Dual EC

a standardized back door

Ruben Niederhagen

Joint work with Stephen Checkoway[1], Matthew Fredrikson[2], Matthew Green[1], Tanja Lange[3], Thomas Ristenpart[2], Daniel J. Bernstein[3,5], Jake Maskiewicz[4], and Hovav Shacham[4]

[1]Johns Hopkins University, [2]University of Wisconsin, [3]Technische Universiteit Eindhoven, [4]UC San Diego, [5]University of Illinois at Chicago

Technische Universiteit Eindhoven University of Technology

April 28th, 2014

Random Numbers in Cryptography

Random numbers are crucial for cryptography:

- generation of private keys for authentication
- generation of secret keys for encryption
- generation of secret nonces for digital signatures
- generation of ephemeral keys for perfect-forward secrecy
- ...

Random Numbers in Cryptography

Random numbers are crucial for cryptography:

- generation of private keys for authentication
- generation of secret keys for encryption
- generation of secret nonces for digital signatures
- generation of ephemeral keys for perfect-forward secrecy
- ...

Must be impossible for an attacker to predict!

Random Numbers in Cryptography

Challenges of random number generation:

- computers are built to be deterministic
- “real” randomness is rare

Random Numbers in Cryptography

Challenges of random number generation:

- computers are built to be deterministic
- "real" randomness is rare

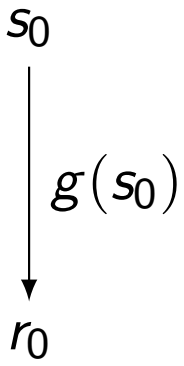
Common approach:

- use *pseudo* random numbers
- start with a random *seed*
- compute subsequent values deterministically
  $\Rightarrow$ update a secret internal state

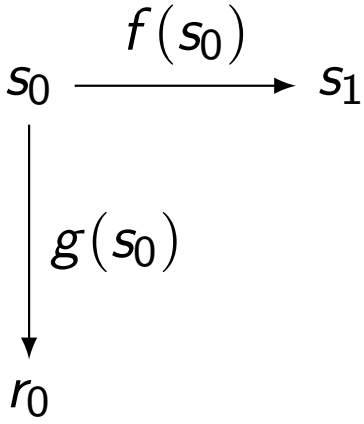
Random Numbers in Cryptography

s_0

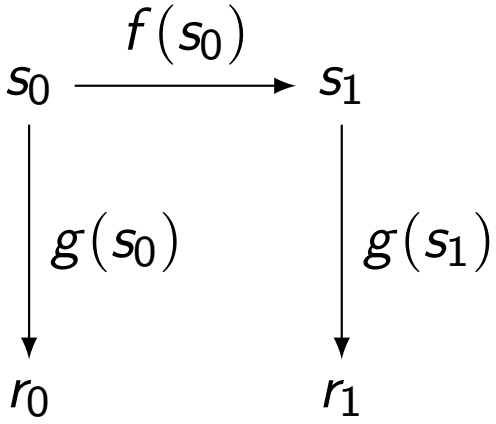
Random Numbers in Cryptography



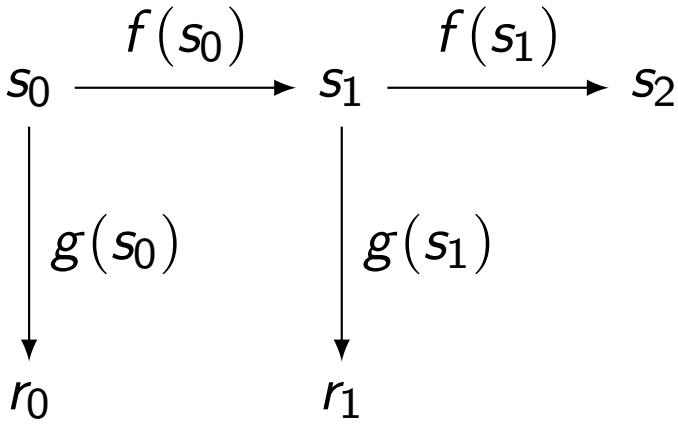
Random Numbers in Cryptography



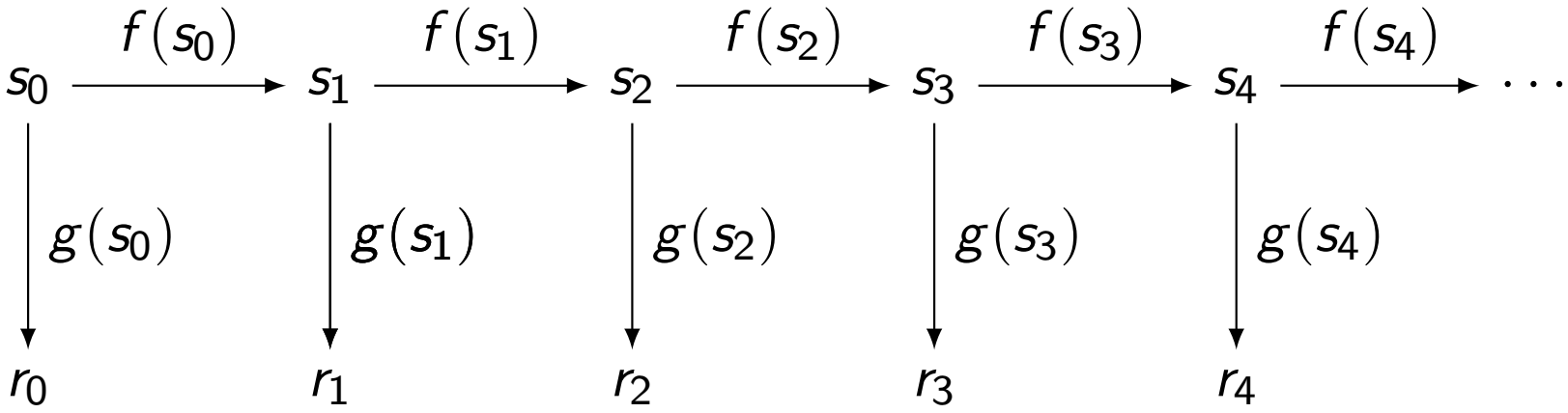
Random Numbers in Cryptography



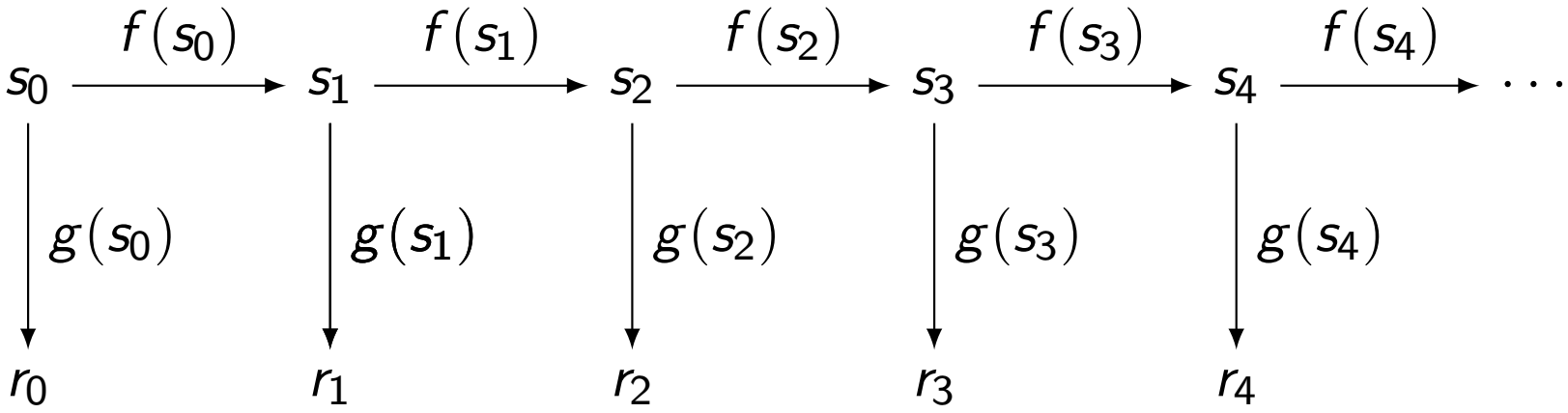
Random Numbers in Cryptography



Random Numbers in Cryptography

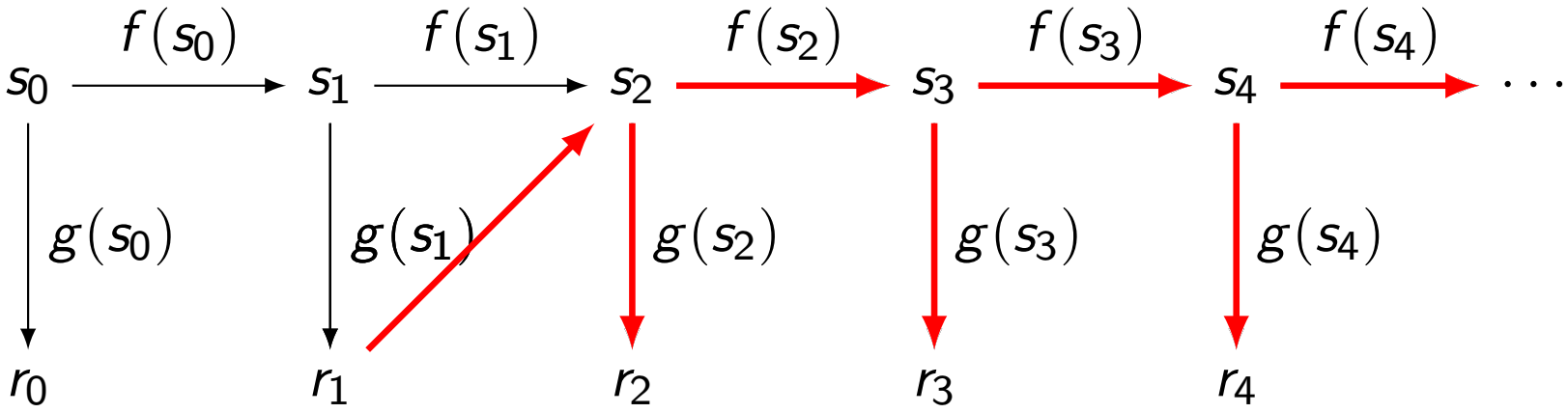


Random Numbers in Cryptography



Broken if attacker learns internal state!

Random Numbers in Cryptography



Broken if attacker learns internal state!

Dual EC – a Standardized Back Door

Topic of this talk:

The "potential" back door in the
Dual Elliptic Curve Deterministic Random Bit Generator (Dual EC)
standardized by ANSI, ISO, and NIST.

History of Dual EC

June 2004 Dual EC appears in an ANSI draft.

History of Dual EC

June 2004	Dual EC appears in an ANSI draft.
in 2004	RSA makes Dual EC the default RNG in BSAFE.

History of Dual EC

June 2004	Dual EC appears in an ANSI draft.
in 2004	RSA makes Dual EC the default RNG in BSAFE.
in 2005	An ISO standard is published including Dual EC.

History of Dual EC

June 2004	Dual EC appears in an ANSI draft.
in 2004	RSA makes Dual EC the default RNG in BSAFE.
in 2005	An ISO standard is published including Dual EC.
Dec. 2005	A draft is released by NIST including Dual EC.

History of Dual EC

June 2004	Dual EC appears in an ANSI draft.
in 2004	RSA makes Dual EC the default RNG in BSAFE.
in 2005	An ISO standard is published including Dual EC.
Dec. 2005	A draft is released by NIST including Dual EC.
early 2006	Several researchers, e.g., Schoenmakers and Sidorenko at TU/e, point out cryptographic weaknesses in Dual EC.

History of Dual EC

June 2004	Dual EC appears in an ANSI draft.
in 2004	RSA makes Dual EC the default RNG in BSAFE.
in 2005	An ISO standard is published including Dual EC.
Dec. 2005	A draft is released by NIST including Dual EC.
early 2006	Several researchers, e.g., Schoenmakers and Sidorenko at TU/e, point out cryptographic weaknesses in Dual EC.
June 2006	NIST SP 800/90A is published including Dual EC, ignoring the warnings.

History of Dual EC

June 2004	Dual EC appears in an ANSI draft.
in 2004	RSA makes Dual EC the default RNG in BSAFE.
in 2005	An ISO standard is published including Dual EC.
Dec. 2005	A draft is released by NIST including Dual EC.
early 2006	Several researchers, e.g., Schoenmakers and Sidorenko at TU/e, point out cryptographic weaknesses in Dual EC.
June 2006	NIST SP 800/90A is published including Dual EC, ignoring the warnings. This includes Dual EC in FIPS 140-2, the typical certification for RNGs.

History of Dual EC

June 2004	Dual EC appears in an ANSI draft.
in 2004	RSA makes Dual EC the default RNG in BSAFE.
in 2005	An ISO standard is published including Dual EC.
Dec. 2005	A draft is released by NIST including Dual EC.
early 2006	Several researchers, e.g., Schoenmakers and Sidorenko at TU/e, point out cryptographic weaknesses in Dual EC.
June 2006	NIST SP 800/90A is published including Dual EC, ignoring the warnings. This includes Dual EC in FIPS 140-2, the typical certification for RNGs.
Aug. 2007	Shumow and Ferguson demonstrate the basic back door.

Recent History of Dual EC

5 Sept. 2013 NSA's "Project Bullrun" is revealed by documents from Edward Snowden with the purpose

"to covertly introduce weaknesses into the encryption standards followed by hardware and software developers around the world."

Recent History of Dual EC

5 Sept. 2013 NSA's "Project Bullrun" is revealed by documents from Edward Snowden with the purpose

"to covertly introduce weaknesses into the encryption standards followed by hardware and software developers around the world."

The New York Times writes that

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

Recent History of Dual EC

5 Sept. 2013	NSA's "Project Bullrun" is revealed by documents from Edward Snowden with the purpose "to covertly introduce weaknesses into the encryption standards followed by hardware and software developers around the world." The New York Times writes that "the NSA had inserted a back door into a 2006 standard adopted by NIST [...] called the Dual EC DRBG standard."
19 Sept. 2013	RSA advises not to use Dual EC.

Recent History of Dual EC

5 Sept. 2013	NSA's "Project Bullrun" is revealed by documents from Edward Snowden with the purpose "to covertly introduce weaknesses into the encryption standards followed by hardware and software developers around the world." The New York Times writes that "the NSA had inserted a back door into a 2006 standard adopted by NIST [...] called the Dual EC DRBG standard."
19 Sept. 2013	RSA advises not to use Dual EC.
20 Dec. 2013	Reuters reports that NSA paid RSA $10 million to use Dual EC as their default RNG.

Recent History of Dual EC

5 Sept. 2013	NSA's "Project Bullrun" is revealed by documents from Edward Snowden with the purpose "to covertly introduce weaknesses into the encryption standards followed by hardware and software developers around the world." The New York Times writes that "the NSA had inserted a back door into a 2006 standard adopted by NIST [...] called the Dual EC DRBG standard."
19 Sept. 2013	RSA advises not to use Dual EC.
20 Dec. 2013	Reuters reports that NSA paid RSA $10 million to use Dual EC as their default RNG.
21 Apr. 2014	NIST removes Dual EC from the standard.

Authors of Dual EC

Kelsey, in December 2013 slides:

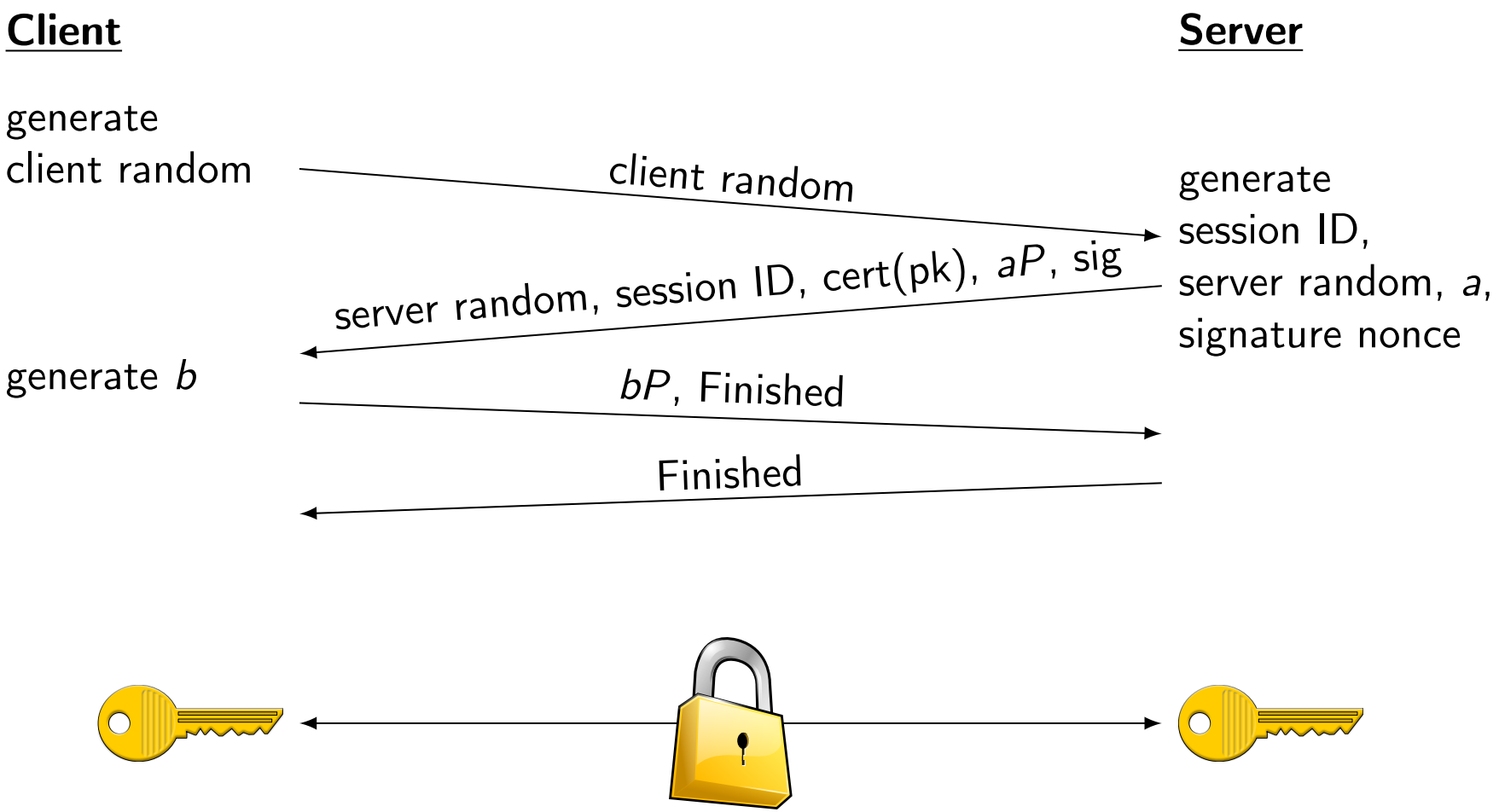
- Standardization effort by "NIST and NSA, with some participation from CSE".
- "Most of work on standards done by US federal employees (NIST and NSA, with some help from CSE)"
- The standard Dual EC parameters P and Q come "ultimately from designers of Dual EC DRBG at NSA".

Attack Target — TLS

Transport Layer Security (TLS)

- Used in the Internet for encryption of communication.
  Examples:
  - eMail transport
  - online banking
  - online shopping
  - ...
- Standard covers a fast amount of protocols and optional features.
- Client and server agree on what parameters to use.
- Client and server agree on a random secret key.

TLS Handshake



Attack Target — TLS

Common TLS implementations:

- RSA's BSAFE
  - RSA BSAFE Share for Java (BSAFE Java)
  - RSA BSAFE Share for C and C++ (BSAFE C)
- Microsoft's SChannel
- OpenSSL

All of these offer Dual EC.

Attack Target — TLS

Common TLS implementations:

- RSA's BSAFE
  - RSA BSAFE Share for Java (BSAFE Java)
  - RSA BSAFE Share for C and C++ (BSAFE C)
- Microsoft's SChannel
- OpenSSL

Remember: NSA paid RSA Security $10 million to use Dual EC as the default RNG!

All of these offer Dual EC.

Elliptic Curve Discrete Logarithm Problem

Arithmetic on Elliptic Curves

Operate on points $P = (x_P, y_P)$ on an elliptic curve.

- addition: $A + B = C$
- scalar mul.: $4 \cdot A = A + A + A + A$

Elliptic Curve Discrete Logarithm Problem

Arithmetic on Elliptic Curves

Operate on points $P = (x_P, y_P)$ on an elliptic curve.

- addition: $A + B = C$
- scalar mul.: $4 \cdot A = A + A + A + A$

Useful in Cryptography:

It is *easy* to compute $k \cdot A$, e.g.:

$$B = 243 \cdot A = A + 2A + 16A + 32A + 64A + 128A$$

Cost: 5 additions and 7 doublings

Elliptic Curve Discrete Logarithm Problem

Arithmetic on Elliptic Curves

Operate on points $P = (x_P, y_P)$ on an elliptic curve.

- addition: $A + B = C$
- scalar mul.: $4 \cdot A = A + A + A + A$

Useful in Cryptography:

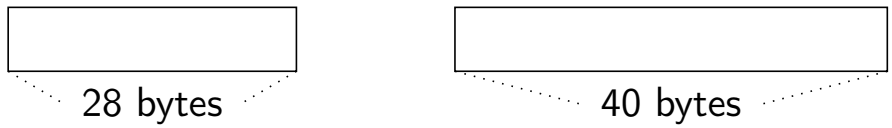
It is *easy* to compute $k \cdot A$, e.g.:

$$B = 243 \cdot A = A + 2A + 16A + 32A + 64A + 128A$$

Cost: 5 additions and 7 doublings

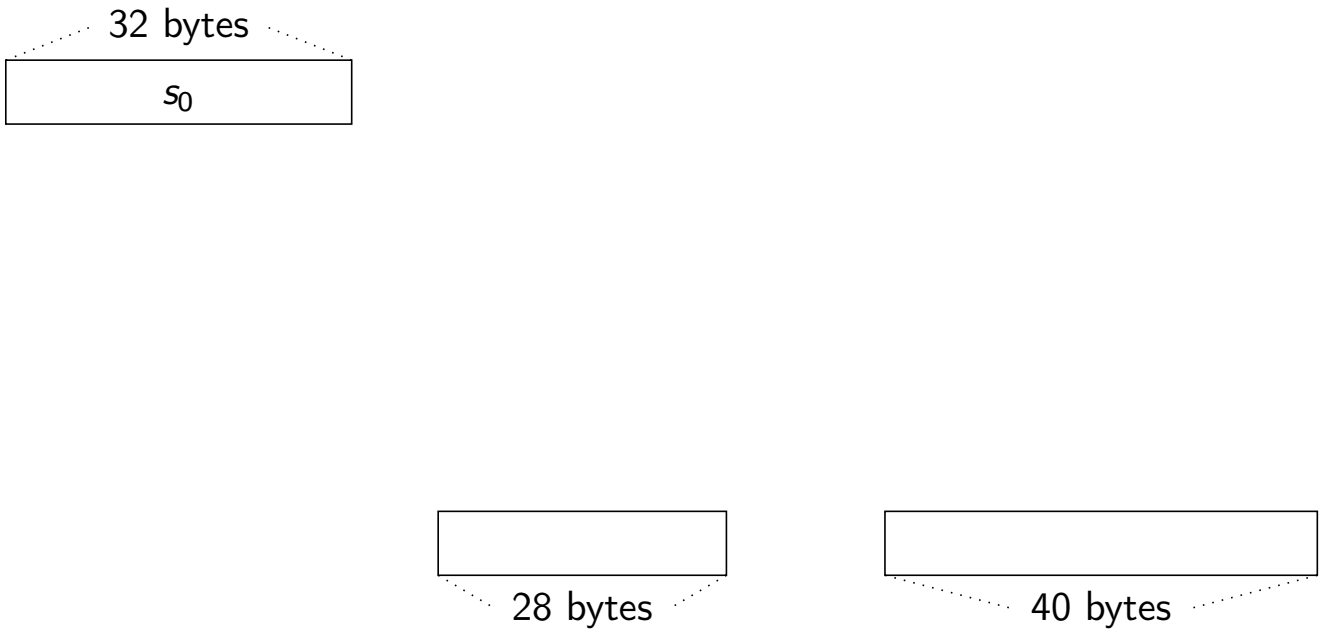
It is *hard* to find k such that $B = k \cdot A$!

Dual EC — Basic Procedure



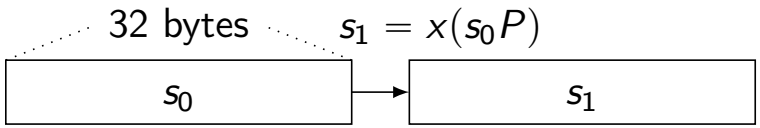
Dual EC — Basic Procedure

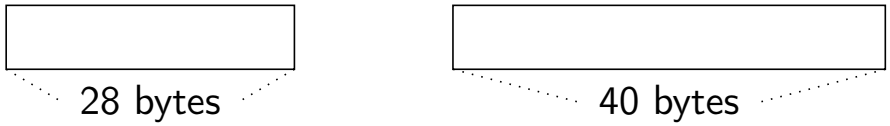
Points Q and P on an elliptic curve.



Dual EC — Basic Procedure

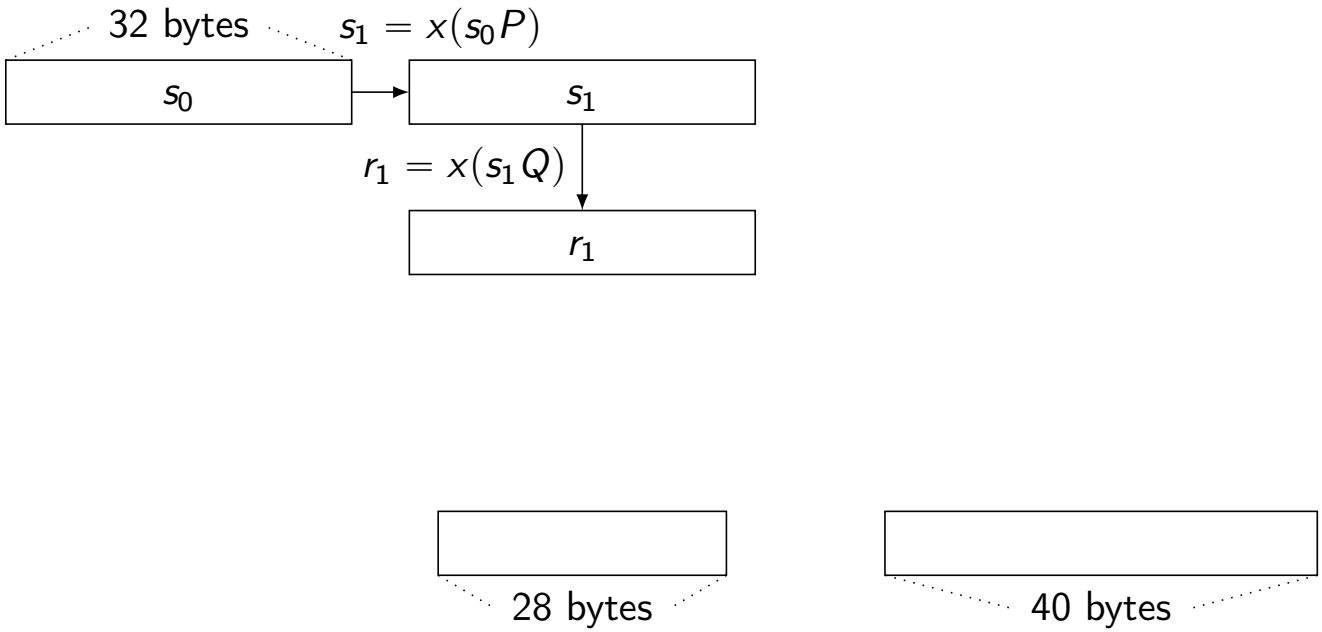
Points Q and P on an elliptic curve.





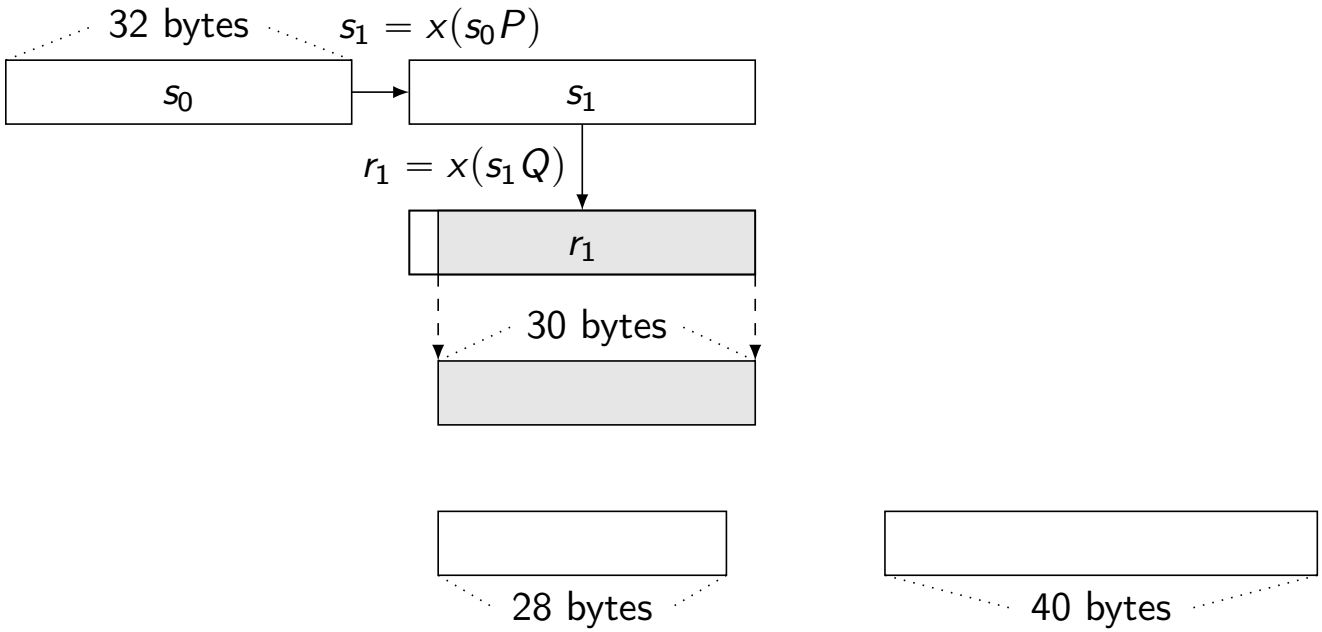
Dual EC — Basic Procedure

Points Q and P on an elliptic curve.



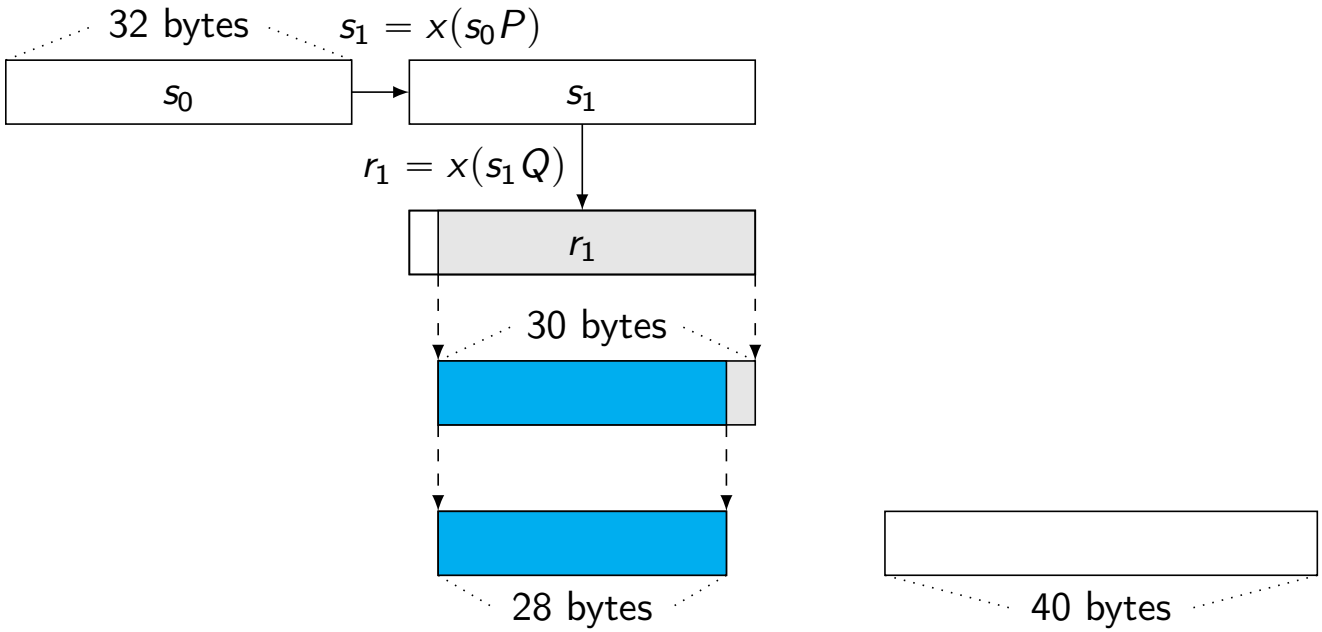
Dual EC — Basic Procedure

Points Q and P on an elliptic curve.



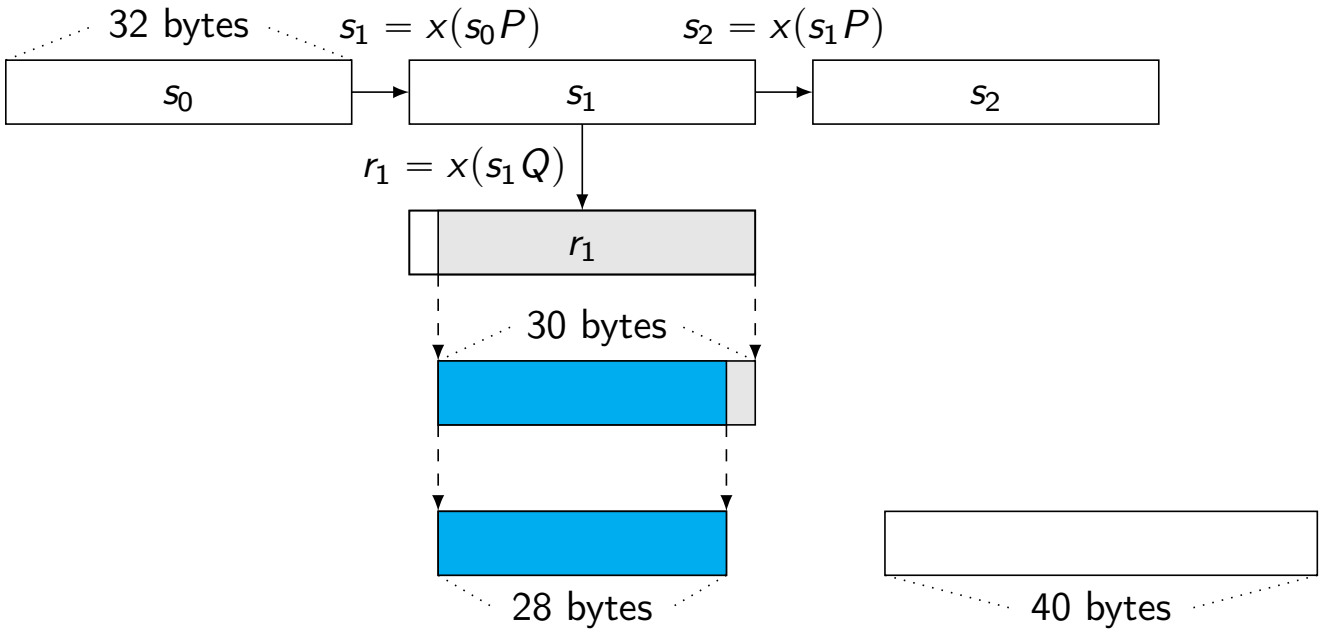
Dual EC — Basic Procedure

Points Q and P on an elliptic curve.



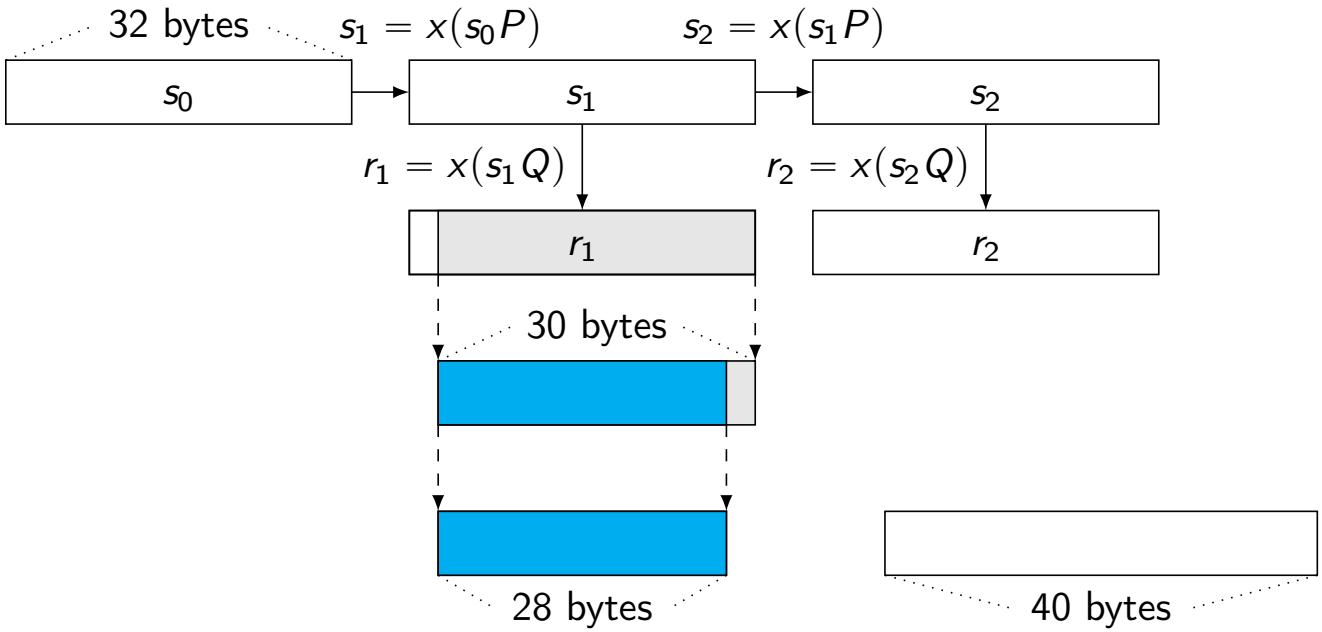
Dual EC — Basic Procedure

Points Q and P on an elliptic curve.



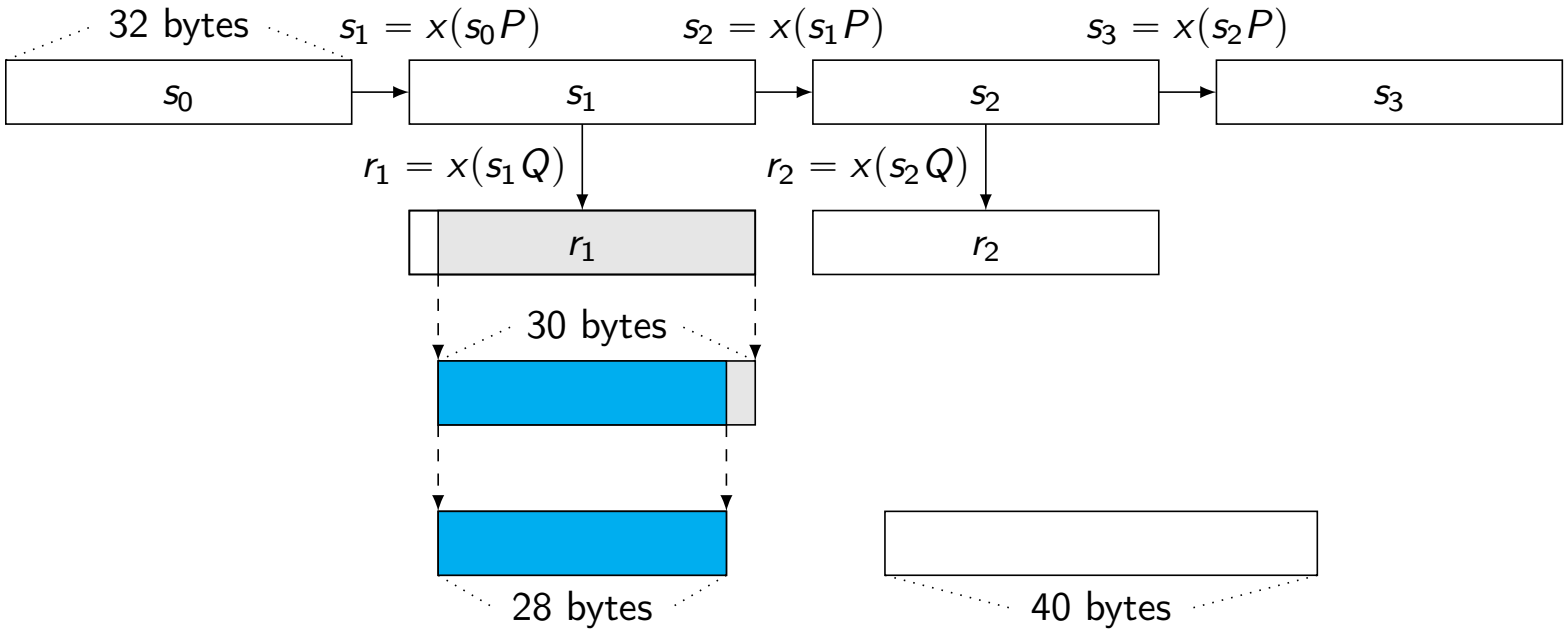
Dual EC — Basic Procedure

Points Q and P on an elliptic curve.



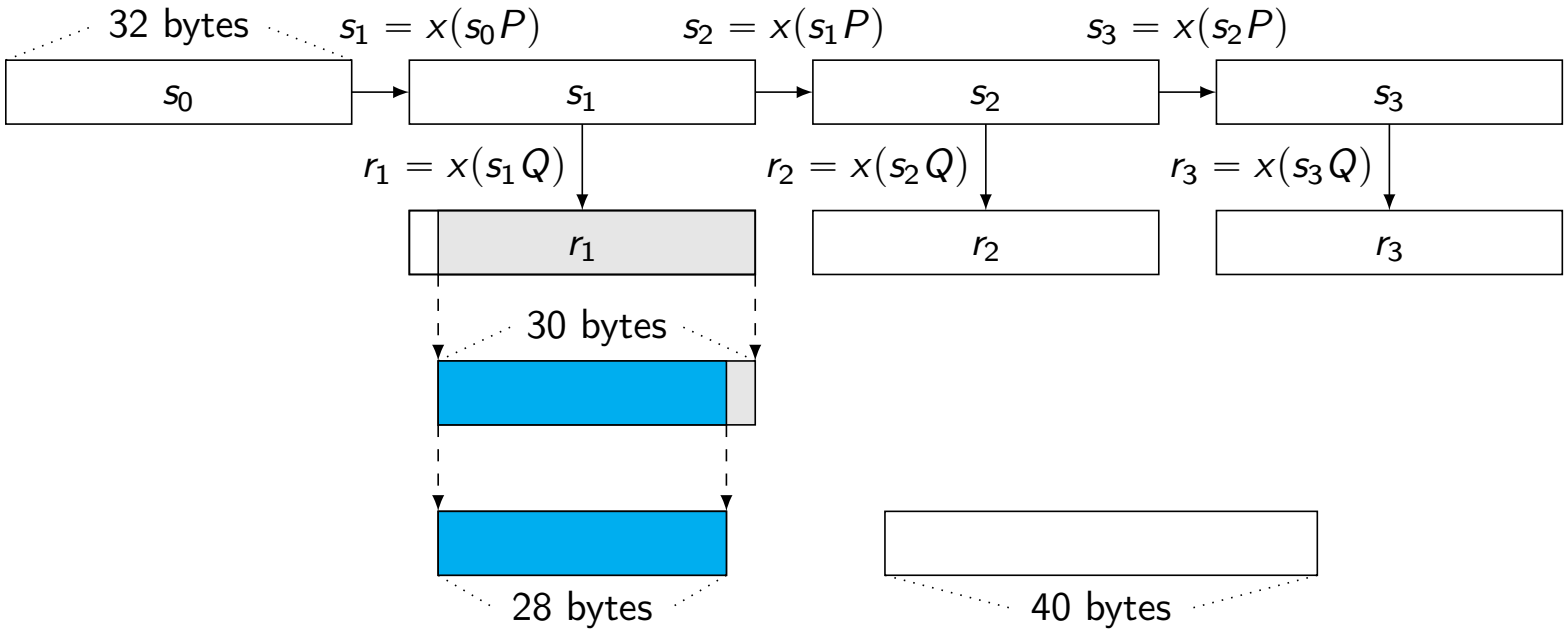
Dual EC — Basic Procedure

Points Q and P on an elliptic curve.



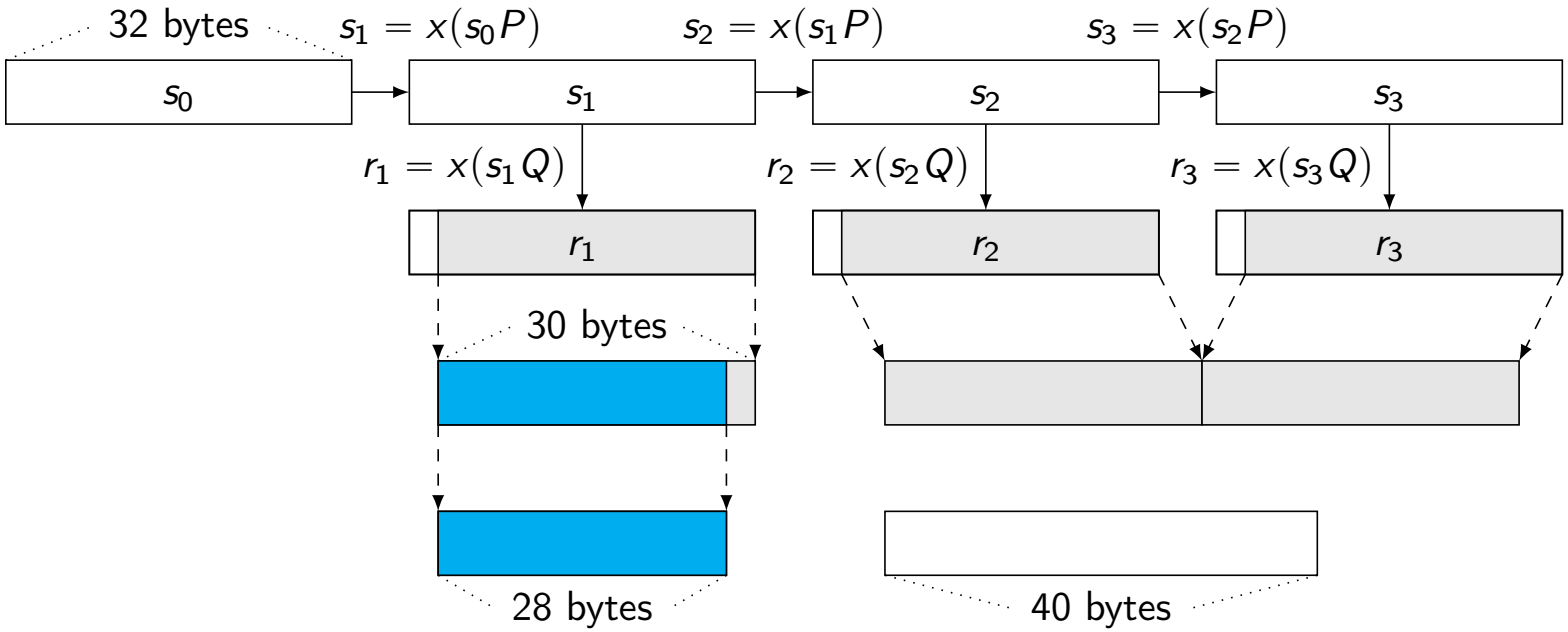
Dual EC — Basic Procedure

Points Q and P on an elliptic curve.



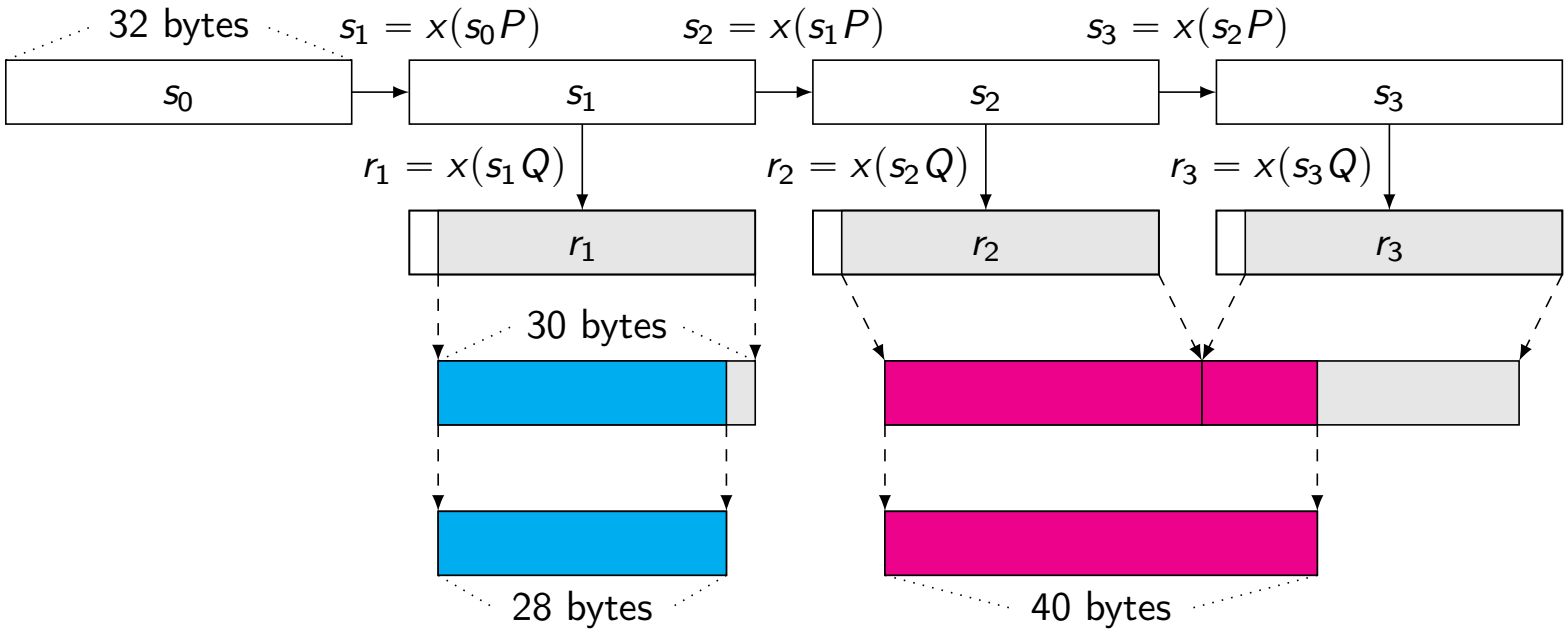
Dual EC — Basic Procedure

Points Q and P on an elliptic curve.



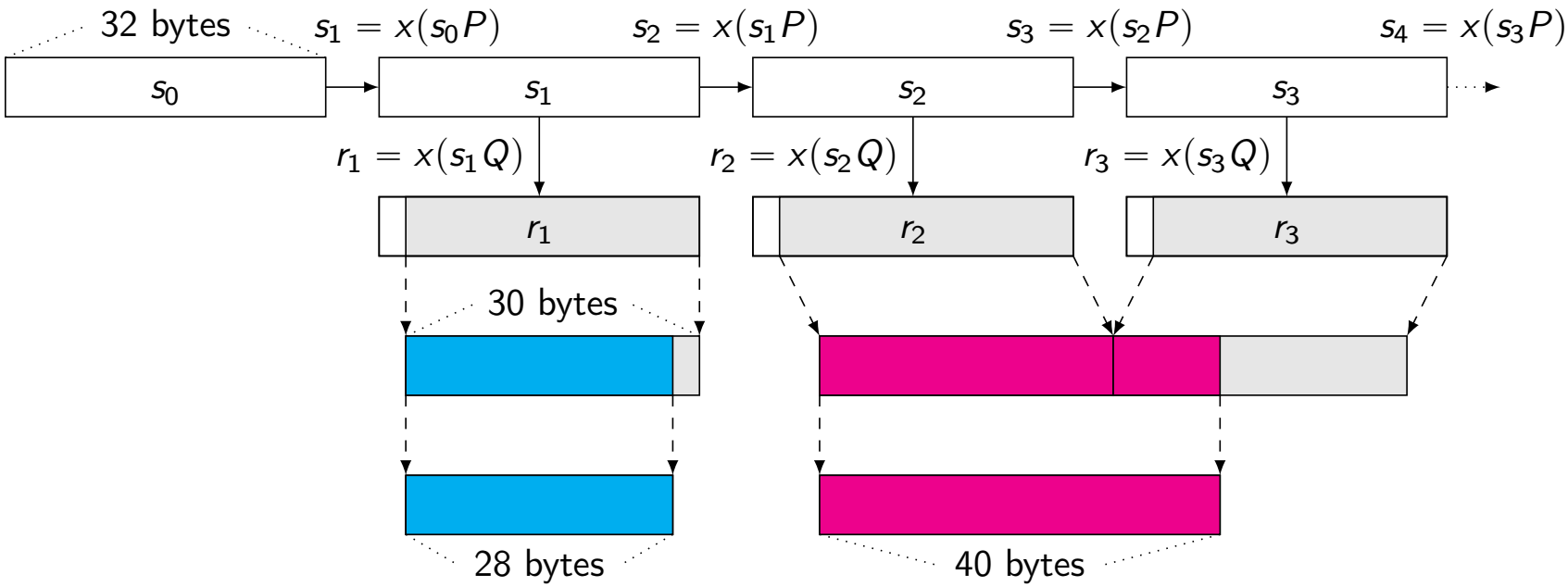
Dual EC — Basic Procedure

Points Q and P on an elliptic curve.



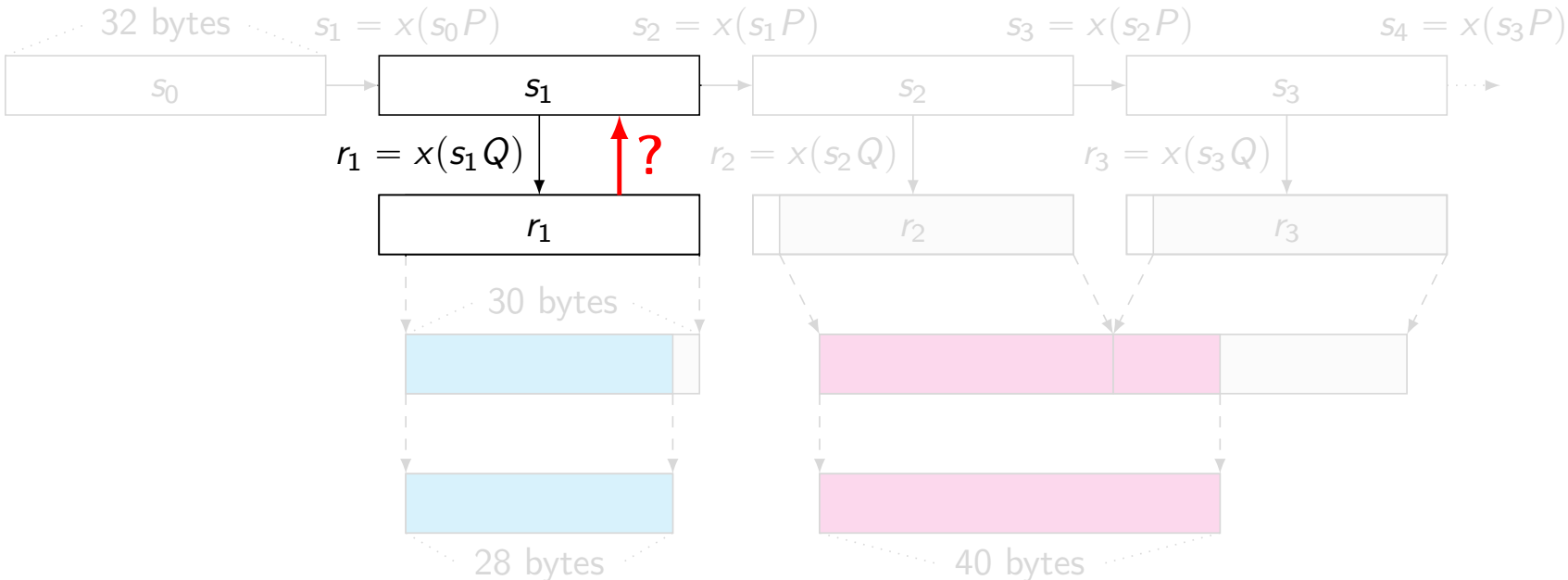
Dual EC — Basic Procedure

Points Q and P on an elliptic curve.



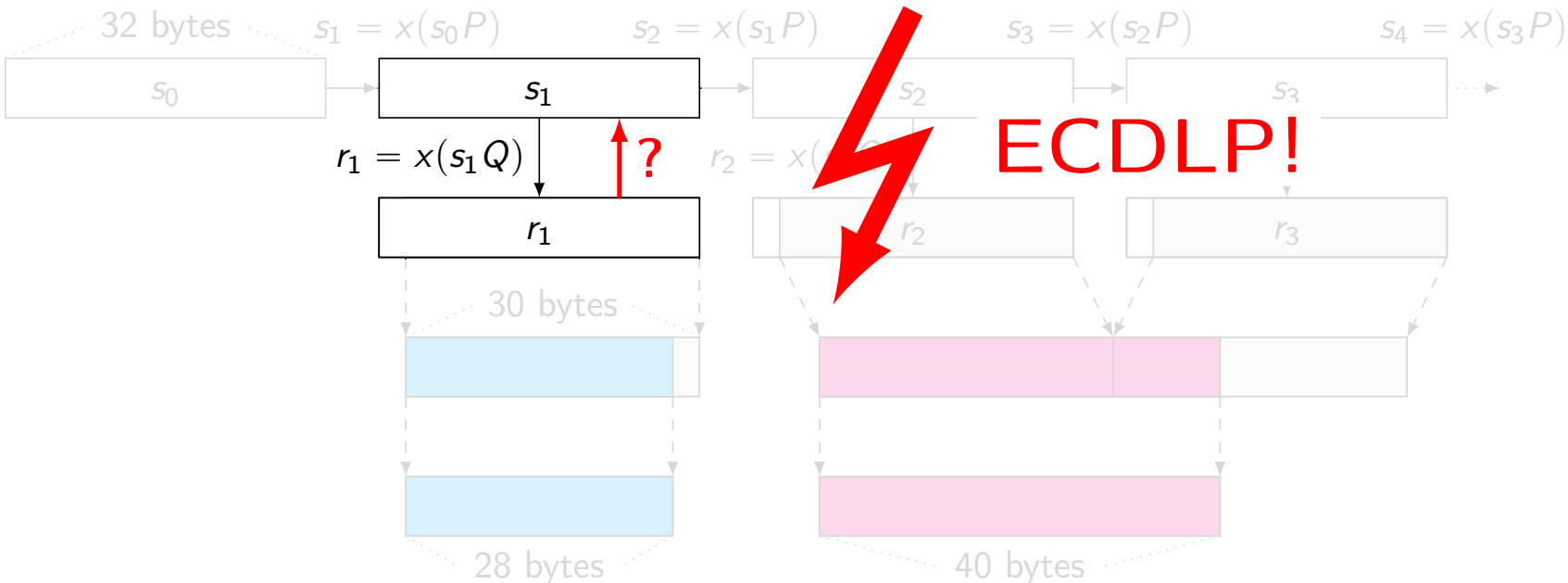
Dual EC — Basic Procedure

Points Q and P on an elliptic curve.



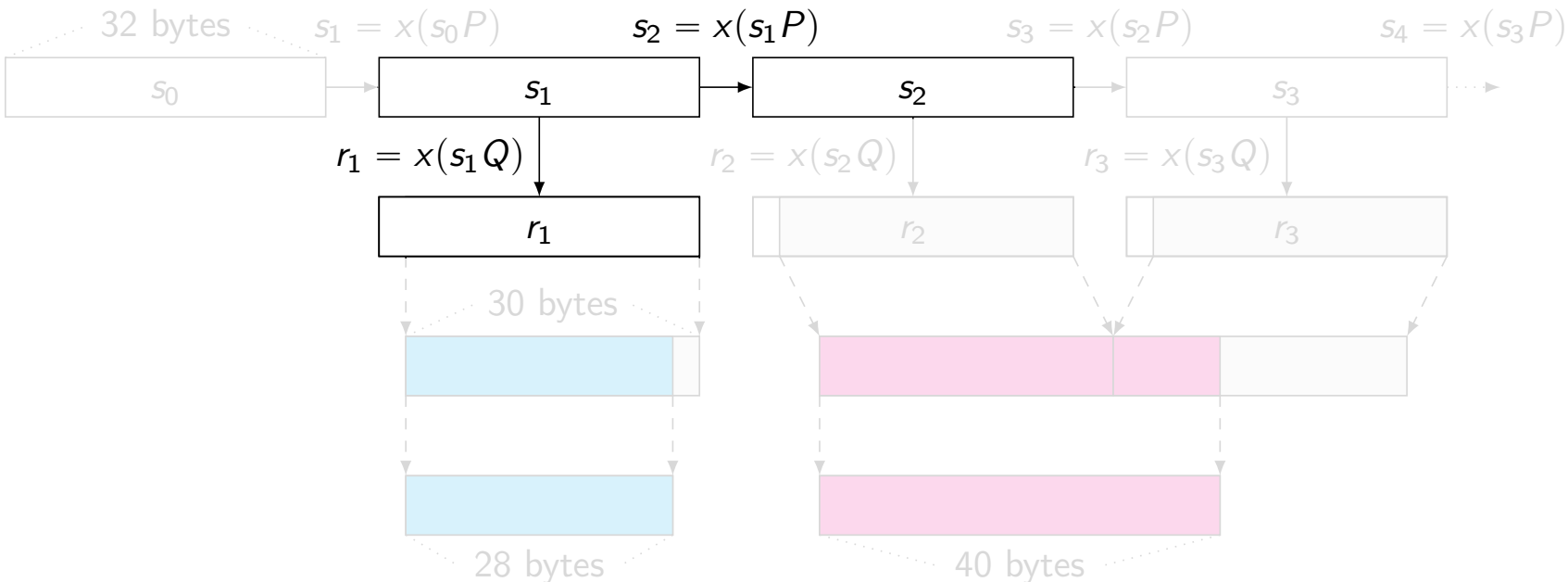
Dual EC — Basic Procedure

Points Q and P on an elliptic curve.



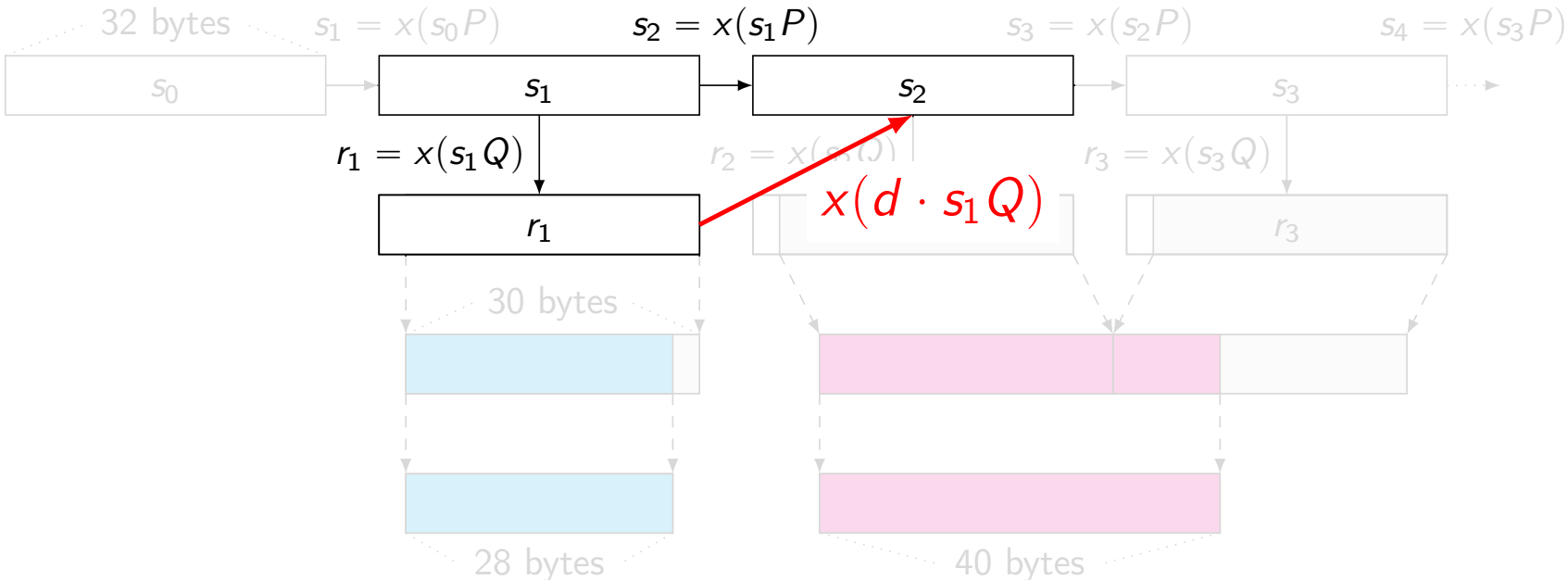
Shumow and Ferguson – the Basic Attack

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



Shumow and Ferguson – the Basic Attack

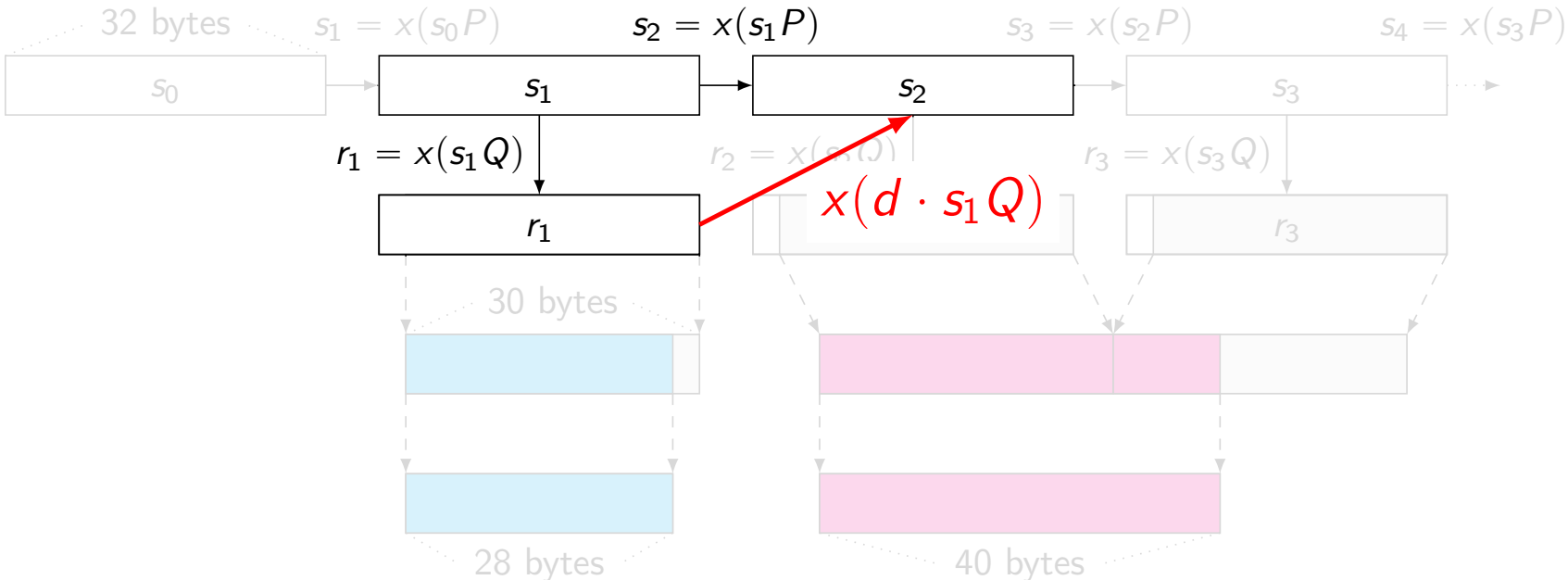
Points Q and $P = dQ$ on an elliptic curve.



Shumow and Ferguson – the Basic Attack

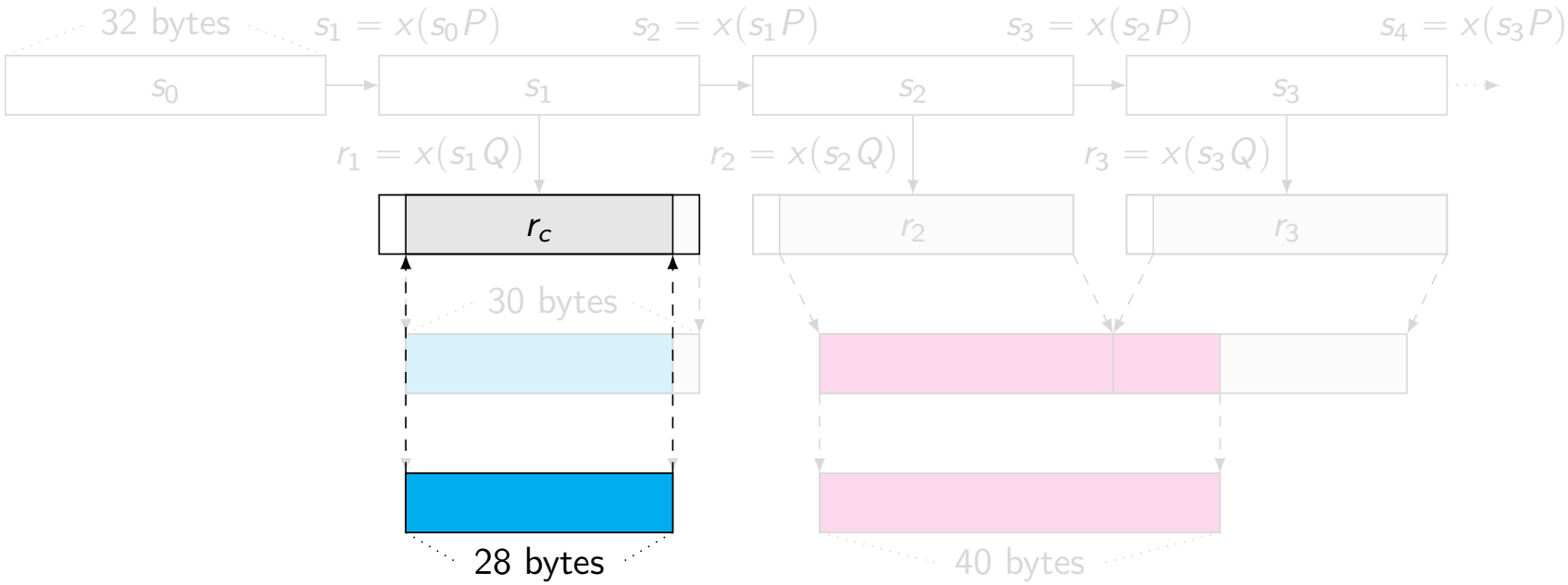
Points Q and $P = dQ$ on an elliptic curve.

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



Shumow and Ferguson – the Basic Attack

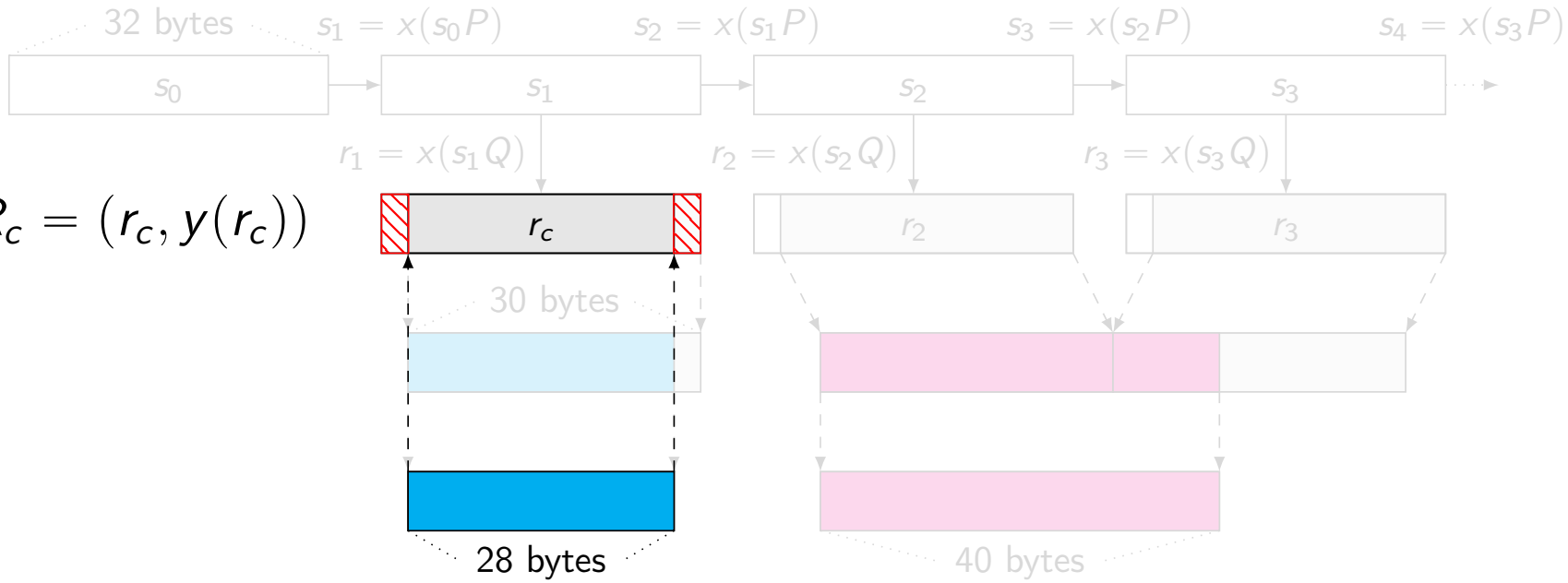
Points Q and $P = dQ$ on an elliptic curve.



Shumow and Ferguson – the Basic Attack

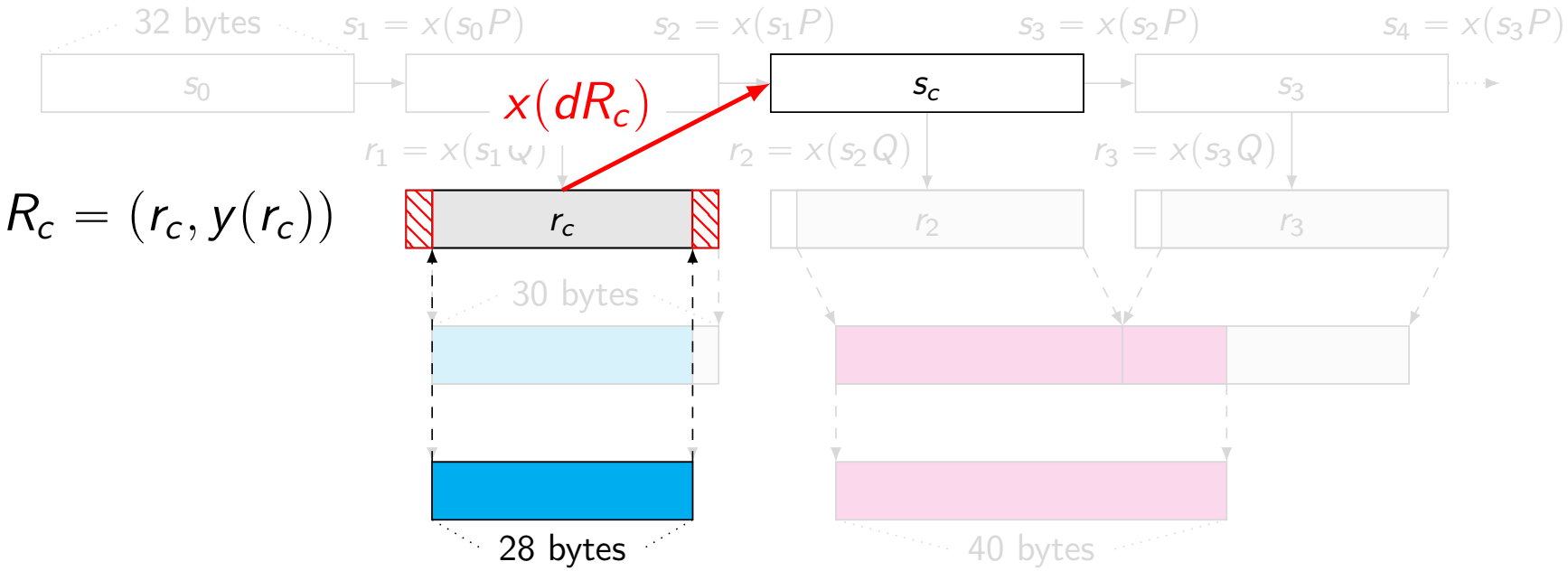
Points Q and $P = dQ$ on an elliptic curve.

$R_c = (r_c, y(r_c))$



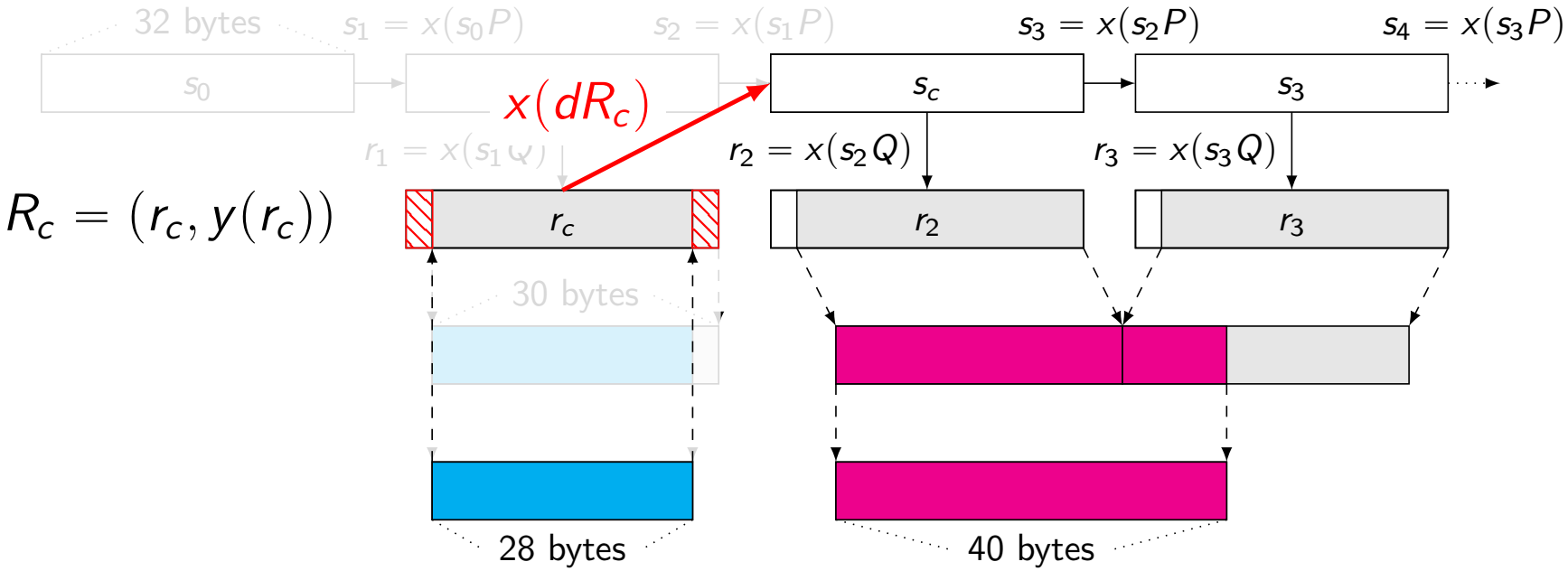
Shumow and Ferguson – the Basic Attack

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

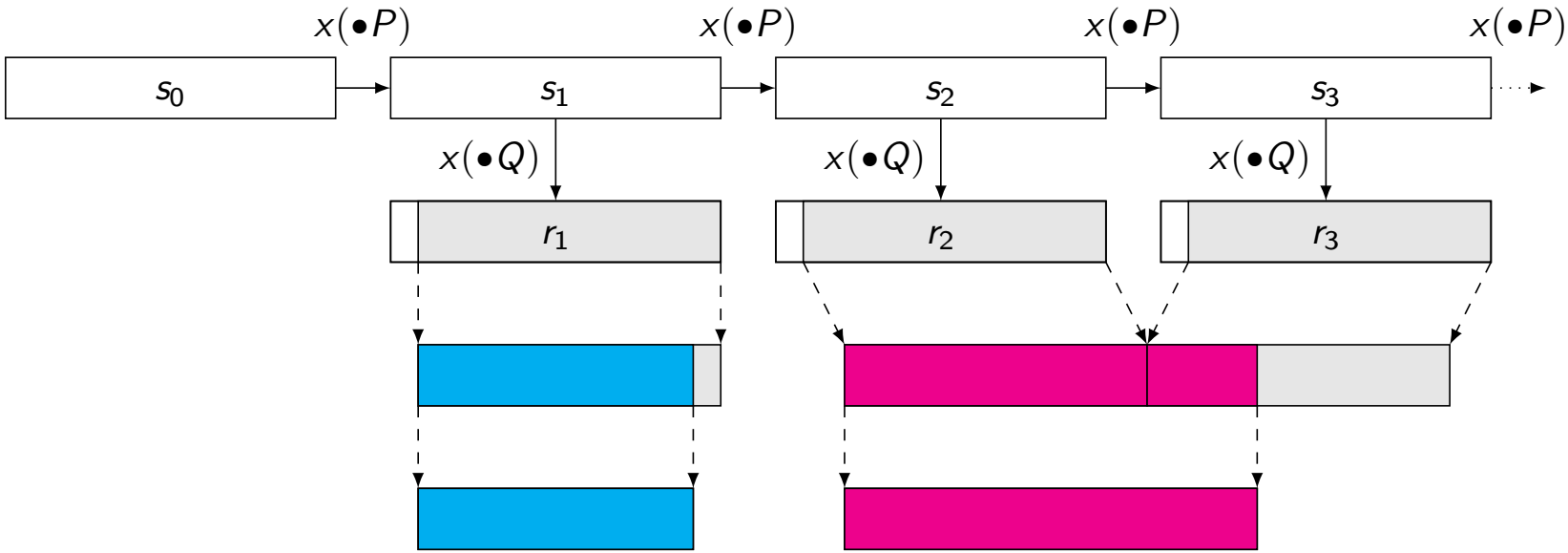


Shumow and Ferguson – the Basic Attack

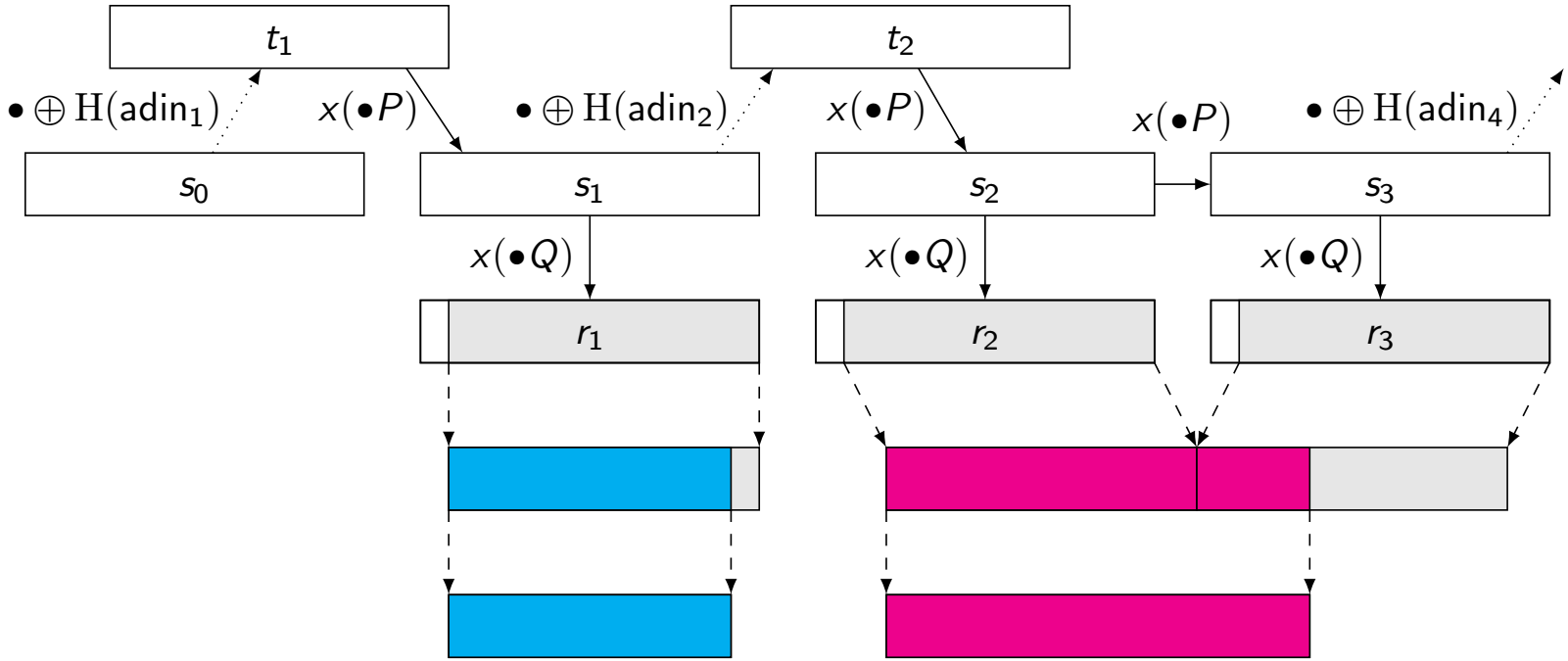
Points Q and $P = dQ$ on an elliptic curve.



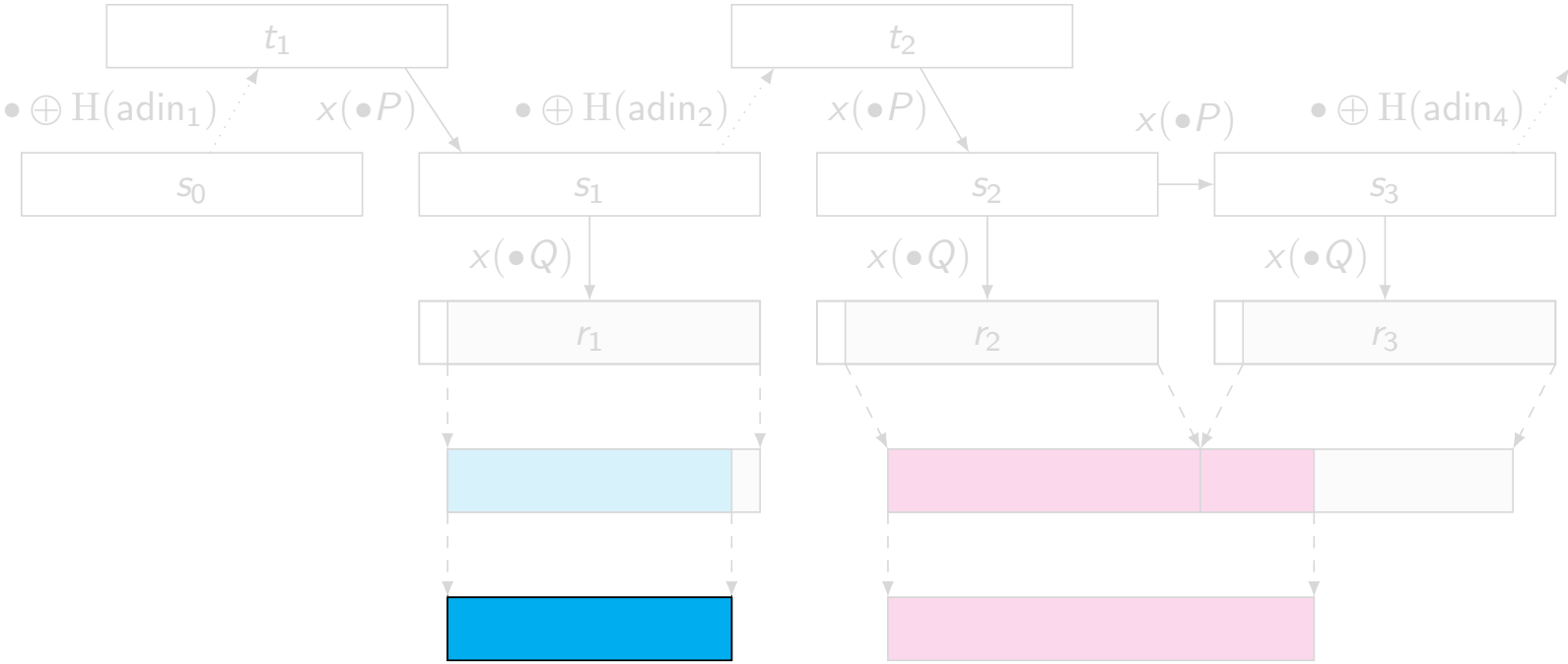
Dual EC — Basic Procedure



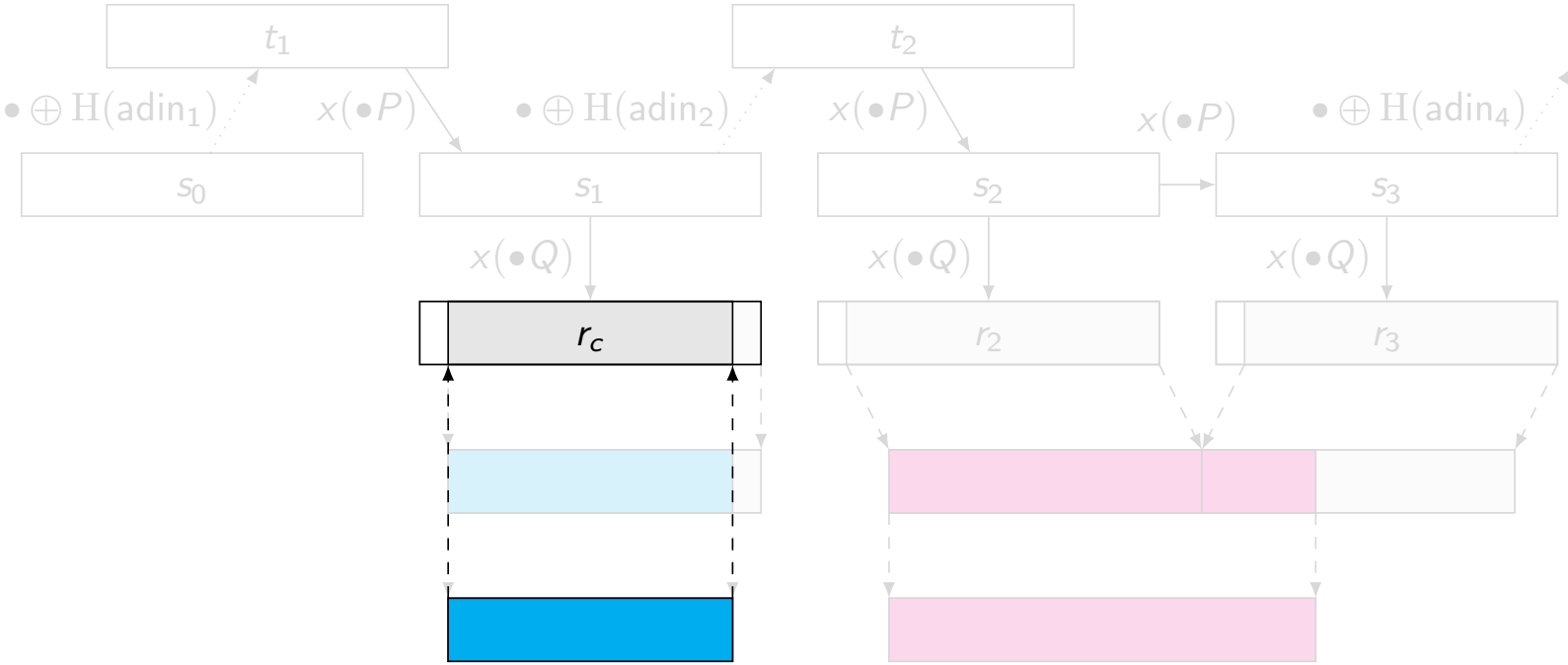
Dual EC — NIST SP800-9 in June 2006



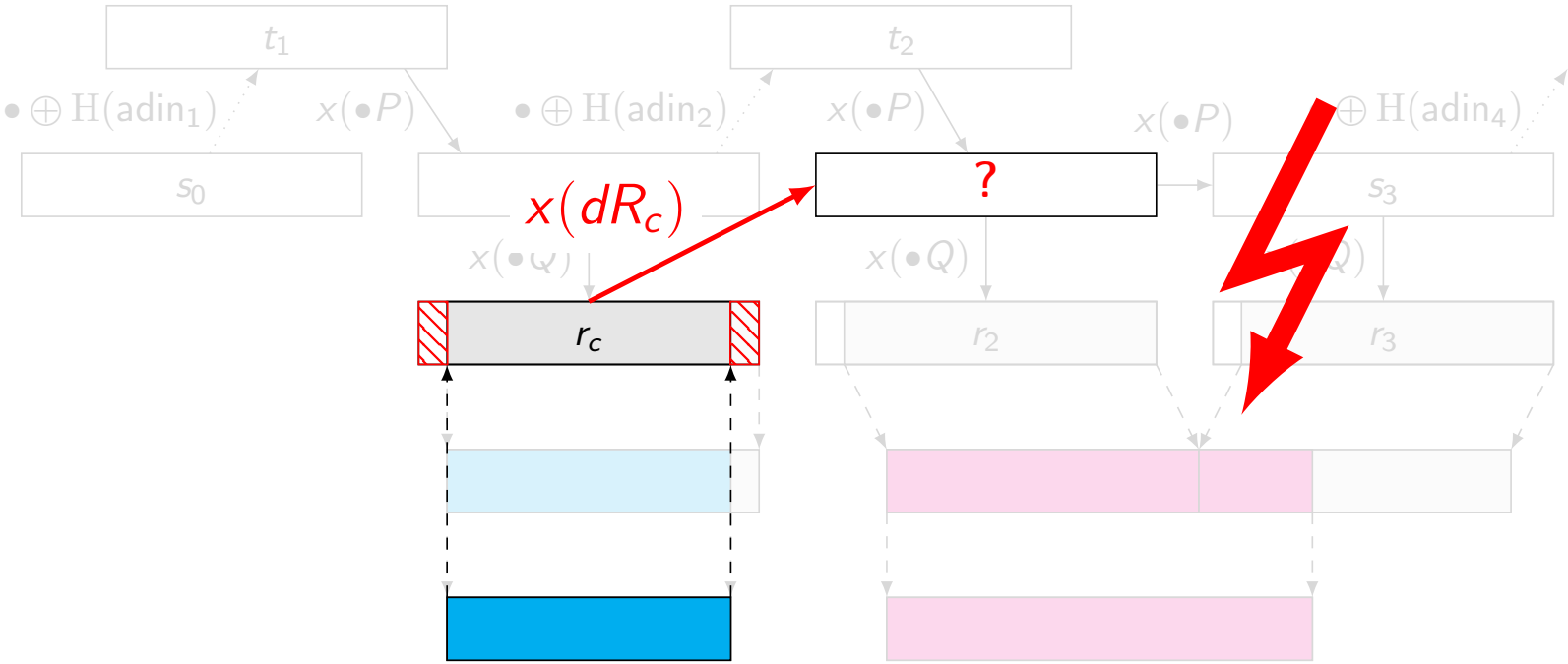
Dual EC — NIST SP800-9 in June 2006



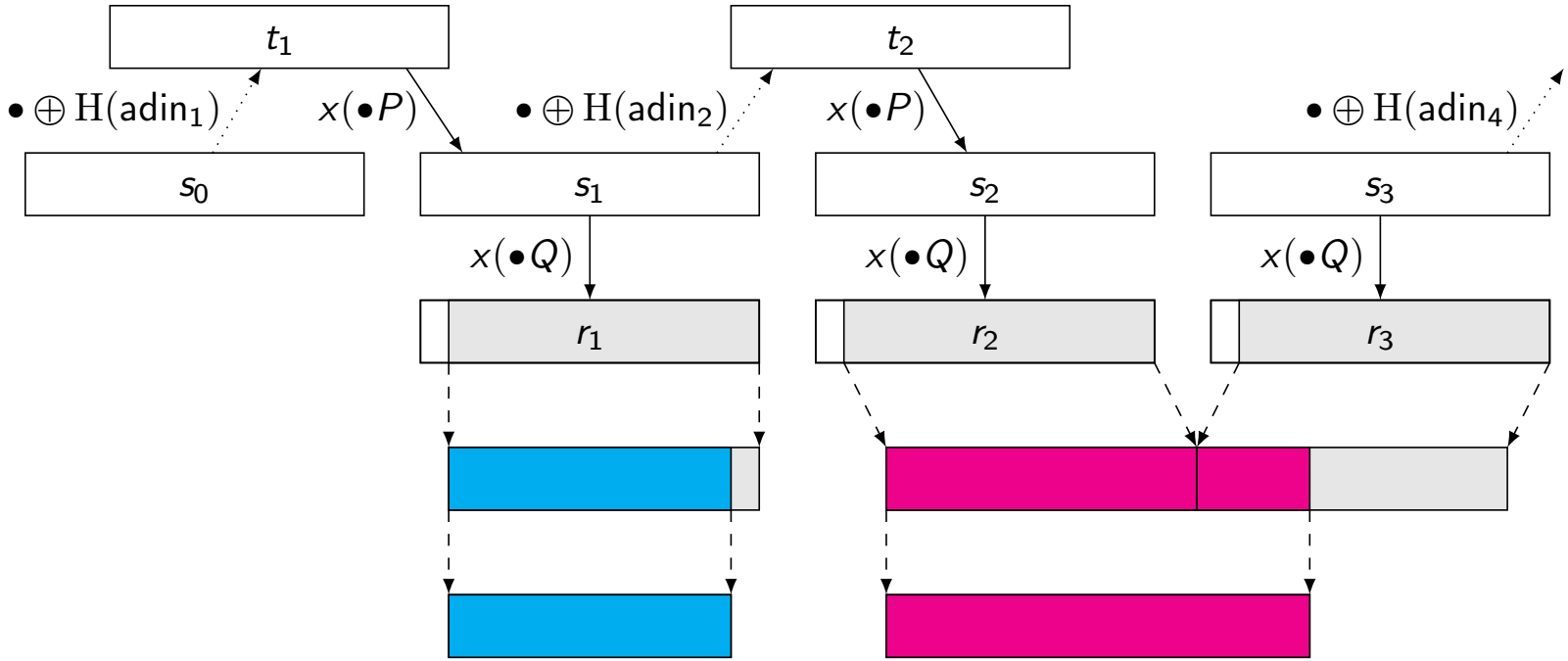
Dual EC — NIST SP800-9 in June 2006



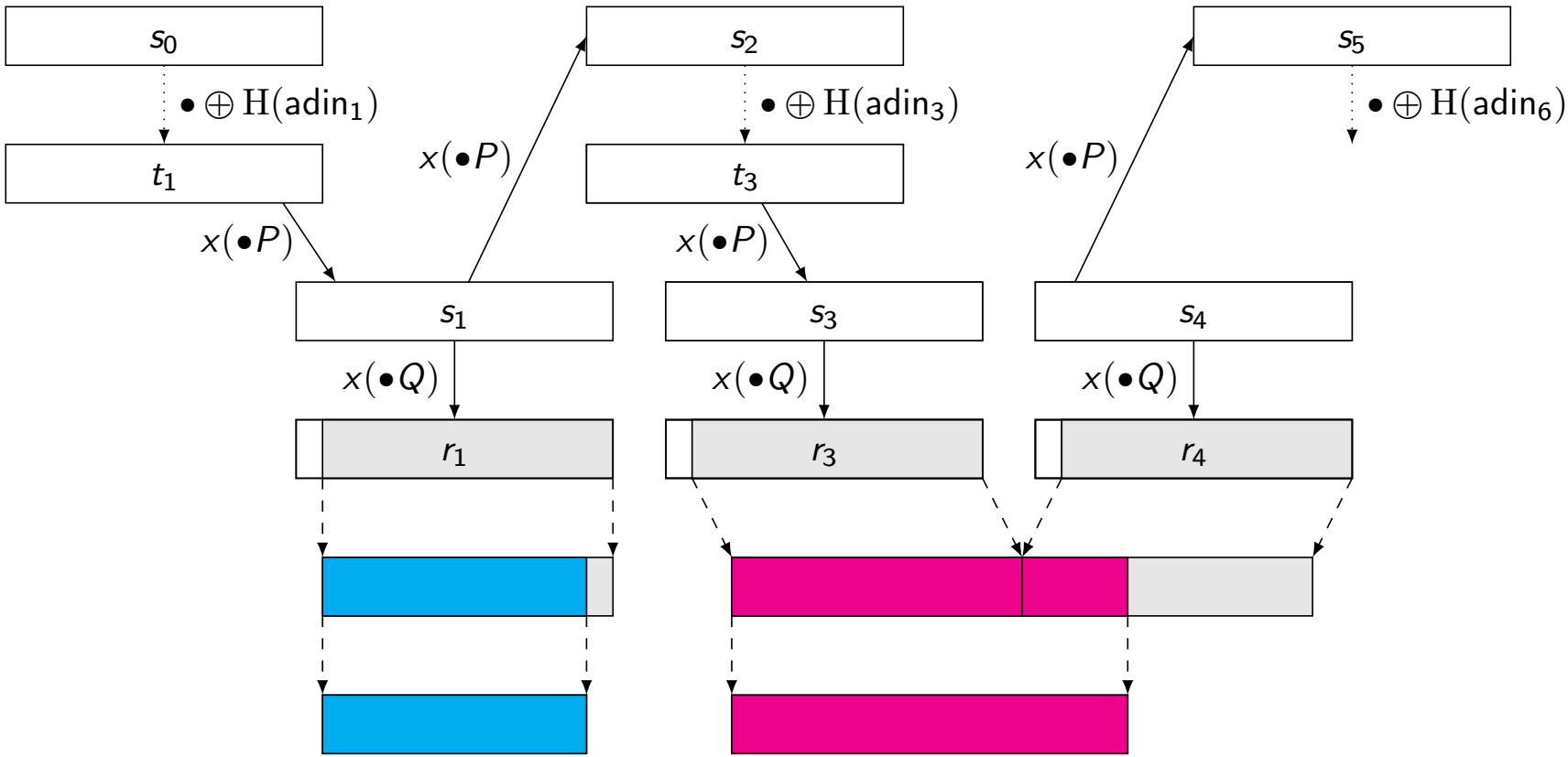
Dual EC — NIST SP800-9 in June 2006



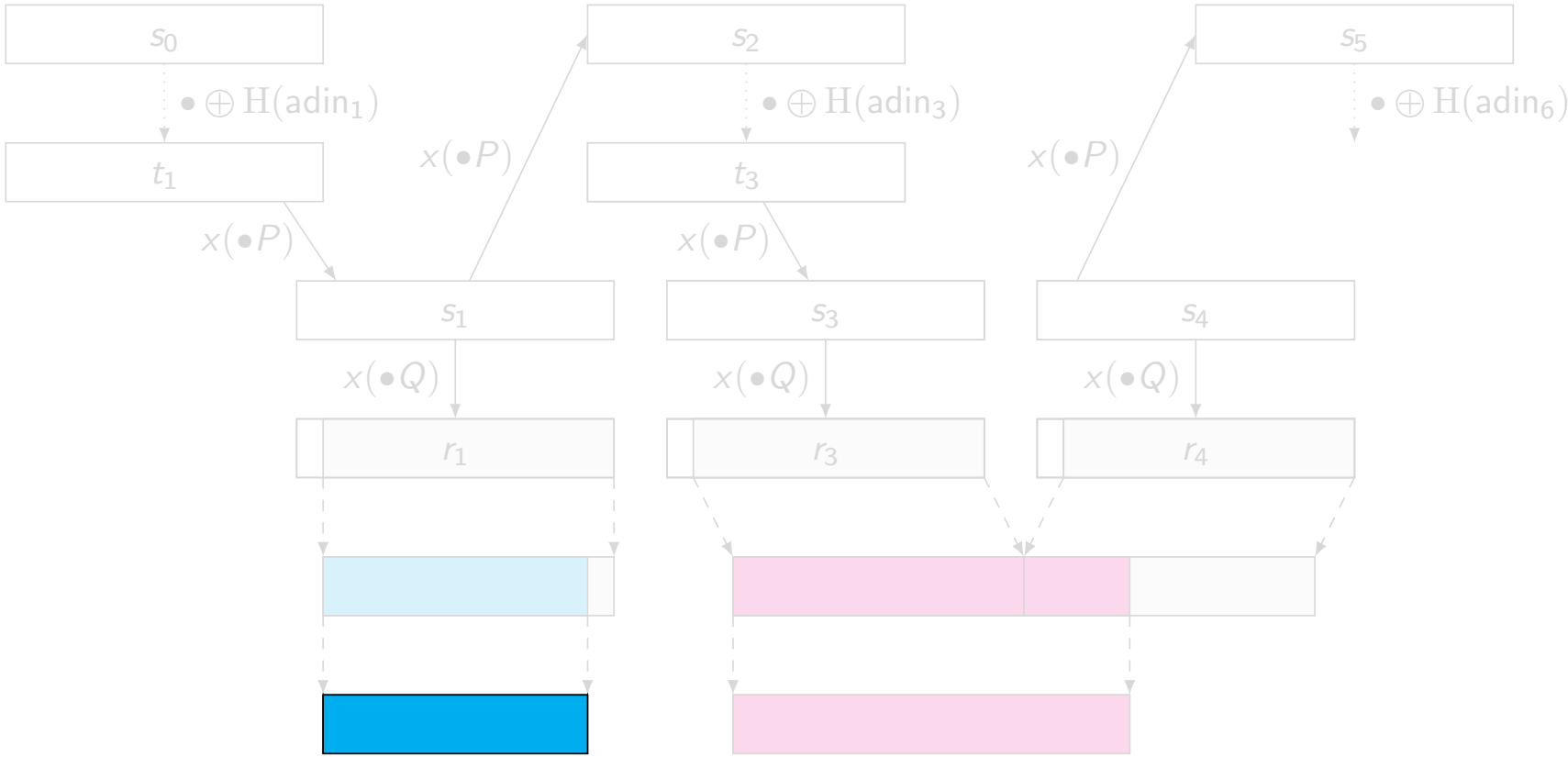
Dual EC — Basic Procedure



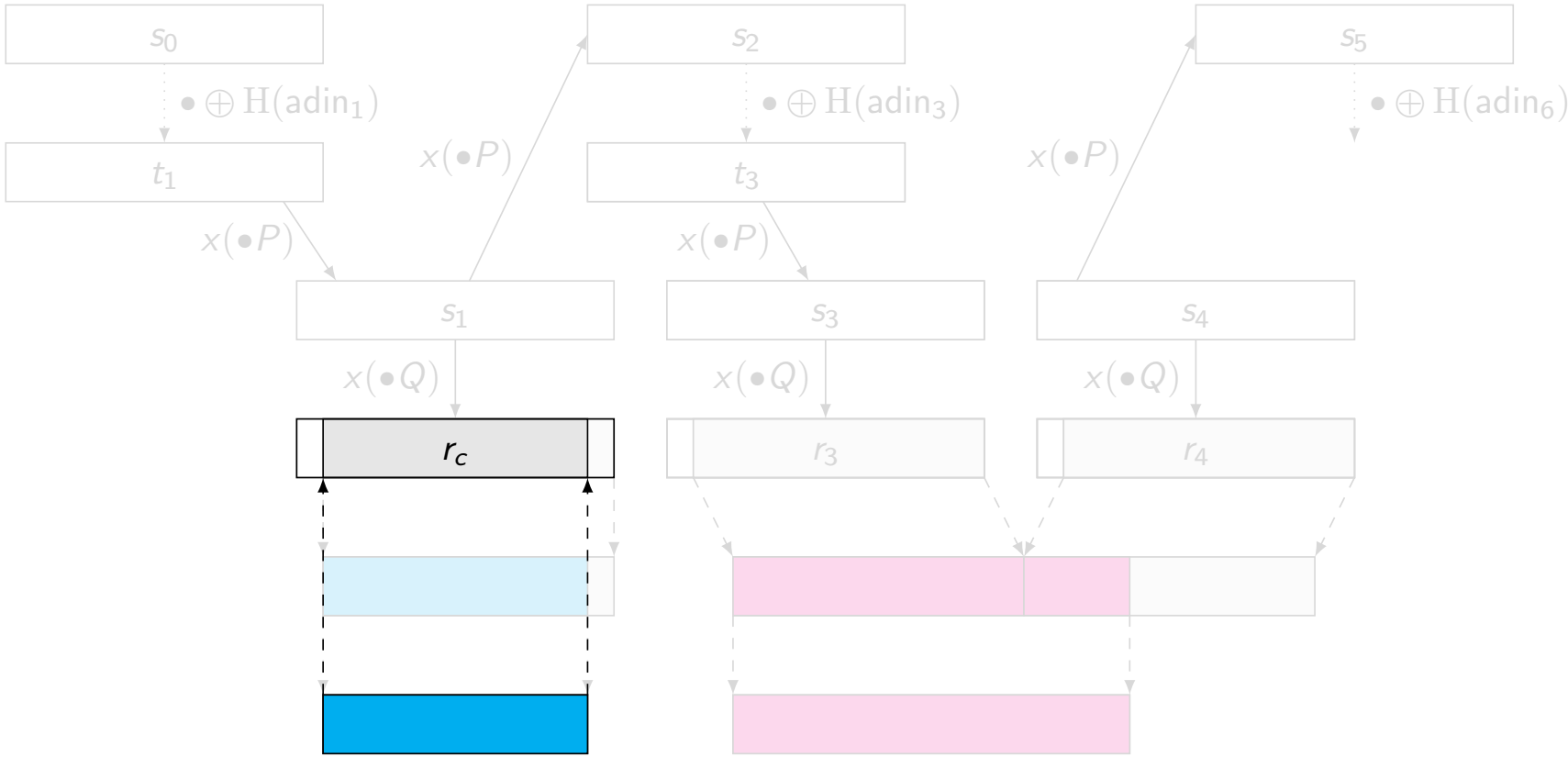
Dual EC — NIST SP800-90 in March 2007



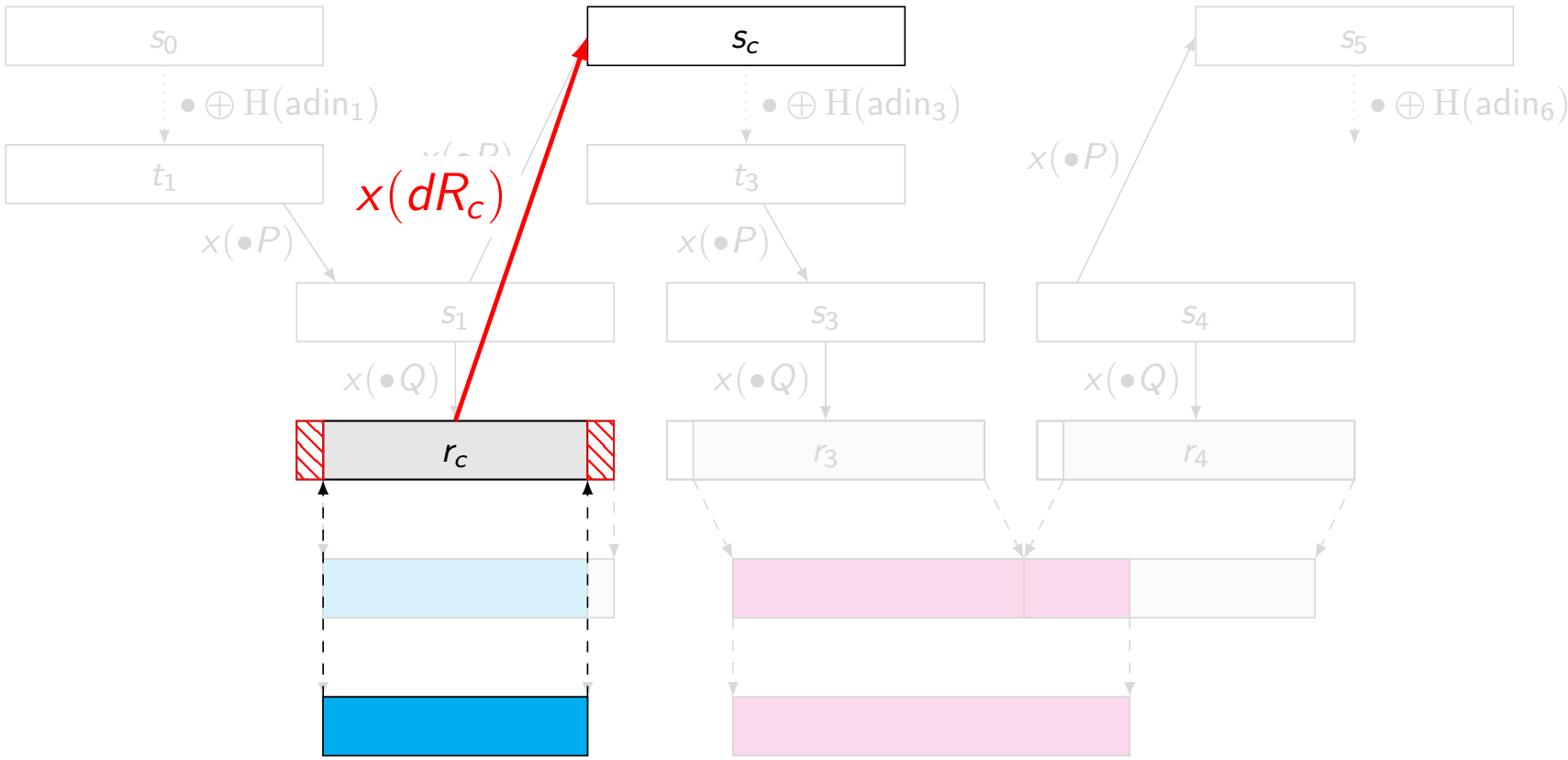
Dual EC — NIST SP800-90 in March 2007



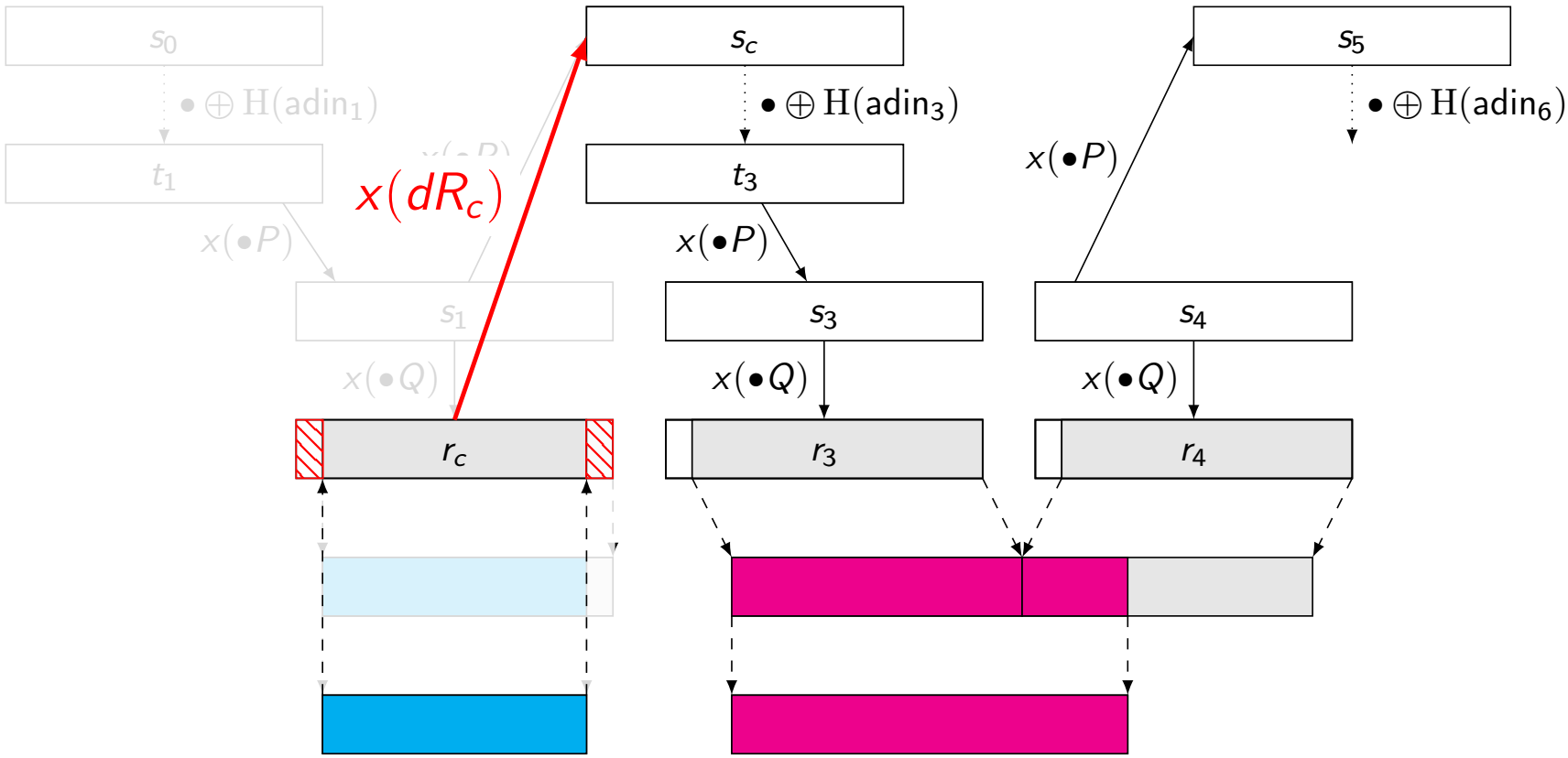
Dual EC — NIST SP800-90 in March 2007



Dual EC — NIST SP800-90 in March 2007



Dual EC — NIST SP800-90 in March 2007



Attack

Attack targets in our analysis:

- RSA's BSAFE
  - RSA BSAFE Share for Java (BSAFE Java)
  - RSA BSAFE Share for C and C++ (BSAFE C)
- Microsoft's SChannel
- OpenSSL

We replaced the points P and Q with points where we know the back-door computation.

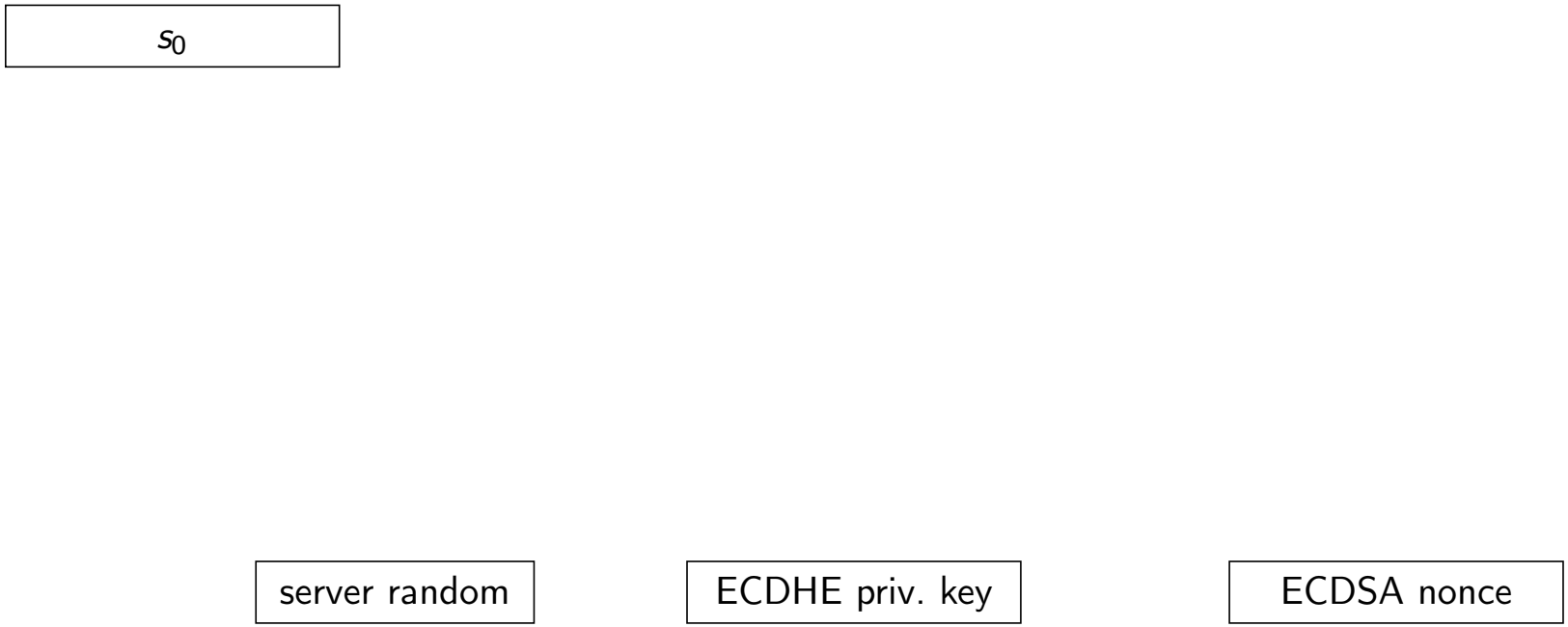
Attack — Example: BSAFE-Java

server random

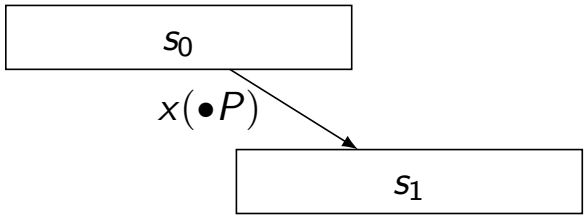
ECDHE priv. key

ECDSA nonce

Attack — Example: BSAFE-Java



Attack — Example: BSAFE-Java

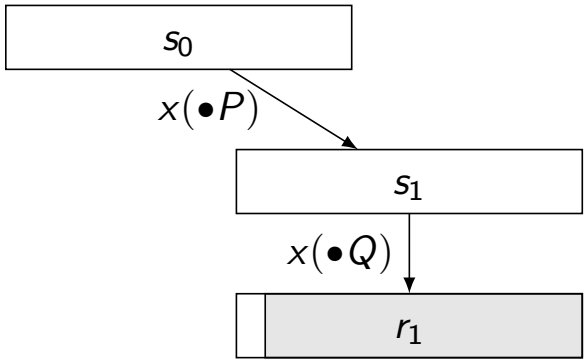


server random

ECDHE priv. key

ECDSA nonce

Attack — Example: BSAFE-Java

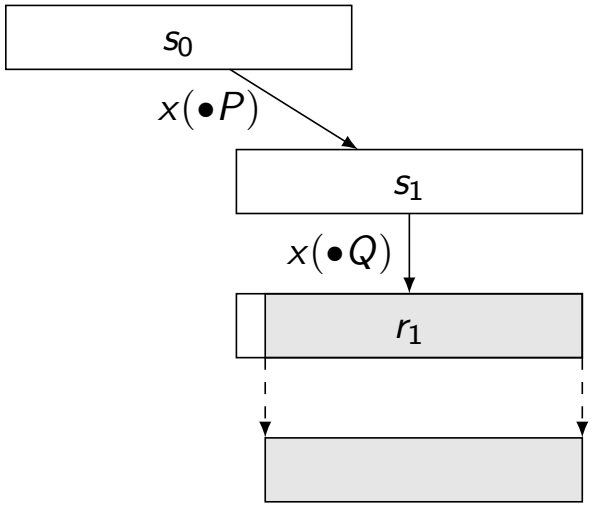


server random

ECDHE priv. key

ECDSA nonce

Attack — Example: BSAFE-Java

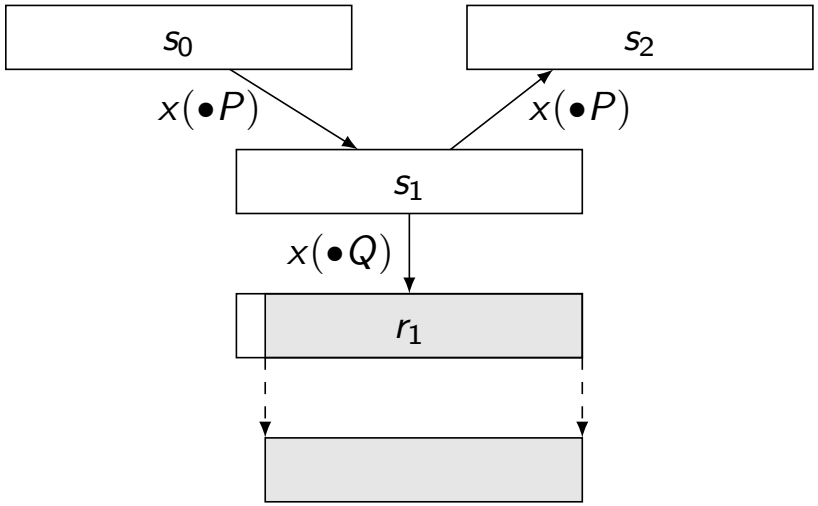


server random

ECDHE priv. key

ECDSA nonce

Attack — Example: BSAFE-Java

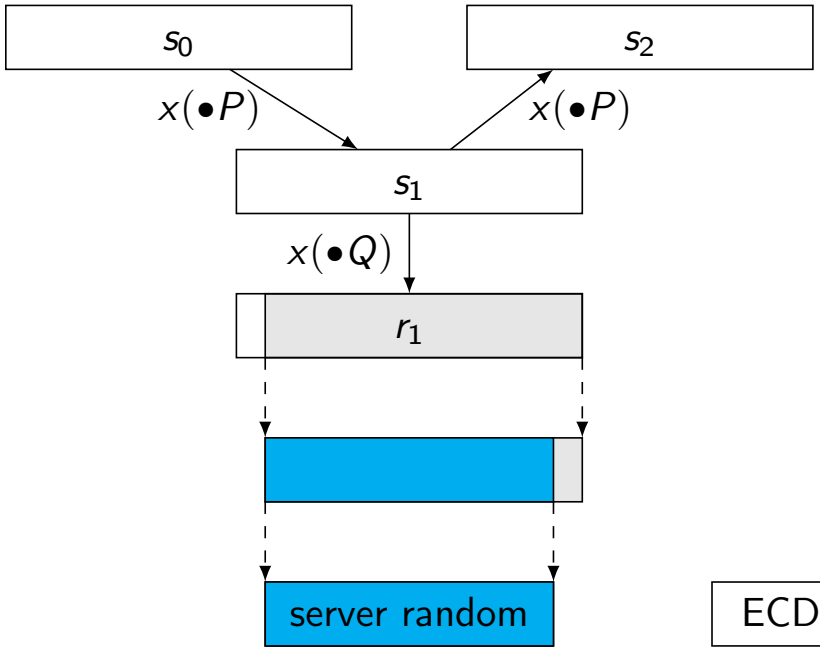


server random

ECDHE priv. key

ECDSA nonce

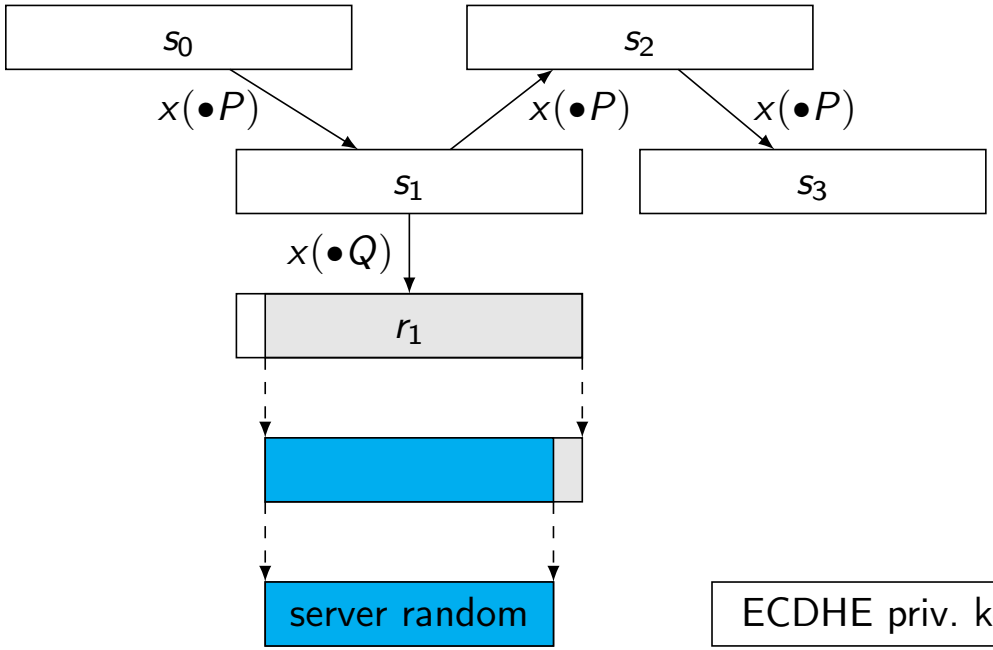
Attack — Example: BSAFE-Java



ECDHE priv. key

ECDSA nonce

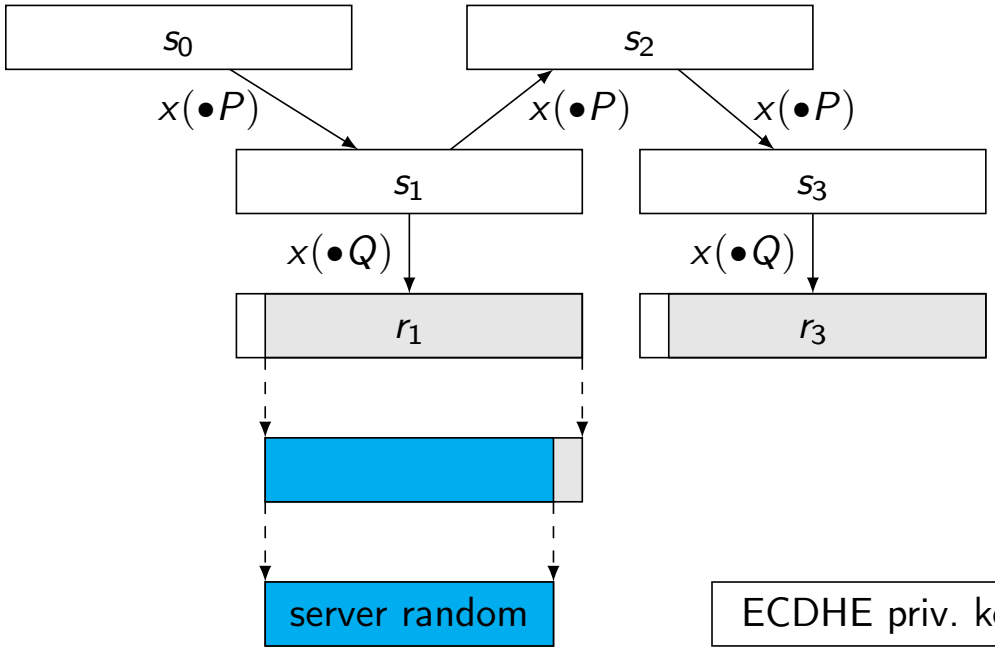
Attack — Example: BSAFE-Java



ECDHE priv. key

ECDSA nonce

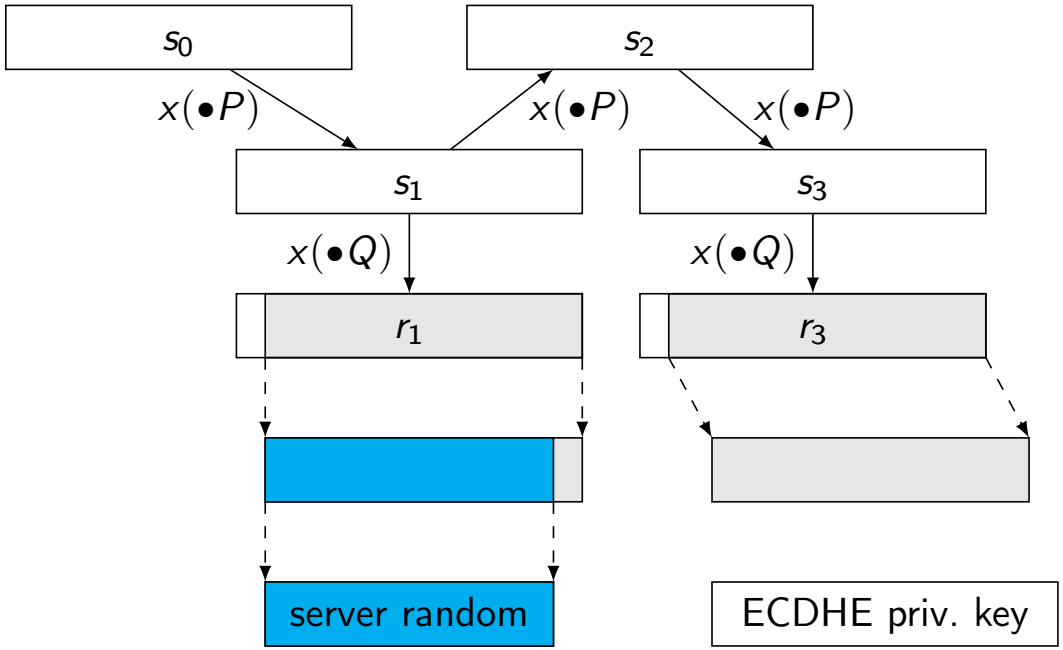
Attack — Example: BSAFE-Java



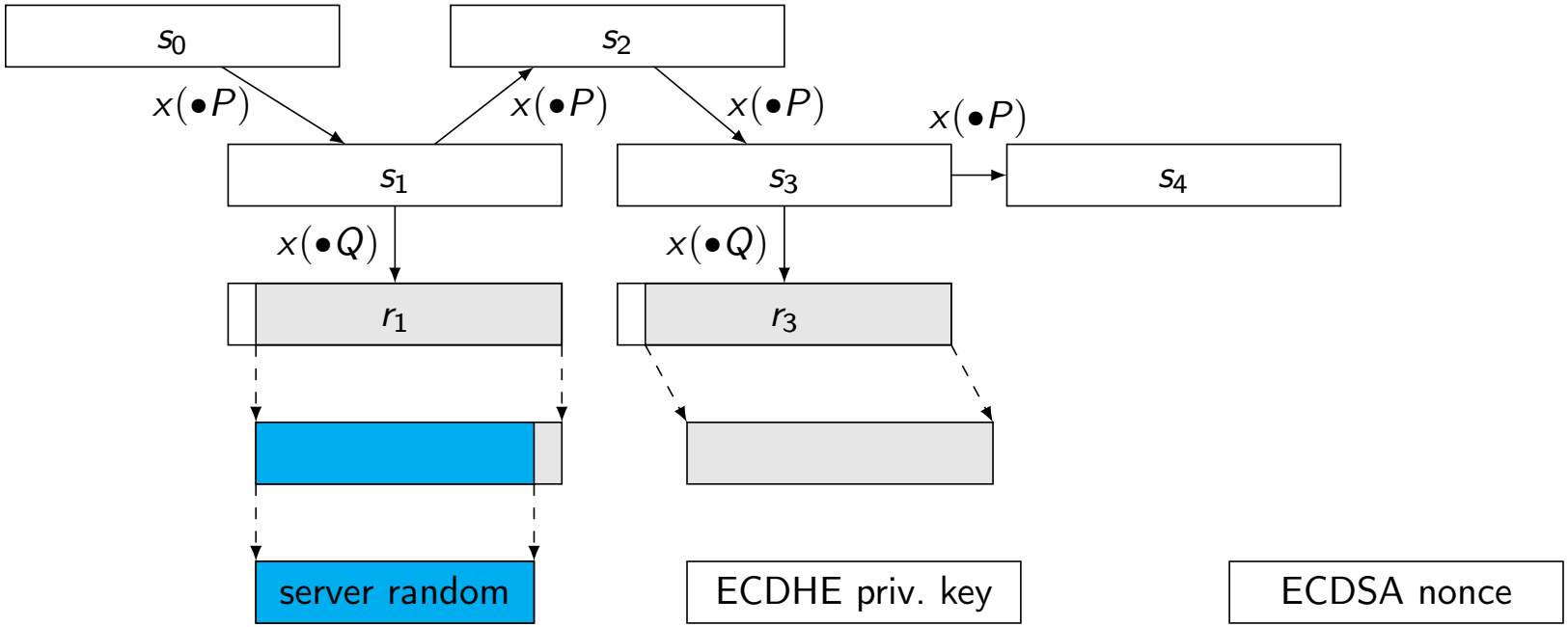
ECDHE priv. key

ECDSA nonce

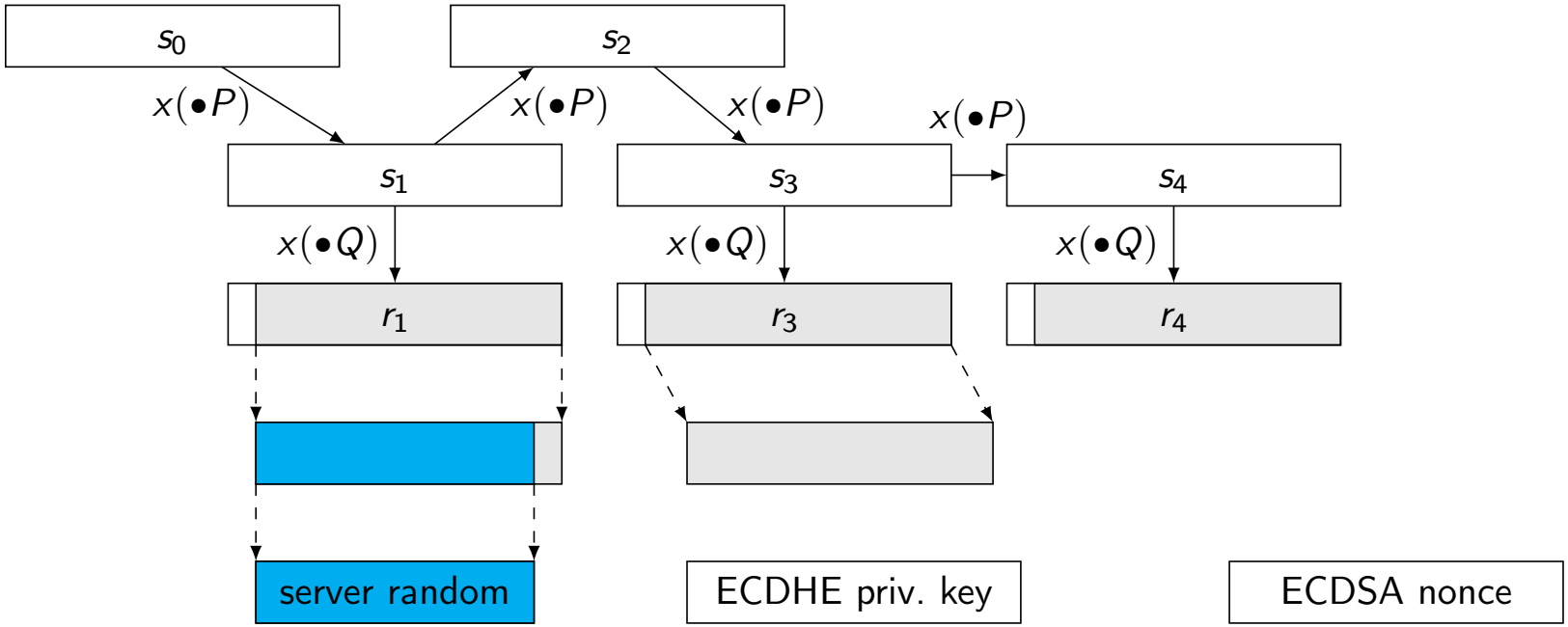
Attack — Example: BSAFE-Java



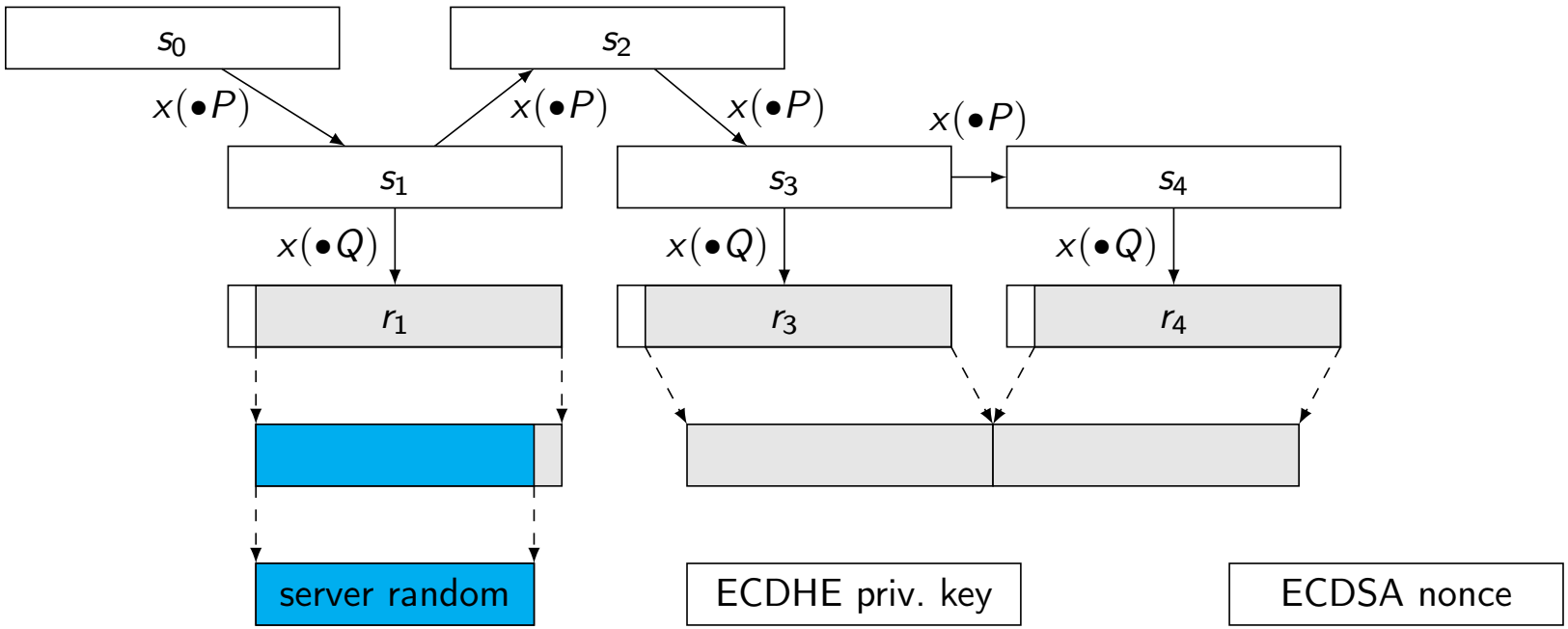
Attack — Example: BSAFE-Java



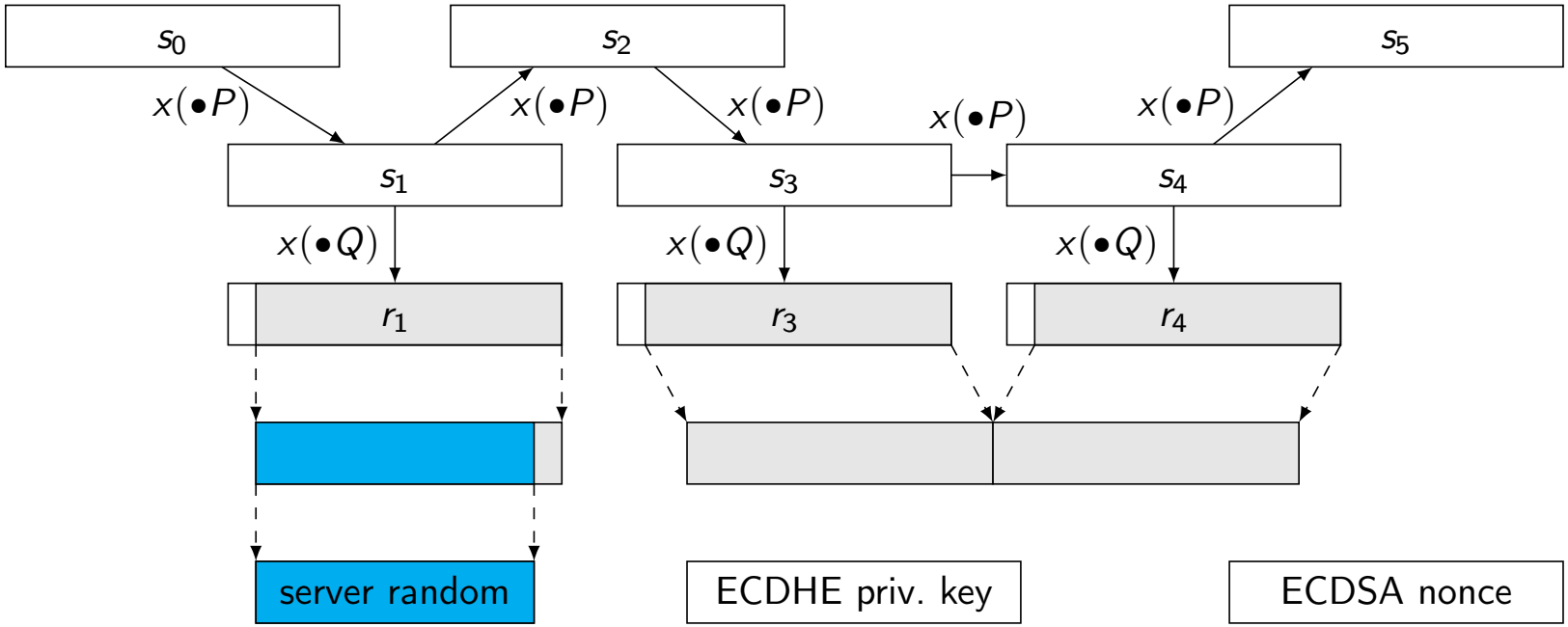
Attack — Example: BSAFE-Java



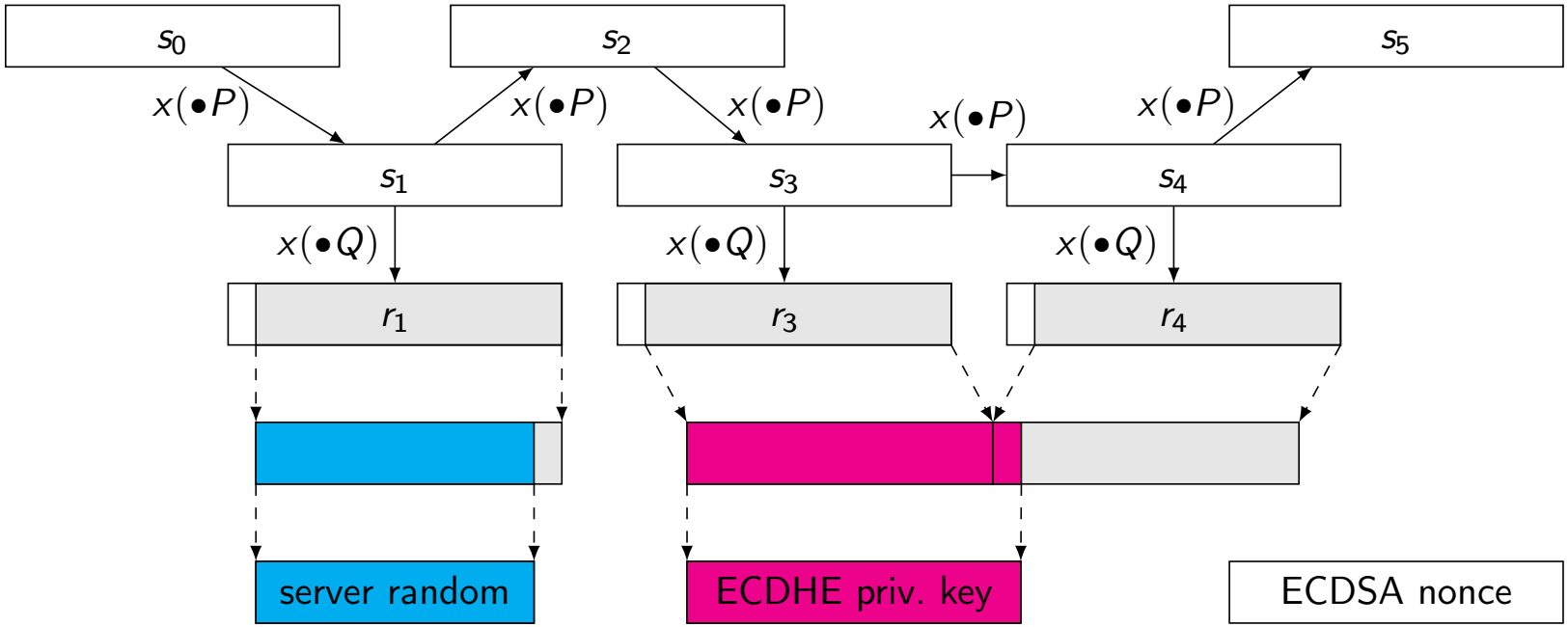
Attack — Example: BSAFE-Java



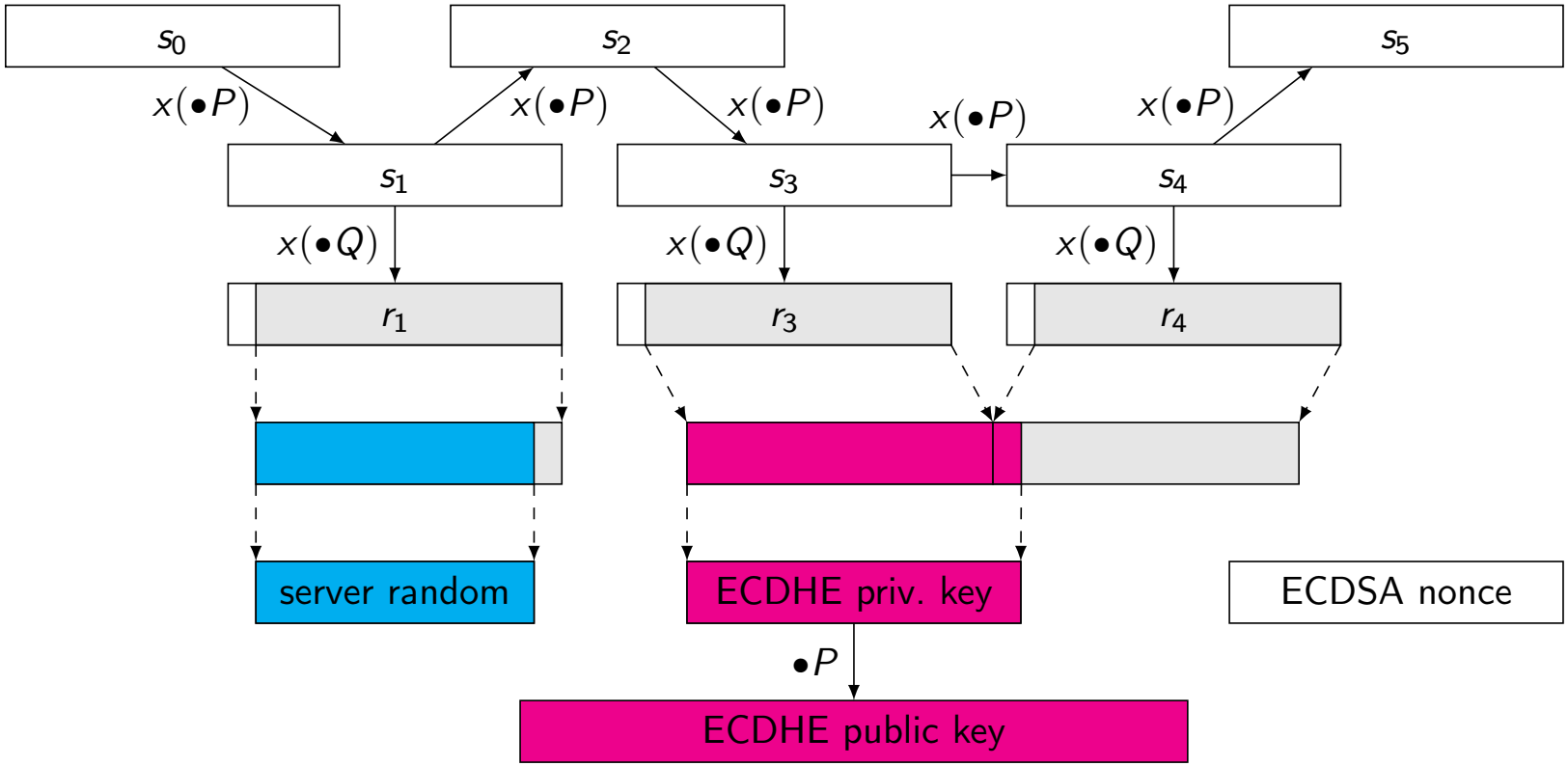
Attack — Example: BSAFE-Java



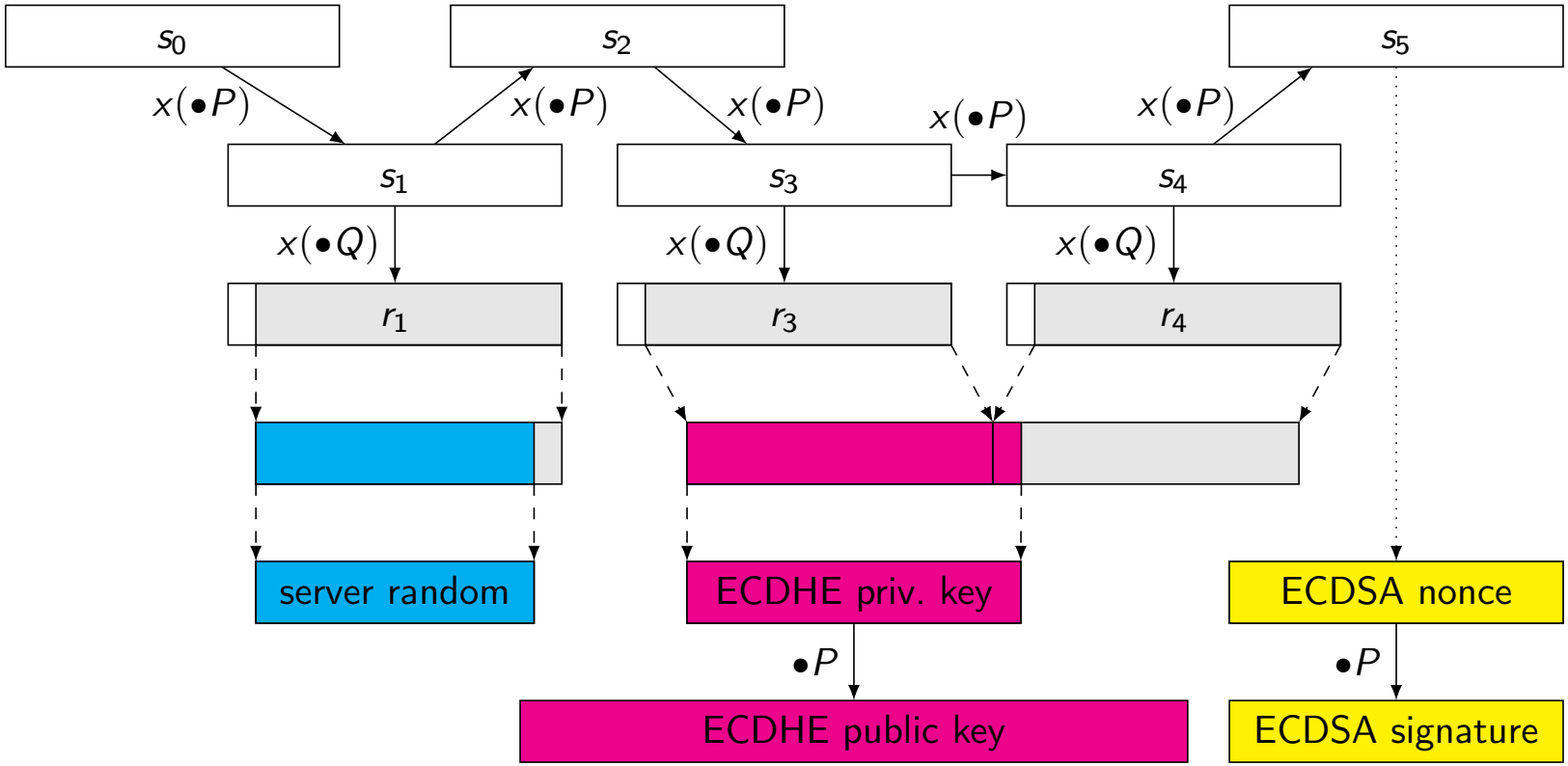
Attack — Example: BSAFE-Java



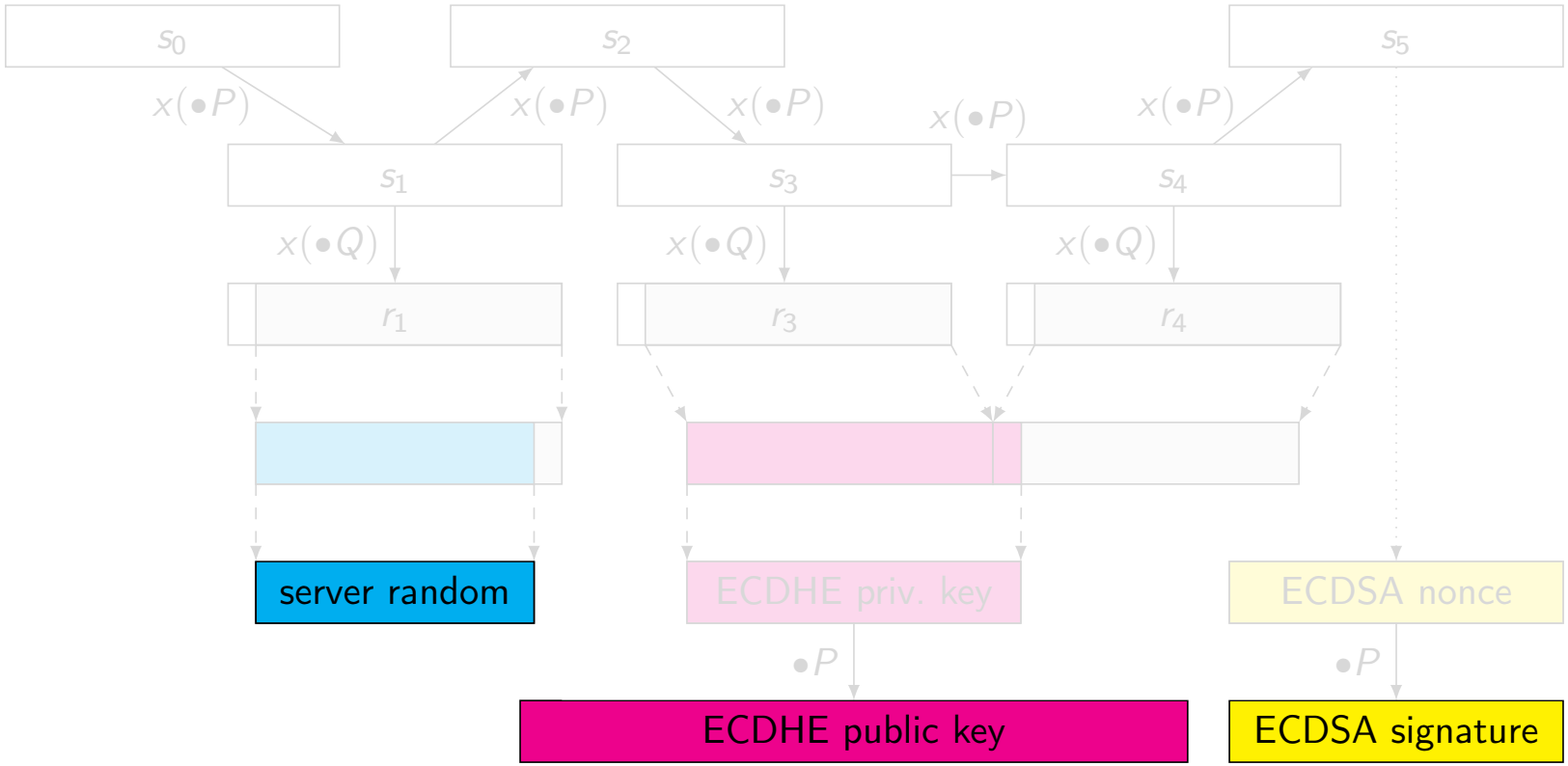
Attack — Example: BSAFE-Java



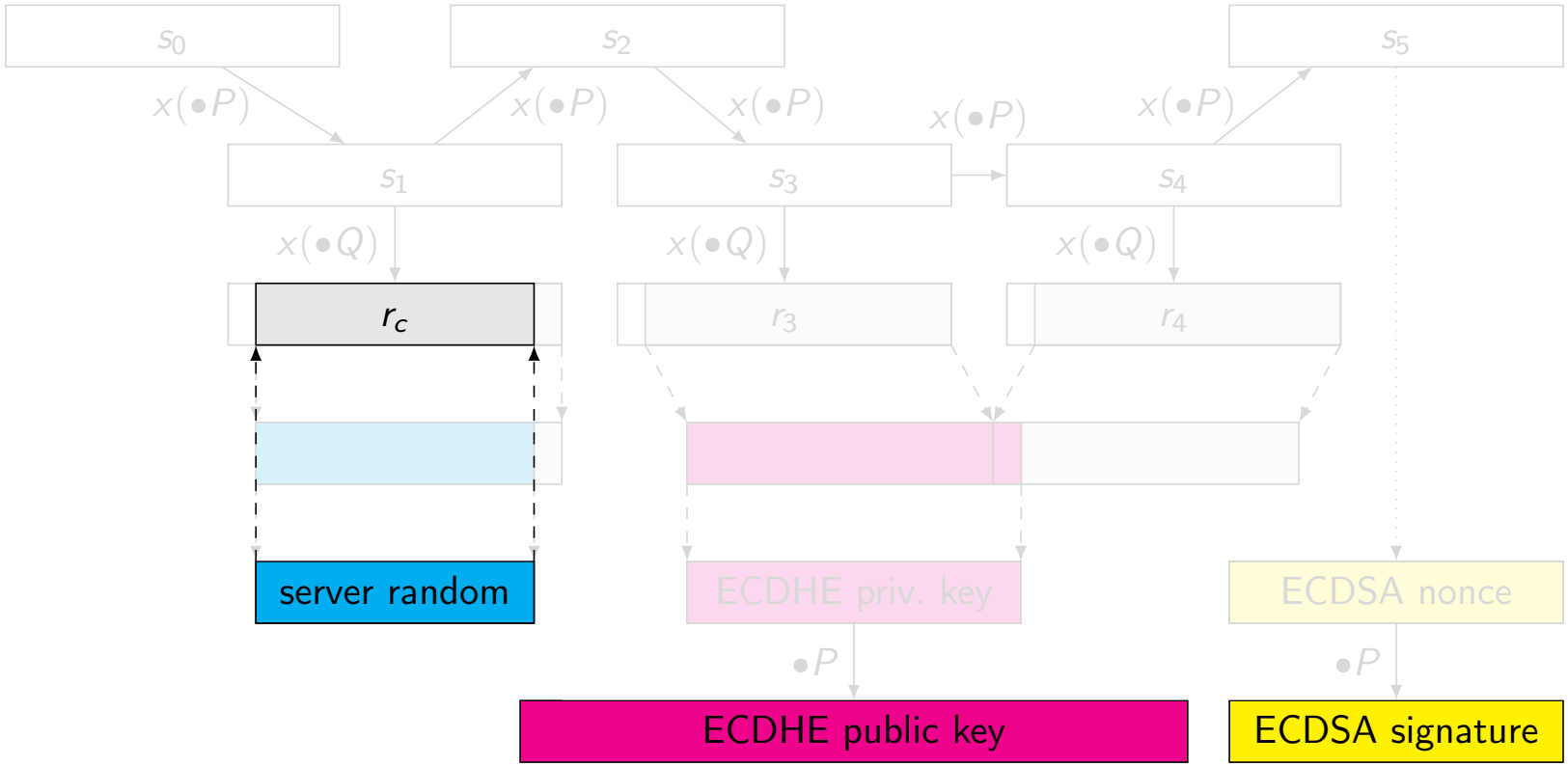
Attack — Example: BSAFE-Java



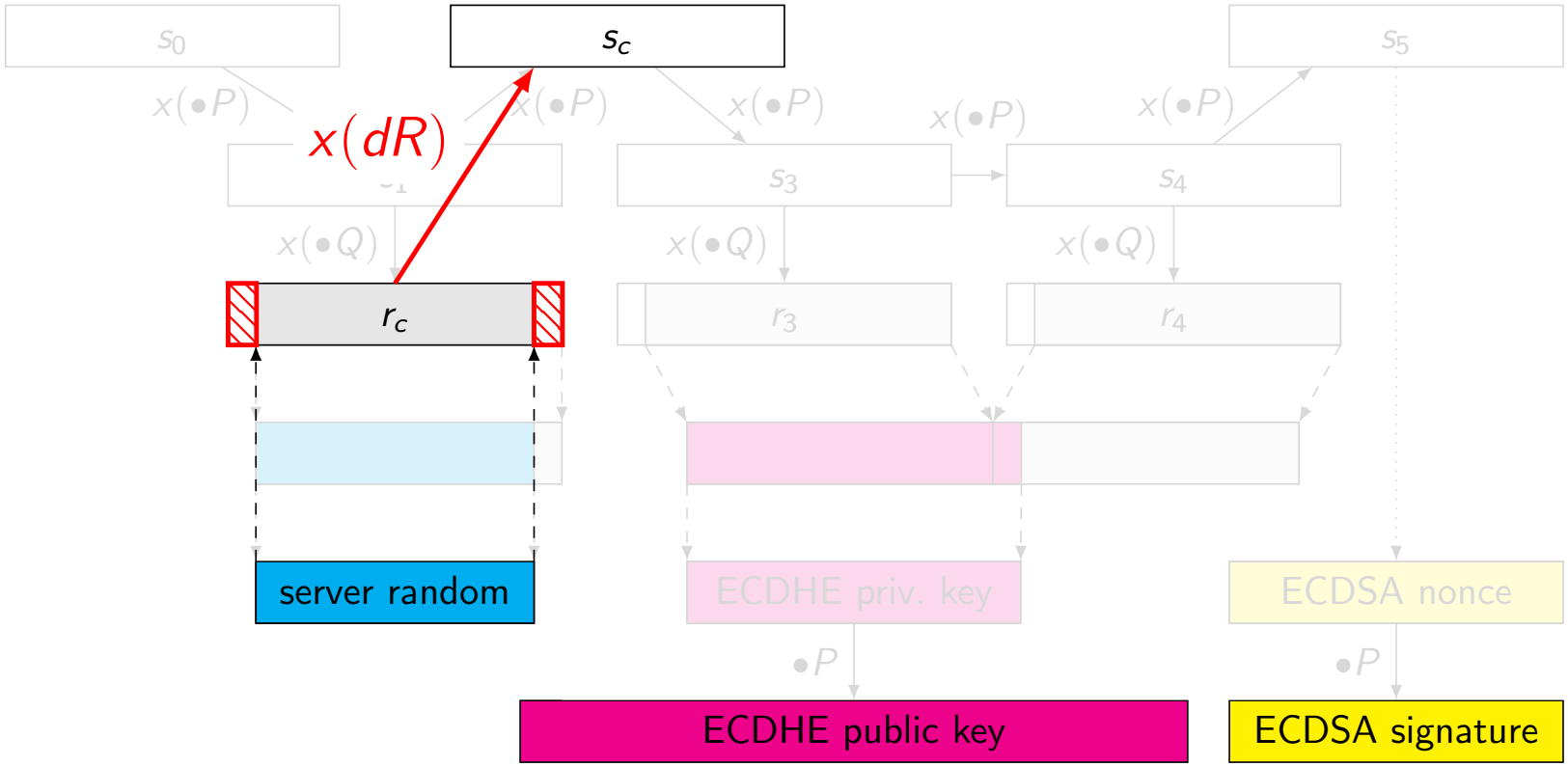
Attack — Example: BSAFE-Java



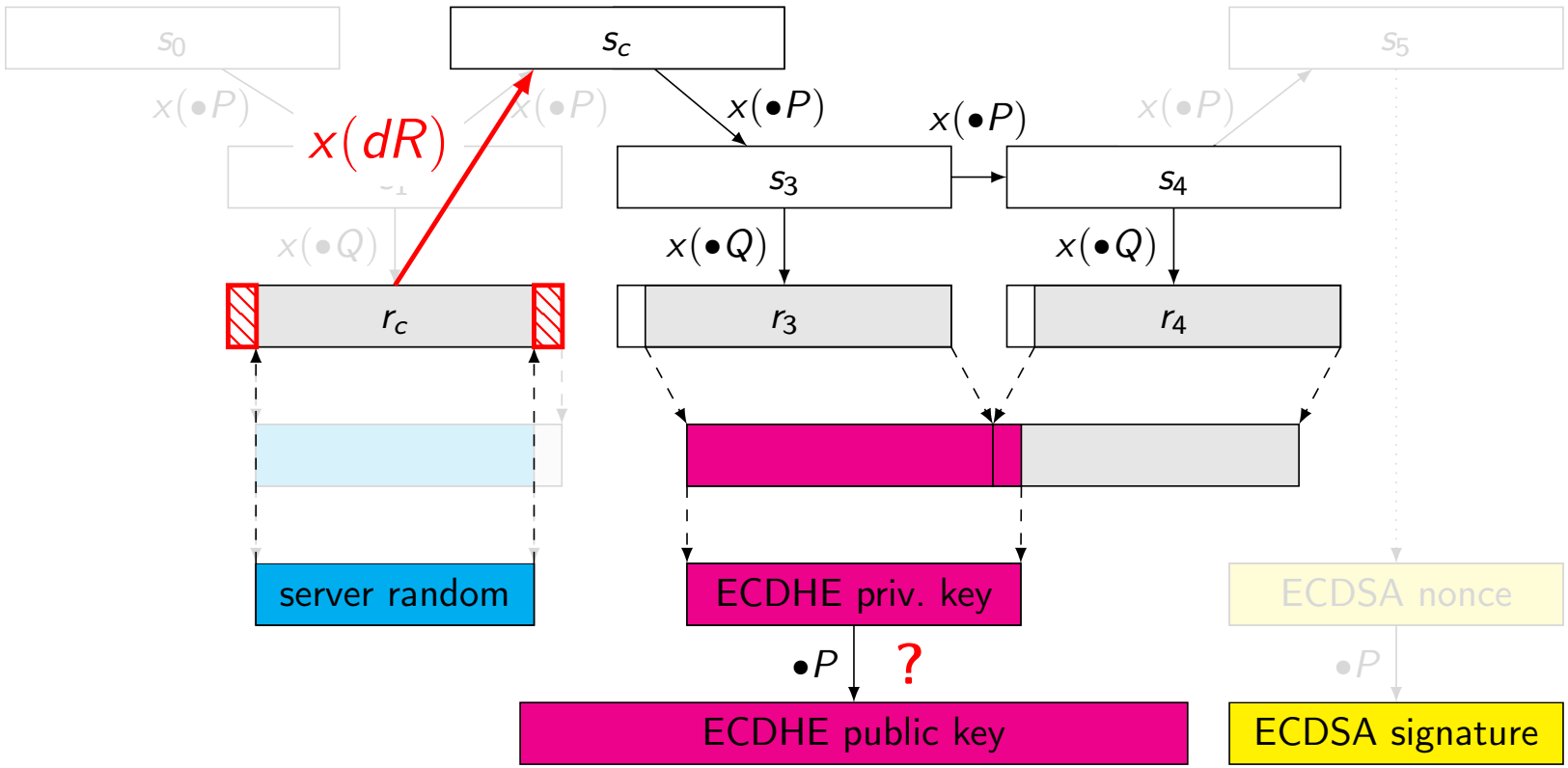
Attack — Example: BSAFE-Java



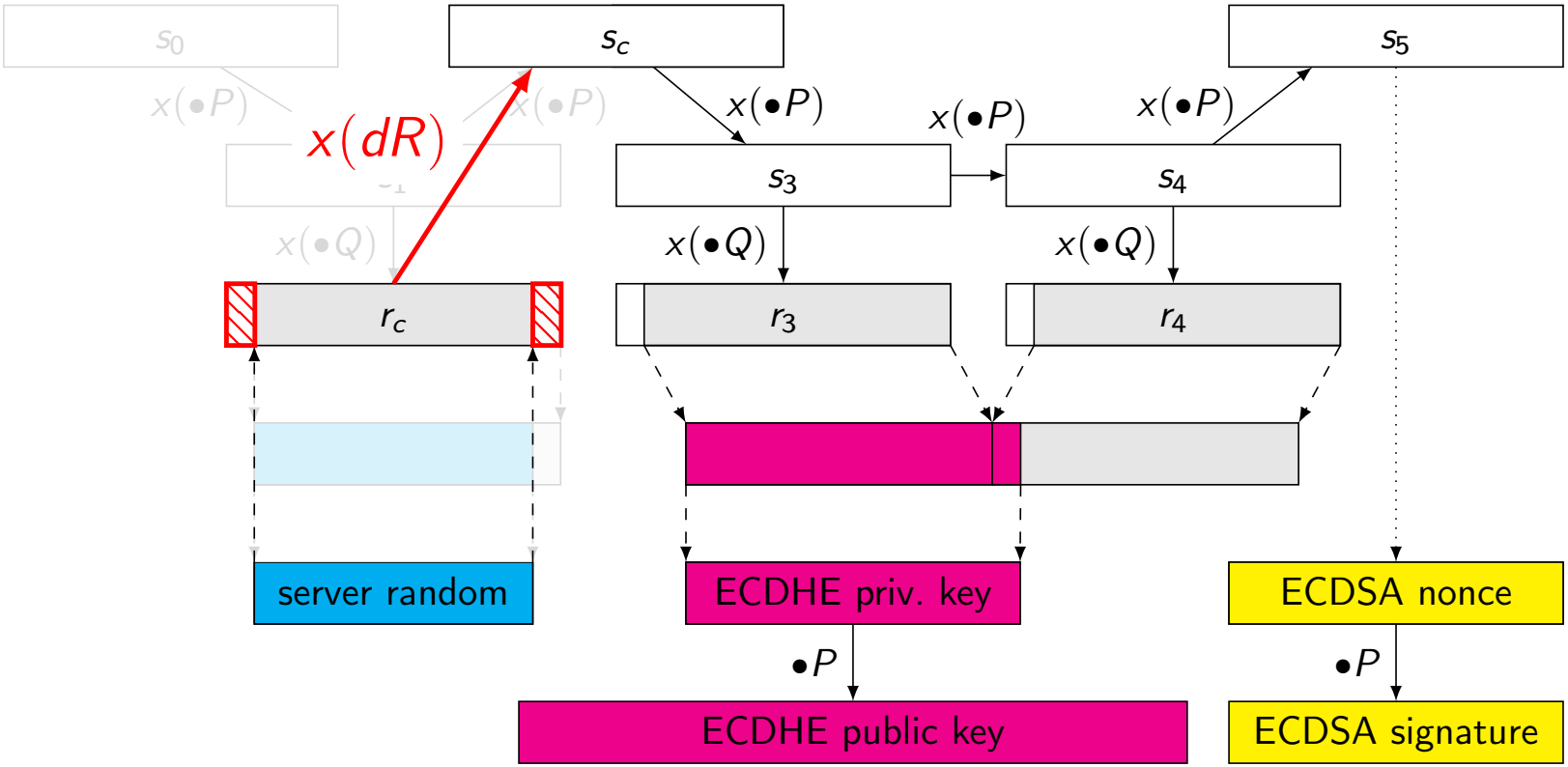
Attack — Example: BSAFE-Java



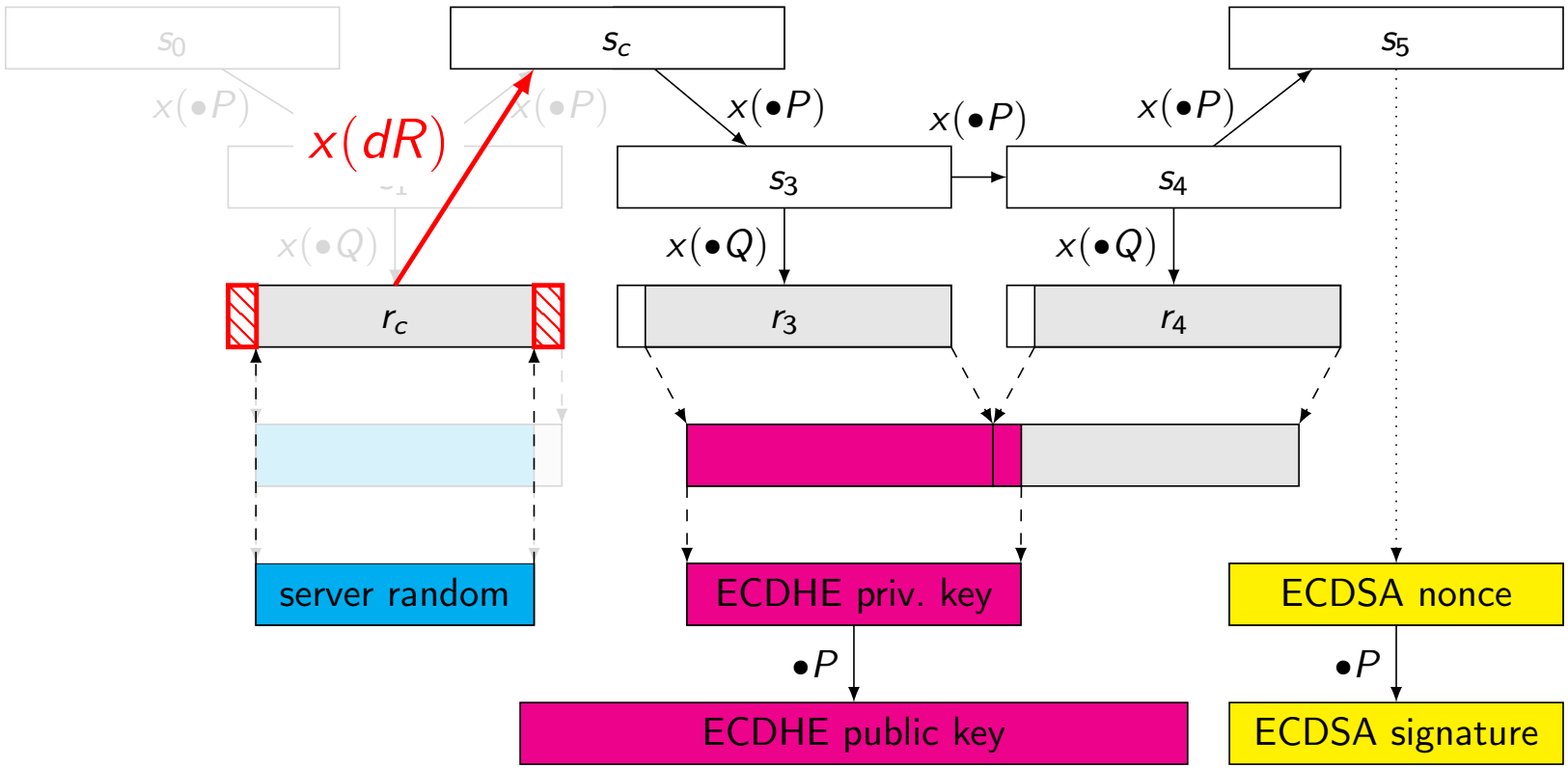
Attack — Example: BSAFE-Java



Attack — Example: BSAFE-Java

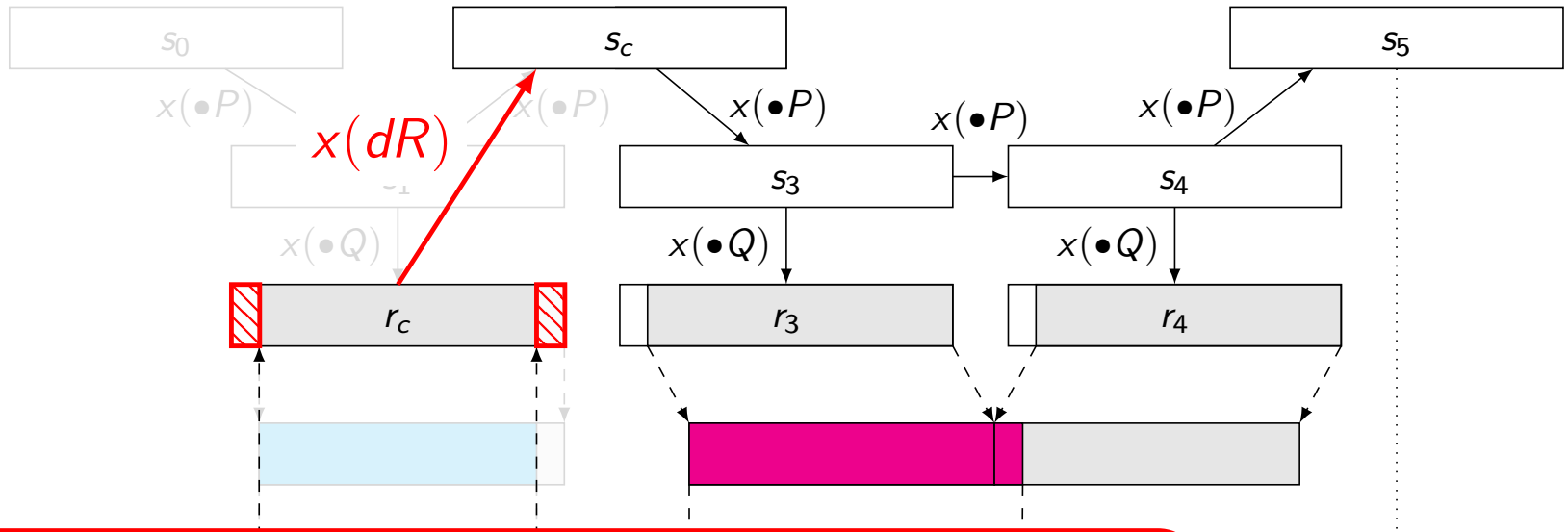


Attack — Example: BSAFE-Java

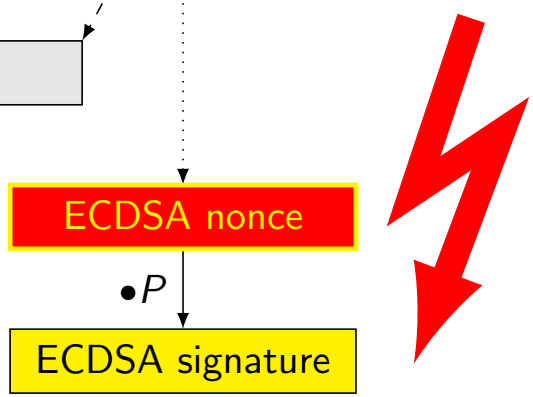


average cost: $2^{31}(C_v + 5C_f)$

Attack — Example: BSAFE-Java

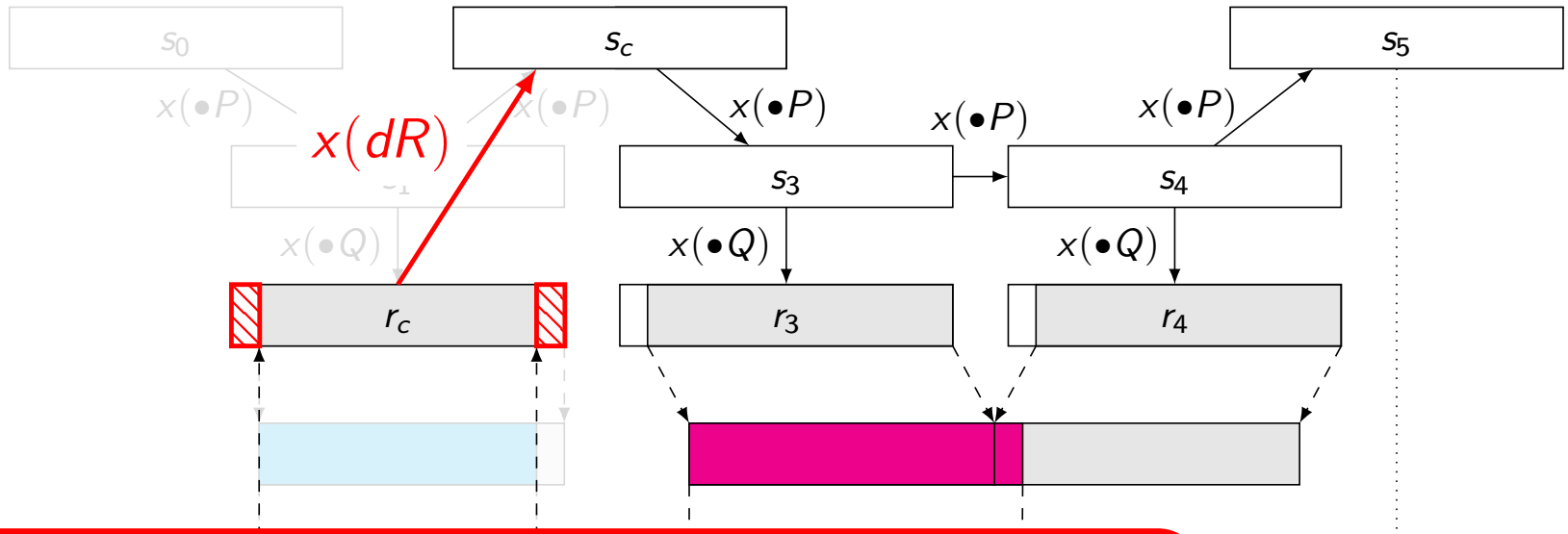


Exposes longterm secret key!
Impersonation attack possible!

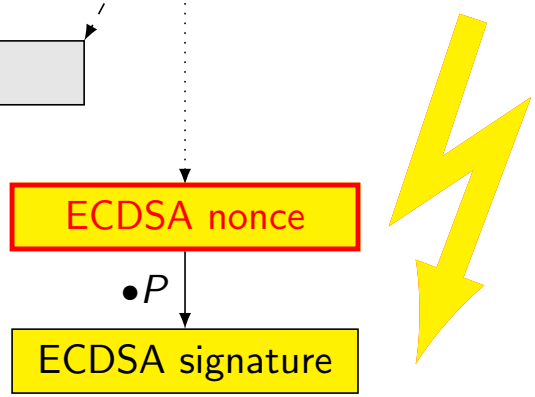


average cost: $2^{31}(C_v + 5C_f)$

Attack — Example: BSAFE-Java



Exposes longterm secret key!
Impersonation attack possible!



average cost: $2^{31}(C_v + 5C_f)$

Attack — Attack Timings

Attack	Intel Xeon CPU		AMD Cluster
	Avg. Time (min)	# for 1s	Tot. Time (min)
BSAFE-C v1.1	0.26	16	0.04
BSAFE-Java v1.1	641	38,500	63.96
SChannel I	619	37,100	62.97
SChannel II	1,760	106,000	182.64
OpenSSL-fixed I	0.04	3	0.02
OpenSSL-fixed II	707	44,200	83.32
OpenSSL-fixed III	$2^k \cdot 707$	$2^k \cdot 44{,}200$	$2^k \cdot 83.32$

Attack — Attack Timings

Attack	Intel Xeon CPU		AMD Cluster
	Avg. Time (min)	# for 1s	Tot. Time (min)
BSAFE-C v1.1	0.26	16	0.04
BSAFE-Java v1.1	641	38,500	63.96
SChannel I	619	37,100	62.97
SChannel II	1,760	106,000	182.64
OpenSSL-fixed I	0.04	3	0.02
OpenSSL-fixed II	707	44,200	83.32
OpenSSL-fixed III	$2^k \cdot 707$	$2^k \cdot 44{,}200$	$2^k \cdot 83.32$

Draft Proposal – Extended Random

Draft for a proposed TLS extension named “Extended Random”:

- allows client to request up to 2^{16} random bytes
- has a weak motivation:
  `The rationale for this as stated by DoD is that the public randomness for each side should be at least twice as long as the security level for cryptographic parity, which makes the 224 bits of randomness provided by the current TLS random values insufficient.`
- was co-authored by an employee of NSA

Draft Proposal – Extended Random

Draft for a proposed TLS extension named “Extended Random”:

- allows client to request up to 2^{16} random bytes
- has a weak motivation:

  `The rationale for this as stated by DoD is that the public randomness for each side should be at least twice as long as the security level for cryptographic parity, which makes the 224 bits of randomness provided by the current TLS random values insufficient.`
- was co-authored by an employee of NSA

Makes Dual EC even more vulnerable!

Summary

Dual EC — a standardized back door:

- (co-)authored by NSA

Summary

Dual EC — a standardized back door:

- (co-)authored by NSA
- may contain a back door (can neither be proven nor disproven)

Summary

Dual EC — a standardized back door:

- (co-)authored by NSA
- may contain a back door (can neither be proven nor disproven)
- allows the back-door owner to compute all future random outputs

Summary

Dual EC — a standardized back door:

- (co-)authored by NSA
- may contain a back door (can neither be proven nor disproven)
- allows the back-door owner to compute all future random outputs
- makes flaw in DSS a back door, allows impersonation

Summary

Dual EC — a standardized back door:

- (co-)authored by NSA
- may contain a back door (can neither be proven nor disproven)
- allows the back-door owner to compute all future random outputs
- makes flaw in DSS a back door, allows impersonation
- proven to be practical in various TLS libraries

Summary

Dual EC — a standardized back door:

- (co-)authored by NSA
- may contain a back door (can neither be proven nor disproven)
- allows the back-door owner to compute all future random outputs
- makes flaw in DSS a back door, allows impersonation
- proven to be practical in various TLS libraries
- was default RNG in RSA's BSAFE library

Summary

Dual EC — a standardized back door:

- (co-)authored by NSA
- may contain a back door (can neither be proven nor disproven)
- allows the back-door owner to compute all future random outputs
- makes flaw in DSS a back door, allows impersonation
- proven to be practical in various TLS libraries
- was default RNG in RSA's BSAFE library
- back door becomes even stronger with proposed Extended Random

Summary

Dual EC — a standardized back door:

- (co-)authored by NSA
- may contain a back door (can neither be proven nor disproven)
- allows the back-door owner to compute all future random outputs
- makes flaw in DSS a back door, allows impersonation
- proven to be practical in various TLS libraries
- was default RNG in RSA's BSAFE library
- back door becomes even stronger with proposed Extended Random

How to fix it?

Summary

Dual EC — a standardized back door:

- (co-)authored by NSA
- may contain a back door (can neither be proven nor disproven)
- allows the back-door owner to compute all future random outputs
- makes flaw in DSS a back door, allows impersonation
- proven to be practical in various TLS libraries
- was default RNG in RSA's BSAFE library
- back door becomes even stronger with proposed Extended Random

Don't use Dual EC!

Summary

Additional information:

https://projectbullrun.org/dual-ec/