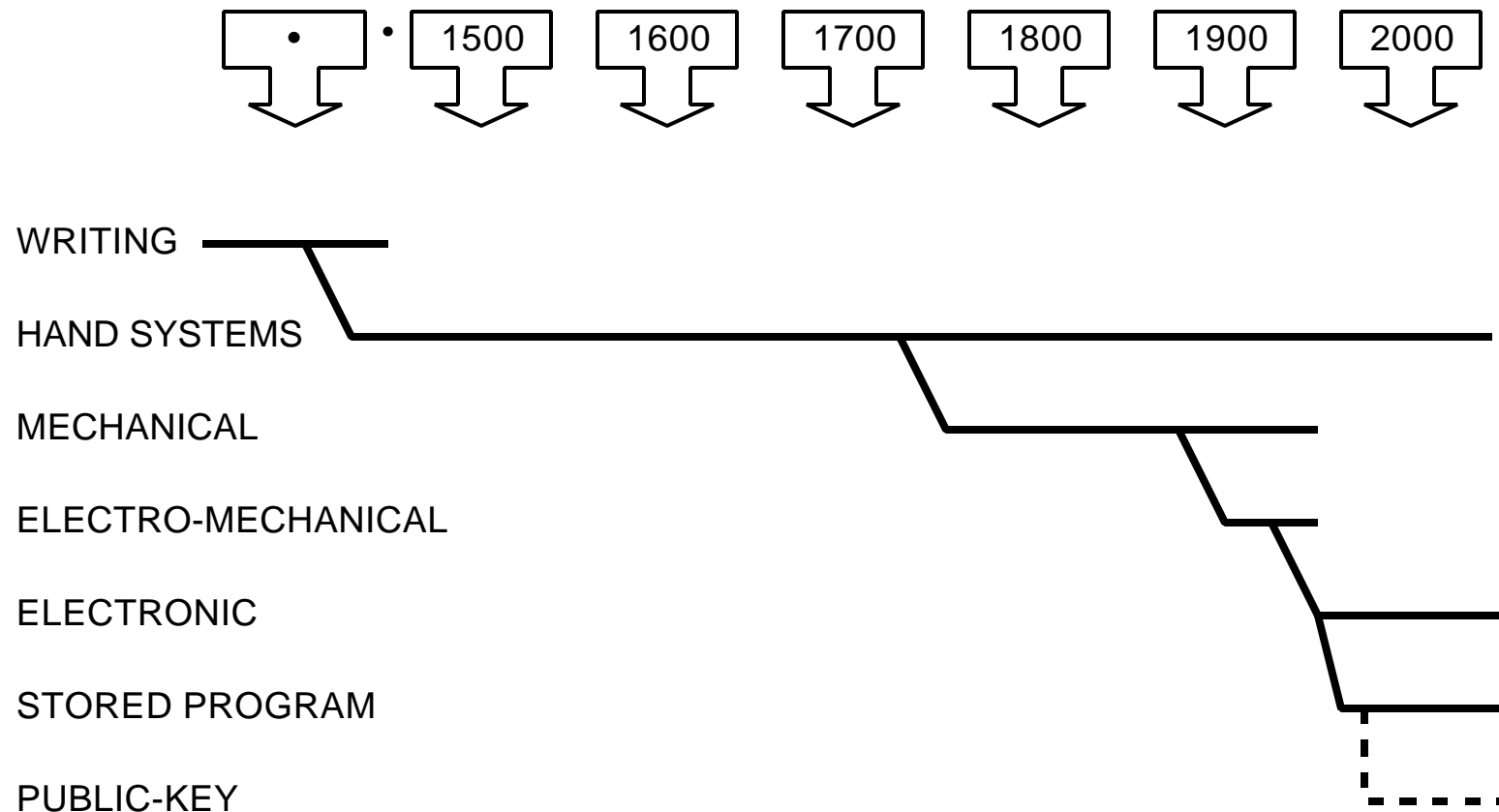
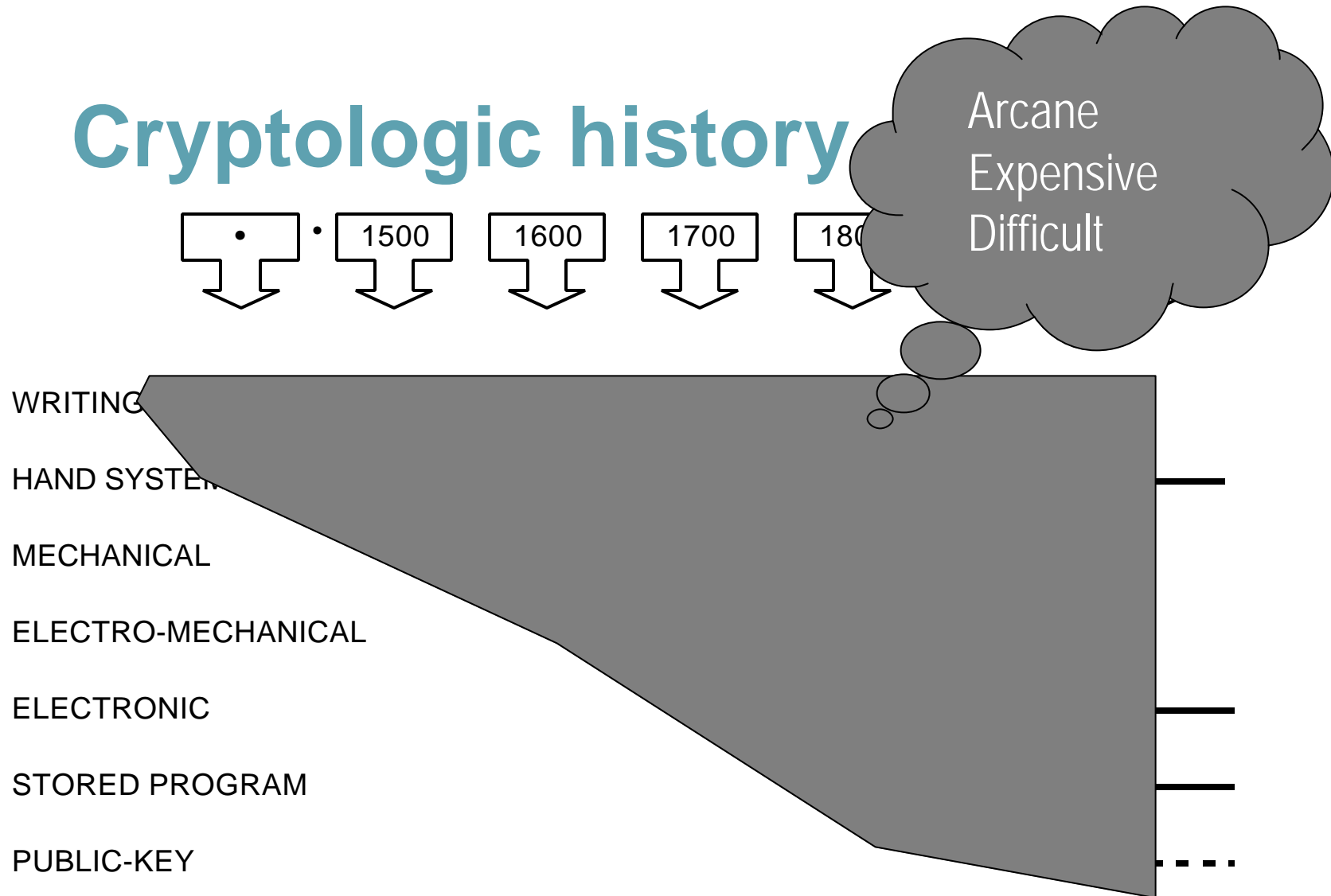


Cryptologic history



Cryptologic history



Xerox Palo Alto Research Center

parc



In the beginning

- Used chiefly by governments
- Taught only to initiates
- Practiced in Star Chambers
- Covered by Black Programs

Mention DES, NDC, RSA, IACR

T.A. Berson 20 June 2000 #3

Xerox Palo Alto Research Center
parc



So everybody came to think

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

Ron Rivest



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

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

The future is not something we enter. The future is something we create.

Leonard I. Sweet

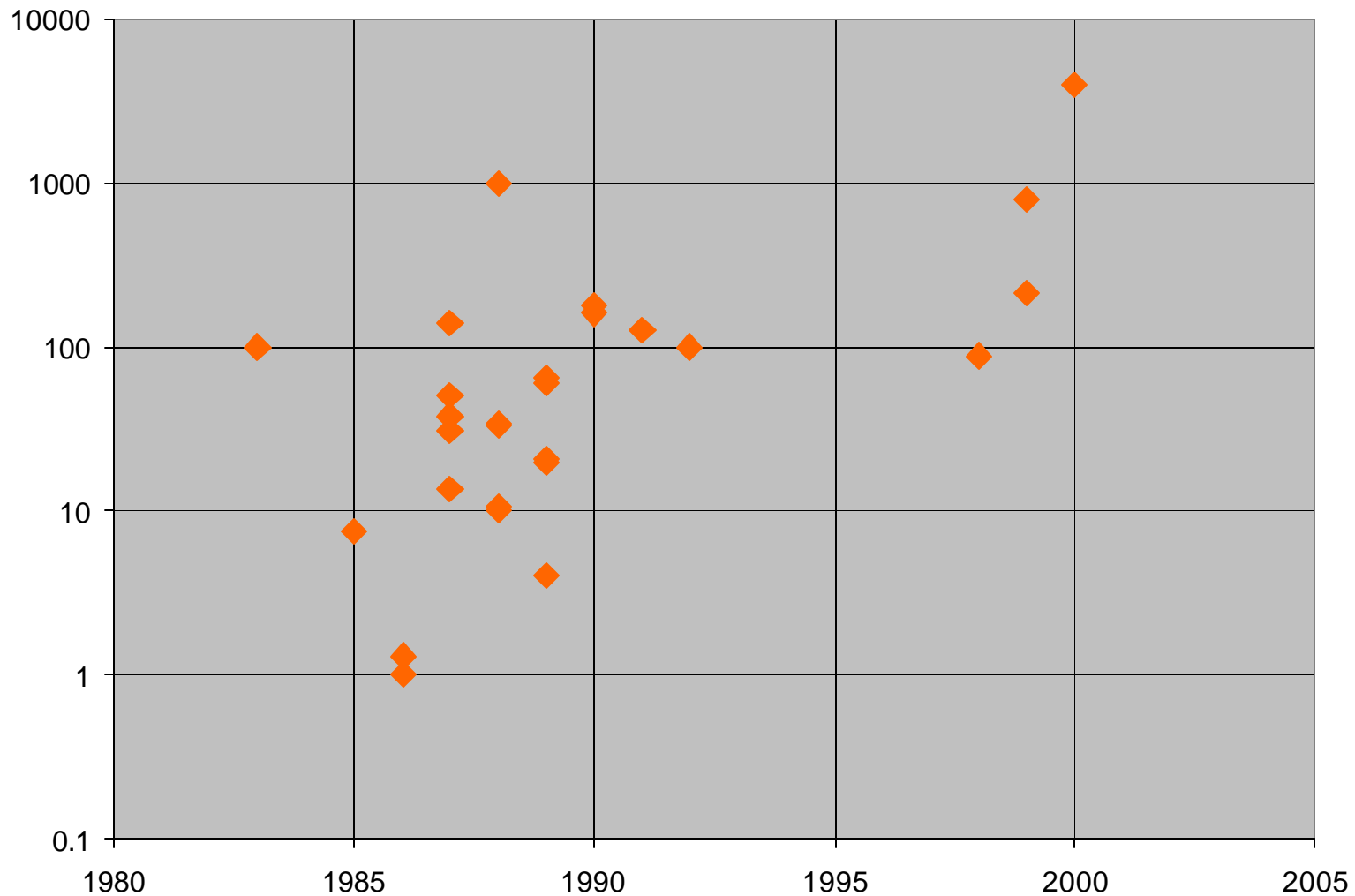
Harvesting the Fruits of Cryptographic Abundance

Tom Berson
Xerox PARC
20 June 2000

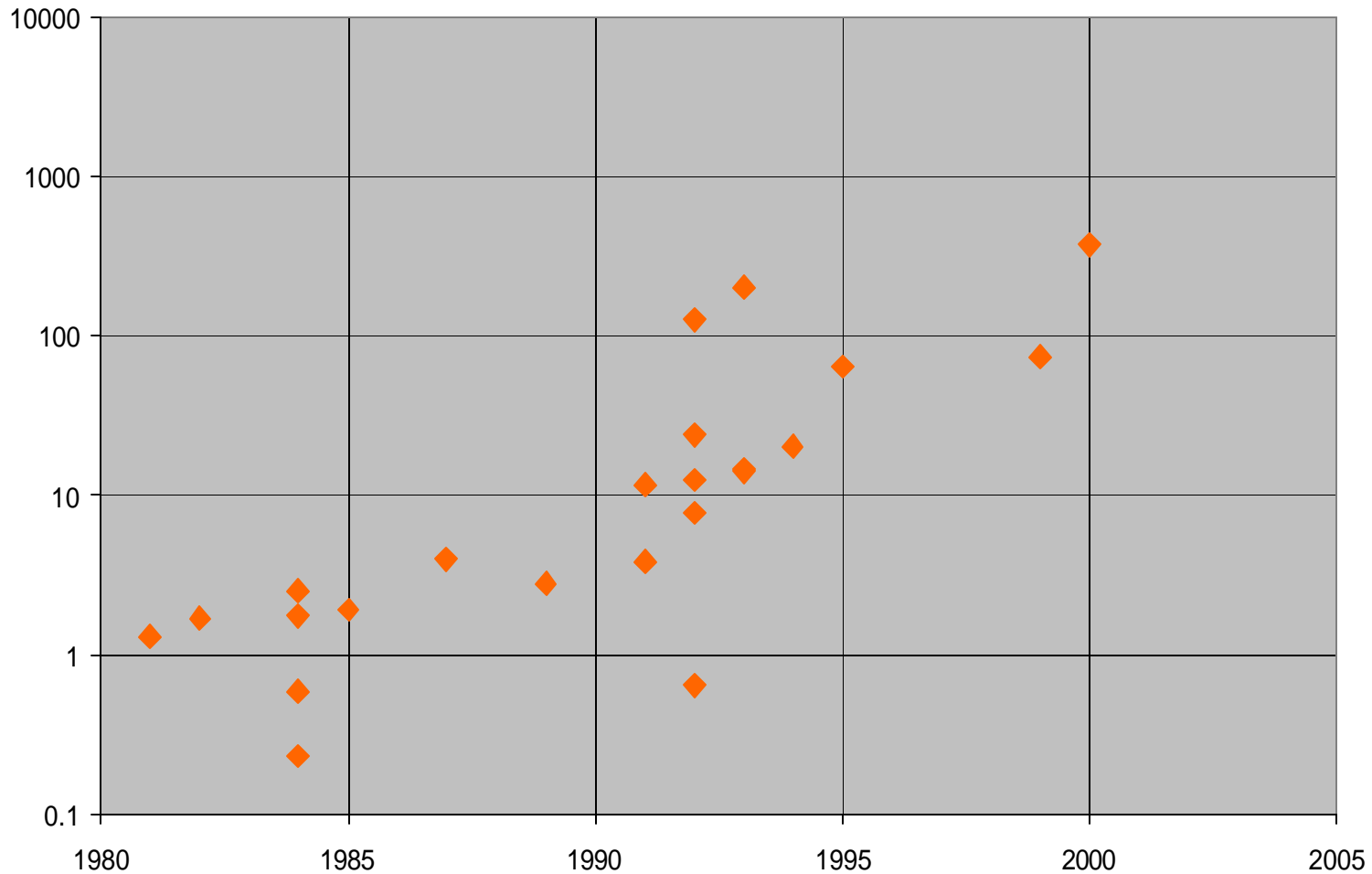
Trends

- 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 integration of cryptographic devices +
- Easing of government regulation

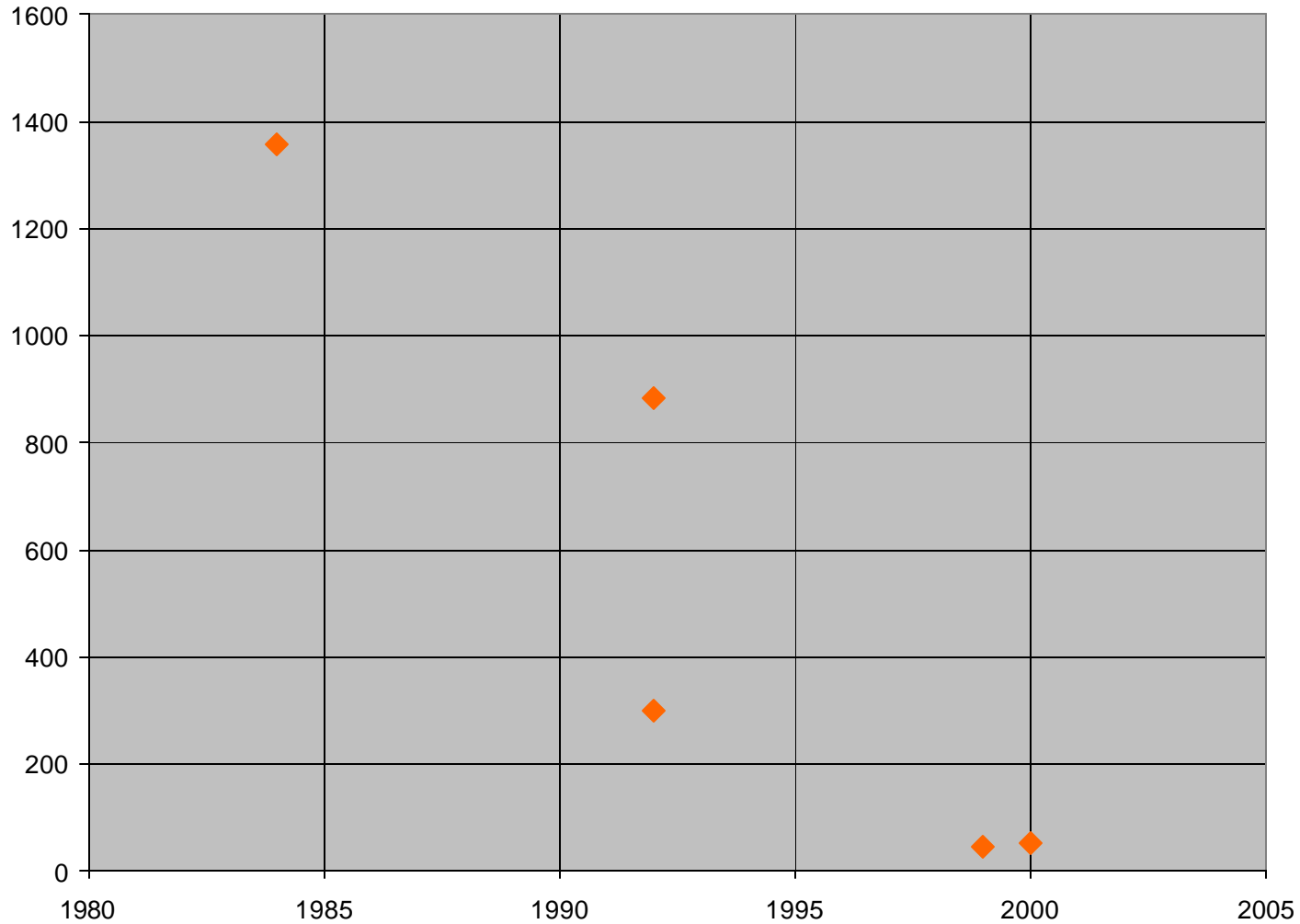
RSA speed (K 512-bit op/sec)



DES speeds (Mbyte/sec)



DES cost (\$/gigabit/sec)



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

Rise of successful businesses

	P/E	Market Cap. (\$Billion)
RSAS	19	2.9
VRSN	N/E	19.5
ENTU	199	1.4
BRCM	489	48.9

As of 11 July 2000, Source: finance.yahoo.com

Consumers make wide use of (hidden) cryptography

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

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

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

Imagine a world of abundant cryptography

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

Will it happen?

- User interface complexity
- Key management
- Government regulation

What would things be like in that world?



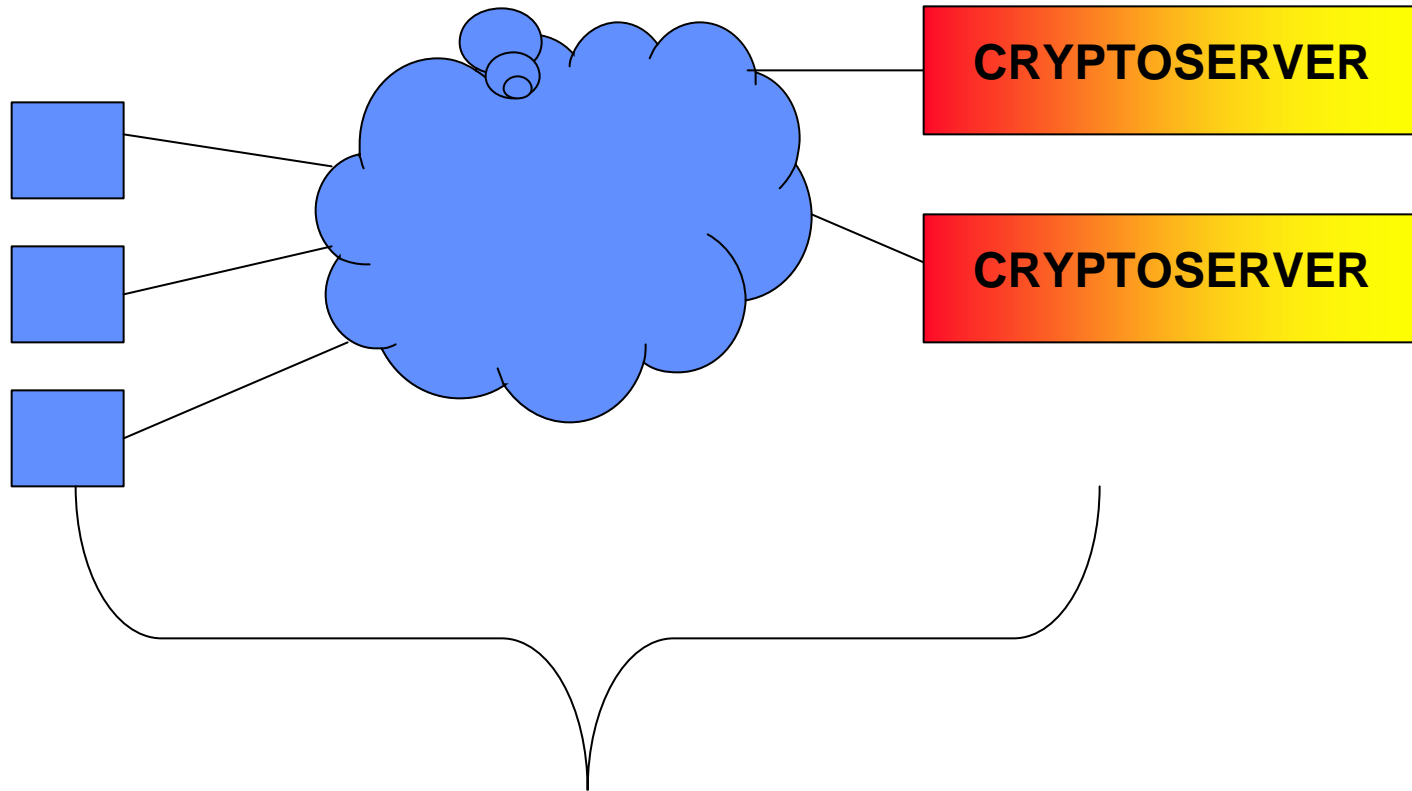
Scientific questions

- Complexity theory
- Information theory

Engineering tradeoffs

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

Cryptography as a network service



Engineering tradeoffs

- Systems engineering
 - Architectural decisions
 - Key management
- Protocols (Show per-tree)
- 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 (mention EU privacy and 3PPP)
- Work practices
- Communities
 - Big
 - Dispersed
 - Frothy
- Ad hoc networks of wearable computers

New businesses possible

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

Economic consequences

- Monetary dematerialization
- Attack vs. defense
 - Implications for SIGINT and surveillance
 - Military implications

People at PARC

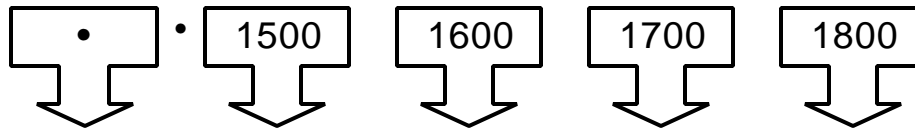
- Drew Dean
- Matt Franklin
- Teresa Lunt
- Diana Smetters
- Paul Stewart
- Interns: Adam Stubblefield,
Michel Abdalla, Michael Semanko

Mention openings

What next?

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

Cryptologic future



WRITING

HAND SYSTEM

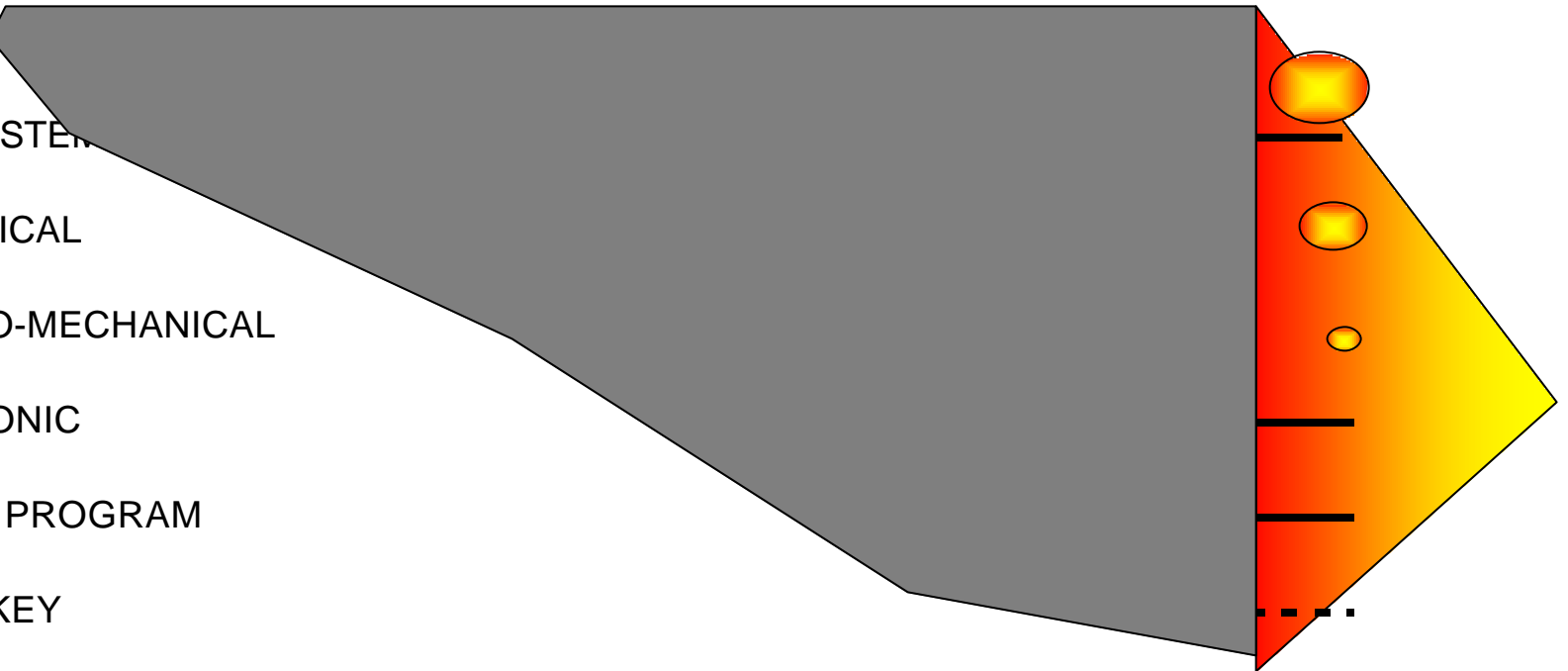
MECHANICAL

ELECTRO-MECHANICAL

ELECTRONIC

STORED PROGRAM

PUBLIC-KEY



Xerox Palo Alto Research Center

parc



