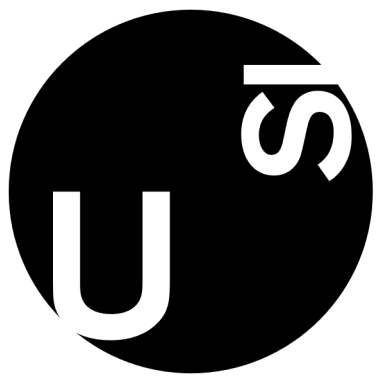
Directions in Applied Cryptography

Matilda Backendal

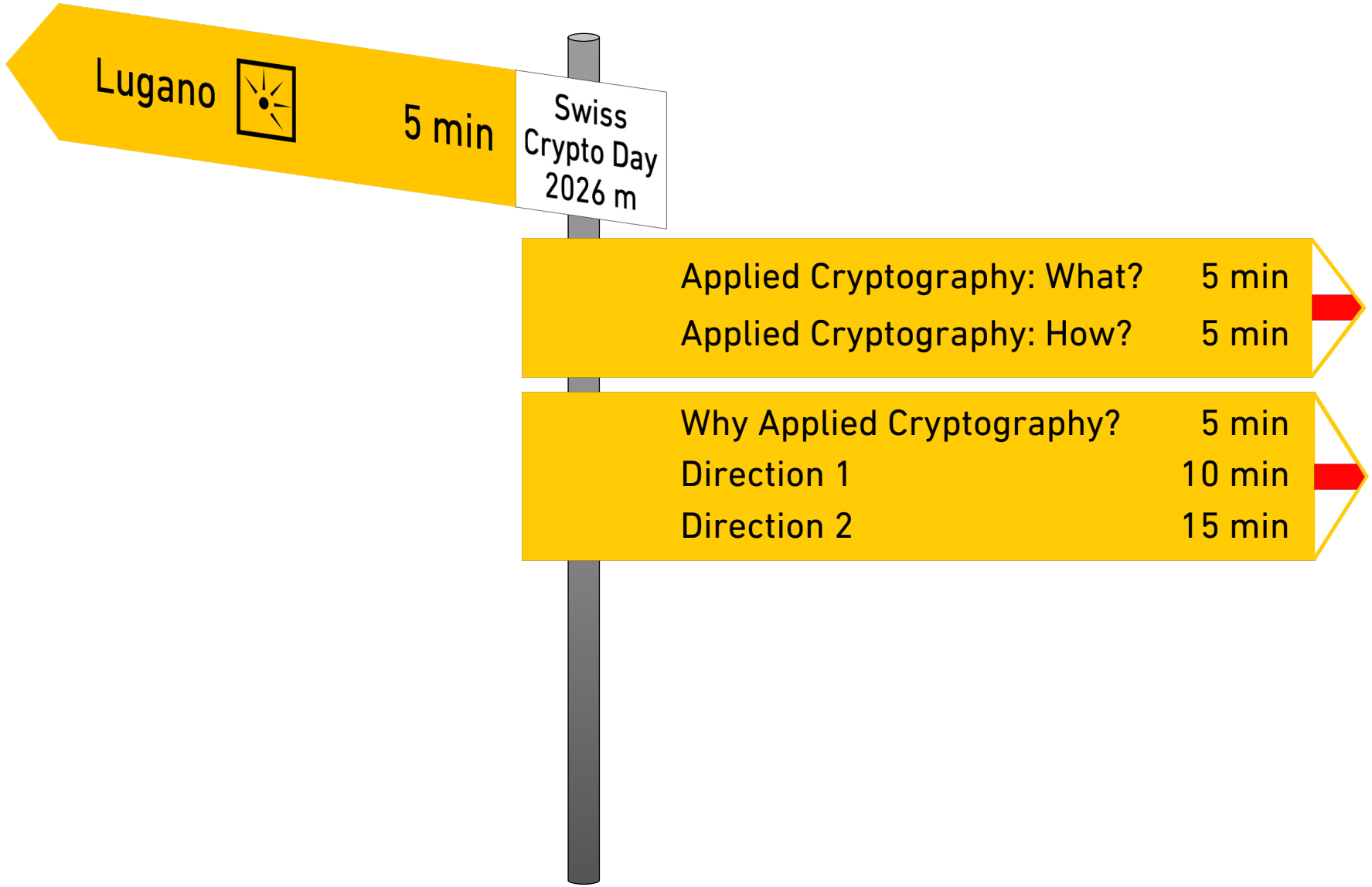
Faculty of Informatics
USI, Lugano

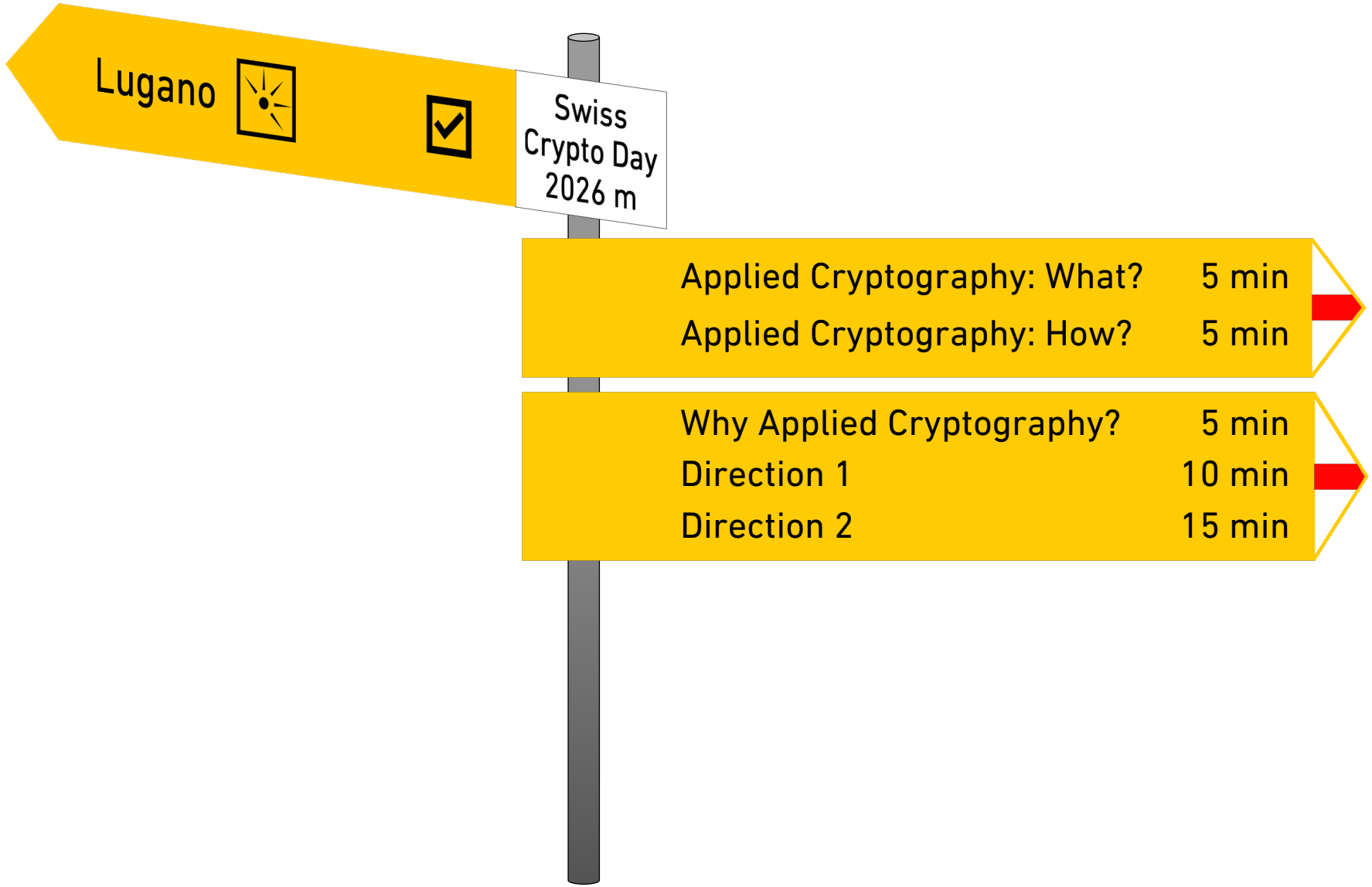


Università della Svizzera italiana

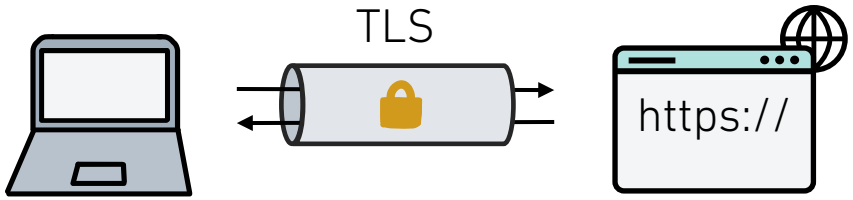
Swiss Crypto Day, September 4, 2026

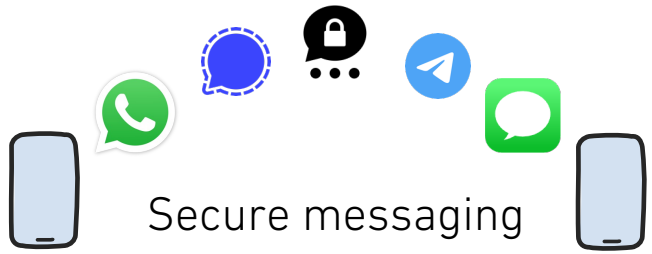
Map by Karte: NordNordWest, CC BY-SA 3.0 de, https://commons.wikimedia.org/w/index.php?curid=36921657

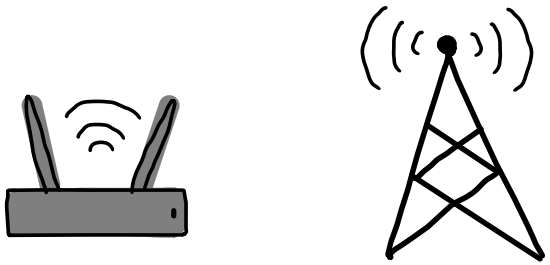

Lugano
5 min
Swiss Crypto Day 2026 m
Applied Cryptography: What? 5 min
Applied Cryptography: How? 5 min
Why Applied Cryptography? 5 min
Direction 1 10 min
Direction 2 15 min

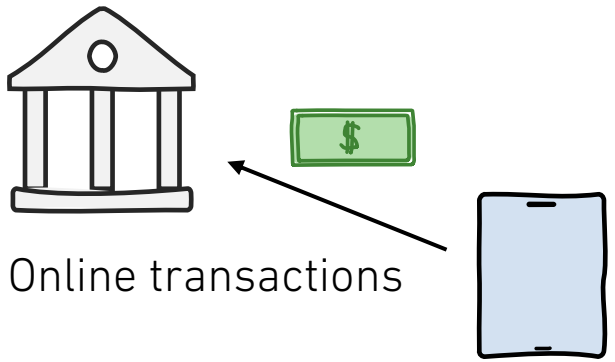

Lugano
Swiss Crypto Day 2026 m
Applied Cryptography: What? 5 min
Applied Cryptography: How? 5 min
Why Applied Cryptography? 5 min
Direction 1 10 min
Direction 2 15 min

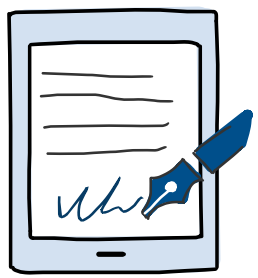
Applied Cryptography: What?

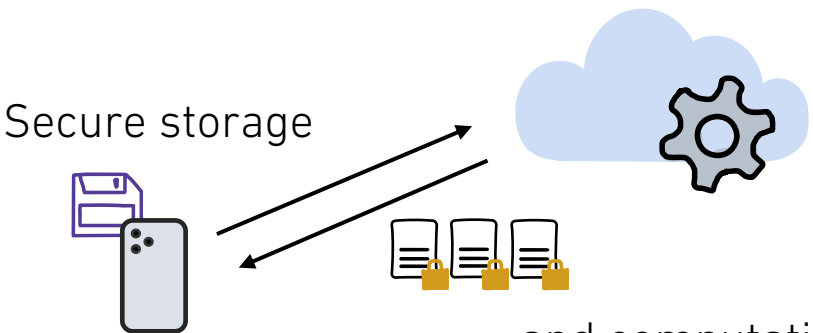


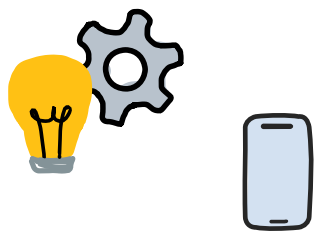




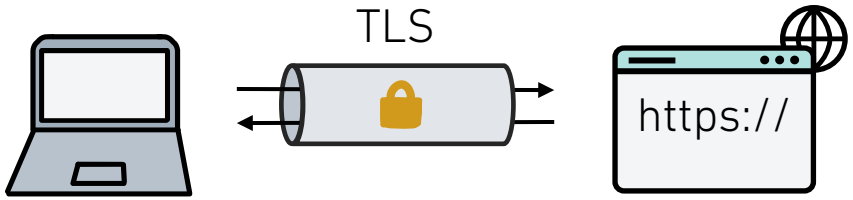


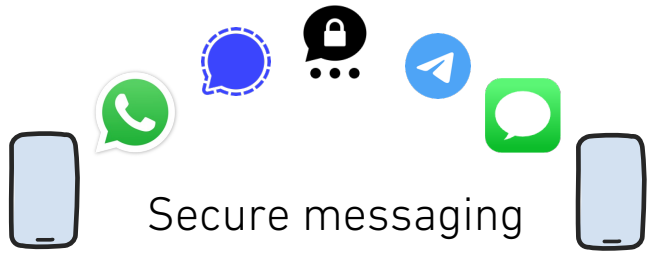


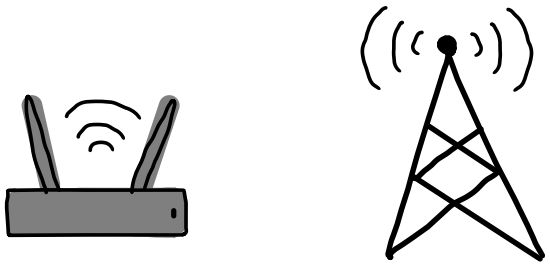




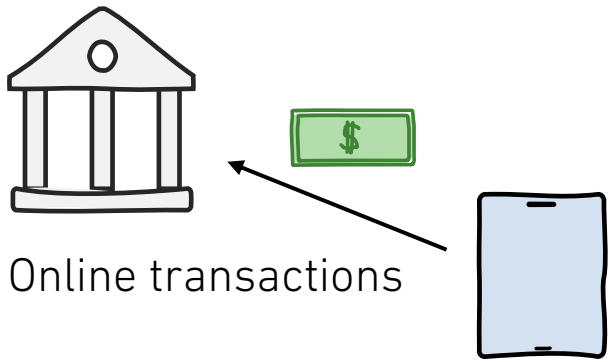
Applied Cryptography: What?

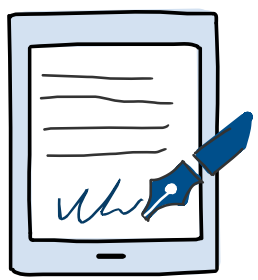


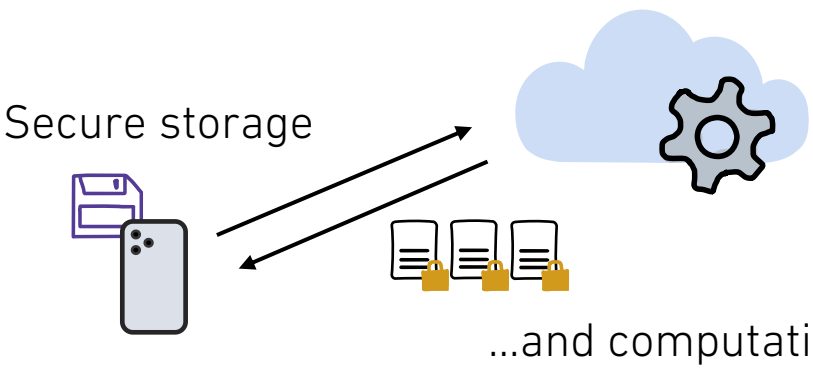


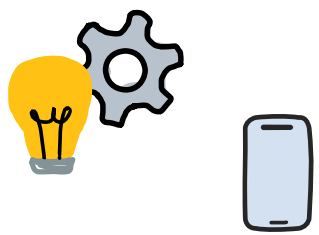


Secure?

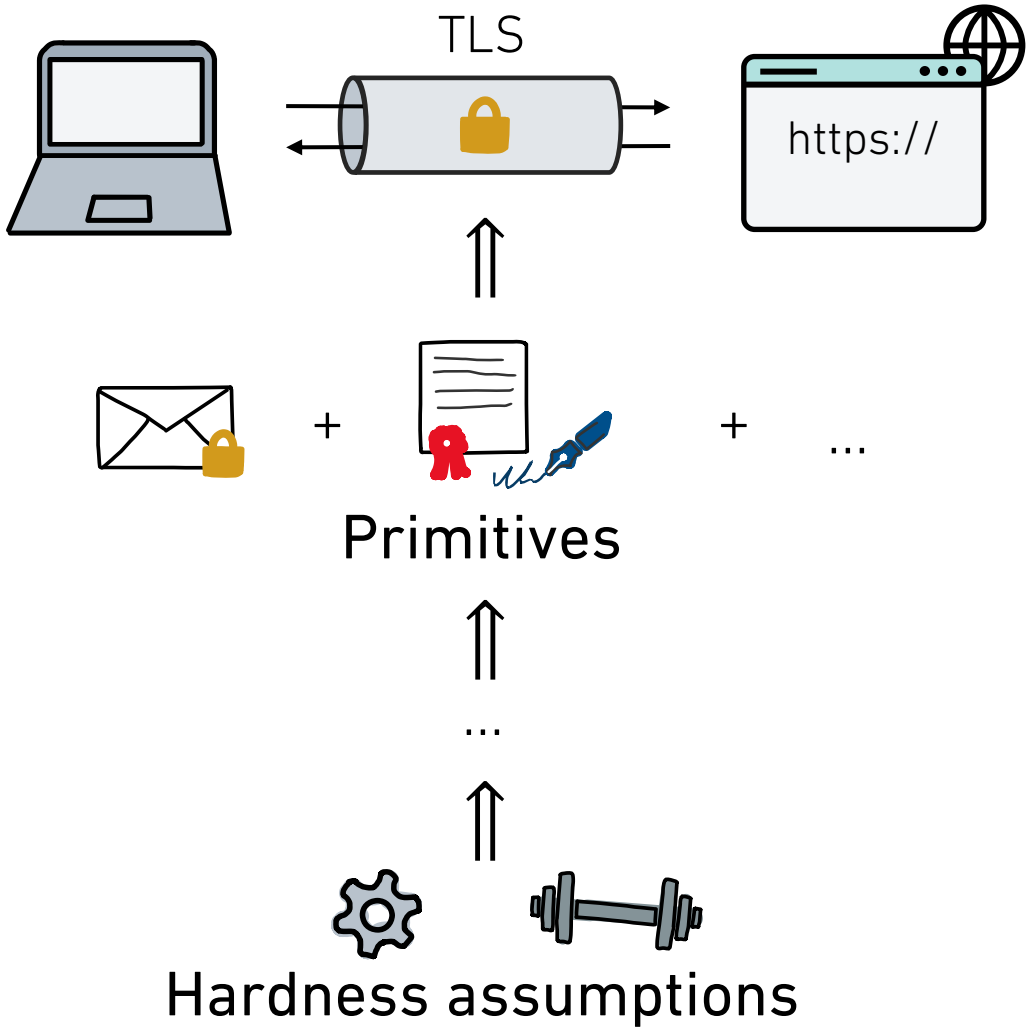




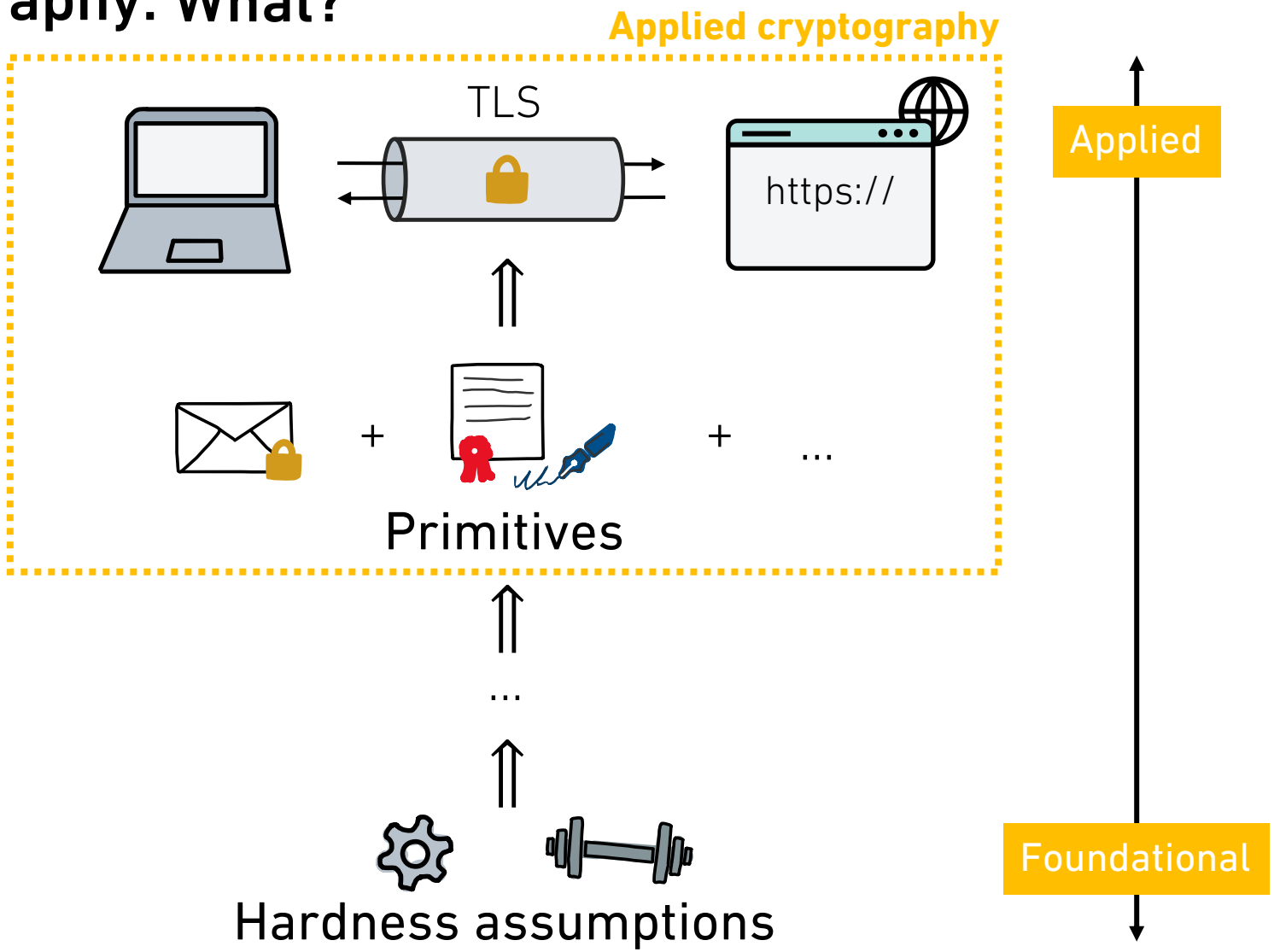


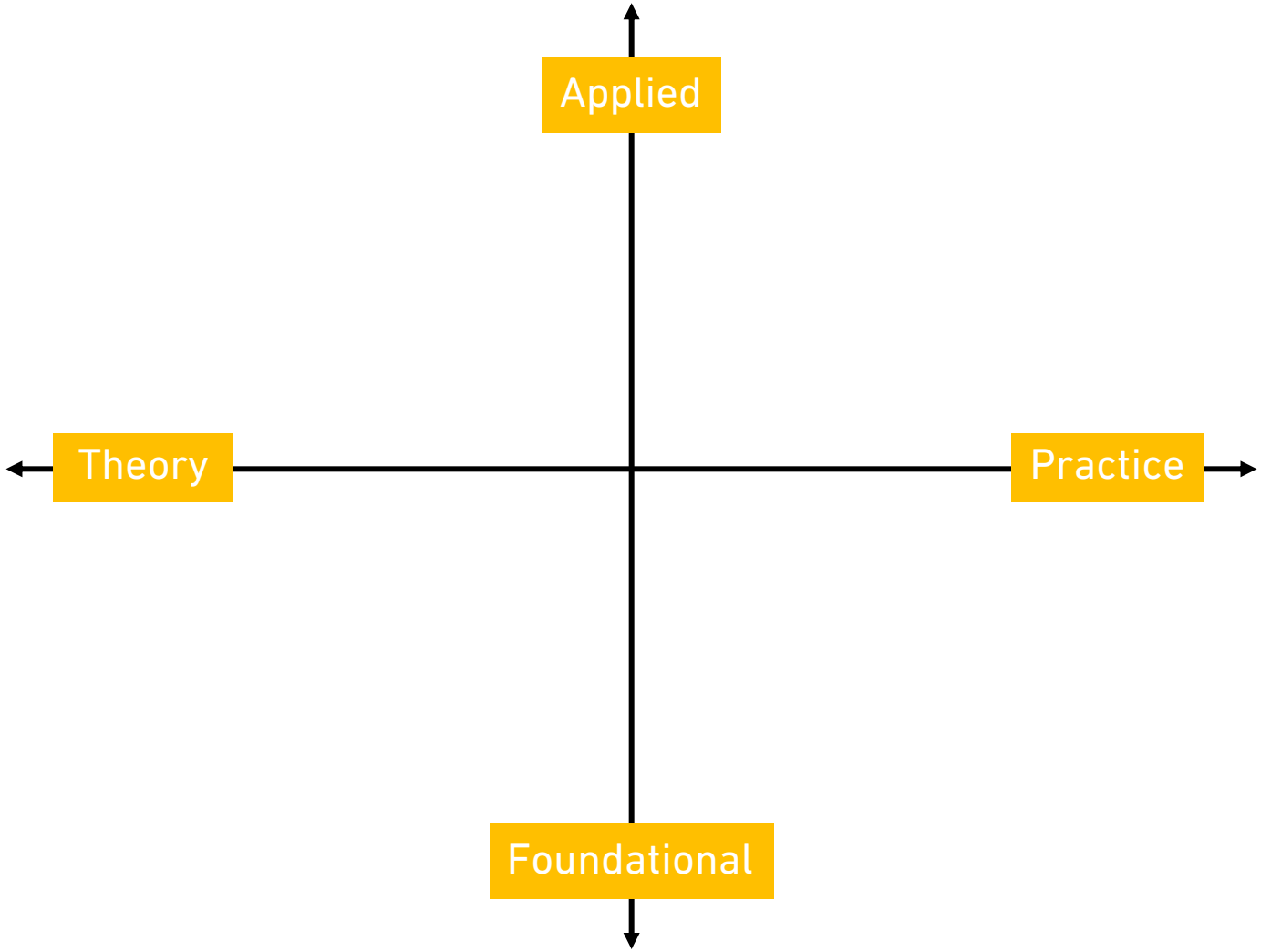


Applied Cryptography: How?

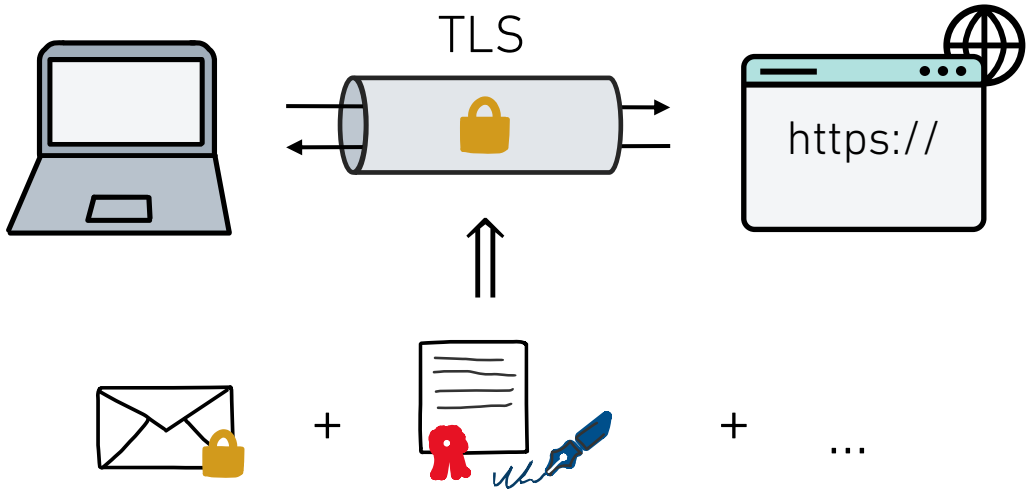


Applied Cryptography: What?




Applied
Theory
Practice
Foundational

Theory — Practice



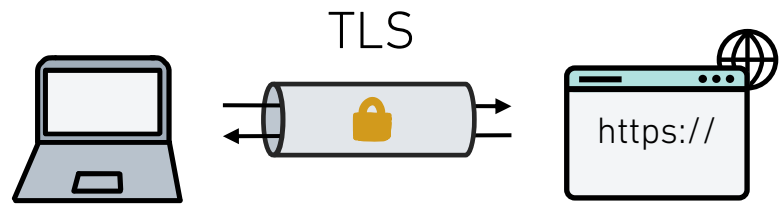
Primitives

...

Hardness assumptions

Theory

Practice

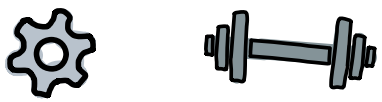


⇑

⇑

...

⇑



Hardness assumptions

Theory

Practice

Secure channel

System model

⇑

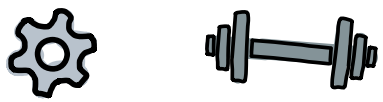
Models of primitives

AEAD

⇑

...

⇑



Hardness assumptions

TLS

Theory

Practice

Secure channel

System model

⇑

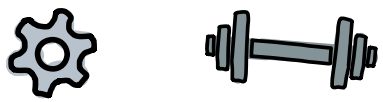
Models of primitives

AEAD

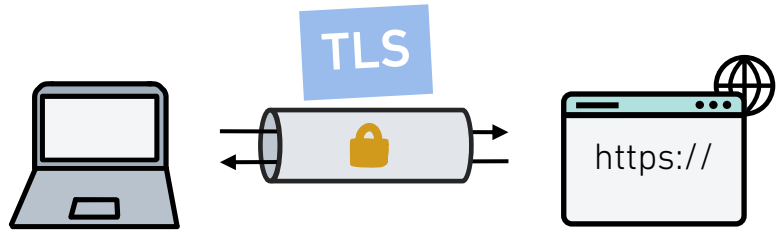
⇑

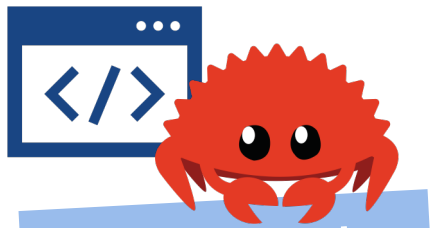
...

⇑

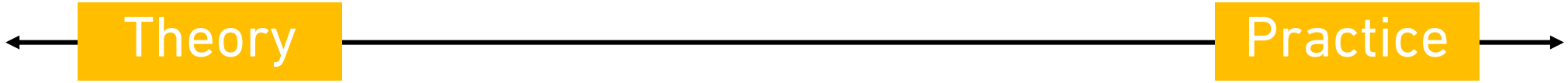


Hardness assumptions

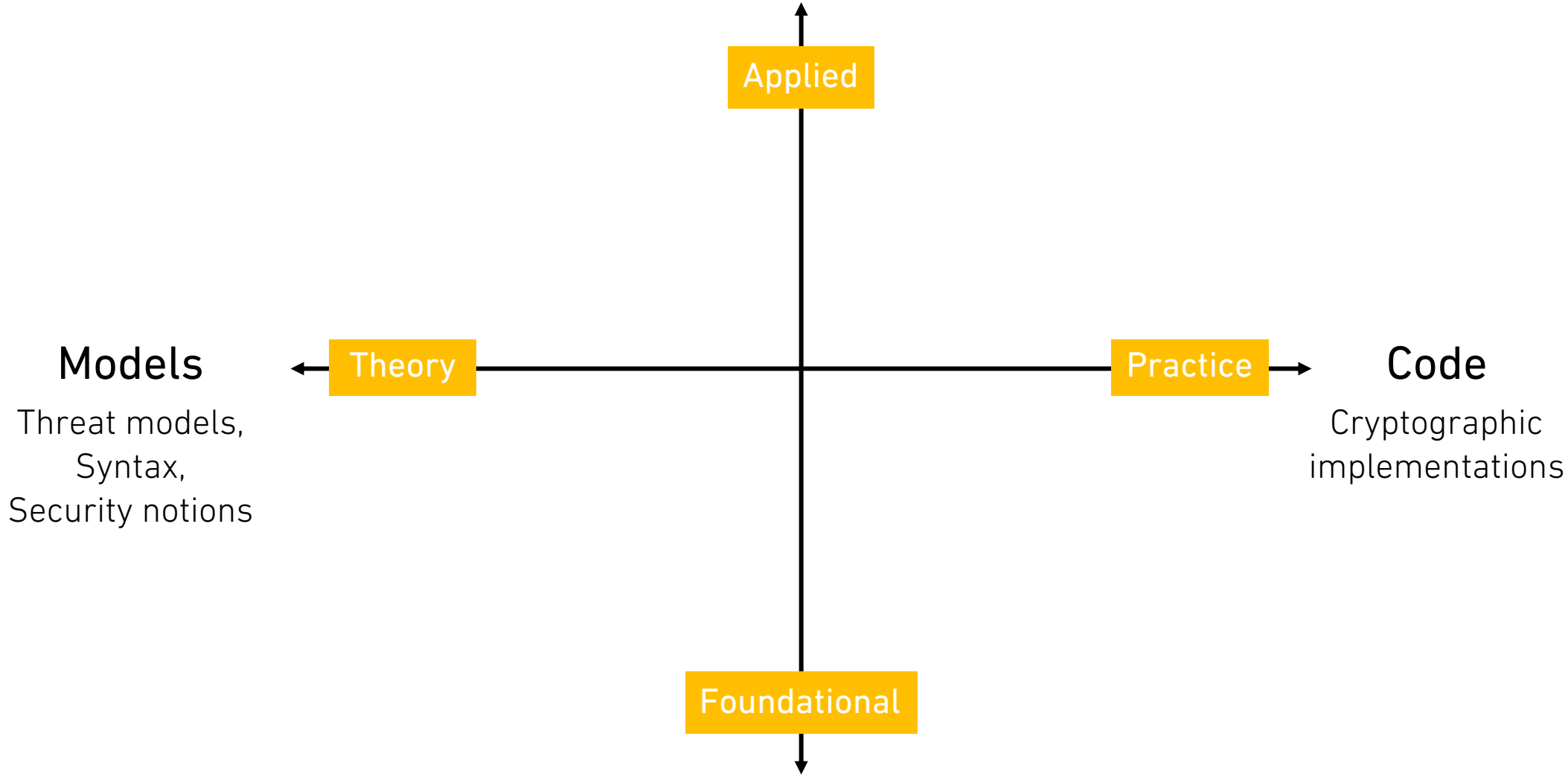




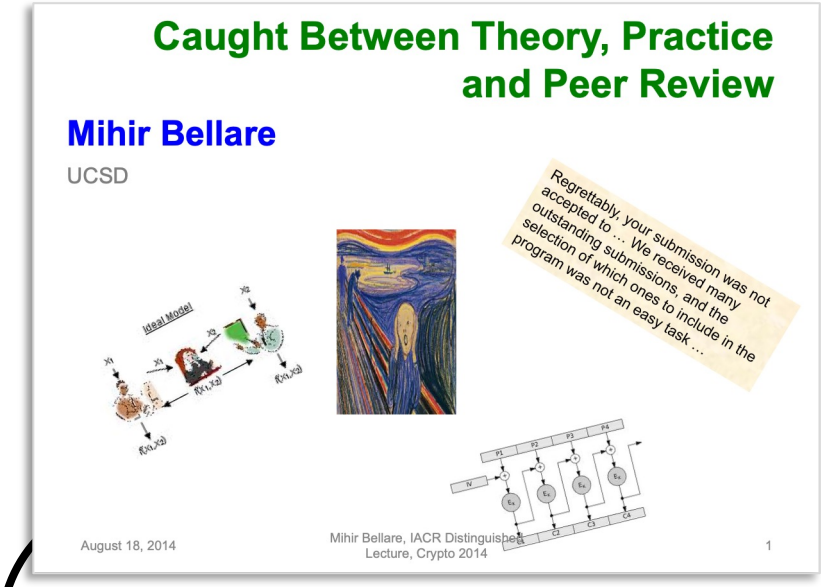
Implementation of AES-GCM in Rust


Theory
Practice

Applied Cryptography: What?



Applied Cryptography: What?



Mihir Bellare's "taxonomy of cryptographers"

Definitions

Proofs

Practice-to-Theory

Models

Threat models, Syntax, Security notions

Theory

Applied Cryptography

Practice

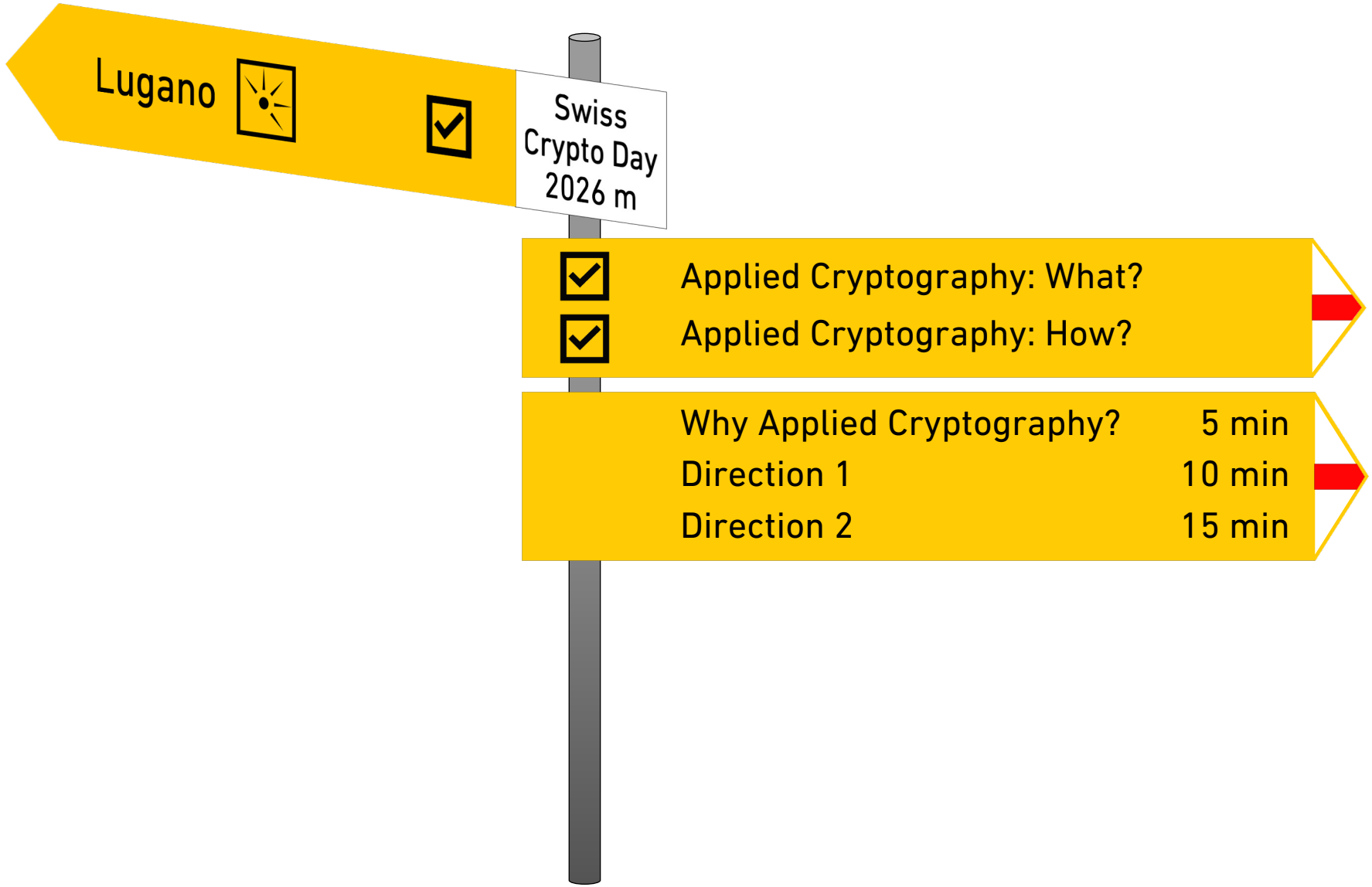
Code

Cryptographic implementations

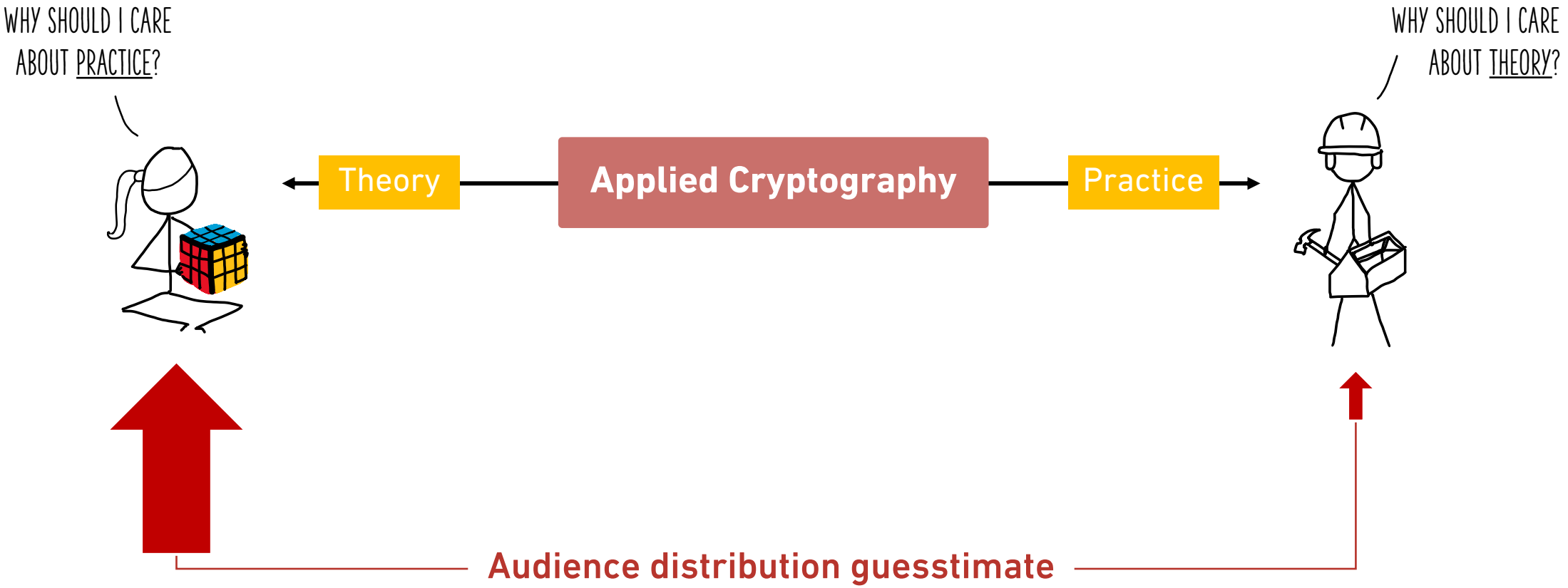
Attacks

Theory-to-Practice

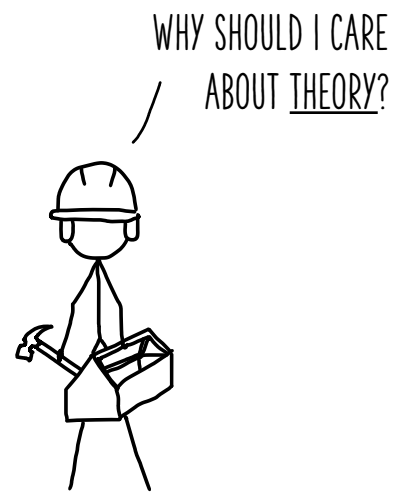
Security guarantees


Lugano
Swiss Crypto Day 2026 m
Applied Cryptography: What?
Applied Cryptography: How?
Why Applied Cryptography? 5 min
Direction 1 10 min
Direction 2 15 min

Why Applied Cryptography?

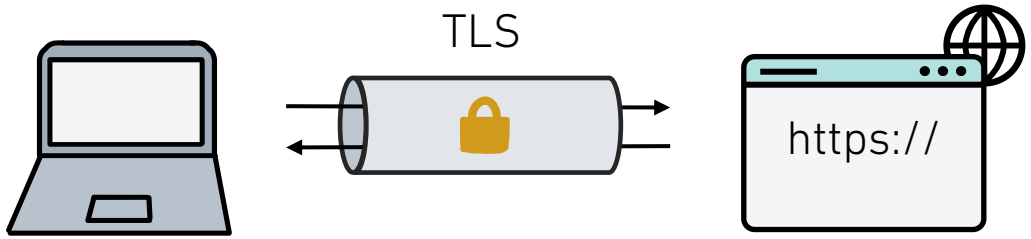


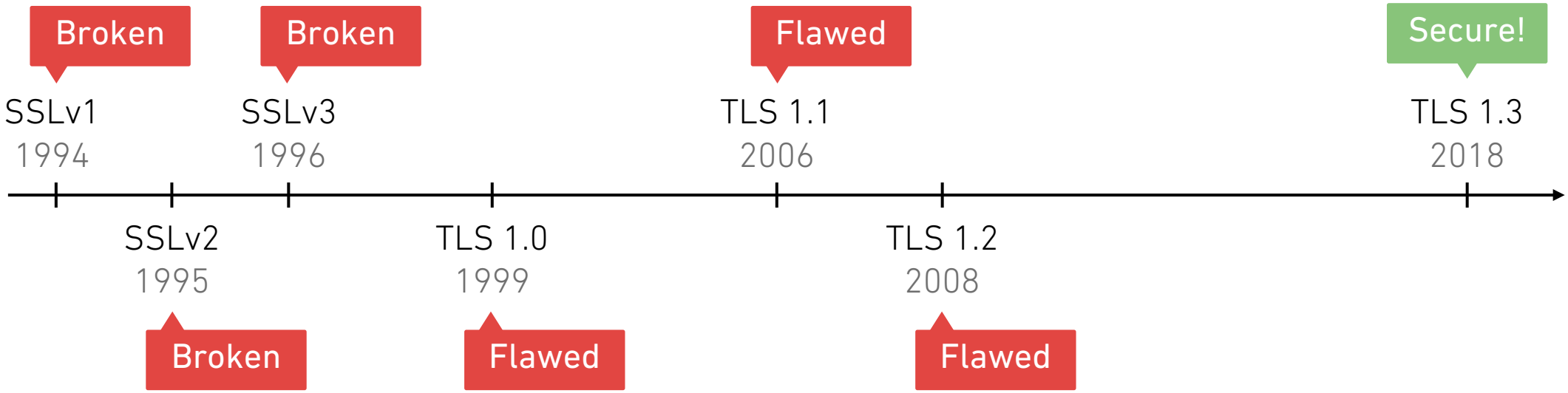
Why Theory?



TLS Saga Elevator Pitch

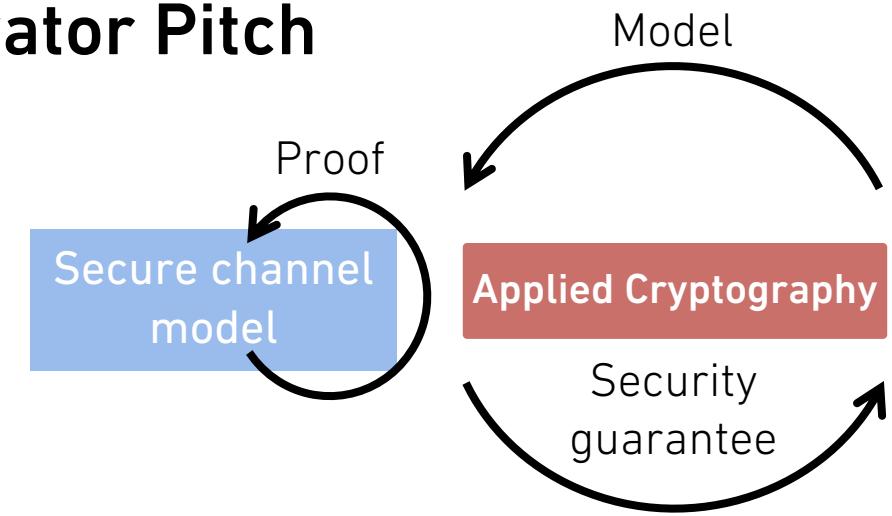
Why Theory?

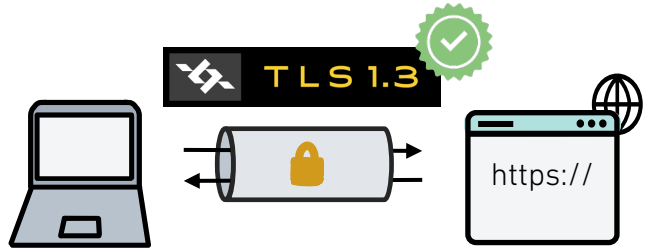


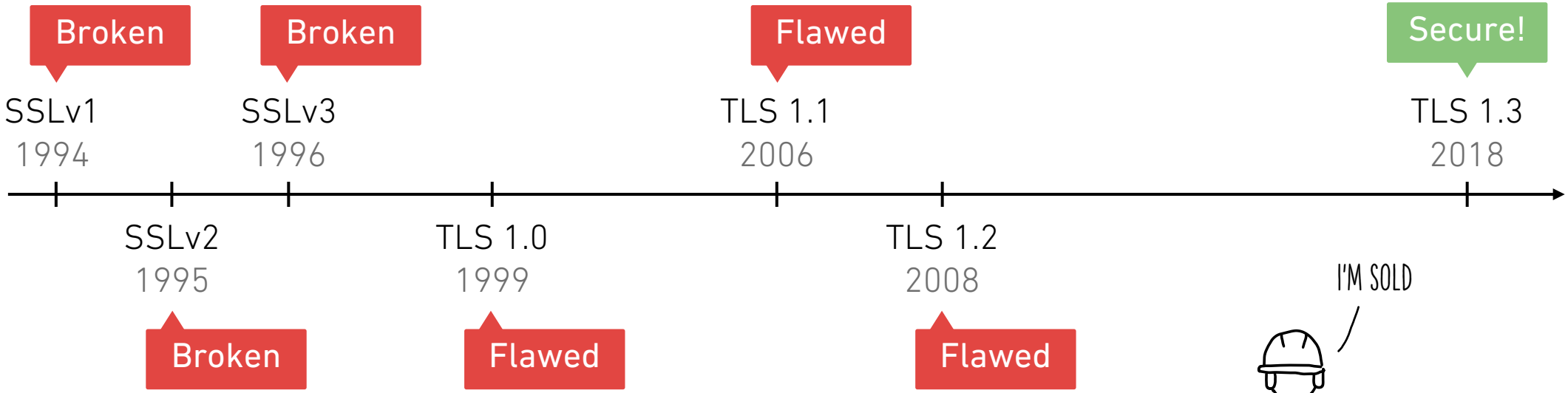


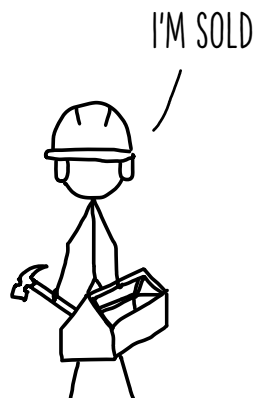
TLS Saga Elevator Pitch

Why Theory?

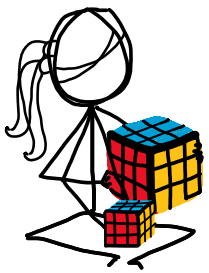






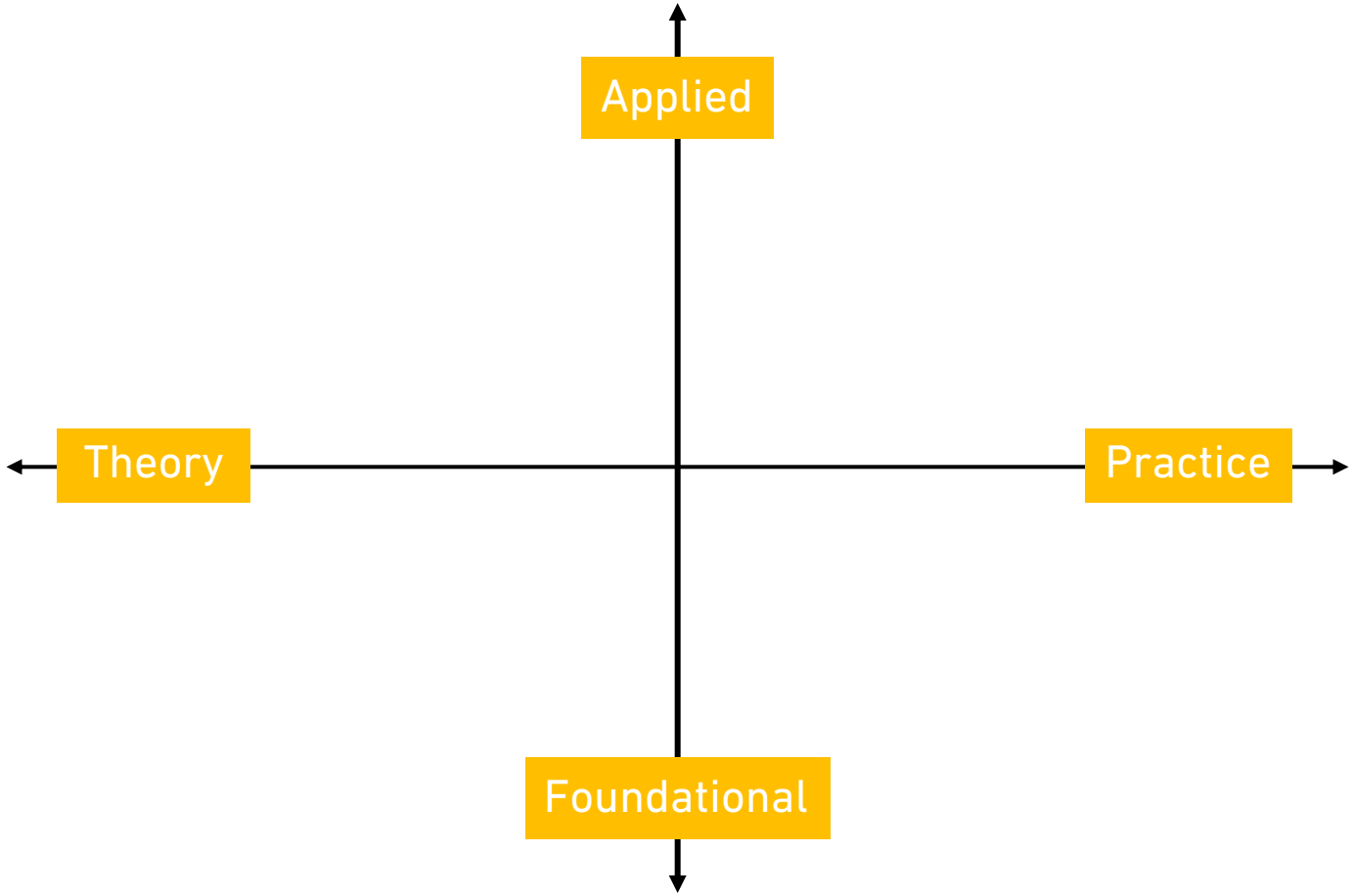


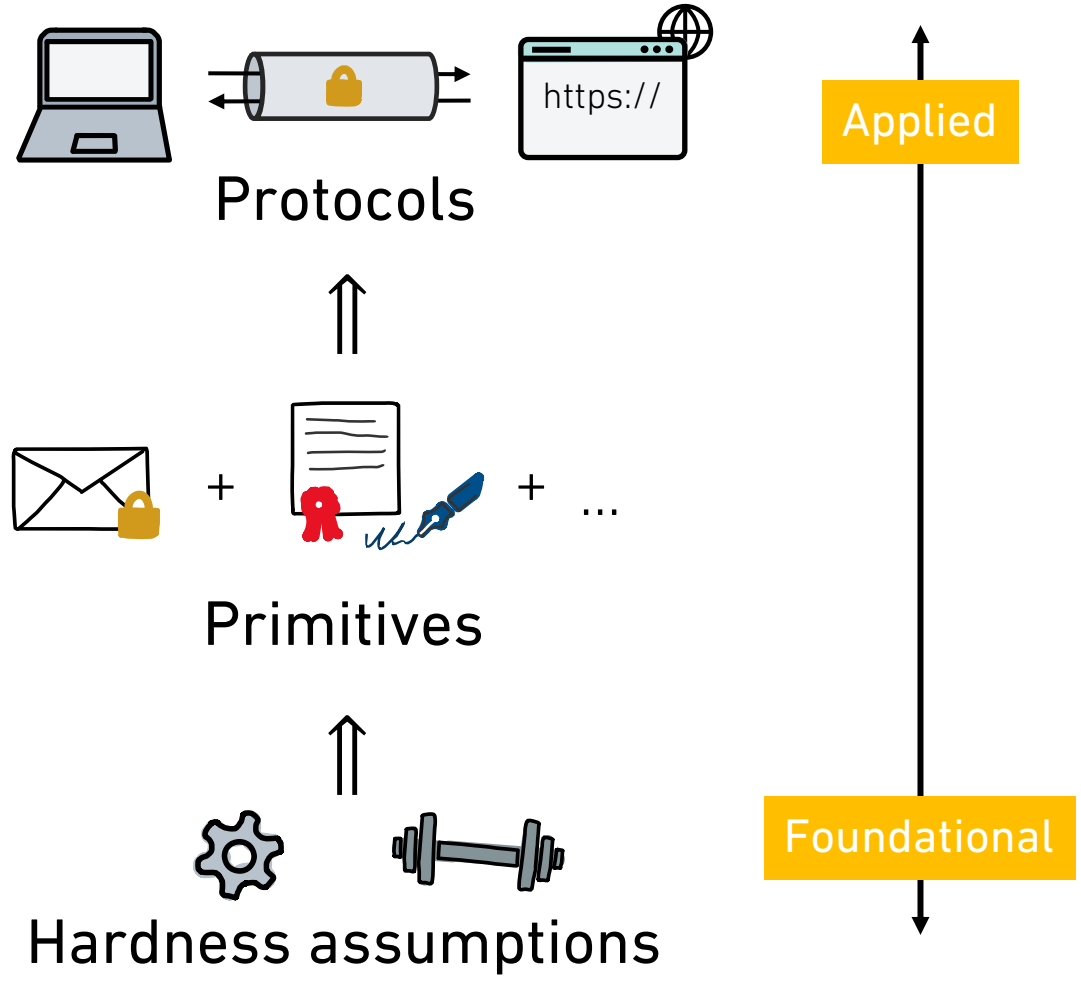
Why Practice?



Real-World Problems

$\Longrightarrow$ **Meaningful Research Directions**

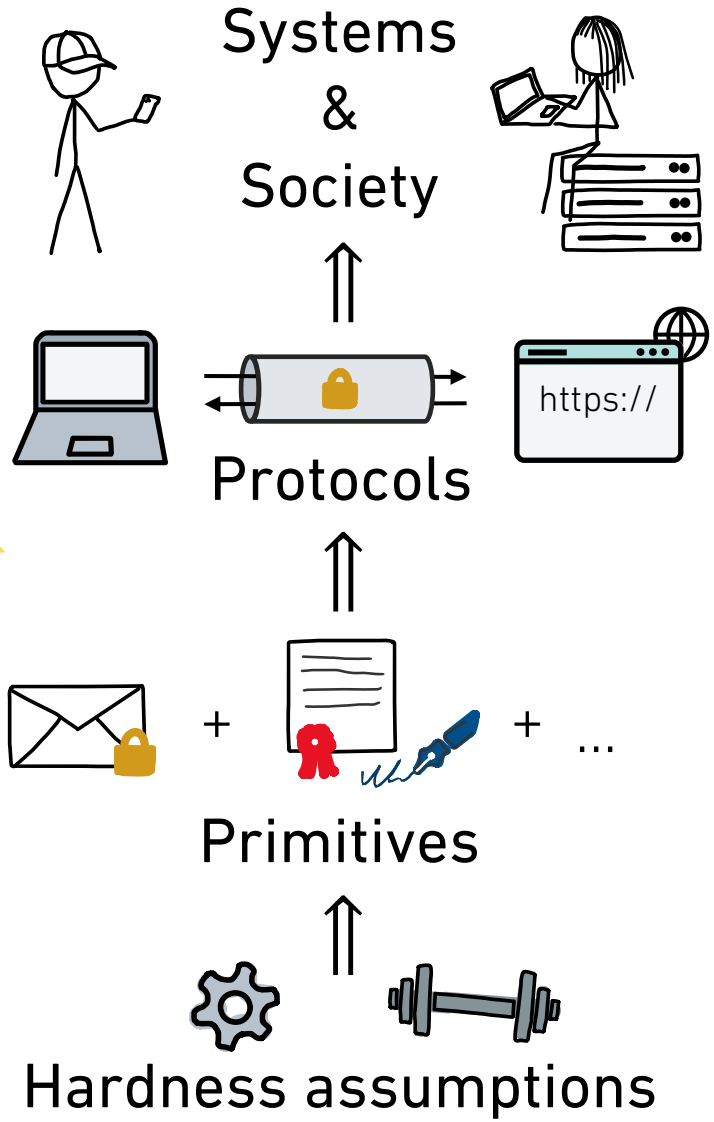

Applied
Theory
Practice
Foundational


https://
Protocols
+
+ ...
Primitives
Hardness assumptions
Applied
Foundational

Direction 1:

Socio-political cryptography

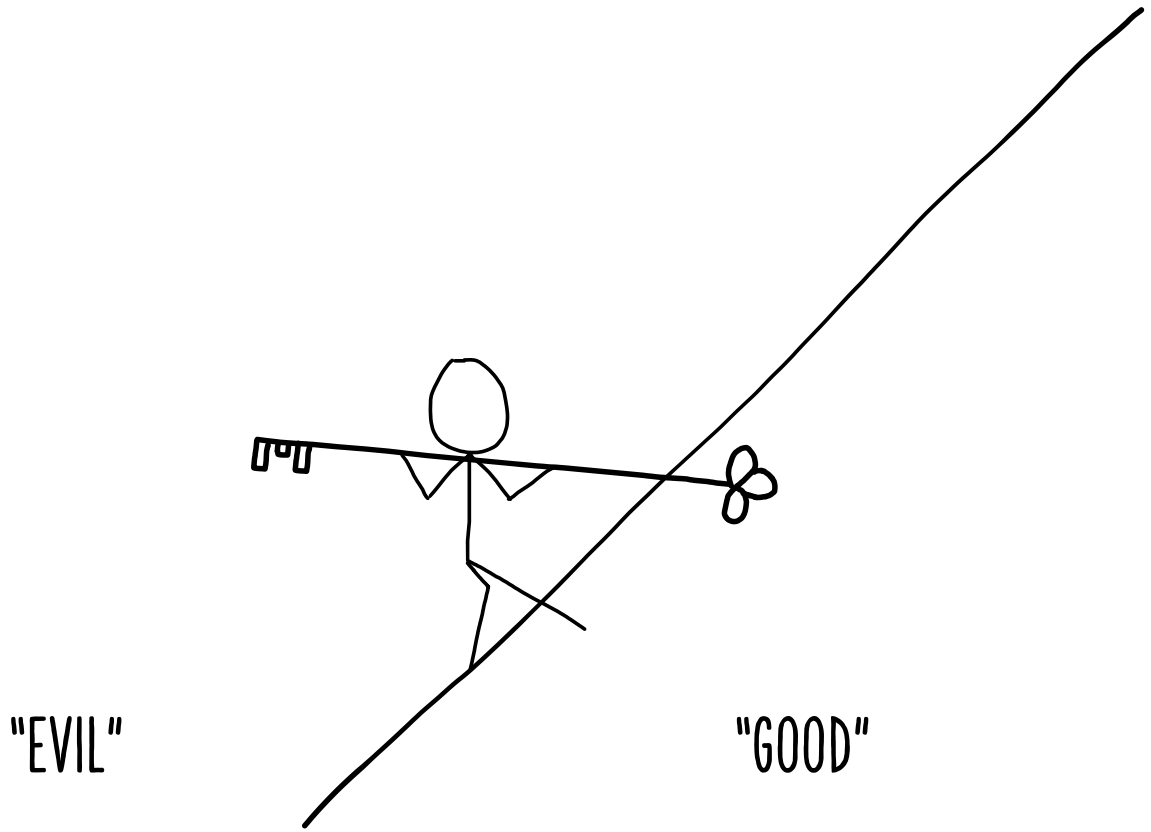
Crypto for people



Applied

Foundational

Cryptography Is a Balancing Act



The Moral Character of Cryptographic Work

The Moral Character of Cryptographic Work*

Phillip Rogaway

Department of Computer Science
University of California, Davis, USA
rogaway@cs.ucdavis.edu

December 2015
(minor revisions March 2016)

Abstract. Cryptography rearranges power: it configures who can do what, from what. This makes cryptography an inherently *political* tool, and it confers on the field an intrinsically *moral* dimension. The Snowden revelations motivate a reassessment of the political and moral positioning of cryptography. They lead one to ask if our inability to effectively address mass surveillance constitutes a failure of our field. I believe that it does. I call for a community-wide effort to develop more effective means to resist mass surveillance. I plead for a reinvention of our disciplinary culture to attend not only to puzzles and math, but, also, to the societal implications of our work.

Keywords: cryptography · ethics · mass surveillance · privacy · Snowden · social responsibility

Preamble. Most academic cryptographers seem to think that our field is a fun, deep, and politically neutral game—a set of puzzles involving communicating parties and notional adversaries. This vision of who we are animates a field whose work is intellectually impressive and rapidly produced, but also quite inbred and divorced from real-world concerns. Is this what cryptography *should* be like? Is it how we *should* expend the bulk of our intellectual capital?

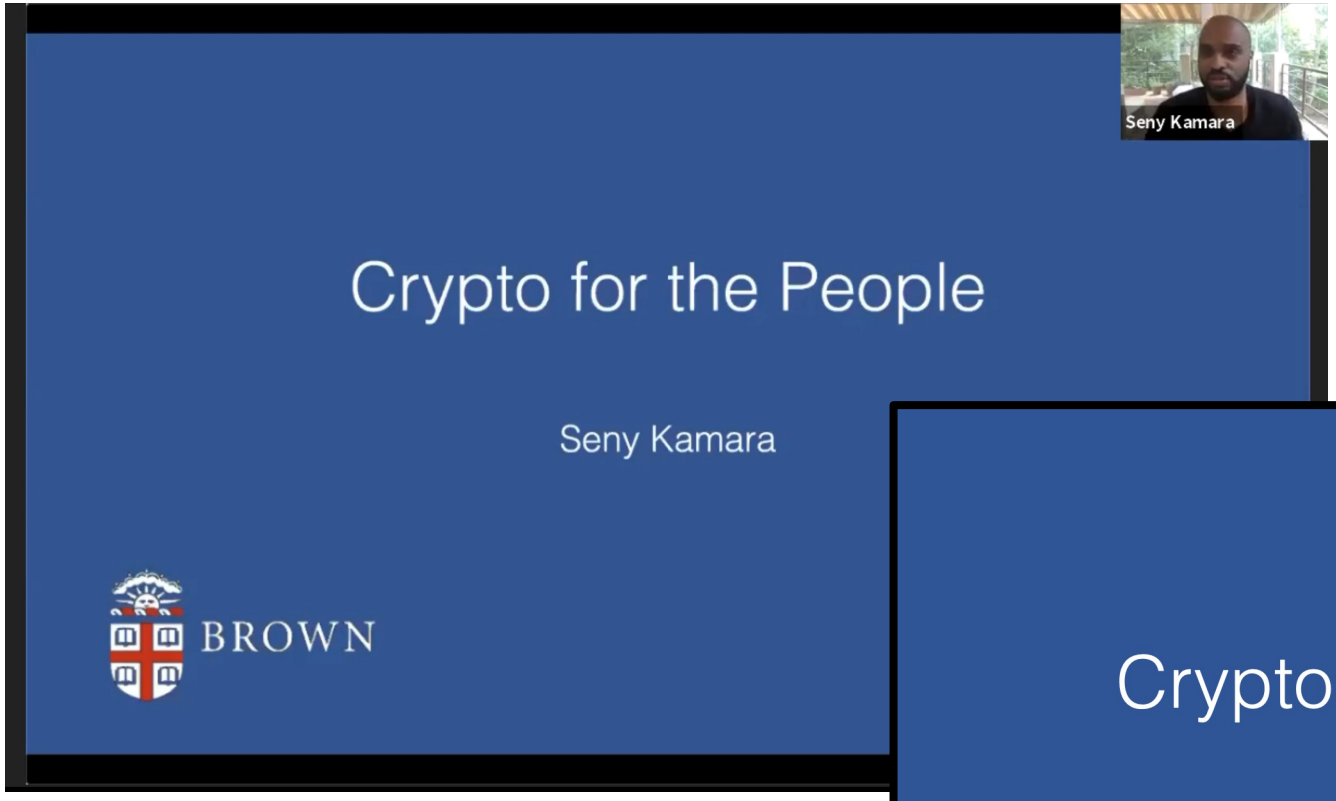
Suggestions:

- *Get a systems-level view.*
  Attend to that which surrounds our field.
- *Regard ordinary people as those whose needs you ultimately aim to satisfy.*
- *Be introspective about* **why** *you are working on the problems you are.*

Phillip Rogaway

"I think we should breathe,
write fewer papers,
and have them matter more."

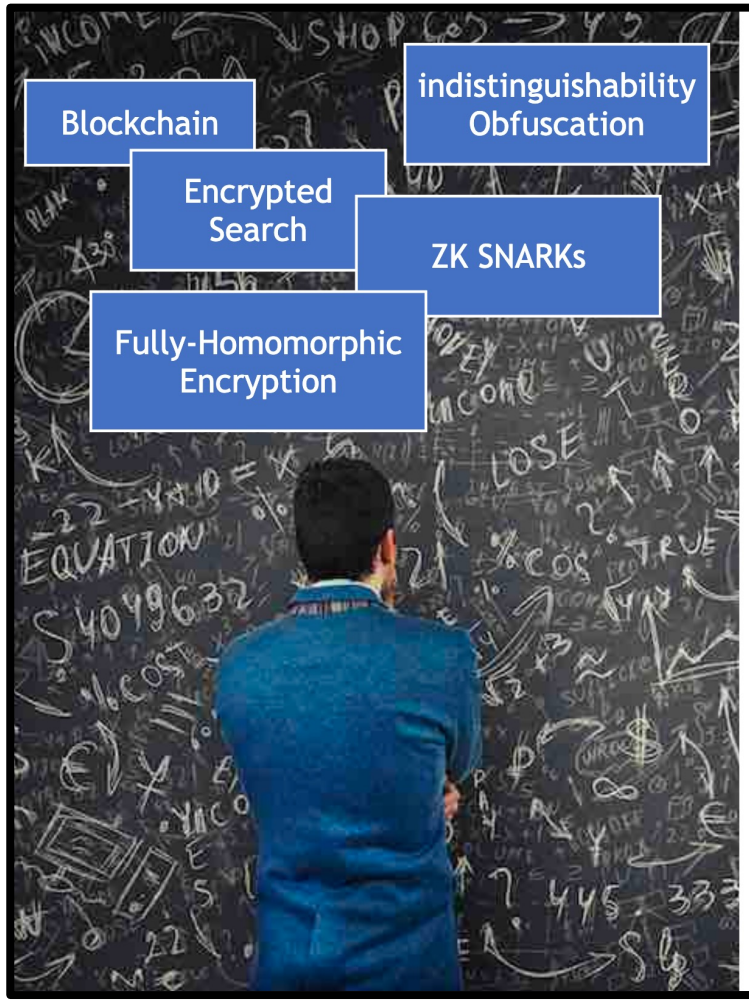
Crypto for the People



Invited talk at Crypto 2020

Keynote at Usenix Enigma 2022

Crypto for the People – Seny Kamara



- Bob likes fancy cryptography
- Bob notices people talking about
  - police violence
  - sexual harassment & assault
  - bias & discrimination in ML
  - misinformation in social networks
- Bob thinks
  - “I’ll use crypto to solve police violence!”

7

Slides by Seny Kamara:
https://www.senykamara.com/assets/pdf/enigma.pdf

Crypto for the People – Seny Kamara

Why is this a Problem?

- Bob is not really interested in the social problem
- Bob is interested in…
  - …*the crypto problem he claims is motivated by the social problem*
- While the crypto problem is “fun” it does not address the real problem
- Bob has a hammer and is looking for a “social nail”

8

Slides by Seny Kamara:
https://www.senykamara.com/assets/pdf/enigma.pdf

Crypto for the People – Seny Kamara

What Should Bob Do?

- If Bob genuinely cares about a social problem
- He should work with experts
  - experts in social sciences & humanities
  - experts with lived experience
- Lived experience is crucial because
  - the details really matter
  - the psychological state really matters
  - the broader context really matters

11

Slides by Seny Kamara:
https://www.senykamara.com/assets/pdf/enigma.pdf

Working with Experts with Lived Experience

SPRING
SECURITY AND PRIVACY ENGINEERING LABORATORY

Carmela Troncoso

> Privacy is not an end goal.
> It's a means to an end.

Working with Experts with Lived Experience

SPRING
SECURITY AND PRIVACY ENGINEERING LABORATORY

Carmela Troncoso

Not Yet Another Digital ID: Privacy-Preserving Humanitarian Aid Distribution

Boya Wang*, Wouter Lueks†, Justinas Sukaitis‡, Vincent Graf Narbel‡, Carmela Troncoso*
*SPRING Lab, EPFL, Lausanne, Switzerland
{boya.wang,carmela.troncoso}@epfl.ch
†CISPA Helmholtz Center for Information Security, Saarbrücken, Germany
lueks@cispa.de
‡International Committee of the Red Cross, Geneva, Switzerland
{jsukaitis,vgraf}@icrc.org

***Abstract*—Humanitarian aid-distribution programs help bring physical goods to people in need. Traditional paper-based solutions to support aid distribution do not scale to large populations and are hard to secure. Existing digital solutions solve these issues, at the cost of collecting large amount of personal information. This lack of privacy can endanger recipients' safety and harm their dignity. In collaboration with the International Committee of the Red Cross, we build a safe digital aid-distribution system. We first systematize the requirements such a system should satisfy. We then propose a decentralized solution based on the use of tokens that fulfills the needs of humanitarian organizations. It provides scalability and strong accountability, and, by design, guarantees the recipients' privacy. We provide two instantiations of our design, on a smart card and on a smartphone. We formally prove the security and privacy properties of these solutions, and empirically show that they can operate at scale.**

***Index Terms*—privacy-preserving technologies, privacy engineering, humanitarian aid distribution**

requires a deep understanding of the hun
We partner with the ICRC to learn the
constraints associated with distributing a
Our interactions reveal the following cha

1) *Secure household-oriented aid.* Aid-di must permit aid allocation per househo unit of several members sharing meal they must ensure that households ca once per distribution round (e.g., per
2) *Avoid reliance on powerful hardwa ity*. Most aid-distribution programs ta affected settings where we cannot ass of last-generation hardware or interne
3) *Auditability*. For accountability reason ganizations need to prove that aid is honest manner, i.e., only to legitimate
4) *Strong privacy.* Aid-distribution sys causing digital harm to the individual must avoid generating databases with r creating digital traces related to recipi

PARTNER WITH EXPERTS TO LEARN REQUIREMENTS

IDENTIFY INHERENT PRIVACY HARMS

On the (Privacy) Harms of the European Digital Identity Framework

Christian Knabenhans*
christian.knabenhans@epfl.ch
EPFL

Shannon Veitch*
shannon.veitch@inf.ethz.ch
ETH Zurich

Mathilde Raynal
mathilde.raynal@epfl.ch
EPFL

Theresa Stadler
theresa.stadler@epfl.ch
Swiss Data Science Center

Sylvain Chatel
sylvain.chatel@cispa.de
CISPA Helmholtz Center for Information Security

Wouter Lueks
lueks@cispa.de
CISPA Helmholtz Center for Information Security

Carmela Troncoso
carmela.troncoso@mpi-sp.org
EPFL, Max Planck Institute for Security and Privacy

Abstract

As digital identity systems gain traction around the world, many see privacy-enhancing technologies (PETs) as the key to ensuring safe deployment. We critically examine whether this is the case using the European Digital Identity Framework (EUDIF) as an example. We leverage techniques from cryptographic modeling to formally capture the necessary leakage of the functionality of the EUDIF and its proposed applications. Then, we develop a harm analysis methodology that illustrates, using harm trees, how this leakage — and other constraints stemming from design decisions or the context of deployment — lead to harms. Moreover, our harm modeling enables us to distinguish between which pathways to harm are inherent to the core functionality, and which pathways can be prevented with PETs. Our analysis shows that, while PETs can reduce information flows, they fall short in mitigating the harms that deploying digital identity can bring to individuals and society.

While the broad deployment of DIFs is anticipated to bring many benefits, civil society has raised concerns about its potential negative impact on certain user groups, such as the exacerbation of structural exclusion or the risk of discrimination [18, 50, 61]. The main response put forward by its proponents to these concerns has been to strictly follow "privacy-by-design" principles and the use of privacy-enhancing technologies (PETs) in the EUDIF's design and development [12, 29, 31]. For example, following feedback from cryptographers [9], the EUDIF implementation recommendations include the use of anonymous credentials. These and other privacy safeguards are often portrayed as a sufficient step to mitigate harms that might arise from the EUDIF's deployment. In this paper, we take a step back and ask whether privacy and PETs are indeed an appropriate answer to concerns about the EUDIF's negative societal impacts. We identify harms that are inherent to the EUDIF and its proposed applications (and any DIF with similar characteristics), and demonstrate that PETs cannot fully protect users from these harms. We make the following contributions.

Keywords

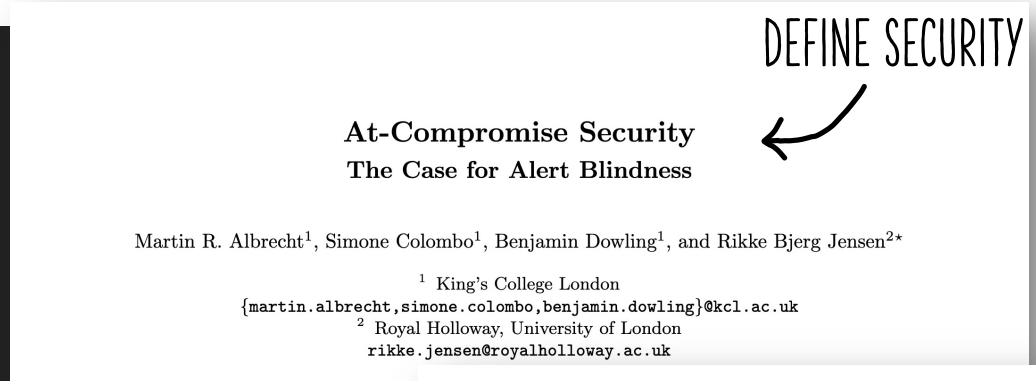
Working with Experts in Humanities

USE ETHNOGRAPHY TO DEFINE SECURITY GOALS

Social Foundations of Cryptography

Ethnography unearths what the group (under study) takes for granted.

https://social-foundations-of-cryptography.gitlab.io/

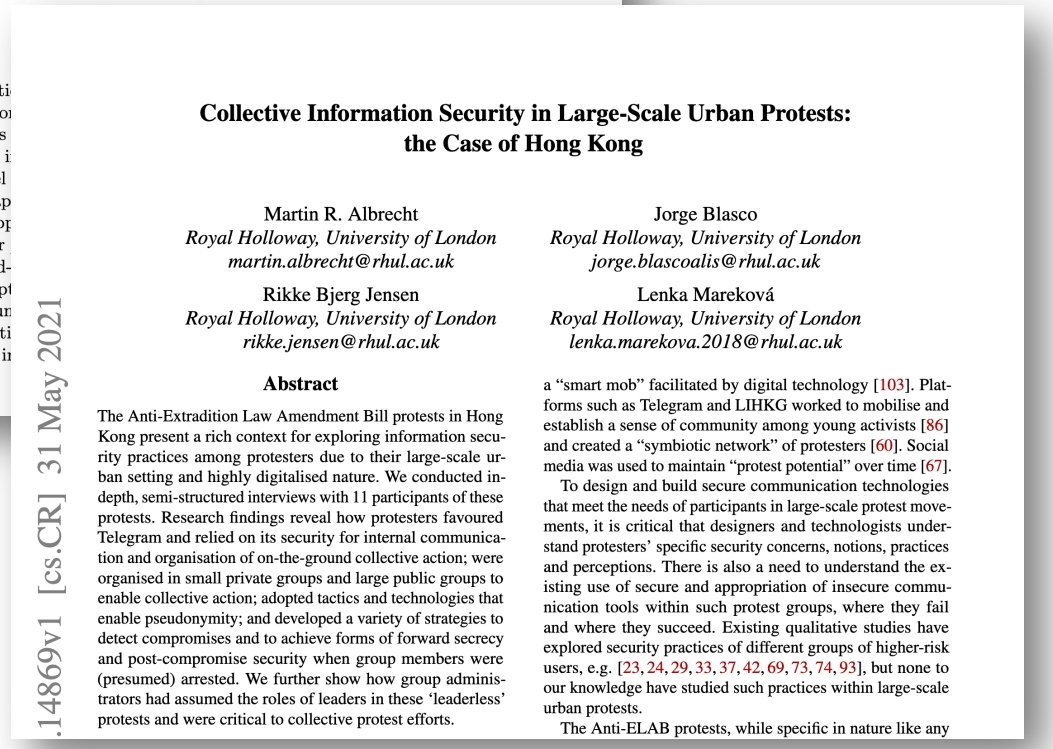


At-Compromise Security
The Case for Alert Blindness

Martin R. Albrecht[1], Simone Colombo[1], Benjamin Dowling[1], and Rikke Bjerg Jensen[2⋆]

[1] King's College London
{martin.albrecht,simone.colombo,benjamin.dowling}@kcl.ac.uk
[2] Royal Holloway, University of London
rikke.jensen@royalholloway.ac.uk

Abstract We start from the observati
– as modelled in games or ideal functio
tography's attentive approach towards
and reductions. To close this gap, we i
games and ideal functionalities model
parties, our methodology is ethnograp
lations in their contexts. As a first ap
study security *at-compromise* (neither
Specifically, in our 2024/2025 six-and-
we observed that alert blindness capt
Kenyan security forces for their presu
assumptions by providing a constructi
construction with some interlocutors i



Collective Information Security in Large-Scale Urban Protests: the Case of Hong Kong

Martin R. Albrecht
Royal Holloway, University of London
martin.albrecht@rhul.ac.uk

Jorge Blasco
Royal Holloway, University of London
jorge.blascoalis@rhul.ac.uk

Rikke Bjerg Jensen
Royal Holloway, University of London
rikke.jensen@rhul.ac.uk

Lenka Mareková
Royal Holloway, University of London
lenka.marekova.2018@rhul.ac.uk

Abstract

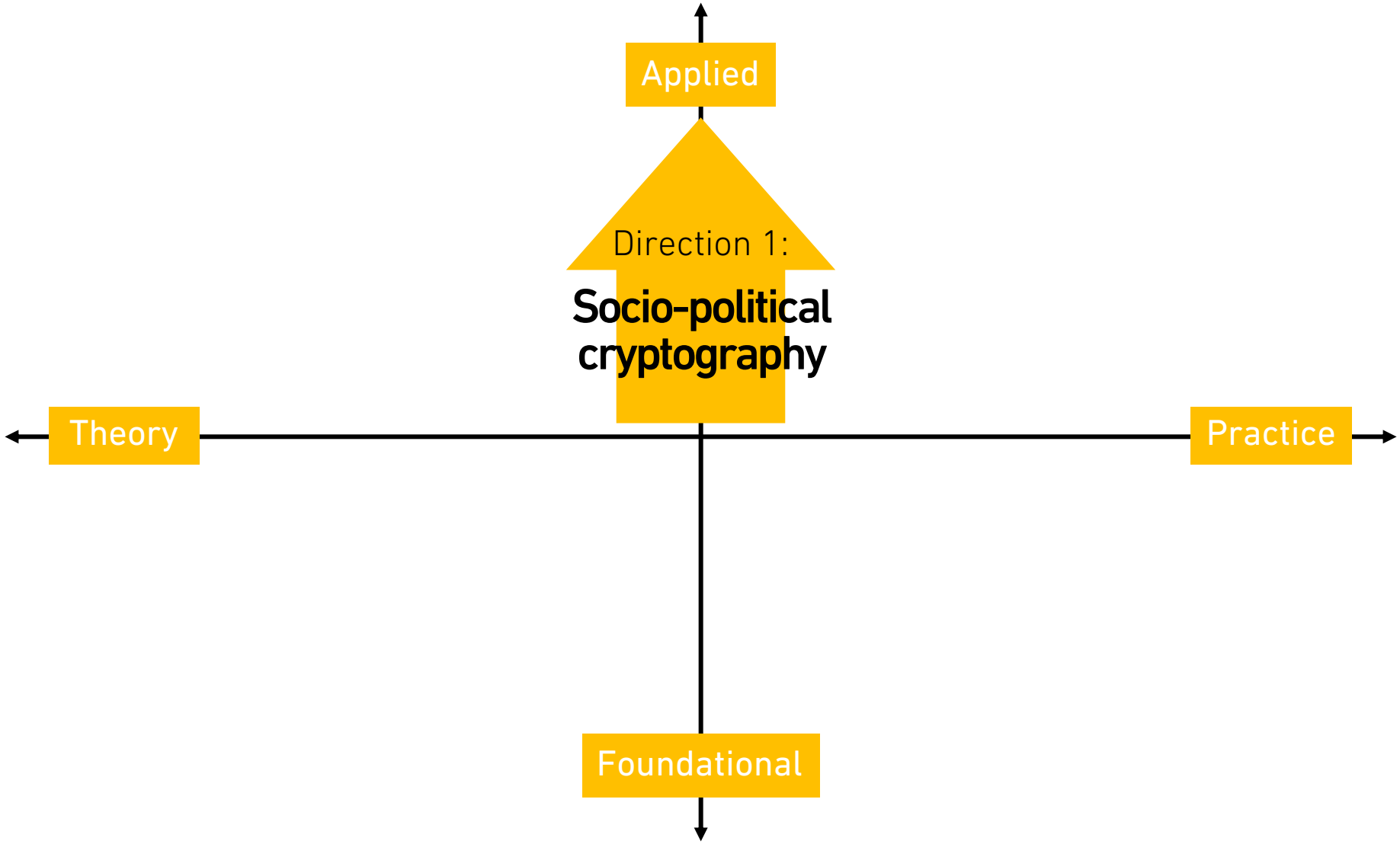
The Anti-Extradition Law Amendment Bill protests in Hong Kong present a rich context for exploring information security practices among protesters due to their large-scale urban setting and highly digitalised nature. We conducted in-depth, semi-structured interviews with 11 participants of these protests. Research findings reveal how protesters favoured Telegram and relied on its security for internal communication and organisation of on-the-ground collective action; were organised in small private groups and large public groups to enable collective action; adopted tactics and technologies that enable pseudonymity; and developed a variety of strategies to detect compromises and to achieve forms of forward secrecy and post-compromise security when group members were (presumed) arrested. We further show how group administrators had assumed the roles of leaders in these 'leaderless' protests and were critical to collective protest efforts.

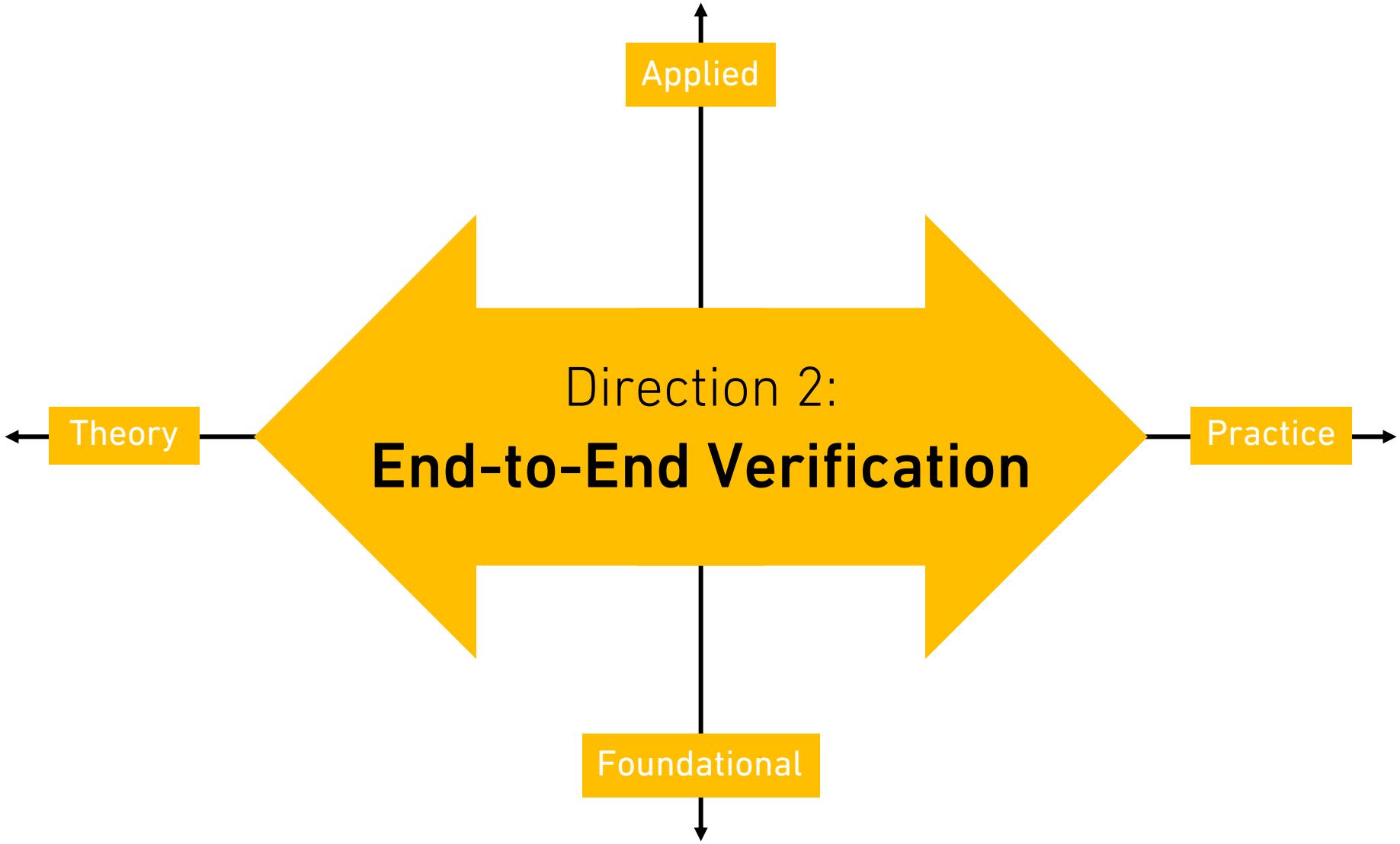
a "smart mob" facilitated by digital technology [103]. Platforms such as Telegram and LIHKG worked to mobilise and establish a sense of community among young activists [86] and created a "symbiotic network" of protesters [60]. Social media was used to maintain "protest potential" over time [67].

To design and build secure communication technologies that meet the needs of participants in large-scale protest movements, it is critical that designers and technologists understand protesters' specific security concerns, notions, practices and perceptions. There is also a need to understand the existing use of secure and appropriation of insecure communication tools within such protest groups, where they fail and where they succeed. Existing qualitative studies have explored security practices of different groups of higher-risk users, e.g. [23, 24, 29, 33, 37, 42, 69, 73, 74, 93], but none to our knowledge have studied such practices within large-scale urban protests.

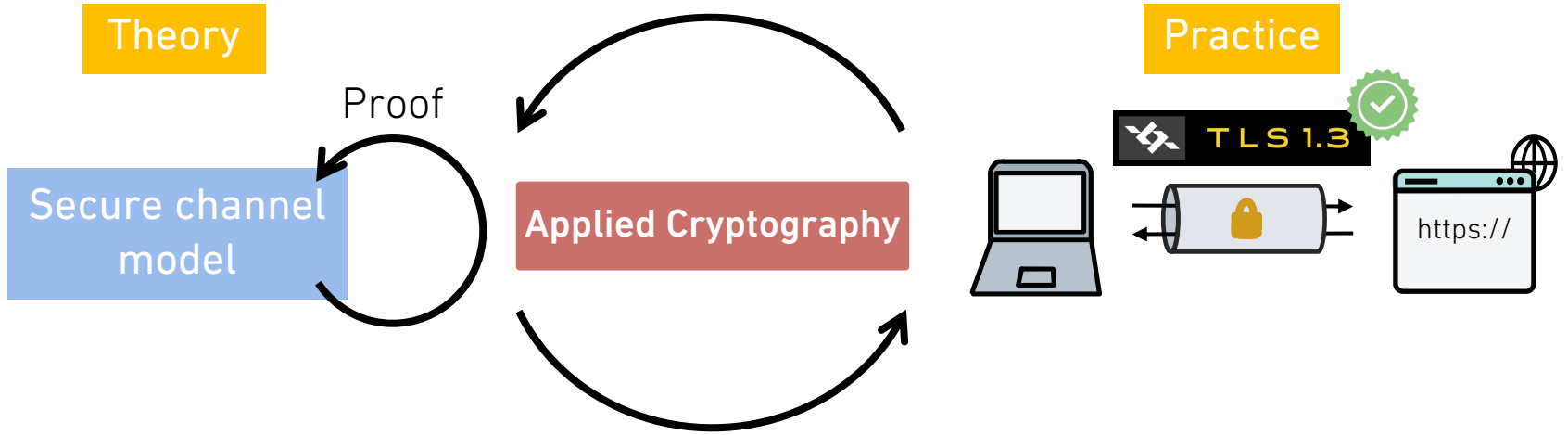
The Anti-ELAB protests, while specific in nature like any

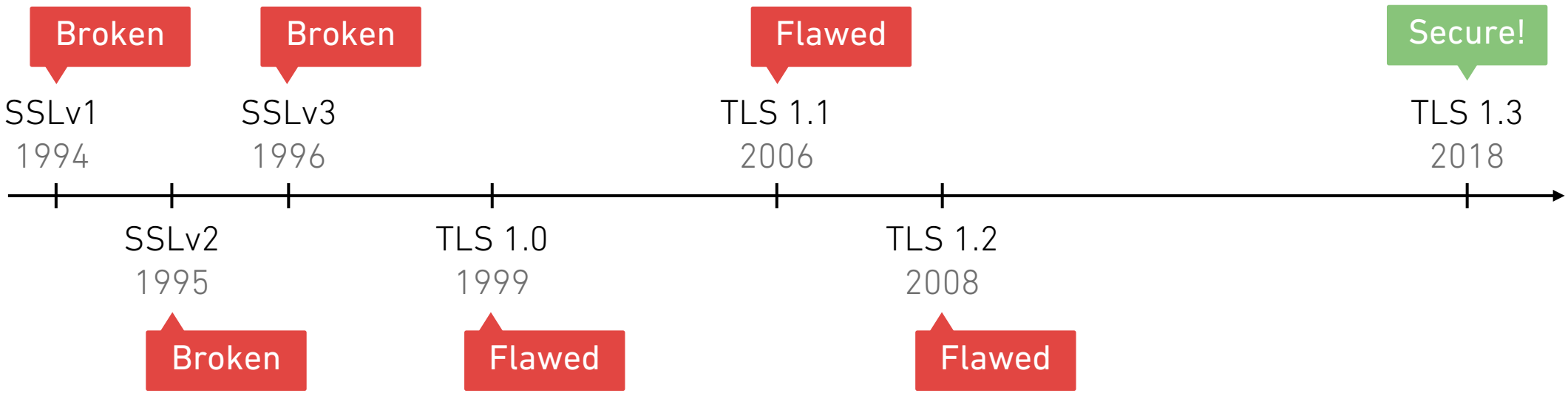
Martin Albrecht, Rikke Bjerg Jensen
Ben Dowling, Andrea Medrado
Keye Tersmette, Mikaela Brough
Samuel Light, Simone Colombo
Mbabazi A. Ntezi, Kirill Kutsenok


Applied
Direction 1:
Socio-political cryptography
Theory
Practice
Foundational


Applied
Theory
Direction 2:
End-to-End Verification
Practice
Foundational

TLS Saga


Theory
Proof
Secure channel model
Applied Cryptography
Practice
TLS 1.3
https://


Broken
Broken
Flawed
Secure!
SSLv1
1994
SSLv3
1996
TLS 1.1
2006
TLS 1.3
2018
SSLv2
1995
TLS 1.0
1999
TLS 1.2
2008
Broken
Flawed
Flawed

Signal Saga*

Signal

Secure messenger

*Highly simplified

Signal protocol & app developed
~2013-2016

2017
"A Formal Security Analysis of the Signal Messaging Protocol"
Cohn-Gordon, Cremers, Dowling, Garratt, Stebila
EURO S&P'17
Security proof

Secure!
Alwen, Coretti, Dodis
EUROCRYPT'19
2019

Chase, Perrin, Zaverucha
CCS'20
2020
Secure!

2022
Bienstock et al.
CRYPTO'22
Secure!

Cremers, Jacomme, Naska
USENIX'23
Attack

Secure!
Bhargavan et al.
USENIX'24
2024

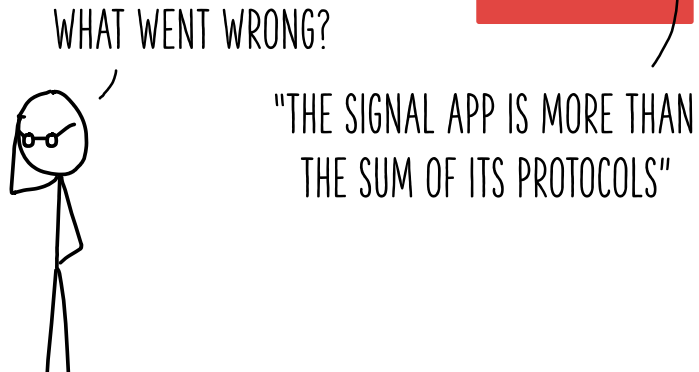
Secure!
Fiedler, Günther
PKC'25

Secure!
Jaeger, Kumar
EUROCRYPT'25

2025

Attack
Cheval, Jacomme, Richards
S&P'26

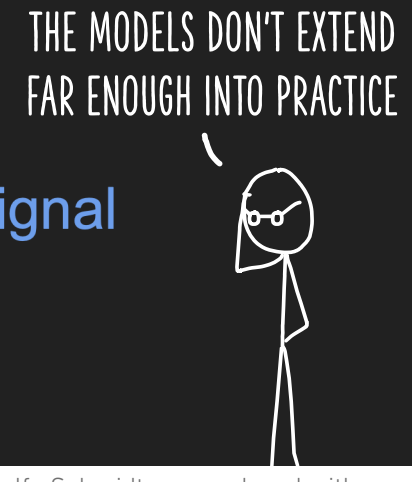
2026
Truong, Terzo, Paterson
USENIX'26
Attack



The Signal Protocol is Proven Secure

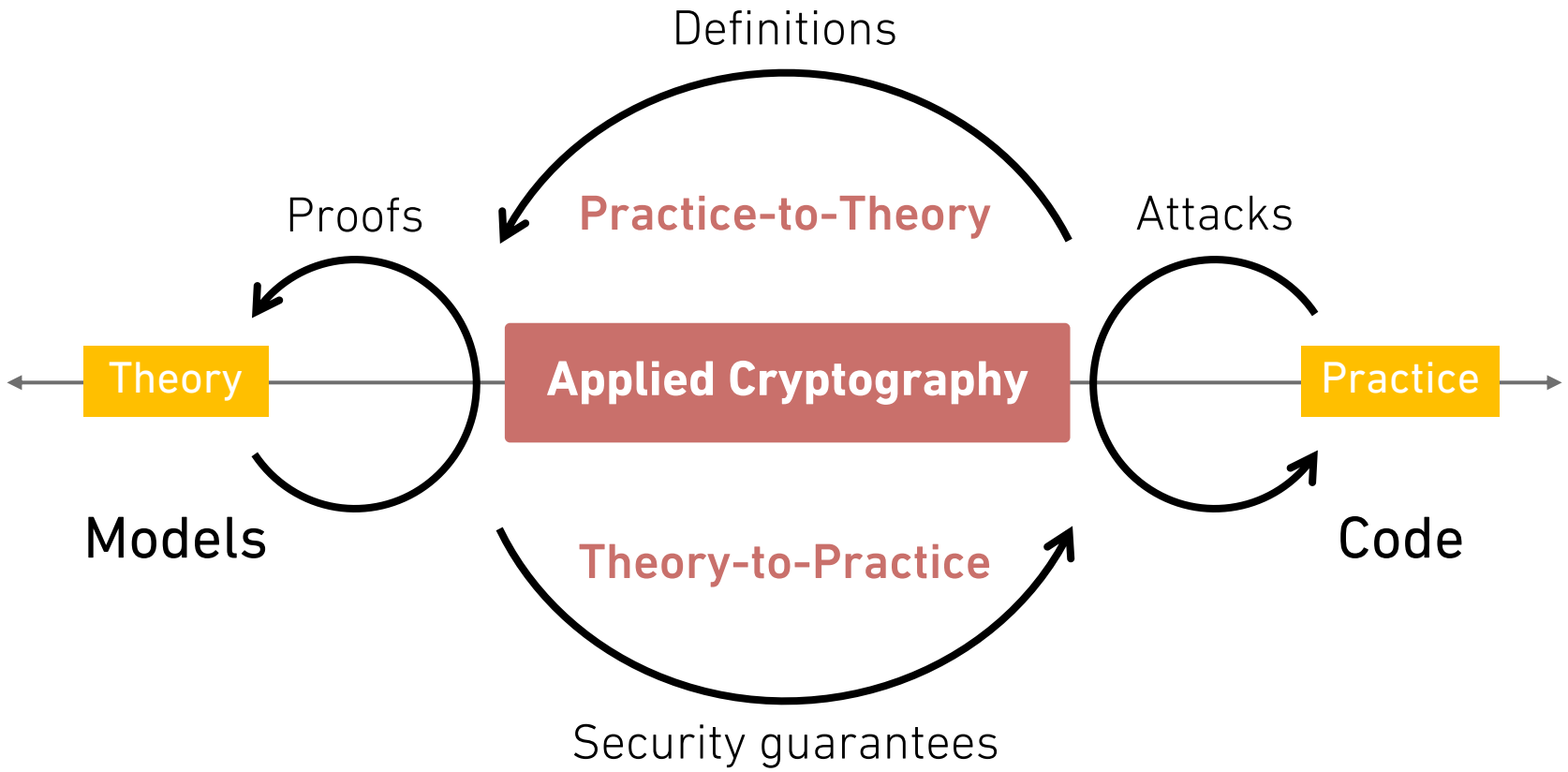
What Could Go Wrong?

Rolfe Schmidt | SKECH ✧ Bertinoro ✧ 2026 | Signal

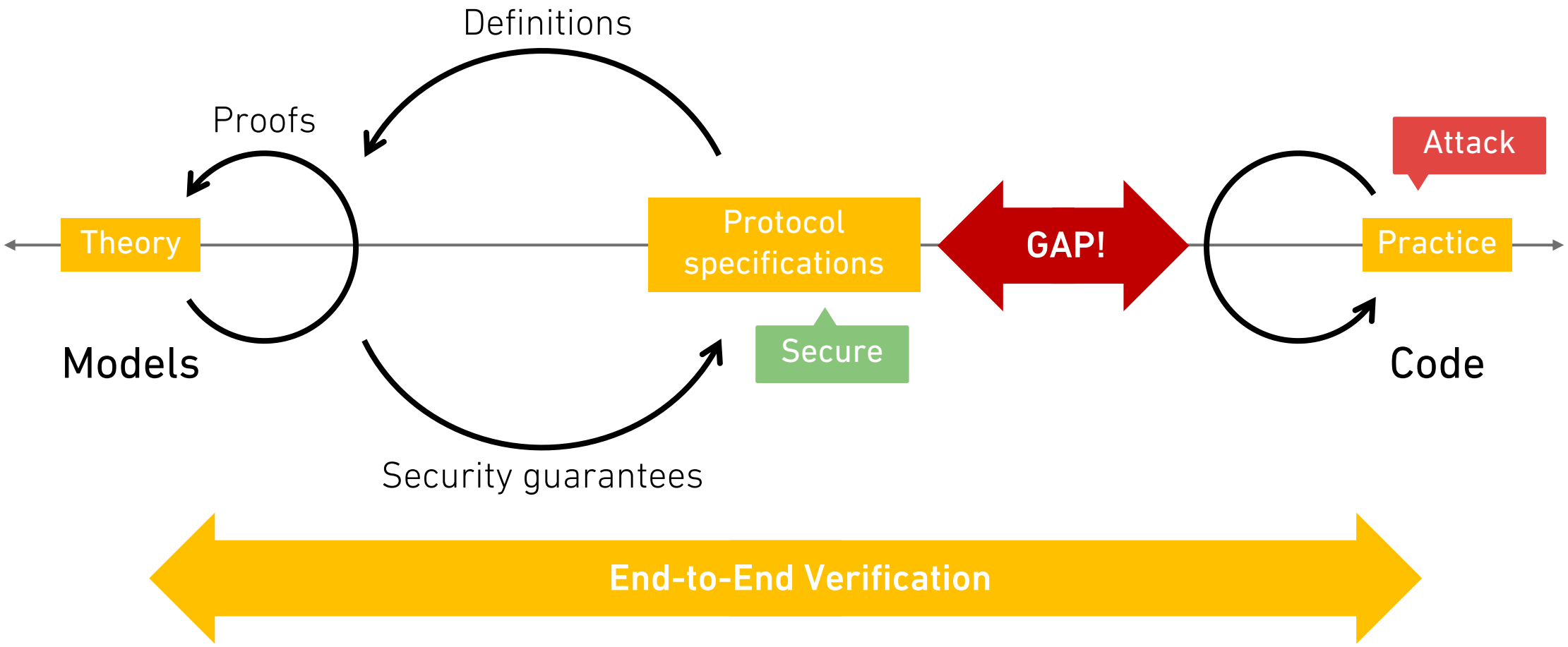


Slide by Rolfe Schmidt – reproduced with permission

The Gap Between Theory and Practice



The Gap Between Theory and Practice



Bridging the Gap

VERIFICATION FOR GAME-HOPPING PROOFS

ProofFrog

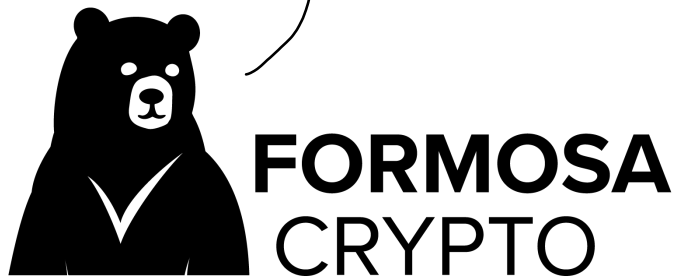
https://prooffrog.github.io/

COMPUTER-AIDED CRYPTOGRAPHIC PROOFS

EasyCrypt

https://easycrypt.gitlab.io
/easycrypt-web/

MACHINE-CHECKED,
HIGH-ASSURANCE CRYPTOGRAPHY



Formosa Crypto

https://formosa-crypto.org/

1 Write fewer papers

but with more purpose

2 Work with experts:

social scientists and users

Bridging the Gap Between Theory and Practice

We need

1 Attacks

to know where the gap is

2 E2E verification

to close the gap

This is an (exciting) open research direction!

Thanks to Giovanni & Mo for the photos!

End of the talk

Crypto for people ? min

E2E verification ? min

RWC Seattle 13 hrs

HACS 13 hrs

CAW, Eindhoven 11 hrs

Lugano 2 hrs

matilda.backendal@usi.ch
mbackendal.github.io

Università della Svizzera italiana

Reading List

Mihir Bellare, *Caught in Between: Theory, Practice, and Peer Review*.
https://iacr.org/publications/dl/bellare14/bellare-crypto-2014.pdf
Phillip Rogaway, *The Moral Character of Cryptographic Work*.
Paper · Slides (Asiacrypt 2015)
Phillip Rogaway, *Practice-Oriented Provable Security and the Social Construction of Cryptography.*
https://www.cs.ucdavis.edu/~rogaway/papers/cc.pdf
Phillip Rogaway, *An Obsession with Definitions.*
https://web.cs.ucdavis.edu/~rogaway/papers/defs2.pdf
Seny Kamara, *Crypto for the People* (Part1: Crypto 2020, Part 2: USENIX Enigma).
Part 1 video · Part 2 slides
Martin Albrecht & Rikke Bjerg Jensen, *What does "secure" mean in Information Security?* (2020).
https://martinralbrecht.wordpress.com/2020/07/10/what-does-secure-mean-in-information-security/