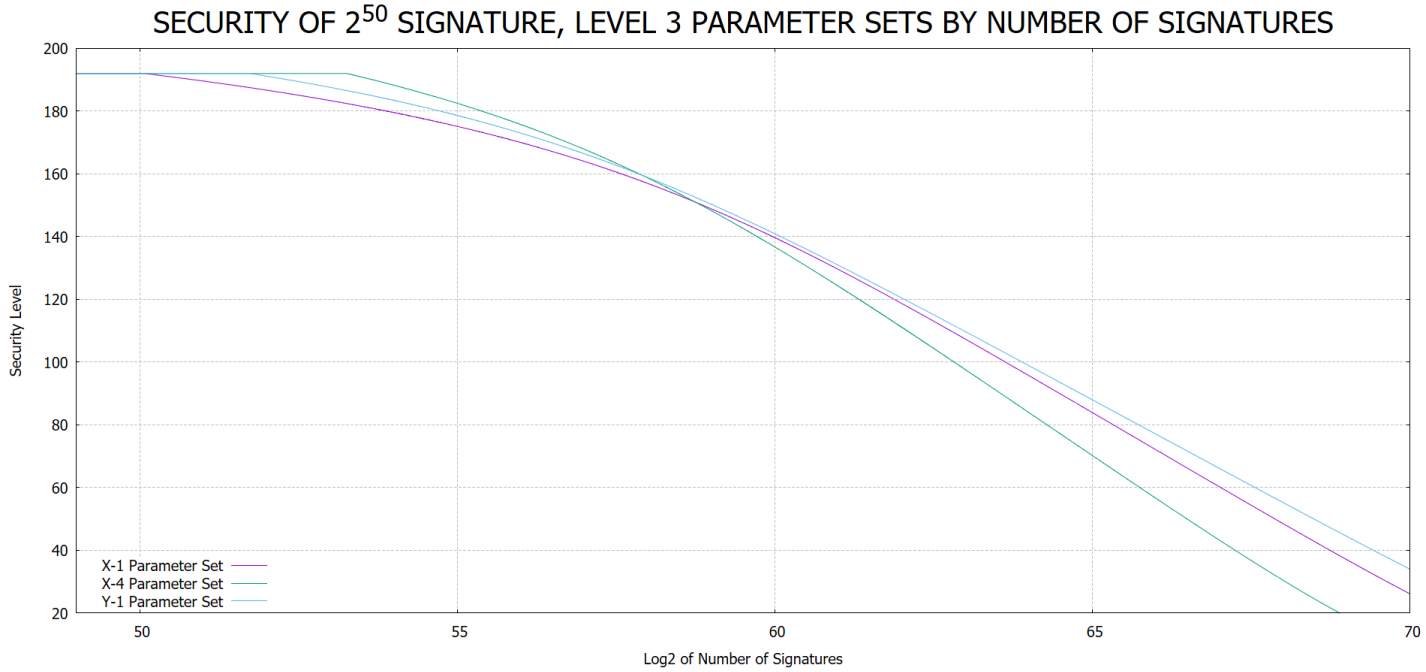


Figure 8: Recommended Parameter Sets

7 Conclusions

In this paper, we figured out what is the success probability of a forgery attack with a random or chosen message by an attacker when they are given 2^m valid signatures. This success probability is called p in the equation (1). For any given parameter set, when m increases, p increases. From here, we plotted the security degradation behavior of a given parameter set, especially at what value of m, the security strength falls below the retained security level which is either 112 or 128 in this paper.

We generated SPHINCS+ parameter sets, then grouped them based on a Selection Set which has 4 variables as following:

- The security level of the parameter sets (either 128 or 192 bits).
- The retained security strength when overuse happens (either 112 or 128 bits).
- The maximum number of signatures allowed to be generated under 1 signing key (either 2^{20}, 2^{30}, 2^{40}, 2^{50}).
- The limit for the numbers of hashes per signing operation (100,000, 1,000,000, 10,000,000 or 100,000,000).

We evaluated the parameter sets under each Selection Set and provided our recommended parameter sets for further consideration. In most cases, the overuse risks and signature sizes among the parameter sets in a group are the most important factors for recommendation considerations. Our recommended parameter sets are repeated below.

Under the selection set (128, 112, 2^{20}, 100,000): A-1 and A-19 1
Under the selection set (128, 112, 2^{20}, 1,000,000): B-1 and B-21 2
Under the selection set (128, 112, 2^{20}, 10,000,000): C-2, C-9, C-11 3
Under the selection set (128, 112, 2^{20}, 100,000, 000): D-1 and D-8 4
Under the selection set (128, 112, 2^{30}, 1,000,000): E-1 and E-20 5
Under the selection set (128, 112, 2^{30}, 10,000,000): F-1 and F-5 6
Under the selection set (128, 112, 2^{30}, 100,000,000): G-1 and G-4 7
Under the selection set (128, 112, 2^{40}, 10,000,000): I-1 and I-14 9

Under the selection set (128, 112, 2^{40}, 100,000,000): J-1 and J-3 10
Under the selection set (128, 112, 2^{50}, 1,000,000): K-1 11
Under the selection set (128, 112, 2^{50}, 10,000,000): L-1 and L-14 12
Under the selection set (128, 112, 2^{50}, 100,000,000): M-1 13
Under the selection set (192, 128, 2^{20}, 1,000,000): N-1 and N-8 14
Under the selection set (192, 128, 2^{20}, 10,000,000): O-1 and O-2 15
Under the selection set (192, 128, 2^{20}, 100,000,000): P-1 16
Under the selection set (192, 128, 2^{30}, 1,000,000): Q-1 and Q-2 17
Under the selection set (192, 128, 2^{30}, 10,000,000): R-2 18
Under the selection set (192, 128, 2^{30}, 100,000,000): S-1 19
Under the selection set (192, 128, 2^{40}, 1,000,000): T-1 and T-7 20
Under the selection set (192, 128, 2^{40}, 10,000,000): U-1 and U-5 21
Under the selection set (192, 128, 2^{40}, 100,000,000): V-1 22
Under the selection set (192, 128, 2^{50}, 10,000,000): X-1 and X-4 24
Under the selection set (192, 128, 2^{50}, 100,000,000): Y-1 25

We generated other parameter sets which were not discussed in the main body of this paper. They are listed in the Appendix A.

References

[1] National Institute of Standards and Technology. Stateless hash-based digital signature standard. (U.S. Department of Commerce, Washington, DC), Draft Federal Information Processing Standards Publication (FIPS) 205, August 2023. https://doi.org/10.6028/NIST.FIPS.205.ipd.

[2] Daniel J. Bernstein, Daira Hopwood, Andreas Huuml;lsing, Tanja Lange, Ruben Niederhagen, Louiza Papachristodoulou, Michael Schneider, Peter Schwabe, and Zooko Wilcox-O'Hearn. Sphincs: Practical stateless hash-based signatures. In *EUROCRYPT (1)*, pages 368–397. Springer, 2015.

[3] National Institute of Standards and Technology. SHA-3 standard: Permutation-based hash and extendable-output functions. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 202, August 2015. https://doi.org/10.6028/NIST.FIPS.202.

[4] National Institute of Standards and Technology. Secure hash standard (SHS). (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 180-4, August 2015. https://doi.org/10.6028/NIST.FIPS.180-4.

[5] National Institute of Standards and Technology. Module-lattice-based digital signature standard. (U.S. Department of Commerce, Washington, DC), Draft Federal Information Processing Standards Publication (FIPS) 204, August 2023. https://doi.org/10.6028/NIST.FIPS.204.ipd.

A Additional parameter sets

We also generated other sets of parameter sets where the signing bound was 100,000 hashes. However, except for the Level 1, 2^{20}-signature parameter sets, we didn't find anything to recommend because either we felt that the signature size reduction was not significant over the *bound-size* or the signatures were even larger than the *bound-size* or the *192-size* for the security Level 1 or Level 3 respectively.

Here are those parameter sets:

For Level 1, 2^{30} signatures:

ID	H	D	A	K	W	SigSize	Sign Time	Verify Time	Sigs/level 112
1	32	8	9	17	16	7728	89319	2452	32.65
2	32	8	9	18	16	7888	90342	2462	33.31
3	36	9	9	15	16	8032	96264	2717	34.79
4	36	9	9	16	16	8192	97287	2727	35.83
5	36	9	9	17	16	8352	98310	2737	36.65
6	36	9	9	18	16	8512	99333	2747	37.31
7	40	10	8	17	16	8704	98597	3005	38.08
8	40	10	8	18	16	8848	99108	3014	39.00
9	40	10	8	19	16	8992	99619	3023	39.74
10	40	10	7	24	16	9328	96030	3044	39.85
11	40	10	7	25	16	9456	96285	3052	40.24

Table 26: Selection set (128, 112, 2^{30}, 100,000)

For Level 1, 2^{40} signatures:

ID	H	D	A	K	W	SigSize	Sign Time	Verify Time	Sigs/level 112
1	40	10	7	29	16	9968	97305	3084	41.44
2	40	10	7	30	16	10096	97560	3092	41.67
3	40	10	7	31	16	10224	97815	3100	41.88
4	40	10	7	32	16	10352	98070	3108	42.07
5	40	10	7	33	16	10480	98325	3116	42.25
6	40	10	7	34	16	10608	98580	3124	42.41
7	40	10	7	35	16	10736	98835	3132	42.57
8	40	10	7	36	16	10864	99090	3140	42.71
9	40	10	7	37	16	10992	99345	3148	42.84
10	40	10	7	38	16	11120	99600	3156	42.97
11	42	14	10	15	16	11168	93635	4143	43.08
12	40	10	7	39	16	11248	99855	3164	43.09
13	44	11	10	14	8	11280	93767	2235	44.09
14	42	14	10	16	16	11344	95682	4154	43.85
15	44	11	10	15	8	11456	95814	2246	45.08
16	42	14	10	17	16	11520	97729	4165	44.48
17	45	15	10	14	16	11600	96083	4416	45.09
18	44	11	10	16	8	11632	97861	2257	45.85
19	45	15	10	15	16	11776	98130	4427	46.08
20	44	11	10	17	8	11808	99908	2268	46.48
21	48	12	10	13	8	11904	97639	2413	46.76
22	45	15	9	18	16	12016	85839	4442	46.31
23	48	12	9	15	8	12016	86373	2420	46.79
24	48	16	10	13	16	12032	98531	4689	46.76
25	48	12	10	14	8	12080	99686	2424	48.09
26	48	16	9	15	16	12144	87265	4696	46.79
27	45	15	9	19	16	12176	86862	4452	46.85
28	48	16	9	16	16	12304	88288	4706	47.83
29	48	12	9	17	8	12336	88419	2440	48.65
30	48	16	9	17	16	12464	89311	4716	48.65
31	48	12	9	18	8	12496	89442	2450	49.31
32	48	16	9	18	16	12624	90334	4726	49.31
33	48	12	9	19	8	12656	90465	2460	49.85
34	51	17	9	15	16	12752	91760	4980	49.79
35	48	16	9	19	16	12784	91357	4736	49.85

36	48	12	9	20	8	12816	91488	2470	50.32
37	51	17	9	16	16	12912	92783	4990	50.83

Table 27: Selection set (128, 112, 2^{40}, 100,000)

For Level 1, 2^{50} signatures:

ID	H	D	A	K	W	SigSize	Sign Time	Verify Time	Sigs/level 112
1	52	13	9	17	8	13136	94338	2629	52.65
2	51	17	9	18	16	13232	94829	5010	52.31
3	52	13	9	18	8	13296	95361	2639	53.31
4	51	17	9	19	16	13392	95852	5020	52.85
5	52	13	9	19	8	13456	96384	2649	53.85
6	54	18	9	16	16	13520	97278	5274	53.83
7	52	13	9	20	8	13616	97407	2659	54.32
8	56	14	9	15	8	13616	98211	2798	54.79
9	54	18	9	17	16	13680	98301	5284	54.65
10	56	14	9	16	8	13776	99234	2808	55.83
11	54	18	9	18	16	13840	99324	5294	55.31
12	56	14	8	20	8	14096	93086	2828	56.35
13	57	19	8	18	16	14160	94603	5560	56.00
14	56	14	8	21	8	14240	93597	2837	56.86
15	57	19	8	19	16	14304	95114	5569	56.74
16	60	15	8	16	8	14320	96961	2981	56.89
17	56	14	8	22	8	14384	94108	2846	57.31
18	57	19	8	20	16	14448	95625	5578	57.35
19	60	15	8	17	8	14464	97472	2990	58.08
20	57	19	8	21	16	14592	96136	5587	57.86
21	60	15	8	18	8	14608	97983	2999	59.00
22	60	20	8	17	16	14624	98587	5835	58.08
23	57	19	8	22	16	14736	96647	5596	58.31
24	60	15	8	19	8	14752	98494	3008	59.74
25	60	20	8	18	16	14768	99098	5844	59.00
26	60	15	8	20	8	14896	99005	3017	60.35
27	60	20	8	19	16	14912	99609	5853	59.74
28	60	20	7	24	16	15248	96020	5874	59.85
29	63	21	7	20	16	15344	99495	6126	60.50

Table 28: Selection set (128, 112, 2^{50}, 100,000)

For Level 3, 2^{20} signatures:

ID	H	D	A	K	W	SigSize	Sign Time	Verify Time	Sigs/level 128
1	20	5	9	31	16	14064	97148	2377	24.29
2	20	5	9	32	16	14304	98171	2387	24.45
3	24	6	8	30	16	14424	93852	2750	26.51
4	24	6	8	31	16	14640	94363	2759	26.73
5	24	6	8	32	16	14856	94874	2768	26.92
6	24	6	8	33	16	15072	95385	2777	27.11
7	24	6	8	34	16	15288	95896	2786	27.28
8	28	7	7	32	16	15408	99769	3149	28.94
9	27	9	9	23	16	17208	82416	3940	29.22
10	27	9	9	24	16	17448	83439	3950	29.59

11	28	7	9	23	8	17472	83778	2143	30.22
12	27	9	9	25	16	17688	84462	3960	29.91
13	27	9	9	26	16	17928	85485	3970	30.20

Table 29: Selection set (192, 128, 2^{20}, 100,000)

For Level 3, 2^{30} signatures:

ID	H	D	A	K	W	SigSize	Sign Time	Verify Time	Sigs/level 128
1	32	8	9	27	8	20136	96477	2456	35.46
2	32	8	9	28	8	20376	97500	2466	35.69
3	30	10	9	31	16	20424	97143	4432	34.29
4	33	11	9	26	16	20520	98571	4794	36.20
5	33	11	9	27	16	20760	99594	4804	36.46
6	36	9	8	28	8	21408	91771	2711	38.01
7	36	12	8	28	16	21624	92824	5198	38.01
8	36	9	8	29	8	21624	92282	2720	38.27
9	36	12	8	29	16	21840	93335	5207	38.27
10	36	9	8	30	8	21840	92793	2729	38.51
11	36	12	8	30	16	22056	93846	5216	38.51
12	36	9	8	31	8	22056	93304	2738	38.73
13	36	12	8	31	16	22272	94357	5225	38.73
14	36	9	8	32	8	22272	93815	2747	38.92
15	40	10	8	25	8	22464	98845	2957	41.03
16	36	12	8	32	16	22488	94868	5234	38.92
17	39	13	8	26	16	22488	98345	5592	40.40

Table 30: Selection set (192, 128, 2^{30}, 100,000)

For Level 3, 2^{40} signatures:

ID	H	D	A	K	W	SigSize	Sign Time	Verify Time	Sigs/level 128
1	39	13	9	33	8	29784	89698	3868	43.61
2	42	14	9	27	8	30024	87863	4080	45.46
3	42	14	9	28	8	30264	88886	4090	45.69
4	42	14	9	29	8	30504	89909	4100	45.91
5	42	14	9	30	8	30744	90932	4110	46.10
6	42	14	9	31	8	30984	91955	4120	46.29
7	45	15	9	25	8	31224	90120	4332	47.91
8	45	15	9	26	8	31464	91143	4342	48.20
9	45	15	9	27	8	31704	92166	4352	48.46
10	45	15	9	28	8	31944	93189	4362	48.69
11	45	15	9	29	8	32184	94212	4372	48.91
12	48	16	9	23	8	32424	92377	4584	50.22
13	40	10	9	31	4	32664	96663	2382	44.29
14	38	19	9	36	16	32832	98977	8171	43.02
15	40	20	9	31	16	32904	97133	8532	44.29
16	40	10	9	32	4	32904	97686	2392	44.45
17	40	20	9	32	16	33144	98156	8542	44.45
18	40	10	9	33	4	33144	98709	2402	44.61
19	42	21	9	27	16	33216	96312	8903	45.46
20	42	21	9	28	16	33456	97335	8913	45.69
21	42	21	9	29	16	33696	98358	8923	45.91

22	44	11	9	25	4	33744	97020	2529	46.91
23	42	21	9	30	16	33936	99381	8933	46.10
24	44	11	9	26	4	33984	98043	2539	47.20
25	44	22	9	25	16	34008	97537	9294	46.91
26	44	11	9	27	4	34224	99066	2549	47.46
27	44	22	9	26	16	34248	98560	9304	47.20
28	44	22	9	27	16	34488	99583	9314	47.46
29	46	23	9	24	16	35040	99785	9695	48.59
30	46	23	8	31	16	35976	91074	9734	48.73
31	48	12	8	27	4	36096	91737	2729	49.72
32	46	23	8	32	16	36192	91585	9743	48.92
33	48	12	8	28	4	36312	92248	2738	50.01
34	48	24	8	27	16	36384	92301	10109	49.72
35	48	24	8	28	16	36600	92812	10118	50.01

Table 31: Selection set (192, 128, 2^{40}, 100,000)

For Level 3, 2^{50} signatures:

ID	H	D	A	K	W	SigSize	Sign Time	Verify Time	Sigs/level 128
1	51	17	8	35	8	36144	91036	4941	54.44
2	51	17	8	36	8	36360	91547	4950	54.59
3	51	17	8	37	8	36576	92058	4959	54.72
4	54	18	8	30	8	36744	92784	5168	56.51
5	54	18	8	31	8	36960	93295	5177	56.73
6	54	18	8	32	8	37176	93806	5186	56.92
7	54	18	8	33	8	37392	94317	5195	57.11
8	54	18	8	34	8	37608	94828	5204	57.28
9	57	19	8	27	8	37776	95554	5413	58.72
10	57	19	8	28	8	37992	96065	5422	59.01
11	57	19	8	29	8	38208	96576	5431	59.27
12	57	19	8	30	8	38424	97087	5440	59.51
13	57	19	8	31	8	38640	97598	5449	59.73
14	57	19	8	32	8	38856	98109	5458	59.92
15	60	20	8	25	8	39024	98835	5667	61.03
16	54	27	7	37	16	41472	97752	11395	55.94
17	54	27	7	38	16	41664	98007	11403	56.10
18	56	14	7	34	4	41832	99600	3172	57.39
19	54	27	7	39	16	41856	98262	11411	56.25
20	56	14	7	35	4	42024	99855	3180	57.59
21	54	18	9	28	4	51672	87090	3990	57.69
22	54	18	9	29	4	51912	88113	4000	57.91
23	54	18	9	30	4	52152	89136	4010	58.10
24	54	18	9	31	4	52392	90159	4020	58.29
25	54	18	9	32	4	52632	91182	4030	58.45
26	54	18	9	33	4	52872	92205	4040	58.61
27	57	19	9	23	4	52968	85222	4146	59.22
28	57	19	9	24	4	53208	86245	4156	59.59
29	57	19	9	25	4	53448	87268	4166	59.91
30	57	19	9	26	4	53688	88291	4176	60.20

Table 32: Selection set (192, 128, 2^{50}, 100,000)