
cisco Live!
ALL IN

The bridge to possible

Public Key Cryptography

From RSA and EC to Post-Quantum

Frederic Detienne
Distinguished Engineer

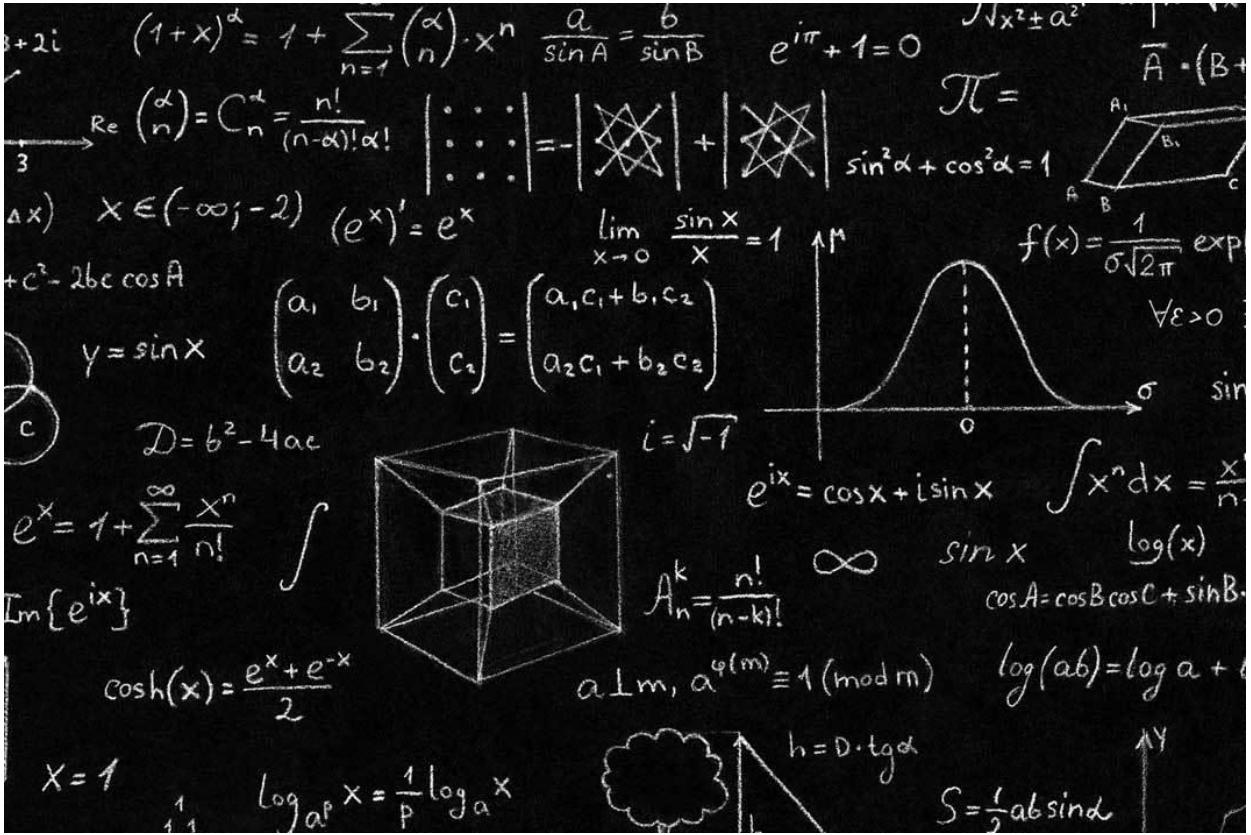
BRKSEC-3129

Agenda

- A Brief Introduction
- MODP: Multiplicative Group of Integers Modulo P
- ECC: Elliptic Curve Cryptography
- Enters The Quantum Computer
- Lattice Based Cryptography
- Conclusion and Recommendations

Introduction

Today is a bout making math fun!



Cryptographic Mechanisms

Encryption

Signatures

Data Authentication (HMAC)

Random Number Generation

Key Establishment

Hashing

Today – Suite B

Authenticated Encryption	AES-GCM
Authentication	HMAC-SHA-2
Key Establishment	ECDH
Digital Signatures	ECDSA
Hashing	SHA-2
Entropy	SP800-90
Protocols	TLSv1.2, IKEv2, IPsec, MACSec

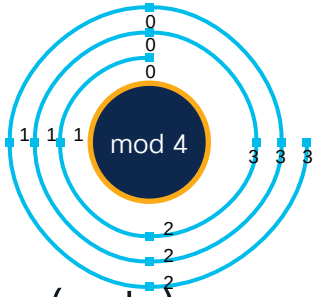
MODP Multiplicative Group of Integers Modulo P

RSA

- Rivest, Shamir, Adleman (1977)
  - Patented but expired => no more royalty
- Public key cryptosystem
- Variable key length (usually 512-2048 bits)
- Based on the (current) difficulty of factoring very large numbers

Modular Arithmetic

- Modulo is like a clock



- $b^x \bmod n = r$ also written as $b^x \equiv r \pmod n$
  - b is the base
  - x is the exponent
  - n is the modulus
  - r is the remainder
- Knowing b, x & n, it is very easy to compute r
- Knowing x, r & n, it is very difficult to compute $b = \sqrt[x]{r} \bmod n$ aka the RSA problem
- Knowing b, r & n, it is very difficult to compute $x = \log_b(r) \bmod n$ aka the discrete log problem

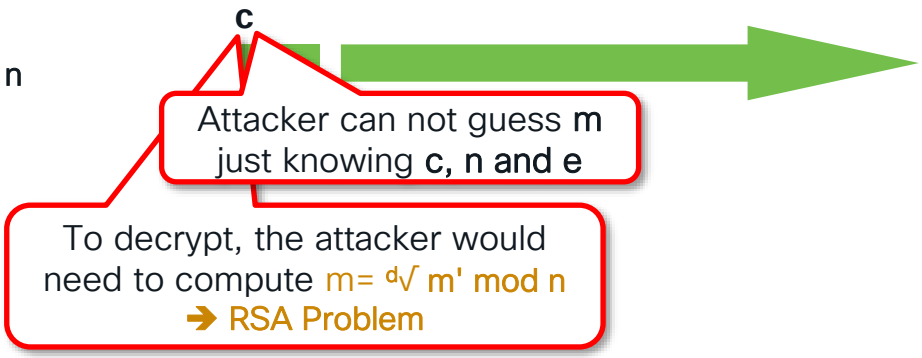
unless there are trapdoors

Encryption with Modular Arithmetic

Alice

Must send a private message **m**

Takes **n** & **e** from Bob
(we assume m < n)
Computes **c = m^e mod n**



Bob

Selects three numbers **n, d & e**
n & **e** are **public**, **d** is **secret**
e, d are chosen such as ed ≡ 1 mod n

Computes **m' = c^d mod n**

$m' = c^d \bmod n$
$= (m^e)^d \bmod n$
$= m^{ed} \bmod n$
$= m^1 \bmod n$
$= m$

➔Bob has reversed the operation !!
➔Bob knows d but nobody else…
➔We have an encryption scheme

Signature with Modular Arithmetic

Alice

Takes **n** & **e** from Bob

Computes **m' = c^e mod n**

m' = c^e mod n
= $(m^d)^e$ mod n
= m^{de} mod n
= m^1 mod n
= m mod n
= m

➔Bob must have sent the **c,m**

Bob

Selects three numbers **n, d & e**
n & **e** are **public**, **d** is **secret**
e, d are chosen such as ed ≡ 1 mod n

Must send a signed message **m**

Computes **c = m^d mod n**
(we assume m < n)

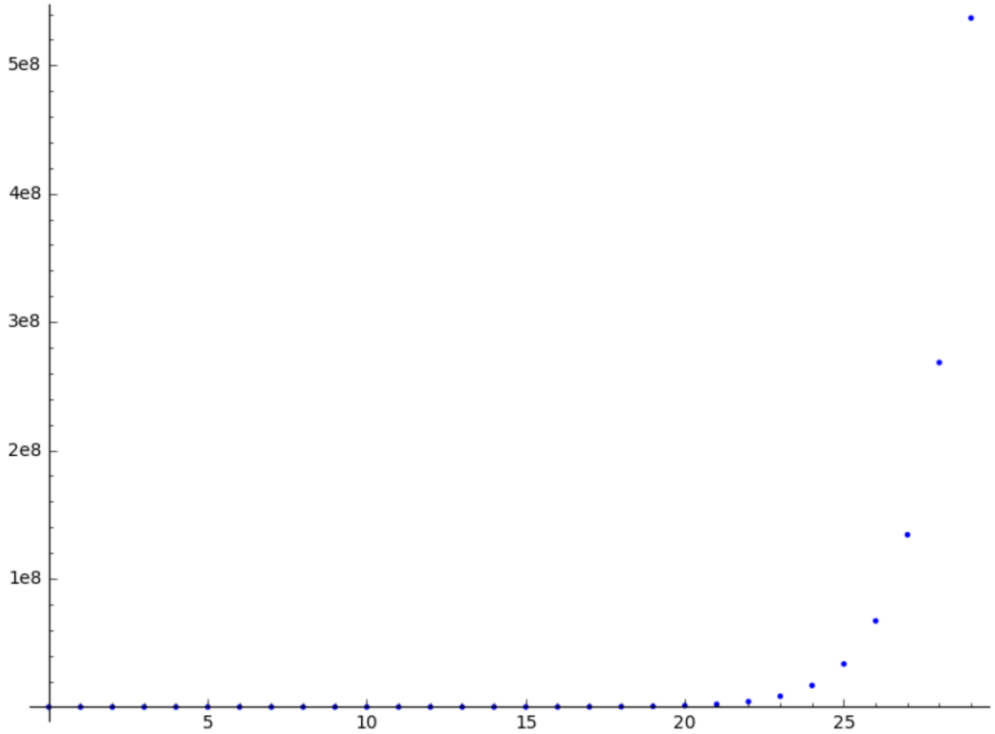
c, m

Attacker can not guess **d** just knowing **m, n and e**

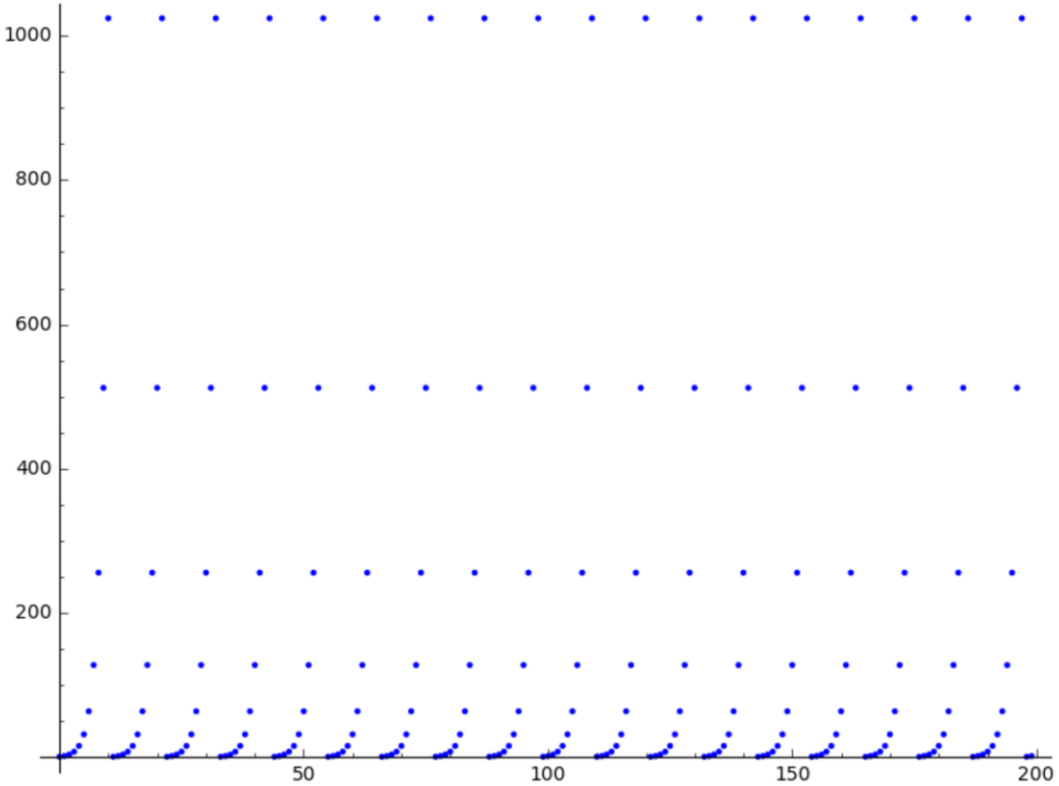
To forge the signature, the attacker would need to compute
$d = \log_e(m') \bmod n$
➔ Discrete Logarithm Problem

Now how can we find such e, d and n ?

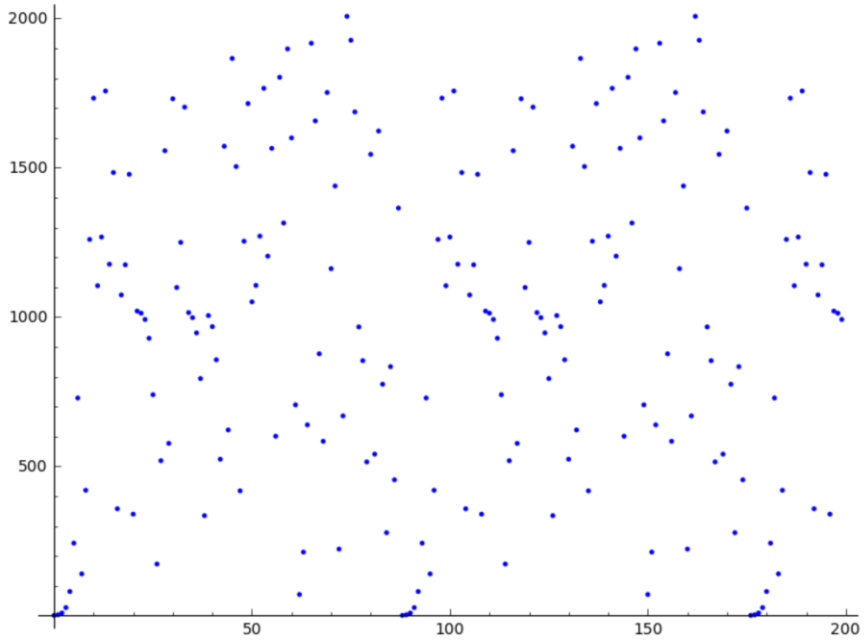
Regular Exponentiation –Dichotomy to reverse

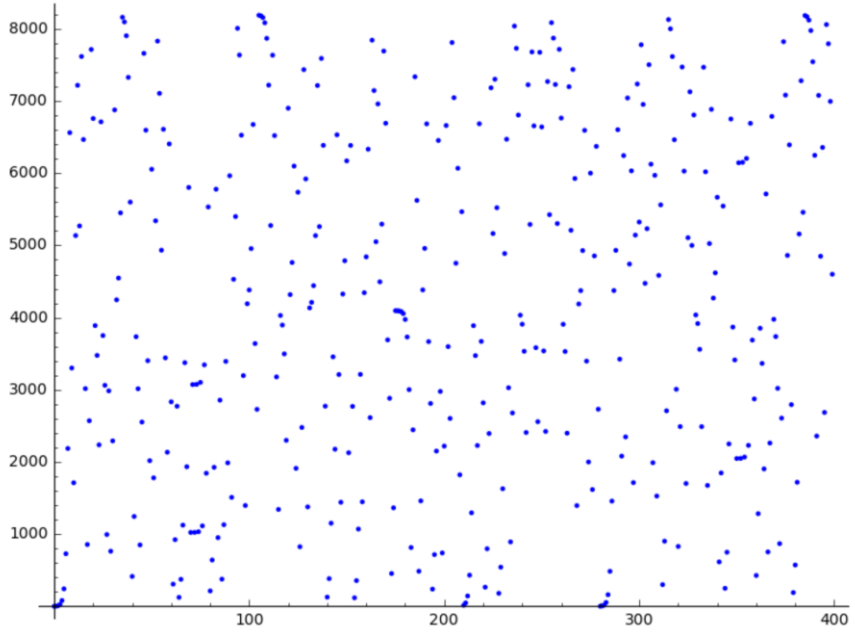


MODP Exponentiation – dichotomy is broken

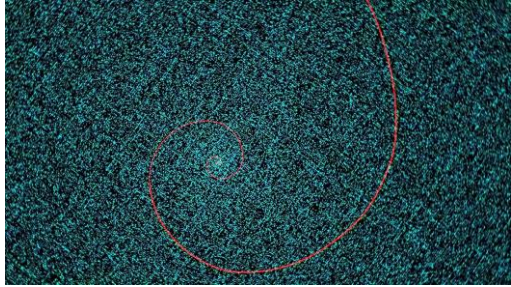


With well chosen numbers...





About Prime Numbers



picture: Khan Academy

- A number is prime if it can be divided by one or itself
- A number is composite is it can be divided by 2 or more prime numbers
  - Factorization is a hard problem. Best algorithm yields $O\left(\exp\left(\left(\frac{64}{9}b\right)^{\frac{1}{3}}(\log b)^{\frac{2}{3}}\right)\right)$.
- Fundamental Theorem of Arithmetic: a given number has a single factorization
- Euclid's theorems: there are infinitely many primes
  - prime density (ratio of primes per composite up to x) is 1/ln(x)
  - density drops off rapidly in the beginning but very slowly after a few powers of 10
  - π(x) = x/ln(x) : number of primes < x
- Euler's φ(n) function or Euleur's totient
  - # of integers in [1,n] that are relatively prime to n: |k ∈ [2,n] | GCD(k,n) = 1|, {1}
  - 2 numbers are coprime if they share no factor other than 1.
  - Property: *n1, n2*, GCD(*n1,n2*)=1 ➔ φ(*n1*n2*)= φ(*n1*)* φ(*n2*) – Totient is multiplicative
  - if x is prime ➔ φ(*n*) = n-1 since 1…n-1 coprime with n and n divisible by itself
- Euler's theorem: $m^{\varphi(n)} \equiv 1 \pmod{n}$ if *m* and *n* are co-prime.

RSA keys – finding e,d,n | $m^{ed} \equiv m \pmod n$

- Choose two distinct prime numbers *p, q* and hide them forever!
- $n = p.q$ ➔ n is hard to factor if p & q are very large
- $\varphi(n) = n-(p+q-1)$
  - p & q are prime ➔ $\varphi(p)=p-1$ $\varphi(q)=q-1$
  - $\varphi(n) = \varphi(pq) = \varphi(p)\,\varphi(q) = (p-1)(q-1) = n-(p+q-1)$
- Final steps — Euler theorem...
  - $1^k = 1$ ➔ $(m^{\varphi(n)})^k \equiv 1^k \pmod n$ ➔ $m^{k\varphi(n)} \equiv 1 \pmod n$
  - $1m = m$ ➔ $m\, m^{k\varphi(n)} \equiv m \pmod n$ ➔ $m^{k\varphi(n)+1} \equiv m \pmod n$
  - we look for e,d,n such that $m^{ed} \equiv m^{k\varphi(n)+1} \equiv m \pmod n$ ➔ $ed = k\,\varphi(n) + 1$
  - ➔ $d = \frac{k\,\varphi(n)+1}{e} = \frac{k\,(n-(p+q-1))+1}{e}$
- Select **e**, small integer and **k** such that GCD(d, $\varphi(n)$) = 1 (i.e. d & $\varphi(n)$ are co-prime)
  - **e** is usually 3 or 65537
  - adjust **k** to make **d** an integer

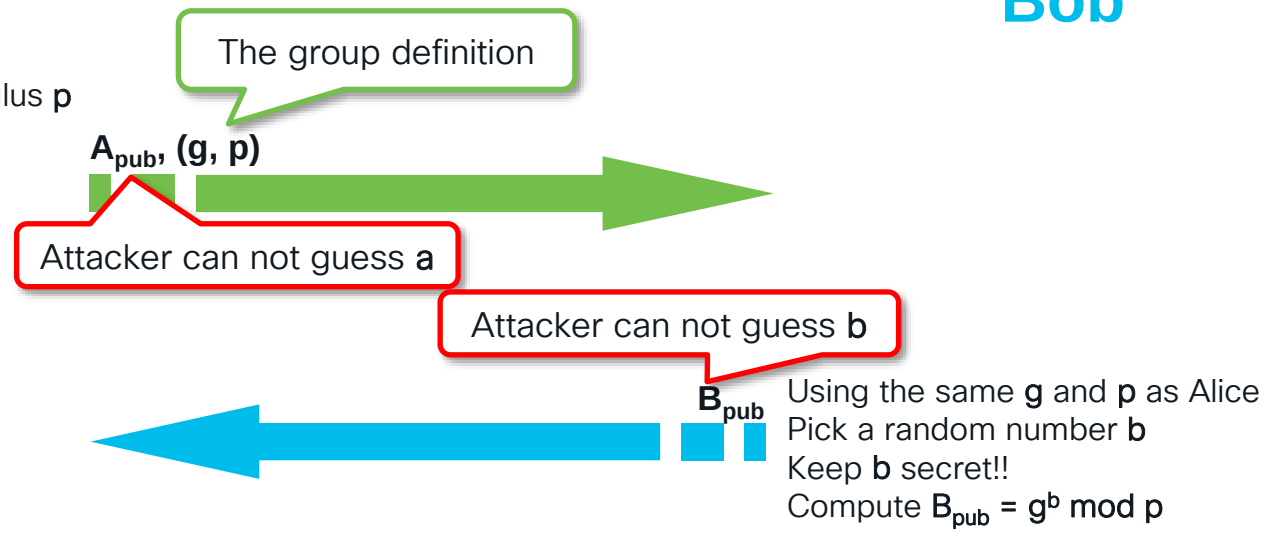
m – arbitrary message
n – the modulus
e – the public key
d – the private key

DH –Diffie–Hellman

Alice

Select a generator **g** and a modulus **p**
Pick a random number **a**
Keep **a** secret!!
Compute $A_{pub} = g^a \bmod p$

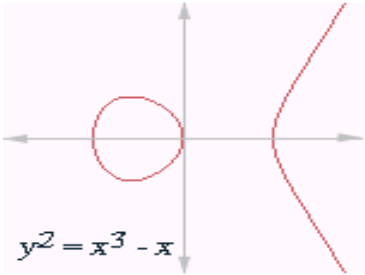
Bob

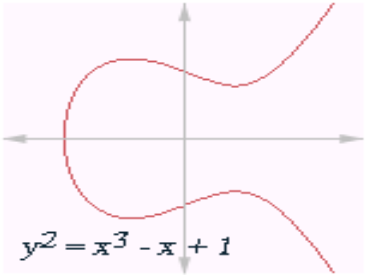


$Secret_{Alice} = (B_{pub})^a \bmod p$ = $Secret = g^{a.b} \bmod p$ = $Secret_{Bob} = (A_{pub})^b \bmod p$

ECC
Elliptic Curve
Cryptography

What is an elliptic curve ?

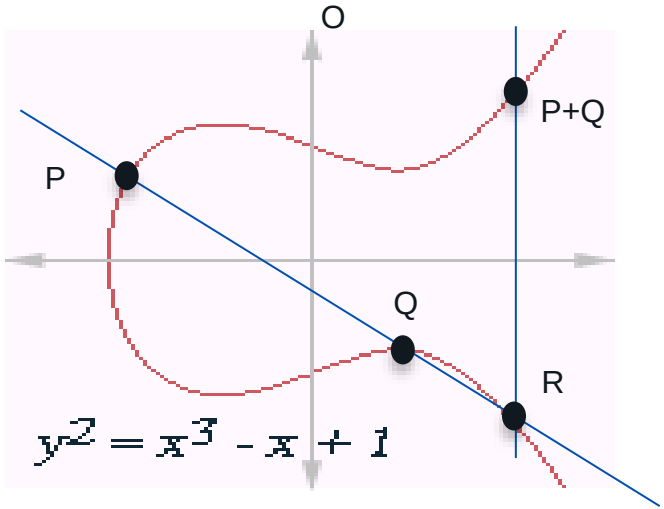


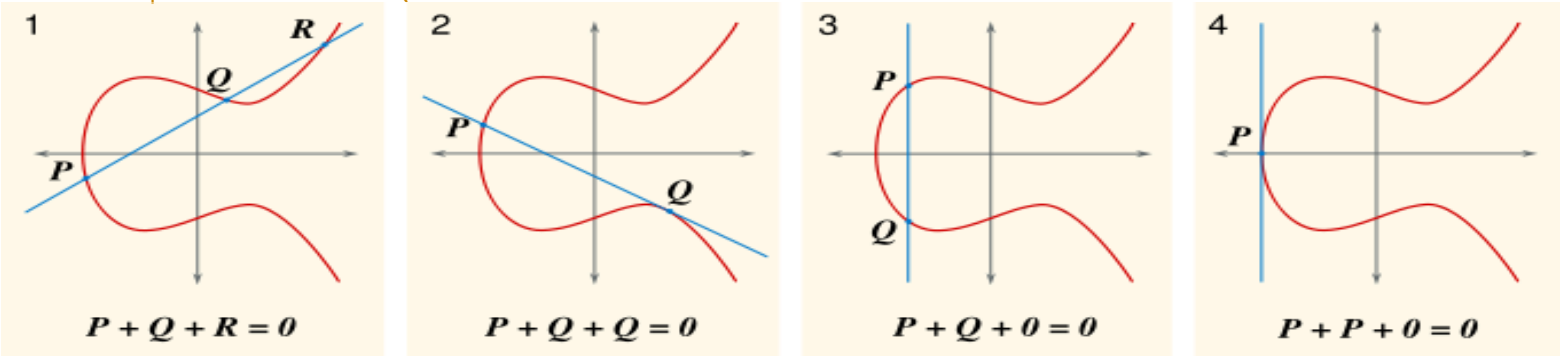


- A curve of general equation $y^2=x^3+ax+b$
  - It MUST be a smooth curve
  - Its discriminant MUST BE NON ZERO: $D = 4A^3 + 27B^2$
- The Elliptic Curve is the set of points
  - that satisfy the equation of the curve (ie. that “belong” to the curve)
  - Plus a special point at infinity that we call O (the letter O)

Elliptic Curve Addition

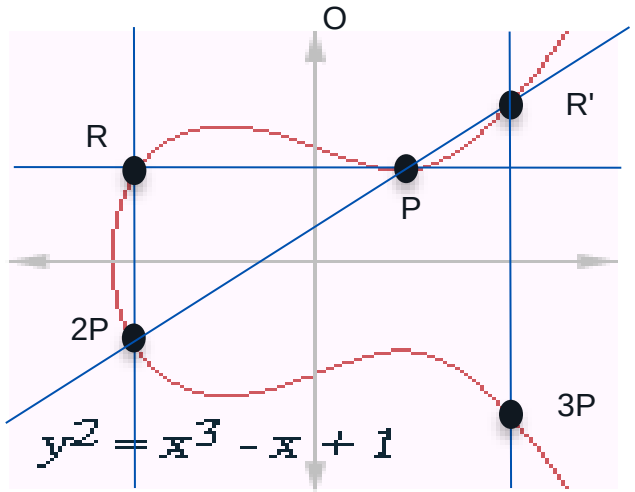
- Let P and Q be two points on the curve
- A line (P,Q) cuts the curve at a third point R
  - If the line is parallel to the Y axis, this point is O
  - If the line is tangent to the curve, the tangent point is counted twice
- The group operator + is defined such as
  - P+Q+R = O; O is the identity
- The reflected point from R is P+Q



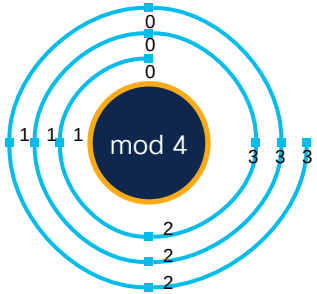


The scalar multiplication n*P

- Let’s start with P+P = 2*P
- For drawing (P,P)
  - draw a tangent to the curve → R
  - (O,R) cuts in P+P=2P
- This is a scalar multiplication
  - One can derive 3P = 2P+P, 4P = 3P+P,...nP = (n-1)P+P



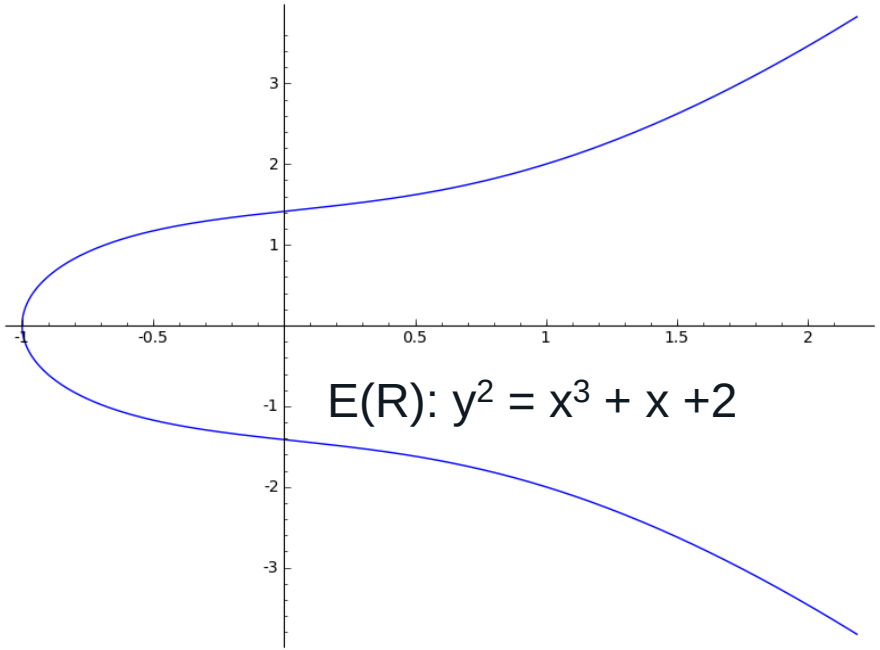
Fast Forward – the finite fields F_m & F_{2^k}



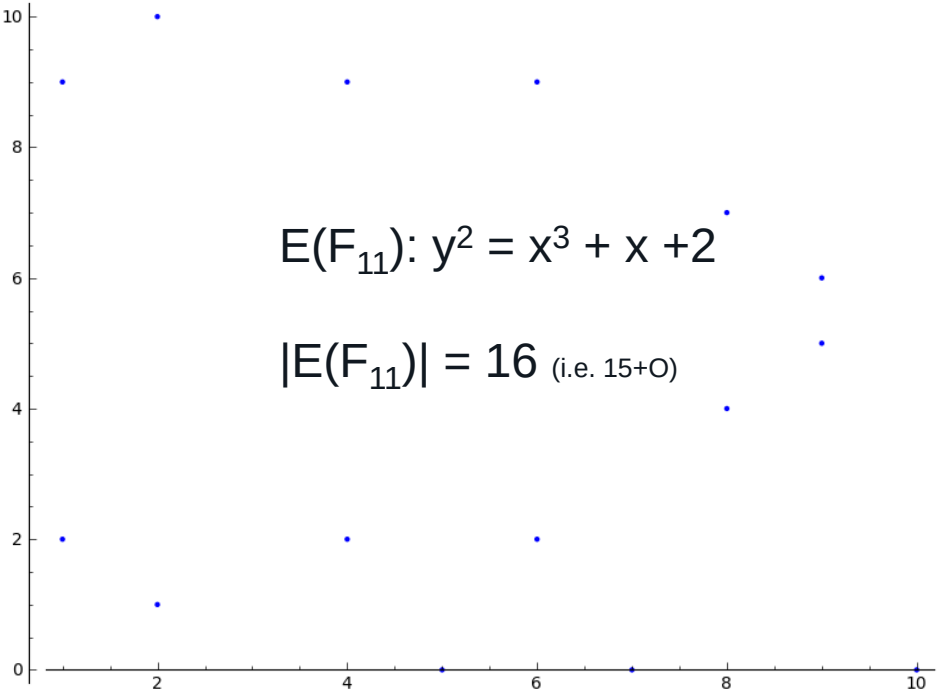
- Remember… modulo arithmetic
- Galois Field = Finite Field
- Let E be an elliptic curve defined over a finite field F_m (modulo m):
  - **$E(Fm):\{\infty\} \cup \{(x,y) \text{ in } F_m x F_m \mid y^2=x^3+ax+b \text{ , } a,b \text{ in } F_m\}$**
  - $E(F_m)$ is the set of points whose coordinates belong to $F_m x F_m$ and satisfy the equation + point at infinity
  - The set along group operations (+, x) seen before form an Abelian Group under multiplication ➔ a field.
  - For cryptography, m should be a prime number

- It **seems (seemed ?)** more computationally efficient if **$m = 2^k-1$** yielding the notation **F_{2^k}**
  - Multiplication supposed to be more efficient ➔ very important for ECDH and ECDS
  - In this case, the Koblitz curve is used: **$y^2 + xy = x^3 + ax^2 + 1$** where **$a=0$** or **$a=1$**
  - For cryptography, k should be a prime number
  - m should remain a prime – it would be called a Mersenne Prime
  - **There is debate about the actual security and efficiency of these curves**!
- The **order of a group *G*** is the **cardinality** of that group written ***ord(G)*** or ***|G|***.
- The order of a **point *P* in a group *G*** is the value *n* such that *n*P = O* written ***ord(p)*** or ***|p|***

Example Curve



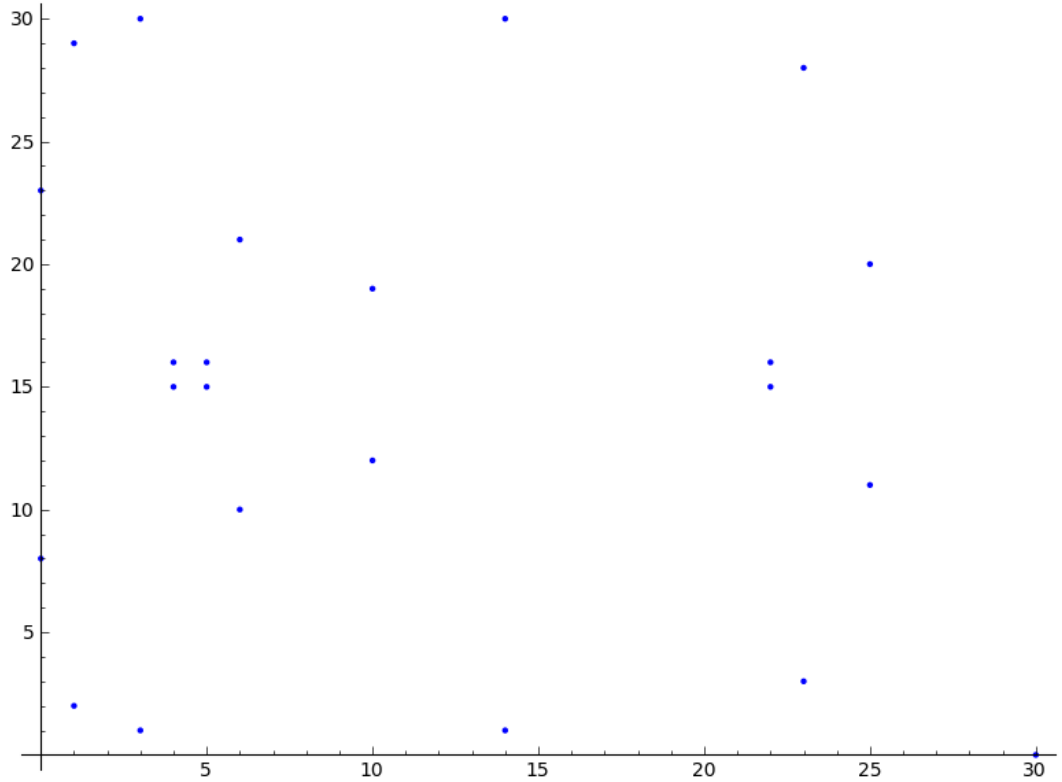
$E(R)$: $y^2 = x^3 + x + 2$



$E(F_{11})$: $y^2 = x^3 + x + 2$

$|E(F_{11})| = 16$ (i.e. 15+O)

Example on F_{31} – Complexity Increases

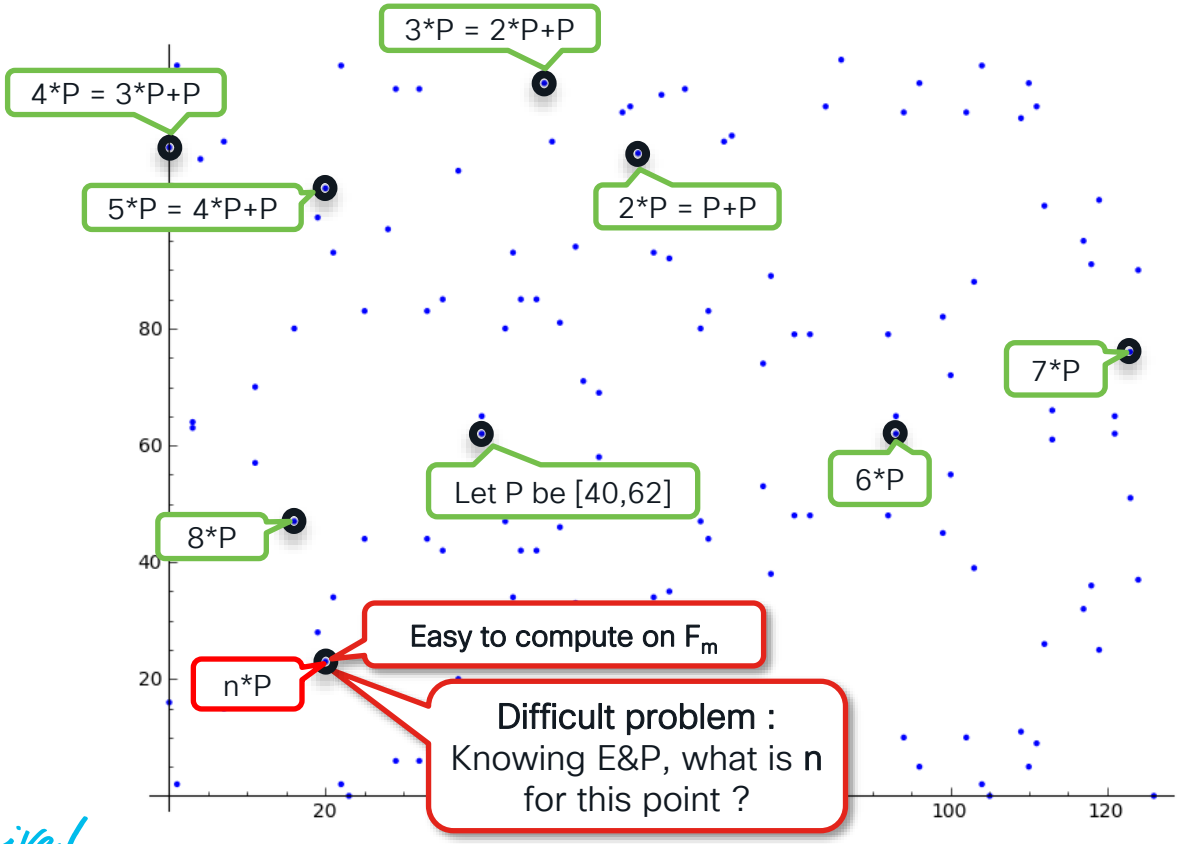


$m = 2^5-1 = 31$

$E(F_{31})$: $y^2 = x^3 + x + 2$

$|E(F_{31})| = 24$

The same on F_{127} – Complexity Further Increases

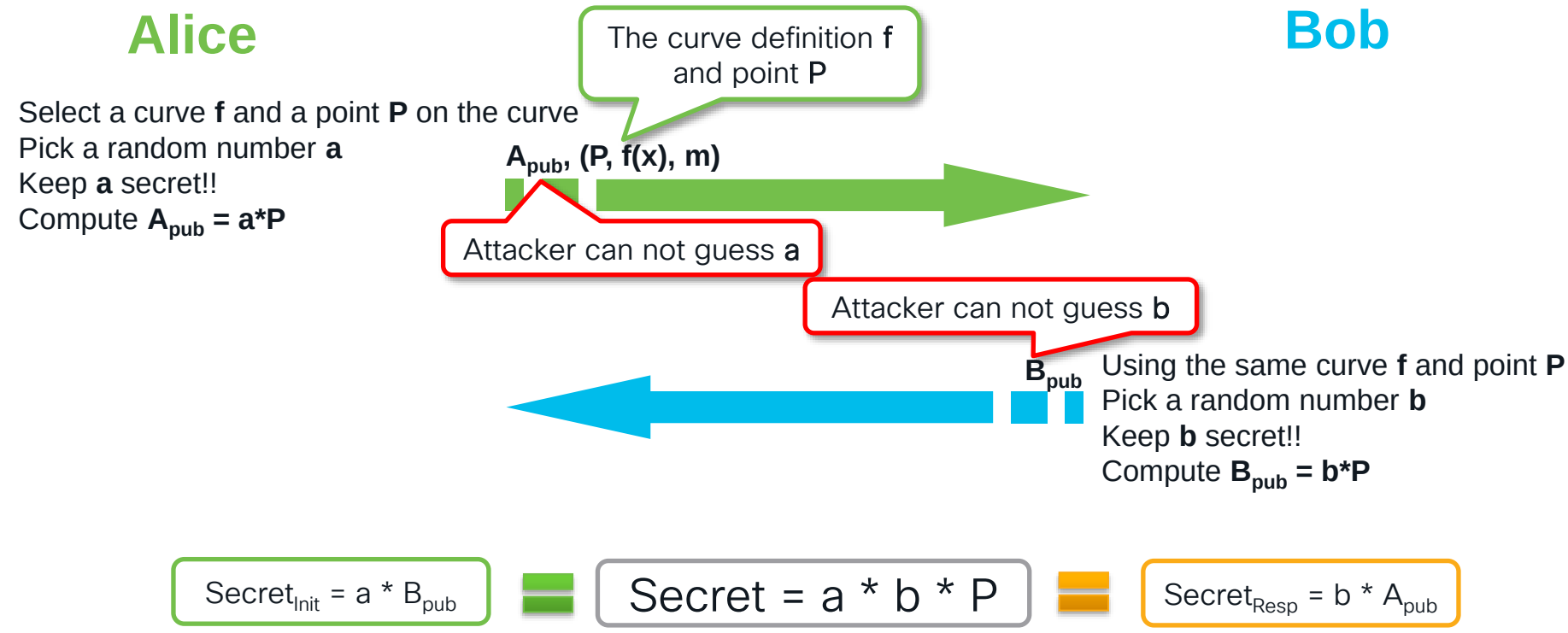


$m = 2^7-1 = 127$

$E(F_{127})$: $y^2 = x^3 + x + 2$

$|E(F_{127})| = 136$

ECDH – Elliptic Curve Diffie-Hellman



Representation of Elliptic Curves

- Elliptic curve domain parameters
  - (p, a, b, G, n, h) for a curve over a prime field F_p
  - (m, f(x), a, b, G, n, h) for a curve over a binary field F_{2^m}
- Where
  - **p** is the prime modulus
  - **G** is the generator (base point) of the curve
  - **n** is the order of G. i.e **n*G=O**
  - **a, b** are the coefficient of $y^2 + xy = x^3 + ax + b \pmod p$
- Who defines elliptic curves ?
  - National Institute of Standards and Technology (NIST)
  - American National Standard Institute (ANSI)
  - Agence Nationale pour la Securité des Systèmes Informatiques(ANSSI)
  - Institute of Electrical and Electronics Engineers (IEEE)
  - Certicom
  - Brainpool ECC

P-256 from "NIST routines"

4.3 Curve P–256

4.3.1 Parameters

The curve P–256 is given by the following parameters (see also [FIPS186-2]). The prime $p_{256} = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$:

$p_{256} =$ 115792089210356248762697446949407573530086143415290314195533631308867097853951

in hexadecimal form:

$p_{256} =$ ffffffff 00000001 00000000 00000000 00000000 ffffffff ffffffff ffffffff

The parameter $a = p_{256} - 3$:

$a =$ 115792089210356248762697446949407573530086143415290314195533631308867097853948

in hexadecimal form:

$a =$ ffffffff 00000001 00000000 00000000 00000000 ffffffff ffffffff fffffffc

the parameter b:

$b =$ 41058363725152142129326129780047268409114441015993725554835256314039467401291

in hexadecimal form:

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

Base point G:

$x_G =$ 48439561293906451759052585252797914202762949526041747995844080717082404635286

$y_G =$ 36134250956749795798585127919587881956611106672985015071877198253568414405109

in hexadecimal form:

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

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

in hexadecimal form with X9.63 compression (lead byte 02 if y_G is even, 03 if y_G is odd):

$\overline{G} =$ 00000003 6b17d1f2 e12c4247 f8bce6e5 63a440f2 77037d81 2deb33a0 f4a13945 d898c296

Order q of the point G (and of the elliptic curve group E):

$q =$ 115792089210356248762697446949407573529996955224135760342422259061068512044369

hexadecimal form:

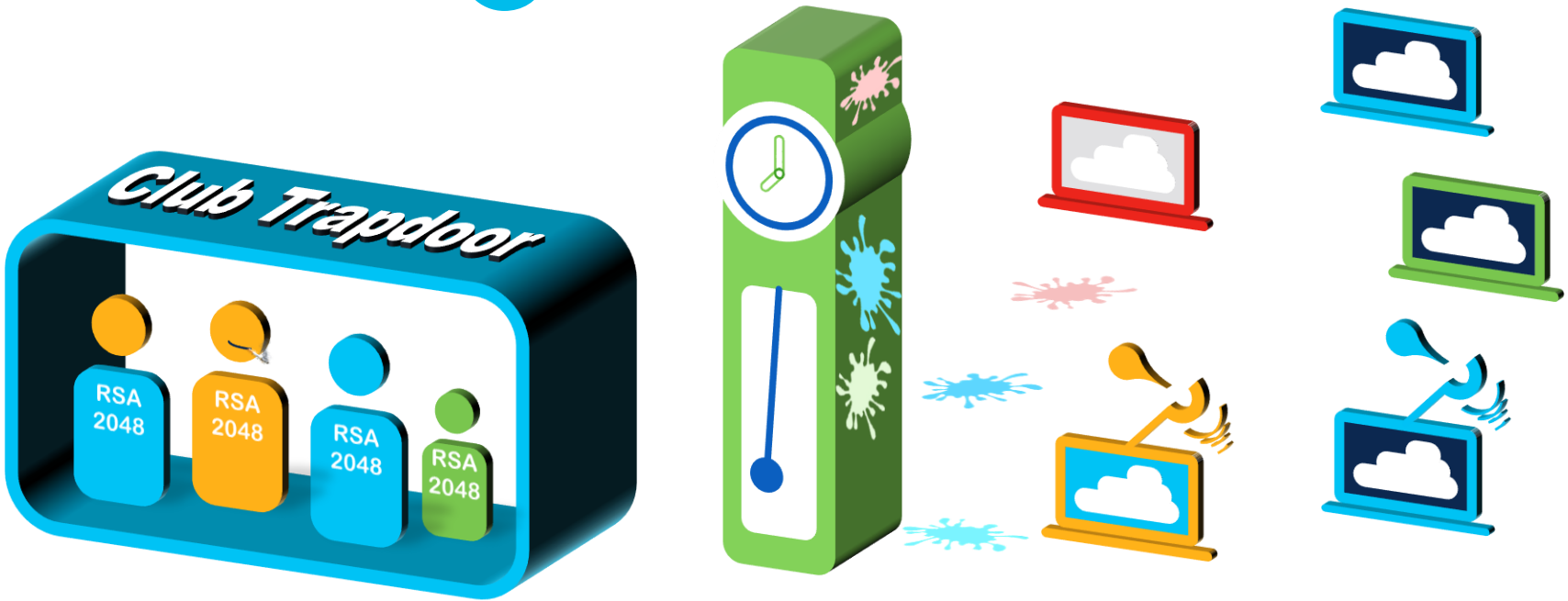
$q =$ ffffffff 00000000 ffffffff ffffffff bce6faad a7179e84 f3b9cac2 fc632551

Enters the Quantum Computer

Today's Cryptography Temporal Defense

TIME PROTECTS PUBLIC KEYS (Until Y2Q)

Public Key = Prime 1 x Prime 2



Shor's Factoring Algorithm

Problem: For a given "N" find a "p" between "1" and "N" that divides "N"

$N = p_1 * p_2$

Peter Shor

1994

Part A
Classic
Reduction of factoring problem to period finding problem

Part B
Quantum
Solve period finding problem using Quantum Fourier Transform

(Probabilistic Algorithm)

(Adjust it to taste if it's wrong)

Shor's algo converts exponential complexity to polynomial complexity

$x^N \rightarrow N^x$ where N is the number of bits

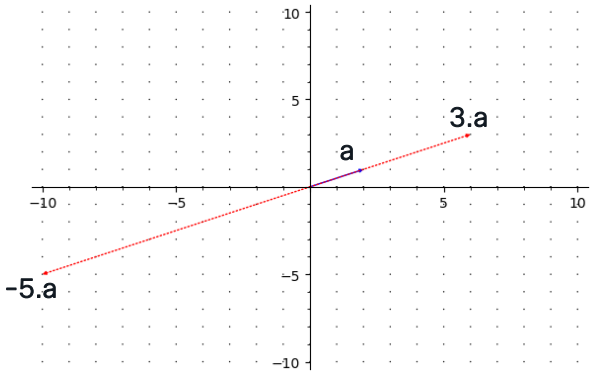
Lattice Based Cryptography

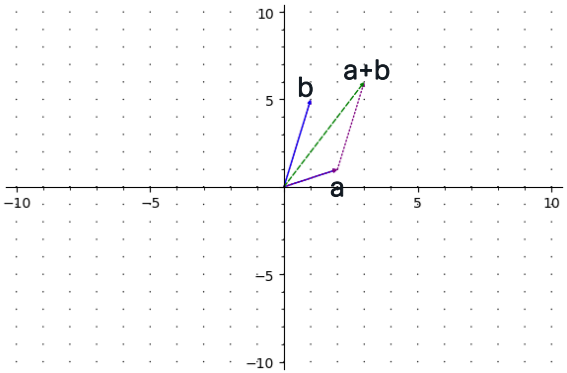
LBC, LWE, NTRU

Vectors

Commonly denoted $\boldsymbol{v}$ or $\vec{v}$
We will use ***v*** *or* $\boldsymbol{v}$

$$\boldsymbol{a} = \begin{bmatrix} a_1 \\ a_2 \\ \dots \\ a_n \end{bmatrix} \qquad \boldsymbol{b} = \begin{bmatrix} b_1 \\ b_2 \\ \dots \\ b_n \end{bmatrix}$$



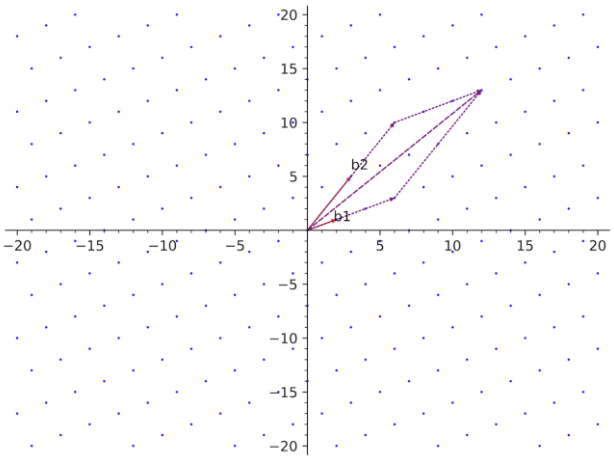


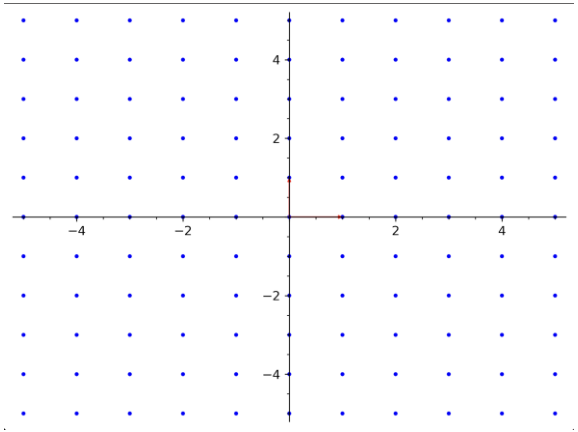
Operation	Formula	Result type
addition	$\boldsymbol{a}+\boldsymbol{b} = (a_1+b_1,\dots,a_2+b_2)$	Vector
Scalar multiplication	$x.\boldsymbol{a} = x.a_1+\dots+x.a_n$	Vector
Inner product	$\boldsymbol{a}.\boldsymbol{b} = a_1b_1+\dots+a_nb_n$	Scalar (number)

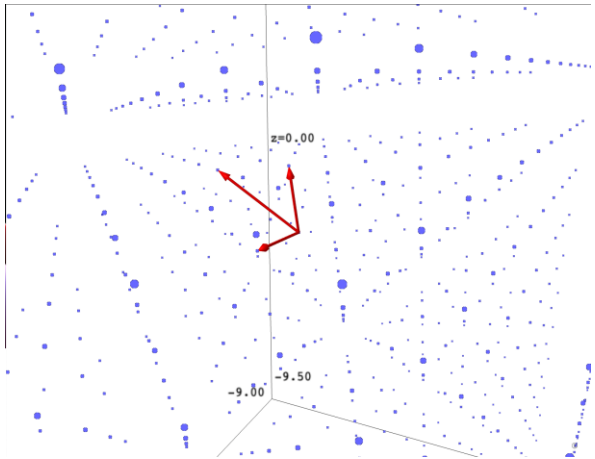
This is not a lattice

What is a Lattice ?

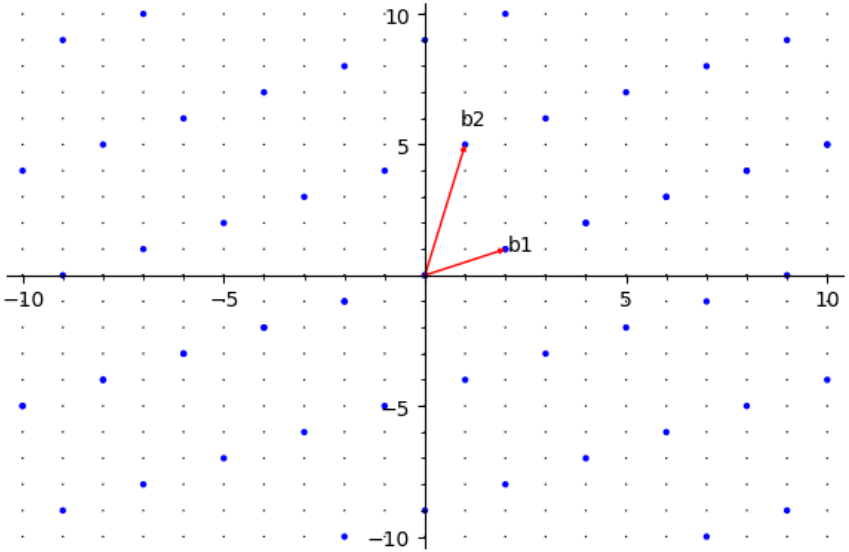
- A periodic “grid” in $\mathbb{Z}^m$
- All integer linear combinatons of n basis vectors $\mathbf{b_1}, \mathbf{b_2}, \ldots, \mathbf{b_n}$
- Basis $\mathbf{B} = \{\mathbf{b_1}, \ldots, \mathbf{b_m}\}$
- Lattice $\mathcal{L} = \sum_{i=1}^{m} a_i \cdot \boldsymbol{b}_i \ , a_i \in \mathbb{Z}$

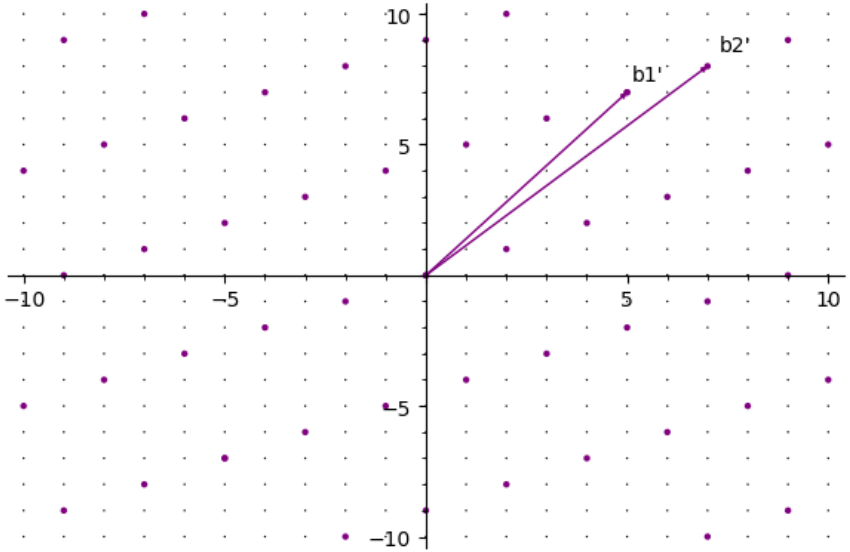






Good Basis, Bad Basis

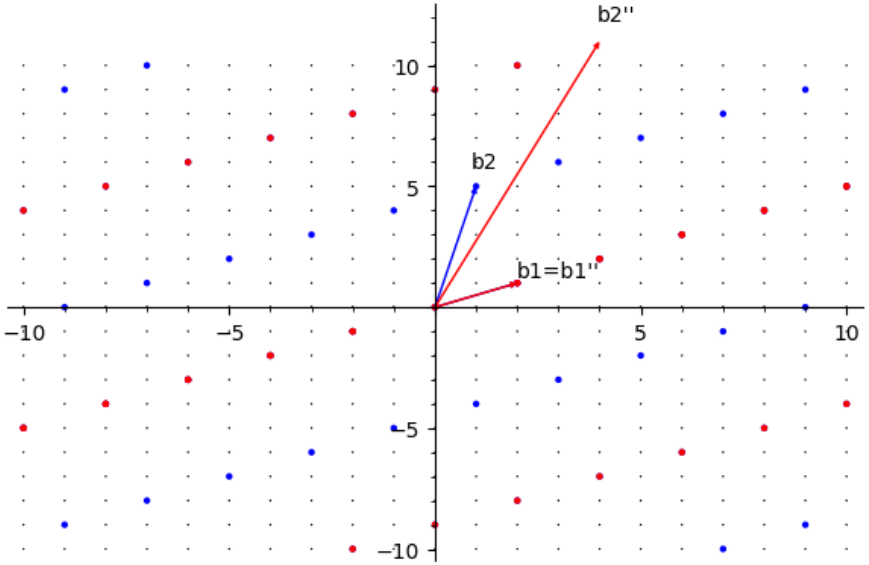




B= {$\mathbf{b}_1$, $\mathbf{b}_2$}: good basis
Short, almost perpendicular vectors

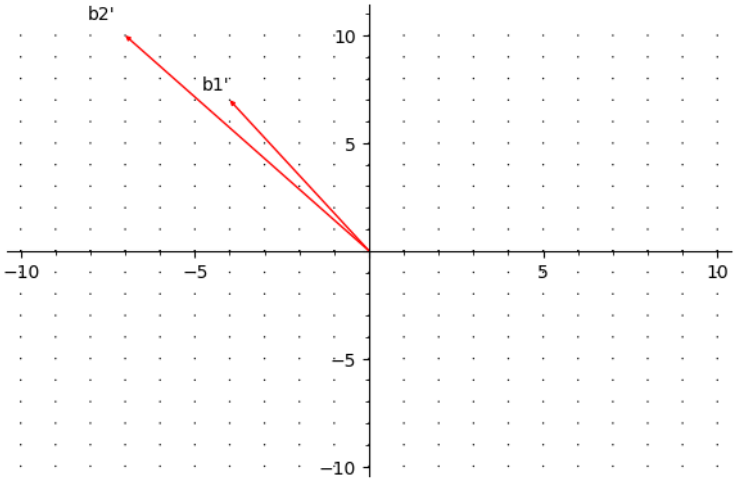
B= {$\mathbf{b}_1$', $\mathbf{b}_2$'}: bad basis
Long, not very perpendicular vectors

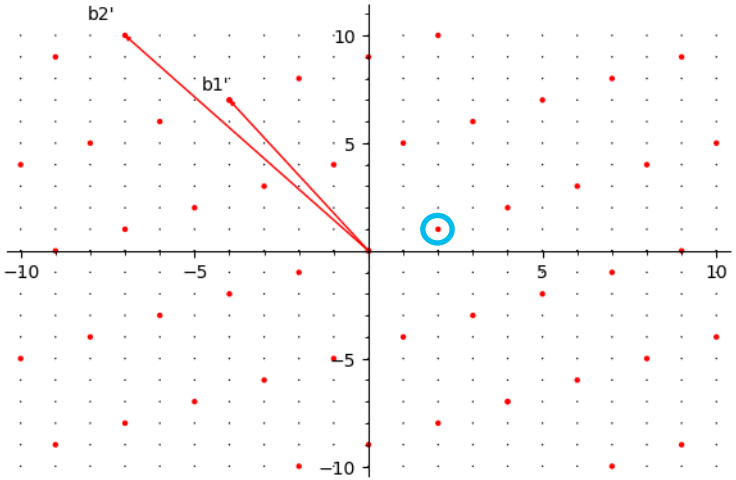
Not a basis



B= {b_1'', b_2''}: not a basis
The lattices do not overlap fully

Short Vectors is a Hard Problem



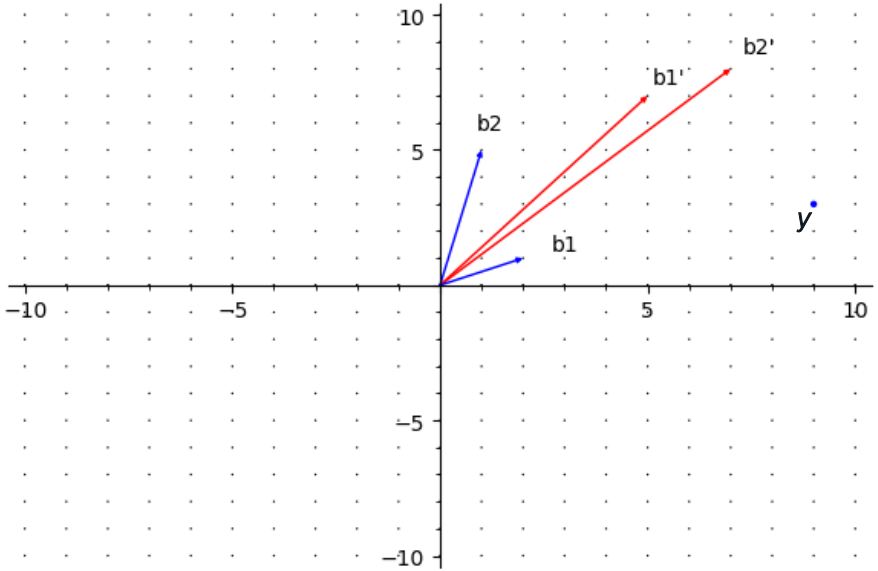


Given this base, what is the shortest possible non-trivial vector ?

Surprise!

Closest Vector Problem is a Hard Problem

What is the closest lattice vector to y ?



Babai's round-off algorithm:

$$\boldsymbol{v} = B.\lfloor B^{-1}.\boldsymbol{y} \rceil$$

Theorem:

$$\|\boldsymbol{v} - \boldsymbol{y}\| \leq \frac{1}{2}\sum \|\boldsymbol{b_i}\|$$

In clear:
Better base ➔ Closer vector

Short Integer Solution & Learning With Errors

SIS

$A\boldsymbol{z} = 0$ with 'short' $\boldsymbol{z} \neq 0$

Average case SVP
(Bounded Distance Decision)

$$\mathcal{L}^{\perp}(A) = \{z \in \mathbb{Z}^m : A\boldsymbol{z} = 0\}$$

LWE

$(A, \boldsymbol{b}^t = \boldsymbol{s}^t A + \boldsymbol{e}^t)$ vs. $(A, \boldsymbol{b}^t)$

Average case BDD
(Bounded Distance Decision)

$$\mathcal{L}\,(A) = \{\boldsymbol{z}^t \equiv \boldsymbol{s}^t A \bmod q\}$$

These are other ways to define a lattice

Example Only!

Goldreich, Goldwasser, Halevi Cryptosystem

Alice

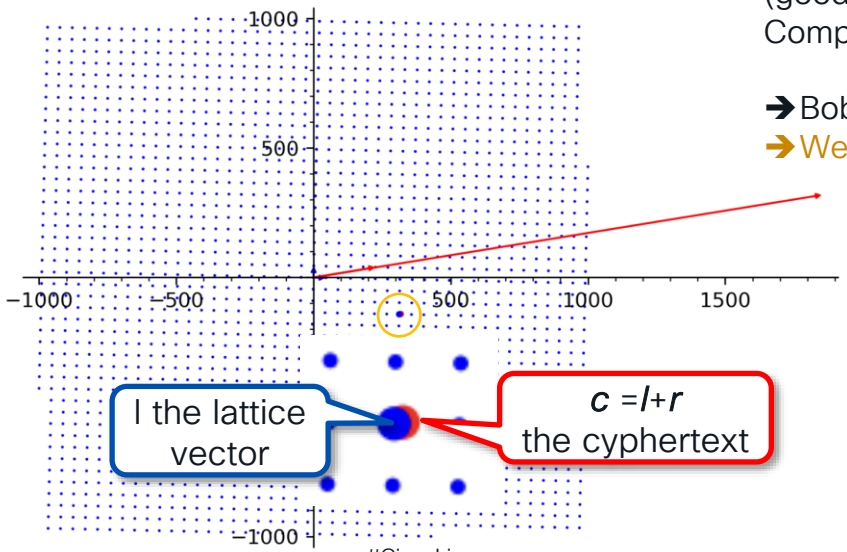
Must send a private message **m**

Takes **V'** from Bob
Computes $l = m * V'$
Generates an error vector r (n)
Computes $c = l + r$

Quantum secure
... but broken ☹

Eve can not guess *m* because of the Closest Vector Problem (bad basis)

c



Bob

Generates **V** (nxn), a good basis
Publishes **V'** (nxn), a bad basis

Applies Babai on (V, *c*) → finds *l*
(good basis → accuracy)
Computes $m = l * V'^{-1}$

➔Bob has reversed the operation !!
➔We have an encryption scheme

Post Quantum Algorithm Selection – Round 3

Type	Name	Math
Pub Key Encr and Key Exchange	Classic McEliece	Linear Code
Pub Key Encr and Key Exchange	CRYSTAL-KYBER	Lattice LWE (CVP)
Pub Key Encr and Key Exchange	NTRU	Lattice SVP
Pub Key Encr and Key Exchange	SABER	Module Learning with Rounding
Digital Signature Algo.	CRYSTAL-DILITHIUM	Lattice LWE (CVP)
Digital Signature Algo.	FALCON	Lattice NTRU(SVP) + FFT
Digital Signature Algo.	Rainbow	Mutlivariate Public Key

Recommendations and Conclusion

Reassurance

- Crypto is not broken; it evolves and so do attackers.
- These are good news! The more research, the more insight.
- Lattices represent an interesting development but are not alone.

Evolve your systems as new recommended algorithms are released !

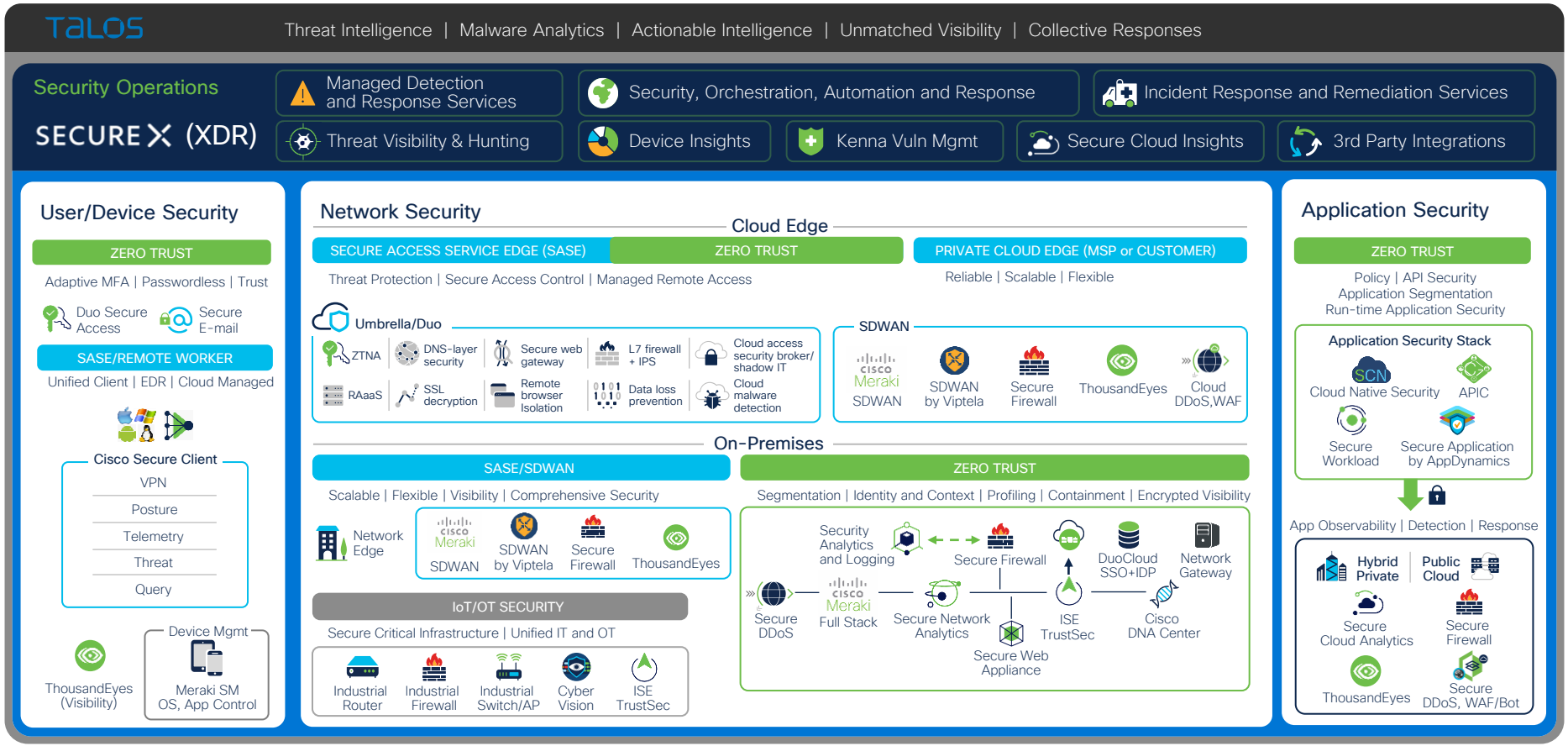
A Short Bibliography

- NIST SP 800-90A : Recommendations for Random Number Generation Using Deterministic Random Bit Generators
- NIST SP 800-38D : Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC
- NIST SP 800-56A (R2): Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (i.e. DH, ECDH + key derivation methods)
- NIST 800-131Ar1: Transitions: Recommendations fro Transitioning the Use of Cryptographic Algorithms and Key Lengths
- NIST FIPS 140-2: Security Requirements for Cryptographic Modules
- NIST FIPS 186-4: Digital Signature Standard (DSS) (DSA, RSA (PKCS#1), ECDSA,...)
- NIST FIPS 180-4: Secure Hash Standard (SHA-1, SHA-256,..., SHA-512)
- NIST Routines: https://www.nsa.gov/ia/_files/nist-routines.pdf (Curve P-192, P-224, P-256 etc.)
- Safe Curves: http://safecurves.cr.yp.to
- Transcript Collision Attacks: Breaking authentication in TLS, IKE and SSH: http://www.mitls.org/downloads/transcript-collisions.pdf

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.

Cisco Secure | Security Reference Architecture



Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

Certify

Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

cisco Live!

Thank you


cisco Live!
ALL IN