Cryptography, The Internet, and Grassroots Organizing

Seny Kamara
Leah Namisa Rosenbloom*

IETF 116
Yokohama, Japan

*speaker

"Cryptography rearranges power"

–Phillip Rogaway

Cryptography, the internet, and technology in general have the potential to rearrange power.

Power for whom?

To what ends?

How do we, as people who create and maintain powerful technologies, understand systems of power?

How does that understanding inform our priorities, threat modeling, and design choices?

How might we work toward building power for communities?

Protocol Design 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, The Internet, and Grassroots Organizing

- Introduction
- Protocol Design 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.

Project Cybersyn

Chile (1971-1973): Popular Unity governemnt envisions distributed decision-making platform

Grassroots Economy: Workers speak straight to the government

An Alternate Vision of the Internet

- Decentralized, worker-owned
- Secondary plan for households
- Destroyed in military coup (1973)

Image Credits: Rama, Jamie (2010)

Operation Vula

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

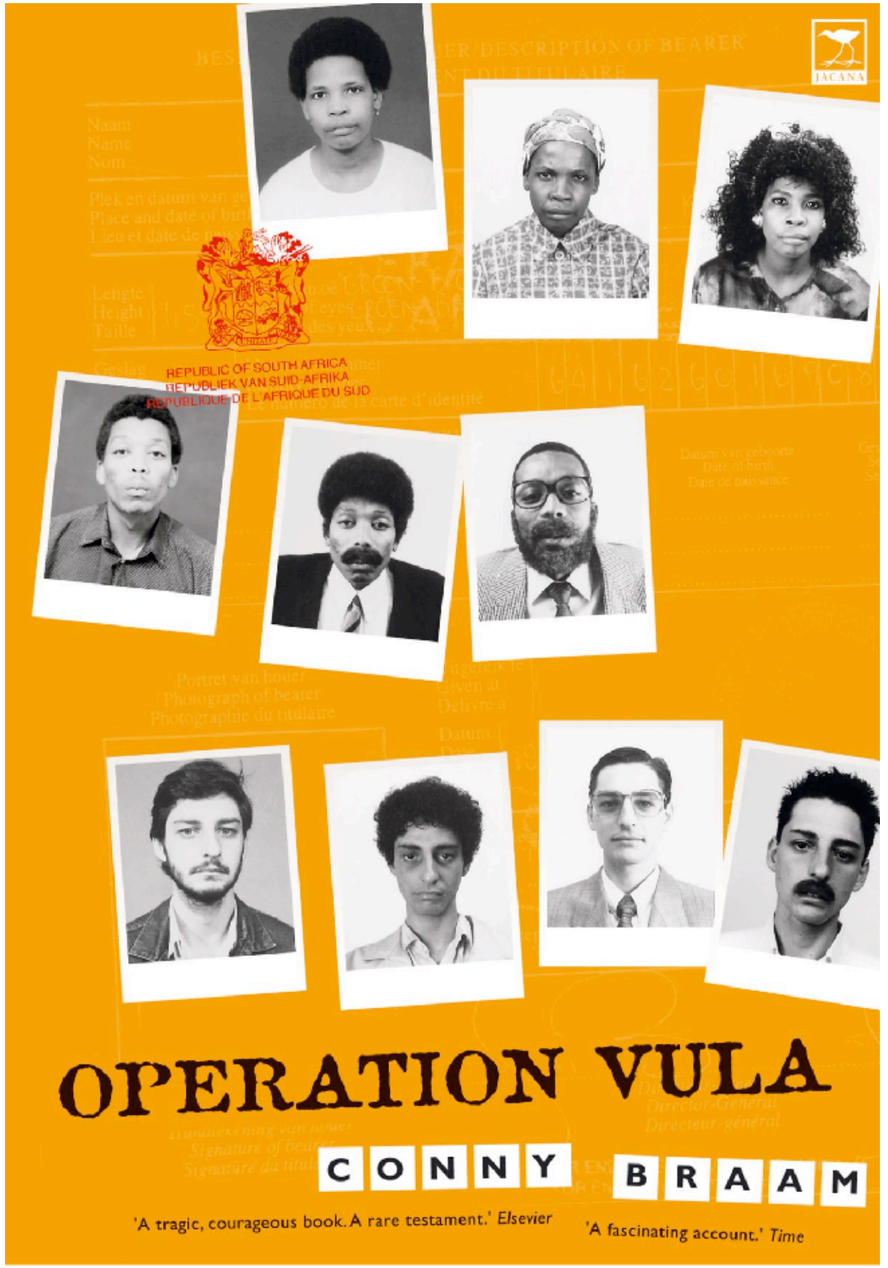


Image Credits: Jacana Media (2004), AP Photo/Udo Weitz, File (1990) via The Washington Post (2019)

Operation Vula

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

Requirements: Asysnchronous, Covert, Long Distance, Public

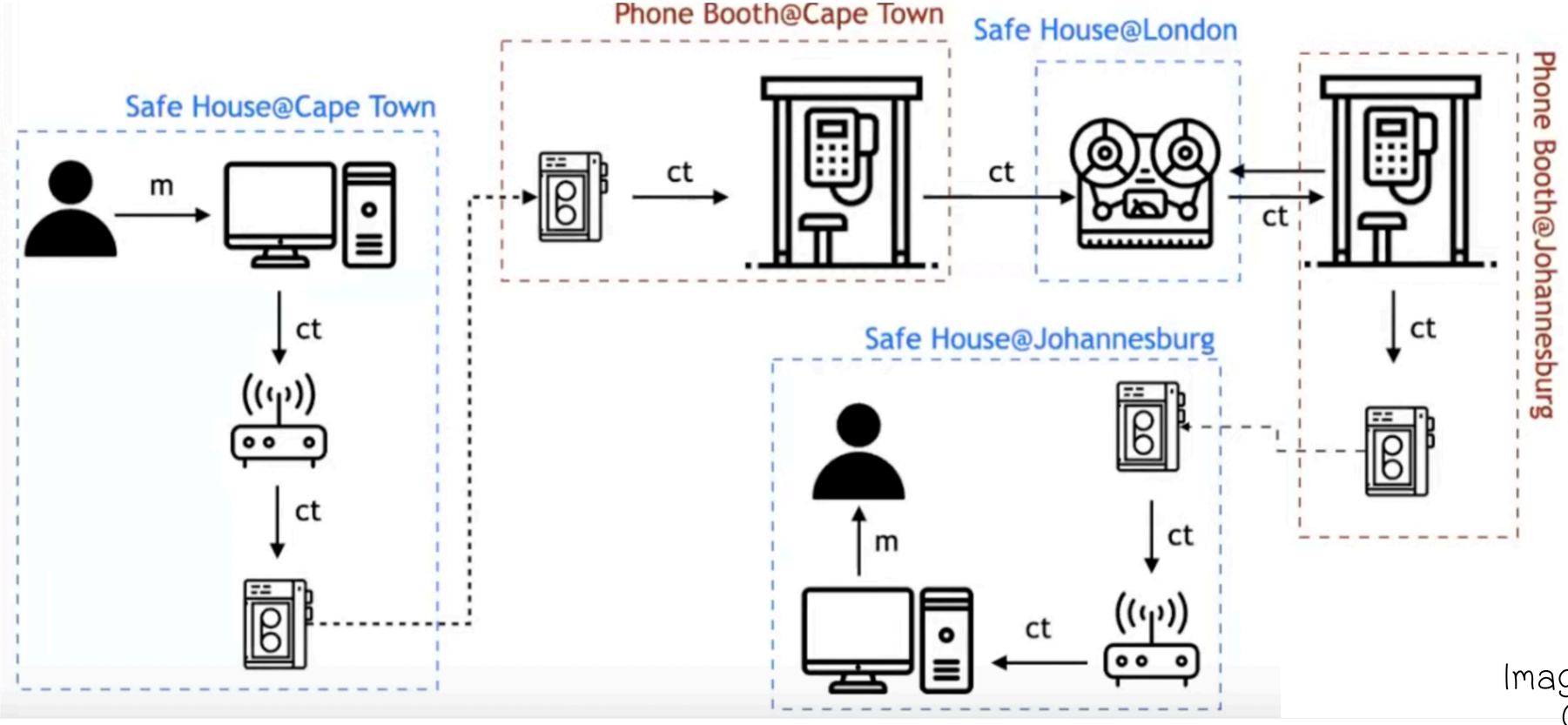


Image Credits: Kamara, CRYPTO (2020)

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

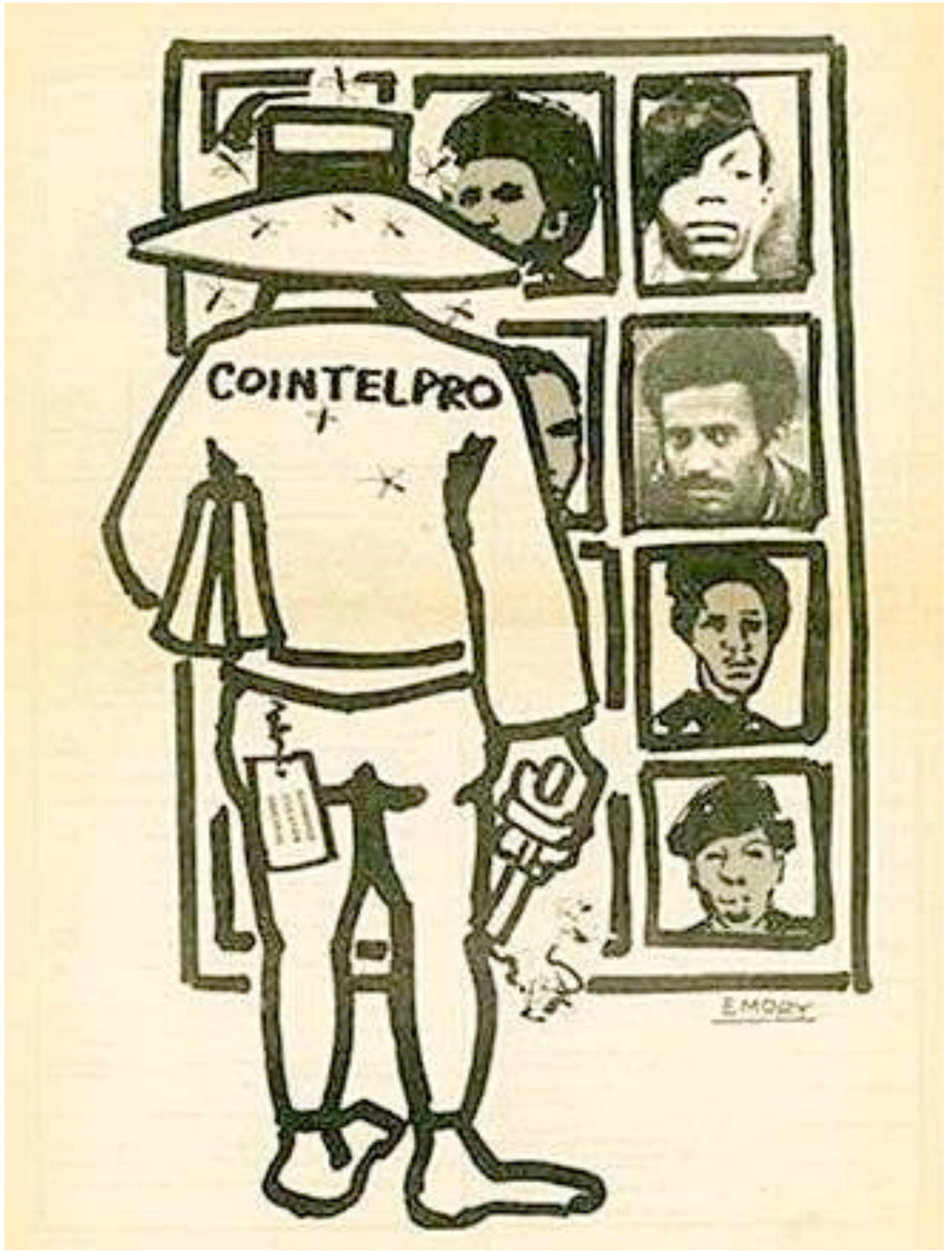


Image Credits: The Melanated Press (2014), Emory Douglas (1976)

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)

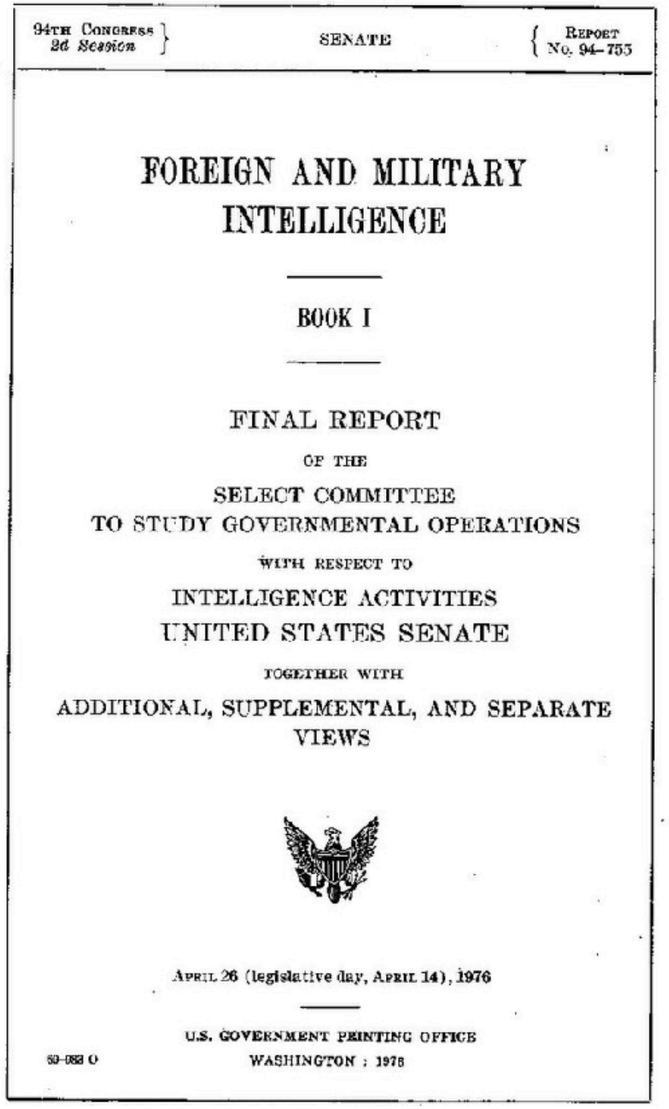
COINTELPRO

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

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**
8. Censorship**

*Facilitated by Information Technology

*Confidentiality, Anonymity

*Integrity, Trust

*Decentralization, Accessability

Be Safe or Be Seen? (Lokot 2018)

Ethnographic Observation of Anti-Corruption Foundation Activists (Russia)

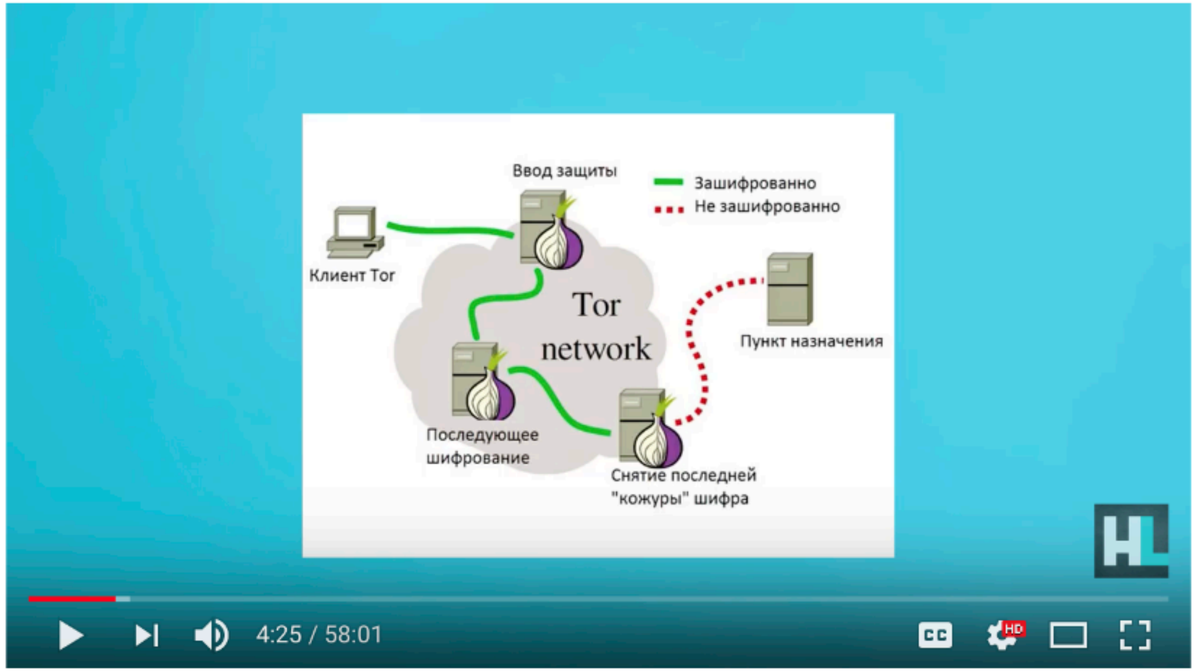
Image Credit: Evgeny Feldman/AP (2018)

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 8.9K 3K SHARE

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

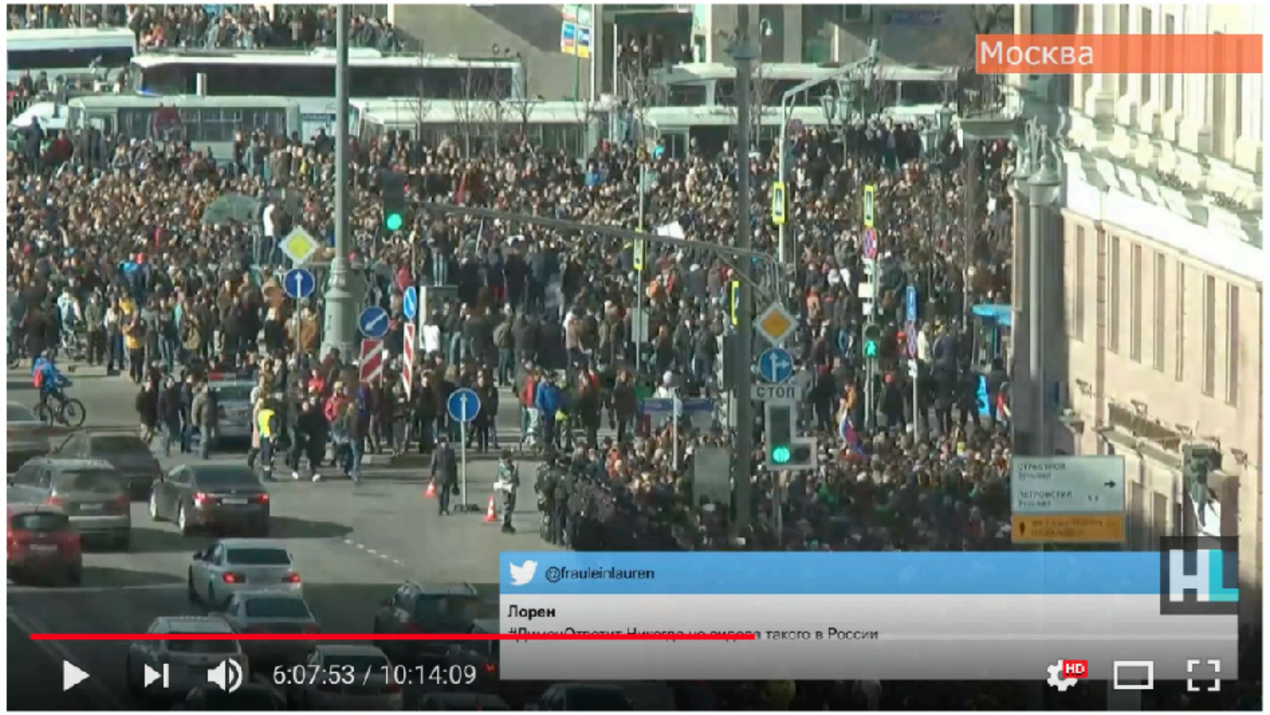


Figure 3. *Screen grab of YouTube live stream syndicated by FBK during the March 26, 2017, anti-corruption protests in Russia.*

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 (ABJM 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 (ABJM 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)

Digital Accessibility is Physical Accessibility (Bohdanova 2014)

Study of the role of social media and ICTs in the Euromaidan uprising (Ukraine)

Image Credit: Kostyantyn Chernichkin (2014)

Digital Accessibility is Physical Accessibility (Bohdanova 2014)

Study of the role of social media and ICTs in the Euromaidan uprising (Ukraine)

Physical IT Tents:

Internet access, equipment

Image Credit: Rosipro (2014)

Digital Accessibility is Physical Accessibility (Bohdanova 2014)

Study of the role of social media and ICTs in the Euromaidan uprising (Ukraine)

Physical IT Tents:

Internet access, equipment

Crowdsourcing:

Ad-hoc groups of people with resources

Image Credit: Rosipro (2014), NBC News (2013)

Digital Accessibility is Physical Accessibility (Bohdanova 2014)

Study of the role of social media and ICTs in the Euromaidan uprising (Ukraine)

Physical IT Tents:

Internet access, equipment

Crowdsourcing:

Ad-hoc groups of people with resources

Led to Technologist-Activist Collaboration: IT tents evolved into idea-generating spaces, development of new, needed tech

Image Credit: Rosipro (2014), NBC News (2013)

Circumventing Censorship and Accessibility Issues

Lower-Tech Fallbacks:

Audio transmission (Operation Vula)

Satellite phones + dialup (Arab Spring)

Word of Mouth (Black Lives Matter)

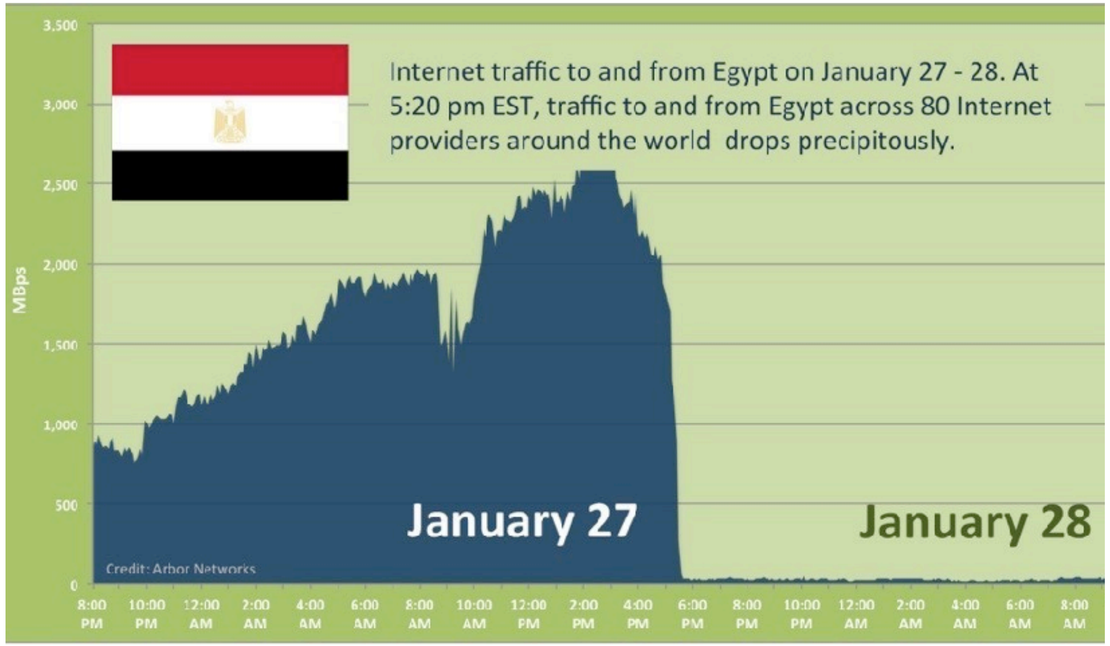


Image Credits: Labovitz/Arbor Networks (2011)

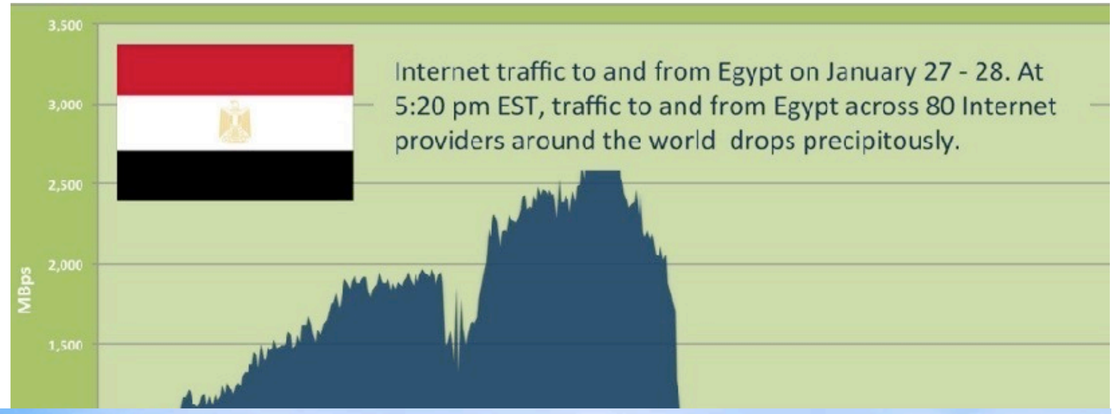
Circumventing Censorship and Accessibility Issues

Lower-Tech Fallbacks:

Audio transmission (Operation Vula)

Satellite phones + dialup (Arab Spring)

Word of Mouth (Black Lives Matter)



Physical Pre-Planning:

IT tents (Euromaidan Uprising)

“Facebook Hill” (Standing Rock)

Image Credits: Labovitz/Arbor Networks (2011), Rob Wilson/Facebook (2016)

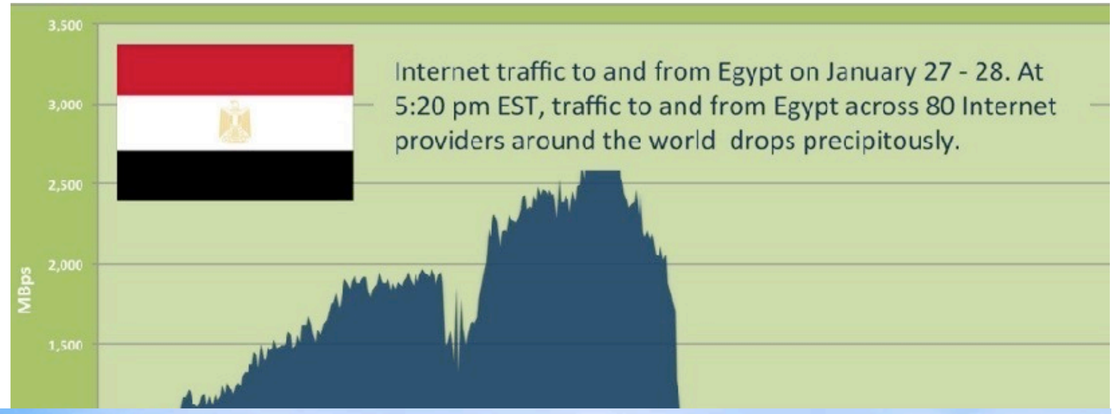
Circumventing Censorship and Accessibility Issues

Lower-Tech Fallbacks:

Audio transmission (Operation Vula)

Satellite phones + dialup (Arab Spring)

Word of Mouth (Black Lives Matter)



Physical Pre-Planning:

IT tents (Euromaidan Uprising)

"Facebook Hill" (Standing Rock)

Toward Community-Based Networks: (Local) accessibility, physical ownership, increases effort required to obtain data

Image Credits: Labovitz/Arbor Networks (2011), Rob Wilson/Facebook (2016)

Device Compromise and Deletion (ABJM 2021)

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

Image Credit: Anthony Kwan/Getty (2019)

Device Compromise and Deletion (ABJM 2021)

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

Full Compromise Security:

Detection and mitigation

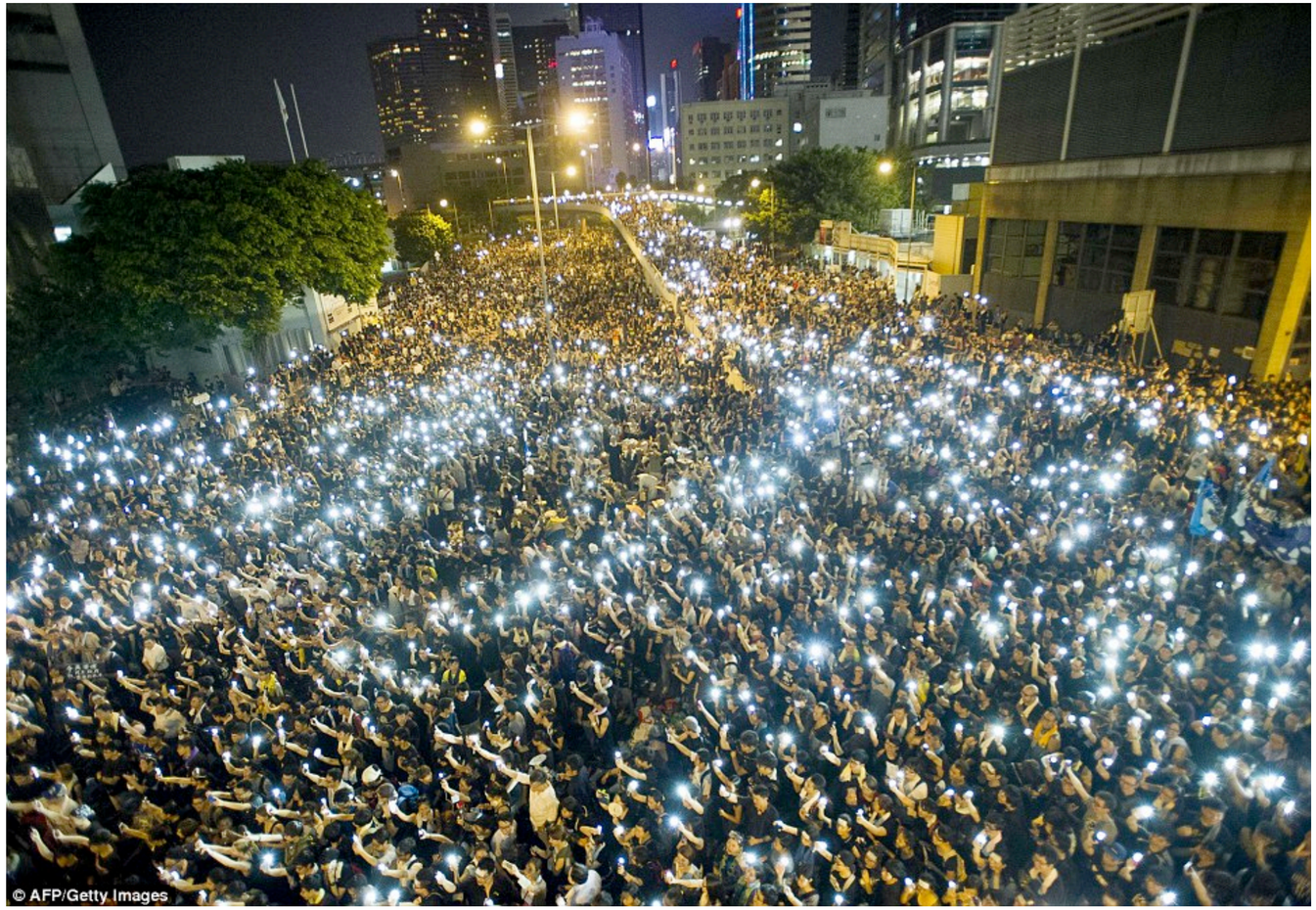


Image Credit: AFP/Getty (2019)

Device Compromise and Deletion (ABJM 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

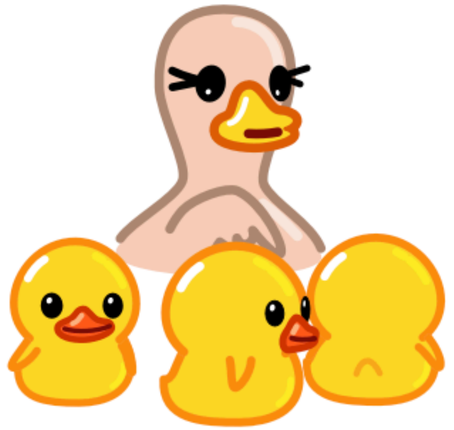


Image Credit: Telegram

Device Compromise and Deletion (ABJM 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: Library of primitives (no bounded association); 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

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

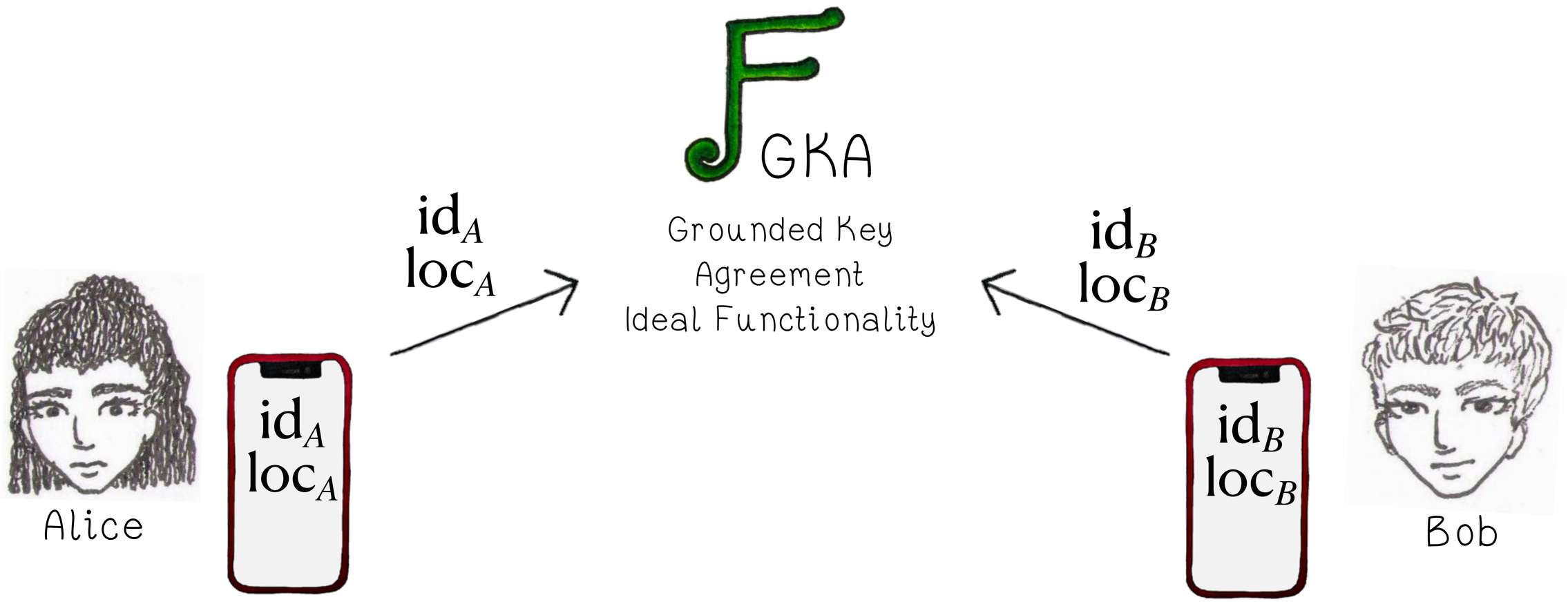
Grounded Annotation System

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



Ground Trust Ceremony

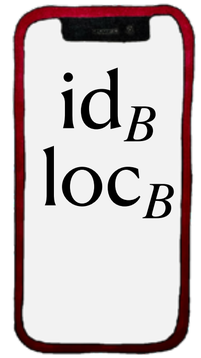
Alice

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

Grounded Key
Agreement
Ideal Functionality

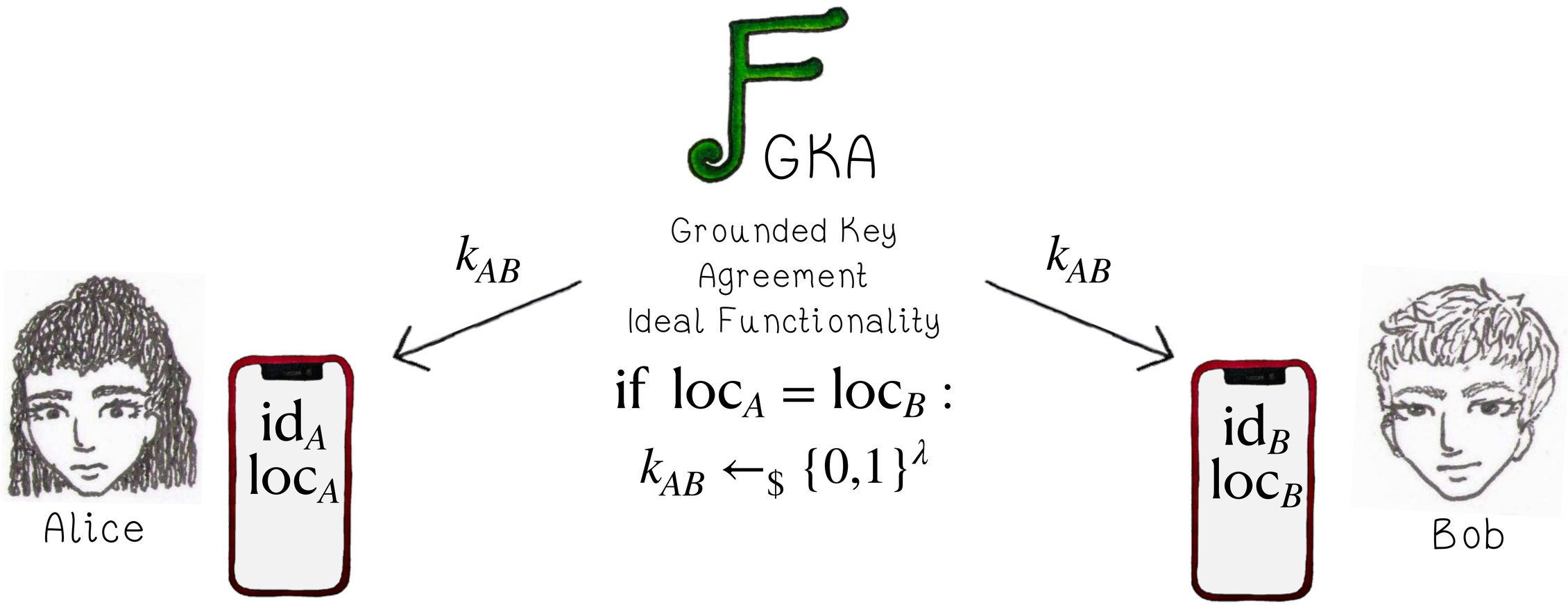
$$\text{if } \mathrm{loc}_A = \mathrm{loc}_B :$$

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



Bob

Ground Trust Ceremony

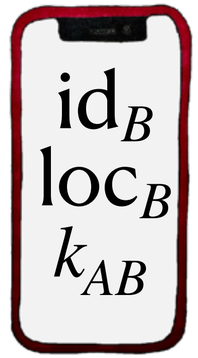


Ground Trust Ceremony

$\mathcal{F}_{GKA}$

Grounded Key
Agreement
Ideal Functionality

Alice

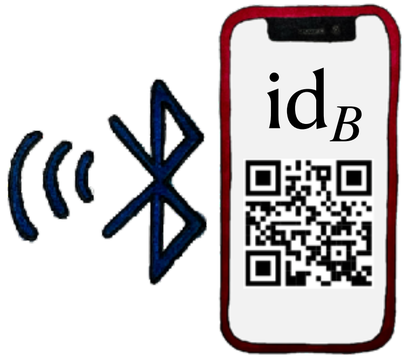


Bob

Ground Trust Ceremony

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

Alice



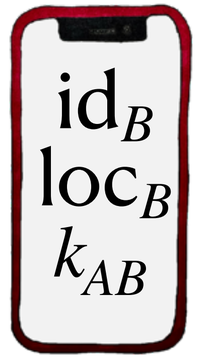
Bob

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

Ground Trust Ceremony

Alice

Alice and Bob now share a key that is rooted in their physical interaction.



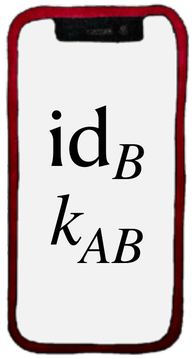
Bob

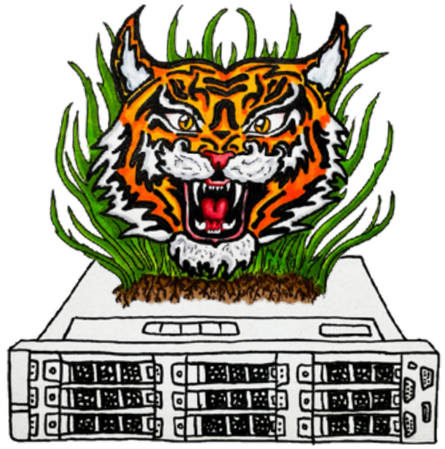
Annotation System

Alice

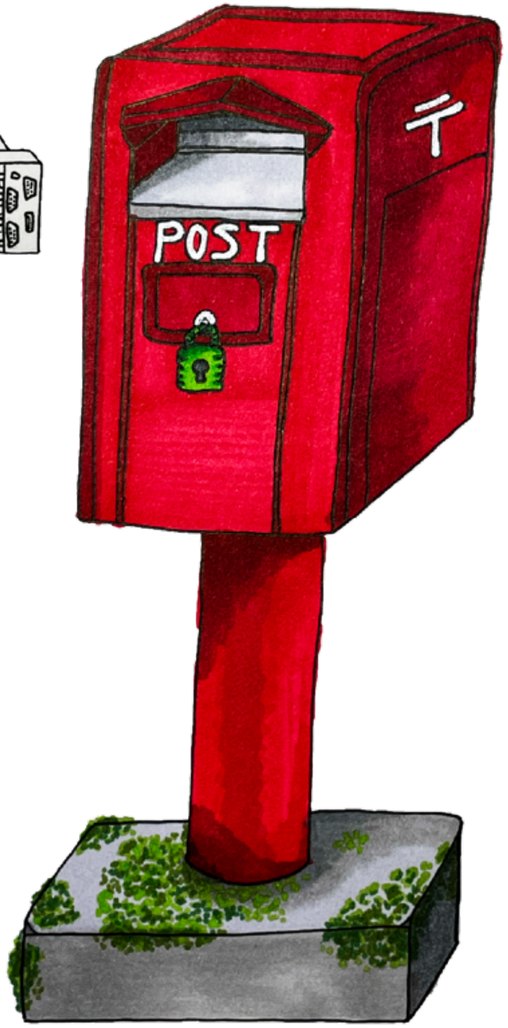
Charlie

Bob





Tigro
Server



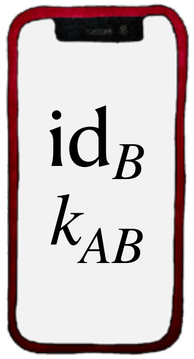
Shared Encrypted
Mailbox (EMB)

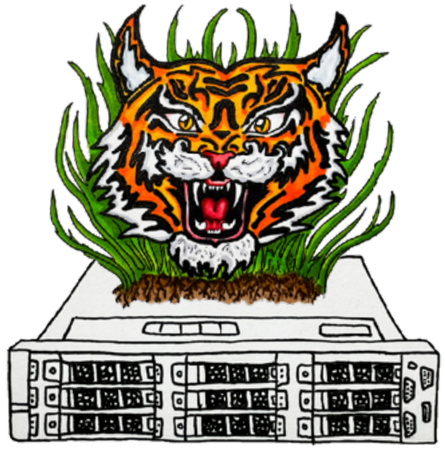
Annotation System

Alice

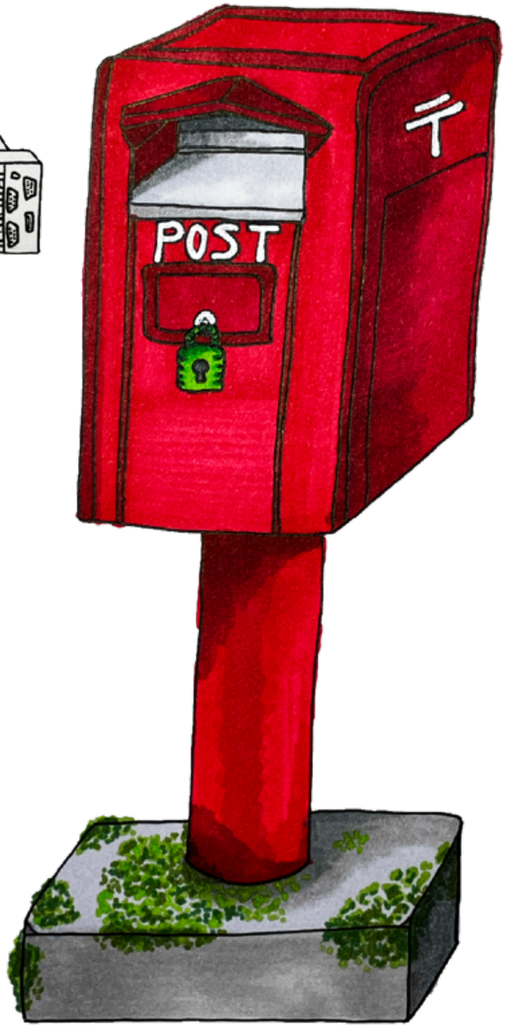
Annotate id_C :
I met them at a mutual aid event. They seem trustworthy.

Bob





Tigro
Server



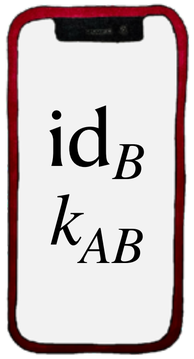
Shared Encrypted Mailbox (EMB)

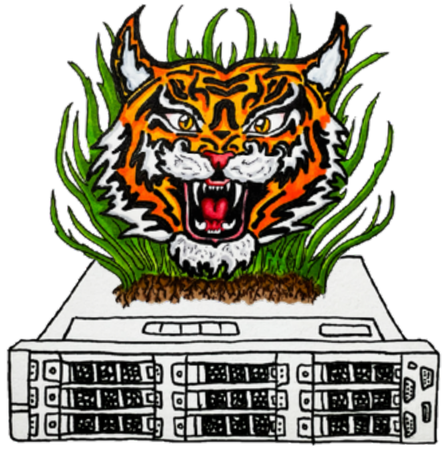
Annotation System

Alice

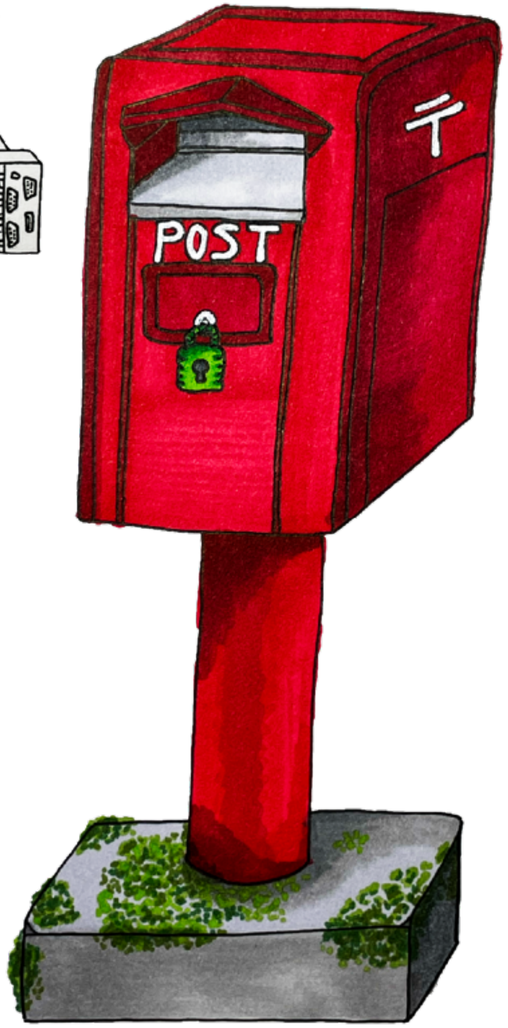
Annotate id_C :
This person was agitating at a sit-in. Vibes were off.

Bob





Tigro Server



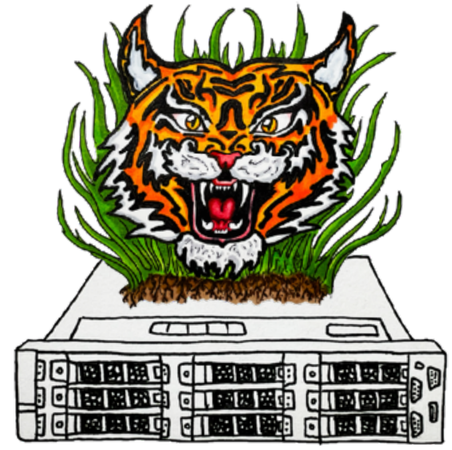
Shared Encrypted Mailbox (EMB)

Annotation System

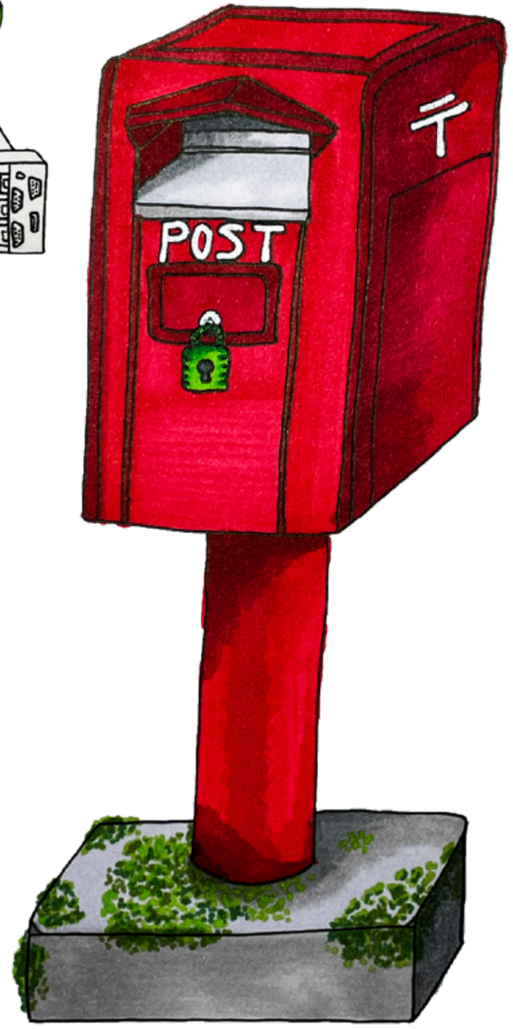
Alice

SendMail

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

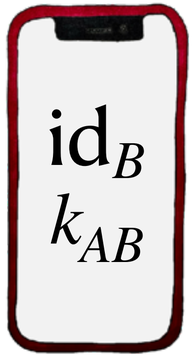


Tigro
Server



Shared Encrypted
Mailbox (EMB)

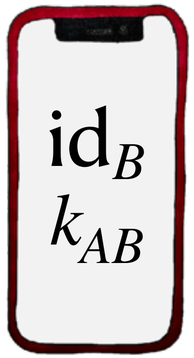
Bob

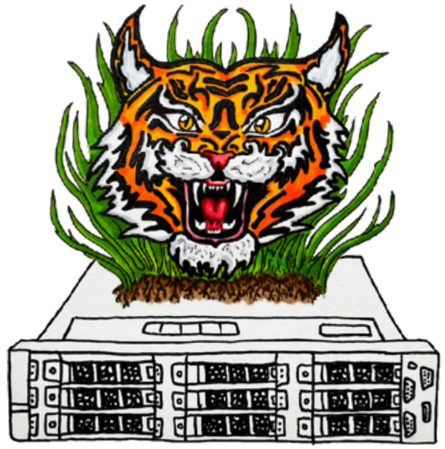


Annotation System

Alice

Bob





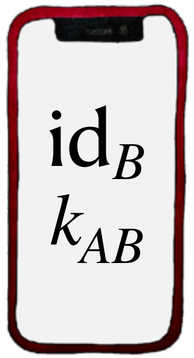
Tigro
Server

Shared Encrypted
Mailbox (EMB)

Annotation System

Alice

Bob



Charlie

Tigro
Server

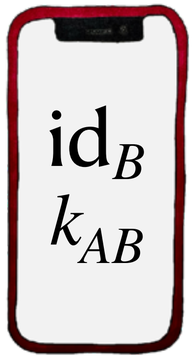
$[id_C, \mathrm{anno}]_{k_{AB}}$

Shared Encrypted
Mailbox (EMB)

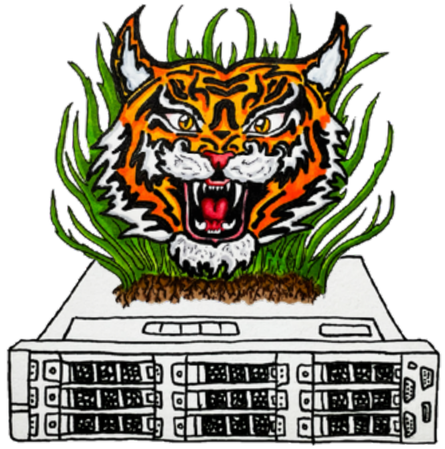
Annotation System

Alice

Bob



GetMail



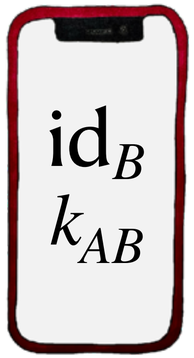
Tigro
Server

Shared Encrypted
Mailbox (EMB)

Annotation System

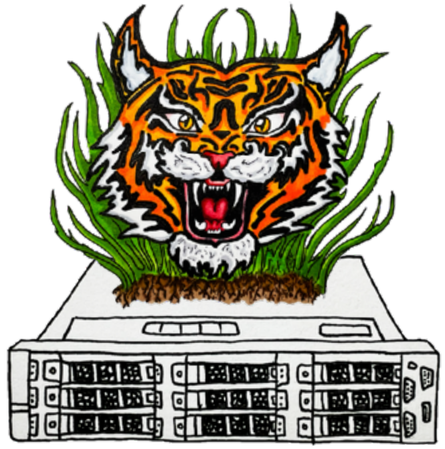
Alice

Bob



GetMail

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



Tigro
Server

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

Shared Encrypted
Mailbox (EMB)

Annotation System

Alice

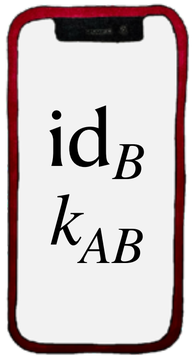
Event:

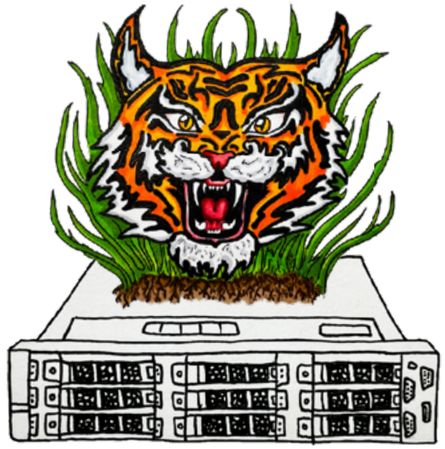
Protest

Organizer:

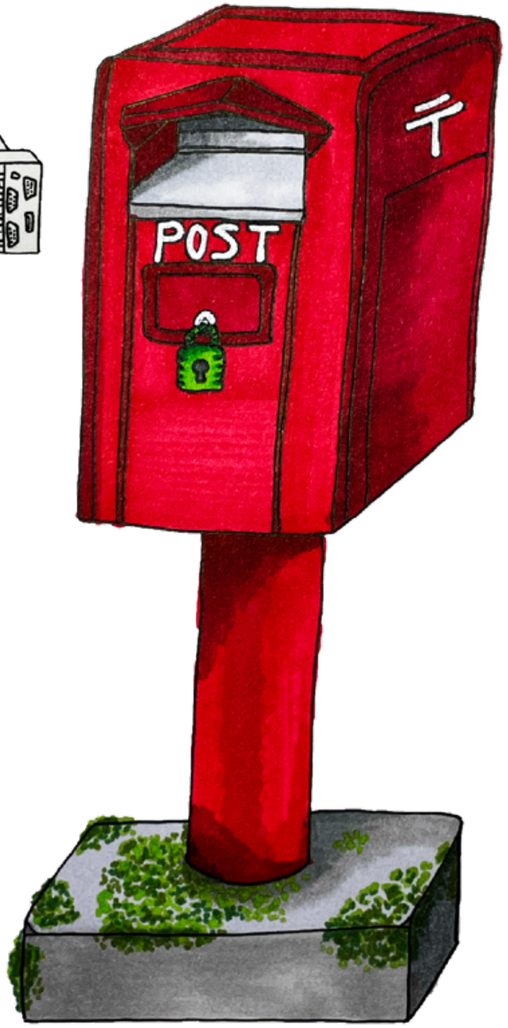
Eve

Bob





Tigro
Server



Shared Encrypted
Mailbox (EMB)

Annotation System

Alice

Event:

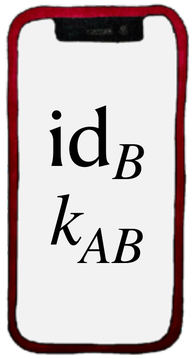
Protest

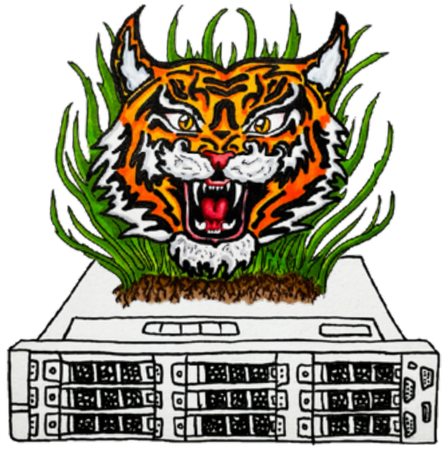
Organizer:

Eve

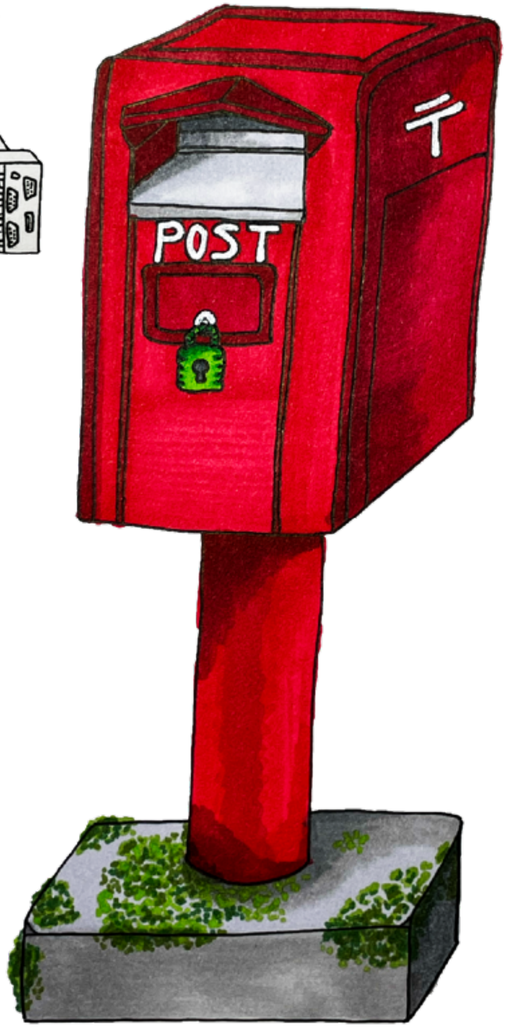
$\mathbf{oid}_E$

Bob





Tigro
Server



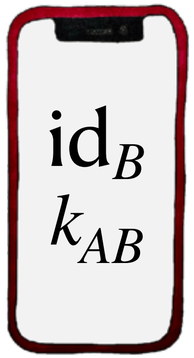
Shared Encrypted
Mailbox (EMB)

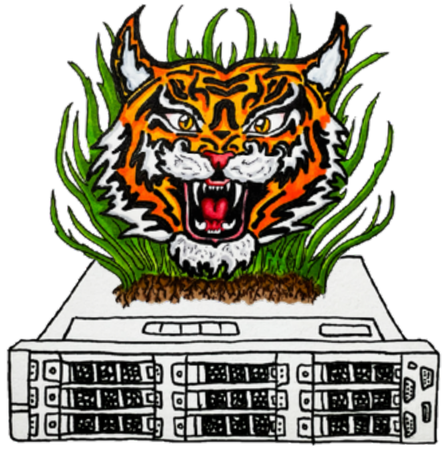
Annotation System

Alice

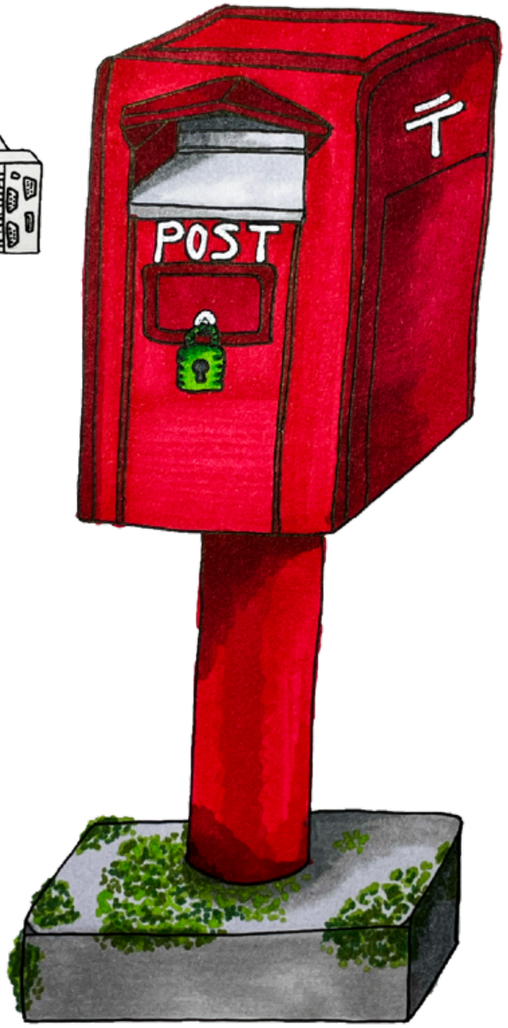
Annotate $\mathbf{oid}_E$: This event is being organized by friends. Hope to see you there.

Bob





Tigro Server



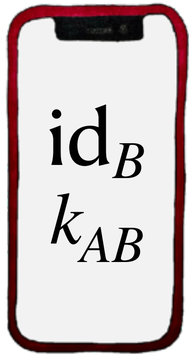
Shared Encrypted Mailbox (EMB)

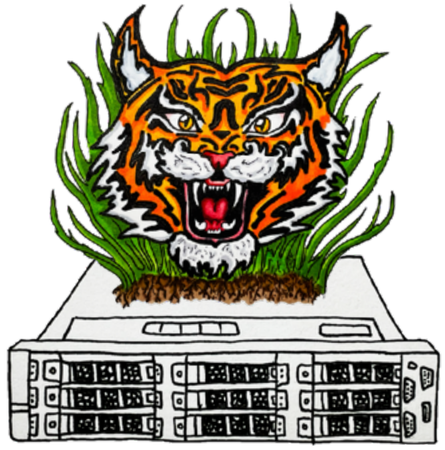
Annotation System

Alice

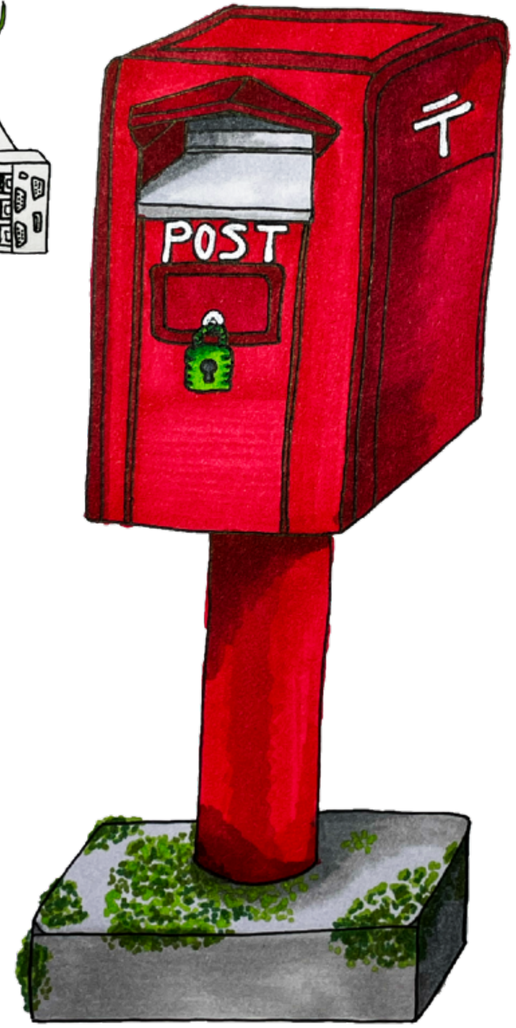
Annotate $\mathbf{oid}_E$: No one I know can confirm the identity of Eve. Proceed with caution.

Bob





Tigro Server



Shared Encrypted Mailbox (EMB)

Annotation System

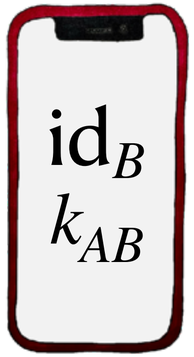
Alice

SendMail

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

Tigro
Server

Bob

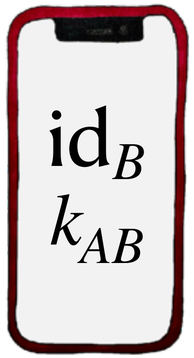


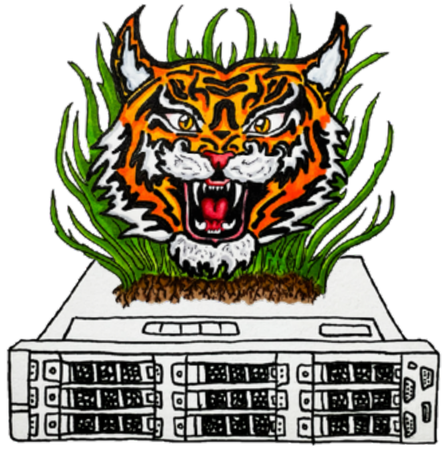
Shared Encrypted
Mailbox (EMB)

Annotation System

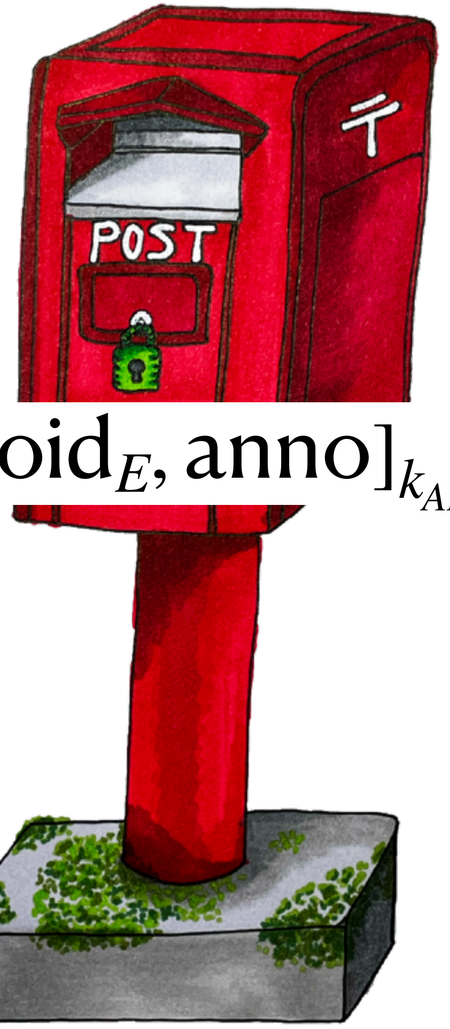
Alice

Bob





Tigro
Server

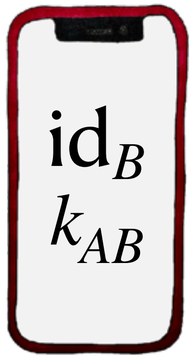


Shared Encrypted
Mailbox (EMB)

Annotation System

Alice

Bob



Event:

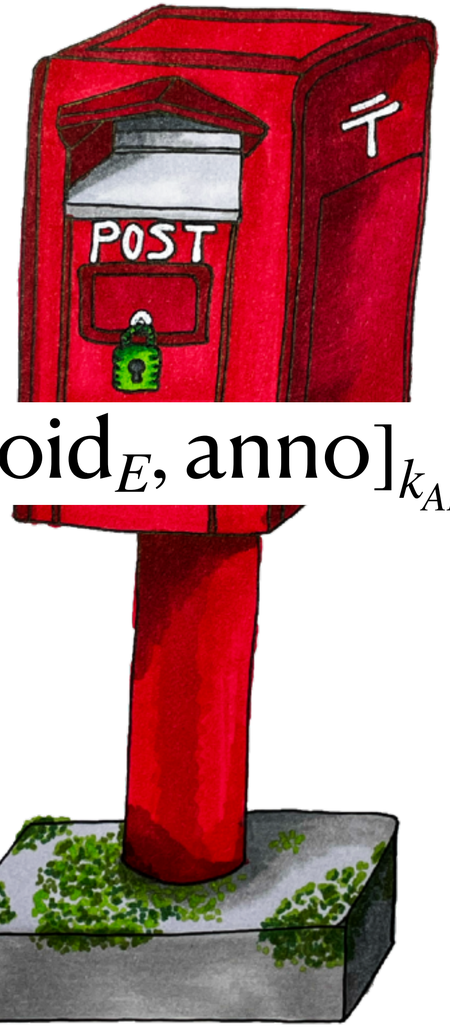
Protest

Organizer:

Eve

oid_E

Tigro Server

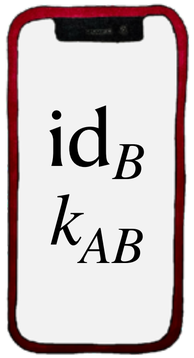


Shared Encrypted Mailbox (EMB)

Annotation System

Alice

Bob



Event:

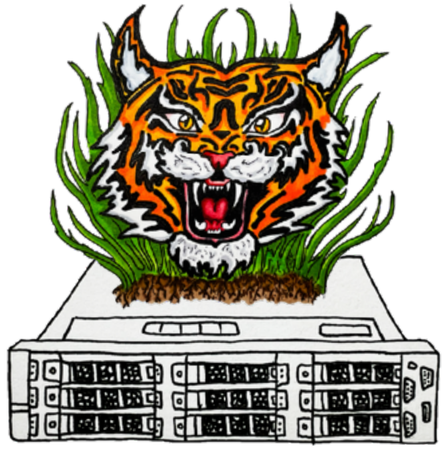
Protest

Organizer:

Eve

oid_E

GetMail



Tigro
Server

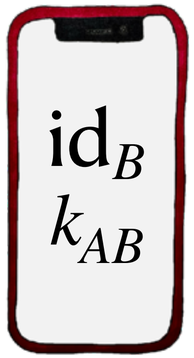
$[\mathrm{oid}_E, \mathrm{anno}]_{k_{AB}}$

Shared Encrypted
Mailbox (EMB)

Annotation System

Alice

Bob



Event:

Protest

Organizer:

Eve

oid_E

GetMail

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

Tigro
Server

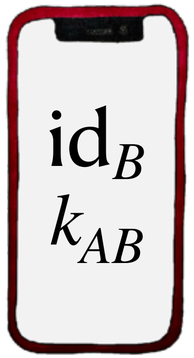
$[\mathrm{oid}_E, \mathrm{anno}]_{k_{AB}}$

Shared Encrypted
Mailbox (EMB)

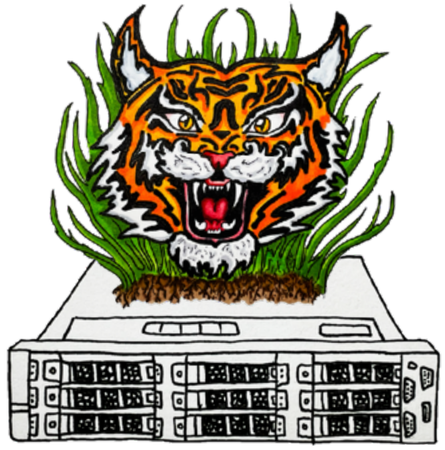
Annotation System

Alice

Bob



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



Tigro Server

Shared Encrypted Mailbox (EMB)

Conclusion

"the way in which infrastructure is designed and implemented impacts people's ability to exercise their freedom of assembly and association...

Endangering characteristics should be mitigated, or at least clearly communicated to the users of these technologies."

– Internet Protocols and the Human Rights to Freedom of Association and Assembly (draft-irtf-hrpc-association-12)

Conclusion

"Who does [our work] serve?

Who holds power?

Who is trusted?

Who has meaningful choices?"

– Daniel Kahn Gillmor (2023)

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. Tetyana Bohdanova. Unexpected revolution: the role of social media in ukraine's euromaidan uprising. *European View*, 13(1):133–142, 2014.
3. Glencora Borradaile. *Defend Dissent.* Oregon State University Corvallis, 2021.
4. J.L. Hall, M.D. Aaron, A. Andersdotter, B. Jones, Feamster N., and Knodel M. *A Survey of Worldwide Censorship Techniques.* The Internet Engineering Task Force pearg Workgroup draft-irtf-pearg-censorship-09, 2023.
5. 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.
6. Seny Kamara. *COINTELPRO.* Algorithms for the People, 2020.
7. Seny Kamara. *Crypto for the People Invited Talk.* The International Association for Cryptologic Research, 2020.
8. 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.
9. N. ten Oever, S. Couture, and Knodel M. *Internet Protocols and the Human Rights to Freedom of Association and Assembly.* The Internet Engineering Task Force Human Rights Protocols Considerations Research Group draft-irtf-hrpc-association-12, 2022.
10. Leah Namisa Rosenbloom. Toward secure social networks for activists. In *Moving technology ethics at the forefront of society, organisations and governments*, pages 491–502. ETHICOMP, 2021.
11. Leah Namisa Rosenbloom. Activists want better, safer technology. *arXiv preprint arXiv:2209.01273*, 2022.