

The World's Fastest Hardware Cipher

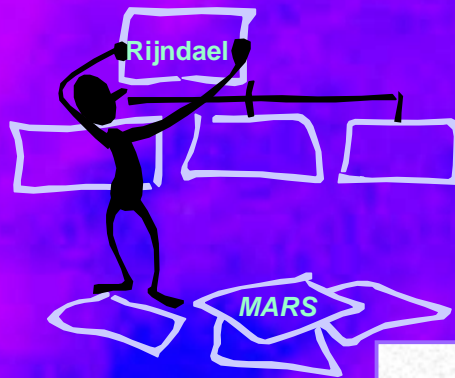
IBM Japan Ltd.

Tokyo Research Laboratory

A.Satoh S.Morioka



Hard Standardization Work

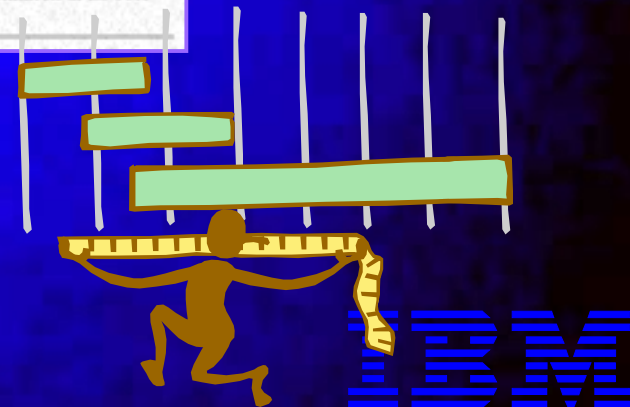


A screenshot of the Cryptographic Standards Research Center (CSRC) website. The page is titled 'AES' (Advanced Encryption Standard) and features a section for 'Draft FIPS for the AES'. The text on the page states: 'On February 28, 2001, NIST announced that a Draft Federal Information Processing Standard (FIPS) for the AES is available for public review and comment.' The website header includes 'NIST' and navigation links like 'Home', 'Library', 'Services', etc.

A screenshot of the NESSIE project website. The title is 'NESSIE' in large red letters, followed by the subtitle 'New European Schemes for Signatures, Integrity, and Encryption' and the identifier 'IST-1999-12324'. Below this, it states: 'NESSIE is a project within the Information Societies Technology (IST) Programme of the European Commission (Key Action II, Action Line II.4.1). A disclaimer at the bottom reads: 'Disclaimer: The information on this web site is provided as is and no guarantee or warranty is given... as the information at its sole...'

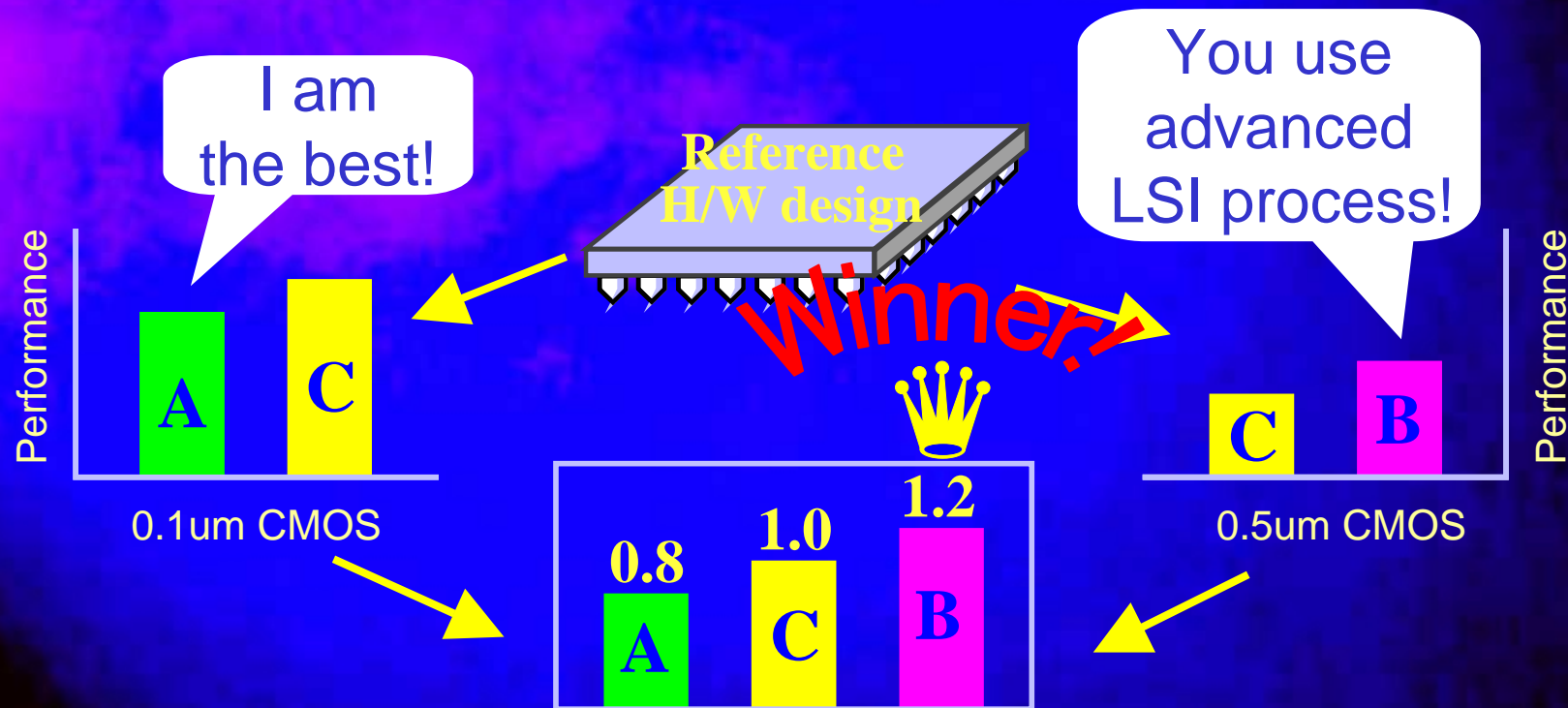
A screenshot of the IPASEC website. The header features the logo 'IPASEC' and the text 'The Information Technology Security Center セキュリティセンター'. The main heading is '暗号技術の評価事業について' (About Cryptography Evaluation Projects). Below this is a list of project topics in Japanese:

- 量子暗号に関する調査・研究報告書 **News!!**
- 次世代認証方式の研究・開発動向の調査報告書 **News!!**
- 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 **News!!**
- 平成12年度暗号技術報告書について **News!!**
- 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



Hard Hardware Comparison

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



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

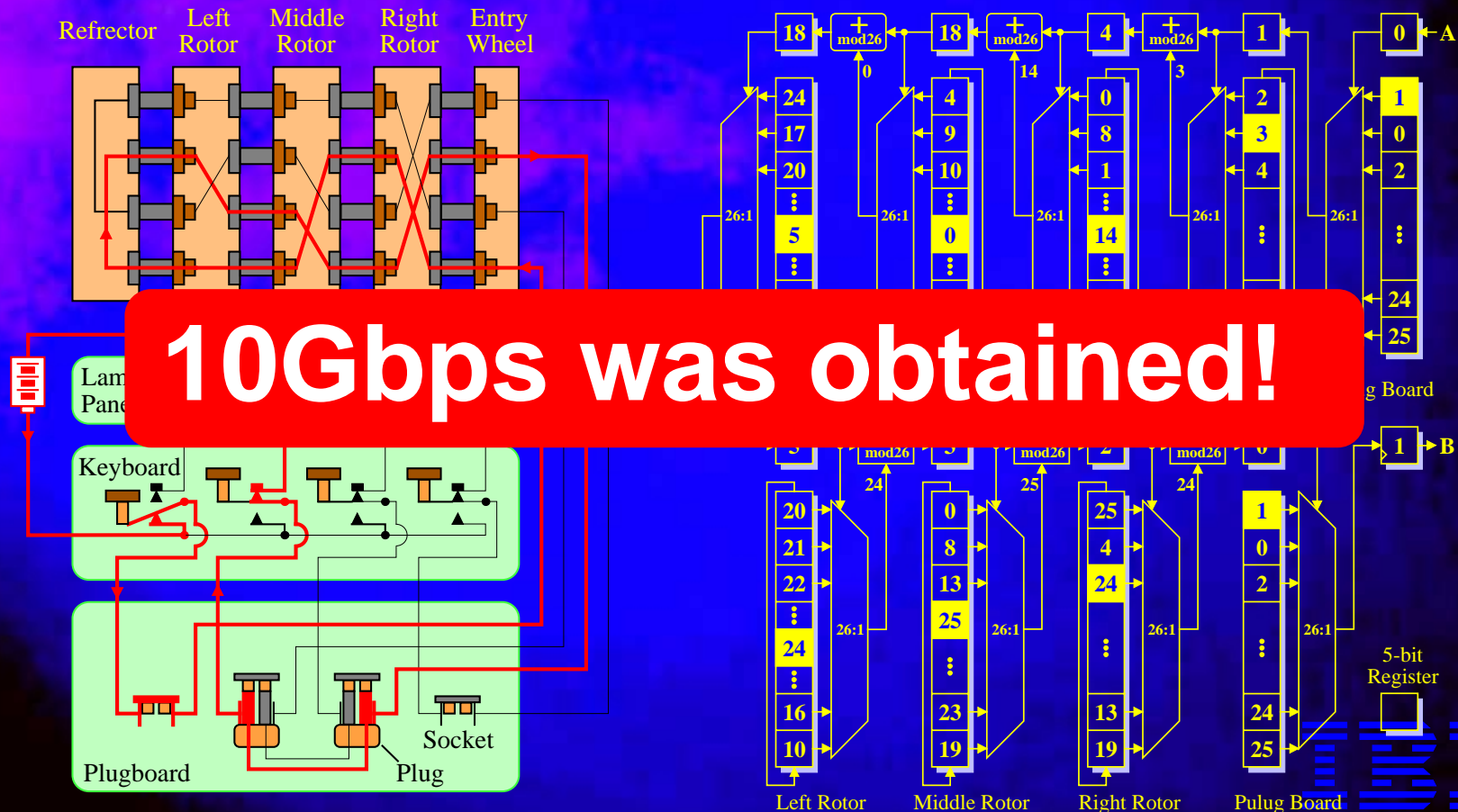


ENIGMA



H/W Emulation H/W

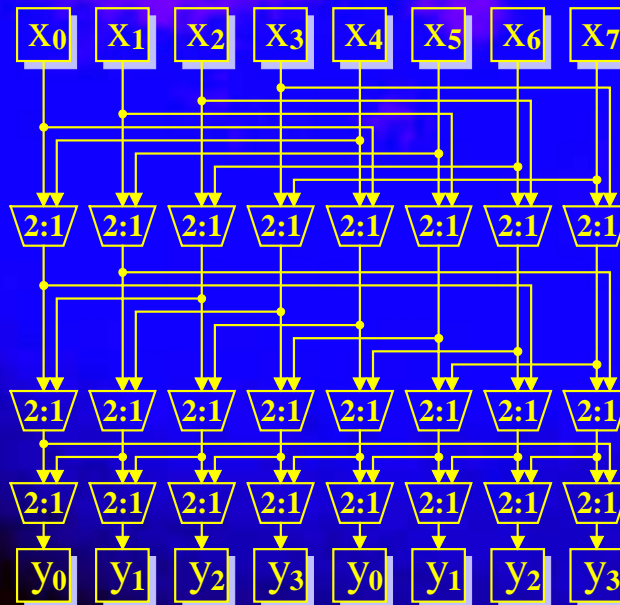
- ◆ Rotors are emulated by shift registers
- ◆ Rotors and plug-board wirings are defined as tables



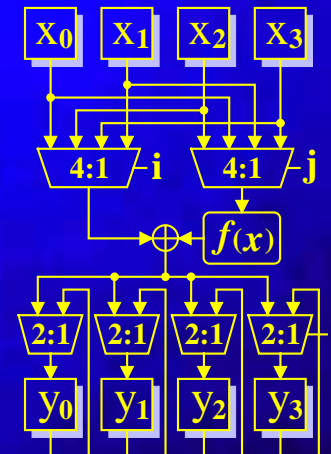
Wires are Weird

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

$y = x \ll n;$



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

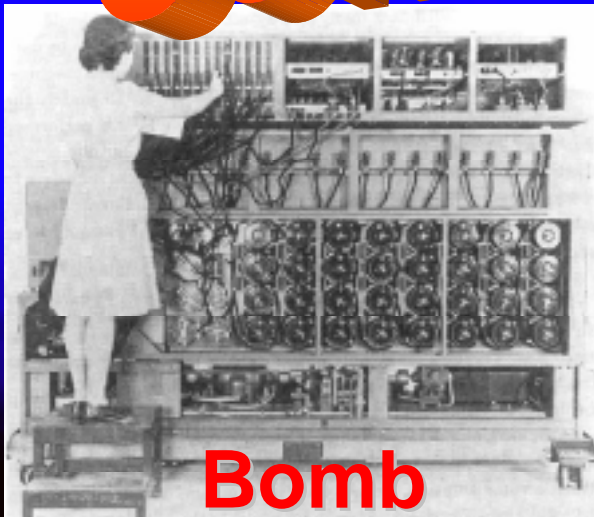


Access Now !

Enigma H/W code is absolutely free!

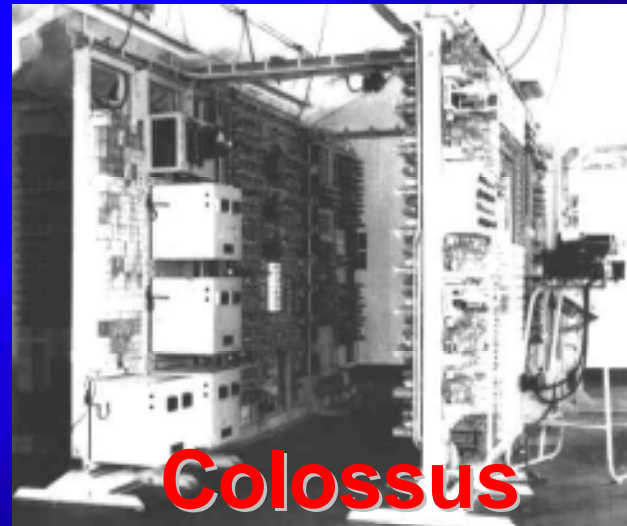
[http://www02.so-net.jp/
~morioka/enigma.htm](http://www02.so-net.jp/~morioka/enigma.htm)

Coming Soon!



Bomb

and



Colossus

