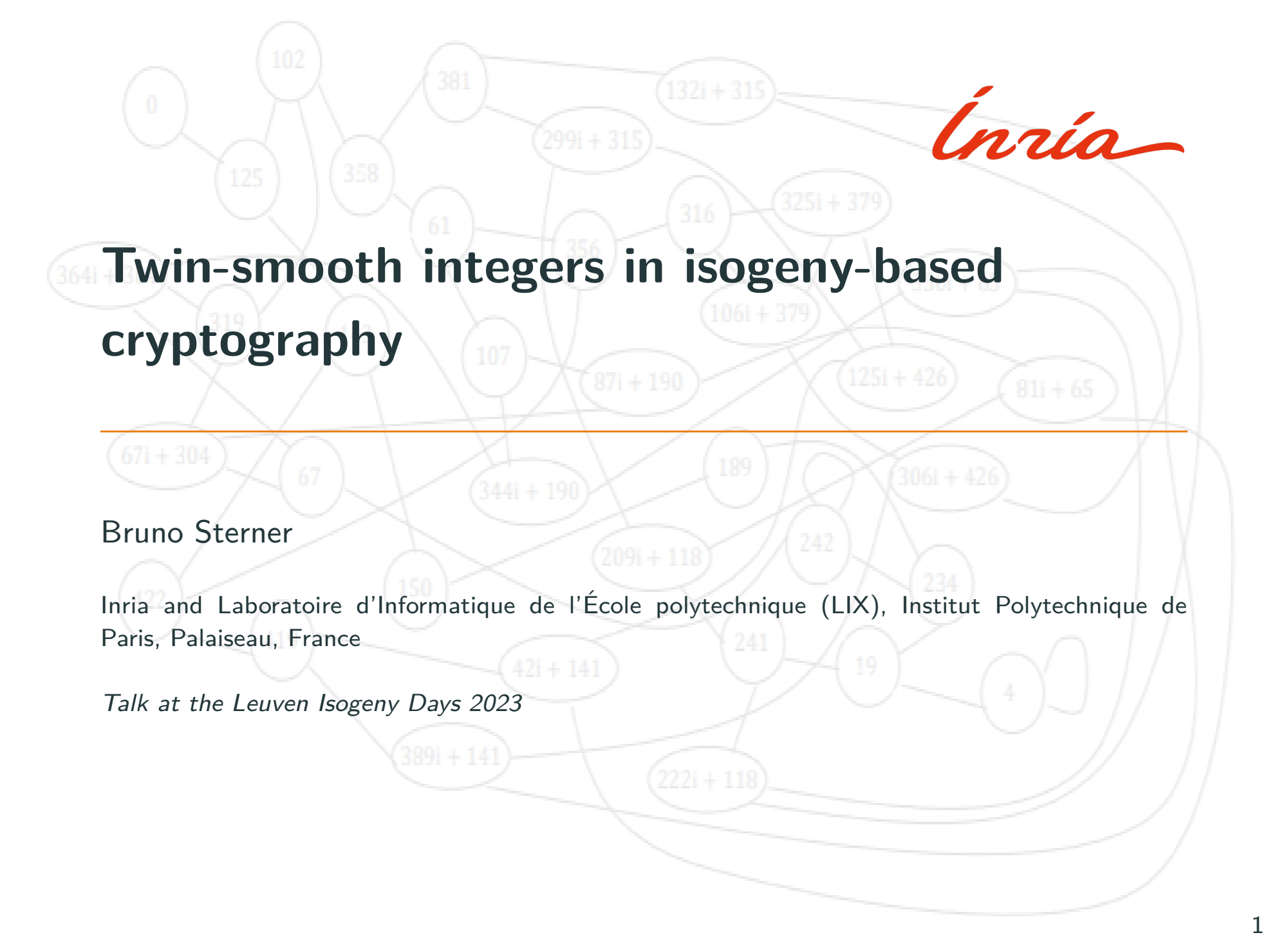


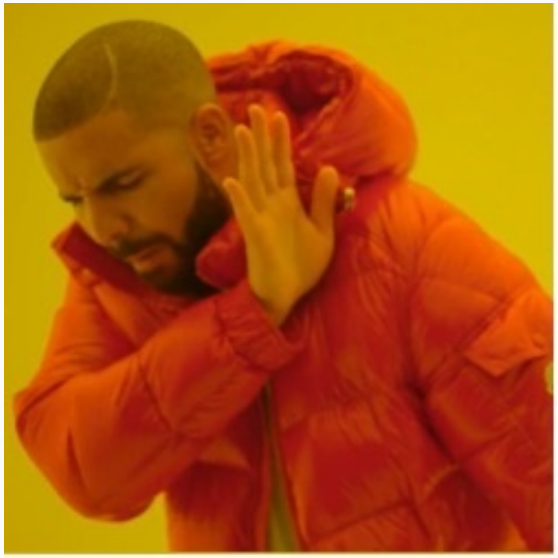
Twin-smooth integers in isogeny-based cryptography

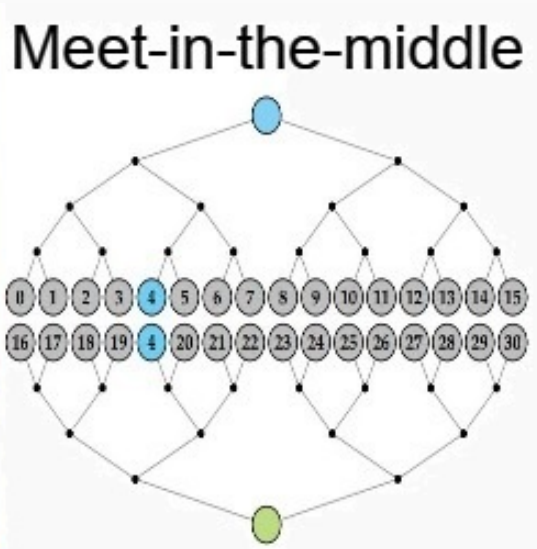
Bruno Sterner

Inria and Laboratoire d'Informatique de l'École polytechnique (LIX), Institut Polytechnique de Paris, Palaiseau, France

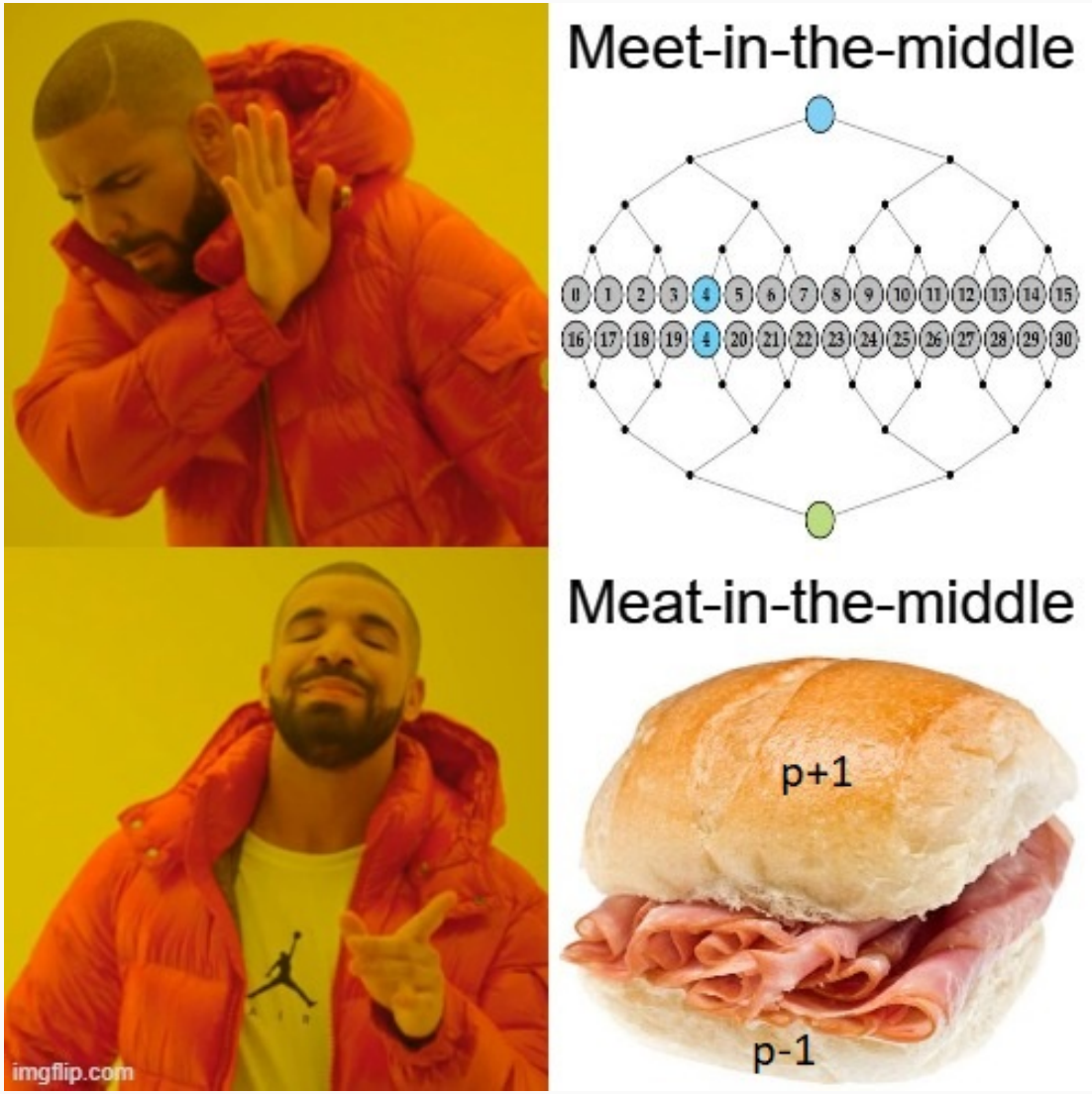
Talk at the Leuven Isogeny Days 2023

Meet-in-the-Middle





Meat-in-the-Middle



Motivation

Cryptographic sized primes p such that $p^2 - 1$ is smooth[1] or has a large smooth cofactor

~~*B-SIDH*~~ $\phi : E \to E'$ *SQISign*

The SQISign NIST submission use the following 254-bit prime

p=0x34E29E286B95D98C33A6A86587407437252C9E49355147FFFFFFFFFFFFFFFFF:

$$p + 1 = 2^{75} \cdot 3^{36} \cdot 23^2 \cdot 59^2 \cdot 101^2 \cdot 109^2 \cdot 197^2 \cdot 491^2 \cdot 743^2 \cdot 1913^2, \text{ and}$$

$$p - 1 = 2 \cdot 7^4 \cdot 11 \cdot 13 \cdot 37 \cdot 89 \cdot 97 \cdot 107 \cdot 131 \cdot 137 \cdot 223 \cdot 239 \cdot 383 \cdot 389 \cdot 499 \cdot 607 \cdot 1033 \cdot 1049 \cdot 1193 \cdot 1973 \cdot 32587069 \cdot 275446333 \cdot 1031359276391767$$

[1] A number n is B-smooth if all the prime factors of n are at most B

Twin-smooth integers

Definition

For an integer B, we say that a pair of consecutive integers, $(r, r+1)$, are B-smooth twins if their product $r(r+1)$ is B-smooth.

For instance, the following are 7-smooth twins:

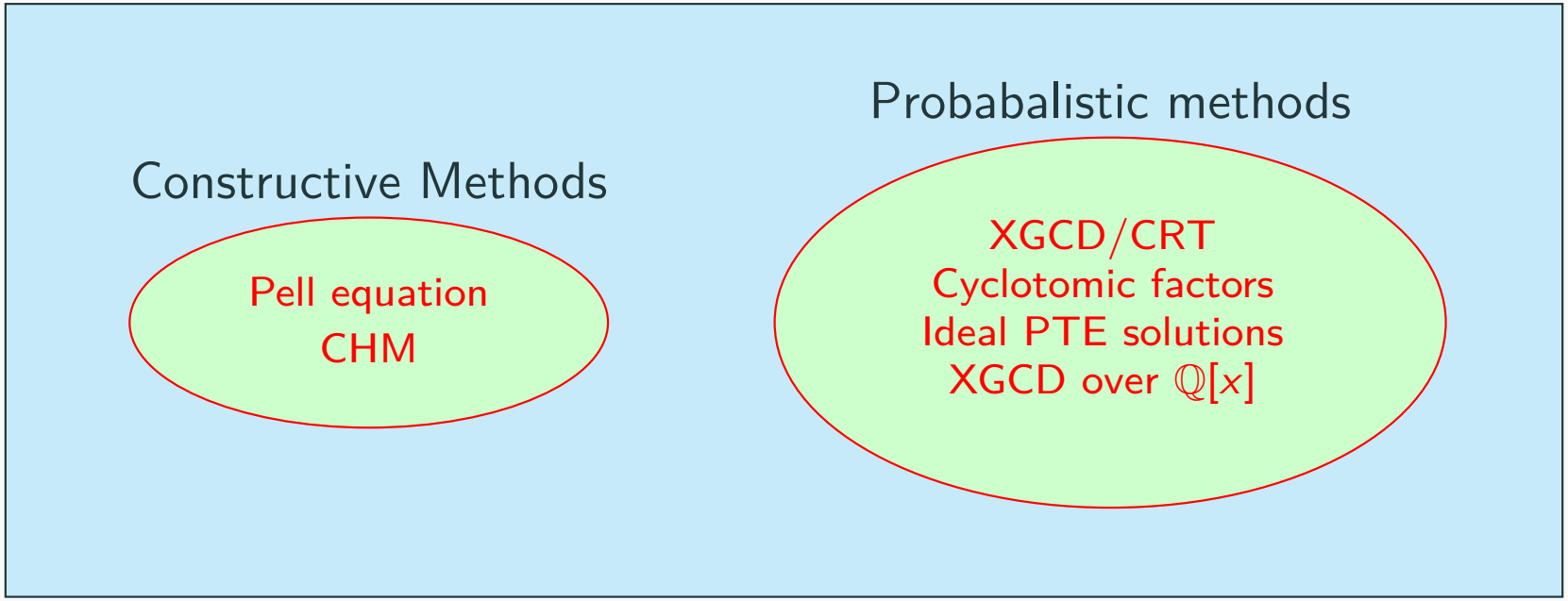
$$r = 4374 = 2 \cdot 3^7, \text{ and } r + 1 = 4375 = 5^4 \cdot 7$$

Remark: If $p = 2r + 1$ is prime then $p^2 - 1 = 4r(r+1)$ is B-smooth and hence can be used in isogeny-based applications

Surprisingly, for a fixed B, the set of B-smooth twins is *finite!*

B	2	3	5	7	11	13	17	.....
# B-smooth twins	1	4	10	23	40	68	108	.....

Current landscape for finding smooth twins



Constructive: Find all or almost all B-smooth twins for a fixed B;

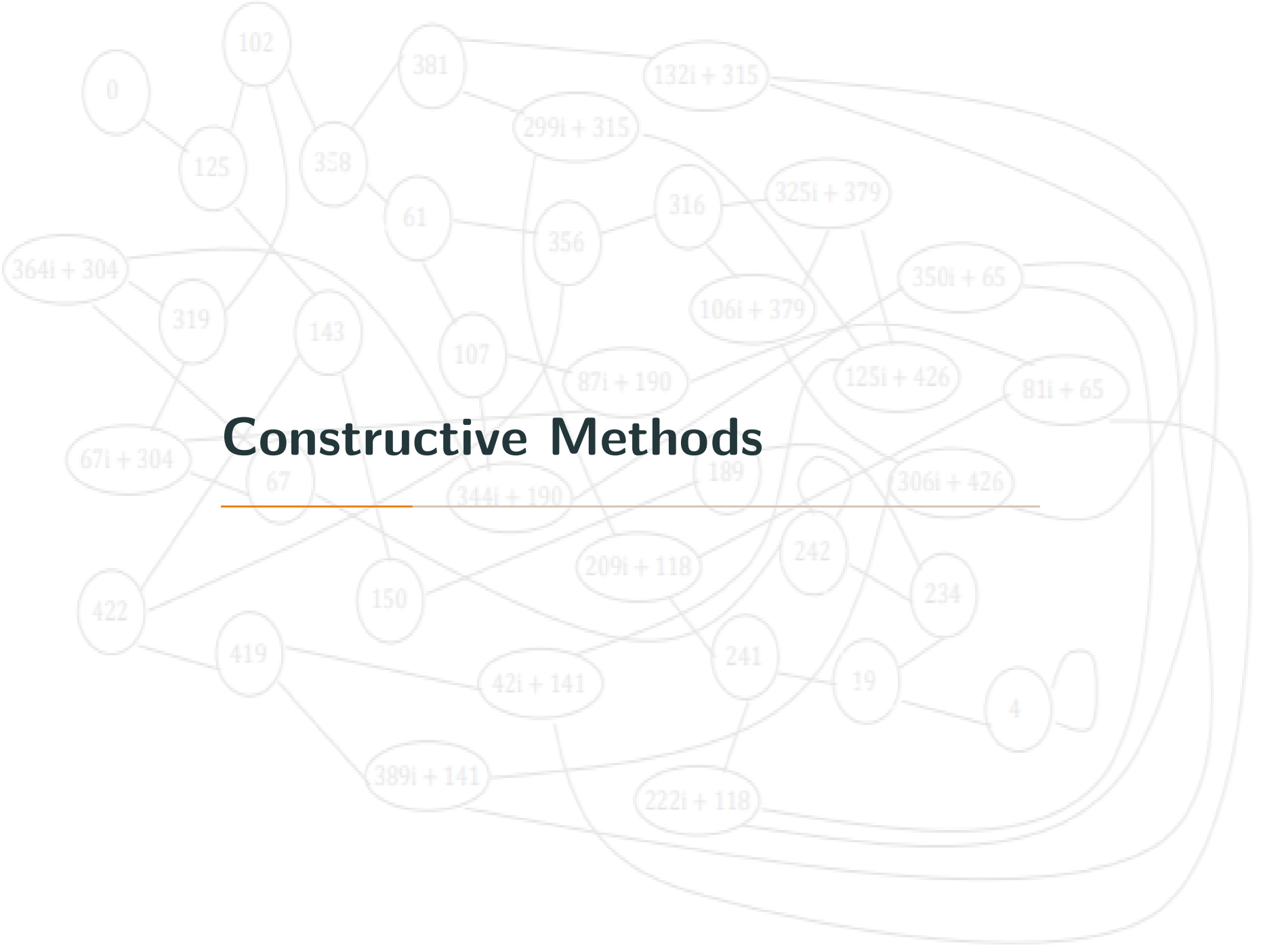
Probabilistic: Find large B-smooth twins of a fixed size.

Outline for consuming our smooth sandwiches

Constructive Methods

Probabilistic Methods

Applications to Isogeny-based Cryptosystems



Constructive Methods

Solutions to the Pell equation

- $(r, r+1)$ – B-smooth twin
- $x \coloneqq 2r+1$, so that $x^2 - 1$ is B-smooth
- Write $x^2 - 1 = Dy^2$ where D, y are B-smooth and D is squarefree
- Then (x, y) is a solution to the Pell conic

$$X^2 - DY^2 = 1$$

Thus solving all $2^{\pi(B)}$ Pell equations (one for each squarefree and B-smooth choice of D) will find the complete set of B-smooth twins

Størmer (1897) and Lehmer (1964) proved this set of solutions with y being B-smooth is finite, so the set of B-smooth twins is *finite*

B	2	3	5	$\cdots$	40	$\cdots$	100	$\cdots$	113
# B-smooth twins	1	4	10	$\cdots$	653	$\cdots$	13374	$\cdots$	33233

CHM algorithm

An algorithm devised by Conrey, Holmstrom and McLaughlin (2012) that finds *almost all* B-smooth twins

- $S^{(0)} = \{1, 2, \cdots, B-1\}$ – representing B-smooth twins $(1,2), (2,3), \cdots, (B-1, B)$
- For each $r, s \in S^{(0)}$ with $r < s$ compute

$$\frac{t}{t'} = \frac{r}{r+1} \cdot \frac{s+1}{s} \qquad \text{with } \gcd(t, t') = 1$$

- $S^{(1)} := S^{(0)} \cup \{\text{new solutions } t : t' = t+1\}$
- Repeat this with $S^{(1)}$ instead of $S^{(0)}$
- Algorithm terminates when $S^{(d+1)} = S^{(d)}$ for some d

When $t' = t + 1$, this equivalent to $t = \frac{r(s+1)}{s-r}$ being an integer

CHM in action

With $B = 7$, the CHM algorithm produces

$$S^{(5)} = S^{(4)} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 14, 15, 20, 24, 27, 35, 48, 49, 63, 80, 125, 224, 2400\}$$

This is not the full set of 7-smooth twins – the largest 7-smooth twin, $(4374, 4375)$, is not found

Running this with $B = 11$ will find this missing twin

$11 \leq B < 41$: finds all B-smooth twins

$B \geq 41$: finds *almost all* B-smooth twins

With $B = 100$ they found all except 41 B-smooth twins. With $B = 200$ they found 346,192 such twins – which took them 2 weeks to run

Our experiments with G. Bruno, M. Cortes-Real Santos, et. al.

We optimised the CHM algorithm and ran $B = 200$ much faster[2]!

Subsequently we ran it fully for $B = 547$ – the largest twin found was the following 122-bit twin

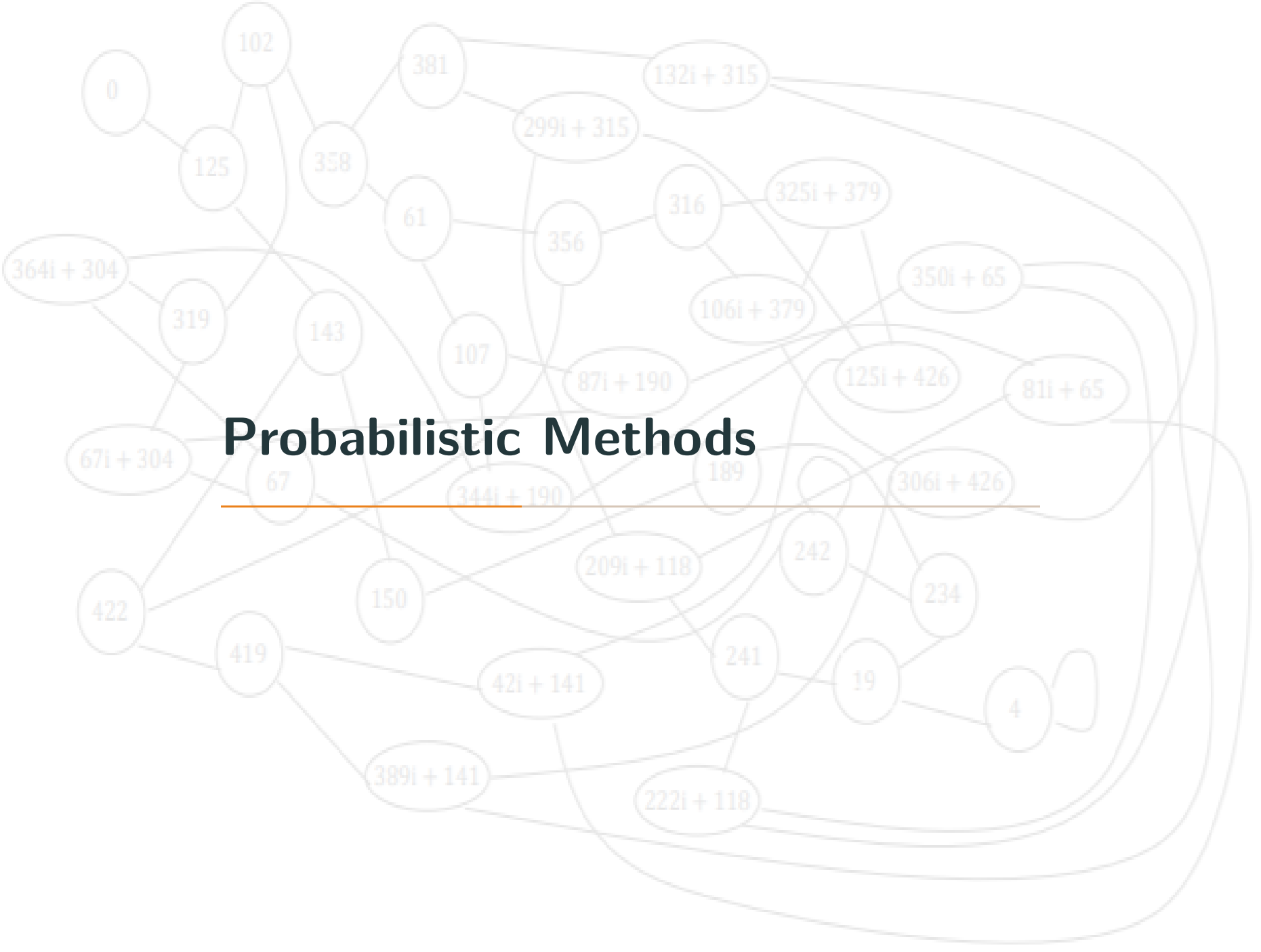
$$r = 5^4 \cdot 7 \cdot 13^2 \cdot 17^2 \cdot 19 \cdot 29 \cdot 41 \cdot 109 \cdot 163 \cdot 173 \cdot 239 \cdot 241^2 \cdot 271 \cdot 283 \cdot 499 \cdot 509, \text{ and}$$
$$r + 1 = 2^8 \cdot 3^2 \cdot 31^2 \cdot 43^2 \cdot 47^2 \cdot 83^2 \cdot 103^2 \cdot 311^2 \cdot 479^2 \cdot 523^2.$$

An additional 2,649 200-smooth twins were found from this computation

Can we be sure this is all of them? No! Only way guarantee the exact number of 200-smooth twins is to solve all $2^{\pi(200)} = 2^{46}$ Pell equations

We also introduced some other optimisations that made it possible for us to run larger values of B (e.g. $B = 2^{11}$)

[2]The computation now takes a mere 7 minutes to run on a laptop



Probabilistic Methods

XGCD over $\mathbb{Z}$ and CRT

Naïve approach: choose a smooth integer r and *hope* the $r + 1$ is also smooth

A much better approach is to force smooth factors $s \mid r$ and $t \mid r + 1$ of size $s \cdot t \approx r$

Instead of hoping that an integer of size r is smooth, one hopes that two integers of size $\approx \sqrt{r}$ are smooth

Algorithmically, this can be achieved with either

- Extended Euclidean algorithm (XGCD) by Costello (2019)
- Chinese remainder theorem (CRT) by De Feo et al. (2020)

Issue with this is that the search space is much too big to find instances with a (relatively) small smoothness bound

Sieving with cyclotomic factors

In Costello's computations with the Pell equations, he noticed that a lot of twins were of the form $(x^2 - 1, x^2)$

To obtain cryptographic sized twins, he generalised this idea to find twins of the form

$$(x^n - 1, x^n) \text{ for even } n$$

$x^n - 1$ factors into its cyclotomic factors, e.g. with $n = 8$ we have

$$x^8 - 1 = (x - 1)(x + 1)(x^2 + 1)(x^4 + 1)$$

So finding smooth twins amounts to seaching for integers ℓ such that $\ell - 1, \ell, \ell + 1, \ell^2 + 1, \ell^4 + 1$ are all smooth

As n increases, the larger degree factors become the bottleneck in reducing the smoothness bound

Sieving using completely split polynomial pairs

More recently, Costello, Meyer and Naehrig (2021) replaced these with polynomial pairs f, g that split completely into linear factors

Namely, pairs of the form

$$f(x) = \prod_{a \in \mathcal{A}} (x + a), \quad g(x) = \prod_{b \in \mathcal{B}} (x + b), \quad \text{with } g - f \equiv C$$

To find smooth twins one searches for integers ℓ such that $\ell + a$ and $\ell + b$ are all smooth. Additionally, one requires $f(\ell) = g(\ell) = 0 \mod C$

All of this results in the twin

$$\left(\frac{f(\ell)}{C}, \frac{g(\ell)}{C} \right)$$

One can find these pairs from solutions to the ideal Prouhet-Tarry-Escott (PTE) problem

Do we have too many linear factors?

At least when $\deg(f) > 6$ we have too many linear factors!

$$f(x) = x(x+4)(x+9)(x+23)(x+27)(x+41)(x+46)(x+50), \text{ and}$$
$$g(x) = (x+1)(x+2)(x+11)(x+20)(x+30)(x+39)(x+48)(x+49).$$

$$f(x) = (x+1)(x+4)(x+9)(x+10)(x+15)(x+18)(x^2+19x-12), \text{ and}$$
$$g(x) = x^2(x+6)^2(x+13)^2(x+19)^2.$$

First pair:	*16* linear factors;
Second pair:	*10* linear factors and *1* quadratic factor

The probability of finding smooth twins from the second pair is *larger* than the first pair

XGCD over $\mathbb{Q}[x]$

These polynomial pairs can be found from the extended Euclidean algorithm over rational polynomial rings

For two polynomials F, G (which we assume are coprime) it computes polynomials S, T with

$$F \cdot S + G \cdot T = 1$$

WLOG assuming that the leading coefficient of $F \cdot S$ is $1/C$ with $C > 0$

Then the following polynomial pairs

$$f(x) = C \cdot F(x) \cdot S(x), \text{ and}$$
$$g(x) = C - C \cdot G(x) \cdot T(x).$$

differ by C

XGCD over rational polynomial rings

Then the following polynomial pairs

$$f(x) = C \cdot F(x) \cdot S(x), \text{ and}$$
$$g(x) = C - C \cdot G(x) \cdot T(x).$$

differ by C

So we have to choose F, G such that S, T has small degree factors

Doing this over $\mathbb{Q}[x]$ is expensive but doing a *precomputation* over $\mathbb{Q}(a_1, \cdots, a_n)[x]$ makes the search faster

- Compute $S, T \in \mathbb{Q}(a_1, \cdots, a_n)[x]$ from $F, G \in \mathbb{Q}(a_1, \cdots, a_n)[x]$
- Exploit all potential factorisations of S and T over $\mathbb{Q}(a_1, \cdots, a_n)[x]$
- Evaluate the variables $a_1, \cdots, a_n$ to obtain polynomials over $\mathbb{Q}[x]$ and factorise each irreducible factor

Degree 8 polynomial pairs

$$f(x) = (x+1)(x+4)(x+9)(x+10)(x+15)(x+18)(x^2+19x-12), \text{ and}$$
$$g(x) = x^2(x+6)^2(x+13)^2(x+19)^2.$$

$$f(x) = (x+2)(x+9)(x+18)(x+24)(x+33)(x+40)(x^2+42x-55), \text{ and}$$
$$g(x) = x^2(x+13)^2(x+29)^2(x+42)^2.$$

$$f(x) = (x+1)(x+3)(x+4)(x+6)(x^2+7x-2)(x^2+7x+4), \text{ and}$$
$$g(x) = x^2(x+2)^2(x+5)^2(x+7)^2.$$

More degree 8 polynomial pairs

$$f(x) = x(x+7)(x^2+2x+5)(x^2+7x+20)(x^2+12x+40), \text{ and}$$
$$g(x) = (x+2)^4(x+5)^4.$$

$$f(x) = x(x+4)(x+7)^2(x+10)(x+14)(x^2+14x+9), \text{ and}$$
$$g(x) = (x+5)^2(x+9)^2(x^2+14x+4)^2.$$

$$f(x) = (x+20)^2(x+48)(x+63)(x+93)^2(x^2+111x-70), \text{ and}$$
$$g(x) = x(x+13)(x+35)^2(x+76)^2(x+98)(x+111).$$

Degree 10 polynomial pairs

$$f(x) = x(x+1)(x+3)(x+7)(x+9)(x+10)(3x^2+21x+16)$$
$$(3x^2+39x+106), \text{ and}$$
$$g(x) = (x+2)^2(x+5)^2(x+8)^2(3x^2+30x+7)^2.$$

$$f(x) = x(x+1)(x+3)(x+11)(x+13)(x+14)(x^2+11x+8)$$
$$(x^2+17x+80), \text{ and}$$
$$g(x) = (x+6)^2(x+7)^2(x+8)^2(x^2+14x+5)^2.$$

$$f(x) = (x+1)(x+4)(x+10)(x+12)(x+18)(x+21)(x^2+20x-9)$$
$$(x^2+24x+35), \text{ and}$$
$$g(x) = x^2(x+3)^2(x+11)^2(x+19)^2(x+22)^2.$$

Degree 12 polynomial pairs

$$f(x) = (x+1)(x+3)(x+7)(x+10)(x+33)(x+36)(x+40)(x+42)$$
$$(x^2+43x-24)(x^2+43x+396), \text{ and}$$
$$g(x) = x^2(x+12)^2(x+31)^2(x+43)^2(x^2+43x+186)^2.$$

$$f(x) = (x+4)(x+7)(x+22)(x+50)(x+56)(x+84)(x+99)(x+102)$$
$$(x^2+75x-136)(x^2+137x+3150), \text{ and}$$
$$g(x) = x^2(x+14)^2(x+39)^2(x+67)^2(x+92)^2(x+106)^2.$$

Searching for smooth twins using these pairs

To find smooth twins one searches for integers ℓ such that

Linear sieve: $\ell + a$ are all smooth

Evaluation: $f(\ell) = g(\ell) = 0 \mod C$

Post-processing: All evaluations of quadratic (or larger degree) factors are smooth

Much like in the PTE sieve, the first step uses a sieve of Eratothenes

Number of approaches to do the post-processing:

- Trial division or ECM
- Sieve of Eratothenes style approach
- Bernsteins algorithm

This work should hopefully be on eprint soon

Comparison of concrete primes

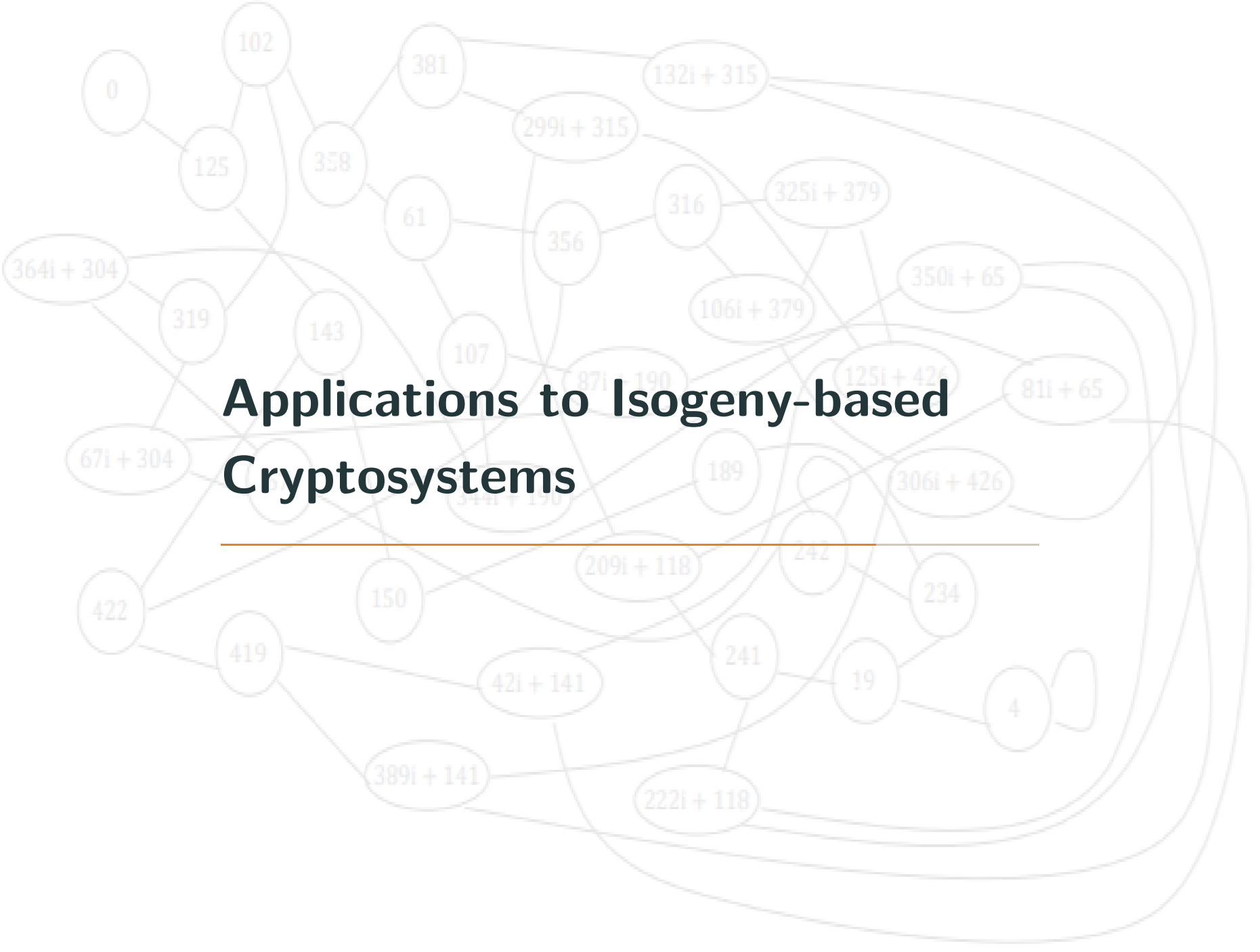
Method	$\log_2(B)$ of smallest smoothness bounds for b-bit primes p		
Constructive Methods	$b \approx 64$	$b \approx 128$	$b > 128$
Pell Equations	6.8	—	—
CHM	6.8	9.8	—
Probabilistic Methods	$b \approx 256$	$b = 384$	$b = 512$
XGCD over $\mathbb{Z}$	22.7	—	—
Cyclotomic factors	18.9	24.4	—
PTE sieve	15.0	21.9	27.9
XGCD over $\mathbb{Q}[x]$	15.4	20.2	24.3

Table 1: A comparison of the smoothness bounds of $p^2 - 1$ for primes p.

Remark: new ideal PTE solutions of size 4

a	b	c	d	e	a	b	c	d	e	a	b	c	d	e
17	5	35	27	32	6620	1940	13289	10985	11664	22572	6660	47545	35152	44217
86	26	221	125	216	6830	2210	53261	9261	53240	22715	6755	50759	34295	48384
171	51	391	256	375	7398	2250	20125	10648	19773	23579	7619	176039	32000	175959
243	75	775	343	768	7749	2289	16459	12000	15379	26010	8070	88501	36501	87880
524	164	2009	729	2000	8021	2561	43931	10976	43875	26672	8720	314465	35937	314432
594	174	1189	1000	1029	8987	2915	76055	12167	76032	28170	8790	103429	39304	102885
605	185	1739	864	1715	10269	3129	28459	14739	28000	29358	8610	59245	48013	52728
965	305	4331	1331	4320	11556	3756	105481	15625	105456	31160	9320	72929	46305	70304
1463	455	5135	2048	5103	12015	3855	73759	16384	73695	31437	10185	255595	42592	255507
1602	510	8245	2197	8232	12386	3806	37541	17576	37125	31841	10421	396611	42875	396576
1790	530	3869	2744	3645	13076	3836	26441	21296	23625	33561	10461	121411	46875	120736
2471	791	14351	3375	14336	14472	4440	43105	20577	42592	33885	9945	68731	54880	61731
2628	780	5785	3993	5488	14573	4745	142715	19683	142688	34047	10335	90895	49152	89167
2889	909	12019	4000	11979	15930	4710	34069	24565	31944	35684	10604	79289	54000	75449
3608	1160	23345	4913	23328	17153	5525	116675	23328	116603	37638	12330	493885	50653	493848
3735	1095	7519	6144	6655	18074	5894	189029	24389	189000	39542	12410	158045	54872	157437
3962	1190	9605	5832	9317	19214	5954	64349	27000	63869	40871	13271	359471	55296	359375
4455	1335	10591	6591	10240	20195	5915	40391	34391	34560	41445	12465	101659	60835	98784
5027	1595	24215	6912	24167	22095	7215	245791	29791	245760	44099	14459	608039	59319	608000
5049	1629	36019	6859	36000	22473	6765	55555	32928	54043					

Table 2: List of all inequivalent and normalised sized 4 ideal PTE solutions of the form $[0, a, a, c] =_3 [b, b, d, e]$ with $0 < b < a < 50000$ and $c, d, e > 0$.



Applications to Isogeny-based Cryptosystems

Isogeny-based Cryptosystems

B-SIDH: (broken) Prime p such that

$$M \mid p-1 \text{ and } N \mid p+1 \text{ are large smooth cofactors}$$

with $M \approx N$. Similar requirements can be made for B-SIDH variants of SIDH countermeasures

SQISign: Prime p such that

$$2^f T \mid p^2 - 1 \text{ is } B\text{-smooth cofactor}$$

with $T \approx p^{5/4+\epsilon}$ and f is large

Sèta: (broken) Prime p such that

$$p^2 - 1 = D \cdot N \text{ is smooth}$$

with $D \approx 2^\lambda$ has small number of prime factors and $N \approx 2^{2\lambda}$

Parameters found by combining techniques

One can find parameters by combining constructive and probabilistic methods

As part of the CHM collaboration with Bruno et. al. (2022) we used CHM twins $(r, r \pm 1)$ and $p_n(x) := 2x^n - 1$ to find SQISign parameters

$$4x^n(x-1) \mid p_n^2(x) - 1 \quad \text{for all } n, \qquad \text{and}$$
$$4x^n(x-1)(x+1) \mid p_n^2(x) - 1 \quad \text{when } n \text{ is even}$$

The amount of *guaranteed smoothness* in $p^2 - 1$ is $\approx p^{1+1/n}$

This can be generalised to polynomials $p_{i,j}$ where

$$x^i(x+1)^j \mid p_{i,j}^2(x) - 1, \quad \text{with } i, j \geq 2, i \neq j \text{ and } \deg(p_{i,j}) < i + j$$

These can be found by doing XGCD with $F(x) = x^i$ and $G(x) = (x+1)^j$

Protocol Specific Polynomials

A common feature is exploiting the large power of x in the polynomial pair $(x^n - 1, x^n)$

Using XGCD over rational polynomials one can find other examples that have large powers of x

$$f(x) = (x-1)(x+2)^2(x^3+3x^2+4), \text{ and}$$
$$g(x) = x^4(x+3)^2.$$

$$f(x) = (x+3)^2(x^2-2x+3)(x^4+4x^3-27), \text{ and}$$
$$g(x) = x^6(x+4)^2.$$

This formalisation is still work-in-progress

Weird degree 8 pairs

The polynomial pair $(x^8 - 1, x^8)$ factorise as

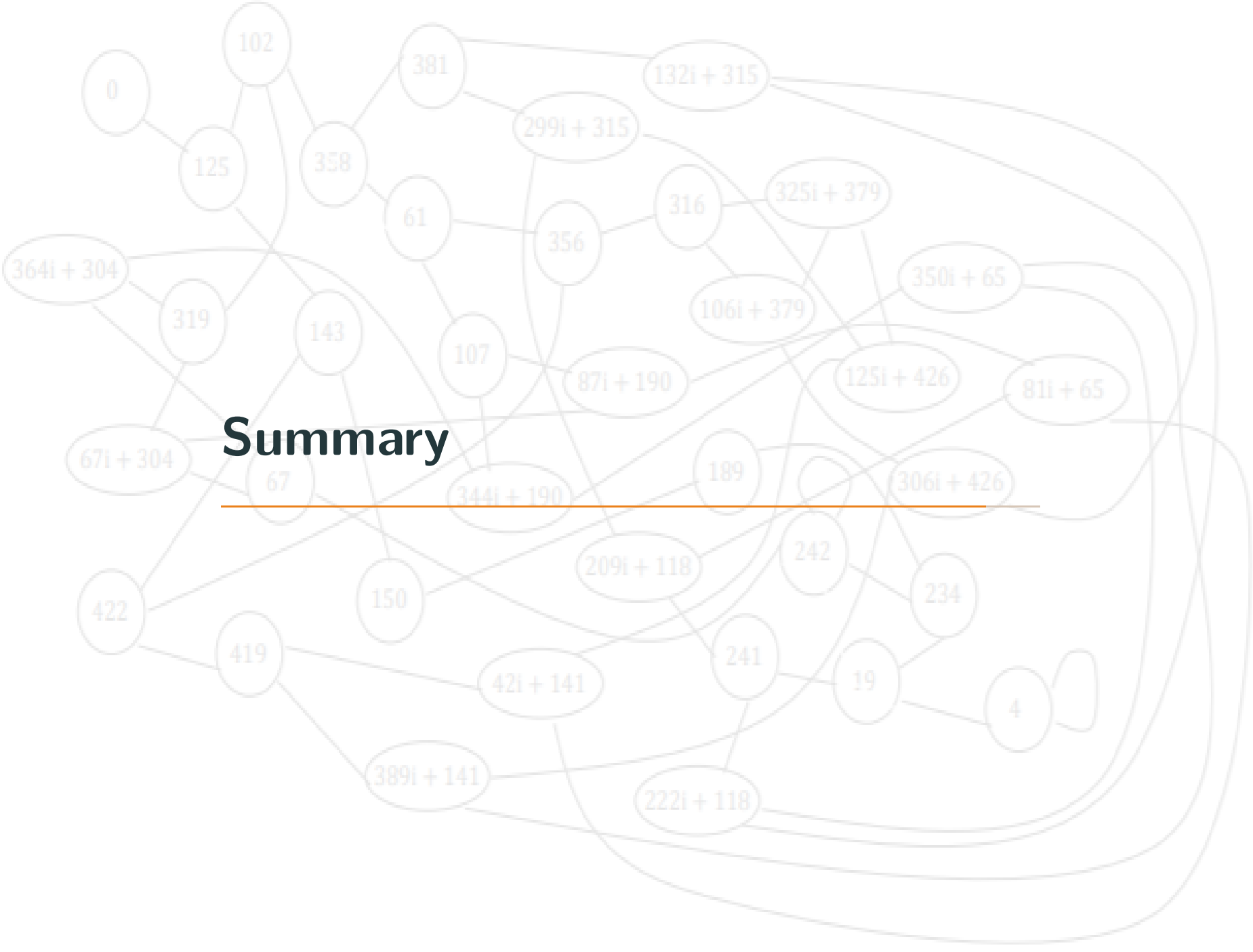
$$x^8 - 1 = (x - 1)(x + 1)(x^2 + 1)(x^4 + 1)$$

Among all polynomial pairs $(ax^n - 1, ax^n)$, with a scaling factor a, one would expect $ax^n - 1$ not to factorise as nicely

Unexpectedly, the polynomial pair $(16x^8 - 1, 16x^8)$ factorise as

$$16x^8 - 1 = (2x^2 - 2x + 1)(2x^2 - 1)(2x^2 + 1)(2x^2 + 2x + 1)$$

This is an extreme special case and no other instance factorise nicely like this


102
0
381
132i + 315
299i + 315
125
358
61
316
325i + 379
356
364i + 304
350i + 65
106i + 379
319
143
107
87i + 190
125i + 426
81i + 65
67i + 304
67
189
306i + 426
344i + 190
242
209i + 118
422
150
234
419
241
42i + 141
19
4
389i + 141
222i + 118

Summary

Smooth sandwiches galore



Photo credit: Anaëlle Le Devehat

Summary

Lots of methods have been presented to find smooth twins and primes p with $p^2 - 1$ being smooth

Up to 128-bits, instances have been found with an optimally small smoothness bound found from the constructive methods (Pell equations, CHM)

For cryptographic-sized instances that have been found from the probabilistic methods the smoothness bound is not optimally small (PTE, XGCD over $\mathbb{Q}[x]$)

Open questions:

- Can we find cryptographic-sized instances that is either optimally small or close to it?
- Further apply these techniques to either existing or new protocols

Thanks for listening
Questions?

My contributions:
ia.cr/2022/1439
ia.cr/2023/TBC