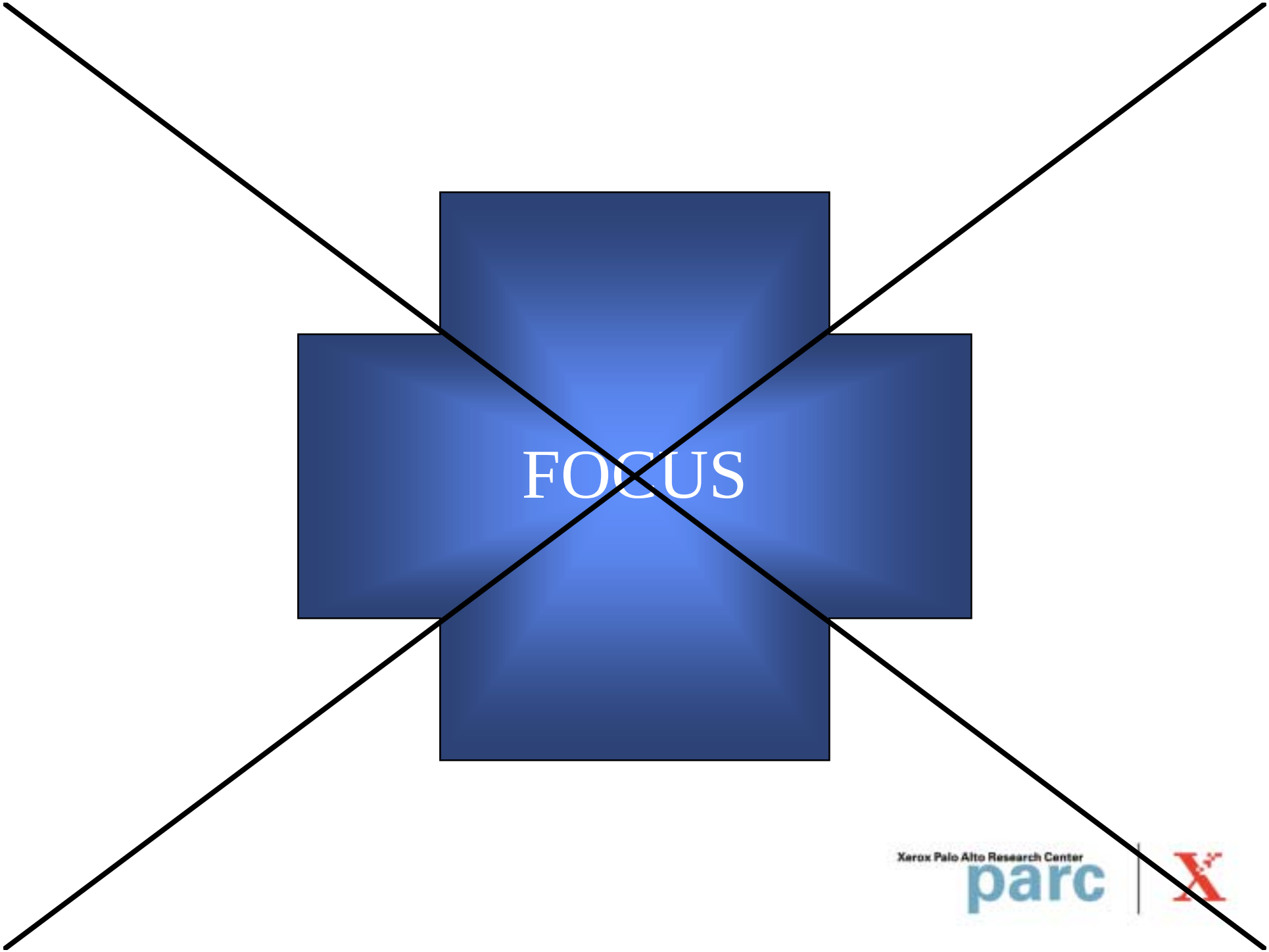
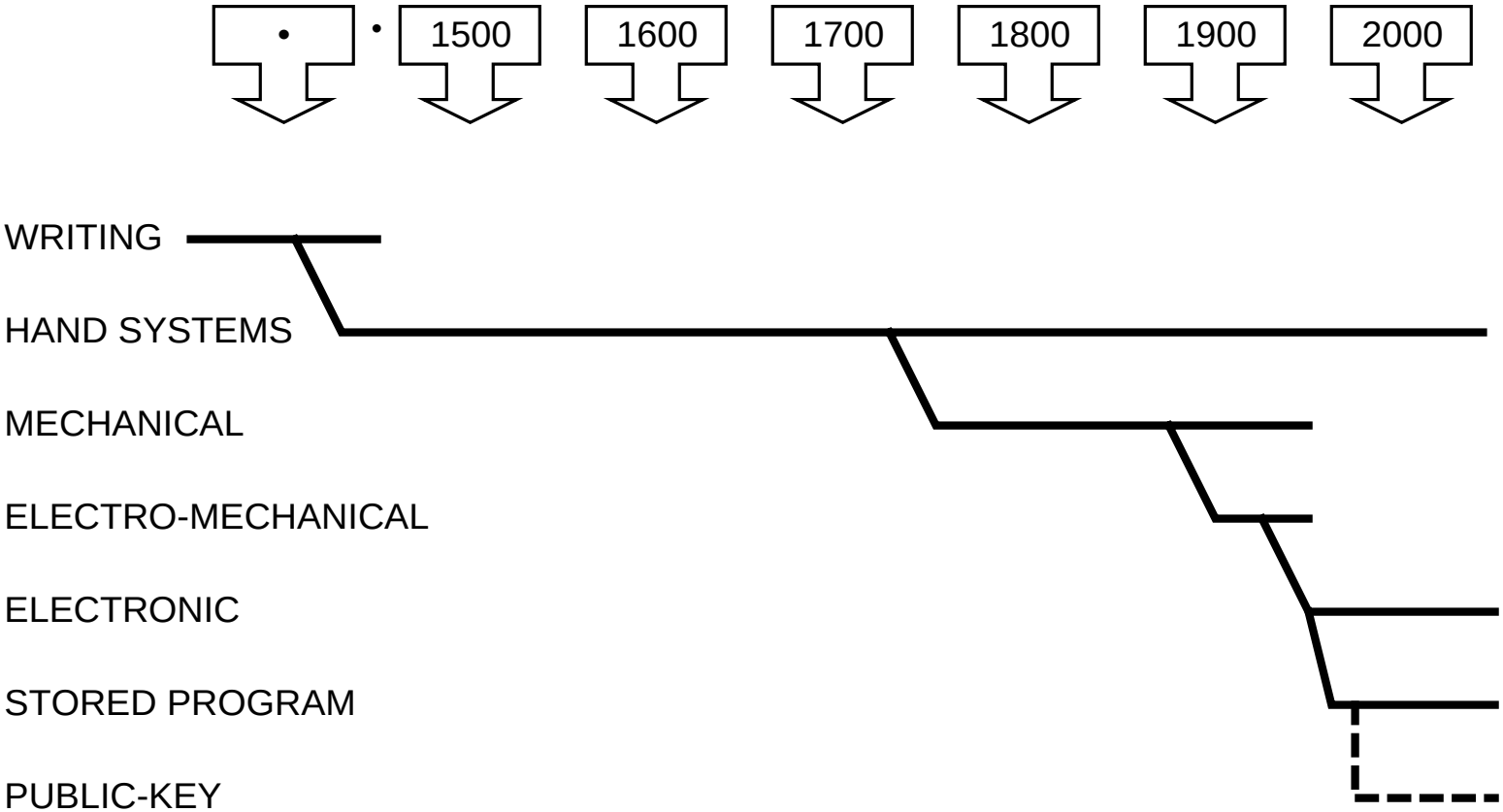


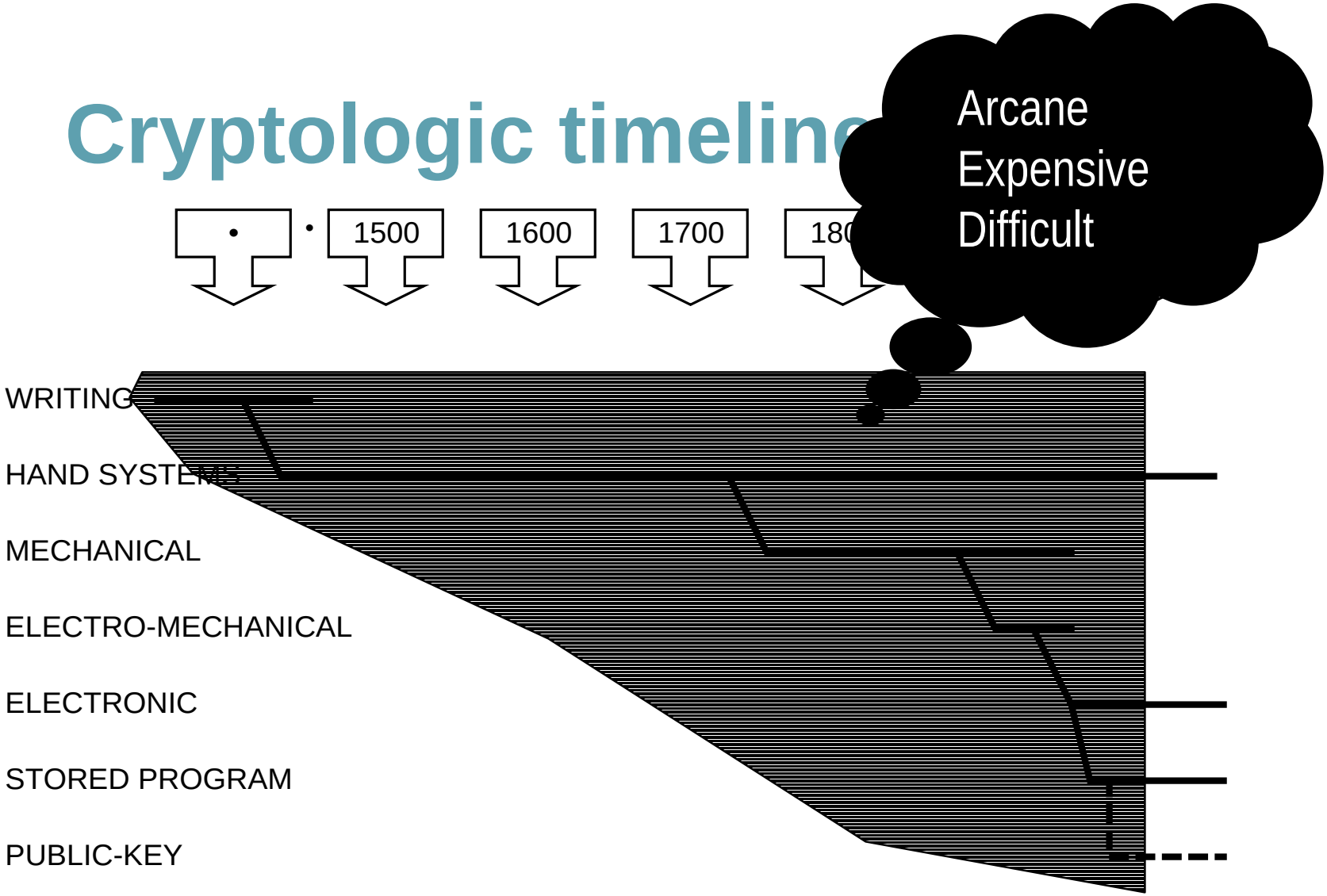
Xerox Palo Alto Research Center
parc

Cryptologic timeline



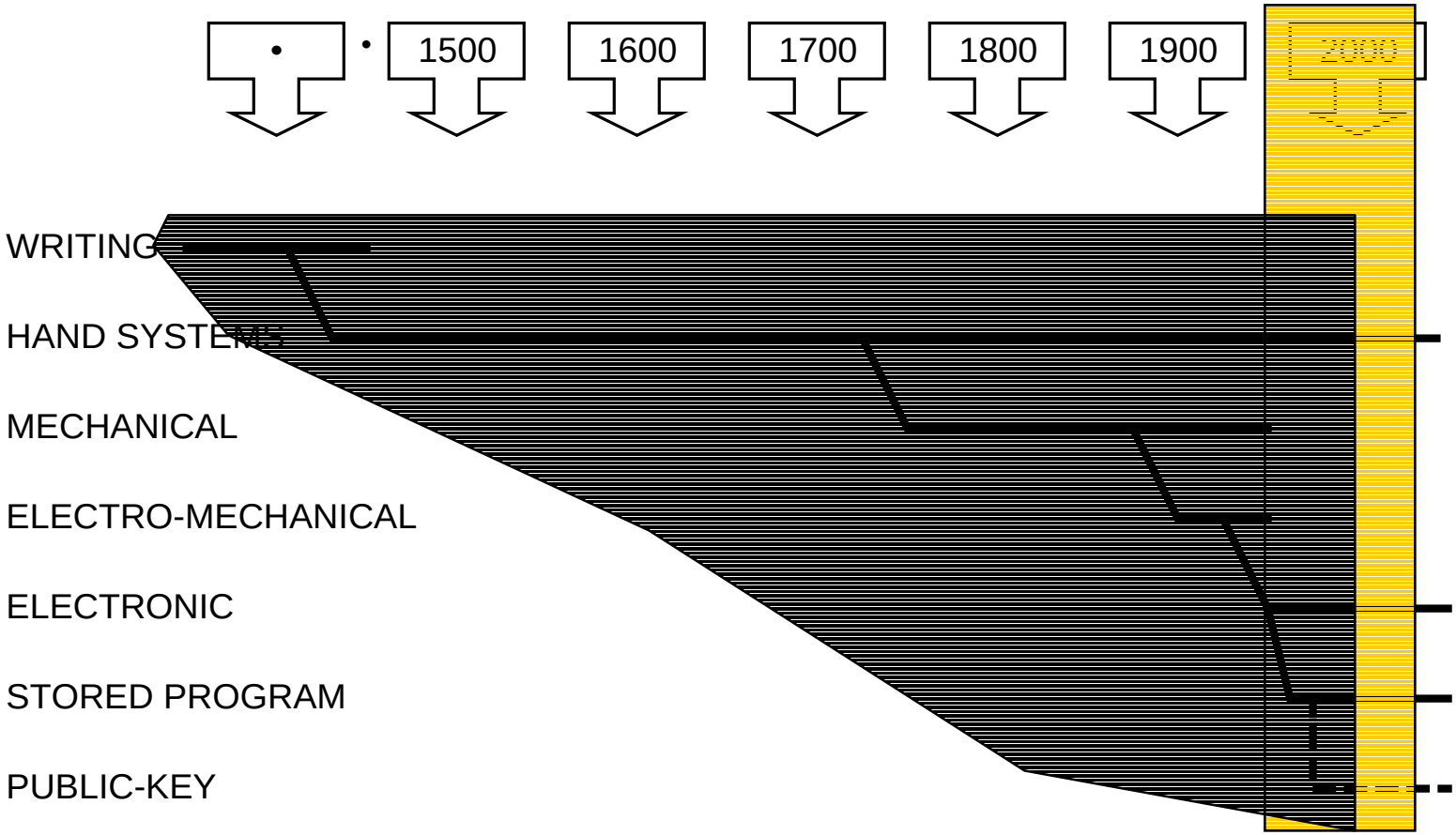
Xerox Palo Alto Research Center
parc

Cryptologic timeline



Xerox Palo Alto Research Center
parc

Cryptologic timeline



Xerox Palo Alto Research Center
parc

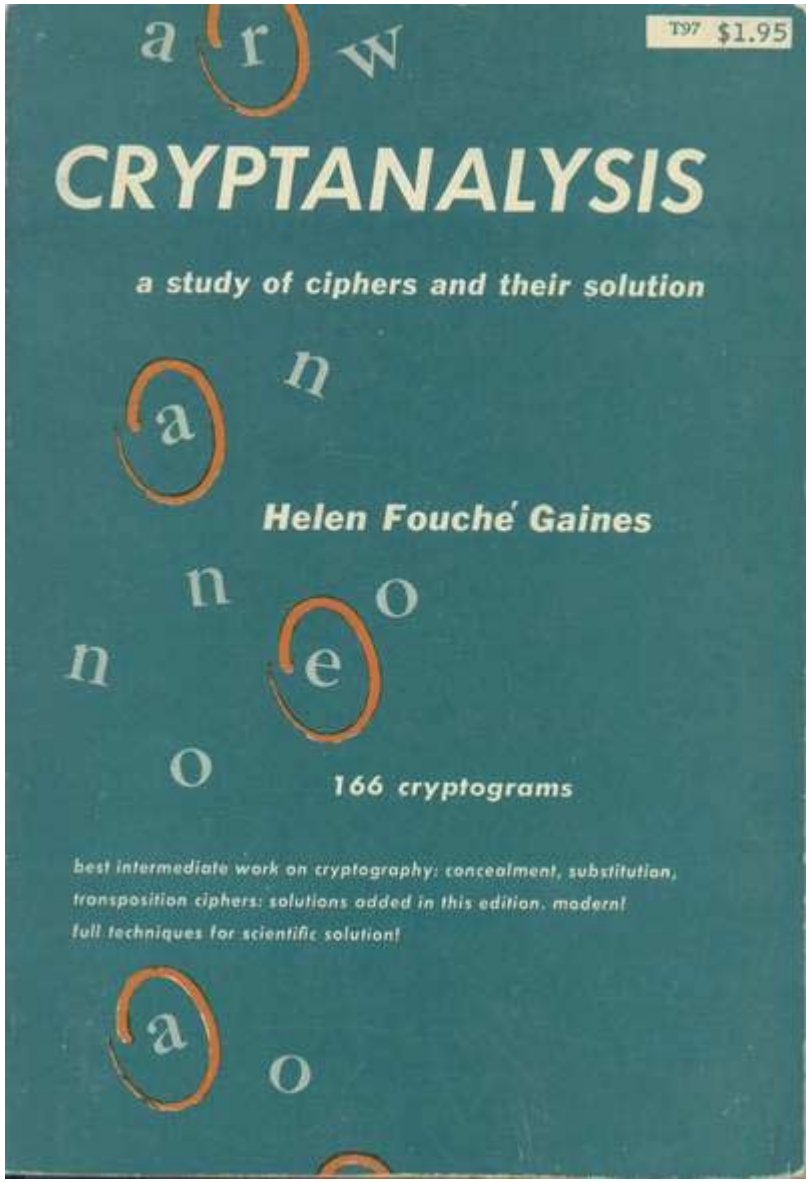
Contents

- Personal reminiscence
- Technical reminiscence
- IACR history
- Vision of a possible future

Thinking points

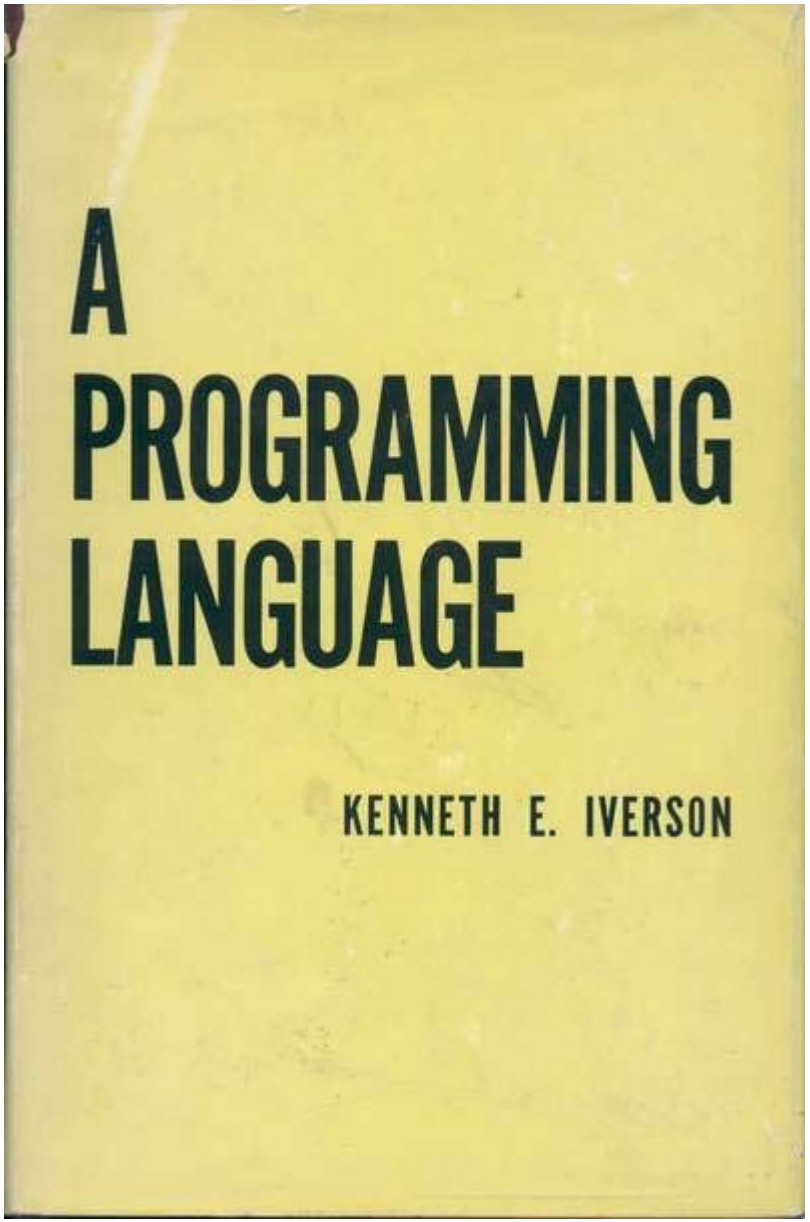
- Social consequences?
- Economic implications?
- New business models?

1956



Xerox Palo Alto Research Center
parc

1967 -- IBM Research

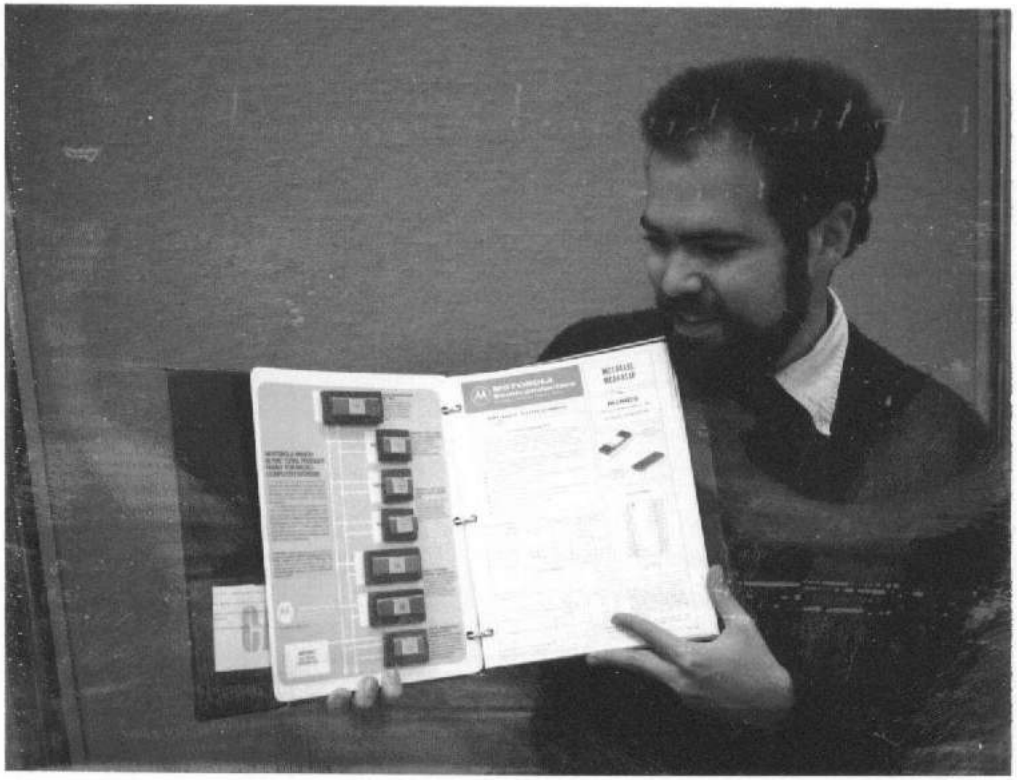


Xerox Palo Alto Research Center
parc

The 1970s

GROOVY

1975 -- Microprocessors



Xerox Palo Alto Research Center
parc

1976 -- New Directions

- public key-distribution
- public-key cryptography
- digital signatures

Xerox Palo Alto Research Center
parc

1977 - DES

Federal Information
Processing Standards Publication 46

1977 January 15

SPECIFICATIONS FOR THE

DATA ENCRYPTION STANDARD

The Data Encryption Standard (DES) shall consist of the following Data Encryption Algorithm to be implemented in special purpose electronic devices. These devices shall be designed in such a way that they may be used in a computer system or network to provide cryptographic protection to binary coded data. The method of implementation will depend on the application and environment. The devices shall be implemented in such a way that they may be tested and validated as accurately performing the transformations specified in the following algorithm.

DATA ENCRYPTION ALGORITHM

Introduction

The algorithm is designed to encipher and decipher blocks of data consisting of 64 bits under control of a 64-bit key. Deciphering must be accomplished by using the same key as for enciphering, but with the schedule of addressing the key bits altered so that the deciphering process is the reverse of the enciphering process. A block to be enciphered is subjected to an initial permutation IP, then to a complex key-dependent computation and finally to a permutation which is the inverse of the initial permutation IP^{-1}. The key-dependent computation can be simply defined in terms of a function f, called the cipher function, and a function KS, called the key schedule. A description of the computation is given first, along with details as to how the algorithm is used for encipherment. Next, the use of the algorithm for decipherment is described. Finally, a definition of the cipher function f is given in terms of primitive functions which are called the selection functions S_i and the permutation function P. S_i, P and KS of the algorithm are contained in the Appendix.

The following notation is convenient: Given two blocks L and R of bits, LR denotes the block consisting of the bits of L followed by the bits of R. Since concatenation is associative $B_1B_2 \ldots B_n$, for example, denotes the block consisting of the bits of B_1 followed by the bits of $B_2 \ldots$ followed by the bits of B_n.

Enciphering

A sketch of the enciphering computation is given in figure 1.

1978 -- RSA

p,q prime

$n = pq$

$ed \equiv 1 \bmod (p\text{-}1)(q\text{-}1)$

$C = M^e \bmod n$

$M = C^d \bmod n$

Cryptography Everywhere

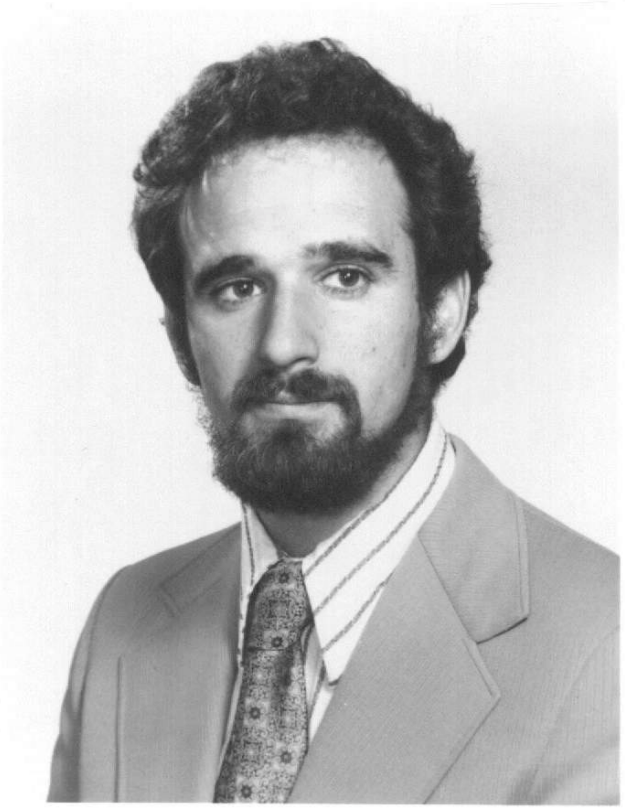
Tom Berson

Anagram Laboratories

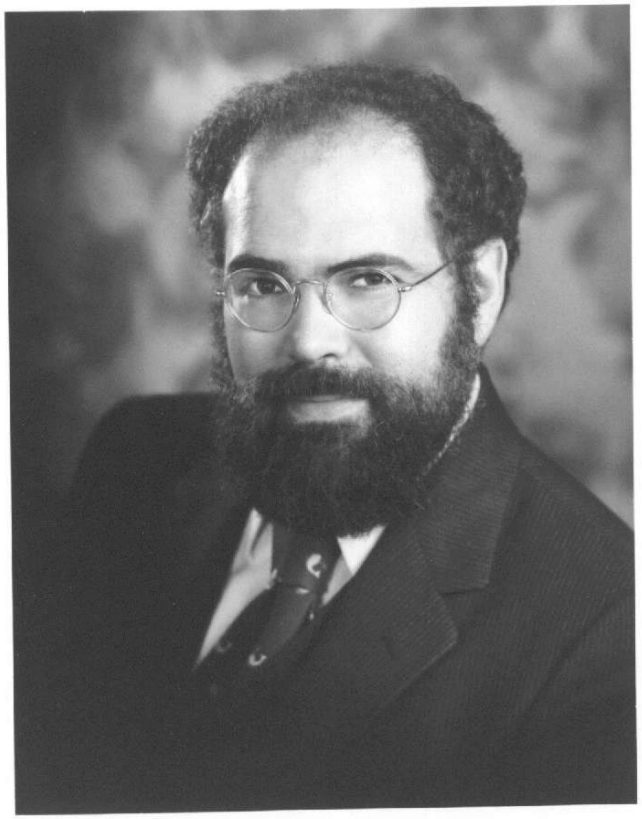
and Xerox PARC

2 December 2000

1980



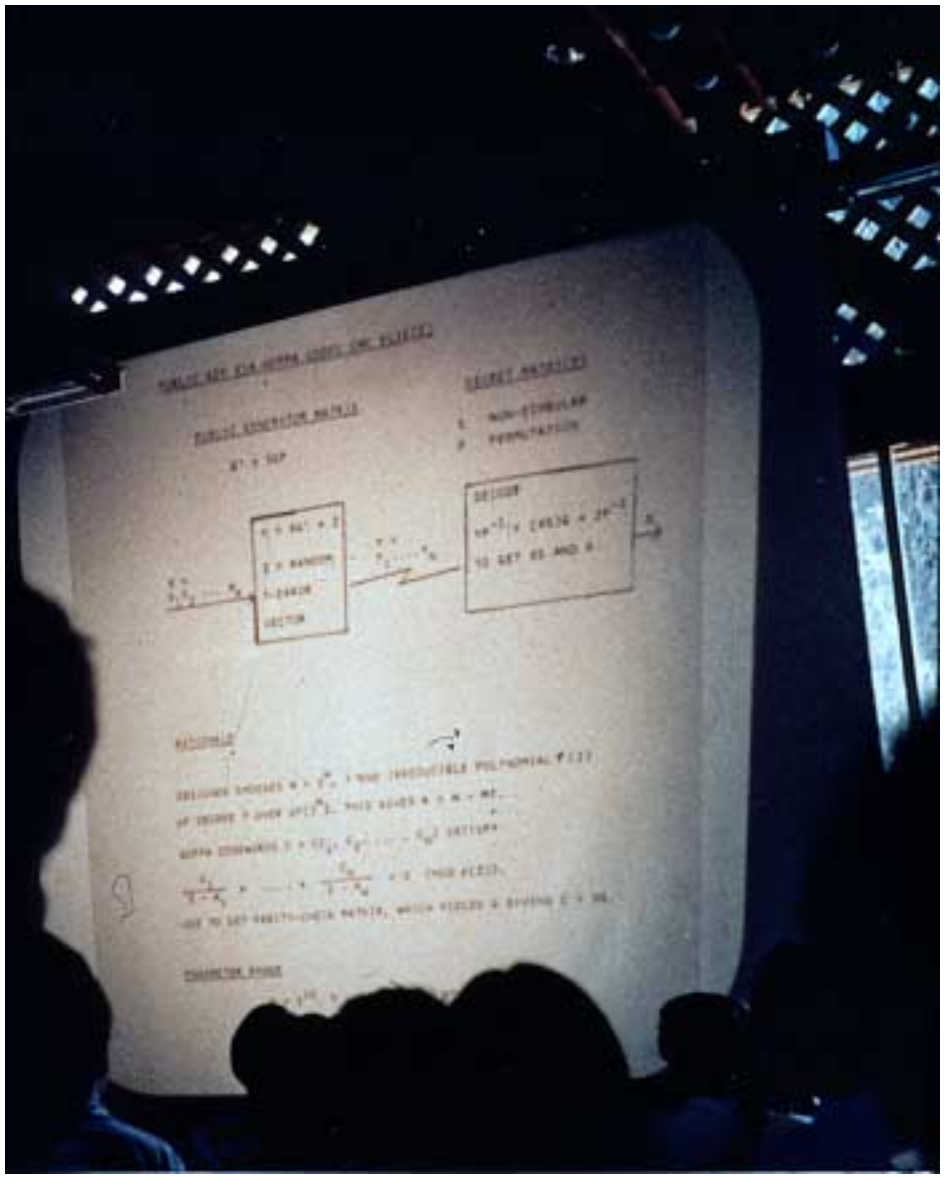
MARTIN E. HELLMAN



THOMAS A. BERSON

Xerox Palo Alto Research Center
parc

Crypto '81



Organizers:

Allen Gersho
Len Adelman
Whit Diffie
Martin Hellman
Dick Kemmerer
Alan Konheim
Ray Pickholtz
Brian Schanning
Gus Simmons
Steve Weinstein

Xerox Palo Alto Research Center
parc

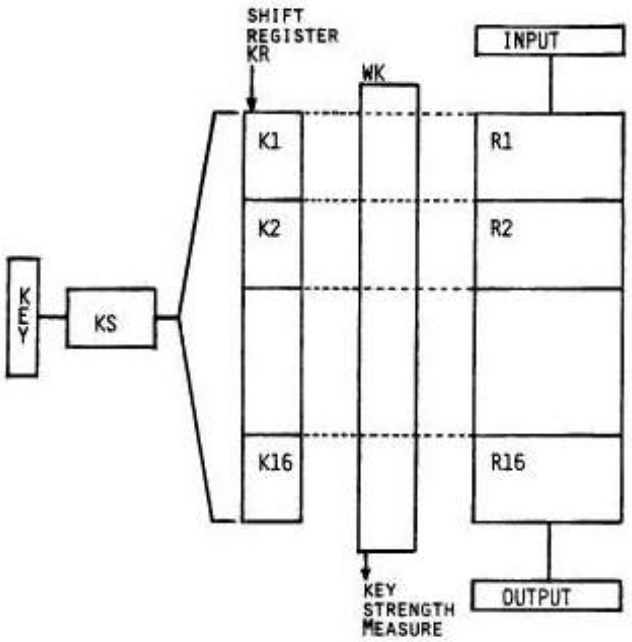
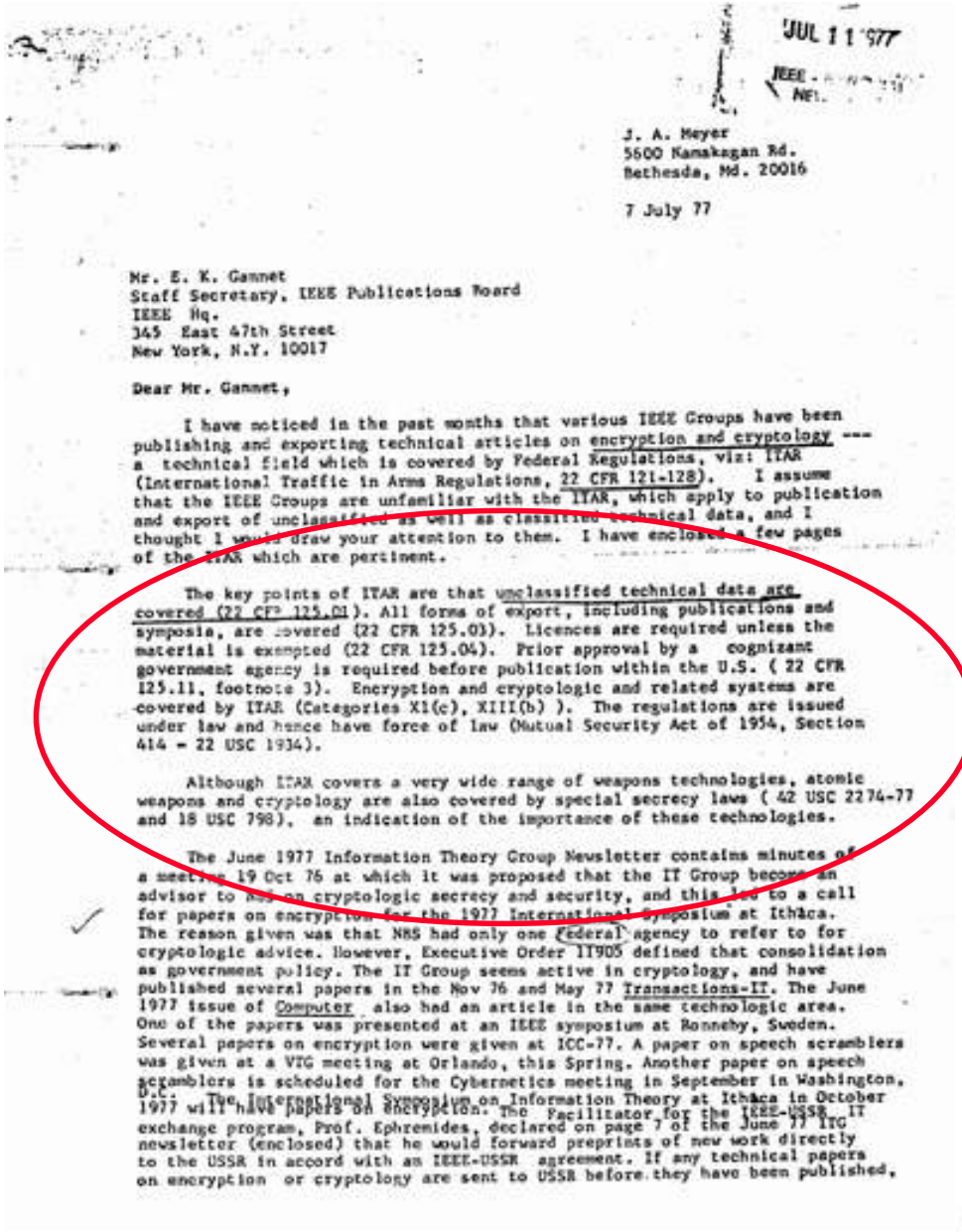


Fig. 1. DES is shown as a pipeline to illustrate the relationship between the Kn and the Rn. Also shown are the proposed placements of KR, a 768-bit key shift register and of WK, a key strength measurement function.

Figure 1 illustrates the relationship between the rounds of DES (R1-R16) and the key (K1-K16). It assumes that all Kn are precomputed and stored in a key register KR. KR is shown as a shift register, although other organizations are also possible (e.g. an array of 16 48-bit words). If the Kn are not stored internally then the same effect can be gained by requiring input of the each Kn at its appropriate round. This may lead to serious timing problems.

No matter how KR is organized, the making of KR (and thereby the Kn) directly accessible allows the user to bypass the standard KS and insert any 768 bits of key.

Would we get arrested?



JUL 11 '977

IEEE - NEL

J. A. Meyer
5600 Kanakagan Rd.
Bethesda, Md. 20016

7 July 77

Mr. E. K. Gannet
Staff Secretary, IEEE Publications Board
IEEE Hq.
345 East 47th Street
New York, N.Y. 10017

Dear Mr. Gannet,

I have noticed in the past months that various IEEE Groups have been publishing and exporting technical articles on encryption and cryptology --- a technical field which is covered by Federal Regulations, viz: ITAR (International Traffic in Arms Regulations, 22 CFR 121-128). I assume that the IEEE Groups are unfamiliar with the ITAR, which apply to publication and export of unclassified as well as classified technical data, and I thought I would draw your attention to them. I have enclosed a few pages of the ITAR which are pertinent.

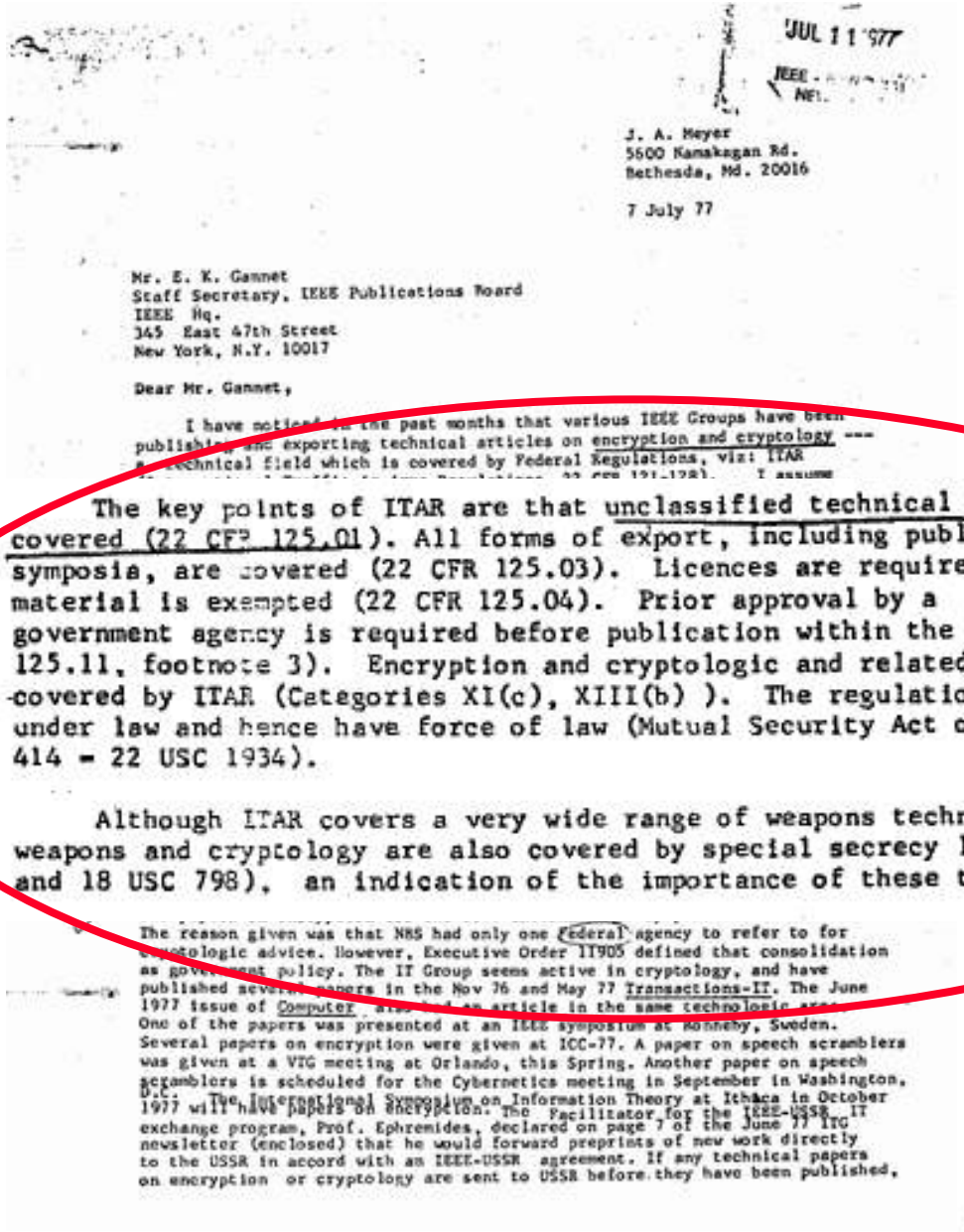
The key points of ITAR are that unclassified technical data are covered (22 CFR 125.01). All forms of export, including publications and symposia, are covered (22 CFR 125.03). Licences are required unless the material is exempted (22 CFR 125.04). Prior approval by a cognizant government agency is required before publication within the U.S. (22 CFR 125.11, footnote 3). Encryption and cryptologic and related systems are covered by ITAR (Categories XI(c), XIII(b)). The regulations are issued under law and hence have force of law (Mutual Security Act of 1954, Section 414 = 22 USC 1934).

Although ITAR covers a very wide range of weapons technologies, atomic weapons and cryptology are also covered by special secrecy laws (42 USC 2274-77 and 18 USC 798), an indication of the importance of these technologies.

The June 1977 Information Theory Group Newsletter contains minutes of a meeting 19 Oct 76 at which it was proposed that the IT Group become an advisor to NSA on cryptologic secrecy and security, and this led to a call for papers on encryption for the 1977 International Symposium at Ithaca. The reason given was that NSA had only one federal agency to refer to for cryptologic advice. However, Executive Order 11905 defined that consolidation as government policy. The IT Group seems active in cryptology, and have published several papers in the Nov 76 and May 77 Transactions-IT. The June 1977 issue of Computer also had an article in the same technologic area. One of the papers was presented at an IEEE symposium at Ronneby, Sweden. Several papers on encryption were given at ICC-77. A paper on speech scramblers was given at a VTG meeting at Orlando, this Spring. Another paper on speech scramblers is scheduled for the Cybernetics meeting in September in Washington, D.C. The International Symposium on Information Theory at Ithaca in October 1977 will have papers on encryption. The Facilitator for the IEEE-USSR IT exchange program, Prof. Ephremides, declared on page 7 of the June 77 ITG newsletter (enclosed) that he would forward preprints of new work directly to the USSR in accord with an IEEE-USSR agreement. If any technical papers on encryption or cryptology are sent to USSR before they have been published,

Xerox Palo Alto Research Center
parc

Would we get arrested?



JUL 11 1977

IEEE - NEL

J. A. Meyer
5600 Kanakagan Rd.
Bethesda, Md. 20016

7 July 77

Mr. E. K. Gannet
Staff Secretary, IEEE Publications Board
IEEE Hq.
345 East 47th Street
New York, N.Y. 10017

Dear Mr. Gannet,

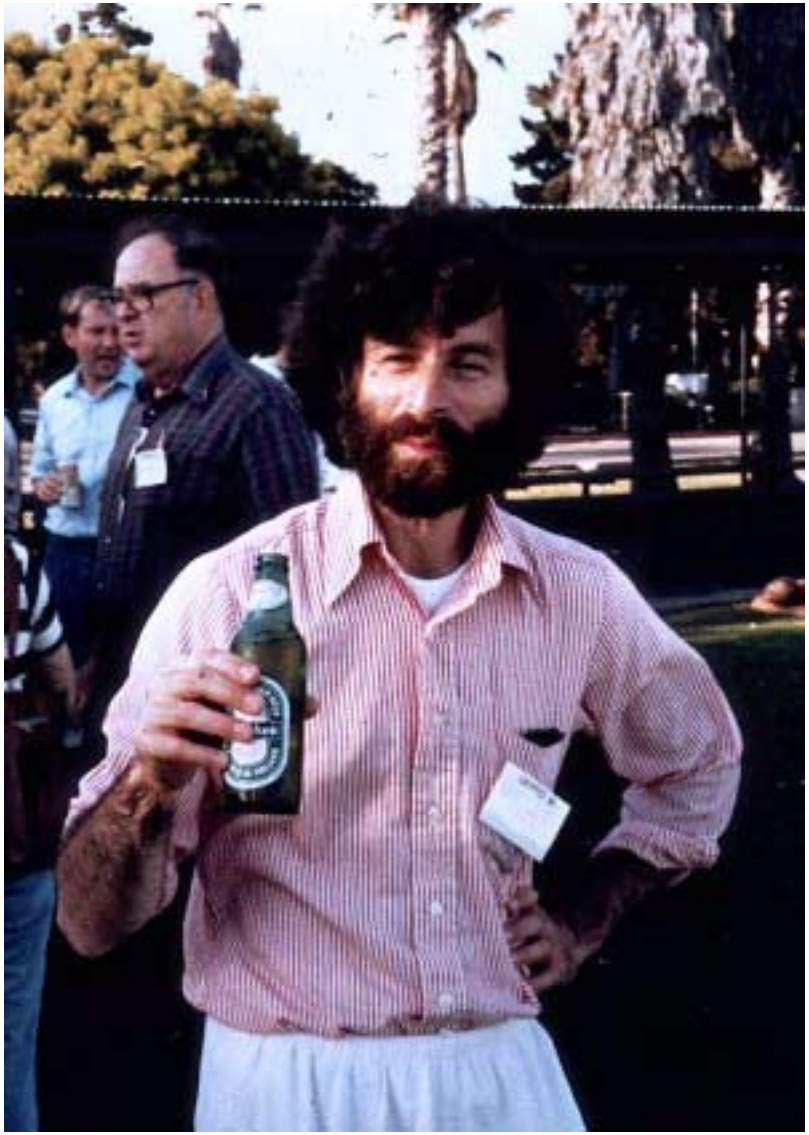
I have noticed in the past months that various IEEE Groups have been publishing and exporting technical articles on encryption and cryptology --- A technical field which is covered by Federal Regulations, viz: ITAR

The key points of ITAR are that unclassified technical data are covered (22 CFR 125.01). All forms of export, including publications and symposia, are covered (22 CFR 125.03). Licences are required unless the material is exempted (22 CFR 125.04). Prior approval by a cognizant government agency is required before publication within the U.S. (22 CFR 125.11, footnote 3). Encryption and cryptologic and related systems are covered by ITAR (Categories XI(c), XIII(b)). The regulations are issued under law and hence have force of law (Mutual Security Act of 1954, Section 414 - 22 USC 1934).

Although ITAR covers a very wide range of weapons technologies, atomic weapons and cryptology are also covered by special secrecy laws (42 USC 2274-77 and 18 USC 798), an indication of the importance of these technologies.

The reason given was that NBS had only one federal agency to refer to for cryptologic advice. However, Executive Order 11905 defined that consolidation as government policy. The IT Group seems active in cryptology, and have published several papers in the Nov 76 and May 77 Transactions-IT. The June 1977 issue of Computer also had an article in the same technologic area. One of the papers was presented at an IEEE symposium at Ronneby, Sweden. Several papers on encryption were given at ICC-77. A paper on speech scramblers was given at a VTG meeting at Orlando, this Spring. Another paper on speech scramblers is scheduled for the Cybernetics meeting in September in Washington, D.C. The International Symposium on Information Theory at Ithaca in October 1977 will have papers on encryption. The Facilitator for the IEEE-USSR IT exchange program, Prof. Ephremides, declared on page 7 of the June 77 ITG newsletter (enclosed) that he would forward preprints of new work directly to the USSR in accord with an IEEE-USSR agreement. If any technical papers on encryption or cryptology are sent to USSR before they have been published,

Xerox Palo Alto Research Center
parc

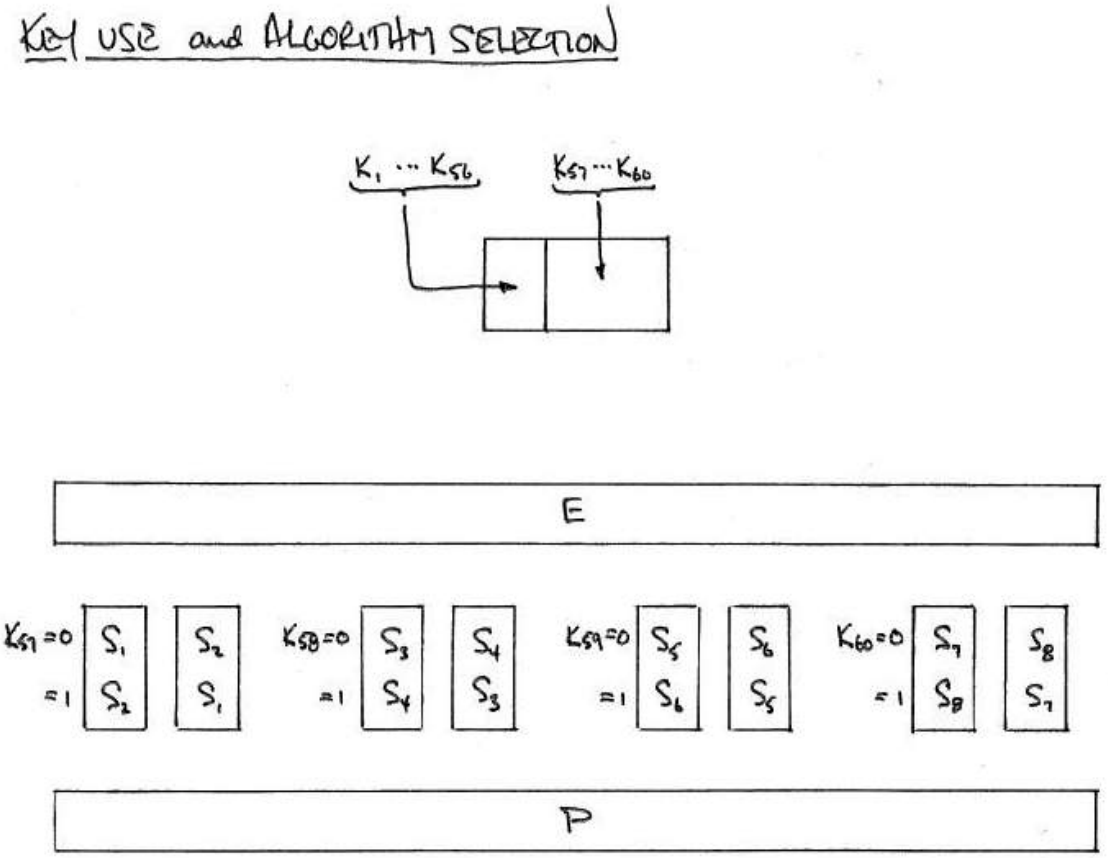


Xerox Palo Alto Research Center
parc

Xerox Palo Alto Research Center
parc

Xerox Palo Alto Research Center
parc

1982 -- Was DES secure?



1983 -- Were PKCs secure?

- DH knapsack broken
- Much factoring work
- Other candidates

1982/83 -- IACR founded

CRYPTO 82

UNIVERSITY OF CALIFORNIA, SANTA BARBARA

BERKELEY • DAVIS • IRVINE • LOS ANGELES • RIVERSIDE • SAN DIEGO • SAN FRANCISCO | SANTA BARBARA • SANTA CRUZ

DEPARTMENT OF COMPUTER SCIENCE

SANTA BARBARA, CALIFORNIA 93106

March 5, 1983

Tom Berson
SYTEK, Inc.
1153 Bordeaux Dr.
Sunnyvale, CA 94086

Dear Tom,

It is my pleasure once again to thank you for all your help in making CRYPTO 82 such a success!

You will be pleased to know that Alan Sherman and Ron Rivest have just sent the proceedings to the publisher. Plenum promised a maximum of 90 days turn-around.

The planning committee nominated during the conference met after lunch on the final day. A working title was adopted: "International Association for Cryptologic Research." Those at the meeting also decided that the organization should sponsor a meeting in Europe this March, and CRYPTO 83 in Santa Barbara in August 83. The EUROCRYPT 83 meeting will be taking place shortly.

I was to be responsible for getting CRYPTO 83 started. In view of this, and my role as general chairman for CRYPTO 82, I asked Alan Konheim to be general chairman for CRYPTO 83. (I had already made the necessary reservations.) He has contacted Neil Sloane, who has agreed to be program chairman.

As you may know, the official sponsorship of CRYPTO 82 remains a confused matter. CRYPTO 83 will be sponsored by the organization and the Computer Science Department. Some progress is being made in trying to roll over the surplus funds (approximatley 3k) for use by CRYPTO 83. I expect that the attendees at CRYPTO 83 will vote to have the CRYPTO n series continue to be sponsored by the organization.

1982/83 -- IACR founded

CRYPTO 82

UNIVERSITY OF CALIFORNIA, SANTA BARBARA

BERKELEY • DAVIS • IRVINE • LOS ANGELES • RIVERSIDE • SAN DIEGO • SAN FRANCISCO | SANTA BARBARA • SANTA CRUZ

DEPARTMENT OF COMPUTER SCIENCE

SANTA BARBARA, CALIFORNIA 93106

March 5, 1983

Tom Berson
SYTEK, Inc.
1153 Bordeaux Dr.
Sunnyvale, CA 94086

Dear Tom,

It is my pleasure once again to thank you for all your help in making CRYPTO 82 such a success!

The planning committee nominated during the conference met after lunch on the final day. A working title was adopted: "International Association for Cryptologic Research." Those at the meeting also decided that the organization should sponsor a meeting in Europe this March, and CRYPTO 83 in Santa Barbara in August 83. The EUROCRYPT 83 meeting will be taking place shortly.

this, and my role as general chairman for CRYPTO 82, I asked Alan Konheim to be general chairman for CRYPTO 83. (I had already made the necessary reservations.) He has contacted Neil Sloane, who has agreed to be program chairman.

As you may know, the official sponsorship of CRYPTO 82 remains a confused matter. CRYPTO 83 will be sponsored by the organization and the Computer Science Department. Some progress is being made in trying to roll over the surplus funds (approximatley 3k) for use by CRYPTO 83. I expect that the attendees at CRYPTO 83 will vote to have the CRYPTO n series continue to be sponsored by the organization.

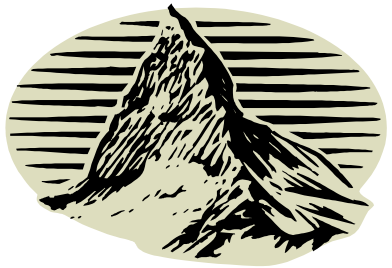
International Association for Cryptologic Research, Inc.

- “To promote research in cryptology”
- Nevada Corporation 16 June 1983
- Directors:
  - Ernest Brickell, David Chaum, Whitfield Diffie, Robert Jueneman, Denning, David Kahn, Stephen Kent
- Paranoid bylaws initially
- US tax-exempt scientific organization

Crypto

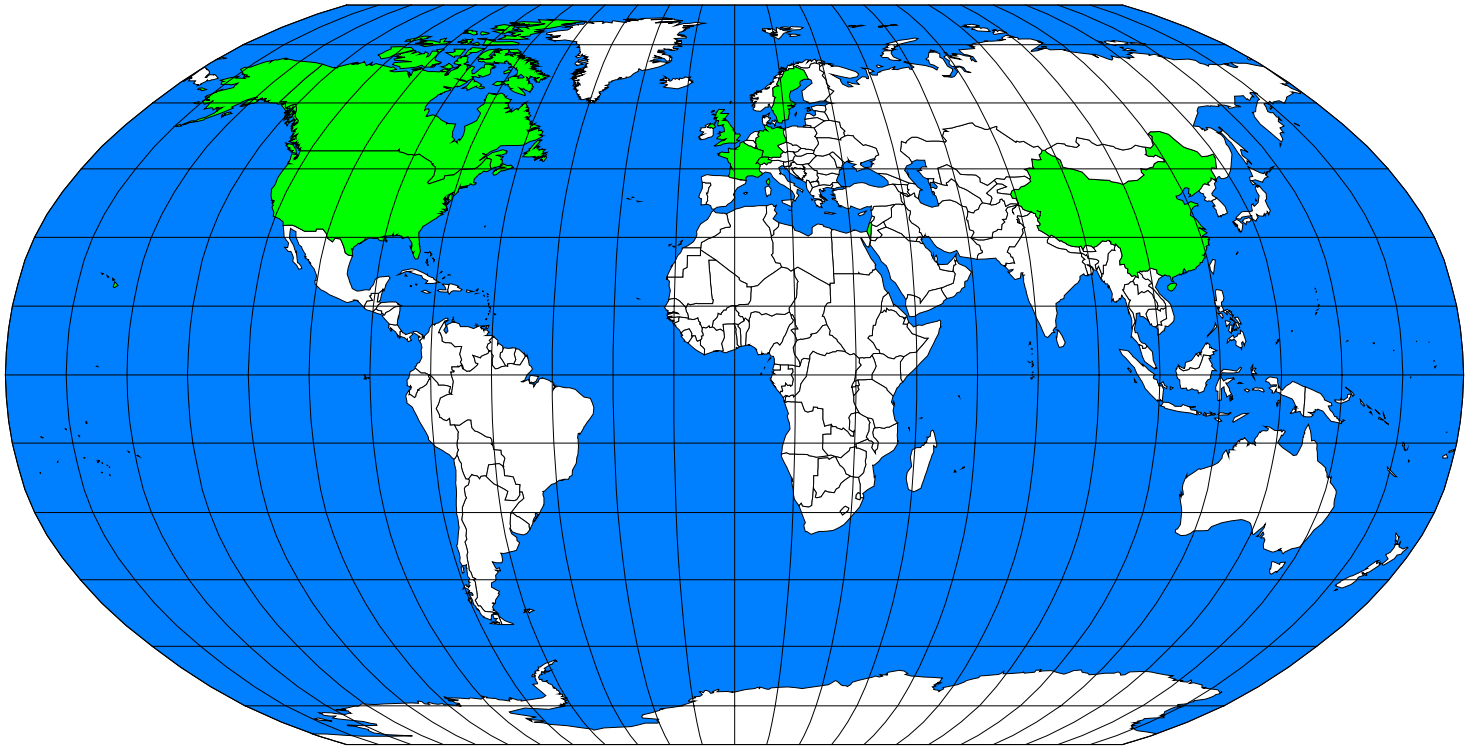
- Crypto ’81-- UCSB
- Crypto ’82
- ➨ Crypto ’83
  - Organizers: Alan Konheim, Neil Sloan, David Chaum, Paul Eggert, Whit Diffie, Selim Akl, Henry Beker, Tom Berson, Dorothy Denning, Allen Gersho, John Gordon, Robert Juneman, Gus Simmons

Eurocrypt



- April ’81 -- Burg Feuerstein, Germany
- ➨ Eurocrypt ’83 -- Udine, Italy
- Organizers
  - Henry Beker, Thomas Beth, David Chaum, John Gordon, Guiseppe Longho, Fred Piper

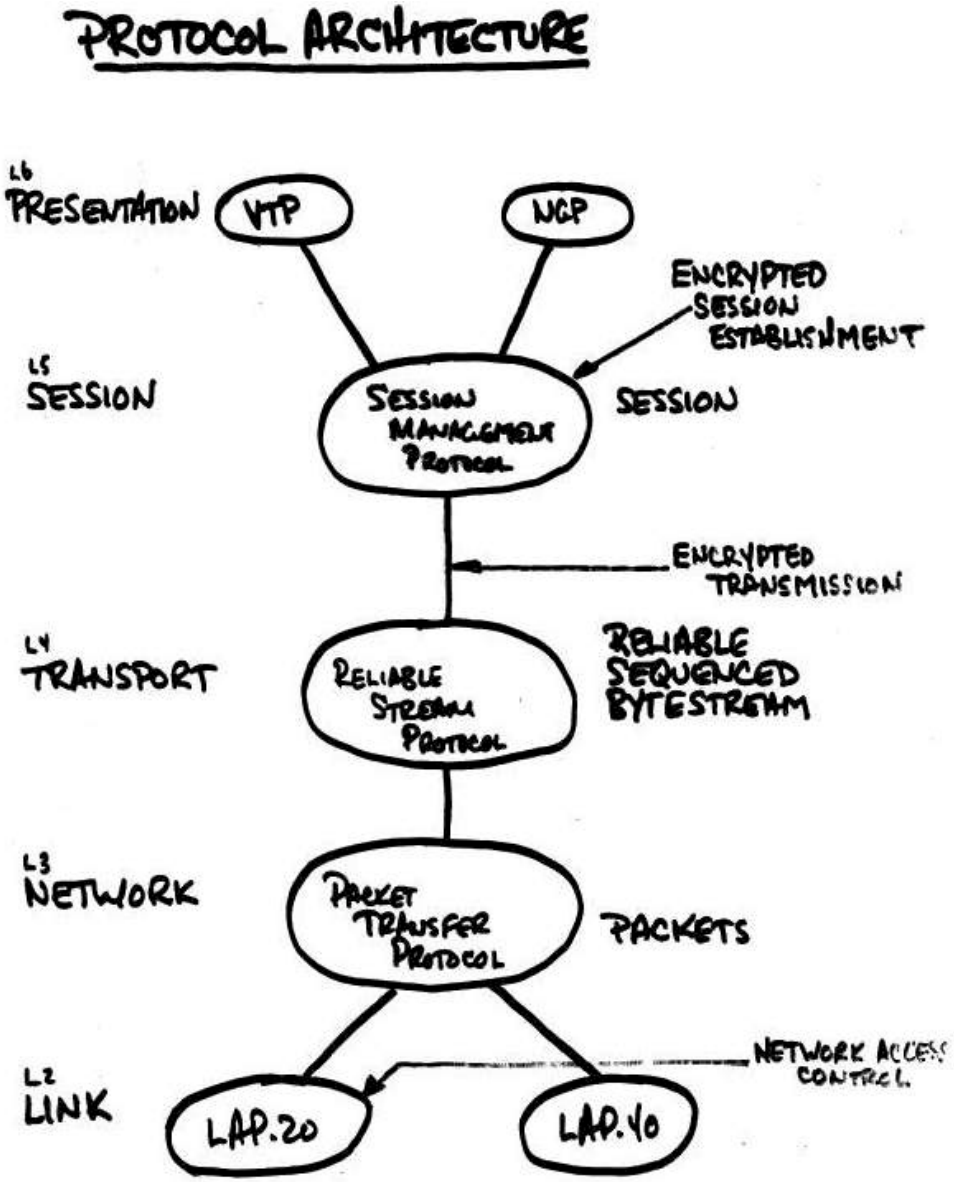
1982 -- IACR had 102 members



from 9 nations

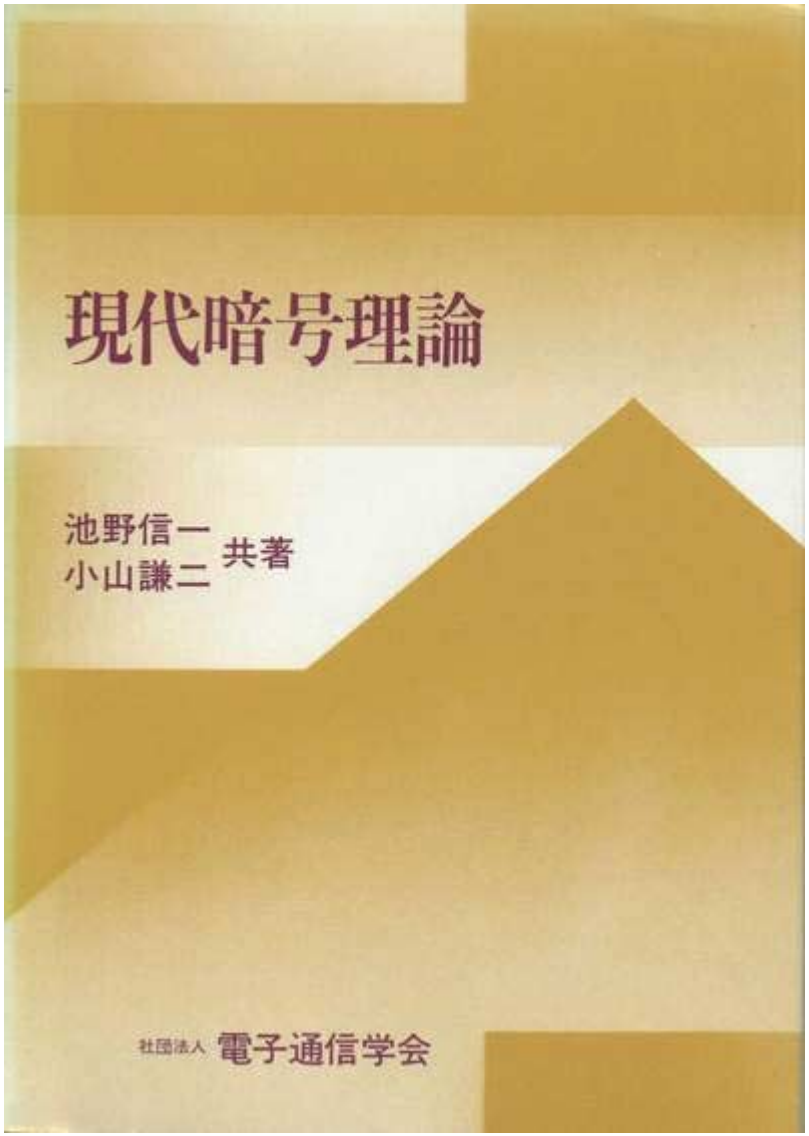
Xerox Palo Alto Research Center
parc

1980s -- LAN cryptosystem



Xerox Palo Alto Research Center
parc

Remembering Kenji Koyama



Xerox Palo Alto Research Center
parc

Asiacrypt

- Asiacrypt ’91 -- Fujiyoshida, Japan
  - Organizers: Shigeo Tsujii, Yoshihiro Idaware, Masao Kasahara, Kenji Koyama, Ryoko Akiyama, Hideki Imai, Toshiya Itoh, Shin-Ichi Kawamura, Naohisa Komatsu, Sadami Kurihara, Kaoro Kurosawa, Tsutomu Matsumoto, Hideo Nakano, Koji Nakao, Kazuo Ohta, Tatsuaki Okamoto, Ryoui Onda, Kazuo Takaragi, Kazue Tanaka, Atsuhiro Yamagishi
- Many other Asiacrypts in many places

➡ Asiacrypt 2000 -- Kyoto, Japan

Asiacrypt '91

Xerox Palo Alto Research Center
parc

1990s -- Differential CA

✘ MD5

~ SAFER (with Lars Knudsen)

✔ McEliece PKC

Related-message Attack

We will now generalize the message-resend attack. Suppose that there are two cryptograms

$$c_1 = m_1 SGP + e_1$$

and $m_1 \neq m_2$, $e_1 \neq e_2$

$$c_2 = m_2 SGP + e_2$$

and that the cryptanalyst knows a linear relation, for example $m_1 + m_2$, between the messages. We call this a *related-message* condition. In this case the cryptanalyst may recover the m_i from the set of c_i by doing one encoding and by then following the attack method of Section 4.1. Here are the details.

Combining the two cryptograms we get

$$c_1 + c_2 = m_1 SGP + m_2 SGP + e_1 + e_2 .$$

Notice that $m_1 SPG + m_2 SGP = (m_1 + m_2)SGP$, a value the cryptanalyst may calculate in a related-message condition from the known relationship and the public key.

The cryptanalyst solves

$$c_1 + c_2 + (m_1 + m_2)SGP = e_1 + e_2$$

and proceeds with the attack as in Section 4.1, using $(c_1 + c_2 + (m_1 + m_2)SGP)$ in place of $(c_1 + c_2)$.

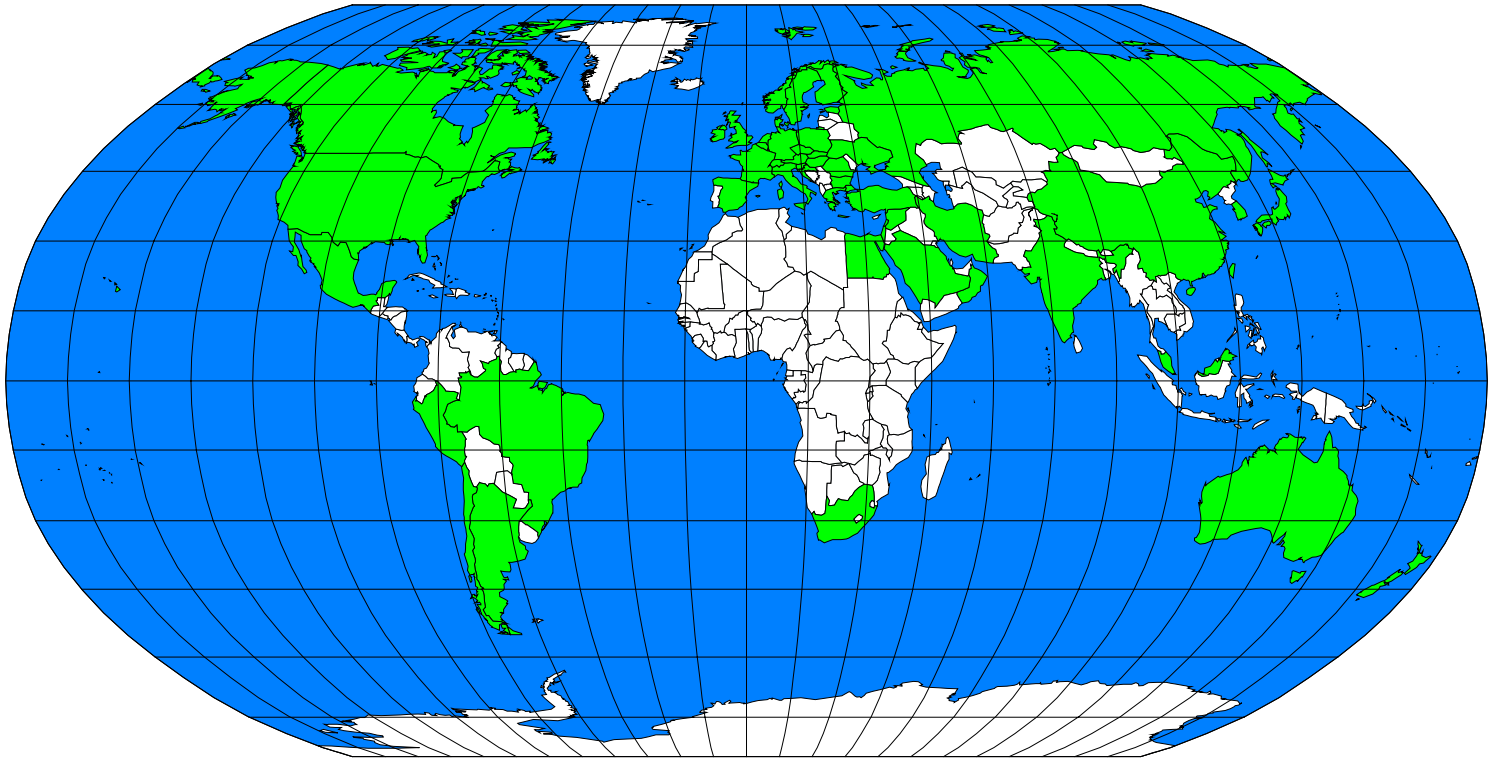
Remark

The message-resend attack is that special case of the related-message attack where $m_1 + m_2 = 0$.

4 December 2000

- PKC accepted and in wide use
- DES secure against all but exhaustive search attack
  - Not even DCA and LCA defeated it
  - Replaced by AES
- Academic cryptography is thriving

2000 -- IACR has 959 members



from 52 nations

Xerox Palo Alto Research Center
parc

In the past 20 years

- Arcane to commonplace
- Difficult to easy
- Expensive to cheap

But “everybody” still believes

- Cryptography is hard and expensive
- Mathematically complex
- Performance slow
- And designs around it

Ron Rivest

- Invented RSA 10 years too soon
- Performance was awful in 1978
- Patent expired on Sept. 20, 2000

Xerox Palo Alto Research Center parc

And that got me to thinking

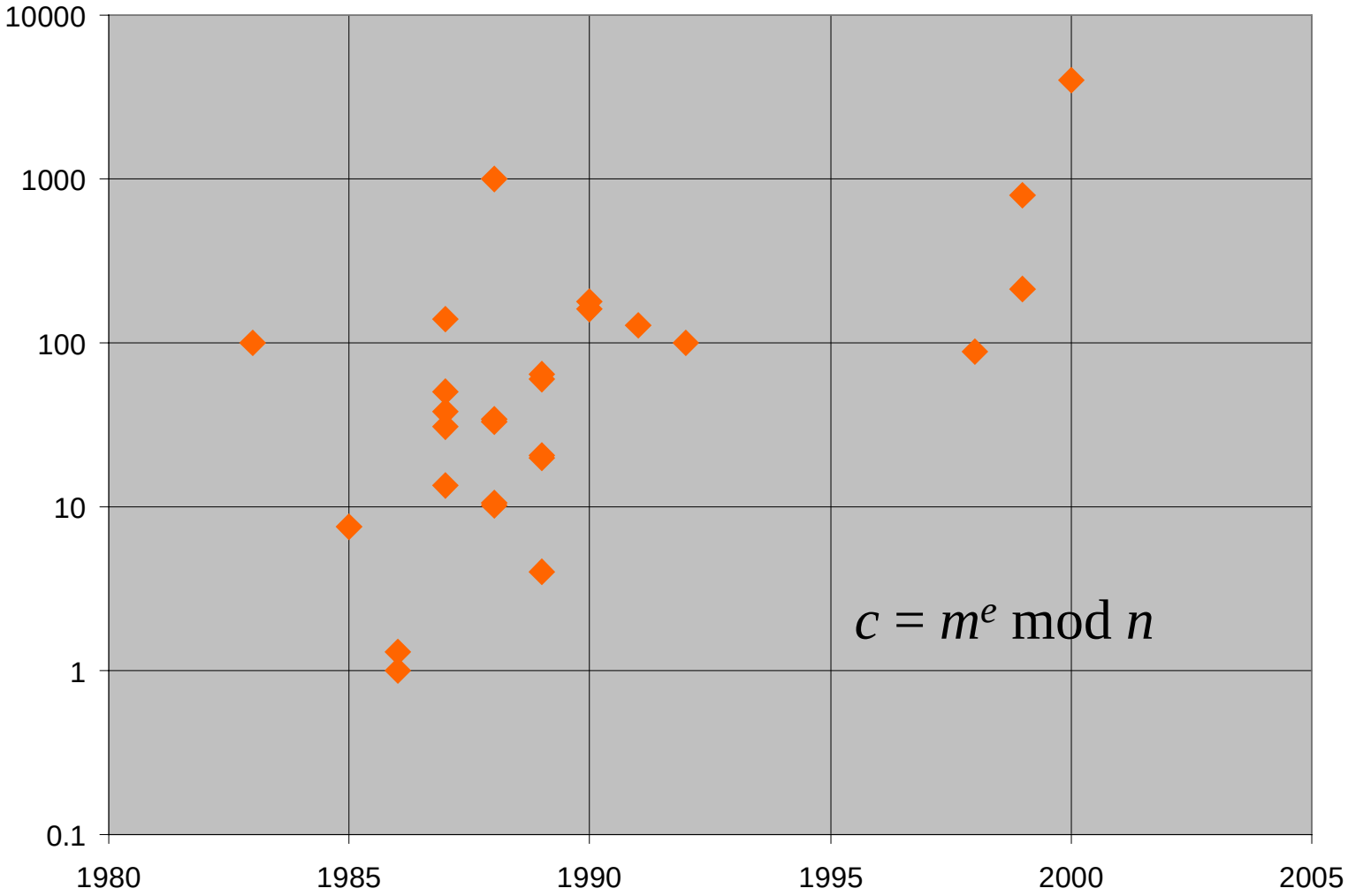
- That what “everybody knows” is wrong
- And is getting more wrong real fast

- What would happen if we started knowing something different

Trends

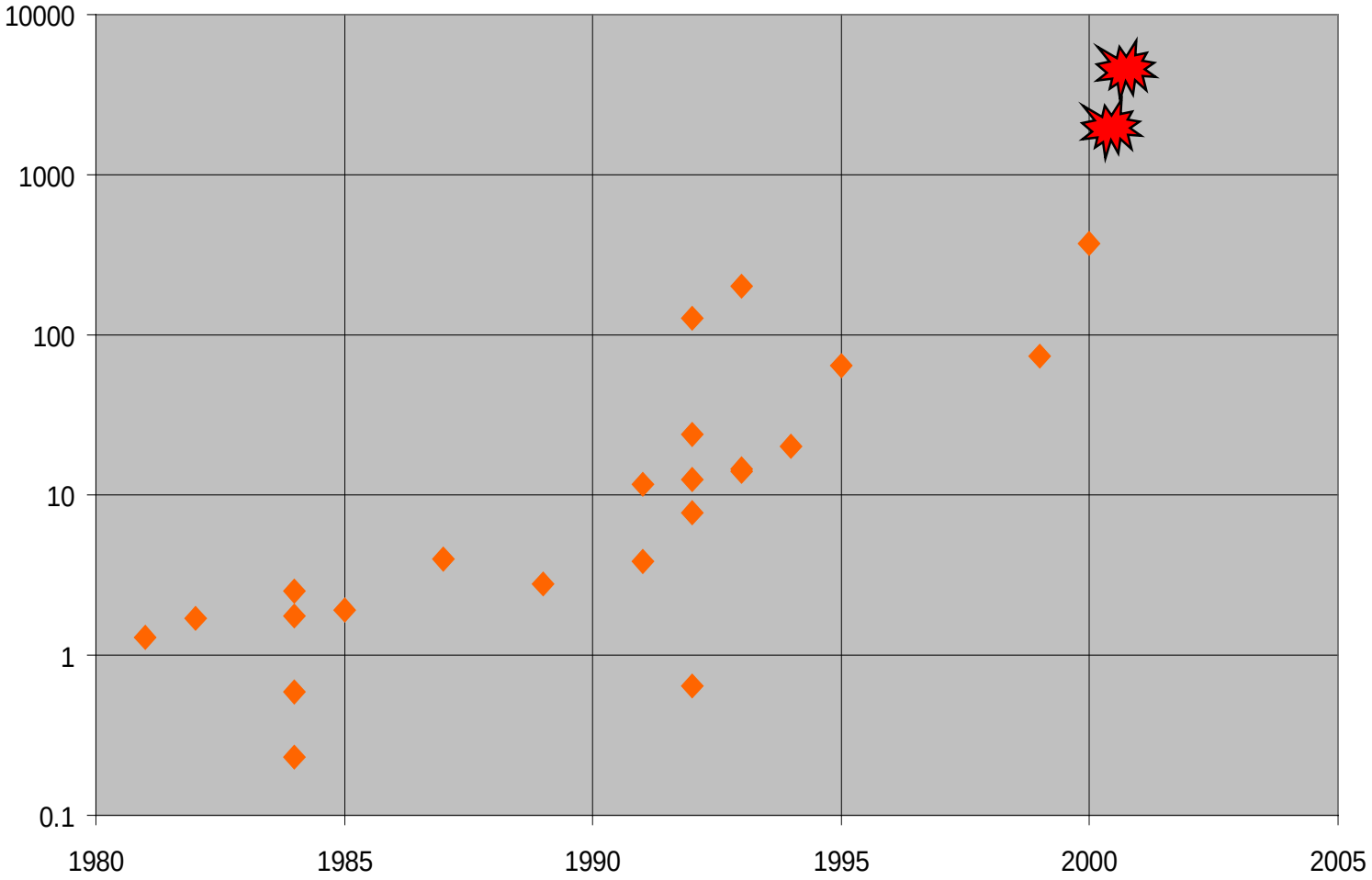
- Moore's Law +
- Open conferences and literature
- Textbooks and handbooks
- Internet, e-commerce, wireless
- Young people entering the field
- Rise of successful businesses
- Consumers use cryptography
- Commodification and integeration of cryptographic devices
- Easing of government regulation

RSA speed (K 512-bit op/sec)



Xerox Palo Alto Research Center
parc

DES speeds (Mbyte/sec)



Xerox Palo Alto Research Center
parc

Xerox Palo Alto Research Center

parc

Young people entering field

- 20% of attendees at Eurocrypt 2000 registered as students
- 300 people signed up for Dan Boneh's Intro to Crypto course at Stanford

Consumers make wide use of (hidden) cryptography

- TLS (SSL) and SET protocols
- Cellular telephony
- Pay television and IPPV
- Point-of-Sale terminals

Trends

- Moore's Law
- Open conferences and literature
- Textbooks and handbooks
- Internet, e-commerce, wireless
- Young people entering the field
- Rise of successful businesses
- Consumers use cryptography
- Commodification and integeration of cryptographic devices +
- Easing of government regulation

Commodification of cryptographic devices

- Ex. BlueSteel Networks
  - Founded April 1999
  - To make accelerator chips
  - First chip sampled September 1999
  - Bought by Broadcom
    - November 1999 -> Mar 2000
    - Gigabit Ethernet, cable modems, set-top boxes

Vision for 2020 -- A future of cryptographic abundance

Xerox Palo Alto Research Center
parc

a•bun•dance, *n.*

1 A great or plentiful amount; ample sufficiency; profusion; copious supply; superfluity.

2 Fullness to overflowing.

3 Wealth.

- -- strictly applicable to quantity only, but sometimes used of number.

No need to conserve

E.g., IP protocol operations

Will it happen?

- User interface complexity?
- Key management issues?
- Government regulation?

What do you think?

Imagine a world of abundant cryptography

- Cryptographic operations fast, plentiful
- Encapsulated and hidden from users

What would things be like in that world?

Xerox Palo Alto Research Center
parc

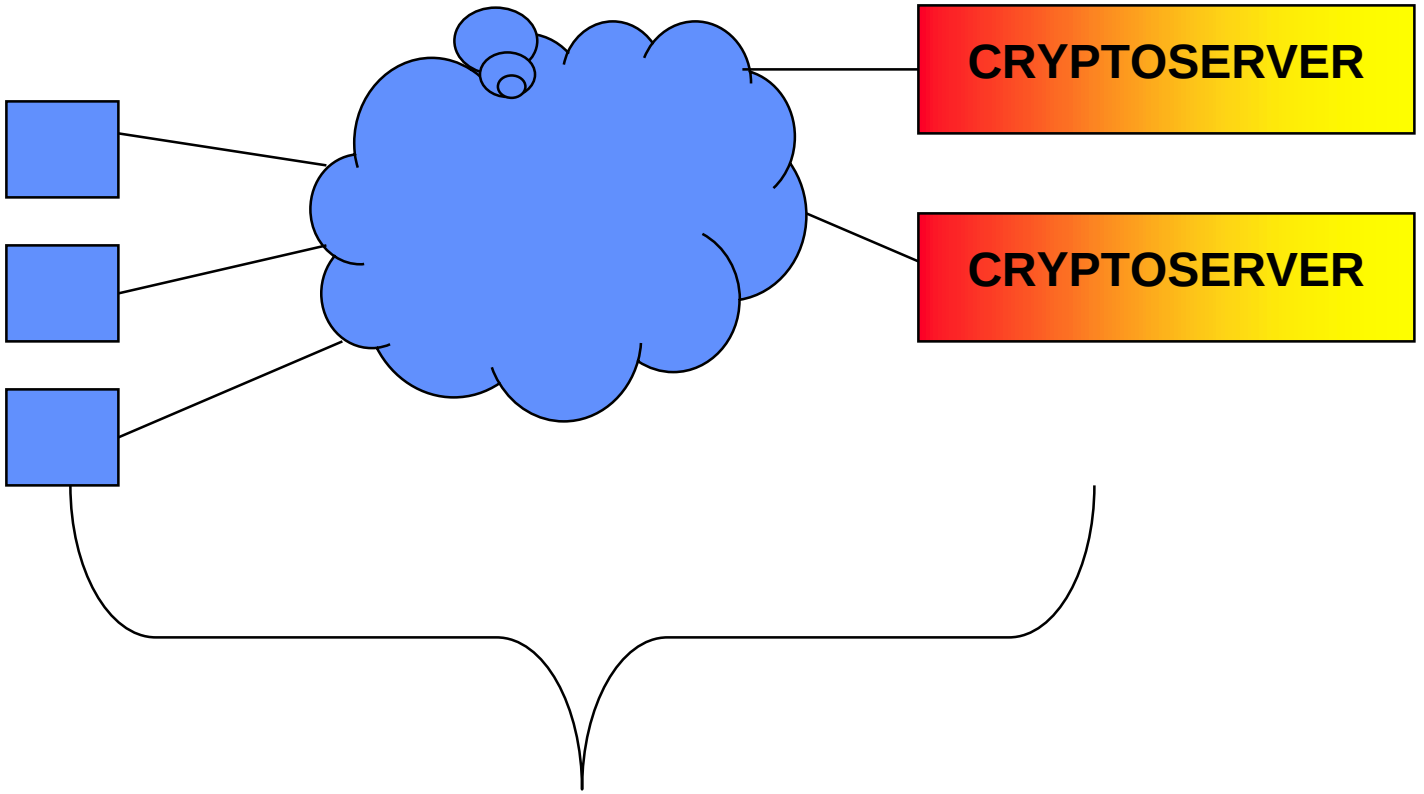
Scientific questions

- Complexity theory
- Information theory

Engineering tradeoffs

- Ecology
- Systems engineering
  - Architectural decisions (Show cryptoserver)
  - Key management
- Protocols
- Infrastructure
- Algorithms

Cryptography as a network service



PARC Cryptoserver

- Network-based cryptographic operations
  - Trust model issues
- >10,000 1024-bit modular exponentiations/sec by December 2001
- We expect 10Gb/sec Ethernet soon after
- At these speeds cryptography is no longer the bottleneck

Complexities of key management must be hidden from the user

- Perhaps even at the expense of security
- PKI acceptance is an Human-Computer Interfacr (HCI) issue
- It’s about usability
- Cryptography needs to disappear into the infrastructure

Engineering tradeoffs

- Systems engineering
  - Architectural decisions
  - Key management
- Protocols
- Infrastructure
- Algorithms

Per-tree pricing protocols

- Privacy scales nearly linearly with computational burden
- Charge per-tree
- Examples:
  - Private information retrieval [Chor et al.][Cachin]
  - Group authentication [Chaum, van Heist] [CDS]
  - Mix networks [Chaum][Jakobsson]

Engineering tradeoffs

- Systems engineering
  - Architectural decisions
  - Key management
- Protocols
- Infrastructure
- Algorithms

Social implications

- Membranes and sinews
- Privacy
- Work practices
- Communities
  - Big
  - Dispersed
  - Frothy

Ad hoc networking

- Blue Tooth (of course)
- Casual LAN (CLANS)
  - Wearable computers
  - Modular robotics

Xerox Palo Alto Research Center
parc

New businesses possible

- Enable the access economy
  - (markets, property) => (networks, access)
- New business models
- New industries

Economic consequences

- Access economy [Herb Simon]
- Authentic experience
- Digital property rights
- Monetary dematerialization
- Attack vs. defense
  - Implications for SIGINT and surveillance
  - Military implications

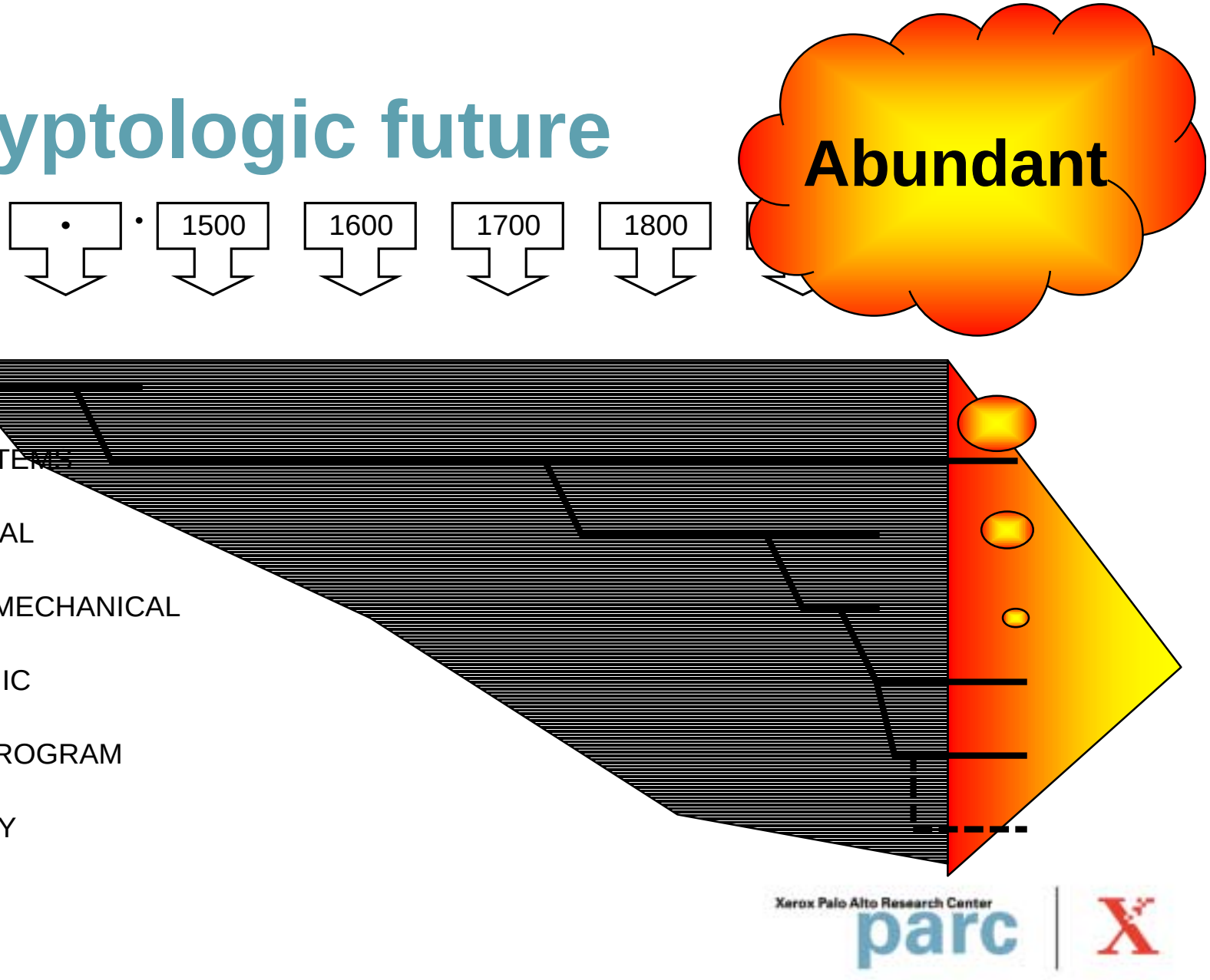
Political implications

- Changing role of government
- Information warfare

What next?

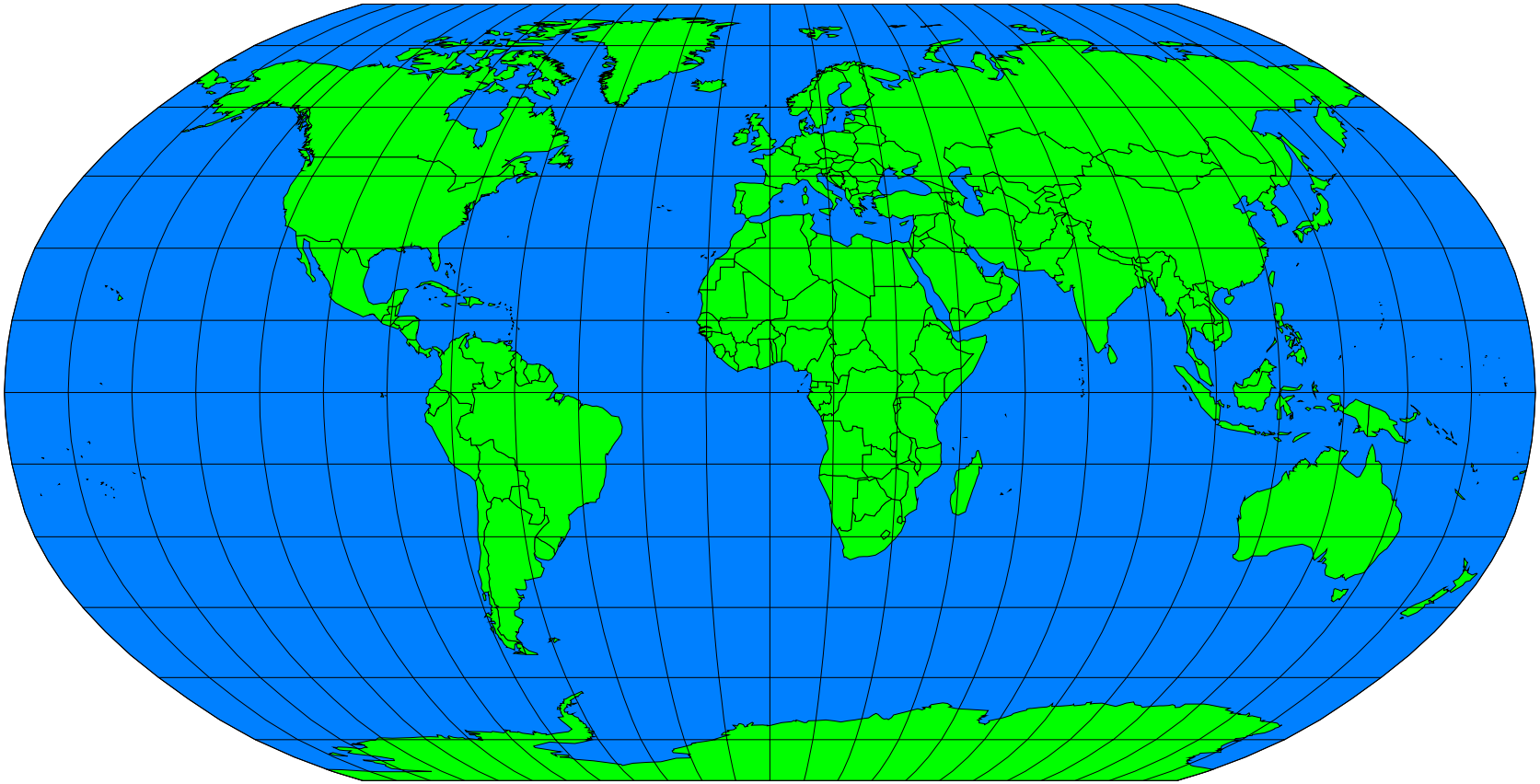
- Does this make sense to you?
- Can you use it in your work?
- Go forth and spread the word

Cryptologic future



Xerox Palo Alto Research Center
parc

2020 - Cryptography Everywhere



Xerox Palo Alto Research Center
parc

berson@anagram.com

Xerox Palo Alto Research Center
parc