Santa Barbara, CA, USA, 19th August 2016
Cryptographic Hardware and Embedded Systems

A High Throughput/Gate AES Hardware Architecture by Compressing Encryption and Decryption Datapaths

—Toward Efficient CBC-Mode Implementation

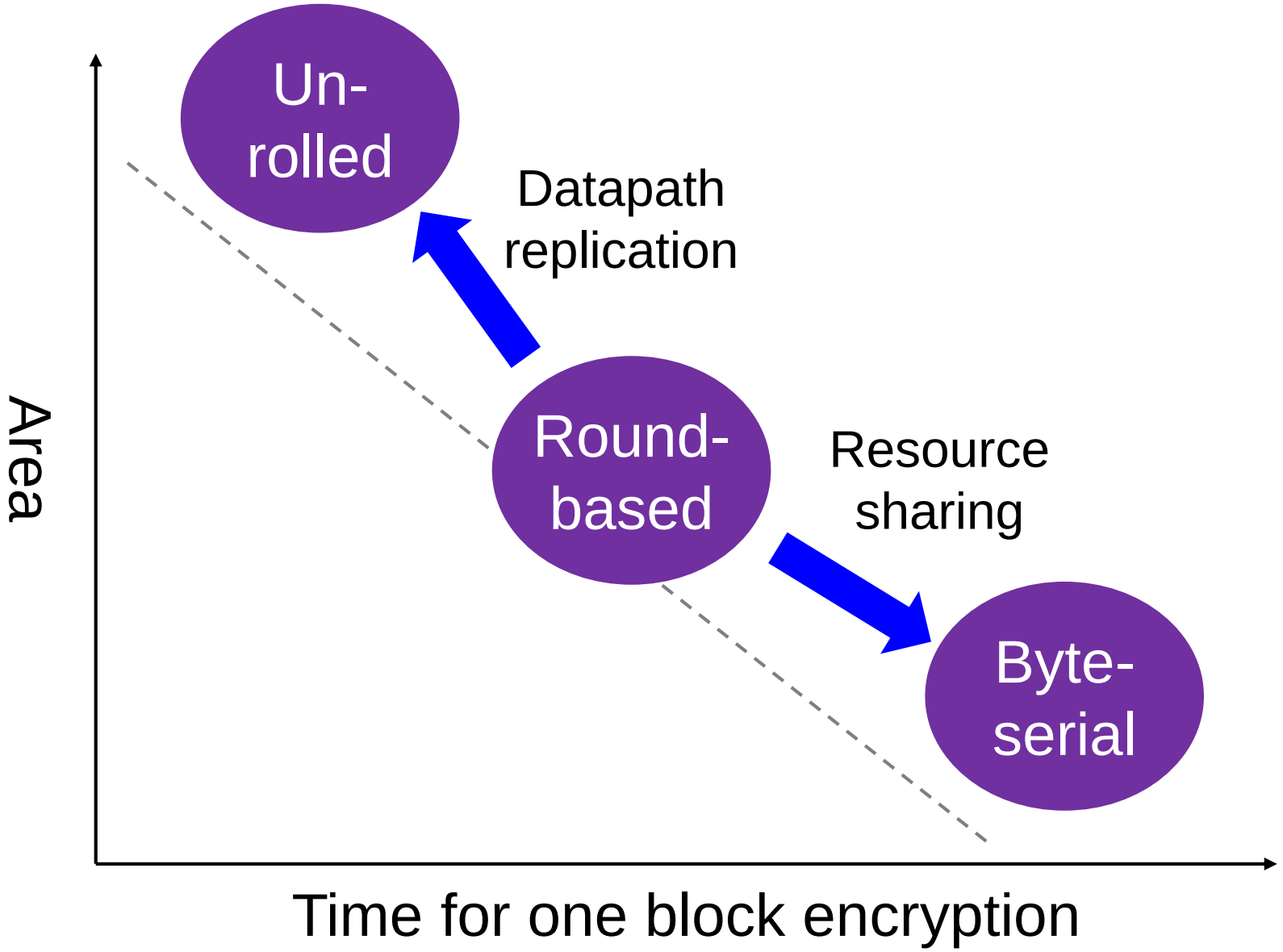
Rei Ueno[1], Sumio Morioka[2], Naofumi Homma[1], and Takafumi Aoki[1]

[1] Tohoku University and [2] NEC Central Laboratories

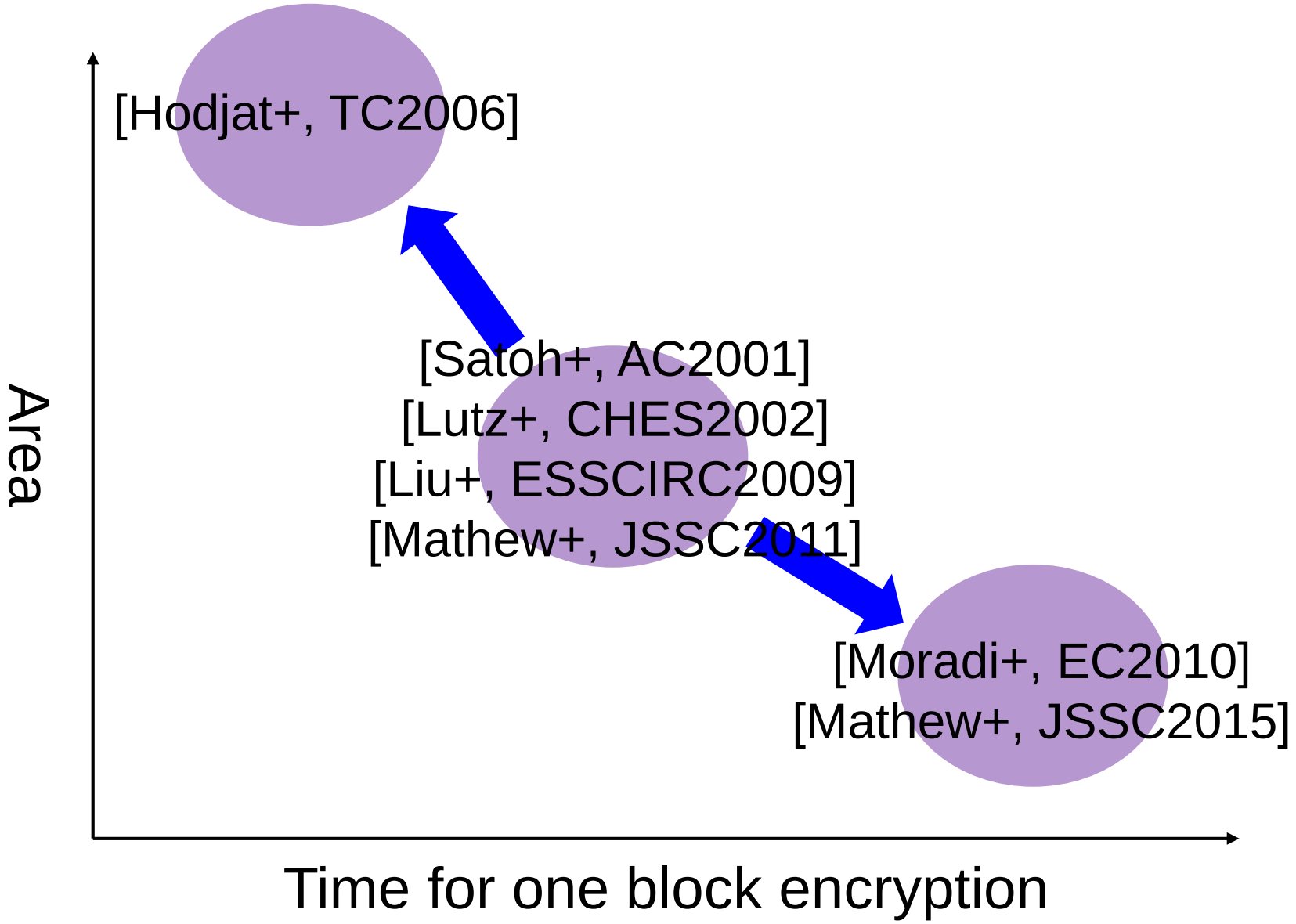
Outline

- Introduction
- Related works
- Proposed architecture
- Performance evaluation
- Concluding remarks

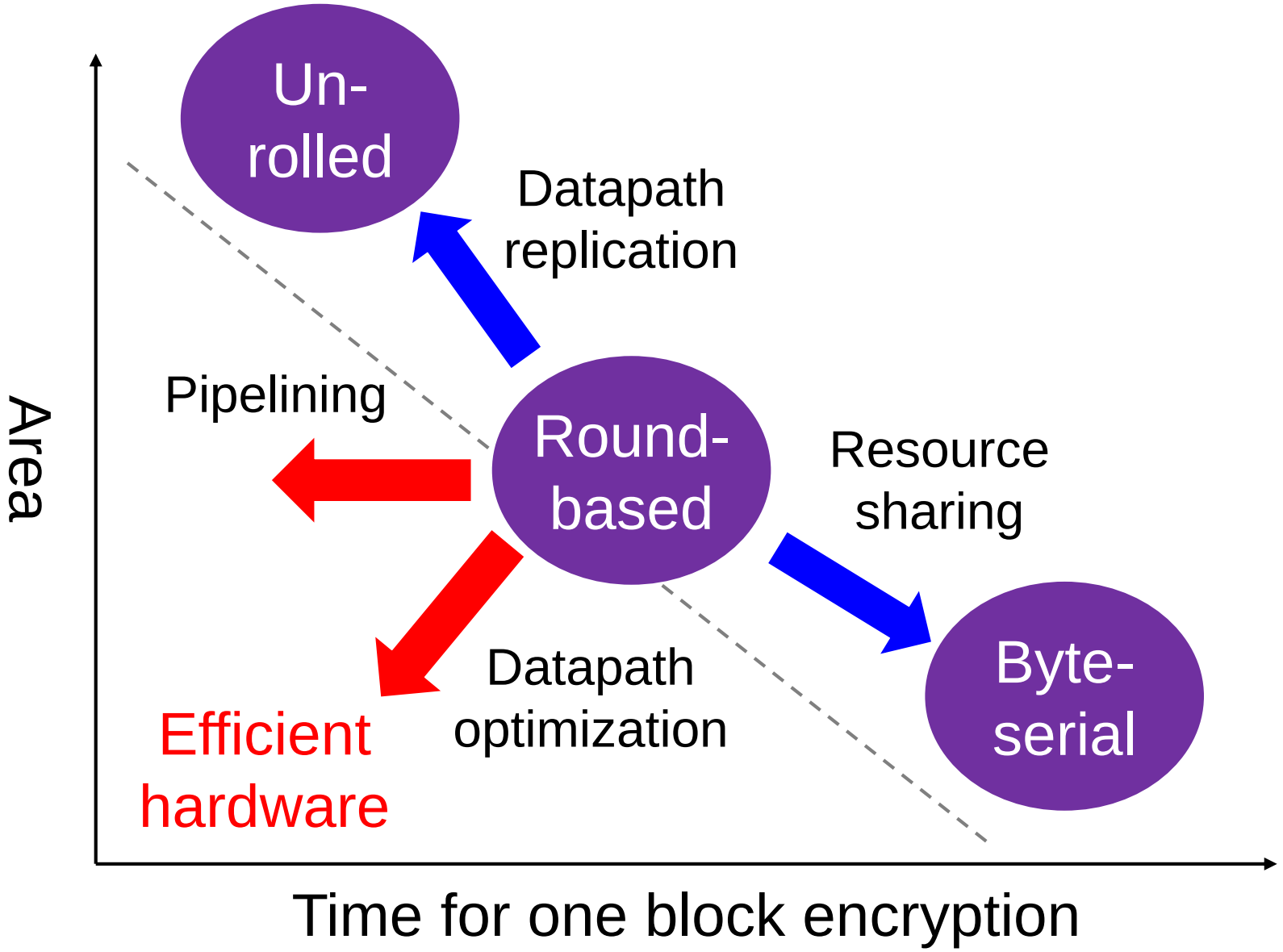
AES hardware architectures



AES hardware architectures

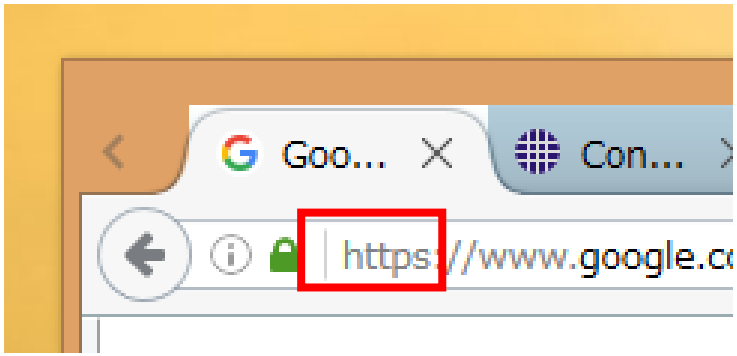


AES hardware architectures



Practical applications

- Block-chaining modes
  - CBC, CMAC, and CCM…
- Both encryption and decryption operations



SSL/TLS

802.11 WLAN

- Issue on block-wise pipelining
  - State-of-the-art AES hardware achieves 53Gbps, but works only on ECB or CTR mode [Mathew+ JSSC2011]
  - Higher throughput ≠ Lower-latency

This work

- Most area-time efficient AES HW architecture
  - Achieve lowest-latency with tower-field inversion
    - Can perform CBC mode most efficiently
  - Support both encryption and decryption
  - Unified on-the-fly key scheduling datapath

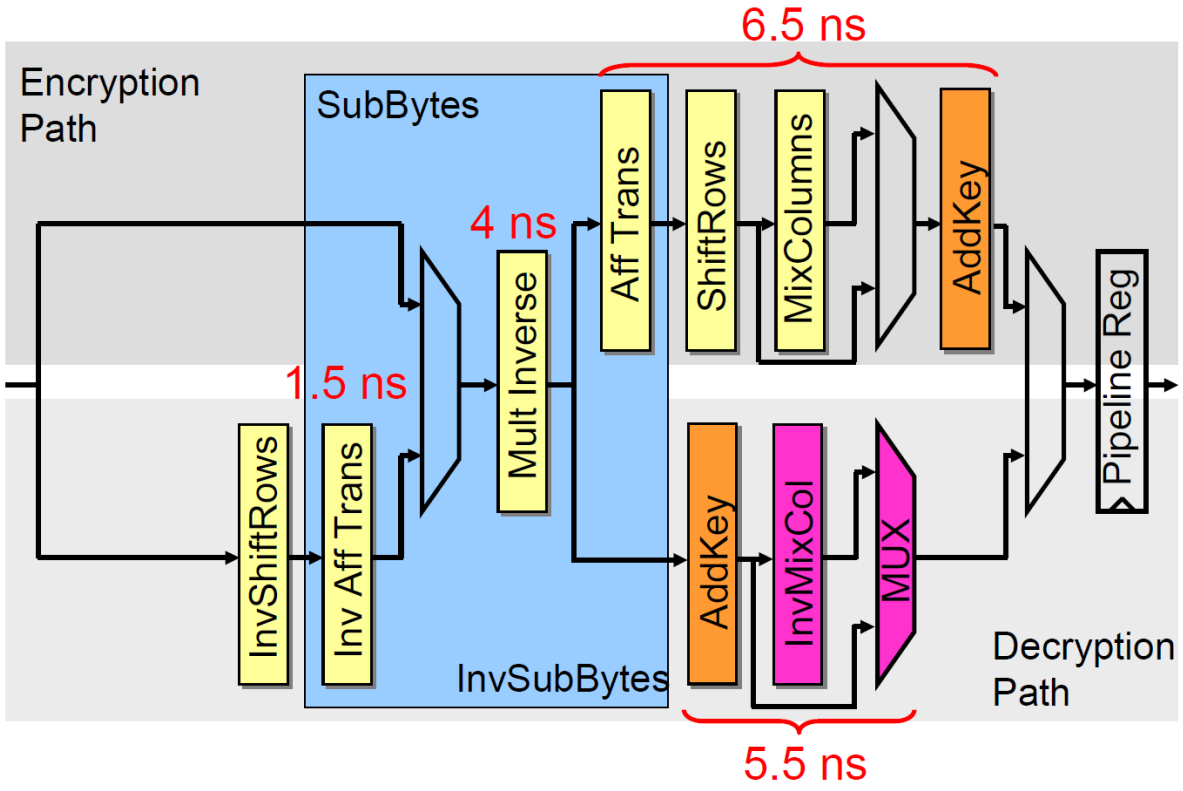
- Results
  - Logic synthesis with three standard CMOS technologies
    - 44-72% higher throughput/gate than conventional ones
  - Power estimation using gate-level dynamic simulation
    - Lowest-energy than ever before

Outline

- Introduction
- Related works
- Proposed architecture
- Performance evaluation
- Concluding remarks

Conventional architecture 1/2 [Lutz+, CHES 2002]

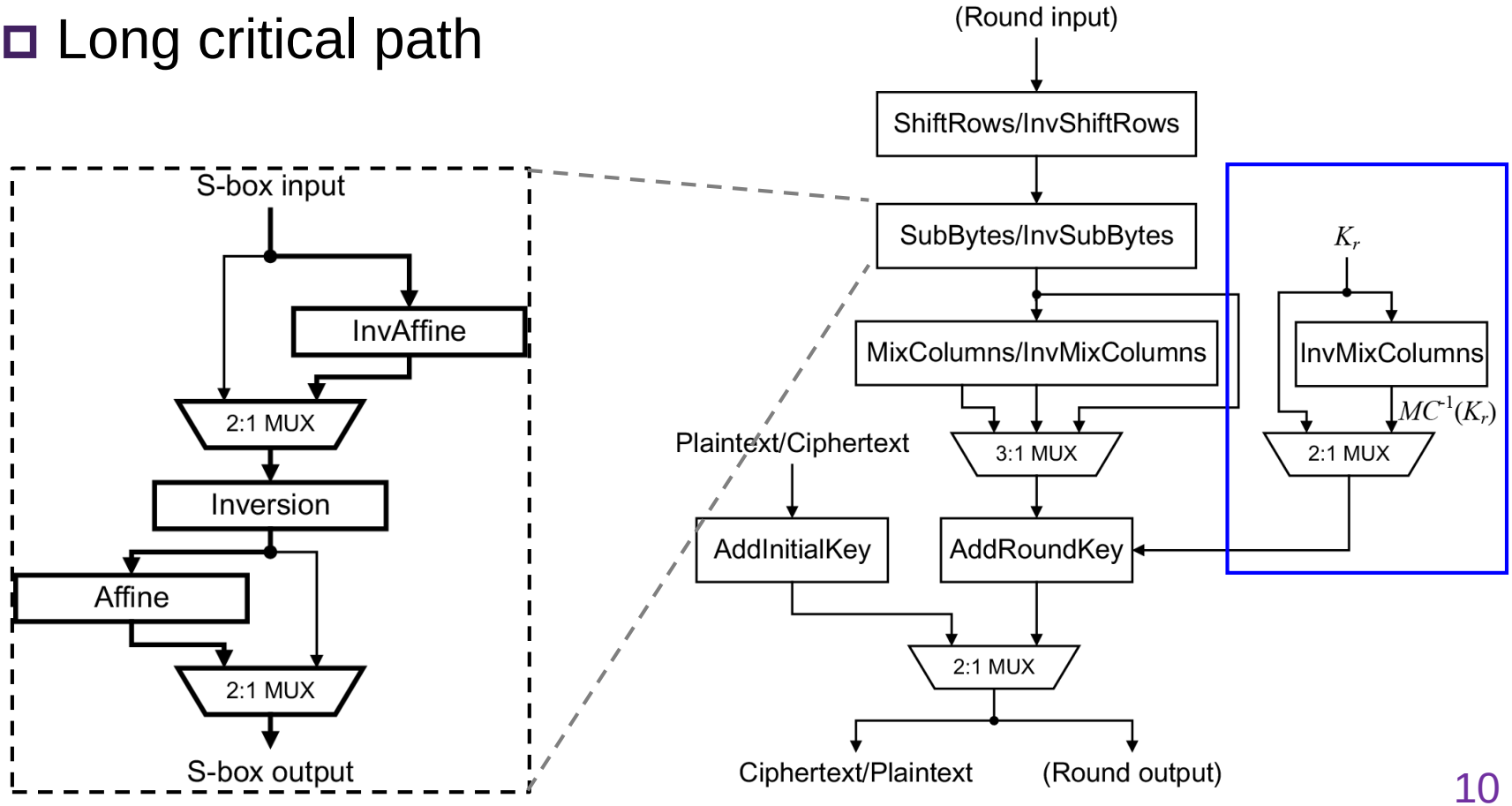
- Enc and Dec datapaths with additional selectors
  - Overhead of selectors for unification is nontrivial
  - False paths appear



www.chesworkshop.org/ches2002/presentations/Lutz.pdf

Conventional architecture 2/2 [Satoh+, AC 2001]

- Unify each pair of operation and its inverse
  - RoundKey requires InvMixColumns
  - Some MUXs in unified operations
  - Long critical path



Tower-field implementation

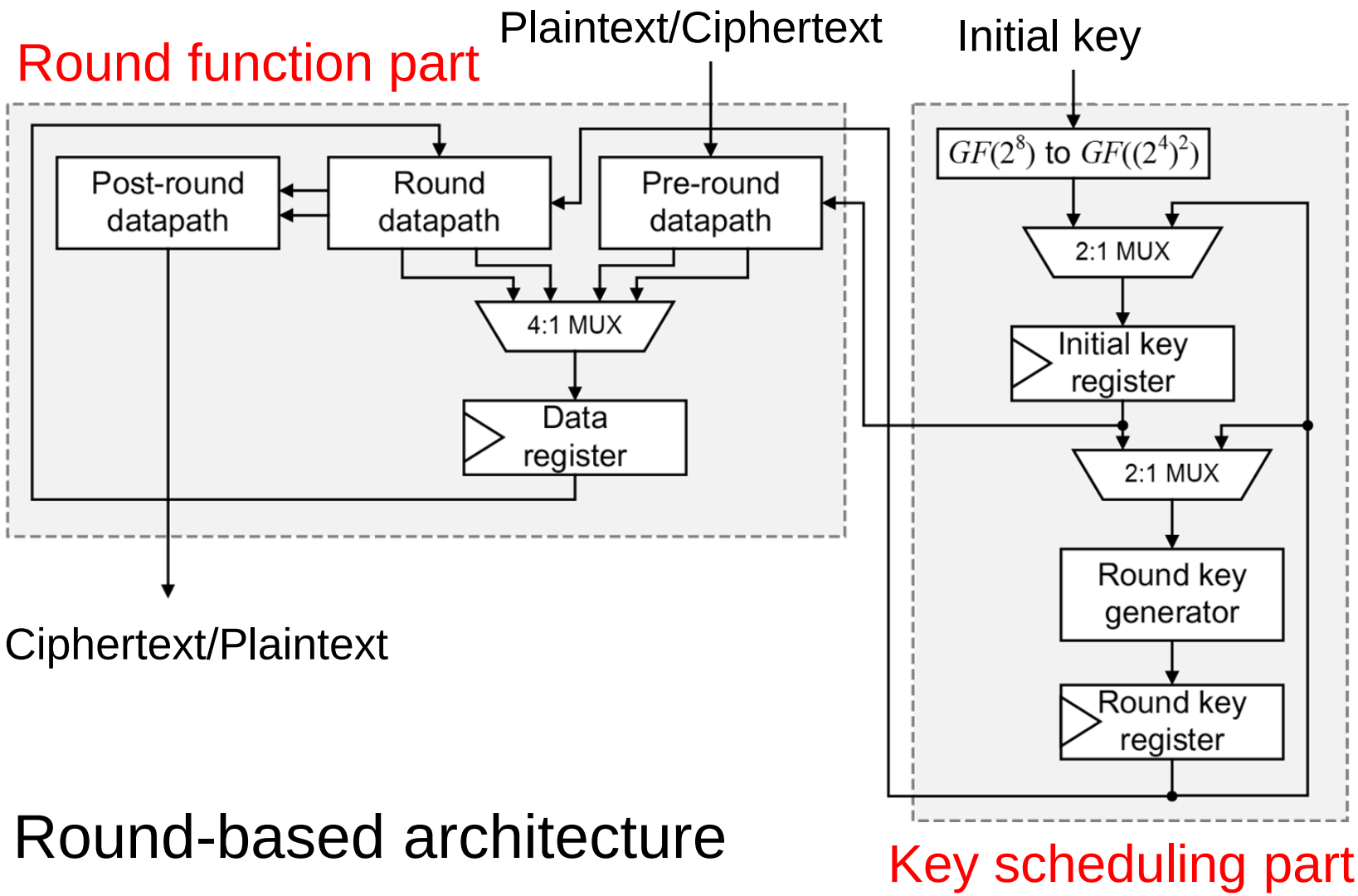
- Inversion should be performed over tower-field
  - Tower-field inversion is more efficient than direct mapping (e.g., table-lookup)
- Two types of tower-field implementation
  - Type-I: only inversion is performed over tower-field
  - Type-II: all operations are performed over tower-field

	Inversion (S-box)	MixColumns InvMixColumns
Type-I	Good	Good
Type-II	Better	Bad

Outline

- Introduction
- Related works
- Proposed architecture
- Performance evaluation
- Concluding remarks

Overall architecture

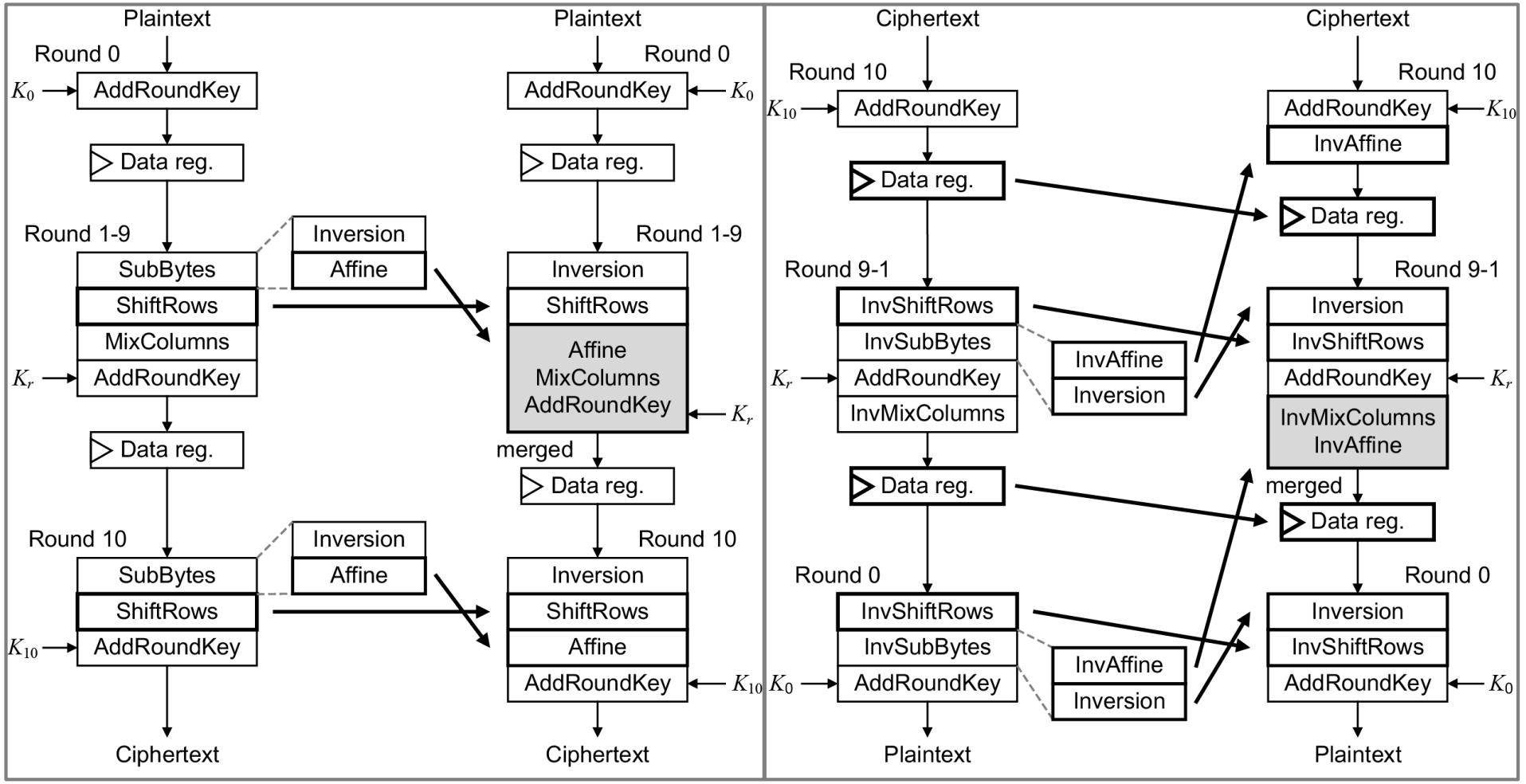


- Round-based architecture
- On-the-fly key scheduler

Round function part

- Compress encryption and decryption datapaths by register-retiming and operation-reordering
  - Unify inversion circuits in encryption and decryption
    - Without any additional selectors (i.e., overheads)
  - Merge linear operations to reduce gates and critical delay
    - Affine/InvAffine and MixColumns/InvMixColumns
    - At most one linear operation for a round
- Type-II tower-field implementation
  - Isomorphic mappings are performed at data I/O
  - Lower-area tower-field (Inv)Affine and (Inv)MixColumns

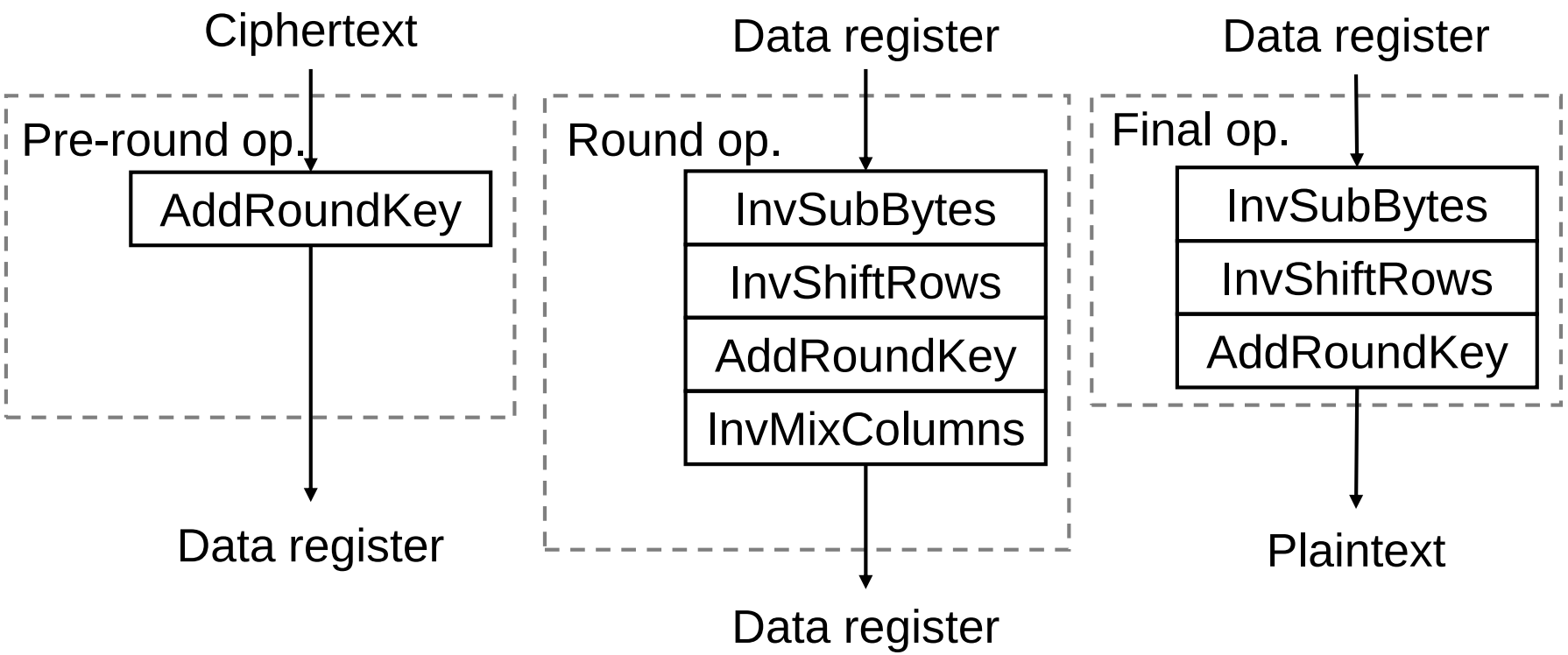
Resister-retiming and operation-reordering



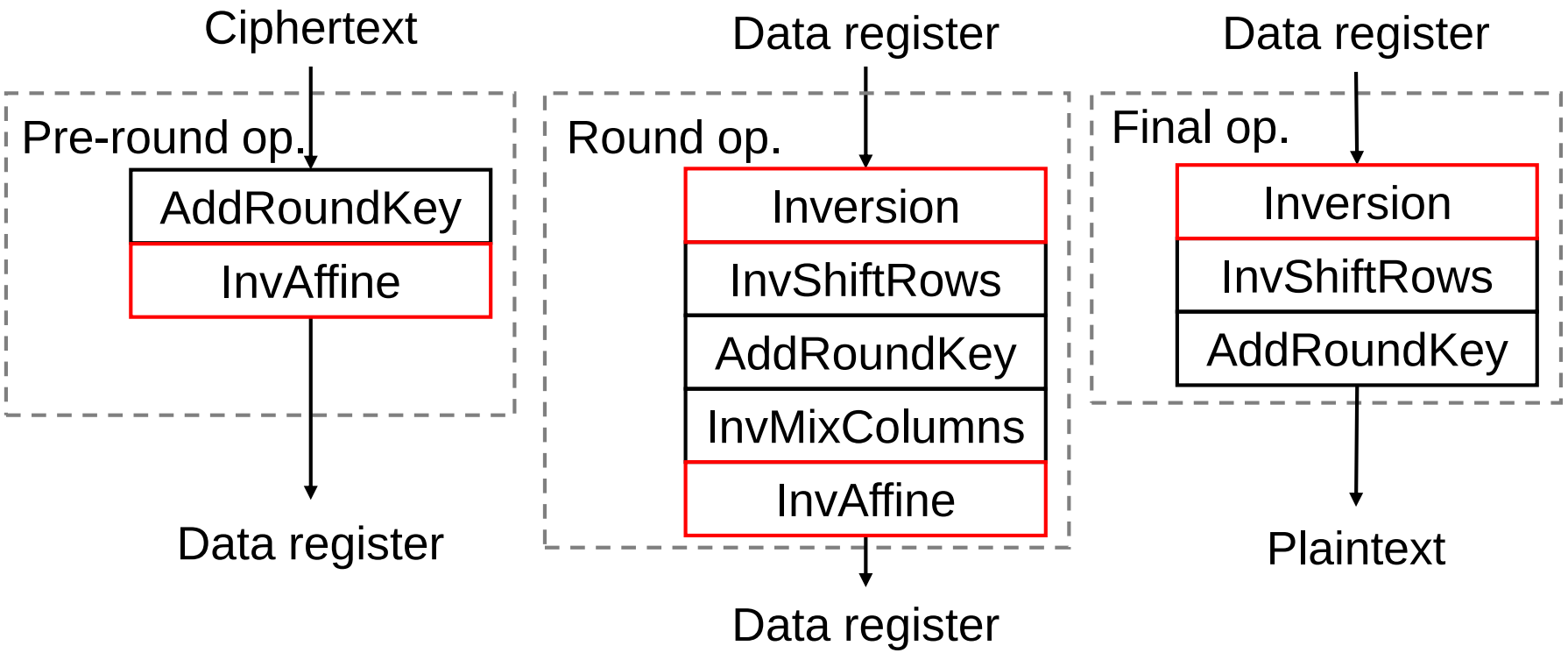
Original Proposed Original Proposed

Encryption Decryption

Key tricks (of decryption)

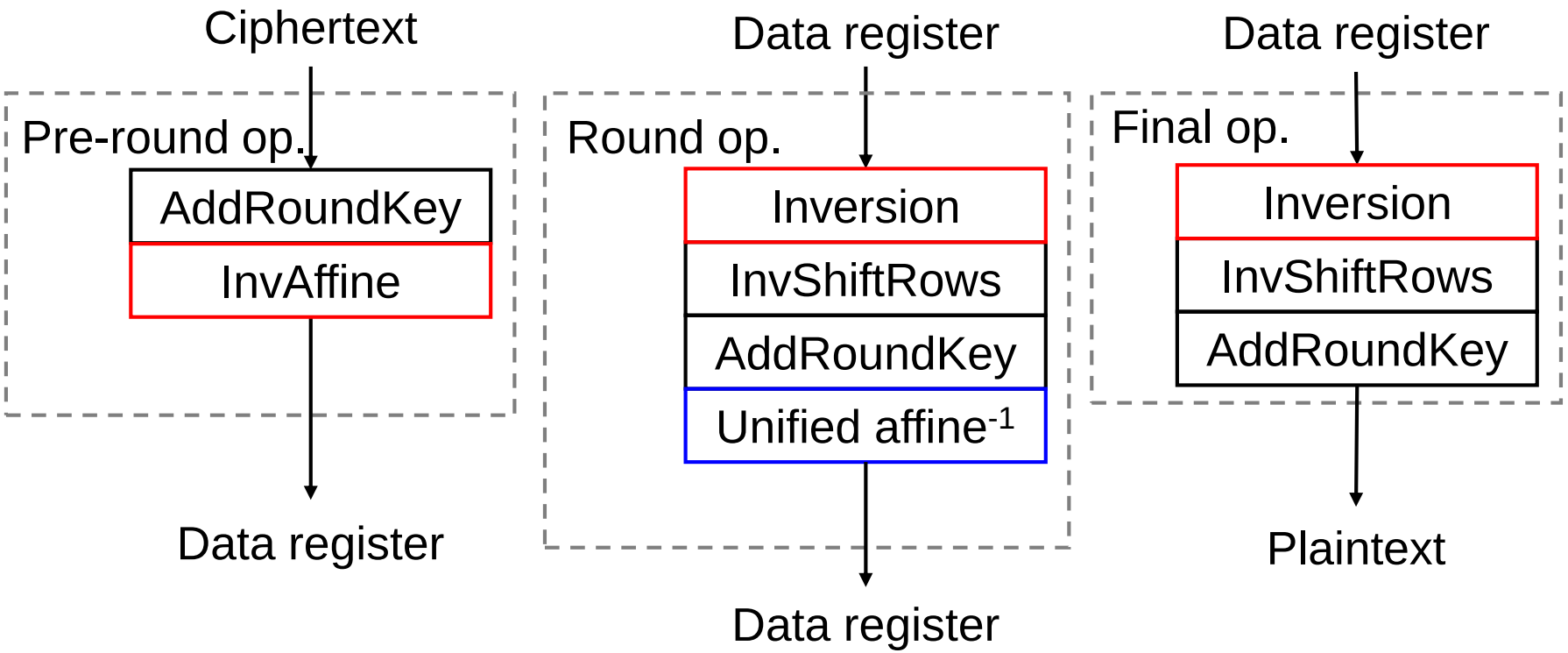


Key tricks (of decryption)



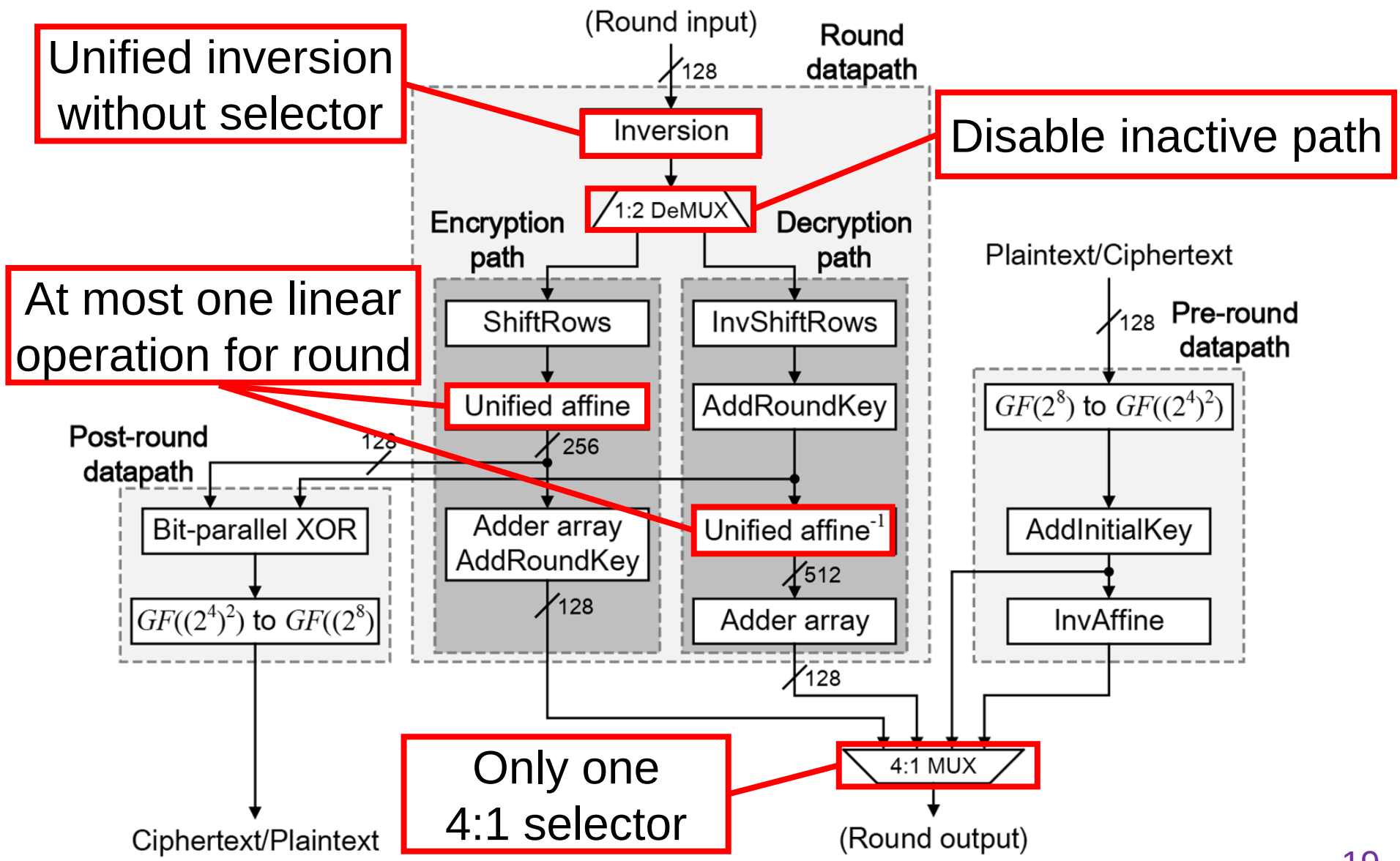
- Decompose InvSubByte to InvAffine and Inversion
- Register-retiming to initially perform inversion in round operations

Key tricks (of decryption)



- Merge linear operations as Unified affine^{-1}
  - InvAffine and InvMixColumns
- Distinct AddRoundKey to avoid additional selectors or InvMixColumns

Resulting datapath



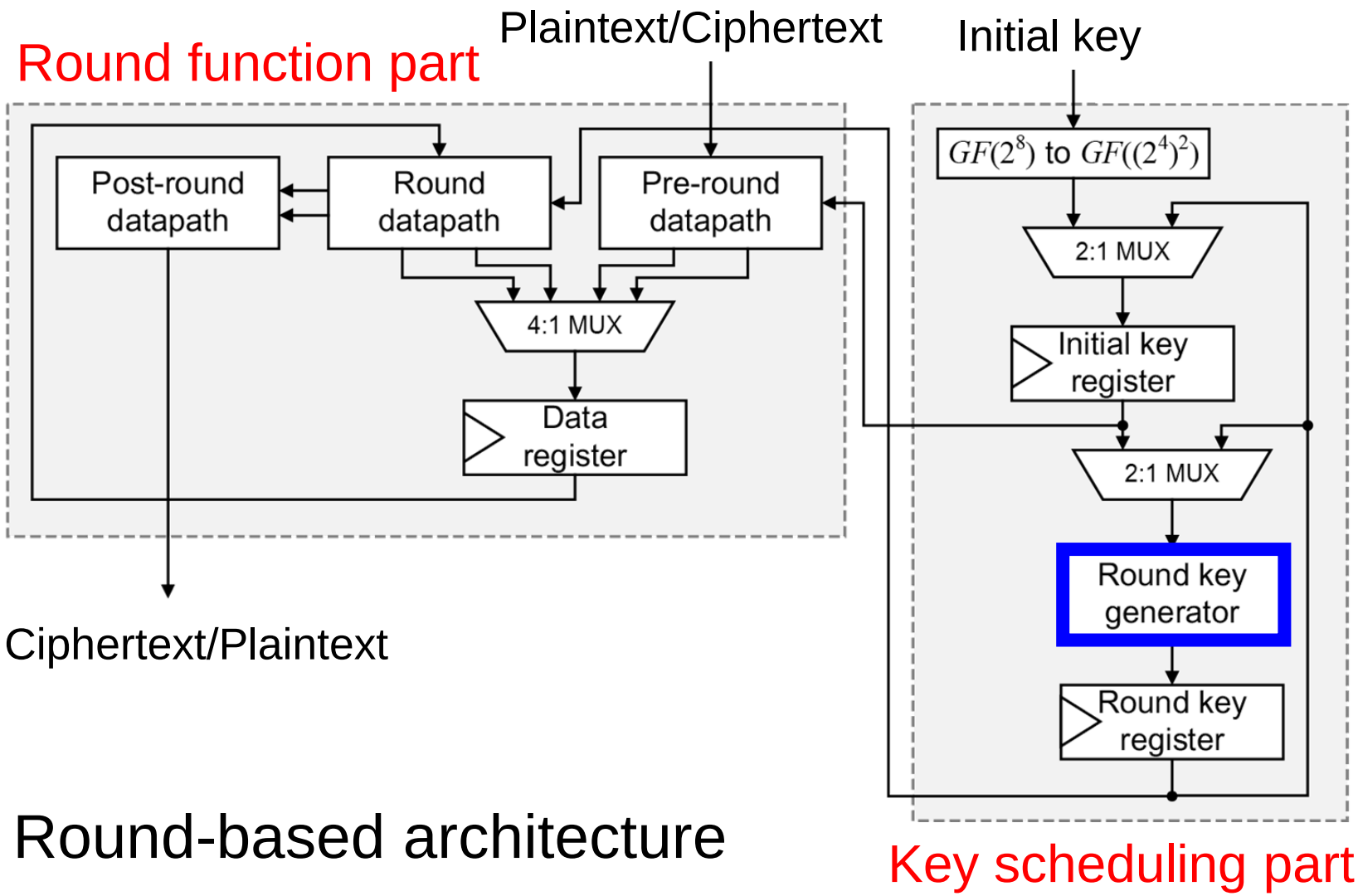
Inversion circuits

- Most area-time efficient inversion circuit [CHES 2015]

	Area [GE]	Timing [ns]	Power [uW]	AT product	PT product
Table look-up	1,209.50	0.66	86.9	798.27	57.35
Satoh+, AC 2001	212.25	2.53	35.0	536.99	88.55
Canright, CHES 2005	175.97	2.49	35.6	438.17	88.64
Nekado+, IWSEC 2012	205.81	1.62	33.1	333.41	53.62
Ueno+, CHES 2015	170.00	1.42	19.3	243.10	27.60

Technology: TSMC 65-nm standard CMOS
Power estimation by gate-level timing simulation at 10MHz

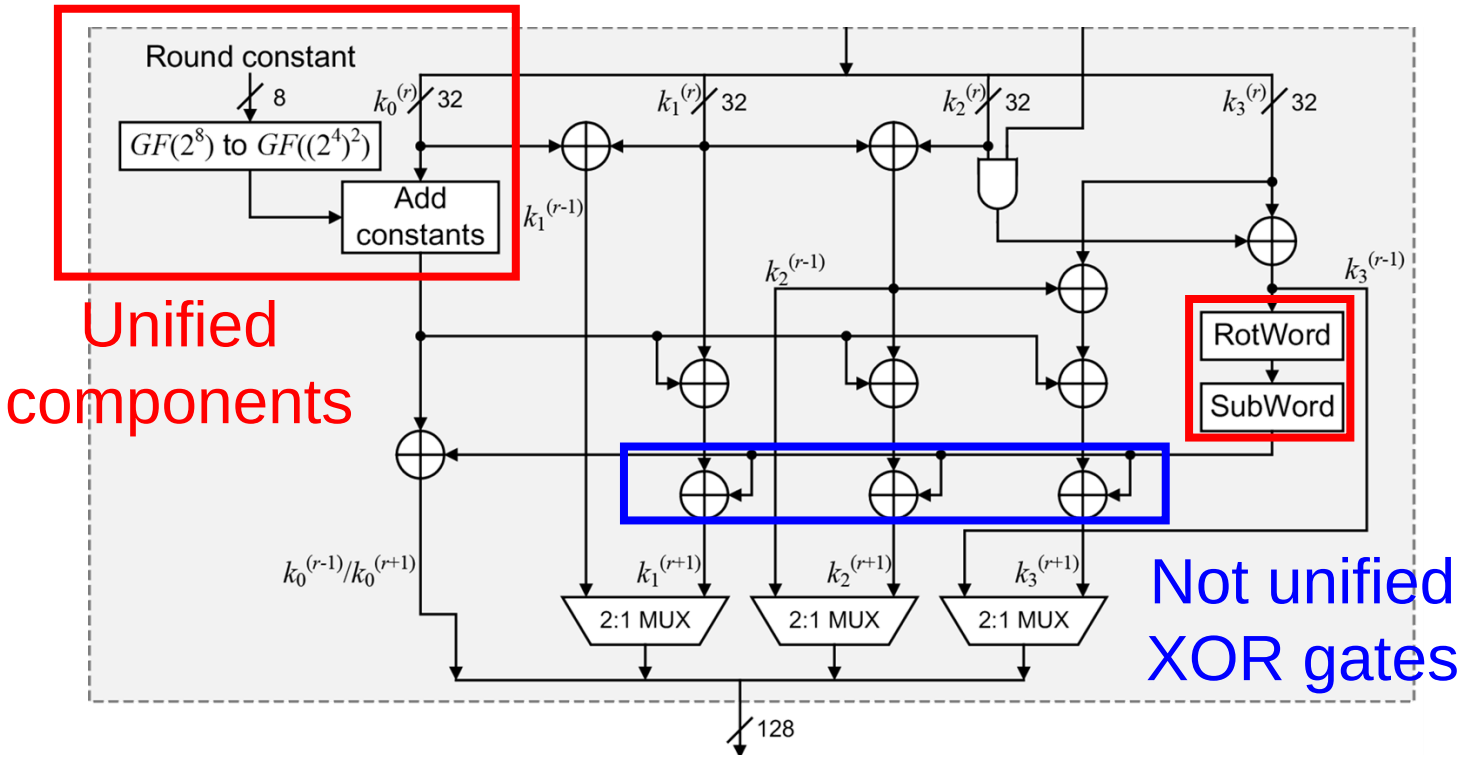
Overall architecture



- Round-based architecture
- On-the-fly key scheduler

Key scheduling part

- Round key generator is dominant
  - Unify encryption and decryption datapaths
  - Shorten critical delay than round function part by NOT unifying some XOR gates



Outline

- Introduction
- Related works
- Proposed architecture
- Performance evaluation
- Concluding remarks

Performance evaluation

- Logic synthesis with area optimizations
  - Logic synthesis: Design Compiler
- Include on-the-fly key scheduler

	Area (GE)	Latency (ns)	Max. freq. (MHz)	Throughput (Gbps)	Efficiency (Kbps/GE)
Satoh et al.	13,671.75	78.10	140.85	1.64	119.88
Lutz et al.	20,380.50	68.50	145.99	1.87	91.69
Liu et al.	12,538.75	85.25	129.03	1.50	119.75
Mathew et al.	20,639.50	97.68	112.61	1.31	63.49
This work	15,242.75	46.97	234.19	2.73	178.78

All architectures were implemented in round-based manner

Performance evaluation

- Logic synthesis with area optimizations
  - Logic synthesis: Design Compiler
- Include on-the-fly key scheduler

	Area (GE)	Latency (ns)	Max. freq. (MHz)	Throughput (Gbps)	Efficiency (Kbps/GE)
Satoh et al.	13,671.75	78.10	140.85	1.64	119.88
Lutz et al.	20,380.50	68.50	145.99	1.87	91.69
Liu et al.	12,538.75	85.25	129.03	1.50	119.75
Mathew et al.	20,639.50	97.68	112.61	1.31	63.49
This work	15,242.75	46.97	234.19	2.73	178.78

All architectures were implemented in round-based manner

+53%

Our architecture achieved highest efficiency

Power consumption estimation

- Power estimation by Power Compiler
  - Gate-level dynamic simulation calculating switching activities with glitch effects

	Power [mW] @ 10 MHz	PT product
Satoh et al.	4.05	316.31
Lutz et al.	3.43	234.96
Liu et al.	4.51	384.48
Mathew et al.	5.49	536.26
This work	2.76	129.63

-20%

-45%

Our architecture achieved lowest power and power-time (PT) product

Concluding remarks

- Most area-time efficient AES HW architecture
  - 44-72% higher throughput/gate efficiency compared to conventional ones
  - Lowest-energy by Power Compiler with gate-level timing simulation
- Future works
  - Post-synthesis evaluation
  - Efficient side-channel-resistant architecture