The Advanced Encryption Standard (Rijndael, AES)

Nicolas T. Courtois
- University College of London

1. Block Ciphers and AES

*Block Ciphers

Make sure you obtain a permutation:

Iterate many times a weak permutation:

- Feistel structure (DES)
  OWF-->OWP
- Substitution – Permutation Networks.
  "Small Permutation Networks…" --> Big Perm.
- AES is not an SPN in the proper (initial) sense, - permutation of wires - but everybody says it is.

AES

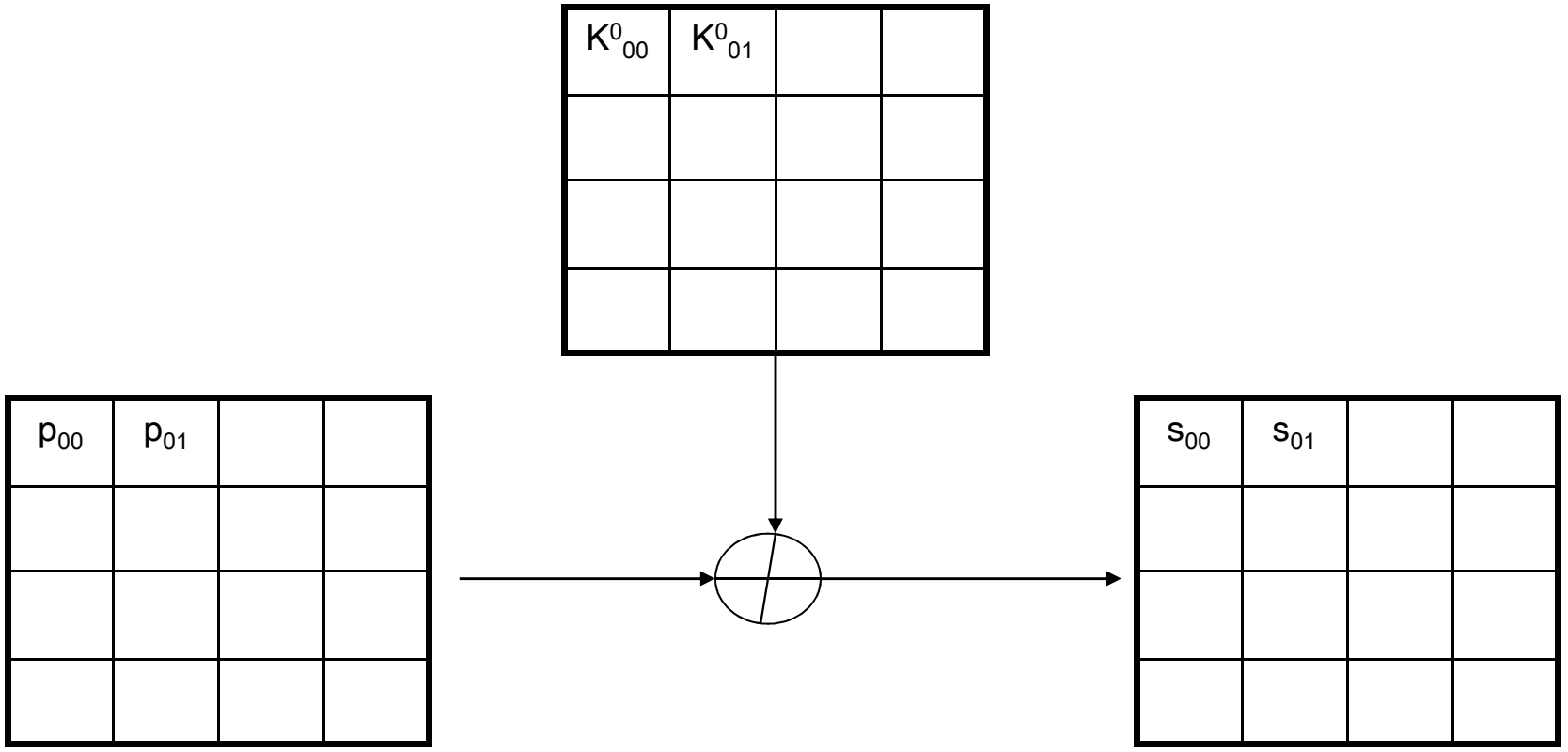
Advanced Encryption Standard (US).

Key sizes 128, 192 and 256 bits.

- In 2000 NIST selected Rijndael as the AES.

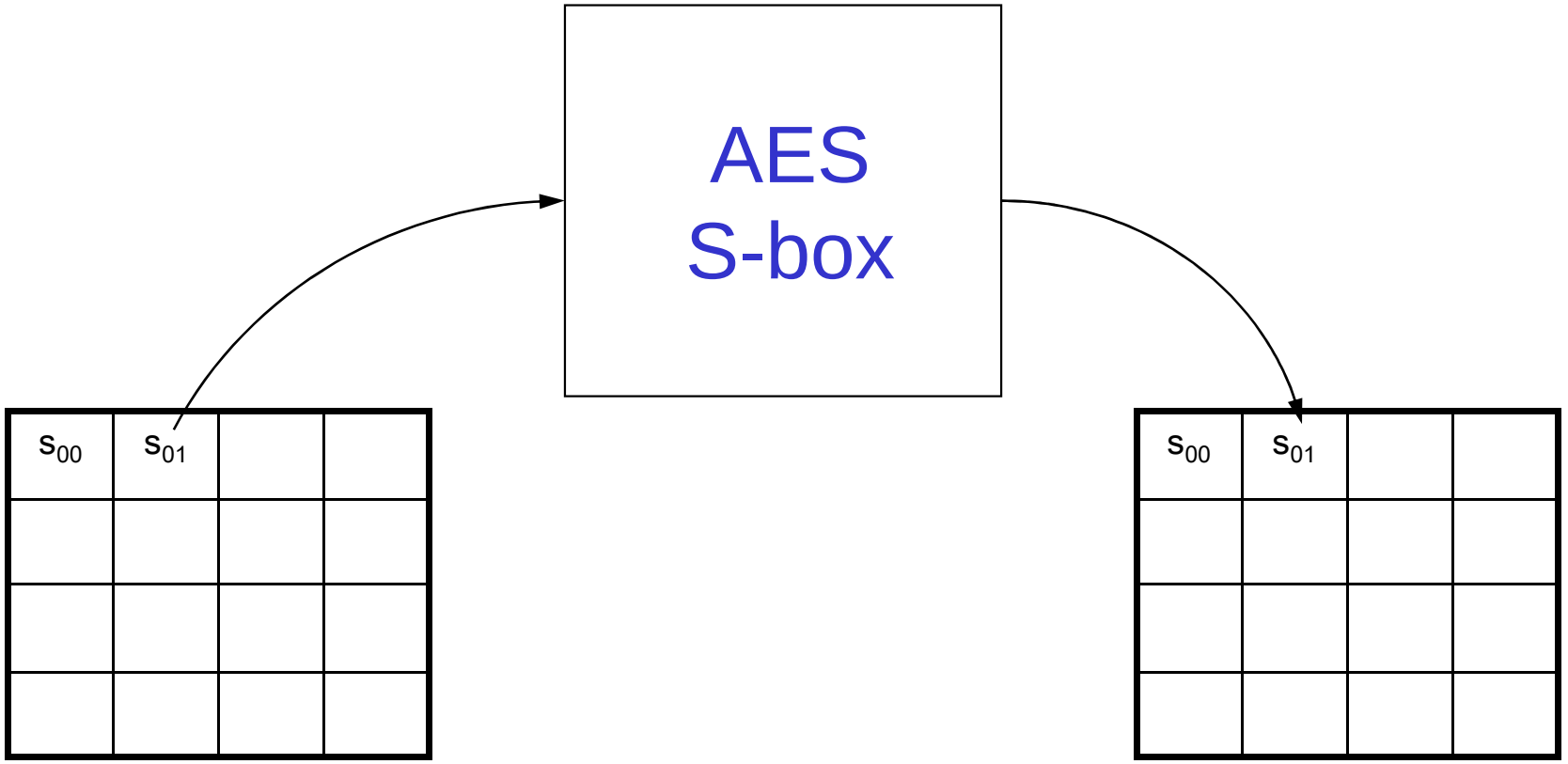
*AES 128 – 10 rounds

A round begins with a XOR with the key number i-1



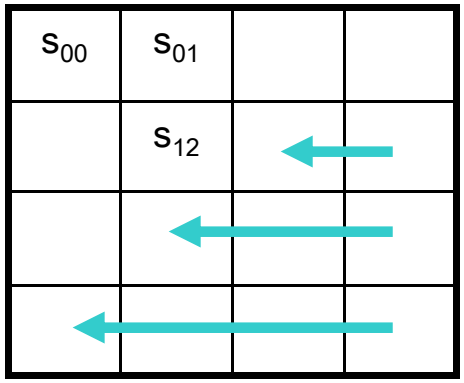
*AES 128 – ByteSub

..continues with a table look-up…



*AES 128 – ShiftRow

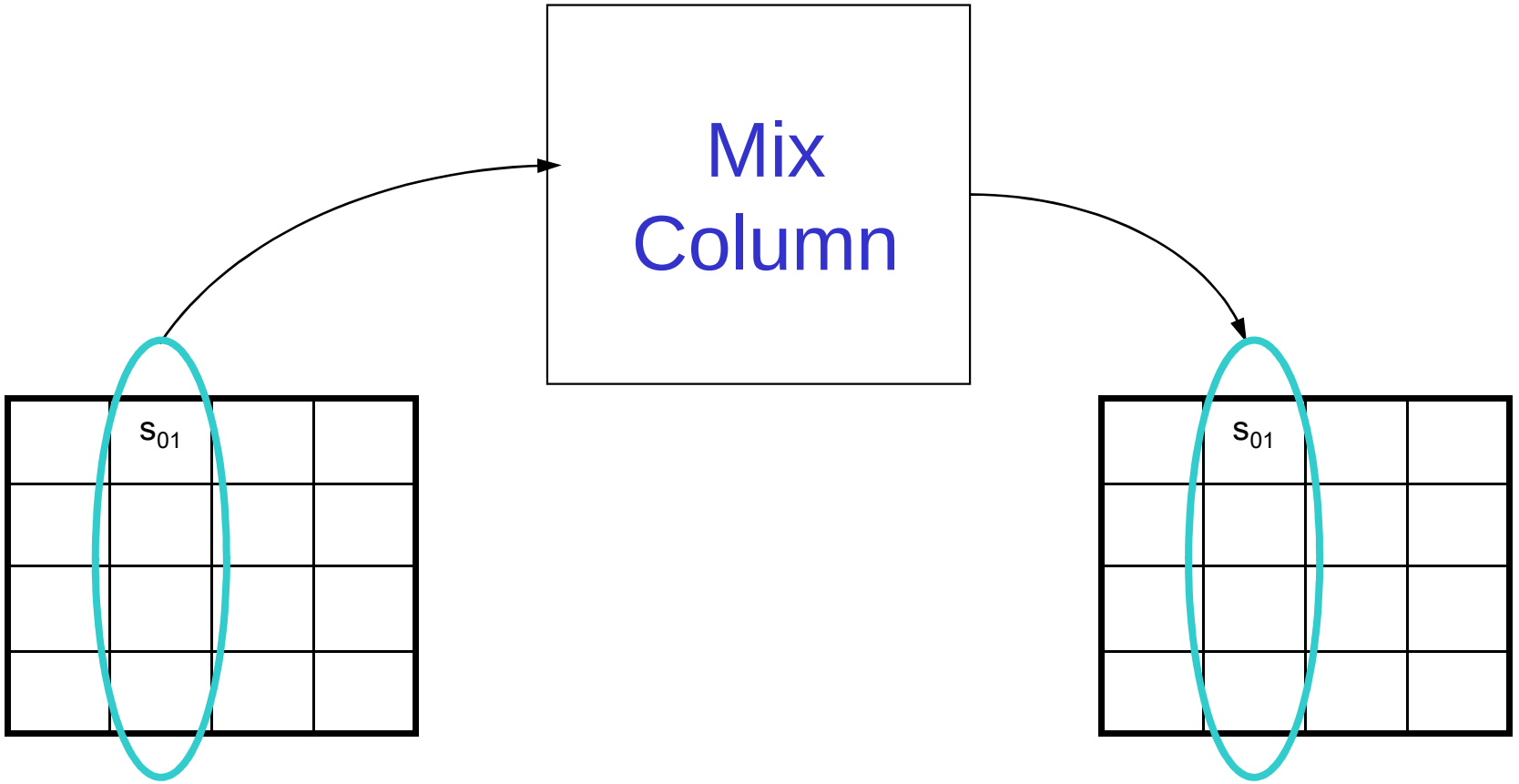
…continues with a permutation…



s_{00}	s_{01}		
s_{12}			

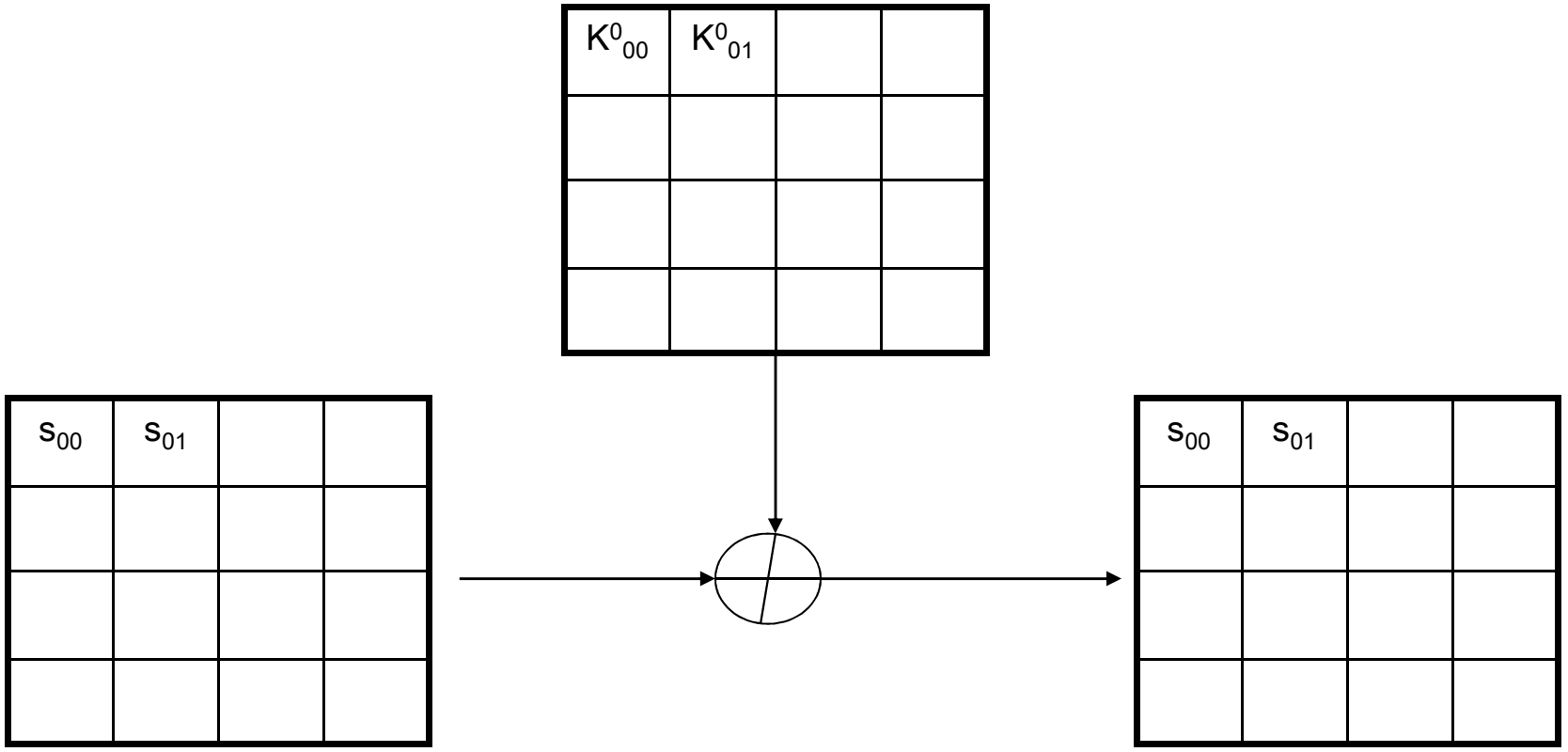
*AES 128 – MixColumn

…continues with a Matrix applied to each column…



*AES – 10 rounds

..and then comes the XOR with the key number i..



Block Ciphers and Algebraic Attacks

What Happened to AES ?

Bad luck: At the time of design: very elegant construction resistant to all known attacks.

Authors tried to make it too good…

Choose the best S-box that could find.

- based on inversion in GF(256)
- better than random permutation box.

Rather strong, maybe too strong to protect 10 rounds of AES against differential, linear and other attacks…

Yet special means dangerous…
In fact AES is a very bad cipher considering new kind of (algebraic) attacks…

Schneier [Applied Cryptography book]

[…] Any algorithm that gets its security from the composition of polynomials over a finite field should be looked upon with scepticism, if not outright suspicion. […]

Written before AES ever existed…

Actually any cipher can be seen in this way…

How do We Attack AES ?

– Very ambitious…

- AES pushes the classical cipher design principles to their limits, optimality.
  - high non-linearity
  - WTS= Wide Trail Strategy:
    - INCREDIBLY strong,
    - first proposed in Vincent Rijmen thesis 1997.
- Explore these limits. Look for pitfalls !

Wide Trail Strategy (WTS):

Assures very good diffusion, proposed by the designers of AES.

- **The "approximation" attacks:**
  - Deadly. Forces to **approximate** great many S-boxes at the same time. AES is very secure against LC/DC.
  - WTS probably kills all these insecure ciphers that are very special…
- **The "exact algebraic" approach:**
  - Combine relations true with probability 1.
  - The wide trail strategy still plays a huge role in practice/theory.