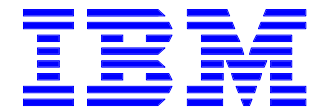


High Performance RSA Hardware Accelerator Design

IBM Research, Tokyo Research Laboratory
IBM Japan, Ltd.



Overview

- High-performance modular exponentiation accelerator (RICO) has been developed by Tokyo Research Laboratory, IBM Japan
 - 22msec for 1024-bit exponent with 5mm² 0.5um CMOS (RICO-1)
- RICO architecture will be presented
- Applications will be presented

Contents

- Why hardware crypto accelerator ?
- Hardware algorithms for modular exponentiation
- RICO architecture
- RICO-1 and RICO-2 VLSI
- Applications
- Next steps
- Summary

Why Hardware Accelerator?

- Performance
- Tamper resist
- Lower power dissipation
- Lower cost for embedded applications
- Smaller foot-print

RICO Architecture

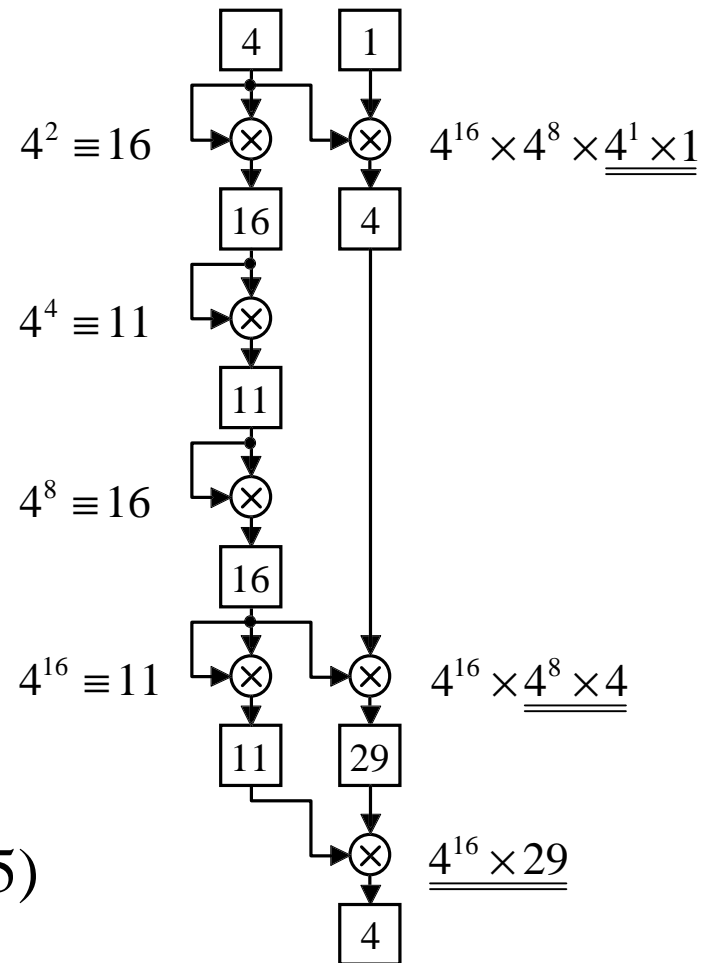
- Pipeline and parallel internal operations
 - $m \times e$ clock cycles for m -bit data and e -bit exponent
- Cycle steal modular operations
 - Zero cycle overhead
- High-speed carry skip adder
 - 47-gate delay for 1035-bit adder
- Optimized trade-off between logic and layout
 - 4.9mm² modular exponentiation core
- Tamper resist especially for timing attack
 - No dependency on bit patterns

LSB First Operation

- $C = M^e \pmod n$
- LSB first operation
 - $M^{2^i} \pmod n$ calculated by square block
 - M^{2^i} multiplied and modulo n calculated in power block when $e_i = 1$

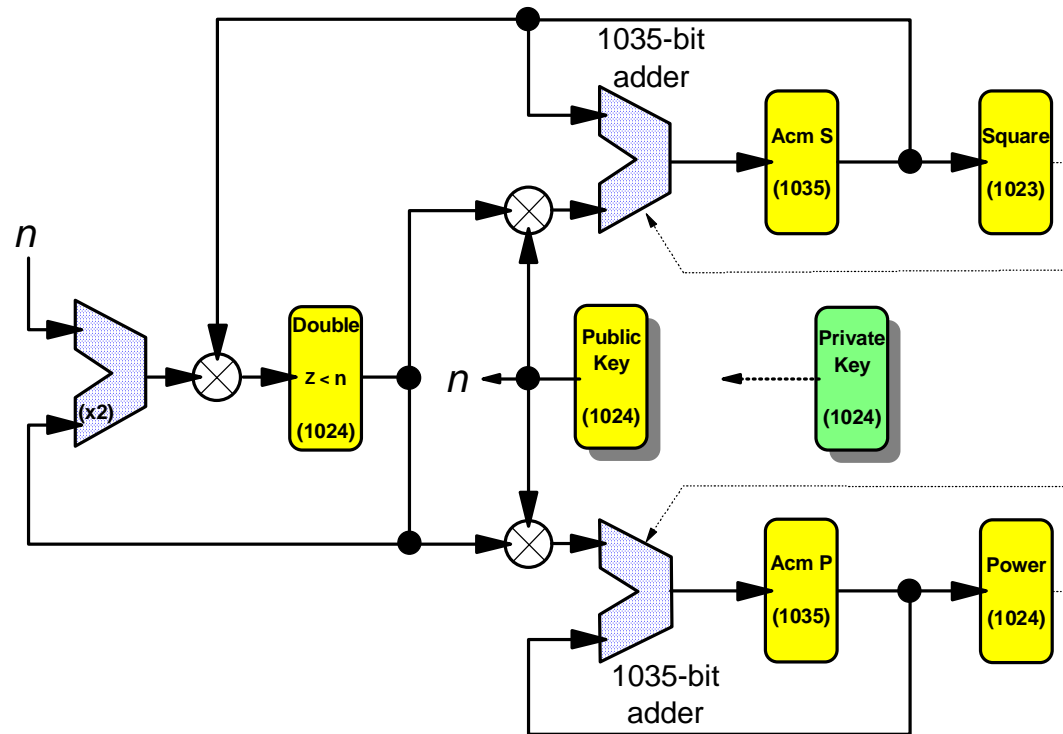
Example:

$$4^{25} = 1100b \pmod{35}$$



RICO Data Path

- Pipeline operation
- Two-way parallel operation

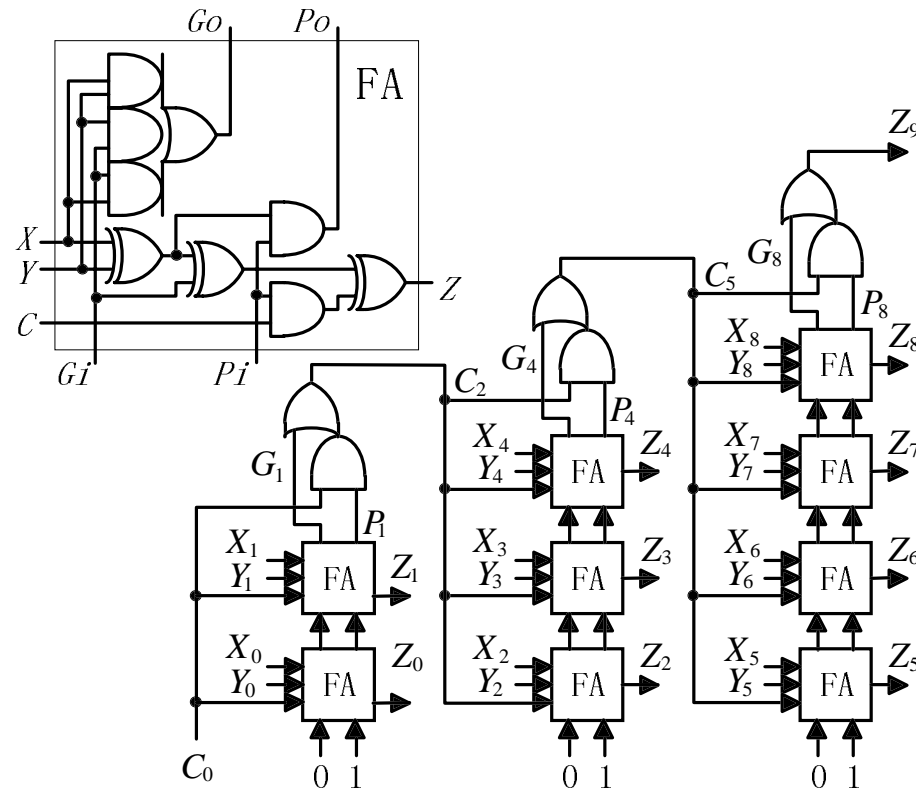


Cycle Steal Modulus

- **$A \times B \pmod{N}$ is calculated by repetition of ADD operations**
 - Addend is reduced to less than N (1024 bit) by Shift-MOD circuit
 - Sum does not exceed 1034 bit (maximum is less than $1024N$)
- **Allow the intermediate sum results in range from $-4N$ to $1024N$**
 - Deduct $4N$ from the intermediate sum when:
 - Adder is free from ADD operation
 - Sum is a positive number
 - 1035-bit adders and accumulation registers

High-speed Carry-skip Adder

- Balanced carry-propagation and block-internal delays
- Regular structure suitable for physical layout
- 47-gate delays for 1035-bit adder



RICO Tamper Resist Design

- Hard attack

Extract private key directly from chip H/W

- ▶ EEPROM (private key) monitoring
- ▶ Circuit reverse engineering

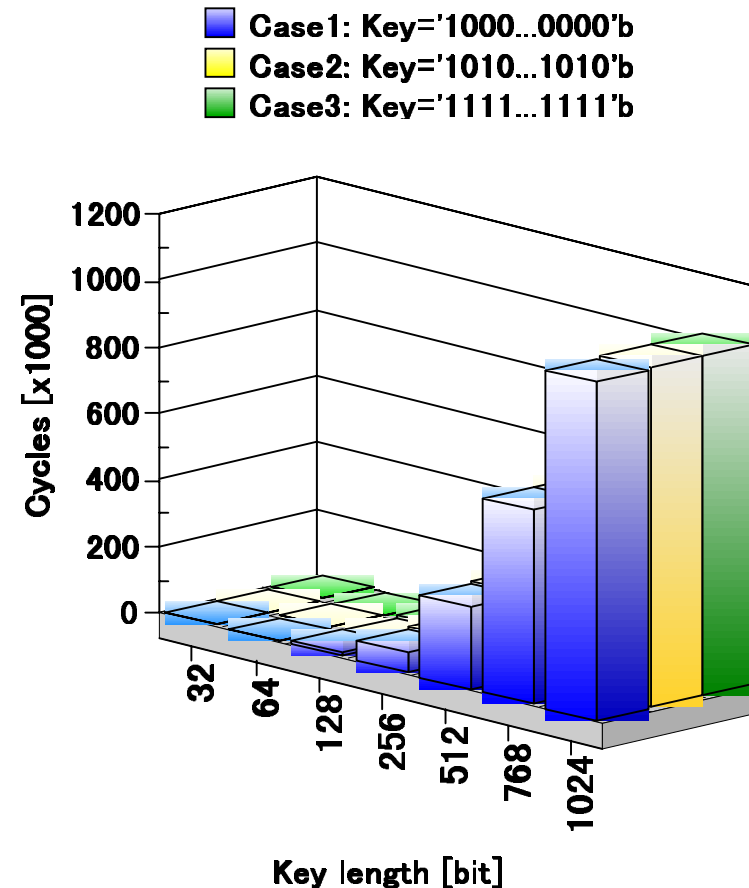
- Soft attack

Investigate behavior shift depending on the bit pattern of private key

- ▶ Timing attack
- ▶ Power monitoring

RICO Tamper Resist Design

- Constant calculation time
 - ▶ Statistically, independent from bit pattern of key
 - ▶ Independent from message pattern
 - ▶ Depend only on key length



RICO-1 VLSI Features

Initial VLSI Implementation of RICO Architecture

- 3 metals, 0.5-um CMOS
- 4.9 mm² RSA core
- Up to 48-MHz operation
- 22msec for 1024-bit RSA
- 350mW max power
- 8-1024 bit keys
- 19.9MB/sec for DES
- 29.7MB/sec for MD5
- 5.31 x 5.31mm² die

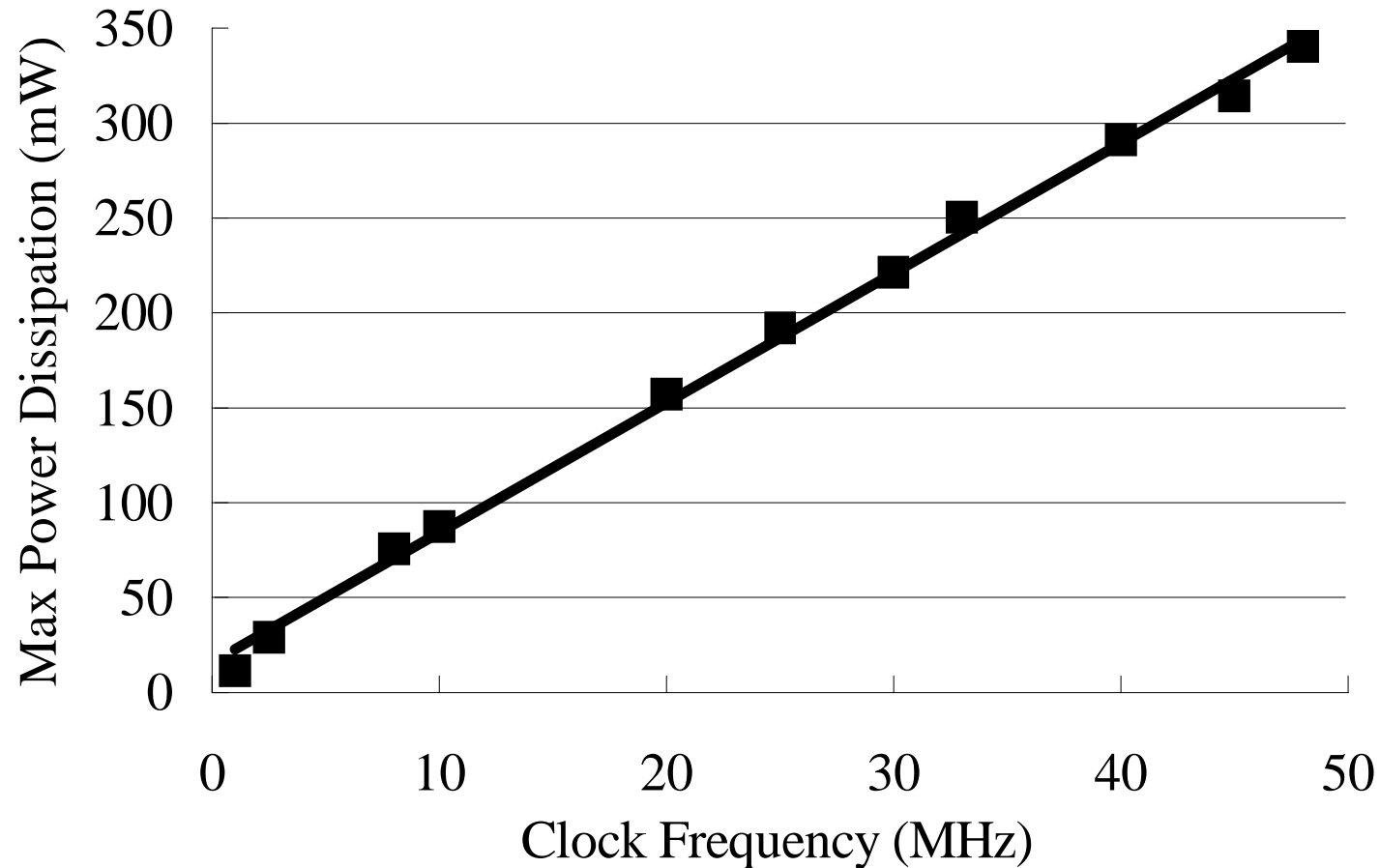


RICO-1 RSA Performance

- 1024-bit RSA
 - $(1024+1) \times (1024+4\text{adjustment}) / 48\text{MHz}$
=22.0 msec

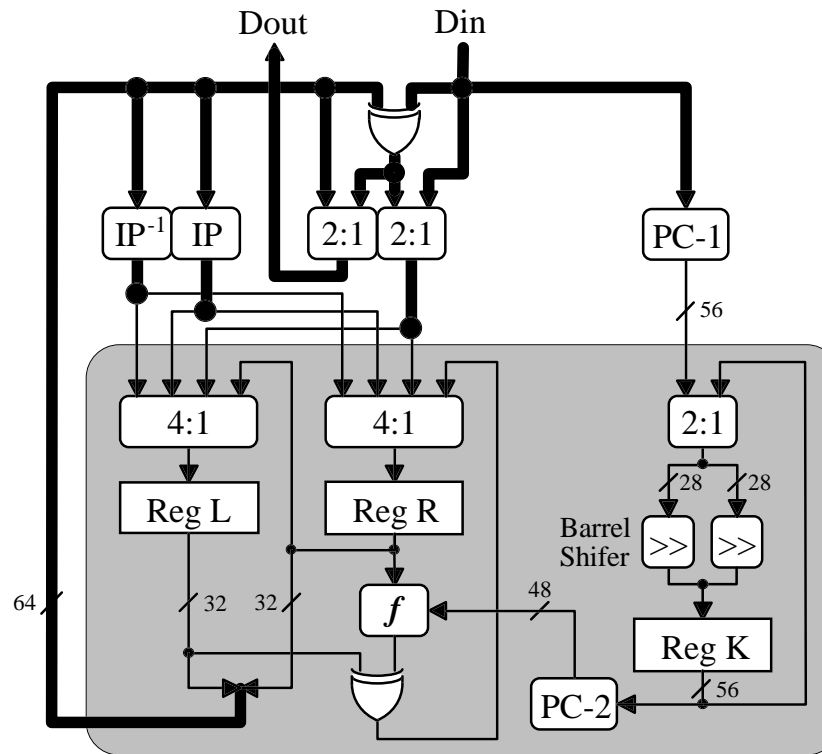
- 512-bit RSA
 - $(512+1) \times (512+4) / 48\text{MHz}$
=5.5 msec

RICO-1 Power Vs Frequency



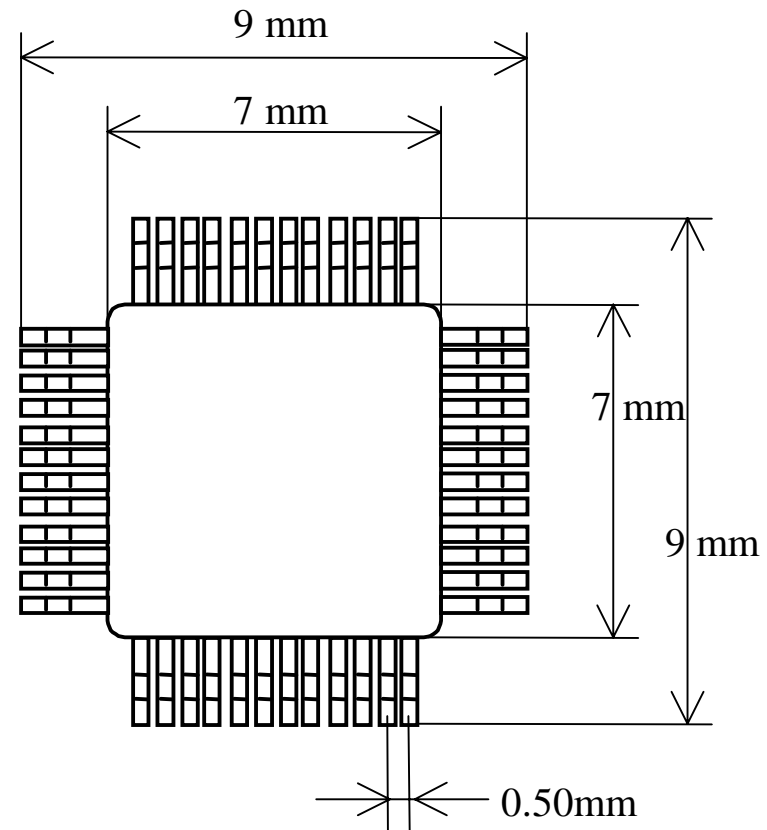
RICO-1 DES Circuit

- 19.9MB/sec @ 45MHz (18cycles for 64-bit data)
- ECB,CBC,CFB,OFB supported by XOR and selector



RICO-2 VLSI

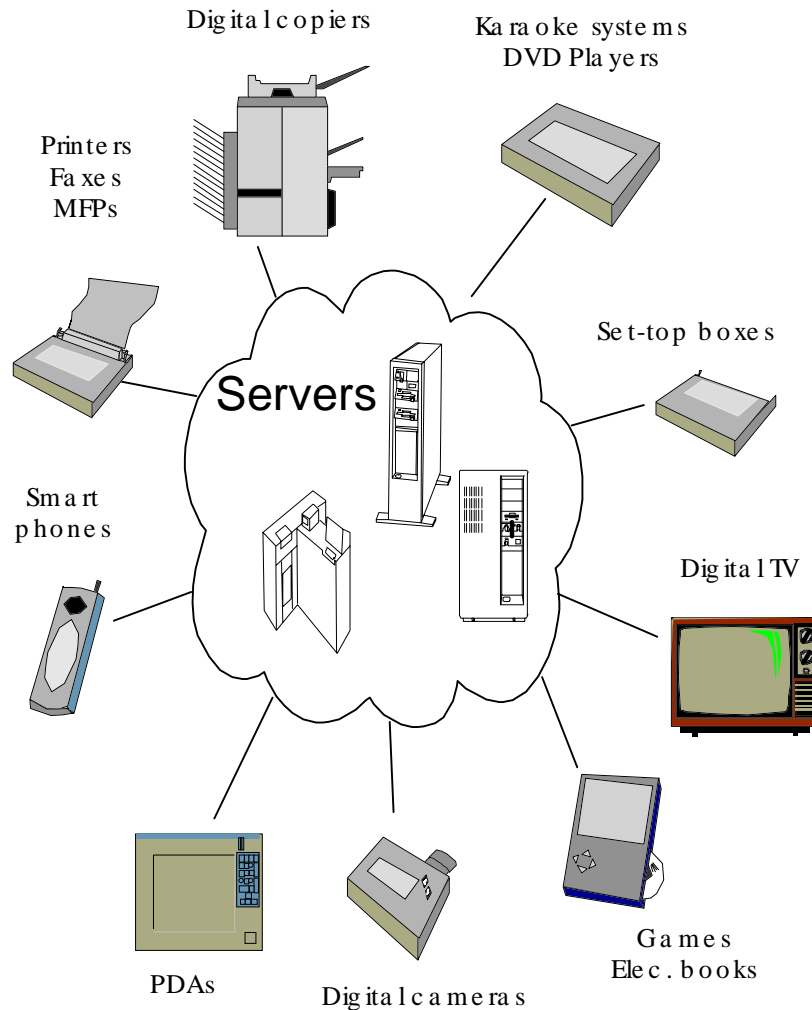
- Same accelerator core with RICO-1
- Tamper resist
 - Write-only key regs.
 - Key scrambling
- 48-pin PQFP
- 5v/3.3v operational
- 0.5um CMOS



Applications

- Various security products using RICO discrete chips
 - Crypto PCI, PCMCIA
- Smartcard chips
- Embedded security for various embedded systems

An Example of Applications



- Various embedded systems are connected to the network
- Those embedded systems require IT security nature
- High-performance and small crypto VLSI (RICO) enables those applications

Next Steps

- Performance-oriented design
 - Combination of multi-stage carry-skip adder and other advanced techniques
 - Only 15-gate delay for 2048-bit adder
 - Less than 10ms for 2048-bit RSA (estimate)
 - Aim at high-performance server applications
- Area-oriented design
 - Optimized area and performance, targeting Smartcard applications

Summary

- High-performance 1024-bit crypto accelerator developed
 - High speed : 22ms @ 48MHz
 - Small : 4.9mm² core
 - Low power : 350mW at max
- RICO architecture
 - Pipeline and parallel operations
 - Cycle steal modular operations
 - High-speed carry-skip adder
 - Optimized logic and layout
 - Tamper resist especially for timing attack