CAST-256

A Submission for the Advanced Encryption Standard

Carlisle Adams
First AES Candidate Conference
August 20-22, 1998

Orchestrating Enterprise Security

“Vital Statistics”

- ✦ Name
  - CAST-256
- ✦ Inventors
  - Carlisle Adams, Howard Heys, Stafford Tavares, Michael Wiener
- ✦ Key Sizes
  - 128, 160, 192, 224, 256 bits
- ✦ Block Size
  - 128 bits

Outline

- ✦ History
- ✦ Description
- ✦ Analysis
- ✦ "Features and Advantages"
- ✦ Conclusions

History

- 1985-86
  - Advice: “don’t go into crypto.; no future”
- 1988-90
  - design procedure for symmetric ciphers
    - Boolean functions, s-boxes, round functions, key scheduling, overall framework
- 1992-93
  - the name “CAST” introduced
  - specification of various parameters
  - CAST-1, CAST-2 in first Entrust product

History (cont'd)

✦ 1993-95

- modified key schedule: CAST-3
- further concentration on round function
- further concentration on s-box design, efficient (networked) construction
  - preliminary s-boxes: CAST-4
  - final s-boxes: CAST-5
- CAST-5 published as "CAST-128"

✦ 1995-97

- draft paper distributed and on web site
- interest begins to rise

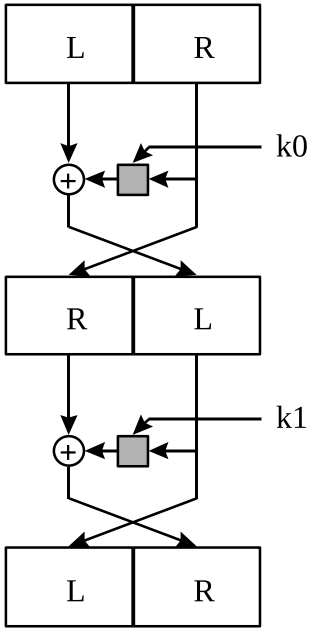
History (cont'd)

- 1997
  - CAST paper published (DCC)
  - CAST-128 cipher published (RFC 2144)
  - interest rises significantly
- 1997-98
  - CAST-128 used to form basis of CAST-256
- 1998
  - CSE endorsement of CAST-128
  - CAST-256 submitted as AES candidate

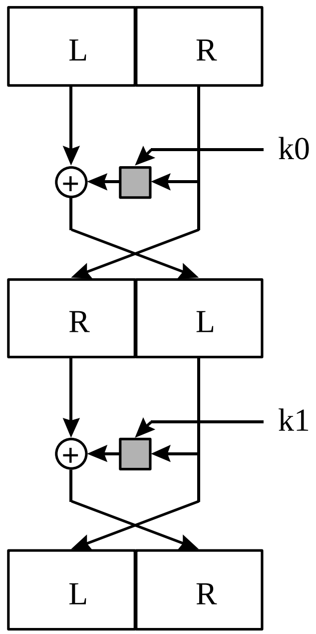
Description

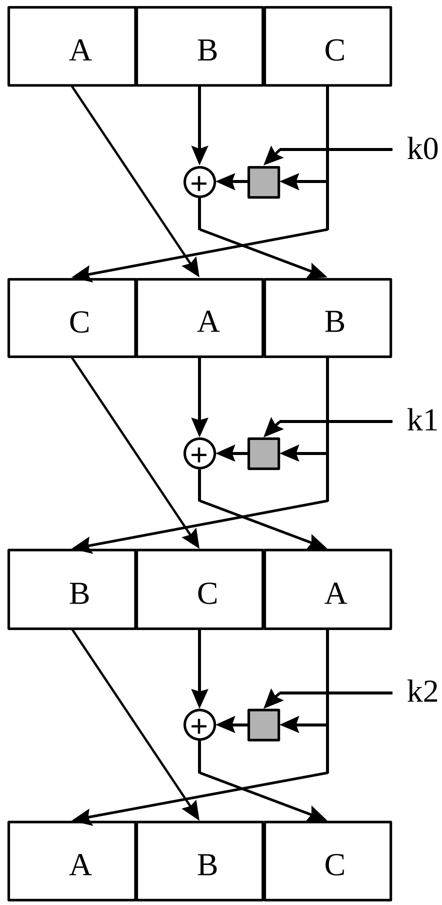
- Based on CAST-128
  - identical round function
- Expansion to 128-bit block
  - simple generalization of Feistel structure
- Expansion to 256-bit key
  - uses encryption (256-bit block) to generate round keys

Feistel Network

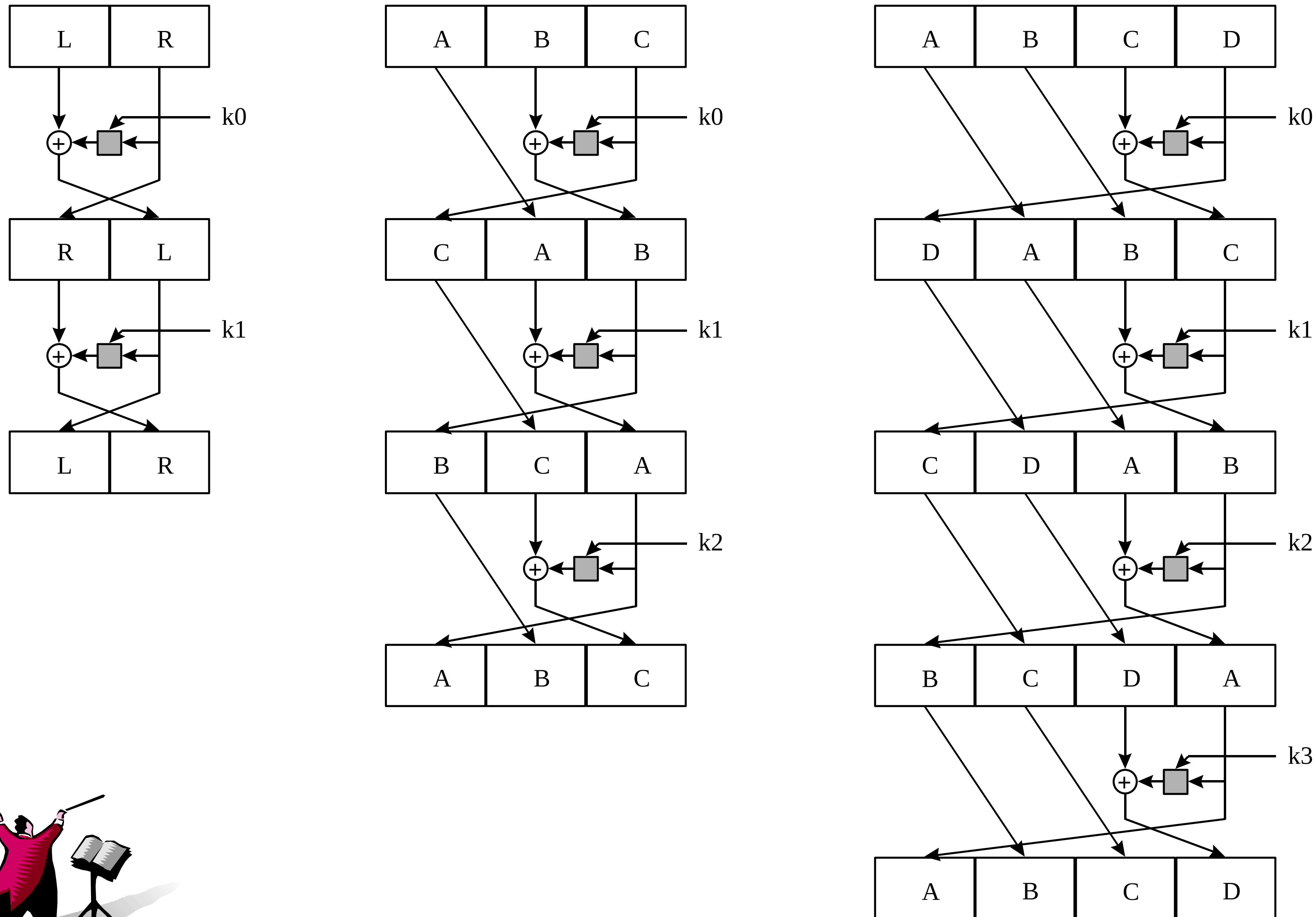


“Incomplete” Feistel Network





“Incomplete” Feistel Network



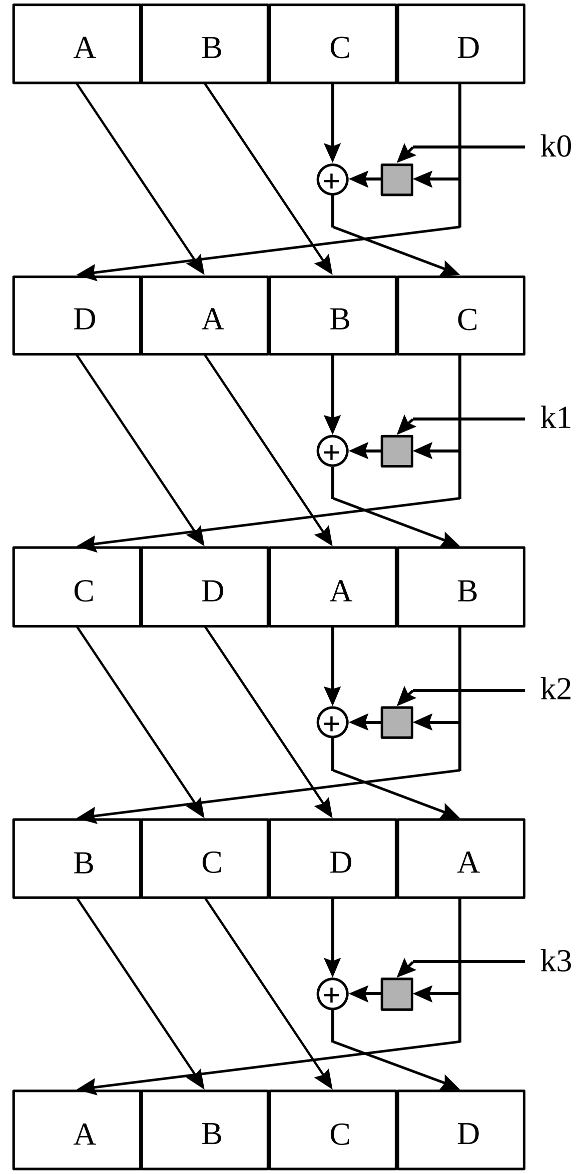
CAST-256 Notation

$$b \leftarrow Q_i(b) \quad \left\{ \begin{array}{l} C = C \oplus f_1(D, k_{r_0}{}^{(i)}, k_{m_0}{}^{(i)}) \\ B = B \oplus f_2(C, k_{r_1}{}^{(i)}, k_{m_1}{}^{(i)}) \\ A = A \oplus f_3(B, k_{r_2}{}^{(i)}, k_{m_2}{}^{(i)}) \\ D = D \oplus f_1(A, k_{r_3}{}^{(i)}, k_{m_3}{}^{(i)}) \end{array} \right.$$

"Forward Quad-Round"

$$b \leftarrow \overline{Q}_i(b) \quad \left\{ \begin{array}{l} D = D \oplus f_1(A, k_{r_3}{}^{(i)}, k_{m_3}{}^{(i)}) \\ A = A \oplus f_3(B, k_{r_2}{}^{(i)}, k_{m_2}{}^{(i)}) \\ B = B \oplus f_2(C, k_{r_1}{}^{(i)}, k_{m_1}{}^{(i)}) \\ C = C \oplus f_1(D, k_{r_0}{}^{(i)}, k_{m_0}{}^{(i)}) \end{array} \right.$$

"Reverse Quad-Round"



CAST-256 Cipher

$b =$ 128 bits of plaintext.

$$
\begin{aligned}
&for(i = 0;\ i < 6;\ i++) \\
&\qquad b \leftarrow Q_i(b) \\
&for(i = 6;\ i < 12;\ i++) \\
&\qquad b \leftarrow \overline{Q}_i(b)
\end{aligned}
$$

128 bits of ciphertext $= b$

CAST-256 Key Schedule

$$k = ABCDEFGH \quad = 256 \text{ bits of primary key, } \quad K.$$

$$
\begin{aligned}
& for\ (i = 0;\ i < 12;\ i++)\{ \\
& \qquad k \leftarrow w_{2i}(k) \\
& \qquad k \leftarrow w_{2i+1}(k) \\
& \qquad k_r^{(i)} \leftarrow k \\
& \qquad k_m^{(i)} \leftarrow k \\
& \}
\end{aligned}
$$

$$
k \leftarrow w_i(k) \left\{
\begin{aligned}
G &= G \oplus f_1(H, t_{r_0}^{(i)}, t_{m_0}^{(i)}) \\
F &= F \oplus f_2(G, t_{r_1}^{(i)}, t_{m_1}^{(i)}) \\
E &= E \oplus f_3(F, t_{r_2}^{(i)}, t_{m_2}^{(i)}) \\
D &= D \oplus f_1(E, t_{r_3}^{(i)}, t_{m_3}^{(i)}) \\
C &= C \oplus f_2(D, t_{r_4}^{(i)}, t_{m_4}^{(i)}) \\
B &= B \oplus f_3(C, t_{r_5}^{(i)}, t_{m_5}^{(i)}) \\
A &= A \oplus f_1(B, t_{r_6}^{(i)}, t_{m_6}^{(i)}) \\
H &= H \oplus f_2(A, t_{r_7}^{(i)}, t_{m_7}^{(i)})
\end{aligned}
\right.
$$

CAST-256 Key Schedule (cont'd)

$$c_m = 2^{30}\sqrt{2} = 5A827999_{16}$$
$$m_m = 2^{30}\sqrt{3} = 6ED9EBA1_{16}$$
$$c_r = 19$$
$$m_r = 17$$

$$
\begin{array}{l}
for(i = 0;\ i < 24;\ i++) \\
\quad\quad for(j = 0;\ j < 8;\ j++)\{ \\
\quad\quad\quad\quad t_{m_j}{}^{(i)} = c_m \\
\quad\quad\quad\quad c_m = (c_m + m_m) \bmod 2^{32} \\
\quad\quad\quad\quad t_{r_j}{}^{(i)} = c_r \\
\quad\quad\quad\quad c_r = (c_r + m_r) \bmod 32 \\
\quad\quad \}
\end{array}
$$

Outline

- ✦ History
- ✦ Description
- ✦ Analysis
- ✦ "Features and Advantages"
- ✦ Conclusions

Analysis

✦ *Inherited from CAST-128*

- Boolean functions
- Substitution boxes
- Key mixing per round
- Mixed operations
- Multiple round functions

Analysis

- *Inherited from CAST-128*
  - Boolean functions
  - Substitution boxes
  - Key mixing per round
  - Mixed operations
  - Multiple round functions

Boolean Functions

- ✦ "Bent" functions of 8 variables
  - highest possible nonlinearity over all binary Boolean functions (120)
  - nonlinear order of 4 (highest possible for bent functions)

Analysis

- *Inherited from CAST-128*
  - Boolean functions
  - Substitution boxes
  - Key mixing per round
  - Mixed operations
  - Multiple round functions

S-Boxes

- Properties
  - XOR difference table of 0's and 2's
  - nonlinearity of 74
  - DMOSAC = 0
  - $\text{DHOBIC}_{32,1} = 36$
  - row weight distribution: approx. binomial
  - row pair wt. distribution: approx. binomial
  - average column weight: 128

Analysis

✦ *Inherited from CAST-128*

- Boolean functions
- Substitution boxes
- Key mixing per round
- Mixed operations
- Multiple round functions

Key Mixing

- ✦ Non-surjective attack considerations
  - key entropy per round = 37 bits
- ✦ Differential, Linear considerations
  - combination of masking key, rotation key, and mixed operations for data combining

Analysis

- *Inherited from CAST-128*
  - Boolean functions
  - Substitution boxes
  - Key mixing per round
  - Mixed operations
  - Multiple round functions

Mixed Operations

- Experimental work
  - combinations of *pairs* and *triples* of s-boxes using XOR, addition, subtraction
    - examination of XOR diff. distribution table
    - significant drop in maximum entry
- Theoretical work
  - deriving probability of maximum entry exceeding a specific bound
    - supports experimental evidence

Mixed Operations (cont'd)

- ✦ Appear to
  - increase resistance to linear, differential attacks by decreasing round probability
- ✦ Appear to
  - significantly increase resistance to higher-order differential attacks

Analysis

- *Inherited from CAST-128*
  - Boolean functions
  - Substitution boxes
  - Key mixing per round
  - Mixed operations
  - Multiple round functions

Multiple Round Functions

- Appear to
  - increase complexity of constructing differential and linear characteristics
    - order of round functions precludes iteration of some low-round characteristics

Analysis (cont'd)

✦ *Particular to CAST-256*

- Generalized ("incomplete") Feistel
  - security of quad-round
  - security of "forward then reverse" quad-rounds
  - number of rounds
- Key schedule
  - security of overall structure
  - equivalent, weak, semi-weak keys

Outline

- ✦ History
- ✦ Description
- ✦ Analysis
- ✦ "Features and Advantages"
- ✦ Conclusions

“Features and Advantages”

✦ History

- CAST design procedure has been under scrutiny for almost 10 years (both public and private)
- minor weaknesses have been found
  - non-surjective attack, HOD attack

  but nothing extendable beyond 5-6 rounds
- CAST-128 has received most extensive analysis and appears to be strong
- CAST-256 inherits the strength of the round fn.

“Features and Advantages” (cont’d)

✦ Framework

- generalized Feistel structure is a clean, intuitive design that facilitates understanding and analysis
- single structure for encryption and decryption
- other blocksizes can be accommodated, if desired
- 48 rounds is a lot of rounds...!

“Features and Advantages” (cont’d)

✦ Key Schedule

- properties of cipher give properties of round keys (e.g., independence)
- provable non-existence of equivalent keys, unlikelihood of weak and semi-weak keys
- partial knowledge of round keys is of little help

Conclusion

- CAST-256 is a strong candidate for AES
  - performance is quite good (2/3 that of CAST-128)
  - code size and complexity are reasonable
  - multiple key sizes supported (without any change in performance)
  - multiple block sizes may also be specified
- **Thanks again** to NIST for designing and running the AES process as well as they have!