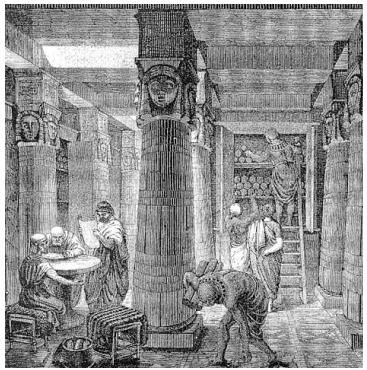
Elliptic Curve Cryptography

Dan Boneh
Stanford University

Diophantus (200-300 AD, Alexandria)

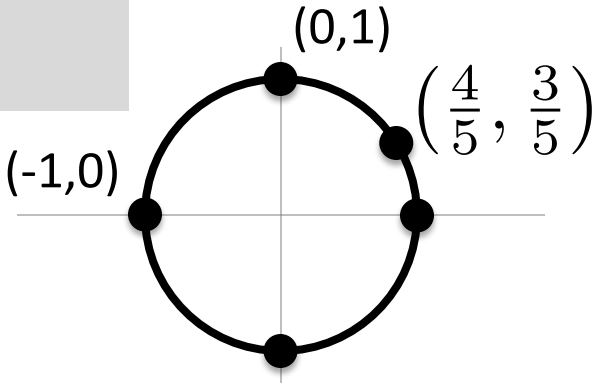


Interested in **rational points** on **curves**

- rational number: 1/2 , 13/8 , but not sqrt(2)
- rational point: (x, y) where x and y are rational

Example: what are the rational points on the curve

$$x^2 + y^2 = 1$$



s rational $\Rightarrow$ $\left(\frac{s^2-1}{s^2+1}, \frac{2s}{s^2+1} \right)$ on curve

Thm: all rational points are obtained this way [except for (1,0)]

Diophantus (200-300 AD, Alexandria)

Studied many similar problems: find rational points on

$$x^2 + 2y^2 = 11 \ , \quad 2x^2 - y^2 = 2 \ , \ \ldots$$

Wrote 13 books of *arithmetica* … six survived (four in Vatican library)

Problem 24 Book IV: find rational points on

$$y^2 = x^3 - x + 9$$

Examples: $(1, \pm 3)$, $(0, \pm 3)$, $(-1, \pm 3)$ are there more?

Elliptic curves

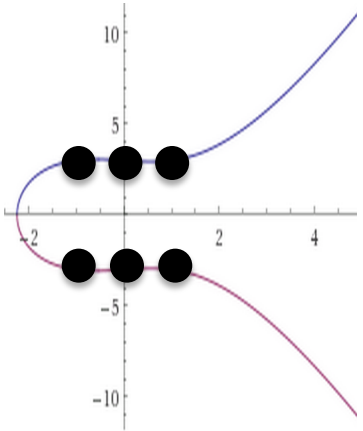
Def: a (rational) **elliptic curve** is a curve $y^2 = x^3 + ax + b$

where a, b are (rational) constants (and $4a^3 + 27b^2 \neq 0$)

Diophantus' curve $y^2 = x^3 - x + 9$ (a = -1, b = 9)

Symmetric about x-axis

(x, y) ⇒ (x, -y)

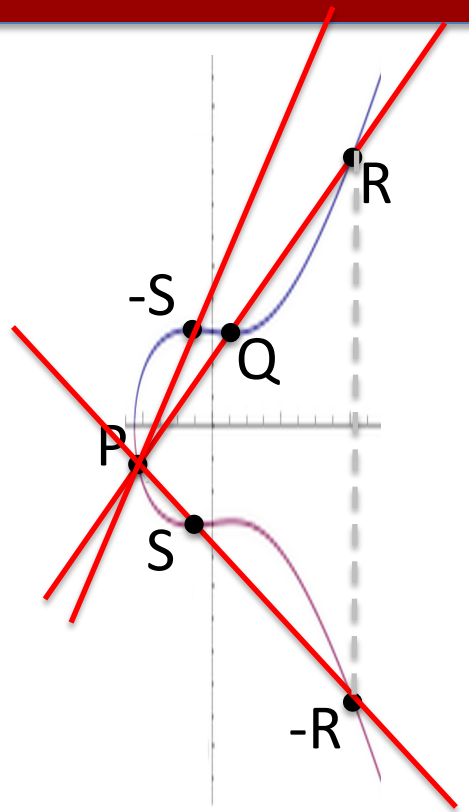


"Why ellipses are not elliptic curves," A. Rice, E. Brown, 2012

An observation

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

Fact: if P and Q are rational point on E
then so is R



Gives an algorithm to build rational points:

P = (0,-3) , Q = (1,3) ⇒ R = (35 , 207)

P , -R ⇒ S = $\left(-\frac{1259}{1225}, -\frac{128211}{42875}\right)$

⋮ ⋮ ⋮

"Diophantus and Diophantine Equations," Bashmakova, 1997

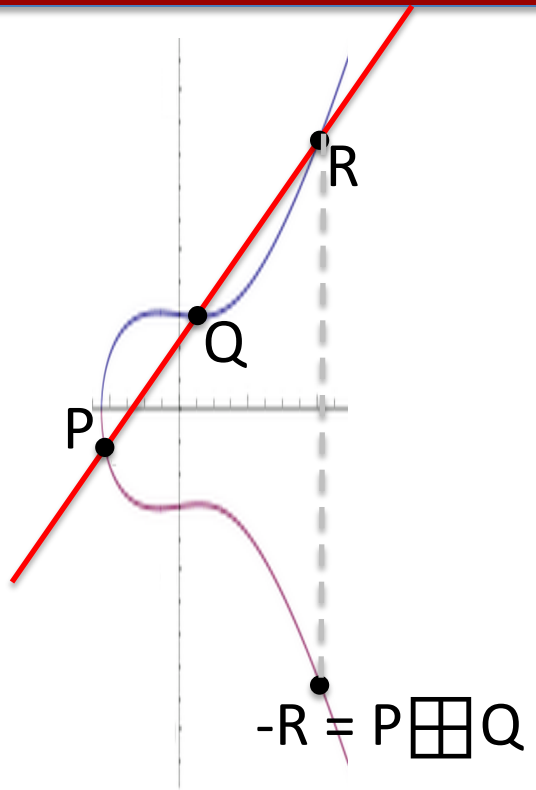
Point addition

Define: $P \boxplus Q = -R$

Why define this way? Associativity!

$$(P \boxplus Q) \boxplus T = P \boxplus (Q \boxplus T)$$

$\Rightarrow$ simply write: $P \boxplus Q \boxplus T$



What if P == Q ?? (point doubling)

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

How to define **P ⊞ P** ??

Define **P ⊞ P = -R**

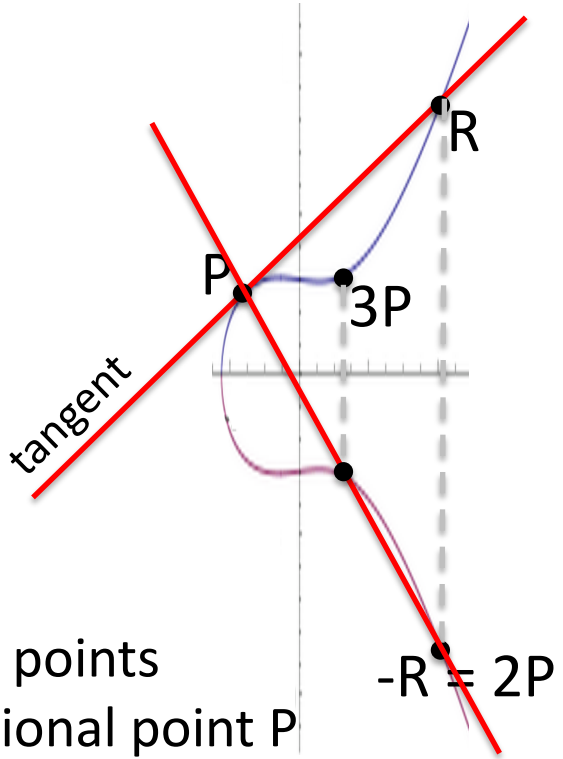
Write: **2P = P ⊞ P**

3P = P ⊞ P ⊞ P

4P = P ⊞ P ⊞ P ⊞ P

new rational points from one rational point P

(… not always new)



Dan Boneh

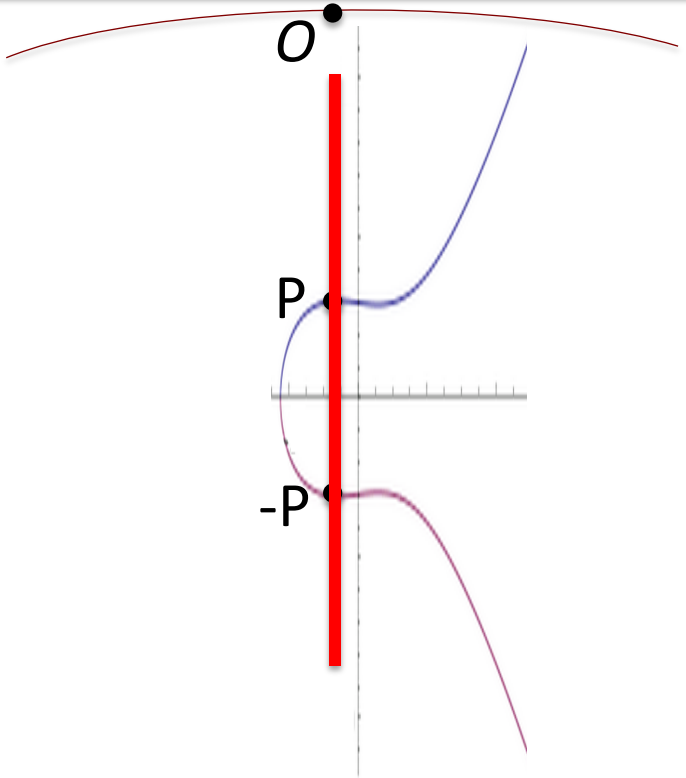
Last corner case

What is **P ⊞ (-P)** ??

O: the point "at infinity"

Define: **P ⊞ (-P) = *O***

P ⊞ O = P



Summary: adding points

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

points on E: $P = (x_1, y_1)$, $Q = (x_2, y_2)$, $R = P \boxplus Q$ (not O)

if P = -Q: $\Rightarrow$ R = O

else if P = Q: $\Rightarrow$ $k = \frac{3x_1^2 + a}{2y_1}$

else (P ≠ ±Q): $\Rightarrow$ $k = \frac{y_2 - y_1}{x_2 - x_1}$

$$\begin{cases} x_{\mathrm{R}} = k^2 - x_1 - x_2 \\ y_{\mathrm{R}} = -y_1 - k(x_{\mathrm{R}} - x_1) \end{cases}$$

$$R = (x_{\mathrm{R}}, y_{\mathrm{R}})$$

Back to Diophantus

Rational points on E: $y^2 = x^3 - x + 9$

$P = (1, -3), \quad 2P = \left(-\frac{17}{9}, \frac{55}{27}\right)$

$Q = (0, 3), \quad 2Q = \left(\frac{1}{36}, \frac{-647}{216}\right), \quad 3Q = (46584,\ 10054377)$

$$P-Q = (-1, 3), \quad 2P+Q = \left(\frac{621}{289}, \frac{-20121}{4913}\right), \quad P+2Q = \left(\frac{-1259}{35^2}, \frac{128211}{35^3}\right), \quad \dots$$

Thm: all rational points on E are obtained as $\{uP + vQ \quad \text{for } u, v \in \mathbb{Z}\}$

$\Rightarrow$ "generated" by two points P and Q $\Rightarrow$ rank(E) = 2

"Elliptic Curves from Mordell to Diophantus and Back," E. Brown, B. Myers, 2002

Curves modulo primes

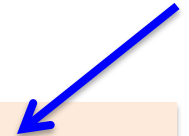
Let p be a prime. Let $F_p = \{0,1,\ldots,p-1\}$

What are the points (x, y) in $F_p \times F_p$ satisfying:

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

Example: nine points on $y^2 = x^3 - x + 9 \pmod{7}$

O, $(1, \pm 3)$, $(0, \pm 3)$, $(-1, \pm 3)$, $(2, \pm 1)$



e.g., the point (2,1): $1^2 \equiv 2^3 - 2 + 9 \pmod{7}$

The number of points

Adding points: use addition formulas "**mod p**"

(-1,3) ⊞ (0,-3) = (2,1) (mod 7)

⇒ addition rule on nine points (mod 7)

Hasse-Weil bound (1949): for all primes p and a,b:

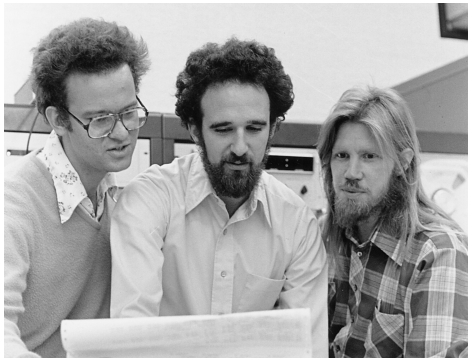
number of points on $y^2 \equiv x^3 + ax + b \pmod{p}$ is "about" p

We have efficient algorithms to compute exact # of points: time = poly(**log p**)

Why are you telling us all this?

What does this have to do
with secure communication?

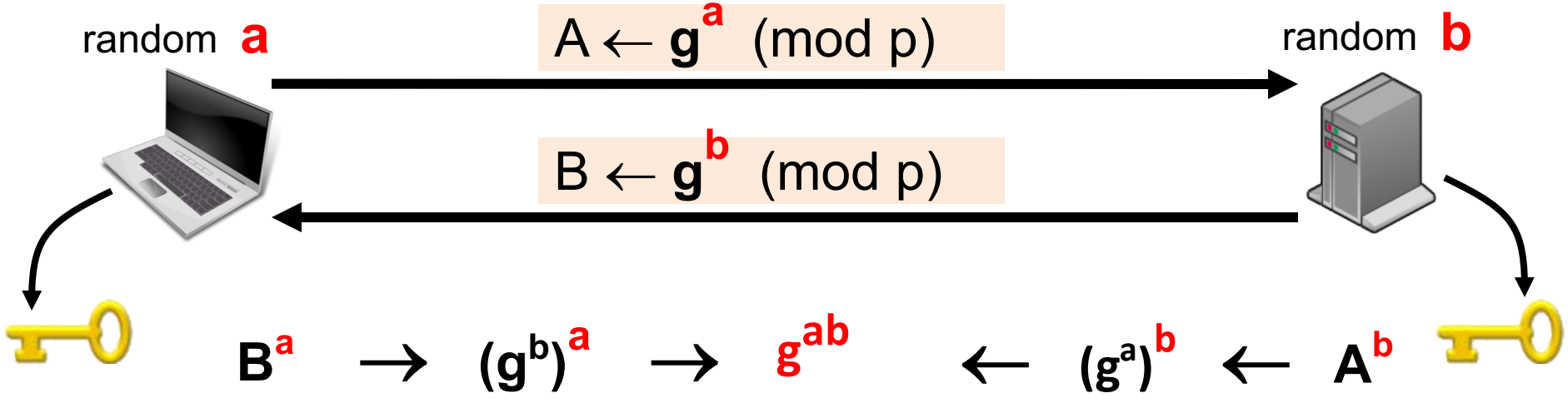
Diffie, Hellman, Merkle: 1976



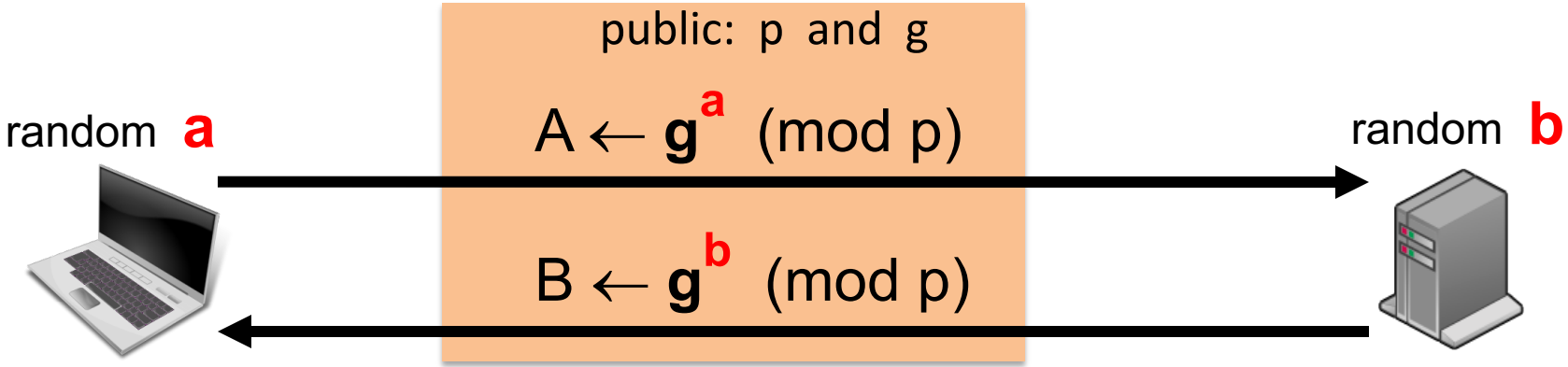
Where do shared secret keys comes from?

A remarkable solution: (**basic) Diffie-Hellman**

Fix prime p and $g \in F_p$



Security of Diffie-Hellman (eavesdropping only)



Eavesdropper sees: p, g, $A=g^a \pmod p$, and $B=g^b \pmod p$

Can she compute $g^{ab} \pmod p$??

CDH problem (mod p): given random (g, g^a, g^b) compute $g^{ab} \pmod p$

How hard is **CDH** mod p ??

Best known algorithm (GNFS): for n-digit prime, time ≈ $2^{\tilde{O}(\sqrt[3]{n})}$

$\Rightarrow$ far faster than "exponential" time $O(2^n)$

$\Rightarrow$ World record: 180-digit prime (2014, ≈50 core years)

In practice, 617-digit primes (2048 bits) are used

(for "comparable" security to AES-128)

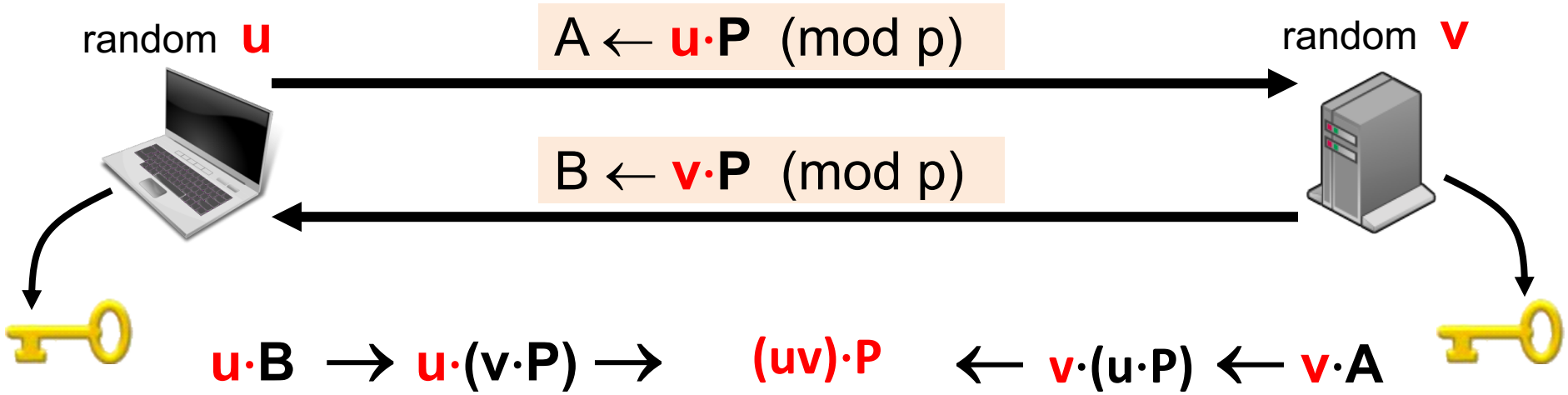
Can we use elliptic curves instead ?? (1985)

Fix prime **p**,

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

and point **P** on curve





Dan Boneh

How hard is CDH on curve?

CDH problem on curve:

$$\mathbf{P},\ u\cdot\mathbf{P},\ v\cdot\mathbf{P} \ \Rightarrow\ (uv)\cdot\mathbf{P}$$

Best known algorithm: for n-digit prime p

CDH(EC) time is $\sqrt{p} \approx 2^{O(n)}$

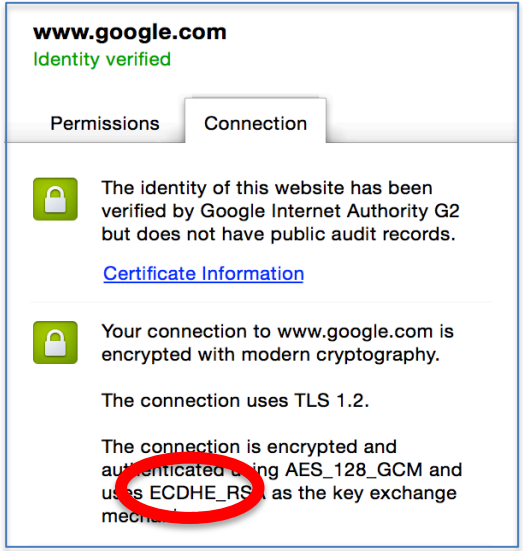
CDH(mod p) time is $2^{\tilde{O}(\sqrt[3]{n})}$

$\Rightarrow$ same security with smaller prime

In practice 77-digit primes (256 bits) are used

- 10x faster than comparable (mod p) security

Taking over the world



also Bitcoin signatures

What curve should we use?

NIST standard (FIPS 186-3 appendix A):

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

A.1.1 Curve P-256

p = 115792089210356248762697446949407573530086143415290314195533631308867097853951

$p = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$

n = 115792089210356248762697446949407573529996955224135760342422259061068512044369

points mod p $\approx 2^{256}$

b = 5ac635d8 aa3a93e7 b3ebbd55 769886bc 651d06b0 cc53b0f6 3bce3c3e 27d2604b

Px = 6b17d1f2 e12c4247 f8bce6e5 63a440f2 77037d81 2deb33a0 f4a13945 d898c296

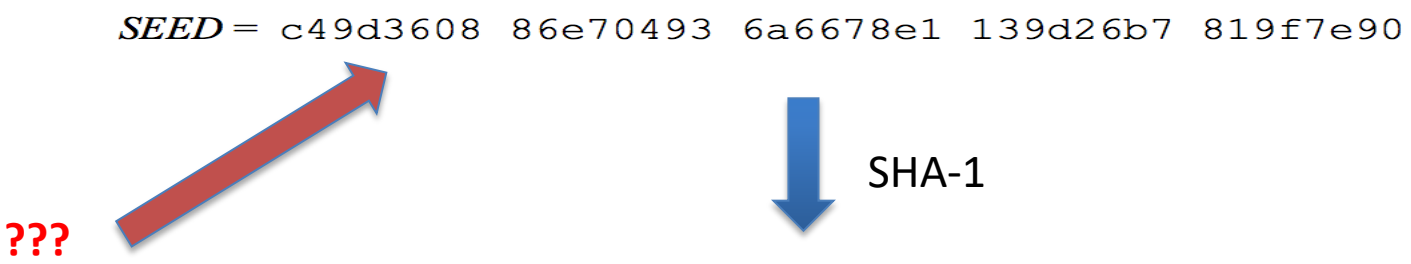
Py = 4fe342e2 fe1a7f9b 8ee7eb4a 7c0f9e16 2bce3357 6b315ece cbb64068 37bf51f5

point $P=(P_x,P_y)$

Of the Web sites that support ECDHE … 96.1% use P-256 [HABJ'14]

Where does P-256 come from?

FIPS 186-3 appendix D.1.2.3:



How hard is CDH on this curve? Unknown …

Alternative curve: Curve25519 (no unexplained constants)

$$y^2 = x^3 + 486662 \cdot x^2 + x \text{ in } \mathbb{F}_p \text{ where } p = 2^{255}\text{-}19$$

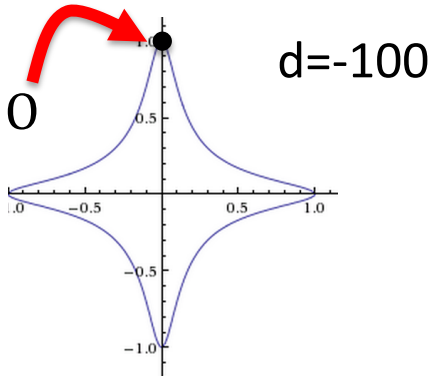
Optimizations

Can we make the addition law faster? Ex: Edwards coordinates

Change of coordinates gives: $x^2 + y^2 = 1 + dx^2y^2$

A complete addition rule:

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right)$$



"Faster Addition and Doubling on Elliptic curves," D. Bernstein and T. Lange, 2007

What does NSA say?

https://www.nsa.gov/business/programs/elliptic_curve.shtml

Jan. 2009

The Case for Elliptic Curve Cryptography

Security Level (bits)	Ratio of DH Cost : EC Cost
80	3:1
112	6:1
128	10:1
192	32:1
256	64:1

Table 2: Relative Computation Costs of Diffie-Hellman and Elliptic Curves[1]

Conclusion:

Elliptic Curve Cryptography provides greater security and more efficient performance than the first generation public key techniques (RSA and Diffie-Hellman) now in use. As vendors look to upgrade their systems they should seriously consider the elliptic curve alternative for the computational and bandwidth advantages they offer at comparable security.

What does NSA say?

Then in August 2015:

Cryptography Today

For those partners and vendors that have not yet made the transition to Suite B elliptic curve algorithms, **we recommend not making** a significant expenditure to do so at this point but instead to prepare for the upcoming quantum resistant algorithm transition.

"A Riddle Wrapped in an Enigma," N. Koblitz, A. Menezes, 2015.

Quantum computing fears?

Quantum computers are good at finding periods:

$f: \mathbb{Z}^n \longrightarrow S$ has period $\pi \in \mathbb{Z}^n$ if $\forall x \in \mathbb{Z}^n$: $f(x+\pi) = f(x)$

Fact (Shor'94): a quantum algorithm can find the period π in time $\log_2(\|\pi\|_2)$ given an oracle for f.

Discrete-log problem: G group of order q with generator $g \in G$

given $g, h \in G$, find $\alpha \in \mathbb{Z}$ s.t. $h = g^{\alpha}$

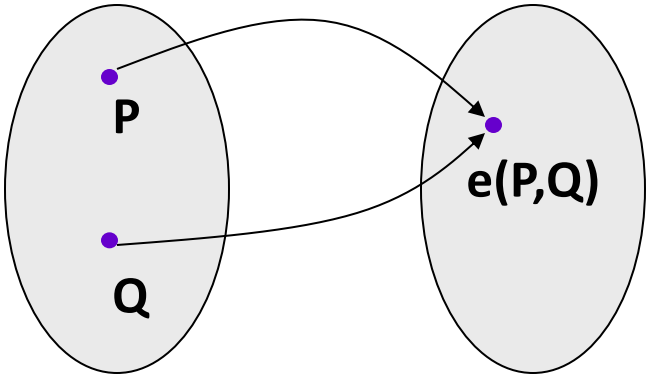
Define: $f(x,y) = g^x \cdot h^y$. Period: $f(x,y) = f(x+\alpha, y-1)$ $\Rightarrow$ $\pi = (\alpha, -1)$

$\Rightarrow$ quantum algorithm can find α in time $O(\log^3 q)$!!

Dan Boneh

Additional Structure on elliptic curves:

Pairing-based Cryptography



A new tool: pairings

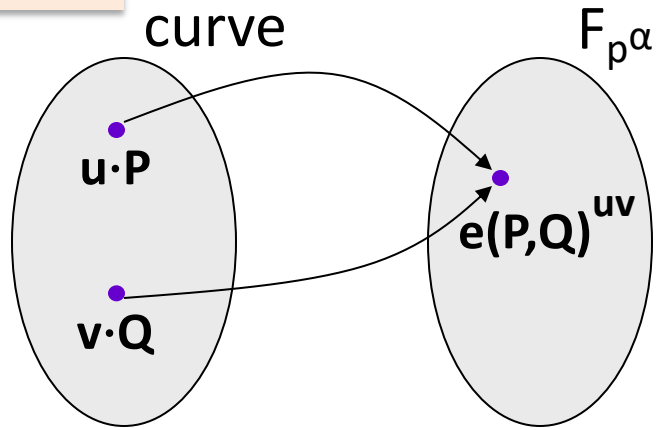
A. Weil (1949): a **pairing** $\hat{\mathbf{e}}(P, Q)$ on elliptic curves

s.t. for all points P, Q and integers u, v:

$$\hat{e}(u\mathbf{P},\ v\mathbf{Q}) = \hat{e}(\mathbf{P}, \mathbf{Q})^{u \cdot v}$$

V. Miller (1986): pairing is efficiently computable!

(u, v unknown)

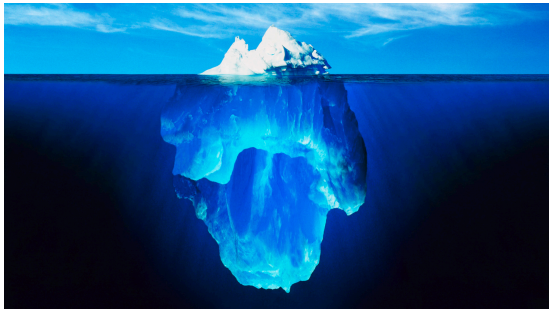


Applications of pairings

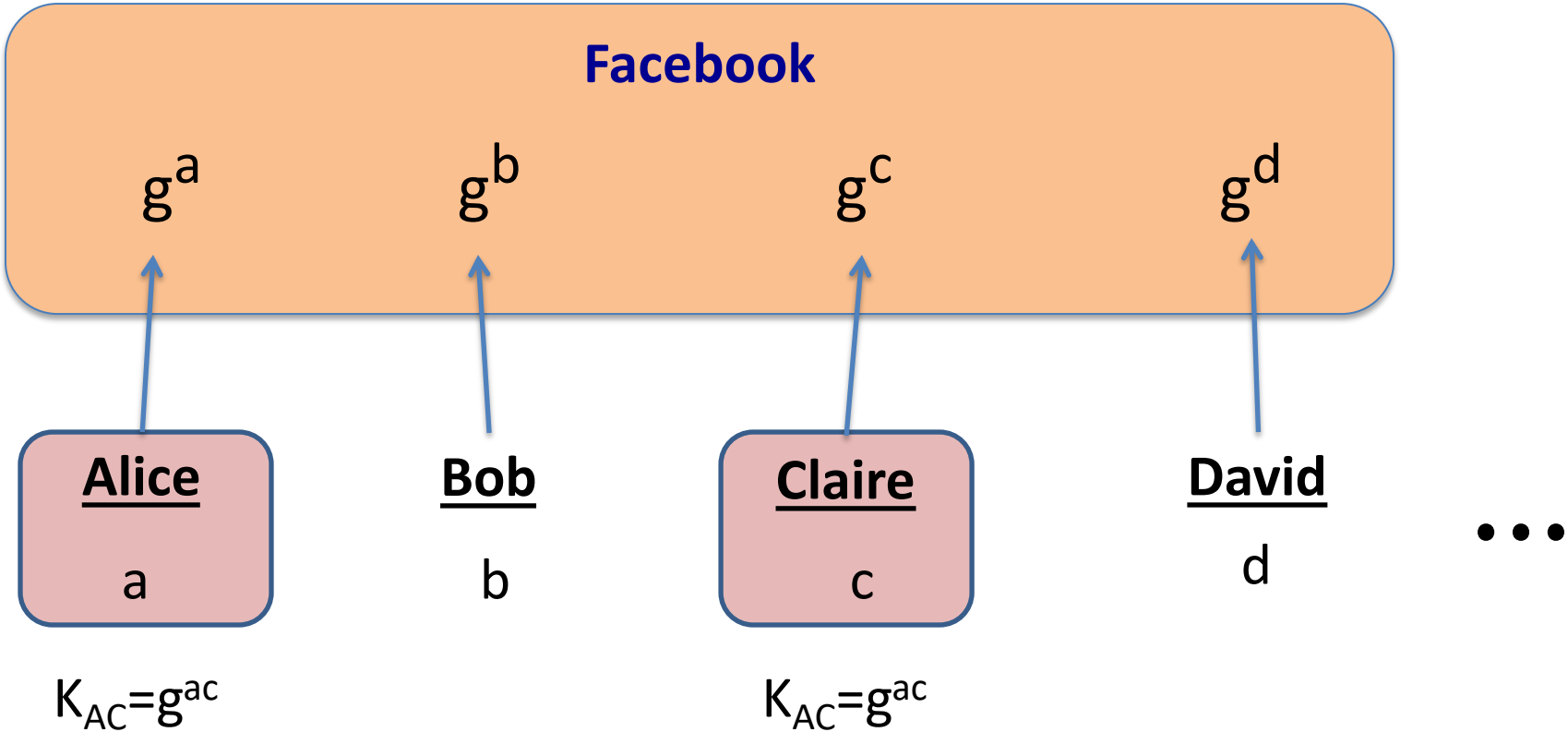
Many many applications for pairings:

- **New signatures**: BLS sigs., group signatures, ring signatures
- **Encryption**: Identity-based encryption, attribute-based encryption, searchable encryption, broadcast encryption
- **Short non-interactive proofs**, **adaptive oblivious transfer**

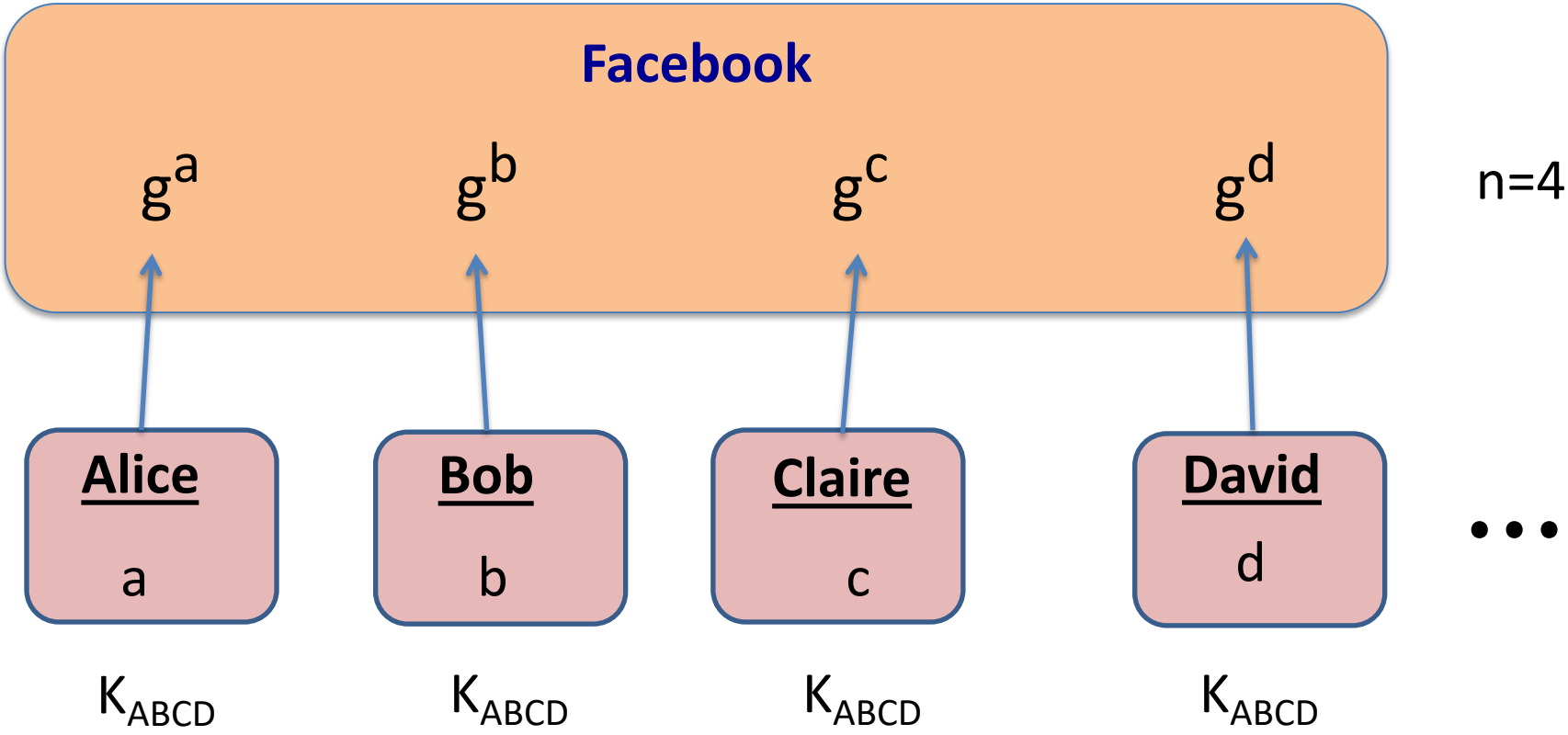
⋮



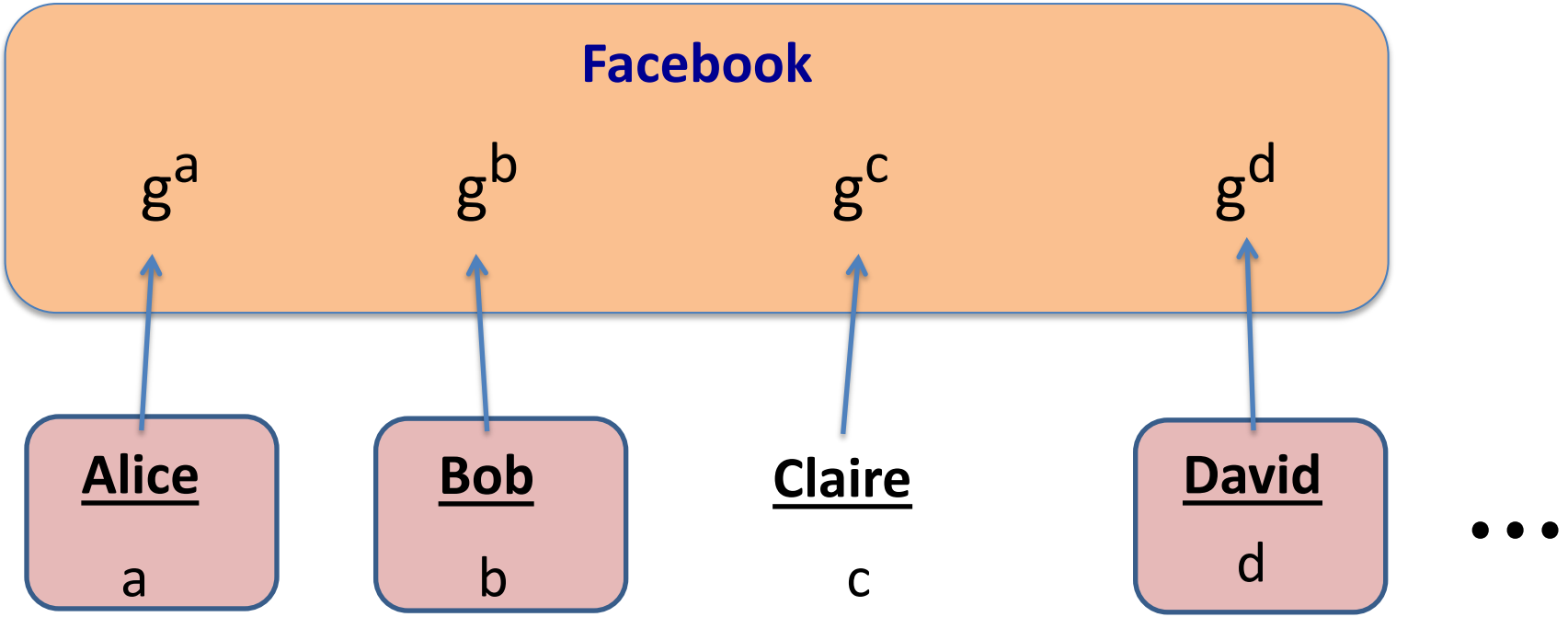
Another look at Diffie-Hellman: non-interactive key exchange



What about n-way Diffie-Hellman?

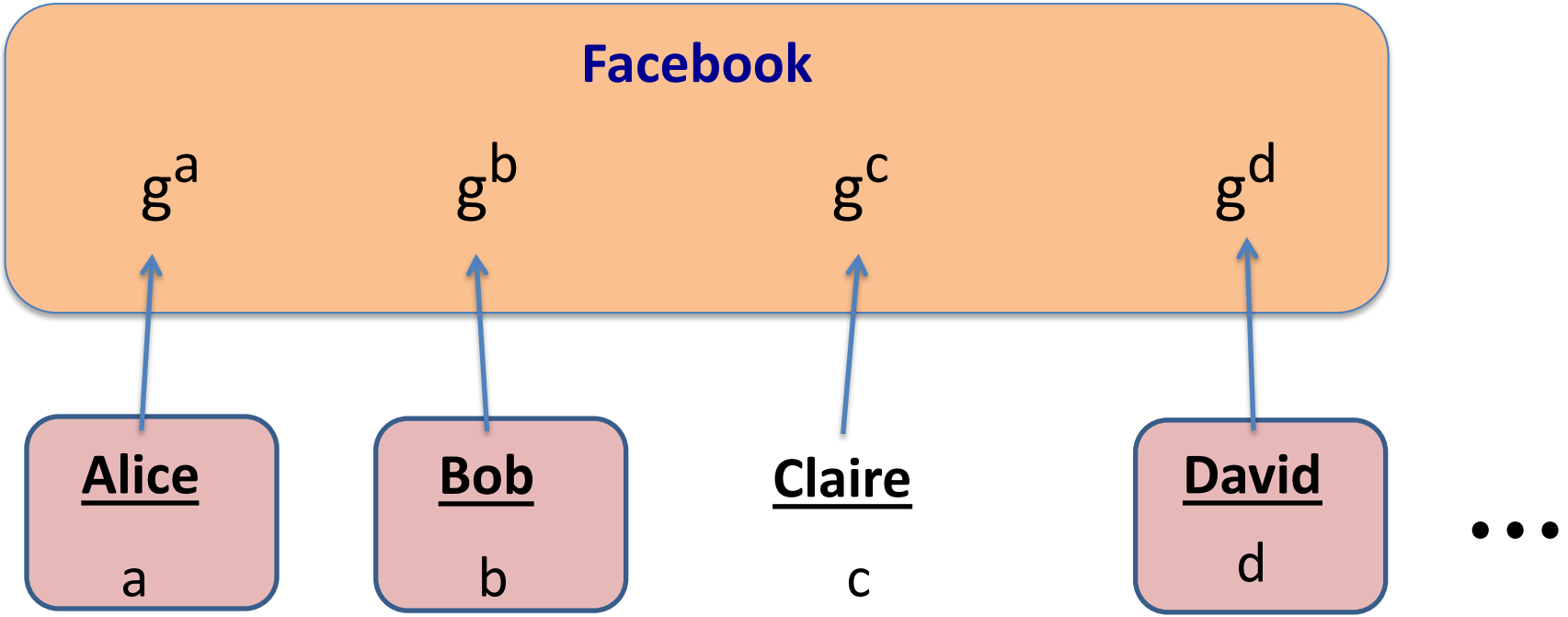


3-way Diffie-Hellman from pairings



$K_{ABD} = e(g,g)^{abd}$

3-way Diffie-Hellman from pairings



$$e(g^b,g^d)^a = e(g^a,g^d)^b = K_{ABD} = e(g^a,g^b)^d$$

Practical n-way Diffie-Hellman ??

Open problem: practical n-way DH for n>3

useful for secure group messaging

B-Zhandry'13: Polynomial time, but impractical construction

THE END

Hope you enjoyed the class !!