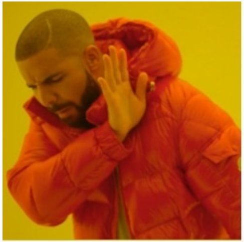
Towards Optimally Small Smoothness Bounds for Cryptographic-Sized Smooth Twins and their Isogeny-based Applications

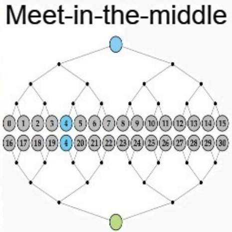
Bruno Sterner

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

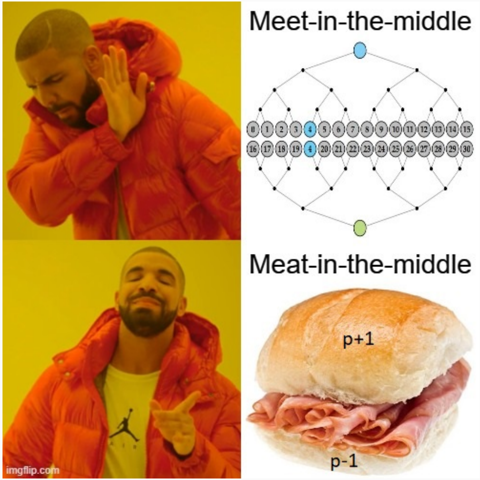
Talk at SAC 2024

Meet-in-the-Middle





Meat-in-the-Middle



Motivation: "smooth sandwiches"

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

~~B-SIDH~~

$$\phi : E \to E'$$
$$\#E(\mathbb{F}_{p^2}) = (p-1)^2, (p+1)^2$$

SQIsign

Example: The SQIsign NIST submission use the following 254-bit prime

$p = \texttt{0x34E29E286B95D98C33A6A86587407437252C9E49355147FFFFFFFFFFFFFFFF}$:

$$p + 1 = 2^{75} \cdot 3^{36} \cdot 23^2 \cdot 59^2 \cdot 101^2 \cdot 109^2 \cdot 197^2 \cdot 491^2 \cdot 743^2 \cdot 1913^2, \text{ and}$$
$$p - 1 = 2 \cdot 7^4 \cdot 11 \cdot 13 \cdot 37 \cdot 89 \cdot 97 \cdot 107 \cdot 131 \cdot 137 \cdot 223 \cdot 239 \cdot 383 \cdot 389 \cdot 499 \cdot 607 \cdot 1033 \cdot 1049$$
$$\cdot 1193 \cdot 1973 \cdot 32587069 \cdot 275446333 \cdot 1031359276391767$$

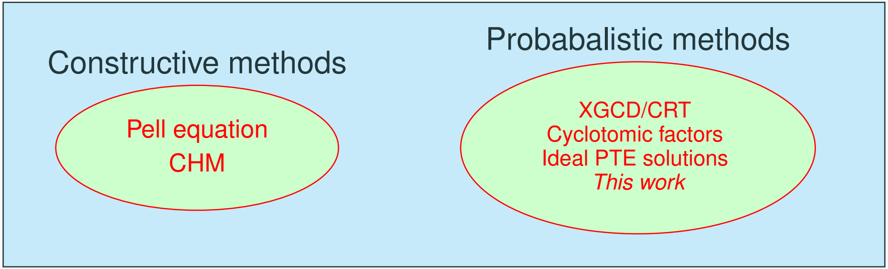
[1] A number n is B-smooth if all prime factors of n are at most B

Smooth twins

Smooth twin: Consecutive smooth integers (e.g. $(r, r+1) = (4374, 4375) = (2 \cdot 3^7, 5^4 \cdot 7)$)

$(r, r+1)$ smooth twin and $p = 2r + 1$ prime $\rightsquigarrow$ $p^2 - 1 = 4r(r+1)$ smooth sandwich

Known algorithms: This is the landscape for finding smooth twins



Overview – evolution of probabilistic methods

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

Slightly better approach: Force coprime smooth factors into r and $r+1$:

$$a \mid r \text{ and } b \mid r+1, \text{ with } a \cdot b \approx r$$

Use the *extended Euclidean algorithm (XGCD)*: solve a Bézout equation $as + bt = 1$ and get a smooth twin $(r, r+1) = (|as|, |bt|)$ when s, t are smooth

Even better approach: Combine many small and smooth integers to get a smooth twin

In this talk we find smooth twins of the following form

$$(r, r+1) = \left(\frac{(\ell+1)(\ell+4)(\ell+9)(\ell+10)(\ell+15)(\ell+18)(\ell^2+19\ell-12)}{1166400}, \left(\frac{\ell(\ell+6)(\ell+13)(\ell+19)}{1080} \right)^2 \right)$$

Probabalistic approaches

Using polynomials to find smooth twins

Cyclotomic factors: Search for twins of the form $(r, r+1) = (\ell^n - 1, \ell^n)$ exploiting the cyclotomic factors of the polynomial $x^n - 1$

The larger degree cyclotomic factors dominate the smoothness probability ✗

PTE solutions: Find polynomials $f, g \in \mathbb{Z}[x]$ that split completely into linear factors and $g - f \equiv C \in \mathbb{Z}$ – getting twins of the form

$$(r, r+1) = \left(\frac{f(\ell)}{C}, \frac{g(\ell)}{C}\right)$$

This increases the smoothness probability compared to the cyclotomic factors ✓

Such polynomials f, g can be found using solutions to the ideal Prouhet-Tarry-Escott (PTE) problem as done by Costello, Meyer and Naehrig (2021)

XGCD generalisation

XGCD over k$[x]$**:** For coprime $F, G \in$ k$[x]$ solve the polynomial Bézout equation:

$$F \cdot S + G \cdot T \equiv 1, \quad \deg(S) < \deg(G) \quad \text{and} \quad \deg(T) < \deg(F)$$

General smooth twin strategy: $-F \cdot S$ and $G \cdot T$ differ[2] by 1 and gives a general platform to find smooth twins – but working with k = $\mathbb{Q}$ (and not k = $\mathbb{Z}$!)

Set $f(x) := -C \cdot F(x) \cdot S(x)$ and $g(x) := C \cdot G(x) \cdot T(x) \in \mathbb{Z}[x]$; and search for $\ell \in \mathbb{Z}$ such that

Smoothness: $P(\ell)$ is smooth for all irreducible $P \mid f \cdot g$

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

Combine this to get a smooth twin

$$(r, r+1) = \left(\frac{f(\ell)}{C}, \frac{g(\ell)}{C}\right)$$

Example: cyclotomic factors

$$F(x) = x - 1 \text{ and } G(x) = x^n \quad \rightsquigarrow \quad (f(x), g(x)) = (x^n - 1, x^n)$$

[2] Assume WLOG that the leading coefficient of these polynomials is positive

Do we have too many linear factors?

Yes, when $\deg(f) > 6$ we can tradeoff the number of linear and quadratic 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

Probabilities: For a fixed smoothness bound, the probability of finding smooth twins with the second pair is expected to be *much larger* than with the first pair

Search for new polynomials

Search strategies using XGCD over k[x]

Natural strategy: Iterate over many polynomials $F, G \in \mathbb{Z}[x]$ (ensuring coprimality)

- ➢ Compute $f, g \in \mathbb{Z}[x]$ (as before) and save the (f, g) that give good smoothness probabilities

However, doing many XGCD's of this type becomes *expensive* ✗

Better strategy: Do an XGCD precomputation over $\mathbb{Q}(a_1, \cdots, a_n)[x]$

- ➢ Use XGCD to compute $S, T \in \mathbb{Q}(a_1, \cdots, a_n)[x]$ and factorise them over $\mathbb{Q}(a_1, \cdots, a_n)[x]$;
- ➢ Evaluate each irreducible factor of $S \cdot T$ at the variables $a_1, \cdots, a_n$ at rationals;
- ➢ Factorise each of these polynomials over $\mathbb{Q}[x]$ and save the desired pairs

Gives a fine-grained searching criterion and is much faster than the natural strategy ✓

Additional trick: Search using *even polynomials*, i.e. $F(x) = \hat{F}(x^2)$ and $G(x) = \hat{G}(x^2)$

Degree 8 search

XGCD precomputation: Apply XGCD to $F(x) = x^2 - c^2$ and $G(x) = \left(x^2 - a^2\right)^2 \left(x^2 - b^2\right)^2$

$$S(x) = -\frac{1}{C}\left(x^2 - (a^2 + b^2 - c^2)\right)\left(x^4 - (a^2 + b^2)x^2 + a^2b^2 + (a^2 - c^2)(b^2 - c^2)\right) \quad \& \quad T(x) = \frac{1}{C}$$

where $C = \left((a^2 - c^2)(b^2 - c^2)\right)^2$

Variable evaluation: Iterate over many $a, b, c \in \mathbb{Q}$ (with $a \neq c$ and $b \neq c$) and see when this quadratic and quartic factorises over $\mathbb{Q}[x]$: e.g. $a = 19/2$, $b = 7/2$ and $c = 1/2$ gives[3]

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

with $C = 1166400$

Remark: This search can be modified to reduce the quartic to a product of two quadratics

[3] After applying the linear shift $x \mapsto x + 19/2$

More pairs found from our experiments

Degree 8:

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

We also searched and found many pairs of larger degree

Degree 10:

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

Degree 12:

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

Concrete smooth twin and sandwich

Sieving using these new pairs

Smoothness step: Split up into two components:

Linear sieve: Use the *sieve of Eratothenes* to identify integers ℓ such that $\ell + a$ are all smooth

e.g. want $\ell, \ell+1, \ell+4, \ell+6, \ell+9, \ell+10, \ell+13, \ell+15, \ell+18, \ell+19$ to be smooth

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

e.g. want $\ell^2 + 19\ell - 12$ to be smooth

Evaluation Step: Checking $f(\ell) = g(\ell) = 0 \mod C$ is done before the post-processing

For this polynomial pair, combining everything gets a smooth twin:

$$(r, r+1) = \left(\frac{(\ell+1)(\ell+4)(\ell+9)(\ell+10)(\ell+15)(\ell+18)(\ell^2+19\ell-12)}{1166400}, \left(\frac{\ell(\ell+6)(\ell+13)(\ell+19)}{1080} \right)^2 \right)$$

Concrete example

Smooth twin: For $\ell = 38295031104$ we have

- $(\ell + a)$'s are all 2^{16}-smooth
- $f(\ell) = g(\ell) = 0 \mod C$
- $\ell^2 + 19\ell - 12$ is 2^{16}-smooth

So combining everything gets a smooth twin $(r, r+1)$

Smooth sandwich: Additionally its sum $p = 2r + 1$ is prime

$p = \texttt{0x447E146069CE1FE610C2F26594ACE5D1973631564A13C01C3C26A126EA258F41FF}$:

$$p + 1 = 2^9 \cdot 7^4 \cdot 11^2 \cdot 31^2 \cdot 37^2 \cdot 43^2 \cdot 241^2 \cdot 617^2 \cdot 809^2 \cdot 1811^2 \cdot 2753^2 \cdot 4283^2 \cdot 5573^2 \cdot 7681^2 \cdot 42577^2$$

$$p - 1 = 2 \cdot 3^2 \cdot 17^2 \cdot 23 \cdot 41 \cdot 71 \cdot 139 \cdot 307 \cdot 397 \cdot 457 \cdot 907 \cdot 971 \cdot 2213 \cdot 2677 \cdot 2801 \cdot 3089 \cdot 3943 \cdot 5923 \cdot 6151 \cdot 8737 \cdot 9679 \cdot 9839 \cdot 21701 \cdot 25439 \cdot 25693 \cdot 38431$$

Results & comparison

Method	$\log_2(B)$ of smallest smoothness bounds for b-bit smooth sandwiches		
	$b \approx 256$	$b \approx 384$	$b = 512$
XGCD over $\mathbb{Z}$	22.7	—	—
Cyclotomic factors	18.9	24.4	—
PTE sieve	15.0	20.6	27.9
XGCD over $\mathbb{Q}[x]$	**15.4**	**19.7**	**24.3**

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

Final remarks

Cryptographic impact

Question: How relevant is this in the context of current isogeny-based cryptography?

Answer: Extremely irrelevant! **:(** — In isogeny-based applications extra conditions on the factorisation of $p^2 - 1$ are needed

Example: SQIsign requirements

$$p^2 - 1 = 2^f \cdot T \cdot R, \qquad f \text{ is large, } T \approx p^{5/4} \text{ is smooth and } R \text{ need not be smooth}$$

The polynomials found in this work are not suited to this due to the large power of two

Summary

***Smoother* smooth sandwiches:** We reduce the smoothness bound of $p^2 - 1$ for large primes p using new polynomial pairs – found using XGCD over k[x]

Future work/open questions: Explore more constructive applications:

- Signing with isogeny skies (SQIsign)
- B-SIDH variants of SIDH countermeasures
- High dimensional (HD) applications

Also answer questions at the mathematical level

- Resolve conjectures made in the paper
- Optimal smooth twins

Thanks for listening
Questions?

ia.cr/2023/1576