Криптография сегодня

JP Aumasson

KUDELSKI SECURITY

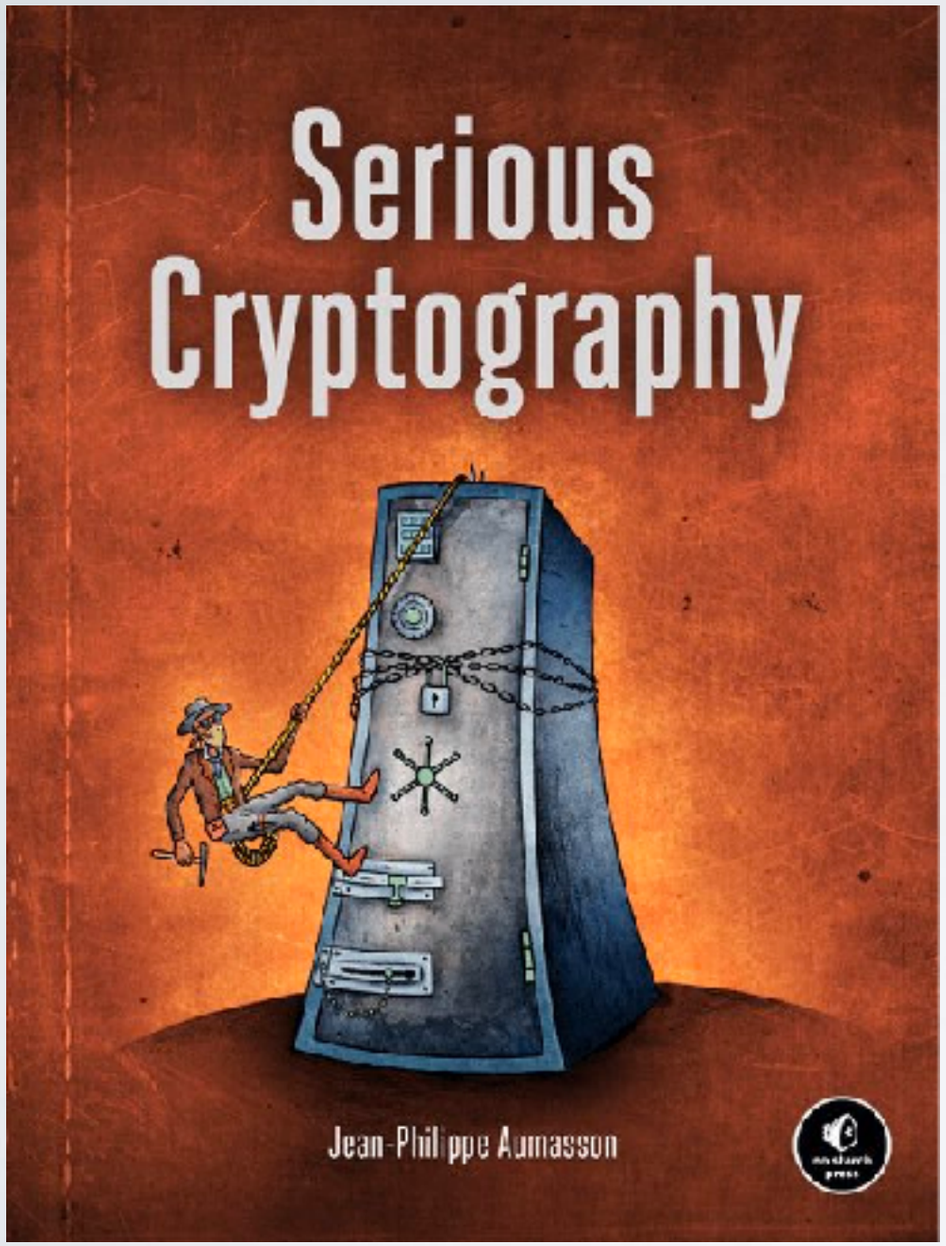
ABOUT ME

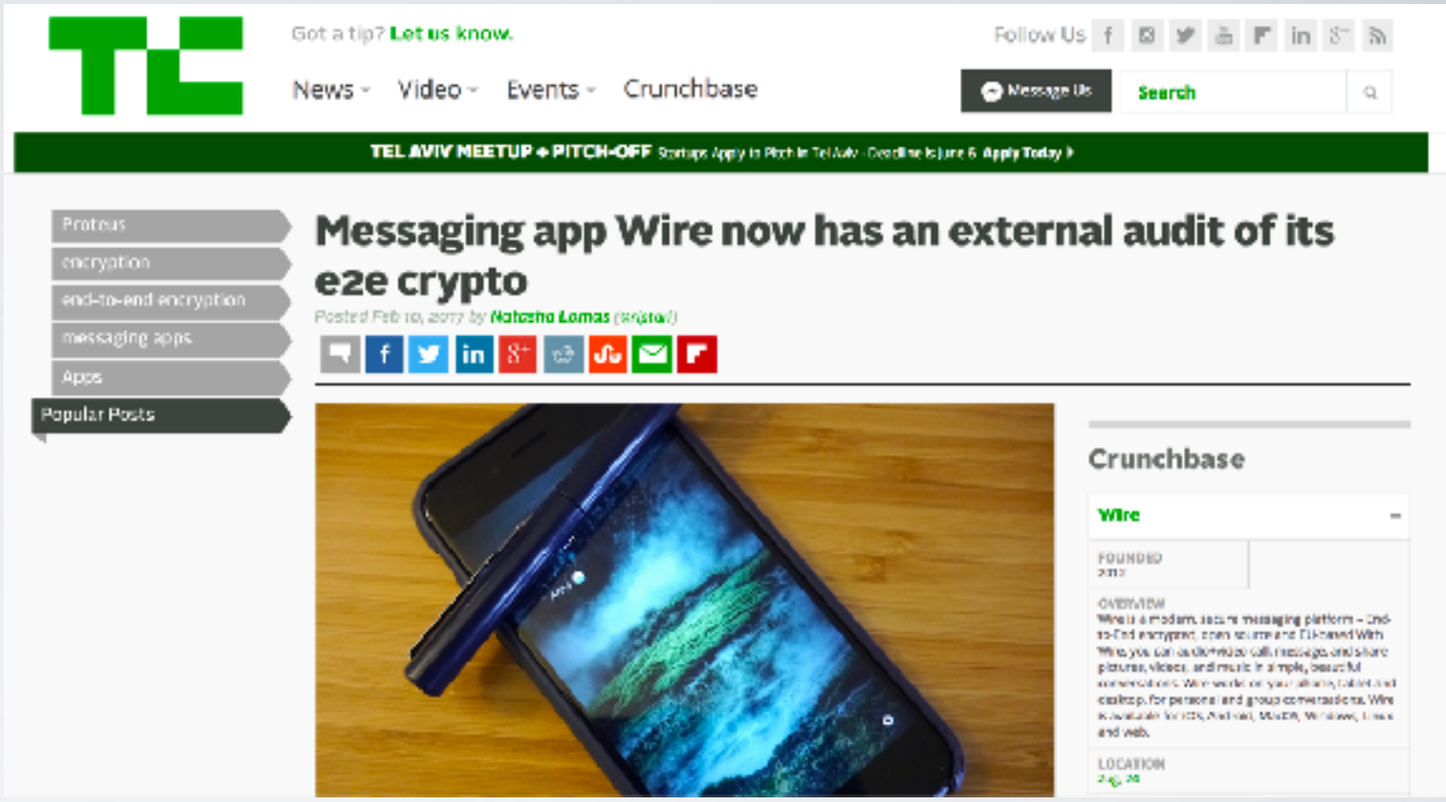
NOW

- Principal research engineer at Kudelski Security
- Applied crypto research, code reviews, infosec consulting, etc.
- Outreach @ Black Hat, Defcon, Zeronights, Troopers, etc.

BEFORE

- 2006-09: PhD in crypto, academic research and papers
- 2010-12: Cryptographer for Pay-TV systems at Nagravision
- BLAKE2, SipHash, organized PHC, Crypto Coding Standard


Serious
Cryptography
Jean-Philippe Aumasson


Got a tip? Let us know.
Follow Us
News
Video
Events
Crunchbase
Message Us
Search
TEL AVIV MEETUP + PITCH-OFF
Proteus
encryption
end-to-end encryption
messaging apps
Apps
Popular Posts
Messaging app Wire now has an external audit of its e2e crypto
Crunchbase
Wire


threatpost
CATEGORIES
FEATURED
PODCASTS
VIDEOS
Welcome > Blog Home > Cryptography > Breaking Signal: A Six-Month Journey
BREAKING SIGNAL: A SIX-MONTH JOURNEY

THIS TALK

What does it take to be a cryptographer in 2017?

CRYPTOGRAPHER

?

CLASSICAL ERA
(-∞ – ~1960)

CLASSICAL ERA

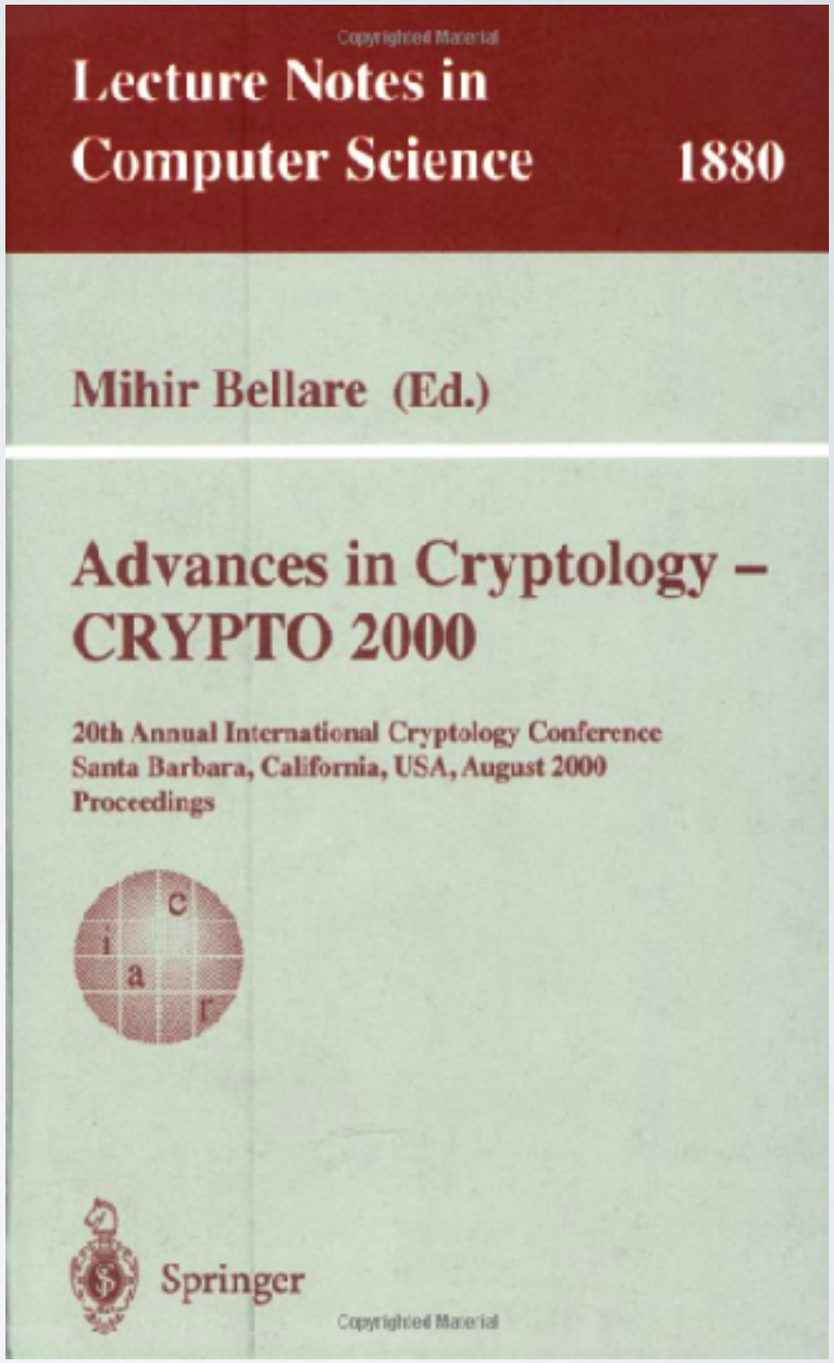
Just want to keep a message secret

Sometimes just for a few hours

Against simple attackers

"Easy"

MODERN ERA (~1960 – 2010)



MODERN ERA

Cryptography for computers:

bits instead of letters, transistors

instead of levers and rotors

MODERN ERA

Public-key crypto: revolutionized crypto, enabled signature and key agreement (via RSA, DH, ECC)

MODERN ERA

More than secrecy: crypto protects integrity, authenticity, availability, anonymity

MODERN ERA

More than ciphers: encryption schemes, modes of operations, and protocols for various functionalities

MODERN ERA

From craft to science: rigorous definitions and models, formalisms enabling security reductions/proofs

MODERN ERA RESULTS

Plenty of ciphers and protocols…

Including many that we don’t use…

MODERN ERA RESULTS

Plenty of **algorithms**…

Symmetric crypto schemes that will remain secure forever (AES, SHA-2/3)

MODERN ERA RESULTS

Plenty of **protocols**…

Key agreement, MPC, ZK, e-voting, secret sharing, group/ring signatures, distance bounding, identification, oblivious transfer, etc. etc.

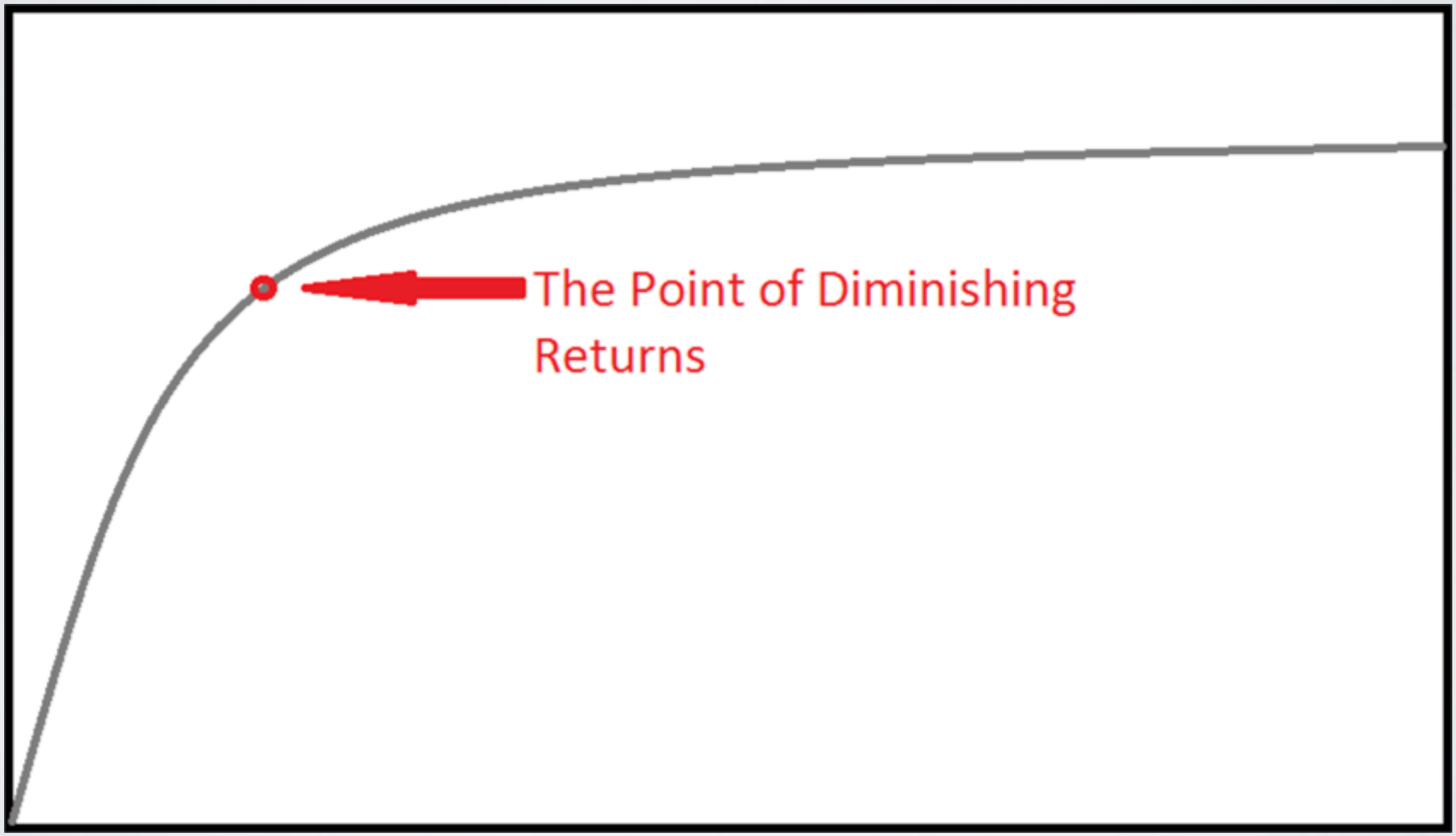
MODERN ERA RESULTS

Most ciphers & protocols **not used**

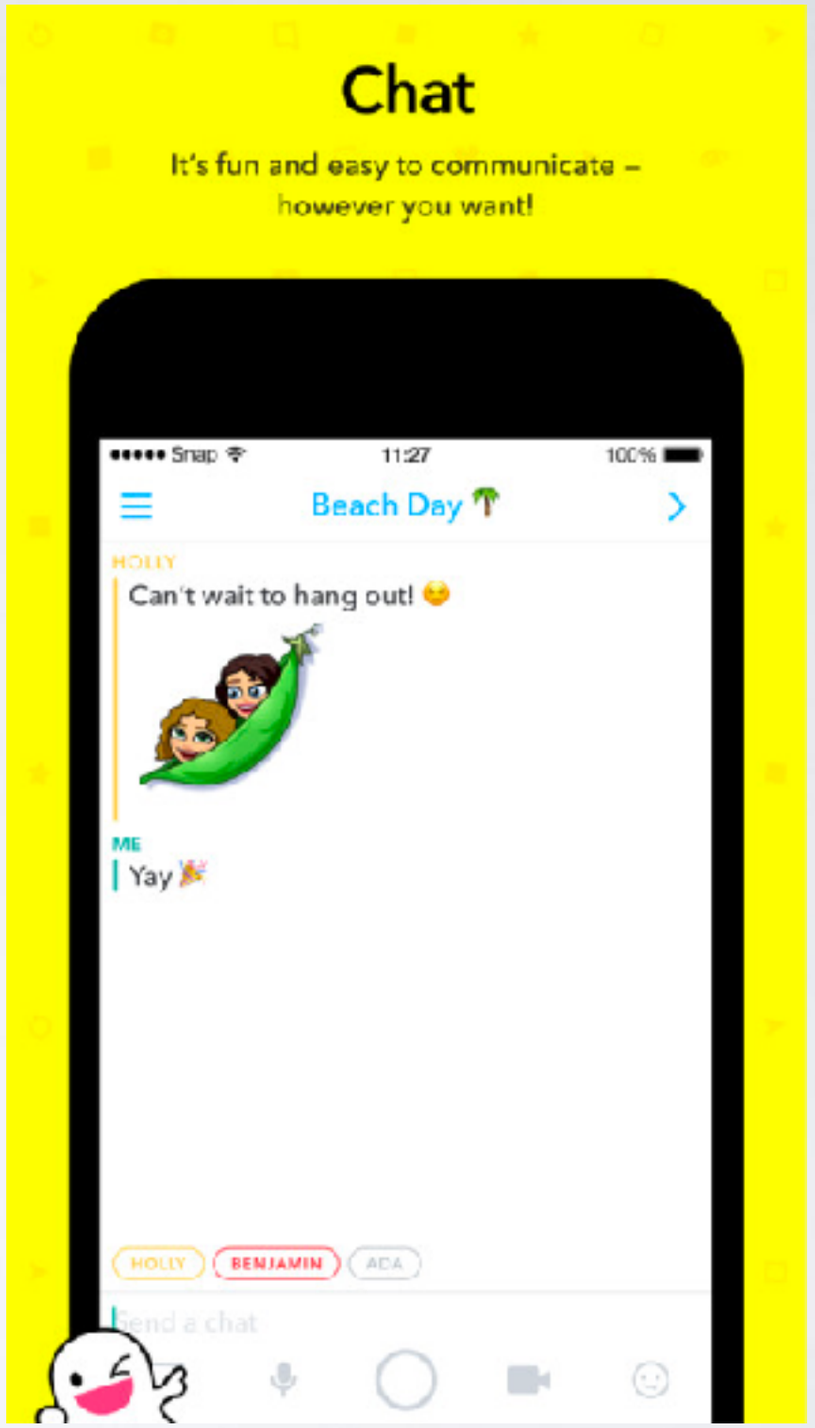
More motivated by research problems than by applications

Researchers sometimes too incentived to publish papers

MODERN ERA LIMITATIONS?



TODAY
(2010 – …)


Chat
It's fun and easy to communicate –
however you want!
Snap
11:27
100%
Beach Day
HOLLY
Can't wait to hang out!
ME
Yay
HOLLY
BENJAMIN
ADA
Send a chat

A NEW WORLD

Keywords: mobile, cloud, IoT, Snowden

Software eating the world

Crypto a small part of infosec

A NEW CRYPTO?

Can no longer be elitist and isolated

Needs to catch up with reality

NEW NEEDS

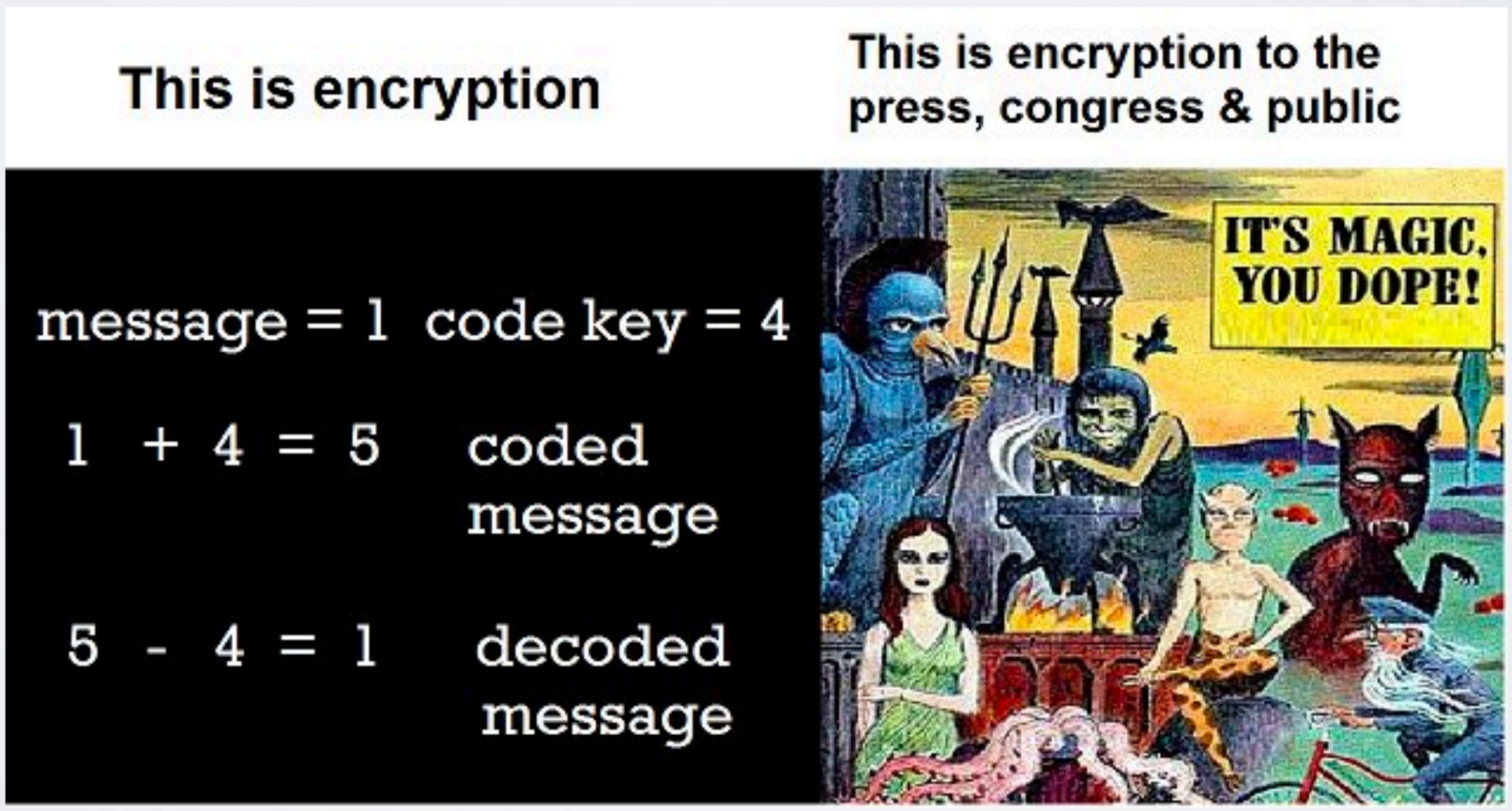
Usability; of user interfaces, APIs

Greater focus on privacy, anonymity

Crypto as a component of a system

NEW NEEDS

Do a better job at teaching and documenting crypto



NEW NEEDS

Focus less on building blocks, build real systems addressing real use cases

Show the code or it didn't happen

HOW CAN WE ADAPT?

TODAY'S CRYPTOGRAPHY

Multidisciplinary: coding, software engineering, reverse engineering, etc.

Fewer hard skills, more soft skills

“When a software engineer says it's impossible, that really just means it's cryptographically interesting.”

—Moti Yung, RWC 2017

Secure https://rwc.iacr.org

Real World Crypto Symposium

RWC Information

- Home
- Leychin Prize
  - Nomination Form
- Form to Nominate an Invited Speaker
- Past RWC
- YouTube Channel
- Twitter
  - Use #realworldcrypt

Real World Crypto Symposium aims to bring together cryptography researchers with developers implementing cryptography i
is to strengthen the dialogue between these two communities. Topics covered focus on uses of cryptography in real-world en
and embedded devices.

The programme consists of invited and contributed talks.

- The contributed talks are selected using light touch review.
- The invited talks are selected by the steering committee. However, you can make us aware of people you think we shou

Unlike other IACR events there are no proceedings/published papers. Talks are selected on the basis of impact on the real wo
audience, and our perceived quality of the speaker.

Since 2018 the Real World Crypto Symposium is organized by the International Association for Cryptologic Research (IACR).

Now more popular than CRYPTO

SOME CRYPTO FROM THE REAL WORLD…

Network Working Group
Internet-Draft
Obsoletes: 5077, 5246 (if approved)
Updates: 4492, 5705, 6066, 6961 (if approved)
Intended status: Standards Track
Expires: November 25, 2017

E. Rescorla
RTFM, Inc.

May 24, 2017

The Transport Layer Security (TLS) Protocol Version 1.3

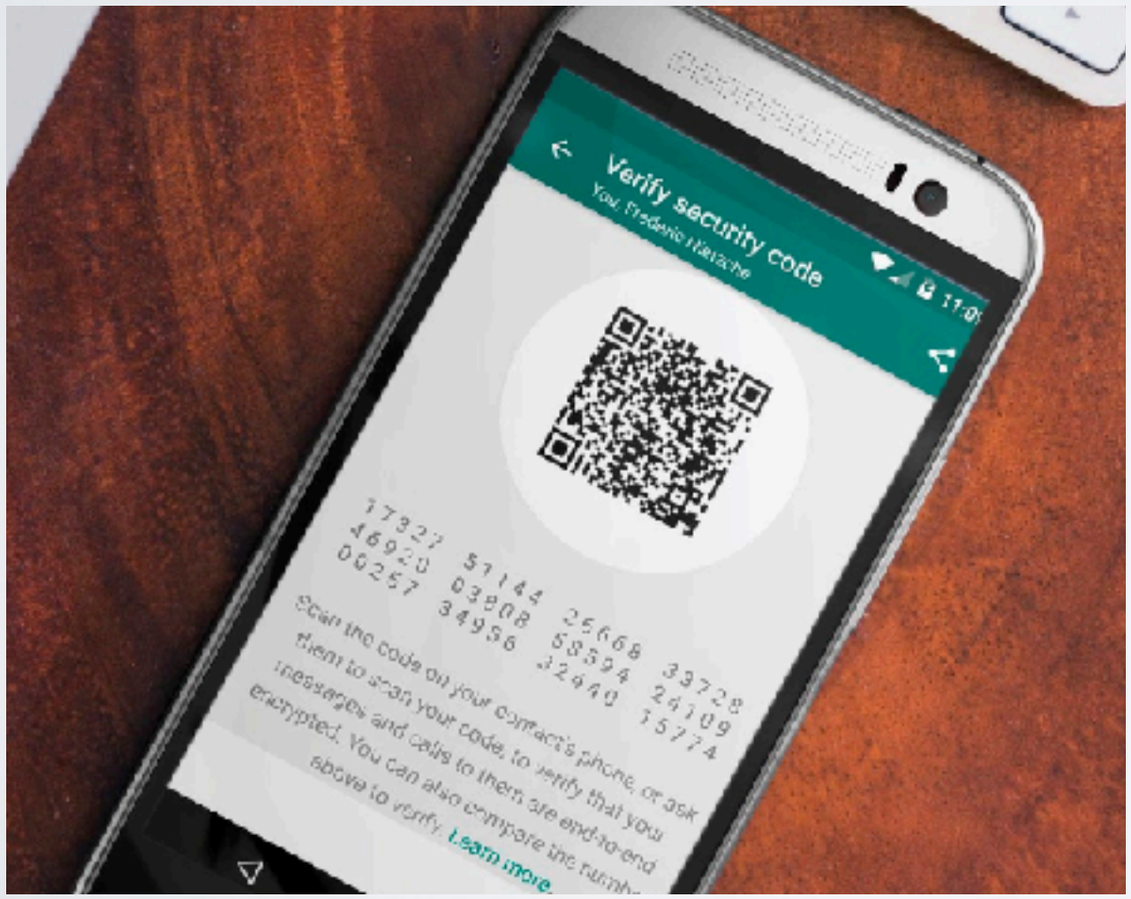
draft-ietf-tls-tls13-latest

Abstract

This document specifies version 1.3 of the Transport Layer Security (TLS) protocol. TLS allows client/server applications to communicate over the Internet in a way that is designed to prevent eavesdropping, tampering, and message forgery.

SIGNAL PROTOCOL

Key agreement X3DH, double ratchet



Noise Protocol Framework

Read Specification

Crypto protocols that are simple, fast, and secure

Noise is a framework for building crypto protocols. Noise protocols support mutual and optional authentication, identity hiding, forward secrecy, zero round-trip encryption, and other advanced features.

The specification

Detailed specification for the Noise Protocol Framework.

Web | PDF | Github

The code

Open source implementations in C, Java, Go, Haskell, and Rust.

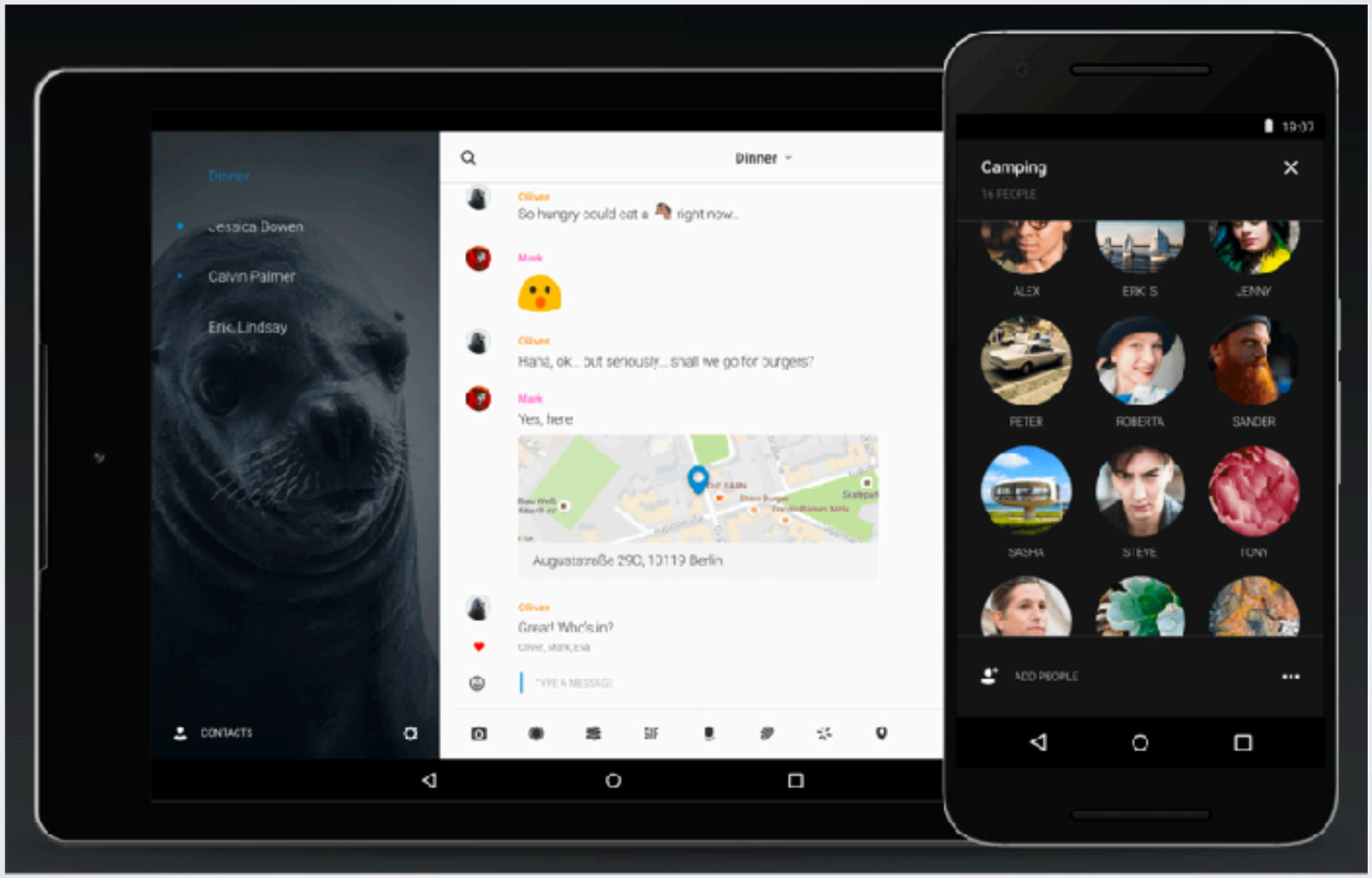
Noise-C | Noise-Java | Noise (Go)

Cacophony (Haskell) | Snow (Rust)

https://noiseprotocol.org/

MULTI-DEVICE / GROUP E2E

Secure sync, trust management, calls, . . .



STEALTH VPN

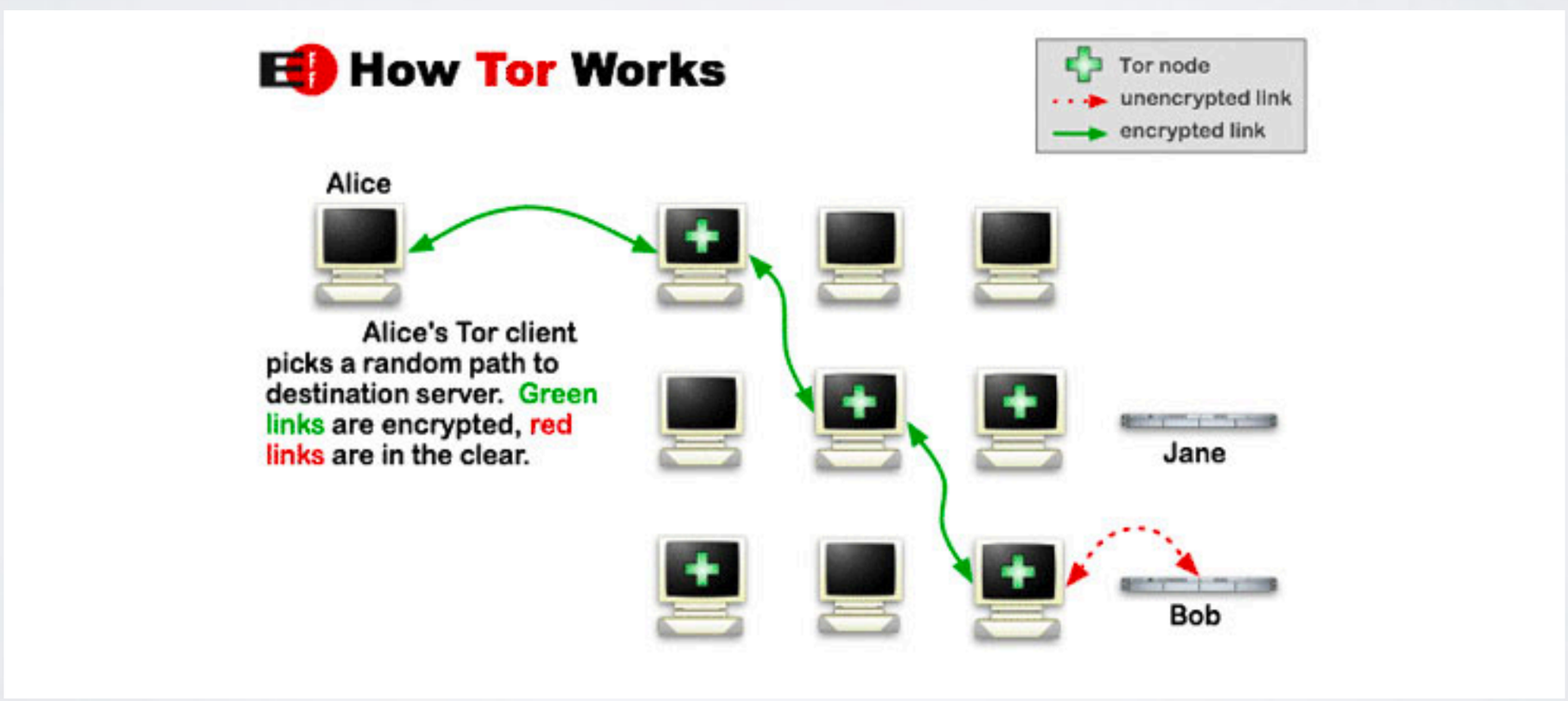
Noise + identity hiding, formally verified

WireGuard is an extremely simple yet fast and modern VPN that utilizes **state-of-the-art** cryptography. It aims to be faster, simpler, leaner, and more useful than IPSec, while avoiding the massive headache. It intends to be considerably more performant than OpenVPN. WireGuard is designed as a general purpose VPN for running on embedded interfaces and super computers alike, fit for many different circumstances. Initially released for the Linux kernel, it plans to be cross-platform and widely deployable. It is currently under heavy development, but already it might be regarded as the most secure, easiest to use, and simplest VPN solution in the industry.

BLOCKCHAIN PROTOCOLS

ethereum


Congratulations!
This browser is configured to use Tor.
You are now free to browse the Internet anonymously.
Test Tor Network Settings
Search securely with Startpage.


How Tor Works
Tor node
unencrypted link
encrypted link
Alice
Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Bob

LINUX FOUNDATION COLLABORATIVE PROJECTS

Documentation Get Help Donate About Us

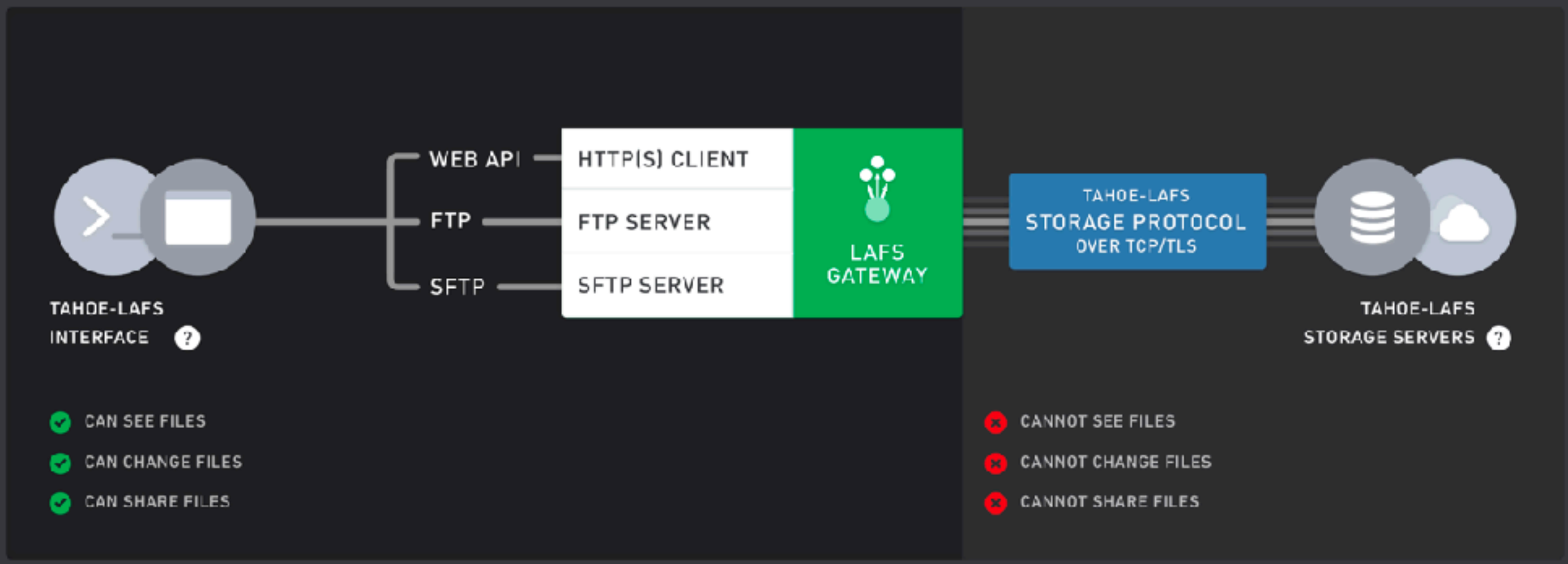
Let's Encrypt is a **free**, **automated**, and **open** Certificate Authority.

Get Started Donate

https://letsencrypt.org/

Tahoe-LAFS Network Topology

S4 is an Amazon S3-based application of Least-Authority File System, or LAFS. LAFS is a free, open source cloud storage system with verifiable end-to-end security. It distributes your data across multiple servers.



https://leastauthority.com/

BOTTOM LINE

Innovation comes from industry, open-source communities, who are directly exposed to the real problems

Academia follows and provides deeper analysis and proofs

EXCEPTION

POST-QUANTUM CRYPTO PROJECT

NEWS -- December 15, 2016: The National Institute of Standards and Technology (NIST) is now accepting submissions for quantum-resistant public-key cryptographic algorithms. The deadline for submission is ***November 30, 2017.*** Please see the Post-Quantum Cryptography Standardization menu at left for the complete submission requirements and evaluation criteria.

In rece tum
compu olve
mathe
compu ble to
break
seriou ations
on the also
called ns that
are se perate
with ex

CONCLUSION

As cryptographers, we need to…

- Go out of our comfort zone, learn about technologies that use crypto
- Acknowledge that research can no longer be disconnected from users

СПАСИБО