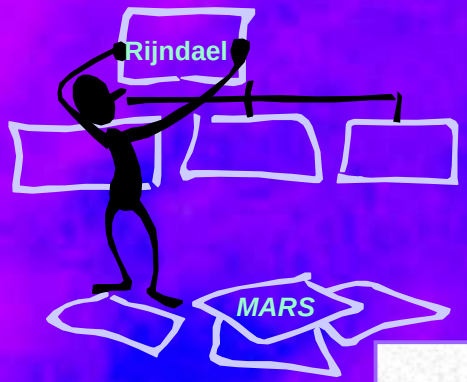
The World's Fastest Hardware Cipher

IBM Japan Ltd.
Tokyo Research Laboratory
A.Satoh S.Morioka

Hard Standardization Work



CSRC NIST

Home Library Services Events Advisories Contact Site Map

SEARCH

GO

advanced search

AES
Draft FIPS
Submit Comments

AES Code & Vectors

/ Encryption / AES

AES

Advanced Encryption Standard

Draft FIPS for the AES

On February 28, 2001, NIST announced that a Draft Federal Information Processing Standard (FIPS) for the AES is available for public review and comment.

NESSIE

New European Schemes for Signatures, Integrity, and Encryption

IST-1999-12324

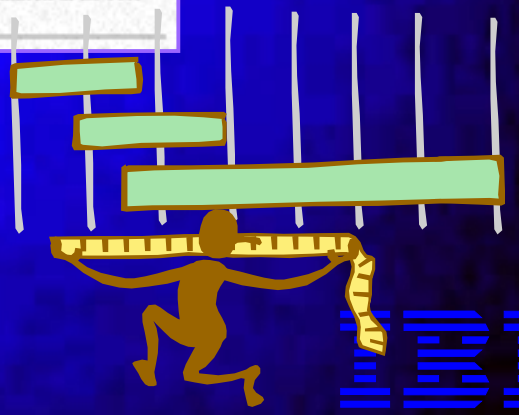
NESSIE is a project within the Information Societies Technology (IST) Programme of the European Commission (Key Action II, Action Line II.4.1).

Disclaimer: The information on this web site is provided as is and no guarantee or warranty is given

IPA ISEC The Information-technology Security Center セキュリティセンター

暗号技術の評価事業について

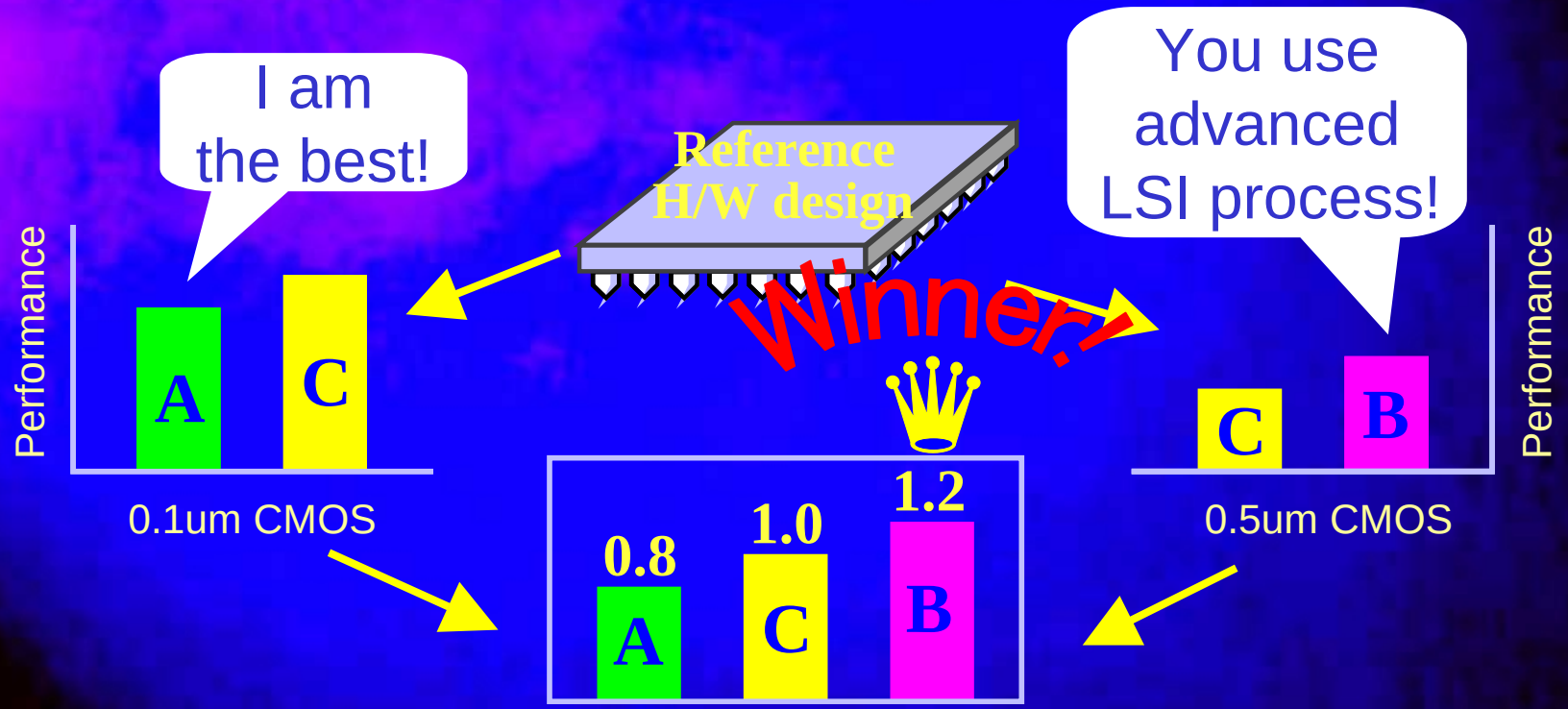
- 量子暗号に関する調査・研究報告書
- 次世代認証方式の研究・開発動向の調査報告書
- 欧州における暗号政策および暗号評価機関に関する調査報告
- 平成12年度暗号技術報告書について
- 暗号技術の詳細評価について
- 暗号技術の公募について
- 暗号技術の評価について



IBM

Hard Hardware Comparison

- Hard to decide superiority of algorithms using H/W implemented by different ASIC libraries



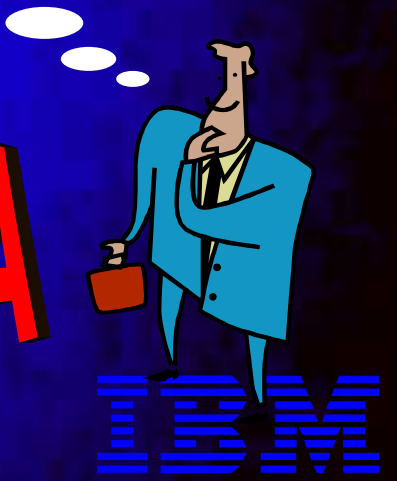
IBM

Best Reference Algorithm

- DES can be the good reference
- High-performance DES H/W design is not free

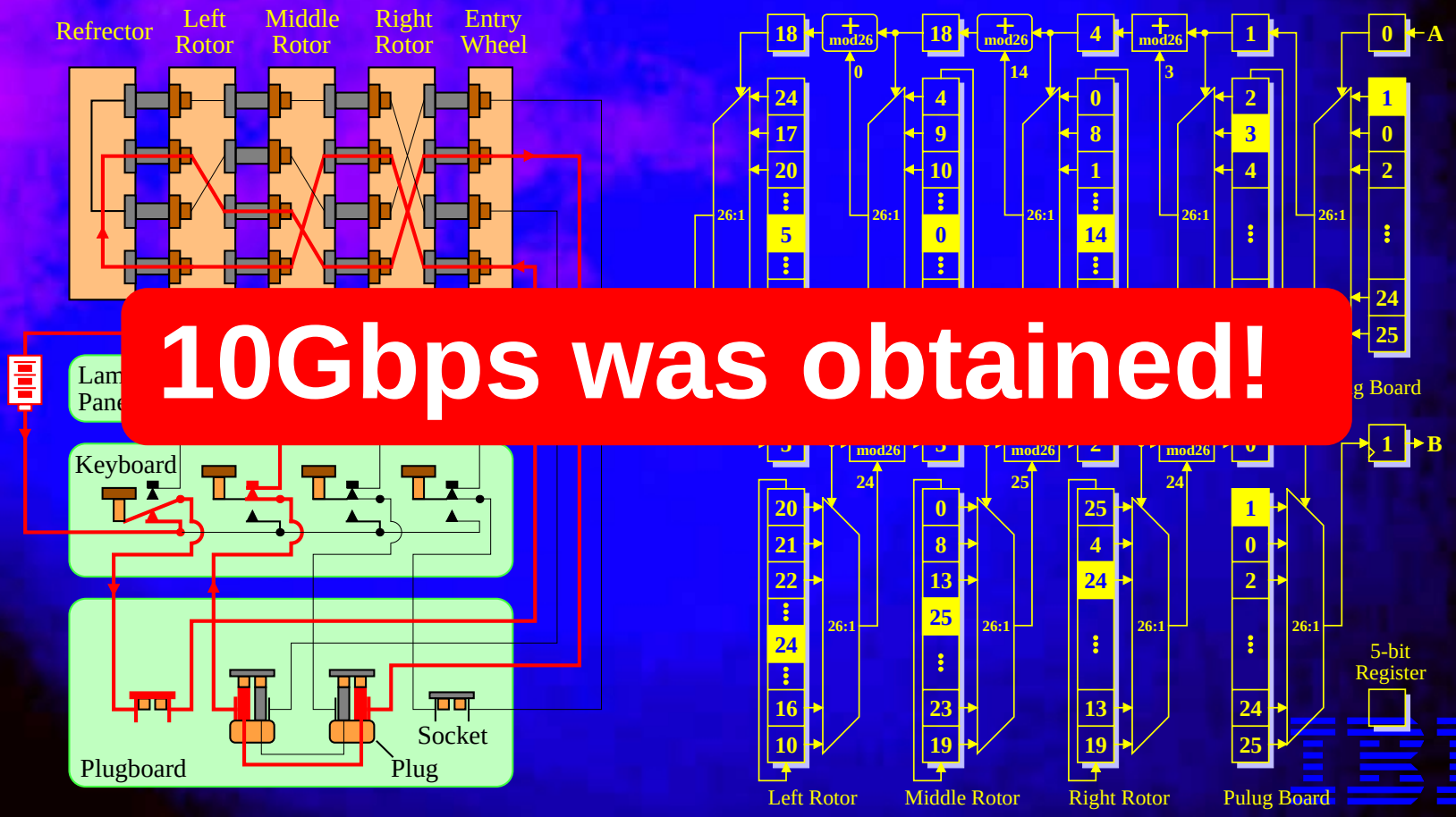
- Widely used
- High performance in H/W
- H/W design can be free

ENIGMA



H/W Emulation H/W

- Rotors are emulated by shift registers
- Rotors and plug-board wirings are defined as tables

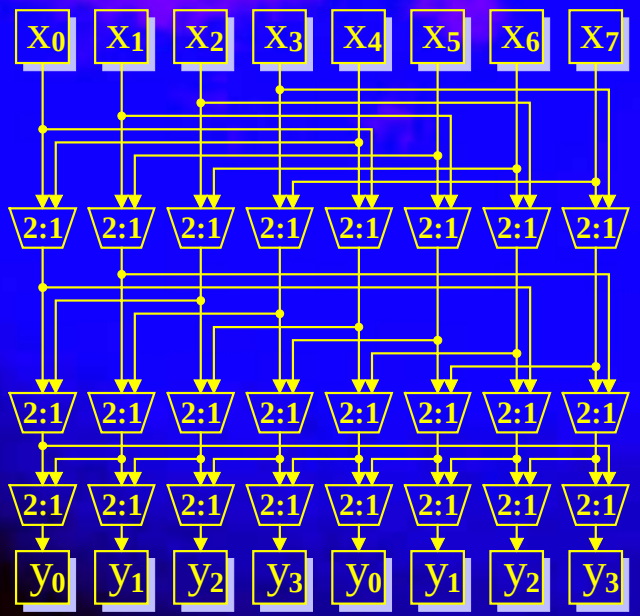


10Gbps was obtained!

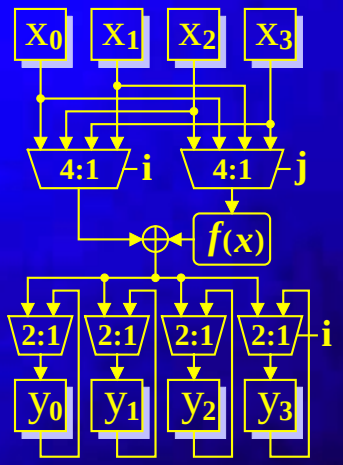
Wires are Weird

- Wires have no function, but
- Wires consume large power dissipation
- Wires spend lot of delay time
- Wires are here, there, everywhere…

```
y = x << n;
```




```
for (i = 0; i < 3 i++) {
    j = i + 1 % 4;
    y(i) = x(j) ^ f(x(i));
}
```



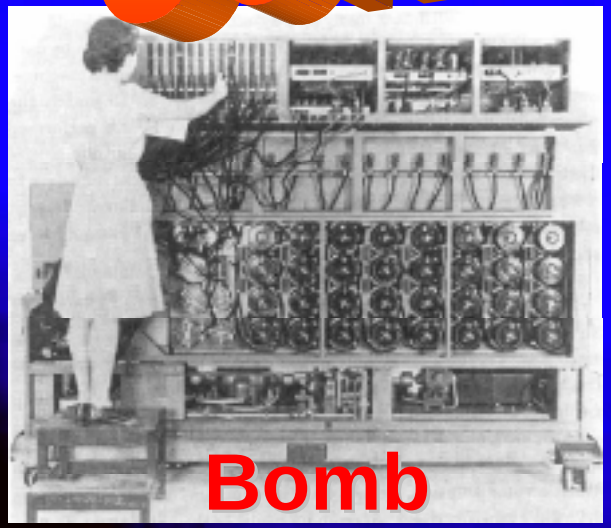
IBM

Access Now !

Enigma H/W code is absolutely free!

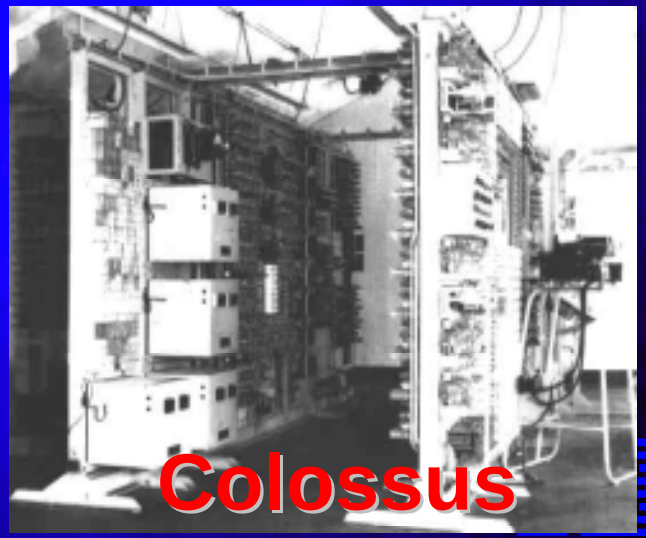
http://www02.so-net.jp/~morioka/enigma.htm

Coming Soon!



Bomb

and



Colossus

IBM