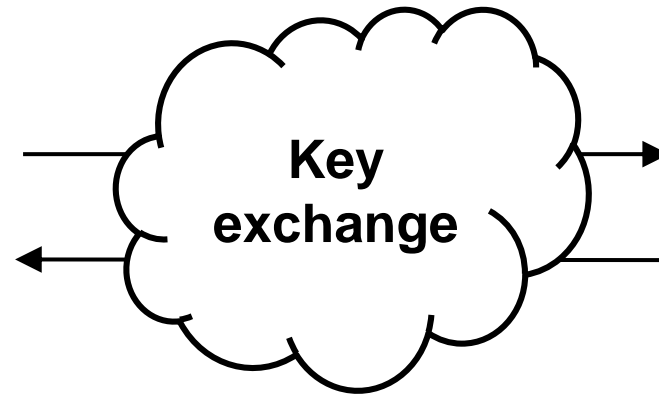
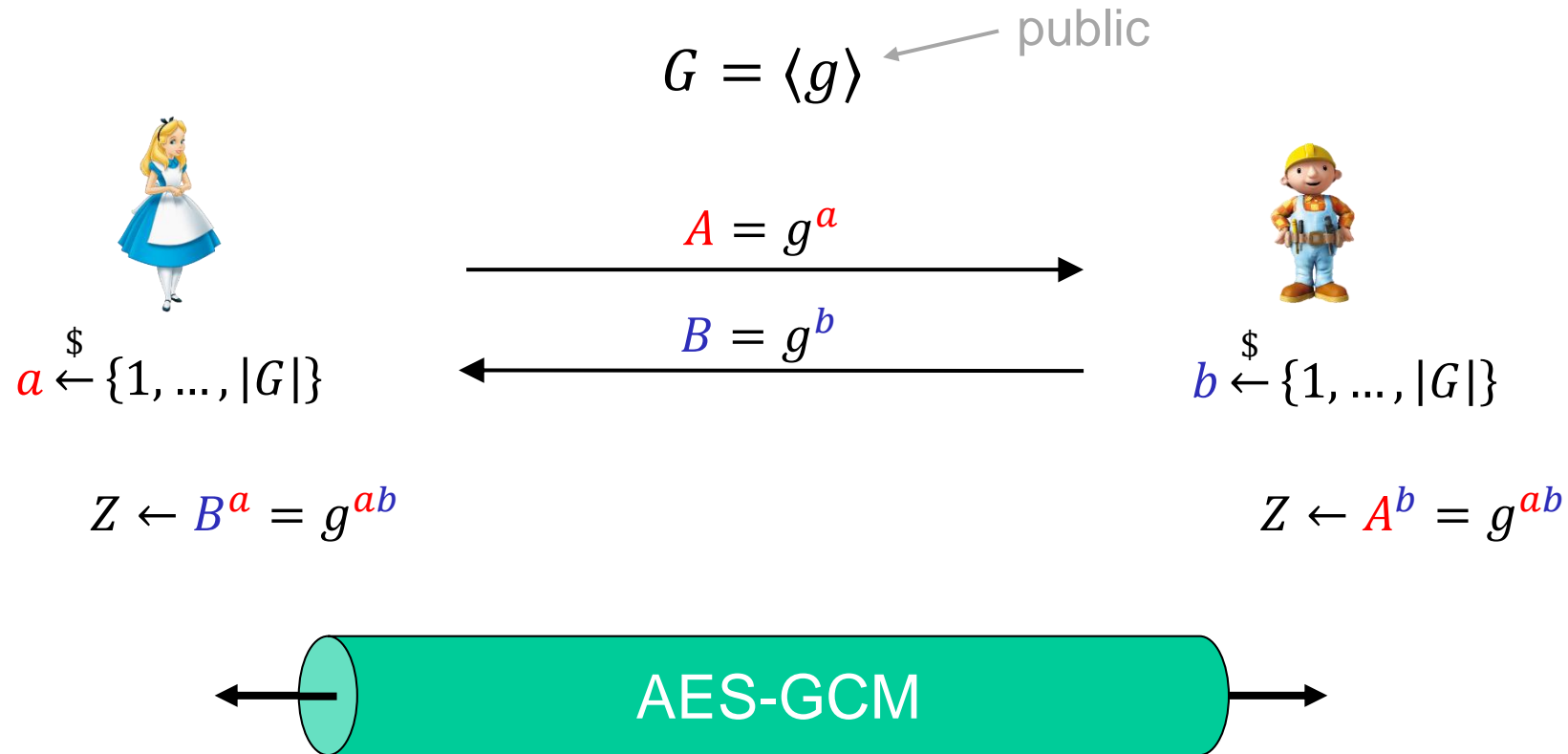

Diffie-Hellman key exchange II, computational aspects

Diffie-Hellman



Diffie-Hellman



Examples:

$$G = (\mathbb{Z}_p^*, \cdot)$$

$$G = (E(\mathbb{Z}_p), +)$$

Why is (\mathbf{Z}_p^*, \cdot) a group?

- $\mathbf{Z}_p^* = \{1, 2, \dots, p - 1\}$
- Associativity ✓ $(a \cdot b) \cdot c = a \cdot (b \cdot c) \pmod p$
- Identity ✓ $1 \cdot a = a \cdot 1 = a \pmod p$
- Inverses ?

Definition: A group (G, \circ) ...

- $\mathcal{G}1: (a \circ b) \circ c = a \circ (b \circ c)$ (associativity)
- $\mathcal{G}2: \exists e \in G: e \circ a = a \circ e = a$ (identity)
- $\mathcal{G}3: \exists a^{-1} \in G: a \circ a^{-1} = a^{-1} \circ a = e$ (inverses)

Given $a \in \mathbf{Z}_p^*$ can we always find $a^{-1} \in \mathbf{Z}_p^*$?

Need to solve: $a \cdot x = 1 \pmod p$

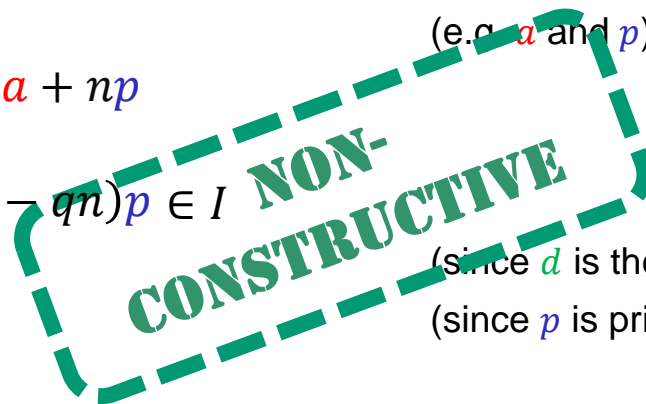
Claim: $\exists m, n \in \mathbf{Z}$ such that $ma + np = 1 \implies ma = 1 - np = 1 \pmod p$
 $\implies a^{-1} = m \pmod p \in \mathbf{Z}_p^*$

Proof: $I = \{sa + tp \mid s, t \in \mathbf{Z}\}$

- 1) I contains a *positive* integer
- 2) I contains a *smallest* positive integer $d = ma + np$
- 3) $p = qd + r$ $0 \leq r < d$
- 4) $r = p - qd = p - q(ma + np) = -qma + (1 - qn)p \in I$
- 5) $r = 0$
- 6) $p = qd \implies d = 1$
- 7) $1 = ma + np$

Q.E.D

How to actually find a^{-1} ?
 Extended Euclidian Algorithm



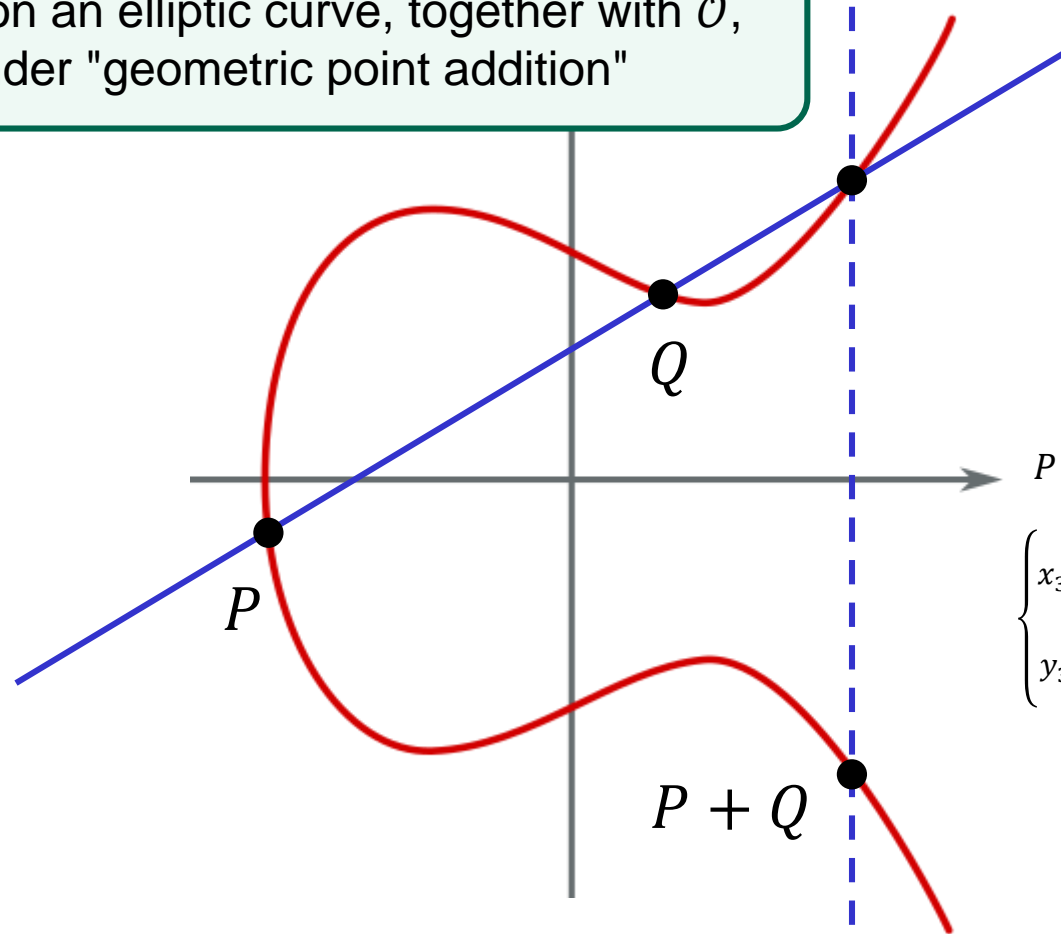
(e.g. a and p)

(since d is the smallest positive integer in I)

(since p is prime and $d \leq a < p$)

Elliptic curves

Theorem: the points on an elliptic curve, together with \mathcal{O} , is an abelian group under "geometric point addition"



$$y^2 = x^3 + ax + b$$

$$a, b, x, y \in \mathbf{Z}_p$$

$$P + Q = (x_1, y_1) + (x_2, y_2) = (x_3, y_3)$$

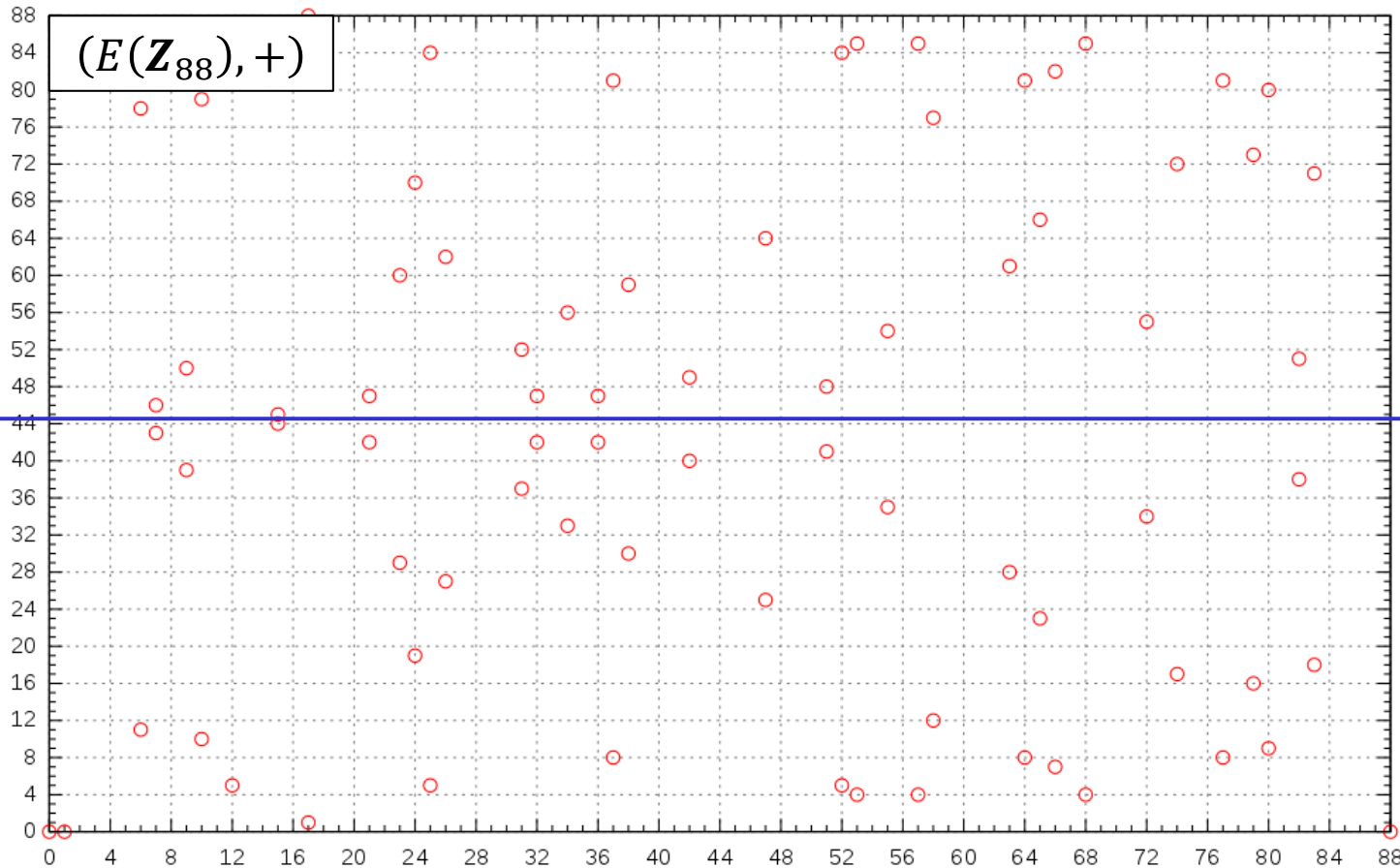
$$\begin{cases} x_3 = \frac{(x_1x_2 - 2a)x_1x_2 - 4b(x_1 + x_2) + a^2}{(x_1x_2 + a)(x_1 + x_2) + 2y_1y_2 + 2b} \\ y_3 = \frac{x_1x_2(x_1 + x_2) - x_3((x_1 + x_2)^2 - x_1x_2 + a) - y_1y_2 - b}{y_1 + y_2} \end{cases}$$

Still valid!

Elliptic curves over finite fields

Theorem: the points on an elliptic curve, together with \mathcal{O} , is an abelian group under "geometric point addition"

Notation: $(E(\mathbf{Z}_p), +)$ = an elliptic curve group defined over \mathbf{Z}_p



$$y^2 = x^3 + ax + b \pmod{p}$$

$$a, b, x, y \in \mathbf{Z}_{88}$$

$$P + Q = (x_1, y_1) + (x_2, y_2) = (x_3, y_3)$$

$$\begin{cases} x_3 = \frac{(x_1x_2 - 2a)x_1x_2 - 4b(x_1 + x_2) + a^2}{(x_1x_2 + a)(x_1 + x_2) + 2y_1y_2 + 2b} \\ y_3 = \frac{x_1x_2(x_1 + x_2) - x_3((x_1 + x_2)^2 - x_1x_2 + a) - y_1y_2 - b}{y_1 + y_2} \end{cases}$$

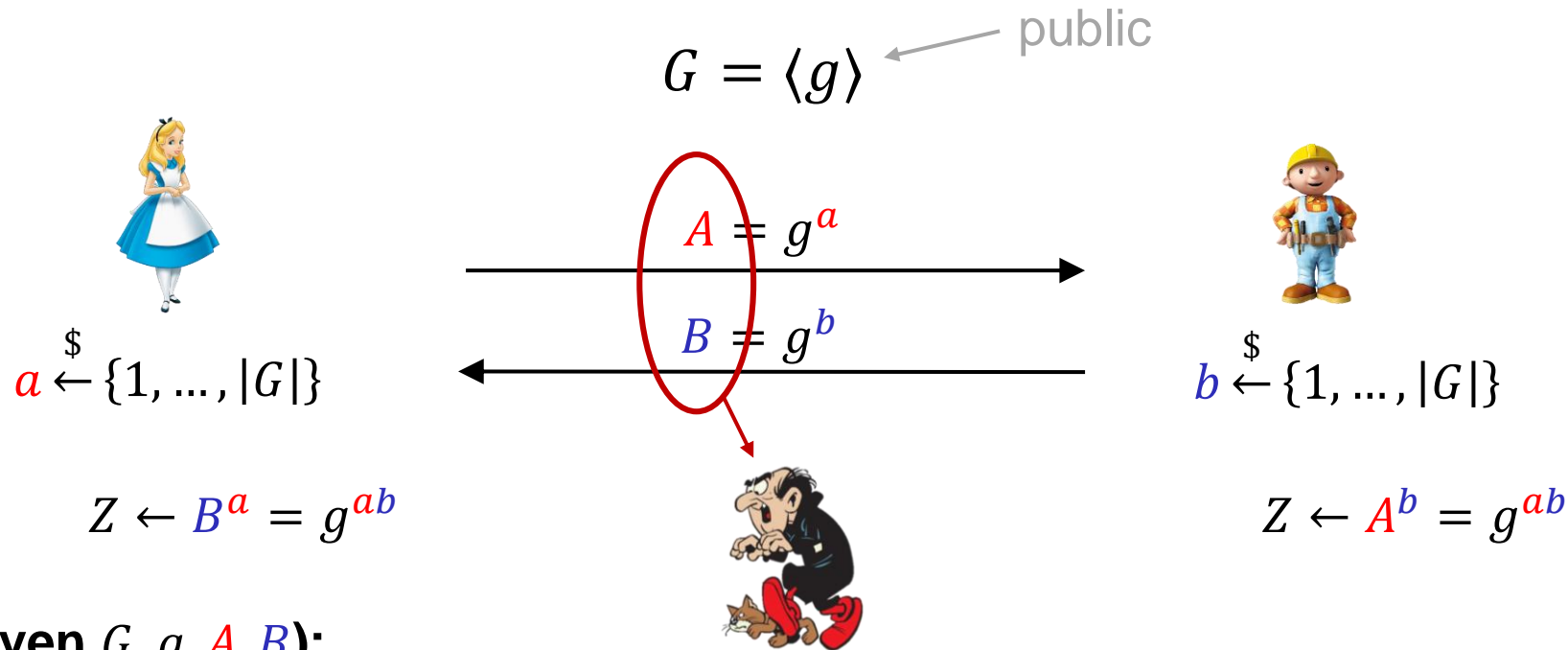
Both addition *and* multiplication needed mod p

Need $(\mathbf{Z}_p, +)$ *and* (\mathbf{Z}_p^*, \cdot)



Finite field: $(F_p, +, \cdot)$

Diffie-Hellman – security



Security (given G, g, A, B):

- Must be hard to compute $Z \leftarrow g^{ab}$
- Must be hard to find a (or b)
- $G = (\mathbf{Z}_p, +)$
- $G = (\mathbf{Z}_p^*, \cdot)$
- $G = (E(\mathbf{F}_p), +)$

(DH assumption)

(DLOG assumption)

not secure

secure* for p large enough (conjectured)

secure* for $|E(\mathbf{F}_p)|$ large enough (conjectured)

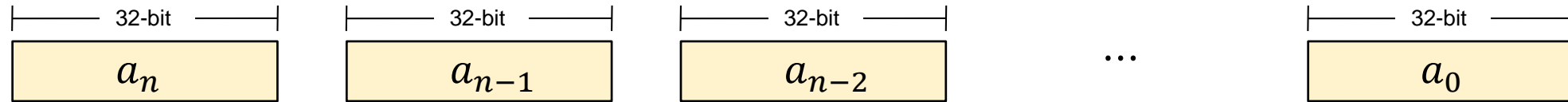
*Many caveats

Large enough?

$p =$ 171254583176141379301960419792575778264088323240375085733932929816426671
397476217788024387752387285929683446135893799323484756135034769321631669
738132186983438164632891441853629126025225404949830905314972329658295365
245072698488256583114202993359222957097432675083225259667739503949192575 $\approx 2^{2048}$
768420387716327420441424710535098501236058838158571626669177751934961573
726561955583057270098912760065140004093658772181713883199238963093777917
625906143118496429613802248519404604217104493689272529748703958739363879
096722748832953774810081504758785902705917983505634881680809238046118223
87520198054002990623911454389104774092183

Big-number arithmetic

$a = 2048\text{-bit integer, } 64\text{-bit CPU}$



Algorithm	Input	Output	Time
ADD	a, b	$a + b$	$\mathcal{O}(n)$
MULT	a, b	ab	$\mathcal{O}(n^2)$
INT-DIV	a, b	(q, r) s.t. $a = qb + r$ and $0 \leq r < b$	$\mathcal{O}(n^2)$
MOD	a, p	$a \bmod p$	$\mathcal{O}(n^2)$
MOD-INV	$a \in \mathbf{Z}_p^*$	$a^{-1} \in \mathbf{Z}_p^*$	$\mathcal{O}(n^2)$

$\mathcal{O}(n \log n)^*$

*all numbers are n bits

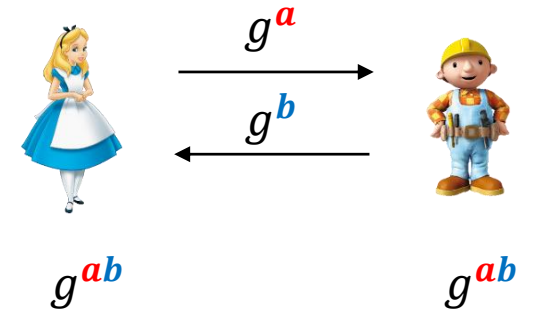
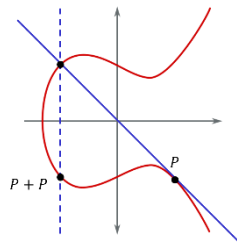
* $n > 2^{713739807325663489766475852620783120641}$

Diffie-Hellman – computations

- (\mathbf{Z}_p^*, \cdot)
 - Find prime p (one-time)
 - Find generator $\langle g \rangle = (\mathbf{Z}_p^*, \cdot)$ (one-time)
 - Compute $g^a = gg \cdots g \pmod p$
 - Multiply $x \cdot y \pmod p$

Group exponentiation g^a

- $(E(\mathbf{F}_p), +)$
 - Find prime p (one-time)
 - Generate curve $y^2 = x^3 + ax + b \pmod p$ (one-time)
 - Find curve group order $|E(\mathbf{F}_p)|$ (one-time)
 - Find generator P (one-time)
 - Compute $aP = P + P + \cdots + P$
 - Point addition



Diffie-Hellman – in (\mathbb{Z}_p^*, \cdot)

$p =$ 17125458317614137930196041979257577826408832324037508573393292981642667139747621778802438775238728592968344613589379932348475613503476932163166973813218698343816463289144185362912602522540494983090531497232965829
 53652450726984882565831142029933592229570974326750832252596677395039491925757684203877163274204414247105350985012360588381585716266691777519349615737265619555830572700989127600651400040936587721817138831992389630
 937779176259061431184964296138022485194046042171044936892725297487039587393687909672274883295377481008150475878590270591798350563488168080923804611822387520198054002990623911454389104774092183



$A = 2$

$\text{mod } p$



323170060713110073003389139264238282488179412411402391
 128420097514007417066343542226196894173635693471179017
 379097041917546058732091950288537589861856221532121754
 125149017745202702357960782362488842461894775876411059
 286460994117232454266225221932305409190376805242355191
 256797158701170010580558776510388618472802579760549035
 697325615261670813393617995413364765591603683178967290
 731783845896806396719009772021941686472258710314113364
 293195361934716365332097170774482279885885653692086452
 96636077250268955059283627511211740969729980684105543
 595848665832916421362182310789909994486524682624169720
 35911852507045361090559

$\$ \leftarrow \{1 \dots p\}$

665680077810100734070476416898417408020670352441378967
 997224101900193957211854827569676933273935982997835638
 067380762809024311842715496660113976613131478051784487
 322446809608196031803691263486170912693625523249742383
 264476433978409434004770395167011614217279552198029936
 108023398643999746539201834933168220864789880837484536
 56306799776127082664223539437541791058416731683176995
 365899867720283590420932417377927106884773199080517477
 615608675490982255098980545292032908358093913531433702
 049429047413071525556307299541445514389721222256380833
 743627991333762777307118317040885305789910094293548481
 5501309561942770687524

$B = 2$

$\text{mod } p$



665680077810100734070476416898417408020670352441378967
 997224101900193957211854827569676933273935982997835638
 067380762809024311842715496660113976613131478051784487
 322446809608196031803691263486170912693625523249742383
 264476433978409434004770395167011614217279552198029936
 108023398643999746539201834933168220864789880837484536
 56306799776127082664223539437541791058416731683176995
 365899867720283590420932417377927106884773199080517477
 615608675490982255098980545292032908358093913531433702
 049429047413071525556307299541445514389721222256380833
 743627991333762777307118317040885305789910094293548481
 5501309561942770687524

$\$ \leftarrow \{1 \dots p\}$

323170060713110073003389139264238282488179412411402391
 128420097514007417066343542226196894173635693471179017
 379097041917546058732091950288537589861856221532121754
 125149017745202702357960782362488842461894775876411059
 286460994117232454266225221932305409190376805242355191
 256797158701170010580558776510388618472802579760549035
 697325615261670813393617995413364765591603683178967290
 731783845896806396719009772021941686472258710314113364
 293195361934716365332097170774482279885885653692086452
 96636077250268955059283627511211740969729980684105543
 595848665832916421362182310789909994486524682624169720
 35911852507045361090559

\times

665680077810100734070476416898417408020670352441378967
 997224101900193957211854827569676933273935982997835638
 067380762809024311842715496660113976613131478051784487
 322446809608196031803691263486170912693625523249742383
 264476433978409434004770395167011614217279552198029936
 108023398643999746539201834933168220864789880837484536
 56306799776127082664223539437541791058416731683176995
 365899867720283590420932417377927106884773199080517477
 615608675490982255098980545292032908358093913531433702
 049429047413071525556307299541445514389721222256380833
 743627991333762777307118317040885305789910094293548481
 5501309561942770687524

$Z \leftarrow 2$

$\text{mod } p$

Recall

Theorem: if (G, \circ) is a finite group, then for all $g \in G$:

$$g^{|G|} = e$$

Corollary I: $g^i = g^{i \bmod |G|}$

Corollary II (Lagrange's theorem):

if $H < G$ then the order of H divides the order of G (i.e. $|H| \mid |G|$)

Diffie-Hellman – in a *subgroup* of (\mathbb{Z}_p^*, \cdot)

$p =$ 17125458317614137930196041979257577826408832324037508573393292981642667139747621778802438775238728592968344613589379932348475613503476932163166973813218698343816463289144185362912602522540494983090531497232965829
53652450726984882565831142029933592229570974326750832252596677395039491925757684203877163274204414247105350985012360588381585716266691777519349615737265619555830572700989127600651400040936587721817138831992389630
9377791762590614311849642961380224851940460421710449368927252974870395873936387909672274883295377481008150475878590270591798350563488168080923804611822387520198054002990623911454389104774092183

$$= 2 \cdot 7 \cdot 13 \cdot q_1 \cdot q_2 \cdot q_3 \cdot q_4 \cdot q_5 + 1$$

323170060713110073003389139264238282488179412411402391
128420097514007417066343542226196894173635693471179017
379097041917546058732091950288537589861856221532121754
125149017745202702357960782362488842461894775876411059
286460994117232454266225221932305409190376805242355191
256797158701170010580558776510388618472802579760549035
697325615261670813393617995413364765591603683178967290
731783845896806396719009772021941686472258710314113364
293195361934716365332097170774482279885885653692086452
966360772502689555059283627511211740969729980684105543
595848665832916421362182310789909994486524682624169720
35911852507045361090559

$$|\mathbb{Z}_p^*| = p - 1$$

$$H = \langle g \rangle < (\mathbb{Z}_p^*, \cdot)$$



$$|H| = q_4 \approx 2^{256}$$

63762351364972653564641699
52920551048926326683418277
1617563631363277932854227

$$A = 2$$

$$\text{mod } p$$



323170060713110073003389139264238282488179412411402391
128420097514007417066343542226196894173635693471179017
379097041917546058732091950288537589861856221532121754
~~320570037040027003259640782362488842461894775876411059~~
~~88606099649032757256185221932305409190376805242355191~~
256797158701170010580558776510388618472802579760549035
697325615261670813393617995413364765591603683178967290
731783845896806396719009772021941686472258710314113364
293195361934716365332097170774482279885885653692086452
966360772502689555059283627511211740969729980684105543
595848665832916421362182310789909994486524682624169720
35911852507045361090559

\$ ← {1 ... p-1}

665680077810100734070476416898417408020670352441378967
997224101900193957211854827569676933273935982997835638
067380762809024311842715496660113976613131478051784487
322446809608196031803691263486170912693625523249742383
264476433978409434004770395167011614217279552198029936
108023398643999746539201834933168220864789880837484536
563067997761270826642223539437541791058416731683176995
365899867720283590420932417377927106884773199080517477
615608675490982255098980545292032908358093913531433702
049429047413071525556307299541445514389721222256380833
743627991333762777307118317040885305789910094293548481
5501309561942770687524

665680077810100734070476416898417408020670352441378967
997224101900193957211854827569676933273935982997835638
067380762809024311842715496660113976613131478051784487
322446809608196031803691263486170912693625523249742383
264476433978409434004770395167011614217279552198029936
108023398643999746539201834933168220864789880837484536
563067997761270826642223539437541791058416731683176995
365899867720283590420932417377927106884773199080517477
615608675490982255098980545292032908358093913531433702
049429047413071525556307299541445514389721222256380833
743627991333762777307118317040885305789910094293548481
5501309561942770687524

\$ ← {1 ... p-1}

$$B = 2$$

$$\text{mod } p$$

Corollary I: $g^i = g^i \text{ mod } |H|$

323170060713110073003389139264238282488179412411402391
128420097514007417066343542226196894173635693471179017
379097041917546058732091950288537589861856221532121754
125149017745202702357960782362488842461894775876411059
286460994117232454266225221932305409190376805242355191
256797158701170010580558776510388618472802579760549035
697325615261670813393617995413364765591603683178967290
731783845896806396719009772021941686472258710314113364
293195361934716365332097170774482279885885653692086452
966360772502689555059283627511211740969729980684105543
595848665832916421362182310789909994486524682624169720
35911852507045361090559

×

665680077810100734070476416898417408020670352441378967
997224101900193957211854827569676933273935982997835638
067380762809024311842715496660113976613131478051784487
322446809608196031803691263486170912693625523249742383
264476433978409434004770395167011614217279552198029936
108023398643999746539201834933168220864789880837484536
563067997761270826642223539437541791058416731683176995
365899867720283590420932417377927106884773199080517477
615608675490982255098980545292032908358093913531433702
049429047413071525556307299541445514389721222256380833
743627991333762777307118317040885305789910094293548481
5501309561942770687524

$$Z \leftarrow 2$$

$$\text{mod } p$$

Diffie-Hellman – in a *subgroup* of (\mathbb{Z}_p^*, \cdot)

$$p = 17125458317614137930196041979257577826408832324037508573393292981642667139747621778802438775238728592968344613589379932348475613503476932163166973813218698343816463289144185362912602522540494983090531497232965829536524507269848825658311420299335922295709743267508322525966773950394919257576842038771632742044142471053509850123605883815857162666917775193496157372656195558305727009891276006514000409365877218171388319923896309377791762590614311849642961380224851940460421710449368927252974870395873936387909672274883295377481008150475878590270591798350563488168080923804611822387520198054002990623911454389104774092183$$

$$= 2 \cdot 7 \cdot 13 \cdot q_1 \cdot q_2 \cdot q_3 \cdot q_4 \cdot q_5 + 1$$

$$H = \langle g \rangle < (\mathbb{Z}_p^*, \cdot)$$

$$|H| = q_4 \approx 2^{256}$$

$$= 63762351364972653564641699529205510489263266834182771617563631363277932854227$$



$$A = g \pmod p$$

370576434640964440325841778231810282485808459400109374
87506489964963471715816



370576434640964440325841778231810282485808459400109374
87506489964963471715816

$\$ \leftarrow \{1 \dots q_4\}$

291776417284848832780691521970891380020649297877535257
36186058877137490281835

$\$ \leftarrow \{1 \dots q_4\}$

$$B = g \pmod p$$

291776417284848832780691521970891380020649297877535257
36186058877137490281835

Corollary I: $g^i = g^{i \pmod{|H|}}$

3231700607131100730033891392642382824881794124114023911284200975140074170663435422261968941736356934711790173790970419175460587320919502885375898618562215321217541251490177452027023579607823624888424618947758764110592864609941172324542662252219323054091903768052423551912567971587011700105805587765103886184728025797605490356973256152616708133936179954133647655916036831789672907317838458968063967190097720219416864722587103141133642931953619347163653320971707744822798858856536920864529663607725026895505928362751121174096972998068410554359584866583291642136218231078990999448652468262416972035911852507045361090559

\times

6656800778101007340704764168984174080206703524413789679972241019001939572118548275696769332739359829978356380673807628090243118427154966601139766131314780517844873224468096081960318036912634861709126936255232497423832644764339784094340047703951670116142172795521980299361080233986439997465392018349331682208647898808374845365630679977612708266422353943754179105841673168317699536589986772028359042093241737792710688477319908051747761560867549098225509898054529203290835809391353143370204942904741307152556307299541445514389721222563808337436279913337627773071183170408853057899100942935484815501309561942770687524

$Z \leftarrow 2$

$\pmod p$

Diffie-Hellman – in a *subgroup* of (\mathbb{Z}_p^*, \cdot)

$$p = 17125458317614137930196041979257577826408832324037508573393292981642667139747621778802438775238728592968344613589379932348475613503476932163166973813218698343816463289144185362912602522540494983090531497232965829536524507269848825658311420299335922295709743267508322525966773950394919257576842038771632742044142471053509850123605883815857162666917775193496157372656195558305727009891276006514000409365877218171388319923896309377791762590614311849642961380224851940460421710449368927252974870395873936387909672274883295377481008150475878590270591798350563488168080923804611822387520198054002990623911454389104774092183$$

$$= 2 \cdot 7 \cdot 13 \cdot q_1 \cdot q_2 \cdot q_3 \cdot q_4 \cdot q_5 + 1$$

$$H = \langle g \rangle < (\mathbb{Z}_p^*, \cdot)$$

$$|H| = q_4 \approx 2^{256}$$

$$= 63762351364972653564641699529205510489263266834182771617563631363277932854227$$



$$A = g \pmod p$$



37057643464096444032584177823181028248580845940010937487506489964963471715816

$\$ \leftarrow \{1 \dots q_4\}$

29177641728484883278069152197089138002064929787753525736186058877137490281835

$\$ \leftarrow \{1 \dots q_4\}$

$$B = g \pmod p$$

Corollary I: $g^i = g^{i \bmod |H|}$

$$Z \leftarrow g \times \pmod p$$

Computing in groups – exponentiation

Goal: compute $g^n \in G$

Naïve approach: $g^n = \overbrace{g \circ g \circ g \circ \cdots \circ g}^n$

- Running time: $n \approx 2^k \Rightarrow 2^k$ group operations!
- Doesn't work for exponent sizes used in cryptography

Computing in groups – exponentiation; square-and-multiply

Goal: compute $g^n \in G$

$$\begin{aligned}n &= (b_5 b_4 b_3 b_2 b_1 b_0)_2 \\ &= 2^5 b_5 + 2^4 b_4 + 2^3 b_3 + 2^2 b_2 + 2^1 b_1 + 2^0 b_0\end{aligned}$$

$$y_6 \leftarrow e$$

$$y_5 \leftarrow y_6^2 \circ g^{b_5} = g^{b_5}$$

$$y_4 \leftarrow y_5^2 \circ g^{b_4} = g^{2b_5 + b_4}$$

$$y_3 \leftarrow y_4^2 \circ g^{b_3} = g^{2^2 b_5 + 2b_4 + b_3}$$

$$y_2 \leftarrow y_3^2 \circ g^{b_2} = g^{2^3 b_5 + 2^2 b_4 + 2b_3 + b_2}$$

$$y_1 \leftarrow y_2^2 \circ g^{b_1} = g^{2^4 b_5 + 2^3 b_4 + 2^2 b_3 + 2b_2 + b_1}$$

$$y_0 \leftarrow y_1^2 \circ g^{b_0} = g^{2^5 b_5 + 2^4 b_4 + 2^3 b_3 + 2^2 b_2 + 2b_1 + b_0}$$

$$\begin{aligned}43 &= 101011_2 \\ &= 2^5 + 2^3 + 2^1 + 2^0\end{aligned}$$

$$y_6 \leftarrow e$$

$$y_5 \leftarrow y_6^2 \circ g^1 = g^1$$

$$y_4 \leftarrow y_5^2 \circ g^0 = g^2$$

$$y_3 \leftarrow y_4^2 \circ g^1 = g^{4+1} = g^5$$

$$y_2 \leftarrow y_3^2 \circ g^0 = g^{10}$$

$$y_1 \leftarrow y_2^2 \circ g^1 = g^{20+1} = g^{21}$$

$$y_0 \leftarrow y_1^2 \circ g^1 = g^{42+1} = g^{43}$$

Computing in groups – exponentiation; square-and-multiply

Goal: compute $g^n \in G$

$$\begin{aligned}n &= (b_5 b_4 b_3 b_2 b_1 b_0)_2 \\ &= 2^5 b_5 + 2^4 b_4 + 2^3 b_3 + 2^2 b_2 + 2^1 b_1 + 2^0 b_0\end{aligned}$$

$$\begin{aligned}43 &= 101011_2 \\ &= 2^5 + 2^3 + 2^1 + 2^0\end{aligned}$$

$$y_6 \leftarrow e$$

$$y_5 \leftarrow y_6^2 \circ g^{b_5} = g^{b_5}$$

$$y_4 \leftarrow y_5^2 \circ g^{b_4} = g^{2b_5 + b_4}$$

$$y_3 \leftarrow y_4^2 \circ g^{b_3} = g^{2^2 b_5 + 2b_4 + b_3}$$

$$y_2 \leftarrow y_3^2 \circ g^{b_2} = g^{2^3 b_5 + 2^2 b_4 + 2b_3 + b_2}$$

$$y_1 \leftarrow y_2^2 \circ g^{b_1} = g^{2^4 b_5 + 2^3 b_4 + 2^2 b_3 + 2b_2 + b_1}$$

$$y_0 \leftarrow y_1^2 \circ g^{b_0} = g^{2^5 b_5 + 2^4 b_4 + 2^3 b_3 + 2^2 b_2 + 2b_1 + b_0}$$

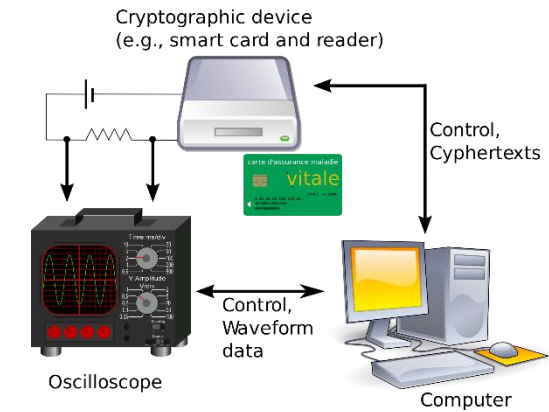
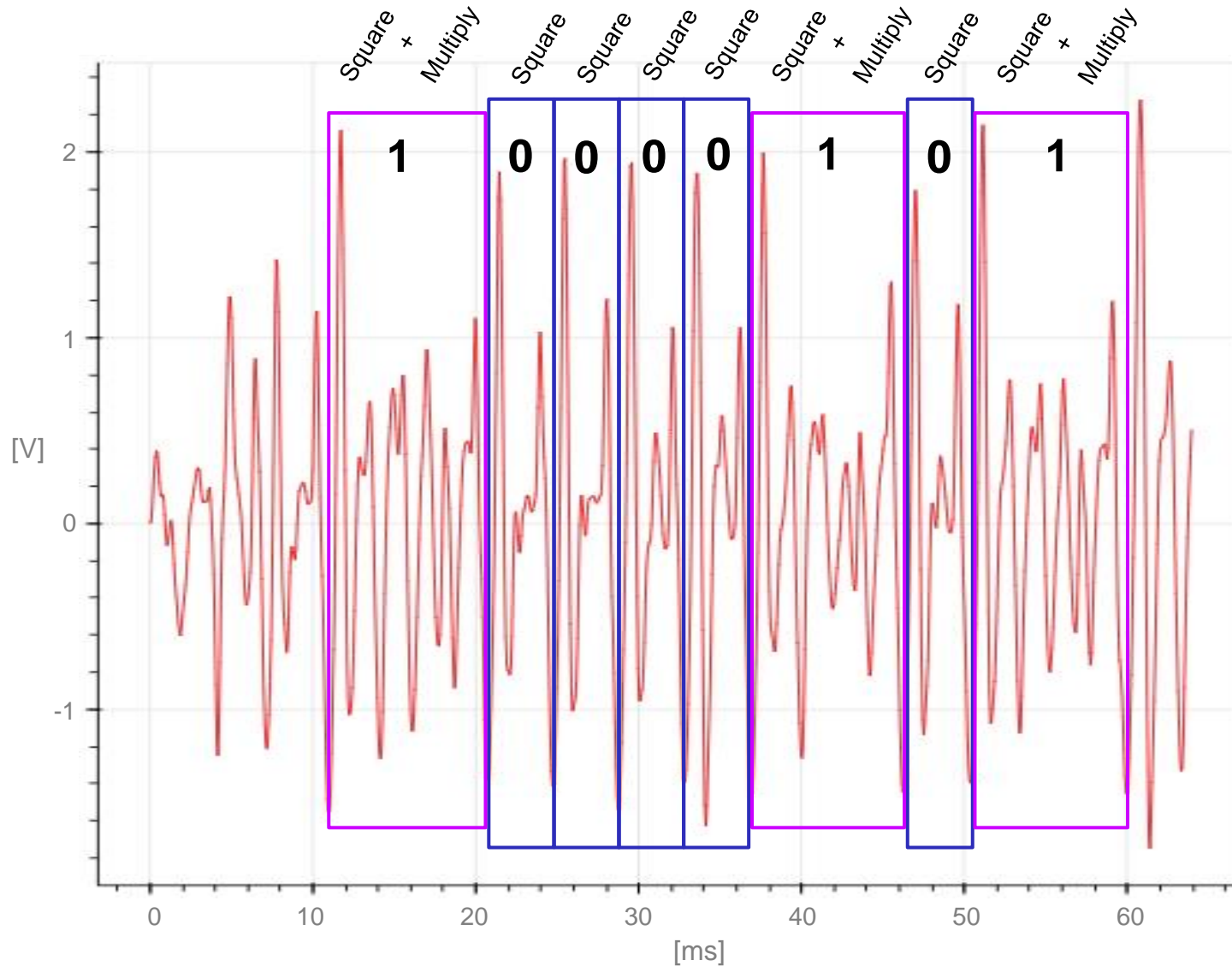
Square-and-Multiply($g \in G, n \in \mathbb{Z}$)

1. if $n < 0$ then $g \leftarrow g^{-1}$ and $n \leftarrow |n|$
2. $n = (b_{t-1} \dots b_1 b_0)_2$
3. $y \leftarrow e$
4. for $i = t - 1$ downto 0 do
5. $y \leftarrow y^2 \circ g^{b_i}$
- 6.
7. return y

Square-and-multiply

- (\mathbf{Z}_p^*, \cdot)
 - Naïve exponentiation: $\mathcal{O}(n) \approx p$
 - Square-and-multiply: $\mathcal{O}(t) = \mathcal{O}(\log_2 n) \approx \log_2 p$
 - $\approx 2^{2048}$ vs. ≈ 2048 multiplications for $p \approx 2^{2048}$
- Prime-order subgroup $H < (\mathbf{Z}_p^*, \cdot)$
 - Naïve exponentiation: $\mathcal{O}(n) \approx q$
 - Square-and-multiply: $\mathcal{O}(t) = \mathcal{O}(\log_2 n) \approx \log_2 q$
 - $\approx 2^{256}$ vs. ≈ 256 multiplications for $q \approx 2^{256}$ and $p \approx 2^{2048}$
- $(E(\mathbf{F}_p), +)$
 - Naïve "exponentiation" (i.e., point multiplication nP): $\mathcal{O}(n) \approx |E(\mathbf{F}_p)|$
 - "Square-and-multiply" (i.e., double-and-add): $\mathcal{O}(t) = \mathcal{O}(\log_2 n) \approx \log_2 |E(\mathbf{F}_p)|$
 - $\approx 2^{256}$ vs. ≈ 256 elliptic-curve additions for NIST P-256 or Curve25519

Side-channel attacks – power analysis



Square-and-Multiply($g \in G, n \in \mathbb{Z}$)

1. **if** $n < 0$ **then** $g \leftarrow g^{-1}$ and $n \leftarrow |n|$
2. $n = (b_{t-1} \dots b_1 b_0)_2$
3. $y \leftarrow e$
4. **for** $i = t - 1$ **downto** 0 **do**
5. $y \leftarrow y^2$
6. **if** $b_i = 1$ **then**
7. $y \leftarrow y \circ g$
8. **return** y

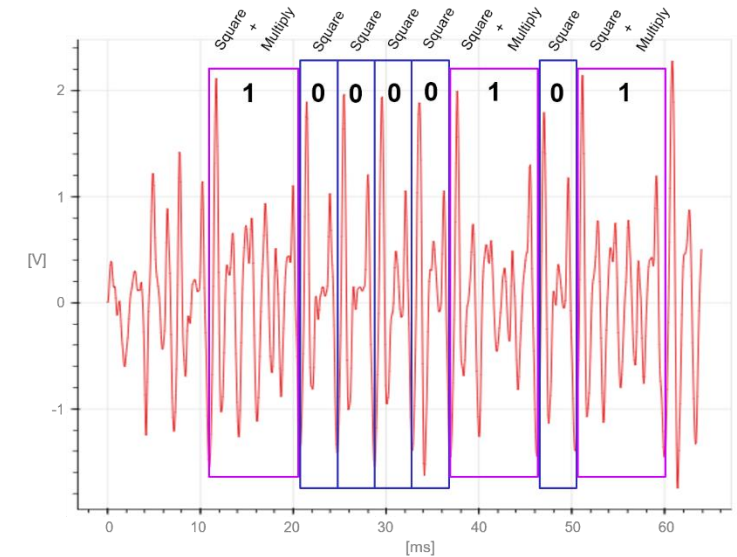
Mitigations

- Power (and time) difference between $b_i = 0$ and $b_i = 1$
- Solution: Square-and-*A*ways-Multiply

Square-and-always-Multiply($g \in G, n \in \mathbb{Z}$)

1. **if** $n < 0$ **then** $g \leftarrow g^{-1}$ and $n \leftarrow |n|$
2. $n = (b_{t-1} \dots b_1 b_0)_2$
3. $y \leftarrow e$
4. **for** $i = t - 1$ **downto** 0 **do**
5. $y \leftarrow y^2$
6. $z \leftarrow y \circ g$ // always perform multiplication
7. **if** $b_i = 1$ **then**
8. $y \leftarrow z$
9. **return** y

- Wastes computations: $\approx t/2$ of multiplications thrown away
- Better solutions: Montgomery ladders



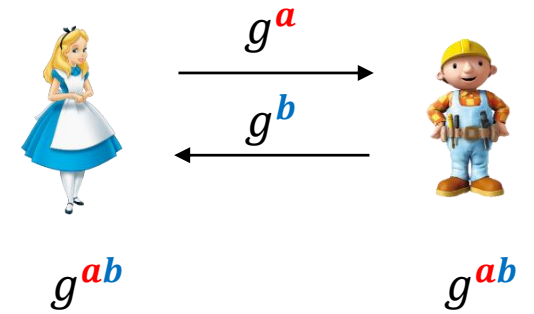
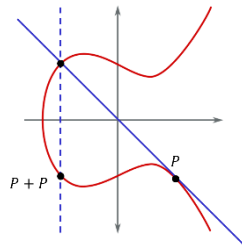
Square-and-Multiply($g \in G, n \in \mathbb{Z}$)

1. **if** $n < 0$ **then** $g \leftarrow g^{-1}$ and $n \leftarrow |n|$
2. $n = (b_{t-1} \dots b_1 b_0)_2$
3. $y \leftarrow e$
4. **for** $i = t - 1$ **downto** 0 **do**
5. $y \leftarrow y^2$
6. **if** $b_i = 1$ **then**
7. $y \leftarrow y \circ g$
8. **return** y

Diffie-Hellman – computations

- (\mathbf{Z}_p^*, \cdot)
 - Find prime p (one-time)
 - Find generator $\langle g \rangle = (\mathbf{Z}_p^*, \cdot)$ (one-time)
 - Compute $g^a = gg \cdots g \pmod p$
 - Multiply $x \cdot y \pmod p$

- $(E(\mathbf{F}_p), +)$
 - Find prime p (one-time)
 - Generate curve $y^2 = x^3 + ax + b \pmod p$ (one-time)
 - Find curve group order $|E(\mathbf{F}_p)|$ (one-time)
 - Find generator P (one-time)
 - Compute $aP = P + P + \cdots + P$
 - Point addition



Finding prime numbers

- We need *large* prime numbers
 - Both for (\mathbf{Z}_p^*, \cdot) and $(E(\mathbf{F}_p), +)$
- No efficient "prime-generating" formula is known
- Simple idea: pick random number and check if it's prime
- Efficient? \Rightarrow What is the success probability?
 - Depends on the ratio primes / non-primes
 - $\pi(n)$ = "#prime numbers $\leq n$ "
 - Prime Number Theorem:** $\frac{\pi(n)}{n} \approx \frac{1}{\ln n}$
 - 2048-bit number: ≈ 700 trials needed

GenPrime(k)

```

1.  while true do
2.       $n \leftarrow$  odd  $k$ -bit integer
3.      if IsPrime( $n$ ) = PRIME then
4.          return  $n$ 
    
```

$$n \approx 2^{2048} \Rightarrow \frac{\pi(n)}{n} \approx \frac{1}{\ln 2^{2048}} \approx \frac{1}{1400}$$

n	100	1000	10^6	10^9	10^{12}	10^{15}
$\pi(n)$	25	168	$\approx 78 \cdot 10^3$	$\approx 50 \cdot 10^6$	$\approx 30 \cdot 10^9$	$\approx 29 \cdot 10^{12}$

Finding prime numbers

- We need *large* prime numbers
 - Both for (\mathbf{Z}_p^*, \cdot) and $(E(\mathbf{F}_p), +)$
- Naïve IsPrime(n):
 - 3 divides n ? Not prime
 - 5 divides n ? Not prime
 - 7 divides n ? Not prime
 - \vdots
 - $\lfloor \sqrt{n} \rfloor$ divides n ? Not prime
 - n is prime!
- *Very* inefficient: $n \approx 2^k \implies \pi(n) \approx \frac{2^k}{\ln 2^k} \approx \frac{2^k}{k}$
- Want: a simple property which *only* holds for prime numbers

GenPrime(k)

```
1.  while true do
2.       $n \stackrel{\$}{\leftarrow}$  odd  $k$ -bit integer
3.      if IsPrime( $n$ ) = PRIME then
4.          return  $n$ 
```


Fermat's theorem

Theorem: if (G, \circ) is a finite group, then for all $g \in G$:

$$g^{|G|} = e$$

$(\mathbf{Z}_p^*, \cdot) = \{1, 2, \dots, p - 1\}$ under multiplication modulo p $|\mathbf{Z}_p^*| = p - 1$ $e = 1$

Fermat's theorem: if p is prime, then for all $a \neq 0 \pmod{p}$:

$$a^{p-1} \equiv 1 \pmod{p}$$

$$\begin{aligned} 2^{560} &= 1 \pmod{561} \\ 3^{560} &= 1 \pmod{561} \\ 4^{560} &= 1 \pmod{561} \\ &\vdots \\ 560^{560} &= 1 \pmod{561} \end{aligned}$$

A \Leftrightarrow B
 p is prime \Rightarrow *all* $a \neq 0 \pmod{p}$ satisfy Fermat's theorem
 p is **not** prime \Leftarrow *some* $a \neq 0 \pmod{p}$ does **not** satisfy Fermat's theorem
 \bar{A} \bar{B}

Carmichael number

Fermat primality test

Fermat's theorem: if p is prime, then for all $a \neq 0 \pmod{p}$:

$$a^{p-1} \equiv 1 \pmod{p}$$

IsPrime(n)

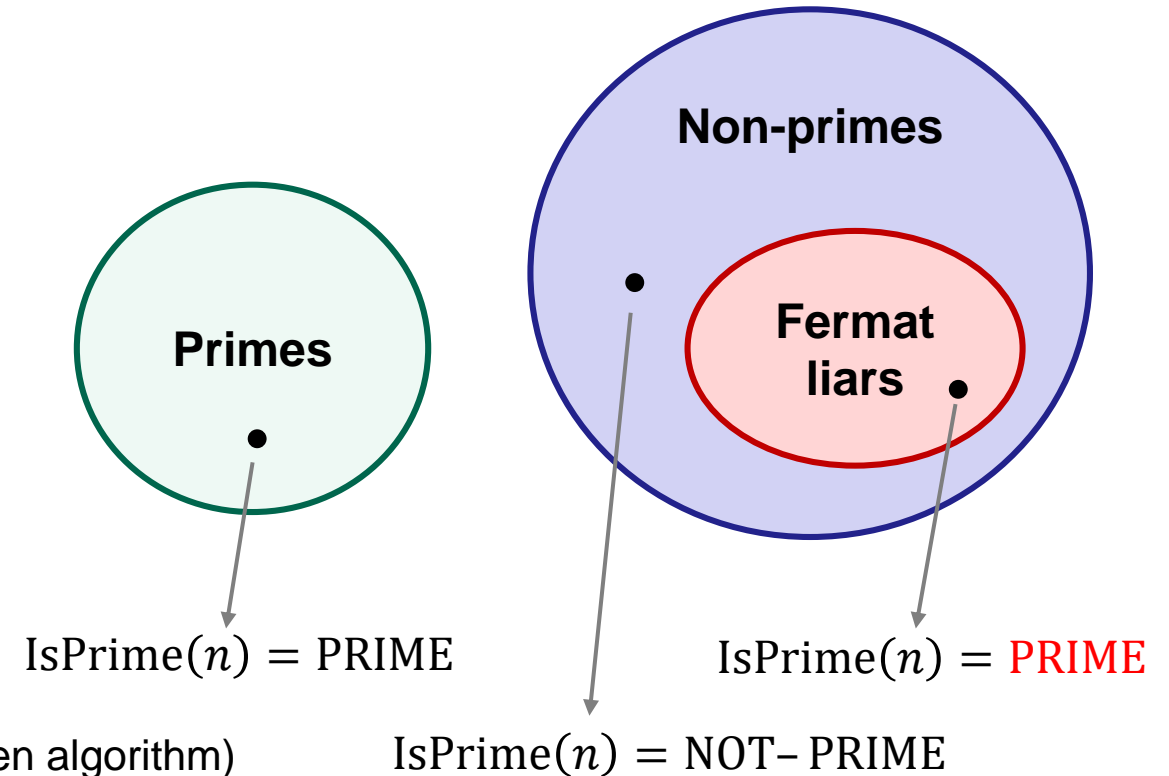
1. **for** $a \in \{2, 3, \dots, t\}$ **do**
2. **if** $a^{n-1} \not\equiv 1 \pmod{n}$ **then**
3. **return** NOT-PRIME
4. **return** PRIME

Better tests exist:

- Euler-test
- Strong pseudoprime-test

(Solovay-Strassen algorithm)

(Miller-Rabin algorithm)

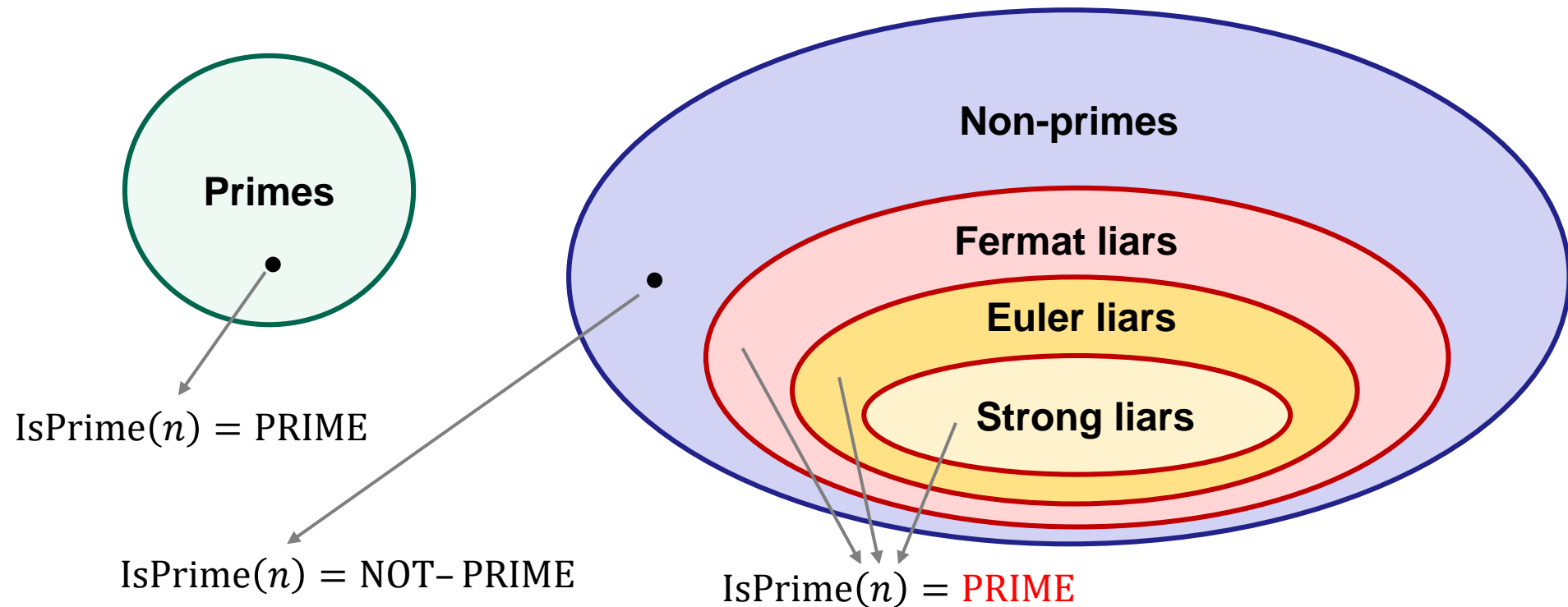


Finding primes

```
IsPrime(n) // Fermat  
1. for  $a \in \{2, 3, \dots, t\}$  do  
2.   if  $\neg$ FermatTest( $a, n$ ) then  
3.     return NOT-PRIME  
4. return PRIME
```

```
IsPrime(n) // Solovay-Strassen  
1. for  $a \in \{2, 3, \dots, t\}$  do  
2.   if  $\neg$ EulerTest( $a, n$ ) then  
3.     return NOT-PRIME  
4. return PRIME
```

```
IsPrime(n) // Miller-Rabin  
1. for  $a \in \{2, 3, \dots, t\}$  do  
2.   if  $\neg$ StrongTest( $a, n$ ) then  
3.     return NOT-PRIME  
4. return PRIME
```



Finding primes in practice

- Miller-Rabin most used in practice
- Failure probability $\leq \frac{1}{4^t}$
- *Deterministic* primality tests
 - Many existed...but none running in polynomial time (P)
 - Open problem for a long time
 - *Agrawal, Kayal & Saxena '02*: "PRIMES is in P"
 - Original running time $\approx \mathcal{O}(k^{12})$
 - Quickly improved to $\approx \mathcal{O}(k^6)$

IsPrime(n) // Miller-Rabin

```
1.  for  $a \in \{2, 3, \dots, t\}$  do  
2.      if  $\neg$ StrongTest( $a, n$ ) then  
3.          return NOT-PRIME  
4.  return PRIME
```

Finding generators

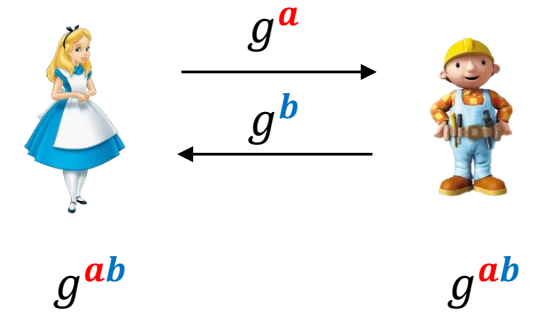
- Easy in prime-order groups
 - All non-identity elements are generators!
- (\mathbf{Z}_p^*, \cdot)
 - Not prime-order!
 - Common in practice: pick element at random; check if generator

Corollary II (Lagrange's theorem):

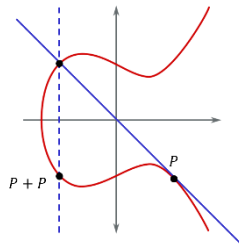
if $H < G$ then $|H|$ divides $|G|$

Diffie-Hellman – computations

- (\mathbf{Z}_p^*, \cdot)
 - Find prime p (one-time)
 - Find generator $\langle g \rangle = (\mathbf{Z}_p^*, \cdot)$ (one-time)
 - Compute $g^a = gg \cdots g \pmod p$
 - Multiply $x \cdot y \pmod p$



- $(E(\mathbf{F}_p), +)$
 - Find prime p (one-time)
 - Generate curve $y^2 = x^3 + ax + b \pmod p$ (one-time)
 - Find curve group order $|E(\mathbf{F}_p)|$ (one-time)
 - Find generator P (one-time)
 - Compute $aP = P + P + \cdots + P$
 - Point addition

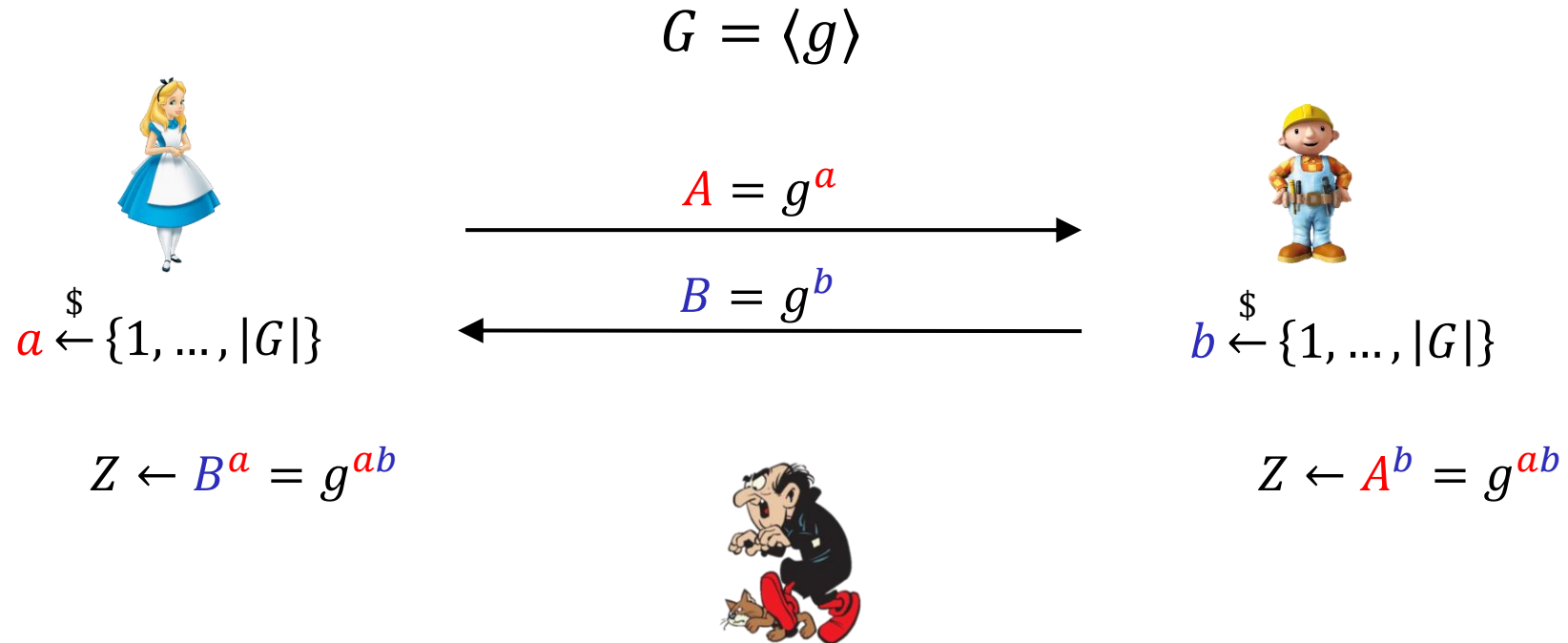


Tricky! $|E(\mathbf{F}_p)| \neq p$ (typically)

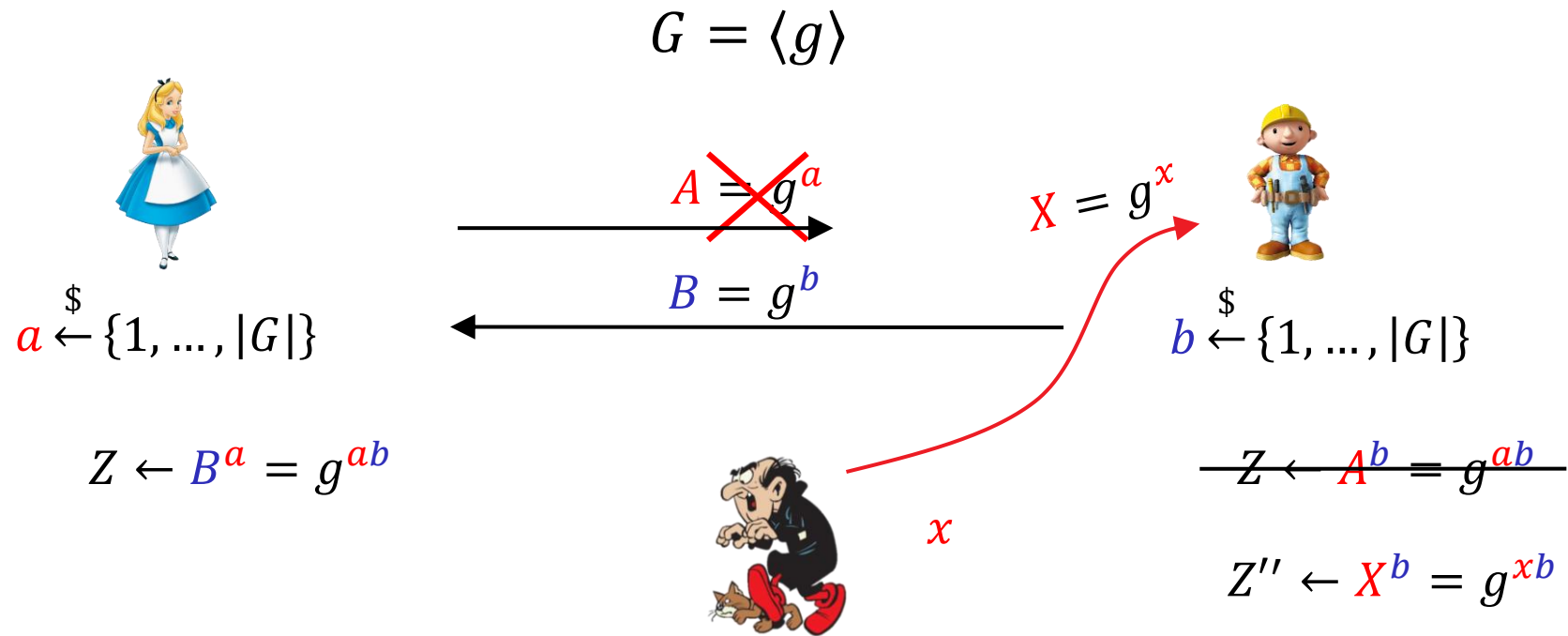
Easy ($|E(\mathbf{F}_p)|$ is usually prime)

Schoof's algorithm

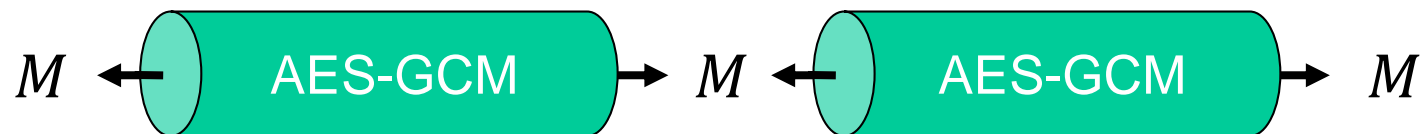
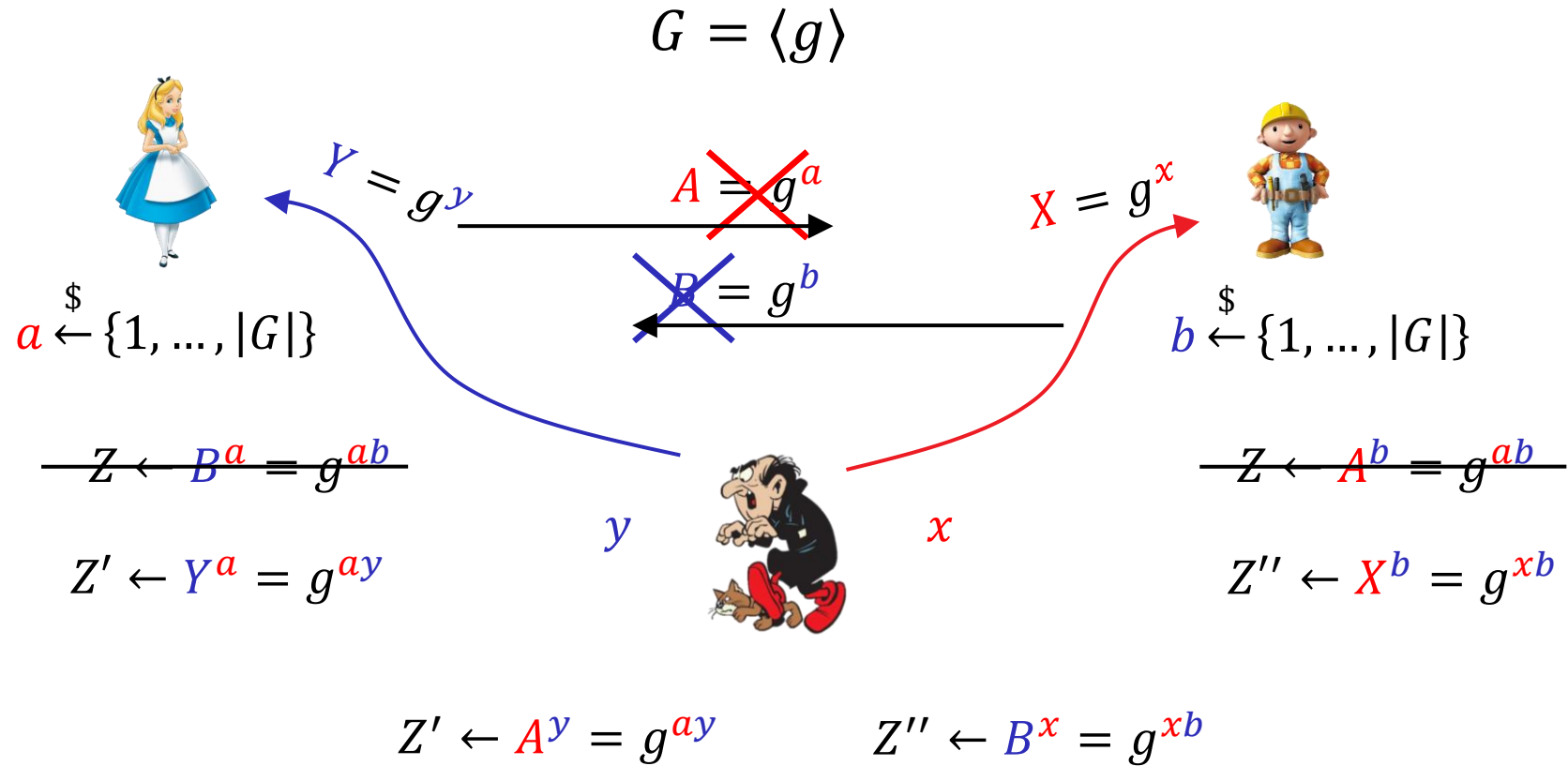
Diffie-Hellman – man-in-the-middle attack



Diffie-Hellman – man-in-the-middle attack



Diffie-Hellman – man-in-the-middle attack



Noise-protocol

Long-term key $\rightarrow A = g^a$



$x \xleftarrow{\$} \{1, \dots, |G|\}$

$G = \langle g \rangle, A, B$

$B = g^b \leftarrow$ Long-term key



$y \xleftarrow{\$} \{1, \dots, |G|\}$

$X = g^x$

$Y = g^y$

$$\begin{aligned} K &\leftarrow H(\text{Alice}, \text{Bob}, X, Y, B^a, Y^x) \\ &= H(\text{Alice}, \text{Bob}, X, Y, g^{ab}, g^{xy}) \end{aligned}$$

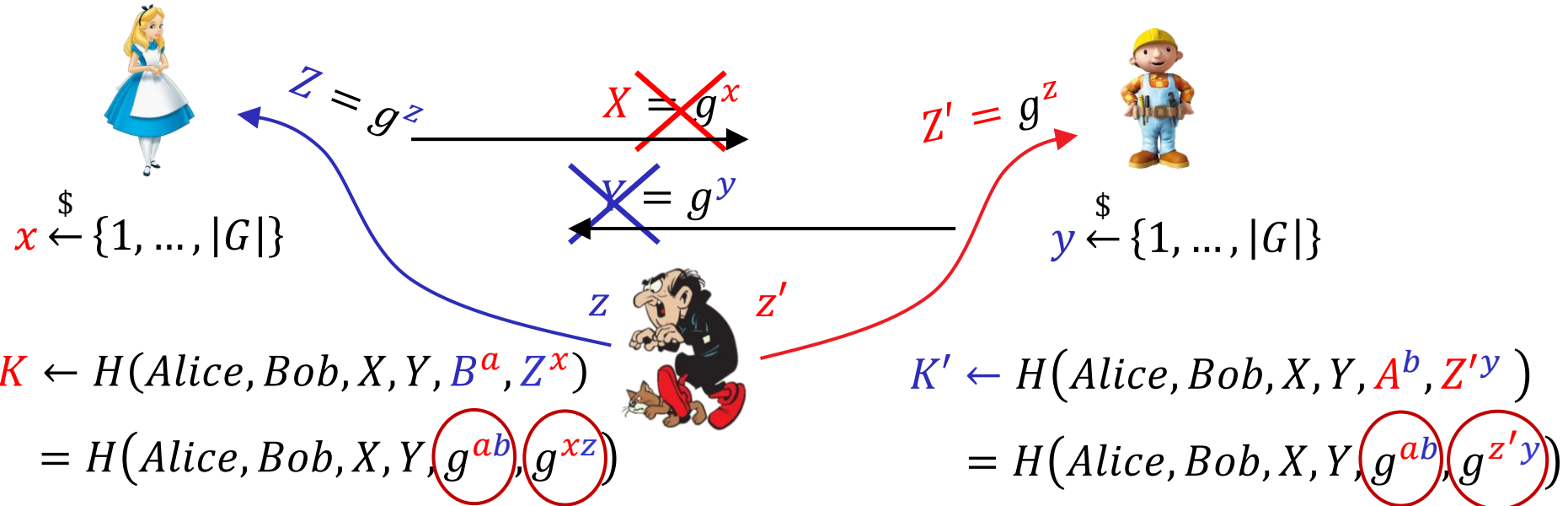
$$\begin{aligned} K &\leftarrow H(\text{Alice}, \text{Bob}, X, Y, A^b, X^y) \\ &= H(\text{Alice}, \text{Bob}, X, Y, g^{ab}, g^{xy}) \end{aligned}$$

Noise-protocol

Long-term key $\rightarrow A = g^a$

$$G = \langle g \rangle, A, B$$

$B = g^b$ \leftarrow Long-term key

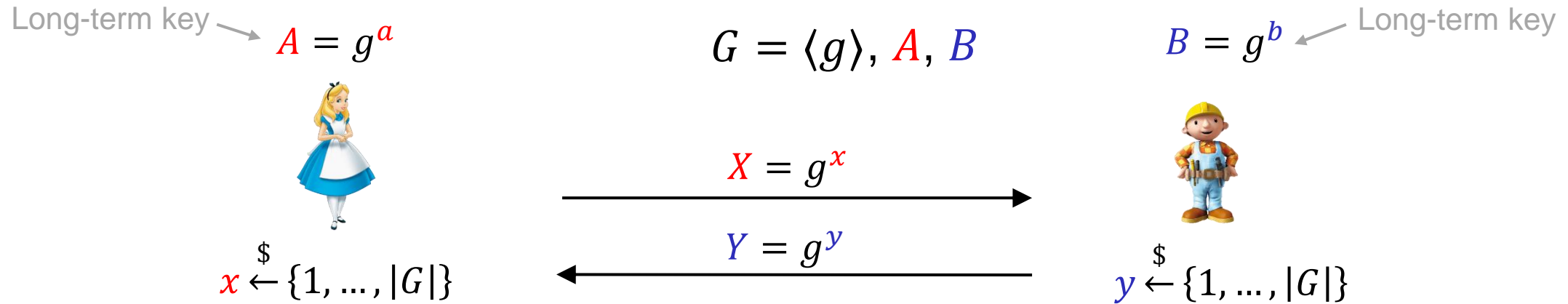


$$K \neq K'$$

$$K \neq K'$$

Can't compute K or K' !

Noise-protocol



$$K \leftarrow H(\text{Alice}, \text{Bob}, X, Y, B^a, Y^x)$$

$$= H(\text{Alice}, \text{Bob}, X, Y, g^{ab}, g^{xy})$$

$$K \leftarrow H(\text{Alice}, \text{Bob}, X, Y, A^b, X^y)$$

$$= H(\text{Alice}, \text{Bob}, X, Y, g^{ab}, g^{xy})$$

Many alternatives:

$$K \leftarrow H(\text{Alice}, \text{Bob}, X, Y, g^{ay}, g^{xb})$$

static-ephemeral, ephemeral-static

$$K \leftarrow H(\text{Alice}, \text{Bob}, X, Y, g^{ay}, g^{xb}, g^{xy})$$

static-ephemeral, ephemeral-static, ephemeral-ephemeral

$$K \leftarrow H(\text{Alice}, \text{Bob}, X, Y, g^{ab}, g^{ay}, g^{xb}, g^{xy})$$

static-static, ephemeral-static, ephemeral-ephemeral, ephemeral-ephemeral

Summary

- Special algorithms needed to deal with the large numbers in asymmetric cryptography
 - Square-and-multiply for group exponentiation
 - Not secure against side-channel attacks
 - Prime finding
 - Common in practice: pick random number; check if prime
 - Primality tests: Fermat's, Miller-Rabin (small one-sided error)
- Plain Diffie-Hellman is *not* secure against active adversaries
 - Man-in-the-middle attack
 - Problem: lack of authentication
 - Common solution: digital signatures (used in TLS, IPsec, SSH)
 - Modern solution: long-term Diffie-Hellman keys mixed with ephemeral Diffie-Hellman keys
 - Noise protocol, Signal, What'sApp, Facebook Messenger Secret Conversations