Modern Crypto

15 Years of Advancement in Cryptography

Steve Weis

saweis.net

8.10.15 v1

90s were a good time for crypto

- T-shirts were once munitions…
- Lots of new libraries, primitives, protocols, theory…
- Crypto War I: US export controls are relaxed
- Dotcom boom: Web browsers bring crypto to everyone.

What have cryptographers been doing since 2000?

Major Themes of 2000-2015

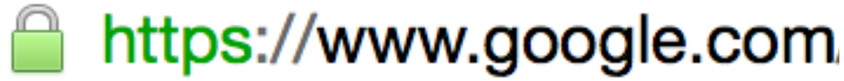
Outline of today's talk:

1. Crypto becomes ubiquitous
2. Breaks in 90s primitives & protocols
3. Modern standards mature and new standard emerge
4. Ciphertext becomes usable in surprising ways

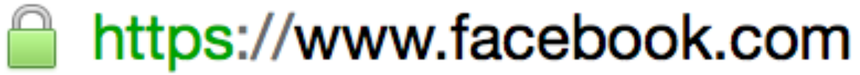
Crypto becomes ubiquitous

HTTPS by Default

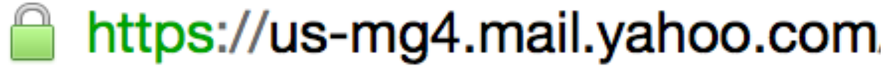
- 2008: Gmail option to always enable HTTPS



- 2010: Gmail defaults to HTTPS
  EFF/Tor Project HTTPS Everywhere
- 2013: Facebook defaults to HTTPS



- 2014: Yahoo Mail uses HTTPS by default



- 2015: “Let’s Encrypt” free CA scheduled

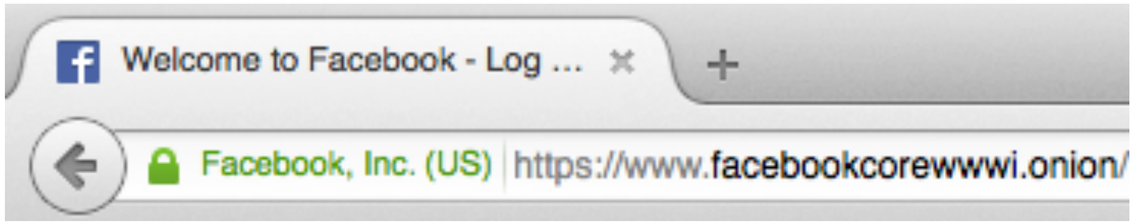
E2E Encrypted Everywhere

- 2003: Encrypted Enterprise AIM
- 2004: Off-the-Record protocol published
- 2010: TextSecure released
- 2013: Axolotl key ratcheting
  iMessage encryption*
- 2014: Signal released

Mainstream Disk Encryption

- 2003: FileVault to encrypt home directories
- 2004: BitLocker full disk encryption
- 2004: Truecrypt released
- 2011: FileVault 2 with full disk encryption
- 2014: iOS & Android disk encryption
  Truecrypt suddenly ceases development

Tor for Cat Photos



- 2002: Tor pre-alpha released
- 2004: Tor paper published
  Tor Hidden Services deployed
- 2006: Tor project launched
- 2008: Tor Browser released
- 2012: NSA “Tor Stinks” presentation
- 2014: wwwfacebookcorewwwi.onion

Image courtesy of Headline Shirts
http://www.headlineshirts.net/

- **2008: Bitcoin paper published**
- **2009: Bitcoin block 0**
- **2011: Silk Road: Tor HS + Bitcoin**
- **2013: Bitcoin price peak**
  Silk Road busted
- **2014: Random Darknet Shopper**
- **2015: Bitcoin ETF**

The Breaks

Fall of the Hash Functions

- 2004: Xiaoyun Wang announces MD5 collisions at Crypto Rump Session
- 2005: SHA-1 weakened
- 2008: Researchers forge rogue CA certificates using MD5
- 2013: Flame malware forges Microsoft certificates using MD5 vulnerabilities

Xiaoyun Wang


RC4
1987-2013

Unknown Pleasures of RC4

- 2001: Mantin & Shamir discover biases in RC4
- 2002: Biases used to attack WEP
- 2013: Plaintext recovery attack against TLS
- 2015: Cloudflare disables RC4
- 2015: 75 hours to recover cookies over HTTPS

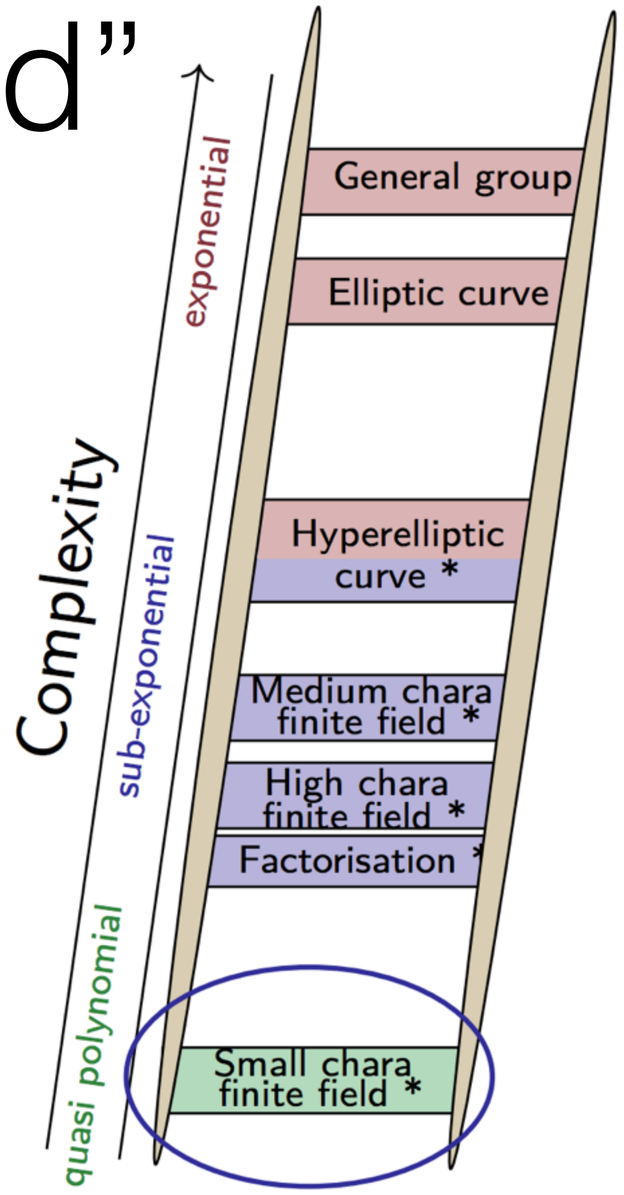
Images courtesy of Tony Arcieri:
https://github.com/tarcieri/unknownciphers

Rise of the Branded Vulnerability

- 2011: BEAST exploits CBC vulnerability in TLS 1.0
- 2012: CRIME
- 2013: BREACH
  Lucky 13
- 2014: Heartbleed
  POODLE padding oracle attack finally kills SSL 3.0

“The Factoring Dead”

- 2013: Multiple advancements in solving the discrete log problem, especially Antoine Joux.
- Algorithm is for small characteristic finite fields.
- Improvements could weaken Diffe-Hellman, DSA, ElGamal, & potentially RSA.
- NSA Suite B doesn’t mention factoring-based keys



US & WORLD NATIONAL SECURITY

NSA paid $10 million to put its backdoor in RSA encryption, according to Reuters report

By Russell Brandom on December 20, 2013 04:54 pm *Email* *@russellbrandom*

- 2004: RSA was allegedly paid $10M to include Dual_EC_DRBG in BSafe product
- 2005: Certicom files patent for backdoor
- 2006: NIST standardizes Dual_EC_DRBG
- 2007: Researchers suspect backdoor
- 2013: Snowden leak reveals alleged payments to RSA

---------- Original Message ----------
Subject: RE: Minding our Ps and Qs in Dual_EC
From: "Don Johnson" <DJohnson@cygnacom.com>
Date: Wed, October 27, 2004 11:42 am
To: "John Kelsey" <john.kelsey@nist.gov>

John,

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

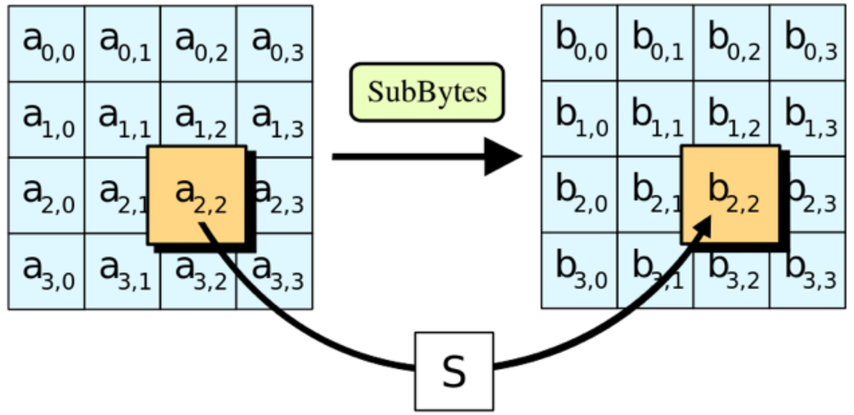
It could also be generated like a(nother) canonical G, but NSA kyboshed this idea, and I was not allowed to publicly discuss it, just in case you may think of going there.

Don B. Johnson


The
MODERN
STANDARDS

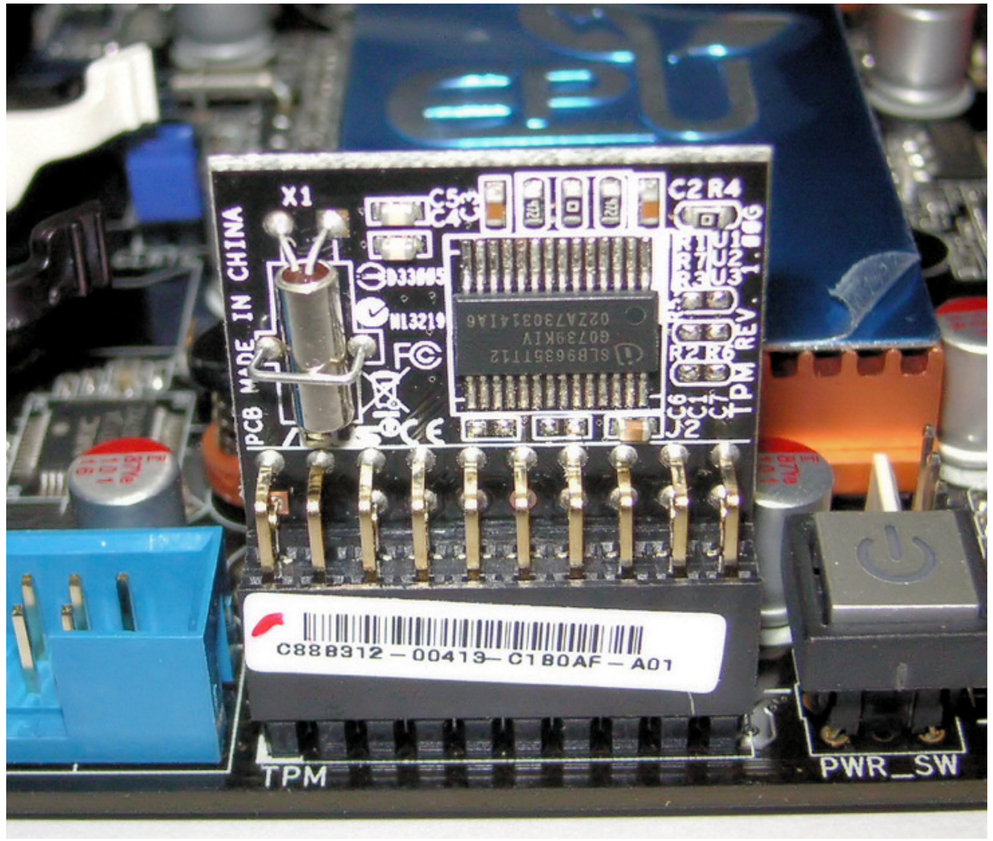
Block Ciphers Grow Up

- 2000: Rijndael wins AES competition
- 2005: AES cache side-channel attacks
  GCM mode published
- 2008: GCM included in NSA Suite B
- 2010: Intel releases AES-NI
- 2011: Intel adds PCLMULQDQ



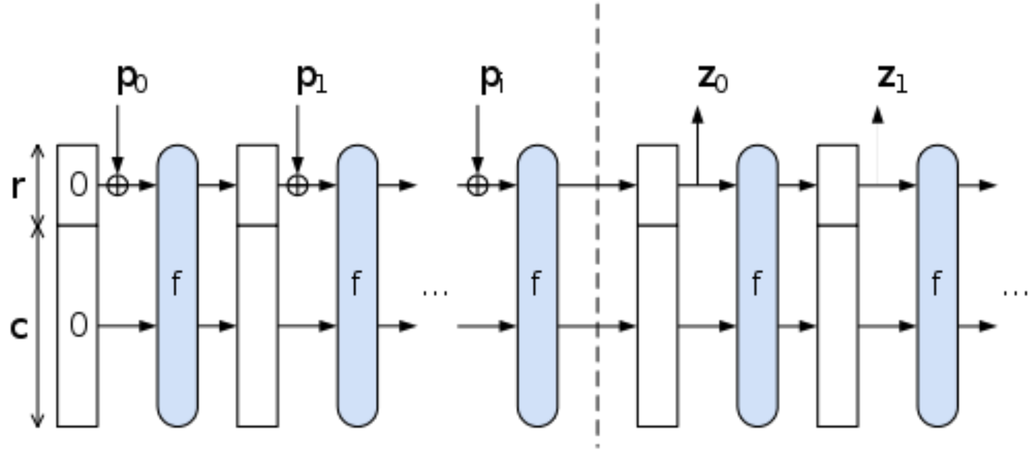
My CPU encrypts AES-GCM at **305 Gbit/s**

Trusted Hardware



- 2001: IBM ships TPM 1.1
- 2003: ARM TrustZone
- 2004: TPM 1.2 released
- 2013: Intel SGX

Better & Faster Hash Functions



- 2007: NIST announces SHA-3 competition
- 2007: Sponge functions published
- 2012: Keccak wins SHA-3 competition
- 2013: Intel SHA Extensions

Password Hashing Competition

- 1999: bcrypt password hashing
- 2009: scrypt password hash published
- 2014: Password Hashing Competition announced
- 2015: Argon2 wins Password Hashing Competition

djb & Friends Replace NIST

- 2005: Curve25519 elliptic curve
  Poly1305 MAC
- 2008: Chacha20 stream cipher
- 2011: NaCL library
- 2013: libsodium portable NaCL library
- 2014: Google supports Chacha20-Poly1305
- 2015: Openssh defaults to Chacha20-Poly1305

Dan Bernstein

Tanja Lange

Post-Quantum Crypto

- What if a large quantum computer is built?
- Broken: RSA, ElGamal, Diffie-Hellman, ECC, etc.
- Survivors: Lattices, multivariate, coding, hash-based, and symmetric crypto
- 2006-2015: PQCrypto.org workshop focused on developing software and standards

Peter Shor

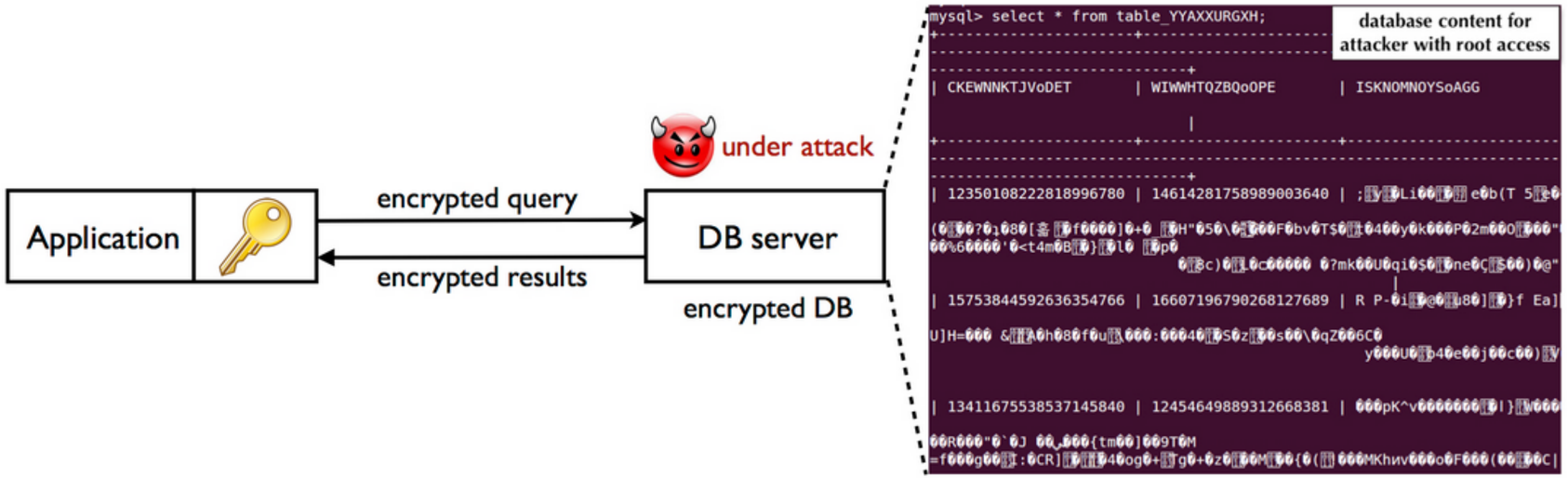
Ciphertext Becomes Usable

The Big Picture

Today: Cryptography allows us to use untrusted networks & untrusted storage.

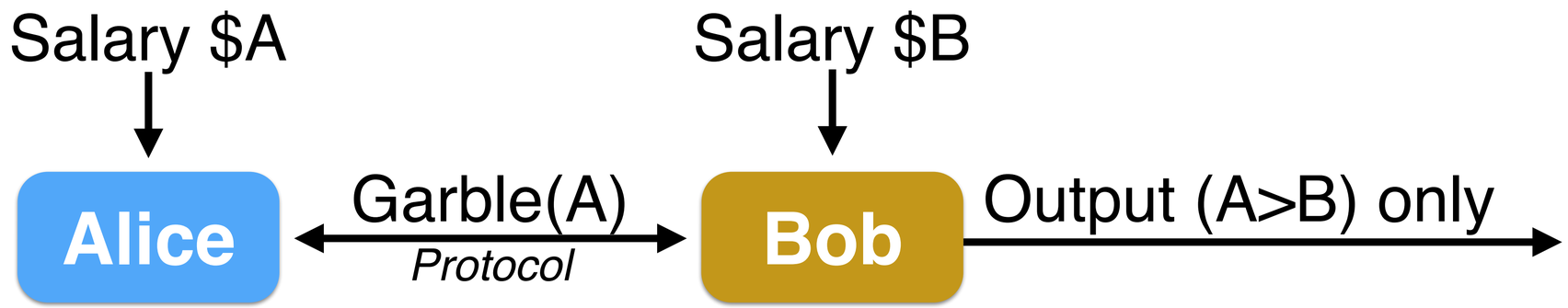
Tomorrow: Cryptography will allow us to use untrusted computation.

Searchable Encryption



- 2000: Search on encrypted data
- 2007: Order-preserving encryption
- 2009: Order-preserving symmetric encryption
- 2011: CryptDB released
- 2013: Google releases Encrypted Big Query client support

Practical Secure Multiparty Computation



- 1982: Yao introduces “secure 2-party computation”
- 2008-2013: Performance & security improvements
- 2013: Dyadic Security founded
- Need to re-garble for each computation

Bilinear Pairings & Maps

A bilinear map $e(\cdot, \cdot)$ takes a pair of inputs and map it to a single output with a useful property:

$$\mathbf{e(g^a, g^b) = e(g, g)^{ab}}$$

Identity Based Encryption

Traditional:

Directory(“Steve”) —> Public Key: “mQINBFUQW0..”

Encrypt(“mQINBFUQW0..”, message) —> ciphertext

IBE:

Encrypt(“Steve”, message) —> ciphertext

MasterKeyServer(“Steve”) —> Decryption Key

2001: Boneh & Franklin, Identity-Based Encryption

2002-2015: Voltage Security (acquired by HP)

Dan Boneh

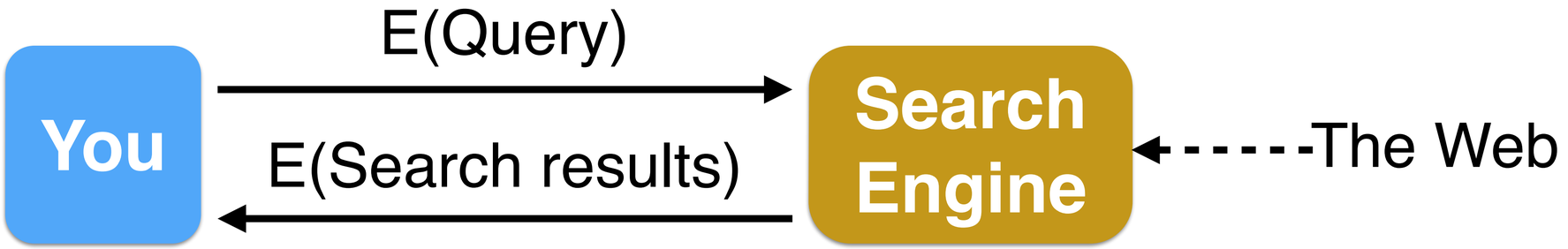
Pairings-Based Everything

- 2002: Hierarchical IBE
- 2003: Aggregate signatures; Ring signatures
- 2004: Short signatures; Group signatures
- 2005: Broadcast encryption
- 2006: Attribute-based encryption

Craig Gentry

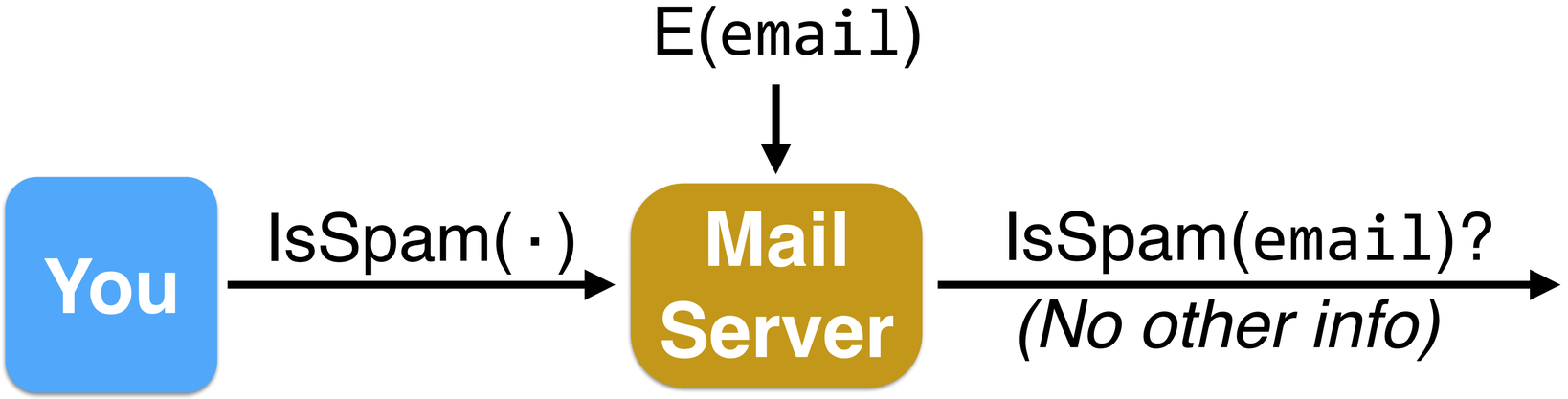
Brent Waters

Fully Homomorphic Encryption



- Example homomorphism: E(A) + E(B) = E(A+B)
- Partially homomorphic (RSA, ElGamal, Paillier): Add (+) or multiply (·), but not both at once.
- 2009: Gentry's Fully Homomorphic Encryption

Functional Encryption



- Traditional public-key encryption: All or nothing
- Functional encryption: Reveal only F(m)
- 2005: “Fuzzy Identity-Based Encryption”
- 2011-2013: Formal definitions & constructions

Multilinear Maps

Like bilinear maps, but with an arbitrary degree:

$$\mathbf{e(g^a, g^b, g^c) = e(g, g, g)^{abc}}$$

$$\mathbf{e(g^{a_1}, g^{a_2}, \ldots, g^{a_n}) = e(g, g, g)^{\Pi a_i}}$$

Software Obfuscation

- 2013: Software obfuscation
- Based on multilinear maps
- Example: Let P(m) := AES(key, m)
  Obfuscate(P(·)) is public-key crypto.

The Next 15 Years?

Welcome to Crypto War II

The New York Times

Security Experts Oppose Government Access to Encrypted Communication

The Washington Post

The Post's View

Putting the digital keys to unlock data out of reach of authorities

Last October in this space, we urged Apple and Google, paragons of innovation, to create a kind of secure golden key that could unlock encrypted devices, under a court order, when needed. The tech sector does not seem so inclined.

The Daily Dot

The rise of the new Crypto War

"Encryption threatens to lead all of us to a very dark place"

James Comey

FBI director

The Washington Post

Compromise needed on smartphone encryption

Predictions

- We'll be able to safely compute on untrusted computers.
- End-to-end encryption will be universal, but not without a fight.
- There will be surprising breaks in crypto we use today.
- We'll see more CPU & architecture hardware security features.
- A quantum computer will factor 35 with Shor's algorithm.

Thanks & Resources

Thanks: Kevin Lewi, Tony Arcieri, Susan Hohenberger, abhi shelat, JP Aumasson, Seny Kamara, Andrew Miller, Elaine Shi, Ling Ren, Paul Grubbs, Alexandre Anzala-Yamajako, Xiaoyong Bai, Abhradeep Guha Thakurta

- Dan Boneh's Coursera Cryptography course: https://www.coursera.org/course/crypto
- Crypto101 Introductory course: https://www.crypto101.io/
- Matasano Crypto Challenges: http://cryptopals.com/
- Modern Crypto mailing lists: https://moderncrypto.org/