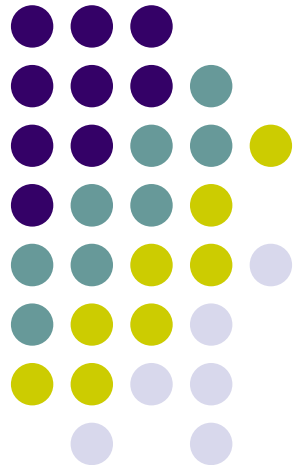
A High-Throughput Low-Power AES Cipher for Network Applications

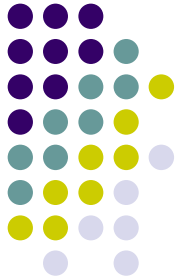
Shin-Yi Lin and Chih-Tsun Huang

ASPDAC 2007

Department of Computer Science
National Tsing Hua University

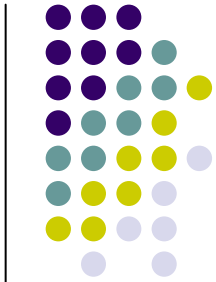


Outline



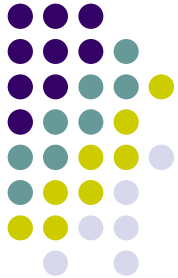
- Introduction
- AES Cryptosystem
- Supported Modes of Operations
- Our AES Architecture
  - Improved Round Function
  - Pipelined Datapath
  - Design, verification and Implementation
- Comparison and Conclusion

Motivation



- Security is the key to protect private data
- Symmetric block cipher Rijndael
  - Selected by NIST (National Institute of Standards and Technology) as the Advanced Encryption Standard (AES)
  - A wide range of applications in Internet, wireless communication, high-speed serial link, etc.
- High-throughput security
  - Serial ATA interface: 1.2Gbps ~ 4.8Gbps
  - Wireless LAN is expected to reach 1Gbps by 2008
- High-throughput comprehensive AES cipher core
  - To fulfill the security needs of widespread network applications
    - Different key sizes in the standard
    - Various popular modes of operations

AES Block Cipher



- AES algorithm:
  - Encryption and decryption procedure
  - Key expansion procedure
- Size of input/output block: 128 bits

a_{00}	a_{01}	a_{02}	a_{03}
a_{10}	a_{11}	a_{12}	a_{13}
a_{20}	a_{21}	a_{22}	a_{23}
a_{30}	a_{31}	a_{32}	a_{33}

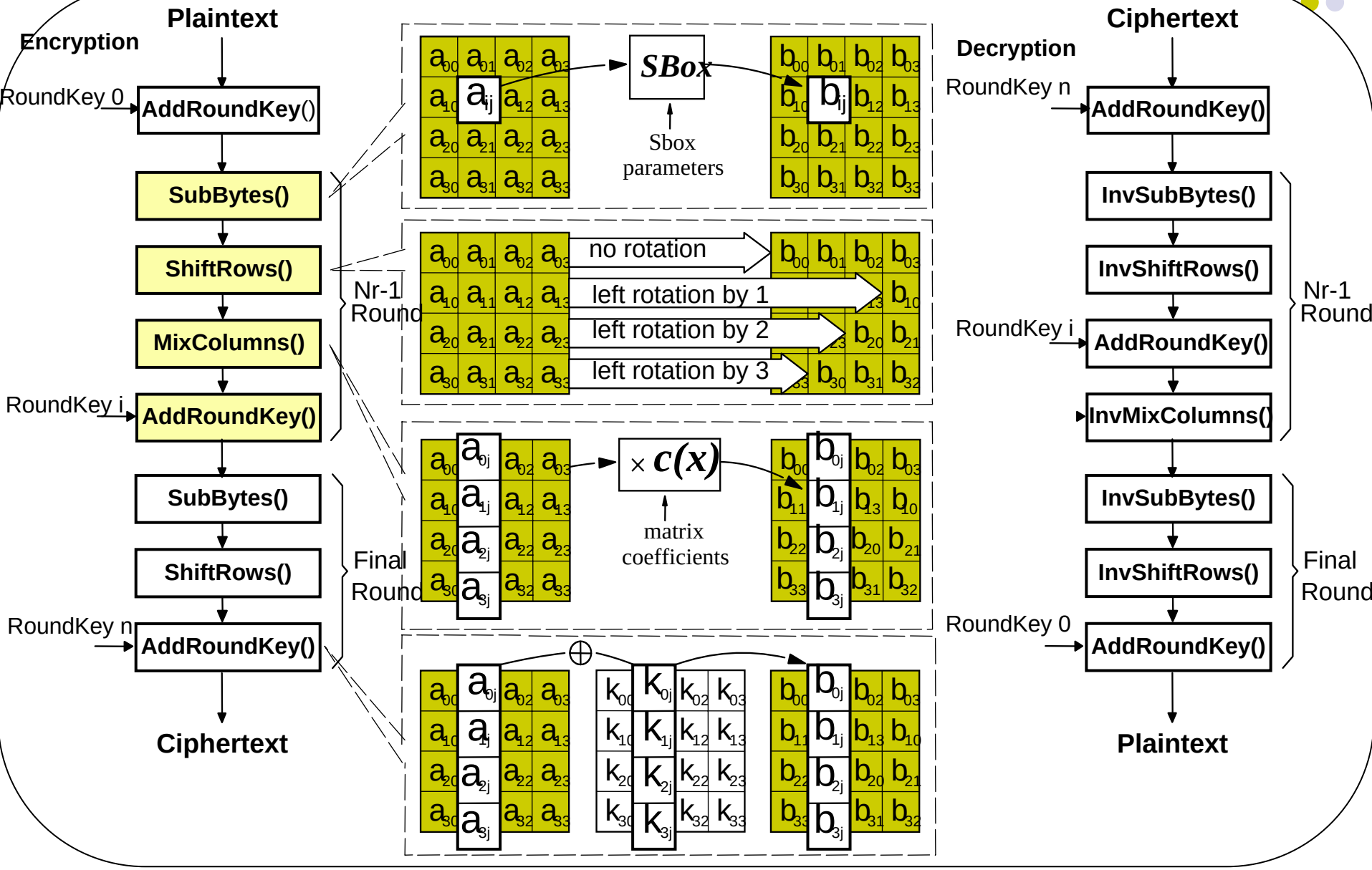
State

K_{00}	K_{01}	K_{02}	K_{03}	K_{04}	K_{05}	K_{06}	K_{07}
K_{10}	K_{11}	K_{12}	K_{13}	K_{14}	K_{15}	K_{16}	K_{17}
K_{20}	K_{21}	K_{22}	K_{23}	K_{24}	K_{25}	K_{26}	K_{27}
K_{30}	K_{31}	K_{32}	K_{33}	K_{34}	K_{35}	K_{36}	K_{37}

Key

- Length of Initial Key: 128, 192, 256 bits
- Iterations (rounds) of process : 10, 12, or 14

Encryption/Decryption Flow

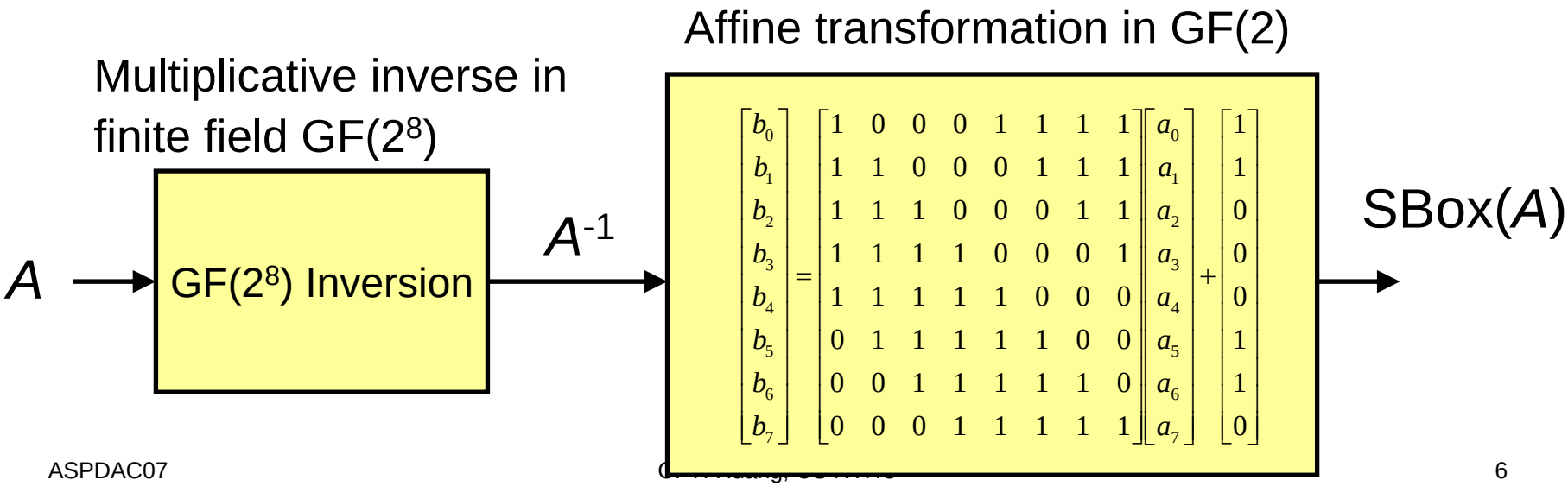


Sub-Bytes (S-Box) Transformation

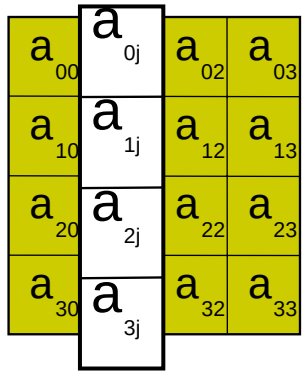
- A non-linear byte substitution

$$\mathrm{SBox}(A) = \left(\mathrm{Affine}(x) \bullet A^{-1}(x) + \mathrm{const}(x)\right) \bmod x^8 + 1$$

  - A: A byte in the State
  - Irreducible polynomial $p(x) = x^8 + x^4 + x^3 + x + 1$
  - $Affine(x) = x^4 + x^3 + x^2 + x + 1$
  - $const(x) = x^6 + x^5 + x + 1$



MixColumns Transformation



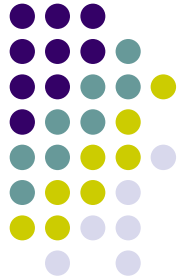
- Column-wise modular-multiplication of a column in the State and a fixed polynomial
  - Coefficients of the polynomials are considered as the elements in GF(2^8)

$$b_j(x) = a_j(x) \bullet c(x) \mod (x^4+1),\ 0 \le j \le 3$$

$$c(x)=\{03\}_x x^3+\{01\}_x x^2+\{01\}_x x+\{02\}_x$$

$$\begin{bmatrix} b_{0j} \\ b_{1j} \\ b_{2j} \\ b_{3j} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} a_{0j} \\ a_{1j} \\ a_{2j} \\ a_{3j} \end{bmatrix}$$

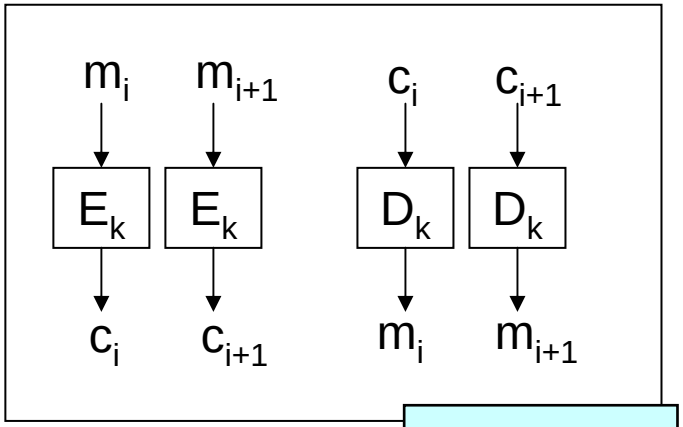
Different Operation Modes



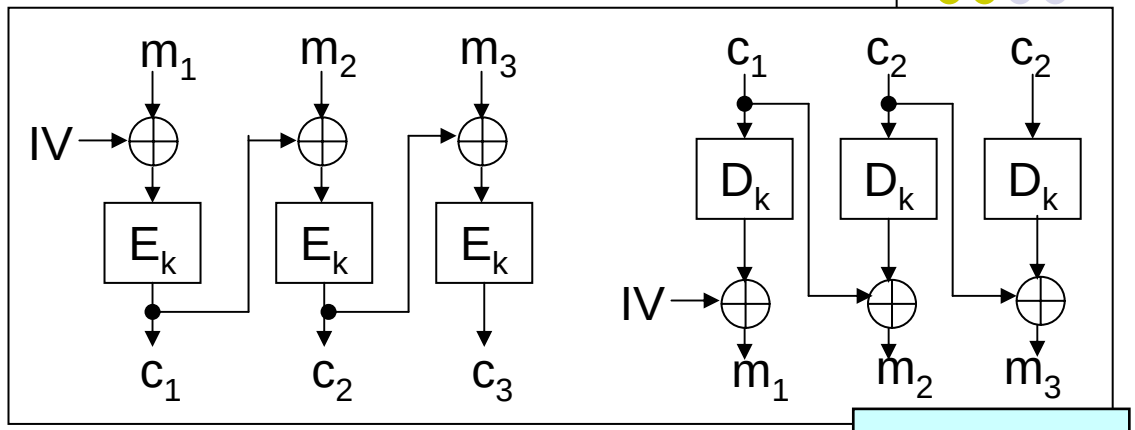
- **Confidentiality Modes**
  - Electronic Codebook (ECB) Mode
  - Cipher Block Chaining (CBC) Mode
  - Counter (CTR) Mode
- **Authenticated Encryption Mode**
  - Counter with CBC-Message Authentication Code (CCM) Mode

Confidentiality Modes

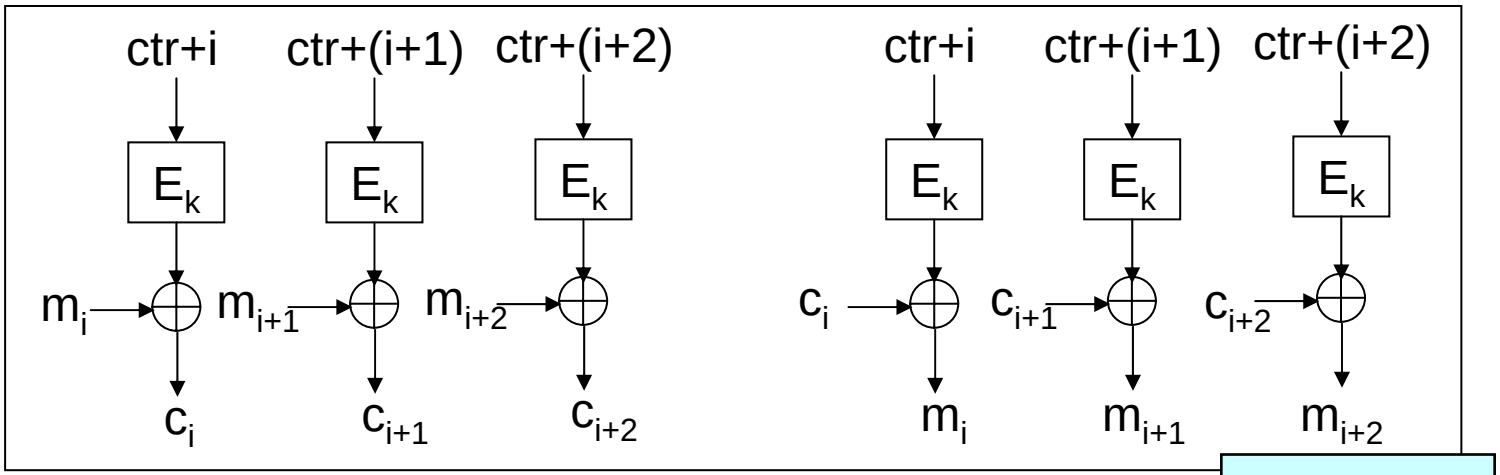
E_k: AES encryption function; D_k: AES decryption function



ECB Mode

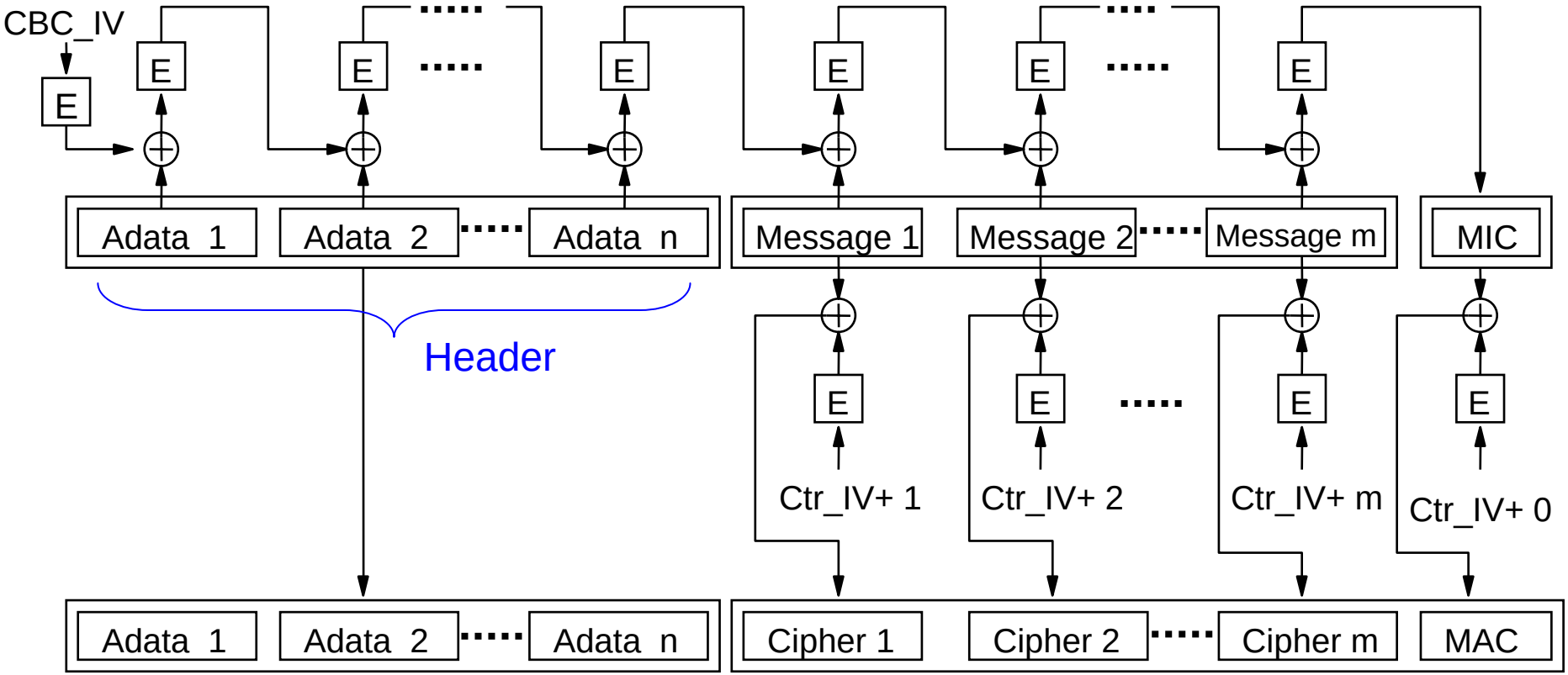


CBC Mode



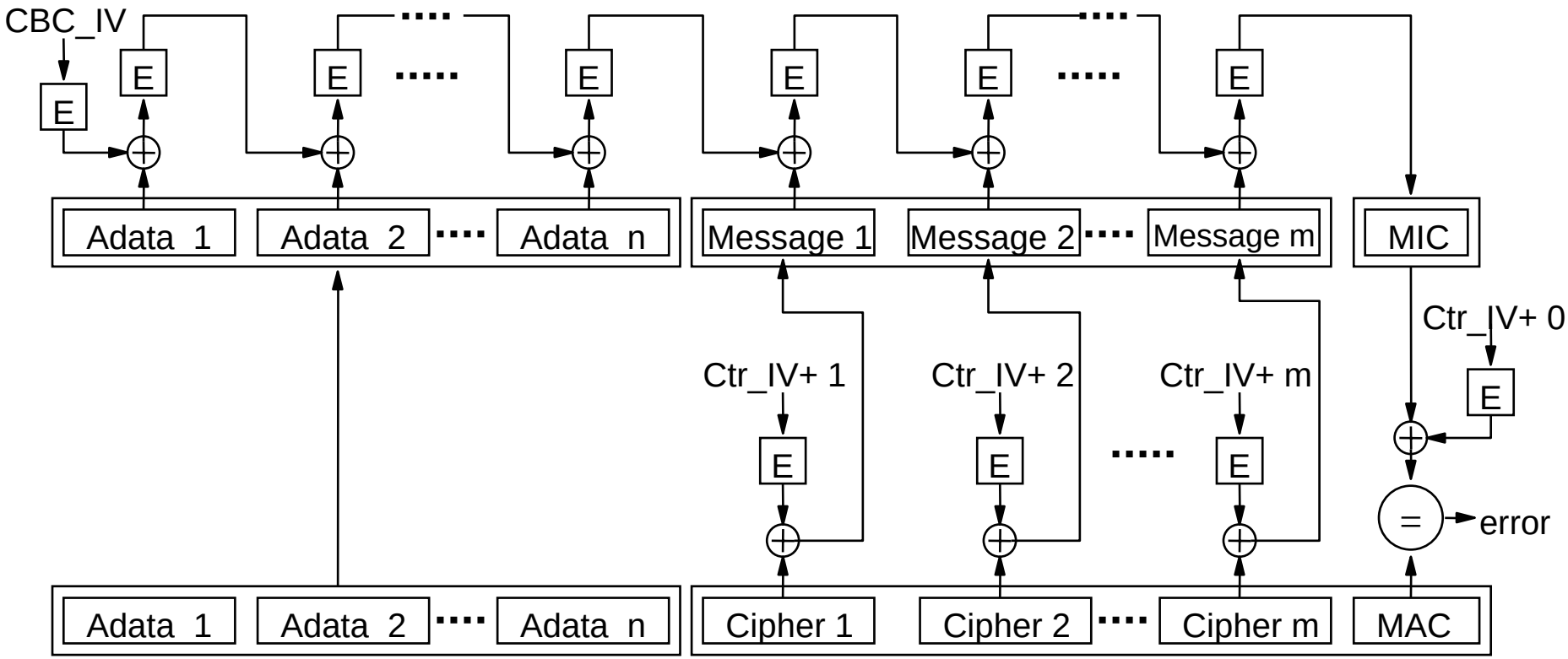
CTR Mode

CCM Encryption Procedure

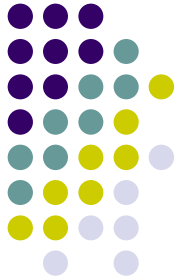


MIC: Message Integration Code
MAC: Message Authentication Code

CCM Decryption Procedure



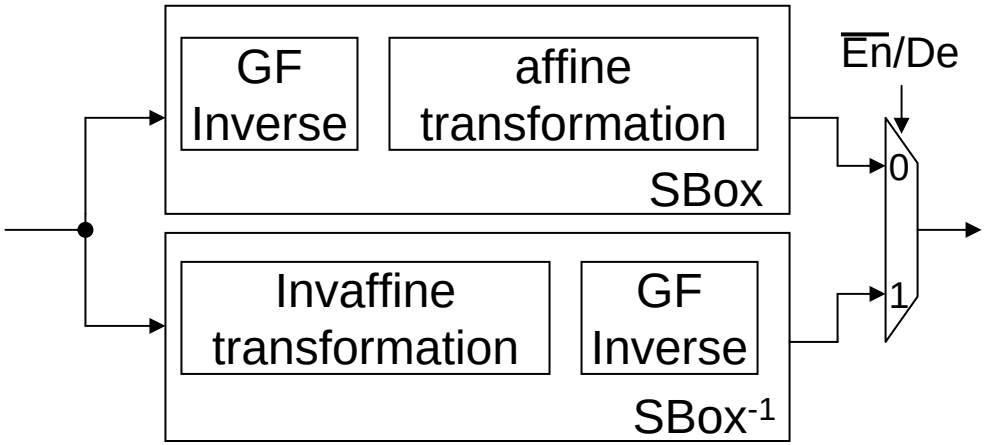
S-Box Implementation



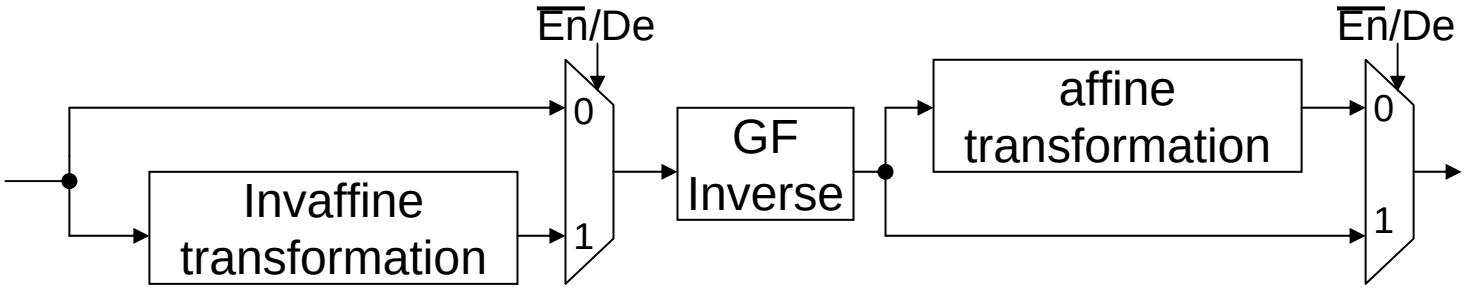
- S-Box alternatives
  - Look-up table (LUT) with 256 entries
  - GF(2^8) inverter + Affine
    - GF(2^8) arithmetic inversion
    - Composite field with GF(2^4) arithmetic operations
- Our approach
  - LUT-based GF(2^8) inverter
  - Optimized by logic synthesis (0.18μm)

Timing Constraint	4ns	3ns	2ns
Composite Field Inverter (KGates)	6.5	9.4	N/A
LUT GF Inverter (KGates)	10.4	11.7	16.5

Resource Sharing Between Encryption and Decryption



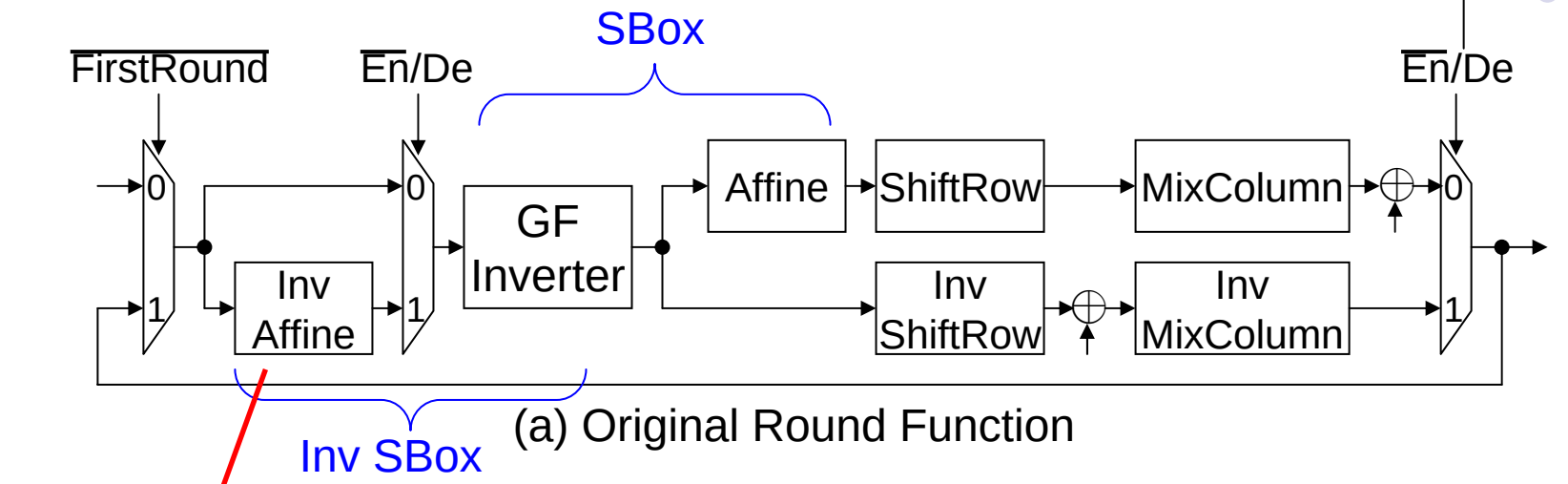
(a) Separate encryption/decryption SBox



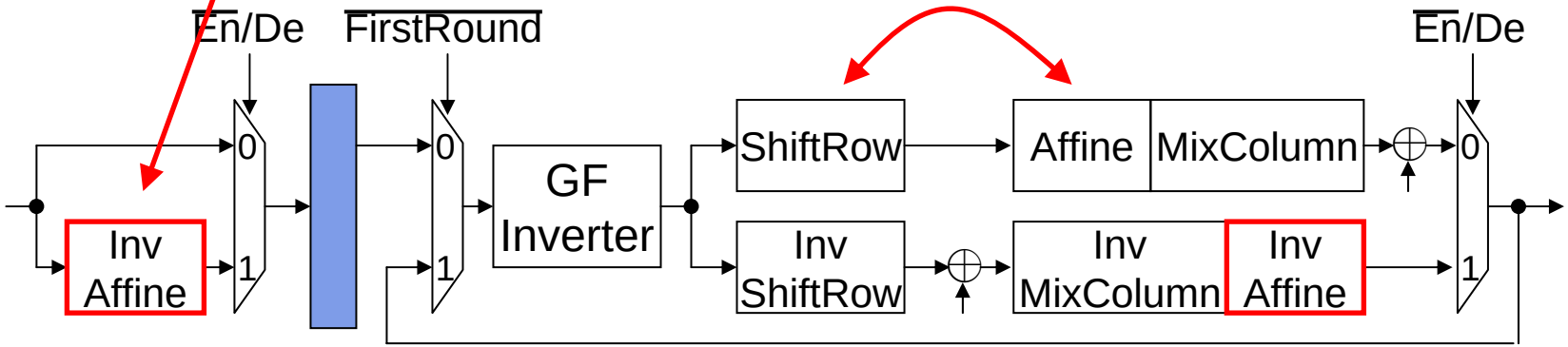
(b) Inverter-Shared SBox

Source: Satoh [7]

Round Function Retiming

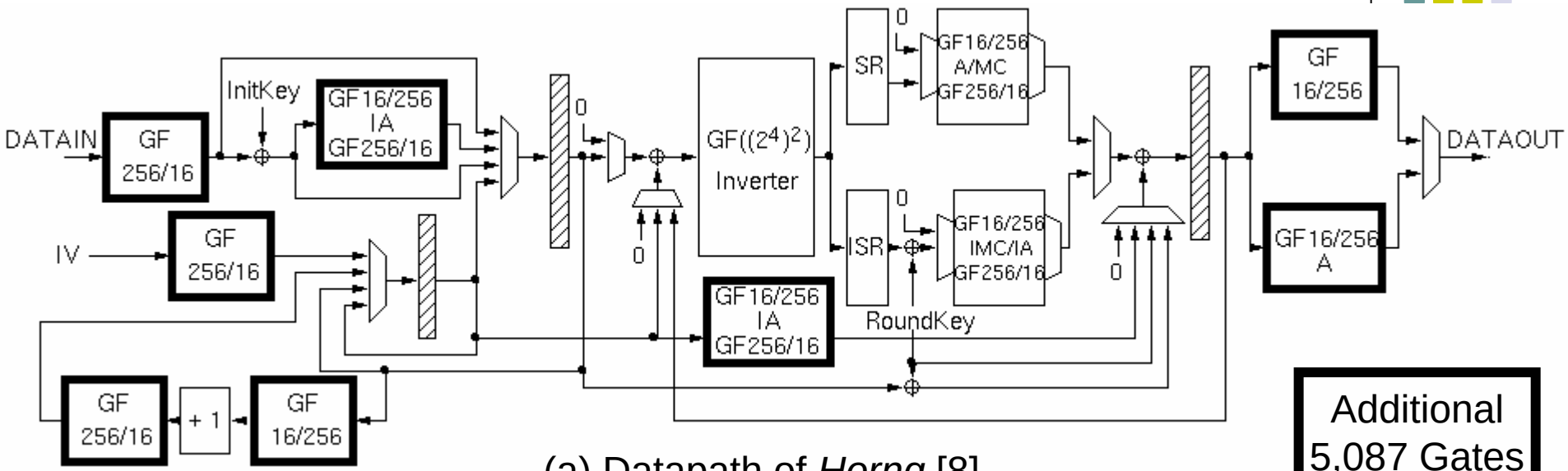


(a) Original Round Function



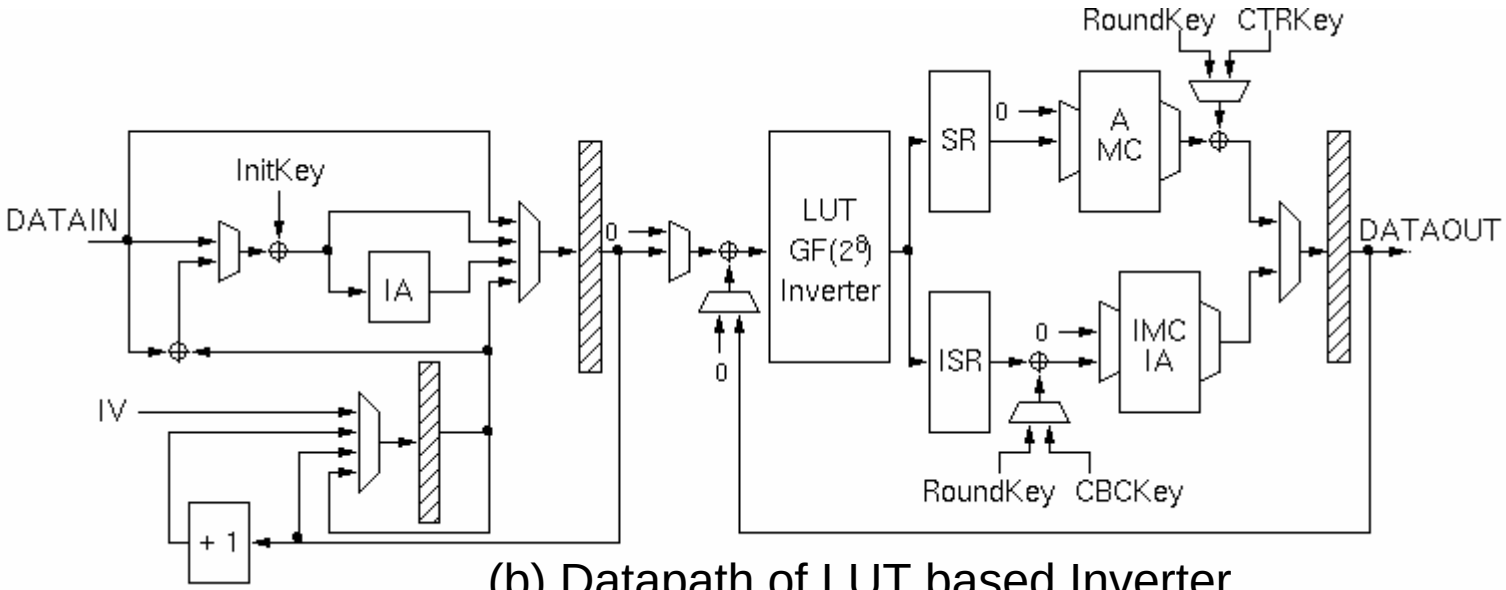
(b) Modified Round Function

Datapath Comparison



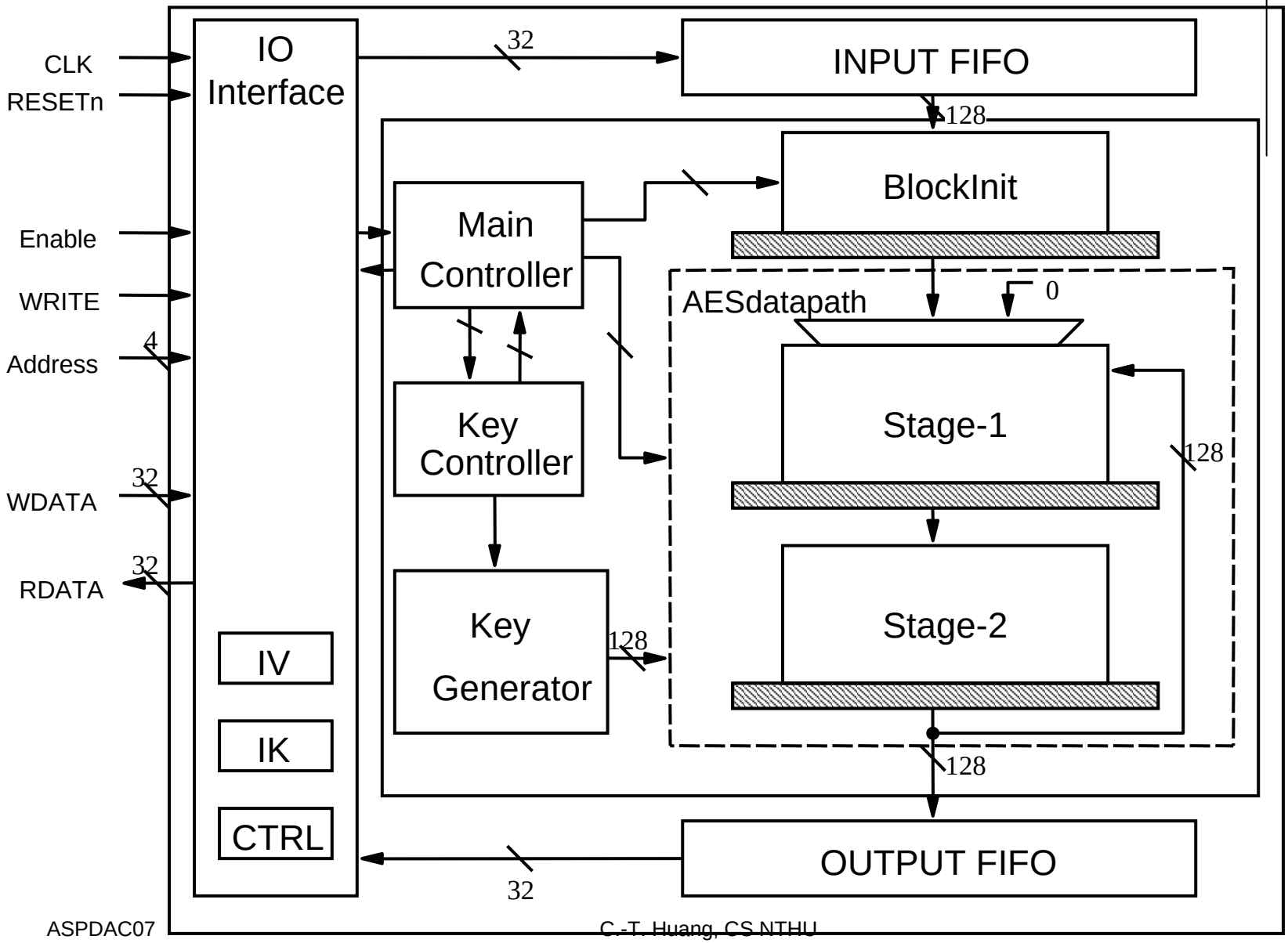
(a) Datapath of *Horng* [8]

Additional 5,087 Gates



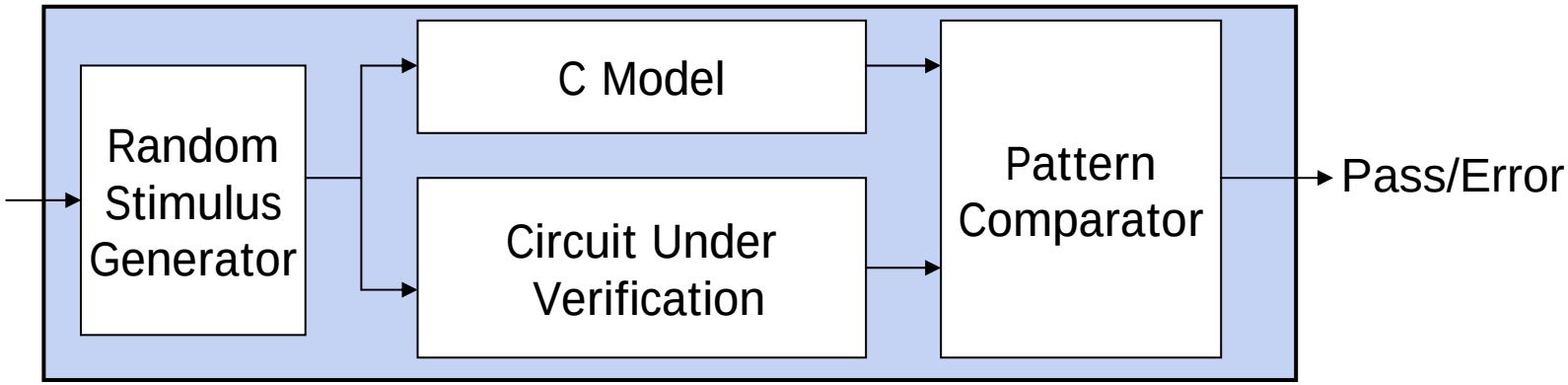
(b) Datapath of LUT based Inverter

Overall AES Arhictecture

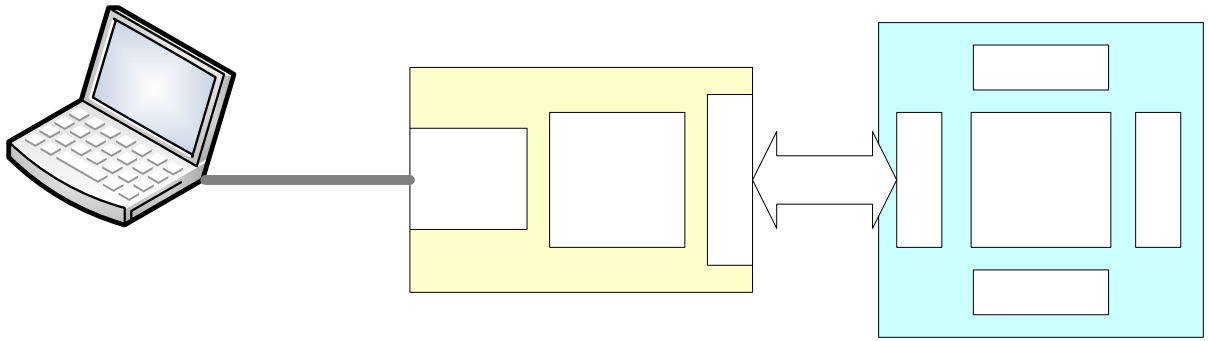


Verification

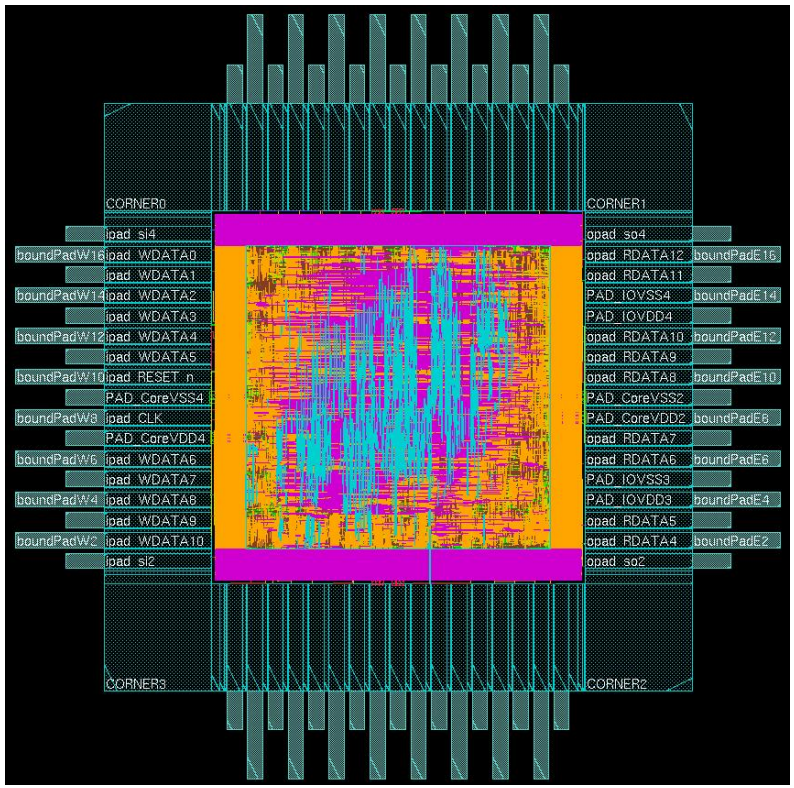
- Random Verification: over 500-million blocks



- FPGA Prototype: video streaming



ASIC Implementation and Characteristics

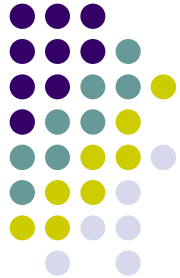


	Test Chip	Silicon IP
Technology	0.13μm	0.13μm
Area	1.82mm^2	1.06mm^2
Frequency	125MHz	333MHz
Maximum Throughput	1.6Gbps	4.27Gbps
Fault Coverage	98.38% w/ four scan chains	99.99% w/ eight scan chains

Comparison

	Kuo[4]	Su[6]	Satoh[7]	Hodjat[5]	Horng[8]	Ours
Technology	0.18	0.25	0.11	0.18	0.18	0.13
Freq. (MHz)	154	250	224	295	125	333
T: Throughput (Gbps)	1.6 1.33 1.14	2.3 2.0 1.74	2.61 (128-bit)	3.43 (128-bit)	1.6 1.33 1.14	4.27 (128-bit) 3.56 (192-bit) 3.05 (256-bit)
A: Gate Count	173K	58.4K	21.3K	73.2K	67.9K	86.2K
T/*A* (Kbps/KGate)	9.25 7.69 6.59	40.77 34.38 29.73	122.28	46.9	23.56 19.63 16.83	49.54 41.30 35.38
Power (mW)	56	230.6	N/A	86	56	40.9
Function	En	En/De	En/De	En	En/De	En/De
Modes	ECB	ECB	ECB CBC	ECB CBC CTR CCM	ECB CBC CTR	ECB CBC CTR CCM
Key Size	All	All	128	128	All	All
Pipeline	1	4	1	1	1	2

Conclusion



- A high-throughput low-power full-featured AES cipher
  - 128-, 192-, 256-bit keys
  - ECB, CBC, CTR and CCM modes
  - 2-stage pipelined datapath
    - Capable of CCM mode using single AES datapath
    - Interleaved execution of two separate data streams
  - LUT-based GF inverter
  - Sharing and retiming techniques
  - Maximum throughput is 4.27Gbps with a clock rate of 333MHz
  - Hardware cost is 86.2K gates
  - The power consumption is 40.9mW