The Twisted Dual Elliptic Curve Deterministic Random Bit Generator

Holden Mui, Linus Tang, Noah Walsh

6.5610 Final Presentation

May 2025

Deterministic Random Bit Generators

A DRBG:

- outputs bit sequence given input seed
- is deterministic (produces same output given same seed)
- is secure (indistinguishable from true randomness without seed)

Why are DRBGs important?

- used to generate keys, nonces, and padding
  - example: TLS session keys, RSA private keys, cryptographic salt
- faster than hardware entropy sources
- debugging

Dual Elliptic Curve DRBG

The Dual EC DRBG:

- standardized by NIST in 2006
- uses elliptic curve

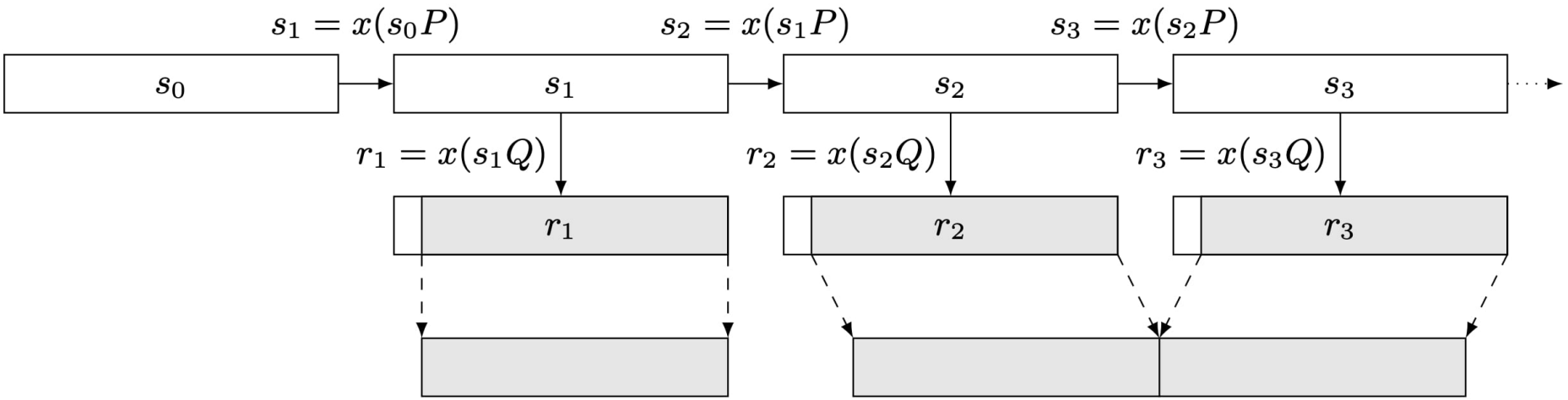
$$y^2 \equiv x^3 - 3x + b \pmod{2^{256} - 2^{224} + 2^{192} + 2^{96} - 1}$$

  with $b =$ 0x5ac...[58 digits]...04b.
- uses two fixed elliptic curve points

$$P = (\texttt{0x6b1}...[58\ \text{digits}]...296, \texttt{0x4fe}...[58\ \text{digits}]...\texttt{1f5}),$$
$$Q = (\texttt{0xc97}...[58\ \text{digits}]...192, \texttt{0xb28}...[58\ \text{digits}]...046).$$

- takes input seed s_0 and integer k, and outputs $240k$ bits

Dual EC DRBG Algorithm

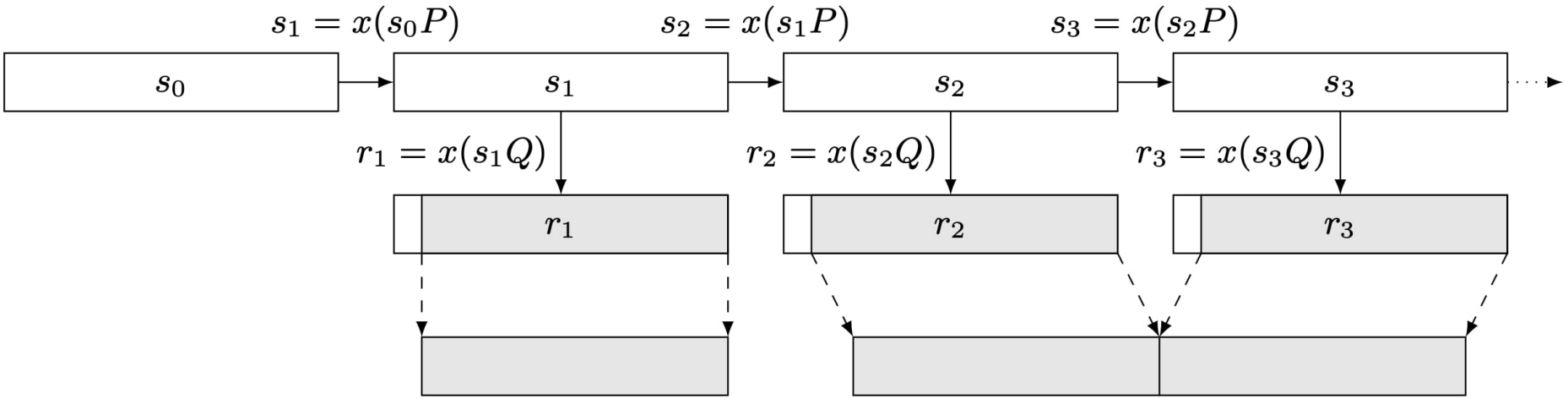


Input: seed $s_0 \in \mathbb{F}_p$ and $k \in \mathbb{Z}^+$

- set internal state s to s_0
- repeat k times:
  - replace s with sP's x-coordinate
  - output last 240 bits of sQ's x-coordinate

Is this secure? No!

Dual EC DRBG Backdoor



If adversary knows k for which $P = kQ$, then knowing sQ allows them to compute $ksQ = skQ = sP$. Since all but 16 bits of sQ's x-coordinate are revealed, an adversary can brute force to find the next internal state.

The Elliptic Curve Discrete Logarithm Problem is (probably) hard, so only the party publishing P and Q could know k...

Dual EC DRBG Timeline

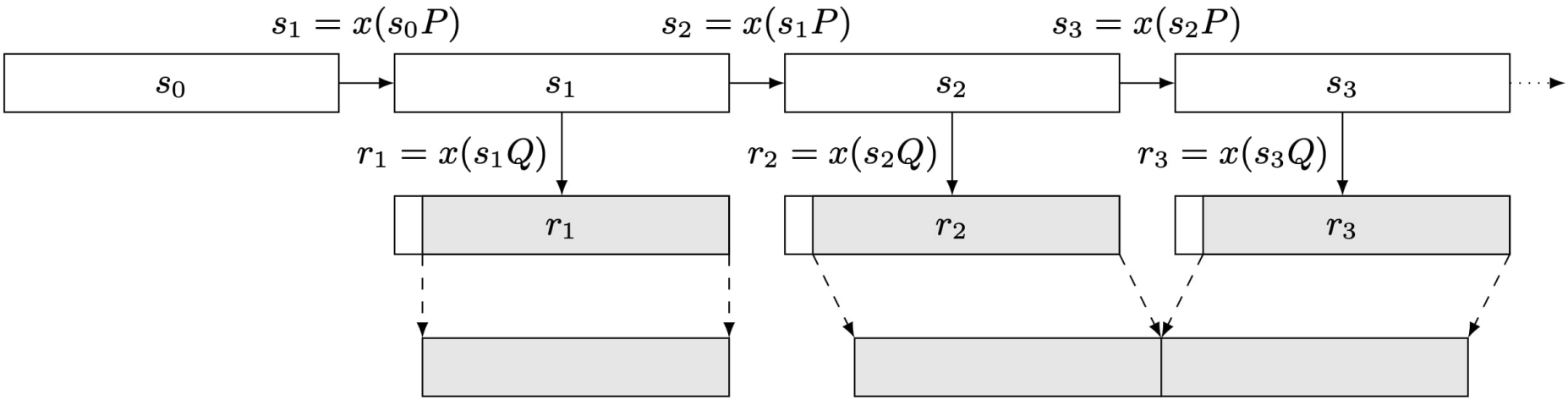
- early 2000s: developed by NSA
- 2004: RSA Security uses Dual EC DRBG as its default PRNG
- 2006: standardized by NIST
- 2007: Shumow and Ferguson demonstrate possible backdoor
  - NIST: "we have no evidence that anyone has, or will ever have, the 'secret numbers' for the backdoor... For this reason, we are not withdrawing the algorithm at this time."
- 2013: Snowden leaks documents suggesting backdoors in standards, including $10 million payment from NSA to RSA Security
- 2014: NIST removes Dual EC DRBG from list of standardized DRBGs

Dual EC DRBG undermined trust in government standards.

The Dual EC DRBG Distinguisher

Even worse: Dual EC DRBG is not a DRBG!

- Schoenmakers and Sidorenko, 2006: There is an algorithm (even without backdoor knowledge) that can distinguish Dual EC DRBG bits from truly random bits
- $\approx$ 2.5 hours with 54.9% success rate



Project Idea

Modify Dual EC DRBG to remove distinguisher but preserve backdoor!

We call our algorithm the *Twisted Dual EC DRBG*.

The Twisted Dual EC DRBG algorithm

Elliptic curve $\mathcal{E}$, quadratic twist $\mathcal{E}'$ over $\mathbb{F}_{2^{384}-2^{128}-2^{96}+2^{32}-1}$, chosen so both have prime order

- $P, Q \in \mathcal{E}$
- $P', Q' \in \mathcal{E}'$

Input: seed $s_0 \in \mathbb{F}_p$ and $k \in \mathbb{Z}^+$

- set internal state $s \in \mathbb{F}_p$ to s_0
- repeat k times:
  - let (a, b) be the last two bits of s
  - replace s with x-coordinate of sP if $a = 0$, sP' if $a = 1$
  - output all 384 bits of x-coordinate of sQ if $b = 0$, sQ' if $b = 1$

Our Work

- Algorithm design
- Security analysis
- Runtime analysis
- Implementation

Thank you!

Questions?