A note on the prime in SQISignHD

Tako Boris Fouotsa

EPFL, Lausanne, Switzerland

Abstract. In this note, we propose new primes for the SQISignHD signature algorithm. SQISignHD uses primes of the form $p = 2^a 3^b f - 1$. We argue that using primes p such that $p^2 - 1$ has a smooth factor $2^{a+1}T$, with $2^a > 2\sqrt{p}\log p$, $T \geq \sqrt{p}$ and T being very smooth allows a faster response verification. Contrarily to SQISign/BSIDH primes, these primes are easy to generate. Moreover, since one has access to smooth torsion of order larger than p, then the degrees of the secret isogenies can be chosen to be larger than p, as opposed to the current SQISignHD version where they are smaller than p.

Keywords: Supersingular Isogenies · SQISign · SQISignHD.

1 Introduction

SQISign [7,8] is a digital signature scheme whose design is inspired by the GPS [10] signature. Its security relies on the problem of computing a non trivial endomorphism of a random supersingular elliptic curve. In the identification scheme used in SQISign, a starting curve E_0 with known endomorphism ring $\mathcal{O}_0$ is fixed, the secret is an isogeny $\tau : E_0 \to E_A$. The commitment is a curve E_1 obtained by computing a random isogeny $\psi : E_0 \to E_1$. The challenge is a random isogeny $\varphi : E_1 \to E_2$. The response consists of a random isogeny $\sigma : E_A \to E_2$. Figure 1 illustrates this identification protocol.

$$\begin{tikzcd}
E_0 \arrow[r, "\tau"] \arrow[d, "\psi"'] & E_A \arrow[d, "\sigma"] \\
E_1 \arrow[r, "\varphi"'] & E_2
\end{tikzcd}$$

Fig. 1. The SQISign identification protocol.

The response computation heavily relies on the so called Deuring correspondence [9] that allows the owner of the secret key to recover the endomorphism rings $\mathcal{O}_A$ and $\mathcal{O}_2$ of E_A and E_2 respectively, to compute the connecting ideal $I = I(\mathcal{O}_A, \mathcal{O}_2)$, to solve for an equivalent ideal $J \sim I$ of smooth norm using an improved version [7] of the the KLPT algorithm [12], and to translate the ideal J into an isogeny σ. The degree of the isogeny σ is very large (roughly $p^{15/4}$). For these computations to be efficient, there are several requirements that need to be satisfied, among which, the prime p used needs to be twin smooth, also referred to as BSIDH primes in Isogeny-Based Cryptography. Finding such primes is not easy [4,7,8,5,1]. This has a negative impact on the efficiency of the scheme and makes it difficult to instantiate SQISign for security levels higher that 128 without efficiency loss.

In the recently proposed SQISignHD [6], the SQISign signature algorithm was redesigned using the SIDH attacks [2,13,16]. In fact, with these attacks, it has been shown by Robert [14] that an isogeny of generic degree can be represented using solely its action on some large enough smooth order torsion points. This means that in SQISign, instead of returning a random isogeny $\sigma : E_A \to E_2$ of large smooth degree, one could return a random short isogeny $\sigma_I : E_A \to E_2$ of generic degree using the new representation. Note that evaluating an isogeny of generic degree has exponential cost in general, but the signer can use the knowledge of the endomorphism rings of E_A and E_2 to solve this task in polynomial time. This change in SQISign, together with other smart tricks, totally remove the many constraints on the base prime and allows to use SIDH primes $p = 2^a 3^b f - 1$, which make it easy to instantiate SQISignHD for any security level. Moreover, the signature scheme is more compact, and the security reduction is much more compelling. For efficiency reasons, the commitment isogeny is computed from E_A and the response isogeny is $\sigma_I : E_1 \to E_2$. This is illustrated in Figure 2.

$$\begin{tikzcd}
E_0 \arrow[r, "\tau"] \arrow[d, "\psi"'] & E_A \arrow[d, "\varphi"] \\
E_1 \arrow[r, "\sigma_I"'] & E_2
\end{tikzcd}$$

Fig. 2. The (high level) SQISignHD identification protocol.

The natural way to represent the isogeny response isogeny σ_I (using only its action on a power of 2 torsion) requires that $\deg \sigma_I < 2^a$. But, in SQISignHD [6, §5.2], it is shown that $q := \deg \sigma_I \leq 2\sqrt{2p}/\pi =: q_{max}$ in general, hence $2^a < q$ most of the time. For an efficient representation of the response isogeny in dimension 4, one further requires that $2^{2r} - q$ is a prime congruent to 1 modulo 4, for some well chosen $r \leq a$. This implies that one should expect $q_{max} < q$ with high probability. The SQISignHD signature algorithm represents the response isogeny σ_I using its evaluation on the 2^r-torsion as far as $q < 2^{2r}$ [6, §5.6].

This representation is less efficient. We hence propose to change of the base p prime in such a way that the 2^a-torsion available satisfies $\deg \sigma_I < 2^a$. In fact, we know that there always exists an ideal I of norm $q < q_{max}$. If we require that $2^r - q$ is a prime, then we can heuristically find such an ideal with the norm $q < q_{max} \log p$. If we further require that the prime $2^r - q$ is congruent to 1 modulo 4, then we can can hope to find such an ideal with with the norm $q < 2q_{max} \log p$. Hence, having 2^a larger than $2q_{max} \log p$ heuristically assures that the optimal isogeny representation will be used. Having 2^a larger than $2q_{max} \log p$ and $p = 2^a 3^b - 1$ means that 3^b is considerably smaller than $\sqrt{p} \approx 2^{\lambda}$. This implies that the secret isogeny, the commitment isogeny and the challenge isogeny do not offer enough security. To address this, we compensate the loss created by increasing a with the smooth part of $p-1$. That is, we choose p such that $p^2 - 1 = 2^{a+1}Tf$ where $T > \sqrt{p}$ is odd and as smooth as possible, ideally T is divisible by a large power of 3. In the building blocks of SQISignHD, one replaces 3^b by T. As opposed to SQISign/BSIDH primes, these primes are relatively easy to generate since there is no other requirement. We suggest a set of such primes for the various security levels (see Table 1). Moreover, since one has access to smooth torsion of order larger than p, then the degrees of the secret and commitment isogenies can be chosen to be larger than p, as opposed to the current SQISignHD version where they are smaller than p. This enables the public curve E_A and the commitment curve E_1 to have a distribution which is slightly closer to the uniform distribution.

Even though the change potentially allows a more efficient signature algorithm (to be confirmed by future implementation), one drawback is that signature size is larger. In fact, since the representation of the isogeny σ_I now uses points of order $\approx 2^{\log q}$ instead of $\approx 2^{\frac{1}{2}\log q}$, then the size of the part of the response (in the signature) representing these points will double. This will lead to signatures that are about 1.24 times larger, but still very compact; say ≈ 140 bytes.

2 Overview of SQISignHD

2.1 New isogeny representation from Kani's theorem

Informally, a *efficient representation* of an isogeny $\varphi : E \to E'$ is any string of polynomial size that allows to evaluate the isogeny φ on any point of E which is defined over a relatively small extension of $\mathbb{F}_{p^2}$. An isogeny $\varphi : E \to E'$ of small prime degree ℓ can be efficiently computed and evaluated from its kernel, or one of its kernel generator. This kernel generator is a point of order ℓ, which is defined over an extension of $\mathbb{F}_{p^2}$ of degree at most $O(\ell)$. This means that any kernel generator P of φ is an efficient representation of φ. If the isogeny φ has large prime power degree, say ℓ^n, then φ can be decomposed as $\varphi = \varphi_n \circ \varphi_{n-1} \circ \cdots \circ \varphi_2 \circ \varphi_1$, where each φ_i has degree ℓ. An efficient representation of φ can be obtained from that of the isogenies φ_i. Moreover, if $n = kd$ and the the ℓ^d torsion is defined over a small extension of $\mathbb{F}_{p^2}$, then one can represent φ more compactly by using a more compact decomposition $\varphi = \psi_k \circ \psi_{k-1} \circ \cdots \circ \psi_2 \circ \psi_1$ where each ψ is represented by one of its kernel generators which is a point of order ℓ^d. This is exactly how the response isogeny is returned in SQISIgn. In fact, in SQISign, the response isogeny σ has degree $2^n \approx p^{15/4}$. Since one only has access to some 2^d torsion where $d < \log p$, σ is efficiently represented as a composition is isogenies of degree at most 2^d. As you may notice, this kernel representation only works for smooth degree isogenies.

In SQISignHD, the picture changes completely, one uses a new representation [15] inspired by the SIDH attacks [2,13,16]. In fact, an isogeny can be represented by its action on some smooth rational torsion points regardless of whether its degree is smooth or not. This representation is a consequence of Kani's theorem [11], and it involves a higher dimension (2, 4 or 8) isogeny. In this note, we are interested in representations that use isogenies in dimension 4. We refer to [6, §3], [16] and [15] for further details.

Dimension 4 representations. Let $\sigma : E_1 \to E_2$ be an isogeny of degree q and let $N > q$ be a smooth integer such that $E_1[N]$ defined over a small extension of $\mathbb{F}_{p^2}$ and $a = N - q = a_1^2 + a_2^2$ is the sum of two squares. Set $\sum = diag(\sigma, \sigma) \in Hom(E_1^2, E_2^2)$ and $\alpha = \begin{bmatrix} a_1 & a_2 \\ -a_2 & a_1 \end{bmatrix}$. Then we have the following diagram, also known as isogeny diamond, where α_1 and α_2 are the endomorphisms whose matrix is α.

$$\begin{tikzcd}
E_1^2 \arrow[r, "\sum"] \arrow[d, "\alpha_1"'] & E_2^2 \arrow[d, "\alpha_2"] \\
E_1^2 \arrow[r, "\sum"'] & E_2^2
\end{tikzcd}$$

Then the higher dimension endomorphism

$$F = \begin{pmatrix} \alpha_1 & \widehat{\sum} \\ -\sum & \widehat{\alpha_2} \end{pmatrix} \in \mathrm{End}(E_1^2 \times E_2^2)$$

has degree $N = a + q$, and we denote this endomorphism by $F(\sigma, a_1, a_2)$. Its kernel is given by

$$\ker(F) = \left\{ \left(\widehat{\alpha_1}(P), \sum(P) \right) \mid P \in E_1^2[N] \right\}.$$

In practice, one chooses N to be as smooth as possible, say a power of 2. For this representation to be possible, $N - q$ needs to be the sum of two squares. One way to achieve this is to require that $N - q$ is a prime number congruent to 1 modulo 4, and to use Cornacchia's algorithm [3] to find a_1 and a_2. When one cannot write $N - q$ as the sum of two squares, one is obliged to do a dimension 8 representation instead. A much less efficient version of SQISignHD uses this diemension 8 representation. But here we discuss only the fast version that uses the dimension 4 representation since it is the practically efficient one.

This means that the response isogeny in SQISign no more needs to be a smooth degree isogeny. In SQISignHD, the very long smooth degree response isogeny is replaced by a short isogeny $\sigma_I : E_1 \to E_2$ of generic degree. In fact, since the signer knows the endomorphism rings $\mathcal{O}_1$ and $\mathcal{O}_2$ of E_1 and E_2 respectively, he can sample a short ideal I of norm q connecting $\mathcal{O}_1$ and $\mathcal{O}_2$, evaluate the corresponding isogeny σ_I on a canonical basis (P, Q) of $E_1[N]$, and return $(\sigma_I(P), \sigma_I(Q), q)$ as a representation of σ_I. The verification consists in checking that $(\sigma_I(P), \sigma_I(Q), q)$ leads to an endomorphism $F(\sigma_I, a_1, a_2) \in \mathrm{End}(E_1^2 \times E_2^2)$ of the correct form. We refer to [6] for more details.

2.2 The SQISignHD identification protocol

In what follows, we provide a simplified description of the SQISignHD identification protocol. Several technical details are omitted since they are not relevant for our exposition. We refer to the SQISignHD paper [6] for more details.

Setup. Let $p = 2^a 3^b f - 1$ be a prime. Consider the supersingular curve $E_0 : y^2 = x^3 + x$ defined over $\mathbb{F}_p$ and let $\mathcal{O}_0 \simeq \mathrm{End}(E_0)$ be its endomorphism ring.

Key generation. Compute a random double-path made of two isogenies $\tau : E_0 \to E_A$ and $\tau' : E_0 \to E_A$ of degree $3^{2b''} \sim p$ and $2^{2a''} \sim p$ respectively. The public key is $\mathsf{pk} = E_A$ and the secret key is $\mathsf{sk} = (\tau, \tau')$.

Commitment. Sample a random isogeny $\psi : E_0 \to E_1$ of degree $3^{2b'} \sim p$. Return $\mathsf{com} = E_1$.

Challenge. Sample a uniformly random isogeny $\varphi : E_A \to E_2$ of degree 3^b. Return $\mathsf{chal} = \varphi$.

Response. Translate ψ into an ideal I_ψ. Use τ' and $I_{\tau'}$ to translate φ into an ideal I_φ. Compute the ideal $J = \overline{I_\psi} I_\tau I_\varphi$. Compute a random short ideal $I \sim J$ such that $2^{2r} - q$ is the sum of two squares for some $r \leq a$, where q is the norm of I. Use $\mathcal{O}_0$, τ, ψ and φ to evaluate the isogeny $\sigma_I : E_1 \to E_2$ corresponding to I on a canonical basis (P, Q) of $E_1[2^r]$. Return $\mathsf{resp} = (\sigma_I(P), \sigma_I(Q), q)$.

Verification. Verify that the response resp parses as (R, S, q) and that this is a valid representation of an isogeny from E_1 to E_2 of degree q. Return 1 if the verification succeeds and 0 if it fails.

2.3 The actual representation and verification in SQISignHD

As you may have notice, in SQISignHD, one represents an isogeny of degree q using its action on the 2^r torsion points where $2^r < q < 2^{2r}$. The trick here is that

$$\begin{tikzcd}
E_0 \arrow[r, bend left, "\tau'"] \arrow[r, bend right, "\tau"'] \arrow[d, "\psi"'] & E_A \arrow[d, "\varphi"] \\
E_1 \arrow[r, "\sigma_I"'] & E_2
\end{tikzcd}$$

Fig. 3. The actual SQISignHD identification protocol.

a cyclic isogeny $\phi : E \to E'$ of degree $d = d_1^2 d_2$ can be recovered from its action on the $d_1 d_2$-torsion group. In fact, one writes $\phi = \phi_2 \circ \phi_1$, where $\deg \phi_1 = d_1 d_2$ and $\deg \phi_2 = d_1$. Then $\ker \phi_1 = E[d_1 d_2] \cap \ker \phi$ and $\ker \widehat{\phi_2} = \phi(E[d_1])$. The same applies to the higher dimension isogeny F. This means that with access to the 2^a torsion points, the degree of F can be chosen to be 2^{2r} with $r \leq a$, and one decomposes F as $F = F_2 \circ F_1$ where $F_1 : E_1^2 \times E_2^2 \to C_1$ and $\widehat{F_2} : E_1^2 \times E_2^2 \to C_2$ have degree 2^r, with C_1 and C_2 be two isomorphic surfaces.

The verification consists in computing the isogenies F_1 and $\widehat{F_2}$ from the action of σ_I on the 2^r torsion, checking that C_1 and C_2 are isomorphic, and that $F = F_2 \circ F_1$ is of the correct form: by mapping a point of the form $(Q, 0, 0, 0)$ through the isogeny F and checking that its image is of the form $([a_1]Q, -[a_2]Q, \star, 0)$. For an efficient isomorphism check between C_1 and C_2, one needs to have $r \leq a-2$ [6, Remark 4.2].

This representation is less optimal. In the next section we suggest to use different primes that will allow to have the optimal representation as presented in Section 2.1.

3 New primes for SQISignHD

3.1 Overview

We describe a variant of SQISignHD that uses primes p such that $p^2 - 1$ has a very smooth part which is larger than p. The aim here is to choose 2^a such that the degree of the response isogeny is always smaller than 2^a. As explained earlier, the prime p is such that $p^2 - 1 = 2^{a+1} T f$ where 2^a is larger than $2 q_{max} \log p$, and $T > \sqrt{p}$ is very smooth. We did a search of such primes and we found the ones described in Table 1 that could be used.

3.2 The new identification protocol

Setup. Let $p \equiv 3 \mod 4$ be a prime such that $p^2 - 1 = 2^{a+1} T f$ as described above. Consider the supersingular curve $E_0 : y^2 = x^3 + x$ defined over $\mathbb{F}_p$ and let $\mathcal{O}_0 \simeq \mathrm{End}(E_0)$ be it endomorphism ring.

λ	$\log p$	a	T_1	T_2
128	254	140	$5^6 * 7^3$	$3^{64} * 23 * 29$
192	382	203	$7^2 * 11^2$	$3^{111} * 5$
256	510	269	$5^3 * 19$	$3^{153} * 13$

Table 1. Suggested primes for SQISignHD. We have $p+1 = 2^a T_1 f_1$ and $p-1 = 2T_2 f_2$, where $T = T_1 T_2$, f_1 and f_2 are co-factors. These primes p_{254}, p_{382} and p_{510} are listed in Appendix A

Key generation. Compute a random double-path made of two isogenies $\tau : E_0 \to E_A$ and $\tau' : E_0 \to E_A$ of degree $T''^2 \sim T^2$ and $2^{2a''} \sim 2^{2a}$ respectively. The public key is $\mathsf{pk} = E_A$ and the secret key is $\mathsf{sk} = (\tau, \tau')$.

Commitment. Sample a random isogeny $\psi : E_0 \to E_1$ of degree $T'^2 \sim T^2$ where $T'|T$. Return $\mathsf{com} = E_1$.

Challenge. Sample a uniformly random isogeny $\varphi : E_A \to E_2$ of degree T. Return $\mathsf{chal} = \varphi$.

Response. Translate ψ into an ideal I_ψ. Use τ' and $I_{\tau'}$ to translate φ into an ideal I_φ. Compute the ideal $J = \overline{I_\psi} I_\tau I_\varphi$. Compute a random short ideal $I \sim J$ such that $2^a - q$ is a sum of two squares where q is the norm of I. Use $\mathcal{O}_0$, τ, ψ and φ to evaluate the isogeny $\sigma_I : E_1 \to E_2$ corresponding to I on a canonical basis (P, Q) of $E_1[2^a]$. Return $\mathsf{resp} = (\sigma_I(P), \sigma_I(Q), q)$.

Verification. Verify that the response resp parses as (R, S, q) and that this is a valid representation of an isogeny from E_1 to E_2 of degree q. Return 1 if the verification succeeds and 0 if it fails.

Algorithmic wise, only the response computation and the verification algorithm are modified as presented above. In the scheme in general, the degrees of some isogenies are changed, but they are still very smooth, hence we do not expect them to impact efficiency that much. On the other hand, the higher dimension isogeny F is directly computed and evaluated without splitting it into two. This will allow a faster response verification. Another advantage is that we have access to the $2^a T > p + 1$ torsion, hence our isogenies are slightly longer, hence offering better security guaranties.

One drawback with computing the higher dimension isogeny in one go is that it is represented with points of order $\approx 2^{\log q}$ instead of $\approx 2^{\frac{1}{2}\log q}$. This implies an increase in the size of the signature. In fact, the returned signature is of the form $||n_2||n_2||q||c_1||c_2||c_3$ where n_1 and n_2 are the $\mathbb{F}_p$-coordinates of $j(E_1)$, c_1, c_2, and c_3 are three of the four coordinates of $\sigma_I(P)$ and $\sigma_I(Q)$ in a canonical basis. The size of the signature is $2\lceil \log(p) \rceil + \log(q) + 3u$ where the order of the points P and Q is 2^u. In SQISignHD, the points P and Q have order $2^{\frac{1}{2}\log q}$ roughly, while in our variant, their order is $2^{\log q}$ roughly. Hence the size of of c_1,

c_2, and c_3 is doubled. This leads to an increase of about 24% in the signature signature size. We stress that the SQISignHD signature algorithm is divinely compact (for example, the signatures for NIST level I security are about 110 bytes), hence this increase in the signature size is affordable provided that the change enables a faster signature algorithm. A future implementation work will help verify these claims.

References

1. Bruno, G., Santos, M.C.R., Costello, C., Eriksen, J.K., Naehrig, M., Meyer, M., Sterner, B.: Cryptographic smooth neighbors. Cryptology ePrint Archive, Report 2022/1439 (2022), https://eprint.iacr.org/2022/1439
2. Castryck, W., Decru, T.: An efficient key recovery attack on SIDH. In: Hazay, C., Stam, M. (eds.) EUROCRYPT 2023, Part V. LNCS, vol. 14008, pp. 423–447. Springer, Heidelberg (Apr 2023). https://doi.org/10.1007/978-3-031-30589-4_15
3. Cornacchia, G.: Su di un metodo per la risoluzione in numeri interi dell'equazione $\sum_{h=0}^{n} c_h x^{n-h} y^h = p$. Giornale di matematiche di Battaglini 46 (1908), pp. 33-90
4. Costello, C.: B-SIDH: Supersingular isogeny Diffie-Hellman using twisted torsion. In: Moriai, S., Wang, H. (eds.) ASIACRYPT 2020, Part II. LNCS, vol. 12492, pp. 440–463. Springer, Heidelberg (Dec 2020). https://doi.org/10.1007/978-3-030-64834-3_15
5. Costello, C., Meyer, M., Naehrig, M.: Sieving for twin smooth integers with solutions to the prouhet-tarry-escott problem. In: Canteaut, A., Standaert, F.X. (eds.) EUROCRYPT 2021, Part I. LNCS, vol. 12696, pp. 272–301. Springer, Heidelberg (Oct 2021). https://doi.org/10.1007/978-3-030-77870-5_10
6. Dartois, P., Leroux, A., Robert, D., Wesolowski, B.: SQISignHD: New Dimensions in Cryptography. Cryptology ePrint Archive, Paper 2023/436 (2023), https://eprint.iacr.org/2023/436, https://eprint.iacr.org/2023/436
7. De Feo, L., Kohel, D., Leroux, A., Petit, C., Wesolowski, B.: SQISign: Compact post-quantum signatures from quaternions and isogenies. In: Moriai, S., Wang, H. (eds.) ASIACRYPT 2020, Part I. LNCS, vol. 12491, pp. 64–93. Springer, Heidelberg (Dec 2020). https://doi.org/10.1007/978-3-030-64837-4_3
8. De Feo, L., Leroux, A., Longa, P., Wesolowski, B.: New algorithms for the deuring correspondence - towards practical and secure SQISign signatures. In: Hazay, C., Stam, M. (eds.) EUROCRYPT 2023, Part V. LNCS, vol. 14008, pp. 659–690. Springer, Heidelberg (Apr 2023). https://doi.org/10.1007/978-3-031-30589-4_23
9. Deuring, M.: Die typen der multiplikatorenringe elliptischer funktionenkörper: G. herglotz zum 60. geburtstag gewidmet. In: Abhandlungen aus dem mathematischen Seminar der Universität Hamburg. vol. 14, pp. 197–272. Springer (1941)
10. Galbraith, S.D., Petit, C., Silva, J.: Identification protocols and signature schemes based on supersingular isogeny problems. In: Takagi, T., Peyrin, T. (eds.) ASIACRYPT 2017, Part I. LNCS, vol. 10624, pp. 3–33. Springer, Heidelberg (Dec 2017). https://doi.org/10.1007/978-3-319-70694-8_1
11. Kani, E.: The number of curves of genus two with elliptic differentials. (1997)
12. Kohel, D., Lauter, K., Petit, C., Tignol, J.P.: On the quaternion ℓ-isogeny path problem. LMS Journal of Computation and Mathematics **17**(A), 418–432 (2014)

13. Maino, L., Martindale, C., Panny, L., Pope, G., Wesolowski, B.: A direct key recovery attack on SIDH. In: Hazay, C., Stam, M. (eds.) EUROCRYPT 2023, Part V. LNCS, vol. 14008, pp. 448–471. Springer, Heidelberg (Apr 2023). https://doi.org/10.1007/978-3-031-30589-4_16
14. Robert, D.: Evaluating isogenies in polylogarithmic time. Cryptology ePrint Archive, Report 2022/1068 (2022), https://eprint.iacr.org/2022/1068
15. Robert, D.: Evaluating isogenies in polylogarithmic time. Cryptology ePrint Archive, Paper 2022/1068 (2022), https://eprint.iacr.org/2022/1068, https://eprint.iacr.org/2022/1068
16. Robert, D.: Breaking SIDH in polynomial time. In: Hazay, C., Stam, M. (eds.) EUROCRYPT 2023, Part V. LNCS, vol. 14008, pp. 472–503. Springer, Heidelberg (Apr 2023). https://doi.org/10.1007/978-3-031-30589-4_17

A Suggested primes

p_{254}	0x311a894ff82fdb307cedb44ecd84afffffffffffffffffffffffffffffffffff
p_{382}	0x2df5a3a93966d718e5975170efb0d1408fd4bfa4bc0737ffffffffffffffffffffffff ffffffffffffffffffffffffff
p_{510}	0x304d3218257f38bca253529e57639d710def7954b3ae134fdc7bc152f44ed fffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff

Table 2. The new primes suggested for SQISignHD