A Privacy-Preserving Aid Distribution System with Assessment Capabilities

Or, a Case Study on Threat Modelling and System Design

Christian Knabenhans [EPFL]

Based on joint work with Lucy Qin [Georgetown U.]
Carmela Troncoso [EPFL+MPI-SP]
Justinas Sukaitis [ICRC]
Vincent Graf Narbel [ICRC]

in collaboration with

EPFL

MAX PLANCK INSTITUTE
FOR SECURITY AND PRIVACY

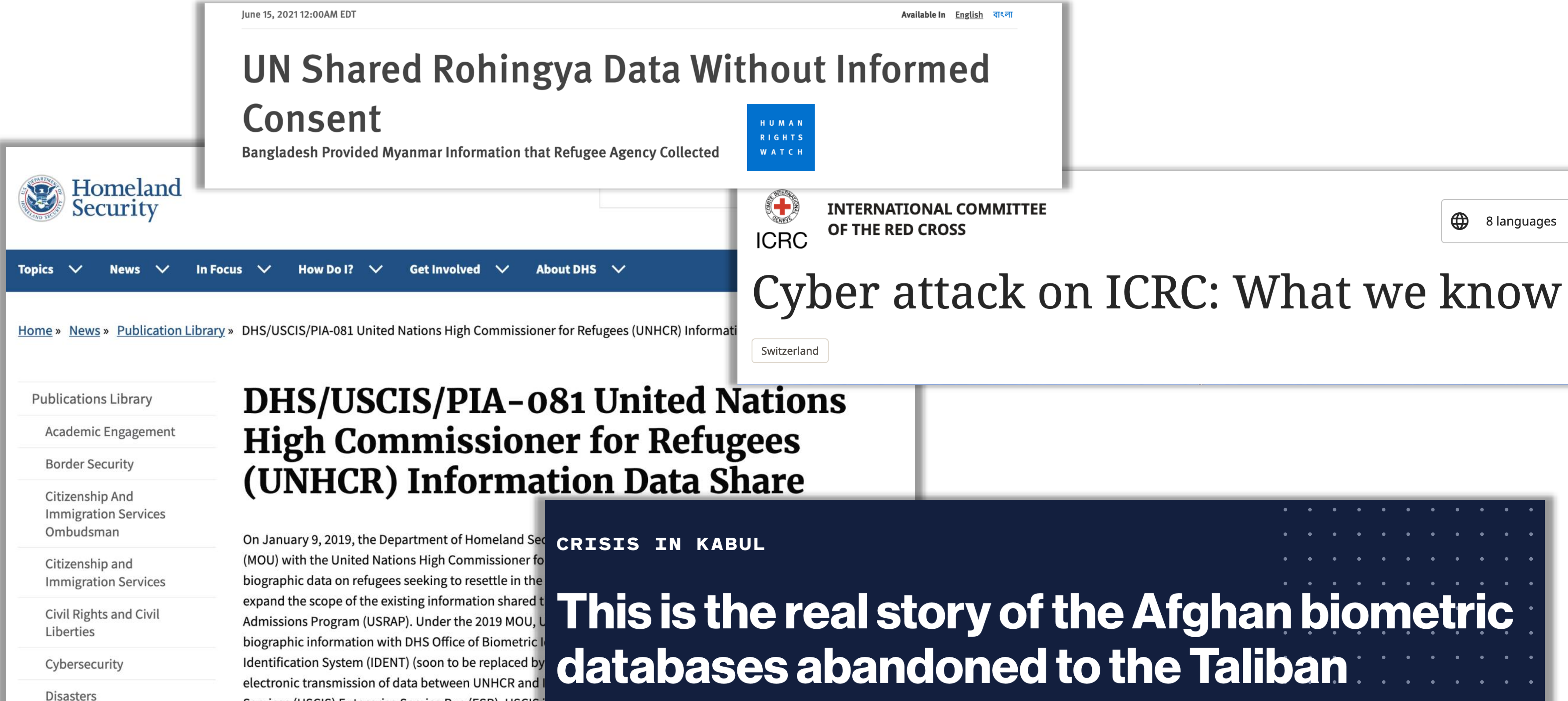
GEORGETOWN UNIVERSITY

ICRC

Historically a manual process,
which may be slow, error-prone, and costly
→ strong push to digitalize

Tougbo subprefecture, 2023. The ICRC and the Red Cross Society of Côte d'Ivoire distribute essential household items to 509 households. © ICRC

Digitalizing humanitarian action is risky



June 15, 2021 12:00AM EDT

Available In English বাংলা

UN Shared Rohingya Data Without Informed Consent

Bangladesh Provided Myanmar Information that Refugee Agency Collected

HUMAN RIGHTS WATCH

Homeland Security

Topics News In Focus How Do I? Get Involved About DHS

Home » News » Publication Library » DHS/USCIS/PIA-081 United Nations High Commissioner for Refugees (UNHCR) Informati

- Publications Library
- Academic Engagement
- Border Security
- Citizenship And Immigration Services Ombudsman
- Citizenship and Immigration Services
- Civil Rights and Civil Liberties
- Cybersecurity
- Disasters

DHS/USCIS/PIA-081 United Nations High Commissioner for Refugees (UNHCR) Information Data Share

On January 9, 2019, the Department of Homeland Sec
(MOU) with the United Nations High Commissioner fo
biographic data on refugees seeking to resettle in the
expand the scope of the existing information shared t
Admissions Program (USRAP). Under the 2019 MOU, U
biographic information with DHS Office of Biometric I
Identification System (IDENT) (soon to be replaced by
electronic transmission of data between UNHCR and I

ICRC INTERNATIONAL COMMITTEE OF THE RED CROSS

8 languages

Cyber attack on ICRC: What we know

Switzerland

CRISIS IN KABUL

This is the real story of the Afghan biometric databases abandoned to the Taliban

Privacy-preserving aid distribution

Anonymous credentials +blocklists +biometrics

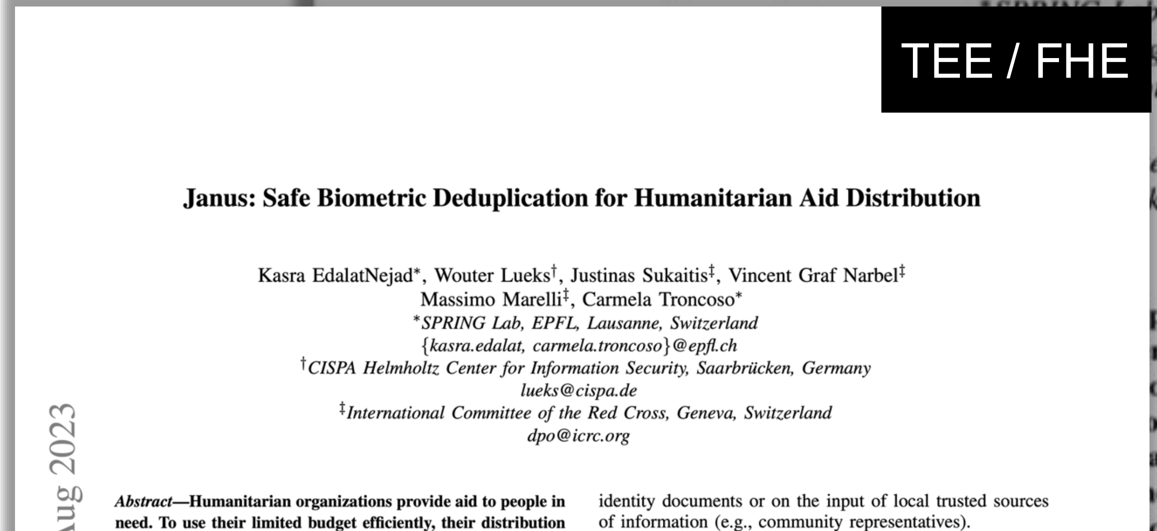
Not Yet Another Digital ID: Privacy-Preserving Humanitarian Aid Distribution

Boya Wang[*], Wouter Lueks[†], Justinas Sukaitis[‡], Vincent Graf Narbel[‡], Carmela Troncoso[*]
[*]SPRING Lab, EPFL, Lausanne, Switzerland
g,carmela.tronco
r Information Se
lueks@cispa.de
ee of the Red Cr
kaitis,vgraf}@ic

p bring
r-based
o large
olutions
amount
ndanger

requi
We
const
Our

1) Se



TEE / FHE

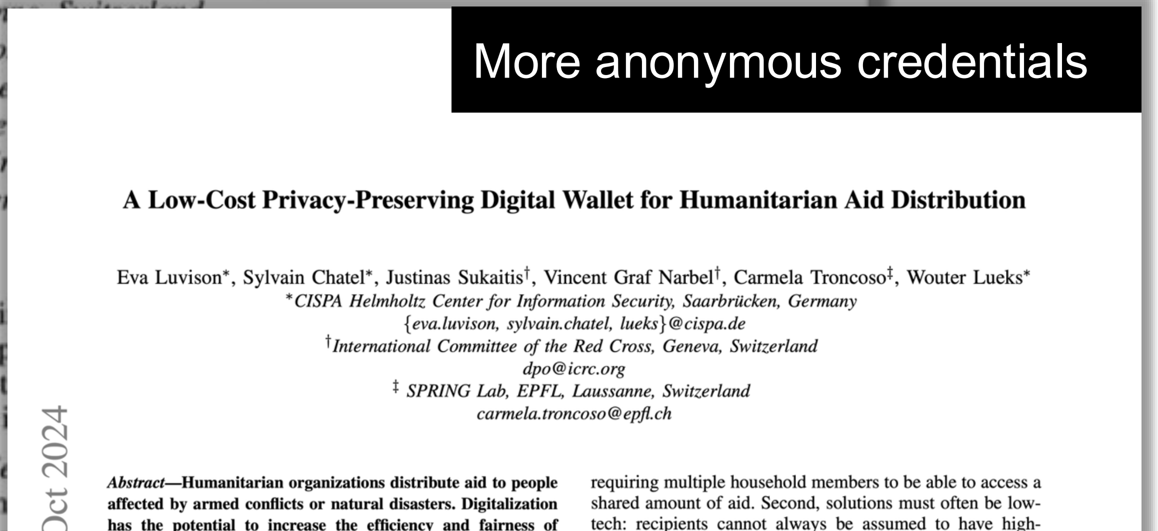
Janus: Safe Biometric Deduplication for Humanitarian Aid Distribution

Kasra EdalatNejad[*], Wouter Lueks[†], Justinas Sukaitis[‡], Vincent Graf Narbel[‡]
Massimo Marelli[‡], Carmela Troncoso[*]
[*]SPRING Lab, EPFL, Lausanne, Switzerland
{kasra.edalat, carmela.troncoso}@epfl.ch
[†]CISPA Helmholtz Center for Information Security, Saarbrücken, Germany
lueks@cispa.de
[‡]International Committee of the Red Cross, Geneva, Switzerland
dpo@icrc.org

Aug 2023

Abstract—**Humanitarian organizations provide aid to people in need. To use their limited budget efficiently, their distribution**

identity documents or on the input of local trusted sources of information (e.g., community representatives).



More anonymous credentials

A Low-Cost Privacy-Preserving Digital Wallet for Humanitarian Aid Distribution

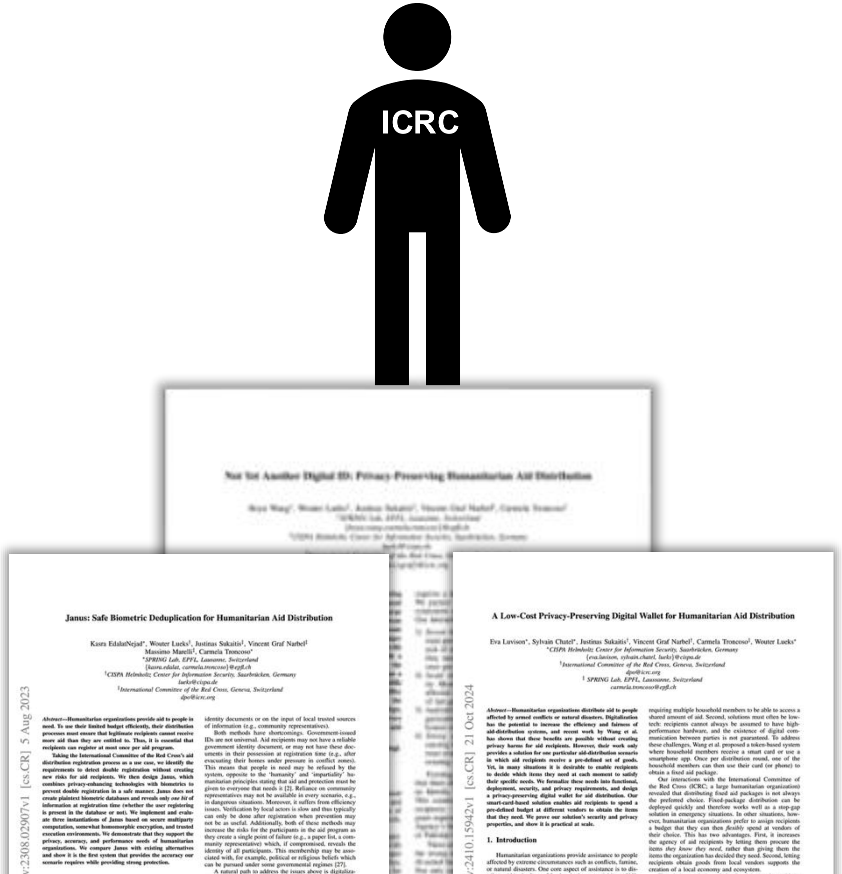
Eva Luvison[*], Sylvain Chatel[*], Justinas Sukaitis[†], Vincent Graf Narbel[†], Carmela Troncoso[‡], Wouter Lueks[*]
[*]CISPA Helmholtz Center for Information Security, Saarbrücken, Germany
{eva.luvison, sylvain.chatel, lueks}@cispa.de
[†]International Committee of the Red Cross, Geneva, Switzerland
dpo@icrc.org
[‡] SPRING Lab, EPFL, Laussanne, Switzerland
carmela.troncoso@epfl.ch

Oct 2024

Abstract—**Humanitarian organizations distribute aid to people affected by armed conflicts or natural disasters. Digitalization has the potential to increase the efficiency and fairness of**

requiring multiple household members to be able to access a shared amount of aid. Second, solutions must often be low-tech: recipients cannot always be assumed to have high-

Privacy-preserving aid distribution is great, but <u>needs assessments</u>



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

Boya Wang, Wouter Lueks, Justinas Sukaitis, Vincent Graf Narbel, Carmela Troncoso

Janus: Safe Biometric Deduplication for Humanitarian Aid Distribution

Kasra EdalatNejad*, Wouter Lueks†, Justinas Sukaitis‡, Vincent Graf Narbel‡
Massimo Marelli‡, Carmela Troncoso*
*SPRING Lab, EPFL, Lausanne, Switzerland
{kasra.edalat, carmela.troncoso}@epfl.ch
†CISPA Helmholtz Center for Information Security, Saarbrücken, Germany
lueks@cispa.de
‡International Committee of the Red Cross, Geneva, Switzerland
dpo@icrc.org

v:2308.02907v1 [cs.CR] 5 Aug 2023

***Abstract*—Humanitarian organizations provide aid to people in need. To use their limited budget efficiently, their distribution processes must ensure that legitimate recipients cannot receive more aid than they are entitled to. Thus, it is essential that recipients can register at most once per aid program.**

Taking the International Committee of the Red Cross's aid distribution registration process as a use case, we identify the requirements to detect double registration without creating new risks for aid recipients. We then design Janus, which combines privacy-enhancing technologies with biometrics to prevent double registration in a safe manner. Janus does not create plaintext biometric databases and reveals only *one bit* of information at registration time (whether the user registering is present in the database or not). We implement and evaluate three instantiations of Janus based on secure multiparty computation, somewhat homomorphic encryption, and trusted execution environments. We demonstrate that they support the privacy, accuracy, and performance needs of humanitarian organizations. We compare Janus with existing alternatives and show it is the first system that provides the accuracy our scenario requires while providing strong protection.

identity documents or on the input of local trusted sources of information (e.g., community representatives).

Both methods have shortcomings. Government-issued IDs are not universal. Aid recipients may not have a reliable government identity document, or may not have these documents in their possession at registration time (e.g., after evacuating their homes under pressure in conflict zones). This means that people in need may be refused by the system, opposite to the 'humanity' and 'impartiality' humanitarian principles stating that aid and protection must be given to everyone that needs it [2]. Reliance on community representatives may not be available in every scenario, e.g., in dangerous situations. Moreover, it suffers from efficiency issues. Verification by local actors is slow and thus typically can only be done after registration when prevention may not be as useful. Additionally, both of these methods may increase the risks for the participants in the aid program as they create a single point of failure (e.g., a paper list, a community representative) which, if compromised, reveals the identity of all participants. This membership may be associated with, for example, political or religious beliefs which can be pursued under some governmental regimes [27].

A natural path to address the issues above is digitaliza-

A Low-Cost Privacy-Preserving Digital Wallet for Humanitarian Aid Distribution

Eva Luvison*, Sylvain Chatel*, Justinas Sukaitis†, Vincent Graf Narbel†, Carmela Troncoso‡, Wouter Lueks*
*CISPA Helmholtz Center for Information Security, Saarbrücken, Germany
{eva.luvison, sylvain.chatel, lueks}@cispa.de
†International Committee of the Red Cross, Geneva, Switzerland
dpo@icrc.org
‡ SPRING Lab, EPFL, Lausanne, Switzerland
carmela.troncoso@epfl.ch

v:2410.15942v1 [cs.CR] 21 Oct 2024

***Abstract*—Humanitarian organizations distribute aid to people affected by armed conflicts or natural disasters. Digitalization has the potential to increase the efficiency and fairness of aid-distribution systems, and recent work by Wang et al. has shown that these benefits are possible without creating privacy harms for aid recipients. However, their work only provides a solution for one particular aid-distribution scenario in which aid recipients receive a pre-defined set of goods. Yet, in many situations it is desirable to enable recipients to decide which items they need at each moment to satisfy their specific needs. We formalize these needs into functional, deployment, security, and privacy requirements, and design a privacy-preserving digital wallet for aid distribution. Our smart-card-based solution enables aid recipients to spend a pre-defined budget at different vendors to obtain the items that they need. We prove our solution's security and privacy properties, and show it is practical at scale.**

1. Introduction

Humanitarian organizations provide assistance to people affected by extreme circumstances such as conflicts, famine, or natural disasters. One core aspect of assistance is to dis-

requiring multiple household members to be able to access a shared amount of aid. Second, solutions must often be low-tech: recipients cannot always be assumed to have high-performance hardware, and the existence of digital communication between parties is not guaranteed. To address these challenges, Wang et al. proposed a token-based system where household members receive a smart card or use a smartphone app. Once per distribution round, one of the household members can then use their card (or phone) to obtain a fixed aid package.

Our interactions with the International Committee of the Red Cross (ICRC; a large humanitarian organization) revealed that distributing fixed aid packages is not always the preferred choice. Fixed-package distribution can be deployed quickly and therefore works well as a stop-gap solution in emergency situations. In other situations, however, humanitarian organizations prefer to assign recipients a budget that they can then *flexibly* spend at vendors of their choice. This has two advantages. First, it increases the agency of aid recipients by letting them procure the items *they know they need*, rather than giving them the items the organization has decided they need. Second, letting recipients obtain goods from local vendors supports the creation of a local economy and ecosystem.

“Optimal privacy is nice…

But also, we need to know whether our distribution
- was successful
- reached the right targets
- does not discriminate“

hot take

Real-world systems need assessments

Not an isolated case! Real-world deployments need assessments

Correctness	debugging fully opaque systems is hard
Transparency	towards users, donors, legislators
Planning	to optimize or rectify deployments

Gathering requirements efficiently and from first principles

Gathering requirements

Data Protection Office

data management policies,
compliance

Program Managers

planning,
deployment

aid distribution

Field Employees

Gathering requirements

Asking the right questions

hot take

What do you want?

What do you need?

Everything!
(and post-quantum please)

Exactly what we have now, but digital and “private”

Gathering requirements

Asking the right questions

hot take

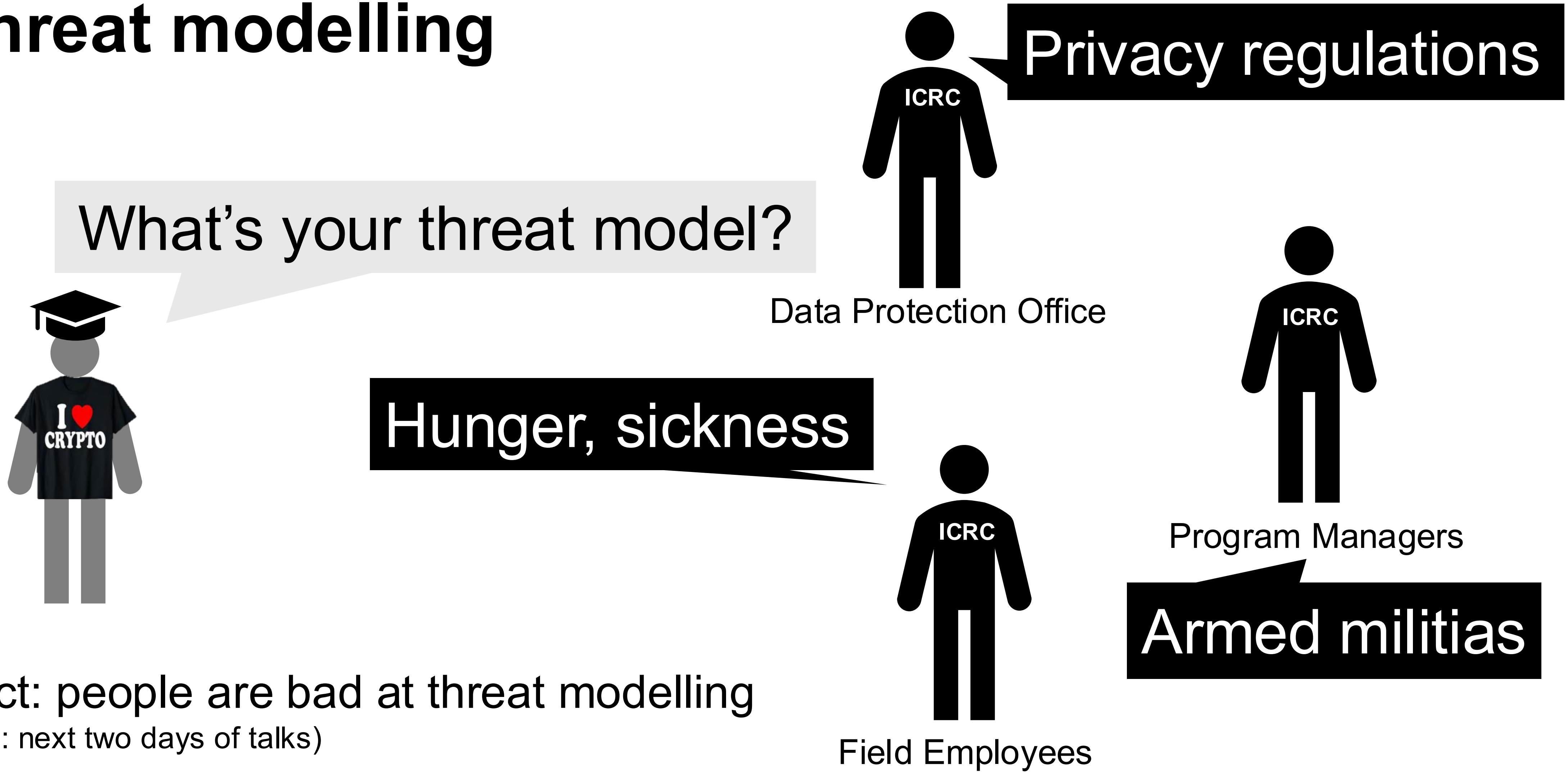
How do you do things?

Functionality	find out what information they actually need to do their job
Creativity	cryptography is unintuitive to non-cryptographers
Boundaries	we’re only designing a small part of a broader system; delineate where there should be a human-in-the-loop

Gathering requirements

Threat modelling

hot take



What’s your threat model?

ICRC

Privacy regulations

Data Protection Office

ICRC

Program Managers

Armed militias

Hunger, sickness

ICRC

Field Employees

Fact: people are bad at threat modelling

(see: next two days of talks)

Gathering requirements

Threat modelling

1. Who might interact with the system?

recipient

other recipients

auditors

nation-state

headquarters

non-state militia

other NGOs

ISP

Gathering requirements

Threat modelling

2. What information might the system need?

biometrics household_size

registration_date is_pregnant

link_registration_distribution

entitlement ethnic_group

Gathering requirements

Threat modelling

3. What concrete harm may happen if *info* is available to *party*?

	Parties									
Info		+	-				++	++	++	
						-		++		
				+		-		++		
				-			+	+		

Gathering requirements
Threat modelling

Everything we deploy comes with some risk

Fundamental leakage, regardless of instantiation

Risk analysis: do we want to deploy this?

No need to protect *info*, since it will leak anyway

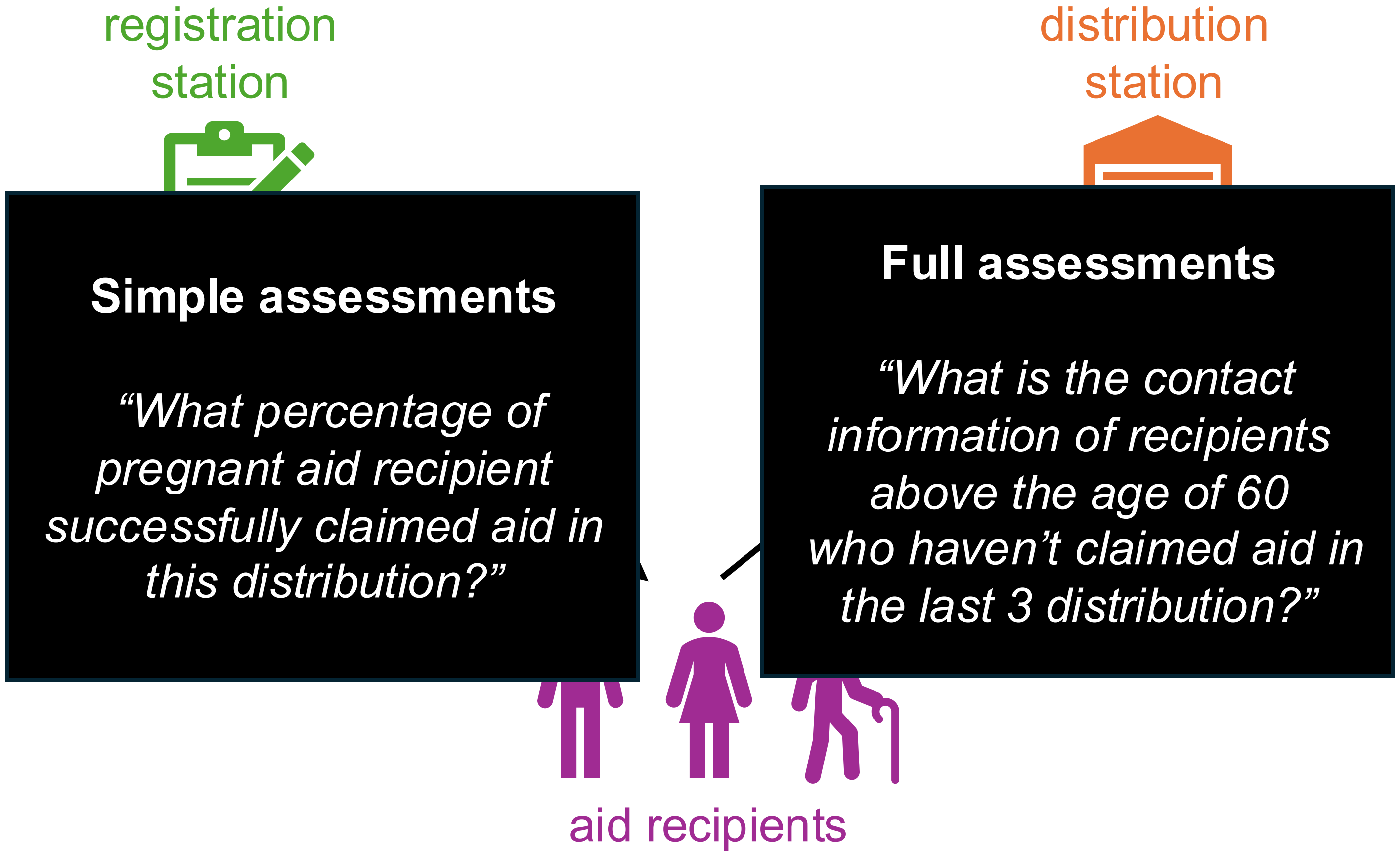
	Parties									
Info		F	F				++	++	++	
						-		++		
				F		-		++		
				F			+	+		

Fundamental information leakage
→ Fundamental risk of harm

Other leakage
→ crypto / privacy-enhancing technologies!

Requirements

Functional requirements



registration station

distribution station

Simple assessments

“What percentage of pregnant aid recipient successfully claimed aid in this distribution?”

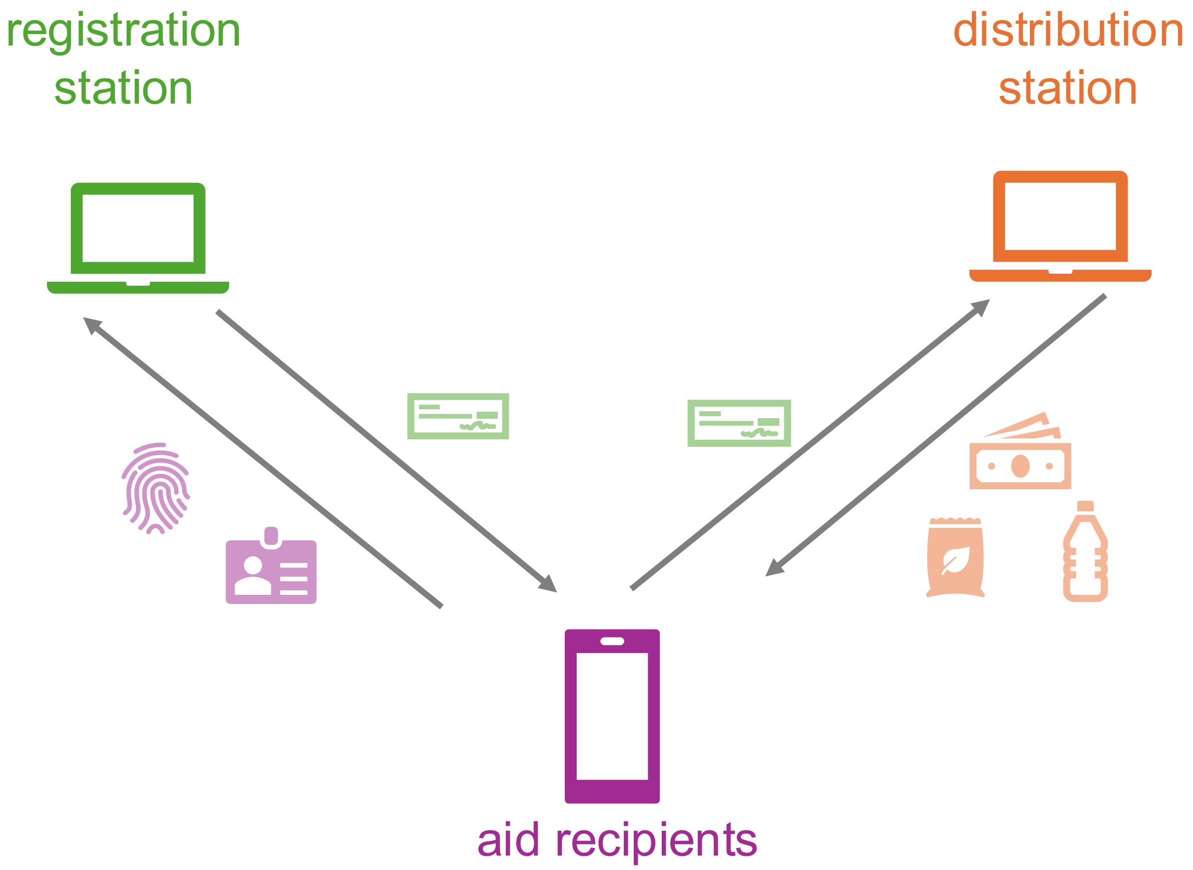
Full assessments

“What is the contact information of recipients above the age of 60 who haven’t claimed aid in the last 3 distribution?”

aid recipients

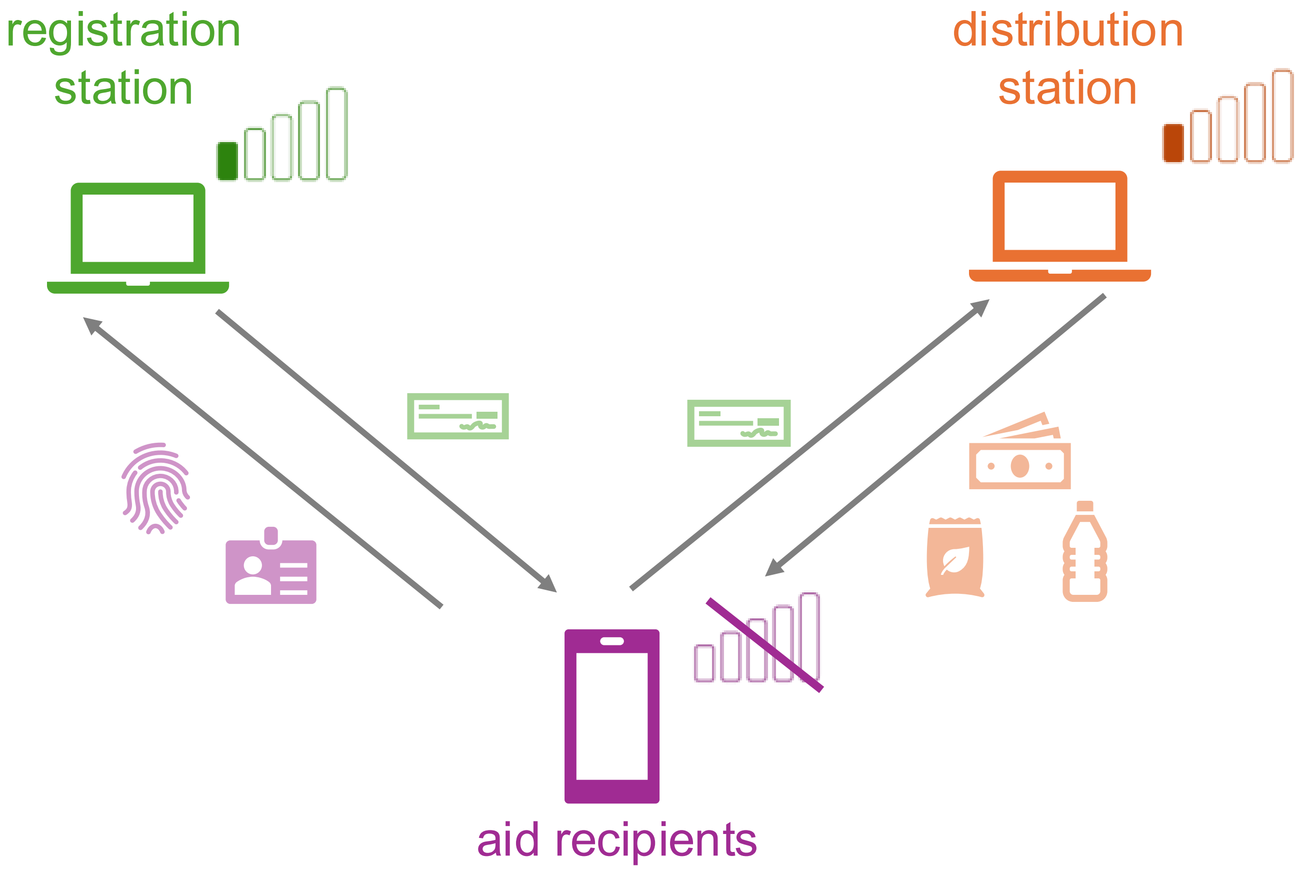
Deployment requirements

Computation



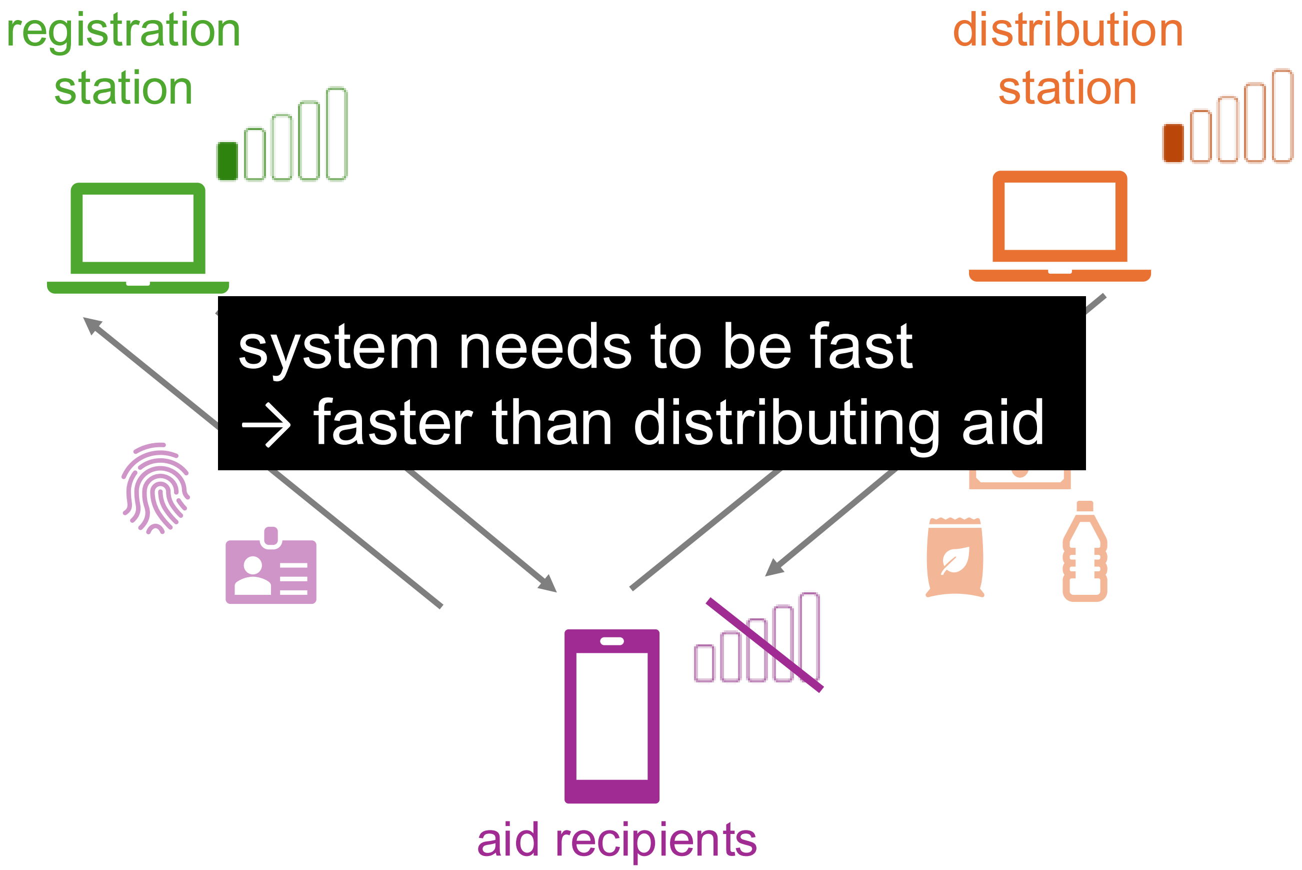
Deployment requirements

Connectivity



Deployment requirements

Efficiency



system needs to be fast
→ faster than distributing aid

Security requirements

Assessment unforgeability

Statistics reflect accurate distribution situation

Assessment privacy

Output parties only learn the intended statistics output

Meta-requirements

Agility

Threat model may be suddenly invalidated, but we might not want to deploy the strongest threat model to maximize utility

→ Need to be able to deploy strengthened protocol or safely shutdown rapidly and seamlessly

Graceful degradation

When threat model is invalidated, the system should not catastrophically collapse, but fail with minimum harm.

→ For each protocol, derive harm for all stronger threat models

Privacy-preserving humanitarian aid distribution with assessment capabilities

Adding assessments

Starting point: Functional Encryption (FE)

Attack: adversary invokes FE different subsets of inputs

Solution:

- semi-honest: one-time functional encryption
- malicious: bind crypto material to physical inventory, use predicate one-time functional encryption

Instantiation: PKE + signatures + {2PC, threshold HE}

A Privacy-Preserving Aid Distribution System with Assessment Capabilities

Or, a Case Study on Threat Modelling and System Design

Christian Knabenhans [EPFL]

Based on joint work with

Carmela Troncoso [EPFL+MPI-SP]
Lucy Qin [Georgetown U.]
Justinas Sukaitis [ICRC]
Vincent Graf Narbel [ICRC]

Thanks to

Boya Wang [EPFL+MPI-SP]
Mathilde Raynal [EPFL]
Theresa Stadler [EPFL]
Saiid El Hajj Chehade [EPFL]
Zayd Maradni [MPI-SP]
Wouter Lueks [CISPA]
Sylvain Chatel [CISPA]
and many more…