Software Engineering Conference Russia 2018

October 13
Moscow

A Briefer History of Cryptoanarchy

Igor Dëmin
nexign

Disclaimer

Докладчик выступает от своего имени. Докладчик не делает каких-либо политических призывов и заявлений. Докладчик приглашает Вас к самостоятельному изучению освещаемых тем, но не несёт ответственности за нарушение сна, пищеварения и любой материальный и нематериальный ущерб.

Crypto is about Cryptography

Без правителей, без лидеров, неподвластность, независимость.

“Law and freedom without force” - I. Kant

Либертарианство

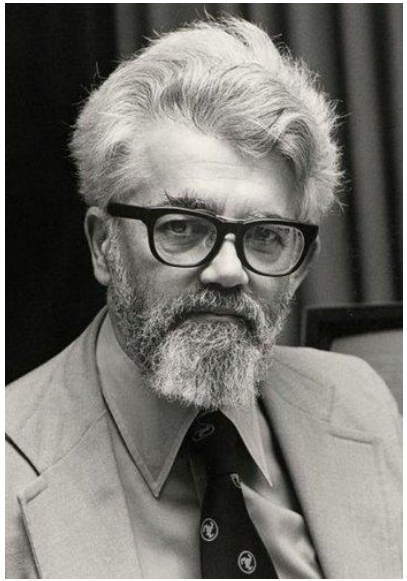
60-70

Whitfield Diffie

SAIL

ARPANET

Home
shopping

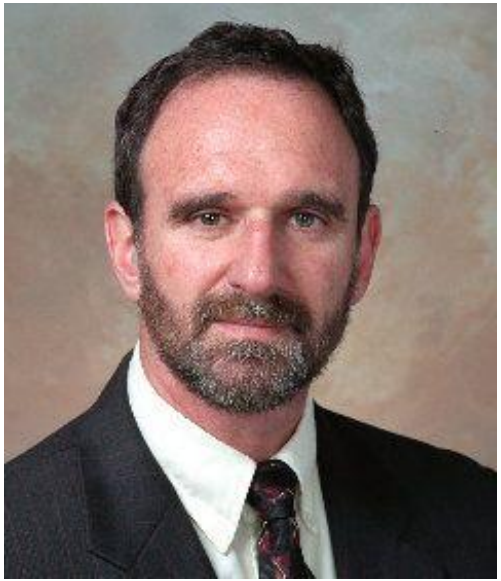


John McCarthy

70-

Whitfield Diffie

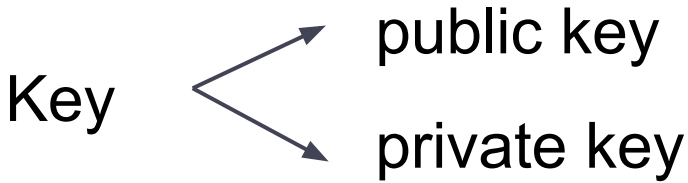
Alan Konheim
IBM Laboratory



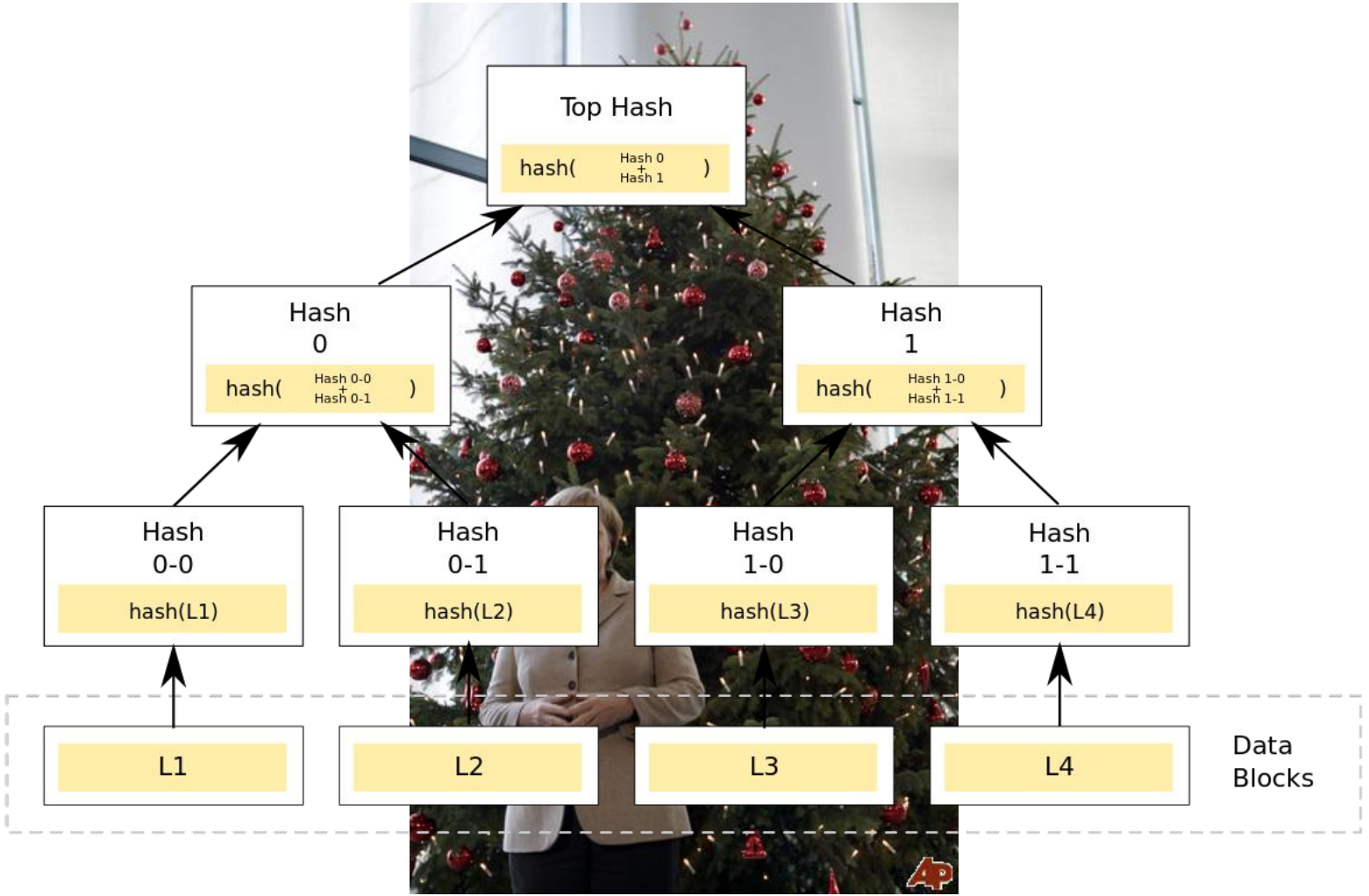
Martin Hellman

70-

1975 (May) - Public Key Cryptography



1975 (Dec) - Multiuser cryptographic techniques
(official publication June, 1976)


Top Hash
hash(Hash 0 + Hash 1)
Hash 0
hash(Hash 0-0 + Hash 0-1)
Hash 1
hash(Hash 1-0 + Hash 1-1)
Hash 0-0
hash(L1)
Hash 0-1
hash(L2)
Hash 1-0
hash(L3)
Hash 1-1
hash(L4)
L1
L2
L3
L4
Data Blocks

70-

Ralph Merkle

Secure communication over insecure channels
1975 (August), но выходит только в 1978 (April)

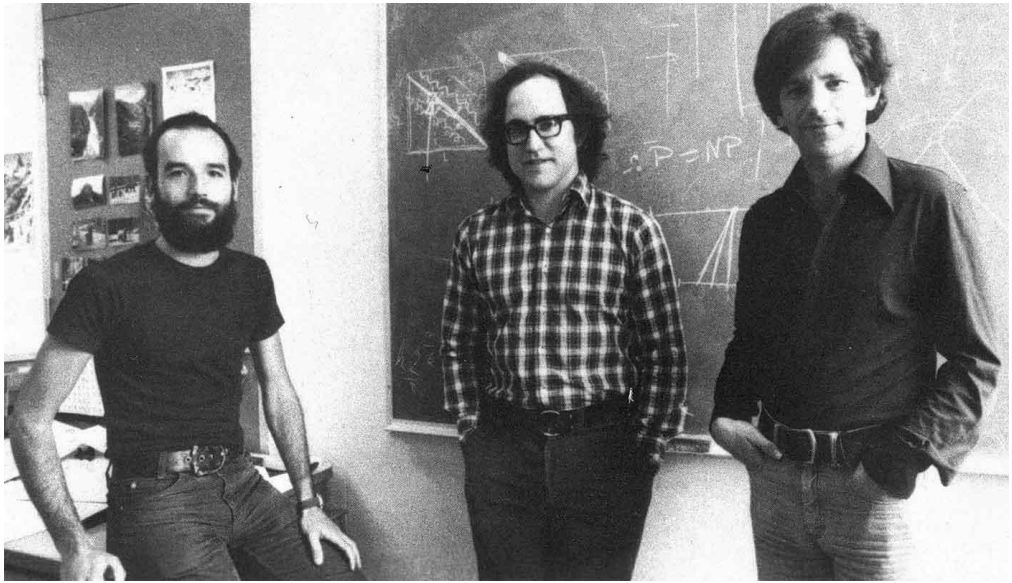
70-

1976 (May) - exponential key exchange

1976 (November) - **New Directions in Cryptography**

“We stand today at the brink of a revolution in cryptography.”

70-



Ron **R**ivest

Adi **S**hamir

Leonard **A**dleman

1977 (April)

1978 (Febrary) - CACM

A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

Ralph Merkle

Programming Techniques
S. L. Graham, R. L. Rivest Editors

Secure Communications Over Insecure Channels

Ralph C. Merkle
Department of Electrical Engineering and Computer Sciences
University of California, Berkeley

Communications of the ACM
April 1978
Volume 21
Number 4

Received August 1975; revised September 1977

References

1. Diffie, W., and Hellman, M. New directions in cryptography. *IEEE Trans. on Inform. IT-22*, 6 (Nov. 1976), 644–654.
2. Feistel, H. Cryptography and computer privacy. *Sci. Amer. 228*, 5 (May 1973), 15–23.
3. Kahn, D. *The Codebreakers.* MacMillan, New York, 1976.
4. Merkle, R., and Hellman, M. Hiding information and receipts in trap door knapsacks. To appear, IEEE Trans. on Inform.
5. Rivest, R.L., Shamir, A., and Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Comm. ACM 21*, 2 (Feb. 1978), 120–126.
6. Shannon, C.E. Communication theory of secrecy systems. *Bell Syst. Tech. J. 28* (1949), 654–715.
7. Wyner, A.D. The wire tap channel. *Bell Syst. Tech. J. 54*, 8 (Oct. 1975), 1355–1387.

80-

David Chaum

1981 - “Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms”

CRYPTO 82

IACR - International Association for Cryptologic Research

“Blind Signatures for Untreaceable Payments”

CRYPTO 83

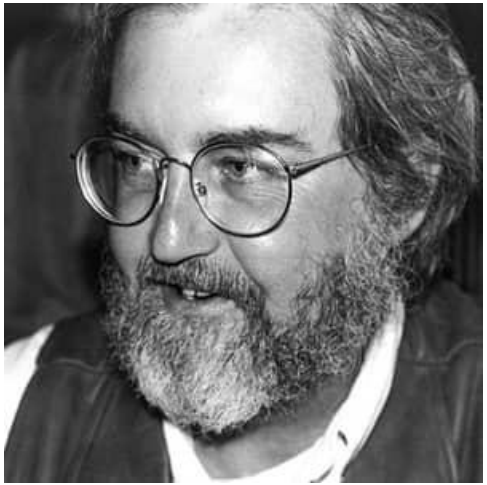
1985 - “Security without identification: Transaction Systems to Make Big Brother Obsolete”

80-

“ [Crypto Anarchy] will alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation.” Timothy May, 1988

Cypherpunks

80-



Timothy May

1988 - The Crypto Anarchist Manifesto

1994 - The Cyphernomicon

90-

John Gilmore

1990(July) - Electronic Frontier Foundation, EFF

90-

Phillip Zimmerman

1991- Pretty Good Privacy

90-

1992 - Timothy May, Eric Hughes, John Gilmore

cipher + cyberpunk = cypherpunk

Cypherpunks mailing list

1993(March) - A Cypherpunk’s Manifesto

A Cypherpunk's Manifesto

- В электронный век для открытого общества необходима конфиденциальность
- Мы не можем ожидать, что правительства, корпорации и другие безликие организации предоставят нам конфиденциальность
- Мы должны защитить нашу собственную конфиденциальность, если ожидаем иметь хоть какую-то.

A Cypherpunk's Manifesto

- Шифропанки пишут код

- Мы знаем, что кто-то должен написать софт для защиты конфиденциальности… и мы собираемся это сделать.

Tim May, John Gilmore, Eric Hughes, Whit Diffie, Nick Szabo

90-00

1994 - DigiCash (David Chaum, Nick Szabo)

1997 - Adam Back - HashCash / PoW

1998 - Wei Dai - bmoney

1997-2000 - Julian Assange - deniable encryption

Julian Assange: в мире вовсю идет война за будущее общественное устройство, но для большинства она невидима. С одной стороны, в ней участвуют государства и корпорации, связанные друг с другом, – они повсеместно шпионят за нами. Им противостоят шифропанки – мастера программирования и криптографии с активной гражданской позицией. Именно в недрах этого движения зародился WikiLeaks.

Wei Dai: я восхищён криптоанархией Тимоти Мэя. В отличии от сообществ, традиционно ассоциирующихся со словом “анархия”, в криптоанархии правительство не просто временно уничтожено, а запрещено и не требуется.
Это сообщество, где угроза насилия бессильна, потому что насилие невозможно, потому что его участники не могут быть связаны с их реальными именами и местоположением.

2000-

2001(Jule) - Bram Cohen - BitTorrent

2000-

2008…　Satoshi Nakamoto - Bitcoin

Contacts

- Igor Dëmin
- Email: igor.demin@nexign-systems.com
- Twitter: idemin1