SPA resistant Exponentiation based on Brun's GCD algorithm

Valérie **Berthé**, Thomas **Plantard**

Paris Diderot Université, University of Wollongong

http://www.uow.edu.au/~thomaspl
thomaspl@uow.edu.au

2019

Introduction

Introduction

Exponentiation

Exponentiation

- RSA: in $(\mathbb{Z}/(N\mathbb{Z}))^*$, compute $g^e \mod N$ using Modular Multiplication and Squaring.
- ECC: on a group, compute kP using $2P$ and $P+Q$.

Exponentiation

Exponentiation

- RSA: in $(\mathbb{Z}/(N\mathbb{Z}))^*$, compute $g^e \mod N$ using Modular Multiplication and Squaring.
- ECC: on a group, compute kP using $2P$ and $P + Q$.

Generic Algorithm

- Right To Left
- Left To Right
- Radix-R exponentiation
- Radix-R exponentiation with Odd Coefficient
- Sliding Window
- Montgomery Ladder

Specific Group

For $(\mathbb{Z}/N\mathbb{Z})$

- Multiply Always
- Square Always
- Square And Multiply Always: 1 replace by $N + 1$
- Exponentiation using multiplicative half-size splitting
- Montgomery Ladder with Common Operand Multiplication

Specific Group

For $(\mathbb{Z}/N\mathbb{Z})$

- Multiply Always
- Square Always
- Square And Multiply Always: 1 replace by $N+1$
- Exponentiation using multiplicative half-size splitting
- Montgomery Ladder with Common Operand Multiplication

For ECC

- NAF Exponentiation: using $-P$
- Addition Chain Exponentiation: No Doubling
- Double Base: exponent in base $2^a 3^b$

Specific Case

Exponentiation with g constant

- Radix-R exponentiation: exponent in base $R = 2^t$
- NAF Representation
- Comb Method
- RNS Digit Exponent: exponent represented in base $m_0 m_1$

Specific Case

Exponentiation with g constant

- Radix-R exponentiation: exponent in base $R = 2^t$
- NAF Representation
- Comb Method
- RNS Digit Exponent: exponent represented in base $m_0 m_1$

Exponentiation with e random

- Addition Chain
- Double Base

In this Work

Exponentiation

- Generic Group
- SPA Protection
- g variable
- e given

In this Work

Exponentiation

- Generic Group
- SPA Protection
- g variable
- e given

Current Solution

- Radix-R
- Memorise g^i, $i \in [1, R]$

Exponentiation: g^e with $e < 2^k$

Left To Right Exponentiation

- $a \leftarrow 1$
- **for** $i = k - 1$ **to** 0 **do**
  - $a \leftarrow a^2$
  - **if** $e_i = 1$ **then**
    - $a \leftarrow a \times g$

Exponentiation: g^e with $e < 2^k$

Left To Right Exponentiation

- $a \leftarrow 1$
- **for** $i = k - 1$ **to** 0 **do**
  - $a \leftarrow a^2$
  - **if** $e_i = 1$ **then**
    - $a \leftarrow a \times g$

Right To Left Exponentiation

- $a \leftarrow 1, b \leftarrow g$
- **for** $i = 0$ **to** $k - 1$ **do**
  - **if** $e_i = 1$ **then**
    - $a \leftarrow a \times b$
  - $b \leftarrow b^2$

SPA Attack

Recognising Operations

- XXXXXXXXXXXXXXXXXXXXXXXXX
- Modular Squaring (S): $a \leftarrow a^2$
- Modular Multiplication (M): $a \leftarrow a \times g$
- SSMSMSSMSMSSSMSMSMSSSSMS

SPA Attack

Recognising Operations

- XXXXXXXXXXXXXXXXXXXXXXXX
- Modular Squaring (S): $a \leftarrow a^2$
- Modular Multiplication (M): $a \leftarrow a \times g$
- SSMSMSSMSMSSSMSMSMSSSSMS

Regroup Operations

SSMSMSSMSMSSSMSMSMSSSSMS
(S)(SM)(SM)(S)(SM)(SM)(S)(S)(SM)(SM)(SM)(S)(S)(S)(SM)(S)

SPA Counter Measure

Classic Solution: Constant Time Algorithm

- Goal: Unlink Sequence of Operations to Secret Key
- Solution: Same Sequence for all secret key
- Drawback: Average Case=Worst Case

SPA Counter Measure

Classic Solution: Constant Time Algorithm

- Goal: Unlink Sequence of Operations to Secret Key
- Solution: Same Sequence for all secret key
- Drawback: Average Case=Worst Case

A second Solution: Stop parenthesing Phase

- Goal: Stop Attacker to be able to regroup operations
- Solution: Use Sequence of Equivalent Operations

Squaring Always

Taylor Formulae

$$A \times B = \left(\frac{A+B}{4}\right)^2 - \left(\frac{A-B}{4}\right)^2$$

Squaring Always

Taylor Formulae

$$A \times B = \left(\frac{A+B}{4}\right)^2 - \left(\frac{A-B}{4}\right)^2$$

Rewriting

- Modular Squaring (S) : $a \leftarrow a^2$
- Modular Multiplication (SS): $a \leftarrow a \times g$
- SSMSMSSMSMSSSMSMSMSSSSMS
- SSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSS

Squaring Always

Taylor Formulae

$$A \times B = \left(\frac{A+B}{4}\right)^2 - \left(\frac{A-B}{4}\right)^2$$

Rewriting

- Modular Squaring (S) : $a \leftarrow a^2$
- Modular Multiplication (SS): $a \leftarrow a \times g$
- SSMSMSSMSMSSSMSMSMSSSSMS
- SSSSSSSSSSSSSSSSSSSSSSSSSSSSSS

Drawback

- Cost of two S greater than M
- Only for $(\mathbb{Z}/N\mathbb{Z})$

Exponentiation based on Euclid Algorithm

Exponentiation

- $a \leftarrow g$, $b \leftarrow g^{2^{\frac{k}{2}}}$
- $u \leftarrow e \mod 2^{\frac{k}{2}}$, $v \leftarrow \frac{e-u}{2^{\frac{k}{2}}}$, $e = u + 2^{\frac{k}{2}} v$
- **while** $v \neq 0$ **do**
  - **if** $u > v$ **then**
    - $u \leftarrow u - v$
    - $b \leftarrow b \times a$
  - **else**
    - $v \leftarrow v - u$
    - $a \leftarrow a \times b$
- $a \leftarrow a^u$

Correctness

Invariant

$$a^u b^v = g^e$$

Correctness

Invariant

$$a^u b^v = g^e$$

Initialisation

$$a^u b^v = g^u(g^{2^{\frac{k}{2}}})^v) = g^{u+v2^{\frac{k}{2}}} = g^e$$

Correctness

Invariant

$$a^u b^v = g^e$$

Initialisation

$$a^u b^v = g^u (g^{2^{\frac{k}{2}}})^v) = g^{u+v2^{\frac{k}{2}}} = g^e$$

In the loop

$$a^{u-v}(ab)^v = a^u b^v$$

$$(ab)^u b^{v-u} = a^u b^v$$

Example: g^{3165}

u	v	a	b	If $u > v$?

Example: g^{3165}

u	v	a	b	If $u > v$?
29	49	g^1	g^{64}	

Example: g^{3165}

u	v	a	b	If $u > v$?				
29	49	g^1	g^{64}	F	29	$49 - 29$	g^{1+64}	g^{64}

Example: g^{3165}

u	v	a	b	If $u > v$?				
29	49	g^1	g^{64}	F	29	$49 - 29$	g^{1+64}	g^{64}
29	20	g^{65}	g^{64}					

Example: g^{3165}

u	v	a	b	If $u > v$?				
29	49	g^1	g^{64}	F	29	$49 - 29$	g^{1+64}	g^{64}
29	20	g^{65}	g^{64}	T	$29 - 20$	20	g^{65}	g^{64+65}

Example: g^{3165}

u	v	a	b	If $u > v$?				
29	49	g^1	g^{64}	F	29	$49 - 29$	g^{1+64}	g^{64}
29	20	g^{65}	g^{64}	T	$29 - 20$	20	g^{65}	g^{64+65}
9	20	g^{65}	g^{129}					

Example: g^{3165}

u	v	a	b	If $u > v$?				
29	49	g^{1}	g^{64}	F	29	$49 - 29$	g^{1+64}	g^{64}
29	20	g^{65}	g^{64}	T	$29 - 20$	20	g^{65}	g^{64+65}
9	20	g^{65}	g^{129}	F	9	$20 - 9$	g^{65+129}	g^{129}

Example: g^{3165}

u	v	a	b	If $u > v$?				
29	49	g^1	g^{64}	F	29	$49 - 29$	g^{1+64}	g^{64}
29	20	g^{65}	g^{64}	T	$29 - 20$	20	g^{65}	g^{64+65}
9	20	g^{65}	g^{129}	F	9	$20 - 9$	g^{65+129}	g^{129}
9	11	g^{194}	g^{129}					

Example: g^{3165}

u	v	a	b	If $u > v$?				
29	49	g^1	g^{64}	F	29	$49 - 29$	g^{1+64}	g^{64}
29	20	g^{65}	g^{64}	T	$29 - 20$	20	g^{65}	g^{64+65}
9	20	g^{65}	g^{129}	F	9	$20 - 9$	g^{65+129}	g^{129}
9	11	g^{194}	g^{129}	F	9	$11 - 9$	$g^{194+129}$	g^{129}

Example: g^{3165}

u	v	a	b	If $u > v$?				
29	49	g^1	g^{64}	F	29	$49 - 29$	g^{1+64}	g^{64}
29	20	g^{65}	g^{64}	T	$29 - 20$	20	g^{65}	g^{64+65}
9	20	g^{65}	g^{129}	F	9	$20 - 9$	g^{65+129}	g^{129}
9	11	g^{194}	g^{129}	F	9	$11 - 9$	$g^{194+129}$	g^{129}
9	2	g^{323}	g^{129}					

Example: g^{3165}

u	v	a	b	If $u > v$?				
29	49	g^{1}	g^{64}	F	29	$49-29$	g^{1+64}	g^{64}
29	20	g^{65}	g^{64}	T	$29-20$	20	g^{65}	g^{64+65}
9	20	g^{65}	g^{129}	F	9	$20-9$	g^{65+129}	g^{129}
9	11	g^{194}	g^{129}	F	9	$11-9$	$g^{194+129}$	g^{129}
9	2	g^{323}	g^{129}	T	$9-2$	2	g^{323}	$g^{129+323}$

Example: g^{3165}

u	v	a	b	If $u > v$?				
29	49	g^1	g^{64}	F	29	$49-29$	g^{1+64}	g^{64}
29	20	g^{65}	g^{64}	T	$29-20$	20	g^{65}	g^{64+65}
9	20	g^{65}	g^{129}	F	9	$20-9$	g^{65+129}	g^{129}
9	11	g^{194}	g^{129}	F	9	$11-9$	$g^{194+129}$	g^{129}
9	2	g^{323}	g^{129}	T	$9-2$	2	g^{323}	$g^{129+323}$
7	2	g^{323}	g^{452}					

Example: g^{3165}

u	v	a	b	If $u > v$?				
29	49	g^{1}	g^{64}	F	29	$49 - 29$	g^{1+64}	g^{64}
29	20	g^{65}	g^{64}	T	$29 - 20$	20	g^{65}	g^{64+65}
9	20	g^{65}	g^{129}	F	9	$20 - 9$	g^{65+129}	g^{129}
9	11	g^{194}	g^{129}	F	9	$11 - 9$	$g^{194+129}$	g^{129}
9	2	g^{323}	g^{129}	T	$9 - 2$	2	g^{323}	$g^{129+323}$
7	2	g^{323}	g^{452}	T	$7 - 2$	2	g^{323}	$g^{452+323}$

Example: g^{3165}

u	v	a	b	If $u > v$?				
29	49	g^{1}	g^{64}	F	29	$49-29$	g^{1+64}	g^{64}
29	20	g^{65}	g^{64}	T	$29-20$	20	g^{65}	g^{64+65}
9	20	g^{65}	g^{129}	F	9	$20-9$	g^{65+129}	g^{129}
9	11	g^{194}	g^{129}	F	9	$11-9$	$g^{194+129}$	g^{129}
9	2	g^{323}	g^{129}	T	$9-2$	2	g^{323}	$g^{129+323}$
7	2	g^{323}	g^{452}	T	$7-2$	2	g^{323}	$g^{452+323}$
5	2	g^{323}	g^{775}					

Example: g^{3165}

u	v	a	b	If $u > v$?				
29	49	g^1	g^{64}	F	29	$49-29$	g^{1+64}	g^{64}
29	20	g^{65}	g^{64}	T	$29-20$	20	g^{65}	g^{64+65}
9	20	g^{65}	g^{129}	F	9	$20-9$	g^{65+129}	g^{129}
9	11	g^{194}	g^{129}	F	9	$11-9$	$g^{194+129}$	g^{129}
9	2	g^{323}	g^{129}	T	$9-2$	2	g^{323}	$g^{129+323}$
7	2	g^{323}	g^{452}	T	$7-2$	2	g^{323}	$g^{452+323}$
5	2	g^{323}	g^{775}	T	$5-2$	2	g^{323}	$g^{775+323}$

Example: g^{3165}

u	v	a	b	If $u > v$?				
29	49	g^1	g^{64}	F	29	$49-29$	g^{1+64}	g^{64}
29	20	g^{65}	g^{64}	T	$29-20$	20	g^{65}	g^{64+65}
9	20	g^{65}	g^{129}	F	9	$20-9$	g^{65+129}	g^{129}
9	11	g^{194}	g^{129}	F	9	$11-9$	$g^{194+129}$	g^{129}
9	2	g^{323}	g^{129}	T	$9-2$	2	g^{323}	$g^{129+323}$
7	2	g^{323}	g^{452}	T	$7-2$	2	g^{323}	$g^{452+323}$
5	2	g^{323}	g^{775}	T	$5-2$	2	g^{323}	$g^{775+323}$
3	2	g^{323}	g^{1098}					

Example: g^{3165}

u	v	a	b	If $u > v$?				
29	49	g^1	g^{64}	F	29	$49 - 29$	g^{1+64}	g^{64}
29	20	g^{65}	g^{64}	T	$29 - 20$	20	g^{65}	g^{64+65}
9	20	g^{65}	g^{129}	F	9	$20 - 9$	g^{65+129}	g^{129}
9	11	g^{194}	g^{129}	F	9	$11 - 9$	$g^{194+129}$	g^{129}
9	2	g^{323}	g^{129}	T	$9 - 2$	2	g^{323}	$g^{129+323}$
7	2	g^{323}	g^{452}	T	$7 - 2$	2	g^{323}	$g^{452+323}$
5	2	g^{323}	g^{775}	T	$5 - 2$	2	g^{323}	$g^{775+323}$
3	2	g^{323}	g^{1098}	T	$3 - 2$	2	g^{323}	$g^{1098+323}$

Example: g^{3165}

u	v	a	b	If $u > v$?				
29	49	g^{1}	g^{64}	F	29	$49-29$	g^{1+64}	g^{64}
29	20	g^{65}	g^{64}	T	$29-20$	20	g^{65}	g^{64+65}
9	20	g^{65}	g^{129}	F	9	$20-9$	g^{65+129}	g^{129}
9	11	g^{194}	g^{129}	F	9	$11-9$	$g^{194+129}$	g^{129}
9	2	g^{323}	g^{129}	T	$9-2$	2	g^{323}	$g^{129+323}$
7	2	g^{323}	g^{452}	T	$7-2$	2	g^{323}	$g^{452+323}$
5	2	g^{323}	g^{775}	T	$5-2$	2	g^{323}	$g^{775+323}$
3	2	g^{323}	g^{1098}	T	$3-2$	2	g^{323}	$g^{1098+323}$
1	2	g^{323}	g^{1421}					

Example: g^{3165}

u	v	a	b	If $u > v$?				
29	49	g^{1}	g^{64}	F	29	$49-29$	g^{1+64}	g^{64}
29	20	g^{65}	g^{64}	T	$29-20$	20	g^{65}	g^{64+65}
9	20	g^{65}	g^{129}	F	9	$20-9$	g^{65+129}	g^{129}
9	11	g^{194}	g^{129}	F	9	$11-9$	$g^{194+129}$	g^{129}
9	2	g^{323}	g^{129}	T	$9-2$	2	g^{323}	$g^{129+323}$
7	2	g^{323}	g^{452}	T	$7-2$	2	g^{323}	$g^{452+323}$
5	2	g^{323}	g^{775}	T	$5-2$	2	g^{323}	$g^{775+323}$
3	2	g^{323}	g^{1098}	T	$3-2$	2	g^{323}	$g^{1098+323}$
1	2	g^{323}	g^{1421}	F	1	$2-1$	$g^{323+1421}$	g^{1421}

Example: g^{3165}

u	v	a	b	If $u > v$?				
29	49	g^{1}	g^{64}	F	29	$49-29$	g^{1+64}	g^{64}
29	20	g^{65}	g^{64}	T	$29-20$	20	g^{65}	g^{64+65}
9	20	g^{65}	g^{129}	F	9	$20-9$	g^{65+129}	g^{129}
9	11	g^{194}	g^{129}	F	9	$11-9$	$g^{194+129}$	g^{129}
9	2	g^{323}	g^{129}	T	$9-2$	2	g^{323}	$g^{129+323}$
7	2	g^{323}	g^{452}	T	$7-2$	2	g^{323}	$g^{452+323}$
5	2	g^{323}	g^{775}	T	$5-2$	2	g^{323}	$g^{775+323}$
3	2	g^{323}	g^{1098}	T	$3-2$	2	g^{323}	$g^{1098+323}$
1	2	g^{323}	g^{1421}	F	1	$2-1$	$g^{323+1421}$	g^{1421}
1	1	g^{1744}	g^{1421}					

Example: g^{3165}

u	v	a	b	If $u > v$?				
29	49	g^{1}	g^{64}	F	29	$49-29$	g^{1+64}	g^{64}
29	20	g^{65}	g^{64}	T	$29-20$	20	g^{65}	g^{64+65}
9	20	g^{65}	g^{129}	F	9	$20-9$	g^{65+129}	g^{129}
9	11	g^{194}	g^{129}	F	9	$11-9$	$g^{194+129}$	g^{129}
9	2	g^{323}	g^{129}	T	$9-2$	2	g^{323}	$g^{129+323}$
7	2	g^{323}	g^{452}	T	$7-2$	2	g^{323}	$g^{452+323}$
5	2	g^{323}	g^{775}	T	$5-2$	2	g^{323}	$g^{775+323}$
3	2	g^{323}	g^{1098}	T	$3-2$	2	g^{323}	$g^{1098+323}$
1	2	g^{323}	g^{1421}	F	1	$2-1$	$g^{323+1421}$	g^{1421}
1	1	g^{1744}	g^{1421}	F	1	$1-1$	$g^{1744+1421}$	g^{1421}

Example: g^{3165}

u	v	a	b	If $u > v$?				
29	49	g^{1}	g^{64}	F	29	$49-29$	g^{1+64}	g^{64}
29	20	g^{65}	g^{64}	T	$29-20$	20	g^{65}	g^{64+65}
9	20	g^{65}	g^{129}	F	9	$20-9$	g^{65+129}	g^{129}
9	11	g^{194}	g^{129}	F	9	$11-9$	$g^{194+129}$	g^{129}
9	2	g^{323}	g^{129}	T	$9-2$	2	g^{323}	$g^{129+323}$
7	2	g^{323}	g^{452}	T	$7-2$	2	g^{323}	$g^{452+323}$
5	2	g^{323}	g^{775}	T	$5-2$	2	g^{323}	$g^{775+323}$
3	2	g^{323}	g^{1098}	T	$3-2$	2	g^{323}	$g^{1098+323}$
1	2	g^{323}	g^{1421}	F	1	$2-1$	$g^{323+1421}$	g^{1421}
1	1	g^{1744}	g^{1421}	F	1	$1-1$	$g^{1744+1421}$	g^{1421}
1	0	g^{3165}	g^{1421}					

Cost

- Squaring: 0.5 k S
- Multiplication: $\sum q_i$ M with

$$q_i = \left\lfloor \frac{a_i}{b_i} \right\rfloor$$

the Partial Quotient of Euclid Algorithm applied on a, b

Cost

- Squaring: 0.5 k S
- Multiplication: $\sum q_i$ M with

$$q_i = \left\lfloor \frac{a_i}{b_i} \right\rfloor$$

the Partial Quotient of Euclid Algorithm applied on a, b

Continued Fractions

$$\frac{u}{v} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cdots + \cfrac{1}{q_n}}}}$$

Euclid Algorithm

Lamé's Theorem

The Maximum Number $l_{(u,v)}$ of steps of Brun Algorithm on the set $u > v > 0$ satisfies

$$l_{(u,v)} \simeq \frac{\log v}{\log \frac{1+\sqrt{5}}{2}}$$

Euclid Algorithm

Lamé's Theorem

The Maximum Number $l_{(u,v)}$ of steps of Brun Algorithm on the set $u > v > 0$ satisfies

$$l_{(u,v)} \simeq \frac{\log v}{\log \frac{1+\sqrt{5}}{2}}$$

Heilbronn's Theorem

The Mean Number of the total number of steps L_N is

$$\frac{12 \log 2}{\pi^2} \log N + O(1) \simeq 0.5841 \log_2 N$$

Euclid Algorithm

Sum of Partial Quotient

The Mean of the Sum of Partial Quotients is

$$\frac{1}{2}\left(\frac{12\log 2}{\pi^2}\log N\right)^2 \simeq 0.17062\log_2 N$$

Euclid Algorithm

Sum of Partial Quotient

The Mean of the Sum of Partial Quotients is

$$\frac{1}{2}\left(\frac{12\log 2}{\pi^2}\log N\right)^2 \simeq 0.17062\log_2 N$$

Exponentiation based on Euclid

- Squaring: $0.5k$ S
- Multiplication: $0.04265k^2$ M

Exponentiation based on Euclid Algorithm

Advantage: parenthesing Phase Blocked

- SSSSSSSSSSSMMMMMMMMMMMMMMMMMMM
- Few S $\simeq 0.5k$

Exponentiation based on Euclid Algorithm

Advantage: parenthesing Phase Blocked

- SSSSSSSSSSSMMMMMMMMMMMMMMMMM
- Few S $\simeq 0.5k$

Inconvenient

- Too Many M
- $GCD(u, v)$ can be big

Exponentiation based on Brun Algorithm

Exponentiation based on Multidimensional GCD Algorithm

Idea

- Cut e in d blocks

$$e = \sum_{i=0}^{d-1} e_i 2^{\frac{ik}{d}}$$

- Apply Multidimensional GCD Algorithm
- Repercuss operations on $g, g^{2^{\frac{k}{d}}}, g^{2^{\frac{2k}{d}}} \ldots$

Exponentiation based on Multidimensional GCD Algorithm

Idea

- Cut e in d blocks

$$e = \sum_{i=0}^{d-1} e_i 2^{\frac{ik}{d}}$$

- Apply Multidimensional GCD Algorithm
- Repercuss operations on $g, g^{2^{\frac{k}{d}}}, g^{2^{\frac{2k}{d}}} \dots$

Cost

- Squaring: $\frac{d-1}{d} k\mathrm{S}$
- Multiplication: $\sum q_i \ \mathrm{M}$

Multidimensional Euclid's algorithms

- Jacobi-Perron Subtract the first one to the two other ones

$$(u_0, u_1, u_2) \mapsto \left(u_2, u_0 - \left\lfloor \frac{u_0}{u_2} \right\rfloor u_2, u_1 - \left\lfloor \frac{u_1}{u_2} \right\rfloor u_2\right)$$

- Brun Subtract the second largest entry $(u_0 \geq u_1 \geq u_2 \geq 0)$

$$(u_0, u_1, u_2) \mapsto (u_0 - u_1, u_1, u_2)$$

- Poincaré Subtract the previous entry $(u_0 \geq u_1 \geq u_2 \geq 0)$

$$(u_0, u_1, u_2) \mapsto (u_0 - u_1, u_1 - u_2, u_2)$$

- Selmer Subtract the smallest to the largest

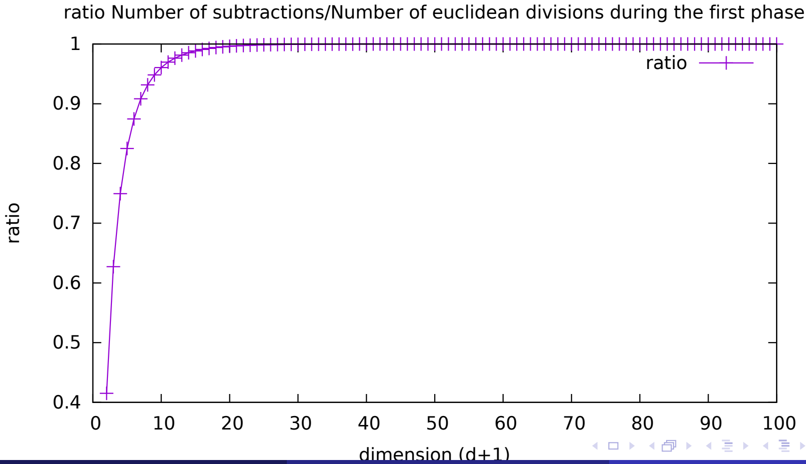
$$(u_0, u_1, u_2) \mapsto (u_0 - u_2, u_1, u_2)$$

- Fully subtractive Subtract the smallest one to the other ones

$$(u_0, u_1, u_2) \mapsto (u_0 - u_2, u_1 - u_2, u_2)$$

On the proportion of quotients equal to 1

- For $d = 16$, more than 99% of the Euclidean divisions are in fact subtractions
- For $d = 50$, the proportion is 99.99%.



Brun Algorithm Number of Step

Lam-Shallit-Vanstone Theorem

The Maximum Number $Q_{(d,N)}$ of steps of Brun Algorithm on the set $N \geq u_0 > u_1 > u_2 > \ldots > u_d > 0$ satisfies

$$Q_{(d,N)} \sim \frac{1}{|\log \tau_d|} \log N \qquad (N \to \infty)$$

Let $\tau_d \in]0, 1[$ be the smallest real root of $X^{d+1} + X - 1$

$$|\log \tau_d| \sim \frac{\log d}{(d+1)} \qquad (d \to \infty)$$

Brun Algorithm Number of Step

Berthé-Lhote-Vallée Theorem

The Mean Number of the total number of steps L_d, when N tends to ∞ is

$$\mathbb{E}_N[L_d] \sim \frac{d+1}{\mathcal{E}_d} \cdot \log N \qquad (N \to \infty)$$

$\mathcal{E}_d$: entropy of the Brun dynamical system

$$\mathcal{E}_d \sim \log d$$

$$\mathcal{E}_d \sim \log d \qquad (d \to \infty)$$

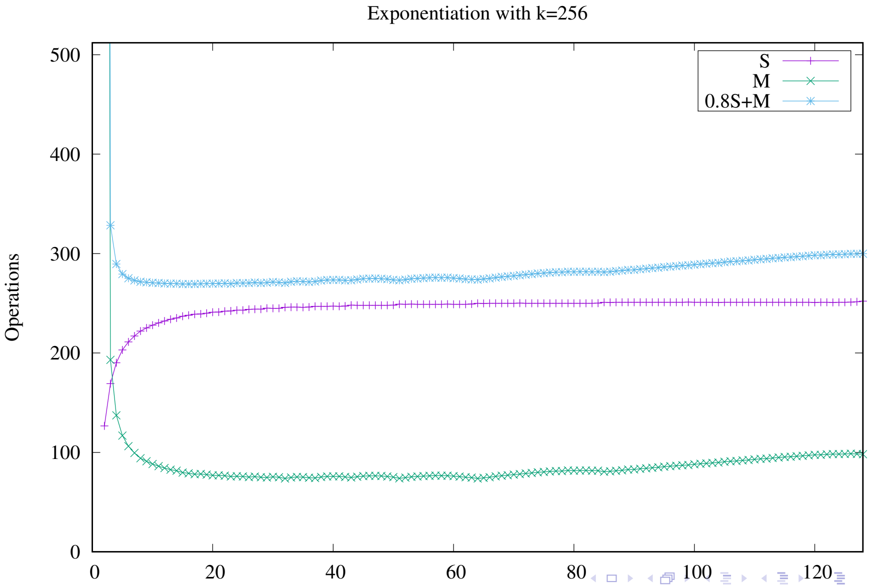
Brun Algorithm

Practical Case

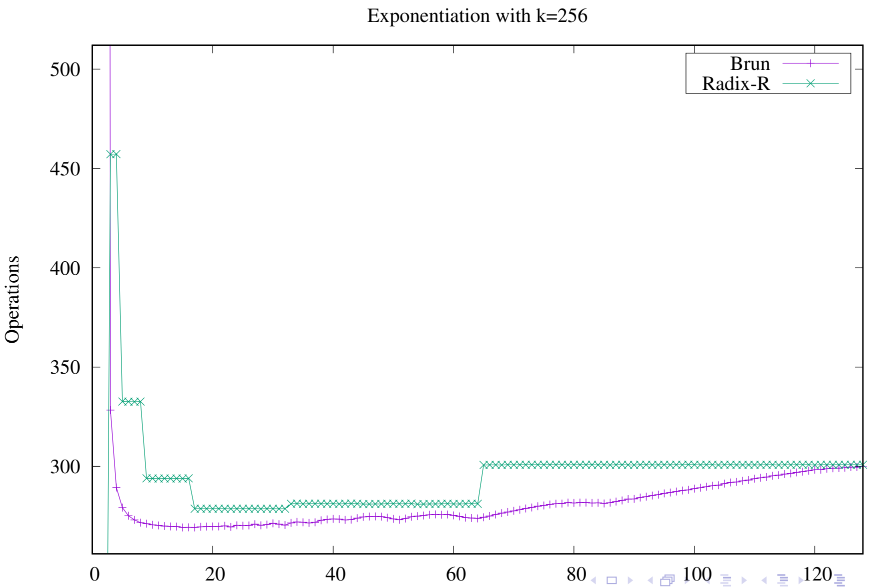
- $\mathbb{E}_N[L_2] = 0.58$
- $\mathbb{E}_N[L_3] = 1.036$
- $\mathbb{E}_N[L_4] = 1.416$
- $\mathbb{E}_N[L_5] = 1.753$
- $\mathbb{E}_N[L_6] = 2.058$
- $\mathbb{E}_N[L_7] = 2.342$

Future Works

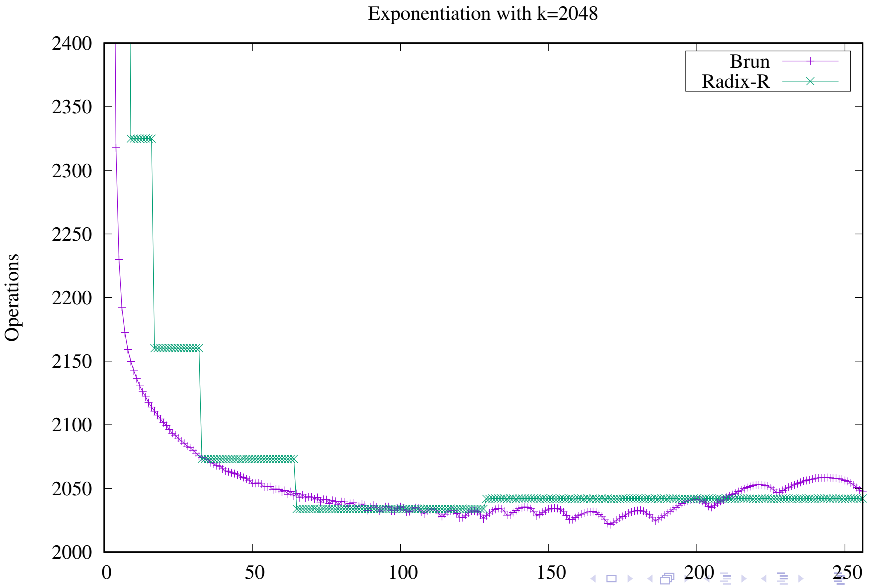
Cost of Exponentiation with Brun's Algorithm



Comparison for $k = 256$



Comparison for $k = 2048$



Conclusion

Exponentiation with Brun Algorithm offers

- Group Genericity
- SPA protection
- Adaptability on memory usage
- Efficiency

Conclusion

Exponentiation with Brun Algorithm offers

- Group Genericity
- SPA protection
- Adaptability on memory usage
- Efficiency

Future Works

- Brun with Euclidean Division
- Adapt to ECC special case: $-P$,co-Z,...