

An Optimized S-Box Circuit Architecture for Low Power AES Design

IBM Japan Ltd.
Tokyo Research Laboratory
Sumio Morioka and Akashi Satoh



Contents

- ◆ Background
- ◆ Power Analysis of Conventional S-Boxes
- ◆ Multi-Stage PPRM S-Box for Low-Power H/W
- ◆ Conclusion

Background

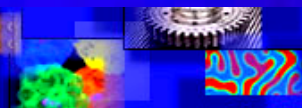


Back Ground

- ◆ In 2001, NIST selected Rijndael as the new symmetric key standard cipher AES
- ◆ AES H/W will be integrated in various applications
- ◆ Low-power feature is important not only in low-end applications but also in high-end servers
 - ◆ A 10-Gbps AES H/W chip consumes several Watts in 0.13- μm CMOS
- ◆ Need for power analysis and development of low-power architectures for AES H/W



**National Institute of
Standards and Technology**

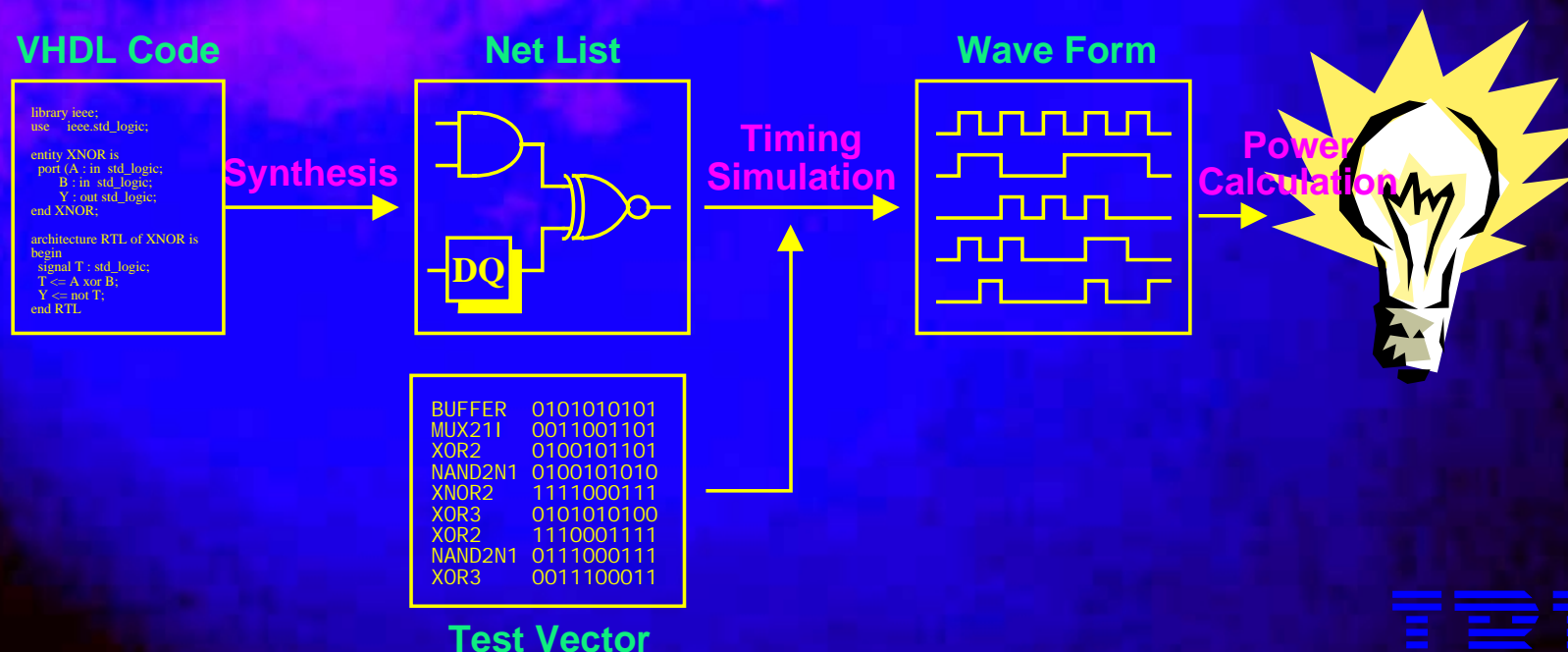


NIST

...working with industry to develop and apply technology, measurements and standards

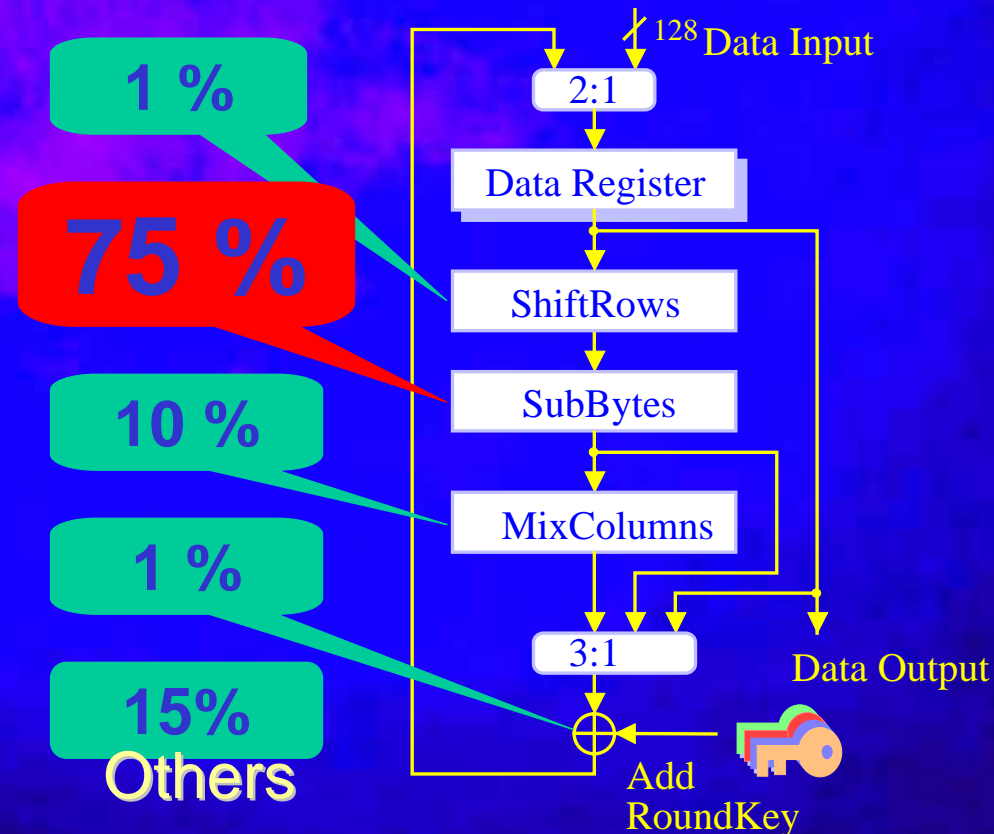
Power Analysis Method

- ◆ Power analysis is based on timing simulation
- ◆ Gate switching including dynamic hazard is evaluated
- ◆ Quite accurate estimation compared with static analysis



Power Analysis in AES H/W

- ◆ 128-bit bus 11-round Loop Architecture
- ◆ Table-lookup-based S-Box using SOP logic



For Low-Power AES H/W

- ◆ Reducing S-Box power is most effective
- ◆ There are various S-Box H/W architectures
- ◆ Which architecture is suitable for low power ?



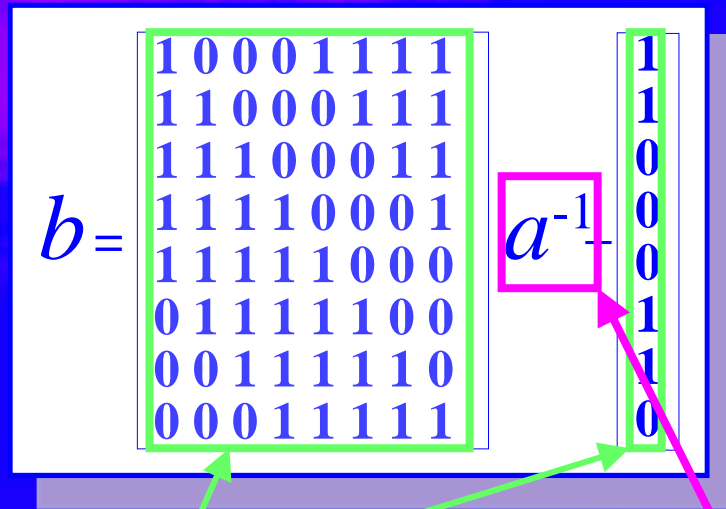
Objectives

- ◆ Investigate performance of all conventional S-Boxes
- ◆ Develop a low-power S-Box architecture

Power Analysis of Conventional S-Boxes

S-Box Definition

- ◆ Nonlinear byte substitution function
- ◆ Multiplicative Inversion on $GF(2^8)$ + affine transformation.



Affine trans.
8x8 XOR matrix

Inversion
Complicated math. logic



S-Box Architectures

GF inverter + affine

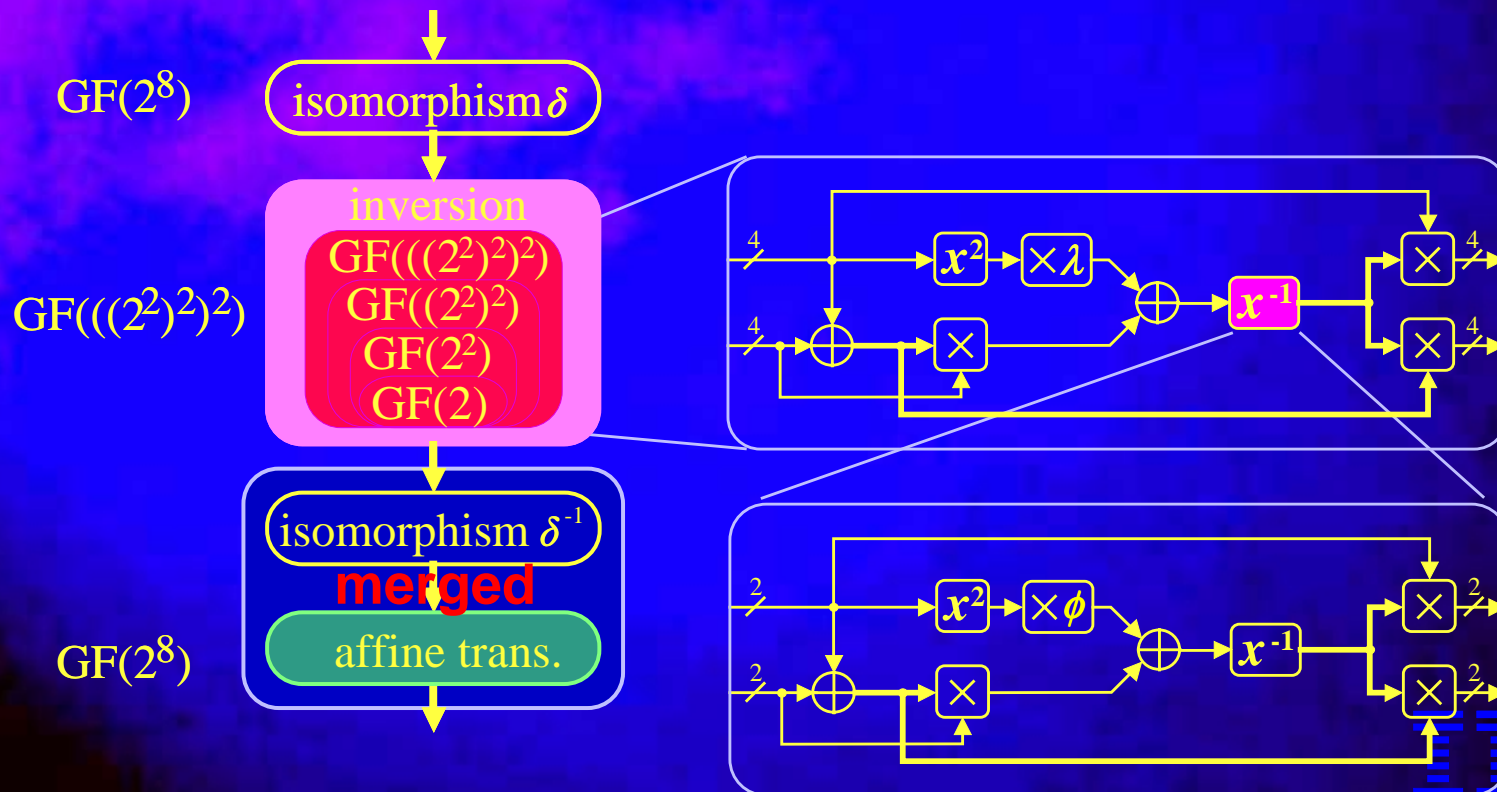
- ◆ Various mathematical techniques can be applied
- ◆ Rather slow
- ◆ Compact implementation
- ◆ S-Box and S-Box⁻¹ can be merged

Direct mapping

- ◆ Generate black box circuit from a truth table
- ◆ High-speed
- ◆ Rather large
- ◆ S-Box and S-Box⁻¹ cannot be merged

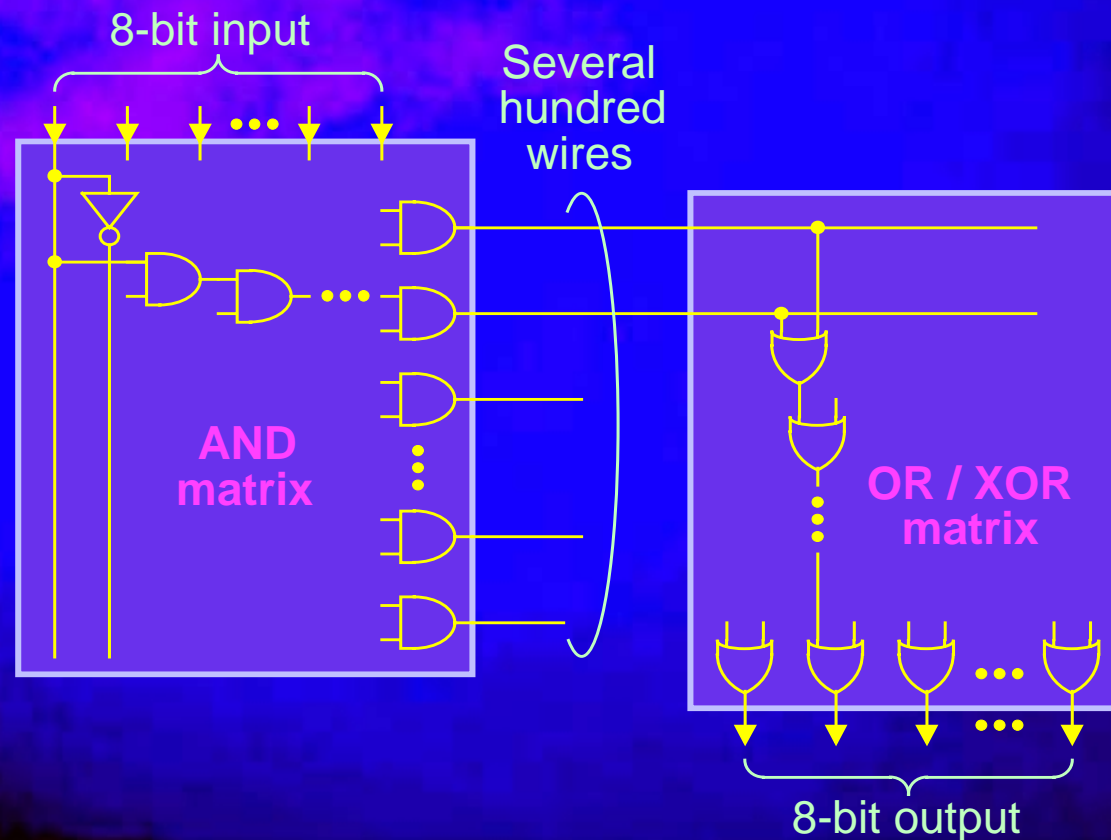
GF Inverter + Affine

- ◆ Apply hierarchical structure of composite field $GF(((2^2)^2)^2)$
 - ◆ Map elements on $GF(2^8)$ onto $GF(((2^2)^2)^2)$ by isomorphism
- ◆ Each component is constructed using AND-XOR logic



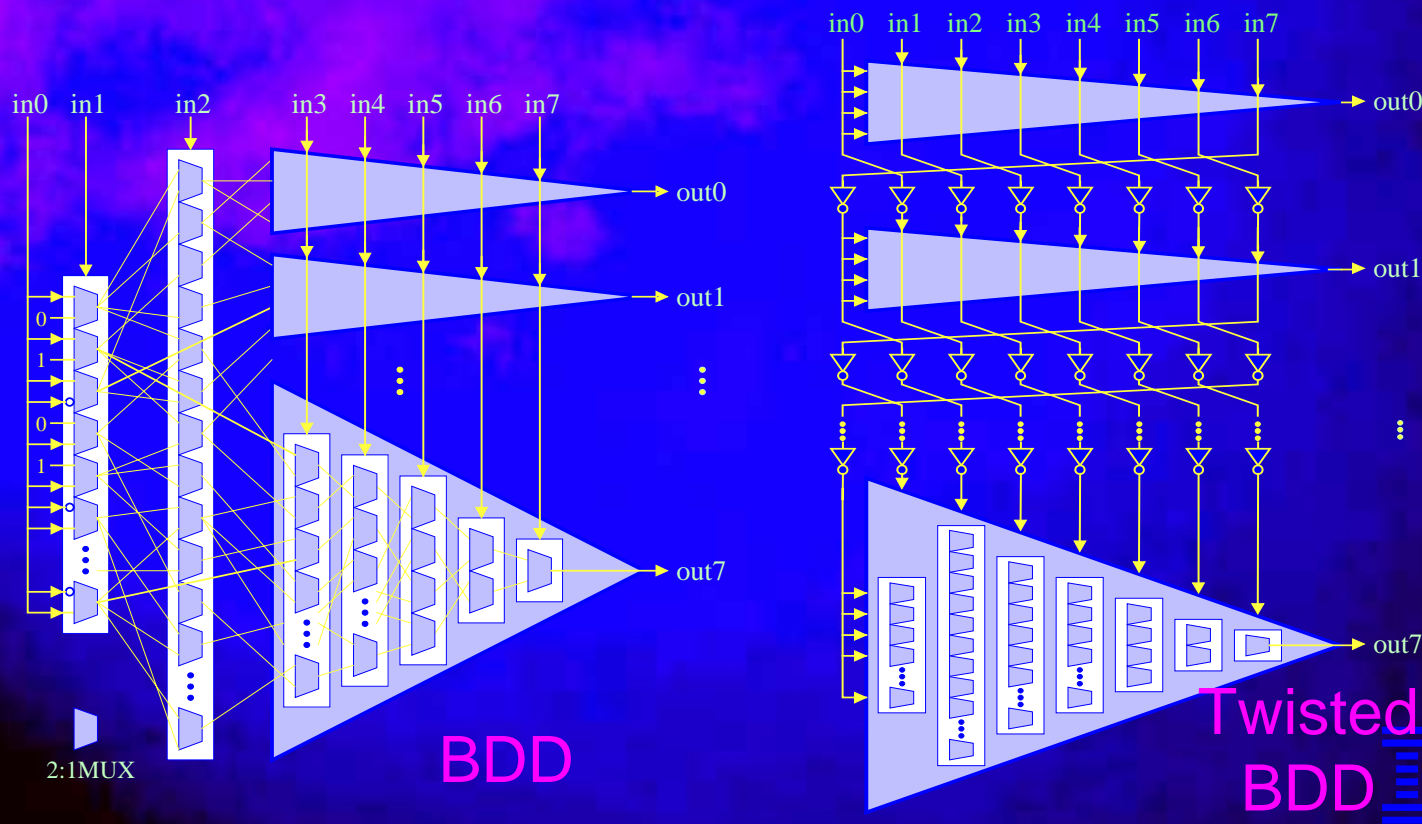
Direct Mapping

- ◆ 2-Level Logic
 - ◆ SOP (Sum of Products) : (NOT)-AND-OR
 - ◆ POS (Product of Sums) : (NOT)-OR-AND
 - ◆ PPRM (Positive Polarity Reed-Muller) : AND-XOR



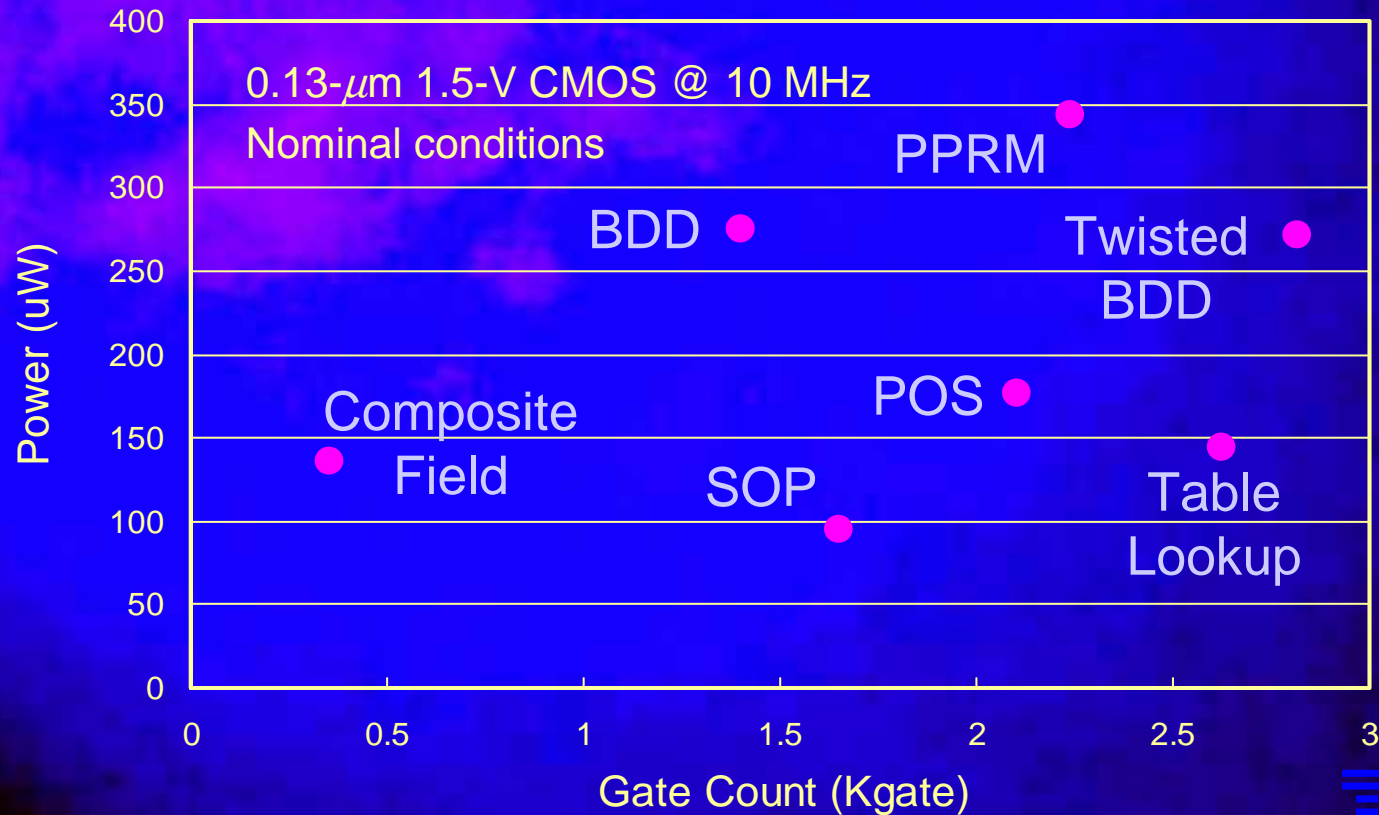
Direct Mapping

- ◆ Selector-Based Logic
 - ◆ BDD (Binary Decision Diagram)
 - ◆ Twisted BDD will appear at ICCD 2002 in Sep.



Power vs. Gate Count

- ◆ Smaller circuits do not always consume less power



Analysis

- ◆ Power consumption of S-Box is greatly influenced by the number of dynamic hazards



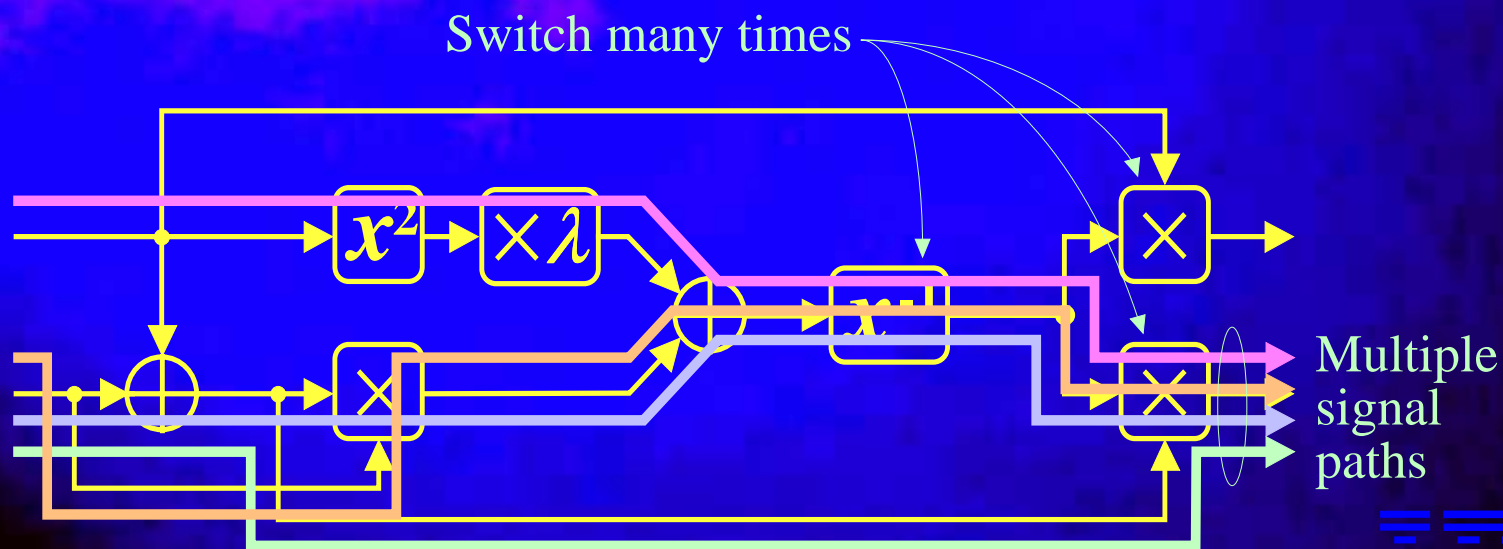
Caused by

- ◆ Differences of signal arrival times at each gate
- ◆ Propagation probability of signal transitions

Analysis

Differences of signal arrival times at each gate

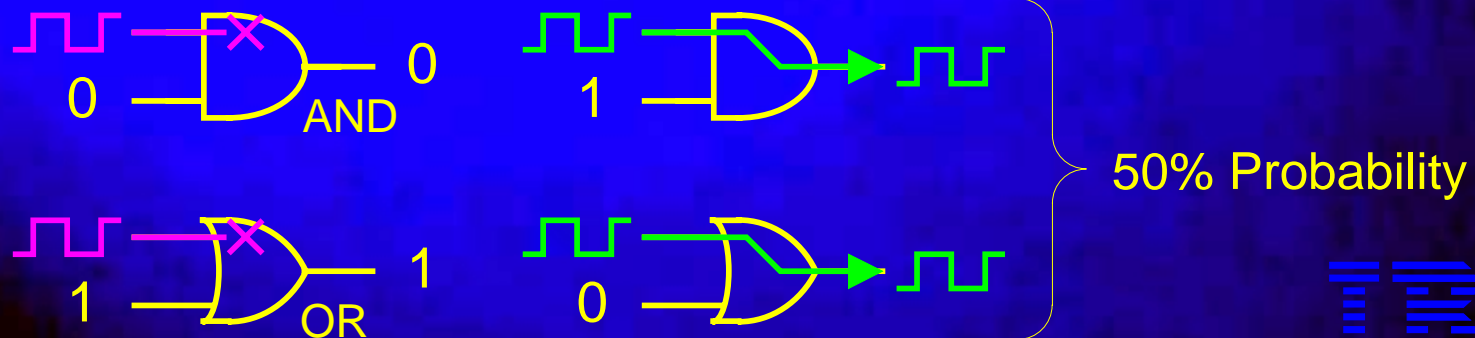
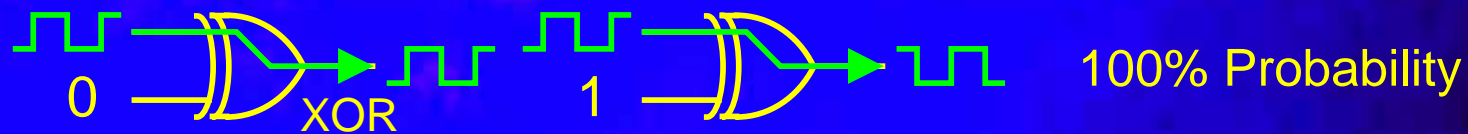
- ◆ Composite field S-Box consumes a lot of power in spite of having the smallest size
- ◆ It has many crossing and branched signal paths



Analysis

Propagation probability of signal transitions

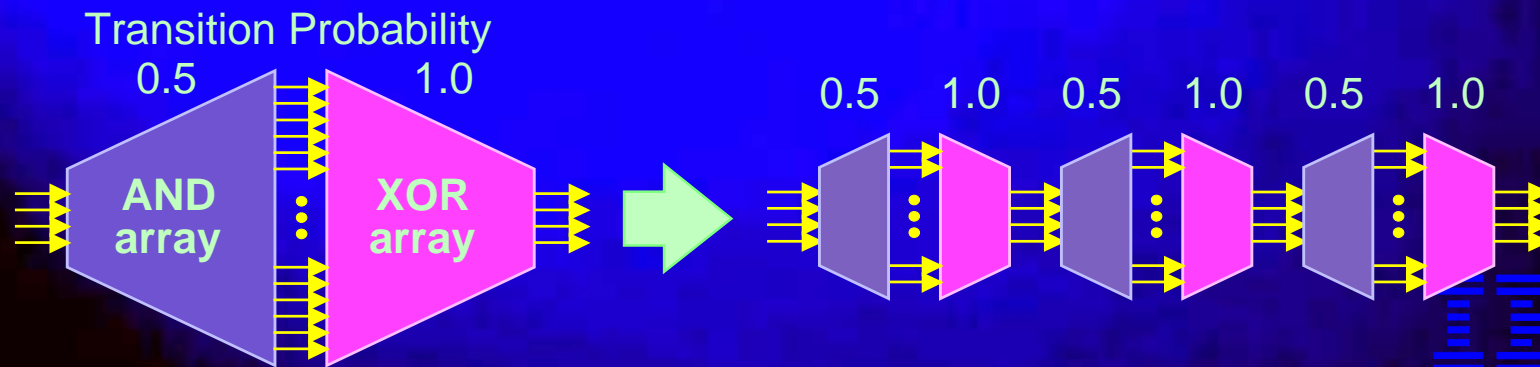
- ◆ An XOR gate transfers signal transitions from input to output with probability 100%
- ◆ For AND, OR gates, the probability is 50%
 - ◆ So power for SOP is lower than PPRM



Multi-Stage PPRM S-Box for Low-Power H/W

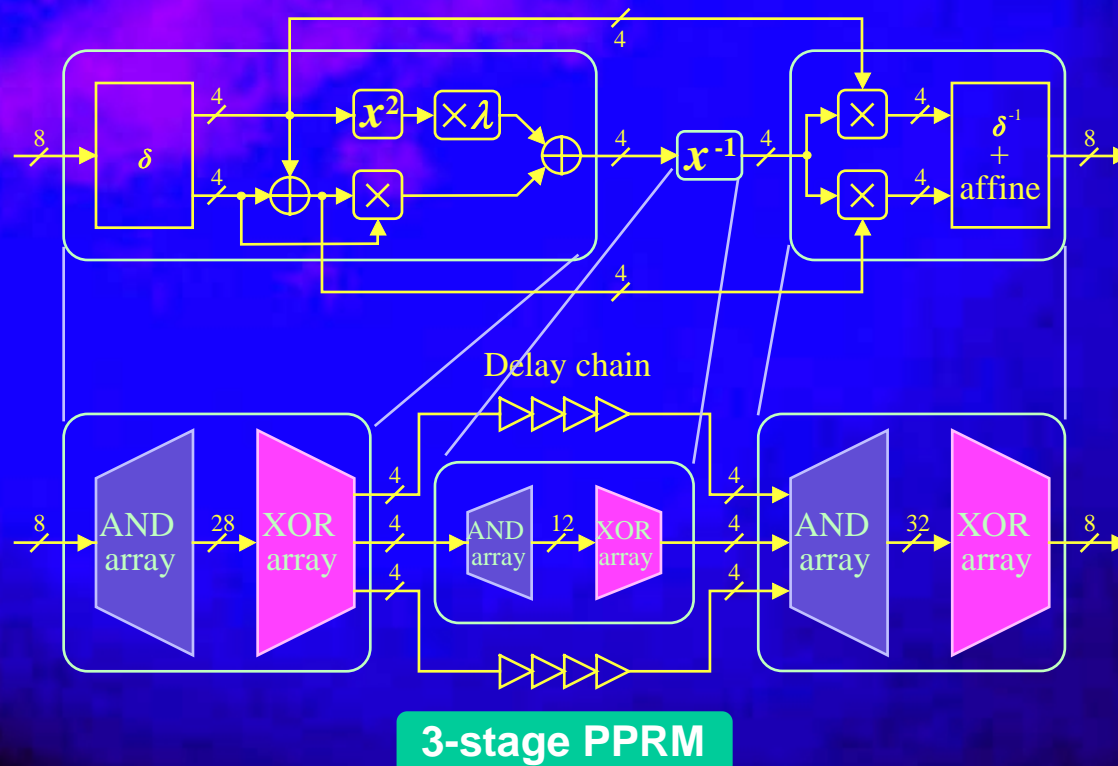
Approach for Low Power S-Box

- ◆ Use composite field S-Box
 - ◆ Reduce gate counts
- ◆ Divide combination logic into multiple stages
 - ◆ Reduce probability of signal transitions
- ◆ Adjust the signal timing between each stage using 2-level logic
 - ◆ Reduce the number of dynamic hazards



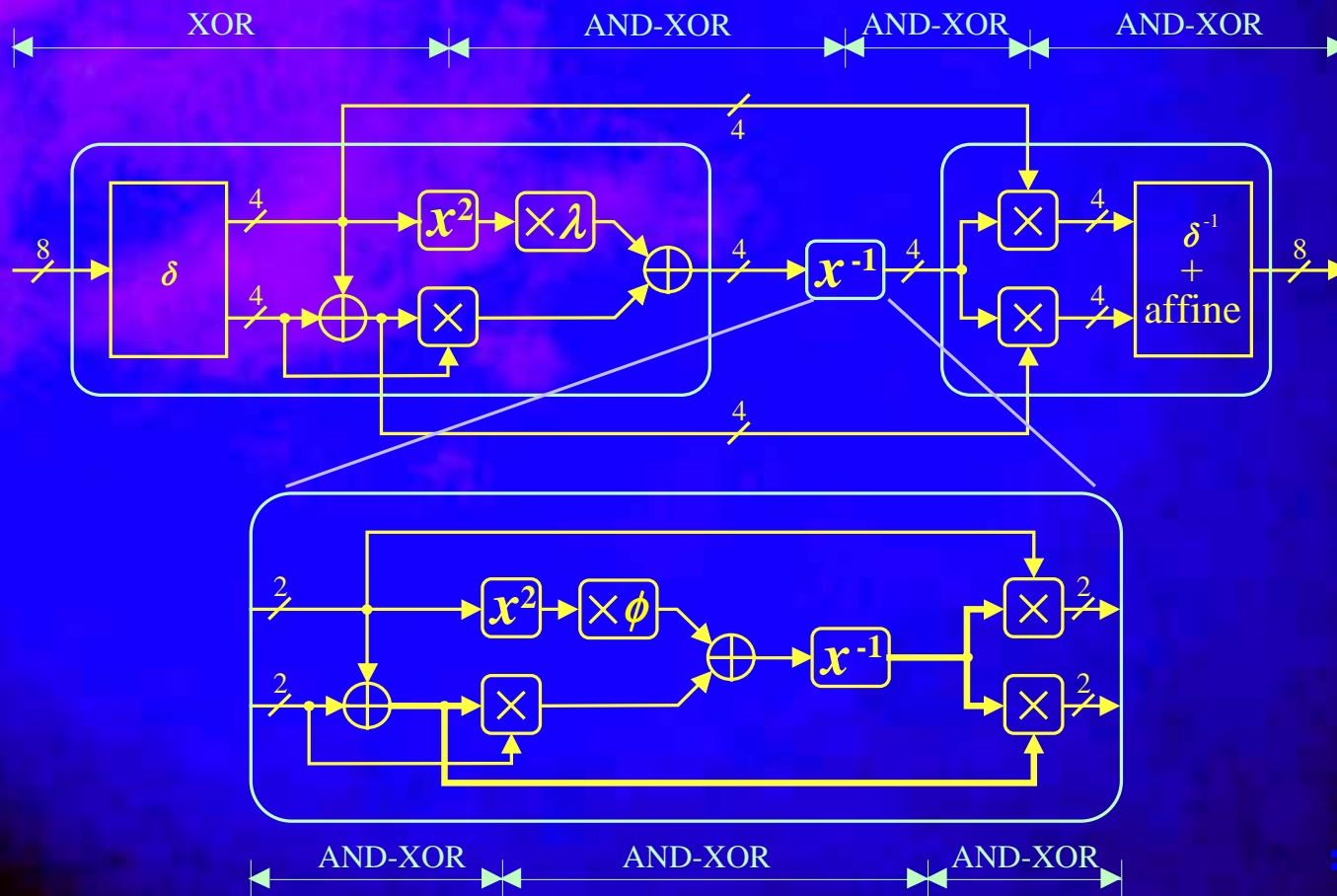
Multi-Stage PPRM

- ◆ Composite field S-Box is divided into several blocks
- ◆ Each block is designed using PPRM logic suitable for GF operations
- ◆ Adjust signal timing by using 2-level (AND-XOR) logic



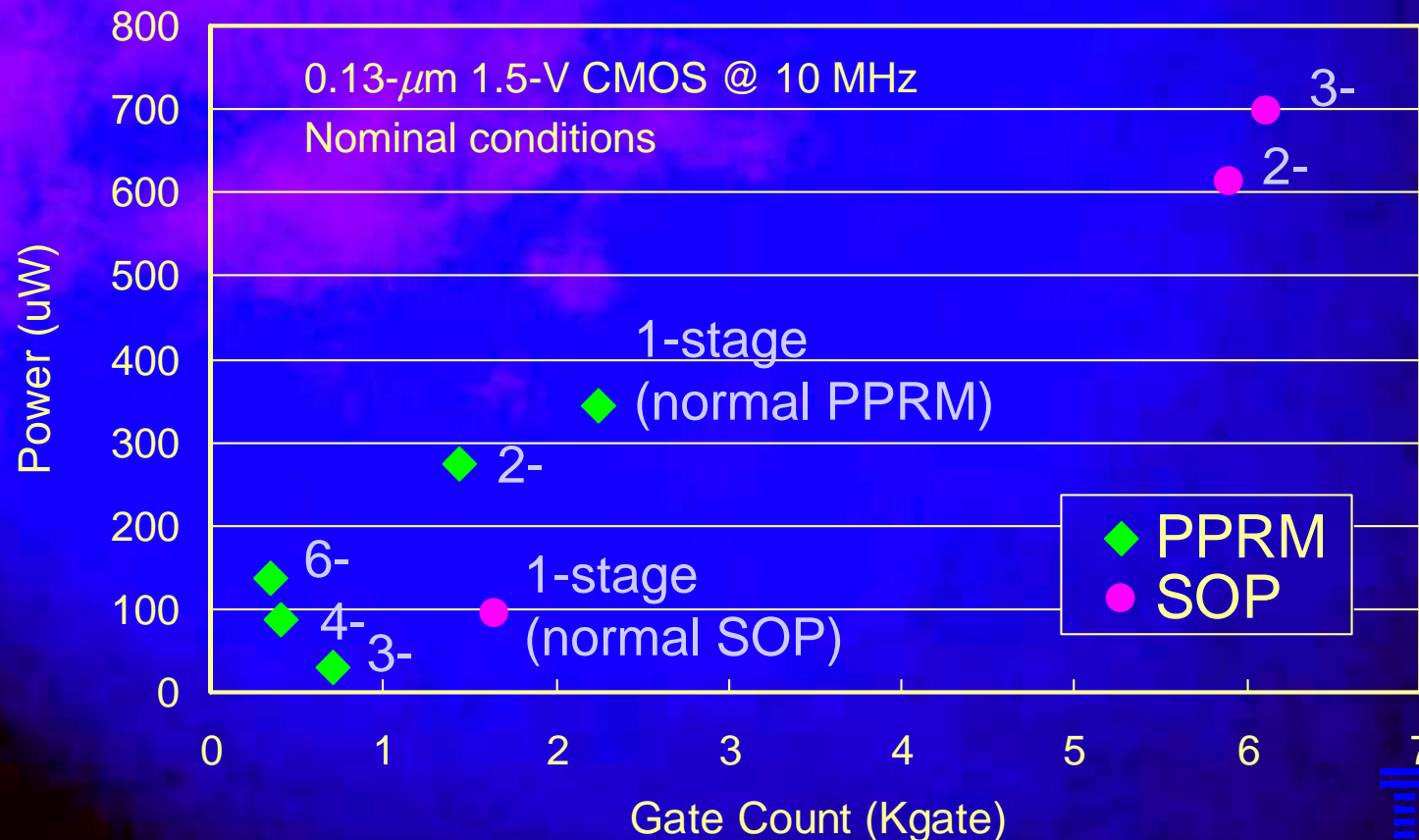
Multi-Stage PPRM

- ◆ PPRM S-Boxes can be divided many ways (1~6-stages)



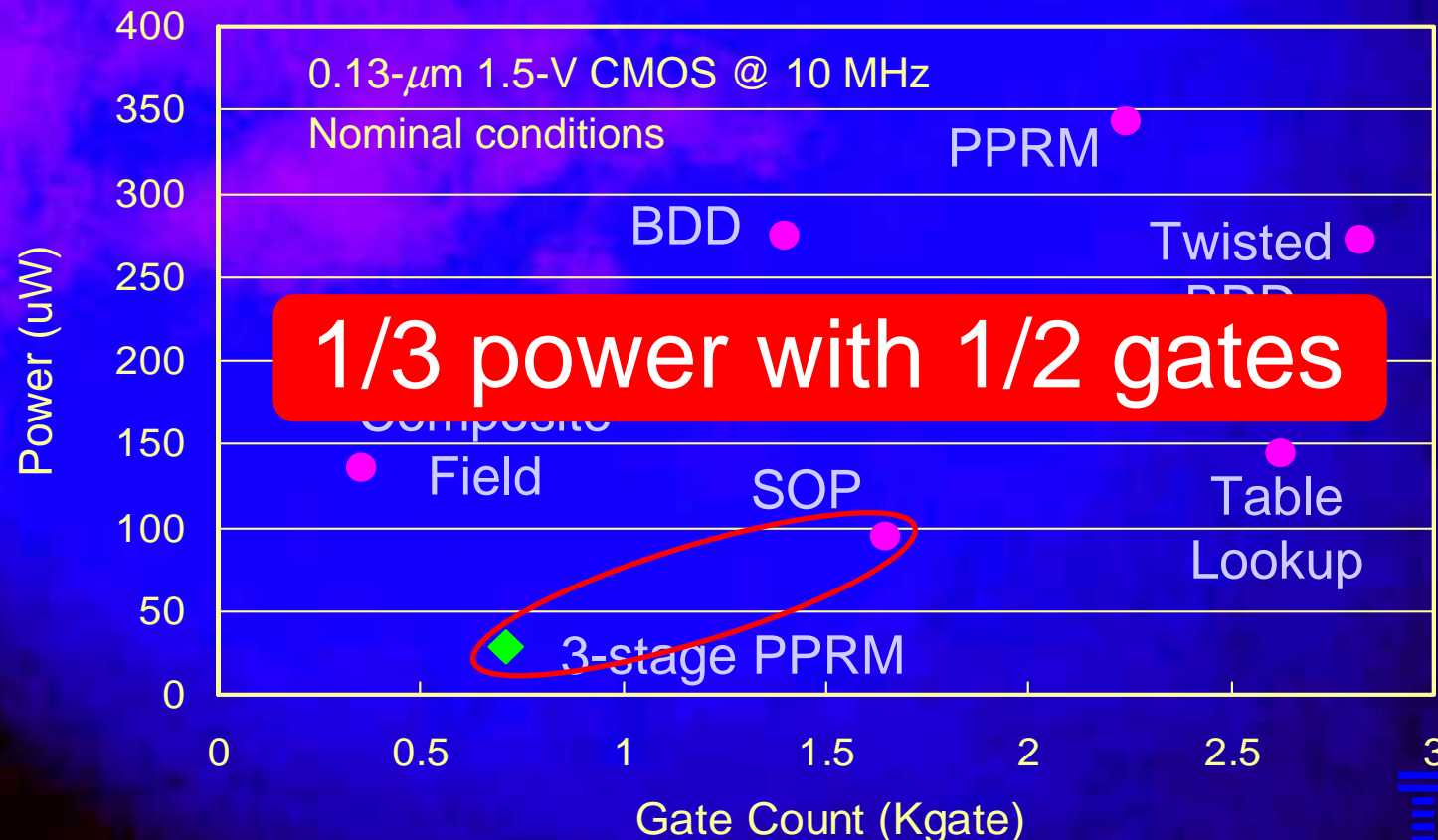
Power vs. Gate Count

- ◆ 3-stage PPRM is the most effective architecture
- ◆ Multi-stage SOP is not suitable for GF operation



Power vs. Gate Count

- ◆ 3-stage PPRM is the most effective architecture
- ◆ Multi-stage SOP is not suitable for GF operation



Conclusion

- ◆ The AES S-Box (SOP logic) consumes 75% of the power
- ◆ Dynamic hazards boost power needs of S-Boxes
- ◆ A multi-stage PPRM architecture based on a composite field S-Box was developed
- ◆ 3-stage PPRM / SOP : **Power = 1/3, Size = 1/2**
- ◆ This architecture can be applied to other S-Boxes defined over Galois fields