CSE 107: Introduction to Modern Cryptography

Nadia Heninger

UCSD

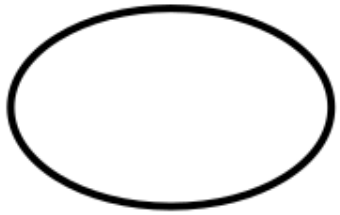
Winter 2025 Lecture 16

Last time:

- Digital signatures

This time:

- Elliptic curve cryptography



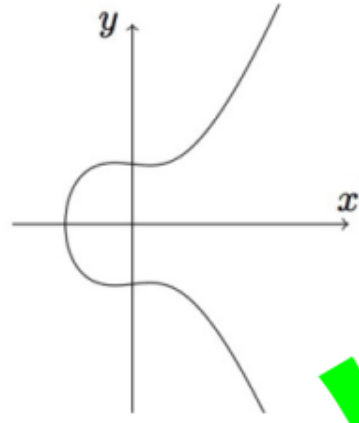
Ellipse

Elliptical

Eclipse

• • •

Ellipsis

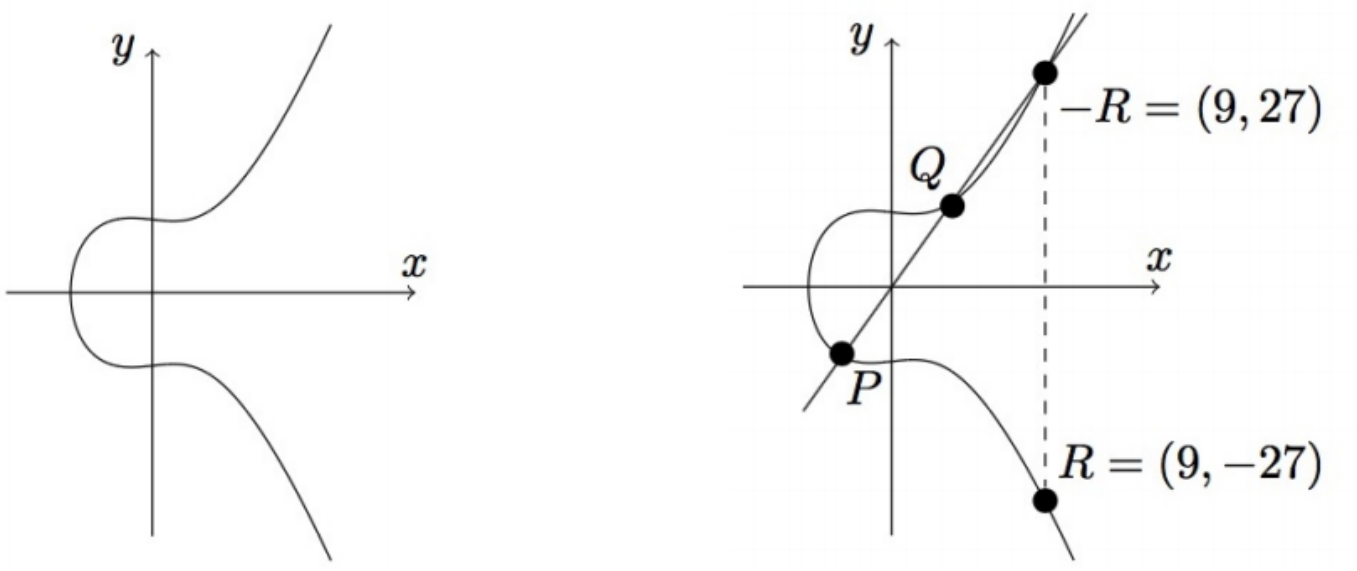


Elliptic Curve

Elliptic curves: Motivations

- Factoring and finite field discrete log both have subexponential-time algorithms.
- Current records: 829 bits for factoring, 795 bits for discrete log.
- Current recommendations: use 2048-bit public keys for RSA, Diffie-Hellman, or DSA.
- These are large, so the operations are slow.
- The best classical cryptanalysis we have for elliptic curves is much weaker, exponential time, so key sizes can be much smaller for the same security level.

Points on an elliptic curve

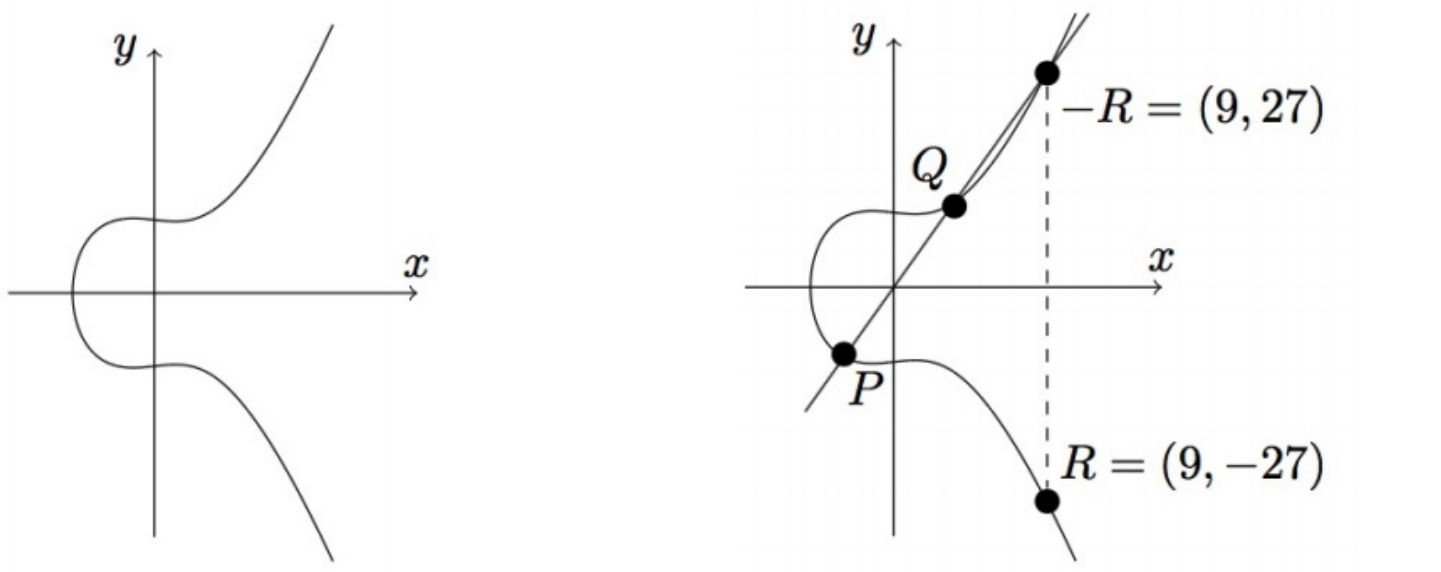


(a) The curve (b) Adding $P = (-1, -3)$ and $Q = (1, 3)$

Figure 15.1: The curve $y^2 = x^3 - x + 9$ over the reals (not drawn to scale)

- Every intro to elliptic curves includes a figure like this.
- The curve is defined by an equation $y^2 = x^3 + ax + b$.
- This picture plots this curve over $\mathbb{R}^2$.
- Classically, Diophantus and Poincaré were interested in rational points $(x, y) \in \mathbb{Q}^2$ on this curve.

Points on an elliptic curve



(a) The curve (b) Adding $P = (-1, -3)$ and $Q = (1, 3)$

Figure 15.1: The curve $y^2 = x^3 - x + 9$ over the reals (not drawn to scale)

- Poincare's method for finding rational points:
  - Take two rational points, define a line (like $y = 3x$ above), and substitute to get a univariate cubic equation.
  - Since it has two rational roots already, the third root is also rational.
  - Get two new points for free: R and $-R$.
- Can define this as a group law: $P + Q = -R$.
- (The operation "+" means apply the above procedure.)

Elliptic curves over finite fields

- For cryptography, we define curves over $\mathbb{F}_p$. Still have curve equation $y^2 = x^3 + ax + b$, with $a, b \in \mathbb{F}_p$, $4a^3 + 27b^2 \neq 0$.
- $E(\mathbb{F}_p) = \{(x, y) \mid x, y \in \mathbb{F}_p, y^2 = x^3 + ax + b \bmod p\}$.
- This is called Weierstrass form. Every elliptic curve can be written in this form.
- Can write down point addition in terms of (x, y) coordinates but it's long and has multiple cases.
- Identity element: Special point $\mathcal{O}$ is "point at infinity".

Elliptic curve point addition in Weierstrass form

PROPOSITION 8.68 *Let $p \geq 5$ be prime and let E be the elliptic curve given by $y^2 = x^3 + Ax + B \bmod p$ where $4A^3 + 27B^2 \neq 0 \bmod p$. Let $P_1, P_2 \neq \mathcal{O}$ be points on E, with $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$.*

1. *If $x_1 \neq x_2$, then $P_1 + P_2 = (x_3, y_3)$ with*

$$x_3 = [m^2 - x_1 - x_2 \bmod p] \quad \text{and} \quad y_3 = [m \cdot (x_1 - x_3) - y_1 \bmod p],$$

where $m = \left[\frac{y_2 - y_1}{x_2 - x_1} \bmod p\right]$.

2. *If $x_1 = x_2$ but $y_1 \neq y_2$ then $P_1 = -P_2$ and so $P_1 + P_2 = \mathcal{O}$.*

3. *If $P_1 = P_2$ and $y_1 = 0$ then $P_1 + P_2 = 2P_1 = \mathcal{O}$.*

4. *If $P_1 = P_2$ and $y_1 \neq 0$ then $P_1 + P_2 = 2P_1 = (x_3, y_3)$ with*

$$x_3 = [m^2 - 2x_1 \bmod p] \quad \text{and} \quad y_3 = [m \cdot (x_1 - x_3) - y_1 \bmod p],$$

where $m = \left[\frac{3x_1^2 + A}{2y_1} \bmod p\right]$.

Edwards curves

Some curves admit nicer representations:

- Edwards curves have a simpler addition law that also allows faster operations.
- A curve $E/\mathbb{F}_p$ in Edwards form can be written $x^2 + y^2 = 1 + dx^2y^2$, $d \in \mathbb{F}_p$, $d \notin \{0, 1\}$.
- Edwards point addition: $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$

$$P_1 + P_2 = \left(\frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right)$$

Elliptic curve scalar multiplication and discrete log

We have a group law $P + Q = R$, usually written as "addition".

Scalar multiplication of points

- If we iterate the group law a times on a point P, we get a point $aP = P + P + \cdots + P$, a times.
- Input: $a \in \mathbb{Z}$, $P \in E(\mathbb{F}_p)$, Output: $aP \in E(\mathbb{F}_p)$
- This can be implemented efficiently (polynomial in $\log a$, $\log p$, with double-and-add, analogous to square-and-multiply that we saw before.

Elliptic curve scalar multiplication and discrete log

We have a group law $P + Q = R$, usually written as "addition".

Scalar multiplication of points

- If we iterate the group law a times on a point P, we get a point $aP = P + P + \cdots + P$, a times.
- Input: $a \in \mathbb{Z}$, $P \in E(\mathbb{F}_p)$, Output: $aP \in E(\mathbb{F}_p)$
- This can be implemented efficiently (polynomial in $\log a$, $\log p$, with double-and-add, analogous to square-and-multiply that we saw before.

Elliptic curve discrete log

- Input: base point P, target $Q \in E(\mathbb{F}_p)$; output a s.t. $aP = Q$.
- For some families of curves, best algorithms known are generic group algorithms like baby step giant step. They take $O(\sqrt{q})$ time for group order q.
- Broken in polynomial time by a quantum computer.

Cyclic groups over elliptic curve points

1. Pick a prime p. Pick $a, b \in \mathbb{F}_p$. Consider the elliptic curve $E(\mathbb{F}_p) = \{(x, y) \mid x, y \in \mathbb{F}_p, y^2 = x^3 + ax + b \bmod p\}$.
2. $E(\mathbb{F}_p)$ is a group with operation point addition. There is an efficient algorithm to compute the order $|E(\mathbb{F}_p)| = m$.
3. Pick a point $G = (x_G, y_G)$ on $E(\mathbb{F}_p)$.
4. Consider the cyclic subgroup $\langle G \rangle \subset E(\mathbb{F}_p)$ generated by G. This contains the points $G, G + G, \ldots,$. At some point you will get $\mathcal{O}$.
5. We can compute the order of $|\langle G \rangle| = n$. For cryptography we want this order n prime.

We constructed Diffie-Hellman key exchange and digital signatures over multiplicative groups modulo p.

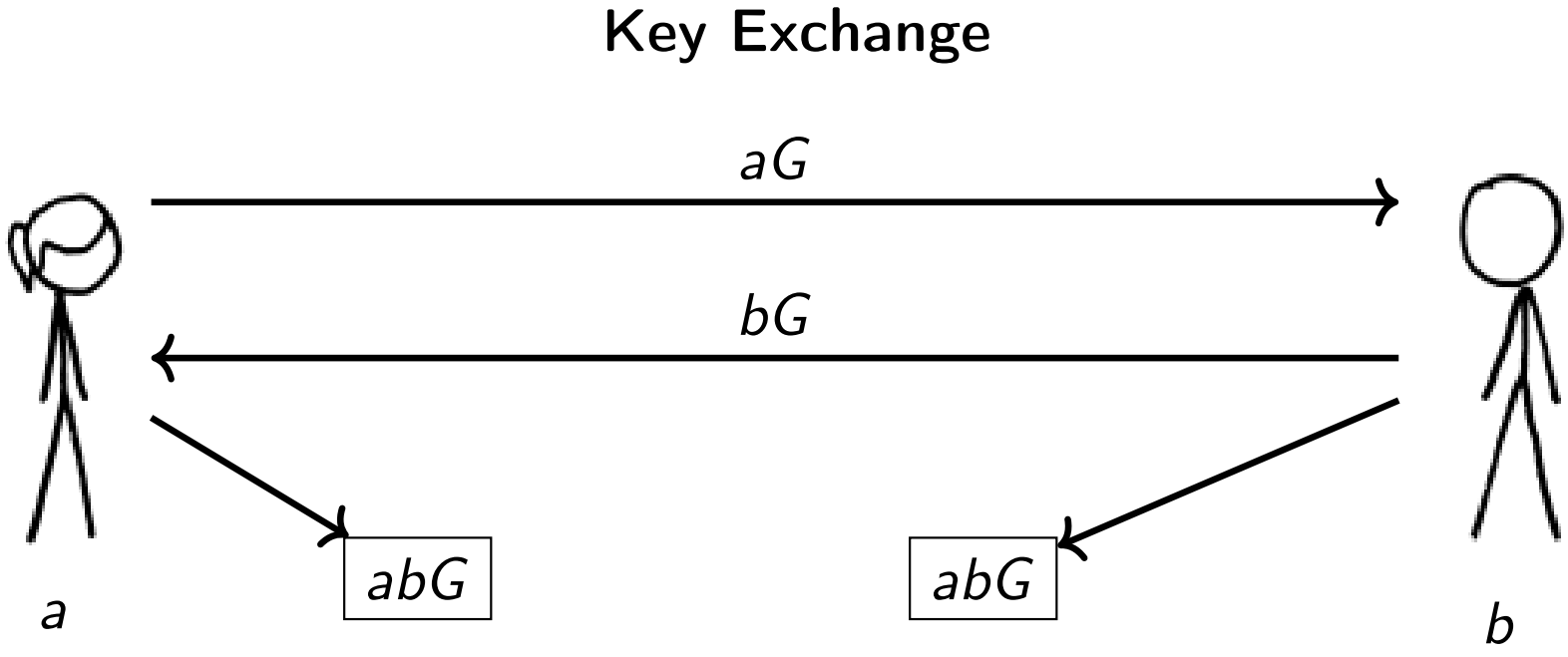
We can now translate these constructions to cyclic groups defined over points on elliptic curves modulo p.

Elliptic Curve Diffie-Hellman

Public Parameters

E an elliptic curve over $\mathbb{F}_p$

G group generator of order n



Elliptic Curve Key Encapsulation Mechanism

Let $E(\mathbb{F}_p)$ be an elliptic curve group with generator G of order n agreed upon by both parties beforehand. Let F be a key derivation function.

- Gen: Input elliptic curve group generator G, order n. Choose x mod n. $pk = X = xG$, $sk = x$.
- E: Generate y mod n, output $Y = yG$.
- D: Input $sk = x$ and public share Y. Output $k = F(xY)$.

The key k can then be used with a CCA-secure encryption scheme like AES-GCM to provide CCA-secure public-key encryption. This is called ECIES (Elliptic Curve Integrated Encryption Scheme).

ECDSA (Digital Signature Algorithm)

Public Key

E an elliptic curve over $\mathbb{F}_p$

G group generator (base point) on E of order n

$Q = dG$

Private Key

d private key

Verify

$u_1 = H(m)s^{-1} \bmod n$

$u_2 = rs^{-1} \bmod n$

$r \stackrel{?}{=} x\text{-coord of } u_1 G + u_2 Q$

Sign

Generate random k.

$r = x\text{-coordinate of } kG.$

$s = k^{-1}(H(m) + dr) \bmod n$

Output (r, s)

Breaking ECDSA with bad signature nonce generation

Sign

1. Input message hash h.
2. Choose integer k mod n.
3. Compute point $(r, y_r) = kG$.
4. Output $(r, s = k^{-1}(h + dr) \bmod n)$.

Potential pitfall #1

k must remain secret, or else the long-term secret key d is revealed.

$$d = (sk - h)r^{-1} \bmod n$$

Breaking ECDSA with bad signature nonce generation

Sign

1. Input message hash h.
2. Choose integer k mod n.
3. Compute point $(r, y_r) = kG$.
4. Output $(r, s = k^{-1}(h + dr) \bmod n)$.

Potential pitfall #2

k must never be reused to sign distinct messages h_1, h_2 or else k and thus d can be computed.

$$k = (h_1 - h_2)(s_1 - s_2)^{-1} \bmod n$$

Standardized Elliptic Curves

Curves that withstand all known attacks are more complex to generate than primes, so everyone uses a small number of curves.

NIST P256

- Works over $\mathbb{F}_p$ with $p \approx 2^{256}$.
- Has prime order $q \approx 2^{256}$.
- Best attack: $\sqrt{q}$ time $\approx 2^{128}$.
- Curve parameters generated from deterministic algorithm by opaque seed of unknown generation.

Standardized Elliptic Curves

Curves that withstand all known attacks are more complex to generate than primes, so everyone uses a small number of curves.

NIST P256

- Works over $\mathbb{F}_p$ with $p \approx 2^{256}$.
- Has prime order $q \approx 2^{256}$.
- Best attack: $\sqrt{q}$ time $\approx 2^{128}$.
- Curve parameters generated from deterministic algorithm by opaque seed of unknown generation.

Curve25519

- Edwards curve designed by Daniel J. Bernstein
- Designed to make implementations "secure by default":
  - Simplified group law easier to protect against side-channel attacks
  - Minimal/no point validation required
  - "Twist-secure": Also minimize validation necessary for implementations that only input x-coordinate.

Elliptic curve choices in TLS 1.3 key exchange

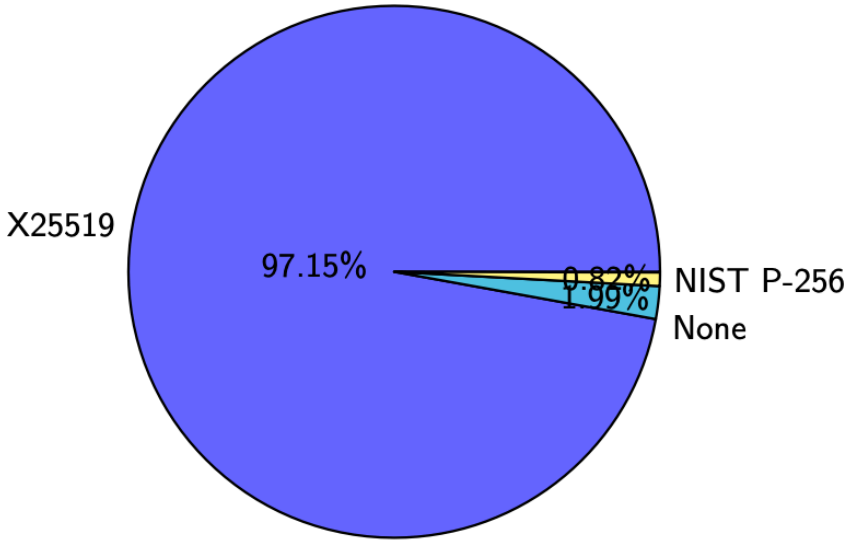


Figure: 2022-02-12 Server Selected Key Shares

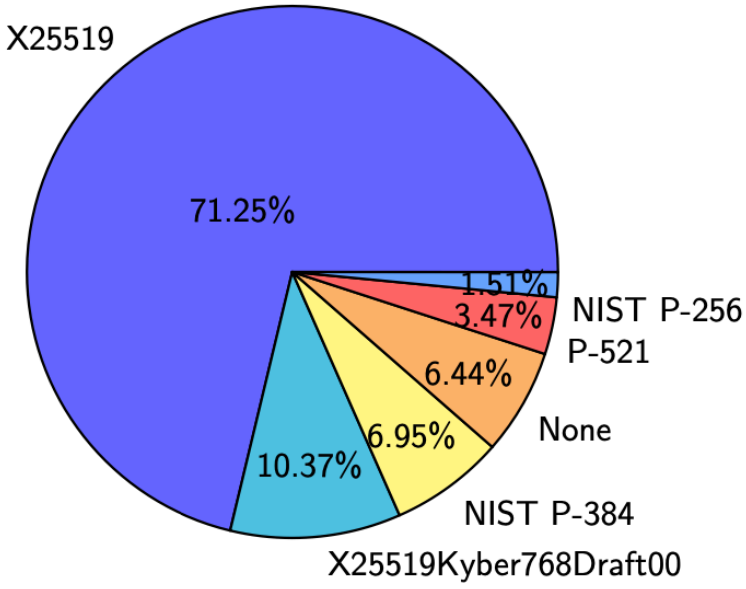


Figure: 2024-08-27 Server Selected Key Shares

Elliptic curves and quantum computers

NSA has been strongly pro elliptic curve cryptography for decades.

In 2015, NSA recommended against transitioning to elliptic curves for people who hadn't already.

Official explanation: Quantum computers are coming, so people should wait for post-quantum crypto.

Plausible explanation:

- Smaller key sizes for ECC mean fewer qubits required to break than 3072-bit factoring.

The Dual EC saga

The "Dual Elliptic Curve Deterministic Random Bit Generator" was a controversial random number generator standard.

It is widely believed to have been backdoored, and the standard has been retracted.

Dual EC DRBG History

- Early 2000s: Created by the NSA and pushed towards standardization
- 2004: Published as part of ANSI X9.82 part 3 draft
- 2004: RSA makes Dual EC the default PRNG in BSAFE
- 2005: Standardized in NIST SP 800-90 draft
- 2007: Shumow and Ferguson demonstrate theoretical backdoor
- 2013: Snowden documents lead to renewed interest in Dual EC
- 2014: Practical attacks on TLS using Dual EC demonstrated
- 2015: NIST removes Dual EC from list of approved PRNGs

Dual EC DRBG

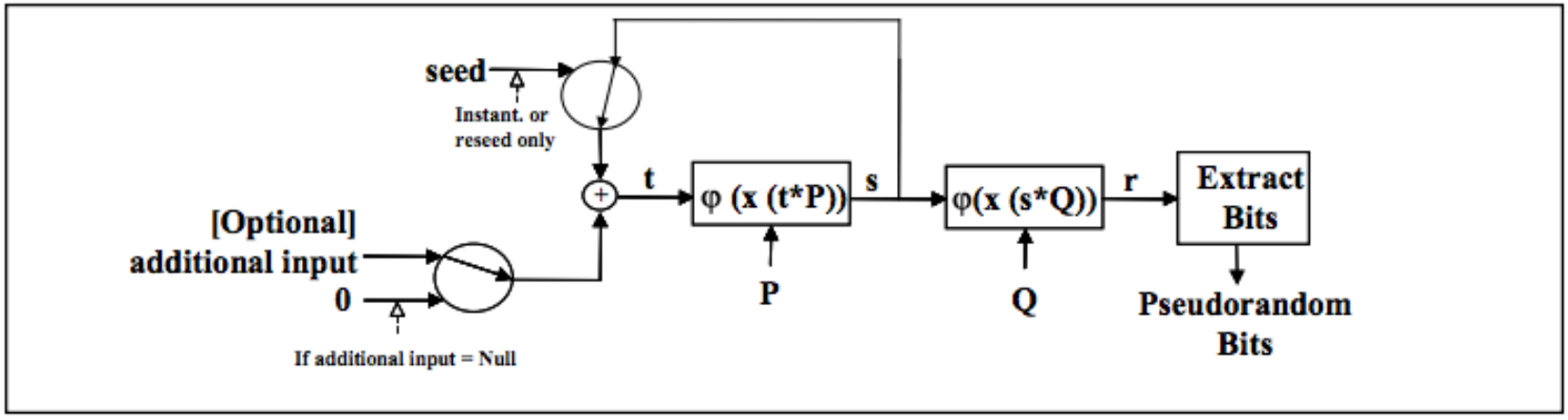


Figure 13: Dual_EC_DRBG

- Parameters: Pre-specified elliptic curve points P and Q.
- Seed: 32-byte integer s
- State: x-coordinate of point sP. ($\phi(x(sP))$ above.)
- Update: $t = s \oplus$ optional additional input. State $s = x(tP)$.
- Output: At state s, compute x-coordinate of point $x(sQ)$, discard top 2 bytes, output 30 bytes.

Shumow and Ferguson 2007

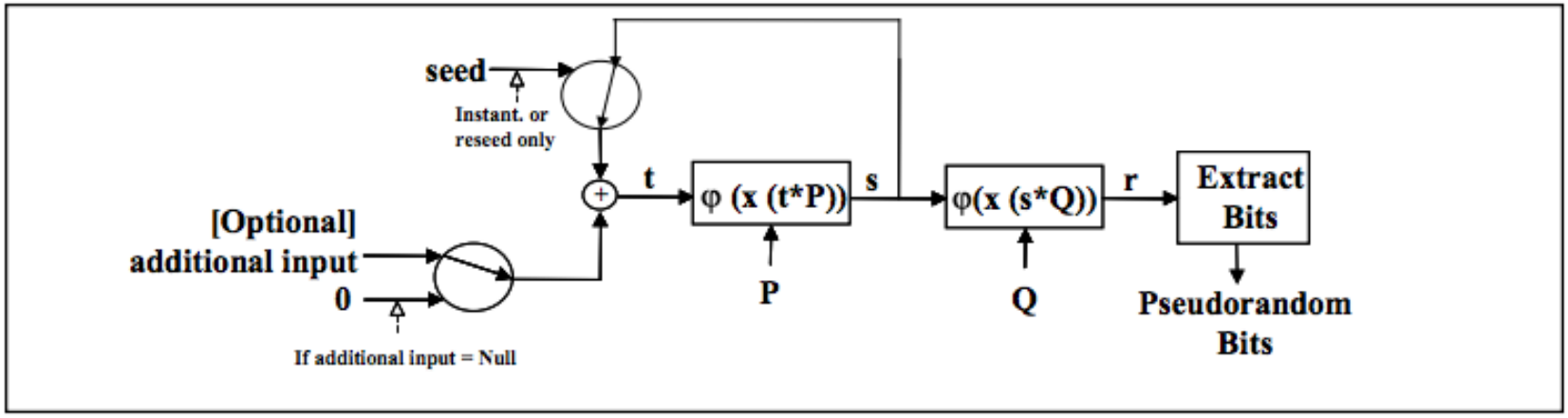


Figure 13: Dual_EC_DRBG

1. Assume attacker controls standard and constructs points with known relationship $P = dQ$.
2. Attacker gets 30 bytes of x-coordinate of sQ. Attacker brute forces 2^{16} MSBs, gets 2^{17} possible y-coordinates, ends up with 2^{15} candidates for sQ.
3. For each candidate sQ attacker computes $dsQ = sP$ and compares to next output.

September 2013: NSA Bullrun in NY Times

- (TS//SI//REL TO USA, FVEY) Insert vulnerabilities into commercial encryption systems, IT systems, networks, and endpoint communications devices used by targets.
- (TS//SI//REL TO USA, FVEY) Collect target network data and metadata via cooperative network carriers and/or increased control over core networks.
- (TS//SI//REL TO USA, FVEY) Leverage commercial capabilities to remotely deliver or receive information to and from target endpoints.
- (TS//SI//REL TO USA, FVEY) Exploit foreign trusted computing platforms and technologies.
- (TS//SI//REL TO USA, FVEY) Influence policies, standards and specification for commercial public key technologies.
- (TS//SI//REL TO USA, FVEY) Make specific and aggressive investments to facilitate the development of a robust exploitation capability against Next-Generation Wireless (NGW) communications.

the grugq
@thegrugq

Follow

Woah! Juniper discovers a backdoor to decrypt VPN traffic (and remote admin) has been inserted into their OS source

Important Announcement about ScreenOS®

IMPORTANT JUNIPER SECURITY ANNOUNCEMENT CUSTOMER UPDATE: DECEMBER 20, 2015 Administrative Access (CVE-2015-7755) only affects ScreenOS 6.3.0r17 through

forums.juniper.net

Summary: Chinese hackers had repurposed Dual EC DRBG backdoor in Juniper's code to compromise Diffie-Hellman key exchange in VPN devices.