E2 - A Candidate Cipher for AES

Masayuki Kanda, Shiho Moriai, Kazumaro Aoki,
Hiroki Ueda, Miyako Ohkubo, Youichi Takashima,
Kazuo Ohta, Tsutomu Matsumoto*

e2@isl.ntt.co.jp

http://info.isl.ntt.co.jp/e2/

Nippon Telegraph and Telephone Corporation (NTT)

*Yokohama National University

Outline

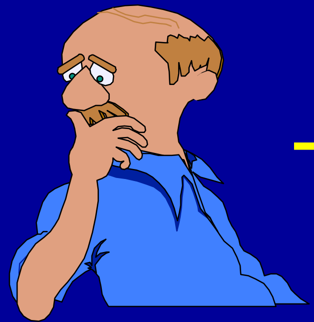
- Overview
- Design
- Security
- Performance
- Conclusion

E2

Design Goals

- A 128-bit symmetric block cipher
- Key length of 128, 192, and 256 bits
- Security : secure against all known attacks and more
- Efficiency : faster than DES
- Flexibility : efficient implementations on various platforms

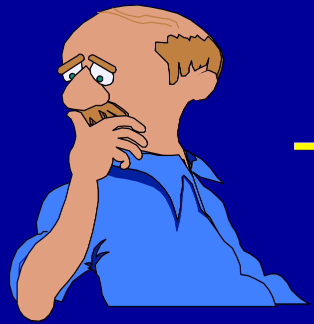
Security of E2 (1)



There are many attacks….

Security of E2   (1)

Brute Force
Attacks

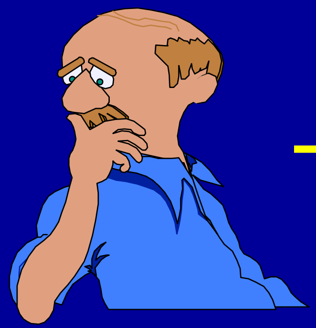


There are many attacks….

Security of E2 (1)

Brute Force Attacks

Differential Cryptanalysis



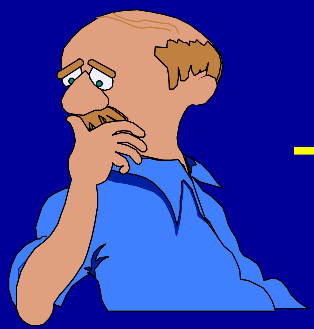
There are many attacks….

Security of E2 (1)

Brute Force Attacks

Differential Cryptanalysis

Linear Cryptanalysis



There are many attacks….

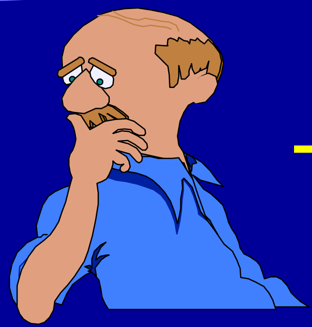
Security of E2 (1)

Brute Force Attacks

Differential Cryptanalysis

Linear Cryptanalysis

Higher Order Differential Attack



There are many attacks….

Security of E2 (1)

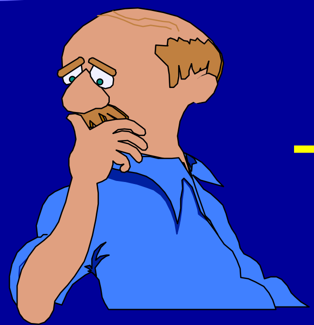
Brute Force Attacks

Differential Cryptanalysis

Linear Cryptanalysis

Higher Order Differential Attack

Interpolation Attack



There are many attacks….

Security of E2 (1)

Brute Force Attacks

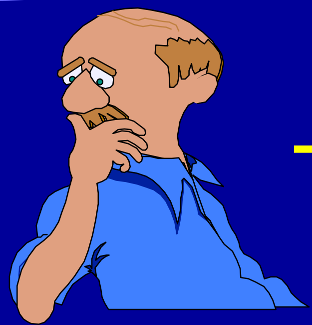
Differential Cryptanalysis

Linear Cryptanalysis

Higher Order Differential Attack

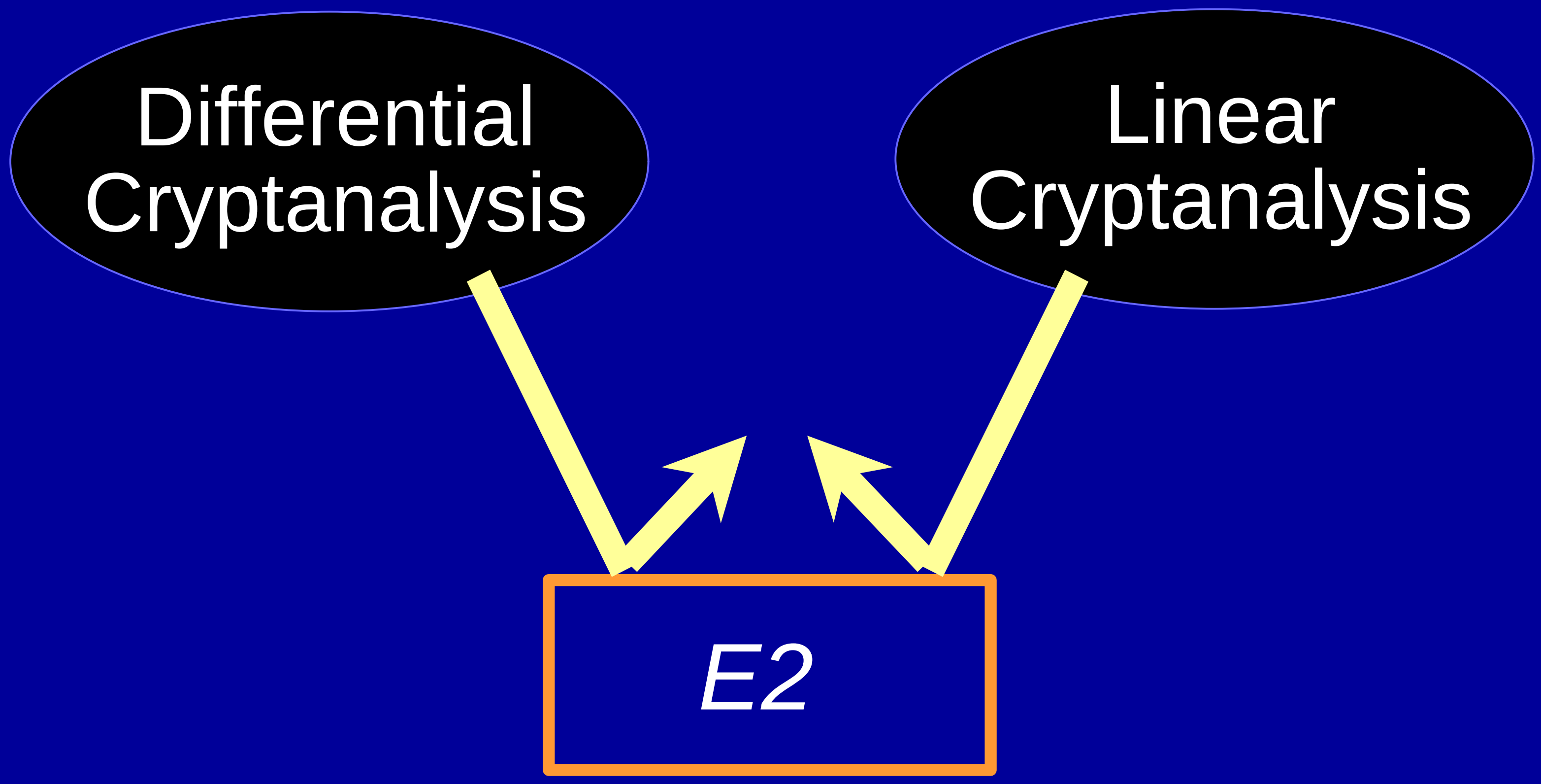
Interpolation Attack

Partitioning Cryptanalysis



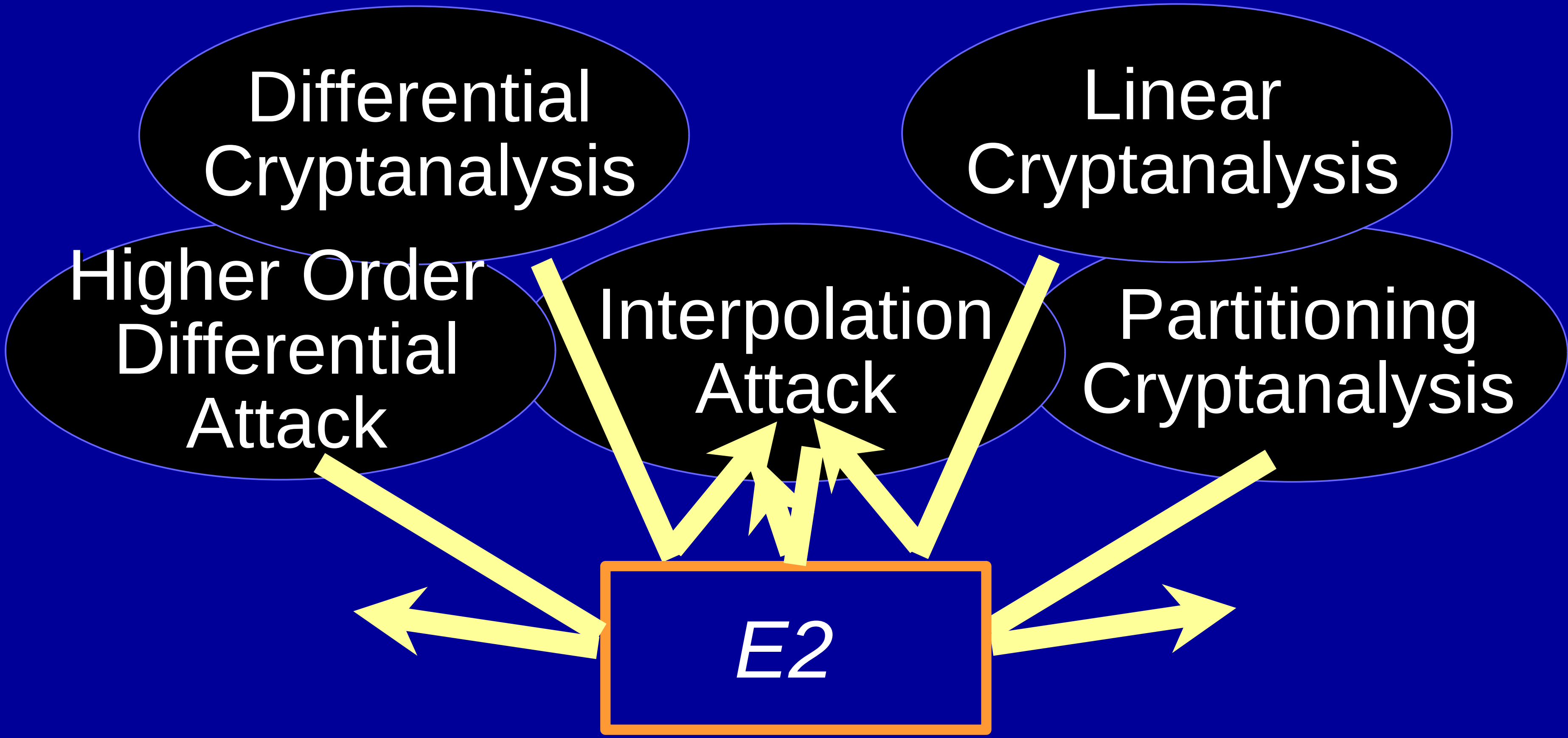
There are many attacks….

Security of E2 (2)



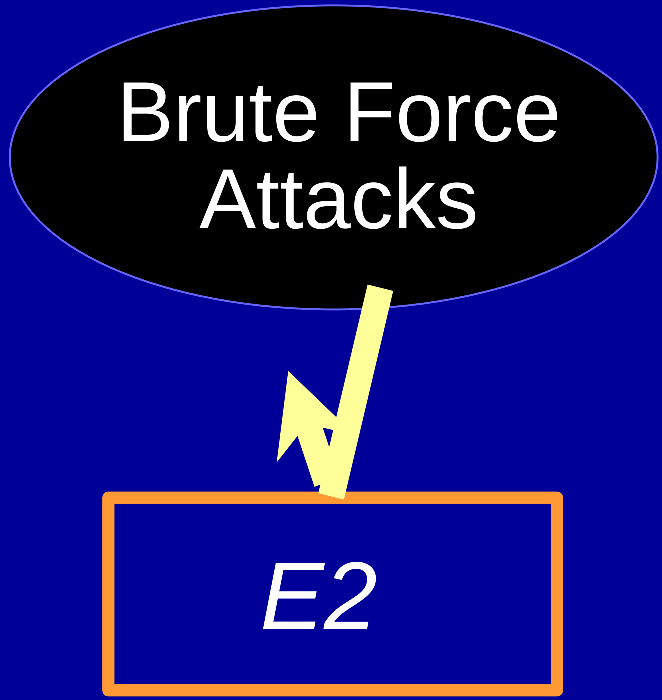
E2 is proven to have sufficient security

Security of E2 (3)



S-box is designed
to have no vulnerabilities

Security of E2 (4)



E2 supports
128-bit block size and
128,192, 256-bit key sizes

Design Goals (cont.)

- A 128-bit symmetric block cipher
- Key length of 128, 192, and 256 bits
- Security : secure against all known attacks and more
- Efficiency : faster than DES
- Flexibility : efficient implementations on various platforms

Efficiency and Flexibility of E2

32-bit CPU

200MHz **Intel Pentium Pro**

ANSI C (Borland C++ 5.02)	Assembly
711 clocks/block	420 clocks/block
36.0 Mbits/sec	61.0 Mbits/sec

64-bit CPU

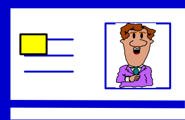
600MHz **DEC 21164A**

Assembly

600 clocks/block
128 Mbits/sec

8-bit CPU

5MHz **Hitachi H8/300**

Assembly 

6,374 clocks/block
100.5 k bits/sec

Efficiency and Flexibility of E2

32-bit CPU

200MHz **Intel Pentium Pro**

ANSI C
(Borland C++ 5.02)

711 clocks/block
36.0 Mbits/sec

Mbits/sec

cf. DES (RSAREF, Borland C++ 5.0)
10.6 Mbits/sec

64-bit CPU

600MHz **DEC 21164A**

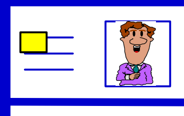
Assembly

600 clocks/block
128 Mbits/sec

8-bit CPU

5MHz **Hitachi H8/300**

Assembly



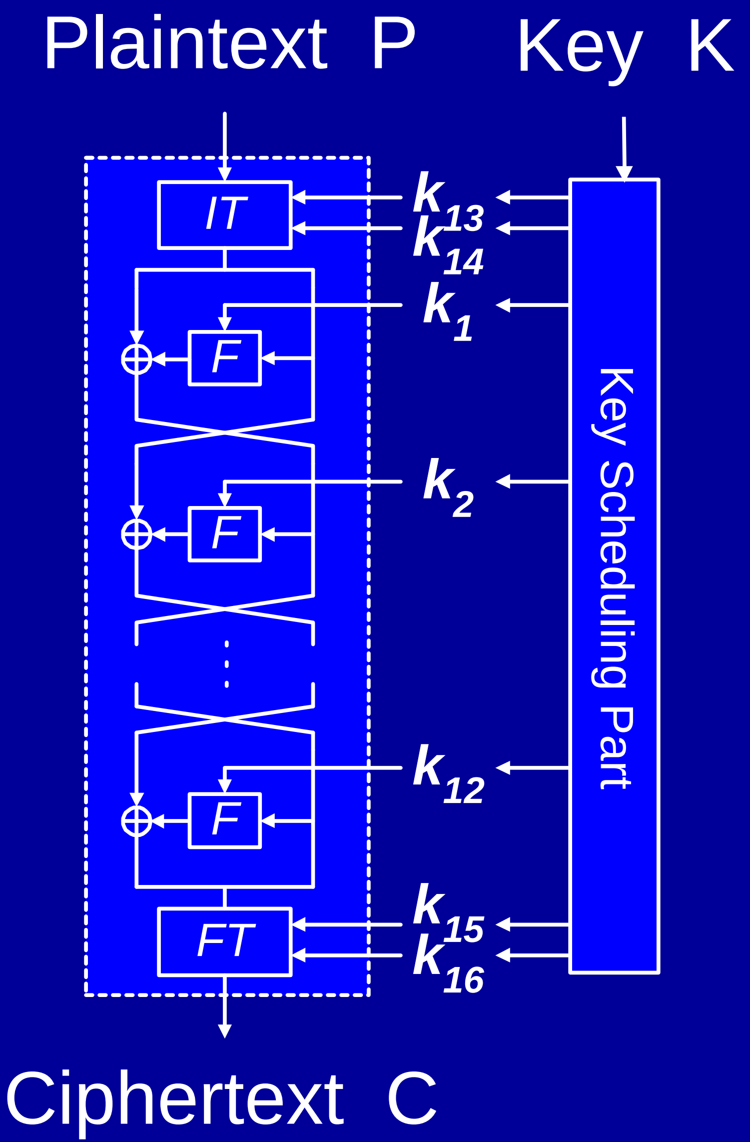
6,374 clocks/block
100.5 k bits/sec

Outline

- Overview
- <u>Design</u>
- Security
- Performance
- Conclusion

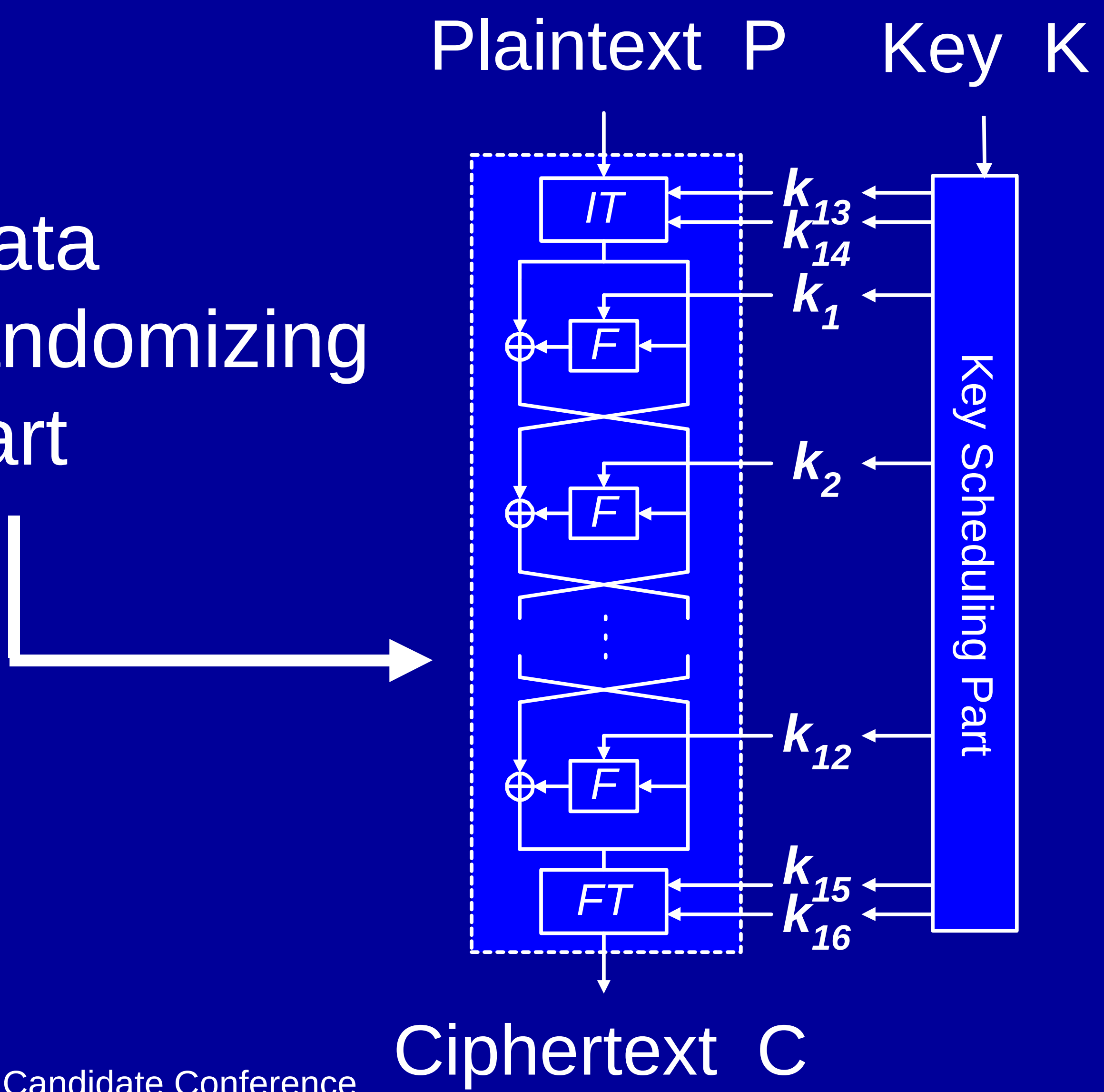
E2

High-level Structure of E2

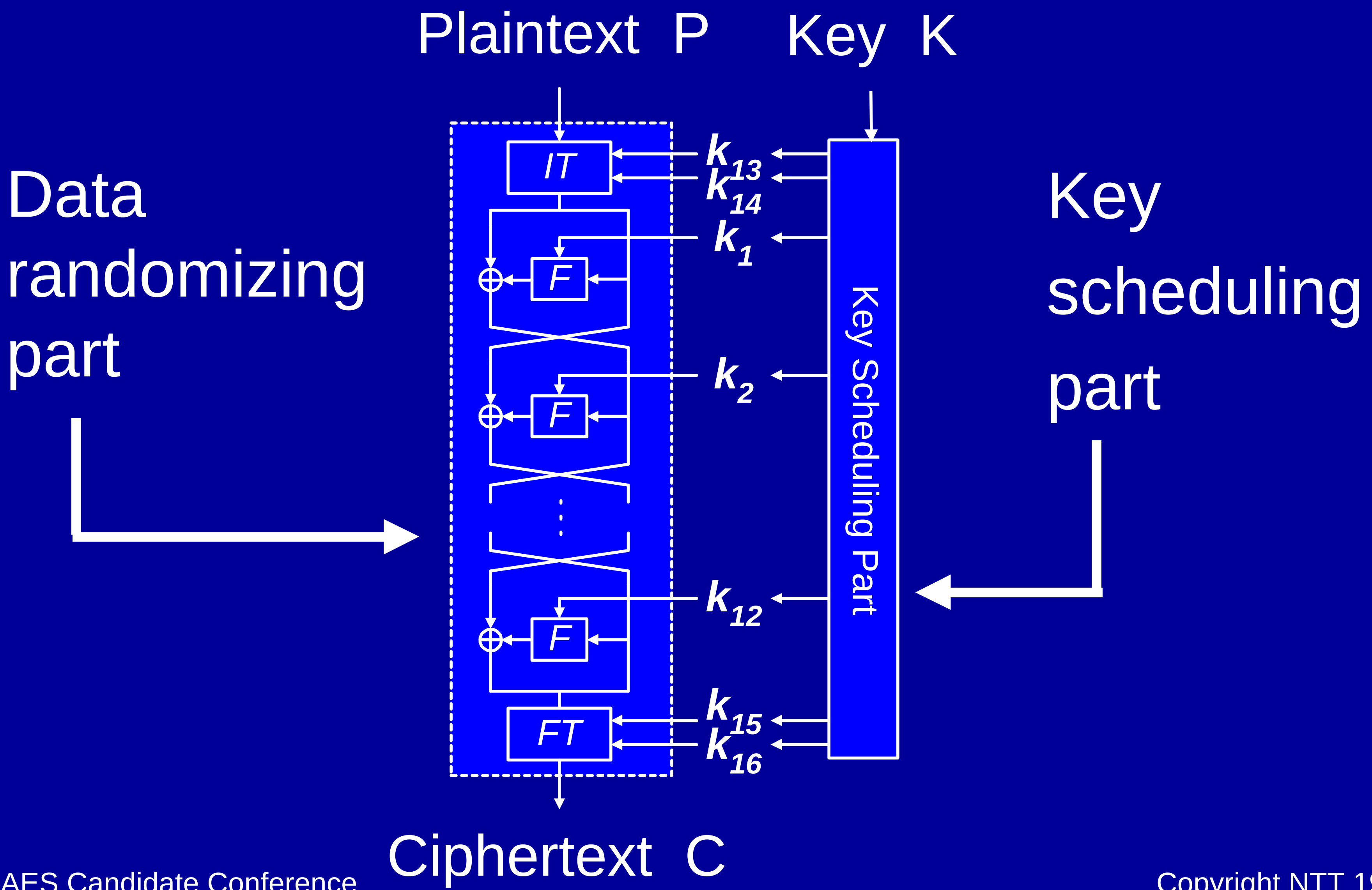


High-level Structure of E2

Data randomizing part

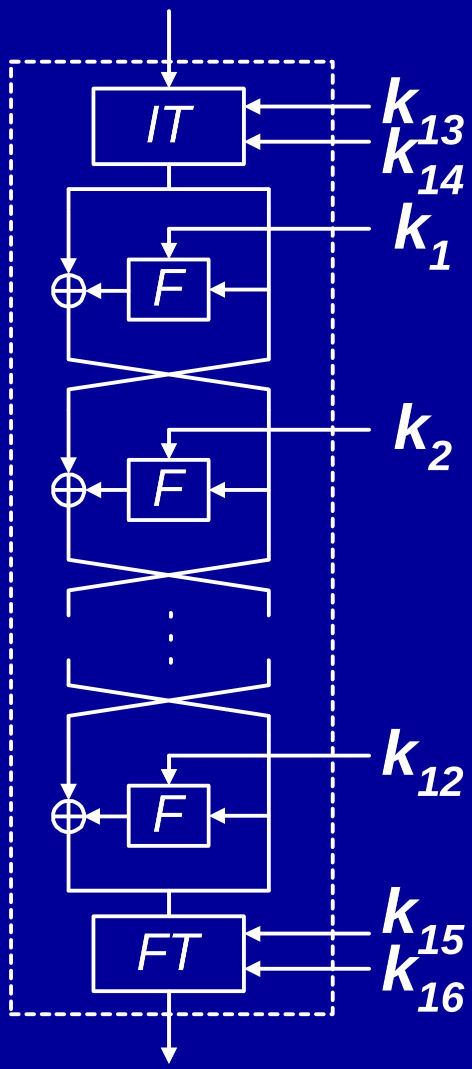


High-level Structure of E2



Data Randomizing Part Framework

- *IT*-Function
  (Initial Transformation)
- Feistel structure
- *FT*-Function
  (Final Transformation)



Design Rationale of Framework

- Feistel structure
  - Widely known and thought to offer long-term security
  - Symmetric encryption and decryption
  - Evaluation of security against DC and LC has been well studied
- *IT*-Function and *FT*-Function
  - Offer a proactive design and hinder later attacks

Design Rationale of Framework

- Feistel structure
  - Widely known and thought to offer long-term security
  - Symmetric encryption and decryption
  - Evaluation of security against DC and LC has been well studied
- *IT*-Function and *FT*-Function
  - Offer a proactive design and hinder later attacks

Design Rationale of F-Function (1)

- Structures for which security evaluation against DC and LC is easy
  - 1-round SPN structure (e.g., DES)
  - Recursive structure (e.g., MISTY)
  - 2-round SPN structure
- Comparing the speed at the same level of security, we decided to adopt 2-round SPN structure

Design Rationale of F-Function (1)

- Structures for which security evaluation against DC and LC is easy
  - 1-round SPN structure (e.g., DES)
  - Recursive structure (e.g., MISTY)
  - 2-round SPN structure
- Comparing the speed at the same level of security, we decided to adopt 2-round SPN structure

Design Rationale of F-Function (1)

- Structures for which security evaluation against DC and LC is easy
  - 1-round SPN structure (e.g., DES)
  - Recursive structure (e.g., MISTY)
  - 2-round SPN structure
- Comparing the speed at the same level of security, we decided to adopt 2-round SPN structure

→ Evaluated using practical measure

Practical Measure for Feistel Cipher

- General case [Knudsen (FSE'93)]
  - Number of rounds: $R = 2r,\ 2r + 1$
  - Evaluation: $UDCP^{(R)} = p^{r}$, $\quad ULCP^{(R)} = q^{r}$
- Bijective case [Kanda et al. (SAC'98)]
  - Number of rounds: $R = 3r,\ 3r + 1,\ 3r + 2$
  - Evaluation: $UDCP^{(R)} = p^{2r}$, $\quad ULCP^{(R)} = q^{2r}$

    $(R = 3r,\ 3r + 1)$

    $UDCP^{(R)} = p^{2r+1}$, $\quad ULCP^{(R)} = q^{2r+1}$

    $(R = 3r + 2)$

Note: p, q : Maximum differential and linear prob. of round function

Practical Measure for Feistel Cipher

- General case [Knudsen (FSE'93)]
  - Number of rounds: $R = 2r, 2r$
  - Evaluation: $UDCP^{(R)} = p^{r}$,

When R = 6

UDCP = p³ [General]

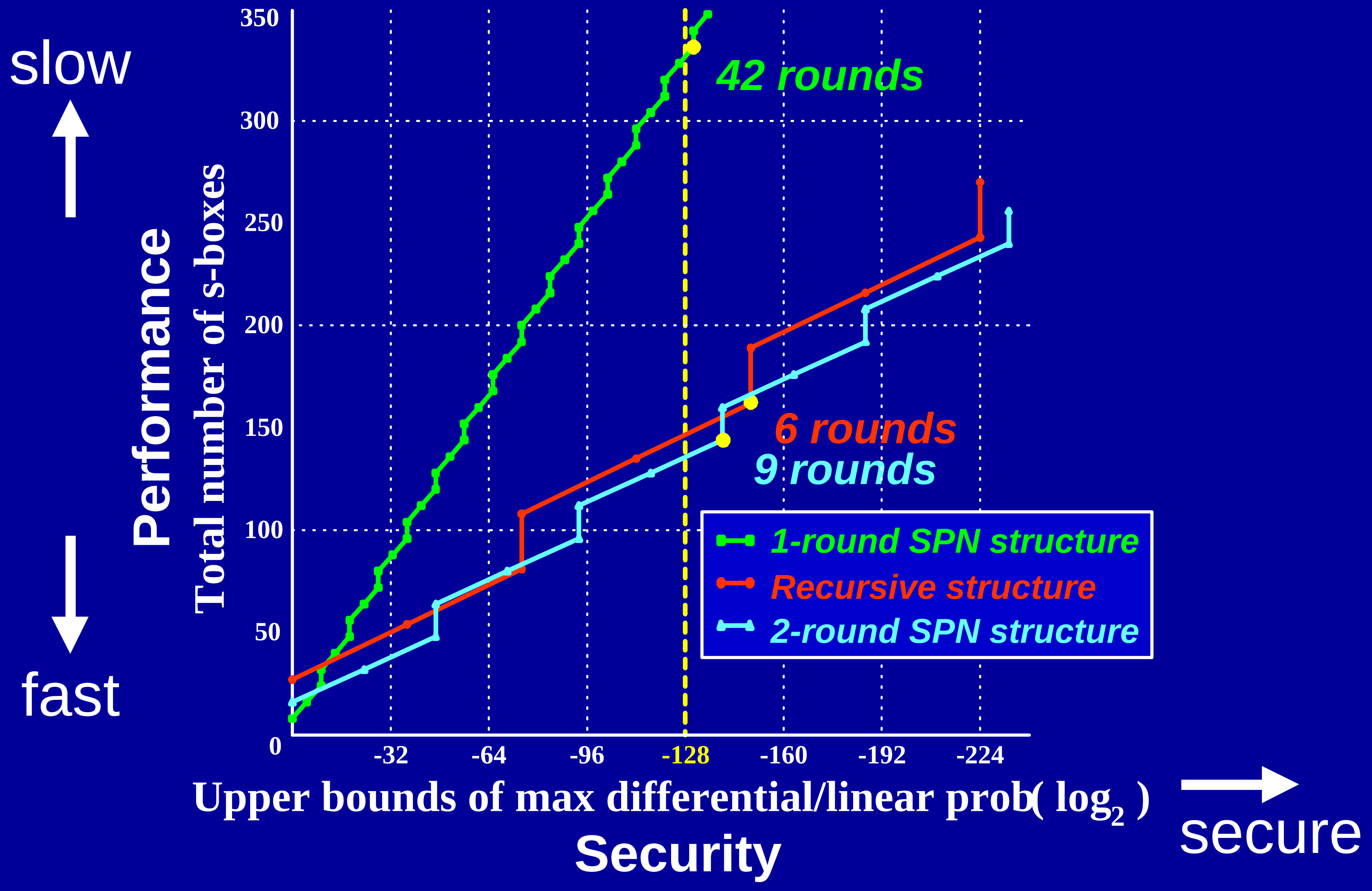
UDCP = p⁴ [Bijective]

- Bijective case [Kanda et a
  - Number of rounds: $R = 3r, 3r + 1, 3r + 2$
  - Evaluation: $UDCP^{(R)} = p^{2r}$, $ULCP^{(R)} = q^{2r}$ $(R = 3r, 3r + 1)$

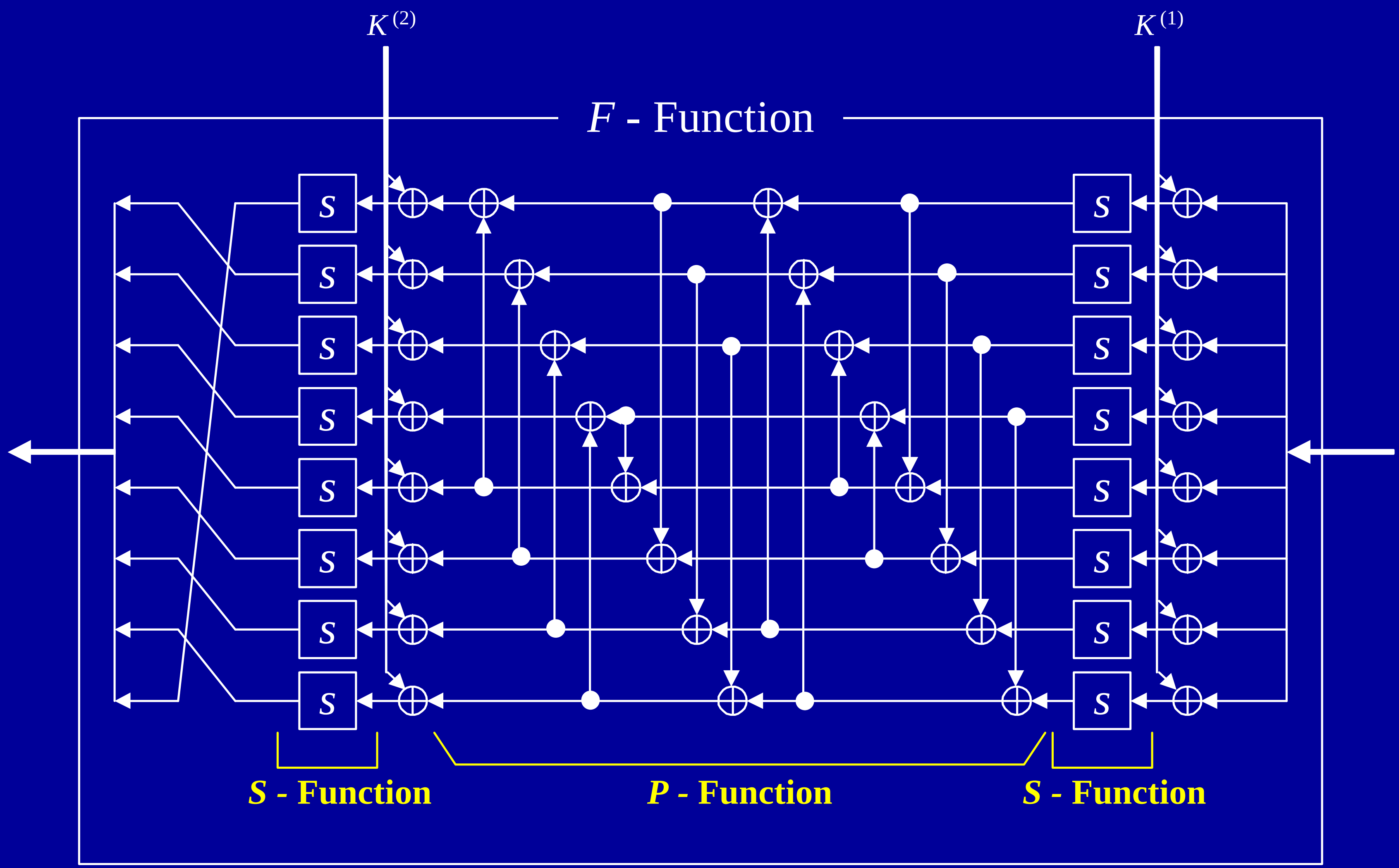
    $UDCP^{(R)} = p^{2r+1}$, $ULCP^{(R)} = q^{2r+1}$ $(R = 3r + 2)$

Note: p, q : Maximum differential and linear prob. of round function

Design Rationale of F-Function (2)



F - Function Overview



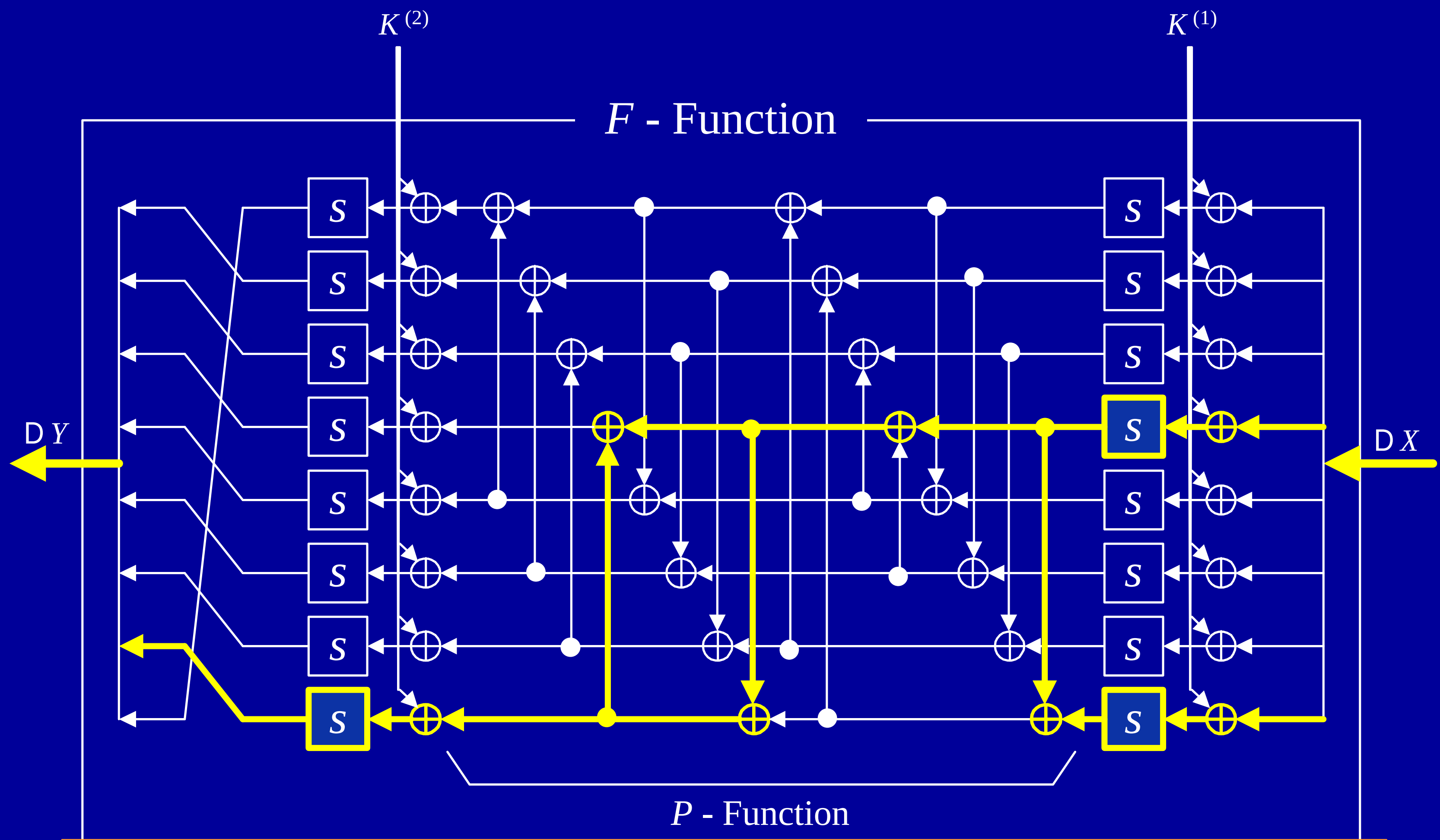
Design Rationale of P-Function

- Maximize minimum number of active *s*-boxes
  - Minimize upper bound of maximum differential / linear prob. of round function
- Use only XOR operation
  - Simple construction
  - Efficient implementations in both software and hardware
- Minimize gate counts required for hardware

Design Rationale of P-Function

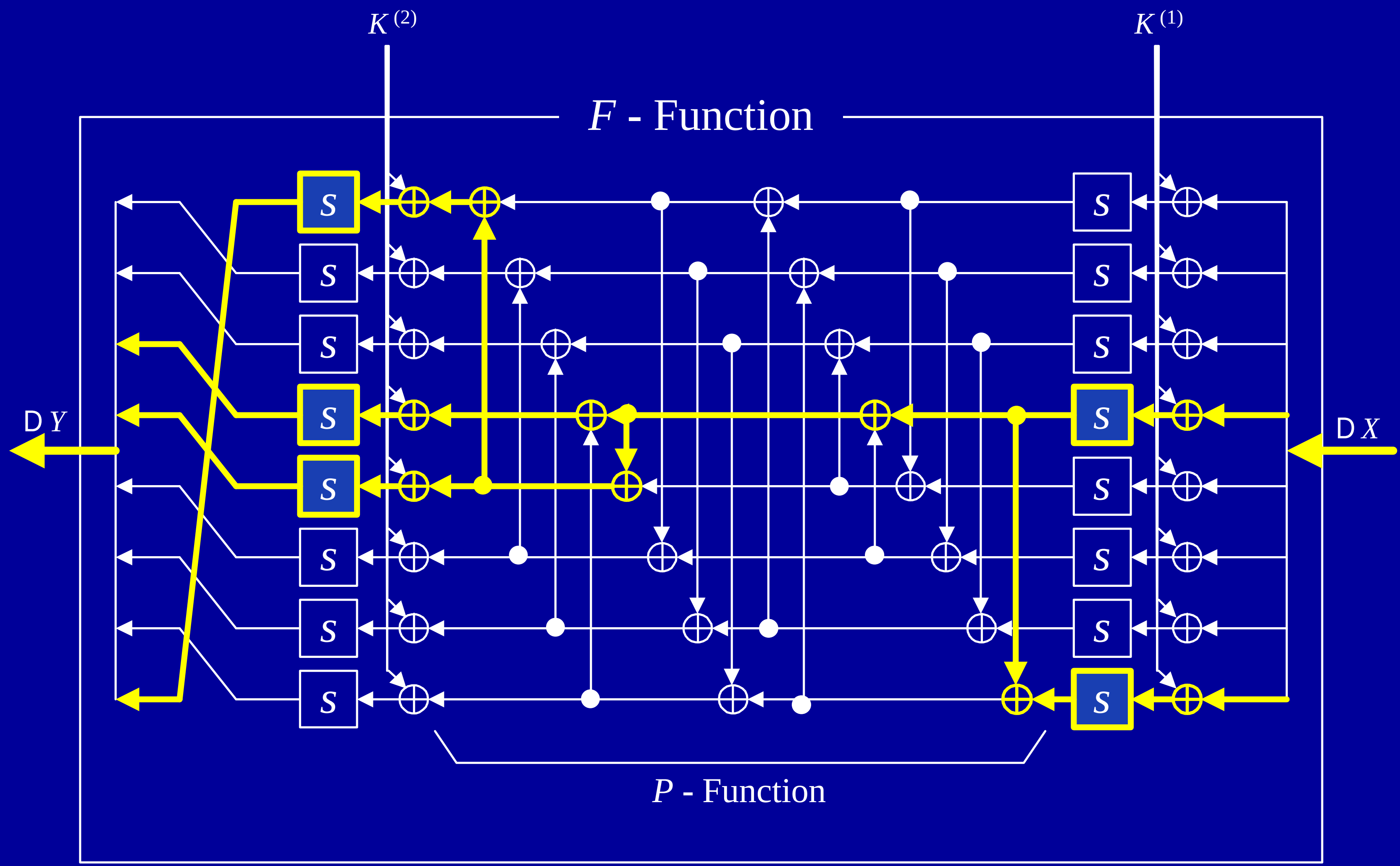
- Maximize minimum number of active *s*-boxes
  - Minimize upper bound of maximum differential / linear prob. of round function
- Use only XOR operation
  - Simple construction
  - Efficient implementations in both software and hardware
- Minimize gate counts required for hardware

of Active s-boxes = 3 (Bad P-Function)

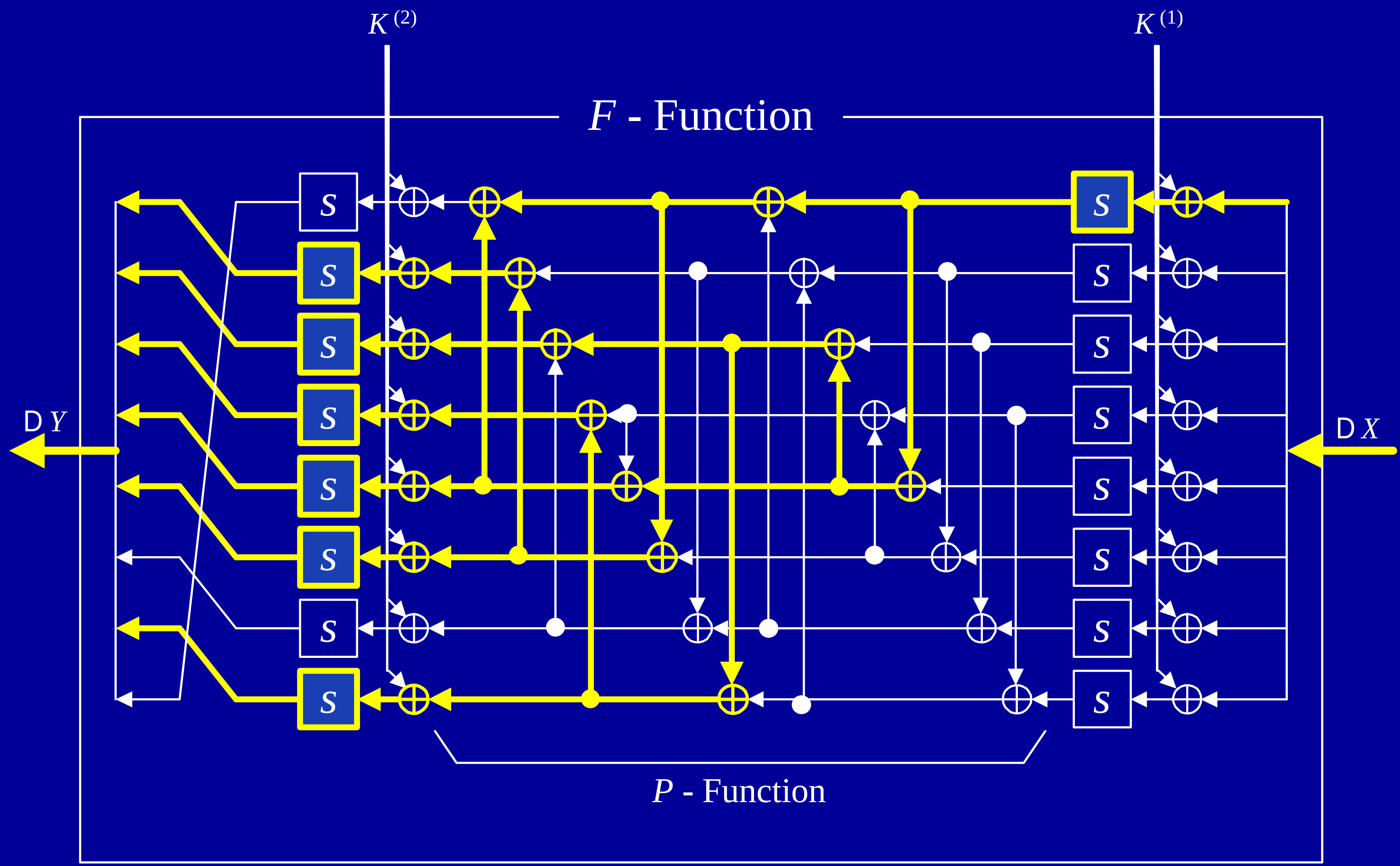


Many active *s*-boxes mean high security against DC.

of Active s-boxes ≥ 5 (E2 P-Function)



of Active s-boxes ≥ 5 (cont.)



Design Rationale of s-box

1. Suitability for various platforms

2. No trap-doors

3. No vulnerability to known attacks

Rationale 1 : Suitability for Various Platforms

- Table-lookup
  - efficiency does not depend on processors with various word-lengths (8, 16, 32, 64 bits)
- One 8-by-8-bit *s*-box
  - consideration for 8-bit smart card implementations

Rationale 2 : No trap-doors

- Design principle is publicly given
- Based on well-known mathematical functions

Candidates of s-box

- $s : GF(2)^8 \longrightarrow GF(2)^8 \; ; \; x \longmapsto s(x) = g\,(\,f\,(x)\,)$

candidates of $f\,(x)$ and $g(x)$

I. x^k in $GF(2^8)$ $\quad \forall\, k \in GF(2^8),\ k \neq 1$

II. u^x in $Z/(2^8+1)Z$ $\quad \forall\, u \in Z/(2^8+1)Z\,,\ u \neq 0,1$

III. x^k in $Z/(2^8+1)Z$ $\quad \forall\, k \in Z/(2^8+1)Z\,,\ k \neq 1$

IV. $ax+b$ in $Z/(2^8)Z$ $\quad \forall\, a, b \in Z/(2^8)Z$

V. $ax+b$ in $Z/(2^8+1)Z$ $\quad \forall\, a, b \in Z/(2^8+1)Z$

$$3 \leq w_H(a), w_H(b) \leq 5$$

Note that $256 \in Z/(2^8+1)Z$ corresponds to $0 \in GF(2)^8$.

Rationale 3 : No Vulnerability to Known Attacks

- Considered Attacks
  - Differential cryptanalysis [BS90]
  - Linear cryptanalysis [M93]
  - Higher order differential attack [JK97]
  - Interpolation attack [JK97]
  - Partitioning cryptanalysis [HM97]

How to select s-box

- $s : GF(2)^8 \longrightarrow GF(2)^8 \,;\, x \mapsto s(x) = g\,(\,f\,(x)\,)$

  I. $f\,(x) = x^{\,e}$ **in GF(2^8)**

  IV. $g(y) = ay + b$ **in Z/(2^8)Z**

Composition of functions

from different groups

expected to be effective in thwarting
algebraic attacks, e.g., interpolation attack

How to select s-box parameters (1)

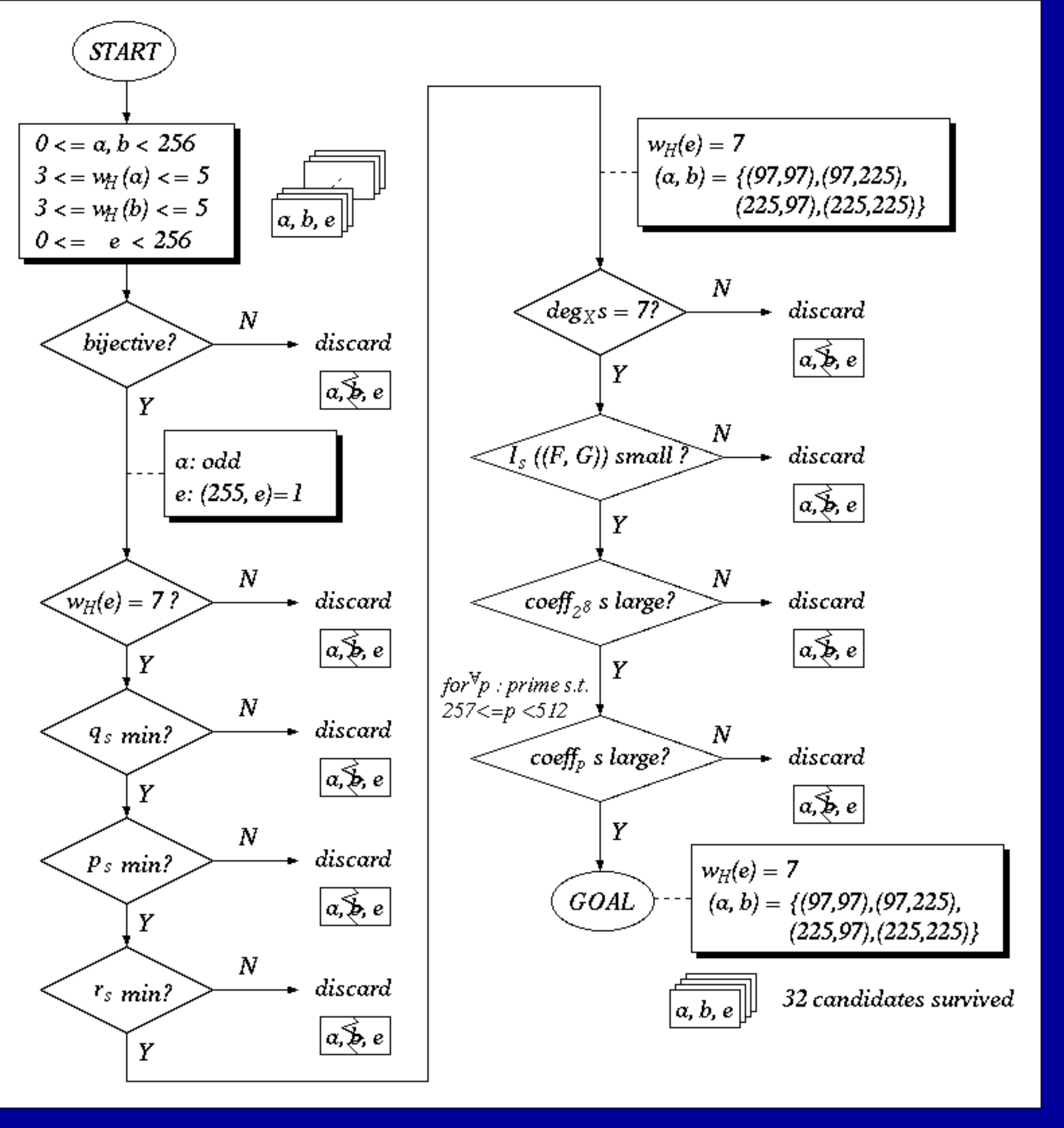
$$s : GF(2)^8 \longrightarrow GF(2)^8 \; ; \; x \longmapsto s(x) = g\,(\,f\,(x)\,)$$

$$f\,(x) = x^{\,e} \qquad \text{in } GF(2^8)$$

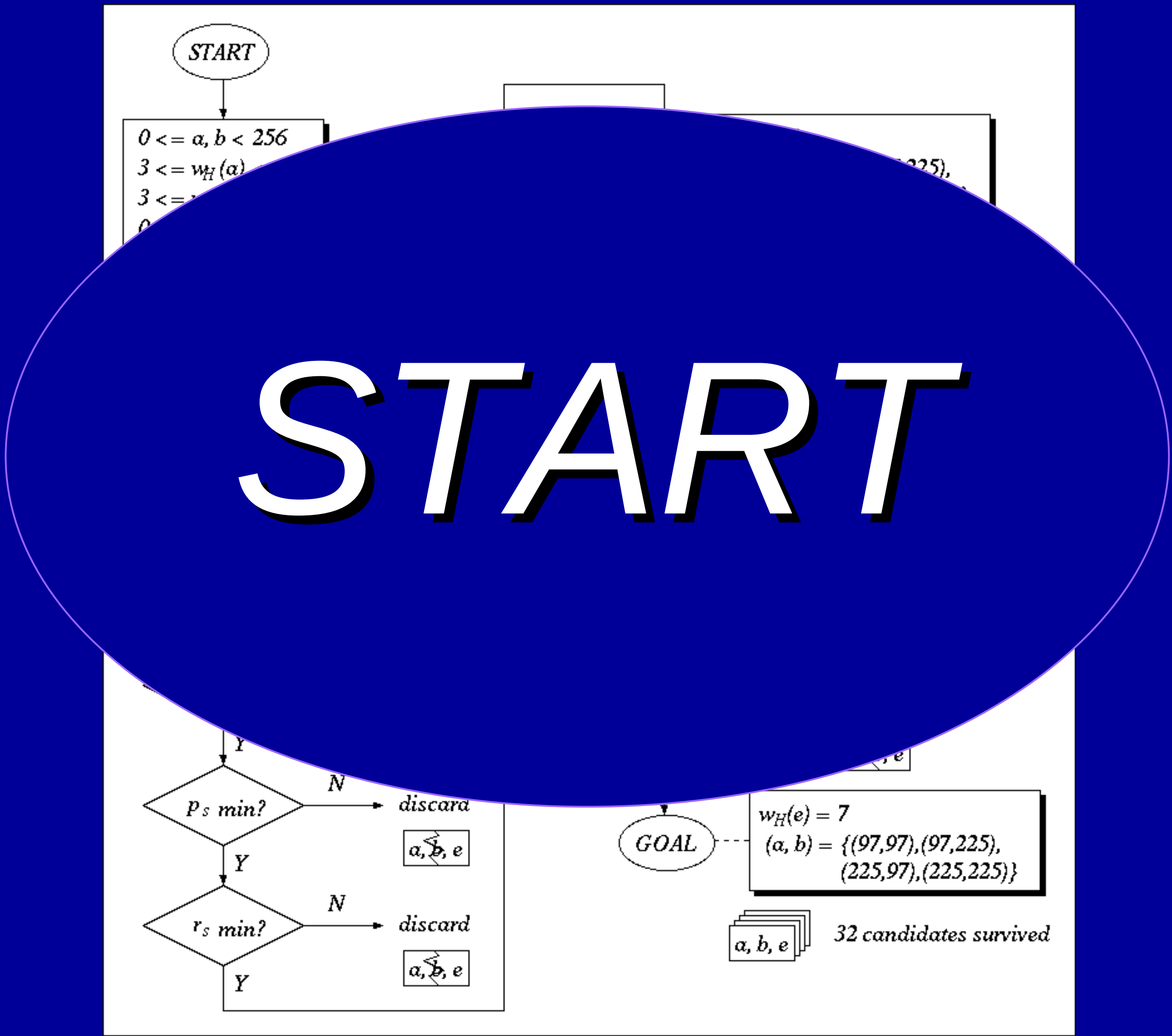
$$g\,(y) = ay + b \quad \text{in } Z/(2^8)Z$$

- Criteria for the considered 5 attacks
- Bijectivity
- Hamming weight of ***a*, *b***
- Differential-linear prob.

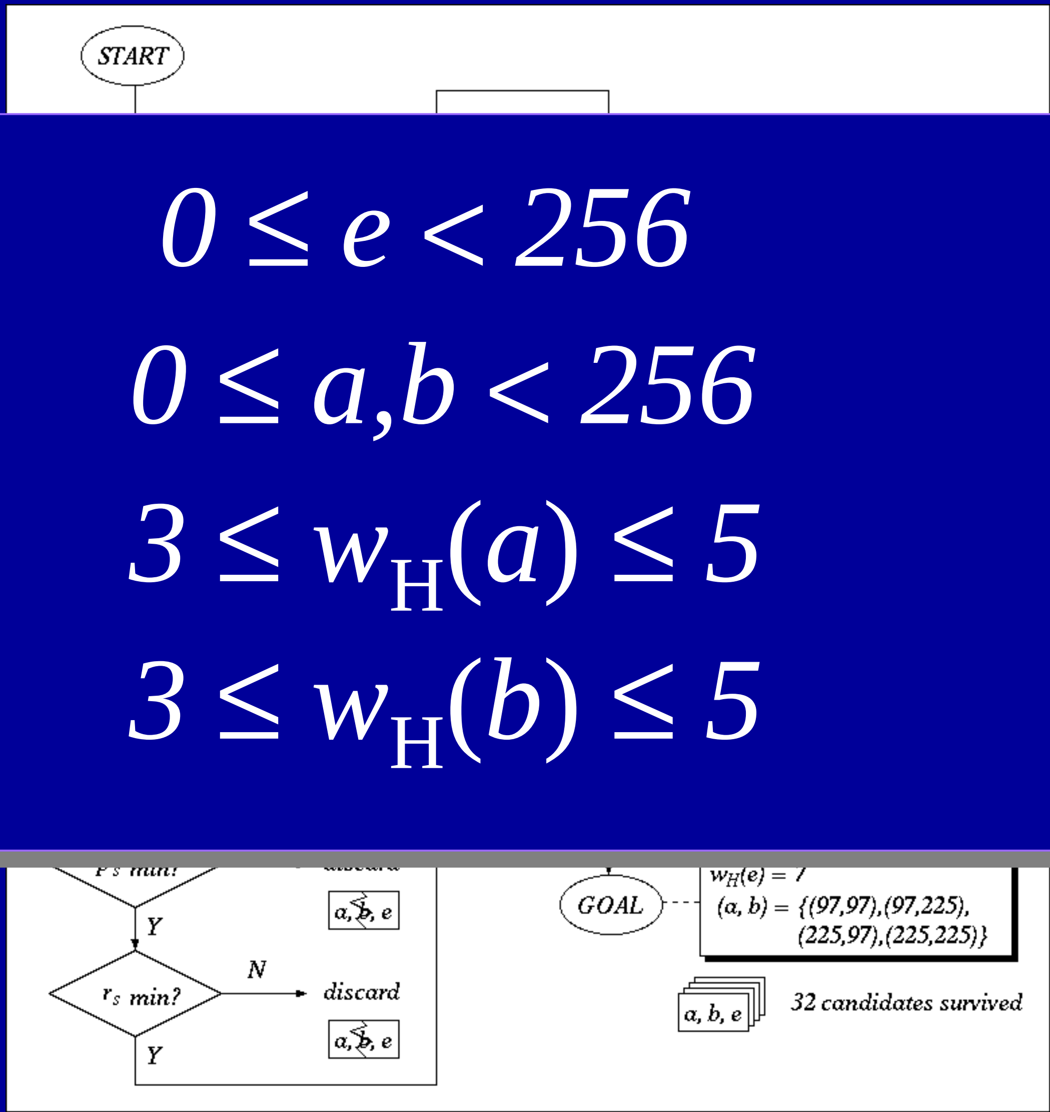
How to select s-box parameters (2)



How to select s-box parameters (2)



How to select s-box parameters (2)



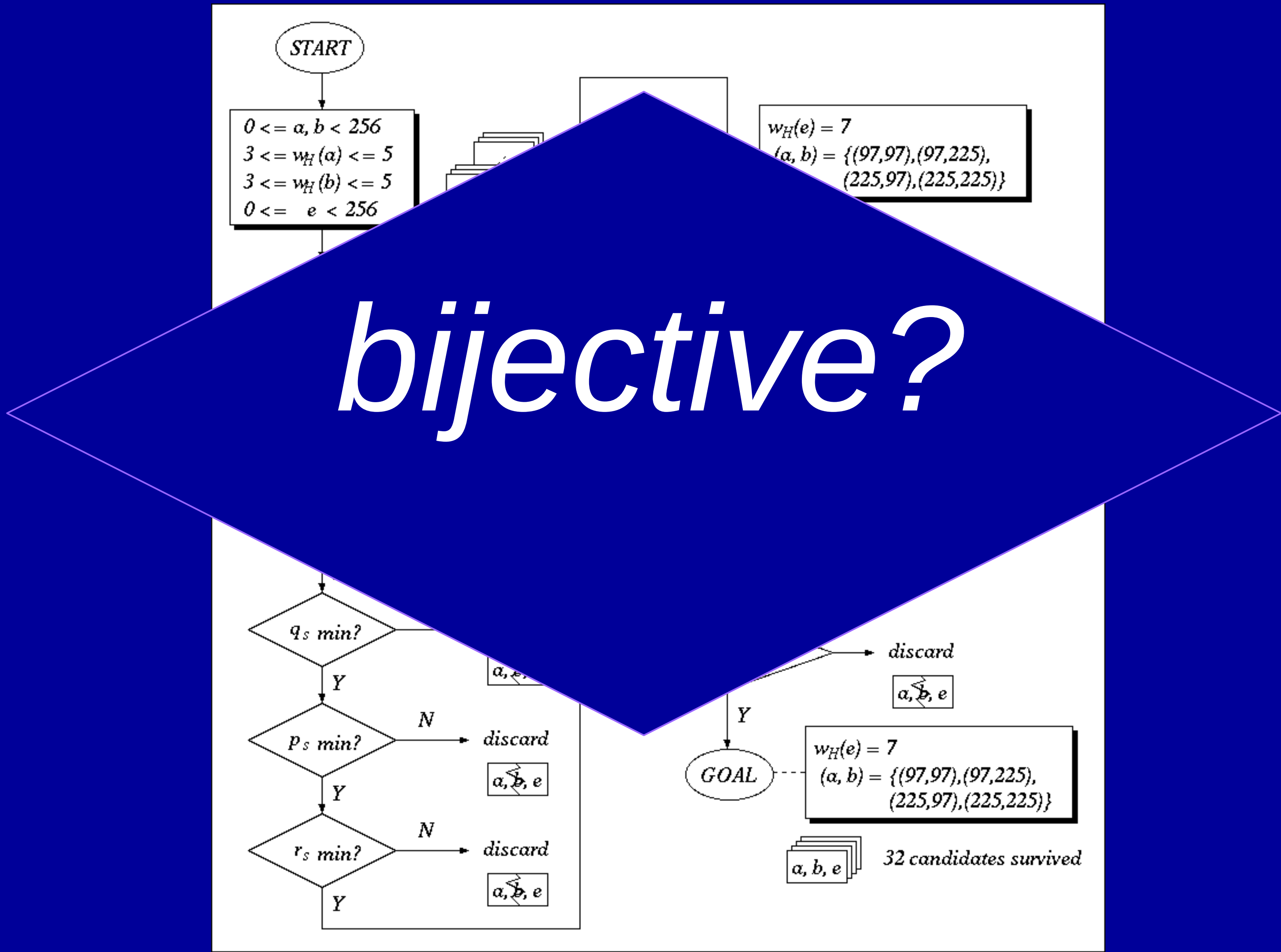
$$0 \le e < 256$$

$$0 \le a,b < 256$$

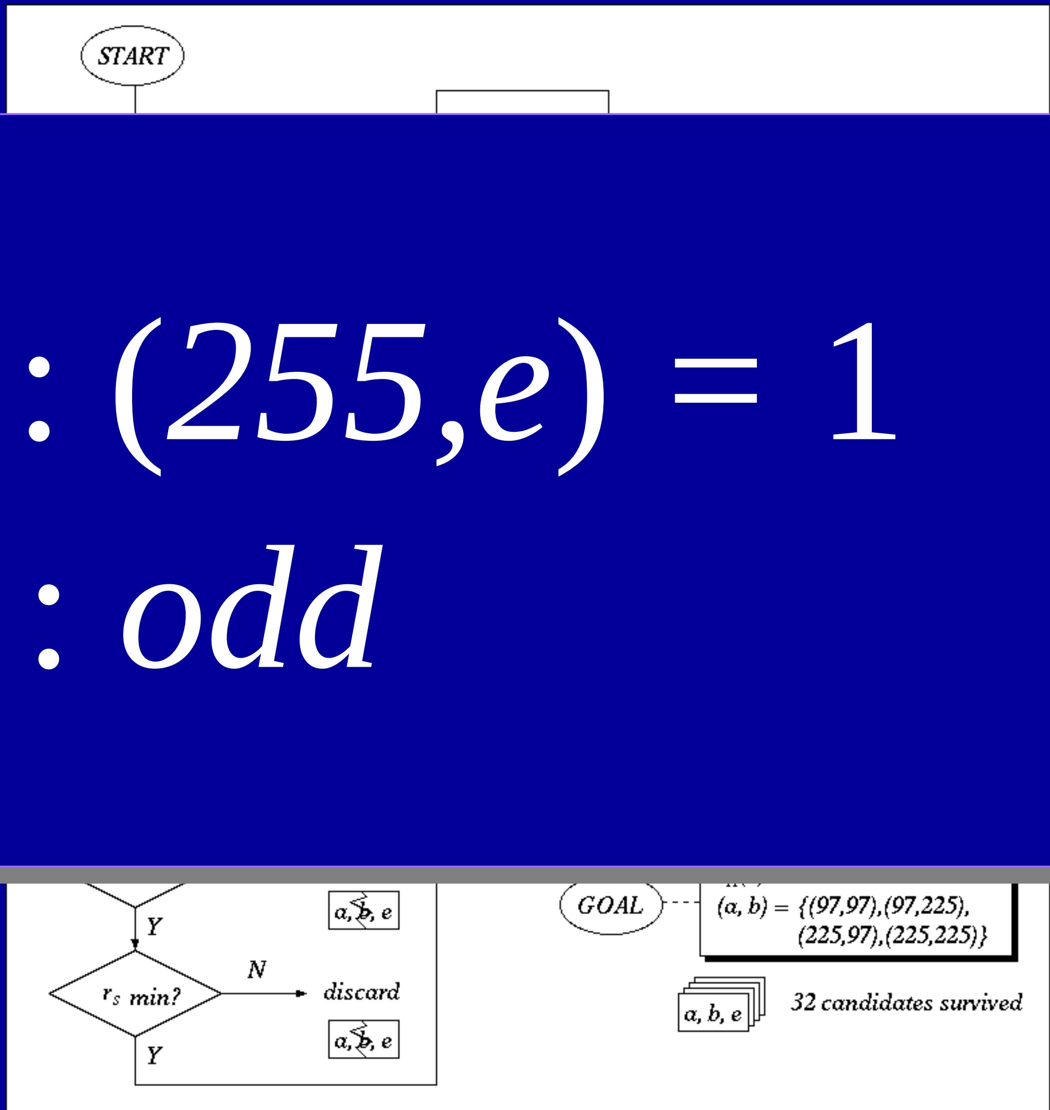
$$3 \le w_{\mathrm{H}}(a) \le 5$$

$$3 \le w_{\mathrm{H}}(b) \le 5$$

How to select s-box parameters (2)



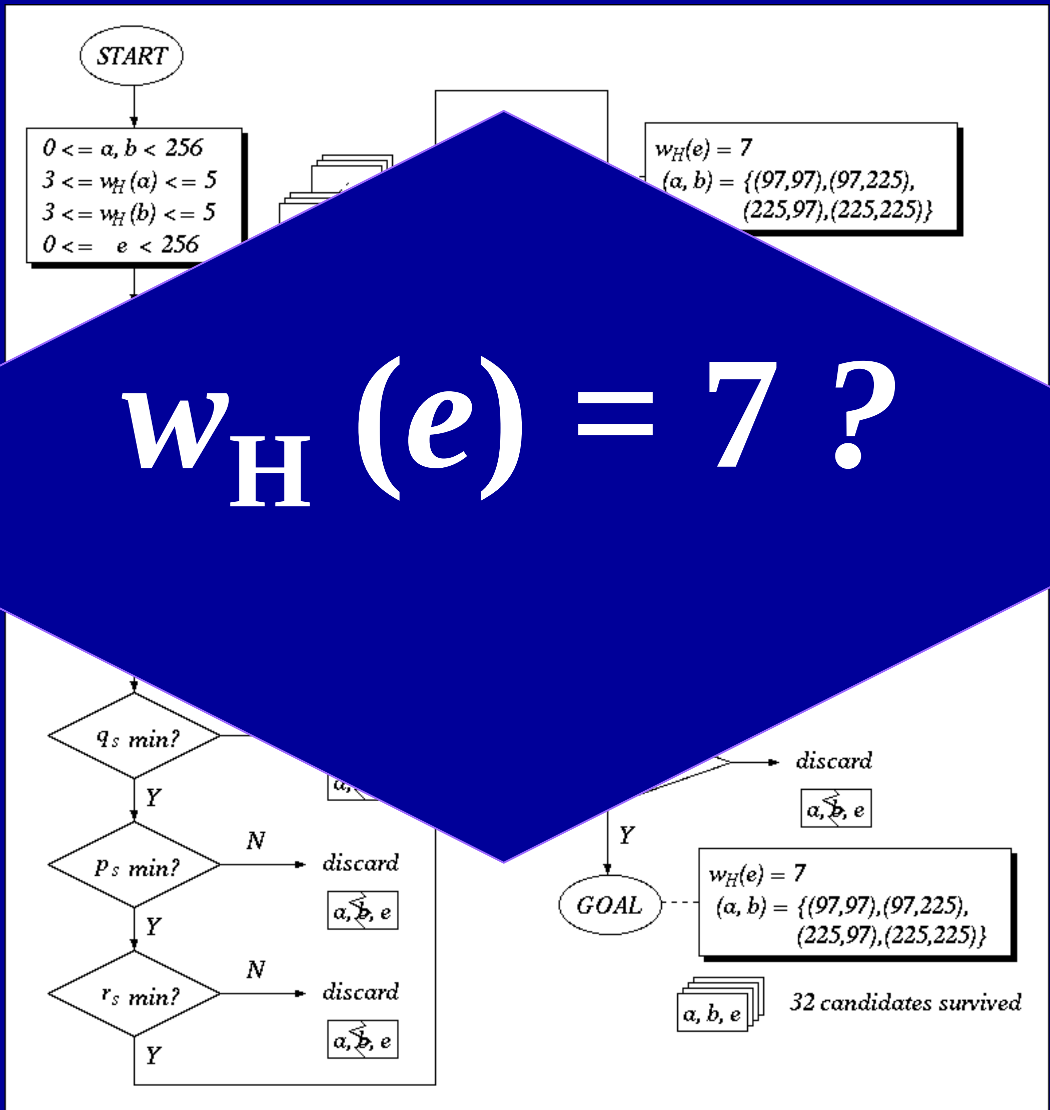
How to select s-box parameters (2)



$$e : (255, e) = 1$$

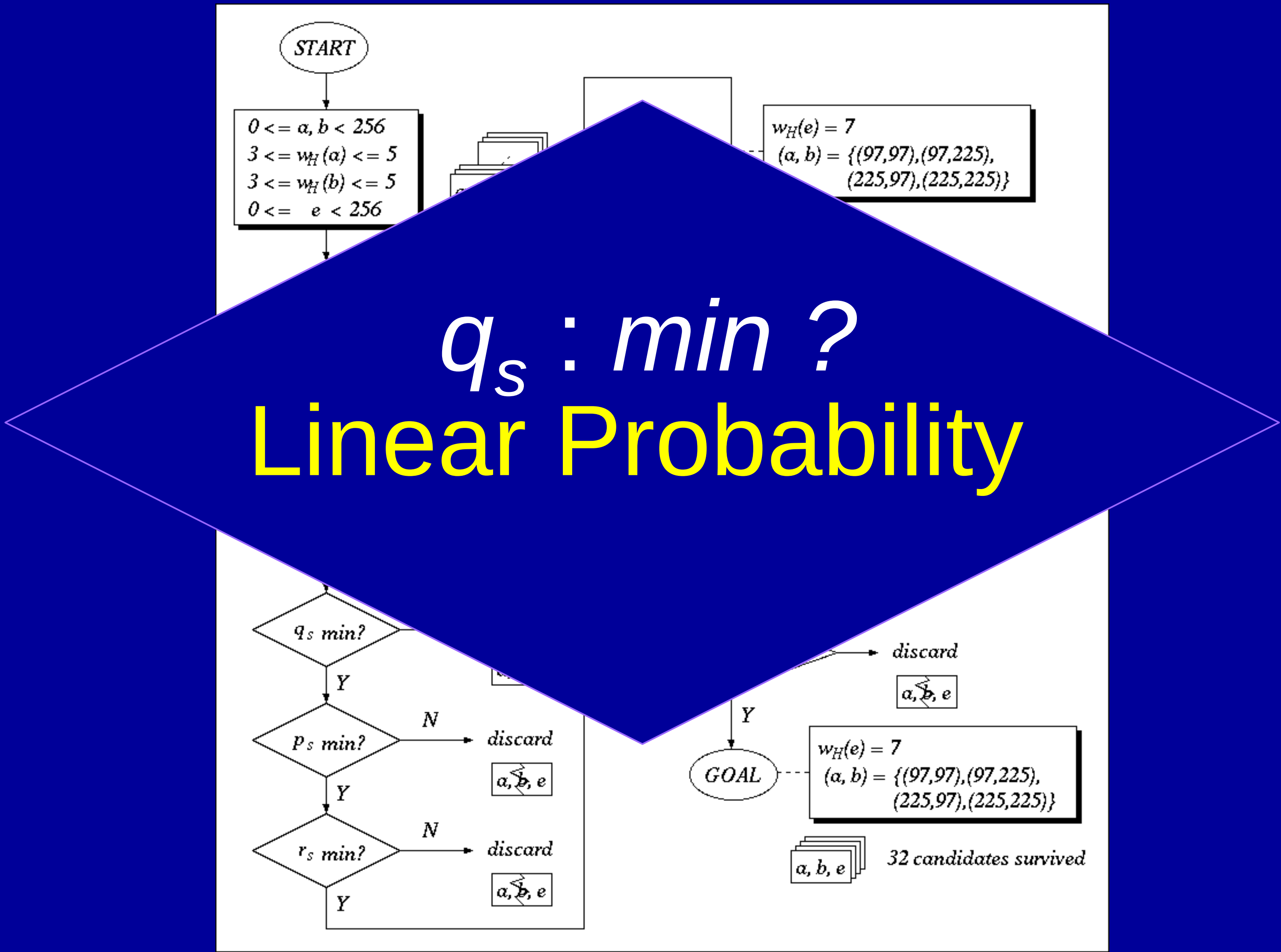
$$a : odd$$

How to select s-box parameters (2)

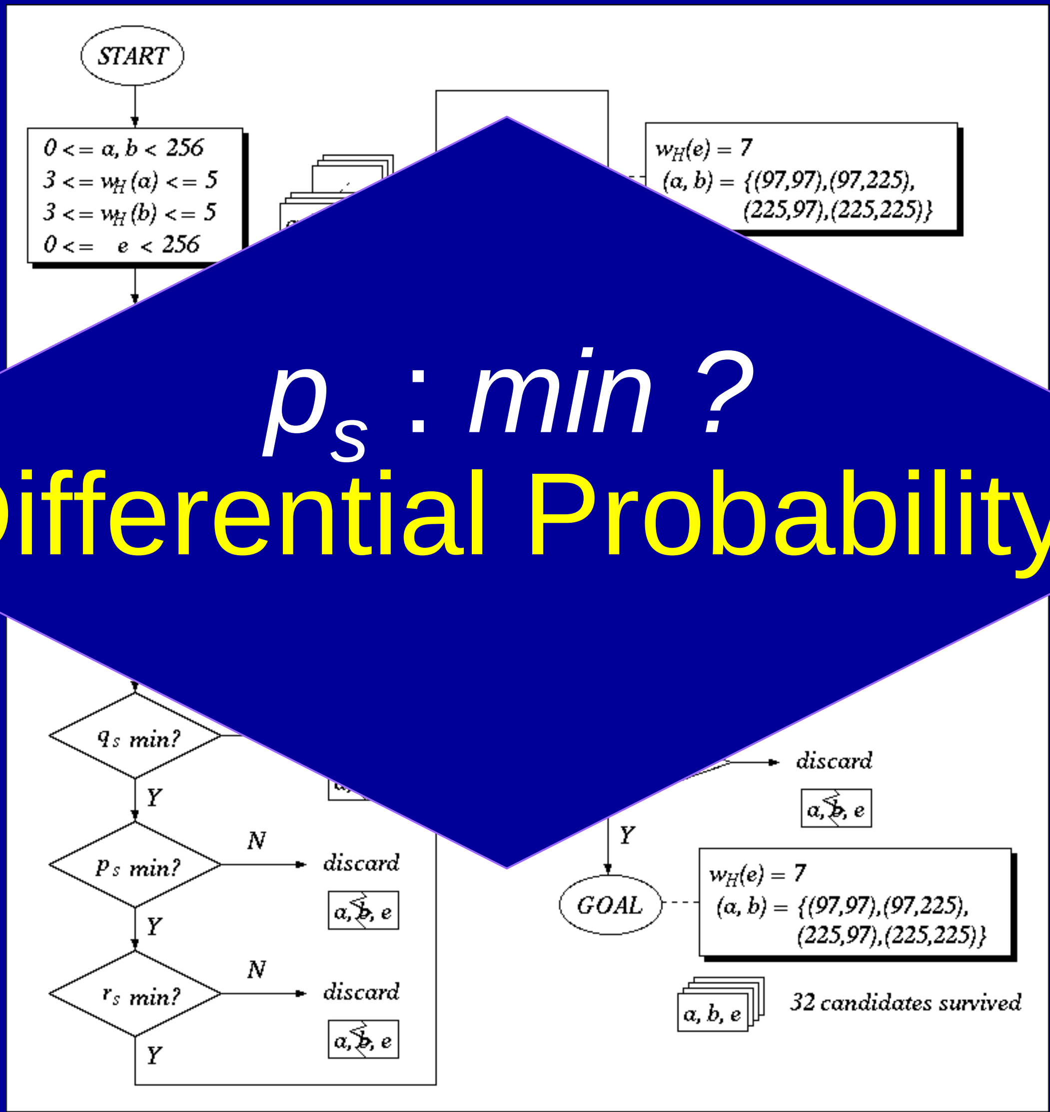


$$w_{\mathrm{H}}(e) = 7\ ?$$

How to select s-box parameters (2)



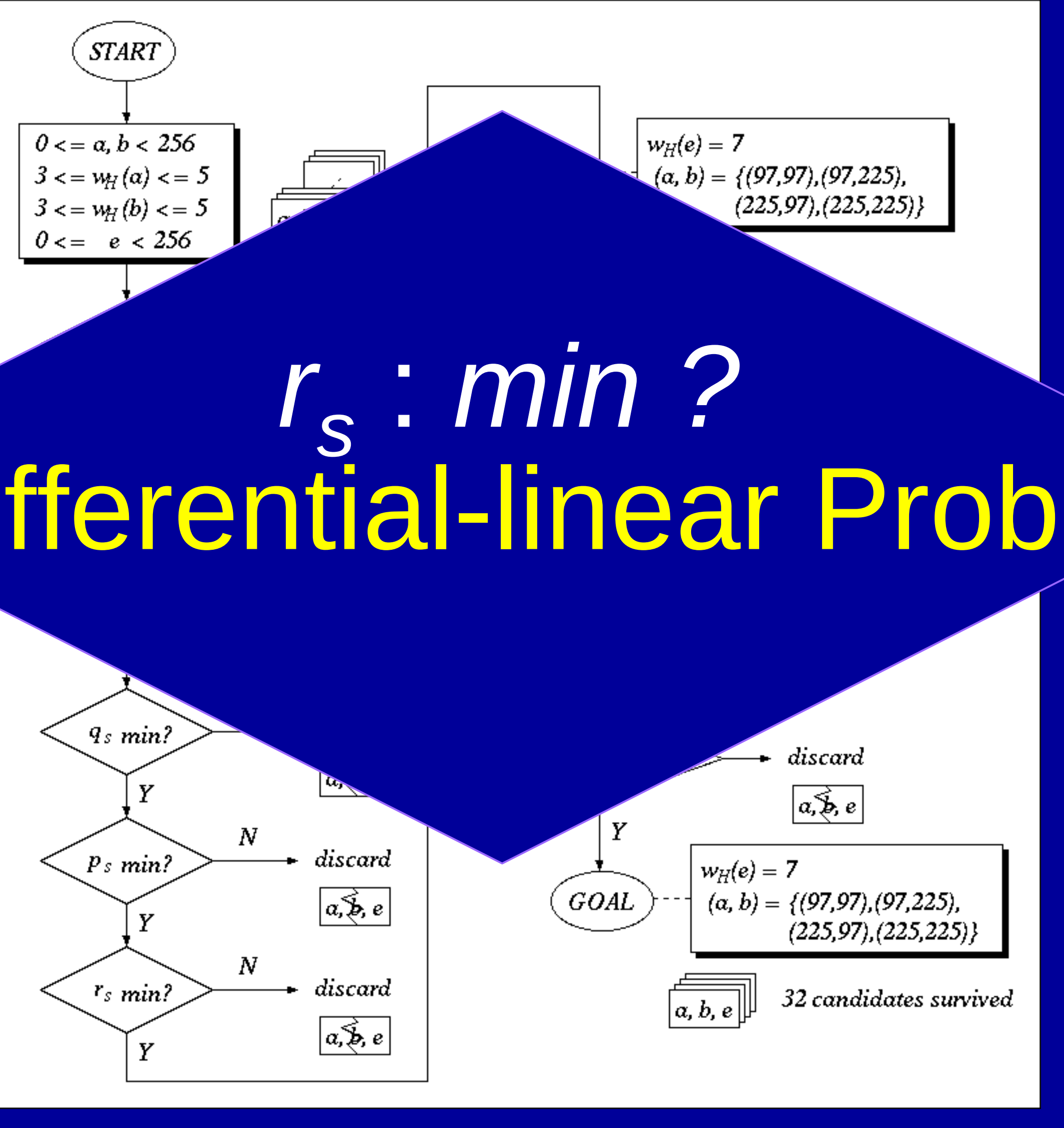
How to select s-box parameters (2)



p_s : *min ?*

Differential Probability

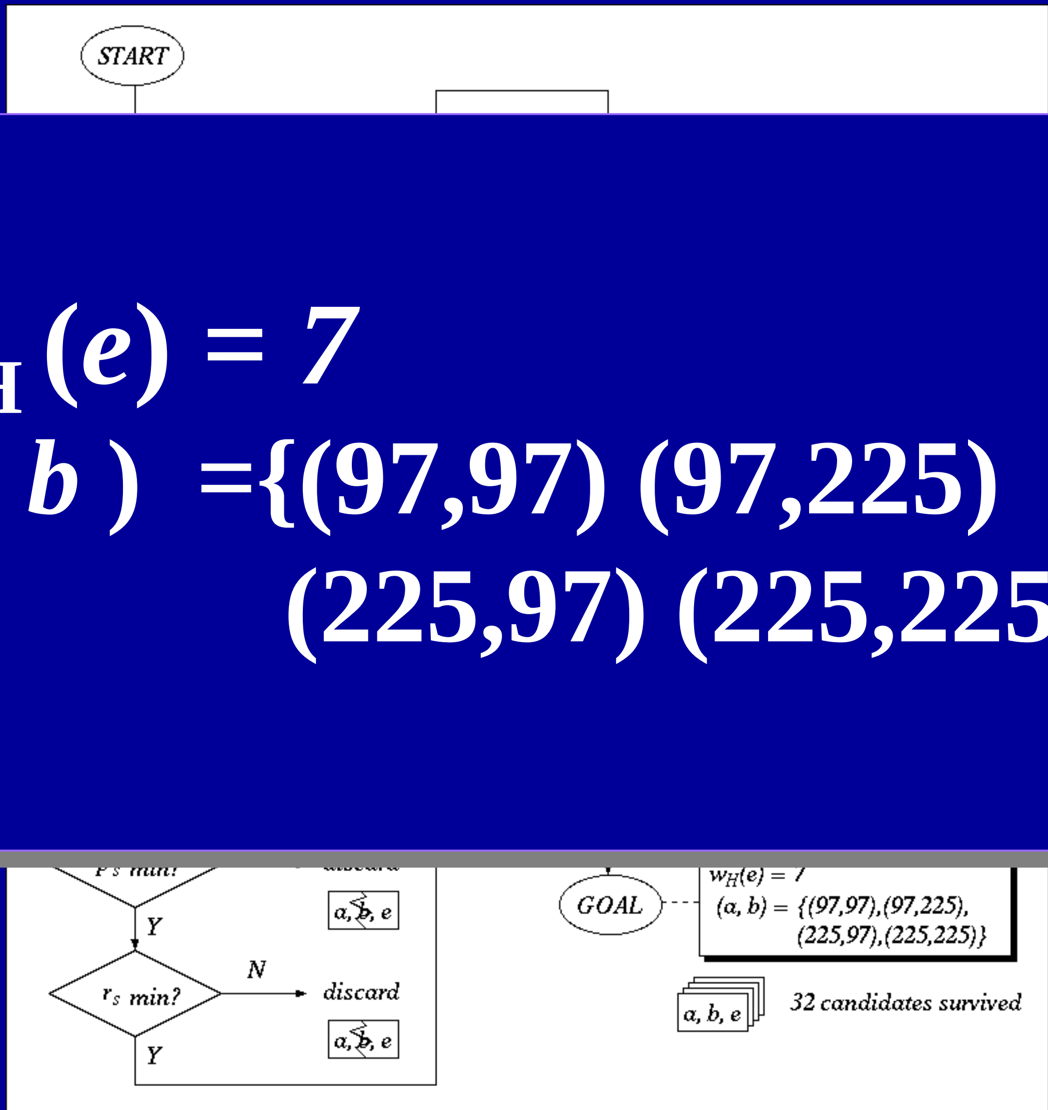
How to select s-box parameters (2)



r_s : min ?

Differential-linear Prob.

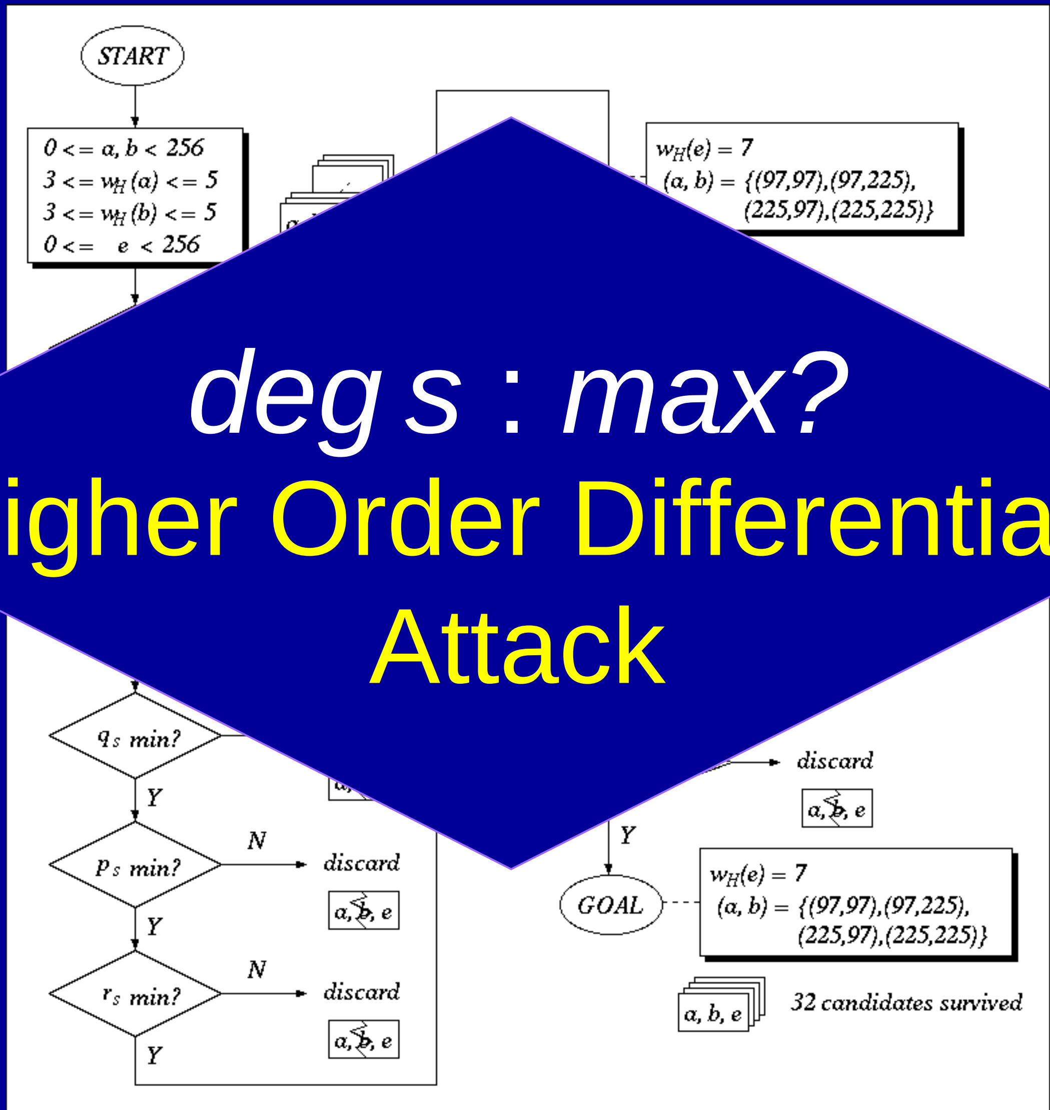
How to select s-box parameters (2)



$$w_H(e) = 7$$

$$(a, b) = \{(97,97)\ (97,225)\ (225,97)\ (225,225)\}$$

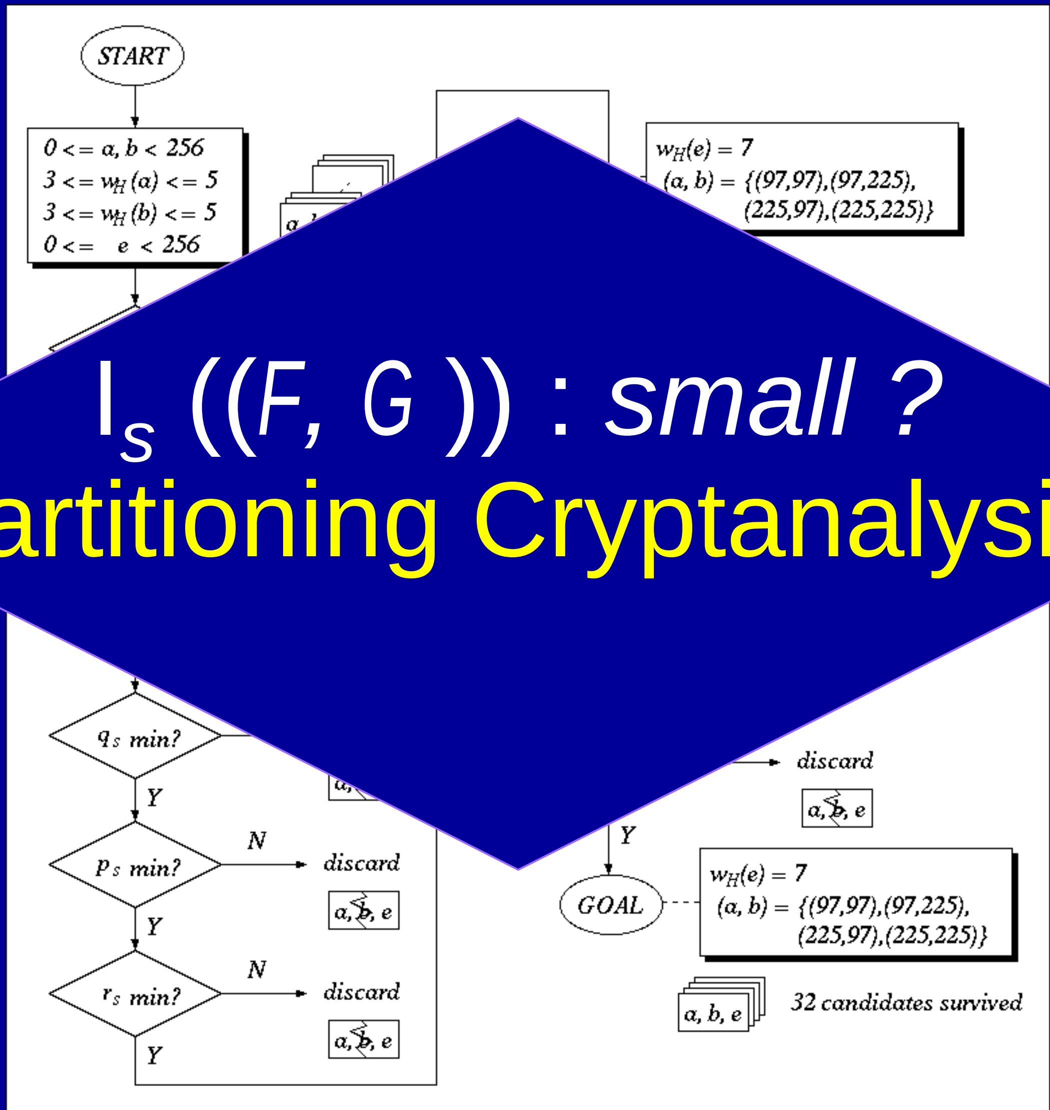
How to select s-box parameters (2)



deg s : max?

Higher Order Differential Attack

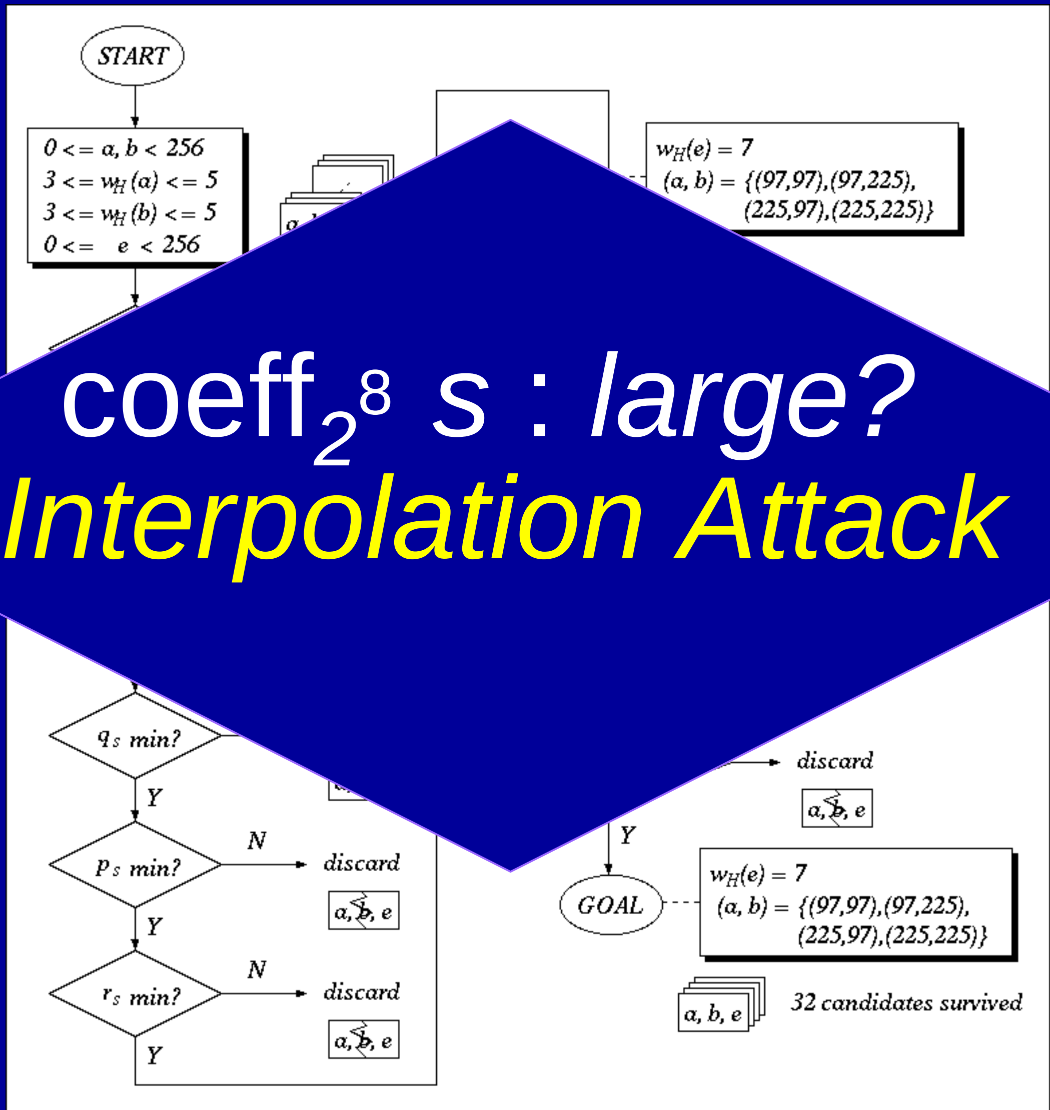
How to select s-box parameters (2)



$I_s((F, G))$: *small ?*

Partitioning Cryptanalysis

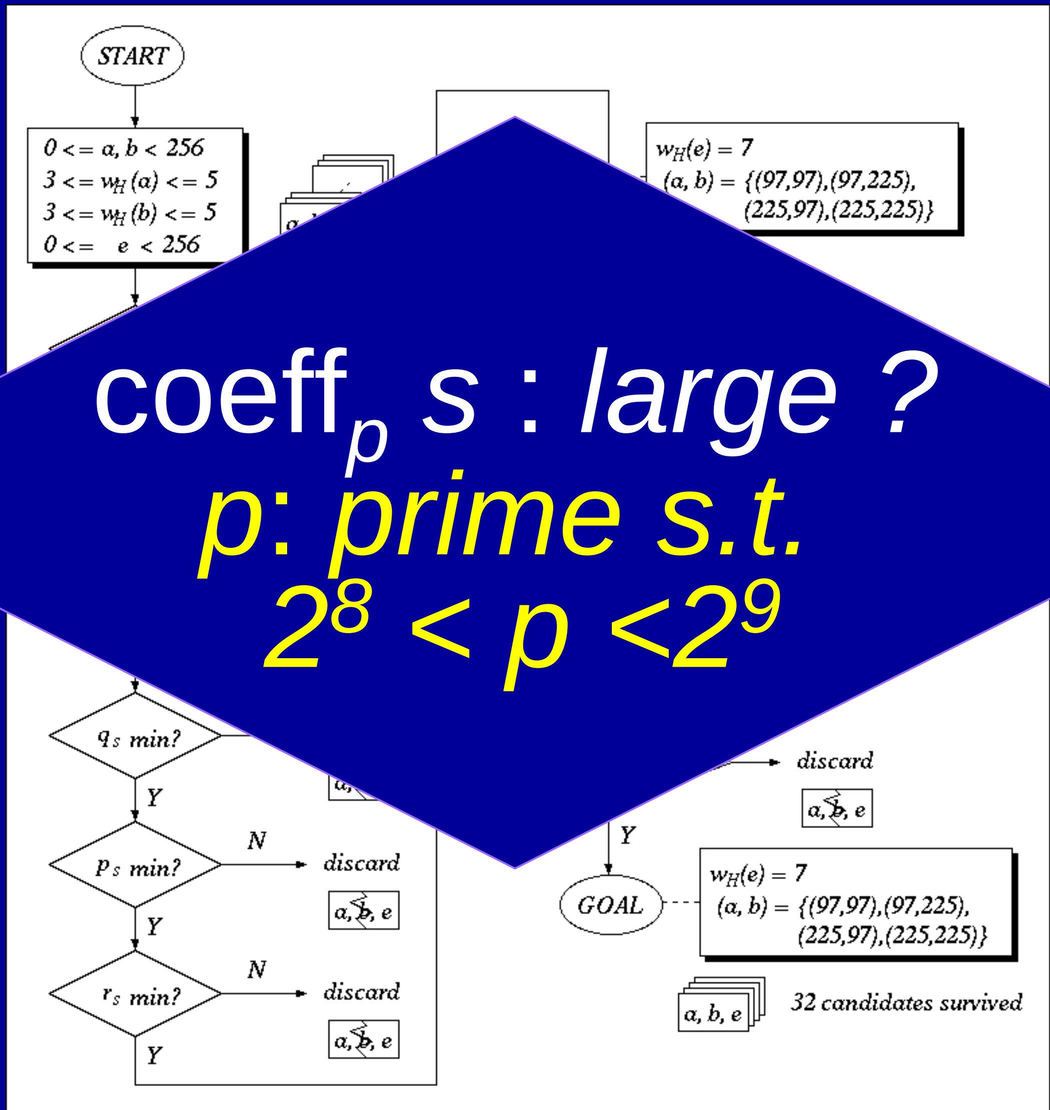
How to select s-box parameters (2)



coeff$_{2^8}$ s : *large?*

Interpolation Attack

How to select s-box parameters (2)

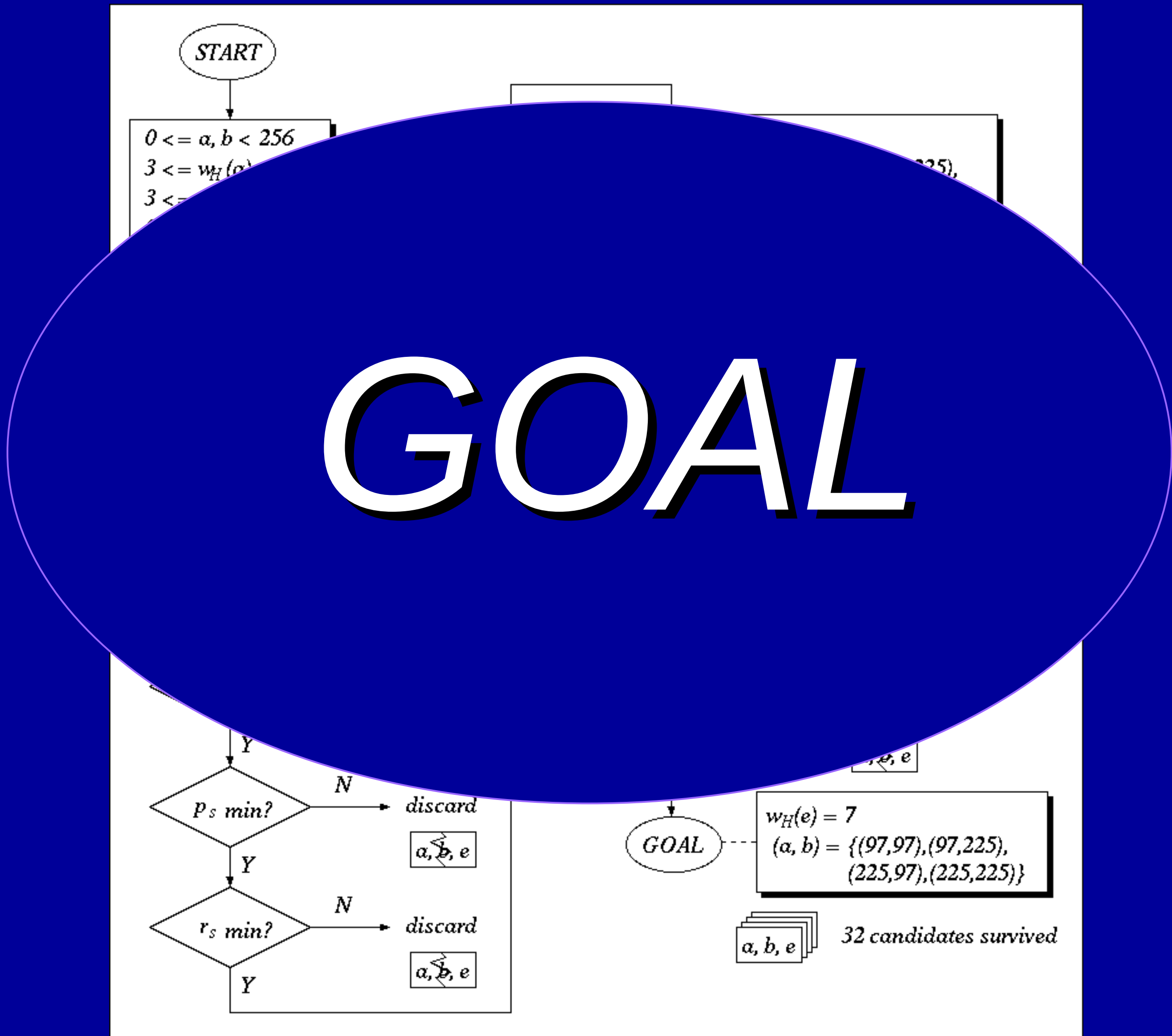


coeff$_p$ *s* : *large ?*

p: *prime s.t.*

$2^8 < p < 2^9$

How to select s-box parameters (2)



How to select s-box parameters (3)

$$s : GF(2)^8 \longrightarrow GF(2)^8 \; ; \; x \longmapsto s(x) = g\,(\,f\,(x)\,)$$

$$f\,(x) = x^{\,e} \qquad \text{in } \; GF(2^8)$$

$$g\,(y) = ay + b \quad \text{in } \; Z/(2^8)Z$$

e = 127, 191, 223, 239, 247, 251, 253, 254

(a, b) = (97, 97), (97, 225), (225, 97), (225, 225)

How to select s-box parameters (3)

$$s : GF(2)^8 \longrightarrow GF(2)^8 \; ; \; x \longmapsto s(x) = g\,(\,f\,(x)\,)$$

$$f\,(x) = x^{\,e} \qquad \text{in } GF(2^8)$$

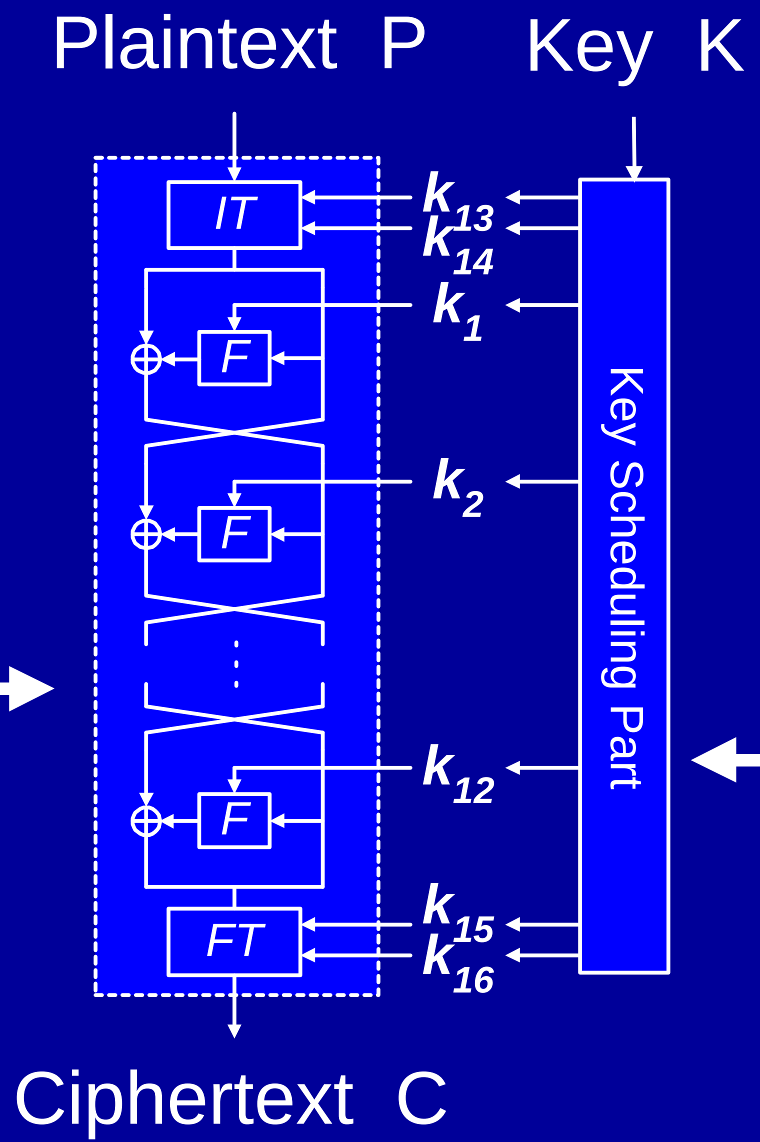
$$g\,(y) = ay + b \quad \text{in } Z/(2^8)Z$$

e	= **127**, 191, 223, 239, 247, 251, 253, 254
(a, b)	= (97, 97), **(97, 225)**, (225, 97), (225, 225)

(a, b, e) = (97, 225, 127) was selected.

High-level Structure of E2

Data randomizing part



Key scheduling part

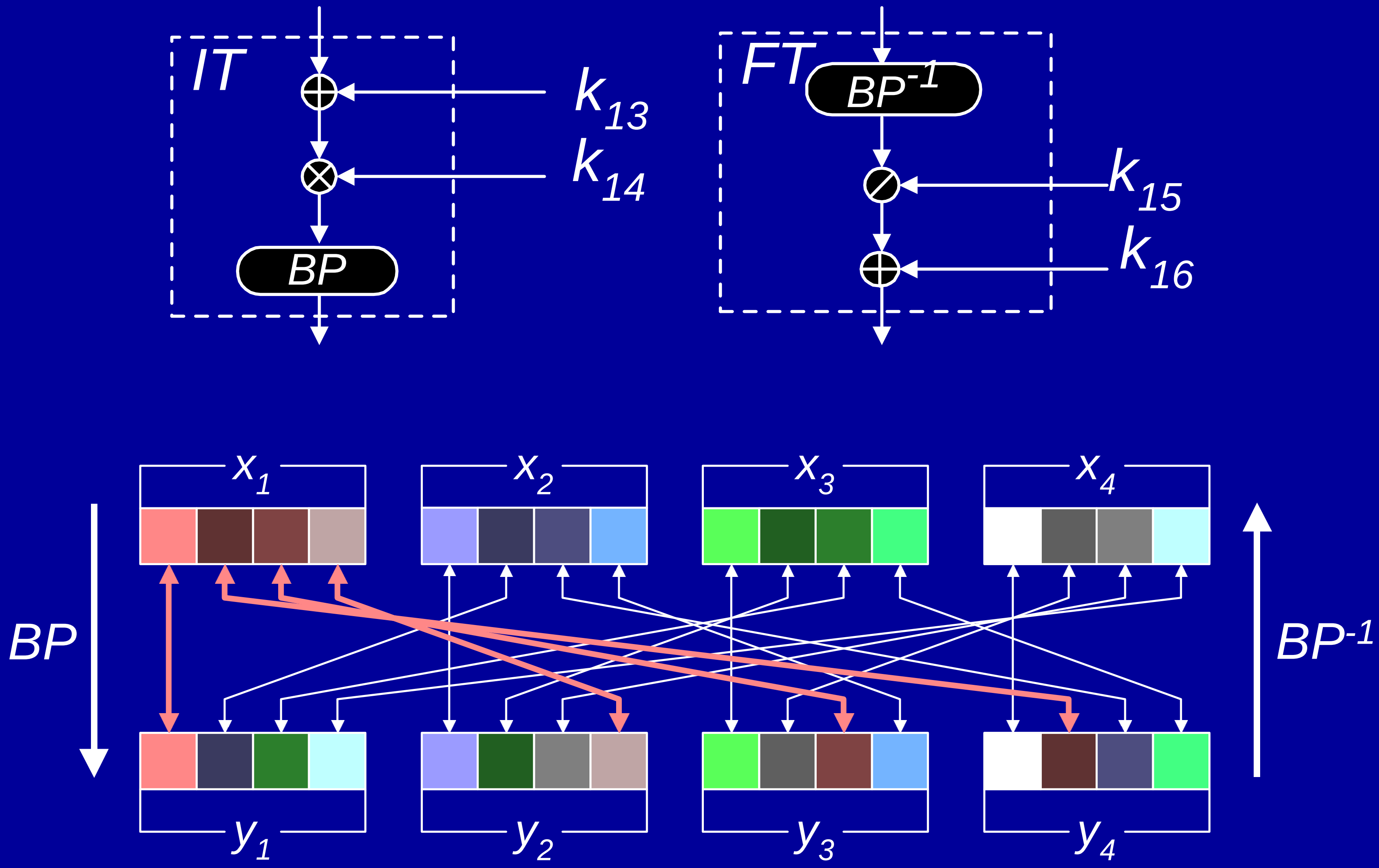
Design Rationale of IT / FT-Functions

Goal: To protect *E2* against future
advances in cryptanalysis

IT-Function: avoid linking plaintext
to inputs to first *F*-Function

FT-Function: avoid linking ciphertext
to outputs from last *F*-Function

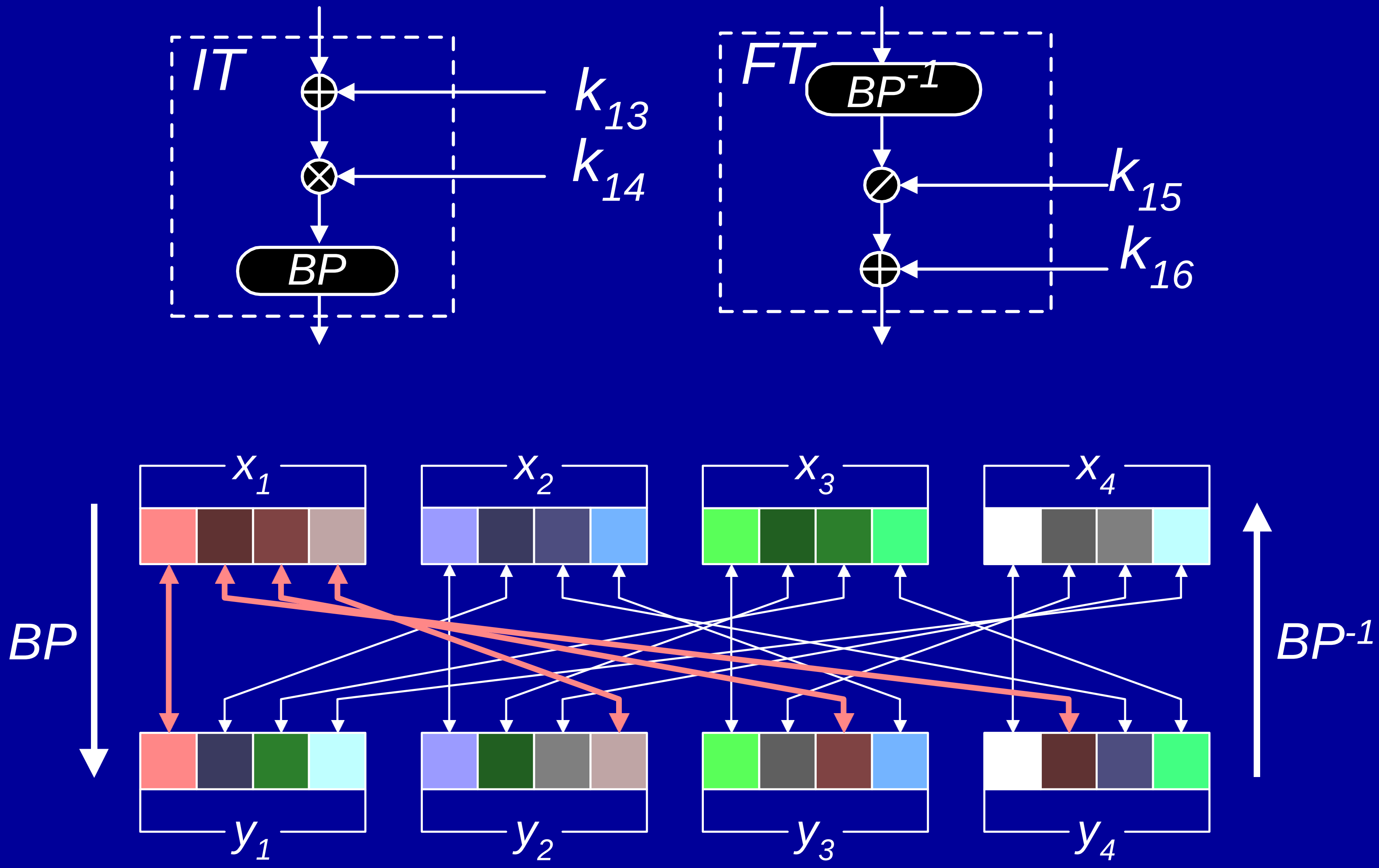
IT-Function and FT-Function Overview



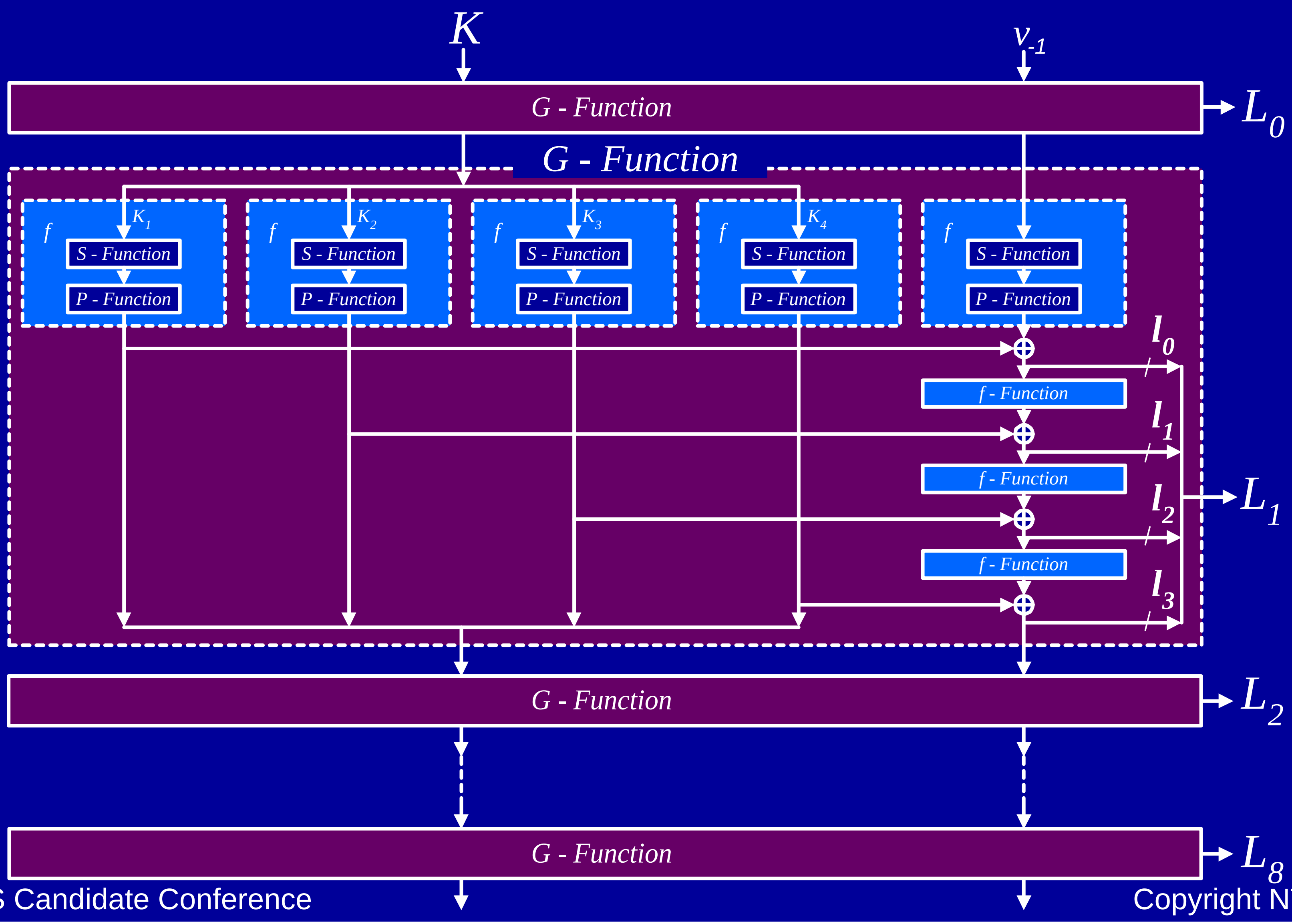
Design Rationale of IT / FT-Functions (cont.)

- multiplication $\otimes$
  - in order for each bit of the subkey to change many bits of output
  - four 32-bit integer multiplications
- XOR $\oplus$
  - improves the level of confusion by mixing incompatible group operations
- byte permutation BP
  - links different subblocks

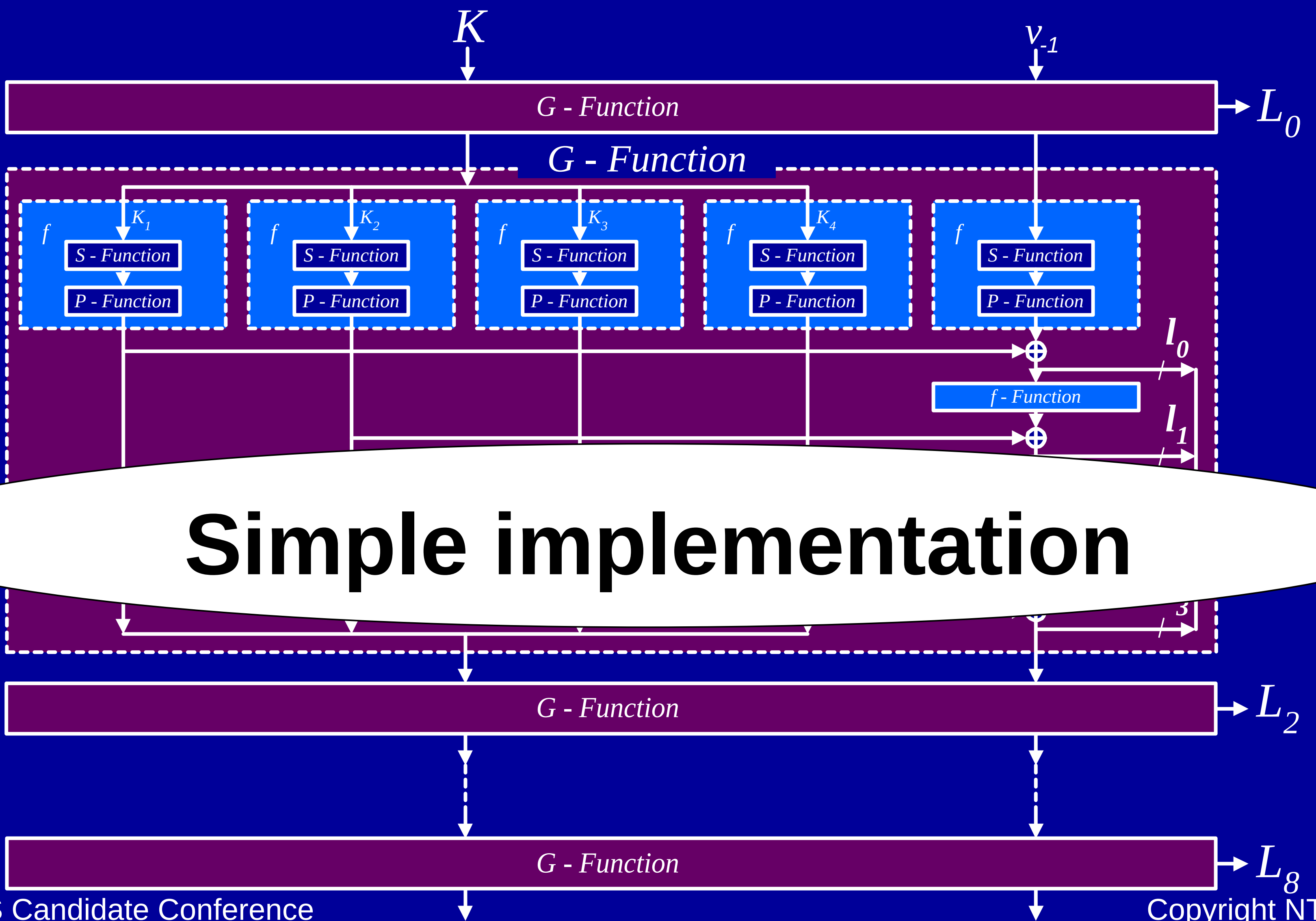
IT-Function and FT-Function Overview



Key Scheduling Part (1)

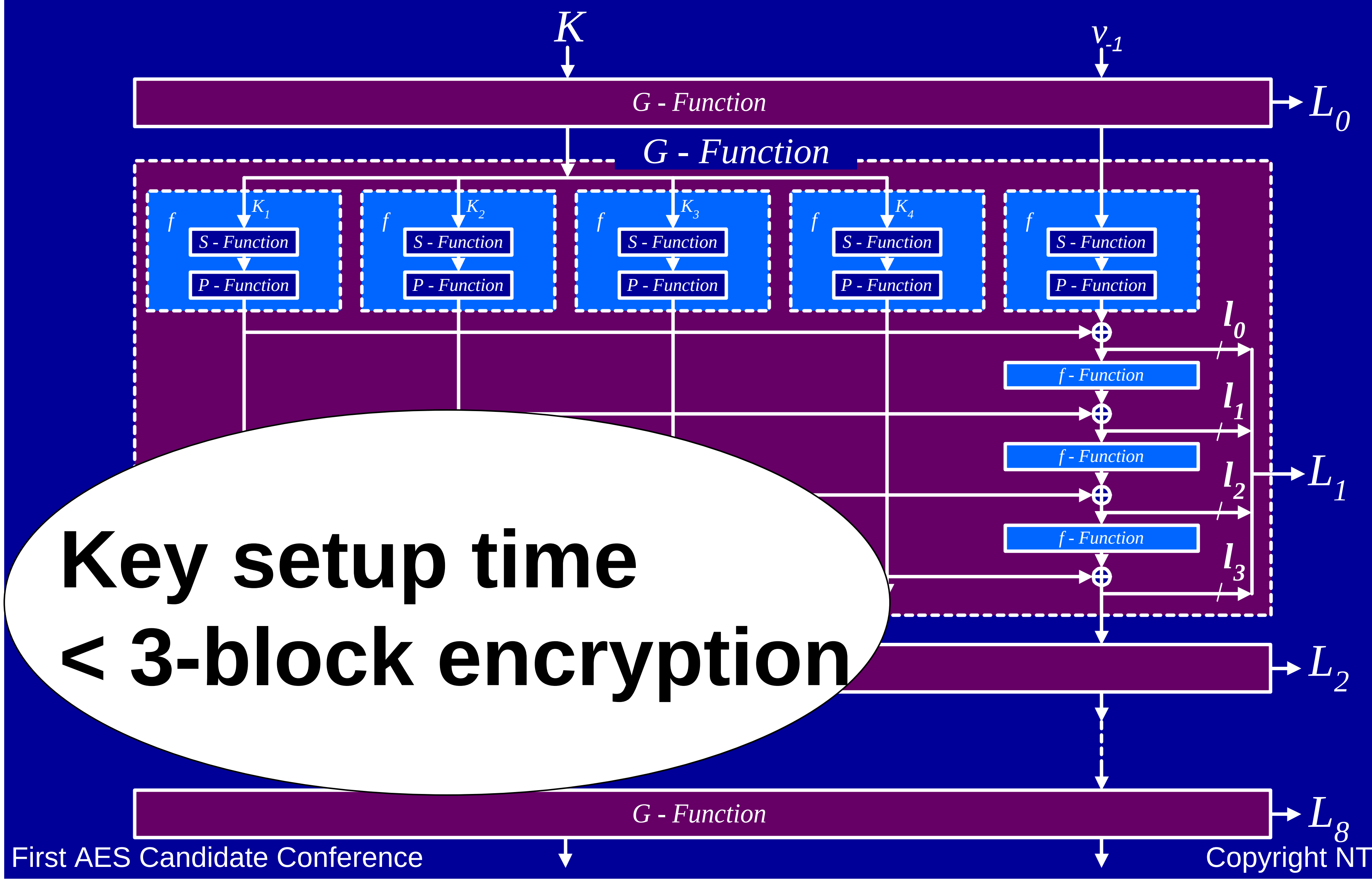


Key Scheduling Part (1)

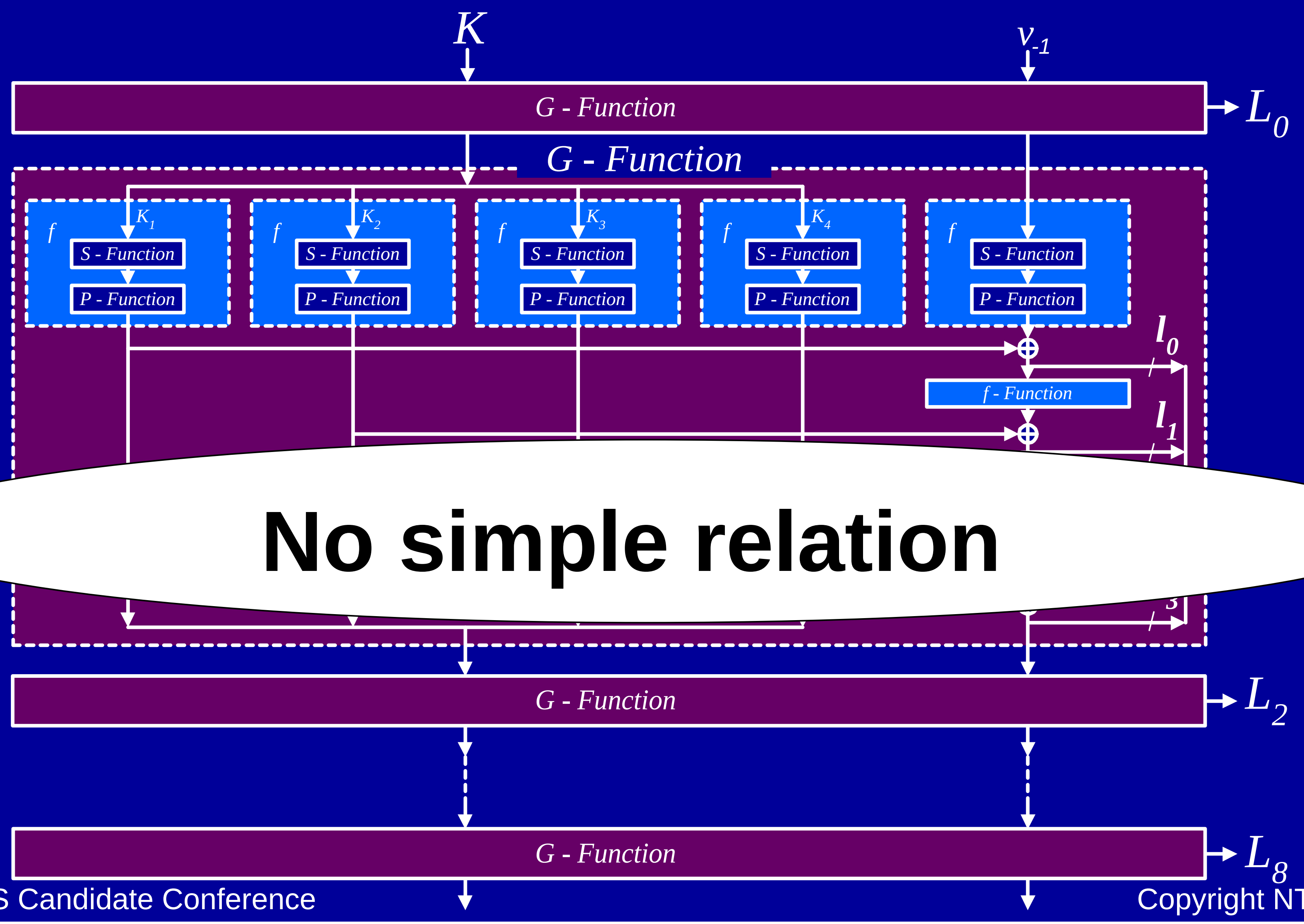


Simple implementation

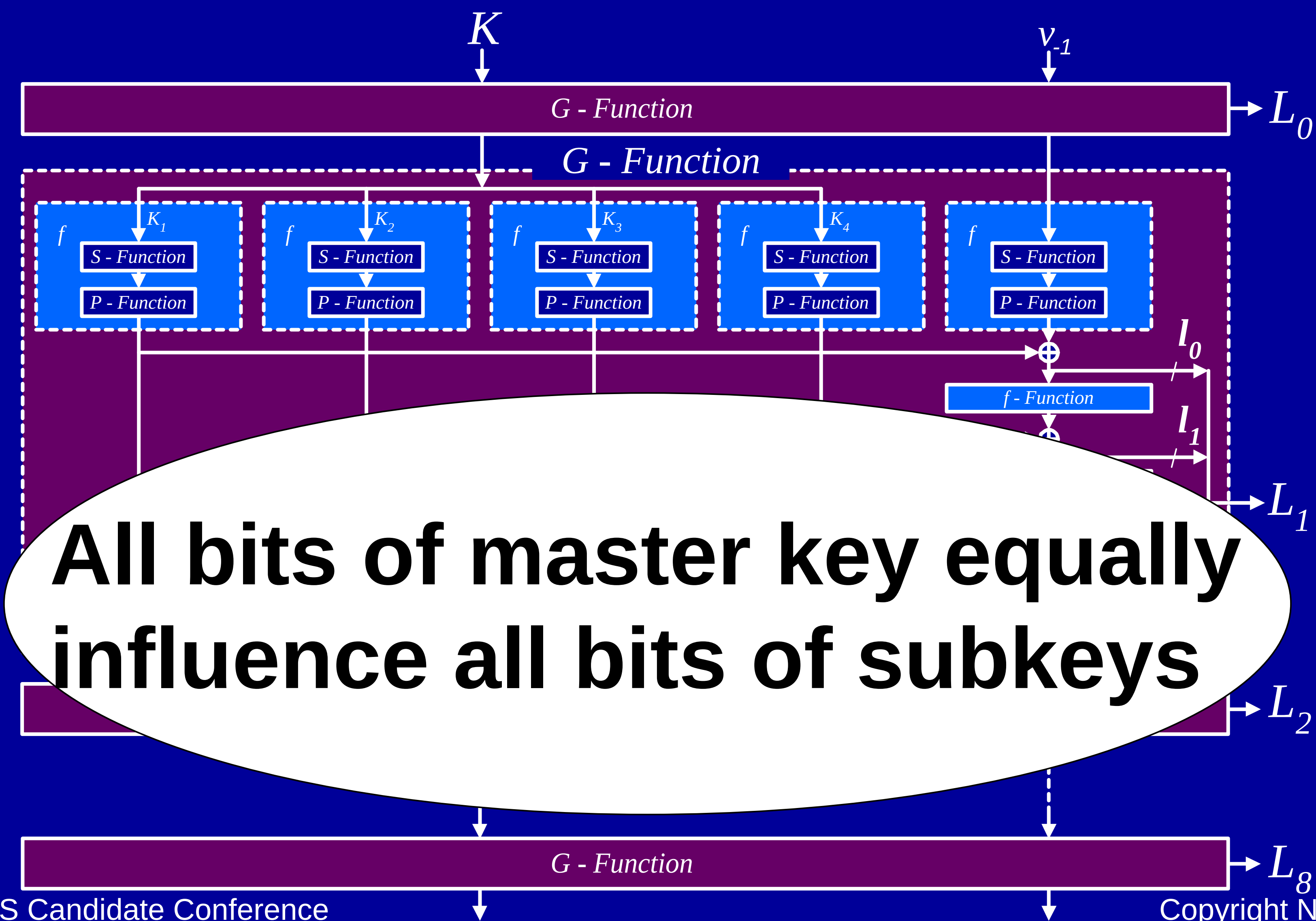
Key Scheduling Part (1)



Key Scheduling Part (1)

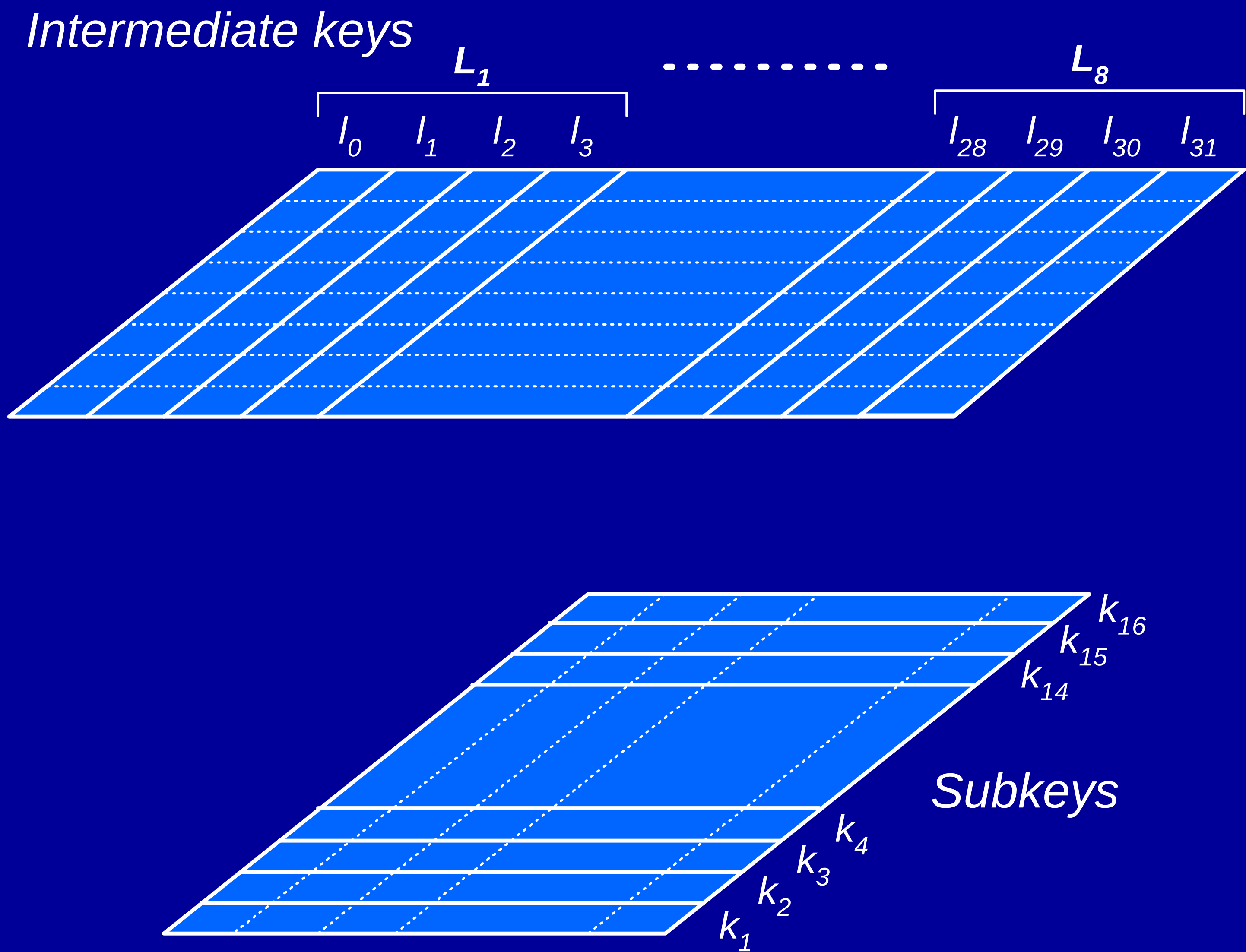


Key Scheduling Part (1)



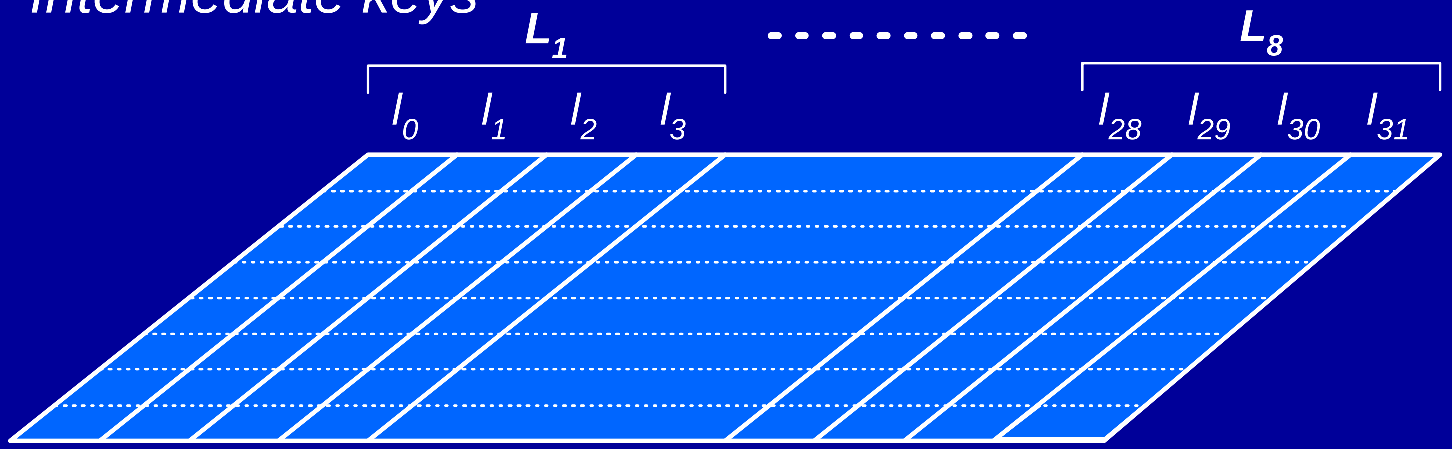
All bits of master key equally influence all bits of subkeys

Key Scheduling Part (2)

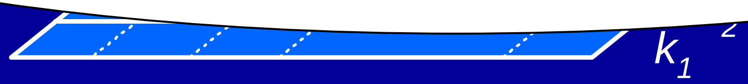


Key Scheduling Part (2)

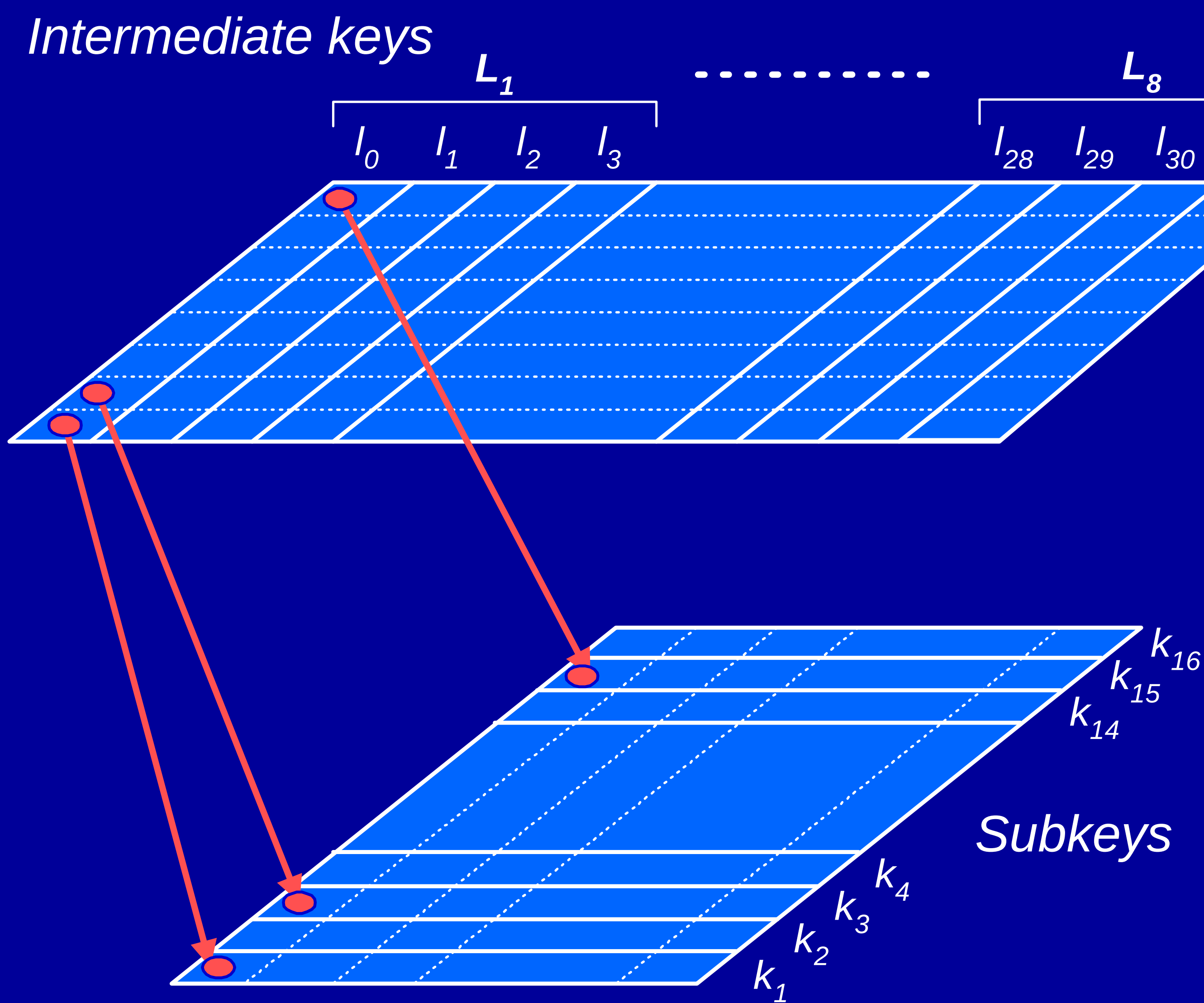
Intermediate keys



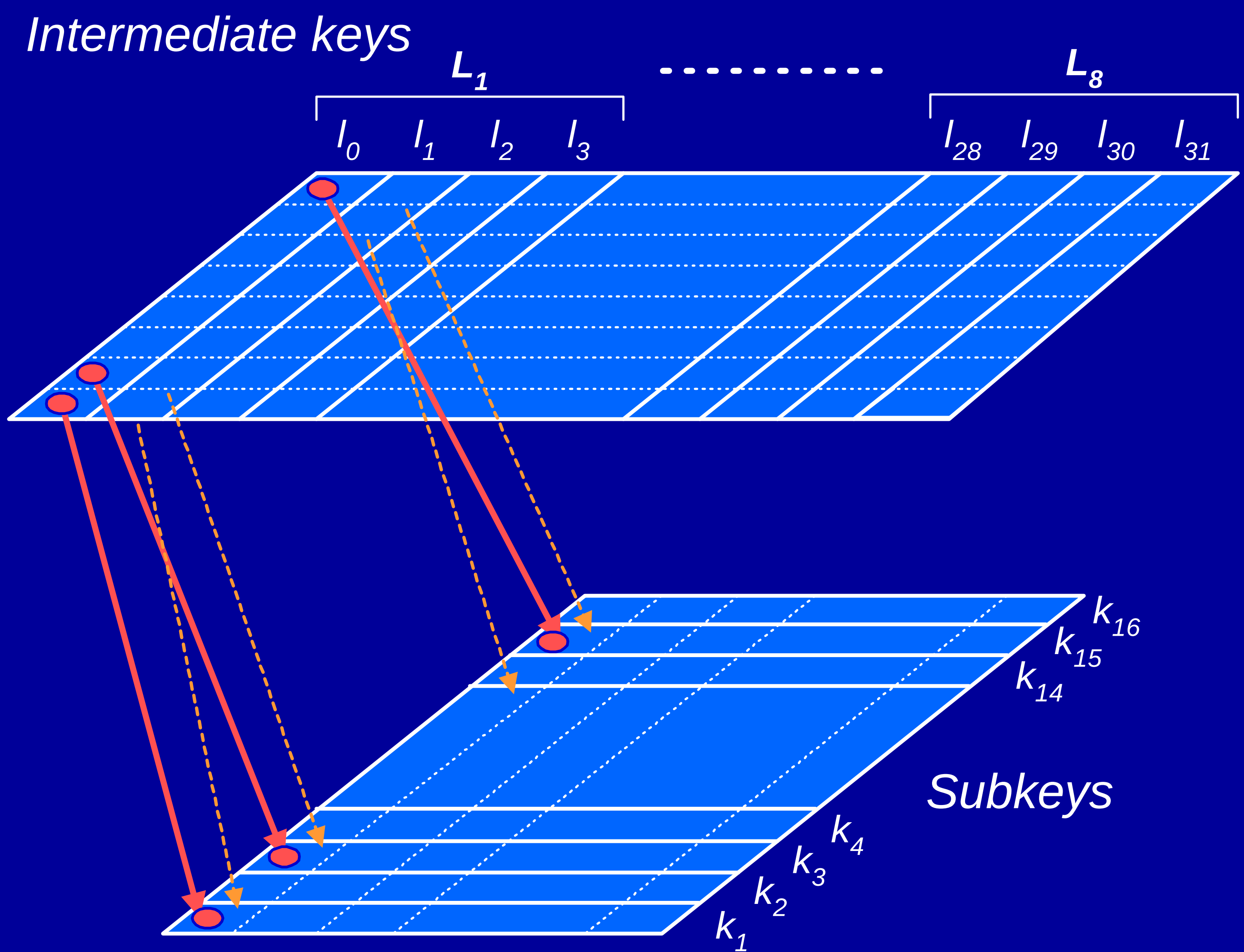
Deriving subkeys or master key from other subkeys is computationally infeasible



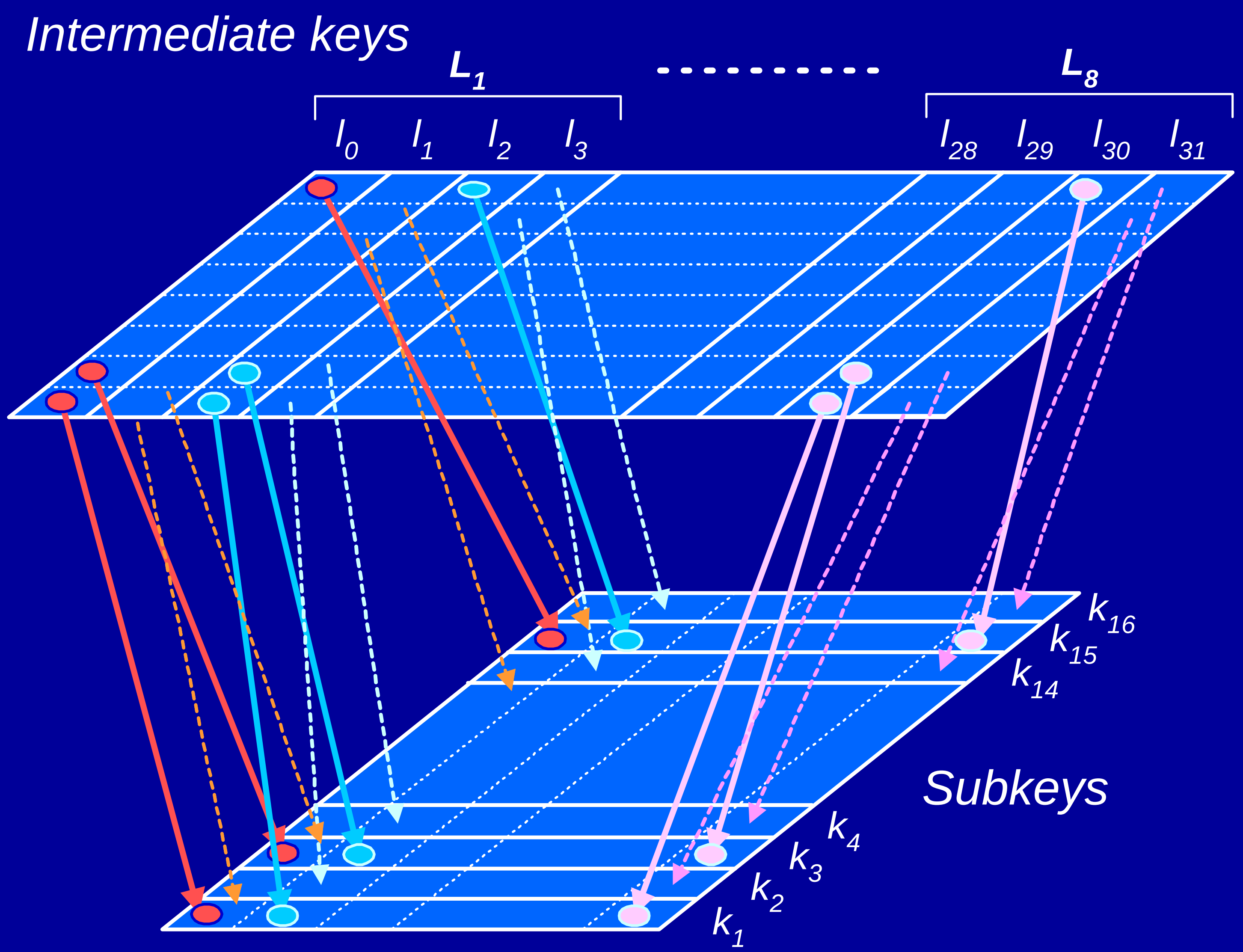
Key Scheduling Part (2)



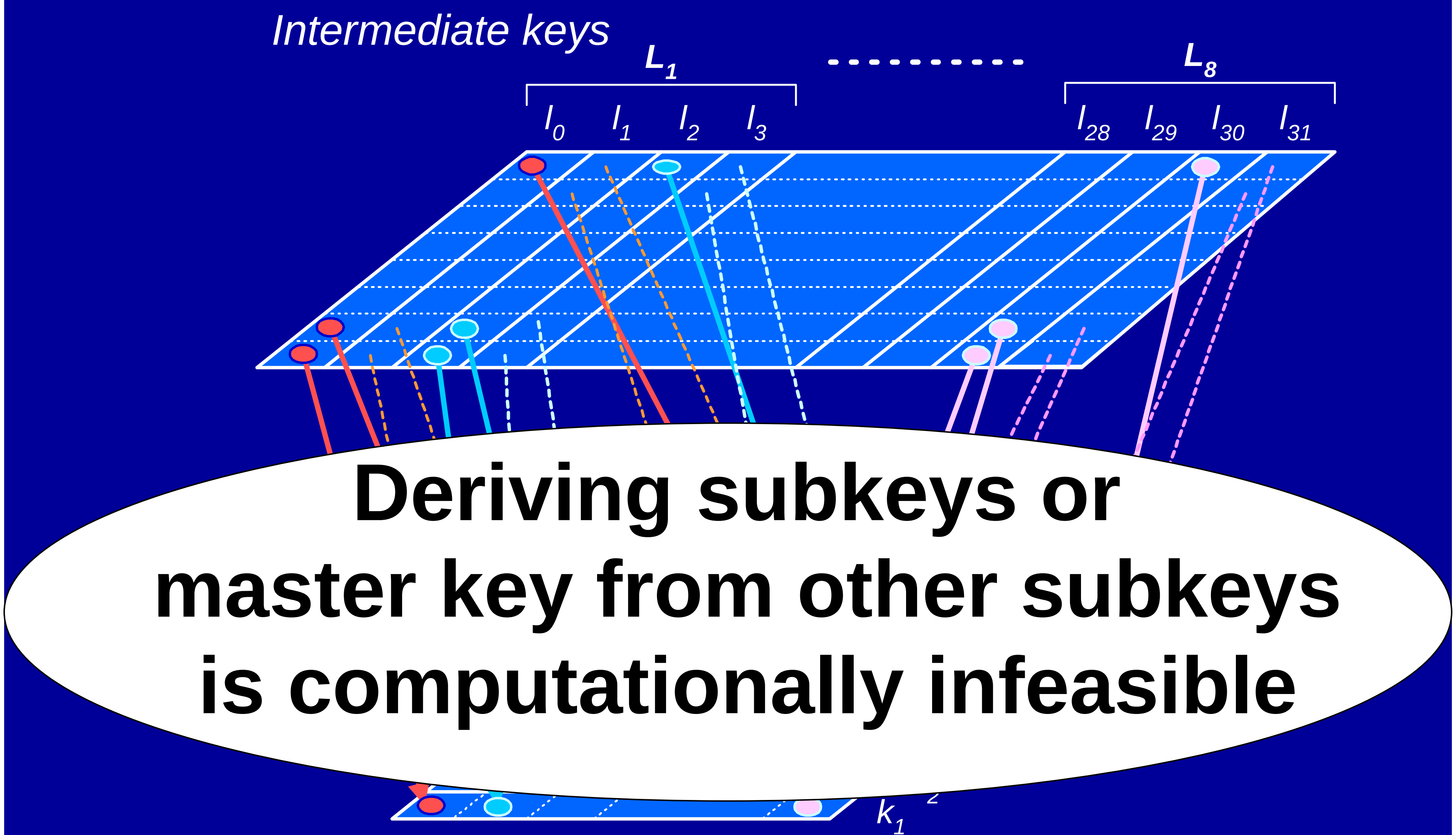
Key Scheduling Part (2)



Key Scheduling Part (2)



Key Scheduling Part (2)



Outline

- Overview
- Design
- <u>Security</u>
- Performance
- Conclusion

E2

Security of Data Randomizing Part

- *s*-box is designed to provide reasonable security against
  - Differential cryptanalysis
  - Linear cryptanalysis
  - Higher order differential attack
  - Interpolation attack, etc.

Properties of s-box

Criteria	Value	Related Attacks
bijectivity	OK	Differential/Linear
$w_{\mathrm{H}}(a)$	$3 \leq w_{\mathrm{H}}(a) \leq 5$	—
$w_{\mathrm{H}}(b)$	$3 \leq w_{\mathrm{H}}(b) \leq 5$	—
p_s	$2^{-4.67}$	Differential
q_s	$2^{-4.38}$	Linear
r_s	$2^{-2.59}$	(Differential-linear)
deg s	7	Higher order differential
$\mathrm{coeff}_{2^8}\ s$	254	Interpolation
$\mathrm{coeff}_{\mathbf{p}}\ s$	254	Interpolation

p : prime, 256 < **p** < 512

Security of Data Randomizing Part (cont.)

- *s*-box is designed to provide reasonable security against DC, LC, higher order differential attack, interpolation attack, etc.
- 9-round *E2* without *IT* / *FT*-Functions has sufficient security against DC and LC
- *IT* / *FT*-Functions are added for “insurance policy”
  - *E2* has 3-round margin + *IT* / *FT*-Functions

Security of Key Scheduling Part

- No known weak keys
- No known equivalent keys
- No known complementation properties

Outline

- Overview
- Design
- Security
- <u>Performance</u>
- Conclusion

E2

Current Software Performance

Platform	Language	Key length (bits)	Key setup (clocks)	Encryption Decryption (clocks/block)	(bits/sec)
Intel Pentium Pro (200MHz)	ANSI C (Borland C++5.02)	128 192 256	2,076 2,291 2,484	711	36.0 M
	Assembly	all	——	420	61.0 M
Hitachi H8 / 300 (5MHz) 8bit CPU for smart card	Assembly	128 192 256	14,041 15,284 16,518	6,374	100.5 k
DEC 21164A (600MHz)	Assembly	all	——	600	128.0 M

E2 **requires no algorithm setup.**
The results contain no API overhead.

Current Hardware Performance

- CMOS 0.25 μm cell based library
- 1 Gbits/sec (typical)
- 482 Mbits/sec
- Total 127k gates
  - including key scheduling, control logic and buffers
- Not fully optimized

Outline

- Overview
- Design
- Security
- Performance
- <u>Conclusion</u>

E2

Conclusion

E2 is

Conclusion

E2 is

- Secure : secure against all known attacks with enough margin

Conclusion

E2 is

- Secure : secure against all known attacks with enough margin
- Fast : faster than DES

Conclusion

E2 is

- Secure : secure against all known attacks with enough margin
- Fast : faster than DES
- Flexible: efficient implementations on various platforms

E2 Home Page

http://info.isl.ntt.co.jp/e2/

Latest information is available.

e-mail: e2@isl.ntt.co.jp