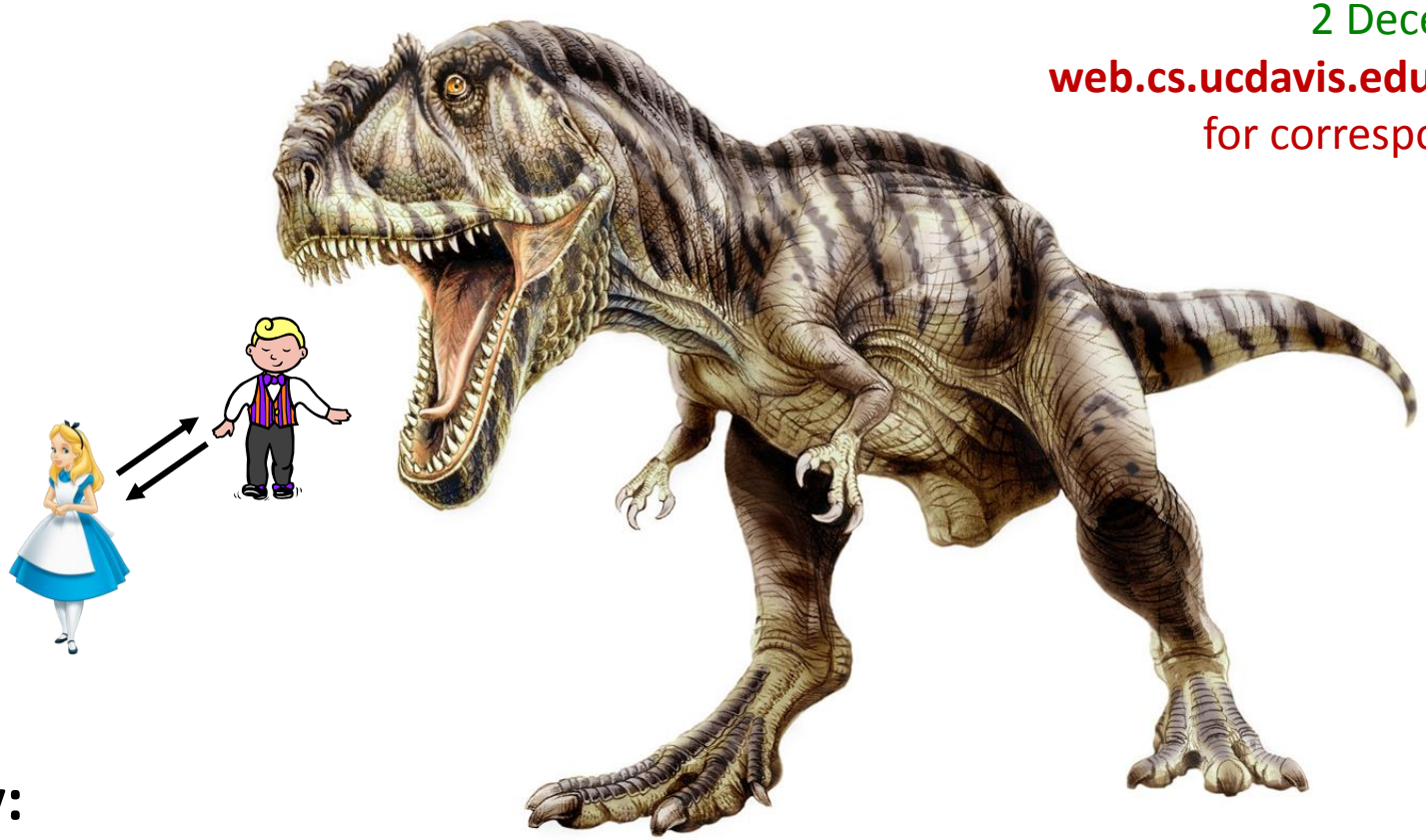
The Moral Character of Cryptographic Work

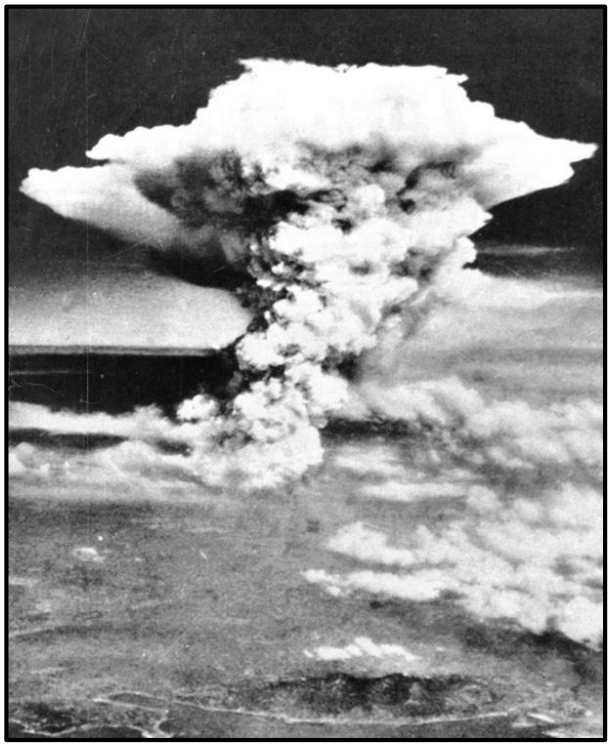
Phillip Rogaway
IACR Distinguished Lecture
Asiacrypt 2015
Auckland, New Zealand
2 December 2015
web.cs.ucdavis.edu/~rogaway/
for corresponding essay



Today:

① Social responsibility of scientists and engineers
② The political character of cryptographic work
③ The dystopian world of pervasive surveillance
④ Creating a more just and useful field

Three events shaping scientists' view of social responsibility



Experience of atomic scientists
Bombing of Hiroshima, 1945

Nuremberg trials
Doctors' trial, 1946-47
Dr. Karl Brandt

Rise of environmental movement
Children spraying DDT, 1953

➔**The Democratization of Responsibility**

The Ethic of Responsibility

for scientists and engineers

- Do **not** contribute with your work to **social harm.**
  A **negative** right. Obliges **inaction**.

- Contribute with your work to the **social good.**
  A **positive** right. Obliges **action**.

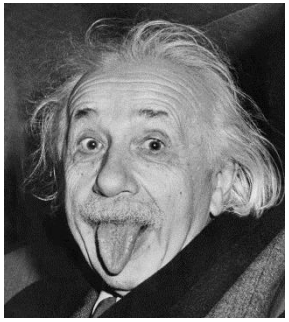
- These obligations stem from your **professional role.**
  For us: as a **cryptographer**, **computer scientist**, and **scientist.**

Ethic of Responsibility becomes the
Doctrinal Norm

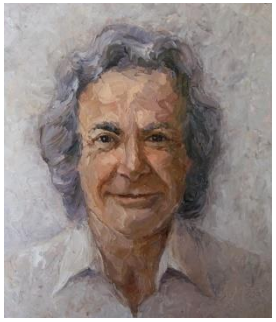
- Professional “Codes of Ethics” like those of ACM and the IEEE
- Organizations like Pugwash, CPSR, EFF, PI, EPIC, CDT, … emerge
- IACR Bylaws:

  “*The purposes of the IACR are*
  to advance the theory and practice of cryptology and related fields, and
  to promote the interests of its members with respect thereto, and
  to ***serve the public welfare****.”*

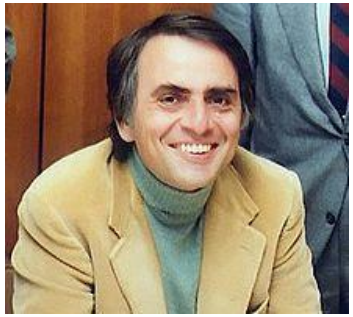
The Good Scientist becomes a Cultural Icon



Albert Einstein



Richard Feynman



Carl Sagan

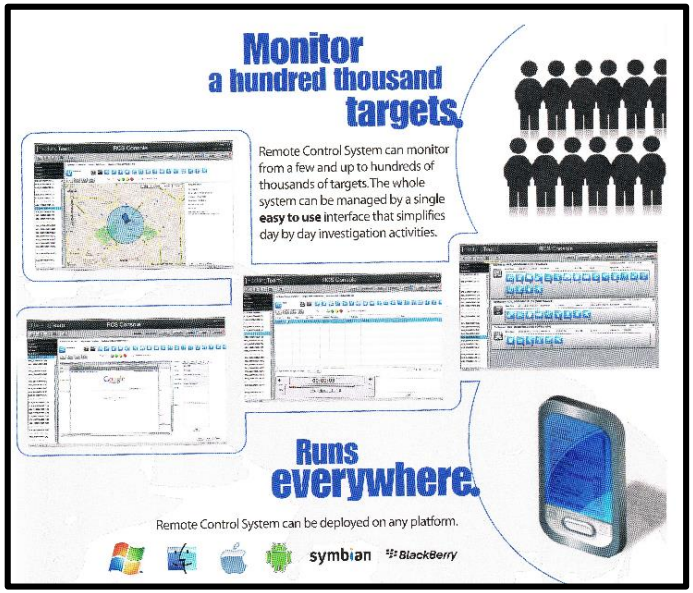
Jonas Salk

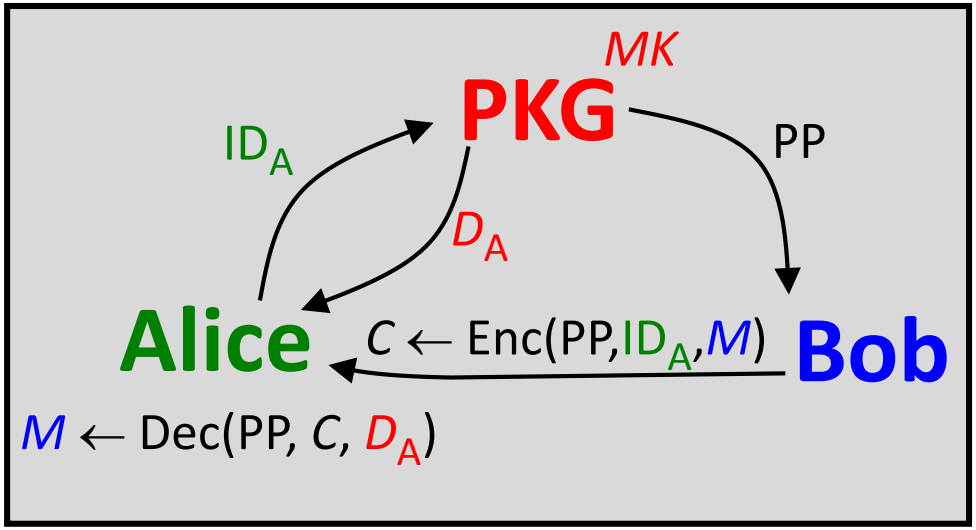
The Ethic of Responsibility in Decline

- Easy to find scientists for military work
- UC runs WMD labs. Universities run on federal/military funding
- Social-utility of work nearly unconsidered by students
- In academia, having a normative vision deprecated:
  Our job is not to save the world, but to interpret it – S. Fish
- CS Faculty recruiting –

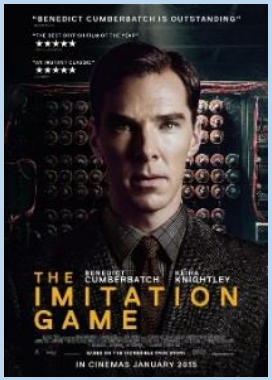
Data-mining faculty candidate

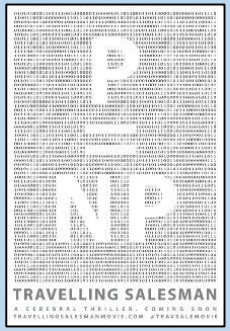
Artifacts and Ideas are Routinely Political

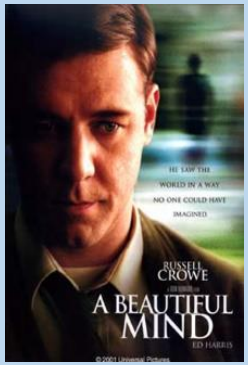


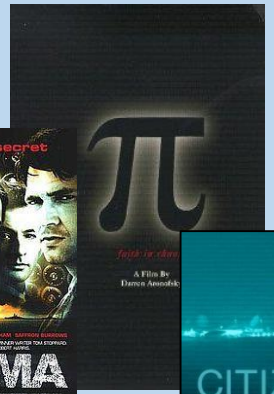


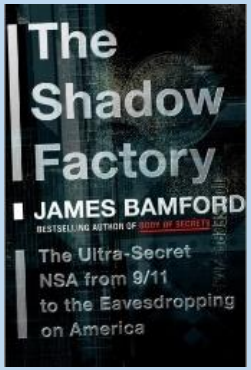
Cryptographer as SPY

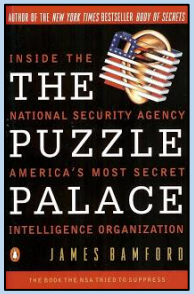


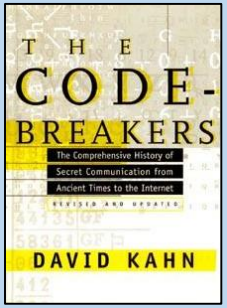




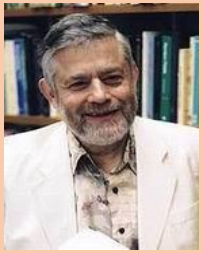


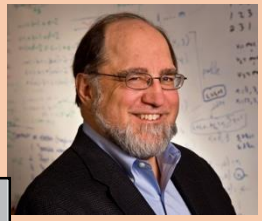


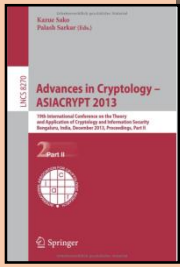


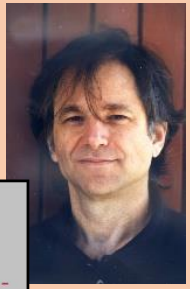


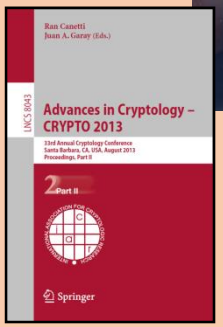
Cryptographer as SCIENTIST











Cryptographers Used to be More Political

I told her [my wife, circa 1976] that we were headed into a world where people would have important, intimate, long-term relationships with people they had never met face to face. I was worried about privacy in that world, and that's why I was working on cryptography.

Whitfield Diffie, testifying at the Newegg vs. TQP patent trial, 2014

Whit Diffie

David Chaum

The foundation is being laid for a dossier society, in which computers could be used to infer individuals' life-styles, habits, whereabouts, and associations from data collected in ordinary consumer transactions. Uncertainty about whether data will remain secure against abuse by those maintaining or tapping it can have a `chilling effect,' causing people to alter their observable activities.

David Chaum: Security without Identification: transaction systems to make big brother obsolete. CACM 1985.

Disciplinary Divide

Venues of the
10 most cited papers citing [Chaum]:
Untraceable electronic mail, 1981
(4481 citations)

1. *Peer-to-Peer Systems*
2. *Designing Privacy Enhancing Technologies*
3. *Proc. of the IEEE*
4. *Wireless Networks*
5. *USENIX Security Symposium*
6. *ACM SIGOPS*
7. *ACM Tran on Inf. Sys*
8. *ACM Comp. Surveys*
9. *ACM MobiSys*
10. *IEEE SAC*

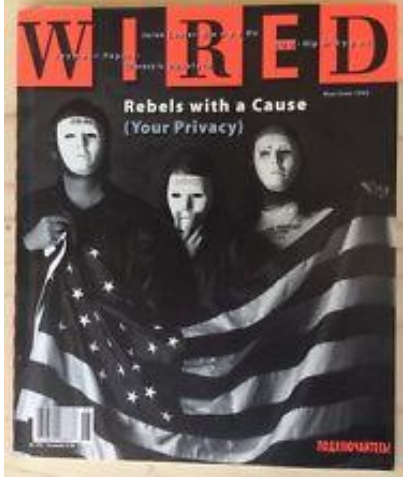
Venues of the
10 most cited papers citing [GM]
Goldwasser and Micali
Probabilistic Encryption, 1982/84
(3818 citations)

1. *CRYPTO*
2. *FOCS*
3. *MobiCom* outlier
4. *CCS*
5. *STOC*
6. *EUROCRYPT*
7. *STOC*
8. *CRYPTO*
9. *FOCS*
10. *CRYPTO*

$$\text{Top10(Chaum)} \cap \text{Top10(GM)} = \varnothing$$

Cypherpunks

The strongest advocates of crypto



Tim May – Eric Hughes – John Gilmore
Steven Levy, "Crypto Rebels", *Wired*, 1993.

We must defend our own privacy if we expect to have any. We must come together and create systems which allow anonymous transactions to take place. … We are defending our privacy with cryptography

***Eric Hughes**, 1993*

But we discovered something. … A strange property of the physical universe that we live in. The universe believes in encryption. It is easier to encrypt information than it is to decrypt it. We saw we could use this strange property to create the laws of a new world

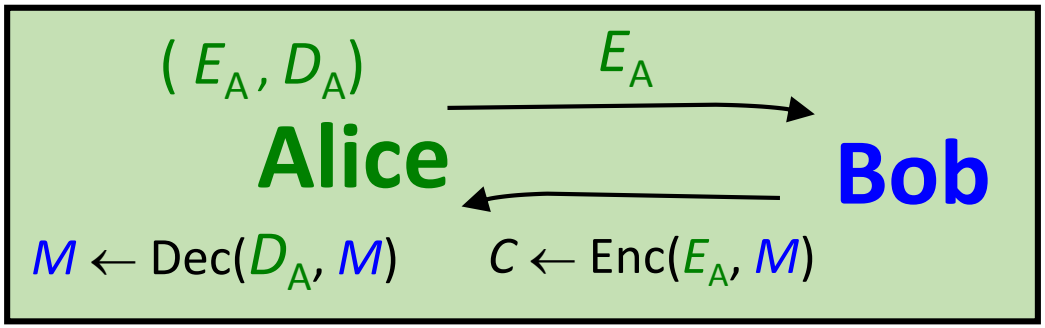
***Julian Assange**, 2012*

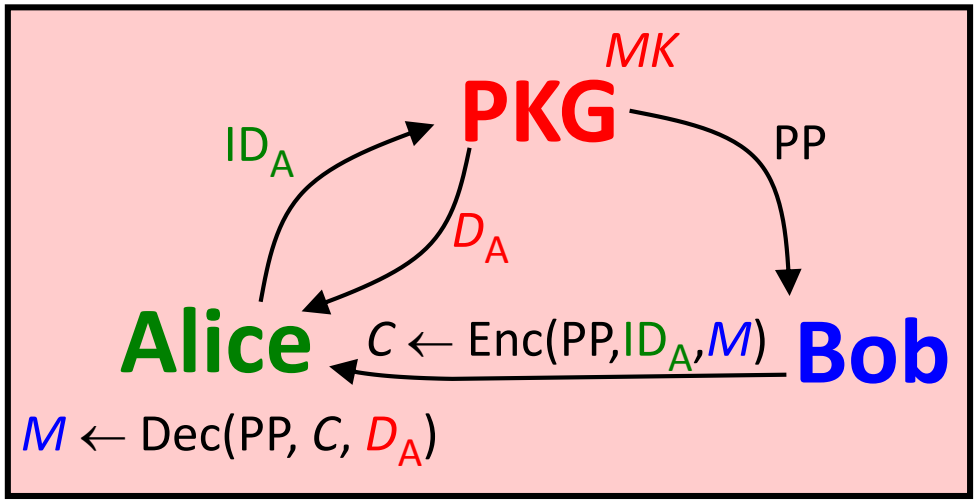
In words from history, let us speak no more of faith in man, but bind him down from mischief by the chains of cryptography.

***Edward Snowden**, 2013*

Cryptography doesn't always favor the weak.
It depends.

1. Conventional encryption (sym or asym)





2. Identity-based encryption (IBE)

3. Fully homomorphic encryption (FHE) and indistinguishability obfuscation (iO)

The Summer of Snowden
2013

Edward Snowden
2013

theguardian

News | US | World | Sports | Comment | Culture | Business | Money

News › World news › The NSA files

Series: Glenn Greenwald on security and liberty

Revealed: how US and UK spy agencies defeat internet privacy and security

- NSA and GCHQ unlock encryption used to protect emails, banking and medical records
- $250m-a-year US program works covertly with tech companies to insert weaknesses into products
- Security experts say programs 'undermine the fabric of the internet'

- Q&A: submit your questions for our privacy experts

James Ball, Julian Borger and Glenn Greenwald
Guardian Weekly, Thursday 5 September 2013
Jump to comments (...)

News › World news › US national security

Series: Glenn Greenwald on security and liberty

NSA collecting phone records of millions of Verizon customers daily

Exclusive: Top secret court order requiring Verizon to hand over all call data shows scale of domestic surveillance under Obama

- Read the Verizon court order in full here
- Obama administration justifies surveillance

Glenn Greenwald
The Guardian, Wednesday 5 June 2013
Jump to comments (...)

Under the terms of the order, the numbers of both parties on a call a
as is location data and the time and duration of all calls. Photograp

The National Security Agency is currently collecting the tel
records of millions of US customers of Verizon, one of Ame
telecoms providers, under a top secret court order issued

The order, a copy of which has been obtained by the Guardian, requires Verizon on an "ongoing, daily basis" to give the NSA information on all telephone calls in its systems, both within the US and between the US and other countries.

The Washington Post

FRIDAY, JUNE 7, 2013

U.S. mines Internet firms' data, documents show

Google, Facebook, Apple, Yahoo deny giving NSA direct access to servers

BY BARTON GELLMAN AND LAURA POITRAS

The National Security Agency and the FBI are tapping directly into the central servers of nine leading U.S. Internet companies, extracting audio and video chats, photographs, e-mails, documents, and connection logs that enable analysts to track foreign

PRISM, has not been made public until now. It may be the first of its kind. The NSA prides itself on stealing secrets and breaking codes, and it is accustomed to corporate partnerships that help it divert data traffic or sidestep barriers. But there has never been a Google or Facebook before, and it is unlikely that there are richer troves of valuable intelligence

tion directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple."

PRISM was launched from the ashes of President George W. Bush's secret program of warrantless domestic surveillance in 2007, after news media disclosures, lawsuits and the Foreign Intelligence Surveillance Court forced the president to look for new authority.

Congress obliged with the Protect America Act in 2007 and the FISA Amendments Act of 2008,

Defense and criticism

Agency knows much about public, but we know little about it

BY ANNE GEARAN

The National Security Agency, nicknamed "No Such Agency" because of its ultra-secrecy, is the government's eavesdropper-in-chief.

Charged primarily with electronic spying around the globe, the NSA collects billions of pieces of intelligence from foreign phone

same information on millions of ordinary Americans.

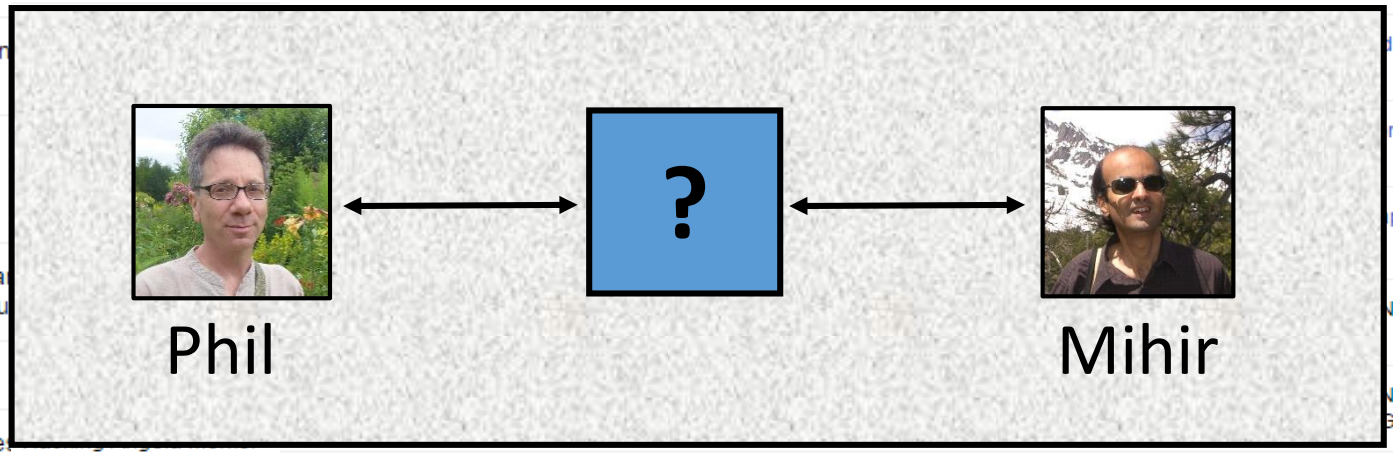
Regarded as the most secretive of the nation's intelligence agencies, the NSA is part of the military but answers to the director of national intelligence. Its major operations are housed in cybersecrecy at Maryland's Fort Meade Army base, the site of the court-martial of Pfc. Bradley Manning, who is charged with stealing government electronic communications and passing them to the anti-secrecy organization WikiLeaks.

The agency

Newseum

Complexity + Secrecy: A Toxic Mix

VictoryDance	Honey Traps	Monitoring Privacy Software	Spying on American Muslims	FBI monitored e-mail of 200 Americans including prominent Muslims such as a former Bush Administration official, two professors, an attorney and the leader of a Muslim civil rights group. NSA
Hammerchant / Hammerstein	Surveillance of 2009 U.N. Climate Change conference	SecondDate	Upstream	The Upstream program collects communications transiting the Internet via commercial partners codenamed Fairview, Stormbrew, Blarney, and Oakstar. NSA
ANT catalog	Spying on Gamers	NoseySmurf, TrackerSmurf, DreamySmurf, ParanoidSmurf	50,000 implants	An NSA map of the 50,000 computers worldwide it has implanted with surveillance malware. NSA
Cracking cellphon encryption				d G20 summits in NSA
Optic Nerve				ne call records - NSA
				pps to identify NSA
Swedish-America surveillance of Ru				NSA
Gilgamesh				NSA and GCHQ
Buddy List, Addre Book Spying				
Hacking Anonymo	Hacking Al Jazeera	Shotgiant	An NSA program to break into Chinese-owned Huawei networks and products.	NSA
Co-Traveler/ FASC	Cellphone Location Test	WillowVixen	An NSA technique to deploy malware by sending out emails that trick targets into clicking a malicious link.	NSA
Hacking OPEC	Tapping Underseas Cables	Turmoil	A large network of clandestine surveillance "sensors" to collect data from satellites, cables, and microwave communications around the world.	NSA
Tracfin	Angry Birds	Turbine	A network of active command and control servers around the world that can be used for "industrial scale exploitation."	NSA
Wellspring	Royal Concierge	Squeaky Dolphin	A British effort to monitor YouTube video views, URLS "liked" on Facebook and Blogger visits.	NSA



Law-Enforcement Framing

U.S. FBI Director
James Comey

Privacy is a **personal good**

Security is a **collective good**

Inherently in **conflict**

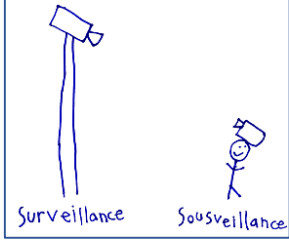
Encryption has destroyed the **balance.** Privacy wins

The **bad guys** may win

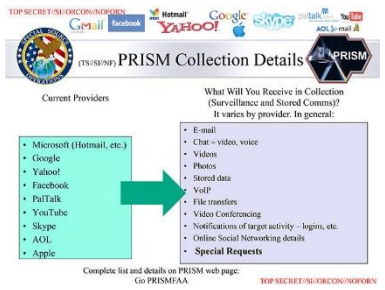
Risk of **Going Dark**.

Surveillance-Studies Framing

Drawing by the six-year-old **daughter of** surveillance-studies scholar **Steve Mann**



Surveillance is an **instrument of power**



Technology makes it **cheap**

Tied to **cyberwar** and **assassinations**

Privacy and security usually **not** in conflict

Makes people **conformant**, **fearful**, **boring**. Stifles **dissent**

Hard to stop. **Cryptography** offers hope

Political Surveillance

KING,

In view of your low grade, abnormal personal behavoir I will not dignify your name with either a Mr. or a Reverend or a Dr. And, your last name calls to mind only the type of King such as King Henry the VIII and his countless acts of adultery and immoral conduct lower than that of a beast.

King, look into your heart. You know you are a complete fraud and a great liability to all of us Negroes. White people in this country have enough frauds of their own but I am sure they don't have one at this time that is any where near your equal. You are no clergyman and you know it. I repeat you are a colossal fraud and an evil, vicious one at that. You could not believe in God and act as you do. Clearly you don't believe in any personal moral principles.

King, like all frauds your end is approaching. You could have been our greatest leader. You, even at an early age have turned out to be not a leader but a dissolute, abnormal moral imbecile. We will now have to depend on our older leaders like Wilkins a man of character and thank God we have others like him. But you are done. Your "honorary" degrees, your Nobel Prize (what a grim farce) and other awards will not save you. King, I repeat you are done.

No person can overcome facts, not even a fraud like yourself. Lend your sexually psychotic ear to the enclosure. You will find yourself and in all your dirt, filth, evil and moronic talk exposed on the record for all time. I repeat - no person can argue successfully against facts. You are finished. You will find on the record for all time your filthy, dirty, evil companions, male and females giving expression with you to your hidious abnormalities. And some of them to pretend to be ministers of the Gospel. Satan could not do more. What incredible evilness. It is all there on the record, your sexual orgies. Listen to yourself you filthy, abnormal animal. You are on the record. You have been on the record - all your adulterous acts, your sexual orgies extending far into the past. This one is but a tiny sample. You will understand this. Yes, from your various evil playmates on the east coast to [redacted] and others on the west coast and outside the country you are on the record. King you are done.

The American public, the church organizations that have been helping - Protestant, Catholic and Jews will know you for what you are - an evil, abnormal beast. So will others who have backed you. You are done.

King, there is only one thing left for you to do. You know what it is. You have just 34 days in which to do (this exact number has been selected for a specific reason, it has definite practical signifficant. You are done. There is but one way out for you. You better take it before your filthy, abnormal fraudulant self is bared to the nation.

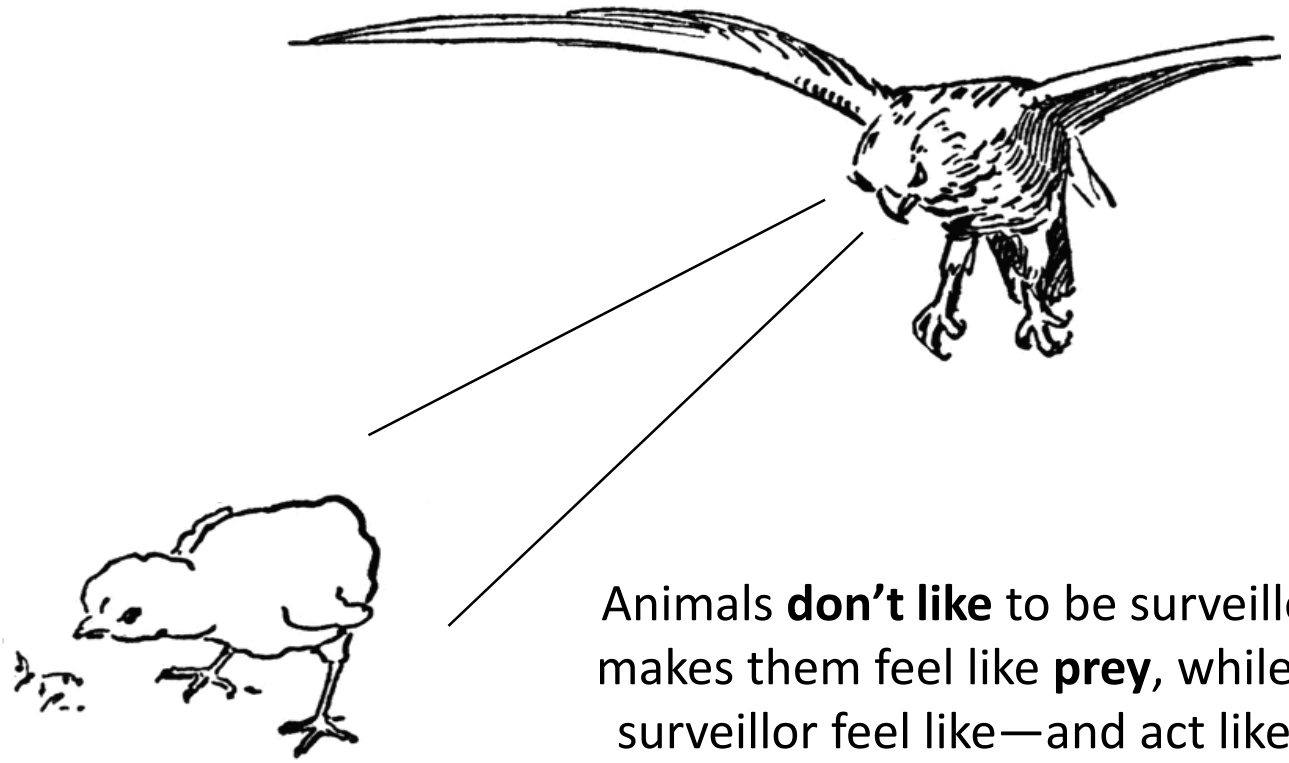
FBI's "suicide letter" to civil rights leader Martin Luther King, Jr 1964

Student activists at UC Berkeley, 1964

Activist
Abdul Ghani Al Khanjar

Free Trade Area of the Americas summit
Miami, 2003

Instinctual Disdain



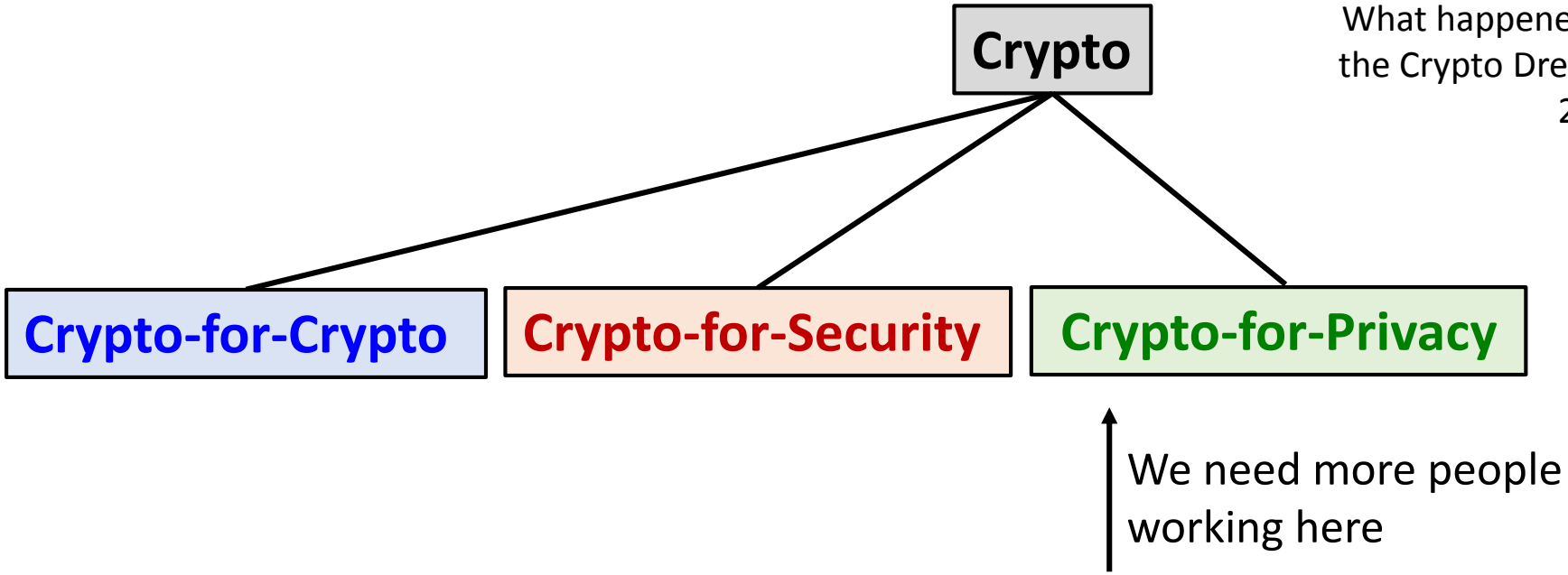
Animals **don't like** to be surveilled because it makes them feel like **prey**, while it makes the surveillor feel like—and act like—a **predator**

Paraphrased from Bruce Schneier*, Data and Goliath*, 2015

Narayanan's taxonomy

What happened to the Crypto Dream?
2013

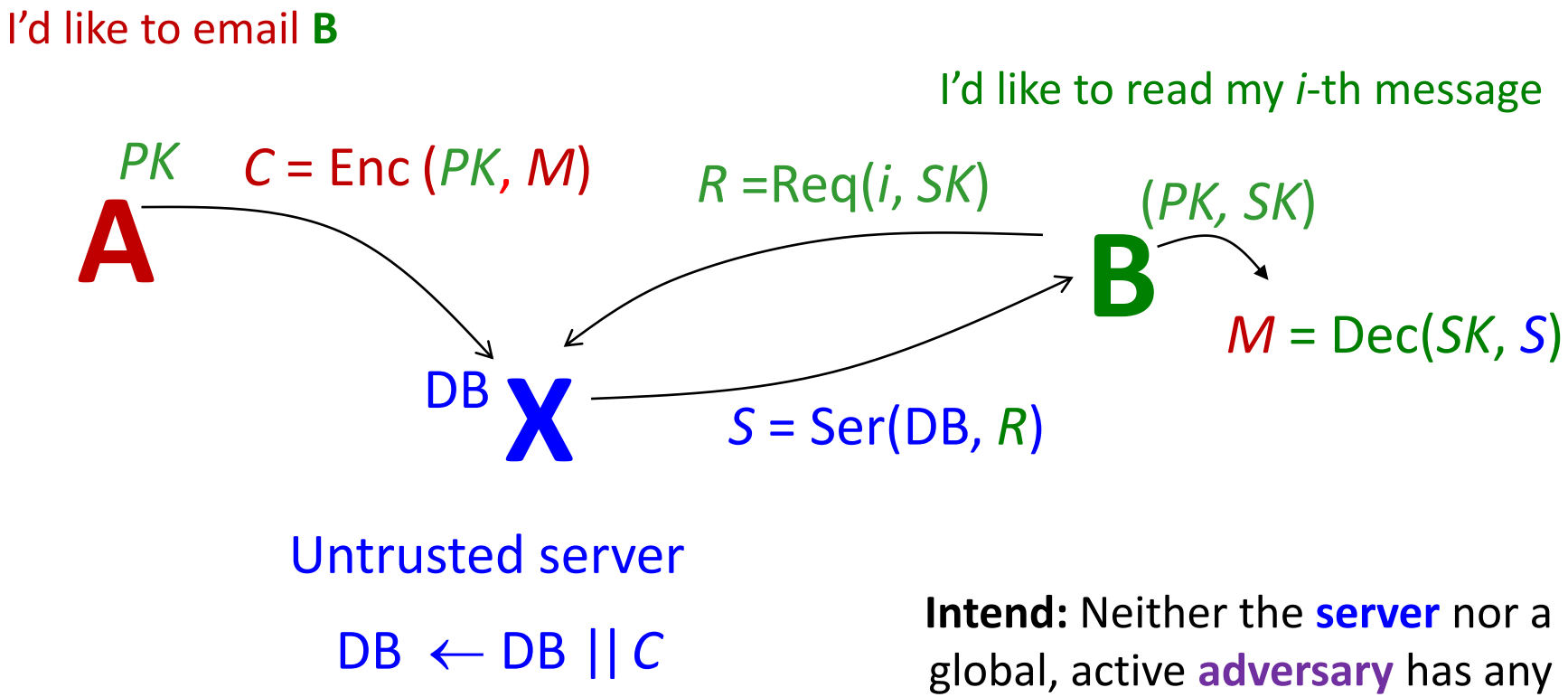
Arvind Narayanan
What happened to the Crypto Dream?
2013



The xMail problem

Secure Messaging Assisted by an Untrusted Server

Work in progress
inspired by
Adam Langley's
Pond

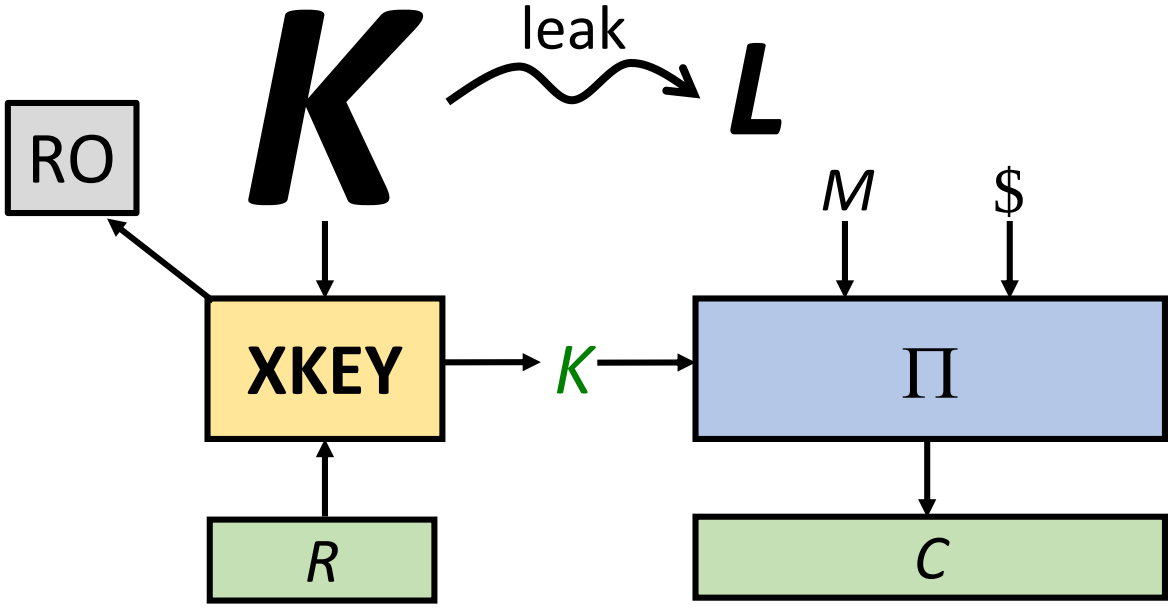


Intend: Neither the **server** nor a global, active **adversary** has any idea **who** sent **what** to **whom**

[Bellare, Kane, Rogaway]

Bigkey Cryptography

how we are going to protect computer systems assuming there are APTs inside already which cannot be detected? Is everything lost? I claim that not, … because the APT is basically going to have a very …narrow pipeline to the outside world. … I would like, for example, …the secret of the Coco-Cola company to be kept not in a tiny file of one kilobyte, …. I want that file to be a terabyte… *Adi Shamir, 2013*



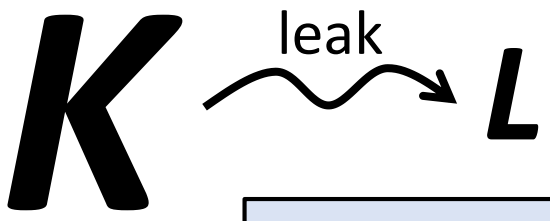
Security in the *bounded-retrieval model*. But we want

- Simple & generic tool
- Tight & explicit bounds
- ROM

[Bellare, Kane, Rogaway]

Bigkey Cryptography

Subkey prediction problem



1. Let the adversary learn some ℓ bits ***L*** about ***K***
2. Choose p random positions into ***K***, $i_1, \ldots, i_p \in [|\boldsymbol{K}|]$
3. Ask the adversary to predict the value of ***K*** at those positions: ***K***[1], …, ***K***[i_p].
4. What's the **best** it can do at getting everything right?

50% leakage: best adversary has advantage at most $\approx \mathbf{2}^{-\mathbf{0.168}\ p}$

$0.168 \approx -\lg(1-c)$ where $c \in [0,1/2]$ satisfies $H_2(c) = 0.5 = |\boldsymbol{L}| / |\boldsymbol{K}|$ with $H_2(x) = -x \lg x - (1-x)\lg(1-x)$ the binary entropy function

More examples of crypto-for-privacy

(beyond the obvious: mix nets, Tor, and bitcoin)

a. **Riposte** [Corrigan-Gibbs, Boneh, Mazières 2015] – *private broadcast*
b. **scrypt** [Percival 2009], [Alwen, Serbinenko 2015], **Argon5** [Biryukov, Dinu, Khovratovich 2015] – *memory-hard password-hashing*
c. **Algorithm substitution attacks** – [Bellare, Peterson, Rogaway 2014]
d. **Logjam attack** [Adrian et al.] – *Two-stage attacks on DH* **...**

...

First suggestions

1. Attend to problems' **social value**. Do **anti-surveillance research**.

2. Be **introspective** about **why** you're working on what you are.

Practice-oriented provable security for crypto-for-privacy

Mihir Bellare, Phil Rogaway

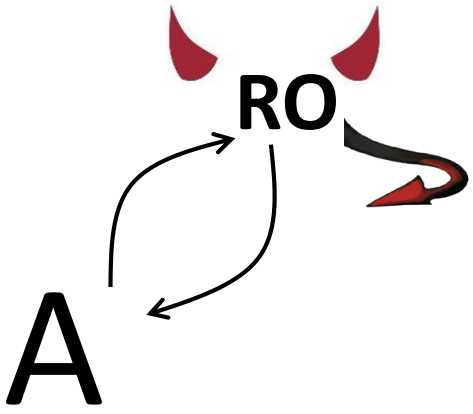
Historical, inessential aspects of **Provable Security**

a. Asymptotics favored
b. Aesthetically-construed minimalism
c. Symmetric primitives ignored
d. Nonconstructive language for stating results
e. EA, KD, and secure messaging ignored
f. Condemnatory attitude towards “non-standard” models

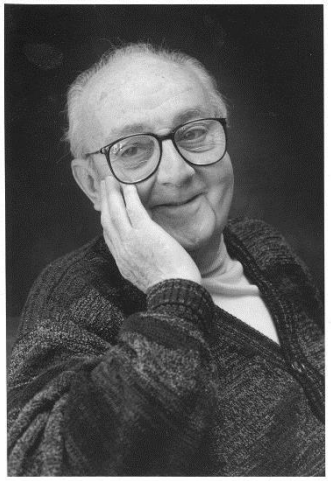
Provable Security

3. Apply **practice-oriented provable-security** to anti-surveillance problems.

Against Dogma



"All models **are wrong, but some are useful"**

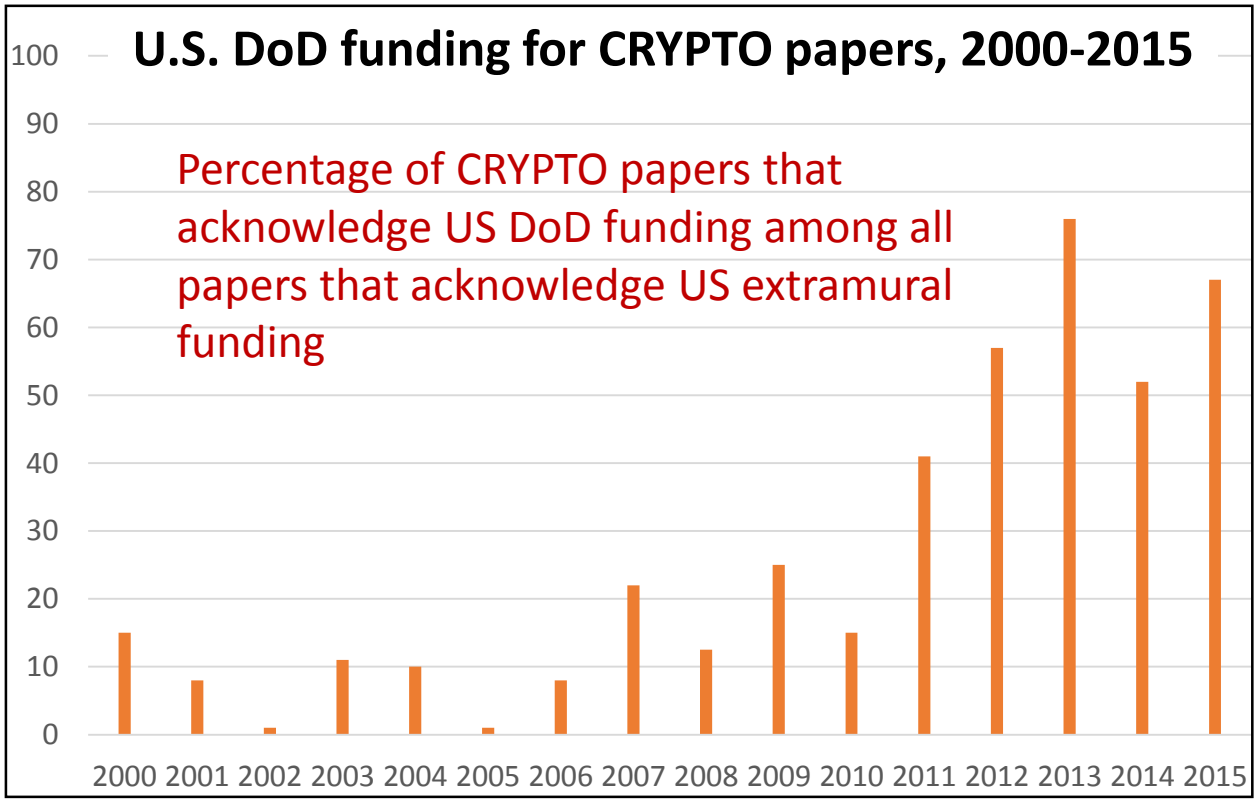


George Box
1919-2013

4. Be open to **diverse models**. Regard **all** models as suspect and dialectical.

Military Funding – 1

U.S. Perspective



Military Funding – 2

Changes our values. **Reflects** our values.

DARPA's Mission: "to invest in the breakthrough technologies that can create the next generation of [U.S.] national security capabilities."

"avoiding *technological surprise* — and creating it for America's enemies."

Military Funding – 3

NSA likes us doing work "which might affect cryptology at some [distant] future time or (more likely) in some other world."

"Three of the last four sessions were of no value whatever, and indeed there was almost nothing at Eurocrypt to interest us (*this is good news!*)"

"There were no proposals of cryptosystems, no novel cryptanalysis of old designs, even very little on hardware design. *I really don't see how things could have been better for our purposes*."

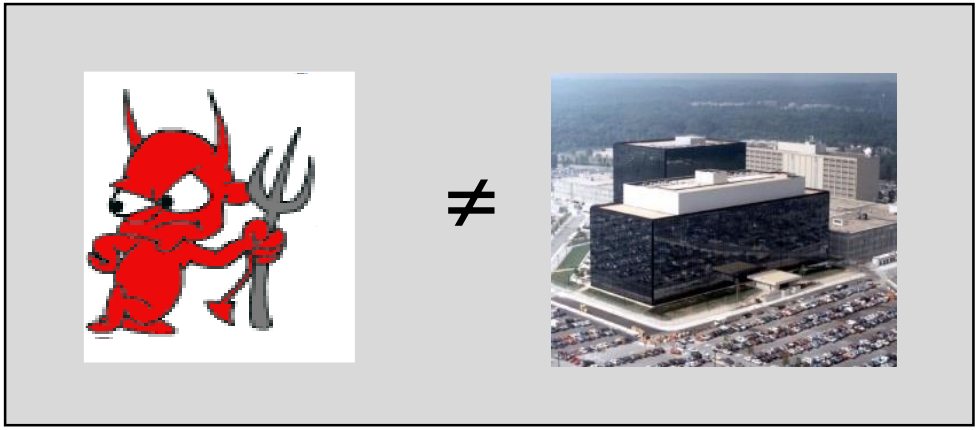
– *NSA CRYPTOLOG*: EUROCRYPT '92 Report

5. **Think twice** about accepting military funding.

6. Regard **ordinary people** as those whose needs you aim to satisfy.

Cute or Scary?

For most cryptographers,
adversaries are **notional**.
We **joke** about them.
We see crypto as a **game**.



7. Stop with the **cutesy pictures**. Take adversaries seriously.

8. Figure out what research would **frustrate the NSA**. Then do it.

More Suggestions

9. Use the **academic freedom** you have.

10. Get a **systems-level** view.

11. Learn some **privacy tools**. **Use** them. **Improve** them.

12. Design and build a broadly useful **cryptographic commons**.

Conclusions

“Truth is Coming and Cannot be Stopped” (2013)
Sarah Lynn Mayhew & D606
Street art in Manchester, UK

- We are twice culpable for the surveillance mess — as computer scientists and as cryptographers.
- A *genuine* dystopia.
- Not optimistic.
  But some reasons for hope.
- Like the cypherpunks, embed *values* in your work.
- *Just because you don’t take an interest in politics doesn’t mean politics won’t take an interest in you*. - Anonymous

Go to my homepage
http://web.cs.ucdavis.edu/~rogaway/
for the paper corresponding to this talk

Suggestions towards

Making cryptography more socially useful

1. Attend to problems' **social value**. Do **anti-surveillance research**.
2. Be **introspective** about **why** you're working on what you are.
3. Apply **practice-oriented provable-security** to anti-surveillance problems.
4. Be open to **diverse models**. Regard **all** models as suspect and dialectical.
5. Think **twice** about accepting military funding.
6. Regard **ordinary people** as those whose needs you aim to satisfy.
7. Stop with the **cutesy pictures**. Take adversaries seriously.
8. Figure out what research would **frustrate the NSA**. Then do it.
9. Use the **academic freedom** you have.
10. Get a **systems-level** view.
11. Learn some **privacy tools**. **Use** them. **Improve** them.
12. Design and build a broadly useful **cryptographic commons**.