The Moral Nature of Cryptographic Work

By Phillip Rogaway

Papers We Love Boston — with Richard Littauer
@richlitt

About

Outline

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

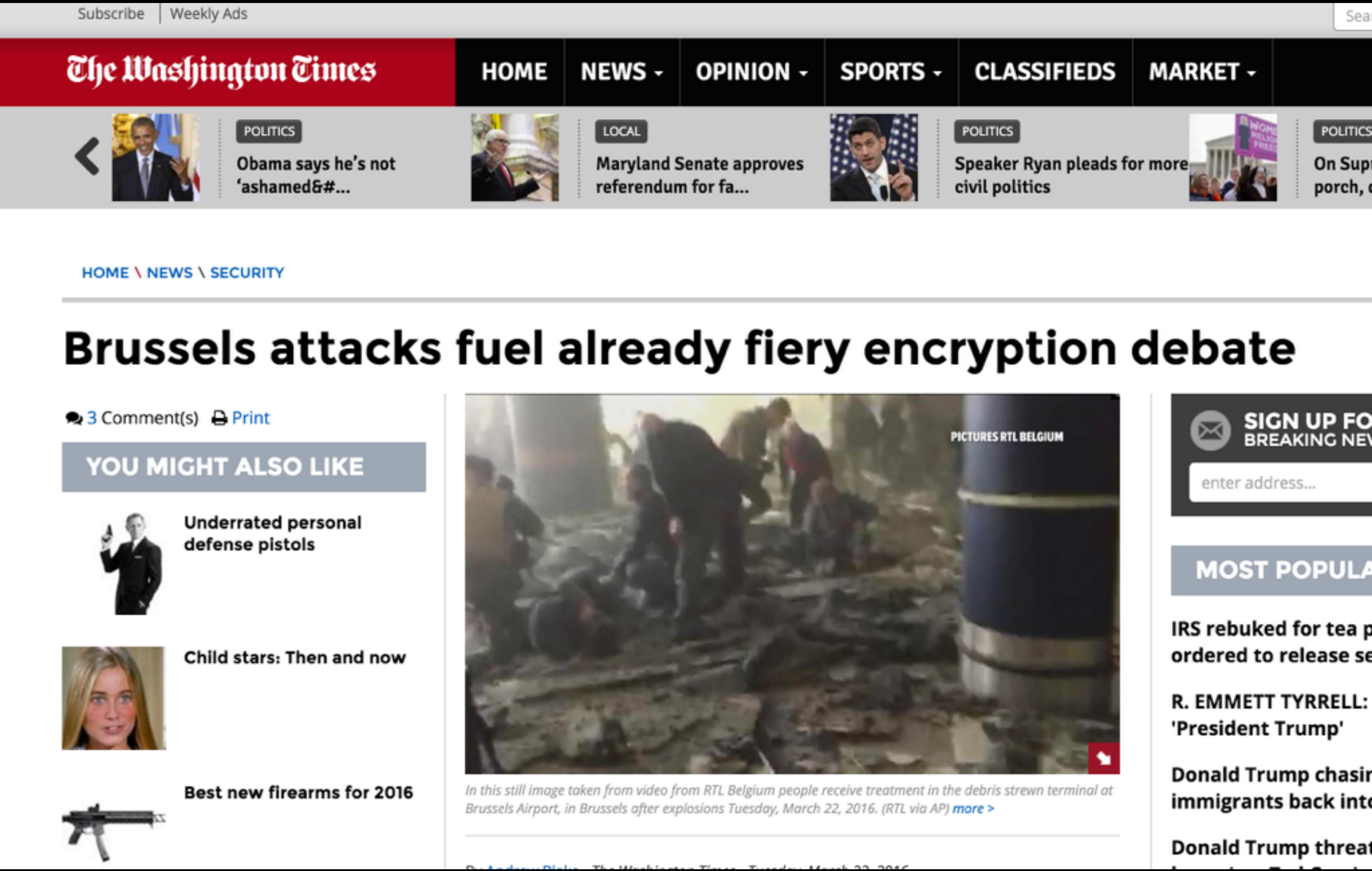
fn(x,…n)

Let’s start with x = 1

Part 1: Social responsibility of scientists and engineers

Two modes of behaving politically

Implicit politics



Subscribe | Weekly Ads

Sea

The Washington Times

HOME | NEWS | OPINION | SPORTS | CLASSIFIEDS | MARKET

POLITICS
Obama says he's not 'ashamed&#...

LOCAL
Maryland Senate approves referendum for fa...

POLITICS
Speaker Ryan pleads for more civil politics

POLITICS
On Sup
porch,

HOME \ NEWS \ SECURITY

Brussels attacks fuel already fiery encryption debate

3 Comment(s) Print

In this still image taken from video from RTL Belgium people receive treatment in the debris strewn terminal at Brussels Airport, in Brussels after explosions Tuesday, March 22, 2016. (RTL via AP) more >

By Andrew Blake - The Washington Times - Tuesday, March 22, 2016

SIGN UP FO
BREAKING NEW

enter address...

MOST POPULA

IRS rebuked for tea p
ordered to release se

R. EMMETT TYRRELL:
'President Trump'

Donald Trump chasin
immigrants back into

Donald Trump threat

The ethic of responsibility

Historical events shaping the ethic of responsibility.

The good scientist

EVIL

The ethic of responsibility
is in decline.

The ethic of responsibility is in decline.

Technological optimism.

Conclusion to Part 1.

Part 2: The political character of cryptographic work

THE
MARTIA
ARE C
THE EARTH

Scientist or Spy?

Academic cryptography used to be more political.

Strip out the politics.

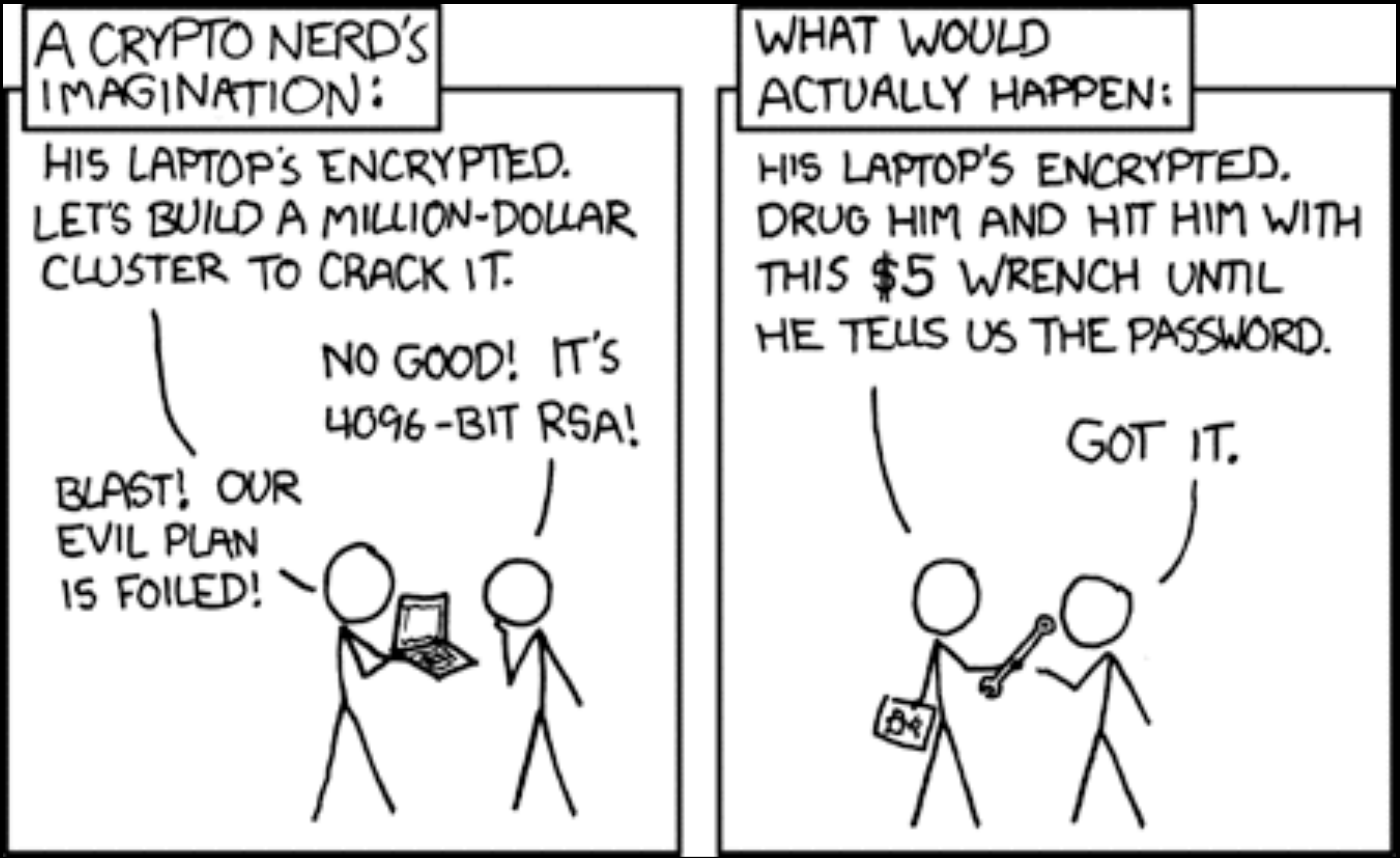
Children of [Chaum81] and [GM82].

Cypherpunks!

Cryptography favors whom?

Encryption

Identity Based Encryption


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

Differential Privacy

FHE and iO

Cryptanalysis

We’re not threatening.

Conclusion to part 2.

Part 3: The dystopian world of pervasive surveillance

Law-enforcement framing.

Surveillance-studies framing.

Our dystopian future.

Conclusion to Part 3

Part 4: Creating a more just and useful field

How one developer just broke Node, Babel and thousands of projects in 11 lines of JavaScript

Code pulled from NPM – which everyone was using

Careful, careful ... Don't fumble this like the JS world (Credit: Claus Rebler)

23 Mar 2016 at 01:24 Chris Williams 1384 572

YOU MUST CHOOSE
WISELY
memegenerator.net

Practice-oriented provable security.

Funding

Academic freedom

DOGMA
Get touched by an angel.

A more expansive view.

Learn some privacy tools.

A cryptographic commons.

Institutional values

Conclusion to it all!

Go make boring stuff.

But remember humanity.

Thanks.