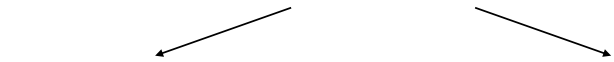
ECE 646 - Lecture 2

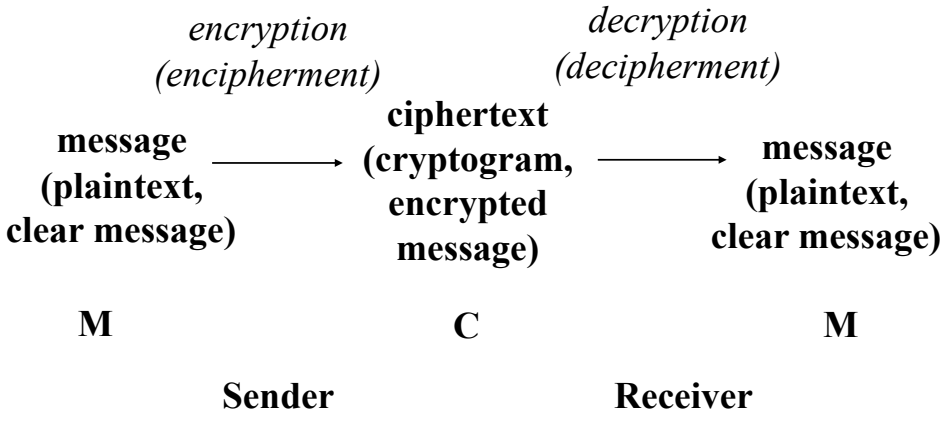
Basic Concepts of Cryptology



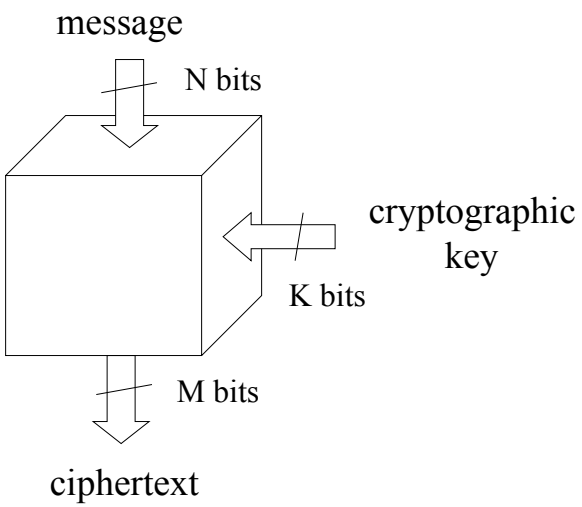
from Greek

cryptos - hidden, secret
logos - word
graphos - writing

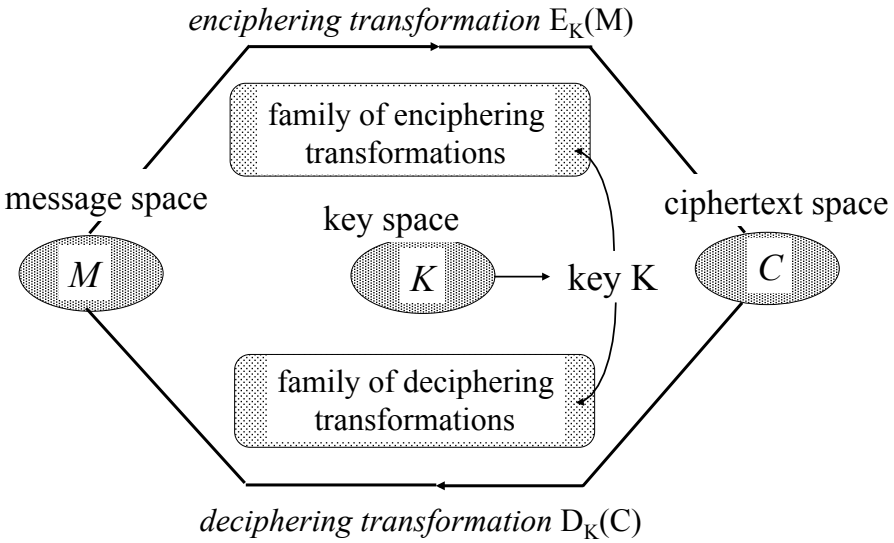
Basic Vocabulary



Cryptosystem (Cipher)



Definition of a cryptosystem (cipher)



$\forall$ K $\in K$ $\forall$ M $\in M$ $\quad D_K(E_K(M)) = M$

Substitution Cipher

Key = $\begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ f & q & i & s & h & n & c & v & j & t & y & a & u & w & d & r & e & x & l & b & m & z & o & g & k & p \end{pmatrix}$

enciphering

TO BE OR NOT TO BE

BD QH DX WDB BD QH

deciphering

TO BE OR NOT TO BE

Number of keys = 26! $\approx 4 \times 10^{26}$

Kerckhoff's principle

The security of a cipher MUST NOT depend on anything that cannot be easily changed

Auguste Kerckhoff, 1883

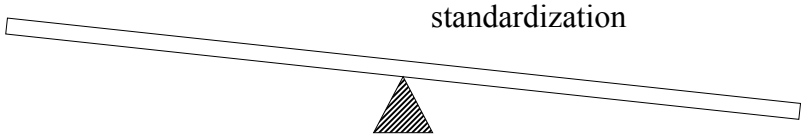
Unpublished vs. published algorithm?

Unpublished algorithm

1. Cryptanalysis must include recovering the algorithm
2. Smaller number of users, smaller motivation to break
3. Unavailable for other countries

Published algorithm

1. The only reliable way of assessing cipher security
2. Prevents backdoors hidden by designers
3. Large number of implementations = low cost + high performance
4. No need for anti-reverse-engineering protection
5. Software implementations
6. Domestic and international standardization



Fundamental Tenet of Cryptography

If lots of smart people have failed to solve a problem, then it probably will not be solved anytime soon.

Security of unpublished ciphers

Commercial packages cracking unpublished encryption schemes built-in:

- MS Word, MS Excel, MS Money
- Word-Perfect, ProWrite, Data Perfect
- Lotus 1-2-3, Symphony, Quattro-Pro
- Paradox, Semantec's Q&A
- PKZip, etc.

Time: 1-2 minutes for old versions of programs
up to several days for new versions of some programs

Price: ~ $99 per module (in the past), $595 per toolkit (49 modules)

Companies: Access Data
Crak Software

Passwords recovered even for empty files!

Breaking ciphers used in GSM, 1999 (1)

GSM - world's most widely used mobile telephone system

- 51% market share of all cellular phones, both analog and digital
- over 215 million subscribers in America, Europe, Asia, Africa, and Australia
- In the US, GSM employed in the "Digital PCS" networks of Pacific Bell, Bell South, Omnipoint, etc.

Two voice *encryption algorithms*:

A5/1 and A5/2

encrypt voice between the cell phone and the base station

Breaking ciphers used in GSM (2)

Both voice encryption algorithms

- never published
- designed and analyzed by the secretive "SAGE" group (part of ETSI – European Telecommunications Standard Institute)
- A5/1 believed to be based on the modified French naval cipher

Both algorithms reverse-engineered by "Marc Briceno" with the Smartcard Developer Association published by the Berkeley group

A5/1 in May 1999,
A5/2 in August 1999

Breaking ciphers used in GSM (3)

Published attacks

A5/2

August 1999, Ian Goldberg and David Wagner, U.C. Berkeley

Number of operations in the attack ~ $\mathbf{2^{16}}$

A5/1

May 1999, Jovan Golic

Number of operations in the attack ~ $\mathbf{2^{40}}$

December 1999, Alex Biryukov and Adi Shamir

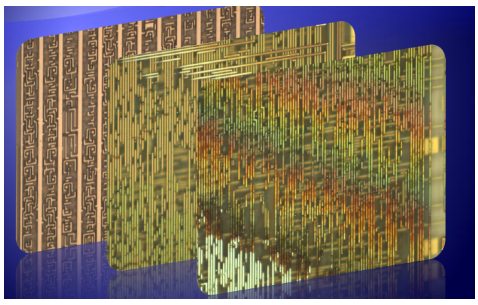
Less than **1 second** on a single PC with 128 MB RAM and two 73 GB hard disks.
Based on the analysis of the A5/1 output during the first two minutes of the conversation.

Attack on Mifare Classics

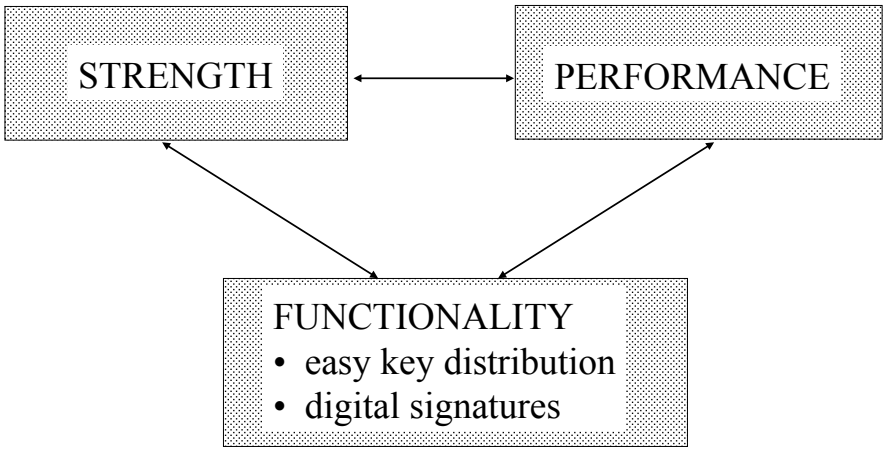
Dec 2007-Apr 2008

Secret algorithm Crypto-1 developed by Philips used, among the others, in the public transport system cards in London (Oyster card), Boston (CharlieCard), Perth (SmartRider), Seoul (T-money), Busan (Mybi), and in Netherlands (OV-Chipkaart) easily broken after successful reverse engineering of the chip.

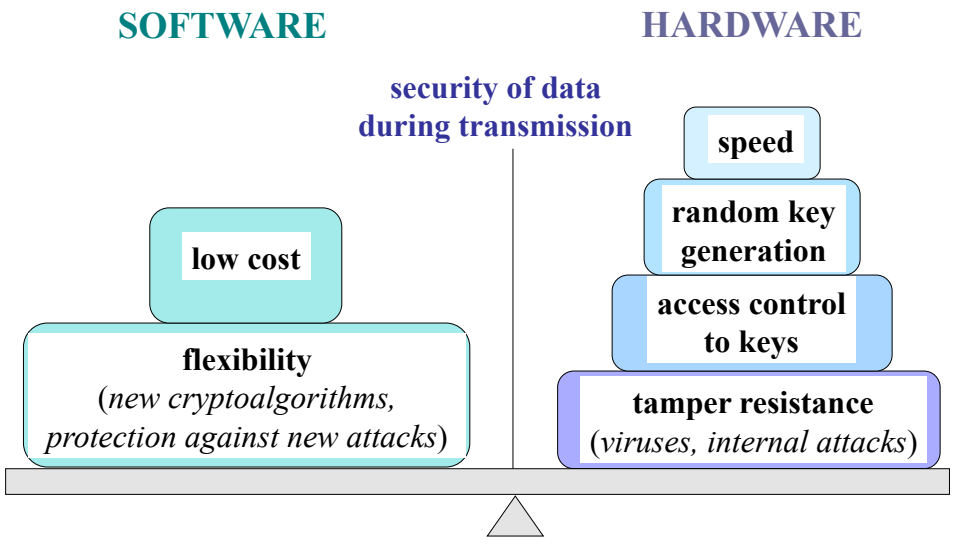
A total of about **1000 million cards** all over the world.



Features required from today's ciphers



Software or hardware?



Basic hardware implementations of cryptography

- VLSI chip (ASIC, FPGA)
- smart card
- PCMCIA card
- cryptographic card
- stand-alone cryptographic device

Why are cryptographic chips needed?

- **hardware accelerators for web servers**

SSL (Secure Socket Layer) – cryptographic protocol used by majority of today's web servers to protect credit card numbers for on-line transactions such as buying a book on the amazon.com

Why are cryptographic chips needed?

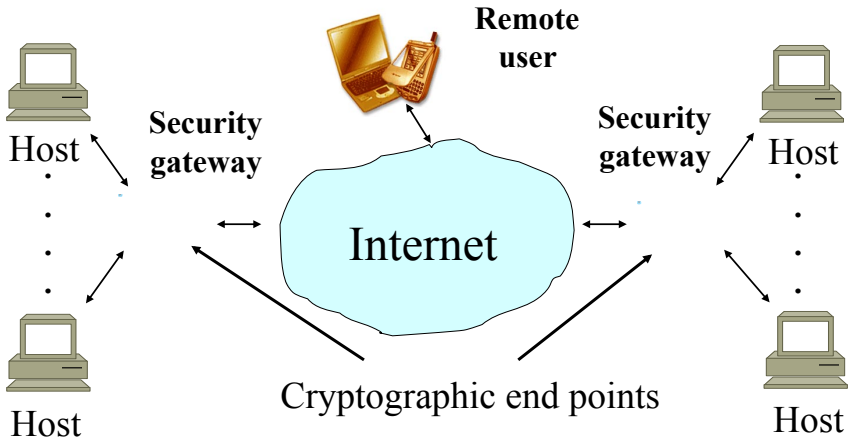
- **hardware accelerators for Virtual Private Networks (VPNs)**

IPSec (Secure Internet Protocol) – cryptographic protocol used to support VPNs (Virtual Private Networks), i.e., secure communication between remote Local Area Networks (LANs) using Internet

IPSec optional in IP ver. 4, required in emerging IP ver. 6

Acceleration can be provided using:
- secure gateways
- secure client PCMCIA cards.

Virtual Private Network

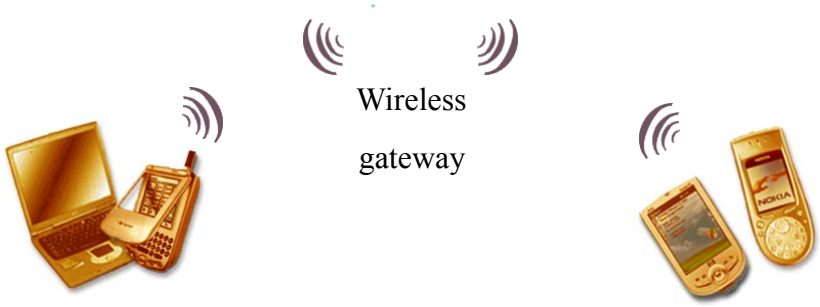


- local networks may belong to the same or different organizations
- security gateways may come from different vendors

Why are cryptographic chips needed?

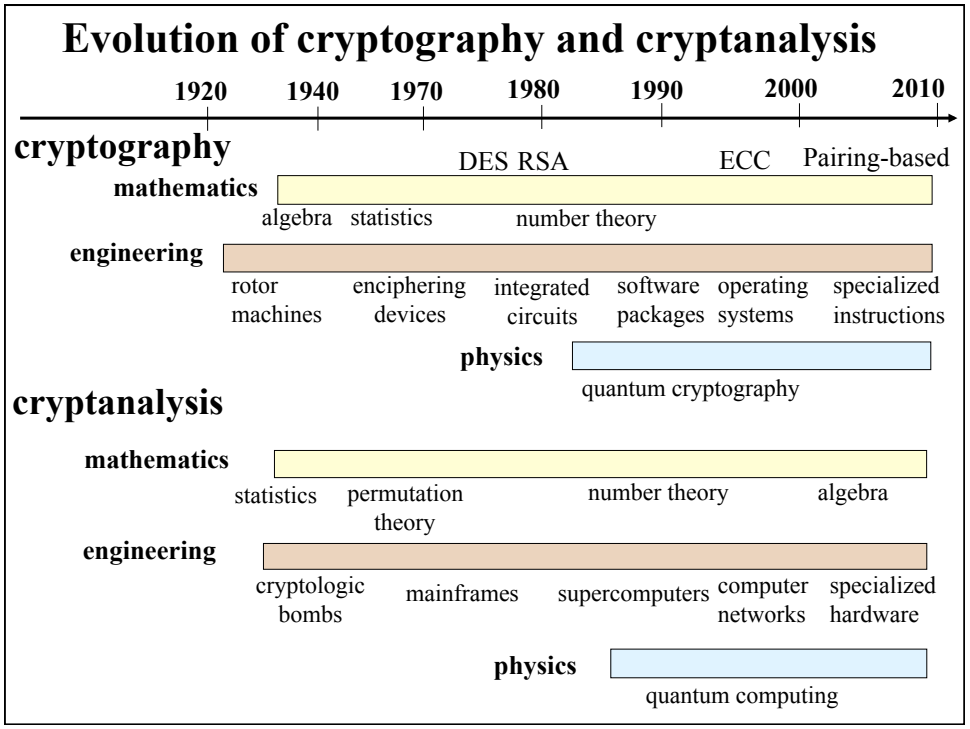
- **hardware accelerators for wireless gateways**

IEEE 802.11 – most popular wireless protocol including strong encryption and authentication

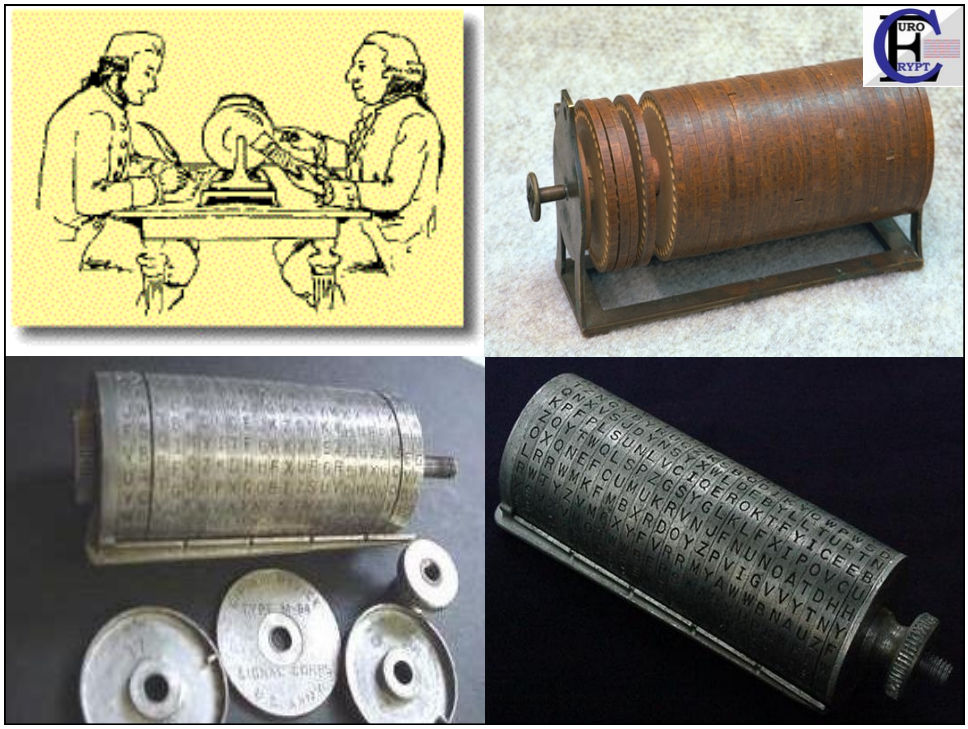


Why are cryptographic chips needed?

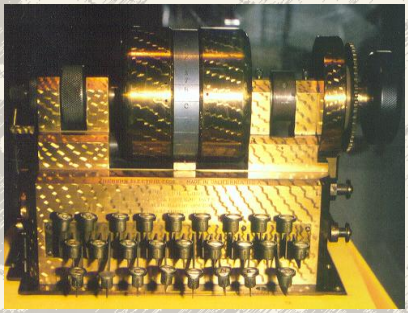
- **secure storage**
- **secure XML supply chain communication**
- **secure phones**
- **secure PDAs**
- **secure satellite communications**
- **cipher breaking**



Progress in Implementations of Cryptography



First Rotor Machines



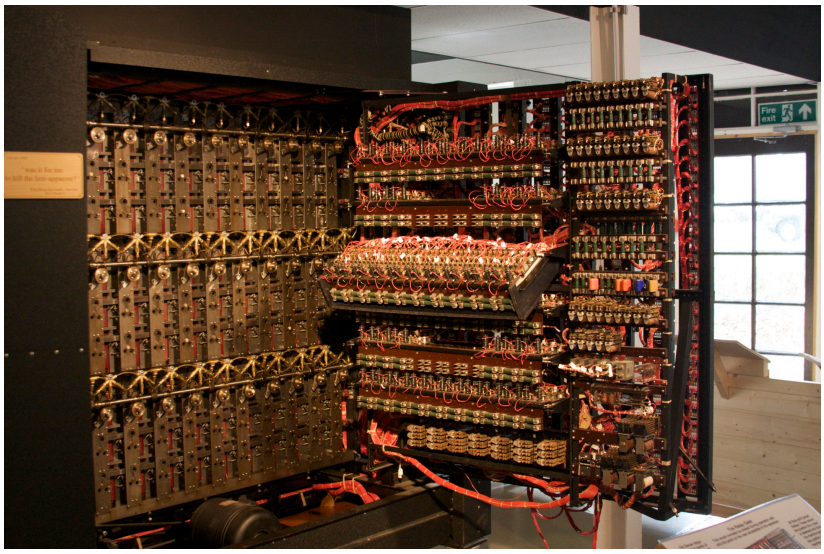
A.Orłowski and K.Gaj

Enigma

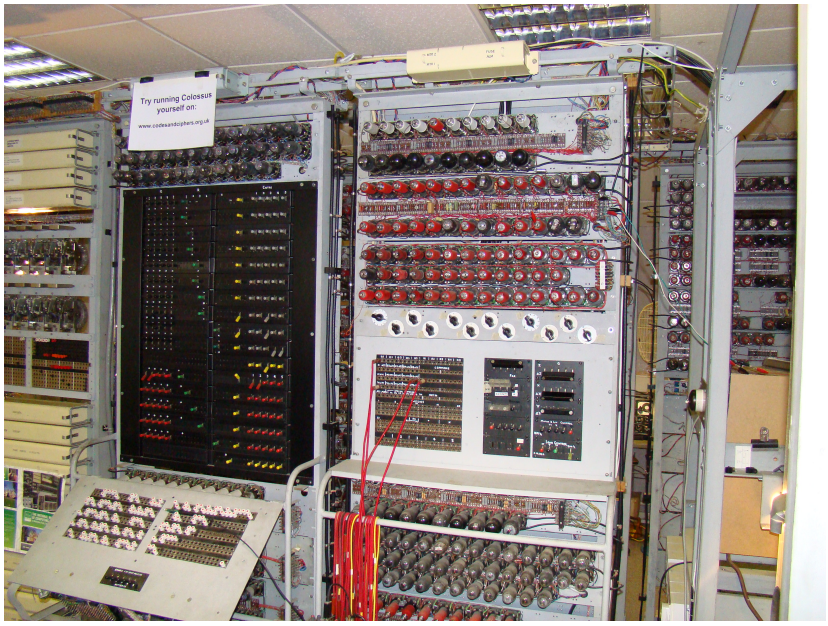
Cryptographic chips and boards

Progress in Implementations of Cryptoanalysis

British Cryptologic Bomb Used to Break Enigma



Colossus: First Mainframe

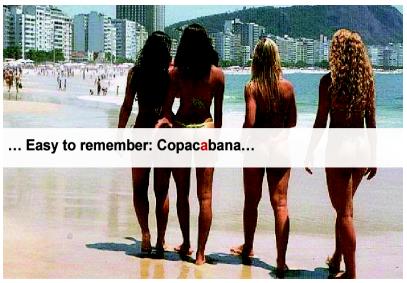


Supercomputer Cray

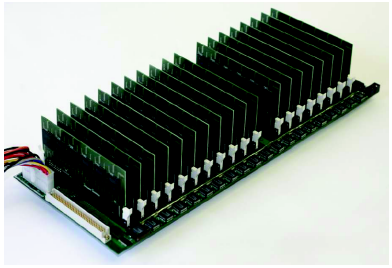
Computer Museum, Mountain View, CA

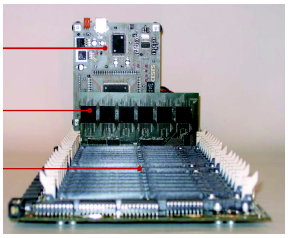
COPACOBANA

Ruhr University, Bochum,
University of Kiel, Germany, 2006



Cost: € 8980

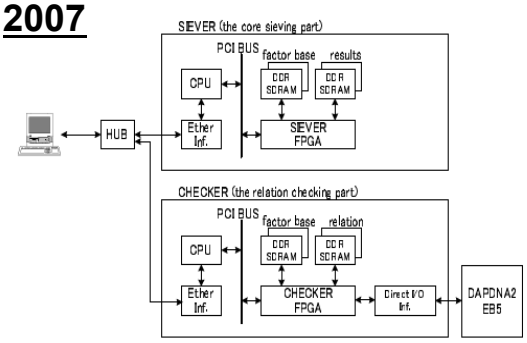


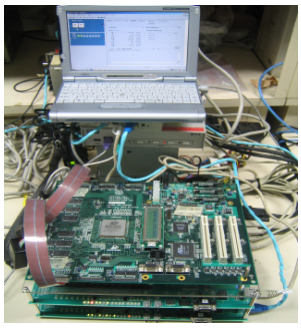


120 Spartan 3 FPGAs
Clock frequency 100 MHz

CAIRN 3 – Specialized Machine to Break RSA

2007





Japan **Tetsuya Izu and Jun Kogure and Takeshi Shimoyama (Fujitsu)**

CHES 2007 – September 2007