

Efficient exponentiation in software and hardware

Joachim von zur Gathen

Paderborn

Overview

Overview

- Exponentiation and the discrete logarithm: cryptography

Overview

- Exponentiation and the discrete logarithm: cryptography
- Addition chains

Overview

- Exponentiation and the discrete logarithm: cryptography
- Addition chains
- Normal bases, Gauß periods

Overview

- Exponentiation and the discrete logarithm: cryptography
- Addition chains
- Normal bases, Gauß periods
- Elements of large order

Overview

- Exponentiation and the discrete logarithm: cryptography
- Addition chains
- Normal bases, Gauß periods
- Elements of large order
- Elliptic curves on field-programmable gate arrays

Collaboration with

Collaboration with

Shuhong Gao, Daniel Panario, Victor Shoup (Toronto)

Collaboration with

Shuhong Gao, Daniel Panario, Victor Shoup (Toronto)

Marcus Bednara, Michael Daldrup, Sandra Feisel, Michael Nöcker, Martin Otto,
Jamshid Shokrollahi, Jürgen Teich (Paderborn)

Collaboration with

Shuhong Gao, Daniel Panario, Victor Shoup (Toronto)

Marcus Bednara, Michael Daldrup, Sandra Feisel, Michael Nöcker, Martin Otto,
Jamshid Shokrollahi, Jürgen Teich (Paderborn)

Arnold Knopfmacher, Lutz Lucht, Amin Shokrollahi, Igor Shparlinski

The Problem

The Problem

x is given. Exponentiation: $e \mapsto y = x^e$

The Problem

x is given. Exponentiation: $e \mapsto y = x^e$

Easy to compute: “repeated squaring”

The Problem

x is given. Exponentiation: $e \mapsto y = x^e$

Easy to compute: “repeated squaring”

Inverse map: $e = \log_x y \leftarrow y$

The Problem

x is given. Exponentiation: $e \mapsto y = x^e$

Easy to compute: “repeated squaring”

Inverse map: $e = \log_x y \leftarrow y$

Finite domain for x : “discrete logarithm”

The Problem

x is given. Exponentiation: $e \mapsto y = x^e$

Easy to compute: “repeated squaring”

Inverse map: $e = \log_x y \leftarrow y$

Finite domain for x : “discrete logarithm”

Usually difficult.

The Problem

x is given. Exponentiation: $e \mapsto y = x^e$

Easy to compute: “repeated squaring”

Inverse map: $e = \log_x y \leftarrow y$

Finite domain for x : “discrete logarithm”

Usually difficult.

Basis for security in cryptography:

RSA

Diffie-Hellman

ElGamal

Schnorr / DSA

⋮

\mathbb{Z} modulo $p \cdot q$

{ finite Field: $\mathbb{Z}_p, \mathbb{F}_{2^n}$

{ elliptic curves over finite fields

Upper and lower Bounds

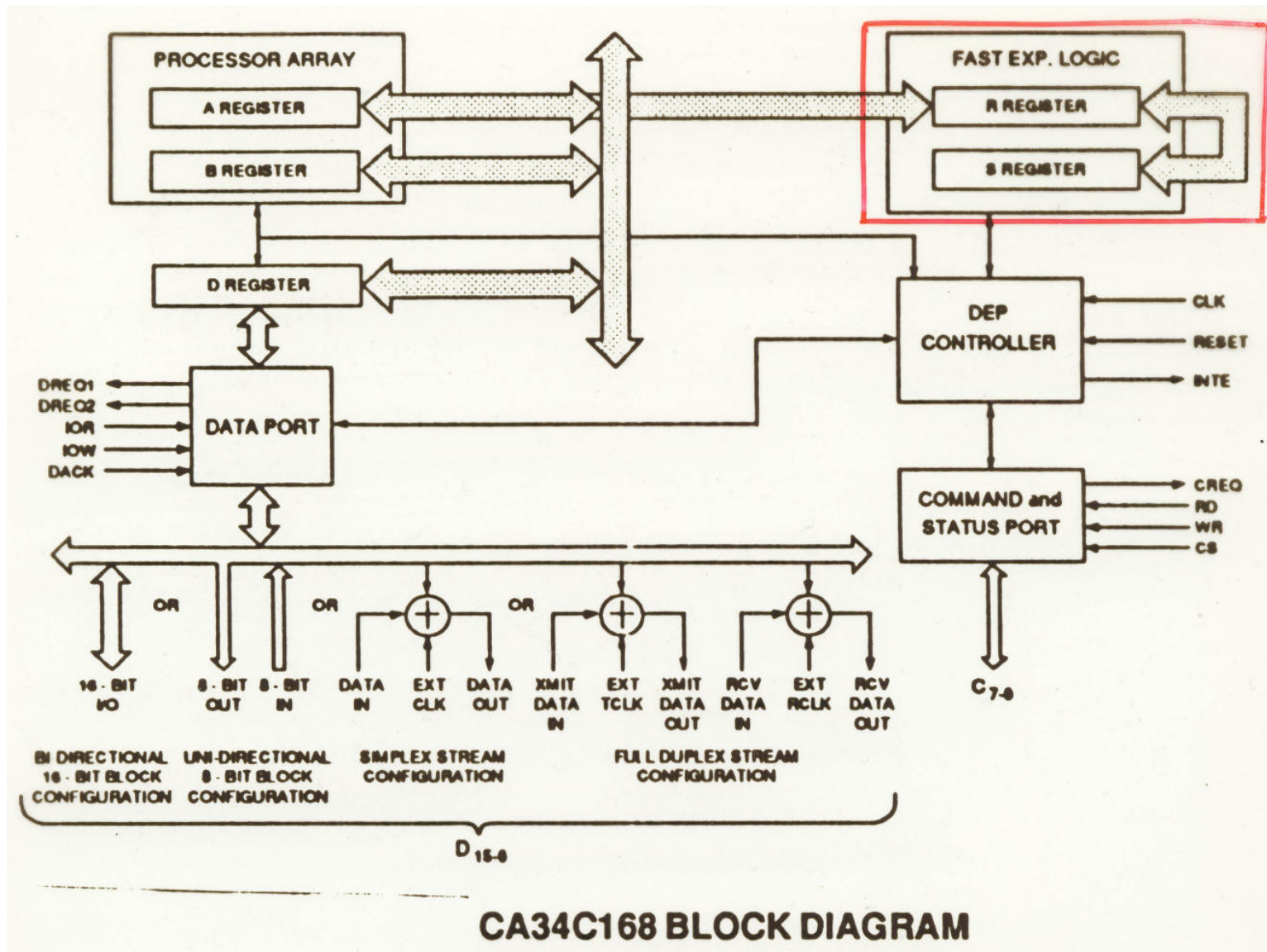
n = binary length of e , w = Hamming weight of e = number of 1's.

This addition chain has length $n + w - 2 \leq 2n - 2$.

Brauer 1939: length $n + \frac{n}{\log n} + o\left(\frac{n}{\log n}\right)$ possible.

Lower bound: length $\geq n$, since one addition can increase the length by at most 1.

Schönhage 1975: length $\geq n + \log_2 w - 2.13$.



CA34C168 BLOCK DIAGRAM

CLASS 2 DEP INSTRUCTION SET

Instruction* OP Code		Operation	Register					DEP cycles
			A	B	D	R	S	
<i>Class 2</i>								
INVA	D0	Compute the inverse of A (Note 1)	A^{-1}	U				50000
MULT	A0	A gets $A * B$	$A * B$					1300
EXP1	B0	Full exponentiation	$(A)^D$					up to 10^6
EXP2	C4	Fast exponentiation (Note 3)	$(A)^{PER}$	$(A)^{PER}$				up to 40000
EXP3	CC	EXP2 PERMR CPA2B SWAPRS EXP2 PERMR SWAPRS (Note 2)	$(A)^{PER.S}$	$(A)^{PER.S}$		R	S	up to 80000

Important domain: $\mathbb{F}_{2^n} = \mathbb{F}_2[x]/(f) = n$ -bit vector space,
 $f \in \mathbb{F}_2[x]$ irreducible of degree n .

Goal: beat the lower bound!

Important domain: $\mathbb{F}_{2^n} = \mathbb{F}_2[x]/(f) = n$ -bit vector space,
 $f \in \mathbb{F}_2[x]$ irreducible of degree n .

Goal: beat the lower bound!

Method: special data structure:

normal basis

Important domain: $\mathbb{F}_{2^n} = \mathbb{F}_2[x]/(f) = n$ -bit vector space,
 $f \in \mathbb{F}_2[x]$ irreducible of degree n .

Goal: beat the lower bound!

Method: special data structure: normal basis

$\alpha \in \mathbb{F}_{2^n}$

$\alpha, \alpha^2, \alpha^4, \alpha^8, \dots, \alpha^{2^{n-1}}$ basis over \mathbb{F}_2 .

Important domain: $\mathbb{F}_{2^n} = \mathbb{F}_2[x]/(f) = n$ -bit vector space,
 $f \in \mathbb{F}_2[x]$ irreducible of degree n .

Goal: beat the lower bound!

Method: special data structure: normal basis

$$\alpha \in \mathbb{F}_{2^n}$$

$\alpha, \alpha^2, \alpha^4, \alpha^8, \dots, \alpha^{2^{n-1}}$ basis over \mathbb{F}_2 .

$$a = \sum_{0 \leq i < n} a_i \alpha^{2^i} \text{ arbitrary, } a_i \in \mathbb{F}_2 = \{0, 1\}$$

Important domain: $\mathbb{F}_{2^n} = \mathbb{F}_2[x]/(f) = n$ -bit vector space,
 $f \in \mathbb{F}_2[x]$ irreducible of degree n .

Goal: beat the lower bound!

Method: special data structure: normal basis

$$\alpha \in \mathbb{F}_{2^n}$$

$\alpha, \alpha^2, \alpha^4, \alpha^8, \dots, \alpha^{2^{n-1}}$ basis over \mathbb{F}_2 .

$$a = \sum_{0 \leq i < n} a_i \alpha^{2^i} \text{ arbitrary, } a_i \in \mathbb{F}_2 = \{0, 1\}$$

$$a^2 = \left(\sum_i a_i \alpha^{2^i} \right)^2 = \sum_i a_i \alpha^{2^{i+1}} = \sum_i a_{i-1} \alpha^{2^i}, \text{ since } (u + v)^2 = u^2 + v^2.$$

Thus: squaring \leftrightarrow cyclic shift – for free!

THEOREM. *Exponentiation with n -bit exponents*

THEOREM. *Exponentiation with n -bit exponents*

- *can be done using $\frac{n}{\log_2 n} (1 + o(1))$ operations in \mathbb{F}_{q^n} ,*

THEOREM. *Exponentiation with n -bit exponents*

- *can be done using $\frac{n}{\log_2 n} (1 + o(1))$ operations in \mathbb{F}_{q^n} ,*
- *needs at least $\frac{1}{3} \frac{n}{\log_2 n}$ operations.*

THEOREM. *Exponentiation with n -bit exponents*

- *can be done using $\frac{n}{\log_2 n} (1 + o(1))$ operations in \mathbb{F}_{q^n} ,*
- *needs at least $\frac{1}{3} \frac{n}{\log_2 n}$ operations.*

Construction of normal bases:

THEOREM. *Exponentiation with n -bit exponents*

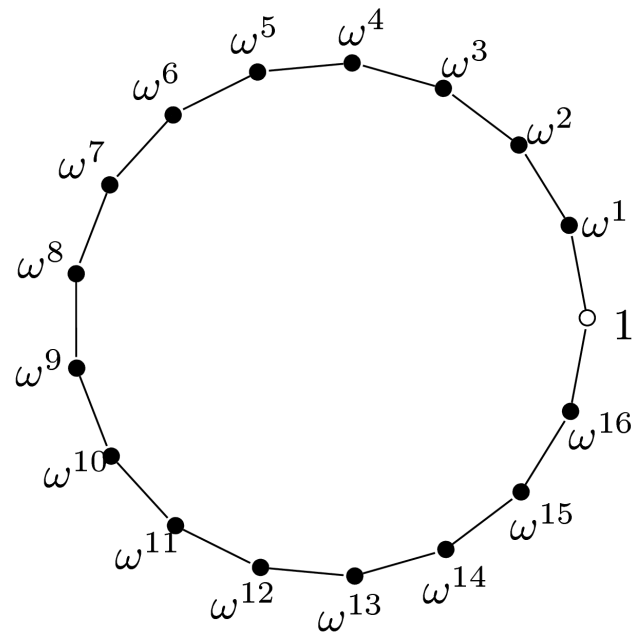
- *can be done using $\frac{n}{\log_2 n} (1 + o(1))$ operations in \mathbb{F}_{q^n} ,*
- *needs at least $\frac{1}{3} \frac{n}{\log_2 n}$ operations.*

Construction of normal bases:

Gauß periods

$$\omega = e^{2\pi i/17}$$

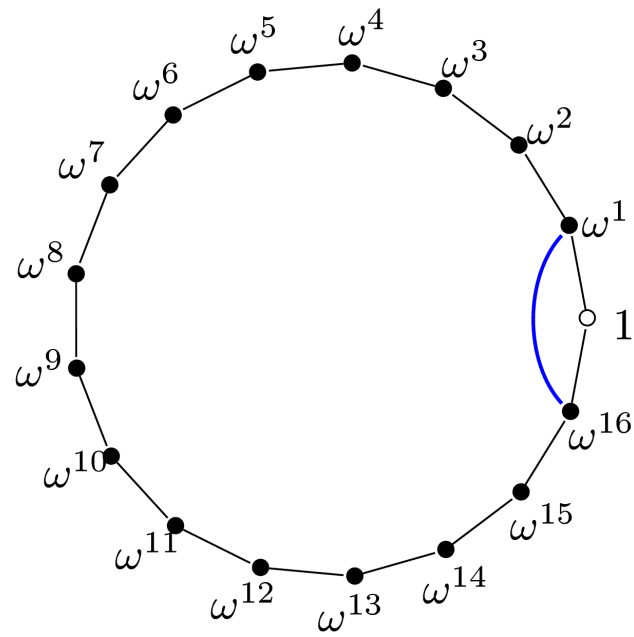
$$\omega = e^{2\pi i/17}$$



$$\underbrace{\{1\}}_{G_0}$$

$$\subseteq \underbrace{\mathbb{Z}_{17}^\times}_{G_4}$$

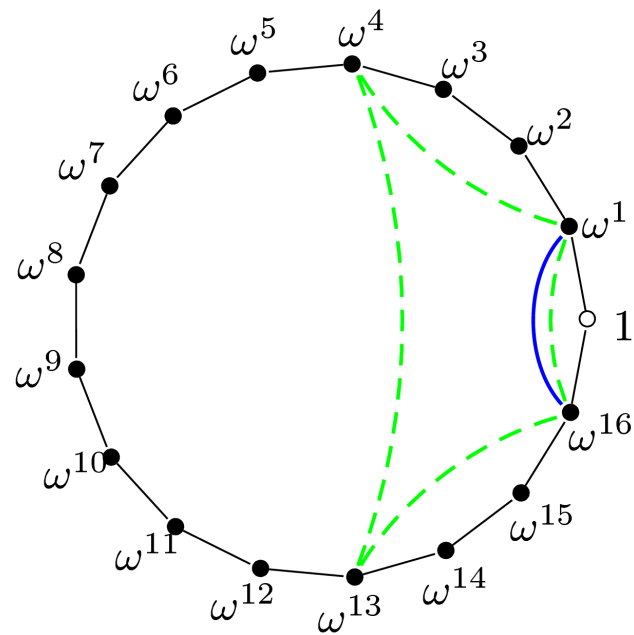
$$\omega = e^{2\pi i/17}$$



$$\underbrace{\{1\}}_{G_0} \subseteq \underbrace{\{1, 16\}}_{G_1}$$

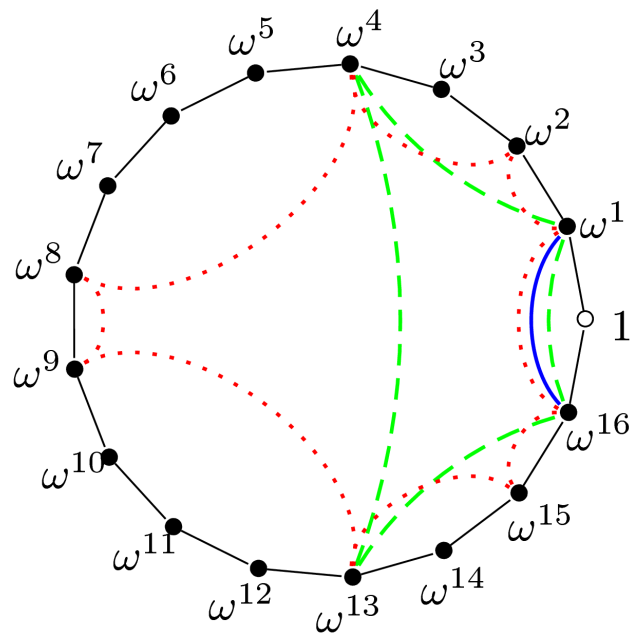
$$\subseteq \underbrace{\mathbb{Z}_{17}^\times}_{G_4}$$

$$\omega = e^{2\pi i/17}$$



$$\underbrace{\{1\}}_{G_0} \subseteq \underbrace{\{1, 16\}}_{G_1} \subseteq \underbrace{\{1, 4, 13, 16\}}_{G_2} \subseteq \underbrace{\mathbb{Z}_{17}^\times}_{G_4}$$

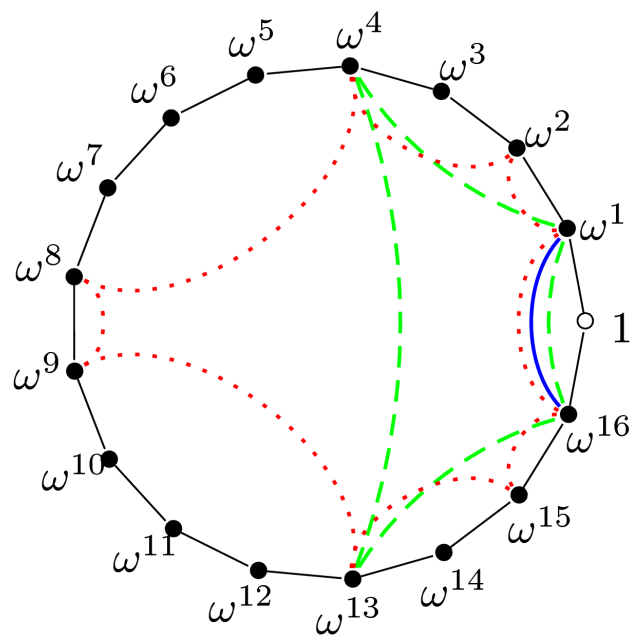
$$\omega = e^{2\pi i/17}$$



$$\underbrace{\{1\}}_{G_0} \subseteq \underbrace{\{1, 16\}}_{G_1} \subseteq \underbrace{\{1, 4, 13, 16\}}_{G_2} \subseteq \underbrace{\{1, 2, 4, 8, 9, 13, 15, 16\}}_{G_3} \subseteq \underbrace{\mathbb{Z}_{17}^\times}_{G_4}$$

$$\omega = e^{2\pi i/17}$$

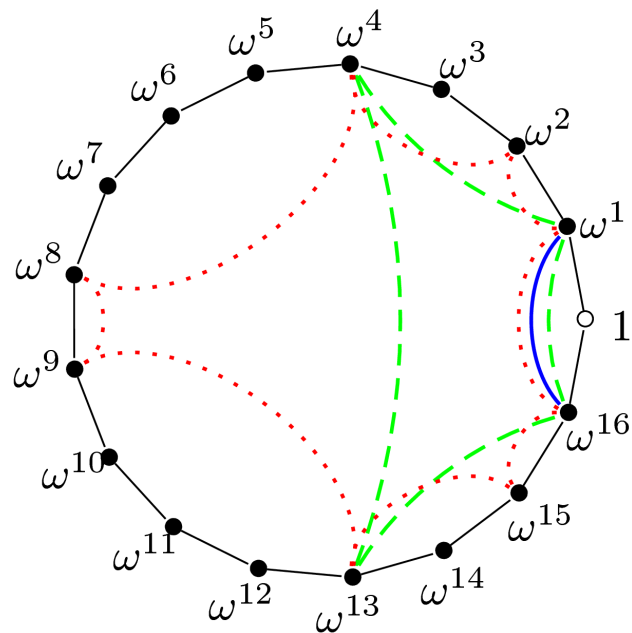
$$\alpha_i = \sum_{a \in G_i} \omega^a$$



$$\underbrace{\{1\}}_{G_0} \subseteq \underbrace{\{1, 16\}}_{G_1} \subseteq \underbrace{\{1, 4, 13, 16\}}_{G_2} \subseteq \underbrace{\{1, 2, 4, 8, 9, 13, 15, 16\}}_{G_3} \subseteq \underbrace{\mathbb{Z}_{17}^\times}_{G_4}$$

$$\omega = e^{2\pi i/17}$$

$$\alpha_i = \sum_{a \in G_i} \omega^a$$



$$\begin{array}{cccccc}
 \underbrace{\{1\}}_{G_0} & \subseteq & \underbrace{\{1, 16\}}_{G_1} & \subseteq & \underbrace{\{1, 4, 13, 16\}}_{G_2} & \subseteq & \underbrace{\{1, 2, 4, 8, 9, 13, 15, 16\}}_{G_3} & \subseteq & \underbrace{\mathbb{Z}_{17}^\times}_{G_4} \\
 \mathbb{Q}(\omega) & \supseteq & \mathbb{Q}(\alpha_1) & \supseteq & \mathbb{Q}(\alpha_2) & \supseteq & \mathbb{Q}(\alpha_3) & \supseteq & \mathbb{Q}(\alpha_4) = \mathbb{Q}
 \end{array}$$

r prime, n divides $r - 1$, say $n \cdot k = r - 1$,

β primitive r th root of unity in \mathbb{F}_q ,

$K \subseteq \mathbb{Z}_r^\times$ (unique) subgroup with k elements,

$$\alpha = \sum_{a \in K} \beta^a \text{ **Gauß period.**}$$

Then $\alpha \in \mathbb{F}_{q^n}$.

THEOREM (Wassermann 1990). α normal over $\mathbb{F}_q \iff \mathbb{Z}_r^\times = \langle q, K \rangle$.

Mullin, Onyszchuk, Vanstone & Wilson 1989: optimal normal basis (over \mathbb{F}_2).

Exponentiation: $O(n^3)$ operations in \mathbb{F}_2 , using Massey-Omura.

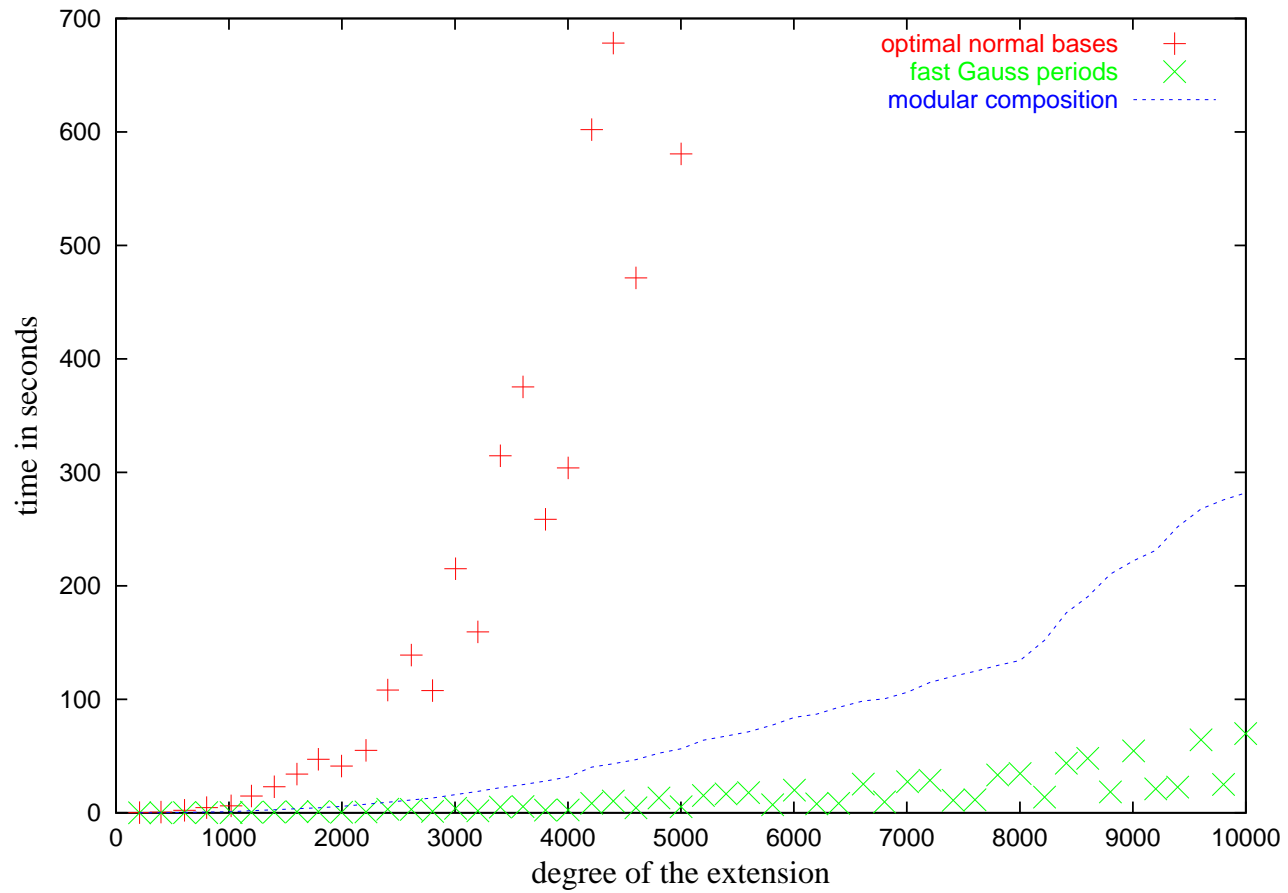
Gao & Lenstra 1992: equivalent to Gauß periods with $k = 1$ or $k = 2$.

Mullin, Onyszchuk, Vanstone & Wilson 1989: optimal normal basis (over \mathbb{F}_2).

Exponentiation: $O(n^3)$ operations in \mathbb{F}_2 , using Massey-Omura.

Gao & Lenstra 1992: equivalent to Gauß periods with $k = 1$ or $k = 2$.

THEOREM. *Exponentiation in \mathbb{F}_2 can be done using $O(n^2 \log \log n)$ operations.*



Comparison of three exponentiation algorithms for $n \leq 10000$ and $k = 1, 2$

Elements of large Order

\mathbb{F}_q : finite field with q elements, q prime power

\mathbb{F}_q^\times has order $q - 1$. An element $\gamma \in \mathbb{F}_q^\times$ is *primitive* if and only if its order is $q - 1$.

Elements of large Order

\mathbb{F}_q : finite field with q elements, q prime power

\mathbb{F}_q^\times has order $q - 1$. An element $\gamma \in \mathbb{F}_q^\times$ is *primitive* if and only if its order is $q - 1$.

Gauß, *Disquisitiones Arithmeticae*, 1801, article 73:

58

DE RESIDUIS POTESTATUM.

Methodus radices primitivas assignandi.

73.

Methodi radices primitivas inveniendi maximam partem tentando innituntur. Si quis ea quae art. 55 docuimus cum iis quae infra de solutione congruentiae $x^n \equiv 1$ trademus confert, omnia fere, quae per methodos directas effici possunt, habebit. Ill. Euler confitetur, *Opusc. Analyt. T. I. p. 152*, maxime difficile videri, hos numeros assignare, eorumque indolem ad profundissima numerorum mysteria esse referendam. At tentando satis expedite sequenti modo determinari possunt. Exercitatus operationis prolixitati per multifaria artificia particularia succurrere sciet: haec vero per usum multo citius quam per praecepta ediscuntur.

Average order of a random element of \mathbb{F}_q :

$$\alpha(q-1) = \frac{1}{q-1} \sum_{a \in \mathbb{F}_q^\times} \text{ord}(a)$$

THEOREM. $\varphi(q-1) \leq \alpha(q-1)$

Average order of a random element of \mathbb{F}_q :

$$\alpha(q-1) = \frac{1}{q-1} \sum_{a \in \mathbb{F}_q^\times} \text{ord}(a)$$

THEOREM. $\varphi(q-1) \leq \alpha(q-1) < A \cdot \varphi(q-1)$,

where $A = \frac{\zeta(2)\zeta(3)}{\zeta(6)} \approx 1.94\dots$

Algorithmic Tasks

Can we solve the following problems in polynomial time $(\log q)^{O(1)}$?

Algorithmic Tasks

Can we solve the following problems in polynomial time $(\log q)^{O(1)}$?

1. Check if $\gamma \in \mathbb{F}_q^\times$ is primitive. The known methods use the factorization of $q - 1$.

Algorithmic Tasks

Can we solve the following problems in polynomial time $(\log q)^{O(1)}$?

1. Check if $\gamma \in \mathbb{F}_q^\times$ is primitive. The known methods use the factorization of $q - 1$.
2. Find a primitive element.

Algorithmic Tasks

Can we solve the following problems in polynomial time $(\log q)^{O(1)}$?

1. Check if $\gamma \in \mathbb{F}_q^\times$ is primitive. The known methods use the factorization of $q - 1$.
2. Find a primitive element.
3. Find an element of large order.

Algorithmic Tasks

Can we solve the following problems in polynomial time $(\log q)^{O(1)}$?

1. Check if $\gamma \in \mathbb{F}_q^\times$ is primitive. The known methods use the factorization of $q - 1$.
2. Find a primitive element.
3. Find an element of large order.
4. Find a small extension \mathbb{F}_{q^s} of \mathbb{F}_q and an element of large order in it.

THEOREM. *We suppose that Artin's conjecture is true for p , so that p is primitive modulo many prime numbers. Then for every number N there exists an $n \geq N$ with $n \in O(N \log N)$ so that $\alpha = \beta + \beta^{-1} \in \mathbb{F}_{p^n}$ is normal with order*

$$\geq 2^{(2n)^{1/2}-2}.$$

THEOREM. *We suppose that Artin's conjecture is true for p , so that p is primitive modulo many prime numbers. Then for every number N there exists an $n \geq N$ with $n \in O(N \log N)$ so that $\alpha = \beta + \beta^{-1} \in \mathbb{F}_{p^n}$ is normal with order*

$$\geq 2^{(2n)^{1/2}-2}.$$

Ultimate goal: order $\approx 2^n$.

General Gauß periods

Gauß, *Disquisitiones Arithmeticae*, 1801, article 356:

DISTRIBUTIO RADICUM Ω IN DUAS PERIODOS.

443

$= \pm \sqrt[n]{n}$, quae theorematum propter elegantiam suam valde sunt memorabilia. Ceterum observamus, signa superiora semper valere, quando pro k accipiatur unitas aut generalius residuum quadraticum ipsius n , inferiora, quando pro k non-residuum assumatur, nec non haecce theorematum salva vel potius aucta elegantia sua etiam ad valores quosvis compositos ipsius n extendi posse: sed de his rebus, quae altioris sunt indaginis, hoc loco tacere earumque considerationem ad aliam occasionem nobis reservare oportet.

$$nk = \varphi(r), K \subseteq \mathbb{Z}_r^\times, \beta \text{ primitive } r\text{-th root unity, } \alpha = \sum_{a \in K} \beta^a.$$

If r is **prime** : α normal $\iff \mathbb{Z}_r^\times = \langle q, K \rangle$.

General Gauß periods

Gauß, *Disquisitiones Arithmeticae*, 1801, article 356:

DISTRIBUTIO RADICUM Ω IN DUAS PERIODOS.

443

$= \pm\sqrt[n]{n}$, quae theorematum propter elegantiam suam valde sunt memorabilia. Ceterum observamus, signa superiora semper valere, quando pro k accipiatur unitas aut generalius residuum quadraticum ipsius n , inferiora, quando pro k non-residuum assumatur, nec non haecce theorematum salva vel potius aucta elegantia sua etiam ad valores quosvis compositos ipsius n extendi posse: sed de his rebus, quae altioris sunt indaginis, hoc loco tacere earumque considerationem ad aliam occasionem nobis reservare oportet.

$$nk = \varphi(r), K \subseteq \mathbb{Z}_r^\times, \beta \text{ primitive } r\text{-th root unity, } \alpha = \sum_{a \in K} \beta^a.$$

If r is **squarefree** : α normal $\iff \mathbb{Z}_r^\times = \langle q, K \rangle$.

General Gauß periods

Gauß, *Disquisitiones Arithmeticae*, 1801, article 356:

DISTRIBUTIO RADICUM Ω IN DUAS PERIODOS.

443

$= \pm \sqrt[n]{n}$, quae theorematum propter elegantiam suam valde sunt memorabilia. Ceterum observamus, signa superiora semper valere, quando pro k accipiatur unitas aut generalius residuum quadraticum ipsius n , inferiora, quando pro k non-residuum assumatur, nec non haecce theorematum salva vel potius aucta elegantia sua etiam ad valores quosvis compositos ipsius n extendi posse: sed de his rebus, quae altioris sunt indaginis, hoc loco tacere earumque considerationem ad aliam occasionem nobis reservare oportet.

$nk = \varphi(r)$, $K \subseteq \mathbb{Z}_r^\times$, β primitive r -th root unity, $\alpha = \dots$

If r is **arbitrary** : α normal $\iff \mathbb{Z}_r^\times = \langle q, K \rangle$.

General Gauß periods

Gauß, *Disquisitiones Arithmeticae*, 1801, article 356:

DISTRIBUTIO RADICUM Ω IN DUAS PERIODOS.

443

$= \pm \sqrt[n]{n}$, quae theorematum propter elegantiam suam valde sunt memorabilia. Ceterum observamus, signa superiora semper valere, quando pro k accipiatur unitas aut generalius residuum quadraticum ipsius n , inferiora, quando pro k non-residuum assumatur, nec non haecce theorematum salva vel potius aucta elegantia sua etiam ad valores quosvis compositos ipsius n extendi posse: sed de his rebus, quae altioris sunt indaginis, hoc loco tacere earumque considerationem ad aliam occasionem nobis reservare oportet.

$nk = \varphi(r)$, $K \subseteq \mathbb{Z}_r^\times$, β primitive r -th root unity, $\alpha = \dots$

If r is **arbitrary** : α normal $\iff \mathbb{Z}_r^\times = \langle q, K \rangle$.

But: different formula for α .

Gauß periods for $q \in \{3, 5, 7, 11\}$ and $2 \leq n \leq 100$ with no prime Gauß period:

q	n	r		k	\mathcal{K}
3	12	35		2	{1, 6}
3	24	119		4	{1, 50, 69, 118}
3	36	95		2	{1, 56}
3	48	119		2	{1, 69}
3	60	155		2	{1, 61}
3	72	323		4	{1, 18, 305, 322}
3	84	203		2	{1, 146}
3	96	896	□	4	{1, 321, 575, 895}
5	10	33		2	{1, 10}
5	20	176	□	4	{1, 23, 65, 87}
5	30	77		2	{1, 76}
5	40	187		4	{1, 67, 120, 186}
5	50	303		4	{1, 10, 91, 100}
5	60	407		6	{1, 100, 175, 232, 307, 406}
5	70	473		6	{1, 122, 221, 252, 351, 472}
5	80	187		2	{1, 120}
5	90	297	□	2	{1, 109}
5	100	1616	□	8	{1, 111, 313, 495, 697, 807, 1009, 1415}
7	28	145		4	{1, 12, 133, 144}
7	56	493		8	{1, 86, 186, 220, 273, 307, 407, 492}
7	84	377		4	{1, 12, 144, 220}
11	44	368	□	4	{1, 137, 47, 183}
11	88	391		4	{1, 183, 254, 344}

Improvements for $q = 2$ and $2 \leq n \leq 111$:

n	$k_{\text{prime}}(2, n)$	$k_{\text{general}}(2, n)$	ratio	r	\mathcal{K}
6	2	1	2.0	9	\square {1}
20	3	1	3.0	25	\square {1}
21	10	2	5.0	49	\square {1, 48}
22	3	2	1.5	69	{1, 68}
27	6	2	3.0	81	\square {1, 80}
34	9	6	1.5	309	{1, 46, 47, 262, 263, 308}
42	5	2	2.5	147	\square {1, 146}
44	9	2	4.5	115	{1, 91}
46	3	2	1.5	141	{1, 140}
54	3	1	3.0	81	\square {1}
55	12	2	6.0	121	\square {1, 120}
57	10	6	1.67	361	\square {1, 68, 69, 292, 293, 360}
68	9	6	1.5	515	\square {1, 46, 56, 356, 366, 411}
70	3	2	1.5	213	{1, 212}
75	10	8	1.25	707	{1, 111, 293, 302, 405, 414, 596, 706}
78	7	2	3.5	169	\square {1, 168}
84	5	2	2.5	203	{1, 202}
92	3	2	1.5	235	{1, 46}
102	6	2	3.0	309	{1, 308}
108	5	2	2.5	405	\square {1, 404}
110	6	1	6.0	121	\square {1}
111	20	8	2.5	1043	{1, 148, 342, 491, 552, 701, 895, 1042}

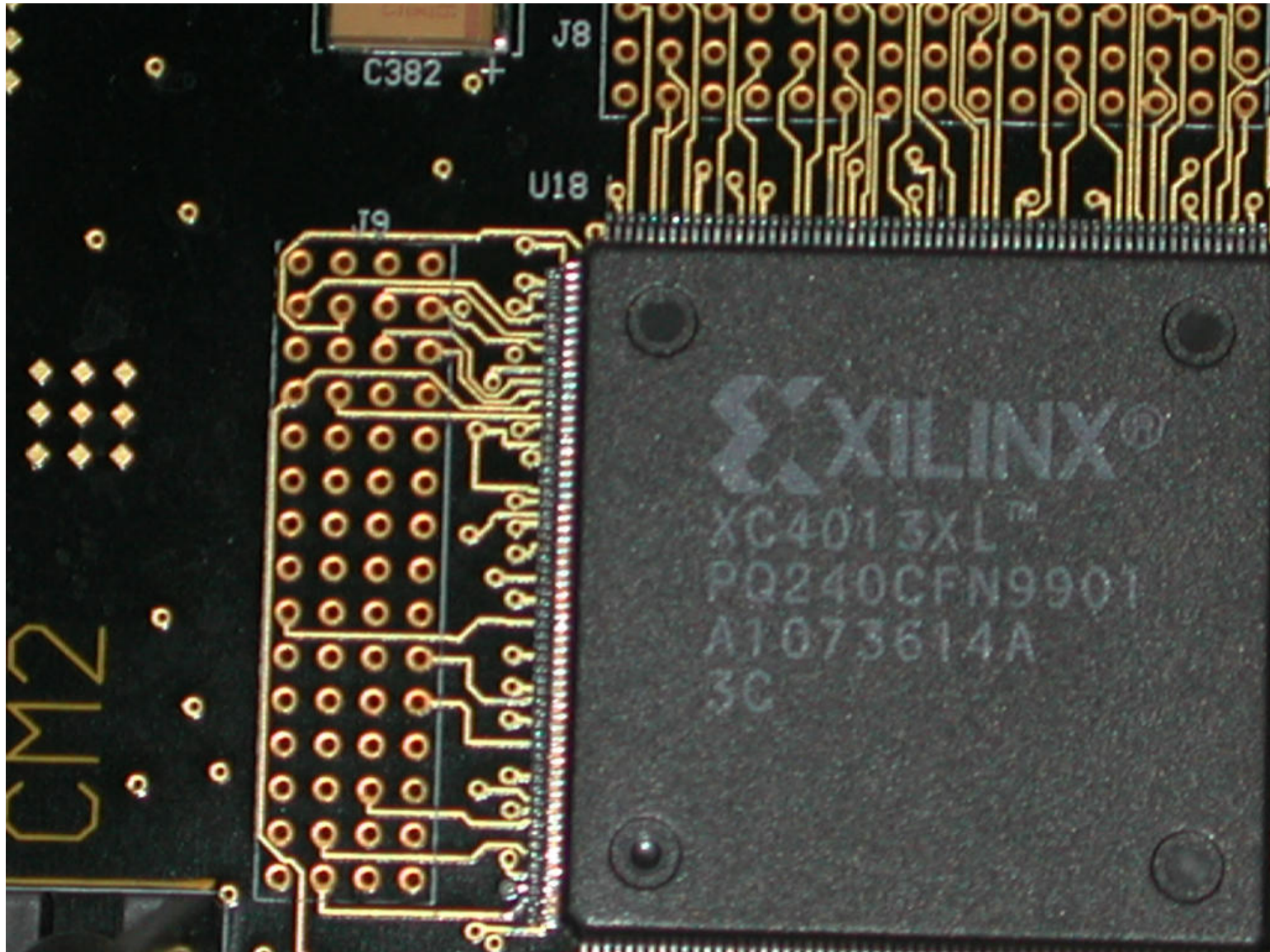
Elliptic Curves

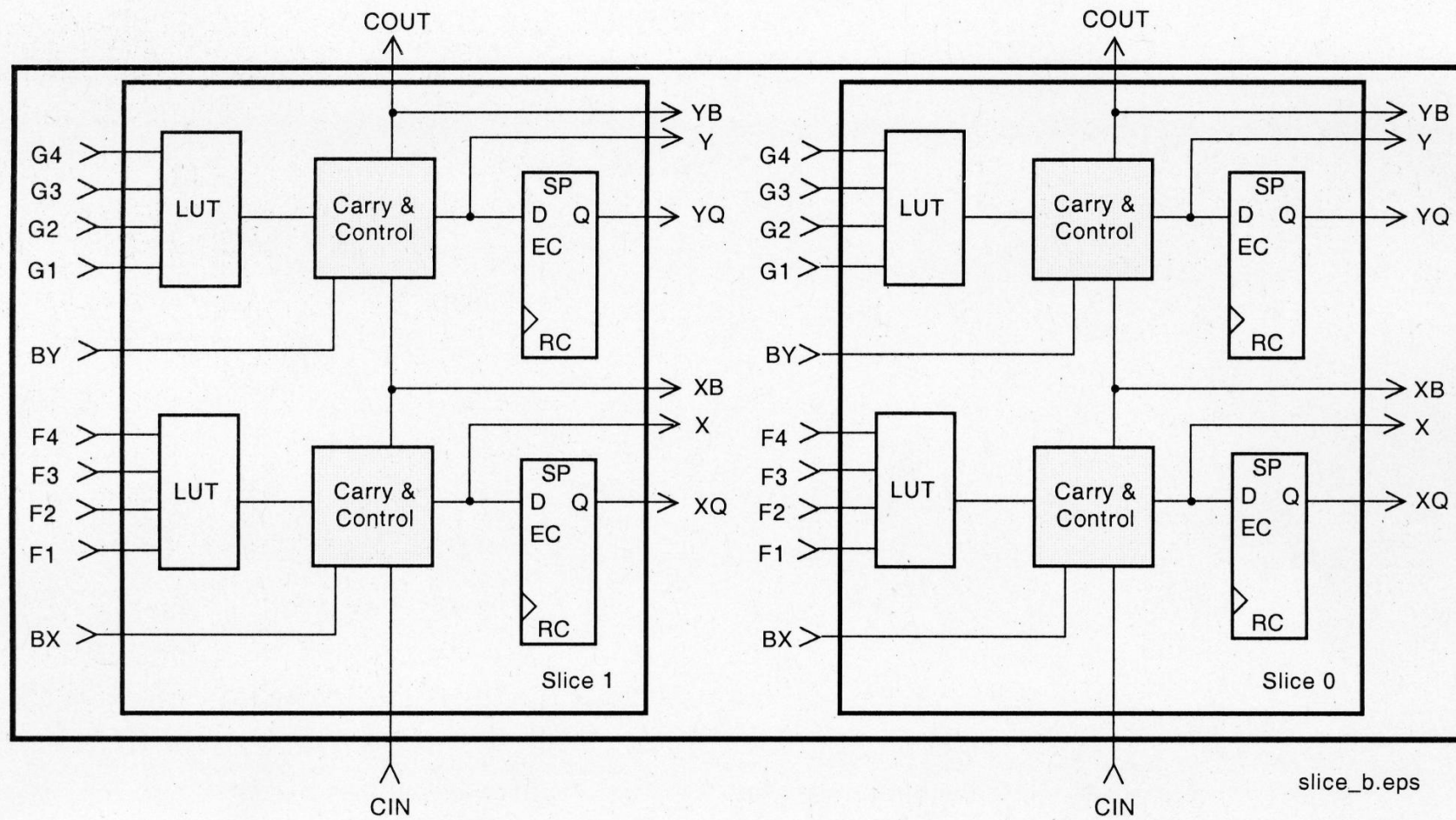
Popular in cryptography.

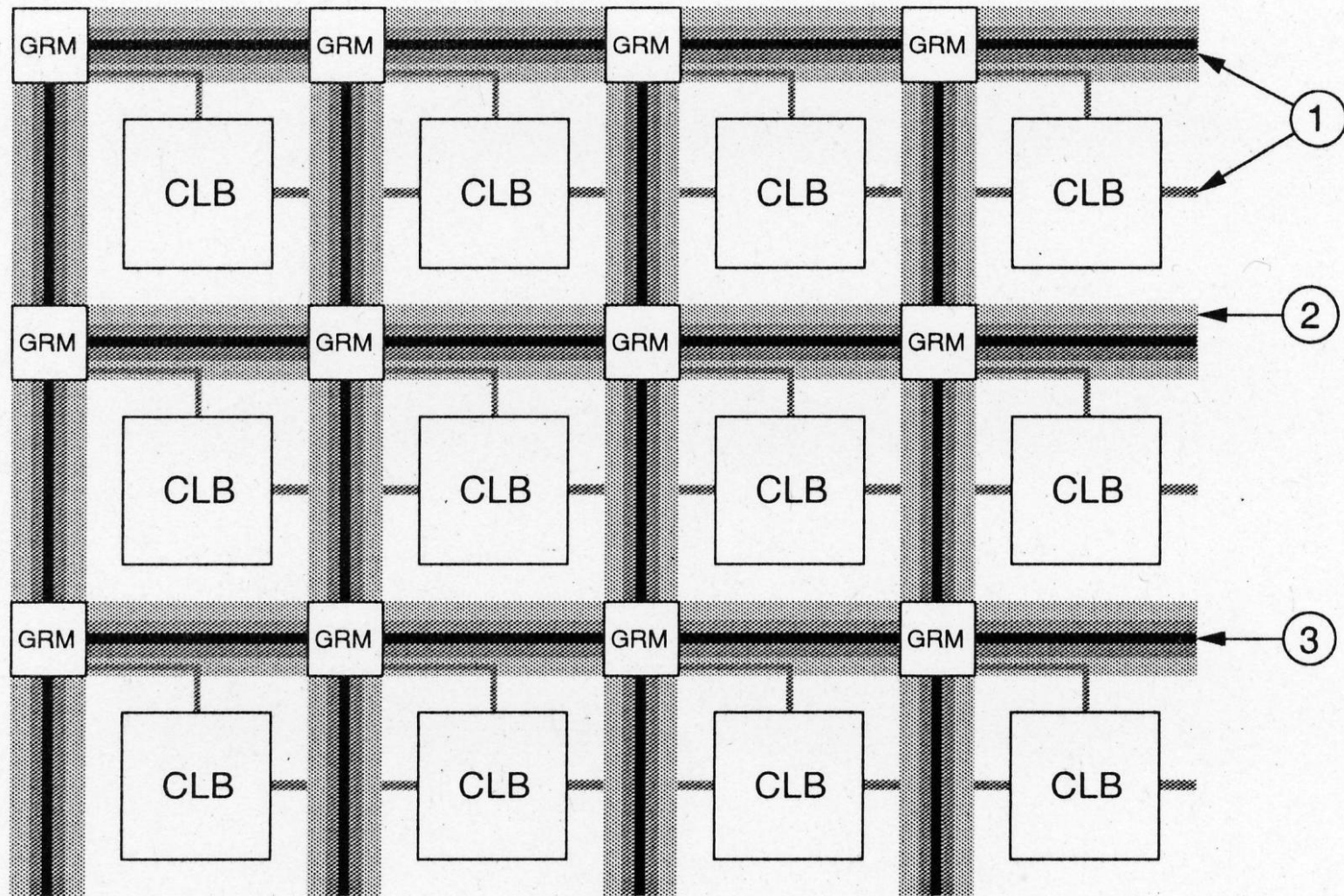
Special: Inversion is very cheap.

Instead of addition chains we consider addition-subtraction chains (Morain & Olivos 1990).

Brauer's window method gives only a small improvement.







Summary

- efficient exponentiation

Summary

- efficient exponentiation
- application: cryptography

Summary

- efficient exponentiation
- application: cryptography
- appropriate data structures

Summary

- efficient exponentiation
- application: cryptography
- appropriate data structures
- software/hardware

Summary

- efficient exponentiation
- application: cryptography
- appropriate data structures
- software/hardware