Recent and Future Trends in Cryptography

CMSC 23200/33250, Winter 2021, Lecture 23

David Cash and Blase Ur

University of Chicago

A Sampling of Recent and Future Trends in Crypto

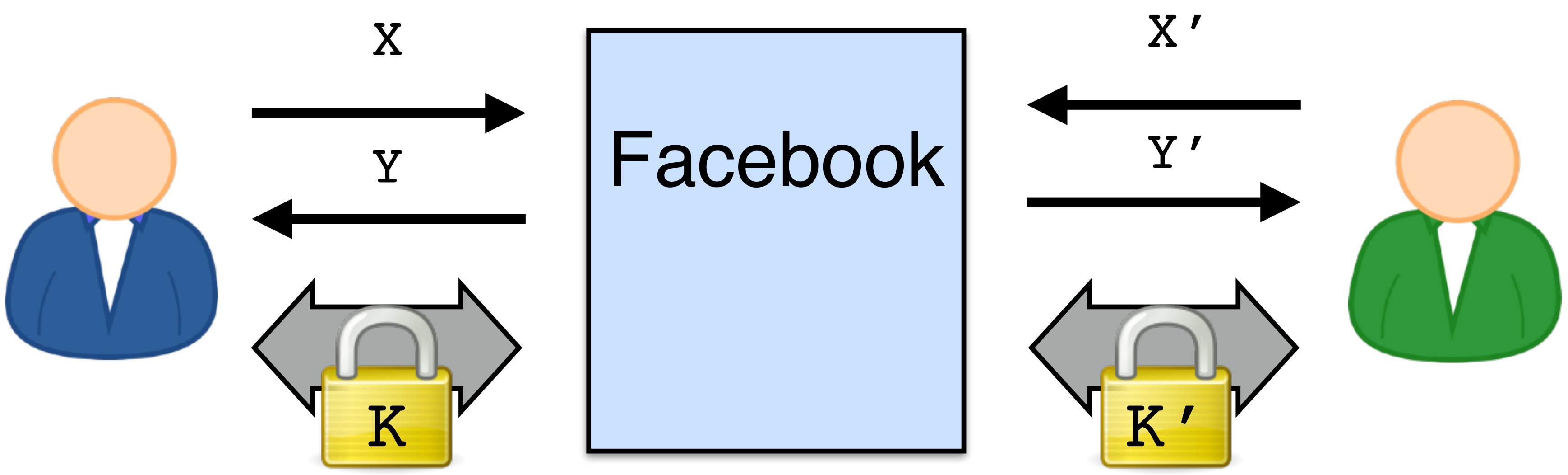
1. End-to-End Messaging
2. Snowden Revelations
3. Homomorphic Encryption (+Post Quantum)
4. Zero-Knowledge Proofs + Password-Authenticated Key Exchange
5. ORAM (Alex)

A Sampling of Recent and Future Trends in Crypto

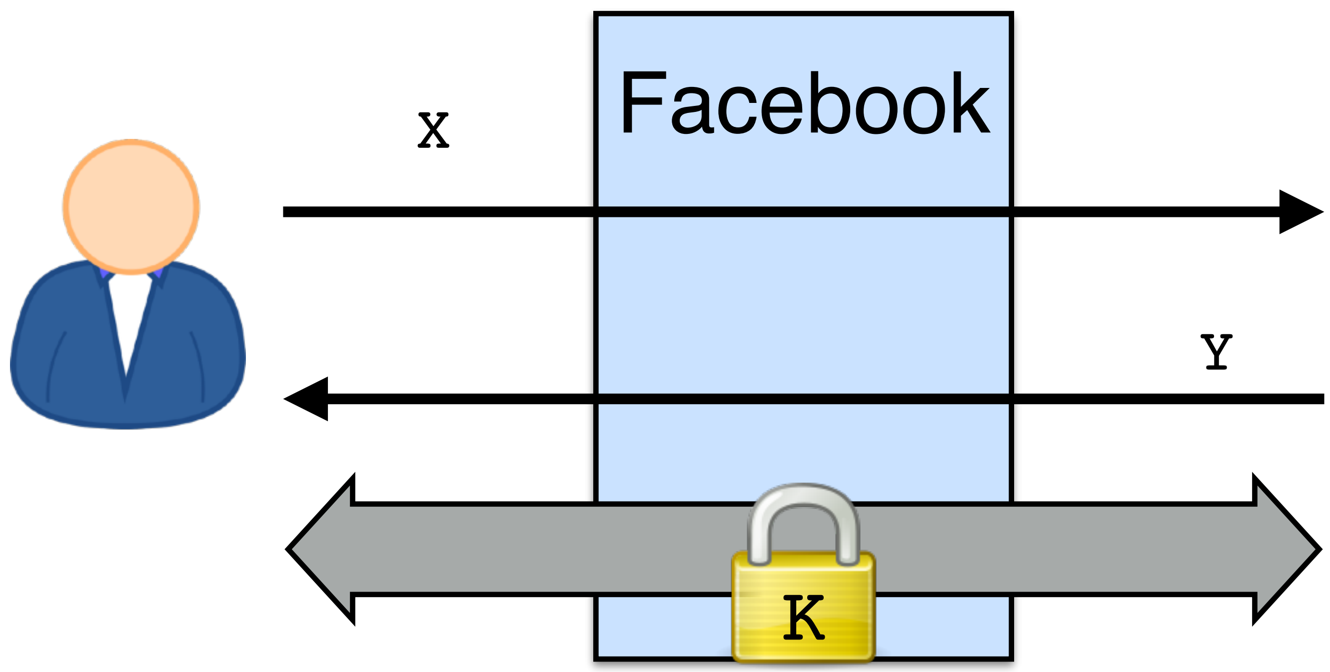
1. **End-to-End Messaging**
2. Snowden Revelations
3. Homomorphic Encryption (+Post Quantum)
4. Zero-Knowledge Proofs + Password-Authenticated Key Exchange
5. ORAM (Alex)


MIT Technology Review
Sign in
Subscribe
Topics
Magazine
Newsletters
Events
Computing / Cybersecurity
Barr's call for encryption backdoors has reawakened a years-old debate
Attorney General William Barr's speech on Tuesday reignited a dispute that's more relevant than ever.
by Patrick Howell O'Neill
Jul 24, 2019
SECURITY WATCH
US Attorney General William Barr Has Encryption All Wrong
Attorney General William Barr has a completely wrong-headed take on encryption, and he's not the only one. Adding backdoors to secure services is a terrible idea, despite its popularity with law enforcement.
By Max Eddy October 10, 2019

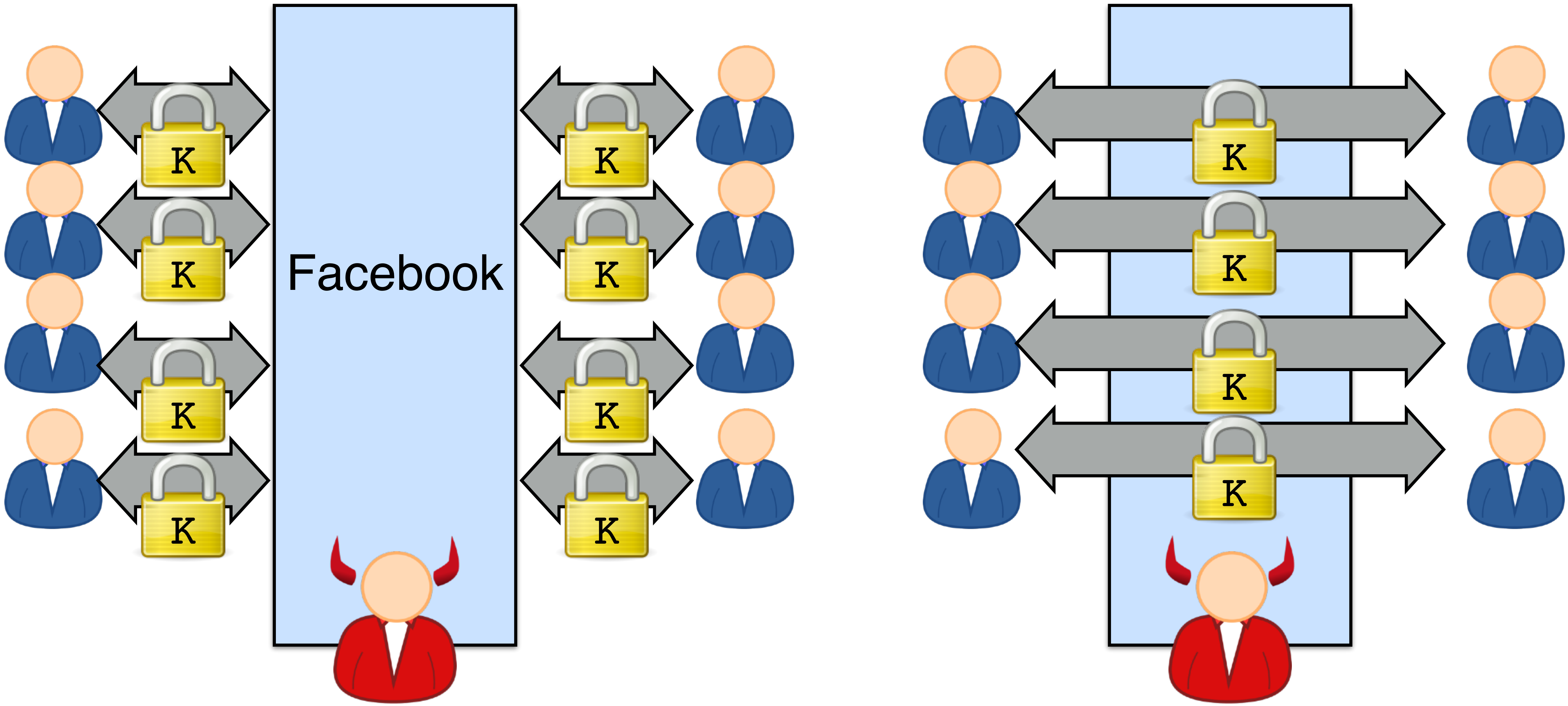
Traditional Diffie-Hellman Deployment (e.g. TLS)



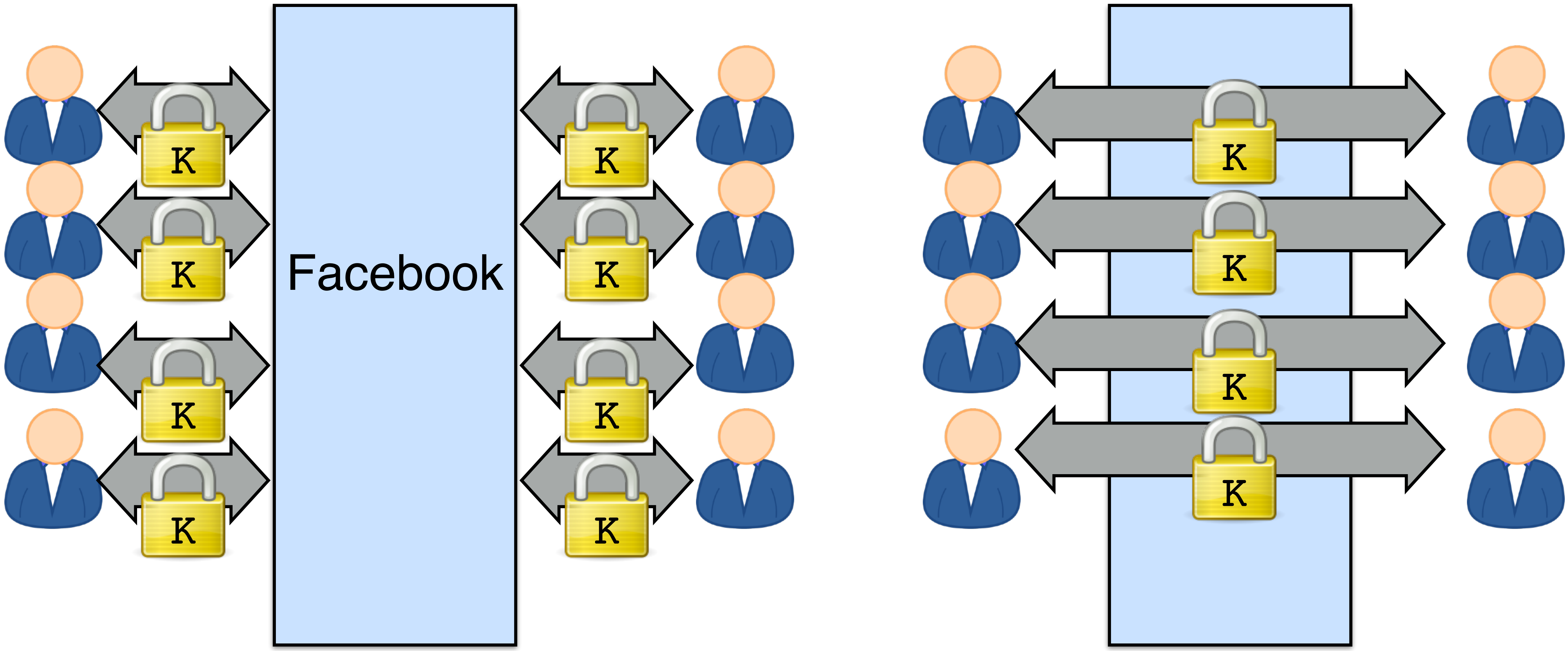
End-to-End Diffie-Hellman



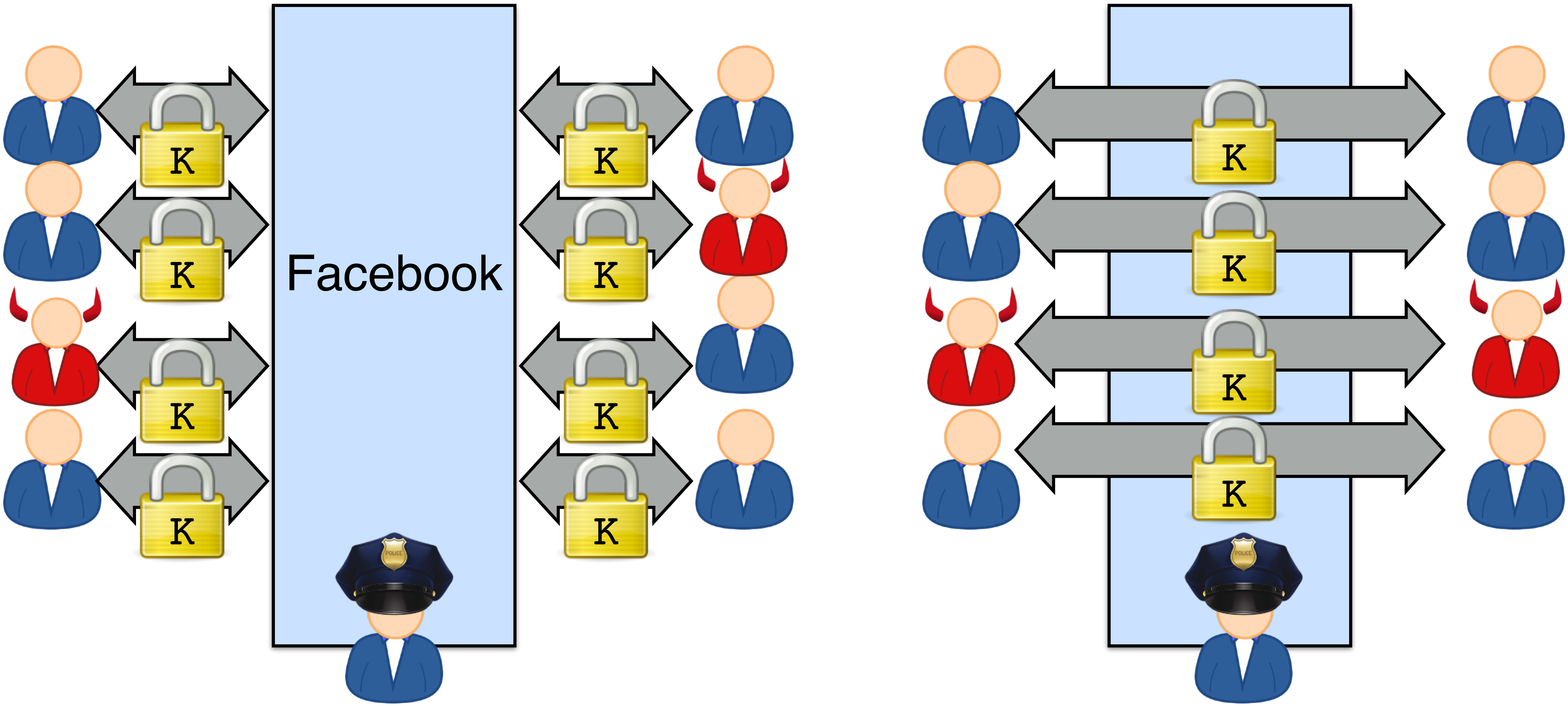
Why End-to-End?



Why *not* End-to-End?



Why *not* End-to-End?



A Sampling of Recent and Future Trends in Crypto

1. End-to-End Messaging

2. Snowden Revelations

3. Homomorphic Encryption (+Post Quantum)

4. Zero-Knowledge Proofs + Password-Authenticated Key Exchange

5. ORAM (Alex)

The Snowden Revelations

2013 Snowden Revelations Included:

1. Collected millions of images from Yahoo! messenger to build facial recognition system (2008-2010)

2. Recorded audio of *every* call in the Bahamas (2009-?)

3. Tapped internal lines for Google and Yahoo! data centers

4. Likely built a crypto backdoor into a NIST algorithm, then paid a company $10 million to use that algorithm

WIRED SUBSCRIBE

KIM ZETTER SECURITY 09.24.13 06:30 AM

How a Crypto 'Backdoor' Pitted the Tech World Against the NSA

ars TECHNICA

BIZ & IT —

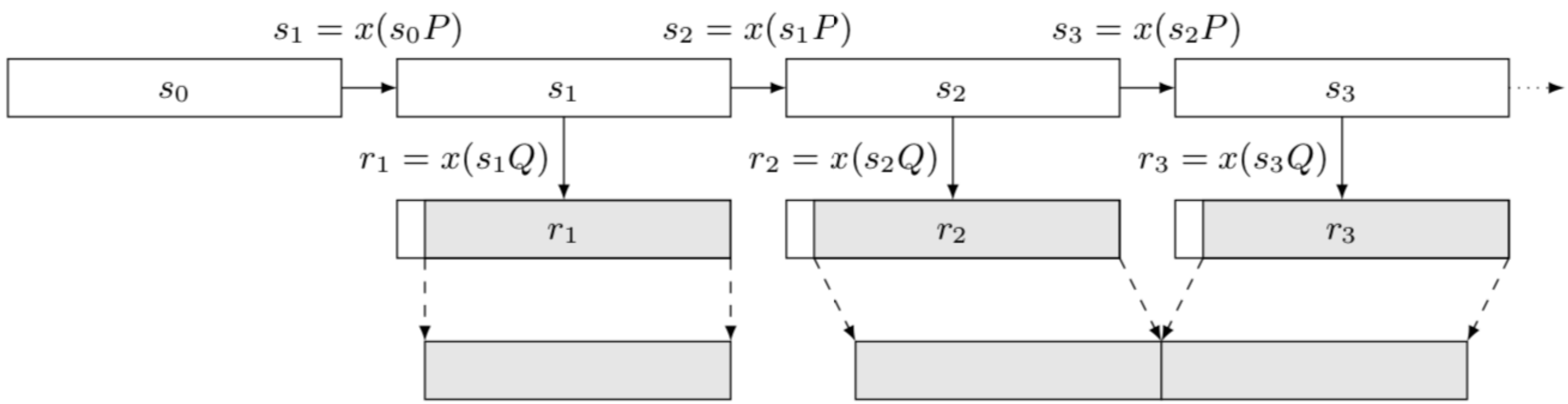
NSA official: Support of backdoored Dual_EC_DRBG was "regrettable"

Agency supported crypto function for years after "trap door" was disclosed.

DAN GOODIN - 1/14/2015, 12:43 PM

Dual_EC_DRBG: A Pseudorandom Generator

Pseudorandom generator: Algorithm for "stretching" a random string.



NIST

NIST Special Publication 800-90A

Recommendation for Random Number Generation Using Deterministic Random Bit Generators

Elaine Barker and John Kelsey

Computer Security Division
Information Technology Laboratory

From: John Kelsey [mailto:john.kelsey@nist.gov]
Sent: Wednesday, October 27, 2004 11:17 AM
To: Don Johnson
Subject: Minding our Ps and Qs in Dual_EC

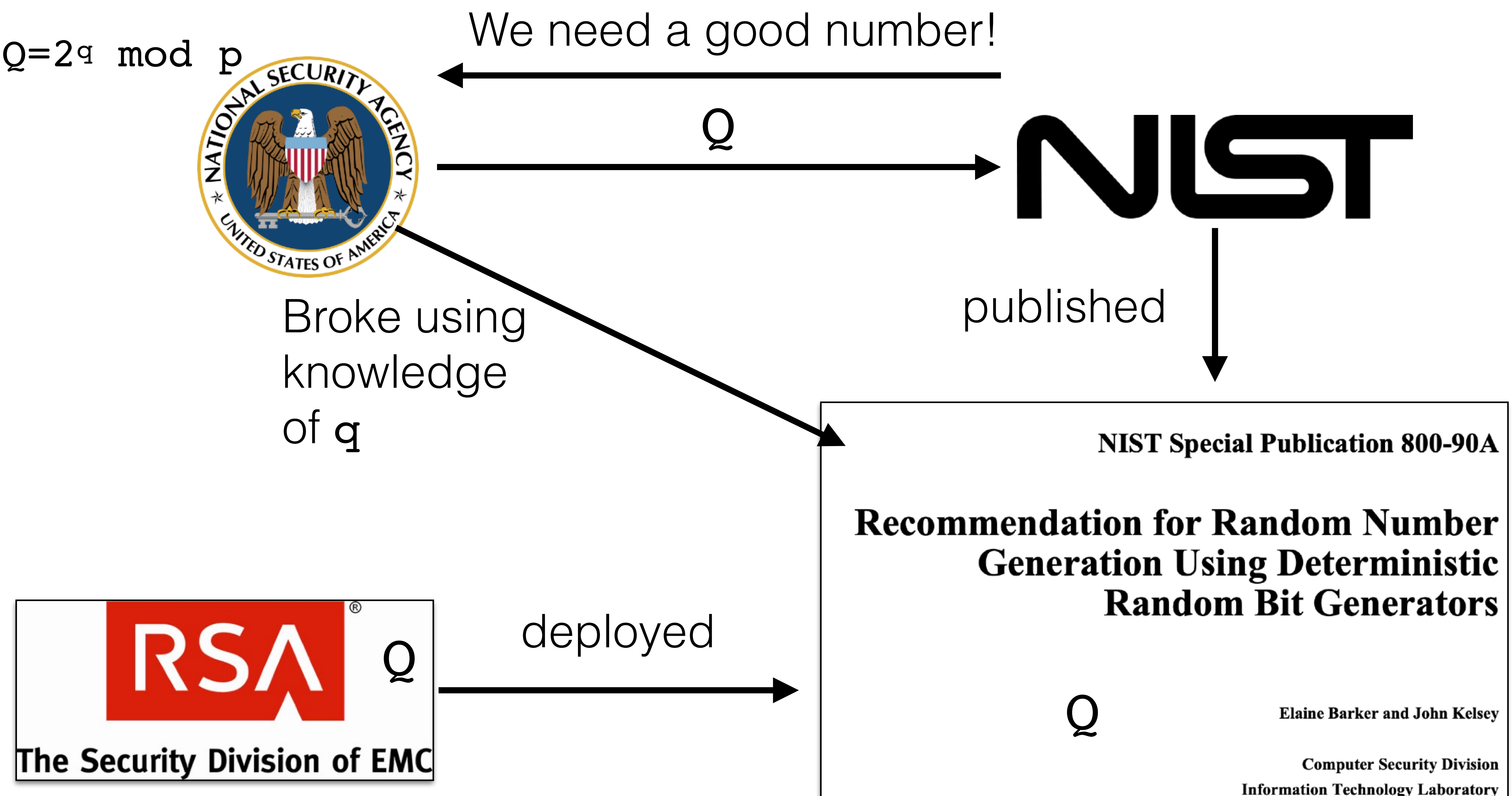
Do you know where Q comes from in Dual_EC_DRBG?

Thanks,

-John

```
Subject: RE: Minding our Ps and Qs in Dual_EC
From: "Don Johnson"
Date: Wed, October 27, 2004 11:42 am
To: "John Kelsey"

John,

P=G.
Q is (in essence) the public key for some
random private key.

It could also be generated like a(nother)
canonical G, but NSA kyboshed this idea, and I
was not allowed to publicly discuss it, just in
case you may think of going there.

Don B. Johnson
```

Dual_EC_DRBG Development Process*



*Actual math is over elliptic curves, and attack is complicated!

A Sampling of Recent and Future Trends in Crypto

1. End-to-End Messaging
2. Snowden Revelations
3. **Homomorphic Encryption (+Post Quantum)**
4. Zero-Knowledge Proofs + Password-Authenticated Key Exchange
5. ORAM (Alex)

Malleable Encryption

$C \leftarrow Enc(PK, M)$

C ⟶

C' ⟶

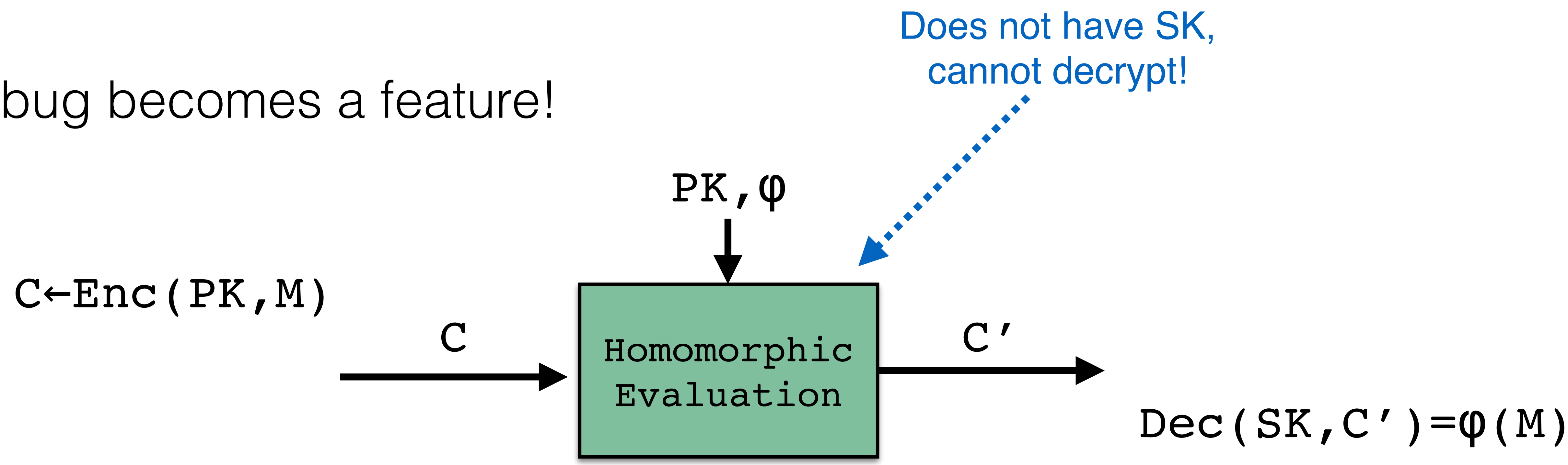
$Dec(SK, C' \bmod N) = M * x$

$C' \leftarrow [(x^e) * C \bmod N]$

- Malleability is usually a bad thing for Plain RSA Enc/Signatures
- Allows adversaries to predictably change plaintexts without permission, and without even knowing the original message

Homomorphic Encryption = Very Malleable Encryption

- A bug becomes a feature!



- RSA is homomorphic for multiplication by some fixed $\mathbf{x}$:

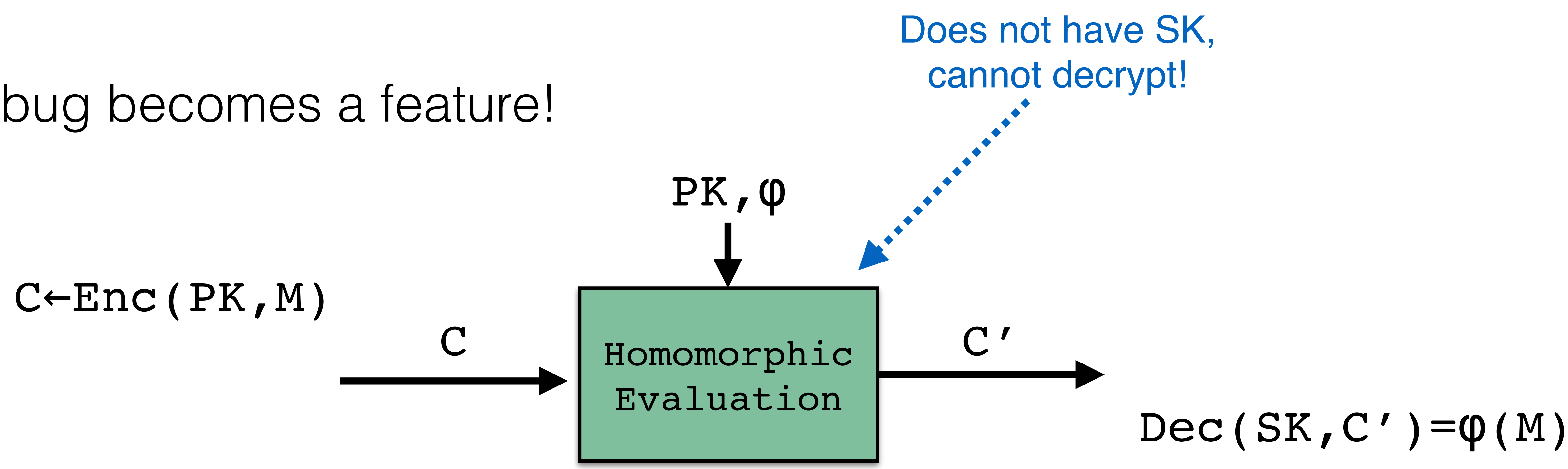
$$\varphi_x(M) = (x*M \bmod N)$$

- RSA does not appear to homomorphic for *addition* by some fixed $\mathbf{x}$:

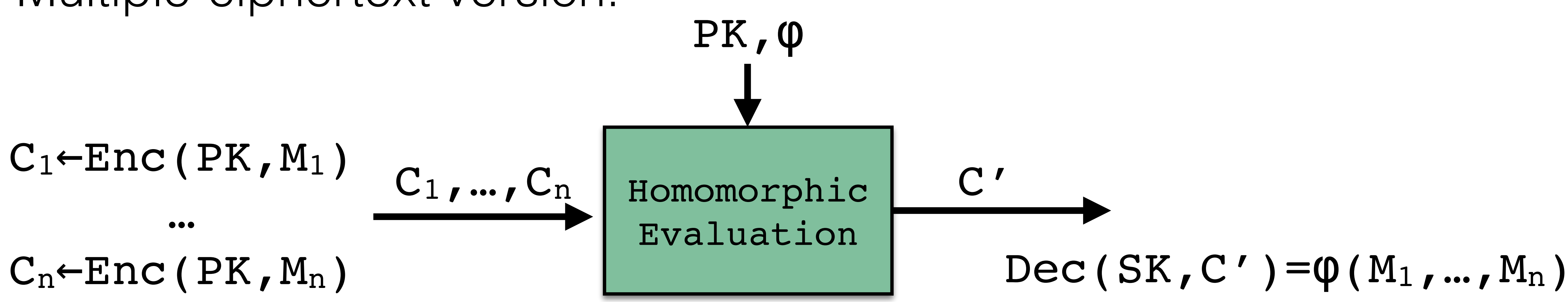
$$\varphi_x(M) = (x+M \bmod N)???$$

Homomorphic Encryption = Very Malleable Encryption

- A bug becomes a feature!



- Multiple-ciphertext version:



Homomorphic Encryption: The Grand Vision (1978)

ON DATA BANKS AND PRIVACY HOMOMORPHISMS

Ronald L. Rivest
Len Adleman
Michael L. Dertouzos

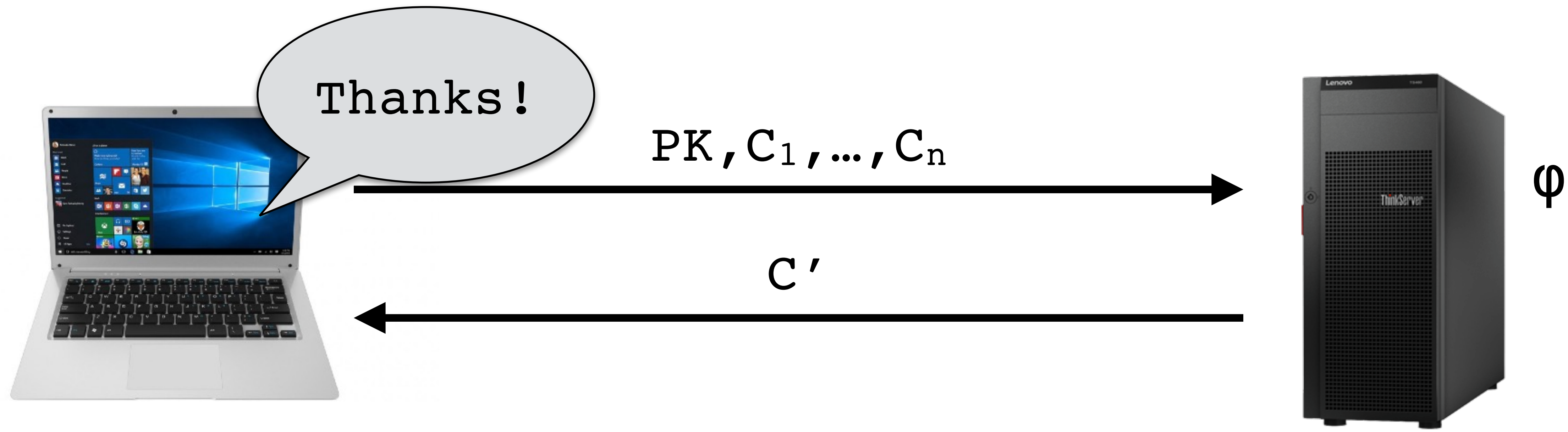
Massachusetts Institute of Technology
Cambridge, Massachusetts

I. INTRODUCTION

Encryption is a well-known technique for preserving the privacy of sensitive information. One of the basic, apparently inherent, limitations of this technique is that an information system working with encrypted data can at most store or retrieve the data for the user; any more complicated operations seem to require that the data be decrypted before being operated on.

Homomorphic Encryption: The Grand Vision (1978)

- Suppose **Enc** is homomorphic for φ using **HomEval**



$C_i \leftarrow \mathtt{Enc}(PK, M_i)$

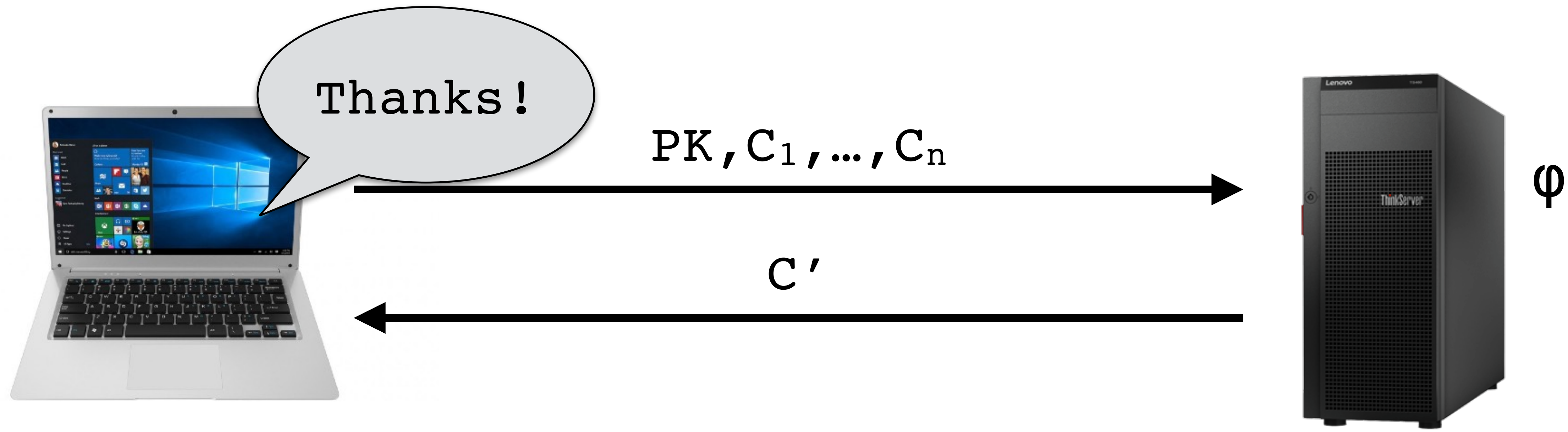
$C' \leftarrow \mathtt{HomEval}(PK, \varphi, C_1, \ldots, C_n)$

$\varphi(M_1, \ldots, M_n) \leftarrow \mathtt{Dec}(SK, C')$

- Client learns φ applied to its own data $M_1, \ldots, M_n$
- Client does not learn φ
- Server does not learn $M_1, \ldots, M_n$

Homomorphic Encryption: The Grand Vision (1978)

- Suppose **Enc** is homomorphic for φ using **HomEval**



$C_i \leftarrow \mathtt{Enc}(PK, M_i)$

…, C_n)

$\varphi(M_1,\ldots,M_n) \leftarrow \mathtt{Dec}(SK, C'$

- Train private machine-learning models
- Run expensive simulations
- Query databases without decrypting

- Client learns φ applie
- Client does not learn
- Server does not learn $M_1,\ldots,M_n$

For which φ can we build homomorphic encryption?

- RSA ('78): **φ** = multiplication mod N of plaintexts and/or constants
- Paillier ('99): **φ** = *addition mod N* of plaintexts and/or constants
- …

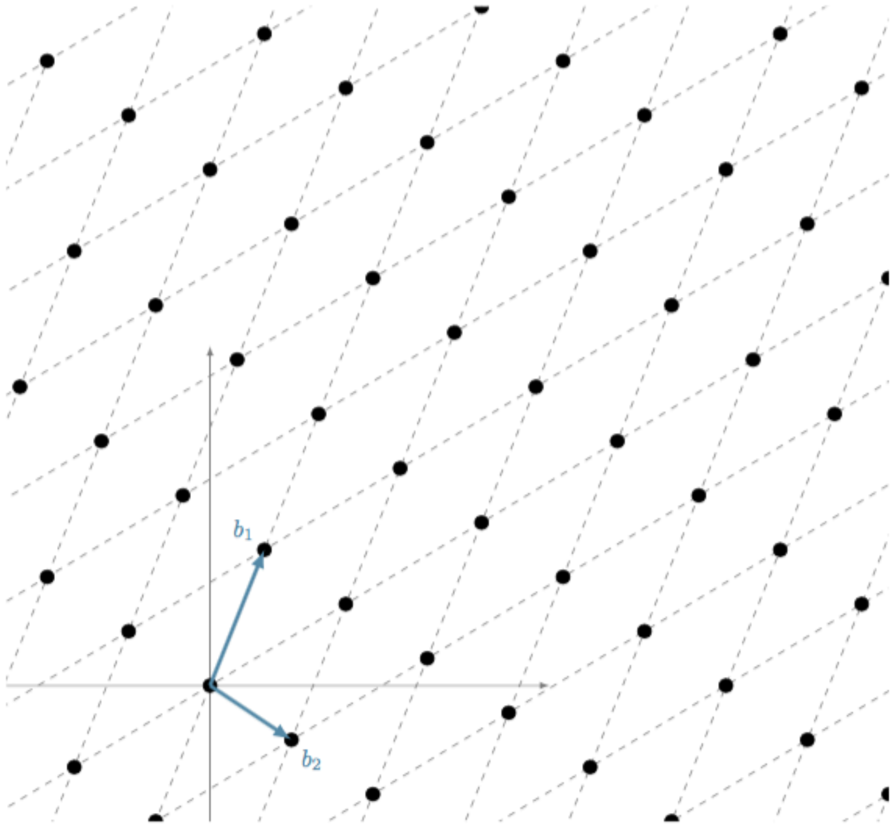
> **Observation**: If an encryption is homomorphic for both additions and multiplications mod N, then it is homomorphic for any **φ**!

- BGN ('06): **φ** = many additions but only one multiplication
- …
- Gentry ('09): Any **φ**! Via new techniques.

Homomorphic Encryption and Lattices (Gentry'09)

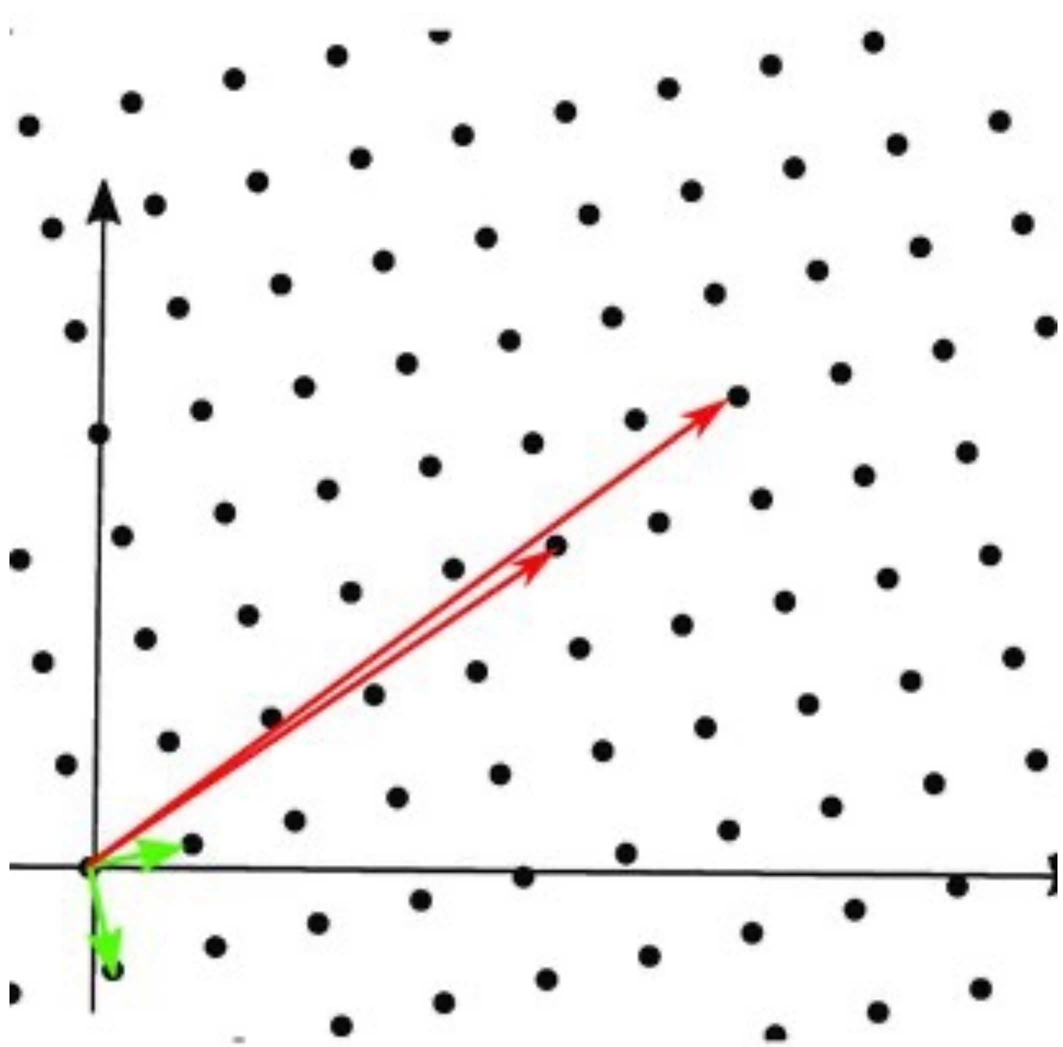
- Based on different math (not RSA/Diffie-Hellman)
- Uses *lattices*, i.e. high-dimension integer grids

- Original construction was too slow
- Tons of research on making it faster



Underlying Hard Problem: Shortest Vector Problem

Input: An n-by-m integer matrix **B** (m<n)
Output: The smallest non-zero **y** such that **Bx**=**y** for some integer **x**.

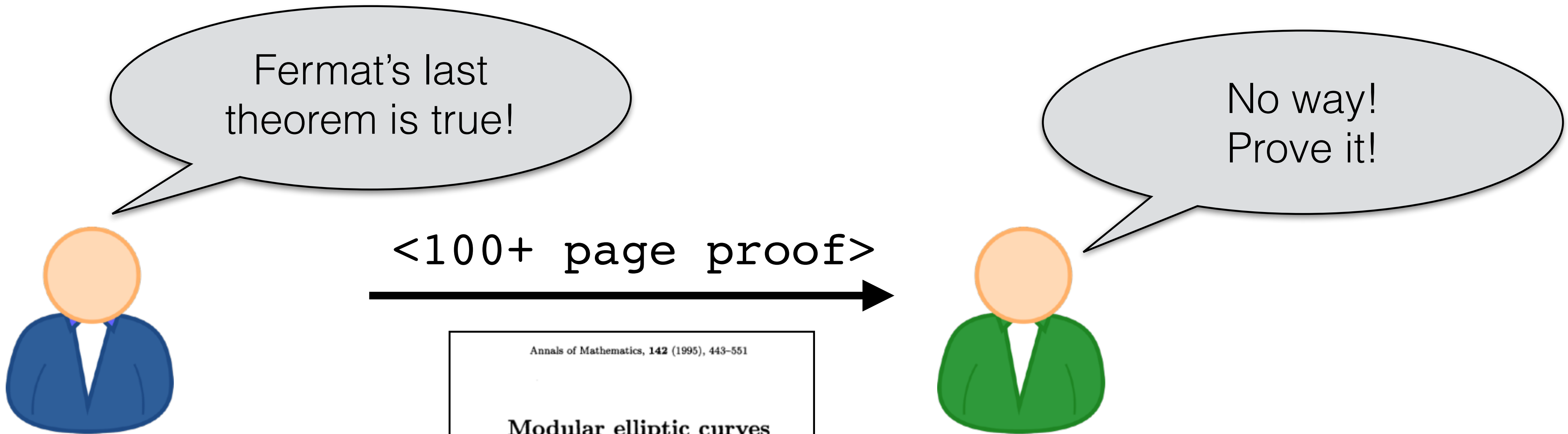


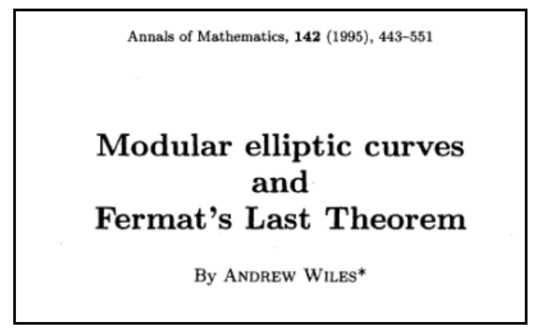
- Easy for small n
- Appears hard for large n…
- Even for quantum computers!

A Sampling of Recent and Future Trends in Crypto

1. End-to-End Messaging
2. Snowden Revelations
3. Homomorphic Encryption (+Post Quantum)
4. **Zero-Knowledge Proofs + Password-Authenticated Key Exchange**
5. ORAM (Alex)

Switching gears: Mathematical Proofs

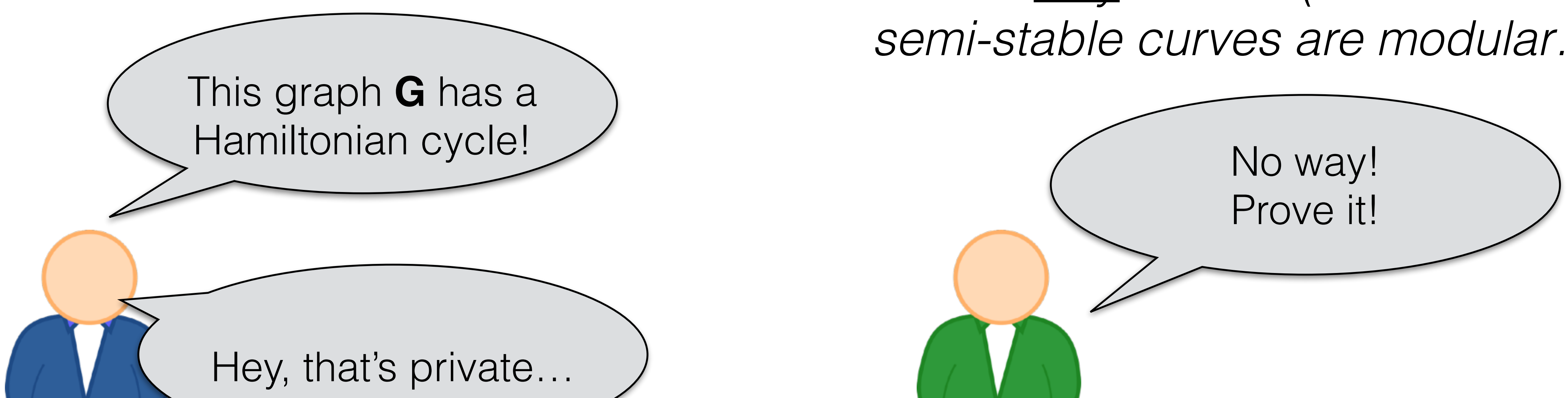



Annals of Mathematics, **142** (1995), 443–551

Modular elliptic curves and Fermat's Last Theorem

By Andrew Wiles*

- Convinced theorem is true
- Learns <u>*why*</u> *it's true (i.e. because all semi-stable curves are modular…)*

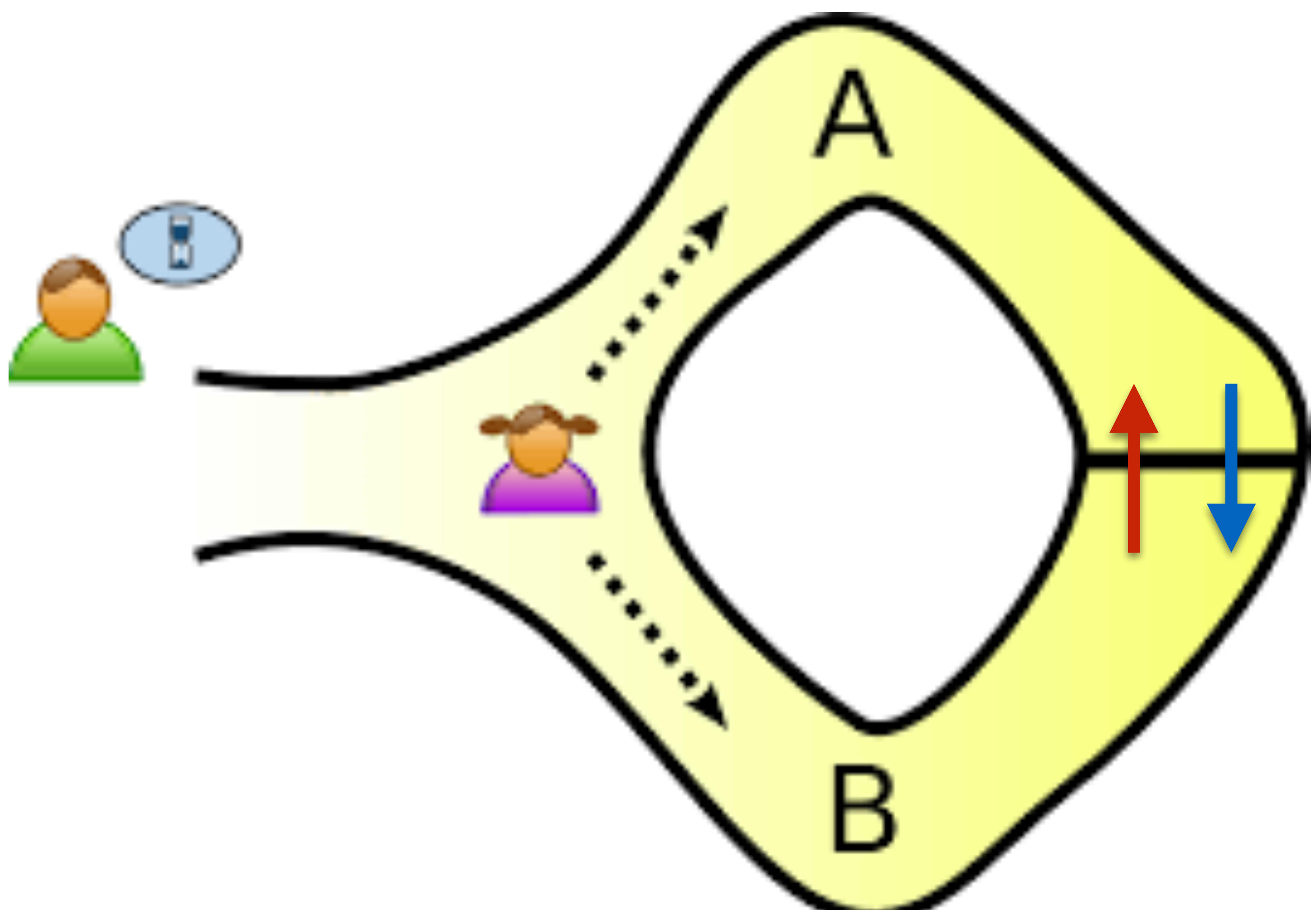


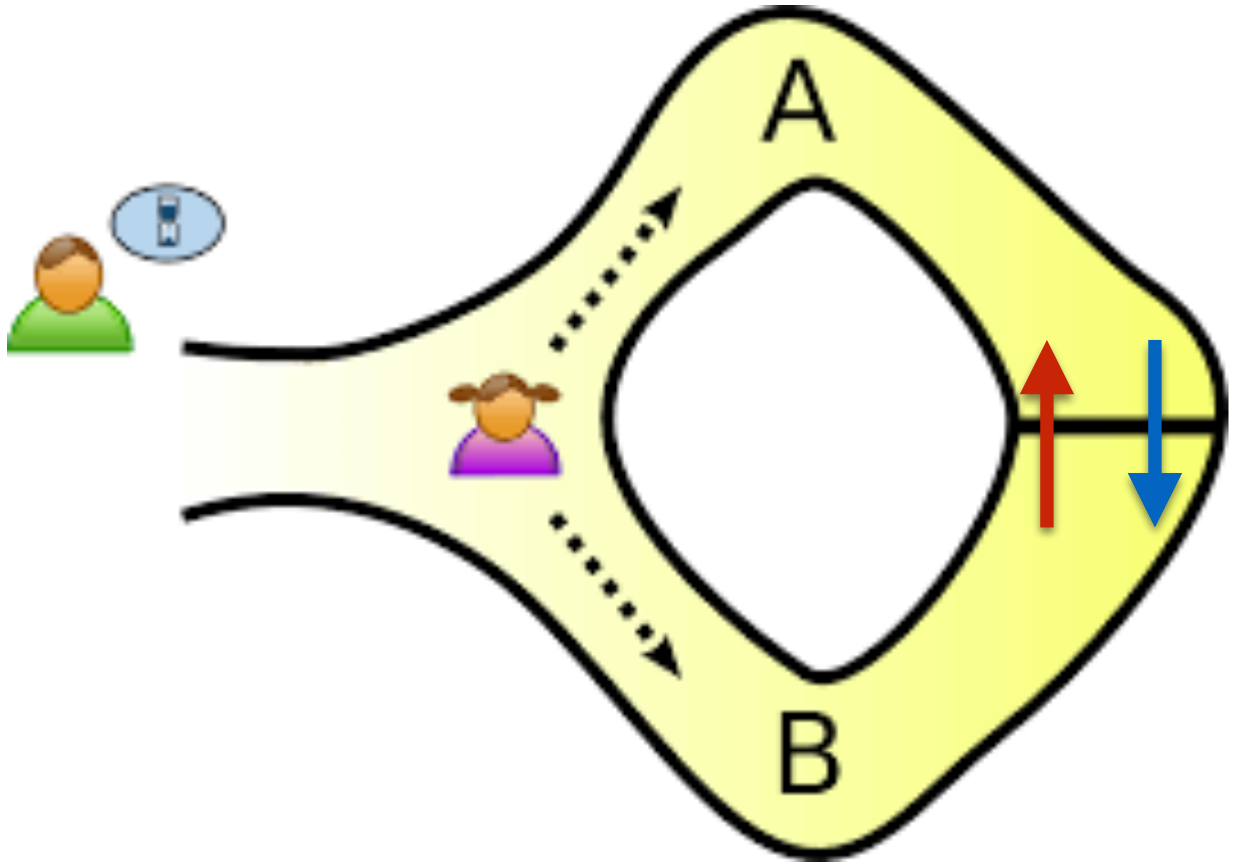
<u>Question</u>: Can one prove something is true…
…without revealing anything about why?

Zero-Knowledge Proofs (Goldwasser,Micali,Rackoff'85)



- Prover claims: There is a one-way door that opens between A and B
- Wants to hide: Which direction the door opens (A→B vs B→A)





Protocol:

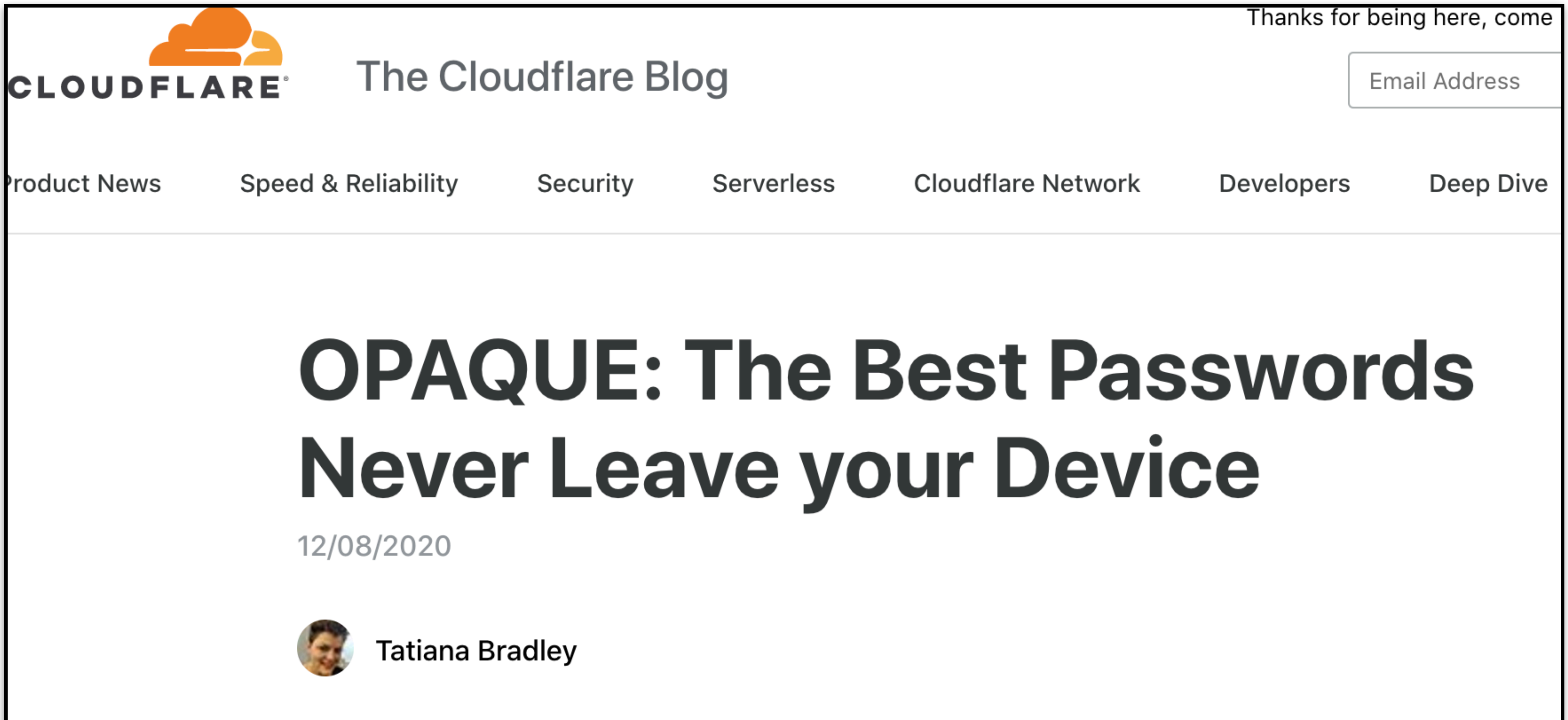
1. Prover walks into cave without Verifier watching
2. Verifier flips a coin and asks Prover to come out A or B side
3. Prove comes out that side, using door if necessary
4. Repeat 100 times. If prover is ever caught lying, **REJECT**.

Soundness: If there is (in fact) no door, then Prover only has $1/2^{100}$ chance to cheat.

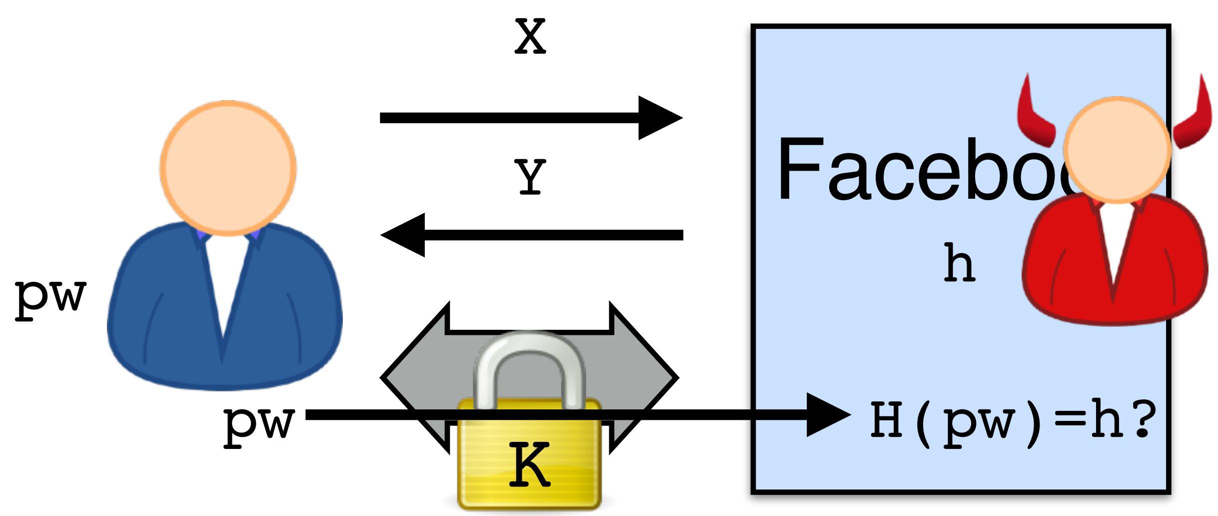
Zero-knowledge: Even if Verifier tries to cheat, it won't learn anything about which way the door opens.

- Key insights:
  - Interaction
  - Randomness

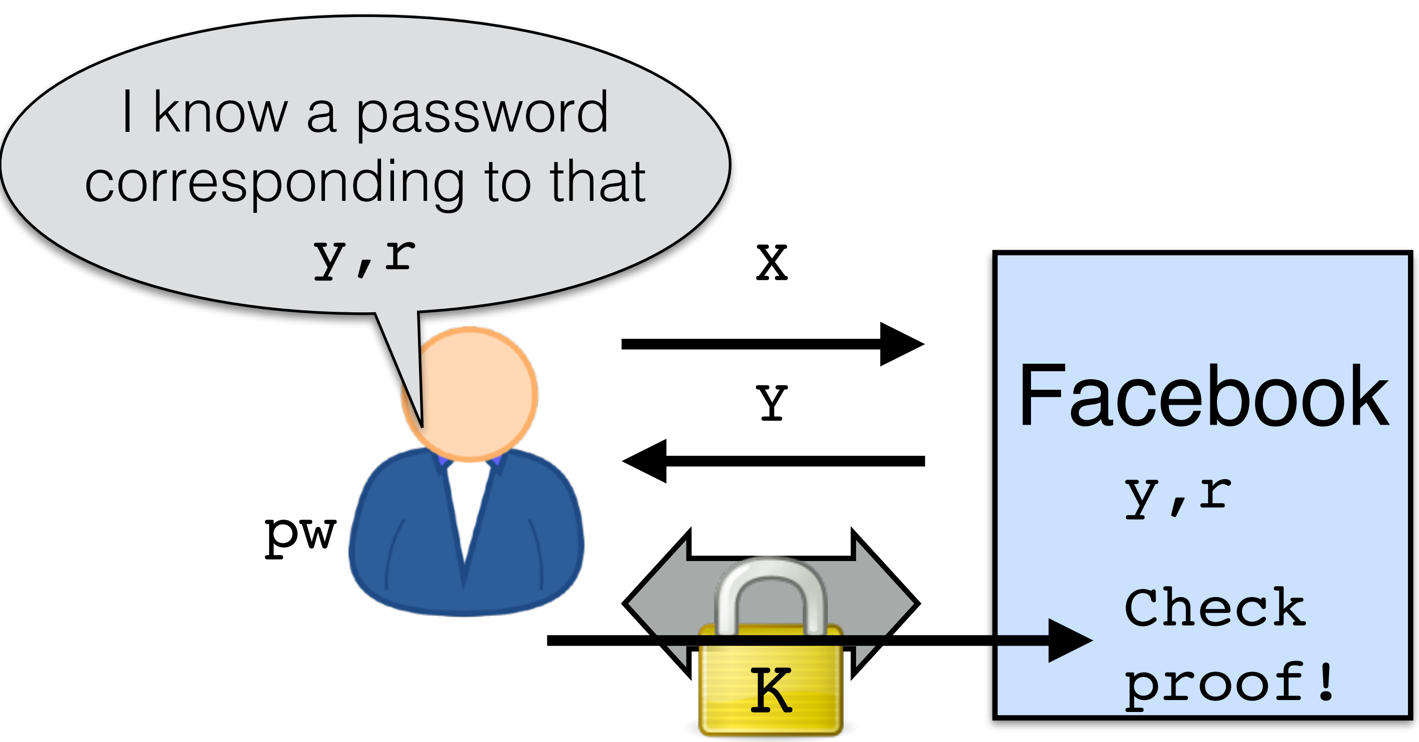
Application: Password-Authenticated Key Exchange



Application: Password-Authenticated Key Exchange



- Hash stored at FB.
- Compromise at server allows stealing pw, even if very strong



- pw never sent to FB, even at registration
- Compromise at server won't allow stealing pw (assuming it is strong)

What are the downsides, if any?

A Sampling of Recent and Future Trends in Crypto

1. End-to-End Messaging
2. Snowden Revelations
3. Homomorphic Encryption (+Post Quantum)
4. Zero-Knowledge Proofs + Password-Authenticated Key Exchange
5. **ORAM** (Alex)

The End