Dual EC and what it taught us about vulnerabilities of the standardization ecosystem

Tanja Lange

Technische Universiteit Eindhoven
http://projectbullrun.org/dual-ec/

30 September 2014

Random numbers are important

- Cryptography needs random numbers to generate long-term secret keys for encryption and signatures.
- Many schemes expect random (or pseudorandom) numbers, e.g.
  - ephemeral keys for DH key exchange,
  - nonces for digital signatures,
  - nonces in authenticated encryption.
- Nonce reuse can reveal long-term secret keys (e.g. PlayStation disaster)
- DSA/ECDSA are so touchy that biased nonces are enough to break them.

Random numbers are important to the NSA

- Cryptography needs random numbers to generate long-term secret keys for encryption and signatures.
- Many schemes expect random (or pseudorandom) numbers, e.g.
  - ephemeral keys for DH key exchange,
  - nonces for digital signatures,
  - nonces in authenticated encryption.
- Nonce reuse can reveal long-term secret keys (e.g. PlayStation disaster)
- DSA/ECDSA are so touchy that biased nonces are enough to break them.

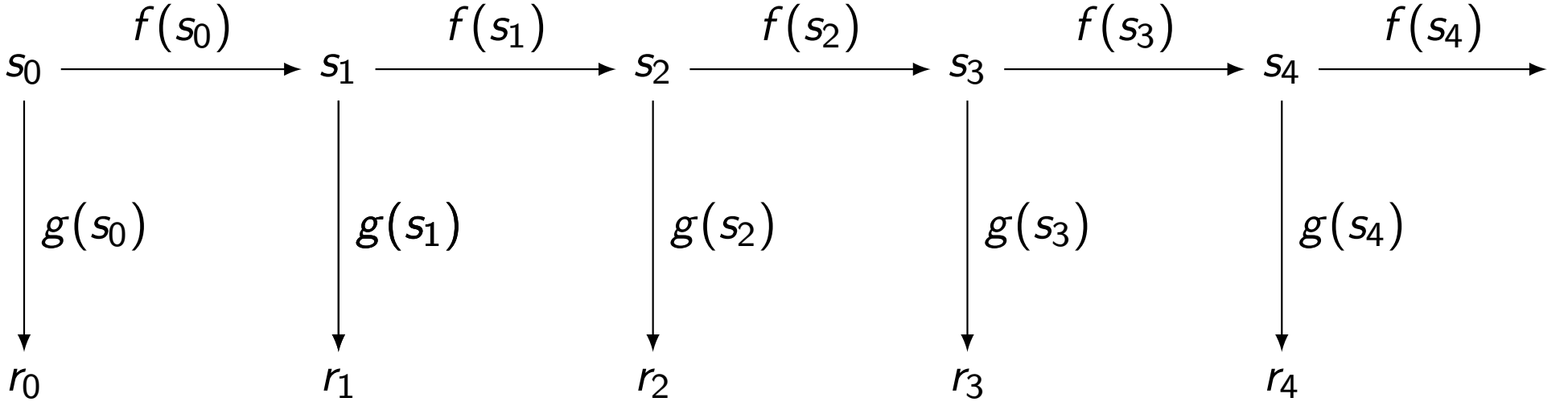
Snowden at SXSW:

> *[..] we know that these encryption algorithms we are using today work typically it is the random number generators that are attacked as opposed to the encryption algorithms themselves.*

Pseudo-random-number generators

Crypto libraries expand short seed into long stream of random bits.
Random bits are used as secret keys, DSA nonces, ...

The usual structure, starting from short seed s_1:



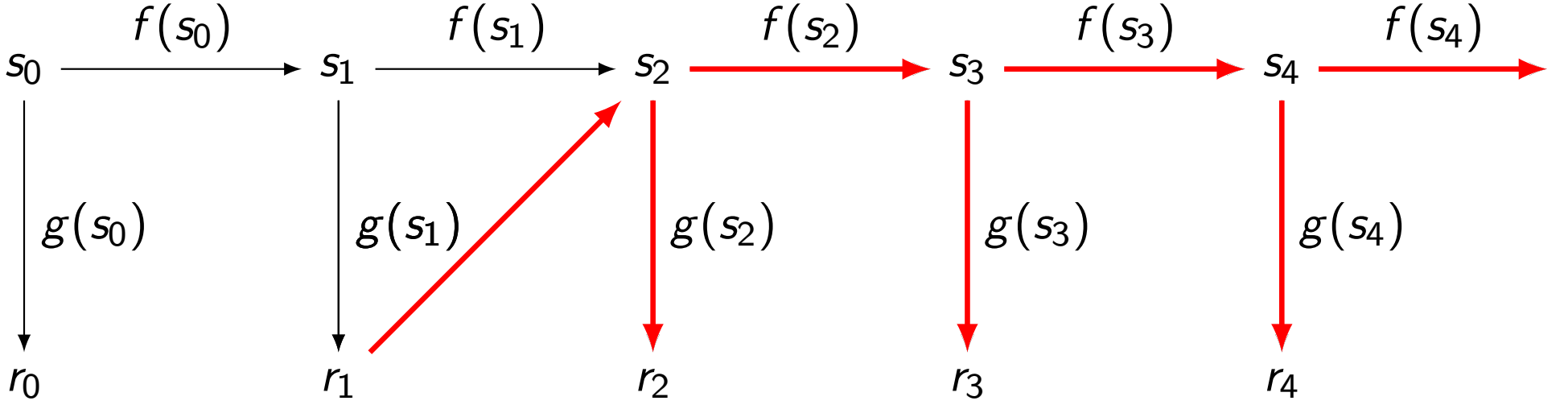
XXX's mission: Predict the "random" output bits.

1. Create protocols that directly output r_n for some reason.

Pseudo-random-number generators

Crypto libraries expand short seed into long stream of random bits.
Random bits are used as secret keys, DSA nonces, ...

The usual structure, starting from short seed s_1:



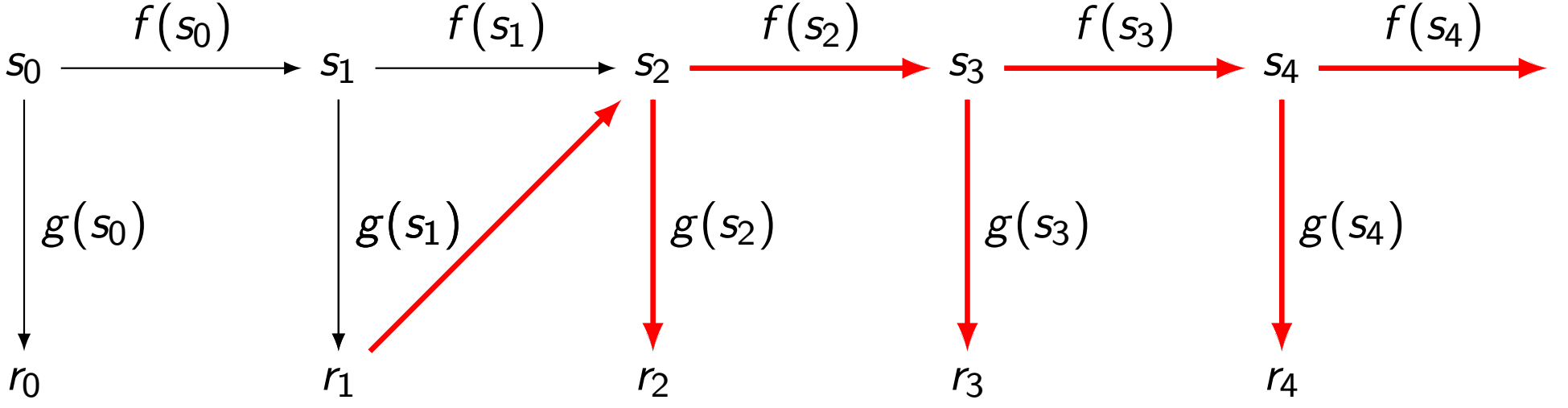
XXX's mission: Predict the "random" output bits.

1. Create protocols that directly output r_n for some reason.
2. Design f, g with back door from r_n to s_{n+1}: i.e., get $f(s)$ from $g(s)$.

Pseudo-random-number generators

Crypto libraries expand short seed into long stream of random bits.
Random bits are used as secret keys, DSA nonces, ...

The usual structure, starting from short seed s_1:



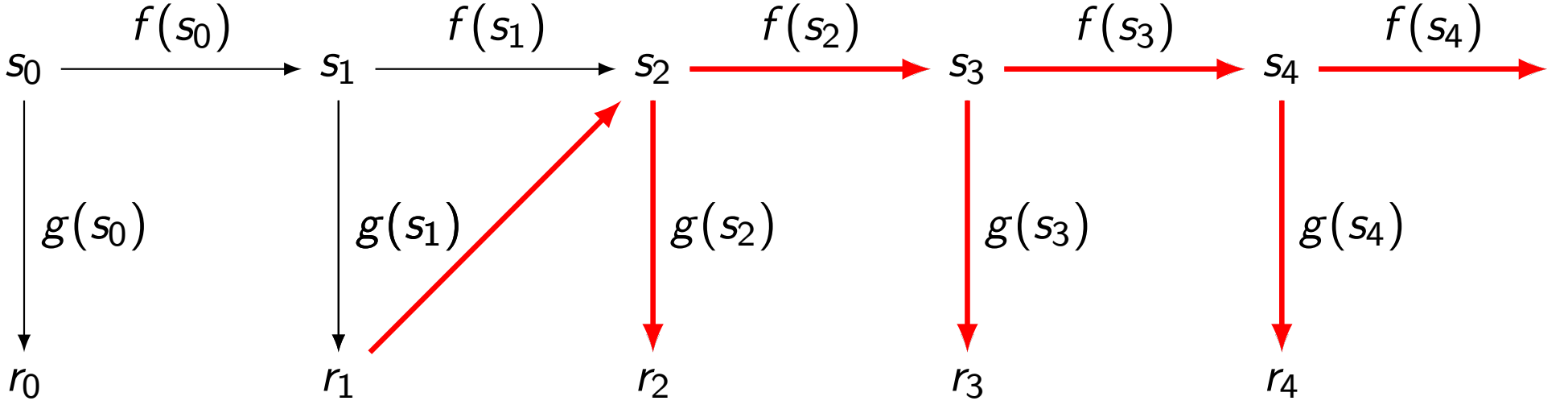
XXX's mission: Predict the "random" output bits.

1. Create protocols that directly output r_n for some reason.
2. Design f, g with back door from r_n to s_{n+1}: i.e., get $f(s)$ from $g(s)$.
3. Standardize this design of f, g.

Pseudo-random-number generators

Crypto libraries expand short seed into long stream of random bits.
Random bits are used as secret keys, DSA nonces, ...

The usual structure, starting from short seed s_1:

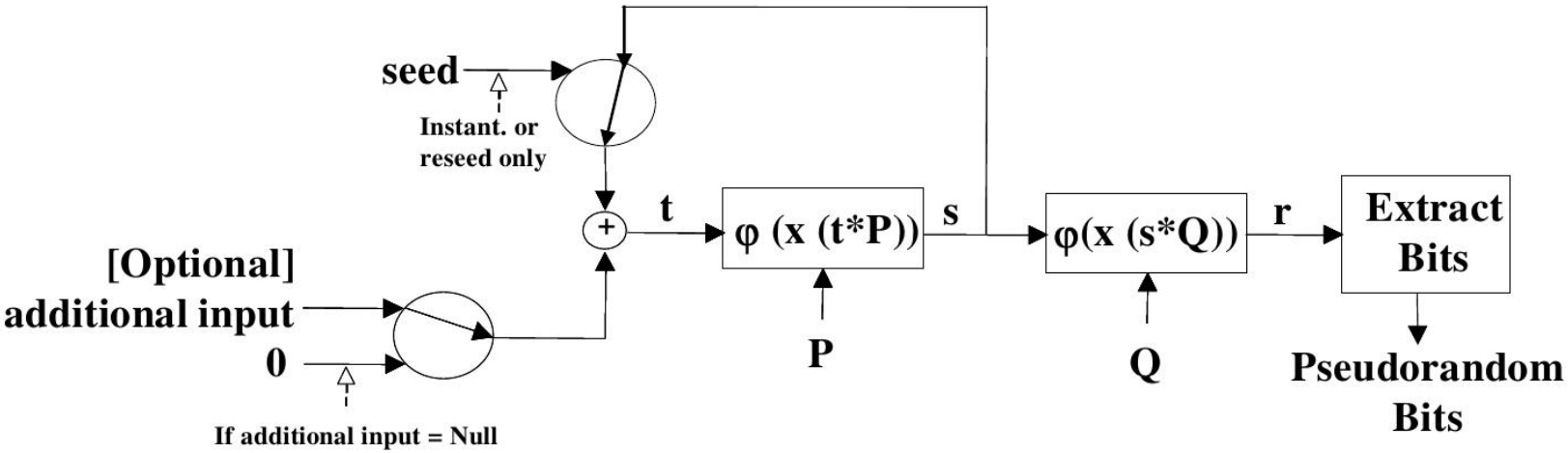


XXX's mission: Predict the "random" output bits.

1. Create protocols that directly output r_n for some reason.
2. Design f, g with back door from r_n to s_{n+1}: i.e., get $f(s)$ from $g(s)$.
3. Standardize this design of f, g.
4. Convince users to switch to this design: e.g., publish "security proof".

DUAL_EC RNG: history part I

Earliest public source (?) June 2004, draft of ANSI X9.82:



Extract gives all but the top 16 bits $\Rightarrow$ about 2^{15} points sQ match given string.

Claim:

Dual_EC_DRBG is based on the following hard problem, sometimes known as the "elliptic curve discrete logarithm problem" (ECDLP): given points P and Q on an elliptic curve of order n, find a such that $Q = aP$.

DUAL_EC RNG: common public history part II

Various public warning signals:

- Gjøsteen (March 2006): output sequence is biased.
- Brown (March 2006): security "proof"
  "This proof makes essential use of Q being random." If d with $dQ = P$ is known then $dR_i = S_{i+1}$, concludes that there might be distinguisher.
- Sidorenko & Schoenmakers (May 2006): output sequence is even more biased. Answer: Too late to change, already implemented.
- Included in standards ISO 18031 (2005), NIST SP 800-90 (2006), ANSI X9.82 (2007).
- Shumow & Ferguson (August 2007): Backdoor if d is known.
- NIST SP800-90 gets appendix about choosing points verifiably at random, but requires use of standardized P, Q for FIPS-140 validation.

September 2013: NSA Bullrun program

- (TS//SI//REL TO USA, FVEY) Influence policies, standards and specification for commercial public key technologies.

September 2013: NSA Bullrun program

- (TS//SI//REL TO USA, FVEY) Influence policies, standards and specification for commercial public key technologies.

NYT:

> *the NSA had inserted a back door into a 2006 standard adopted by NIST [..] called the Dual EC DRBG standard.*

September 2013: NSA Bullrun program

- (TS//SI//REL TO USA, FVEY) Influence policies, standards and specification for commercial public key technologies.

NYT:

> *the NSA had inserted a back door into a 2006 standard adopted by NIST [..] called the Dual EC DRBG standard.*

. . . but surely nobody uses that!?!

September 2013: NSA Bullrun program

- (TS//SI//REL TO USA, FVEY) Influence policies, standards and specification for commercial public key technologies.

NYT:

> *the NSA had inserted a back door into a 2006 standard adopted by NIST [..] called the Dual EC DRBG standard.*

. . . but surely nobody uses that!?!

NIST's DRBG Validation List: more than 70 validations of Dual_EC_DRBG;
RSA's BSAFE has Dual_EC_DRBG enabled as default,.

September 2013: NSA Bullrun program

- (TS//SI//REL TO USA, FVEY) Influence policies, standards and specification for commercial public key technologies.

NYT:

> *the NSA had inserted a back door into a 2006 standard adopted by NIST [..] called the Dual EC DRBG standard.*

. . . but surely nobody uses that!?!

NIST's DRBG Validation List: more than 70 validations of Dual_EC_DRBG;
RSA's BSAFE has Dual_EC_DRBG enabled as default,.

NIST re-opens discussions on SP800.90; recommmends against using Dual_EC.
RSA suggests changing default in BSAFE.

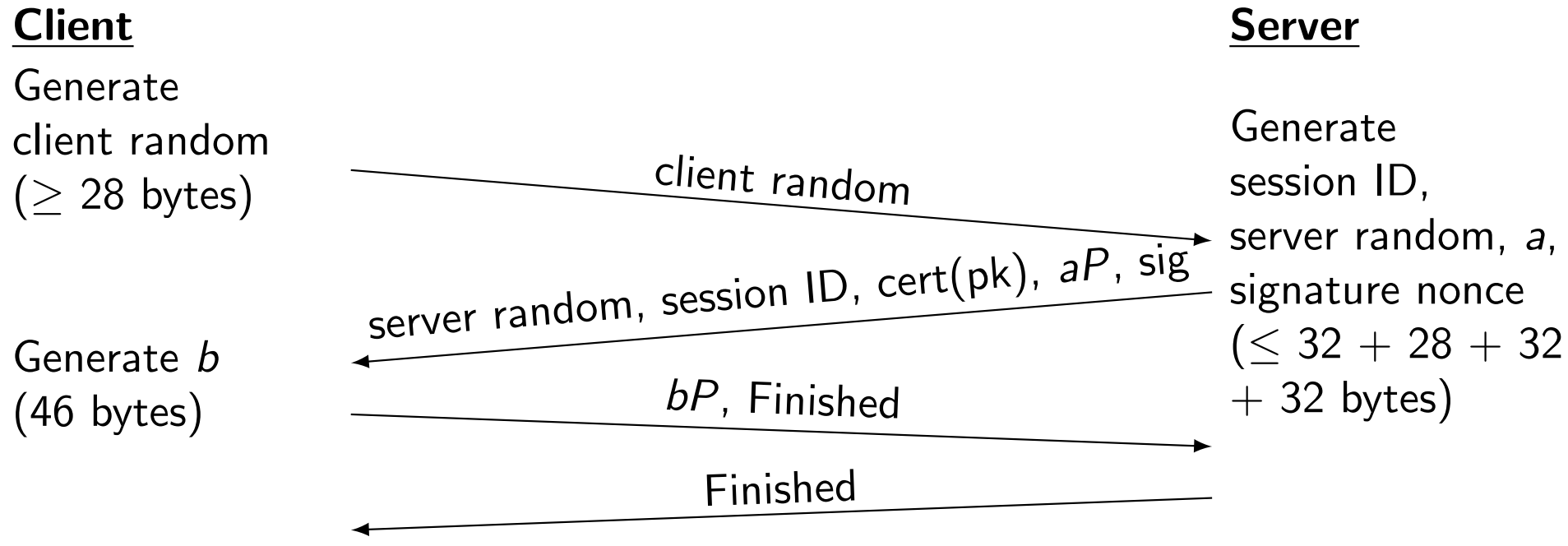
21 April 2014 NIST removes Dual EC from the standard.

SSL/TLS/HTTPS – internet security protocols

How are RNGs actually used? Do implementations actually leak enough of r_n?

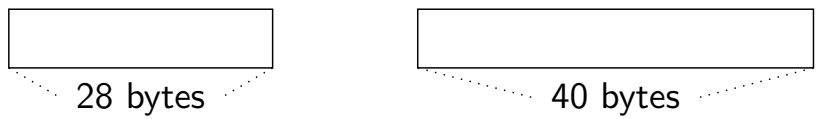
SSL/TLS/HTTPS – internet security protocols

How are RNGs actually used? Do implementations actually leak enough of r_n?



MS = PRF($x(abP)$, "master secret", client random —— server random)

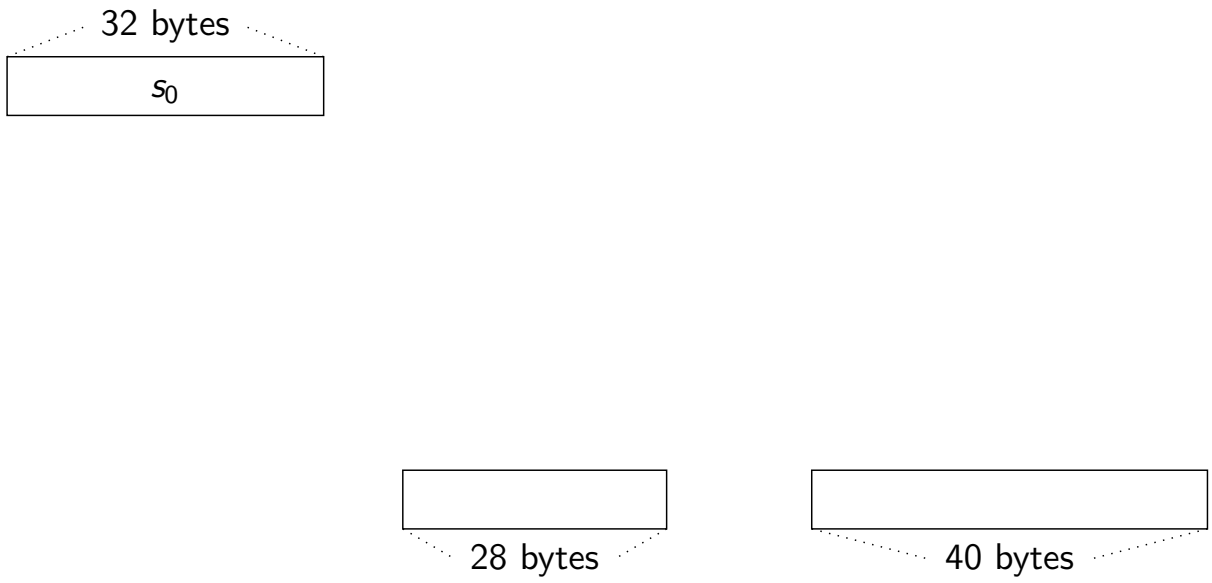
Dual EC in TLS



Graphic thanks to Ruben Niederhagen.

Dual EC in TLS

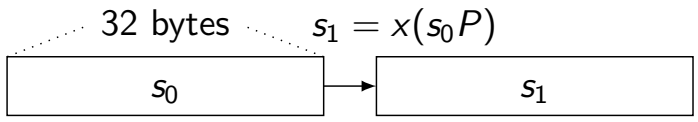
Points Q and P on an elliptic curve.

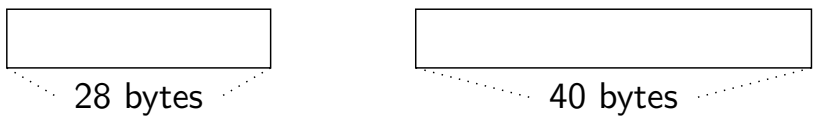


Graphic thanks to Ruben Niederhagen.

Dual EC in TLS

Points Q and P on an elliptic curve.

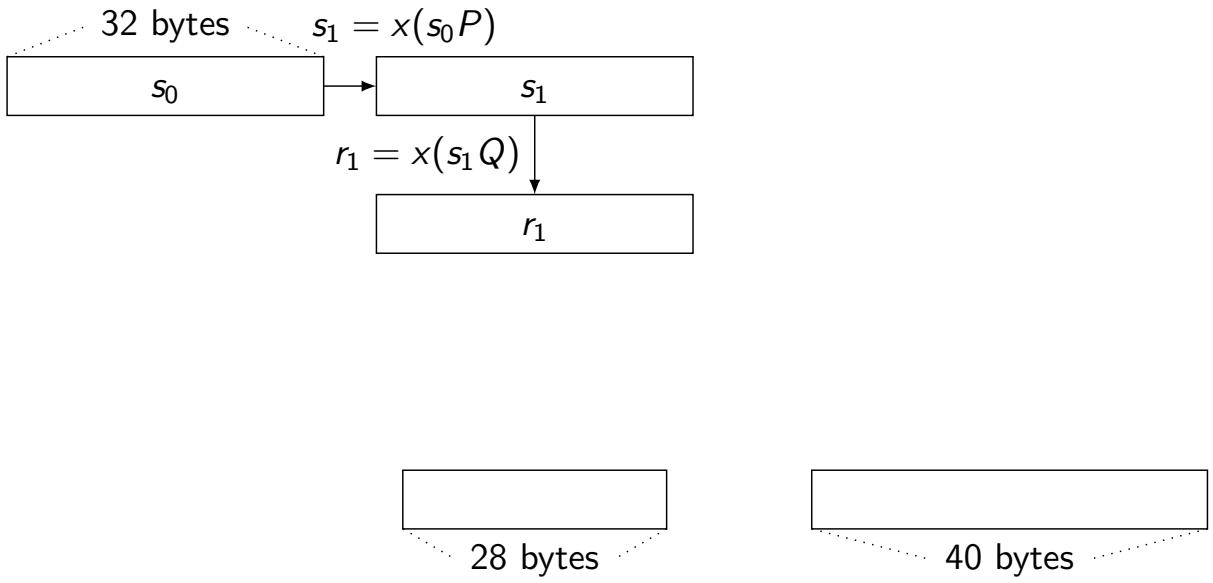




Graphic thanks to Ruben Niederhagen.

Dual EC in TLS

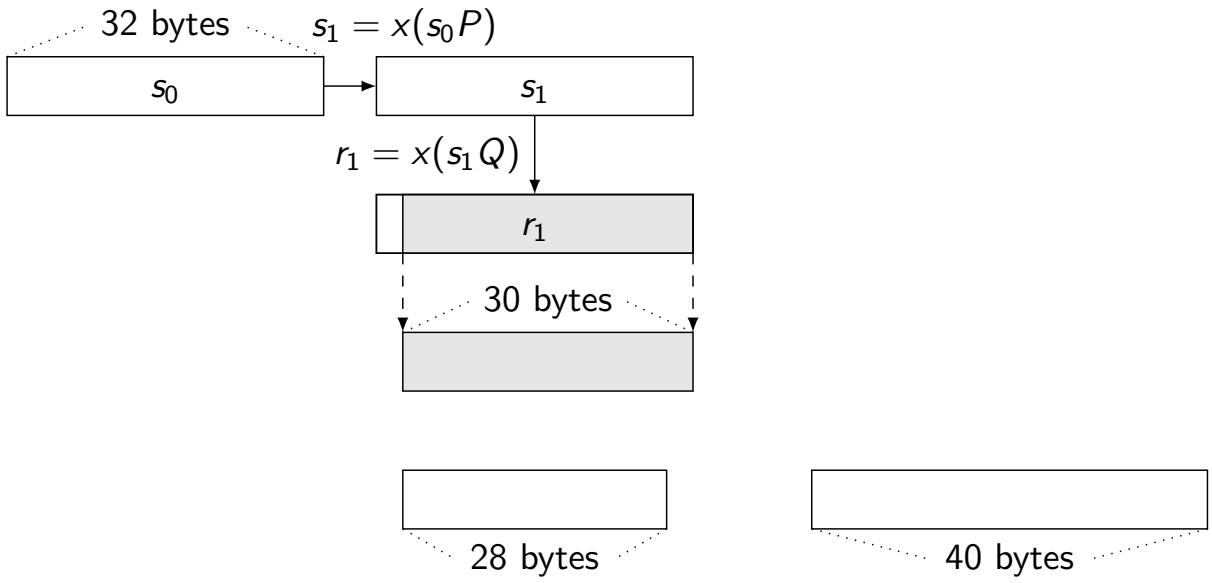
Points Q and P on an elliptic curve.



Graphic thanks to Ruben Niederhagen.

Dual EC in TLS

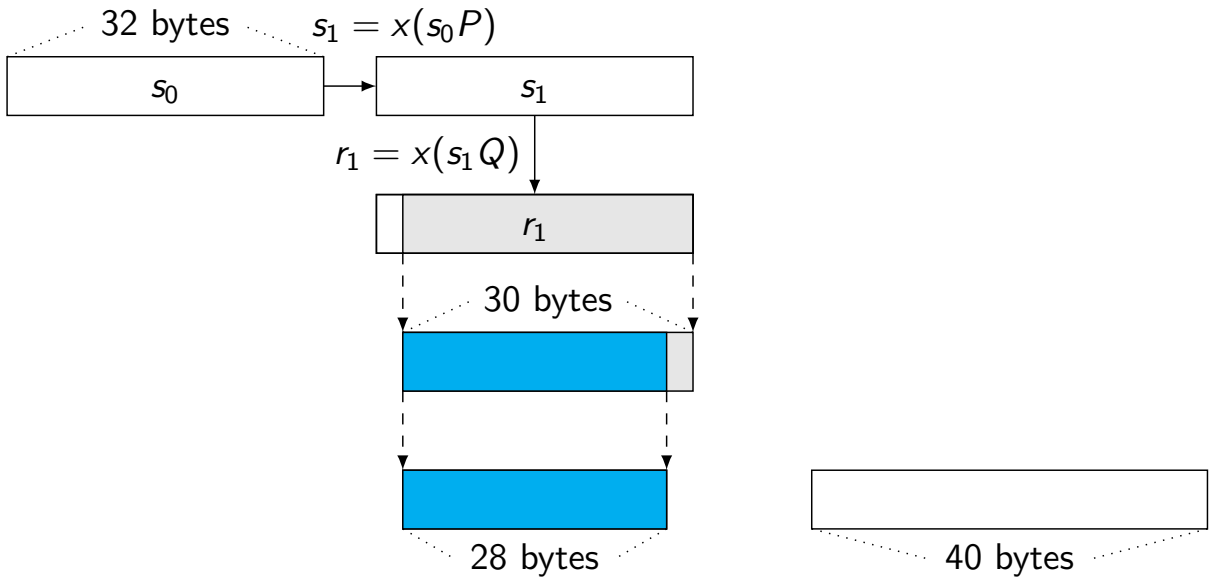
Points Q and P on an elliptic curve.



Graphic thanks to Ruben Niederhagen.

Dual EC in TLS

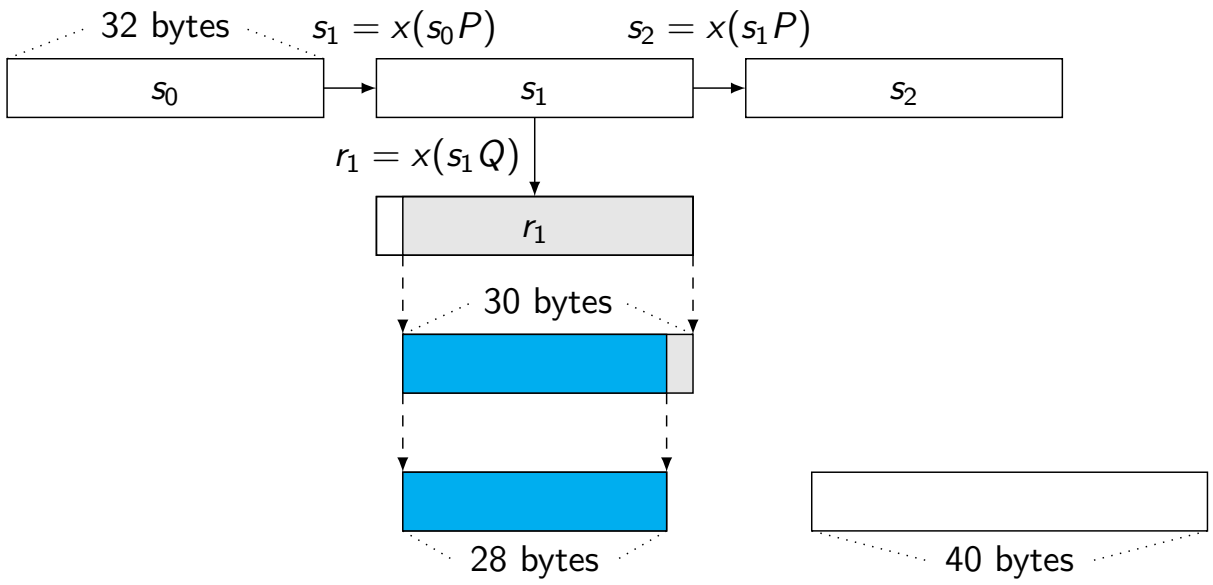
Points Q and P on an elliptic curve.



Graphic thanks to Ruben Niederhagen.

Dual EC in TLS

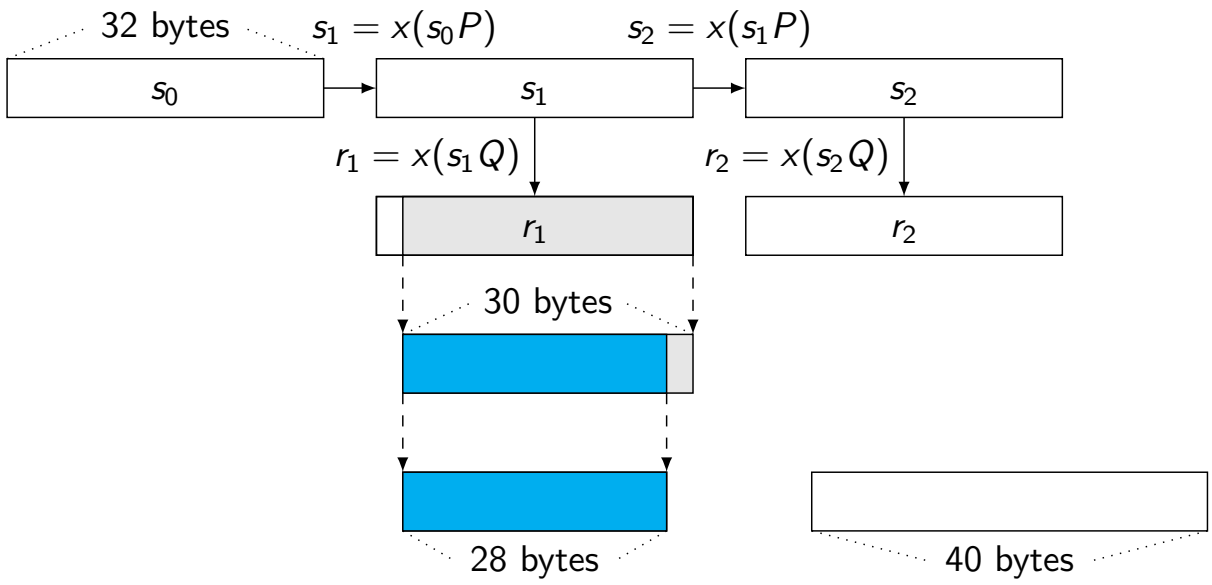
Points Q and P on an elliptic curve.



Graphic thanks to Ruben Niederhagen.

Dual EC in TLS

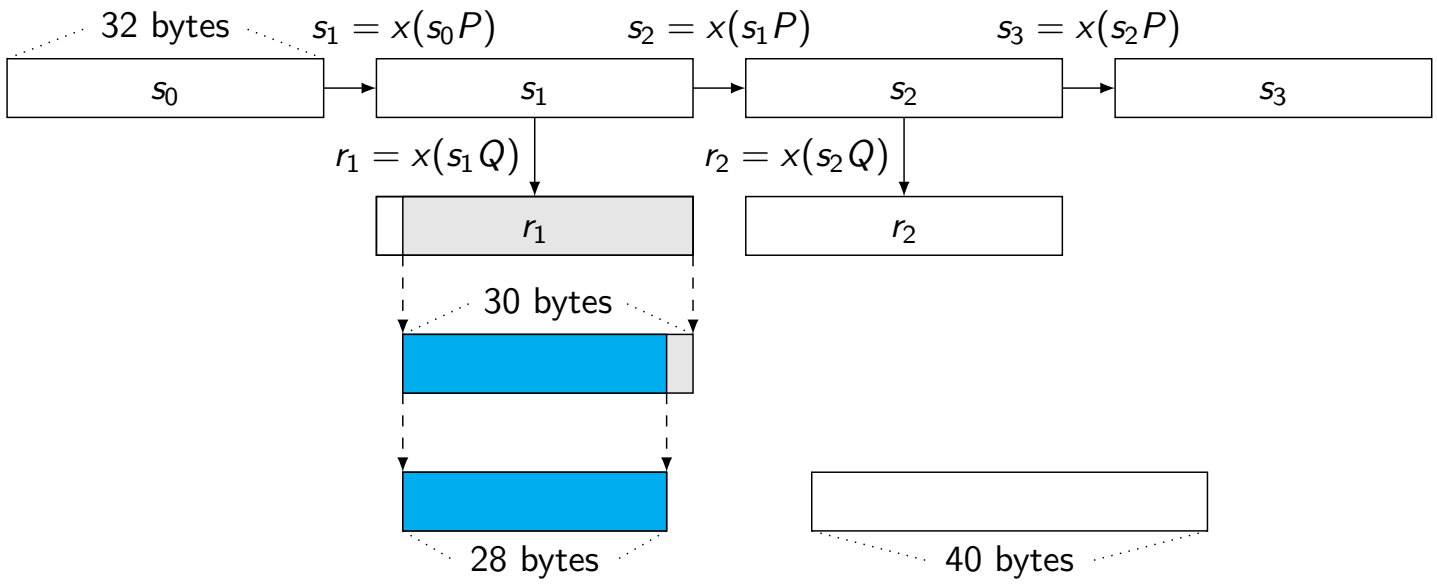
Points Q and P on an elliptic curve.



Graphic thanks to Ruben Niederhagen.

Dual EC in TLS

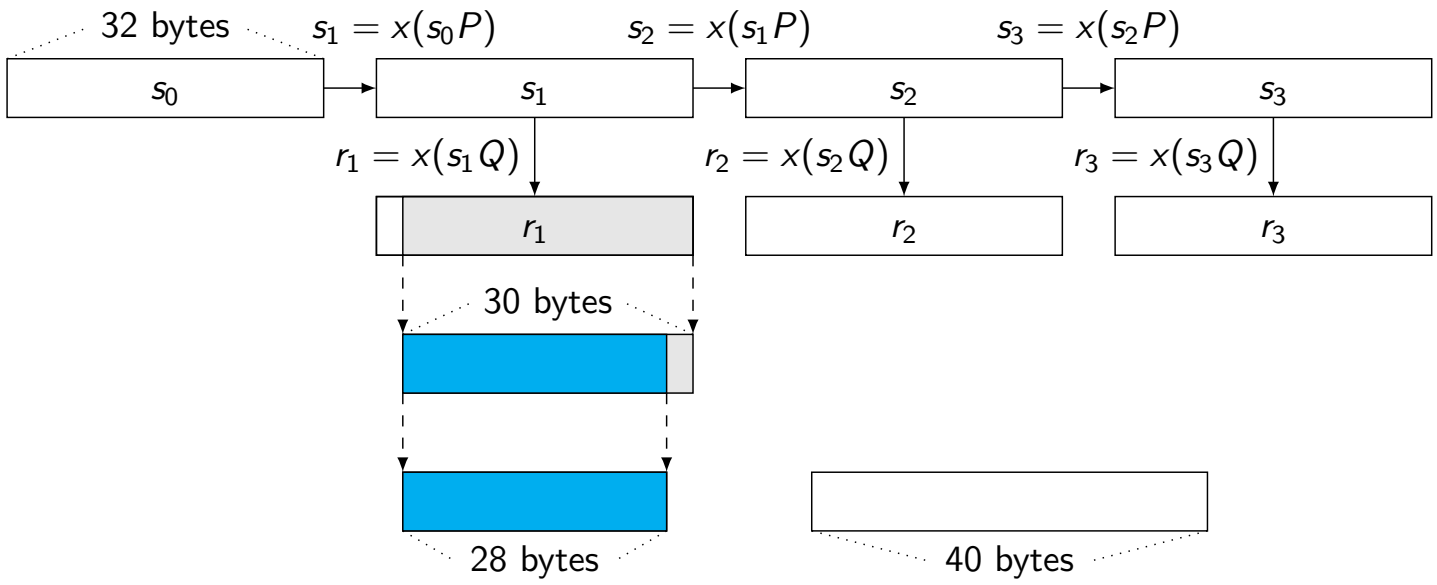
Points Q and P on an elliptic curve.



Graphic thanks to Ruben Niederhagen.

Dual EC in TLS

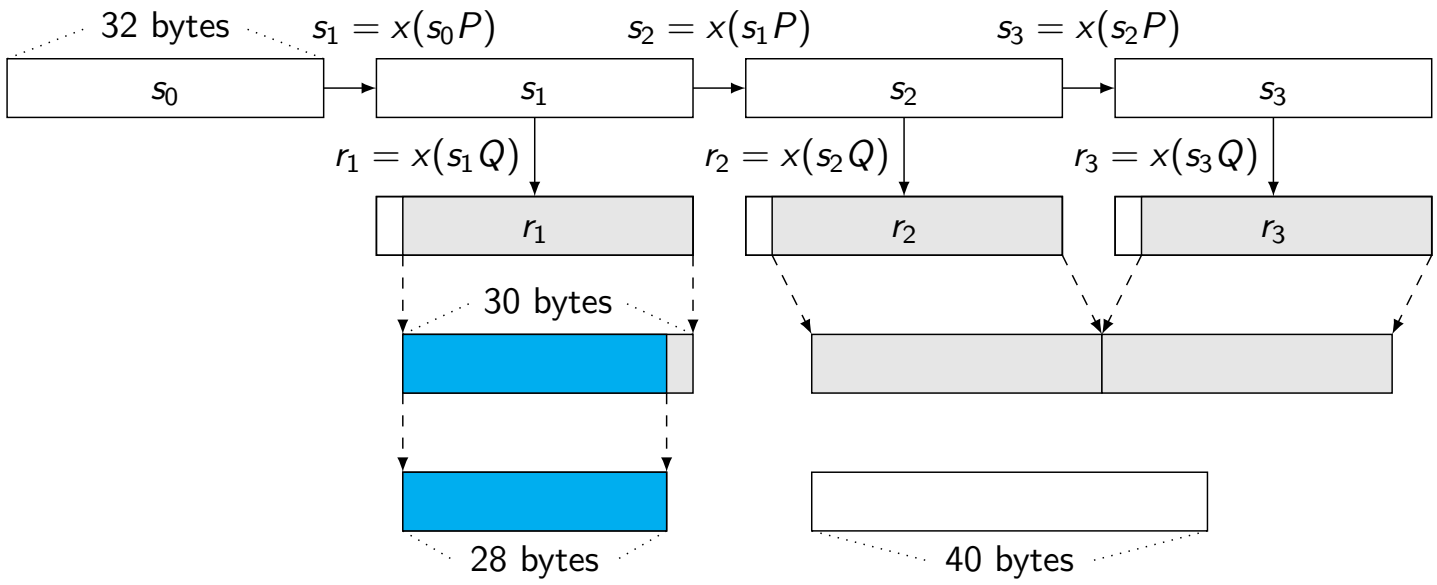
Points Q and P on an elliptic curve.



Graphic thanks to Ruben Niederhagen.

Dual EC in TLS

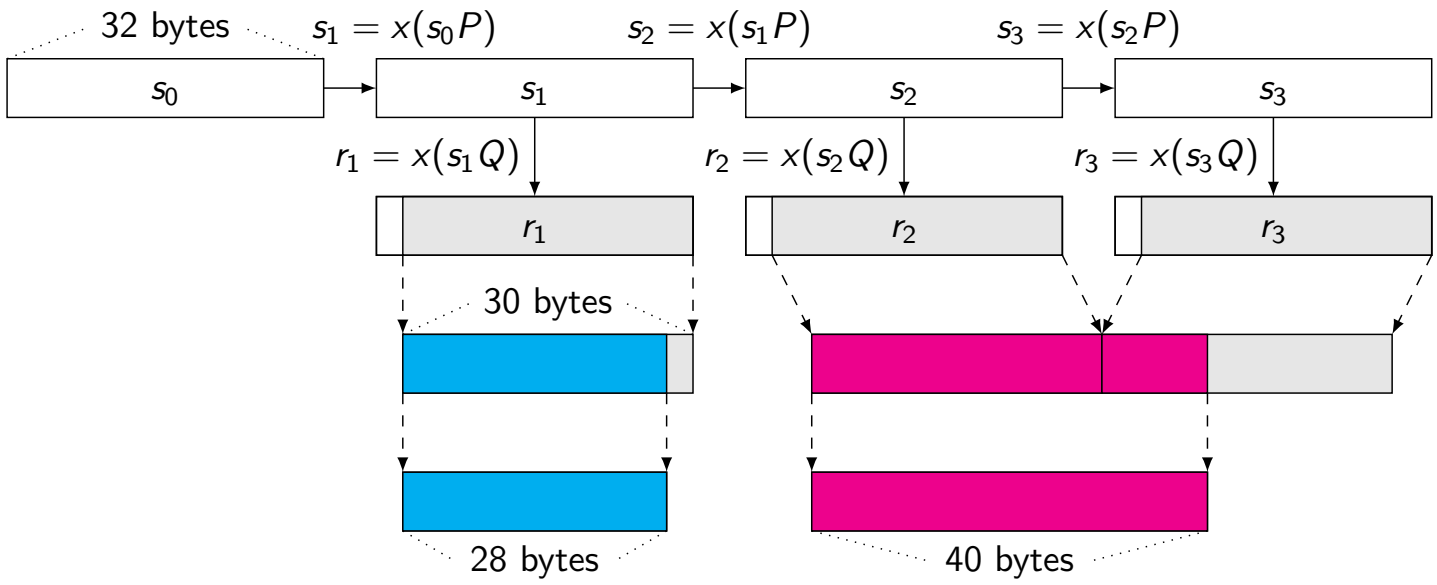
Points Q and P on an elliptic curve.



Graphic thanks to Ruben Niederhagen.

Dual EC in TLS

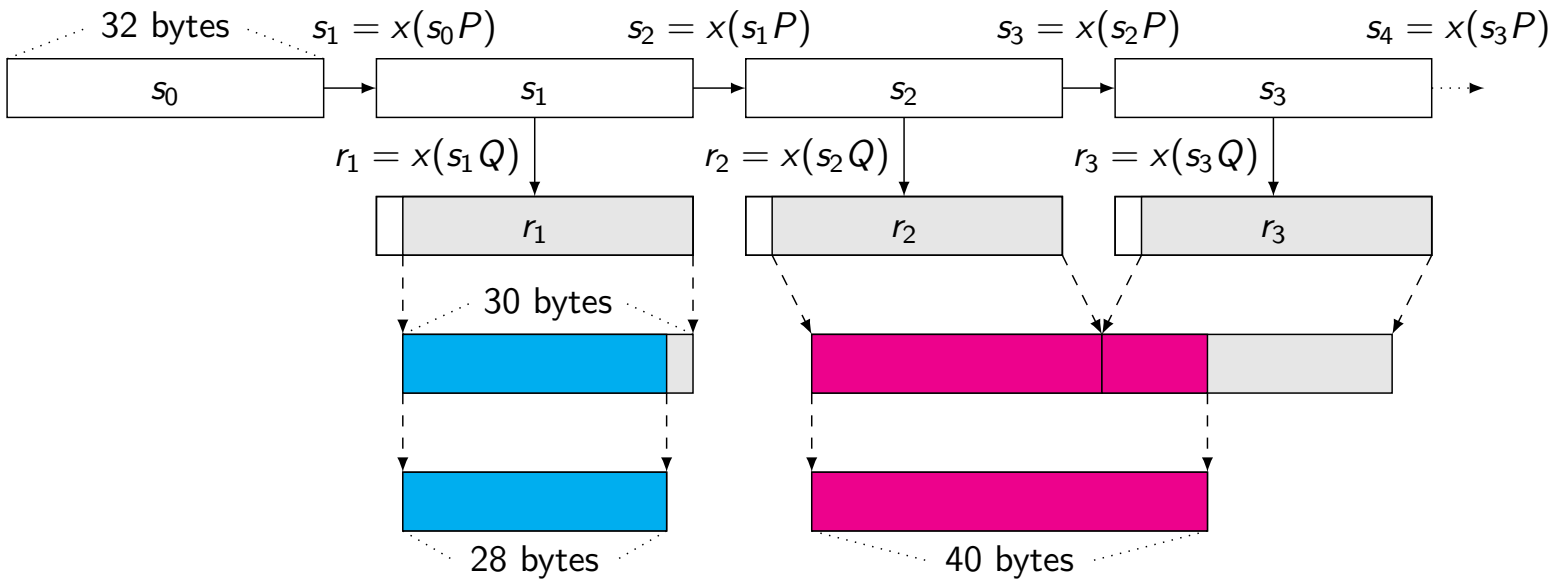
Points Q and P on an elliptic curve.



Graphic thanks to Ruben Niederhagen.

Dual EC in TLS

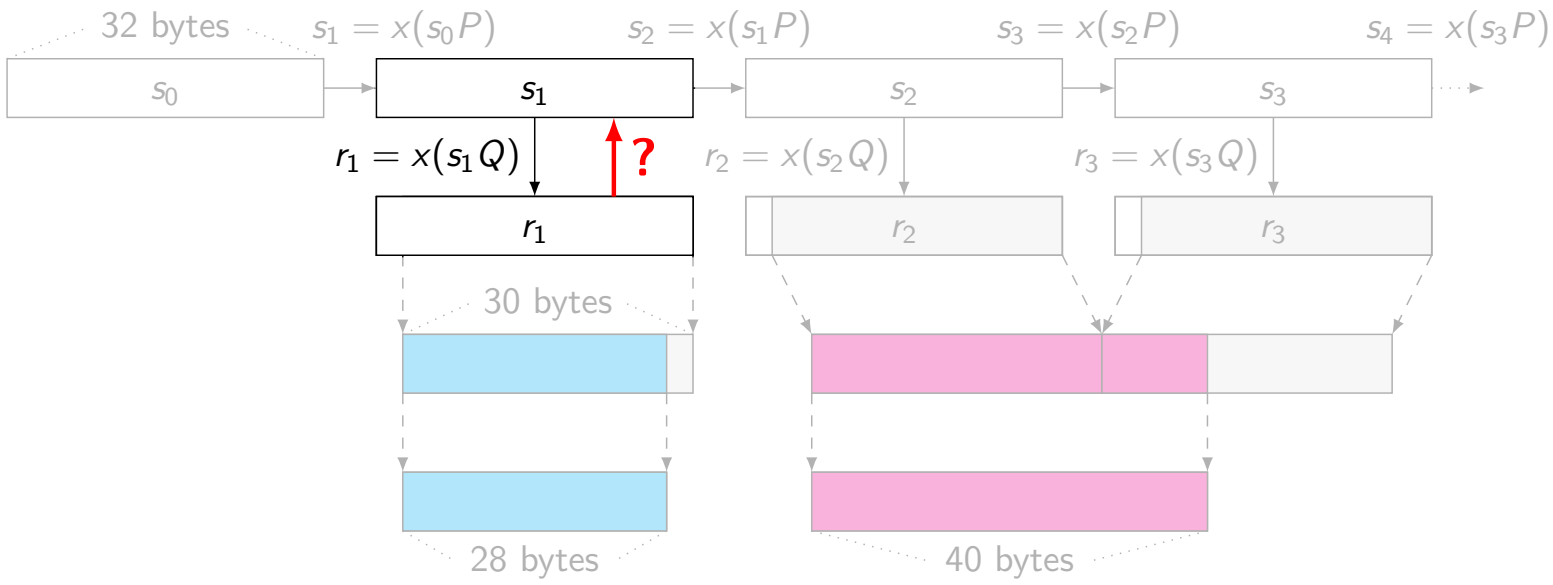
Points Q and P on an elliptic curve.



Graphic thanks to Ruben Niederhagen.

Dual EC in TLS

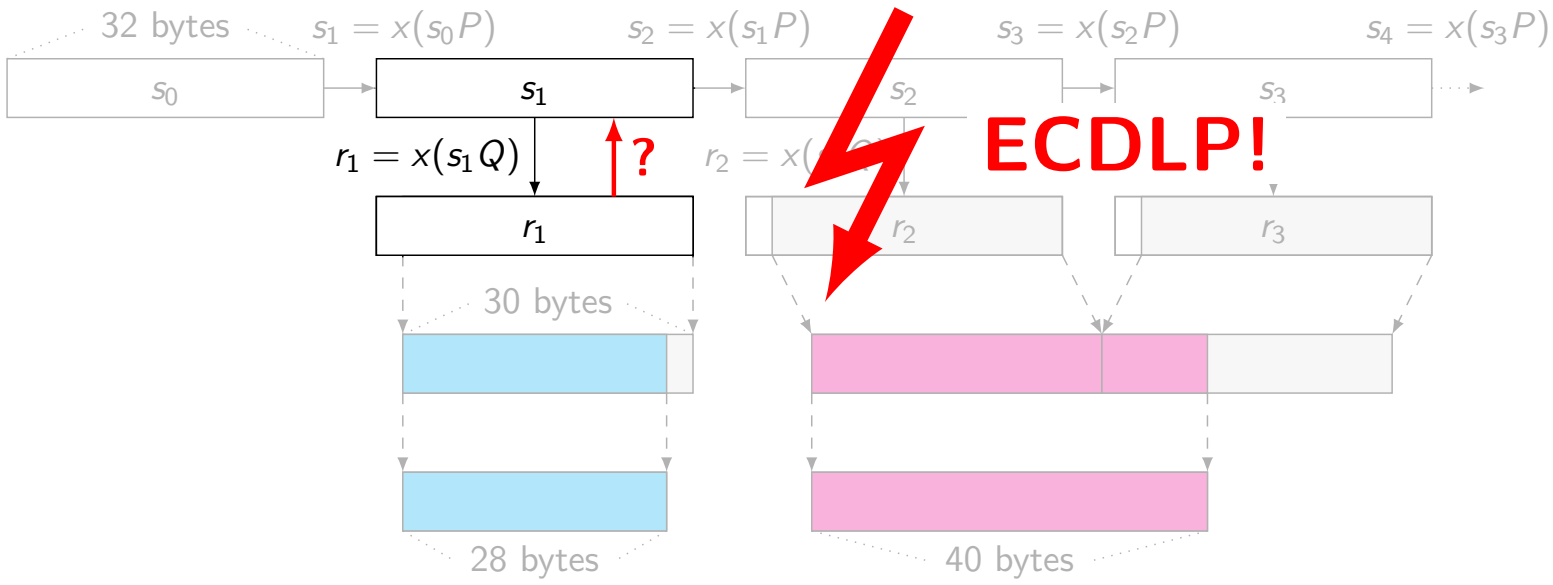
Points Q and P on an elliptic curve.



Graphic thanks to Ruben Niederhagen.

Dual EC in TLS

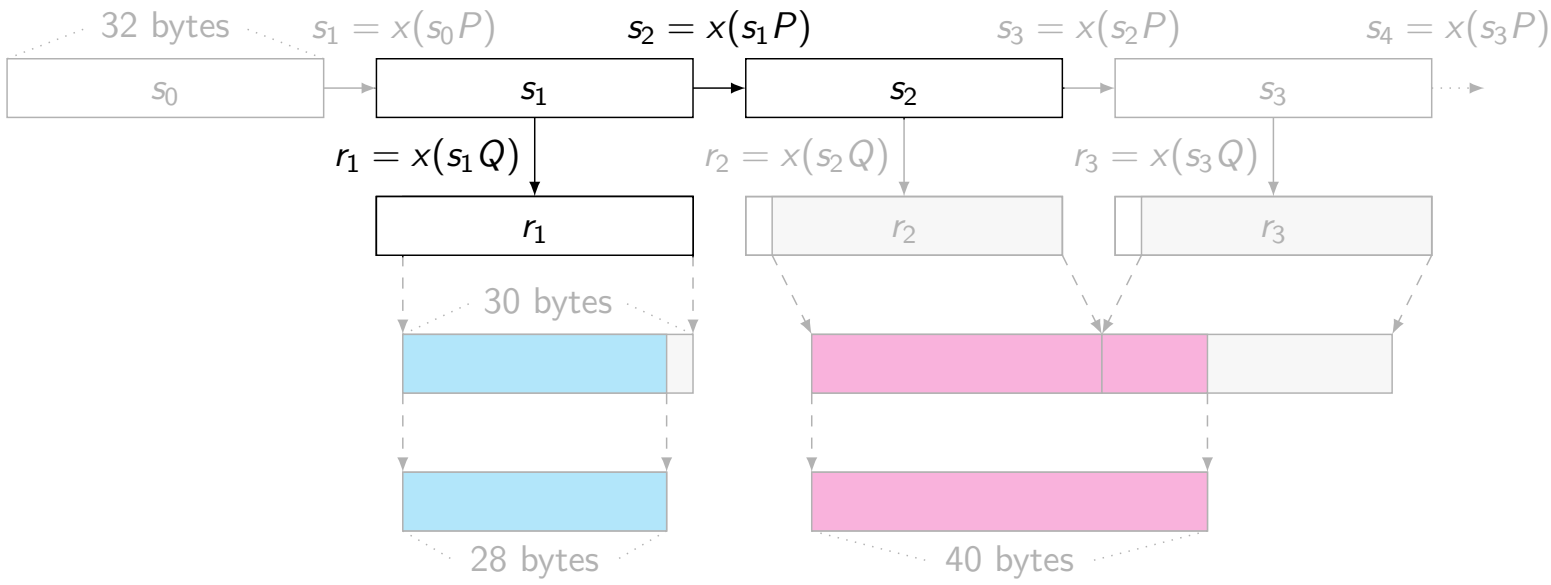
Points Q and P on an elliptic curve.



Graphic thanks to Ruben Niederhagen.

Basic attack

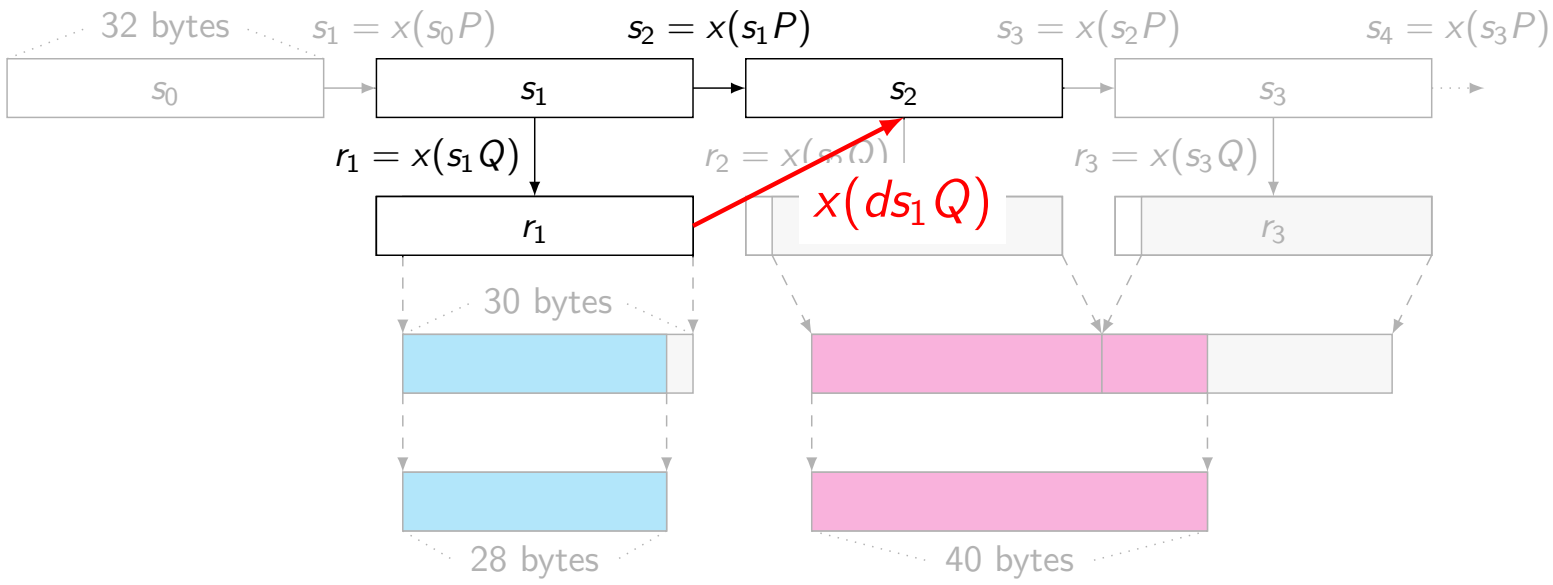
Points Q and $P = dQ$ on an elliptic curve.



Graphic thanks to Ruben Niederhagen.

Basic attack

Points Q and $P = dQ$ on an elliptic curve.

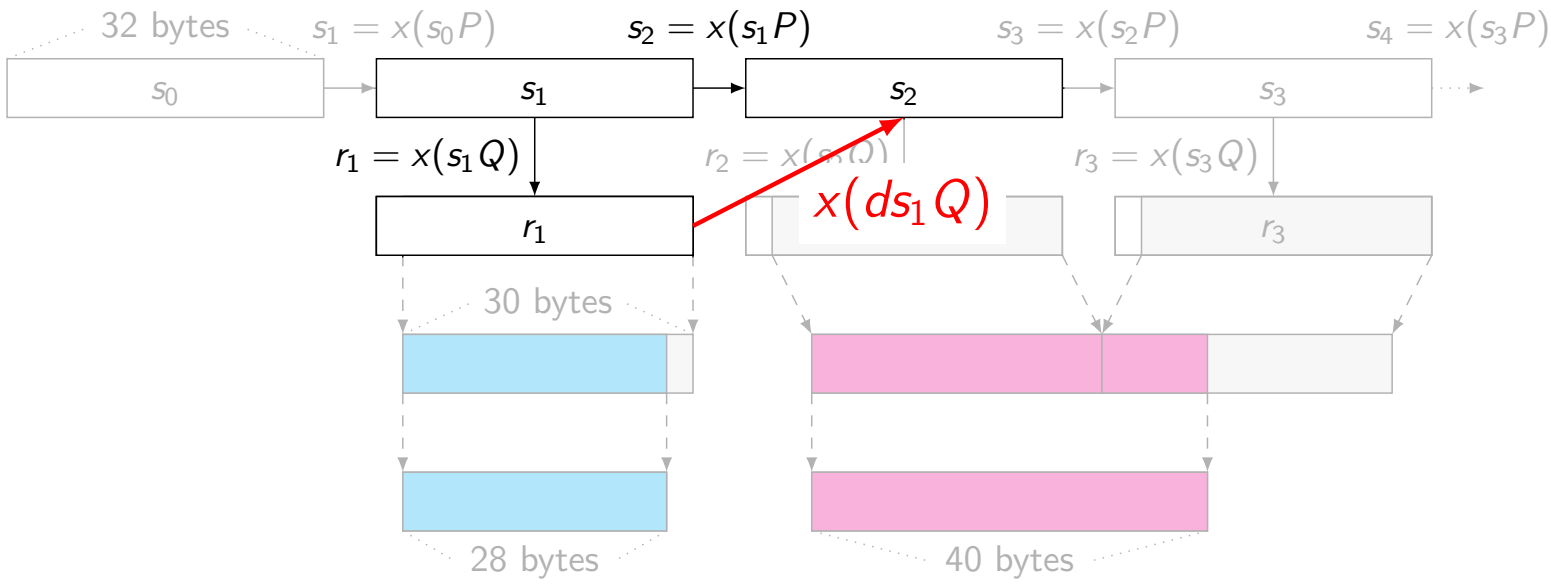


Graphic thanks to Ruben Niederhagen.

Basic attack

Points Q and $P = dQ$ on an elliptic curve.

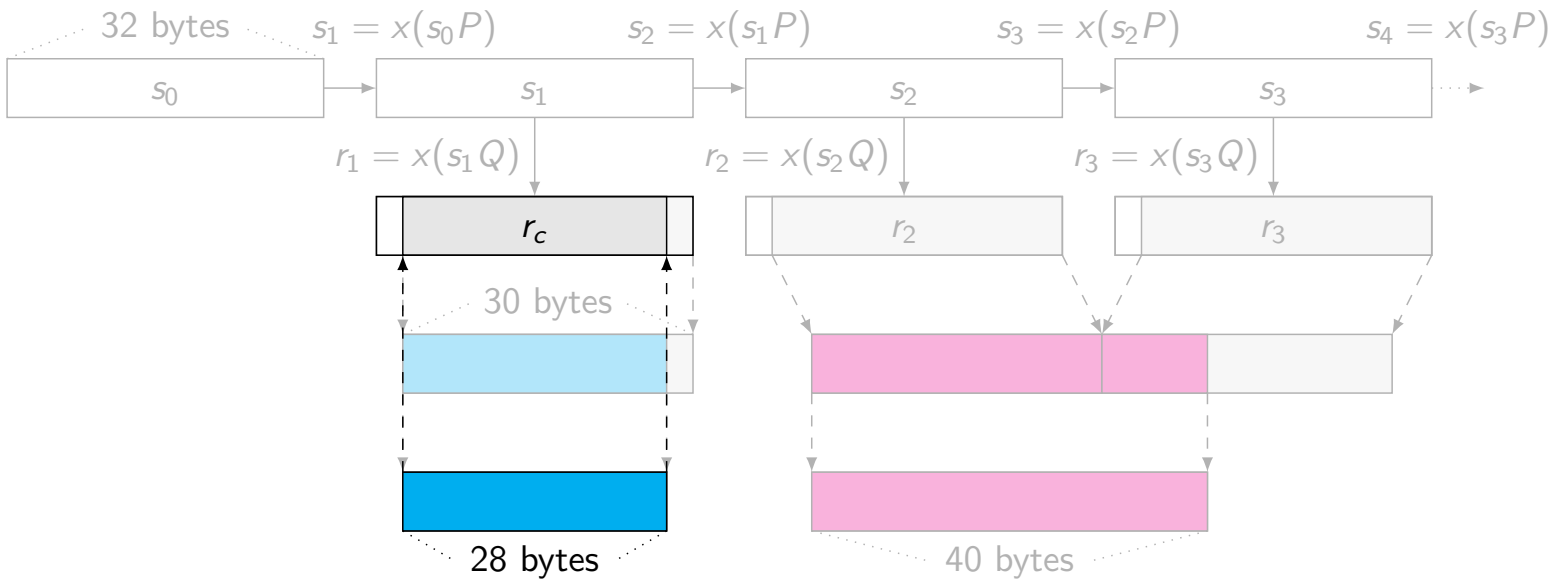
$$s_2 = x(s_1 P) = x(s_1 dQ)$$



Graphic thanks to Ruben Niederhagen.

Basic attack

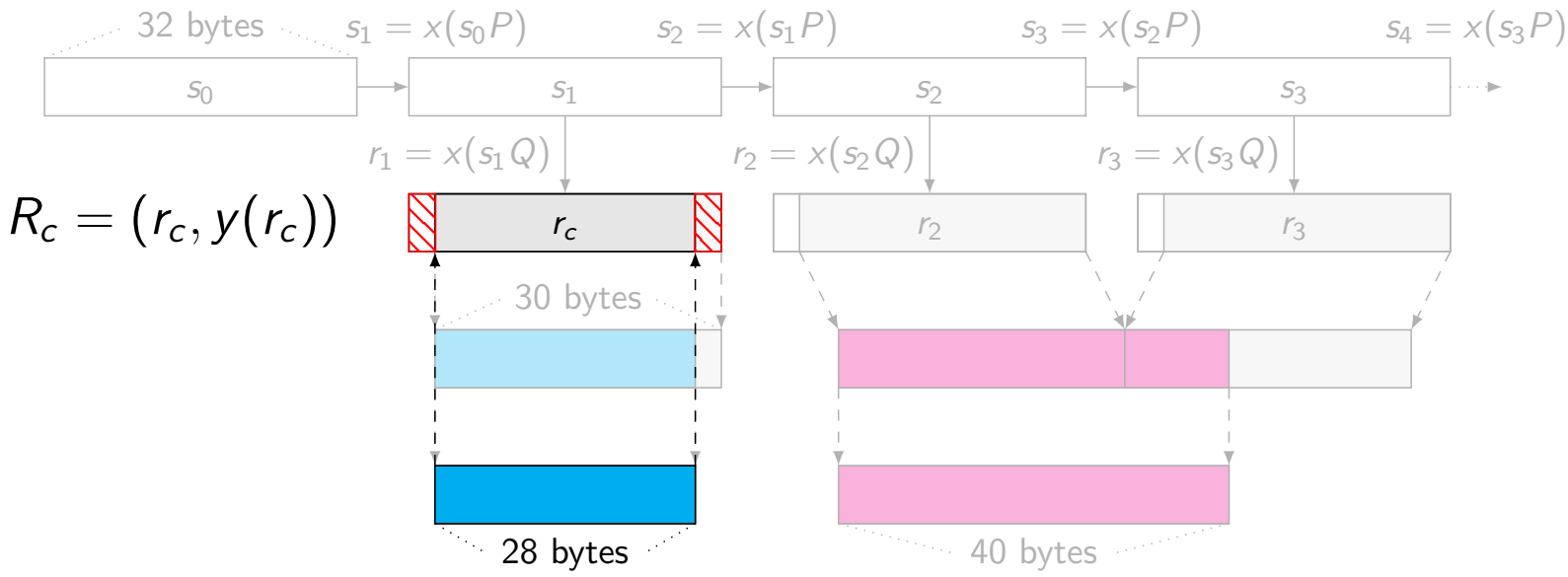
Points Q and $P = dQ$ on an elliptic curve.



Graphic thanks to Ruben Niederhagen.

Basic attack

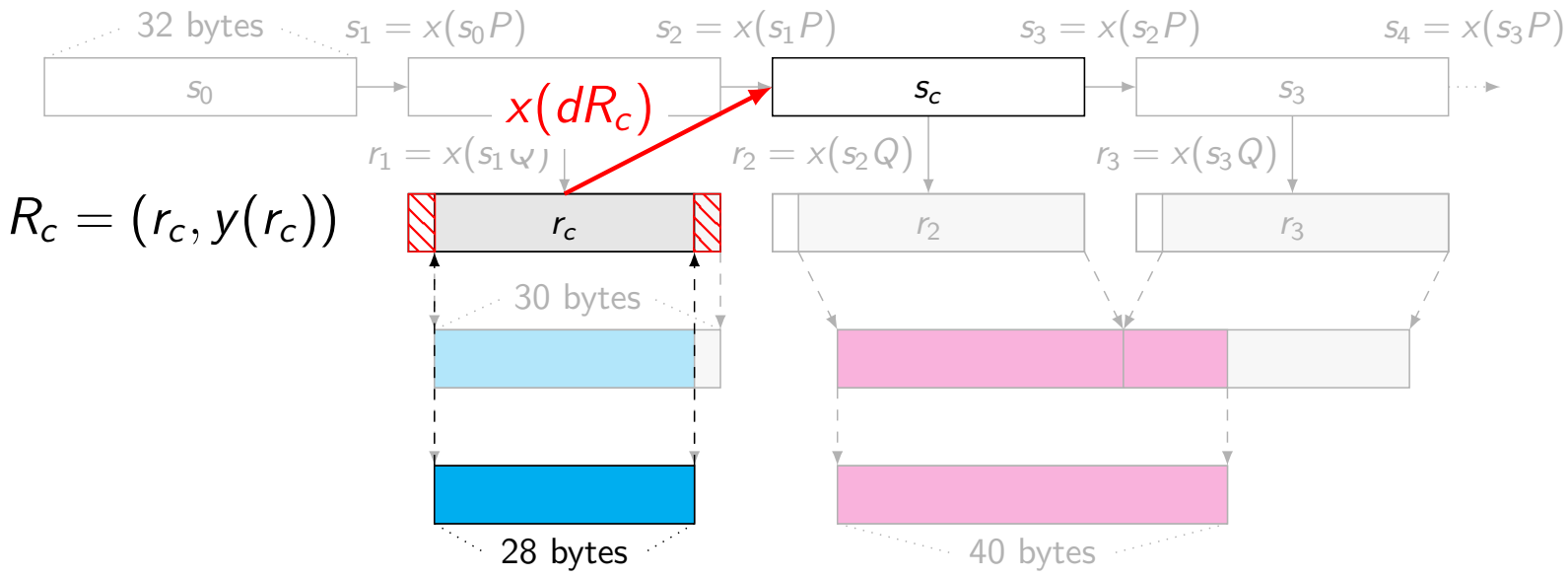
Points Q and $P = dQ$ on an elliptic curve.



Graphic thanks to Ruben Niederhagen.

Basic attack

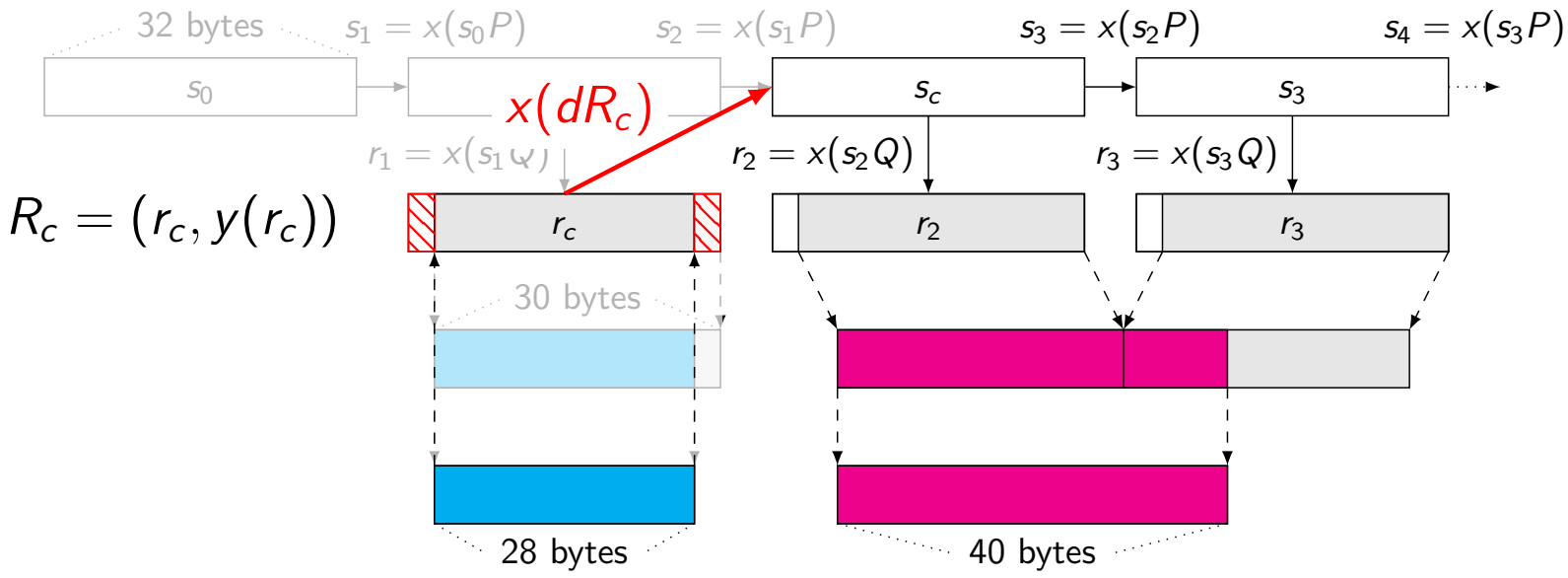
Points Q and $P = dQ$ on an elliptic curve.



Graphic thanks to Ruben Niederhagen.

Basic attack

Points Q and $P = dQ$ on an elliptic curve.



Graphic thanks to Ruben Niederhagen.

Timings

Attack	Bytes per session	Additional entropy (bits)	Time (min)
BSAFE-C v1.1	31–60		0.04*
BSAFE-Java v1.1	28		63.96*
SChannel I	28		62.97*
SChannel II	30		182.64*
OpenSSL-fixed I	32	20	0.02*
OpenSSL-fixed II	32	35	83.32*
OpenSSL-fixed III	32	$35+k$	$2^k \cdot 83.32$

*measured on 16 core cluster

How did we get here . . .

Official editors of SP800-90 are Elaine Barker and John Kelsey.

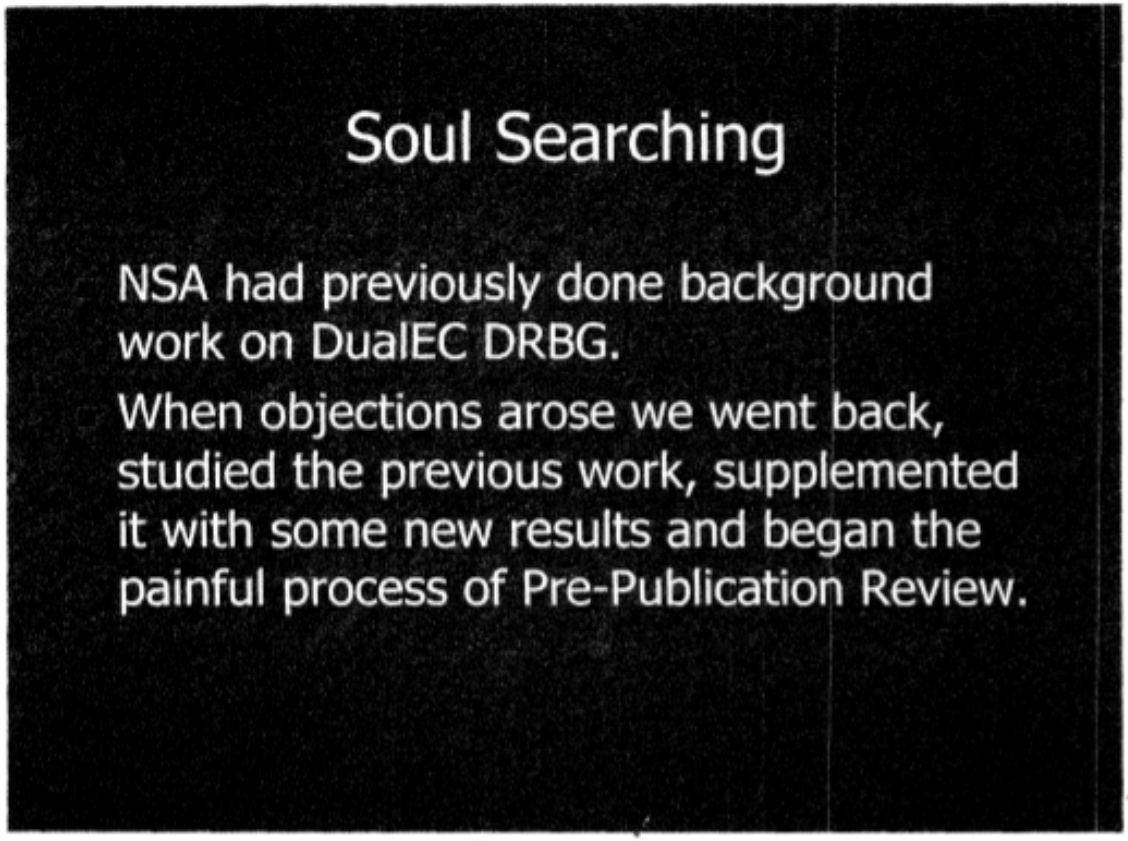
No editors stated for ANSI X9.82 nor for ISO 18031.

Interesting Dec 2013 slide deck by John Kelsey 800 – 90 and Dual EC DRBG.

- Standardization effort by NIST and NSA, with some participation from CSE.
- Most of work on standards done by US federal employees (NIST and NSA, with some help from CSE).
- The standard Dual EC parameters P and Q come ultimately from designers of Dual EC DRBG at NSA.

NIST FOIA

Two FOIA requests by Andrew Crocker and Nate Cardozo of EFF and Matthew Stoller and Rep. Alan Grayson. Files hosted by Matt Green at https://github.com/matthewdgreen/nistfoia. Interesting documents, e.g.



This is most likely a reaction to the research on biases.

From 011 – 9.12 Choosing a DRBG Algorithm.pdf

9.12 Choosing a DRBG Algorithm

Almost no system designer starts out with the idea that he's going to generate good random bits. Instead, he typically starts with some goal he wishes to accomplish, then decides on

X.2 DRBGs Based on Block Ciphers

[[This is all assuming my block cipher based schemes are acceptable to the NSA guys doing the review.--JMK]]

X.3 DRBGs Based on Hard Problems

[[Okay, so here's the limit of my competence. Can Don or Dan or one of the NSA guys with some number theory/algebraic geometry background please look this over? Thanks! --JMK]]

[[I'm really blowing smoke here. Would someone with some actual understanding of these attacks please save me from diving off a cliff right here? --JMK]]

US 20070189527A1

(19) **United States**

(12) **Patent Application Publication**

(10) **Pub. No.: US 2007/0189527 A1**

(43) **Pub. Date: Aug. 16, 2007**

Brown et al.

(54) **ELLIPTIC CURVE RANDOM NUMBER GENERATION**

(76) Inventors: **Daniel R. L. Brown**, Mississauga (CA); **Scott A. Vanstone**, Campbellville (CA)

Correspondence Address:
Blake, Cassels & Graydon LLP
Commerce Court West
P.O. Box 25
Toronto, ON M5L 1A9 (CA)

(21) Appl. No.: **11/336,814**

(22) Filed: **Jan. 23, 2006**

Related U.S. Application Data

(60) Provisional application No. 60/644,982, filed on Jan. 21, 2005.

Publication Classification

(51) **Int. Cl.**
H04L 9/00 (2006.01)

(52) **U.S. Cl.** **380/44**

(57) **ABSTRACT**

An elliptic curve random number generator avoids escrow keys by choosing a point Q on the elliptic curve as verifiably random. An arbitrary string is chosen and a hash of that string computed. The hash is then converted to a field element of the desired field, the field element regarded as the x-coordinate of a point Q on the elliptic curve and the x-coordinate is tested for validity on the desired elliptic curve. If valid, the x-coordinate is decompressed to the point Q, wherein the choice of which is the two points is also derived from the hash value. Intentional use of escrow keys can provide for back up functionality. The relationship between P and Q is used as an escrow key and stored by for a security domain. The administrator logs the output of the generator to reconstruct the random number with the escrow key.

Hat tip @nymble.

Certicom patents

The Canadian company Certicom (now part of Blackberry) has patents in multiple countries on

- Dual EC exploitation: the use of Dual EC for key escrow (i.e., for a deliberate back door)
- Dual EC escrow avoidance: modifying Dual EC to avoid key escrow.

The patent filing history also shows that

- Certicom knew the Dual EC back door by 2005;
- NSA was informed of the Dual EC back door by 2005, even if they did not know it earlier;
- the patent application, including examples of Dual EC exploitation, was publicly available in July 2006, just a month after SP800-90 was standardized.

http://projectbullrun.org/dual-ec/patent.html

References

Many more results and much more background is provided at http://projectbullrun.org/dual-ec/.

The research on breaking TLS by using the back door in Dual EC is joint work with Stephen Checkoway, Matthew Fredrikson, Ruben Niederhagen, Adam Everspaugh, Matthew Green, Tanja Lange, Thomas Ristenpart, Daniel J. Bernstein, Jake Maskiewicz, Hovav Shacham reported in "On the Practical Exploitability of Dual EC DRBG in TLS Implementations" published at USENIX Security 2014.