SQISign primes:
Fantastic p's and where to find them

Isogeny Club

14 March 2023

Michael Meyer

University of Regensburg, Germany

joint work with Giacomo Bruno, Maria Corte-Real Santos, Craig Costello, Jonathan Komada Eriksen, Michael Naehrig, and Bruno Sterner

Outline

Part I:

Isogenies and twin smooths

Part II:

Searching for twin smooths

Part III:

Constructing twin smooths

Part IV:

From twin smooths to SQISign primes

Motivation [graphs stolen from Craig Costello]

Toy example for SIDH†: $p = 431 = 2^4 3^3 - 1$; curves with $\#E(\mathbb{F}_{p^2}) = (p+1)^2$.

Motivation [graphs stolen from Craig Costello]

Toy example for SIDH†: $p = 431 = 2^4 3^3 - 1$; curves with $\#E(\mathbb{F}_{p^2}) = (p+1)^2$.

Alice

secret 2^4-isogeny

Bob

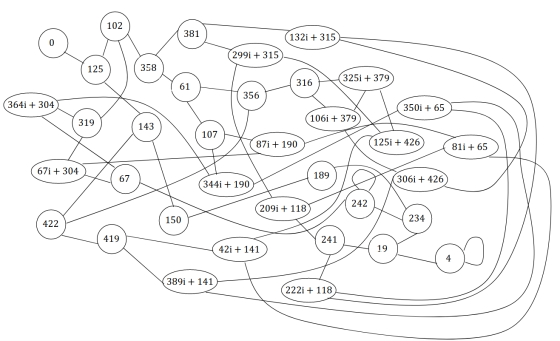
secret 3^3-isogeny

Motivation [graphs stolen from Craig Costello]

Toy example for SIDH†: $p = 431 = 2^4 3^3 - 1$; curves with $\#E(\mathbb{F}_{p^2}) = (p+1)^2$.

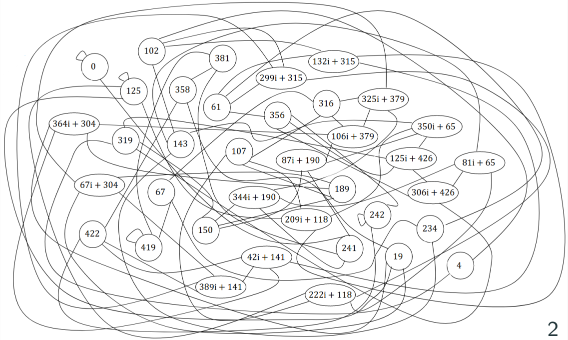
Alice

secret 2^4-isogeny



Bob

secret 3^3-isogeny



Motivation [graphs stolen from Craig Costello]

Toy example for B-SIDH†: $p = 431 = 2^4 3^3 - 1$

Motivation [graphs stolen from Craig Costello]

Toy example for B-SIDH†: $p = 431 = 2^4 3^3 - 1$

<u>Alice</u>

curves with $\#E(\mathbb{F}_{p^2}) = (p+1)^2$

<u>Bob</u>

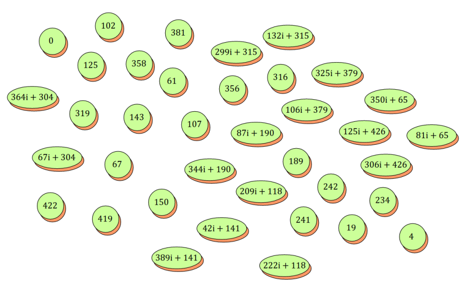
curves with $\#E(\mathbb{F}_{p^2}) = (p-1)^2$

Motivation [graphs stolen from Craig Costello]

Toy example for B-SIDH†: $p = 431 = 2^4 3^3 - 1$

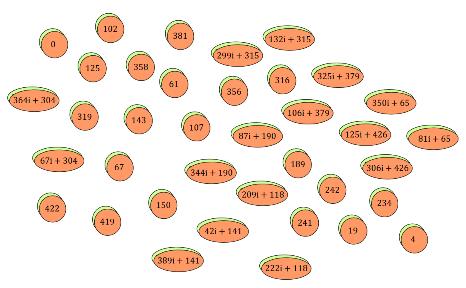
Alice

curves with $\#E(\mathbb{F}_{p^2}) = (p+1)^2$



Bob

curves with $\#E(\mathbb{F}_{p^2}) = (p-1)^2$

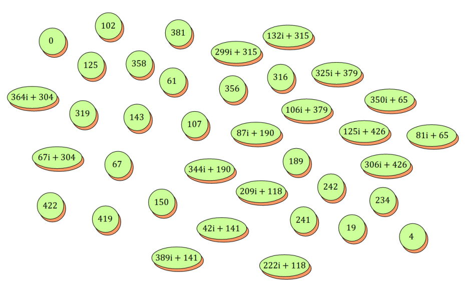


Motivation [graphs stolen from Craig Costello]

Toy example for B-SIDH†: $p = 431 = 2^4 3^3 - 1$

<u>Alice</u>

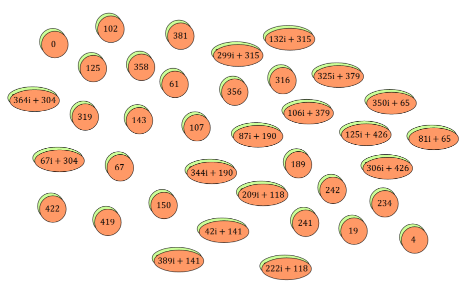
curves with $\#E(\mathbb{F}_{p^2}) = (p+1)^2$



$\rightsquigarrow$ isogeny of degree $p + 1 = 2^4 \cdot 3^3$

<u>Bob</u>

curves with $\#E(\mathbb{F}_{p^2}) = (p-1)^2$



$\rightsquigarrow$ isogeny of degree $\frac{p-1}{2} = 5 \cdot 43$

Smoothness

- Problem: Find primes p of fixed sizes (e.g. 256, 384, 512 bits), such that $p+1$ and $p-1$ are as smooth as possible.

Smoothness

- Problem: Find primes p of fixed sizes (e.g. 256, 384, 512 bits), such that $p+1$ and $p-1$ are as smooth as possible.
- B-smoothness: For $B > 0$, $m \in \mathbb{Z}$ is B-smooth if any prime divisor $q|m$ satisfies $q \leq B$.

Smoothness

- Problem: Find primes p of fixed sizes (e.g. 256, 384, 512 bits), such that $p+1$ and $p-1$ are as smooth as possible.
- B-smoothness: For $B > 0$, $m \in \mathbb{Z}$ is B-smooth if any prime divisor $q|m$ satisfies $q \leq B$.
- Twin smooth integers: Pairs of B-smooth integers integers $(m, m+1)$ for $B > 0$.

Smoothness

- Problem: Find primes p of fixed sizes (e.g. 256, 384, 512 bits), such that $p+1$ and $p-1$ are as smooth as possible.
- B-smoothness: For $B > 0$, $m \in \mathbb{Z}$ is B-smooth if any prime divisor $q|m$ satisfies $q \leq B$.
- Twin smooth integers: Pairs of B-smooth integers integers $(m, m+1)$ for $B > 0$.
- Equivalent problem: Find twin B-smooth integers $(m, m+1)$ of a given size with B as small as possible, such that $2m+1$ is prime.

  $\rightsquigarrow$ $p = 2m+1$ is prime

  $\rightsquigarrow$ $(p-1, p+1) = (2m, 2(m+1))$ are B-smooth

Examples

5-smooth twins:

$(m, m+1)$	$2m+1$
$(1,2)$	3
$(2,3)$	5
$(3,4)$	7
$(4,5)$	9
$(5,6)$	11
$(8,9)$	17
$(9,10)$	19
$(15,16)$	31
$(24,25)$	49
$(80,81)$	161

19-smooth twins:

$$11859205 = 5 \cdot 31 \cdot 76511$$
$$11859206 = 2 \cdot 83 \cdot 199 \cdot 359$$
$$11859207 = 3 \cdot 733 \cdot 5393$$
$$11859208 = 2^3 \cdot 149 \cdot 9949$$
$$11859209 = 41 \cdot 289249$$
$$11859210 = 2 \cdot 3^4 \cdot 5 \cdot 11^4$$
$$11859211 = 7 \cdot 13 \cdot 19^4$$
$$11859212 = 2^2 \cdot 383 \cdot 7741$$

Outline

Part I:

Isogenies and twin smooths

Part II:

Searching for twin smooths

Part III:

Constructing twin smooths

Part IV:

From twin smooths to SQISign primes

Smoothness probabilities

- Let $\Psi(N, B) = \#\{1 \leq m \leq N \mid m \text{ is } B\text{-smooth}\}$

Smoothness probabilities

- Let $\Psi(N, B) = \#\{1 \leq m \leq N \mid m \text{ is } B\text{-smooth}\}$
- Smoothness probability for a random $1 \leq m \leq N$:

$$\frac{\Psi(N, B)}{N} \approx \rho(\log(N)/\log(B)) \text{ as } N \to \infty,$$

ρ: Dickman-De Bruijn function

Smoothness probabilities

- Let $\Psi(N, B) = \#\{1 \leq m \leq N \mid m \text{ is } B\text{-smooth}\}$
- Smoothness probability for a random $1 \leq m \leq N$:

$$\frac{\Psi(N, B)}{N} \approx \rho(\log(N)/\log(B)) \text{ as } N \to \infty,$$

ρ: Dickman-De Bruijn function

- Example: $\Pr(m \leftarrow [0, 2^{256}), 2^{16}\text{-smooth})$:

$$\frac{\Psi(2^{256}, 2^{16})}{2^{256}} \approx \rho(256/16) < 2^{-69.6}$$

Smoothness probabilities

- Let $\Psi(N, B) = \#\{1 \leq m \leq N \mid m \text{ is } B\text{-smooth}\}$
- Smoothness probability for a random $1 \leq m \leq N$:

$$\frac{\Psi(N, B)}{N} \approx \rho(\log(N)/\log(B)) \text{ as } N \to \infty,$$

ρ: Dickman-De Bruijn function

- Example: $\Pr(m \leftarrow [0, 2^{256}), 2^{16}\text{-smooth})$:

$$\frac{\Psi(2^{256}, 2^{16})}{2^{256}} \approx \rho(256/16) < 2^{-69.6}$$

$\rightsquigarrow$ Hopeless to find twin smooths with a naïve search.

B-SIDH & SQISign parameters

Smoothness probabilities for 256-bit numbers and smoothness bound $B = 2^{16}$:

- XGCD: pick smooth coprime $\alpha \approx \beta$; compute r, s s.t. $\alpha s + \beta t = 1$.

$\Pr(\text{smooth}) \approx 2^{-49.8}$

B-SIDH & SQISign parameters

Smoothness probabilities for 256-bit numbers and smoothness bound $B = 2^{16}$:

- XGCD: pick smooth coprime $\alpha \approx \beta$; compute r, s s.t. $\alpha s + \beta t = 1$.

$\Pr(\text{smooth}) \approx 2^{-49.8}$

- Polynomials x^n: e.g. x^4 and $x^4 - 1 = (x-1)(x+1)(x^2+1)$.

$\Pr(\text{smooth}) \approx 2^{-47.9}$

B-SIDH & SQISign parameters

Smoothness probabilities for 256-bit numbers and smoothness bound $B = 2^{16}$:

- XGCD: pick smooth coprime $\alpha \approx \beta$; compute r, s s.t. $\alpha s + \beta t = 1$.

  $\Pr(\text{smooth}) \approx 2^{-49.8}$

- Polynomials x^n: e.g. x^4 and $x^4 - 1 = (x-1)(x+1)(x^2+1)$.

  $\Pr(\text{smooth}) \approx 2^{-47.9}$

- Idea: Use fully split polynomials $a(x) = \prod_i (x - a_i)$, $b(x) = \prod_i (x - b_i)$ with $a(x) - b(x) = 1$.

  $\Pr(\text{smooth}) \approx 2^{-41.4}$ for degree 6

  $\Pr(\text{smooth}) \approx 2^{-27.3}$ for degree 8

The Prouhet-Tarry-Escott problem

Given a size n and degree k, find distinct multisets of integers $A = \{a_1, \ldots, a_n\}$ and $B = \{b_1, \ldots, b_n\}$, such that

$$\begin{aligned} a_1 + \cdots + a_n &= b_1 + \cdots + b_n, \\ a_1^2 + \cdots + a_n^2 &= b_1^2 + \cdots + b_n^2, \\ \vdots \qquad & \qquad \vdots \\ a_1^k + \cdots + a_n^k &= b_1^k + \cdots + b_n^k. \end{aligned}$$

Write $[a_1, \ldots, a_n] =_k [b_1, \ldots, b_n]$.

The Prouhet-Tarry-Escott problem

Example: size 6, degree 5

$[0, 5, 6, 16, 17, 22] =_5 [1, 2, 10, 12, 20, 21]$

$$
\begin{aligned}
0 + 5 + 6 + 16 + 17 + 22 &= 1 + 2 + 10 + 12 + 20 + 21 &&= 66, \\
0^2 + 5^2 + 6^2 + 16^2 + 17^2 + 22^2 &= 1^2 + 2^2 + 10^2 + 12^2 + 20^2 + 21^2 &&= 1090, \\
0^3 + 5^3 + 6^3 + 16^3 + 17^3 + 22^3 &= 1^3 + 2^3 + 10^3 + 12^3 + 20^3 + 21^3 &&= 19998, \\
0^4 + 5^4 + 6^4 + 16^4 + 17^4 + 22^4 &= 1^4 + 2^4 + 10^4 + 12^4 + 20^4 + 21^4 &&= 385234, \\
0^5 + 5^5 + 6^5 + 16^5 + 17^5 + 22^5 &= 1^5 + 2^5 + 10^5 + 12^5 + 20^5 + 21^5 &&= 7632966.
\end{aligned}
$$

Ideal PTE solutions

- Solutions $[a_1, \ldots, a_n] =_k [b_1, \ldots, b_n]$ with $k = n - 1$ are called ideal solutions (known for $n \in \{2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$).

Ideal PTE solutions

- Solutions $[a_1, \ldots, a_n] =_k [b_1, \ldots, b_n]$ with $k = n - 1$ are called ideal solutions (known for $n \in \{2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$).
- Define $a(x) = \prod_{i=1}^{n}(x - a_i)$ and $b(x) = \prod_{i=1}^{n}(x - b_i)$.

Ideal PTE solutions

- Solutions $[a_1, \ldots, a_n] =_k [b_1, \ldots, b_n]$ with $k = n - 1$ are called ideal solutions (known for $n \in \{2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$).
- Define $a(x) = \prod_{i=1}^{n}(x - a_i)$ and $b(x) = \prod_{i=1}^{n}(x - b_i)$.
- Theorem: $[a_1, \ldots, a_n] =_{n-1} [b_1, \ldots, b_n]$
$$\Leftrightarrow \quad a(x) - b(x) = C \in \mathbb{Z}.$$

Ideal PTE solutions

- Solutions $[a_1, \dots, a_n] =_k [b_1, \dots, b_n]$ with $k = n - 1$ are called ideal solutions (known for $n \in \{2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$).
- Define $a(x) = \prod_{i=1}^{n}(x - a_i)$ and $b(x) = \prod_{i=1}^{n}(x - b_i)$.
- Theorem: $[a_1, \dots, a_n] =_{n-1} [b_1, \dots, b_n]$
$$\Leftrightarrow \quad a(x) - b(x) = C \in \mathbb{Z}.$$
- Example: $[1, 1, 8, 8, 15, 15] =_5 [0, 3, 5, 11, 13, 16]$
$$\rightsquigarrow a(x) = (x-1)^2(x-8)^2(x-15)^2,$$
$$b(x) = x(x-3)(x-5)(x-11)(x-13)(x-16).$$
$$\rightsquigarrow a(x) - b(x) = 14400 = 2^6 \cdot 3^2 \cdot 5^2.$$

Ideal PTE solutions & twin smooth integers

For ideal solutions of size n: $a(x) - b(x) = C \in \mathbb{Z}$.

$\rightsquigarrow$ Define $a_C(x) = a(x)/C$ and $b_C(x) = b(x)/C$.

Ideal PTE solutions & twin smooth integers

For ideal solutions of size n: $a(x) - b(x) = C \in \mathbb{Z}$.

$\rightsquigarrow$ Define $a_C(x) = a(x)/C$ and $b_C(x) = b(x)/C$.

$\rightsquigarrow$ $a_C(x) - b_C(x) = 1$.

Ideal PTE solutions & twin smooth integers

For ideal solutions of size n: $a(x) - b(x) = C \in \mathbb{Z}$.

$\rightsquigarrow$ Define $a_C(x) = a(x)/C$ and $b_C(x) = b(x)/C$.

$\rightsquigarrow$ $a_C(x) - b_C(x) = 1$.

Assume $a_C(x) \in \mathbb{Z}$ for an $x \in \mathbb{Z}$.

$\rightsquigarrow$ $m + 1 = a_C(x) = 1/C \cdot \prod_{i=1}^{n}(x - a_i)$ and

$m = b_C(x) = 1/C \cdot \prod_{i=1}^{n}(x - b_i)$ split in n $\sim$equally sized factors.

Ideal PTE solutions & twin smooth integers

For ideal solutions of size n: $a(x) - b(x) = C \in \mathbb{Z}$.

$\rightsquigarrow$ Define $a_C(x) = a(x)/C$ and $b_C(x) = b(x)/C$.

$\rightsquigarrow$ $a_C(x) - b_C(x) = 1$.

Assume $a_C(x) \in \mathbb{Z}$ for an $x \in \mathbb{Z}$.

$\rightsquigarrow$ $m + 1 = a_C(x) = 1/C \cdot \prod_{i=1}^{n}(x - a_i)$ and
$m = b_C(x) = 1/C \cdot \prod_{i=1}^{n}(x - b_i)$ split in n $\sim$equally sized factors.

$\rightsquigarrow$ Good chances to find twin smooth integers :)

The PTE sieve

Phase 1: Identify B-smooth numbers in a given interval.

Phase 2: Check if PTE solution aligns with the smooth numbers.

(parallelizes perfectly)

The PTE sieve

Phase 1 example: Identify 7-smooth numbers in [4350,4399].

4350	4351	4352	4353	4354	4355	4356	4357	4358	4359
1	1	1	1	1	1	1	1	1	1
4360	4361	4362	4363	4364	4365	4366	4367	4368	4369
1	1	1	1	1	1	1	1	1	1
4370	4371	4372	4373	4374	4375	4376	4377	4378	4379
1	1	1	1	1	1	1	1	1	1
4380	4381	4382	4383	4384	4385	4386	4387	4388	4389
1	1	1	1	1	1	1	1	1	1
4390	4391	4392	4393	4394	4395	4396	4397	4398	4399
1	1	1	1	1	1	1	1	1	1

The PTE sieve

Phase 1 example: multiples of 2

4350	4351	4352	4353	4354	4355	4356	4357	4358	4359
2	1	2	1	2	1	2	1	2	1
4360	4361	4362	4363	4364	4365	4366	4367	4368	4369
2	1	2	1	2	1	2	1	2	1
4370	4371	4372	4373	4374	4375	4376	4377	4378	4379
2	1	2	1	2	1	2	1	2	1
4380	4381	4382	4383	4384	4385	4386	4387	4388	4389
2	1	2	1	2	1	2	1	2	1
4390	4391	4392	4393	4394	4395	4396	4397	4398	4399
2	1	2	1	2	1	2	1	2	1

The PTE sieve

Phase 1 example: multiples of $2^2 = 4$

4350	4351	4352	4353	4354	4355	4356	4357	4358	4359
2	1	4	1	2	1	4	1	2	1
4360	4361	4362	4363	4364	4365	4366	4367	4368	4369
4	1	2	1	4	1	2	1	4	1
4370	4371	4372	4373	4374	4375	4376	4377	4378	4379
2	1	4	1	2	1	4	1	2	1
4380	4381	4382	4383	4384	4385	4386	4387	4388	4389
4	1	2	1	4	1	2	1	4	1
4390	4391	4392	4393	4394	4395	4396	4397	4398	4399
2	1	4	1	2	1	4	1	2	1

The PTE sieve

Phase 1 example: multiples of $2^3 = 8$

4350	4351	4352	4353	4354	4355	4356	4357	4358	4359
2	1	8	1	2	1	4	1	2	1
4360	4361	4362	4363	4364	4365	4366	4367	4368	4369
8	1	2	1	4	1	2	1	8	1
4370	4371	4372	4373	4374	4375	4376	4377	4378	4379
2	1	4	1	2	1	8	1	2	1
4380	4381	4382	4383	4384	4385	4386	4387	4388	4389
4	1	2	1	8	1	2	1	4	1
4390	4391	4392	4393	4394	4395	4396	4397	4398	4399
2	1	8	1	2	1	4	1	2	1

The PTE sieve

Phase 1 example: multiples of $2^4 = 16$

4350	4351	4352	4353	4354	4355	4356	4357	4358	4359
2	1	16	1	2	1	4	1	2	1
4360	4361	4362	4363	4364	4365	4366	4367	4368	4369
8	1	2	1	4	1	2	1	16	1
4370	4371	4372	4373	4374	4375	4376	4377	4378	4379
2	1	4	1	2	1	8	1	2	1
4380	4381	4382	4383	4384	4385	4386	4387	4388	4389
4	1	2	1	16	1	2	1	4	1
4390	4391	4392	4393	4394	4395	4396	4397	4398	4399
2	1	8	1	2	1	4	1	2	1

The PTE sieve

Phase 1 example: multiples of $2^5 = 32$

4350	4351	4352	4353	4354	4355	4356	4357	4358	4359
2	1	32	1	2	1	4	1	2	1
4360	4361	4362	4363	4364	4365	4366	4367	4368	4369
8	1	2	1	4	1	2	1	16	1
4370	4371	4372	4373	4374	4375	4376	4377	4378	4379
2	1	4	1	2	1	8	1	2	1
4380	4381	4382	4383	4384	4385	4386	4387	4388	4389
4	1	2	1	32	1	2	1	4	1
4390	4391	4392	4393	4394	4395	4396	4397	4398	4399
2	1	8	1	2	1	4	1	2	1

The PTE sieve

Phase 1 example: multiples of $2^6 = 64$

4350	4351	4352	4353	4354	4355	4356	4357	4358	4359
2	1	64	1	2	1	4	1	2	1
4360	4361	4362	4363	4364	4365	4366	4367	4368	4369
8	1	2	1	4	1	2	1	16	1
4370	4371	4372	4373	4374	4375	4376	4377	4378	4379
2	1	4	1	2	1	8	1	2	1
4380	4381	4382	4383	4384	4385	4386	4387	4388	4389
4	1	2	1	32	1	2	1	4	1
4390	4391	4392	4393	4394	4395	4396	4397	4398	4399
2	1	8	1	2	1	4	1	2	1

The PTE sieve

Phase 1 example: multiples of $2^7 = 128$

4350	4351	4352	4353	4354	4355	4356	4357	4358	4359
2	1	128	1	2	1	4	1	2	1
4360	4361	4362	4363	4364	4365	4366	4367	4368	4369
8	1	2	1	4	1	2	1	16	1
4370	4371	4372	4373	4374	4375	4376	4377	4378	4379
2	1	4	1	2	1	8	1	2	1
4380	4381	4382	4383	4384	4385	4386	4387	4388	4389
4	1	2	1	32	1	2	1	4	1
4390	4391	4392	4393	4394	4395	4396	4397	4398	4399
2	1	8	1	2	1	4	1	2	1

The PTE sieve

Phase 1 example: multiples of $2^8 = 256$

4350	4351	4352	4353	4354	4355	4356	4357	4358	4359
2	1	256	1	2	1	4	1	2	1
4360	4361	4362	4363	4364	4365	4366	4367	4368	4369
8	1	2	1	4	1	2	1	16	1
4370	4371	4372	4373	4374	4375	4376	4377	4378	4379
2	1	4	1	2	1	8	1	2	1
4380	4381	4382	4383	4384	4385	4386	4387	4388	4389
4	1	2	1	32	1	2	1	4	1
4390	4391	4392	4393	4394	4395	4396	4397	4398	4399
2	1	8	1	2	1	4	1	2	1

The PTE sieve

Phase 1 example: multiples of $2^9 = 512$

4350	4351	4352	4353	4354	4355	4356	4357	4358	4359
2	1	256	1	2	1	4	1	2	1
4360	4361	4362	4363	4364	4365	4366	4367	4368	4369
8	1	2	1	4	1	2	1	16	1
4370	4371	4372	4373	4374	4375	4376	4377	4378	4379
2	1	4	1	2	1	8	1	2	1
4380	4381	4382	4383	4384	4385	4386	4387	4388	4389
4	1	2	1	32	1	2	1	4	1
4390	4391	4392	4393	4394	4395	4396	4397	4398	4399
2	1	8	1	2	1	4	1	2	1

The PTE sieve

Phase 1 example: multiples of 3

4350	4351	4352	4353	4354	4355	4356	4357	4358	4359
6	1	256	3	2	1	12	1	2	3
4360	4361	4362	4363	4364	4365	4366	4367	4368	4369
8	1	6	1	4	3	2	1	48	1
4370	4371	4372	4373	4374	4375	4376	4377	4378	4379
2	3	4	1	6	1	8	3	2	1
4380	4381	4382	4383	4384	4385	4386	4387	4388	4389
12	1	2	3	32	1	6	1	4	3
4390	4391	4392	4393	4394	4395	4396	4397	4398	4399
2	1	24	1	2	3	4	1	6	1

The PTE sieve

Phase 1 example: multiples of $3^2 = 9$

4350	4351	4352	4353	4354	4355	4356	4357	4358	4359
6	1	256	3	2	1	36	1	2	3
4360	4361	4362	4363	4364	4365	4366	4367	4368	4369
8	1	6	1	4	9	2	1	48	1
4370	4371	4372	4373	4374	4375	4376	4377	4378	4379
2	3	4	1	18	1	8	3	2	1
4380	4381	4382	4383	4384	4385	4386	4387	4388	4389
12	1	2	9	32	1	6	1	4	3
4390	4391	4392	4393	4394	4395	4396	4397	4398	4399
2	1	72	1	2	3	4	1	6	1

The PTE sieve

Phase 1 example: multiples of $3^3 = 27$

4350	4351	4352	4353	4354	4355	4356	4357	4358	4359
6	1	256	3	2	1	36	1	2	3
4360	4361	4362	4363	4364	4365	4366	4367	4368	4369
8	1	6	1	4	9	2	1	48	1
4370	4371	4372	4373	4374	4375	4376	4377	4378	4379
2	3	4	1	54	1	8	3	2	1
4380	4381	4382	4383	4384	4385	4386	4387	4388	4389
12	1	2	9	32	1	6	1	4	3
4390	4391	4392	4393	4394	4395	4396	4397	4398	4399
2	1	72	1	2	3	4	1	6	1

The PTE sieve

Phase 1 example: multiples of $3^4 = 81$

4350	4351	4352	4353	4354	4355	4356	4357	4358	4359
6	1	256	3	2	1	36	1	2	3
4360	4361	4362	4363	4364	4365	4366	4367	4368	4369
8	1	6	1	4	9	2	1	48	1
4370	4371	4372	4373	4374	4375	4376	4377	4378	4379
2	3	4	1	162	1	8	3	2	1
4380	4381	4382	4383	4384	4385	4386	4387	4388	4389
12	1	2	9	32	1	6	1	4	3
4390	4391	4392	4393	4394	4395	4396	4397	4398	4399
2	1	72	1	2	3	4	1	6	1

The PTE sieve

Phase 1 example: multiples of $3^5 = 243$

4350	4351	4352	4353	4354	4355	4356	4357	4358	4359
6	1	256	3	2	1	36	1	2	3
4360	4361	4362	4363	4364	4365	4366	4367	4368	4369
8	1	6	1	4	9	2	1	48	1
4370	4371	4372	4373	4374	4375	4376	4377	4378	4379
2	3	4	1	486	1	8	3	2	1
4380	4381	4382	4383	4384	4385	4386	4387	4388	4389
12	1	2	9	32	1	6	1	4	3
4390	4391	4392	4393	4394	4395	4396	4397	4398	4399
2	1	72	1	2	3	4	1	6	1

The PTE sieve

Phase 1 example: multiples of $3^6 = 729$

4350	4351	4352	4353	4354	4355	4356	4357	4358	4359
6	1	256	3	2	1	36	1	2	3
4360	4361	4362	4363	4364	4365	4366	4367	4368	4369
8	1	6	1	4	9	2	1	48	1
4370	4371	4372	4373	4374	4375	4376	4377	4378	4379
2	3	4	1	1458	1	8	3	2	1
4380	4381	4382	4383	4384	4385	4386	4387	4388	4389
12	1	2	9	32	1	6	1	4	3
4390	4391	4392	4393	4394	4395	4396	4397	4398	4399
2	1	72	1	2	3	4	1	6	1

The PTE sieve

Phase 1 example: multiples of $3^7 = 2187$

4350	4351	4352	4353	4354	4355	4356	4357	4358	4359
6	1	256	3	2	1	36	1	2	3
4360	4361	4362	4363	4364	4365	4366	4367	4368	4369
8	1	6	1	4	9	2	1	48	1
4370	4371	4372	4373	4374	4375	4376	4377	4378	4379
2	3	4	1	4374	1	8	3	2	1
4380	4381	4382	4383	4384	4385	4386	4387	4388	4389
12	1	2	9	32	1	6	1	4	3
4390	4391	4392	4393	4394	4395	4396	4397	4398	4399
2	1	72	1	2	3	4	1	6	1

The PTE sieve

Phase 1 example: multiples of 5

4350	4351	4352	4353	4354	4355	4356	4357	4358	4359
30	1	256	3	2	5	36	1	2	3
4360	4361	4362	4363	4364	4365	4366	4367	4368	4369
40	1	6	1	4	45	2	1	48	1
4370	4371	4372	4373	4374	4375	4376	4377	4378	4379
10	3	4	1	4374	5	8	3	2	1
4380	4381	4382	4383	4384	4385	4386	4387	4388	4389
60	1	2	9	32	5	6	1	4	3
4390	4391	4392	4393	4394	4395	4396	4397	4398	4399
10	1	72	1	2	15	4	1	6	1

The PTE sieve

Phase 1 example: multiples of $5^2 = 25$

4350	4351	4352	4353	4354	4355	4356	4357	4358	4359
150	1	256	3	2	5	36	1	2	3
4360	4361	4362	4363	4364	4365	4366	4367	4368	4369
40	1	6	1	4	45	2	1	48	1
4370	4371	4372	4373	4374	4375	4376	4377	4378	4379
10	3	4	1	4374	25	8	3	2	1
4380	4381	4382	4383	4384	4385	4386	4387	4388	4389
60	1	2	9	32	5	6	1	4	3
4390	4391	4392	4393	4394	4395	4396	4397	4398	4399
10	1	72	1	2	15	4	1	6	1

The PTE sieve

Phase 1 example: multiples of $5^3 = 125$

4350	4351	4352	4353	4354	4355	4356	4357	4358	4359
150	1	256	3	2	5	36	1	2	3
4360	4361	4362	4363	4364	4365	4366	4367	4368	4369
40	1	6	1	4	45	2	1	48	1
4370	4371	4372	4373	4374	4375	4376	4377	4378	4379
10	3	4	1	4374	125	8	3	2	1
4380	4381	4382	4383	4384	4385	4386	4387	4388	4389
60	1	2	9	32	5	6	1	4	3
4390	4391	4392	4393	4394	4395	4396	4397	4398	4399
10	1	72	1	2	15	4	1	6	1

The PTE sieve

Phase 1 example: multiples of $5^4 = 625$

4350	4351	4352	4353	4354	4355	4356	4357	4358	4359
150	1	256	3	2	5	36	1	2	3
4360	4361	4362	4363	4364	4365	4366	4367	4368	4369
40	1	6	1	4	45	2	1	48	1
4370	4371	4372	4373	4374	4375	4376	4377	4378	4379
10	3	4	1	4374	625	8	3	2	1
4380	4381	4382	4383	4384	4385	4386	4387	4388	4389
60	1	2	9	32	5	6	1	4	3
4390	4391	4392	4393	4394	4395	4396	4397	4398	4399
10	1	72	1	2	15	4	1	6	1

The PTE sieve

Phase 1 example: multiples of $5^5 = 3125$

4350	4351	4352	4353	4354	4355	4356	4357	4358	4359
150	1	256	3	2	5	36	1	2	3
4360	4361	4362	4363	4364	4365	4366	4367	4368	4369
40	1	6	1	4	45	2	1	48	1
4370	4371	4372	4373	4374	4375	4376	4377	4378	4379
10	3	4	1	4374	625	8	3	2	1
4380	4381	4382	4383	4384	4385	4386	4387	4388	4389
60	1	2	9	32	5	6	1	4	3
4390	4391	4392	4393	4394	4395	4396	4397	4398	4399
10	1	72	1	2	15	4	1	6	1

The PTE sieve

Phase 1 example: multiples of 7

4350	4351	4352	4353	4354	4355	4356	4357	4358	4359
150	1	256	3	14	5	36	1	2	3
4360	4361	4362	4363	4364	4365	4366	4367	4368	4369
40	7	6	1	4	45	2	1	336	1
4370	4371	4372	4373	4374	4375	4376	4377	4378	4379
10	3	4	1	4374	4375	8	3	2	1
4380	4381	4382	4383	4384	4385	4386	4387	4388	4389
60	1	14	9	32	5	6	1	4	21
4390	4391	4392	4393	4394	4395	4396	4397	4398	4399
10	1	72	1	2	15	28	1	6	1

The PTE sieve

Phase 1 example: multiples of $7^2 = 49$

4350	4351	4352	4353	4354	4355	4356	4357	4358	4359
150	1	256	3	14	5	36	1	2	3
4360	4361	4362	4363	4364	4365	4366	4367	4368	4369
40	49	6	1	4	45	2	1	336	1
4370	4371	4372	4373	4374	4375	4376	4377	4378	4379
10	3	4	1	4374	4375	8	3	2	1
4380	4381	4382	4383	4384	4385	4386	4387	4388	4389
60	1	14	9	32	5	6	1	4	21
4390	4391	4392	4393	4394	4395	4396	4397	4398	4399
10	1	72	1	2	15	28	1	6	1

The PTE sieve

Phase 1 example: multiples of $7^3 = 343$

4350	4351	4352	4353	4354	4355	4356	4357	4358	4359
150	1	256	3	14	5	36	1	2	3
4360	4361	4362	4363	4364	4365	4366	4367	4368	4369
40	49	6	1	4	45	2	1	336	1
4370	4371	4372	4373	4374	4375	4376	4377	4378	4379
10	3	4	1	4374	4375	8	3	2	1
4380	4381	4382	4383	4384	4385	4386	4387	4388	4389
60	1	14	9	32	5	6	1	4	21
4390	4391	4392	4393	4394	4395	4396	4397	4398	4399
10	1	72	1	2	15	28	1	6	1

The PTE sieve

Phase 1 example: index $\stackrel{?}{=}$ number

4350	4351	4352	4353	4354	4355	4356	4357	4358	4359
150	1	256	3	14	5	36	1	2	3
4360	4361	4362	4363	4364	4365	4366	4367	4368	4369
40	49	6	1	4	45	2	1	336	1
4370	4371	4372	4373	4374	4375	4376	4377	4378	4379
10	3	4	1	4374	4375	8	3	2	1
4380	4381	4382	4383	4384	4385	4386	4387	4388	4389
60	1	14	9	32	5	6	1	4	21
4390	4391	4392	4393	4394	4395	4396	4397	4398	4399
10	1	72	1	2	15	28	1	6	1

The PTE sieve

Phase 1 example: bitstring representation of 7-smooth integers

4350	4351	4352	4353	4354	4355	4356	4357	4358	4359
0	0	0	0	0	0	0	0	0	0
4360	4361	4362	4363	4364	4365	4366	4367	4368	4369
0	0	0	0	0	0	0	0	0	0
4370	4371	4372	4373	4374	4375	4376	4377	4378	4379
0	0	0	0	1	1	0	0	0	0
4380	4381	4382	4383	4384	4385	4386	4387	4388	4389
0	0	0	0	0	0	0	0	0	0
4390	4391	4392	4393	4394	4395	4396	4397	4398	4399
0	0	0	0	0	0	0	0	0	0

The PTE sieve

Phase 2 example: $[1, 1, 8, 8, 15, 15] =_5 [0, 3, 5, 11, 13, 16]$.
$\rightsquigarrow$ factors $x - 16, x - 15, x - 13, x - 11, x - 8, x - 5, x - 3, x - 1, x$

The PTE sieve

Phase 2 example: $[1, 1, 8, 8, 15, 15] =_5 [0, 3, 5, 11, 13, 16]$.
$\rightsquigarrow$ factors $x - 16, x - 15, x - 13, x - 11, x - 8, x - 5, x - 3, x - 1, x$

Idea: this corresponds to the bit pattern $11x1x1xx1xx1x1x11$

The PTE sieve

Phase 2 example: $[1, 1, 8, 8, 15, 15] =_5 [0, 3, 5, 11, 13, 16]$.
$\rightsquigarrow$ factors $x - 16, x - 15, x - 13, x - 11, x - 8, x - 5, x - 3, x - 1, x$

Idea: this corresponds to the bit pattern $11x1x1xx1xx1x1x11$
$\rightsquigarrow$ search this pattern in the bitstring of smooth numbers

The PTE sieve

Phase 2 example: $[1, 1, 8, 8, 15, 15] =_5 [0, 3, 5, 11, 13, 16]$.

Interval: $5170314186700 + t$ for $t \in \{30, 31, \ldots, 59\}$, $B = 2^{15} = 32768$

The PTE sieve

Phase 2 example: $[1,1,8,8,15,15] =_5 [0,3,5,11,13,16]$.

Interval: $5170314186700 + t$ for $t \in \{30,31,\ldots,59\}$, $B = 2^{15} = 32768$

t	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59
smooth?	1	0	0	0	0	0	0	0	1	1	1	0	1	0	1	0	0	1	0	0	1	0	1	0	1	1	0	0	0	0
⋮																														
✗		1	1		1		1			1			1		1		1	1												
✗					1	1		1		1			1			1		1		1	1									
✗							1	1		1		1			1			1		1		1	1							
✗									1	1		1		1			1			1		1		1	1					
✓										1	1		1		1			1			1		1		1	1				

The PTE sieve

Phase 2 example: $[1, 1, 8, 8, 15, 15] =_5 [0, 3, 5, 11, 13, 16]$.

Interval: $5170314186700 + t$ for $t \in \{30, 31, \ldots, 59\}$, $B = 2^{15} = 32768$

t	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59
smooth?	1	0	0	0	0	0	0	0	1	1	1	0	1	0	1	0	0	1	0	0	1	0	1	0	1	1	0	0	0	0
$\vdots$																														
✗		1	1		1		1			1			1		1		1	1												
✗					1	1		1		1			1			1		1		1	1									
✗							1	1		1		1			1			1		1		1	1							
✗									1	1		1		1			1			1		1		1	1					
✓										1	1		1		1			1			1		1		1	1				

$\rightsquigarrow$ $u = 5170314186755$ is a candidate for producing twin 2^{15}-smooths

The PTE sieve

$$[1, 1, 8, 8, 15, 15] =_5 [0, 3, 5, 11, 13, 16], \; C = 14400, \; u = 5170314186755.$$

$$a(x) = (x-1)^2(x-8)^2(x-15)^2$$

$$a(u) \equiv 0 \mod C$$

$$m + 1 = a(u)/C$$

$$b(x) = x(x-3)(x-5)(x-11)(x-13)(x-16)$$

$$b(u) \equiv 0 \mod C$$

$$m = b(u)/C$$

The PTE sieve

$$[1, 1, 8, 8, 15, 15] =_5 [0, 3, 5, 11, 13, 16], \; C = 14400, \; u = 5170314186755.$$

$$a(x) = (x-1)^2(x-8)^2(x-15)^2 \qquad b(x) = x(x-3)(x-5)(x-11)(x-13)(x-16)$$

$$a(u) \equiv 0 \mod C \qquad b(u) \equiv 0 \mod C$$

$$m + 1 = a(u)/C \qquad m = b(u)/C$$

p = 2m+1 = 265319464891319853876302880884726722210256475303002503310412276022343680

The PTE sieve

$$[1,1,8,8,15,15] =_5 [0,3,5,11,13,16],\ C = 14400,\ u = 5170314186755.$$

$$a(x) = (x-1)^2(x-8)^2(x-15)^2 \qquad b(x) = x(x-3)(x-5)(x-11)(x-13)(x-16)$$

$$a(u) \equiv 0 \mod C \qquad b(u) \equiv 0 \mod C$$

$$m+1 = a(u)/C \qquad m = b(u)/C$$

p = 2m+1 = 265319464891319853876302880884726722210256475303002503310412276022343680 1 is prime!

The PTE sieve

$$[1,1,8,8,15,15] =_5 [0,3,5,11,13,16], \; C = 14400, \; u = 5170314186755.$$

$$a(x) = (x-1)^2(x-8)^2(x-15)^2 \qquad b(x) = x(x-3)(x-5)(x-11)(x-13)(x-16)$$

$$a(u) \equiv 0 \mod C \qquad b(u) \equiv 0 \mod C$$

$$m+1 = a(u)/C \qquad m = b(u)/C$$

p = 2m+1 = 2653194648913198538763028808847267222102564753030025033104122760223436801 is prime!

$$p+1 = 2 \cdot 3^2 \cdot 23^2 \cdot 41^2 \cdot 71^2 \cdot 83^2 \cdot 919^2 \cdot 1117^2 \cdot 1163^2 \cdot 1237^2 \cdot 6571^2 \cdot 11927^2 \cdot 18637^2 \cdot 32029^2$$

$$p-1 = 2^{12} \cdot 5^2 \cdot 7^2 \cdot 11^2 \cdot 13^2 \cdot 17 \cdot 29 \cdot 31 \cdot 43 \cdot 53 \cdot 103 \cdot 113 \cdot 181 \cdot 191 \cdot 211 \cdot 277 \cdot 557 \cdot 1093$$
$$\cdot 2663 \cdot 2897 \cdot 3347 \cdot 4783 \cdot 7963 \cdot 8623 \cdot 9787 \cdot 19841 \cdot 31489$$

Wrap-up: The PTE sieve

Wrap-up: The PTE sieve

- Python implementation of the PTE sieve

Wrap-up: The PTE sieve

- Python implementation of the PTE sieve
- C implementation of the sieving step

Wrap-up: The PTE sieve

- Python implementation of the PTE sieve
- C implementation of the sieving step
- Checks many PTE solutions in a single sieving step

Wrap-up: The PTE sieve

- Python implementation of the PTE sieve
- C implementation of the sieving step
- Checks many PTE solutions in a single sieving step
- $\sim$256-bit primes with 2^{15}-smooth neighbors

Wrap-up: The PTE sieve

- Python implementation of the PTE sieve
- C implementation of the sieving step
- Checks many PTE solutions in a single sieving step
- $\sim$256-bit primes with 2^{15}-smooth neighbors
- $\sim$384-bit primes with 2^{21}-smooth neighbors

Wrap-up: The PTE sieve

- Python implementation of the PTE sieve
- C implementation of the sieving step
- Checks many PTE solutions in a single sieving step
- $\sim$256-bit primes with 2^{15}-smooth neighbors
- $\sim$384-bit primes with 2^{21}-smooth neighbors
- $\sim$512-bit primes with 2^{29}-smooth neighbors

Wrap-up: The PTE sieve

- Python implementation of the PTE sieve
- C implementation of the sieving step
- Checks many PTE solutions in a single sieving step
- $\sim$256-bit primes with 2^{15}-smooth neighbors
- $\sim$384-bit primes with 2^{21}-smooth neighbors
- $\sim$512-bit primes with 2^{29}-smooth neighbors
- Variant that allows for non-smooth cofactors

Outline

Part I:

Isogenies and twin smooths

Part II:

Searching for twin smooths

Part III:

Constructing twin smooths

Part IV:

From twin smooths to SQISign primes

Størmer

- Consider twin B-smooths $(r, r+1)$ and $x = 2r + 1$.

Størmer

- Consider twin B-smooths $(r, r+1)$ and $x = 2r+1$.
- Let D be the square-free part of $(x-1)(x+1)$.
  $\rightsquigarrow x^2 - 1 = Dy^2$.

Størmer

- Consider twin B-smooths $(r, r+1)$ and $x = 2r+1$.
- Let D be the square-free part of $(x-1)(x+1)$.
  $\rightsquigarrow x^2 - 1 = Dy^2$.
- Størmer reverses this argument:

Størmer

- Consider twin B-smooths $(r, r+1)$ and $x = 2r + 1$.
- Let D be the square-free part of $(x-1)(x+1)$.
  $\rightsquigarrow x^2 - 1 = Dy^2$.
- Størmer reverses this argument:
  - Solve Pell equation $x^2 - Dy^2 = 1$ for all $2^{\pi(B)}$ possible choices of D.

Størmer

- Consider twin B-smooths $(r, r+1)$ and $x = 2r + 1$.
- Let D be the square-free part of $(x-1)(x+1)$.
  $\rightsquigarrow x^2 - 1 = Dy^2$.
- Størmer reverses this argument:
  - Solve Pell equation $x^2 - Dy^2 = 1$ for all $2^{\pi(B)}$ possible choices of D.
  - If y is smooth, we found twin smooths.

Størmer

- Consider twin B-smooths $(r, r+1)$ and $x = 2r+1$.
- Let D be the square-free part of $(x-1)(x+1)$.
  $\rightsquigarrow x^2 - 1 = Dy^2$.
- Størmer reverses this argument:
  - Solve Pell equation $x^2 - Dy^2 = 1$ for all $2^{\pi(B)}$ possible choices of D.
  - If y is smooth, we found twin smooths.
  - This method finds all B-smooth twins!

Størmer

- Consider twin B-smooths $(r, r+1)$ and $x = 2r + 1$.
- Let D be the square-free part of $(x-1)(x+1)$.
  $\rightsquigarrow x^2 - 1 = Dy^2$.
- Størmer reverses this argument:
  - Solve Pell equation $x^2 - Dy^2 = 1$ for all $2^{\pi(B)}$ possible choices of D.
  - If y is smooth, we found twin smooths.
  - This method finds all B-smooth twins!
  - But requires solving $2^{\pi(B)}$ Pell equations!
  - Solved up to $B = 113$ [see Costello's B-SIDH paper]; not large enough for cryptographic parameters.

The Conrey-Holmstrom-McLaughlin (CHM) algorithm

Main idea: given twin smooths $(r, r+1)$ and $(s, s+1)$ with $r < s$, we "often" have

$$\frac{r}{r+1} \cdot \frac{s+1}{s} = \frac{t}{t+1}.$$

The Conrey-Holmstrom-McLaughlin (CHM) algorithm

Main idea: given twin smooths $(r, r+1)$ and $(s, s+1)$ with $r < s$, we "often" have

$$\frac{r}{r+1} \cdot \frac{s+1}{s} = \frac{t}{t+1}.$$

$\rightsquigarrow$ CHM algorithm for finding B-smooth numbers:

- Start with $S^{(0)} = \{1, \ldots, B-1\}$.

The Conrey-Holmstrom-McLaughlin (CHM) algorithm

Main idea: given twin smooths $(r, r+1)$ and $(s, s+1)$ with $r < s$, we "often" have

$$\frac{r}{r+1} \cdot \frac{s+1}{s} = \frac{t}{t+1}.$$

$\rightsquigarrow$ CHM algorithm for finding B-smooth numbers:

- Start with $S^{(0)} = \{1, \ldots, B-1\}$.
- Run the CHM check for all $(r, s) \in S^{(0)} \times S^{(0)}$ and define $S^{(1)}$ as union of all new twins smooths and $S^{(0)}$.

The Conrey-Holmstrom-McLaughlin (CHM) algorithm

Main idea: given twin smooths $(r, r+1)$ and $(s, s+1)$ with $r < s$, we "often" have

$$\frac{r}{r+1} \cdot \frac{s+1}{s} = \frac{t}{t+1}.$$

$\rightsquigarrow$ CHM algorithm for finding B-smooth numbers:

- Start with $S^{(0)} = \{1, \ldots, B-1\}$.
- Run the CHM check for all $(r, s) \in S^{(0)} \times S^{(0)}$ and define $S^{(1)}$ as union of all new twins smooths and $S^{(0)}$.
- Repeat until $S^{(d)} = S^{(d-1)}$.

The Conrey-Holmstrom-McLaughlin (CHM) algorithm

Example: 5-smooth twins

The Conrey-Holmstrom-McLaughlin (CHM) algorithm

Example: 5-smooth twins

- $S^{(0)} = \{1, 2, 3, 4\}$

The Conrey-Holmstrom-McLaughlin (CHM) algorithm

Example: 5-smooth twins

- $S^{(0)} = \{1, 2, 3, 4\}$
- $(2, 3)$, $(2, 4)$ and $(3, 4)$ produce new twin smooths via CHM steps:

$$\frac{2}{2+1} \cdot \frac{3+1}{3} = \frac{8}{9}, \quad \frac{2}{2+1} \cdot \frac{4+1}{4} = \frac{5}{6}, \quad \text{and} \quad \frac{3}{3+1} \cdot \frac{4+1}{4} = \frac{15}{16}$$

The Conrey-Holmstrom-McLaughlin (CHM) algorithm

Example: 5-smooth twins

- $S^{(0)} = \{1, 2, 3, 4\}$
- $(2,3)$, $(2,4)$ and $(3,4)$ produce new twin smooths via CHM steps:

$$\frac{2}{2+1} \cdot \frac{3+1}{3} = \frac{8}{9}, \quad \frac{2}{2+1} \cdot \frac{4+1}{4} = \frac{5}{6}, \quad \text{and} \quad \frac{3}{3+1} \cdot \frac{4+1}{4} = \frac{15}{16}$$

$\rightsquigarrow S^{(1)} = \{1, 2, 3, 4, 5, 8, 15\}$

The Conrey-Holmstrom-McLaughlin (CHM) algorithm

Example: 5-smooth twins

- $S^{(0)} = \{1, 2, 3, 4\}$
- $(2, 3)$, $(2, 4)$ and $(3, 4)$ produce new twin smooths via CHM steps:

$$\frac{2}{2+1} \cdot \frac{3+1}{3} = \frac{8}{9}, \quad \frac{2}{2+1} \cdot \frac{4+1}{4} = \frac{5}{6}, \quad \text{and} \quad \frac{3}{3+1} \cdot \frac{4+1}{4} = \frac{15}{16}$$

$\rightsquigarrow S^{(1)} = \{1, 2, 3, 4, 5, 8, 15\}$

- $S^{(2)} = \{1, 2, 3, 4, 5, 8, 9, 15, 24\}$

The Conrey-Holmstrom-McLaughlin (CHM) algorithm

Example: 5-smooth twins

- $S^{(0)} = \{1, 2, 3, 4\}$
- $(2, 3)$, $(2, 4)$ and $(3, 4)$ produce new twin smooths via CHM steps:

$$\frac{2}{2+1} \cdot \frac{3+1}{3} = \frac{8}{9}, \quad \frac{2}{2+1} \cdot \frac{4+1}{4} = \frac{5}{6}, \quad \text{and} \quad \frac{3}{3+1} \cdot \frac{4+1}{4} = \frac{15}{16}$$

$\rightsquigarrow S^{(1)} = \{1, 2, 3, 4, 5, 8, 15\}$

- $S^{(2)} = \{1, 2, 3, 4, 5, 8, 9, 15, 24\}$
- $S^{(3)} = S^{(4)} = \{1, 2, 3, 4, 5, 8, 9, 15, 24, 80\}$

The Conrey-Holmstrom-McLaughlin (CHM) algorithm

Example: 5-smooth twins

- $S^{(0)} = \{1, 2, 3, 4\}$
- $(2, 3)$, $(2, 4)$ and $(3, 4)$ produce new twin smooths via CHM steps:

$$\frac{2}{2+1} \cdot \frac{3+1}{3} = \frac{8}{9}, \quad \frac{2}{2+1} \cdot \frac{4+1}{4} = \frac{5}{6}, \quad \text{and} \quad \frac{3}{3+1} \cdot \frac{4+1}{4} = \frac{15}{16}$$

  $\rightsquigarrow S^{(1)} = \{1, 2, 3, 4, 5, 8, 15\}$
- $S^{(2)} = \{1, 2, 3, 4, 5, 8, 9, 15, 24\}$
- $S^{(3)} = S^{(4)} = \{1, 2, 3, 4, 5, 8, 9, 15, 24, 80\}$ is the full set of 5-smooth twins!

The Conrey-Holmstrom-McLaughlin (CHM) algorithm

Question: Does this scale to larger smoothness bounds?

The Conrey-Holmstrom-McLaughlin (CHM) algorithm

Question: Does this scale to larger smoothness bounds?

- CHM paper: run for $B = 100$ found 13 333 twin smooths (largest: 58 bit)

The Conrey-Holmstrom-McLaughlin (CHM) algorithm

Question: Does this scale to larger smoothness bounds?

- CHM paper: run for $B = 100$ found 13 333 twin smooths (largest: 58 bit)
- 37 missing twins

The Conrey-Holmstrom-McLaughlin (CHM) algorithm

Question: Does this scale to larger smoothness bounds?

- CHM paper: run for $B = 100$ found 13 333 twin smooths (largest: 58 bit)
- 37 missing twins
- 36 of these were found with CHM and $B = 200$ (and all for $B = 227$)

The Conrey-Holmstrom-McLaughlin (CHM) algorithm

Question: Does this scale to larger smoothness bounds?

- CHM paper: run for $B = 100$ found 13 333 twin smooths (largest: 58 bit)
- 37 missing twins
- 36 of these were found with CHM and $B = 200$ (and all for $B = 227$)
- CHM for $B = 200$ found 346 192 twin smooths (largest: 79 bit)

The Conrey-Holmstrom-McLaughlin (CHM) algorithm

Question: Does this scale to larger smoothness bounds?

- CHM paper: run for $B = 100$ found 13 333 twin smooths (largest: 58 bit)
- 37 missing twins
- 36 of these were found with CHM and $B = 200$ (and all for $B = 227$)
- CHM for $B = 200$ found 346 192 twin smooths (largest: 79 bit)

$\rightsquigarrow$ Conjecture: The CHM algorithm finds “almost all” twin B-smooths.

The Conrey-Holmstrom-McLaughlin (CHM) algorithm

Question: Does this scale to larger smoothness bounds?

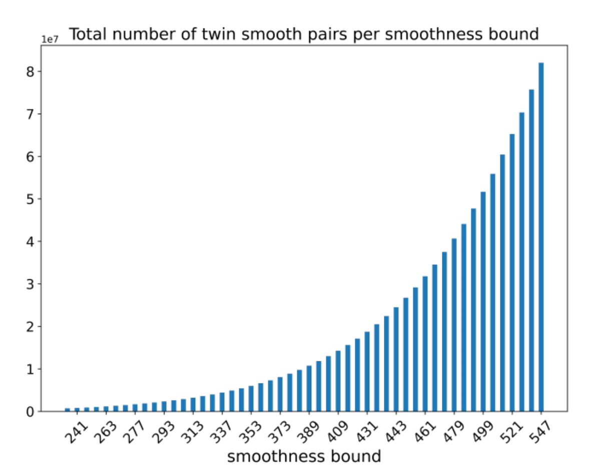
- CHM paper: run for $B = 100$ found 13 333 twin smooths (largest: 58 bit)
- 37 missing twins
- 36 of these were found with CHM and $B = 200$ (and all for $B = 227$)
- CHM for $B = 200$ found 346 192 twin smooths (largest: 79 bit)

$\rightsquigarrow$ Conjecture: The CHM algorithm finds "almost all" twin B-smooths.

$\rightsquigarrow$ CHM: "The unanswered question in all of this is why does it work?"

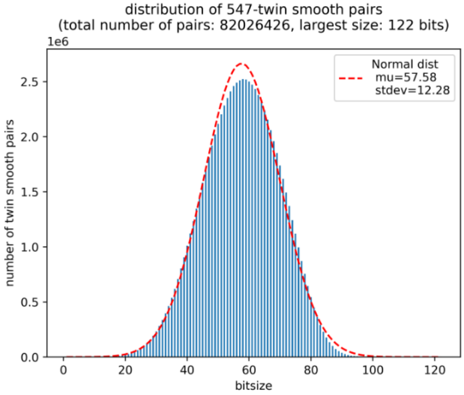
The Conrey-Holmstrom-McLaughlin (CHM) algorithm

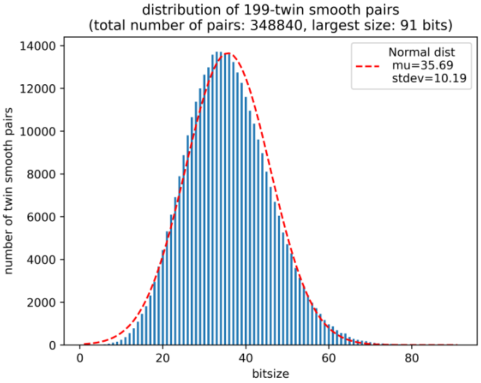
We implemented CHM in C++ and ran it up to $B = 547$.



The Conrey-Holmstrom-McLaughlin (CHM) algorithm

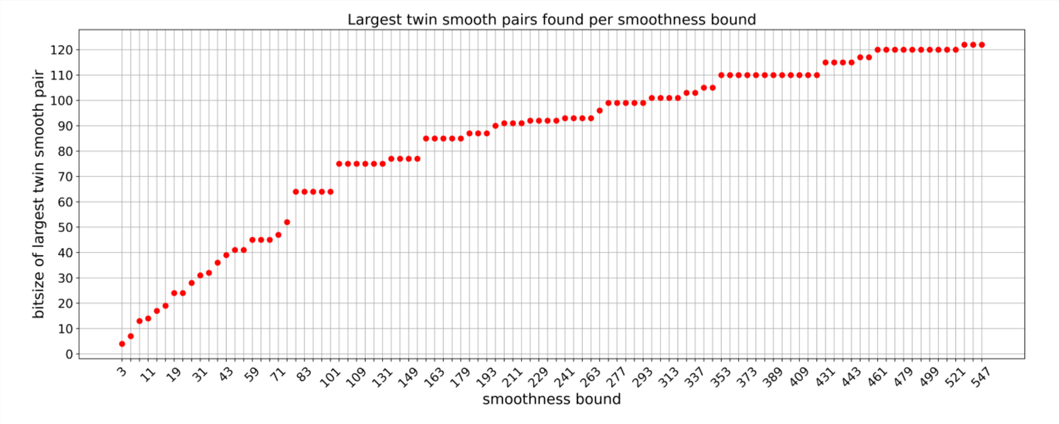
We implemented CHM in C++ and ran it up to $B = 547$.





The Conrey-Holmstrom-McLaughlin (CHM) algorithm

We implemented CHM in C++ and ran it up to $B = 547$.



CHM optimizations

Observation: We need optimizations and have to sacrifice completeness for larger twin smooths.

CHM optimizations

Observation: We need optimizations and have to sacrifice completeness for larger twin smooths.

- We only get new twins with $t > r, s$ if $r < s < 2r$.

CHM optimizations

Observation: We need optimizations and have to sacrifice completeness for larger twin smooths.

- We only get new twins with $t > r, s$ if $r < s < 2r$.
- Better chances if r, s are k-balanced $(r < s < kr)$ for $k = 1 + \varepsilon$.

CHM optimizations

Observation: We need optimizations and have to sacrifice completeness for larger twin smooths.

- We only get new twins with $t > r, s$ if $r < s < 2r$.
- Better chances if r, s are k-balanced ($r < s < kr$) for $k = 1 + \varepsilon$.
  - $\rightsquigarrow$ `global-`k variant checks only k-balanced pairs of twins.

CHM optimizations

Observation: We need optimizations and have to sacrifice completeness for larger twin smooths.

- We only get new twins with $t > r, s$ if $r < s < 2r$.
- Better chances if r, s are k-balanced ($r < s < kr$) for $k = 1 + \varepsilon$.
  $\rightsquigarrow$ `global-`k variant checks only k-balanced pairs of twins.
- Lots of time wasted for size checks, i.e. if $s < kr$

CHM optimizations

Observation: We need optimizations and have to sacrifice completeness for larger twin smooths.

- We only get new twins with $t > r, s$ if $r < s < 2r$.
- Better chances if r, s are k-balanced ($r < s < kr$) for $k = 1 + \varepsilon$.
  $\rightsquigarrow$ `global-k` variant checks only k-balanced pairs of twins.
- Lots of time wasted for size checks, i.e. if $s < kr$
  $\rightsquigarrow$ `constant-range` variant checks a fixed number of neighbors of each r.

CHM optimizations

Observation: We need optimizations and have to sacrifice completeness for larger twin smooths.

- We only get new twins with $t > r, s$ if $r < s < 2r$.
- Better chances if r, s are k-balanced ($r < s < kr$) for $k = 1 + \varepsilon$.
  $\rightsquigarrow$ `global-`k variant checks only k-balanced pairs of twins.
- Lots of time wasted for size checks, i.e. if $s < kr$
  $\rightsquigarrow$ `constant-range` variant checks a fixed number of neighbors of each r.
- Other variants like `variable-range` or `iterative-`k seem to perform worse.

CHM optimizations

Comparison for $B = 300$.

Variant	Parameter	Runtime	Speedup	#twins	#twins from largest 100
Full CHM	-	4705s	1	2300724	100
`global-`k	$k = 2.0$	364s	13	2289000	86
	$k = 1.5$	226s	21	2282741	82
	$k = 1.05$	27s	174	2206656	65
`constant-range`	$R = 10000$	82s	57	2273197	93
	$R = 5000$	35s	134	2247121	87
	$R = 1000$	16s	294	2074530	75

CHM optimizations

Even with optimizations and larger smoothness bounds we are not able to generate twin smooths $> 2^{200}$...

CHM optimizations

Even with optimizations and larger smoothness bounds we are not able to generate twin smooths $> 2^{200}$...

... but we can generate lots of twin smooths below 100-bit, and some up to 128-bit.

CHM optimizations

Even with optimizations and larger smoothness bounds we are not able to generate twin smooths $> 2^{200}$...

... but we can generate lots of twin smooths below 100-bit, and some up to 128-bit.

Is this still useful for generating SQISign primes?

Outline

Part I:

Isogenies and twin smooths

Part II:

Searching for twin smooths

Part III:

Constructing twin smooths

Part IV:

From twin smooths to SQISign primes

SQISign requirements

SQISign prime requirements:

- $\approx$ 256-bit prime for NIST-I
- $\approx$ 384-bit prime for NIST-III
- $\approx$ 512-bit prime for NIST-V
- B-smooth factor $T' = 2^f \cdot T \mid p^2 - 1$
- $T \approx p^{5/4}$
- f as large as possible
- Signing cost metric: $\sqrt{B}/f$

Boosting twin smooths

Idea: use primes of the form $p_n = 2x^n - 1$ and plug in twin smooths $(x-1, x)$

$n = 2$: $p_2(x)^2 - 1 = 4x^2(x-1)(x+1)$

Boosting twin smooths

Idea: use primes of the form $p_n = 2x^n - 1$ and plug in twin smooths $(x-1, x)$

$n = 2$: $p_2(x)^2 - 1 = 4x^2(x-1)(x+1)$

$\rightsquigarrow$ smooth factor T' of size $p^{3/2}$ guaranteed!

Boosting twin smooths

Idea: use primes of the form $p_n = 2x^n - 1$ and plug in twin smooths $(x-1, x)$

$n = 2$: $p_2(x)^2 - 1 = 4x^2(x-1)(x+1)$

$\rightsquigarrow$ smooth factor T' of size $p^{3/2}$ guaranteed!

$n = 3$: $p_3(x)^2 - 1 = 4x^3(x-1)(x^2+x+1)$

$\rightsquigarrow$ smooth factor T' of size $p^{4/3}$ guaranteed!

Boosting twin smooths

Idea: use primes of the form $p_n = 2x^n - 1$ and plug in twin smooths $(x-1, x)$

$n = 2$: $p_2(x)^2 - 1 = 4x^2(x-1)(x+1)$

$\rightsquigarrow$ smooth factor T' of size $p^{3/2}$ guaranteed!

$n = 3$: $p_3(x)^2 - 1 = 4x^3(x-1)(x^2+x+1)$

$\rightsquigarrow$ smooth factor T' of size $p^{4/3}$ guaranteed!

$n = 4$: $p_4(x)^2 - 1 = 4x^4(x-1)(x+1)(x^2+1)$

$\rightsquigarrow$ smooth factor T' of size $p^{5/4}$ guaranteed!

Boosting twin smooths

Idea: use primes of the form $p_n = 2x^n - 1$ and plug in twin smooths $(x-1, x)$

$n = 2$: $p_2(x)^2 - 1 = 4x^2(x-1)(x+1)$

$\rightsquigarrow$ smooth factor T' of size $p^{3/2}$ guaranteed!

$n = 3$: $p_3(x)^2 - 1 = 4x^3(x-1)(x^2+x+1)$

$\rightsquigarrow$ smooth factor T' of size $p^{4/3}$ guaranteed!

$n = 4$: $p_4(x)^2 - 1 = 4x^4(x-1)(x+1)(x^2+1)$

$\rightsquigarrow$ smooth factor T' of size $p^{5/4}$ guaranteed!

$n = 6$: $p_6(x)^2 - 1 = 4x^6(x-1)(x+1)(x^2-x+1)(x^2+x+1)$

$\rightsquigarrow$ smooth factor T' of size $p^{7/6}$ guaranteed!

Boosting twin smooths

Idea: use primes of the form $p_n = 2x^n - 1$ and plug in twin smooths $(x-1, x)$

$n = 2$: $p_2(x)^2 - 1 = 4x^2(x-1)(x+1)$

$\rightsquigarrow$ smooth factor T' of size $p^{3/2}$ guaranteed!

$n = 3$: $p_3(x)^2 - 1 = 4x^3(x-1)(x^2+x+1)$

$\rightsquigarrow$ smooth factor T' of size $p^{4/3}$ guaranteed!

$n = 4$: $p_4(x)^2 - 1 = 4x^4(x-1)(x+1)(x^2+1)$

$\rightsquigarrow$ smooth factor T' of size $p^{5/4}$ guaranteed!

$n = 6$: $p_6(x)^2 - 1 = 4x^6(x-1)(x+1)(x^2-x+1)(x^2+x+1)$

$\rightsquigarrow$ smooth factor T' of size $p^{7/6}$ guaranteed!

$\rightsquigarrow$ Smaller CHM/PTE twins can generate SQISign-friendly primes!

NIST-I results

253-bit prime $p = 2r^4 - 1$ from 467-smooth twins (CHM) with $r = 8077251317941145600$:

$$p + 1 = 2^{49} \cdot 5^8 \cdot 13^4 \cdot 41^4 \cdot 71^4 \cdot 113^4 \cdot 181^4 \cdot 223^4 \cdot 457^4, \text{ and}$$

$$p - 1 = 2 \cdot 3^2 \cdot 7^5 \cdot 17 \cdot 31 \cdot 53 \cdot 61 \cdot 73 \cdot 83 \cdot 127 \cdot 149 \cdot 233 \cdot 293 \cdot 313 \cdot 347 \cdot 397 \cdot 467 \cdot 479 \cdot 991 \cdot 1667 \cdot 19813 \cdot 211229 \cdot 107155419089 \cdot 295288804621$$

Signing cost metric: $\sqrt{B}/f \approx 0.45$

Smooth factor of size: $\log_p(T) \approx 1.30$

NIST-III results

382-bit prime $p = 2r^6 - 1$ from 547-smooth twins (CHM) with $r = 11896643388662145024$:

$$p + 1 = 2^{79} \cdot 3^6 \cdot 23^{12} \cdot 107^6 \cdot 127^6 \cdot 307^6 \cdot 401^6 \cdot 547^6, \text{ and}$$
$$p - 1 = 2 \cdot 5^2 \cdot 7 \cdot 11 \cdot 17 \cdot 19 \cdot 47 \cdot 71 \cdot 79 \cdot 109 \cdot 149 \cdot 229 \cdot 269 \cdot 283 \cdot 349 \cdot 449$$
$$\cdot 463 \cdot 1019 \cdot 1033 \cdot 1657 \cdot 2179 \cdot 2293 \cdot 4099 \cdot 5119 \cdot 10243 \cdot 381343$$
$$\cdot 19115518067 \cdot 740881808972441233 \cdot 83232143791482135163921.$$

Signing cost metric: $\sqrt{B}/f \approx 1.28$

Smooth factor of size: $\log_p(T) \approx 1.30$

NIST-V results

508-bit prime $p = 2r^4 - 1$ from 15263-smooth twins (PTE) with
$r = 123794274387474298912742543819242587136$:

$$p + 1 = 2^{41} \cdot 13^{16} \cdot 17^8 \cdot 1871^8 \cdot 2503^8 \cdot 2837^8 \cdot 9109^8, \text{ and}$$

$$\begin{aligned} p - 1 = {} & 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 29 \cdot 31^2 \cdot 41 \cdot 61 \cdot 67 \cdot 199 \cdot 241 \cdot 439 \cdot 557 \cdot 563 \cdot 827 \\ & \cdot 1061 \cdot 1433 \cdot 1579 \cdot 1741 \cdot 2633 \cdot 6089 \cdot 7151 \cdot 15263 \cdot 798697 \cdot 377541617 \\ & \cdot 152092926281 \cdot 318679033448456045803337 \cdot 10285349110889775504103 3 \\ & \cdot 725324272785121916930700 1. \end{aligned}$$

Signing cost metric: $\sqrt{B}/f \approx 3.01$
Smooth factor of size: $\log_p(T) \approx 1.29$

Wrap-up

- We can find (lots of) smaller twin smooths with CHM.
- We can construct SQISign primes from smaller twin smooths.
- Performance gain still unclear for NIST-I.
- First practical parameters for NIST-III and NIST-V.

Wrap-up

- We can find (lots of) smaller twin smooths with CHM.
- We can construct SQISign primes from smaller twin smooths.
- Performance gain still unclear for NIST-I.
- First practical parameters for NIST-III and NIST-V.

https://ia.cr/2020/1283

https://ia.cr/2022/1439