Efficient and Cryptographically Secure Addition in the Ideal Class Groups of Hyperelliptic Curves

Diploma thesis

Andrey Bogdanov*

Scientific advisors: Prof. Dr. Dr. h.c. Gerhard Frey

Prof. Dr. Vladimir Anashin

Russian State University for the Humanities

Faculty of Information Security

---

*Supported by the Institute for Experimental Mathematics, University of Duisburg-Essen, Germany

Motivation

- A careful study of genus 2 hyperelliptic curve based cryptography;
- A proper analyse of its suitability for real-world applications;
- Efficiency estimates known and improvements;
- Vulnerability against simple side-channel attacks (SCA) — no generic algorithmic solution for the time being;
- The SCA question is especially topical for characteristic 2!

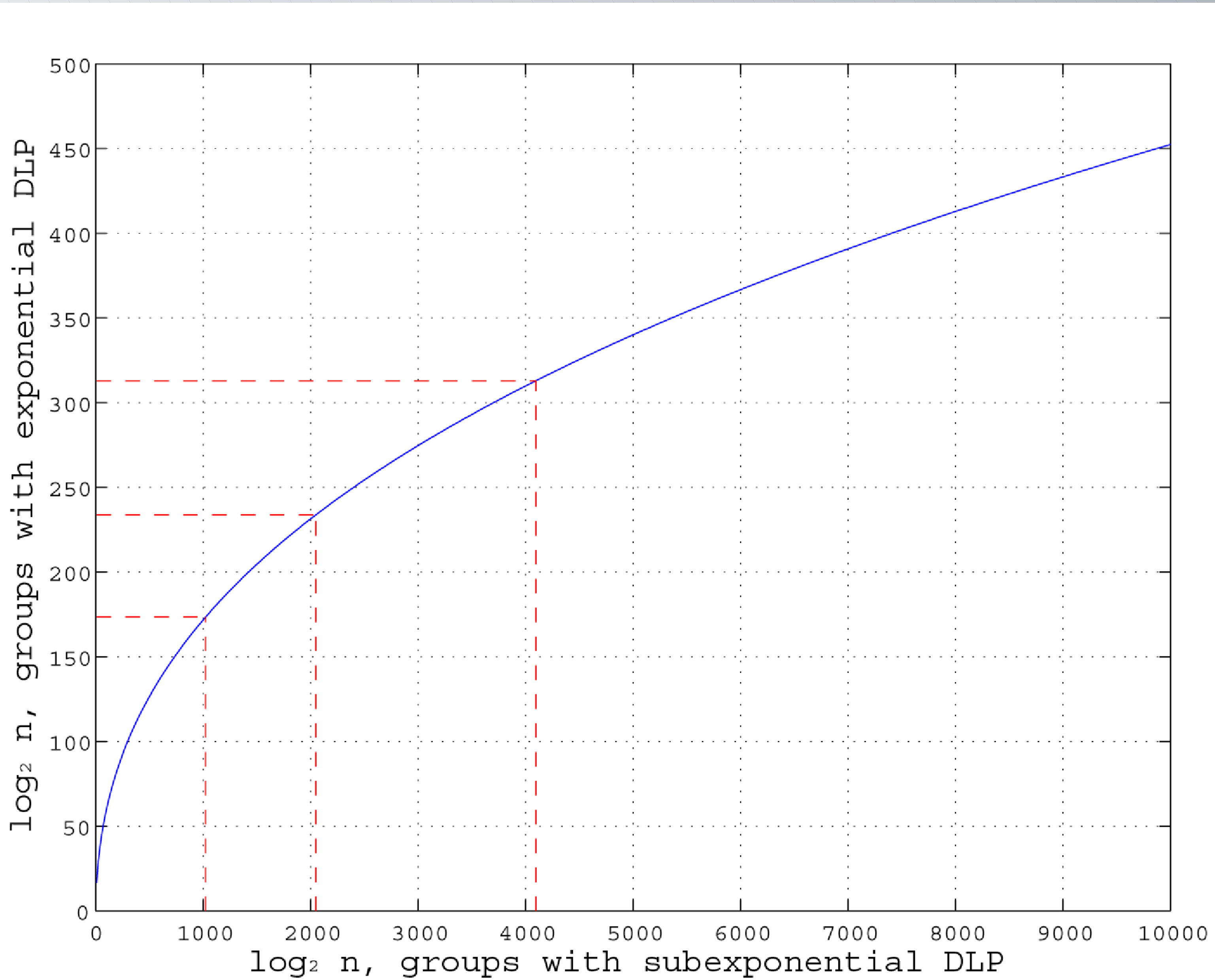
Groups Suitable for Cryptography

For G one should have simultaneously:

- Exponential complexity of the DLP for prime group order $n = |G|$;
- Efficient representation: constructive + bit length $O(\log_2 |G|)$;
- Efficiently performable group law in G.

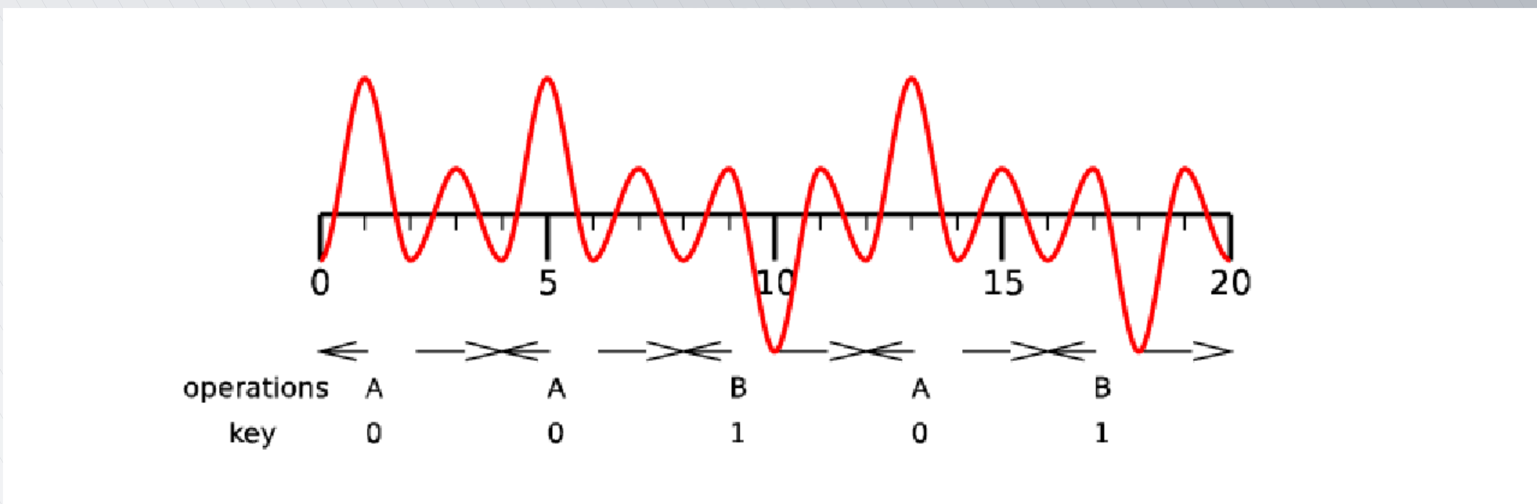
Degree 0 Picard groups Pic$^0_{\mathbb{F}_q}(C)$ of low genus hyperelliptic curves C fulfill the requirements perfectly!

Subexponential and exponential DLP



Simple Side-Channel Attacks

- Simple power attack — a single power profile;
- If key bits and operation flow are tightly connected;



- **Standard scalar multiplication vulnerable!**

R1: Correct Addition $\mathrm{Pic}^0_{\mathbb{F}_q}(C)$

- Publicly accepted formulae contained some relatively hidden but important errors;
- The errors have been found and corrected;
- The new formulae have been tested by numerous examples.

R2: Compression in $\mathrm{Pic}^0_{\mathbb{F}_{2^d}}(C)$

For genus 2 hyperelliptic curves over binary finite fields GF(2^d) of odd extension degree d:

- An efficient variant of a point decompression technique has been proposed;
- The complexity of our technique is:
  I+10M+(d+2)S,
  where:
  - I = field inversion,
  - M = field multiplication,
  - S = field squaring.

R3: Montgomery representation,1

For genus 2 hyperelliptic curves over arbitrary finite fields:

- Though publicly believed, group doubling in $\mathrm{Pic}^0_{\mathbb{F}_q}(C)$ **cannot** be solely parameterized by the u-coordinate in the Mumford representation;
- Cantor's division polynomials deliver **no proof** of this for degree 2 divisors;
- Some **additional** information needed.

R3: Montgomery representation,2

For genus 2 hyperelliptic curves over arbitrary finite fields:

- One should search for an effective invertible map φ : $\mathrm{Pic}^0_{\mathbb{F}_q}(C) \to \mathbb{K}$ to the related **Kummer surface** $\mathbb{K}$ — a quartic surface in $\mathbb{P}^3$ with $\varphi(D_1) = \varphi(-D_1)$, $D_1 \in \mathrm{Pic}^0_{\mathbb{F}_q}(C)$
- No group structure (but doubling possible);
- On the basis of $\varphi(D_1), \varphi(D_2), \varphi(D_1 - D_2)$ it is possible to construct explicit formulae for $\varphi(D_1 + D_2)$, $D_1, D_2 \in \mathrm{Pic}^0_{\mathbb{F}_q}(C)$

Conclusion

For genus 2 hyperelliptic curves over finite fields:

- Addition and doubling formulae corrected for $\mathrm{Pic}^0_{\mathbb{F}_q}(C)$;
- Complexity of point decompression improved;
- Framework for getting SCA-resistant Montgomery-like arithmetic provided.

Motivation

- Careful study of genus 2 hyperelliptic curve based cryptography;
- Efficiency estimates and improvements;
- Resistance against simple side-channel attacks — no optimal solution for the time being, especially for even characteristic.

Groups Suitable for Cryptography

For G one should have simultaneously:

- Exponential complexity of the DLP for prime group order $n = |G|$;
- Efficient representation: constructive + bit length $O(\log_2 |G|)$;
- Efficiently performable group law in G.

Degree 0 Picard groups Pic$^0_{\mathbb{F}_q}(C)$ of low genus hyperelliptic curves C fulfill the requirements perfectly!

Hyperelliptic curves

We take a middle-brow approach and deal directly with imaginary quadratic hyperelliptic curves curves.

- An imaginary quadratic hyperelliptic curve C of genus $g \geq 1$ over $\mathbb{F}_q$ is defined by:

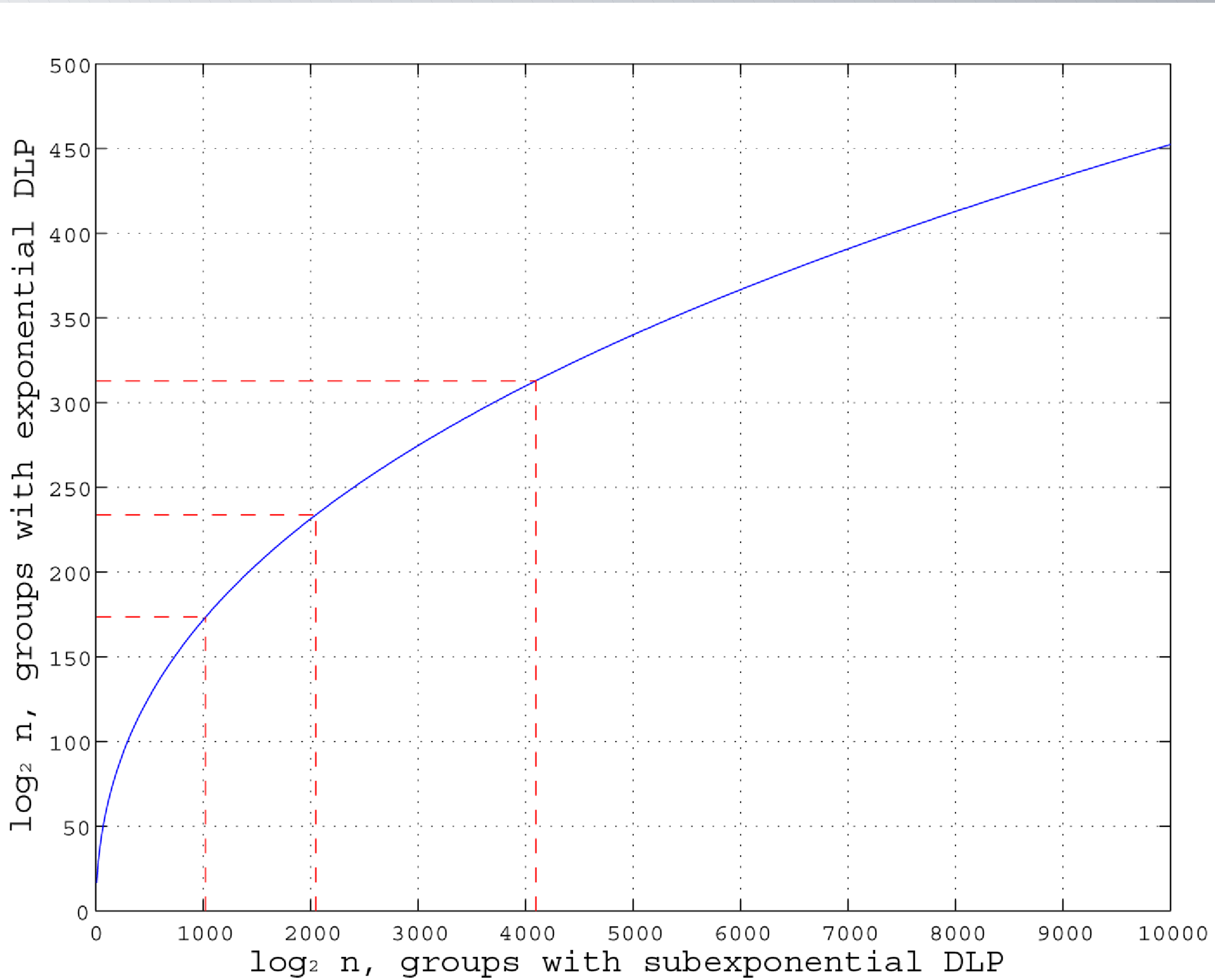
$$C : y^2 + h(x) = f(x) \in \mathbb{F}_q[x, y], \text{ where}$$

  - $h(x) \in \mathbb{F}_q[x]$ with $\deg(h) \leq g$;
  - $f(x) \in \mathbb{F}_q[x]$ is monic with $\deg(f) = 2g + 1$.
- By definition there is (at least) one Weierstraß point $P_\infty \notin \mathbb{A}^2(\overline{\mathbb{F}}_q)$, but $P_\infty \in \mathbb{P}^2(\mathbb{F}_q)$.

Ideal class group

- For a non-singular curve C $M \subset K(C)$ is a fractional $K[C]$-ideal, if $\exists f \in K(C)^* : f$M is an ideal of $K[C]$. $M \subset K(C)$ is an invertible ideal, if there exists $N \subset K(C)$: $NM = K[C]$.
- $K[C]$ is a Dedekind domain $\Leftrightarrow$ every fractional $K[C]$-ideal is invertible.
- The non-zero fractional $K[C]$-ideals form a group I with respect ideal multiplication.
- $f \in K(C)$ defines a fractional $K[C]$-ideal (f) — a *principle fractional ideal*, the set of f forms a subgroup $P \triangleleft I$.
- $H_{K(C)} = I/P$ — *ideal class group*.

Subexponential and exponential DLP



Mumford representation

For a genus g hyperelliptic curve C one has the following group isomorphism:

- $\mathrm{Pic}^0_{\mathbb{F}_q}(C) \cong H_{\mathbb{F}_q(C)}$,
  where $H_{\mathbb{F}_q(C)}$ is the ideal class group of C.

$\forall$ non-trivial $I \in H_{\mathbb{F}_q(C)}$ can be represented via a unique ideal $J \subset \mathbb{F}_q[C]$ generated by 2 polynomials:

- $J =< a(x), y - b(x) >$, $a(x), b(x) \in \mathbb{F}_q[x]$;
- a monic;
- $\deg b < \deg a \leq g$;
- $a | b^2 + bh - f$.

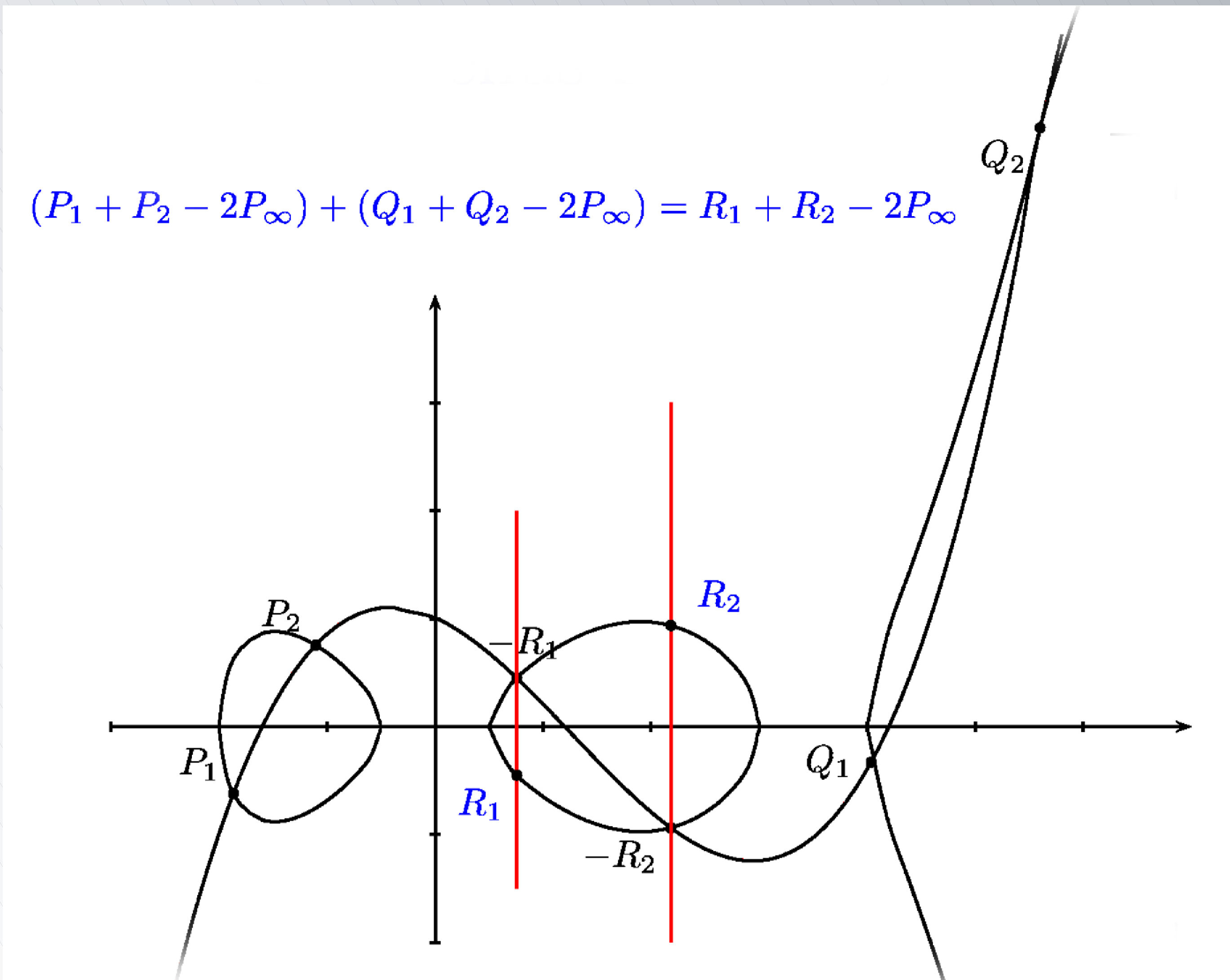
Picard group cardinality

For a genus g hyperelliptic curve C the following bounds on the cardinality of $\mathrm{Pic}^0_{\mathbb{F}_q}(C)$ exist:

- $(q^{1/2}-1)^{2g} \leq |\,\mathrm{Pic}^0_{\mathbb{F}_q}(C)| \leq (q^{1/2}+1)^{2g}$,
- or $|\,\mathrm{Pic}^0_{\mathbb{F}_q}(C)| \approx q^g$.

Cantor's addition algorithm

Example over the reals $\mathbb{R}$:



Explicit group law complexity, 1

Addition in $\mathrm{Pic}^0_{\mathbb{F}_q}(C)$, $g = 2$, q odd

Operation	Costs
$\mathcal{N} + \mathcal{N} = \mathcal{N}$	47M+7S
$\mathcal{P} + \mathcal{P} = \mathcal{P}$	47M+4S
$\mathcal{A} + \mathcal{A} = \mathcal{A}$	I+22M+3S

Doubling in $\mathrm{Pic}^0_{\mathbb{F}_q}(C)$, $g = 2$, q odd

Operation	Costs
$2\mathcal{P} = \mathcal{P}$	38M+6S
$2\mathcal{N} = \mathcal{N}$	34M+7S
$2\mathcal{A} = \mathcal{A}$	I+22M+5S

Explicit group law complexity, 2 ..

Addition in $\mathrm{Pic}^0_{\mathbb{F}_{2^d}}(C)$, $g = 2$, q even, d odd

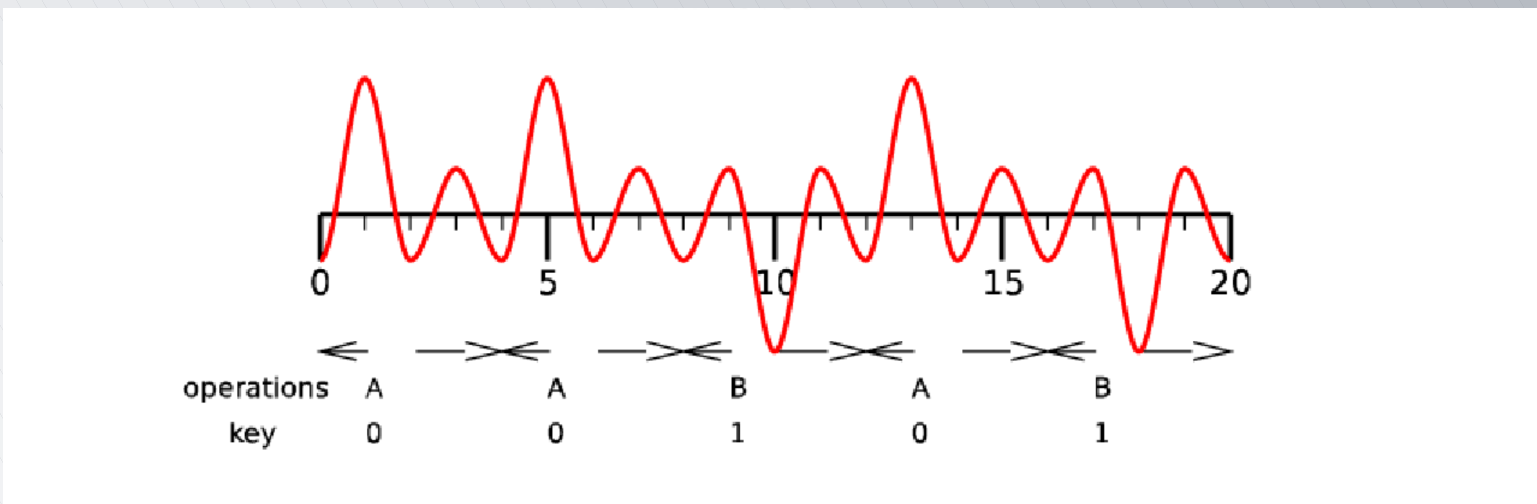
Operation	Costs
$\mathcal{R} + \mathcal{R} = \mathcal{R}$	49M+8S
$\mathcal{A} + \mathcal{A} = \mathcal{A}$	I+21M+3S

Doubling in $\mathrm{Pic}^0_{\mathbb{F}_{2^d}}(C)$, $g = 2$, q even, d odd

Operation	Costs
$2\mathcal{P} = \mathcal{P}$	22M+6S
$2\mathcal{R} = \mathcal{R}$	20M+8S
$2\mathcal{A} = \mathcal{A}$	I+5M+6S

Simple Side-Channel Attacks

- Simple power attack — a single power profile;
- If key bits and operation flow are tightly connected;



- **Standard scalar multiplication vulnerable!**

Montgomery Ladder, 1

- A simple method to homogenize group scalar multiplication:

INPUT: $\alpha \in G$, $k = (k_{l-1} \ldots k_0)_2 \in \{1, 2, \ldots, n-1\}$

---

1. $\beta_0 \leftarrow 1$, $\beta_1 \leftarrow \alpha$
2. for j from $l-1$ downto 0 do

   if $k_j = 0$ then $\beta_1 \leftarrow \beta_1 + \beta_0$, $\beta_0 \leftarrow 2\beta_0$

   else [if $k_j = 1$] $\beta_0 \leftarrow \beta_1 + \beta_0$, $\beta_1 \leftarrow 2\beta_1$

OUTPUT: $\beta_0 = k\alpha$

Montgomery Ladder, 2

- For the scalar multiplier k define:

$$L_j = \sum_{i=j}^{l-1} k_i 2^{i-j} \text{ and } H_j = L_j + 1.$$

- Fact 1:

$$\begin{aligned}
&(1)\ L_j = 2L_{j+1} + k_j,\\
&(2)\ L_j = L_{j+1} + H_{j+1} + k_j - 1,\\
&(3)\ L_j = 2H_{j+1} + k_j - 2.
\end{aligned}$$

- Fact 2:

$$(L_j g, H_j g) = \begin{cases} ((2L_{j+1})g, (L_{j+1} + H_{j+1})g), k_j = 0, \\ ((L_{j+1} + H_{j+1})g, (2H_{j+1})g), k_j = 1. \end{cases}$$

Montgomery Ladder, 3

Useful observations:

- $\beta_1 - \beta_0 = \alpha = const$ throughout the algorithm, this can be used in some groups to speed-up addition;
- At each iteration the operations (D and A) are independent and can be performed in parallel;
- At each iteration, the operations (D and A) share a common operand which can be of advantage too.

The Montgomery arithmetic can really be very efficient. For instance, elliptic curves!

R1: Correct Addition $\mathrm{Pic}^0_{\mathbb{F}_q}(C)$

- Publicly accepted formulae contained some relatively hidden but important errors;
- The errors have been found and corrected;
- The new formulae have been tested by numerous examples.

R2: Compression in $\mathrm{Pic}^0_{\mathbb{F}_{2^d}}(C)$

For genus 2 hyperelliptic curves over binary finite fields GF(2^d) of odd extension degree d:

- An efficient variant of a point decompression technique has been proposed;
- The complexity of our technique is:
  I+10M+(d+2)S,
  where:
  - I = field inversion,
  - M = field multiplication,
  - S = field squaring.

R3: Montgomery representation,1

For genus 2 hyperelliptic curves over arbitrary finite fields:

- Though publicly believed, group doubling in $\mathrm{Pic}^0_{\mathbb{F}_q}(C)$ **cannot** be solely parameterized by the u-coordinate in the Mumford representation;
- Cantor's division polynomials deliver no proof of this for degree 2 divisors;
- Some additional information needed.

R3: Montgomery representation,2

For genus 2 hyperelliptic curves over arbitrary finite fields:

- One should search for an effective invertible map $\varphi : \mathrm{Pic}^0_{\mathbb{F}_q}(C) \to \mathbb{K}$ to the related Kummer surface $\mathbb{K}$ — a quartic surface in $\mathbb{P}^3$ with $\varphi(D_1) = \varphi(-D_1)$, $D_1 \in \mathrm{Pic}^0_{\mathbb{F}_q}(C)$
- No group structure (but doubling possible);
- On the basis of $\varphi(D_1), \varphi(D_2), \varphi(D_1 - D_2)$ it is possible to construct explicit formulae for $\varphi(D_1 + D_2)$, $D_1, D_2 \in \mathrm{Pic}^0_{\mathbb{F}_q}(C)$

Conclusion

For genus 2 hyperelliptic curves over finite fields:

- Addition and doubling formulae corrected for $\mathrm{Pic}^0_{\mathbb{F}_q}(C)$;
- Complexity of point decompression improved;
- Framework for getting SCA-resistant Montgomery-like arithmetic provided.