



Hardware Implementation of RSA in Japan

1997 RSA Data Security Conference

Katsuhiko AOKI (aoki@ao.nel.co.jp)

NTT Electronics Technology Corporation

NEL



Outline

1. Merits of Hardware Implementation

- Performance
- Tamper-proof Key Storage

2. RSA LSI and Applications

- New Modular Exponentiation LSI
- PCcard, ISA Adapter
- System Application

3. Consideration of Fault-Based Attacks

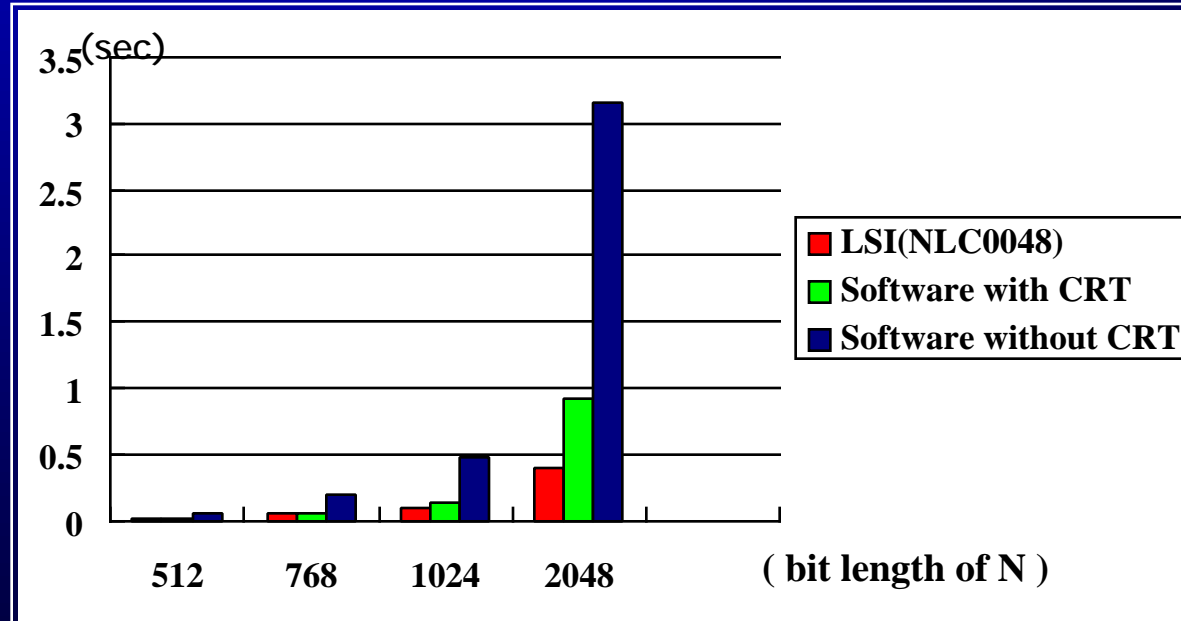


Merits of Hardware Implementation(1)

❖ Improve System Performance

- High-Speed Operation by Specified LSI
- Eliminate CPU Load

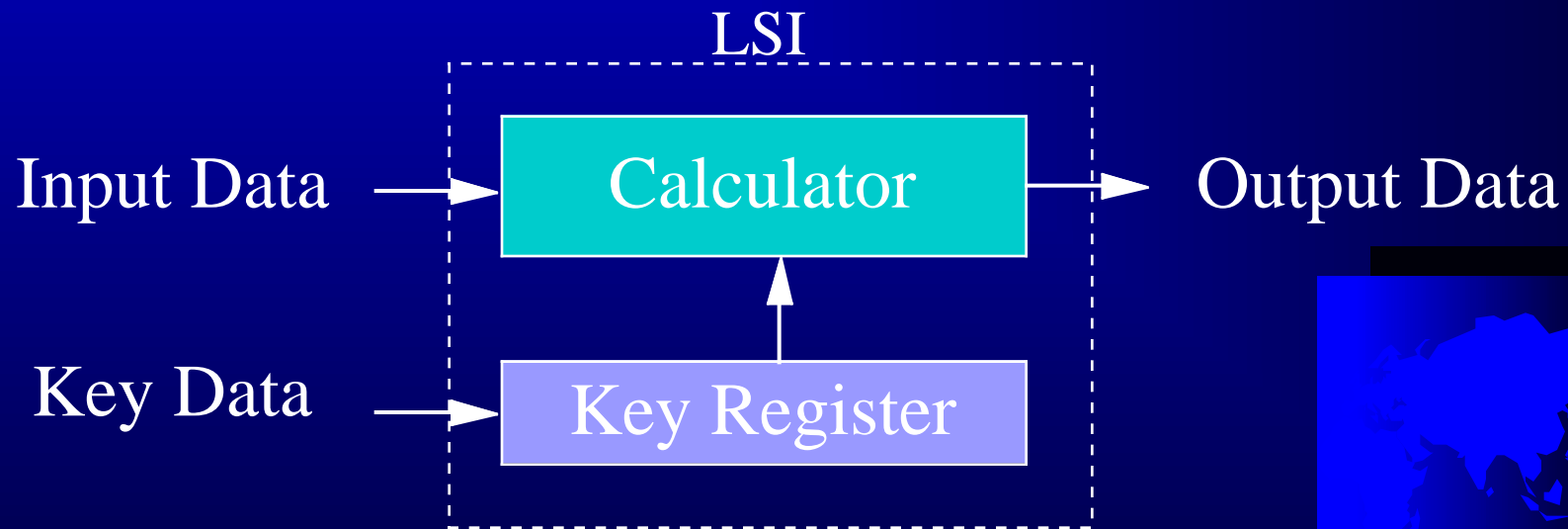
Execution time of $C = M^e \bmod N$



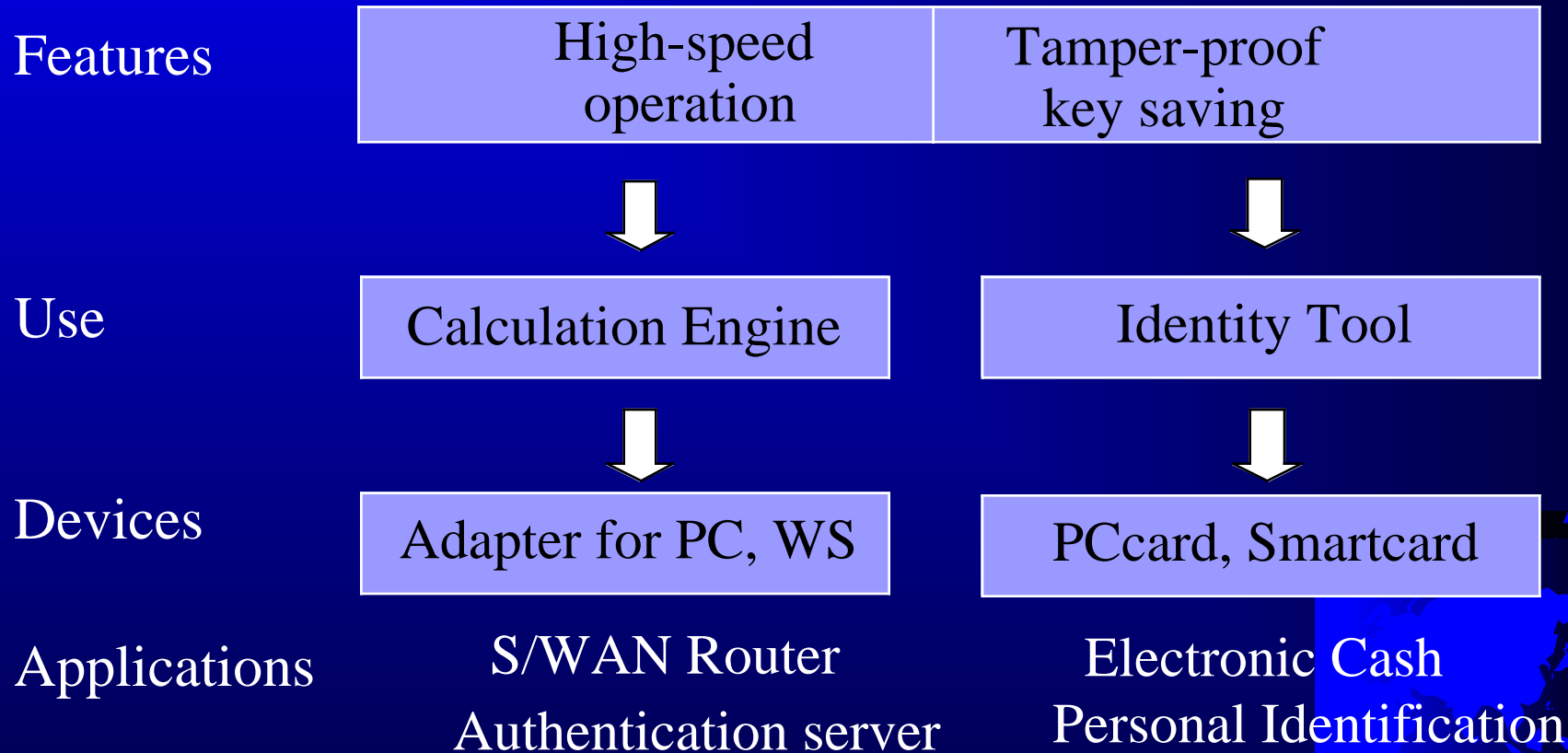
Merits of Hardware Implementation(2)

❖ Tamper-proof Key storage

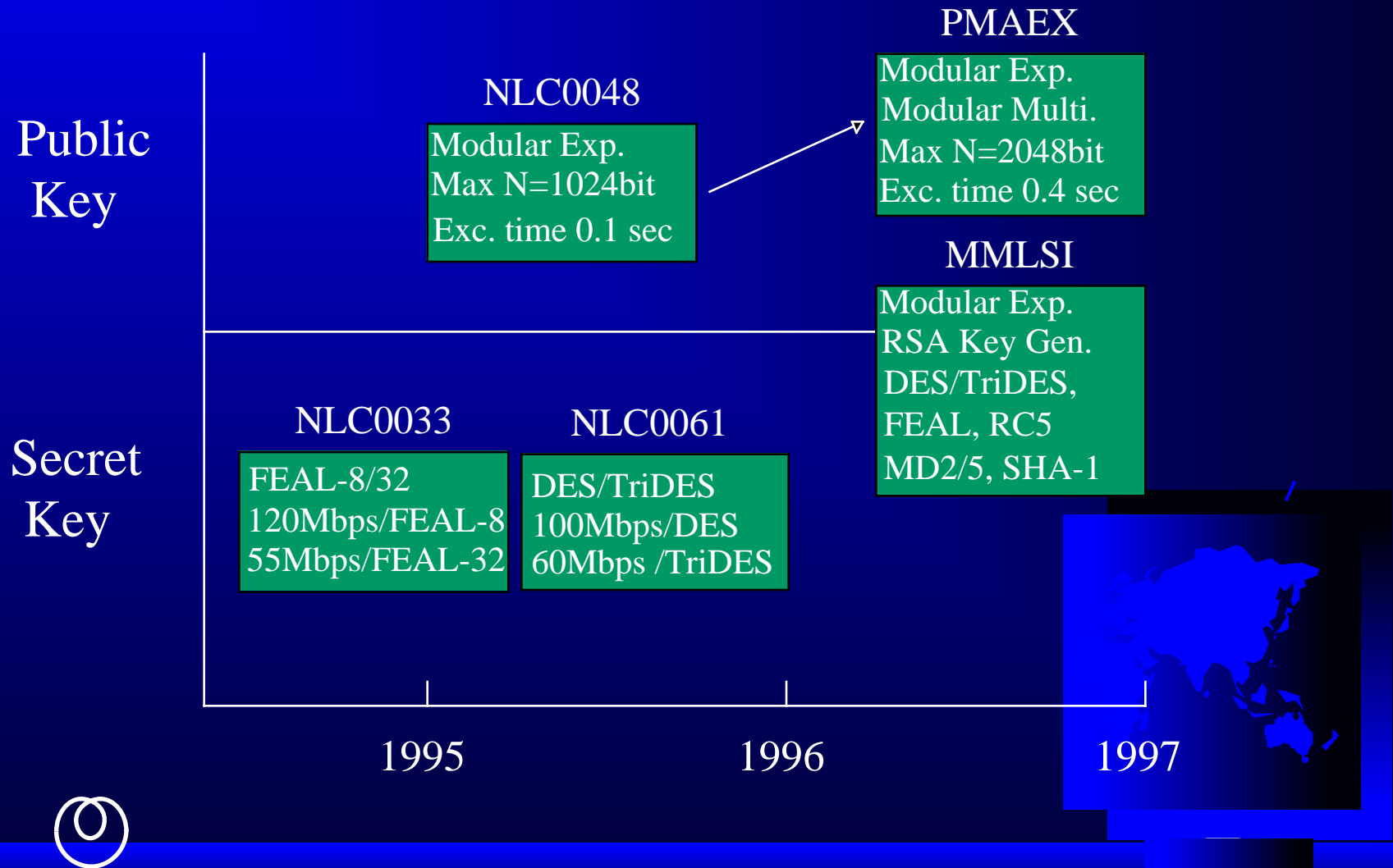
Write-only register in LSI makes it impossible for anyone to read or copy key data.



Usage of this feature



NEL Crypto LSIs (preliminary)



Overview of NLC0048(1)

- ❖ Execute modular exponentiation with arbitrary parameter lengths of up to 1024 bits.

$$C = M^e \bmod n \quad (n, e, M \in \dots 1024)$$

- ❖ High-speed operation. The longest parameters of 1024 bits are processed in an average of 0.1 seconds.

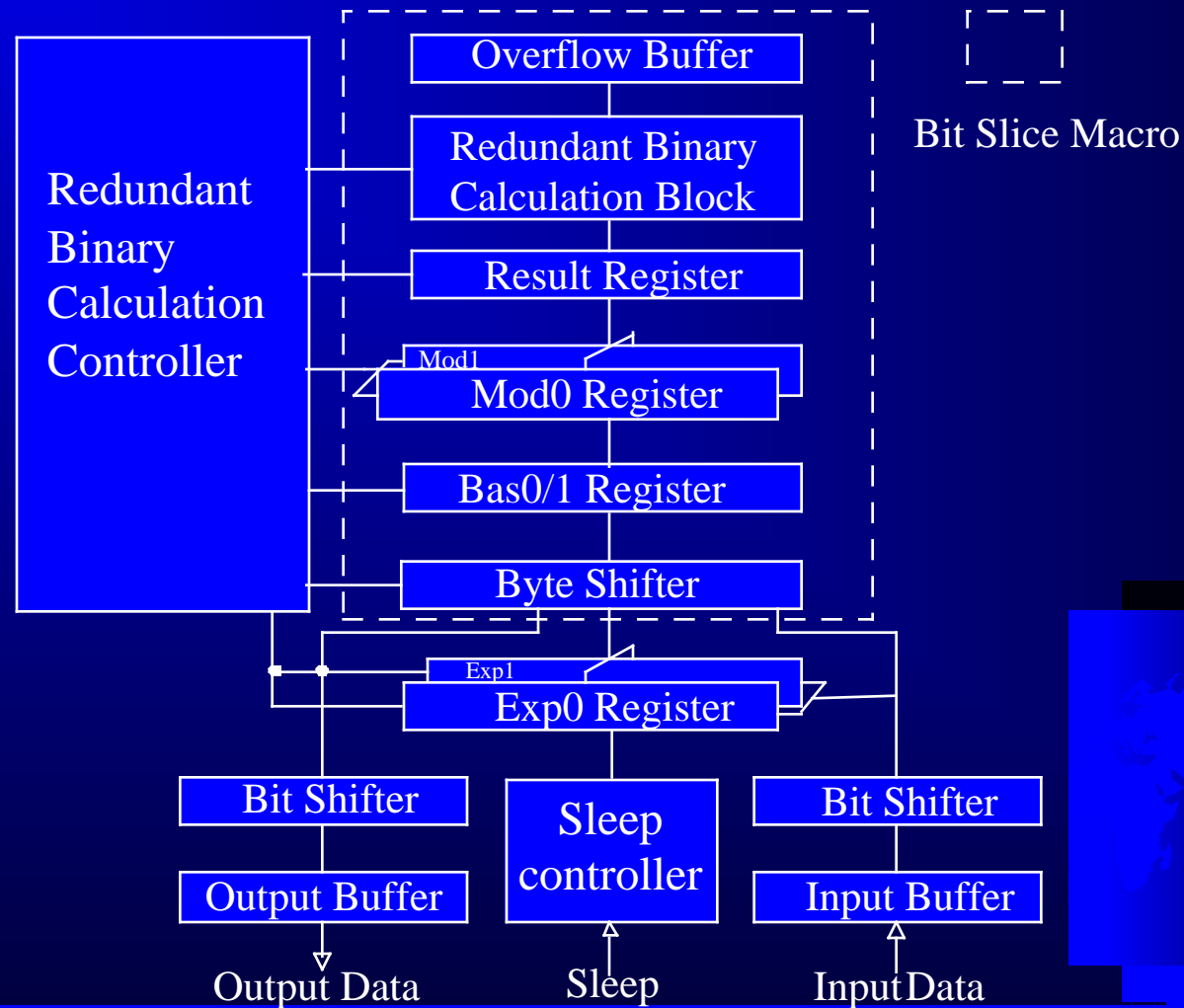


Overview of NLC0048(2)

- ❖ Two register groups for encryption and decryption.
One exponentiation parameter is held in the write-only register.
- ❖ The byte length of the processing results is attached to the head of readout data.
- ❖ Full CMOS logic enables battery back.



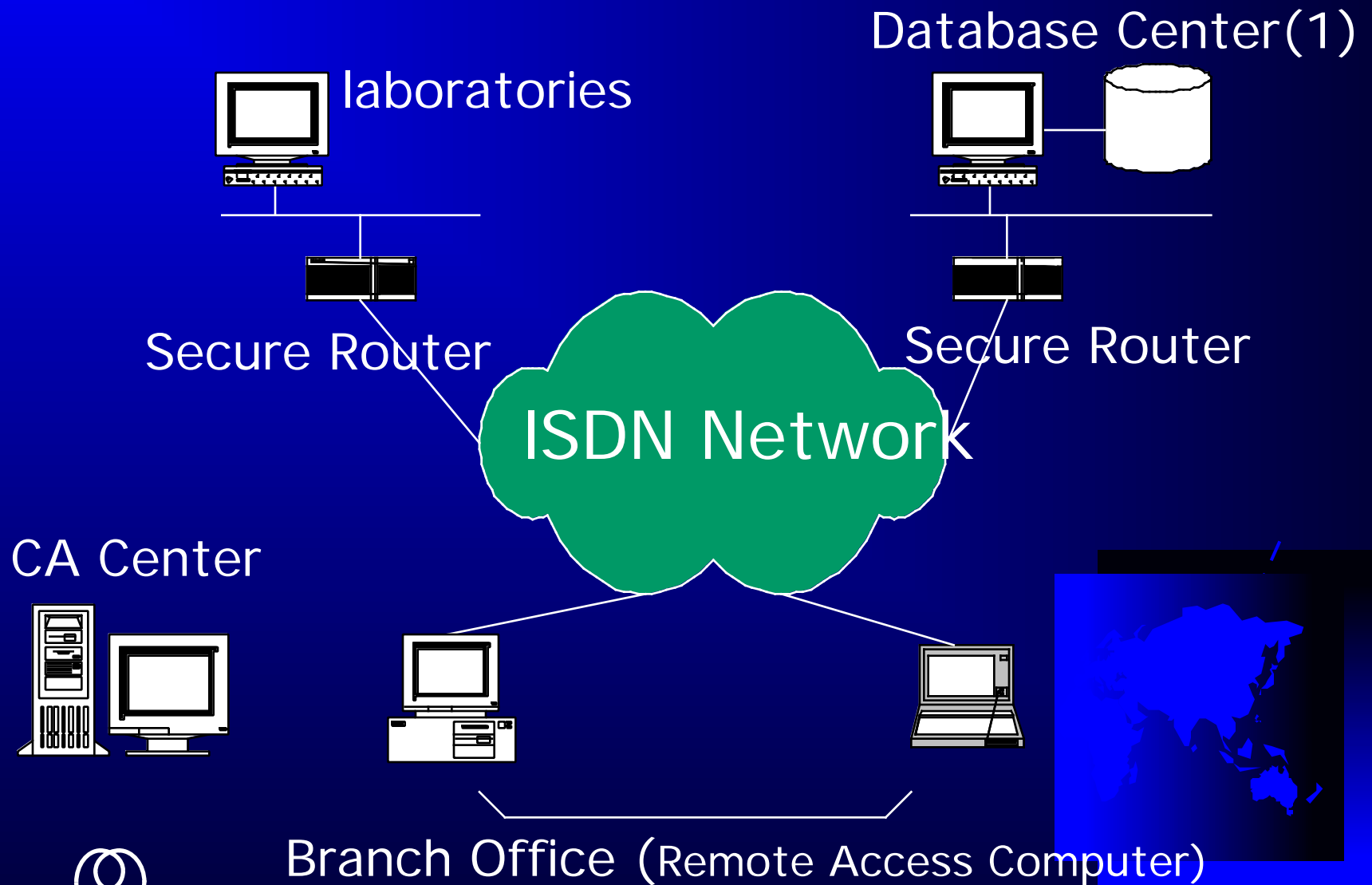
Block Diagram of NLC0048



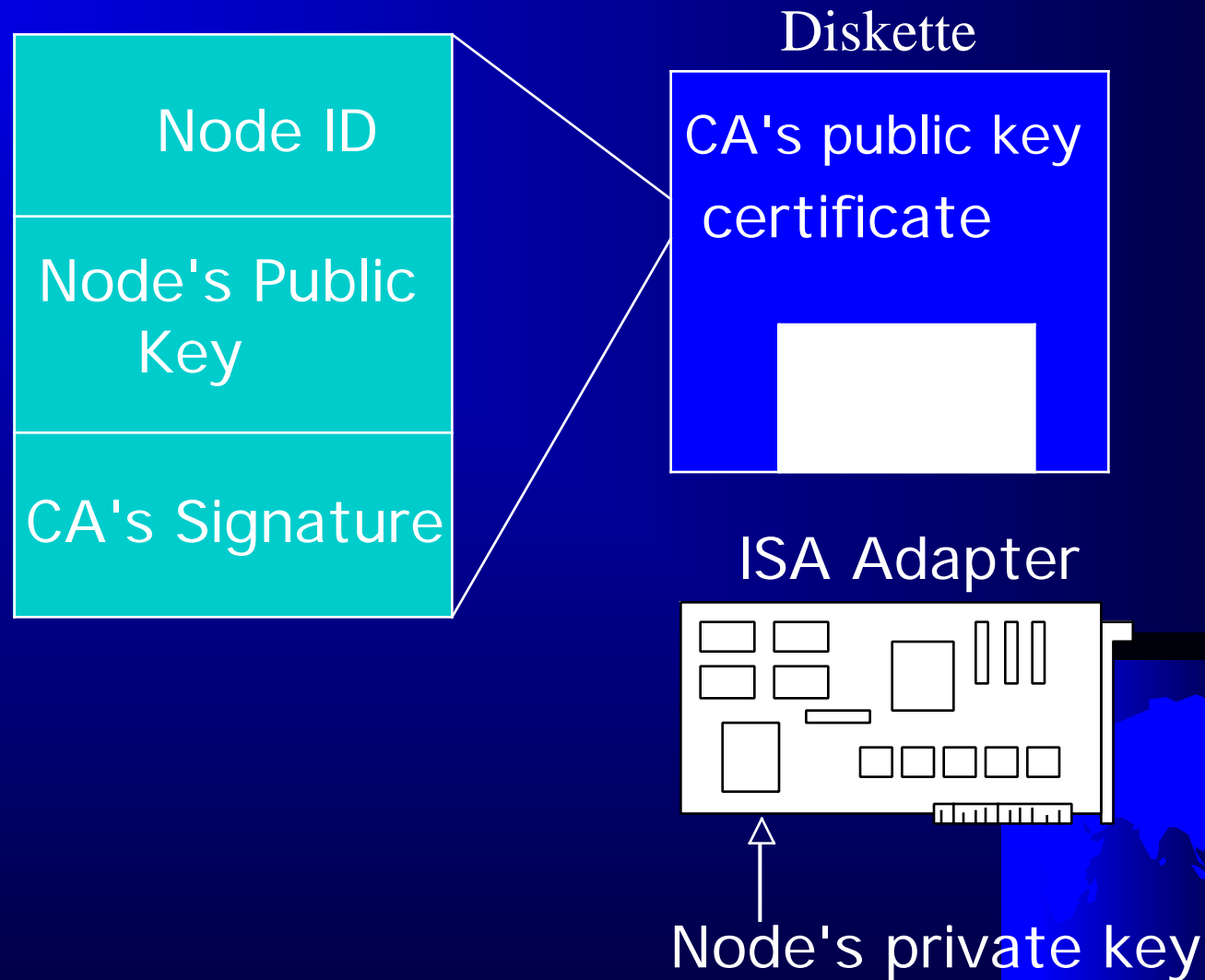
ISA Adapter, PCcard

	DES/RSA PCard DES/RSA ISA Adapter	High Security Card
Type	Intelligent	Non Intelligent
Main LSIs	CPU, NLC0048, RAM 512Kbyte FlashROM 4Mbyte	NLC0061T(DES/ TriDES), NLC0048(Modular Exp.)
Functions	User Identification Mutual Authentication Encryption by RSA Random Number Gen.	DES/ TriDES Operation Modular Exponentiation
Application Example	Secure WAN System	Data Vault System

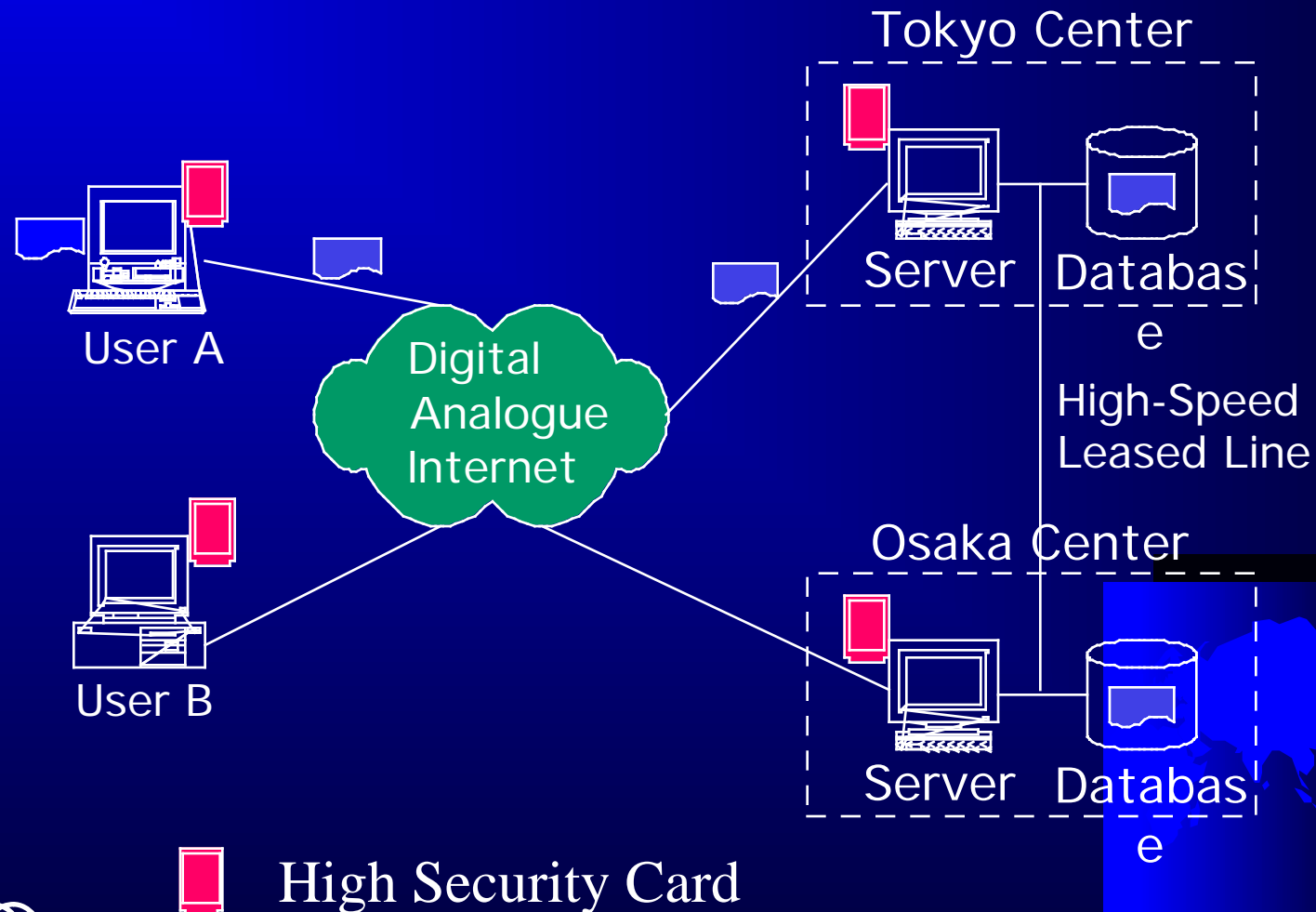
One Example of Secure WAN System



Certificate



Network of Data Vault System



Defense Against Fault-Based Attacks(1)

- ❖ Researchers: D.Boneh, R.Demillo, R.Lipton
- ❖ Target Protocol: RSA with CRT
- ❖ Fault required: Any fault
- ❖ Stress: Incorrect Voltage, Atypical Clock, Heat, Ionizing radiation ...
- ❖ Defense: Difficult to provide hardware against all kinds of stress...
Verification after signing



Defense Against Fault-Based Attack(2)

- ❖ Researchers: D.Boneh, R.Demillo, R.Lipton
E.Biham, A.Shamir
- ❖ Target Protocol: RSA without CRT
Secret Key (DES, RC5...)
- ❖ Fault required: Single bit Error
- ❖ Stress: Ionizing radiation ...
- ❖ Defense: Use of SIMOX Substrate



SIMOX

