Cryptography for Grassroots Organizing

Seny Kamara
Leah Namisa Rosenbloom*
RWC 2023
Tokyo, Japan

*speaker

"Cryptography rearranges power"

–Phillip Rogaway

"Cryptographers are professional catastrophizers."

–Lucy Qin

"Awareness is two steps forward—
paranoia is two steps back."

–Kim Marks/Civil Liberties Defense Center

How do we, as cryptographers, understand systems of power?

How does our understanding inform our threat modeling and design choices?

How might we work toward building power for communities?

Threat Modeling Paradigm Shift

One Size Fits One: Protocol design begins with the unique needs of the population the protocol is meant to serve

Trust Is Human: Digital trust is recognized as an extension of highly complex human trust relationships

Full Compromise Security: Threat modeling is redesigned to center people's actual needs and lived experiences

Grassroots Optimization: Scale, efficiency, and accessibility are optimized for communities (not coroporations and governments)

Cryptography for Grassroots Organizing

- Introduction
- Threat Modeling Paradigm Shift
- Definition of Grassroots Organizing
- Lessons from History
- Lessons from the Current Landscape
- tigro: Trust Infrastructure for Grassroots Organizing
- Conclusion

Definition of Grassroots Organizing

Grassroots organizing is a process by which people work from within marginalized communities to effect social, political, economic, and environmental change.

Operation Vula

South Africa (1986–1990): African National Congress (ANC) creates cryptography for grassroots organizing

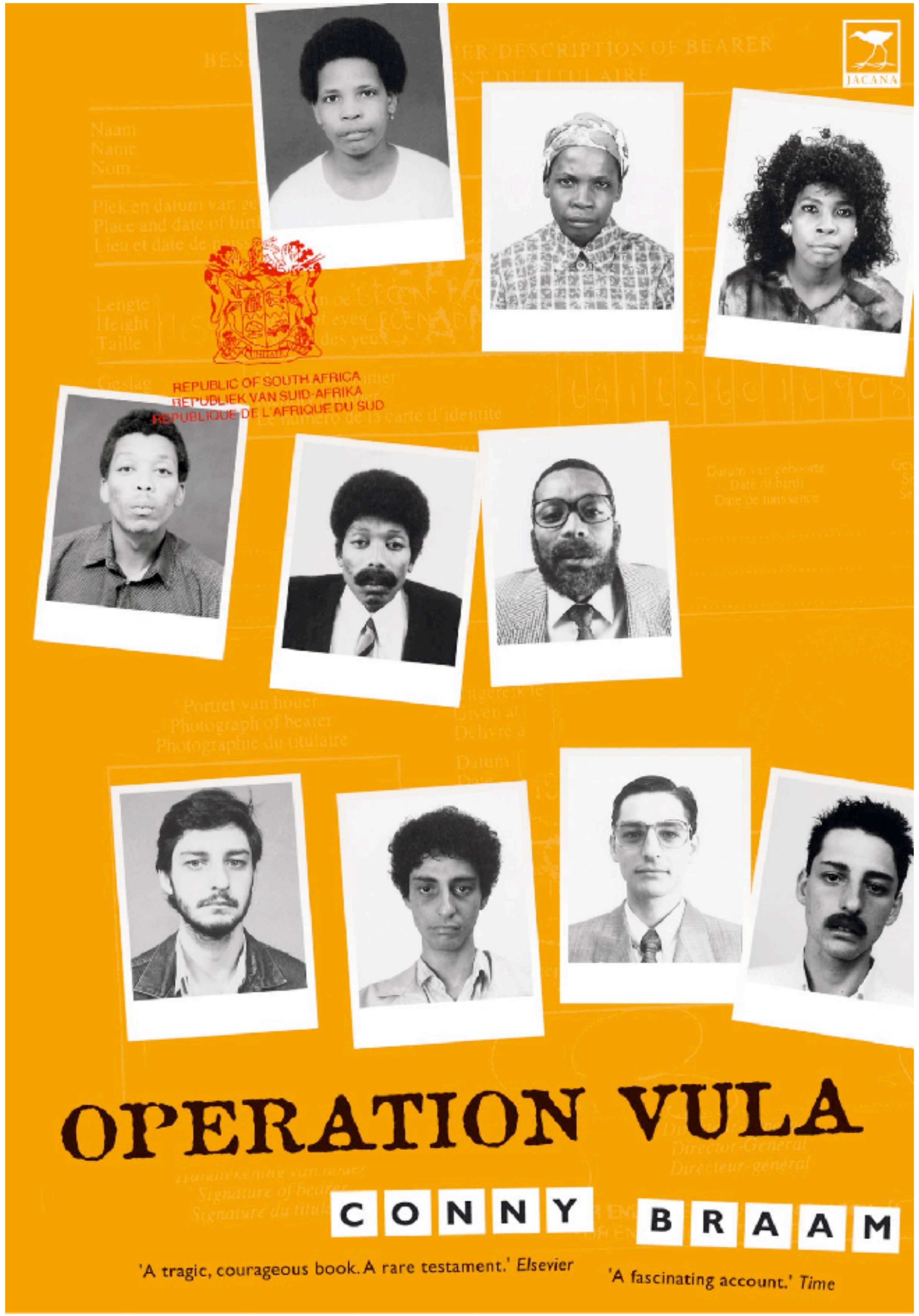

OPERATION VULA
CONNY BRAAM
'A tragic, courageous book. A rare testament.' Elsevier
'A fascinating account.' Time
REPUBLIC OF SOUTH AFRICA
REPUBLIEK VAN SUID-AFRIKA
REPUBLIQUE DE L'AFRIQUE DU SUD
JACANA

Image Credits: Jacana Media (2004), AP Photo/Udo Weitz, File (1990) via The Washington Post (2019)

Operation Vula

South Africa (1986–1990): African National Congress (ANC) creates cryptography for grassroots organizing

Requirements: Asysnchronous, Covert, Long Distance, Public

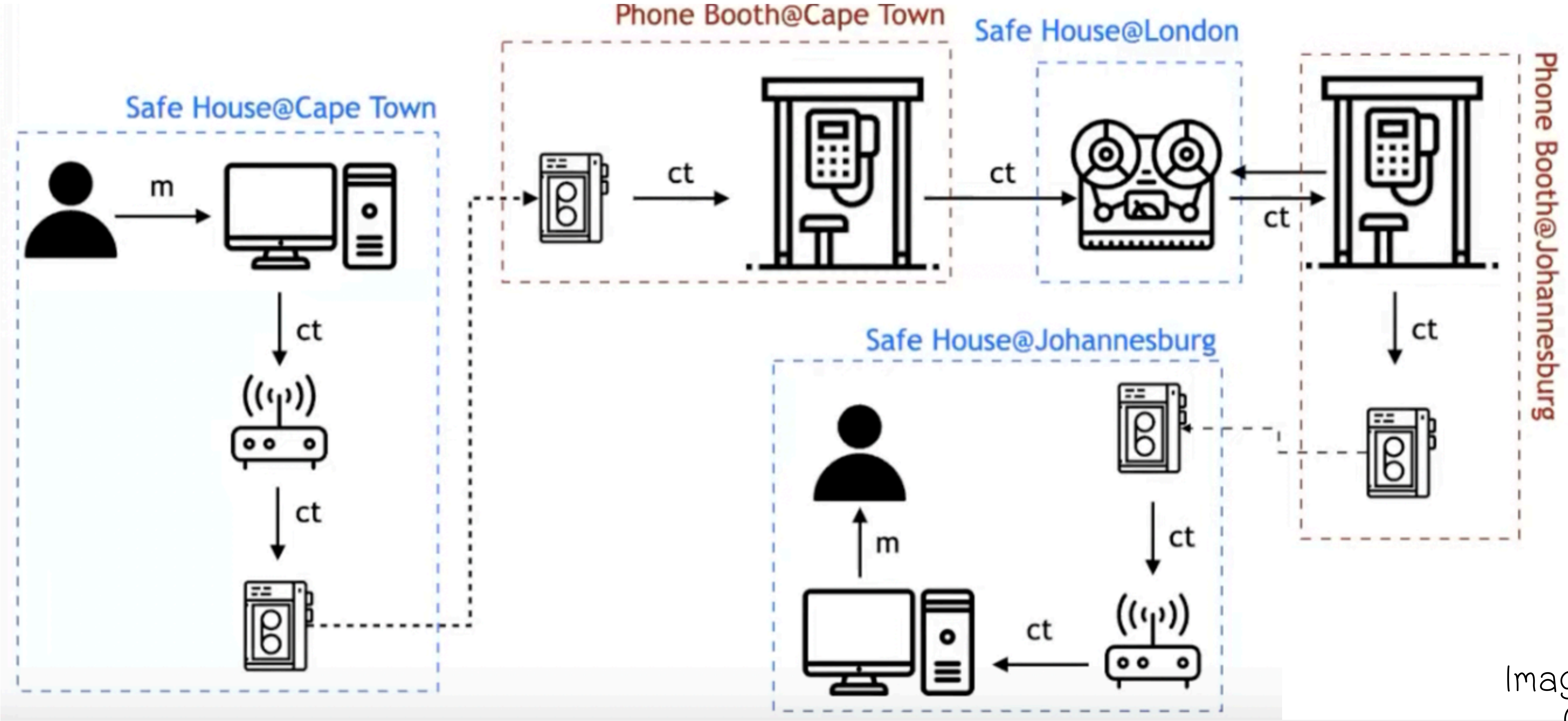


Image Credits: Kamara, CRYPTO (2020)

Operation Vula

ANC Activist Tim Jenkin (1995): "I went to find out about secure encryption algorithms...

All I discovered was that cryptology was an arcane science for bored mathematicians, not for underground activists.

However I learned a few tricks and used these to develop a system to meet our security needs."

COINTELPRO

United States (1956–1971): Federal Bureau of Investigation (FBI) illegally & extensively surveils activists

COINTELPRO
FREE
AMERICAN INDIAN MOVEMENT

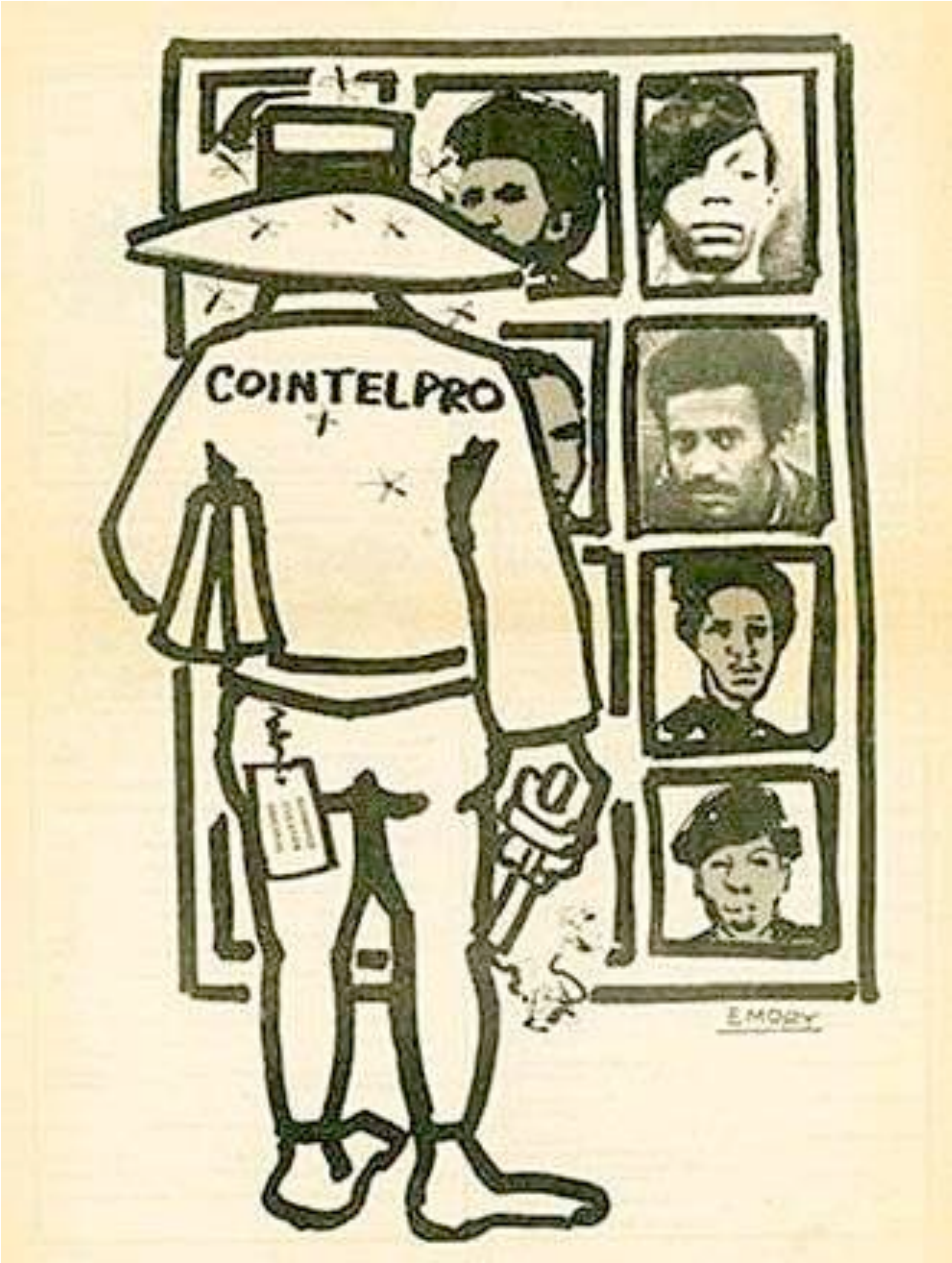


Image Credits: The Melanated Press (2014), Emory Douglas (1976)

COINTELPRO

United States (1956–1971): Federal Bureau of Investigation (FBI) illegally & extensively surveils activists

Blurred Boundaries: Surveillance leads to assassination, incarceration

Fred Hampton (1948–1969)

Angela Davis

Mae Mallory

Ericka Huggins

Image Credits: Atlanta Black Star (2015), Madison365 (2019), What'sHerName Podcast (2018), Ericka Huggins Official Website (2016)

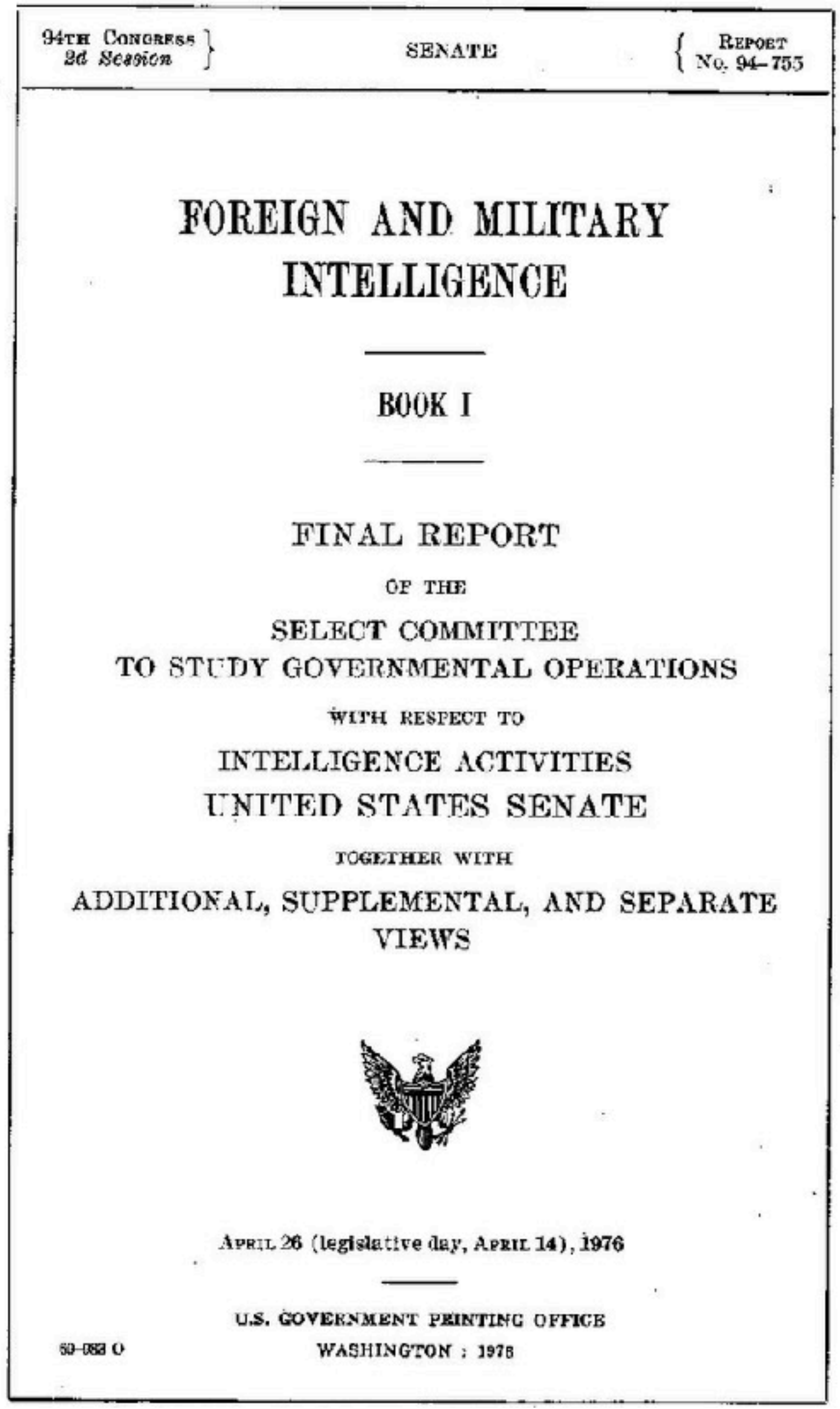
COINTELPRO

United States (1956–1971): Federal Bureau of Investigation (FBI) illegally & extensively surveils activists

Blurred Boundaries: Surveillance leads to assassination, incarceration

The Church Committee Report (1975):

- Intimidation, manipulation, dragnet tactics
- No meaningful oversight & accountability
- Digital equivalents (Snowden 2013)



94TH CONGRESS
2d Session

SENATE

REPORT
No. 94–755

FOREIGN AND MILITARY INTELLIGENCE

BOOK I

FINAL REPORT
OF THE
SELECT COMMITTEE
TO STUDY GOVERNMENTAL OPERATIONS
WITH RESPECT TO
INTELLIGENCE ACTIVITIES
UNITED STATES SENATE
TOGETHER WITH
ADDITIONAL, SUPPLEMENTAL, AND SEPARATE VIEWS

APRIL 26 (legislative day, APRIL 14), 1976

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON : 1976

59–083 O

Image Credit: U.S. Senate Select Committee on Intelligence (1975)

The Arab Spring

Many Countries (2010-2012): Tunisia, Libya, Egypt, Yemen, Syria, Bahrain, Morocco, Iraq, Algeria, Lebanon, Jordan, Kuwait, and many more with minor protests

Image Credits: CBS News (2012), Reuters (2012)

The Arab Spring

Many Countries (2010-2012): Tunisia, Libya, Egypt, Yemen, Syria, Bahrain, Morocco, Iraq, Algeria, Lebanon, Jordan, Kuwait, and many more with minor protests

The Role of Social Media

- Speed, Scope, and Scale (Rosenbloom 2021)
- Facilitator rather than direct or independent cause of chage

Image Credits: Amin Ansari (2012), Anna Lena Schiller (2012), Wikimedia Commons (2011)

The Arab Spring

Many Countries (2010-2012): Tunisia, Libya, Egypt, Yemen, Syria, Bahrain, Morocco, Iraq, Algeria, Lebanon, Jordan, Kuwait, and many more with minor protests

The Role of Social Media

- Speed, Scope, and Scale (Rosenbloom 2021)
- Facilitator rather than direct or independent cause of chage

Inspired Countless Movements

Modes of Suppression (Borradaile 2021; Boykoff 2007)

1. Direct Violence
2. The Legal System
3. Employment Deprivation
4. Conspicuous Surveillance**
5. Covert Surveillance**
6. Deception**
7. Mass Media Influence**

*Information Technology Interference

*Confidentiality, Anonymity

*Integrity, Trust

Be Safe or Be Seen? (Lokot 2018)

Ethnographic Observation of Anti-Corruption Foundation Activists (Russia)

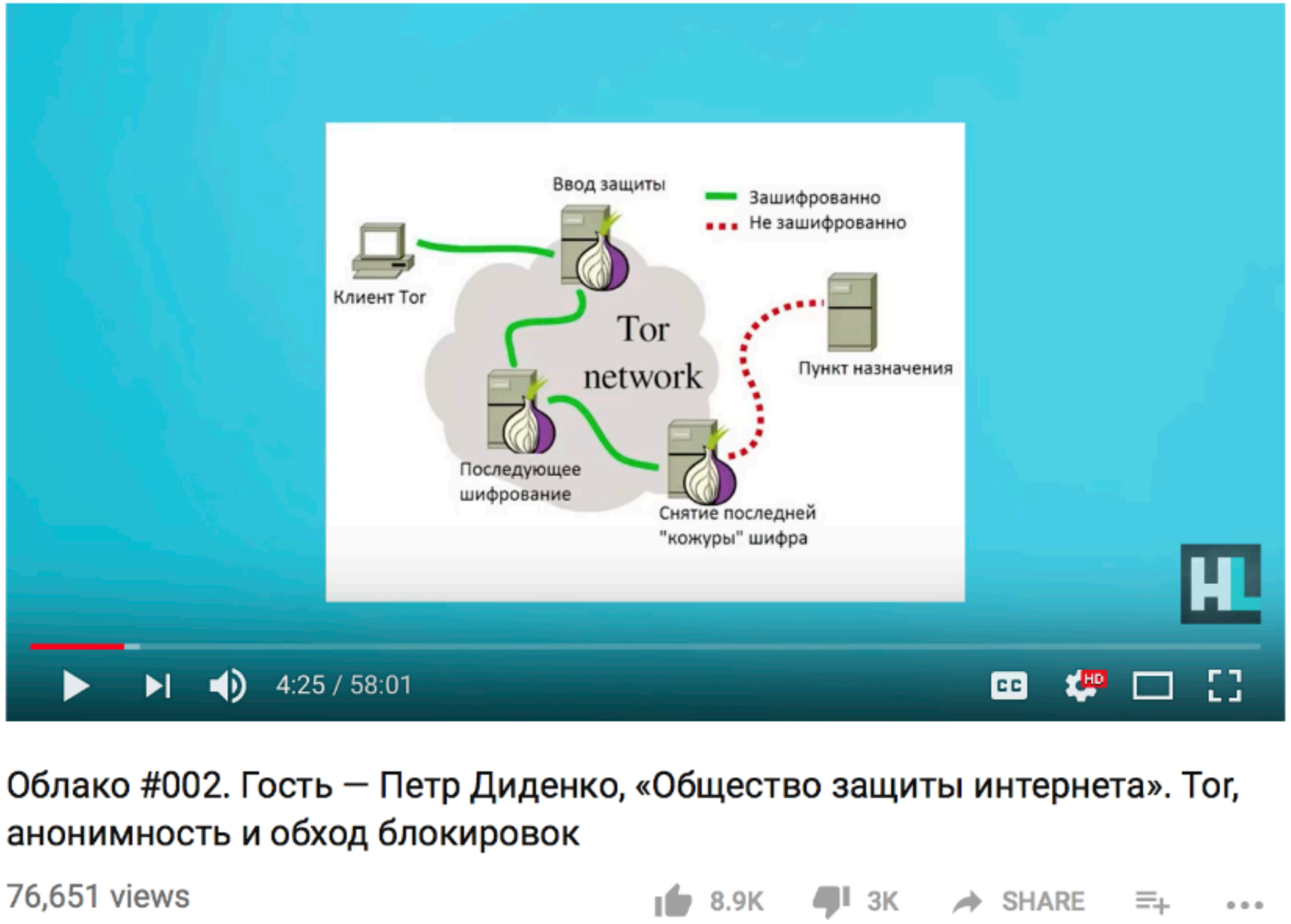
Image Credit: Evgeny Feldman/AP (2018)

Be Safe or Be Seen? (Lokot 2018)

Ethnographic Observation of Anti-Corruption Foundation Activists (Russia)

Conspicuous Security:

Tools and Education



Облако #002. Гость — Петр Диденко, «Общество защиты интернета». Tor, анонимность и обход блокировок

76,651 views

Figure 2. *Screen grab from YouTube talk show "The Cloud," hosted by Leonid Volkov, explaining the basics of the Tor network. Episode 002 was devoted to online anonymity and circumventing website blocks.*

Image Credit: Lokot (2018)

Be Safe or Be Seen? (Lokot 2018)

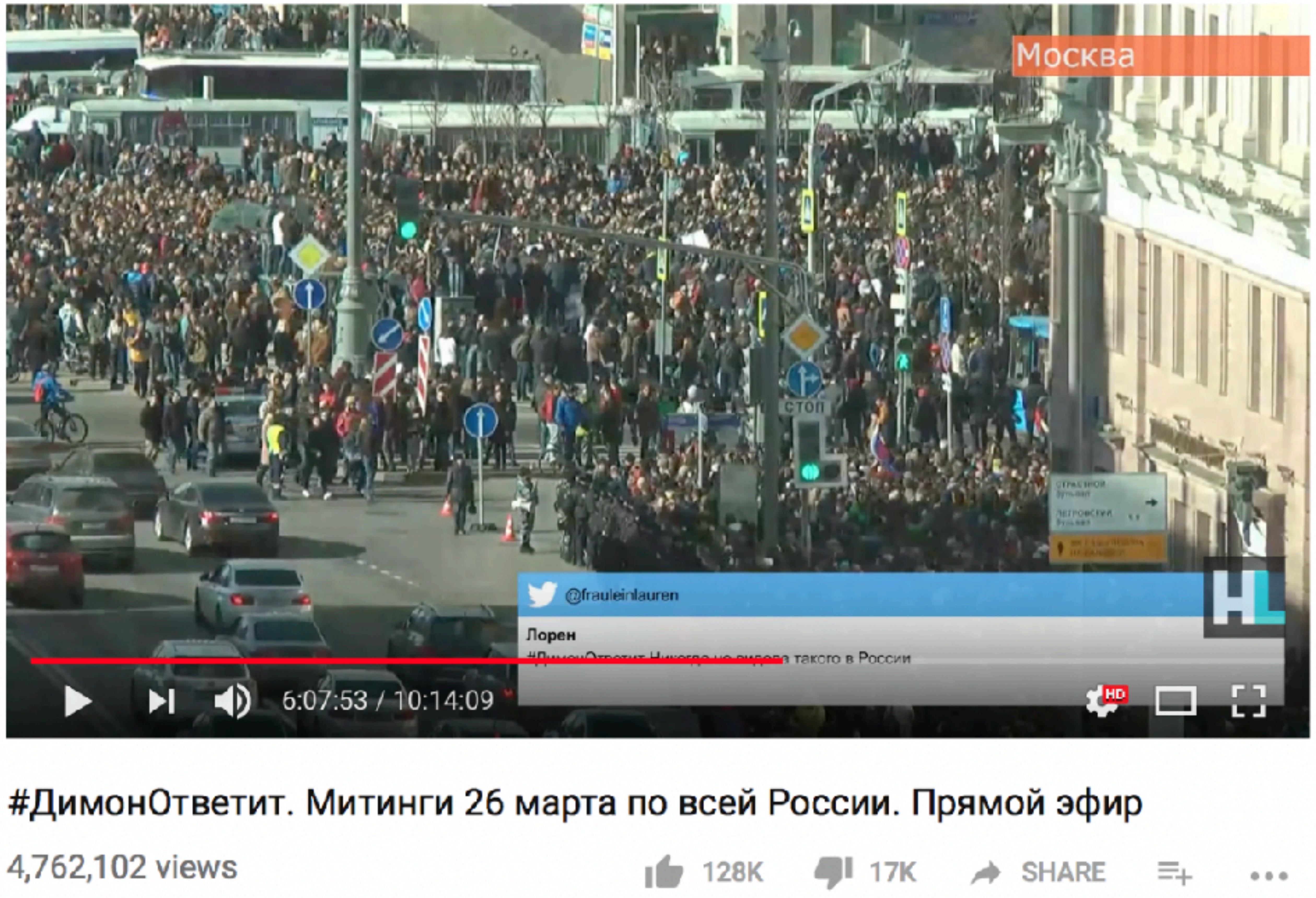
Ethnographic Observation of Anti-Corruption Foundation Activists (Russia)

Conspicuous Security:

Tools and Education

Strategic Visibility:

Transparency and Community



Лорен

#ДимонОтветит Никогда не видела такого в России

#ДимонОтветит. Митинги 26 марта по всей России. Прямой эфир

4,762,102 views

Figure 3. *Screen grab of YouTube live stream syndicated by FBK during the March 26, 2017, anti-corruption protests in Russia.*

Image Credit: Lokot (2018)

Be Safe or Be Seen? (Lokot 2018)

Ethnographic Observation of Anti-Corruption Foundation Activists (Russia)

Conspicuous Security:

Tools and Education

Strategic Visibility:

Transparency and Community

Hong Kong (Albrecht et al. 2021): Bigger public groups, smaller encrypted groups with rigorous onboarding process

Image Credit: Reclaim The Net (2019)

Digital Trust is Physical Trust (Rosenbloom 2020)

Semi-Structured Interviews with 50 Black Lives Matter Activists (U.S.)

Image Credit: Tyger Williams/AP (2020)

Digital Trust is Physical Trust (Rosenbloom 2020)

Semi-Structured Interviews with 50 Black Lives Matter Activists (U.S.)

Dangers of Immediacy, Anonymity:

Lack of information integrity online

Image Credit: Jason Peters (2020)

Digital Trust is Physical Trust (Rosenbloom 2020)

Semi-Structured Interviews with 50 Black Lives Matter Activists (U.S.)

Dangers of Immediacy, Anonymity:

Lack of information integrity online

Direct Action Decision-Making:

Word of mouth, community evaluation

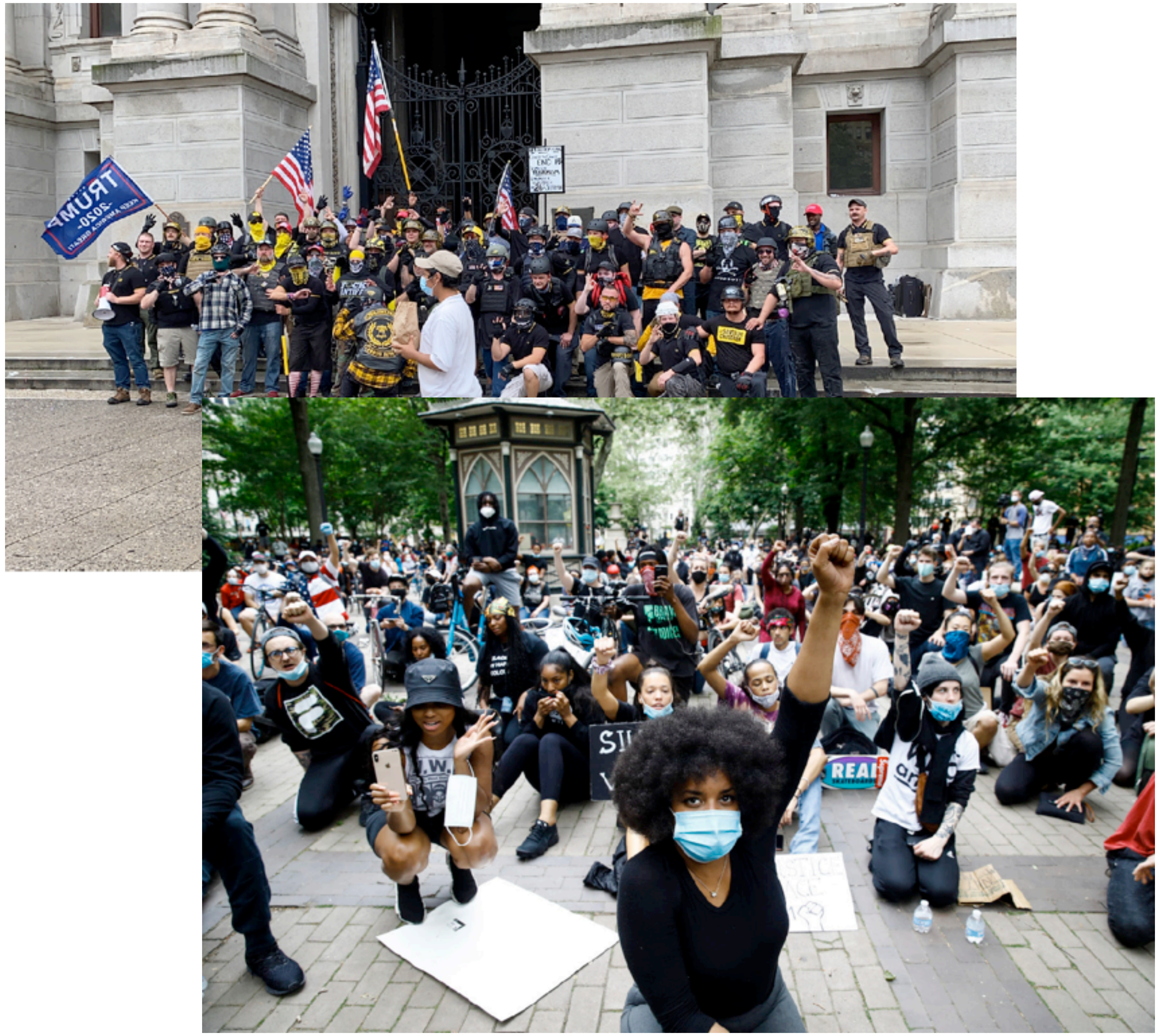


Image Credits: Jason Peters (2020), Matt Rourke/AP (2020)

Digital Trust is Physical Trust (Rosenbloom 2020)

Semi-Structured Interviews with 50 Black Lives Matter Activists (U.S.)

Dangers of Immediacy, Anonymity:

Lack of information integrity online

Direct Action Decision-Making:

Word of mouth, community evaluation

Hong Kong (Albrecht et al. 2021): face-to-face preceeds phone-to-phone because "'standing on the front line together is very important for trust' (P10)"

Image Credits: Justin Chin/Bloomberg/Getty (2020)

Device Compromise and Deletion (Albrecht et al. 2021)

Semi-Structured Interviews with 11 Anti-ELAB Protesters (Hong Kong)

Image Credit: Anthony Kwan/Getty (2019)

Device Compromise and Deletion (Albrecht et al. 2021)

Semi-Structured Interviews with 11 Anti-ELAB Protesters (Hong Kong)

Full Compromise Security:

Detection and mitigation

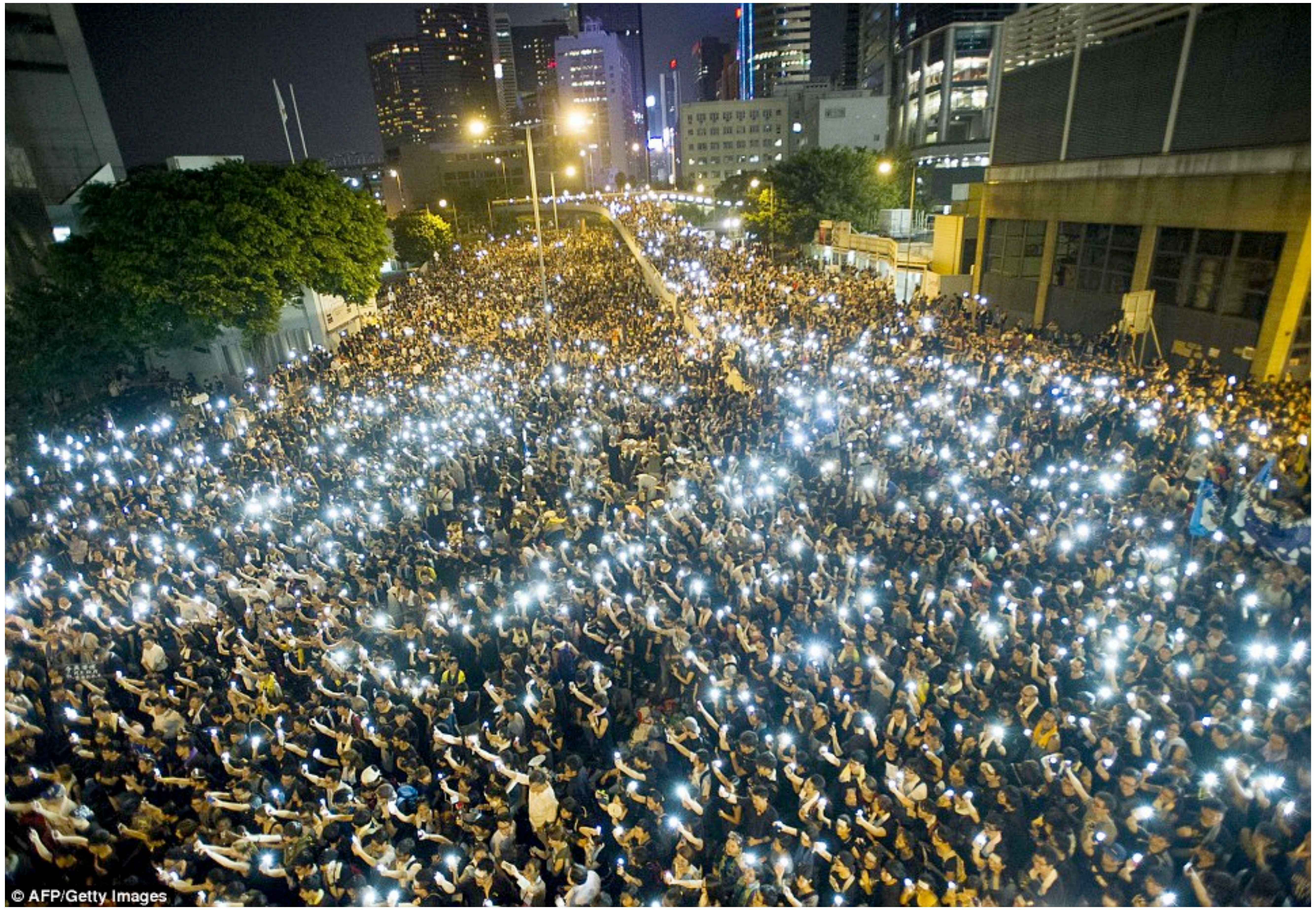


Image Credit: AFP/Getty (2019)

Device Compromise and Deletion (Albrecht et al. 2021)

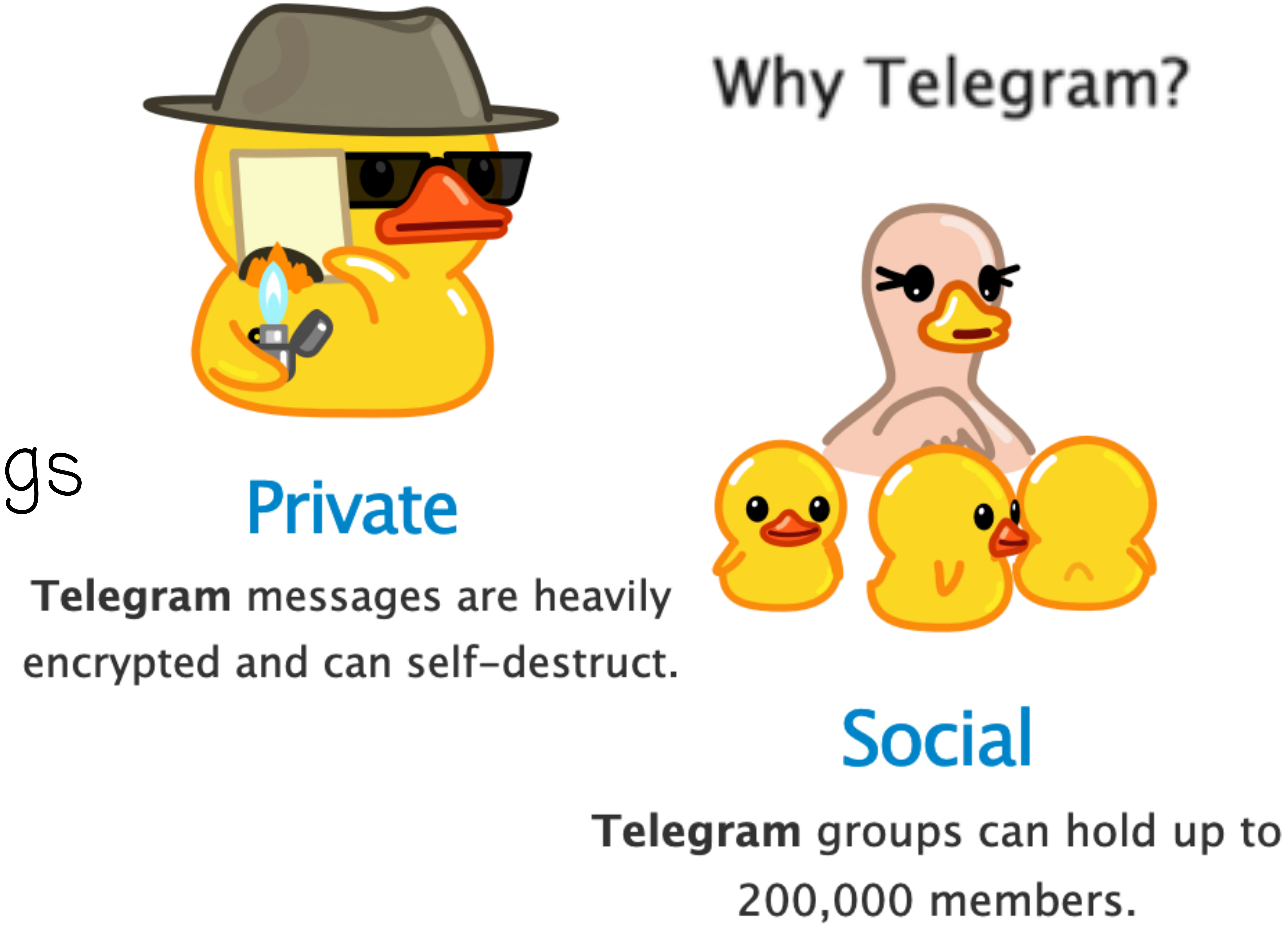
Semi-Structured Interviews with 11 Anti-ELAB Protesters (Hong Kong)

Full Compromise Security:

Detection and mitigation

Scheduled v. Remote Deletion:

Arrest compromises contacts, logs



Why Telegram?

Private

Telegram messages are heavily encrypted and can self-destruct.

Social

Telegram groups can hold up to 200,000 members.

Image Credit: Telegram

Device Compromise and Deletion (Albrecht et al. 2021)

Semi-Structured Interviews with 11 Anti-ELAB Protesters (Hong Kong)

Full Compromise Security:

Detection and mitigation

Scheduled v. Remote Deletion:

Arrest compromises contacts, logs

Collective Security Culture (Borradaile 2021): Group reflex to minimize information sharing, digitizing, and retaining

Image Credit: Alamy Live News (2019)

tigro: Trust Infrastructure for Grassroots Organizing

How might we use cryptographic tools to adapt the existing trust and communication protocols of grassroots organizers from physical to digital spaces,

without increasing the risk of surveillance, disinformation, and infiltration of grassroots movements?

tigro: Trust Infrastructure for Grassroots Organizing

One Size Fits One: Flexible library of primitives; applies (private) trust network information to any digital setting

Trust is Human: “On-the-ground” key agreement using Bluetooth; roots digial trust in interpersonal interaction

Toward Full Compromise Security: Contacts hold minimal information; anyone with shared key can delete

Grassroots Optimization: Individual device computation v. server computation over relatively small data sets

tigro Adversarial Model

How might we model existing threats and mitigation strategies in digital space?

Digital Infiltration Adversary

- collects and aggregates as much information as possible
- corrupts (subpoenas) the server, corrupts (seizes) devices
- poses as a group member, spreads false information, entraps

Semi-Honest Server: Privacy and Correctness

Malicious Server: Privacy but Not Correctness, Deletion

Security Strategy

Establish digital equivalents of existing security practices

Establishing Security = Trust

Human trust as a core digital security concept

One Size Fits One

How organizers build and assess trust depends on:

- the person, place, or thing to be trusted (profiles, events, posts)
- the risk level associated with trust
- personal experience, collective security culture, etc.

"Grounded" Cryptographic Protocols

Digital trust reduces to:

- physical interactions that establish "grounded pairs"
- qualitative trust measurements between grounded pairs

tigro Core Protocols

Ground Trust Ceremony

Like a key signing ceremony in spirit, but:

- Establishes a symmetric key linked to a physical meeting
- No PKI: digital activity is not linkable to a persistent identifier

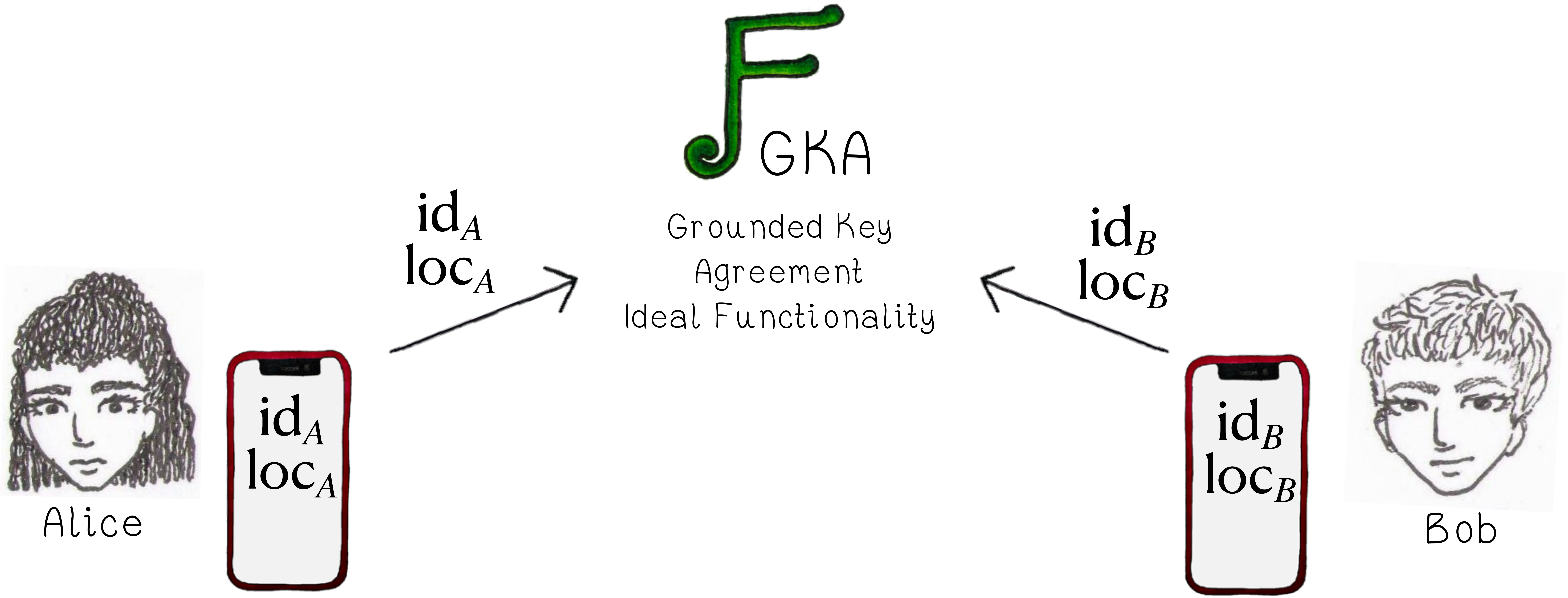
Grounded Annotation System

Allows grounded pairs to share digital annotations of arbitrary people, places, and things

(Grounded) Trust Metrics

Quantify trust using social network analytics (eg. HITS algorithm)

Ground Trust Ceremony



$\mathcal{F}_{\mathrm{GKA}}$

Grounded Key Agreement Ideal Functionality

id_A loc_A
id_B loc_B
Alice
id_A loc_A
id_B loc_B
Bob

Ground Trust Ceremony

$\mathcal{F}_{\text{GKA}}$

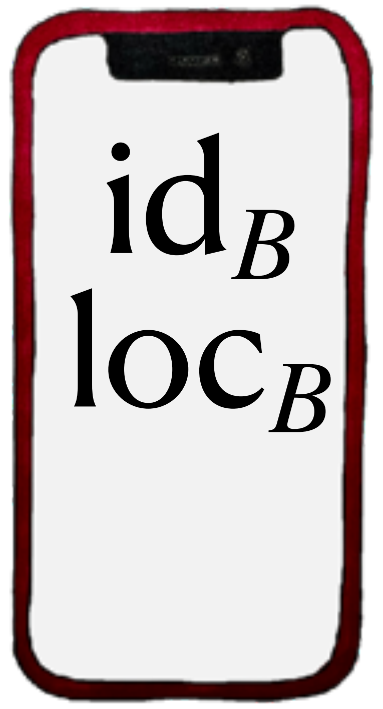
Grounded Key
Agreement
Ideal Functionality

$$\text{if } \mathrm{loc}_A = \mathrm{loc}_B :$$

$$k_{AB} \leftarrow_{\$} \{0,1\}^{\lambda}$$

Alice

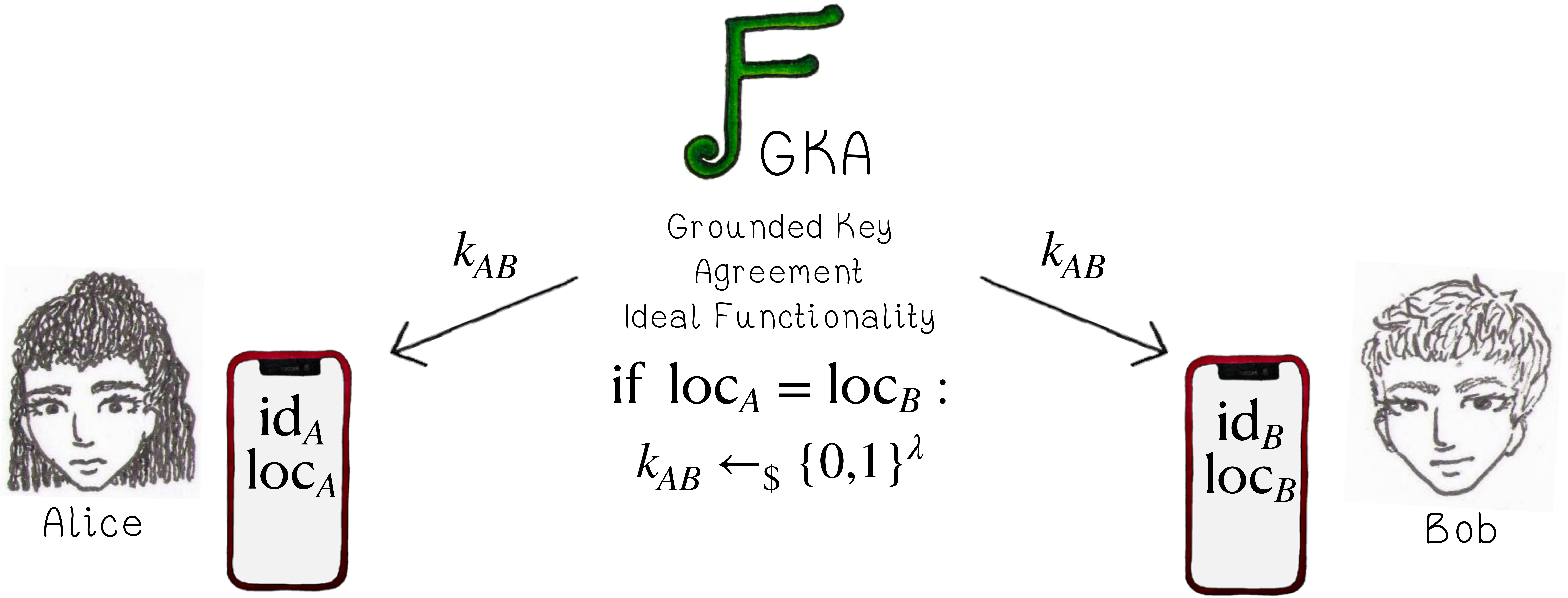
id_A
loc_A



id_B
loc_B

Bob

Ground Trust Ceremony



$\mathcal{F}_{\text{GKA}}$

Grounded Key Agreement Ideal Functionality

if $\text{loc}_A = \text{loc}_B$:

$k_{AB} \leftarrow_{\$} \{0,1\}^{\lambda}$

k_{AB}

k_{AB}

Alice

id_A
loc_A

id_B
loc_B

Bob

Ground Trust Ceremony

$\mathcal{F}_{\text{GKA}}$

Grounded Key
Agreement
Ideal Functionality

Alice

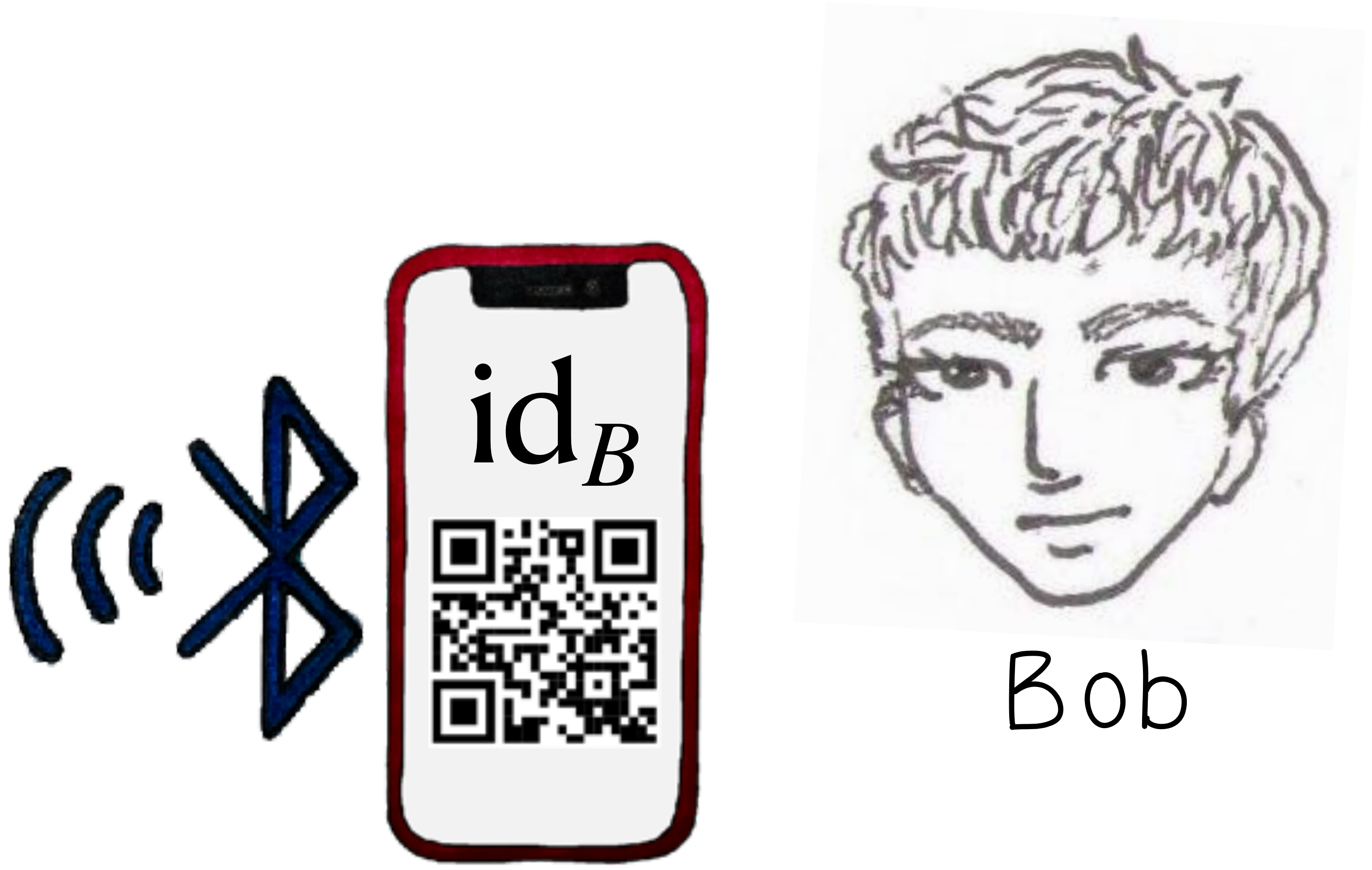
id_A
loc_A
k_{AB}

id_B
loc_B
k_{AB}

Bob

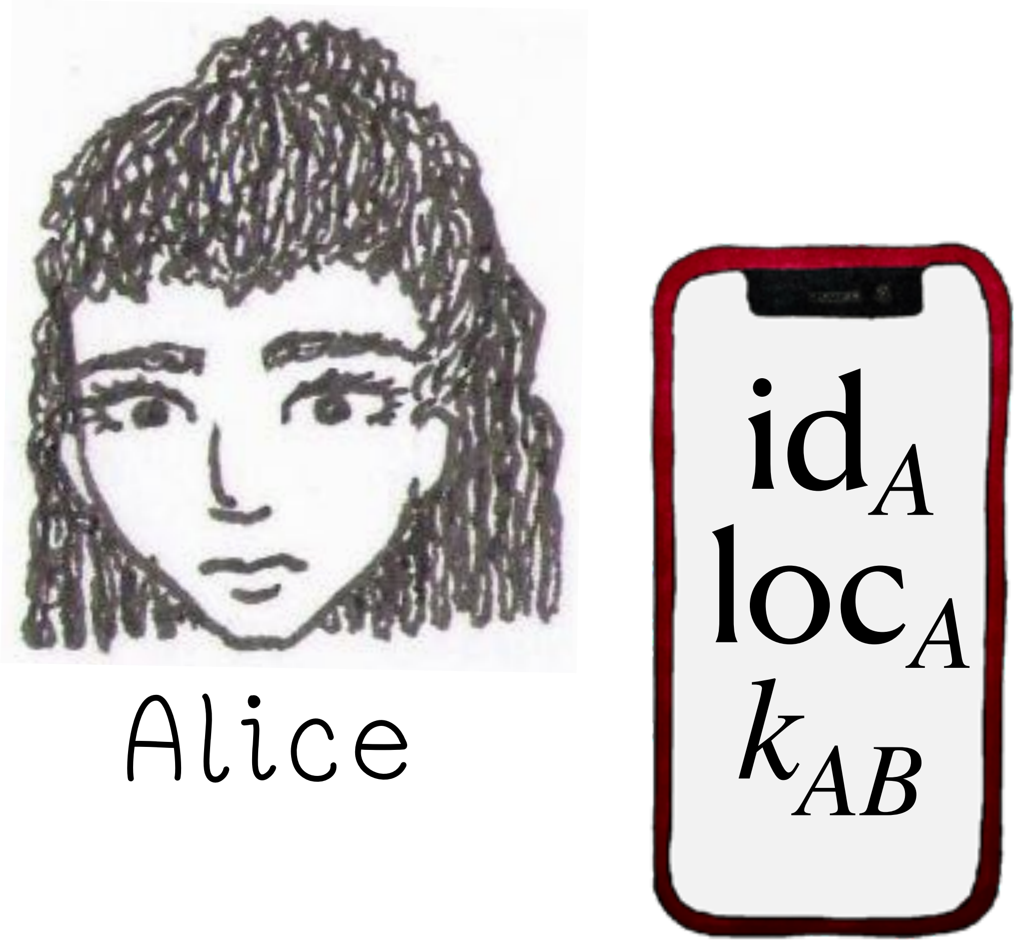
Ground Trust Ceremony

In practice, we can replace the key agreement ideal functionality with Diffie-Hellman over QR code exchange.

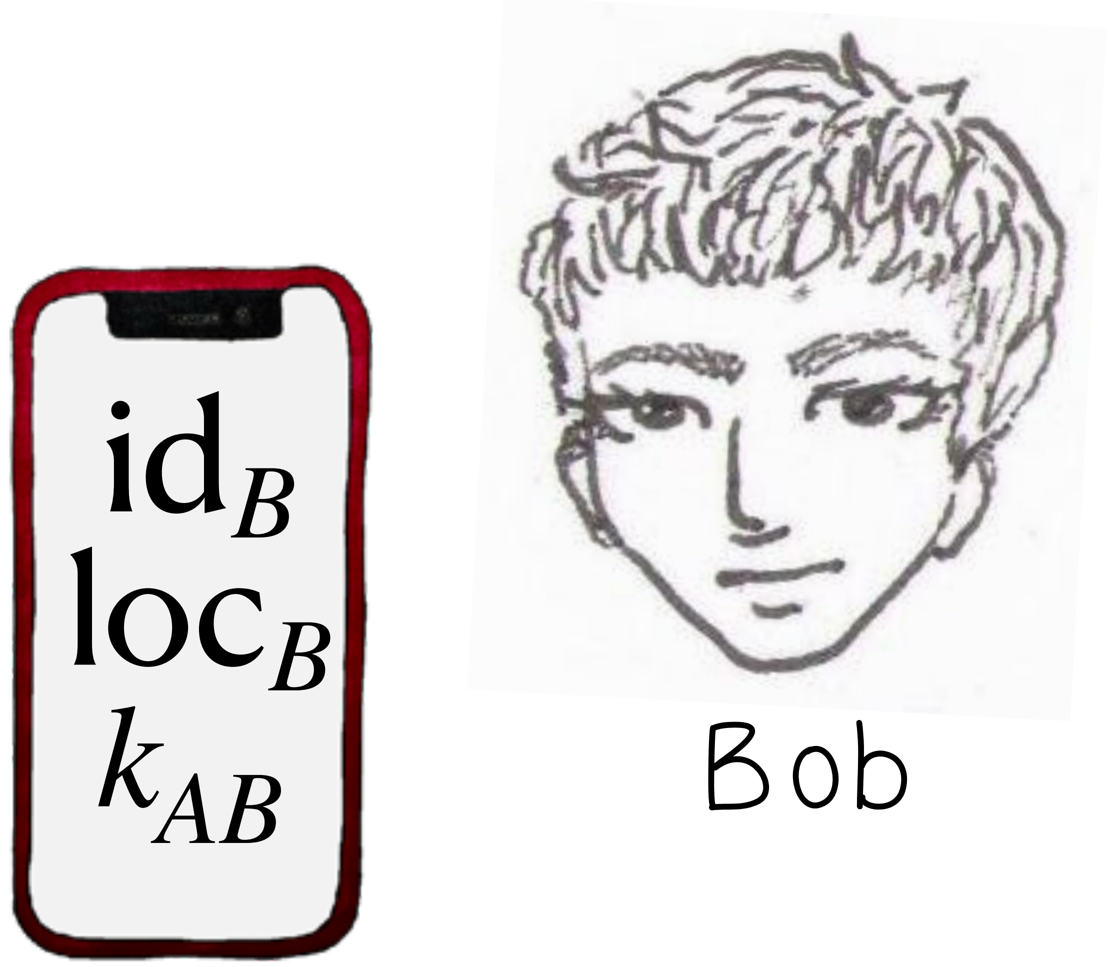


Alice and Bob can run further computations over an authenticated Bluetooth channel.

Ground Trust Ceremony



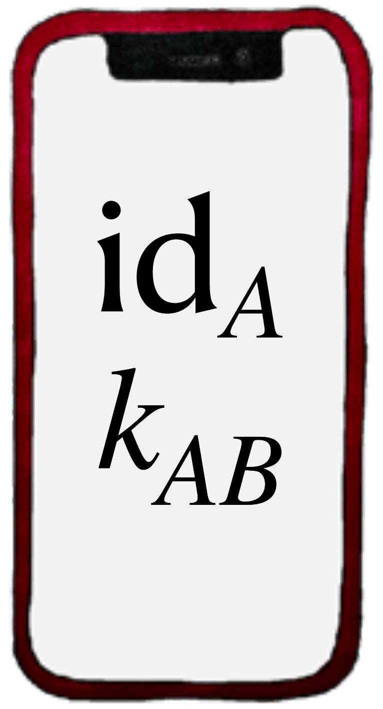
Alice and Bob now share a key that is rooted in their <u>physical interaction</u>.



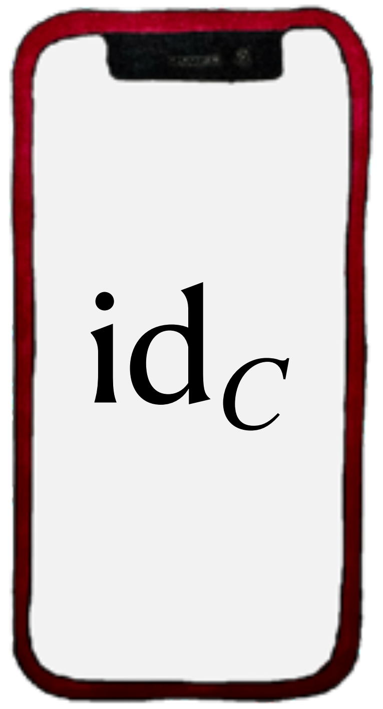
Annotation System

Charlie

Alice

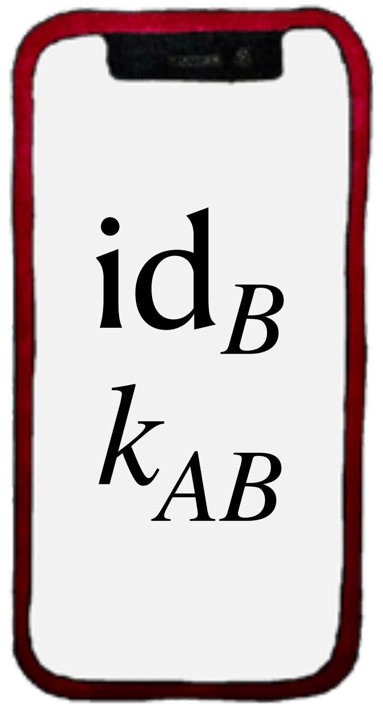


id_A
k_{AB}



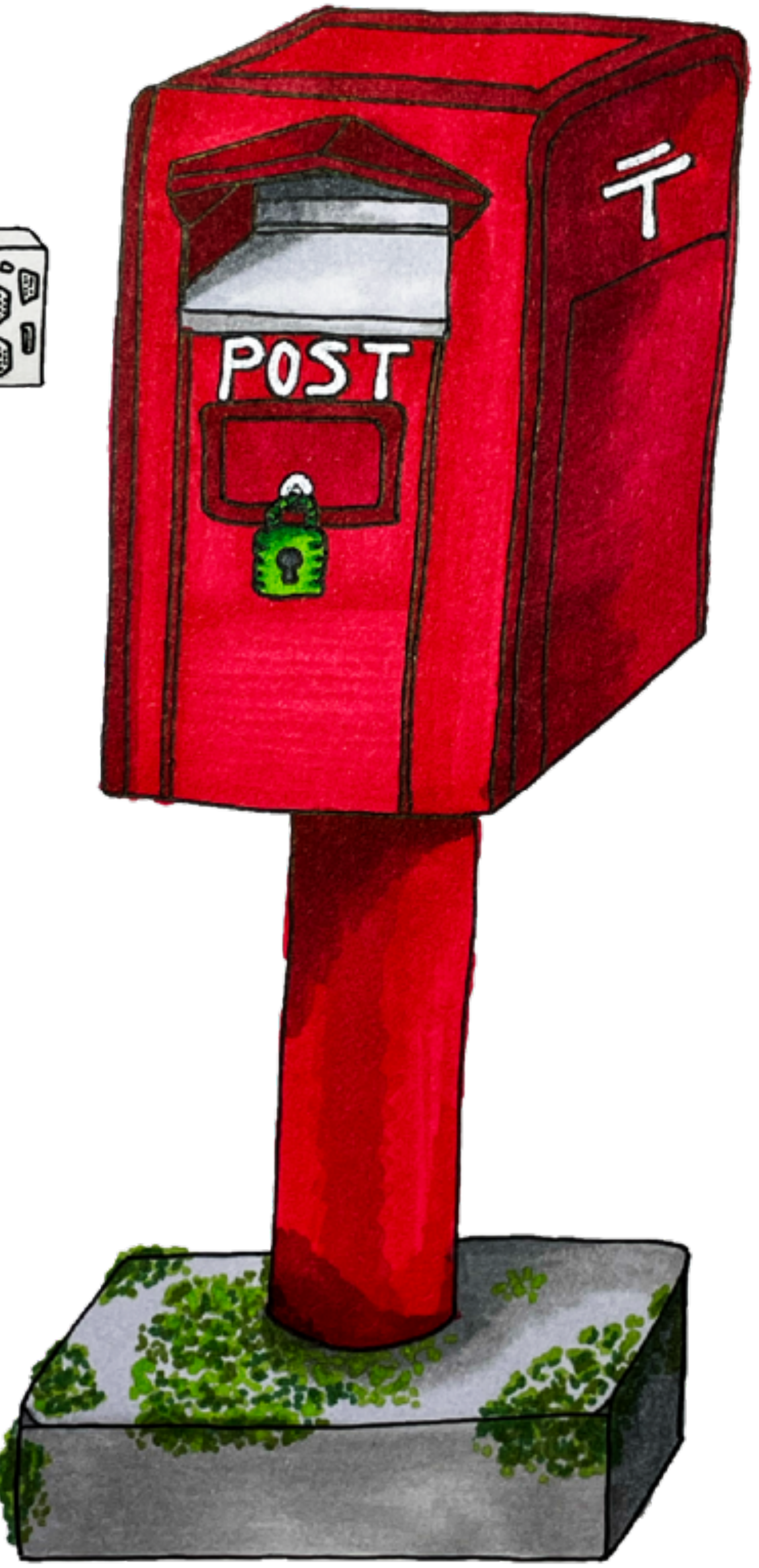
id_C

Bob



id_B
k_{AB}

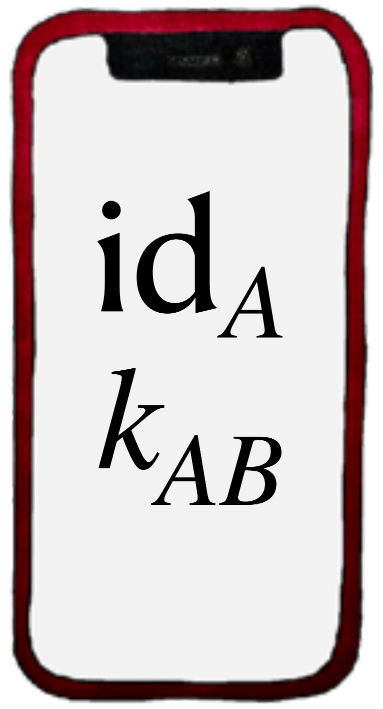
Tigro
Server



Shared Encrypted
Mailbox (EMB)

Annotation System

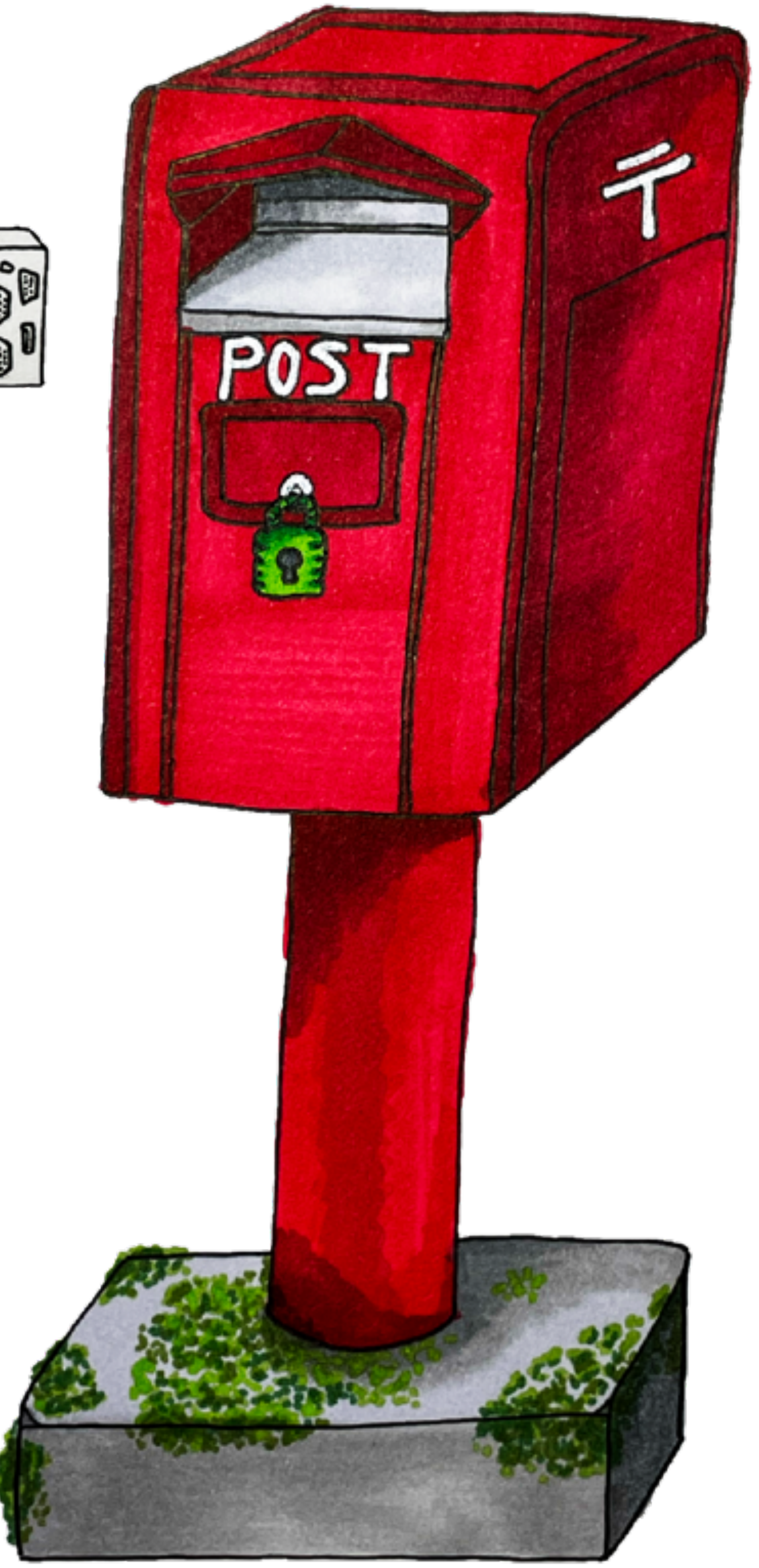
Alice



id_A
k_{AB}

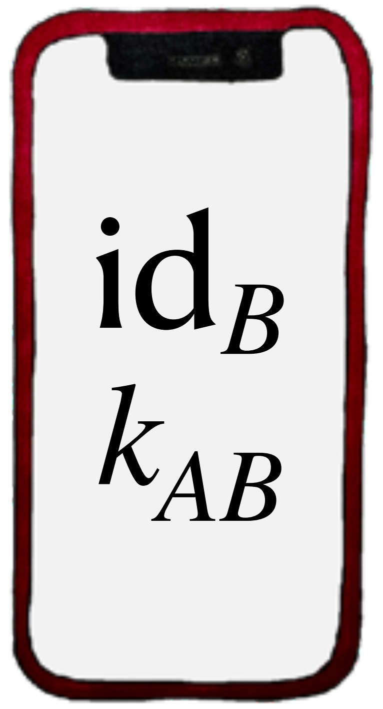
Annotate id_C :
I met them at a
mutual aid event.
They seem
trustworthy.

Tigro
Server



Shared Encrypted
Mailbox (EMB)

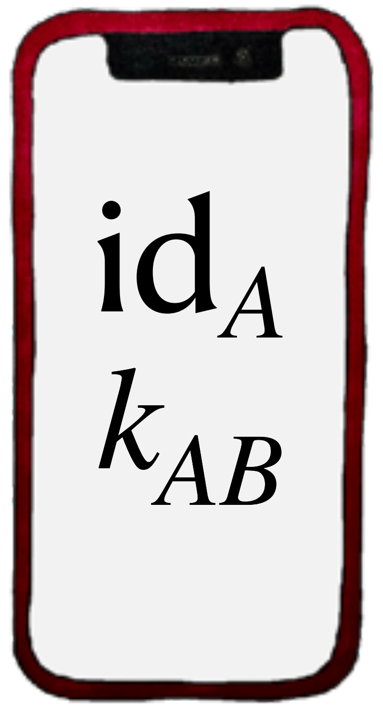
Bob



id_B
k_{AB}

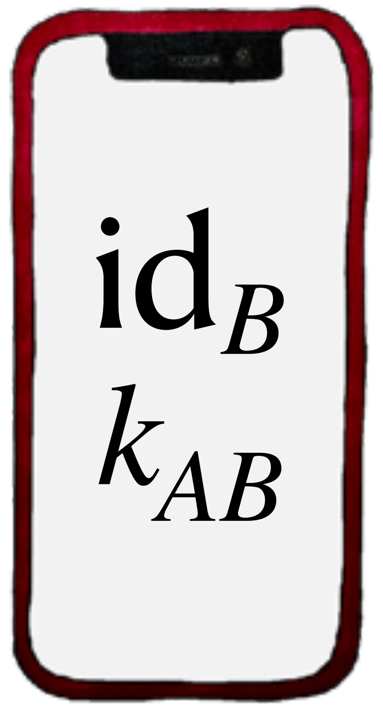
Annotation System

Alice

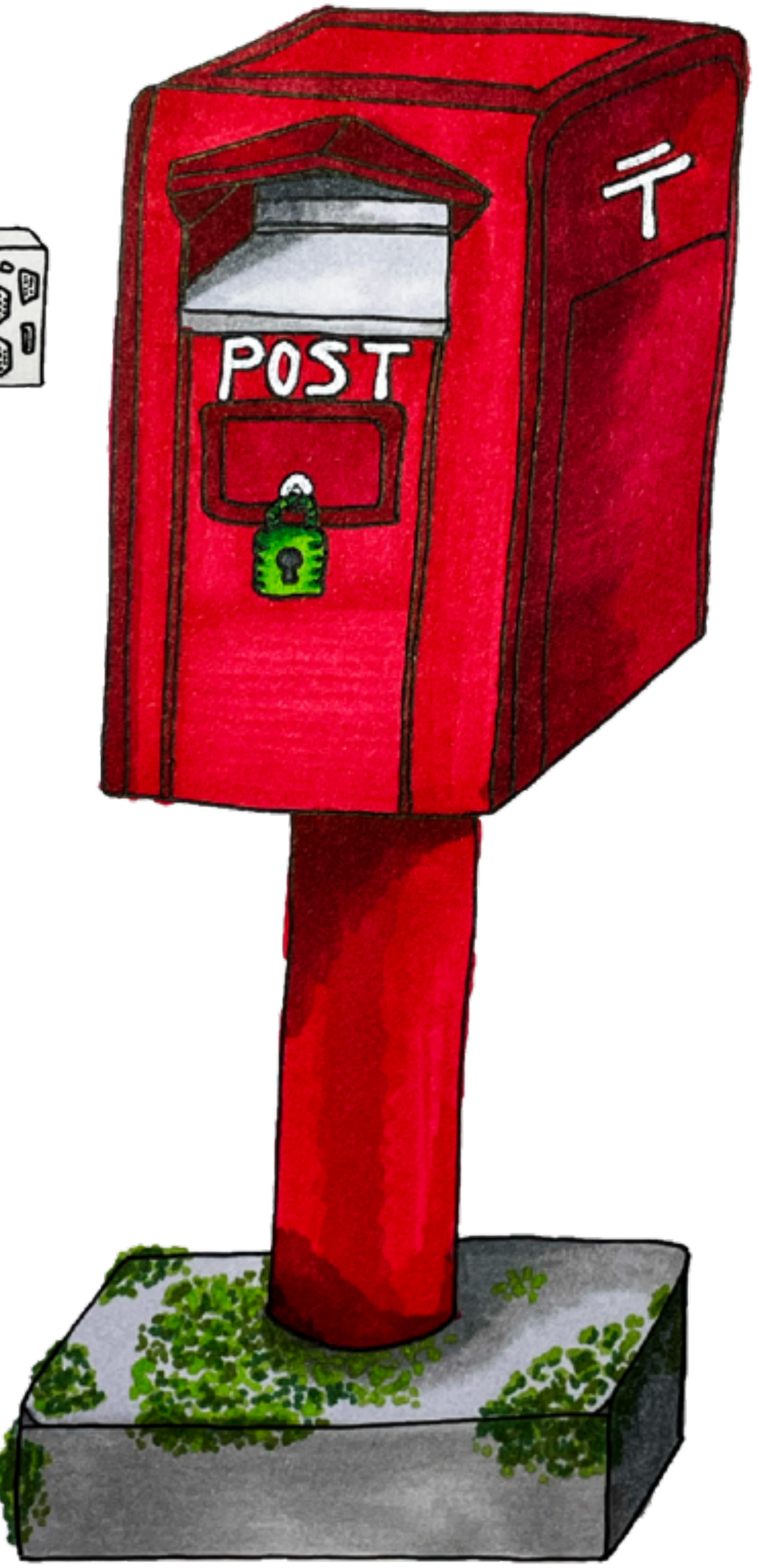


Annotate id_C :
This person
was agitating
at a sit-in.
Vibes were off.

Bob

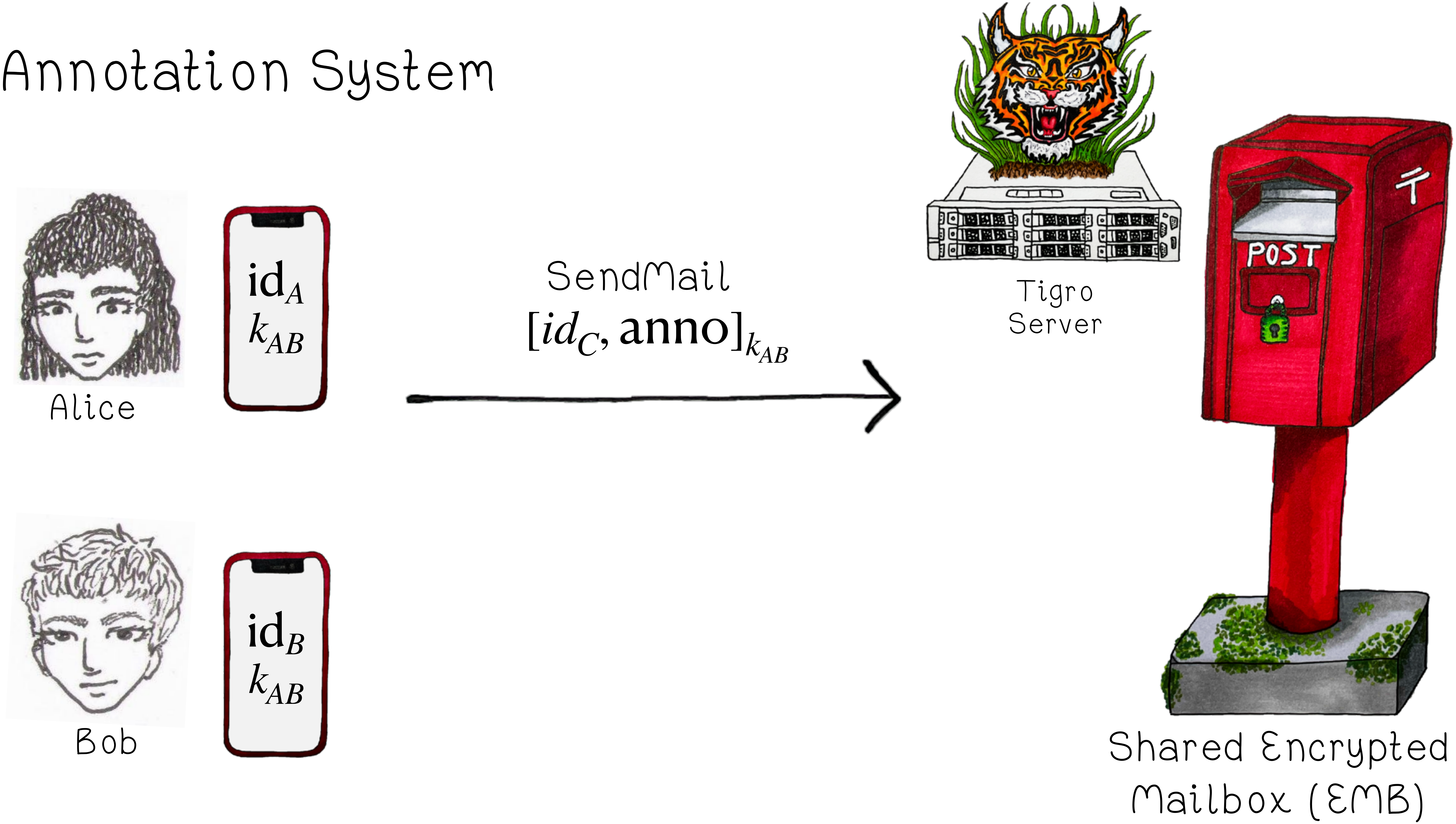


Tigro
Server



Shared Encrypted
Mailbox (EMB)

Annotation System



Alice

id_A
k_{AB}

Bob

id_B
k_{AB}

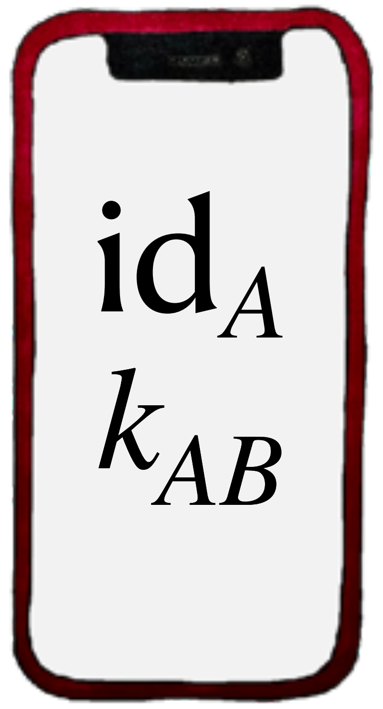
SendMail
$[id_C, \mathbf{anno}]_{k_{AB}}$

Tigro
Server

Shared Encrypted
Mailbox (EMB)

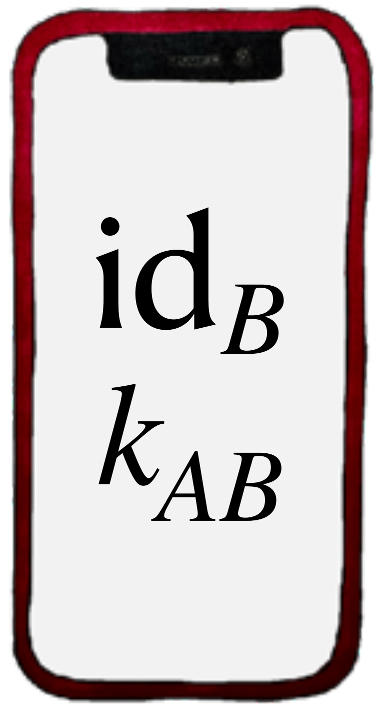
Annotation System

Alice



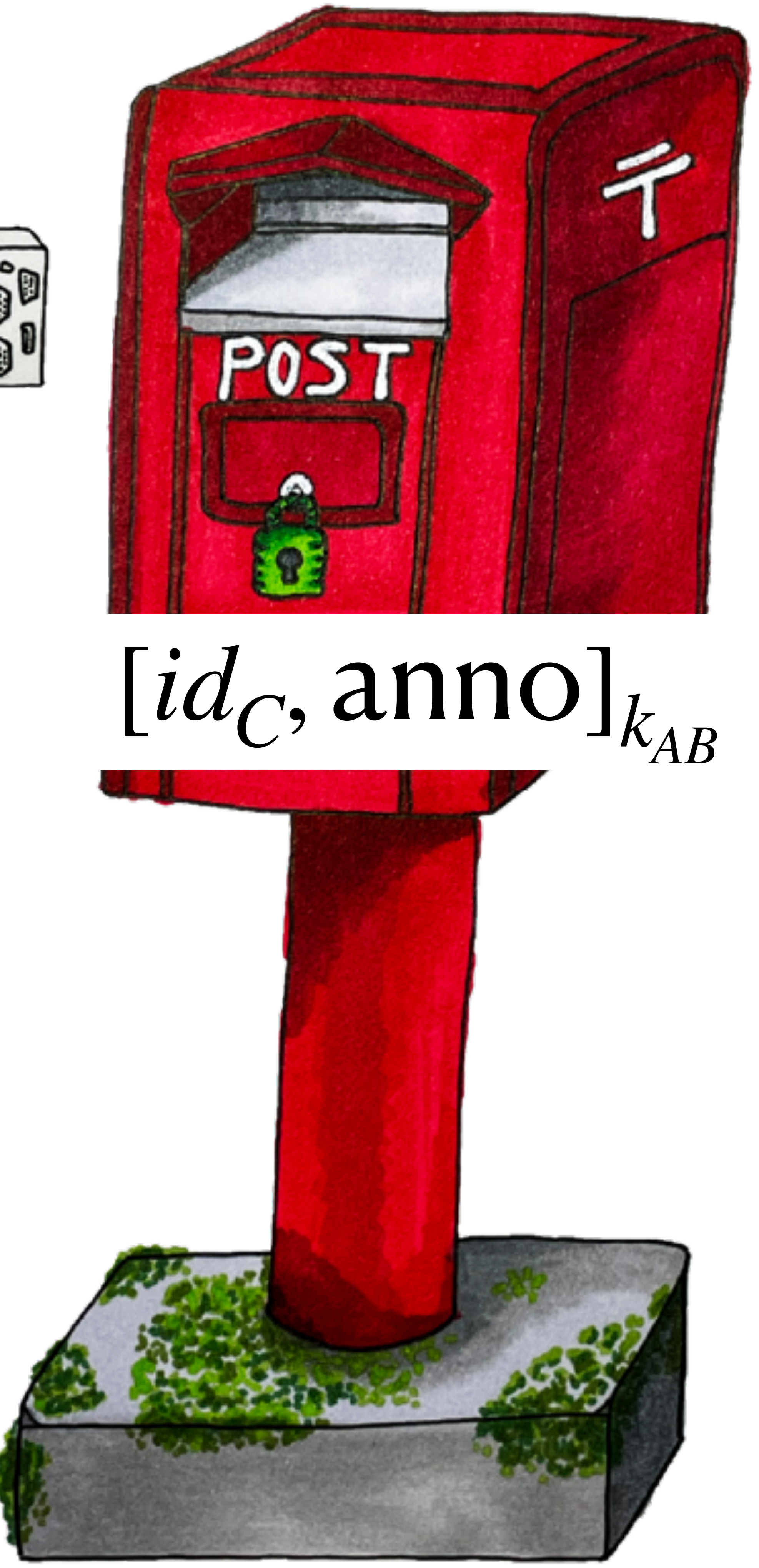
id_A
k_{AB}

Bob



id_B
k_{AB}

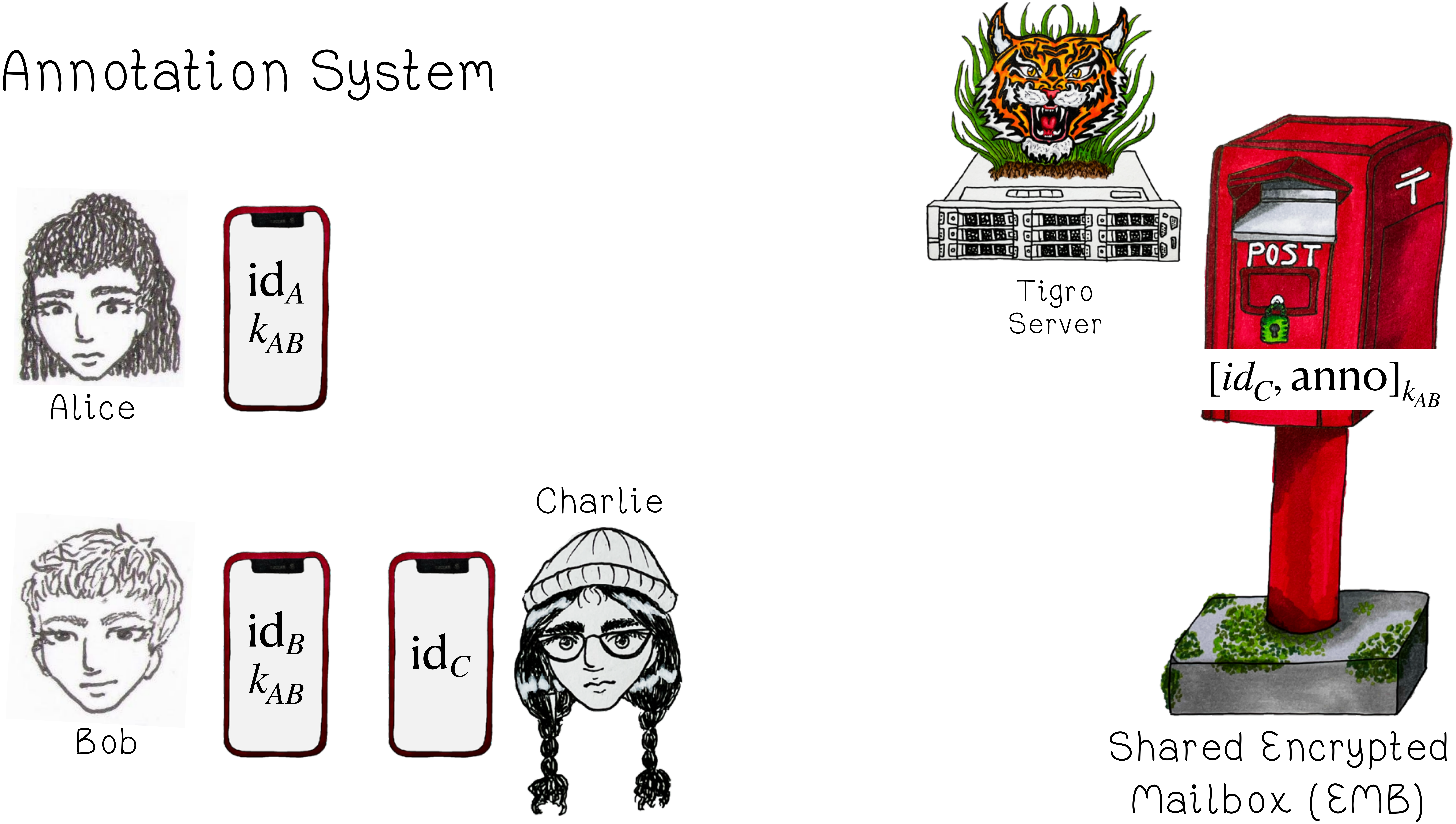
Tigro
Server



$[id_C, \mathrm{anno}]_{k_{AB}}$

Shared Encrypted
Mailbox (EMB)

Annotation System



Alice

id_A
k_{AB}

Bob

id_B
k_{AB}

id_C

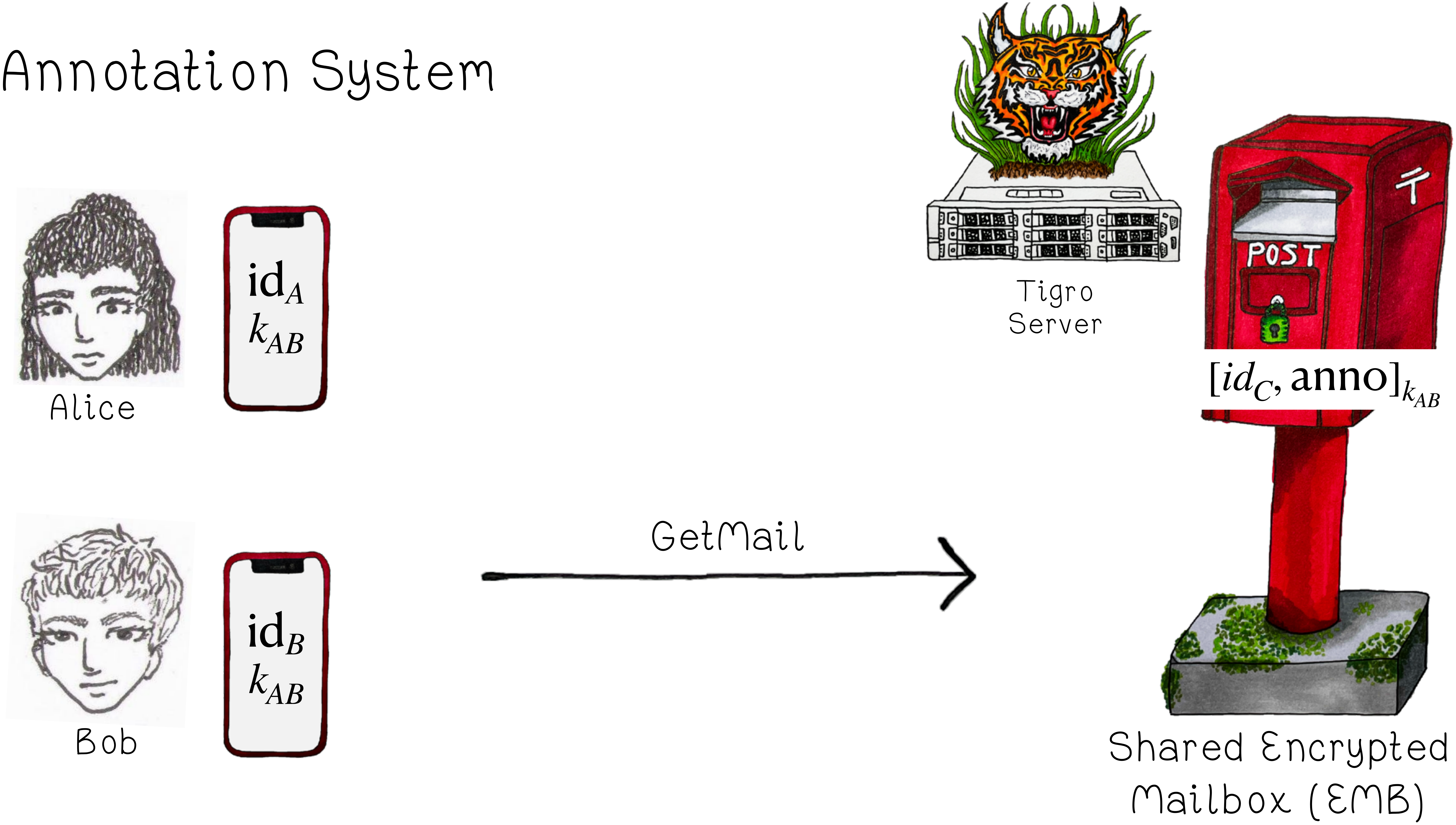
Charlie

Tigro
Server

$[id_C, \mathrm{anno}]_{k_{AB}}$

Shared Encrypted
Mailbox (EMB)

Annotation System



Alice

id_A
k_{AB}

Bob

id_B
k_{AB}

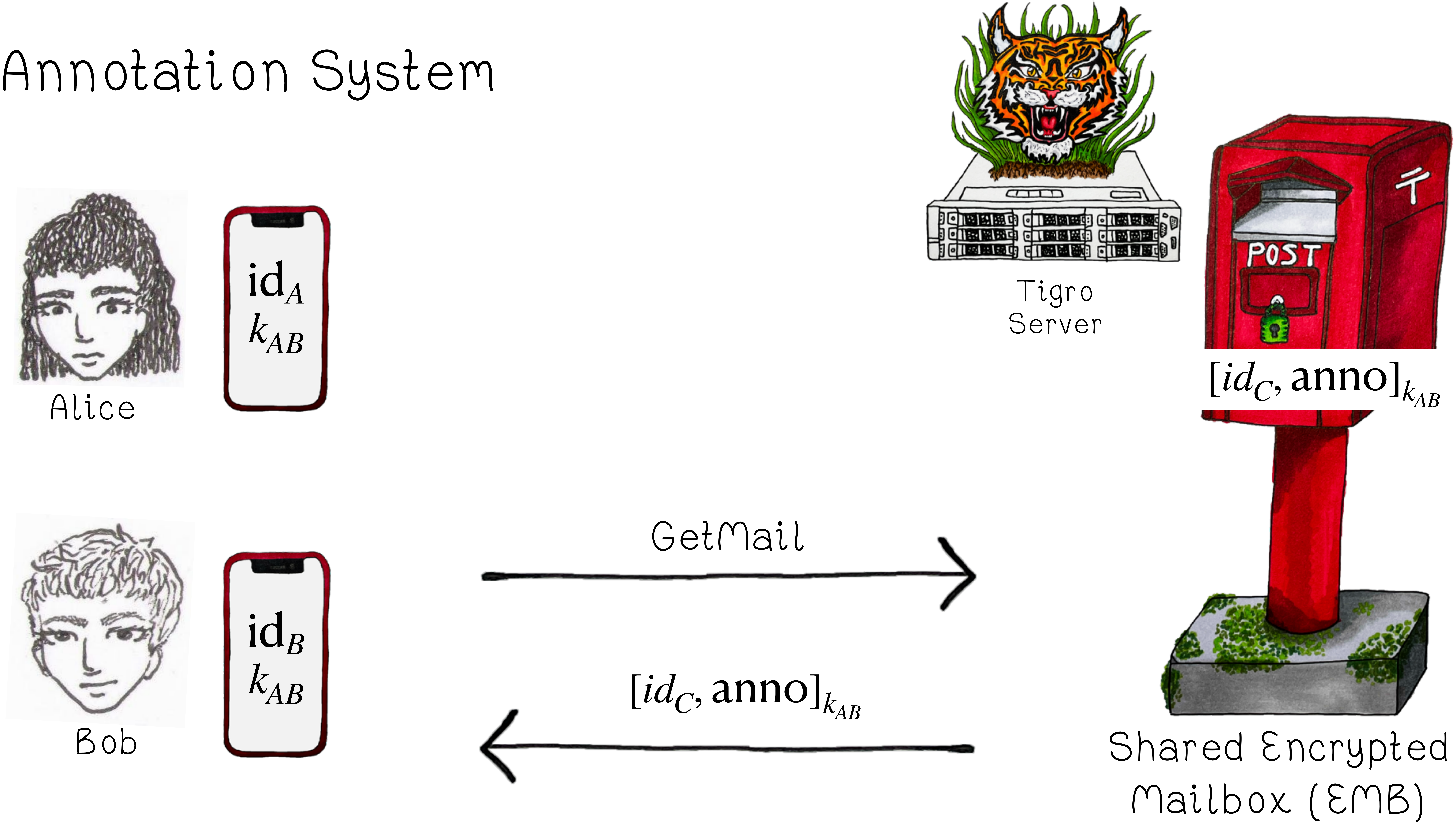
GetMail

Tigro
Server

$[id_C, \mathrm{anno}]_{k_{AB}}$

Shared Encrypted
Mailbox (EMB)

Annotation System


Alice
id_A
k_{AB}
Bob
id_B
k_{AB}
GetMail
$[id_C, \mathrm{anno}]_{k_{AB}}$
Tigro Server
〒
POST
$[id_C, \mathrm{anno}]_{k_{AB}}$
Shared Encrypted Mailbox (EMB)

Annotation System

Alice

id_A
k_{AB}

Event:

Protest

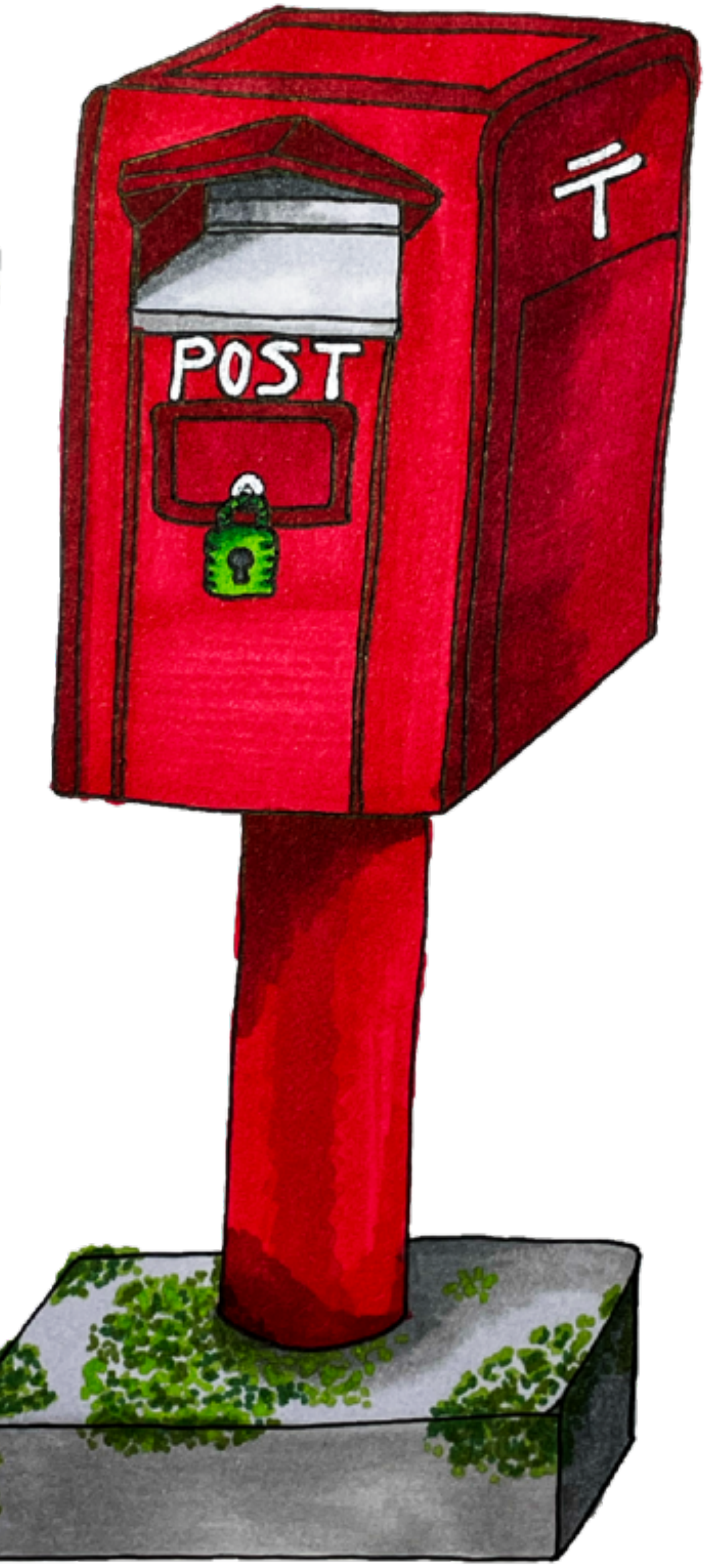
Organizer:

Eve

Bob

id_B
k_{AB}

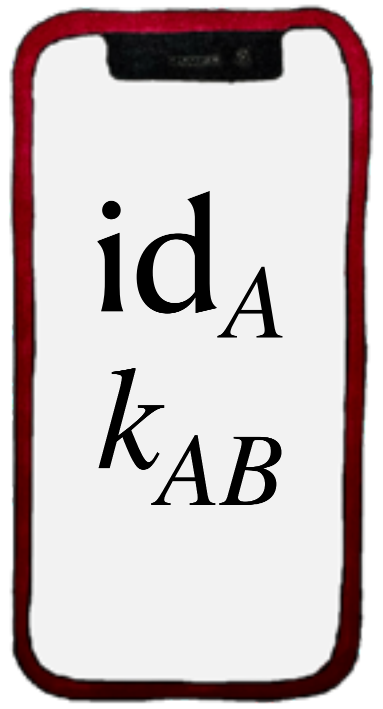
Tigro
Server



Shared Encrypted
Mailbox (EMB)

Annotation System

Alice



$\mathbf{id}_A$

k_{AB}

Event:

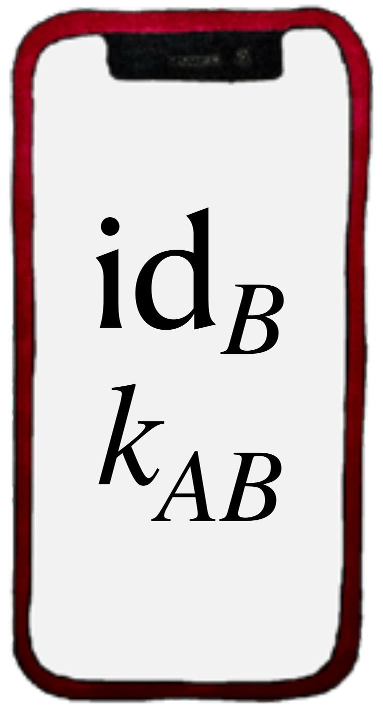
Protest

Organizer:

Eve

$\mathbf{oid}_E$

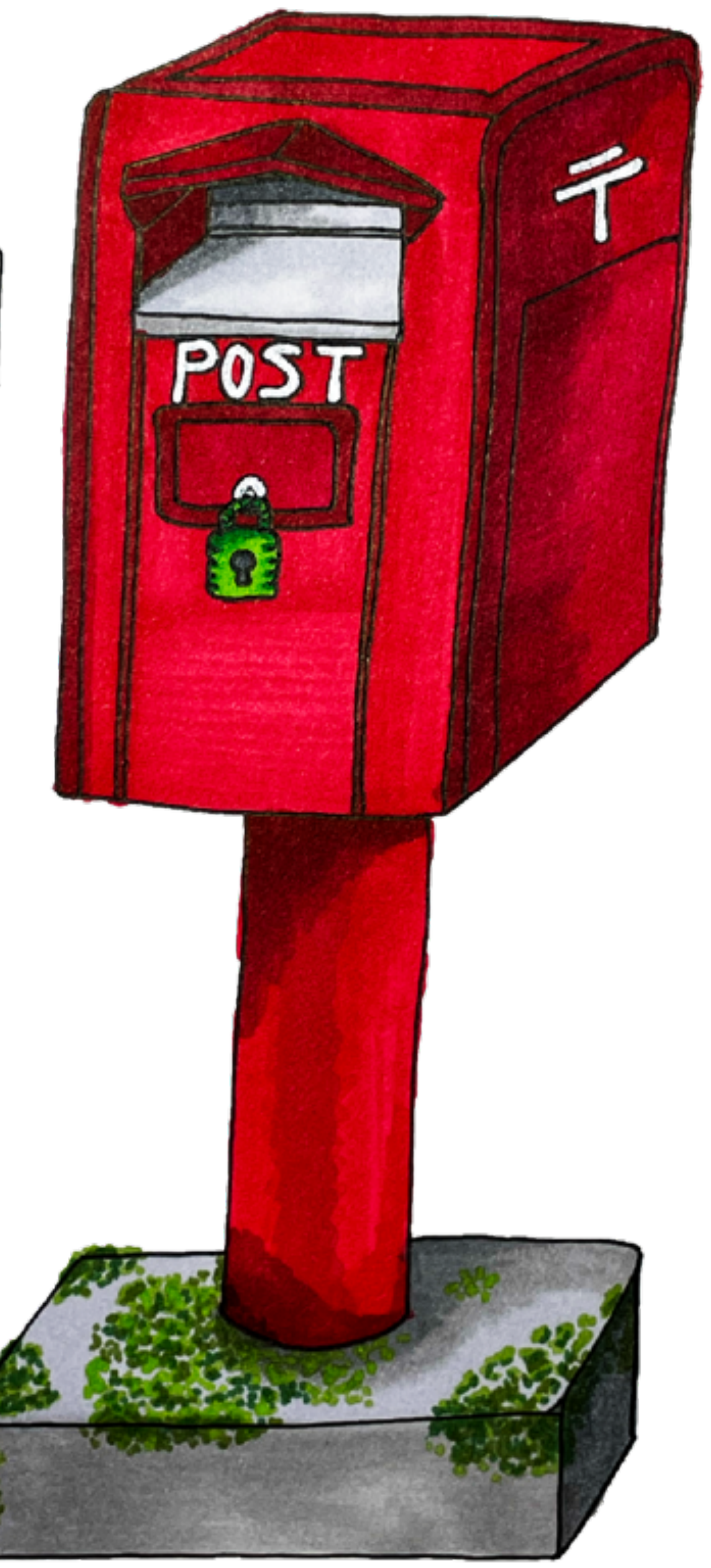
Bob



$\mathbf{id}_B$

k_{AB}

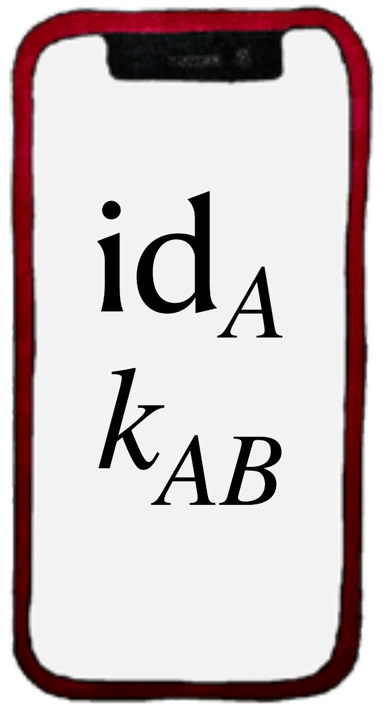
Tigro Server



Shared Encrypted Mailbox (EMB)

Annotation System

Alice

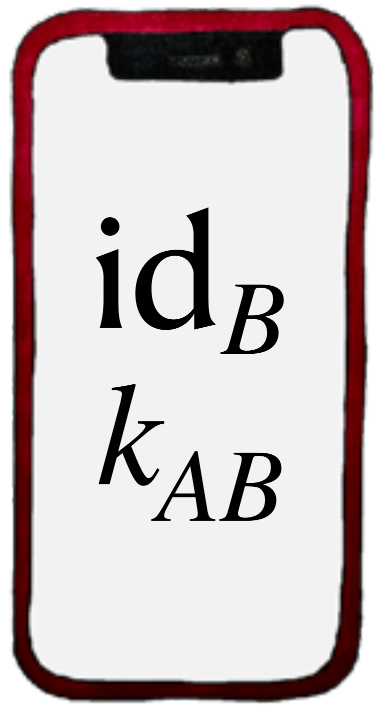


id_A

k_{AB}

Annotate $\mathbf{oid}_E$: This event is being organized by friends. Hope to see you there.

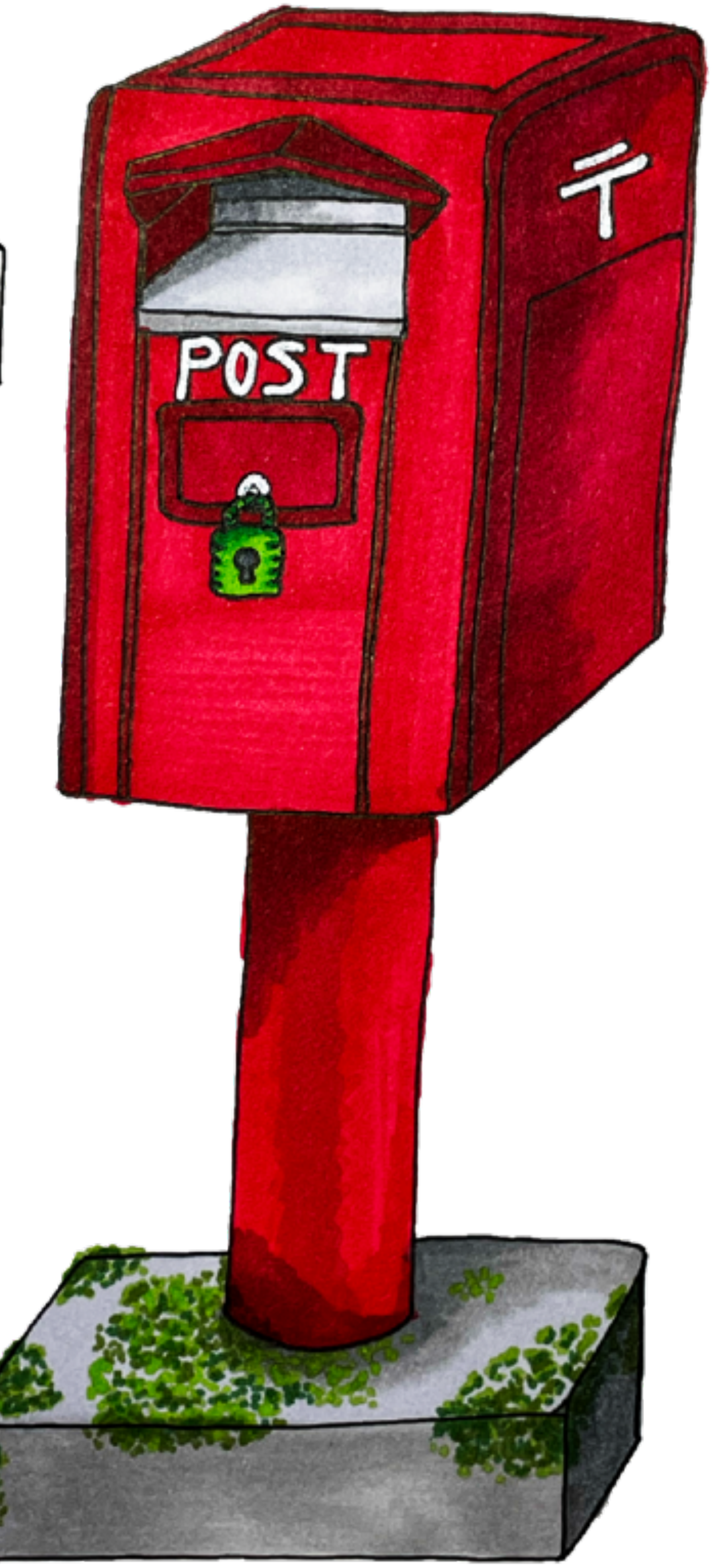
Bob



id_B

k_{AB}

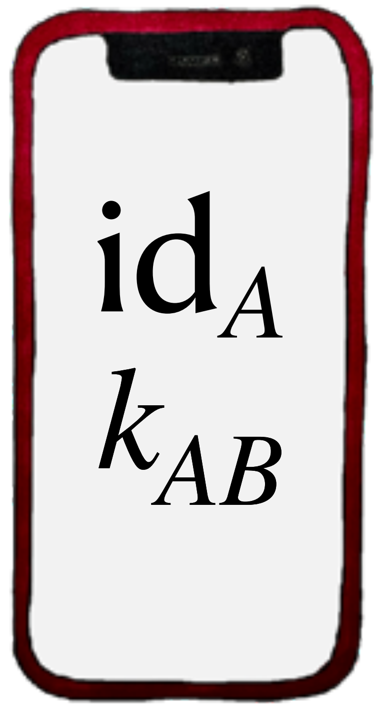
Tigro Server



Shared Encrypted Mailbox (EMB)

Annotation System

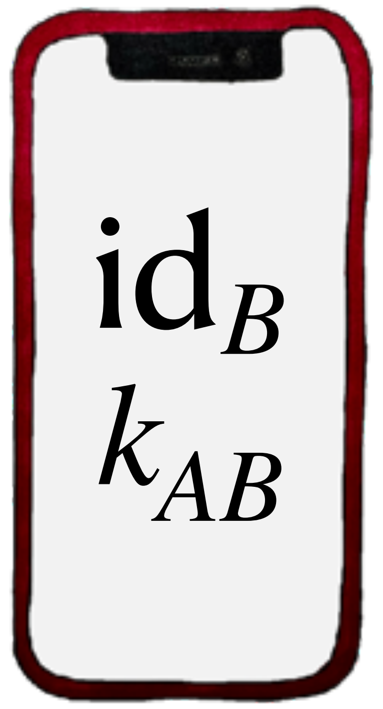
Alice



$\mathbf{id}_A$
k_{AB}

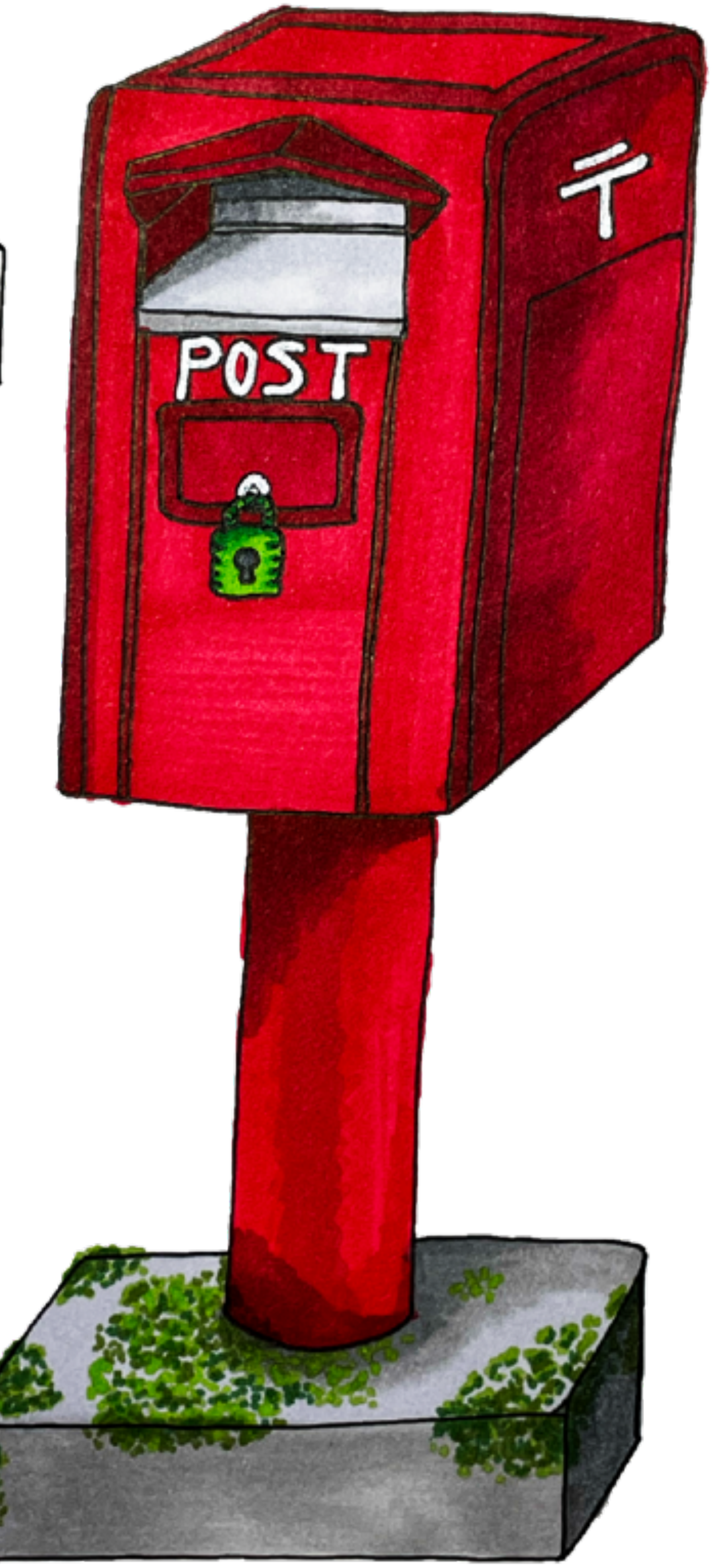
Annotate $\mathbf{oid}_E$: No one I know can confirm the identity of Eve. Proceed with caution.

Bob



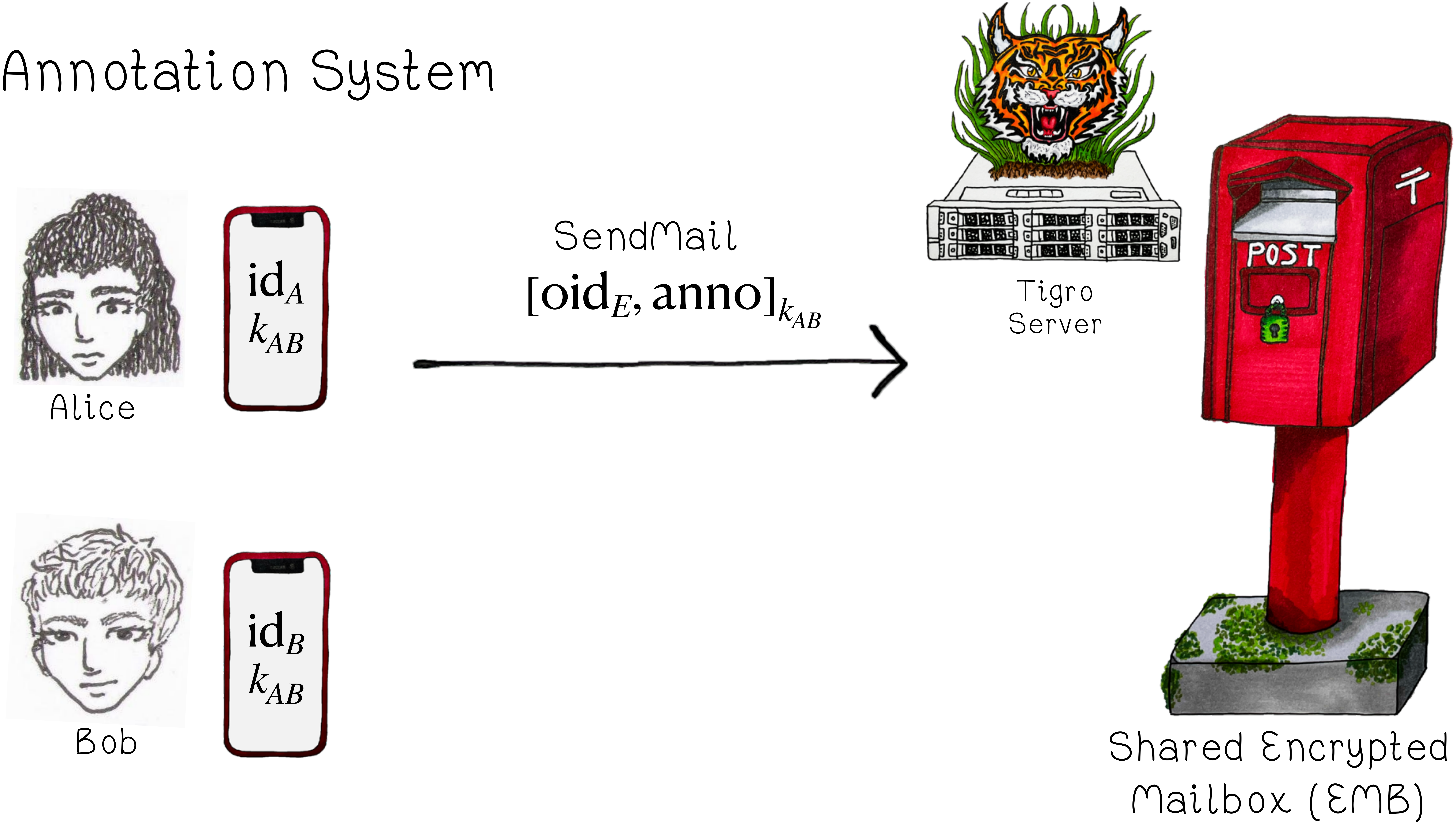
$\mathbf{id}_B$
k_{AB}

Tigro
Server



Shared Encrypted
Mailbox (EMB)

Annotation System



Alice

id_A
k_{AB}

SendMail
$[\mathrm{oid}_E, \mathrm{anno}]_{k_{AB}}$

Tigro
Server

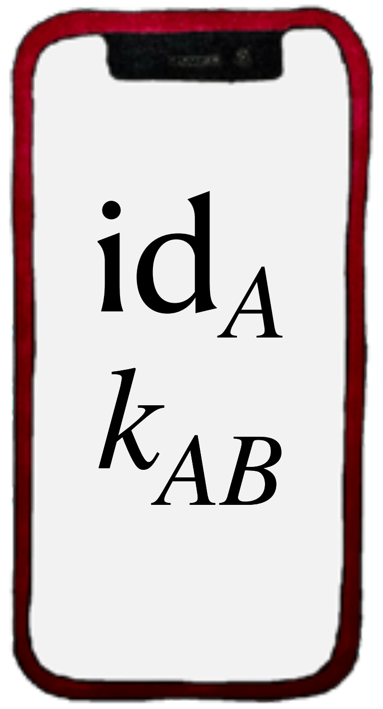
Bob

id_B
k_{AB}

Shared Encrypted
Mailbox (EMB)

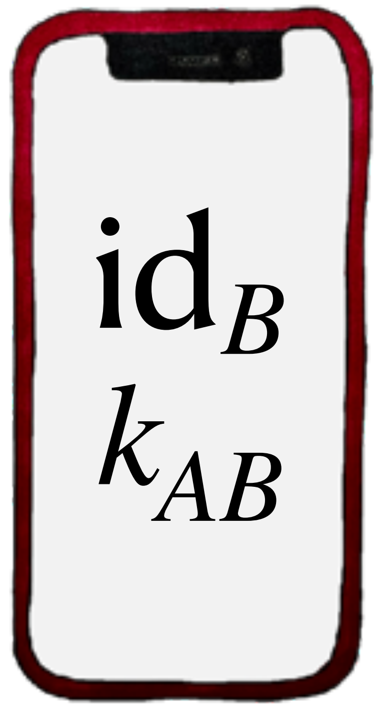
Annotation System

Alice



id_A
k_{AB}

Bob



id_B
k_{AB}

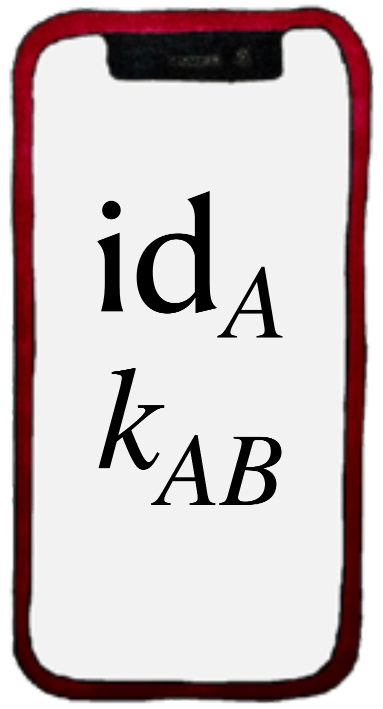
Tigro
Server

$[\mathrm{oid}_E, \mathrm{anno}]_{k_{AB}}$

Shared Encrypted
Mailbox (EMB)

Annotation System

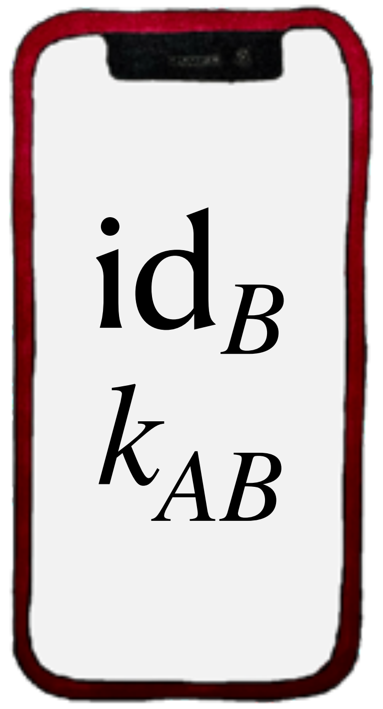
Alice



id_A

k_{AB}

Bob



id_B

k_{AB}

Event:

Protest

Organizer:

Eve

$\mathbf{oid}_E$

Tigro Server

$[\mathrm{oid}_E, \mathrm{anno}]_{k_{AB}}$

Shared Encrypted Mailbox (EMB)

Annotation System

Alice

id_A
k_{AB}

Bob

id_B
k_{AB}

Event:

Protest

Organizer:

Eve

$\mathbf{oid}_E$

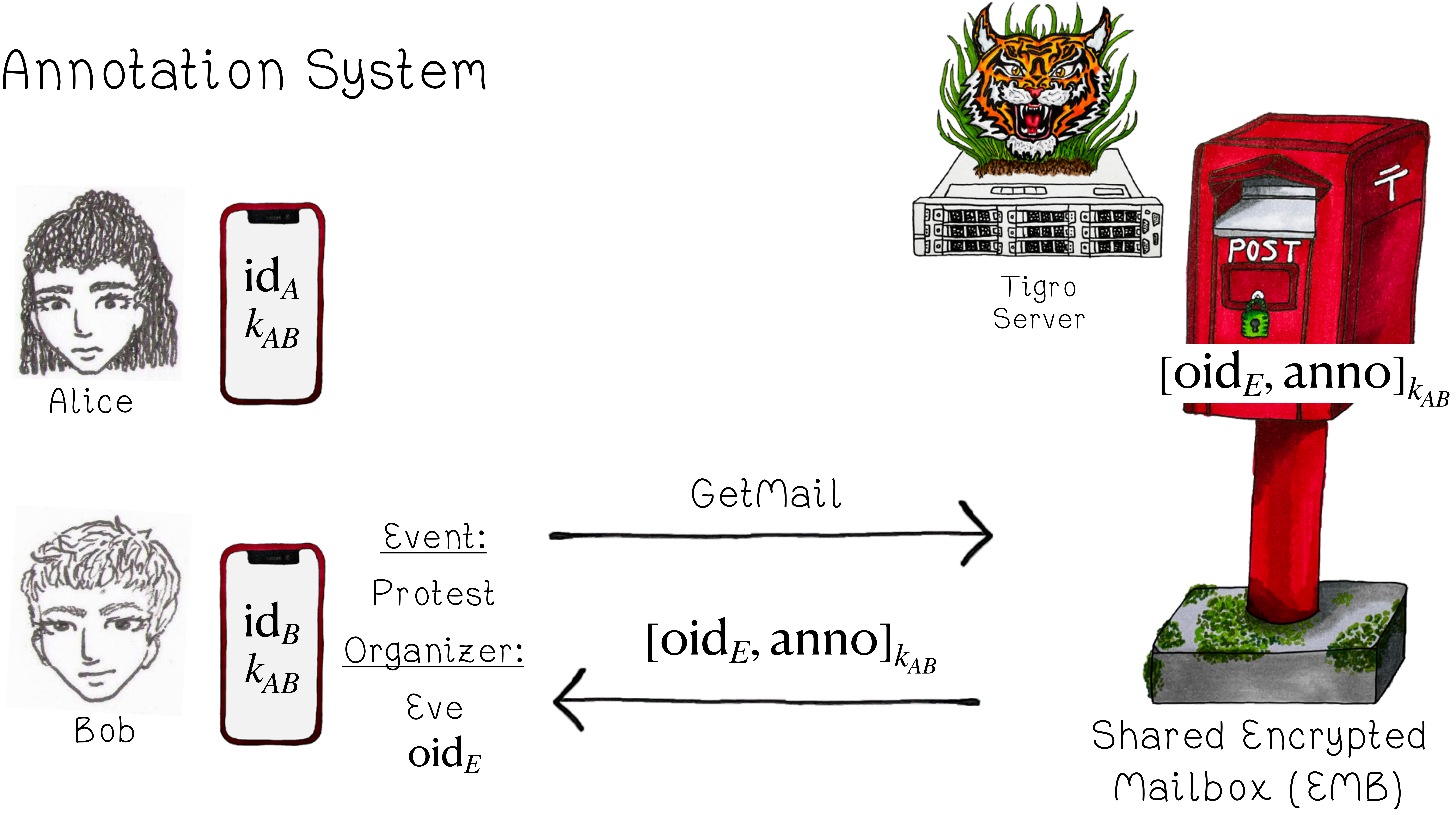
GetMail →

Tigro Server

$[\mathrm{oid}_E, \mathrm{anno}]_{k_{AB}}$

Shared Encrypted Mailbox (EMB)

Annotation System



Alice

id_A
k_{AB}

Bob

id_B
k_{AB}

Event:
Protest
Organizer:
Eve
$\mathbf{oid}_E$

GetMail

$[\mathrm{oid}_E, \mathrm{anno}]_{k_{AB}}$

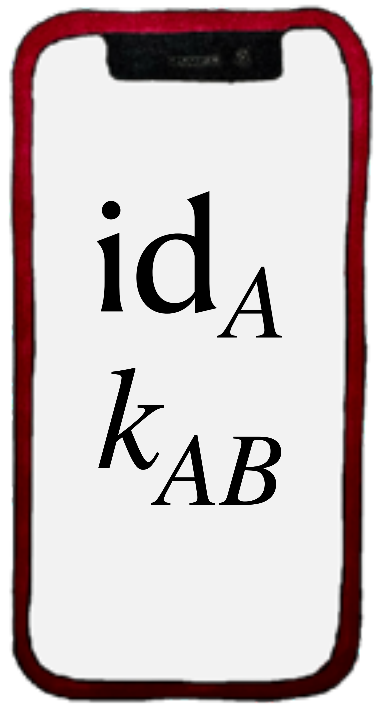
Tigro
Server

$[\mathrm{oid}_E, \mathrm{anno}]_{k_{AB}}$

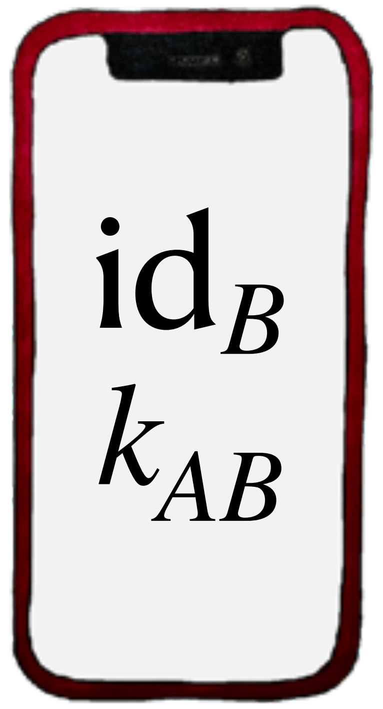
Shared Encrypted
Mailbox (EMB)

Annotation System

Alice

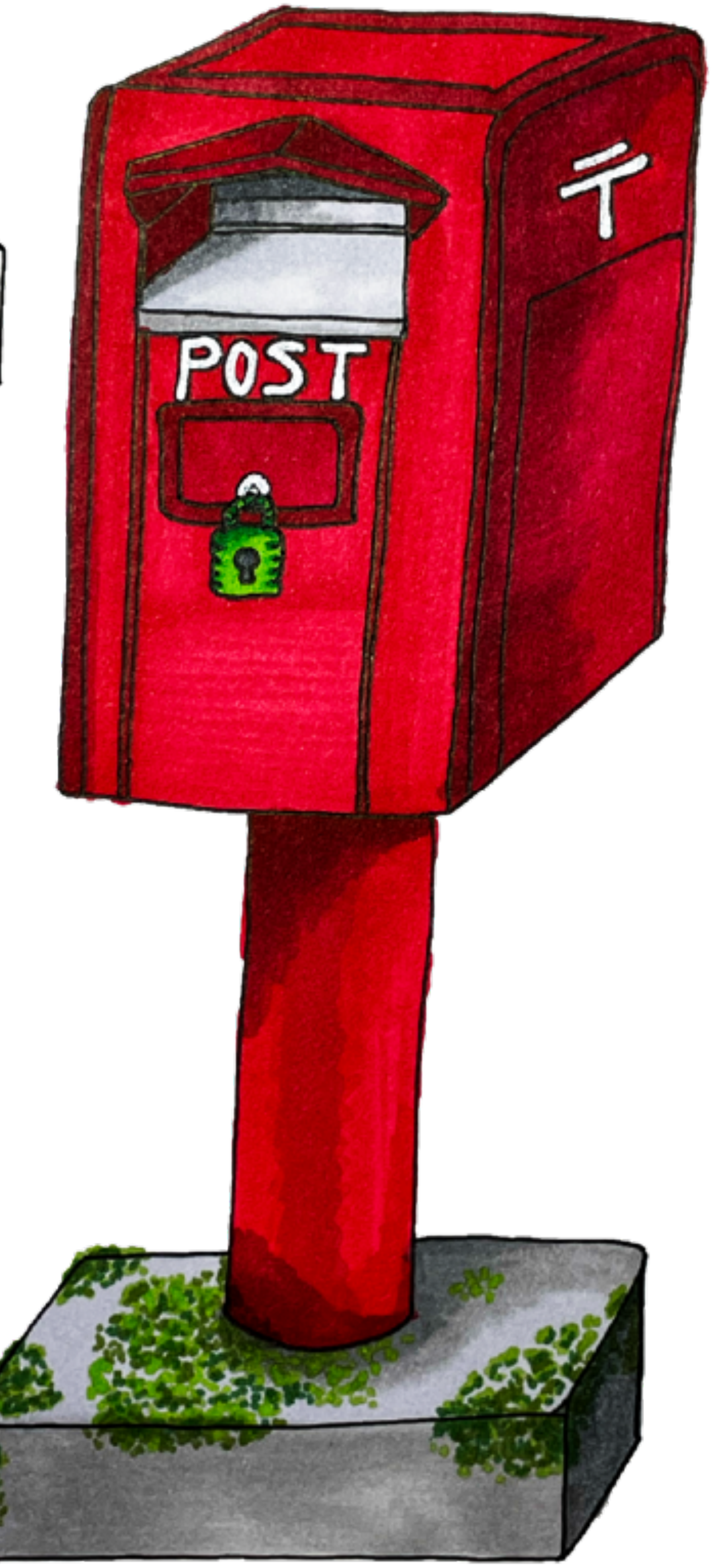


Bob



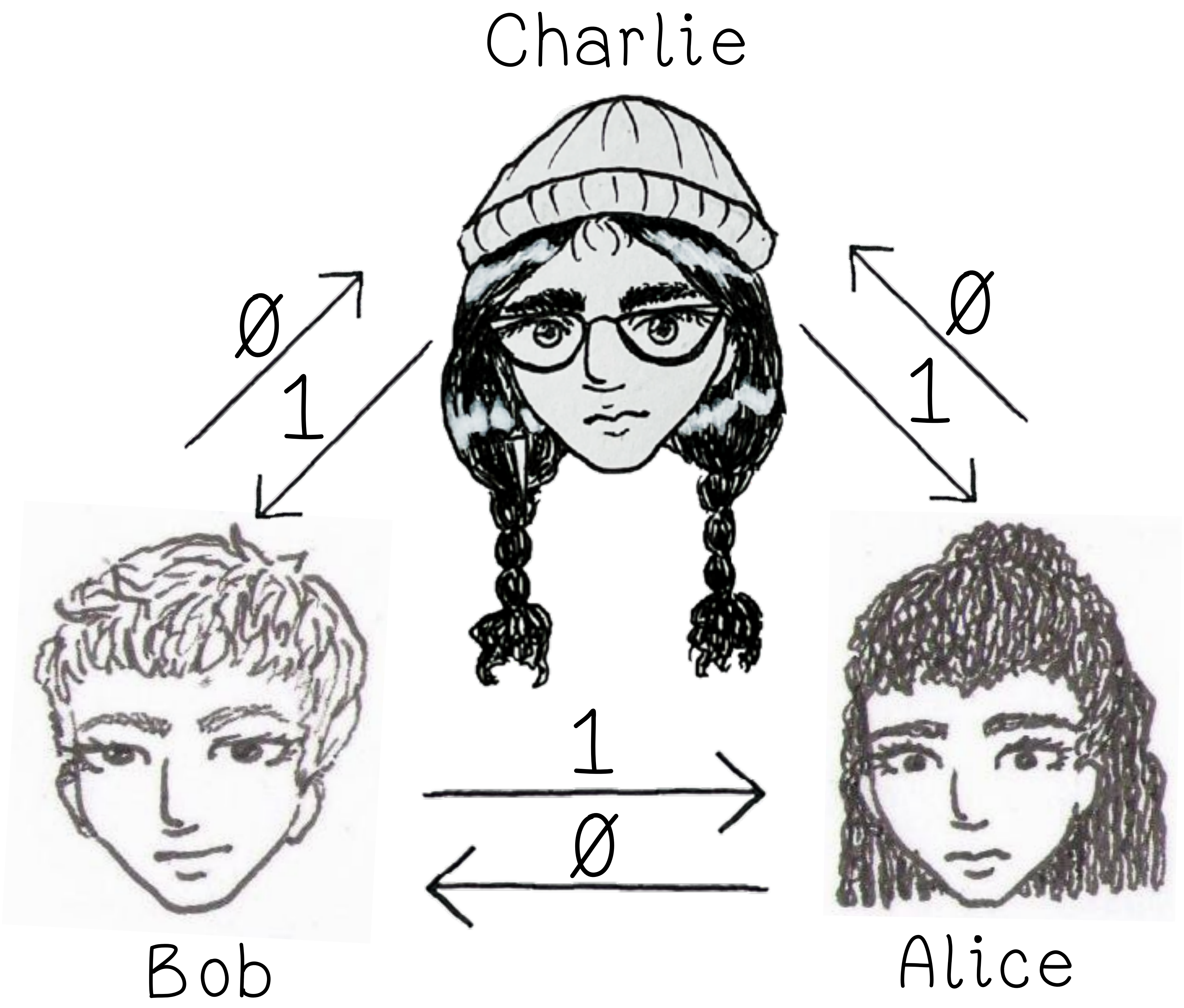
Alice and Bob can digitally & confidentially share trust assessments of any person, place, or thing.

Tigro Server



Shared Encrypted Mailbox (EMB)

Trust Metrics Over Social Networks



Tentative Hypothesis:

Over a grounded social network graph, the Hyperlink-Induced Topic Search (HITS) algorithm can meaningfully measure a person's:

- Connectivity (physical proximity) to trusted organizers (Hub Measure)
- Leadership role in relation to others (Authority Measure)

Disclaimers: Quantifiable metrics are still functions of qualitative metrics; Edge weights are up for debate (eg. could replace Ø/1 with a survey); Digitizing this data (even in encrypted form) may be too risky.

tigro Long-Term Goals

*Help with work & funding welcome!

Phase Ø: Finish analysis of the cryptographic protocols

Phase 1: Prototype protocols and conduct user studies*

- Implementation: toward multi-platform design & security
- User studies: capturing the right notion of trust & UI/UX

Phase 2: Build out applications, more user studies*

- Implementation: context-dependent applications & security
- User studies: assess relevance of specific designs & UI/UX

What kind of world do we want to build with our work?

Thank you for listening!

Interested in getting involved in the tigro project? Please find me! Or, email leah_rosenbloom@brown.edu

Resources

1. Martin R Albrecht, Jorge Blasco, Rikke Bjerg Jensen, and Lenka Mareková. Collective information security in large-scale urban protests: the case of hong kong. *arXiv preprint arXiv:2105.14869*, 2021.
2. Glencora Borradaile. *Defend Dissent.* Oregon State University Corvallis, 2021.
3. Philip N Howard, Aiden Duffy, Deen Freelon, Muzammil M Hussain, Will Mari, and Marwa Maziad. Opening closed regimes: what was the role of social media during the arab spring? *Available at SSRN 2595096*, 2011.
4. Seny Kamara. *COINTELPRO.* Algorithms for the People, 2020.
5. Seny Kamara. *Crypto for the People Invited Talk.* The International Association for Cryptologic Research, 2020.
6. Seny Kamara, Kweku Kwegyir-Aggrey, and Lucy Qin. *Algorithms for the People Course Syllabus.* Brown University, 2021.
7. Tetyana Lokot. Be safe or be seen? how russian activists negotiate visibility and security in online resistance practices. *Surveillance & Society*, 16(3):332–346, 2018.
8. Phillip Rogaway. The moral character of cryptographic work. *Cryptology ePrint Archive*, 2015.
9. Leah Rosenbloom. Toward secure social networks for activists. In *Moving technology ethics at the forefront of society, organisations and governments*, pages 491–502. ETHICOMP, 2021.
10. Leah Namisa Rosenbloom. Activists want better, safer technology. *arXiv preprint arXiv:2209.01273*, 2022.