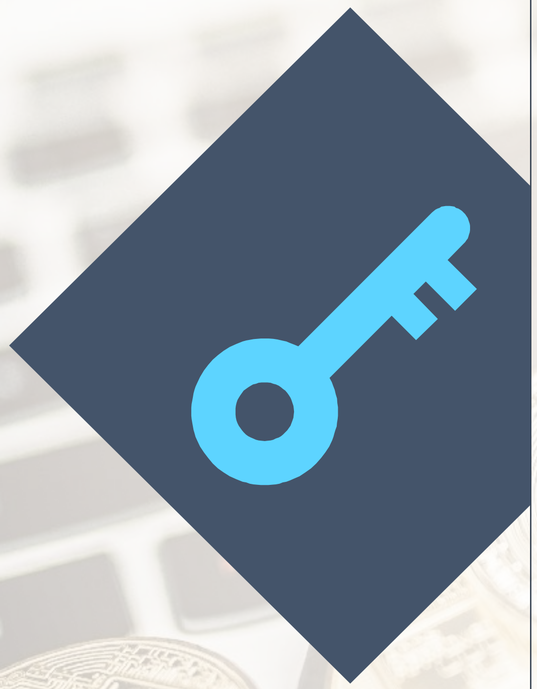
EMERGING CRYPTOGRAPHY

Steve Weis

Facebook Data Privacy

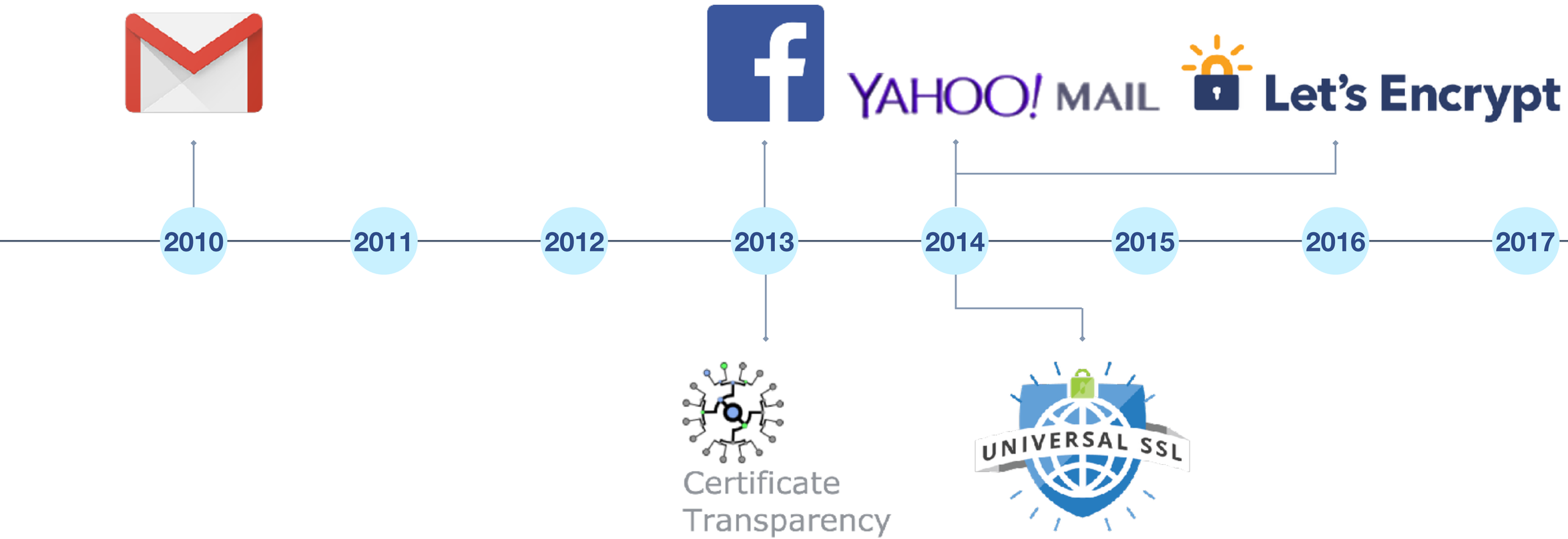
#EmergingCryptography



CRYPTOGRAPHY IS EVERYWHERE


People Emerging Online

TRANSPORT ENCRYPTION EVERYWHERE



TLS SECURITY VS. ACCESS

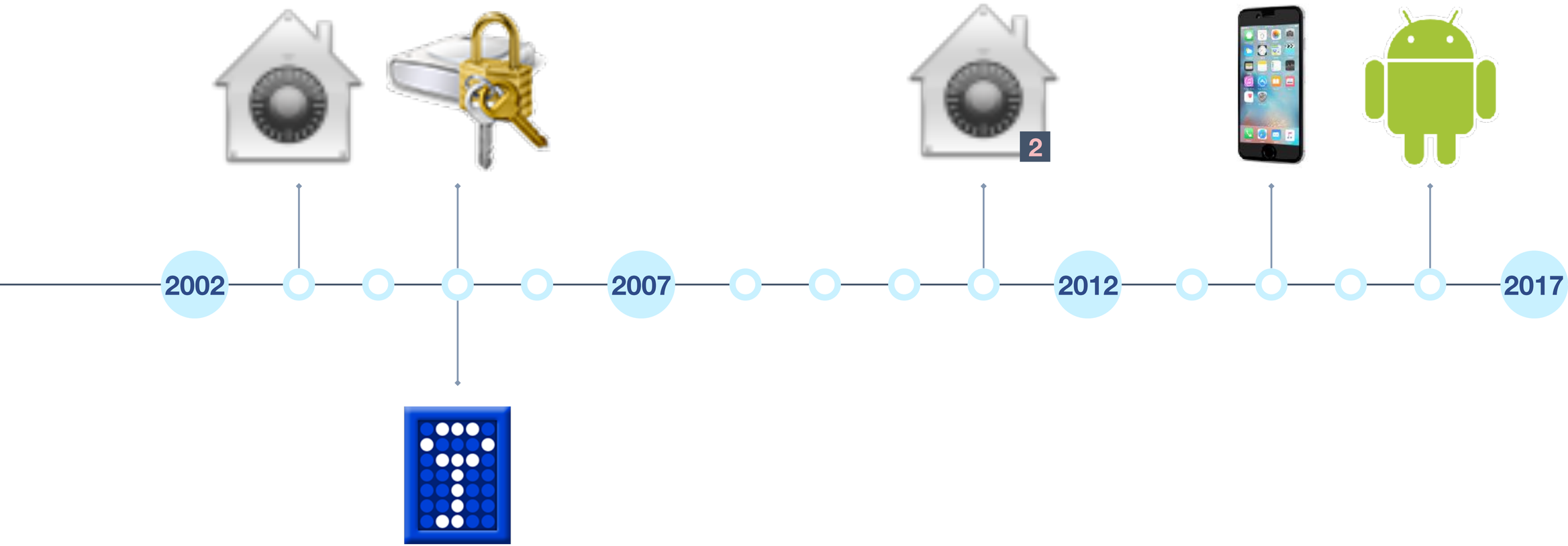
Lucky Thirteen

2012 — 2013 — 2014 — 2015 — 2016 — 2017

The FREAK Attack

Logjam Attack

DISK ENCRYPTION BY DEFAULT



Disk Encryption Works

E2E ENCRYPTION FOR EVERYONE

2010 — 2011 — 2012 — 2013 — 2014 — 2015 — 2016 — 2017

bitcoin

Silk Road

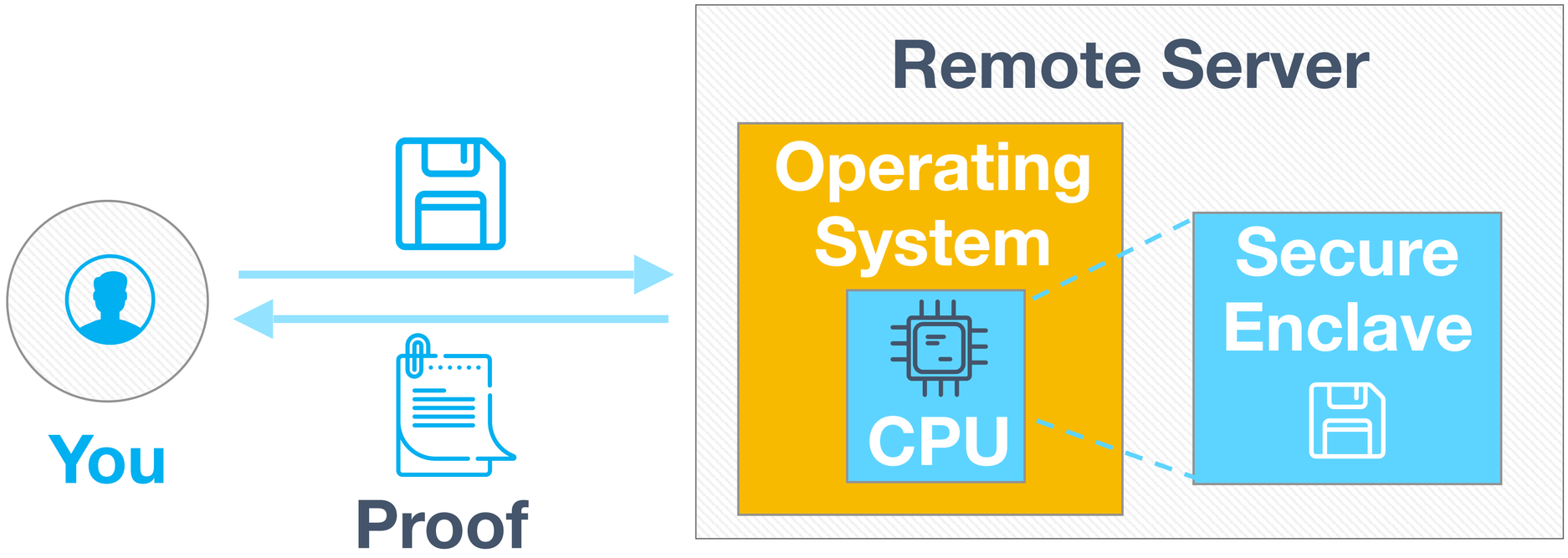
anonymous marketplace

Private Computation?

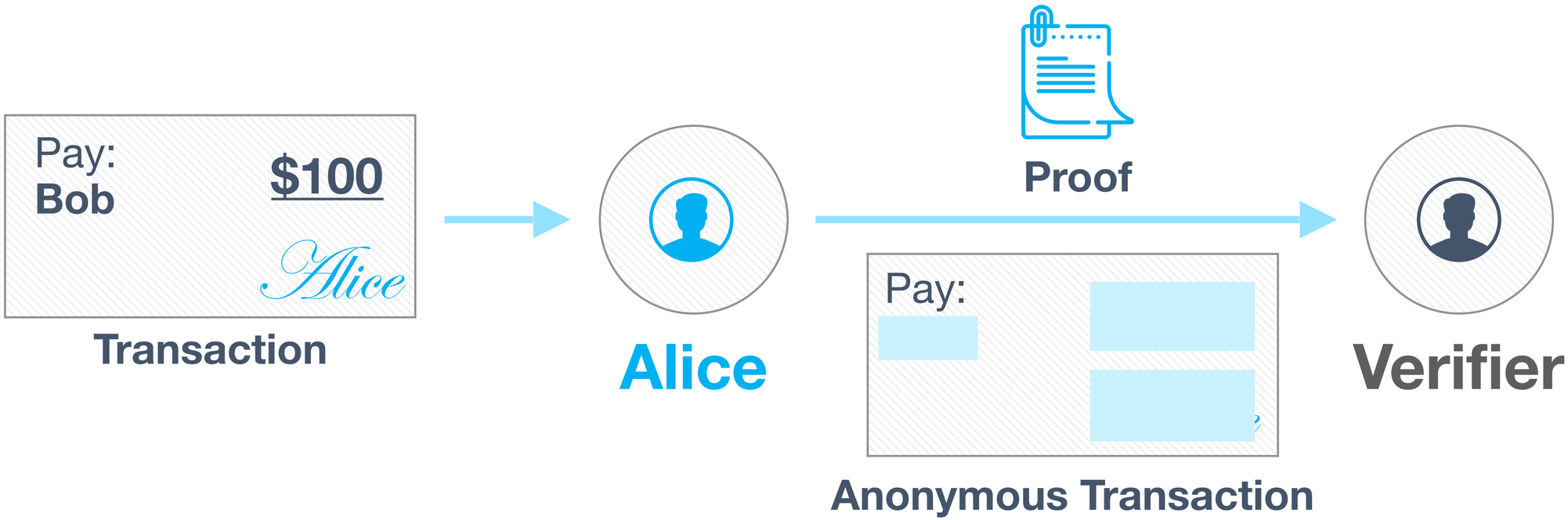
Private Communication

Private Storage

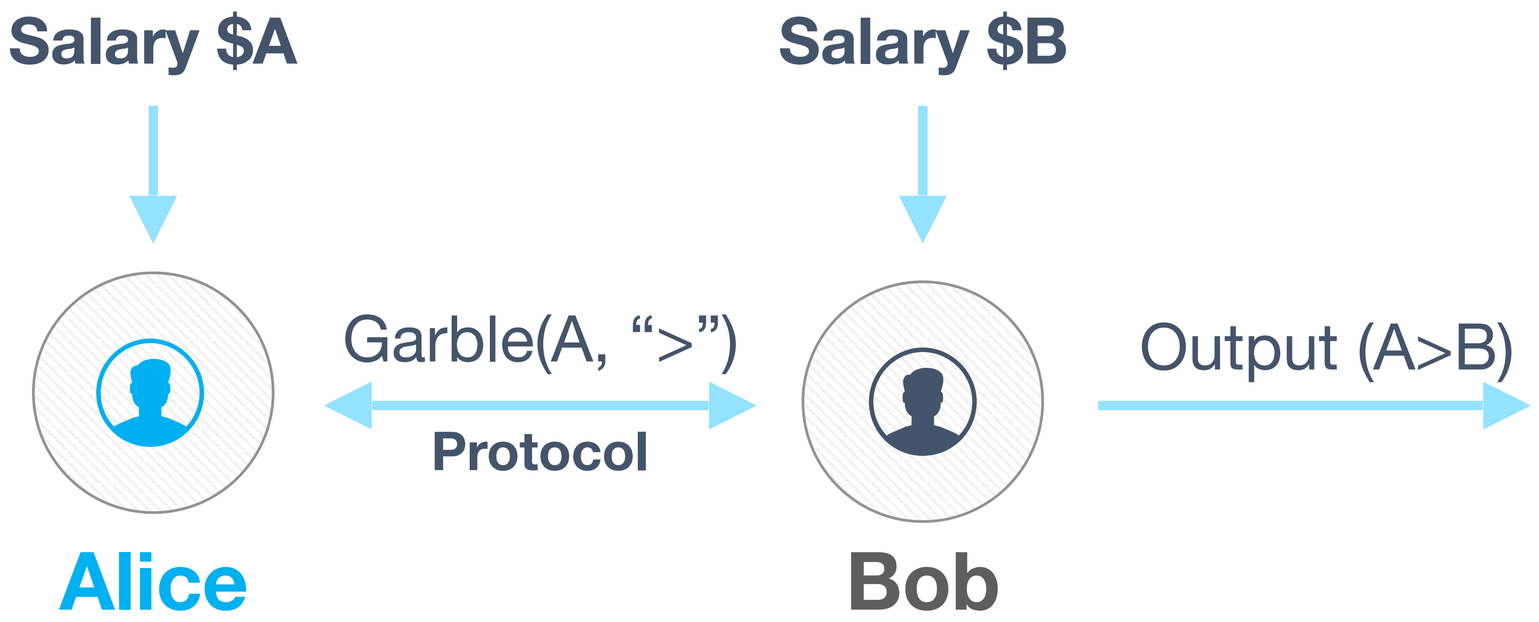
SOFTWARE GUARD EXTENSIONS



GETTING SNARKY



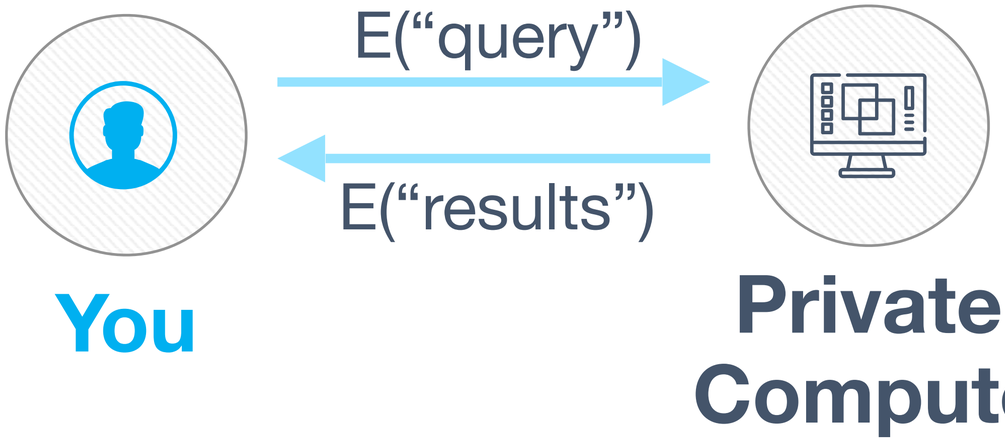
MULTIPARTY COMPUTATION

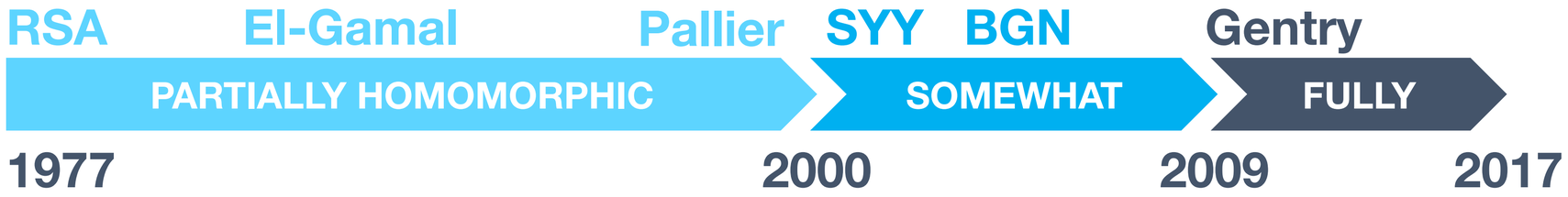


HOMOMORPHIC ENCRYPTION

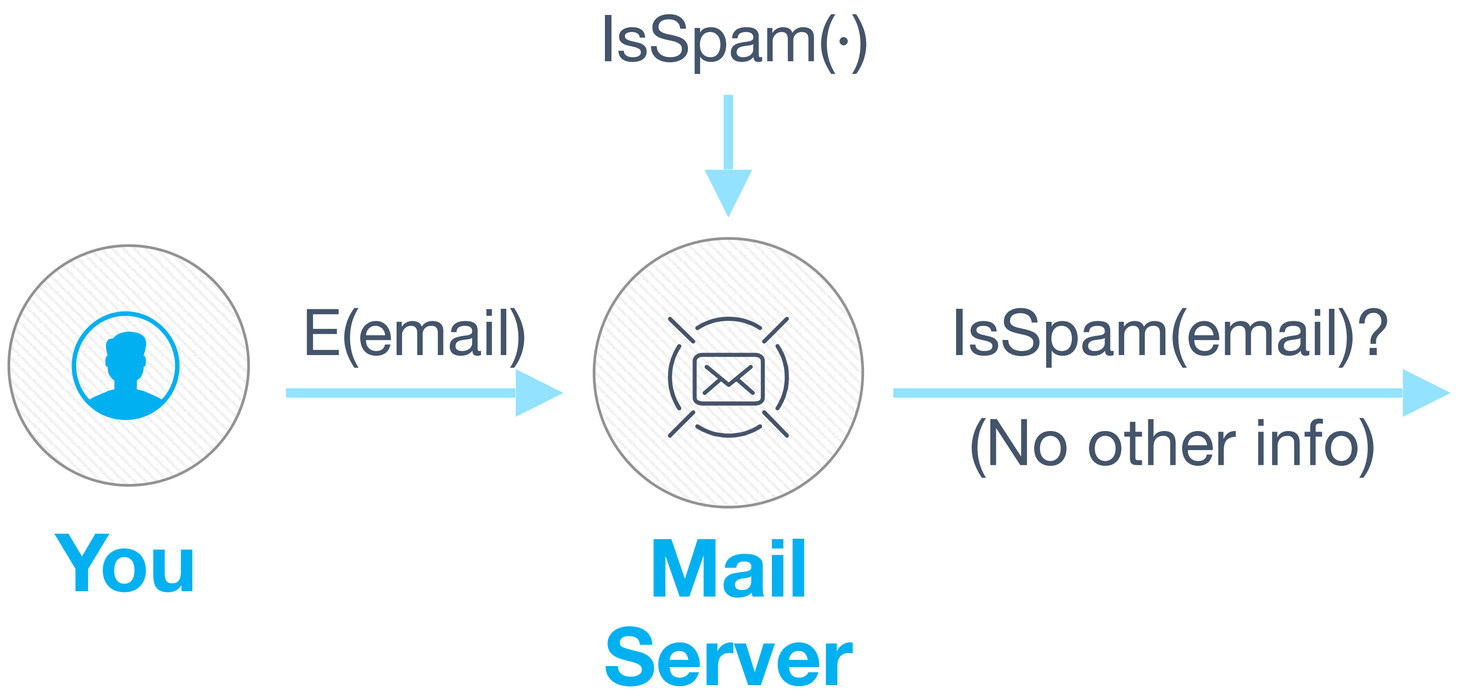
› Addition: E(A) + E(B) = E(A+B)

› Multiplication: E(A) · E(B) = E(A · B)





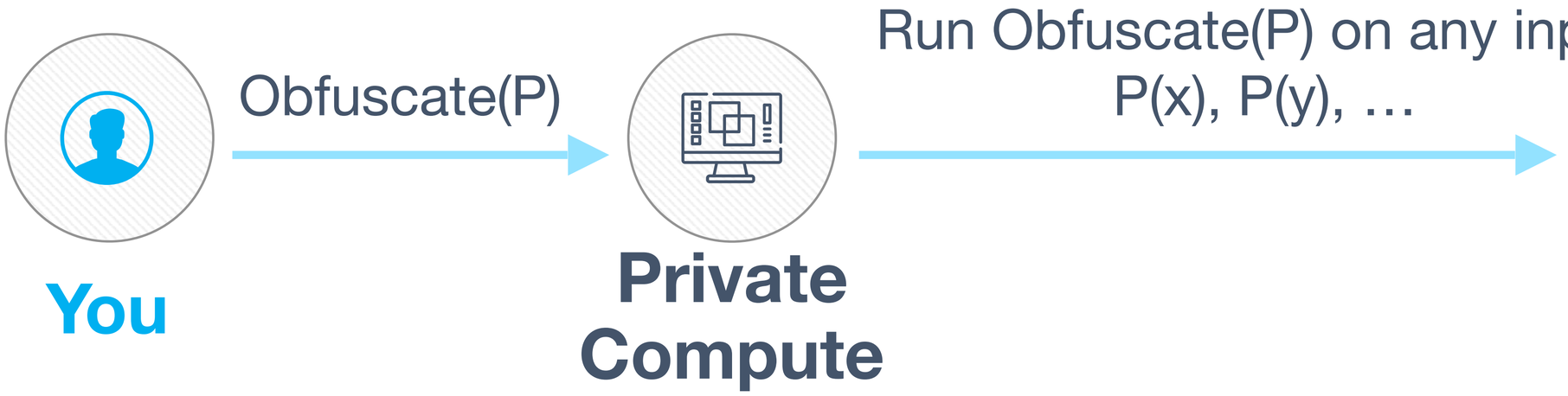
FUNCTIONAL ENCRYPTION



Traditional public-key encryption:
Decrypt all or nothing

Functional encryption:
Reveal only a function F(m)

INDISTINGUISHABILITY OBFUSCATION



Function Obfuscate() takes a program P as input

Suppose P(m):=AES(key, m). Obfuscate(P) is public-key crypto.

How can we all benefit?

“Encryption threatens to lead all of us to a very dark place.”

James Comey
Former FBI director

CRYPTO SCHMYPTO —

FBI director: Unbreakable encryption is a “huge, huge problem”

“I get it, there’s a balance that needs to be struck,” Christopher Wray said.

CYRUS FARIVAR - 10/23/2017, 3:56 PM

“There is no constitutional right to sell warrant-proof encryption.”

Rod J. Rosenstein
Deputy Attorney General

Deputy Attorney General Rosenstein’s “Responsible Encryption” Demand is Bad and He Should Feel Bad

LEGAL ANALYSIS BY KURT OPSAHL | OCTOBER 10, 2017

#EmergingCryptography

THANK YOU