

AT-COMPROMISE SECURITY: THE CASE FOR ALERT BLINDNESS

CRYPTOGRAPHIC APPLICATIONS WORKSHOP, ROME, 10 MAY 2026

Martin R. Albrecht¹, Simone Colombo¹, Benjamin Dowling¹ and Rikke Bjerg Jensen²

¹King's College London, ²Royal Holloway, University of London

CONTENT WARNING

I use examples from fieldwork, several of which concern abductions and torture.

SOCIAL FOUNDATIONS OF CRYPTOGRAPHY

“NATURAL SECURITY CONCERNS”

Goldreich has argued cryptographic practice proceeds through “the identification, conceptualization and rigorous definition of cryptographic tasks which capture natural security concerns.”

[...]

But ...How does one identify such “natural security concerns”? On these questions, the literature remains silent.

— Jean-François Blanchette. **Burdens of proof: Cryptographic culture and evidence law in the age of electronic documents.** MIT Press, 2012, p. 89

OUR RESPONSE: ETHNOGRAPHY

1. Based on **ethnographic findings**,
2. we initiate the cryptographic study of **at-compromise security**.

OUR RESPONSE: ETHNOGRAPHY

1. Based on **ethnographic findings**,
2. we initiate the cryptographic study of **at-compromise security**.

Ethnography is the study of people in naturally occurring settings or 'fields' by means of methods which capture their social meanings and ordinary activities.

— John Brewer. **Ethnography**. Open University Press, 2000, p. 3

THIS TALK

Social Foundations of Cryptography

The Setting

Research Design

Ethnographic Findings

At-Compromise Alert Blindness

Last Thoughts!

THE SETTING

ANTI-FINANCE BILL PROTESTS, KENYA



Figure 1: Protest poster for 25 June

- Unprecedented **large-scale protests** across Kenya starting on 18 June 2024, sparked by the 2024 **Finance Bill**.
- **Poor, working and middle class** protesters.
- **Violent responses from State forces**: killing, arresting, injuring and abducting many.
- The 2024 Finance Bill was **withdrawn on 26 June**; smaller-scale protests continued until 8 August.

A MOMENT OF REVOLUTIONARY RELIEF: 25 JUNE 2024

*"I am so happy. This is not just the poor, but this is **everyone coming together**."
(Protester, Nairobi, 25 June 2024)*



Figure 2: 25 June, Nairobi (photo by author)

On **25 June 2024** protesters breached the fence around Kenya's Parliament, some entered Parliament and the Senate.

State security forces killed and injured protesters; international diplomatic forces publicly urged them to practice "restraint" [Bri24].

Ruto called the breach "treasonous" and protesters "organised criminals" [MBNP24].

A SURGE IN ABDUCTIONS

- **Ruto's security forces** abducted several people during and since these protests.
 - 82 abductions [Ken24] between June and December 2024.
 - 15 abductions in connection with the one-year anniversary protests [Ken25].
- Abductions a **new security threat** during *these* protests.
- **Several of those abducted are still missing.**

A SURGE IN ABDUCTIONS

- **Ruto's security forces** abducted several people during and since these protests.
 - 82 abductions [Ken24] between June and December 2024.
 - 15 abductions in connection with the one-year anniversary protests [Ken25].
- Abductions a **new security threat** during *these* protests.
- **Several of those abducted are still missing.**

Abduction Squads Established

Central security units, specifically the Directorate of Criminal Investigations (DCI), supported by the Rapid Deployment Unit (RPU), military intelligence, the Anti-Terrorism Police Unit (ATPU) and the National Intelligence Service (NIS).

RESEARCH DESIGN

*We establish our **technique** by introducing ethnography to cryptography.*

- Ethnography comprises **data collection methods** and **analytical steps**.
- We bridge a methodological gap in cryptography to establish **realism**.
- It is through the application of this technique that we arrived at our **new security notion**.

Longer-term access to and immersion in a social movement in Kenya.

- **4 – 18 April 2024: Scoping Nairobi** (meeting gatekeepers, planning full fieldwork)
- **3 June – 20 September 2024: Fieldwork Nairobi (Kisumu, Mombasa)** (active participant observation and ethnographic interviews)
- **1 January – 23 February 2025: Fieldwork Nairobi** (active participant observation and ethnographic interviews)

Building rapport over time enabled access to a wide network of activists and groupings.

...“localized, long-term, close-in, vernacular field research” [Gee98].



Figure 3: Group meeting, Nairobi (photo by author).



Figure 4: 25 June 2024, Nairobi (photo by author).

ACTIVE PARTICIPANT OBSERVATION

Field access through local gatekeepers and interlocutors and continuously re-established.

11 large and smaller street protests in Nairobi, including 18, 20 and 25 June.

Activist meetings, protest planning, strategic discussions, community gatherings and organising meetings.

Social activities in informal settlements in Nairobi, including community reach-outs, hospital and prison visits and group meetings.

Observational data: Field notes and reflective notes.



Figure 5: 25 June 2024, Nairobi (photo by author).

ETHNOGRAPHIC INTERVIEWS

Shaped by an established relationship between the fieldworker and interlocutors.



Figure 6: Social justice centre, Nairobi (photo by author).

Ethnographic interviews with **77 protesters** during the fieldwork (organisers, frontliners, first-time and seasoned protesters), **eight of whom had been abducted**.

Loosely structured around an **evolving topic guide**.

Ethnographic interviews lasted between 43 minutes and over three hours.

Interview data: Interview transcripts and interview notes.

ANALYSIS: BRINGING ETHNOGRAPHY TO CRYPTOGRAPHY

Iterative analysis at several stages of the research across ethnography and cryptography.

- Analysis across ethnography and cryptography: during, between and after fieldwork.
- **Inductive reasoning**: theory developed from empirical data (grounded theory).
- We did not set out to test an intuited security notion, but analysed the data to **discover** it.
- Initial analysis by fieldworker, followed by collective, **reflexive analysis** and formalisation with cryptographers and fieldworker.

ETHNOGRAPHIC FINDINGS

EMERGENCE OF ABDUCTIONS

The fieldwork revealed how abduction was not a security concern before June 2024:

*“No, no, no. There wasn’t a concern at that point [...] We have done demonstrations before. The worst that they [the security forces] can do ...they normally arrest you, then they charge you and then give you a cash bail or whatever. **It had never reached a point where they could torture people or go beyond that.** You see now, for us, this is something that was normal to us. Abductions weren’t.” (P51, abductee, Nairobi)*

THE DIFFERENT PHASES OF ABDUCTIONS

Our analysis uncovered distinct phases of abductions during this period.



Figure 7: Protests against abductions, 6 January 2025

- **Preparing for Abductions**
 1. Shifting security outlook
 2. Changing practices
- **Contours of Abductions**
 1. Capture
 2. Interrogation
- **Protection during Abductions**
 1. Raising the alarm
 2. Shouting

PREPARING FOR ABDUCTIONS: SHIFTING SECURITY OUTLOOK

“We have never experienced anything like this [abductions] before, so tomorrow we have to stay together” (FN4, group strategy meeting on 24 June 2024).

Abductions shifted protest planning and security outlook for activist groups.

- Moving in groups with established check-in protocols.
- Temporarily moving in with friends or family.
- Carrying a second (clean) phone.
- Several phone numbers linked to other people's IDs.

PREPARING FOR ABDUCTIONS: CHANGING PRACTICES

The level of preparation depended on self-perceived targeting, with some developing elaborate practices in an attempt to protect themselves.

“I was entirely in hiding, but they found me even though my phone had been off for, like, two days” (P37, abductee, Nairobi).

CONTOURS OF ABDUCTIONS: CAPTURE

Those abducted were taken individually by between four and eight **masked, unidentified individuals**.

- Everyone, except P51 and P60, were **captured at or near their home**.
- Their **phones were taken and asked to unlock** them, except P72 who smashed theirs.
- They were **blindfolded, their hands were tied** and they were shuffled into a car, where they sat between two of their abductors.

THE CONTOURS OF ABDUCTIONS: CAPTURE

When P22 was captured at their home in the early days of the protests; their abductors immediately secured P22's devices.

"The next thing I know, I was being beaten. The other guy went for my laptop and my phone [...] He wanted me to unlock my phone, but I refused [...] I was blindfolded and put into a car and we drove around for maybe two hours [...] After some time the car stopped and I was being taken out of the car. I was still only in my t-shirt and shorts, hands tied behind my back and blindfolded. I was taken down some stairs into a very cold room. They told me to lie on my stomach [...] They would come in the morning and tightened the blindfold again" (P22, abductee, Nairobi).

THE CONTOURS OF ABDUCTIONS: INTERROGATION

All abducted persons we spoke to shared how they had been *handed over* to interrogators, who also **forced access to their phones**.

*“I never knew a human can be that strong, that a jab can be that heavy, you know. I don’t even know how I found myself on the ground because I was seated [...] at first I wondered what had brought the ground to my hand, only to realise that it is me who had fallen down. **So I just gave them my password now [...] They told me ‘if it doesn’t work, now we are finishing you’.** But, you know, I had given them the right password” (P60, abductee, Kisumu).*

PROTECTION DURING ABDUCTIONS: RAISING THE ALARM

In the boot of their abductors' car, P51 remembered they still had their second phone.

*“**Very brief message: ‘Hey, I’m being abducted. I don’t know where I am’ [...]** After I had texted him, **he took the screenshot [of the message] and posted it on X.** So that is how it spread [...] funnily enough, after like 30 minutes or so, as they [the abductors] were driving me around, the car stopped again. And then they came out. They opened the trunk, and then they started beating me up. And then they asked me: ‘Where is that phone?’ So they knew that I had another phone because my friend shared my screenshot [...] **I think that is the only thing that saved me.** Because if it wasn’t for that message, these guys had another motive. Because nobody was aware of my abduction, apart from that one message. So they could have killed me and taken me somewhere, nobody could have known. So the fact that I was now out saved me” (P51, abductee, Nairobi).*

PROTECTION DURING ABDUCTIONS: SHOUTING



Figure 8: Posters calling for the release of abducted protesters.

- Some would write or **schedule posts** to go out on X in the event of abduction, e.g. P37 (abductee, Nairobi) “had planned tweets on my laptop that I would send out in the event that I would be taken”.
- **“Guys are outside where I am. They have come for me guys at 3am”**, then they went silent (FN4).
- Once the alarm had been raised, shouting could happen across platforms.
- **Network** of connected and known activists.
- **Feedback loop** to abductors.

AT-COMPROMISE ALERT BLINDNESS

AT COMPROMISE ALERT BLINDNESS

When taken, abducted persons can alert their network without the adversary noticing.

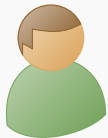
AT COMPROMISE ALERT BLINDNESS

When taken, abducted persons can alert their network without the adversary noticing.

AT COMPROMISE ALERT BLINDNESS

When taken, abducted persons can alert their network without the adversary noticing.

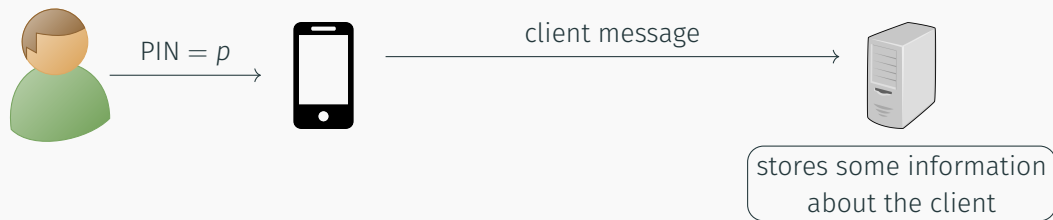
OUR PROTOCOL: SETUP PHASE



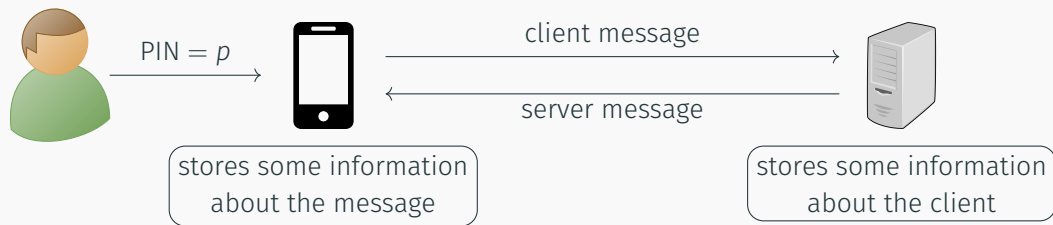
OUR PROTOCOL: SETUP PHASE



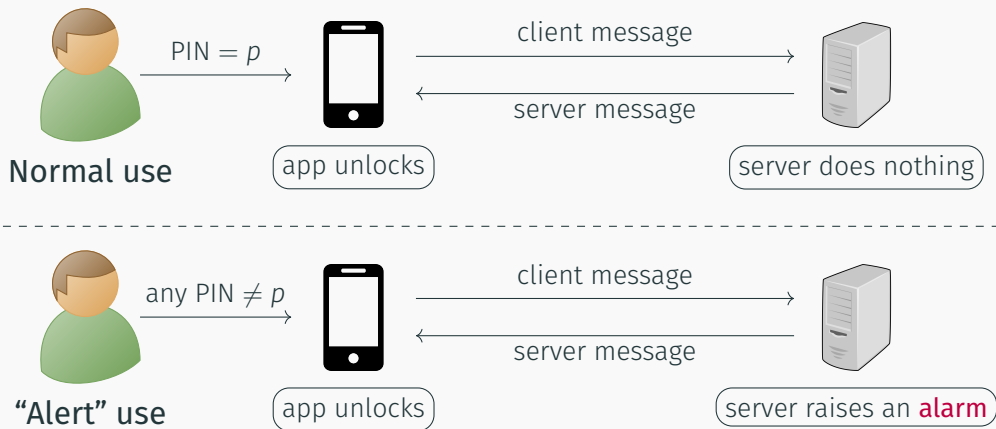
OUR PROTOCOL: SETUP PHASE



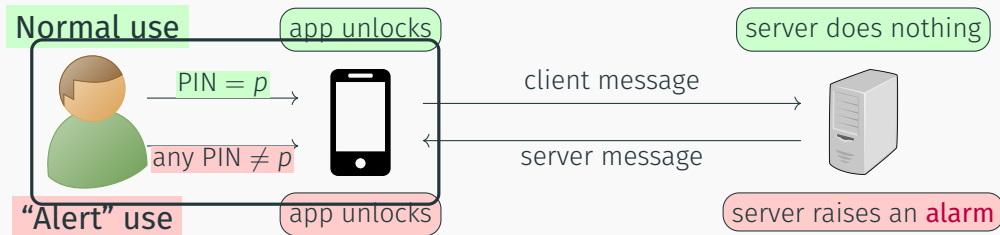
OUR PROTOCOL: SETUP PHASE



OUR PROTOCOL: ALERT PHASE

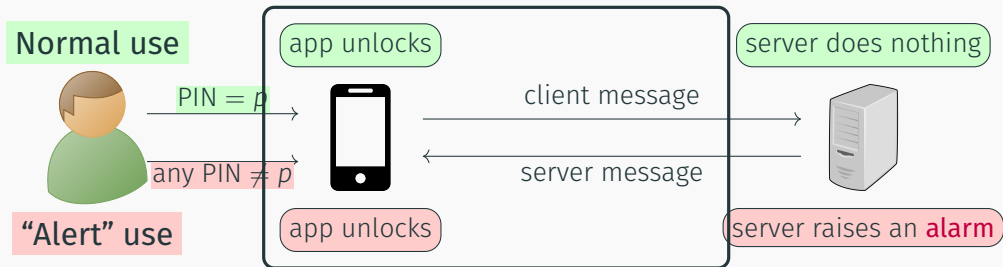


REALISM: PINS



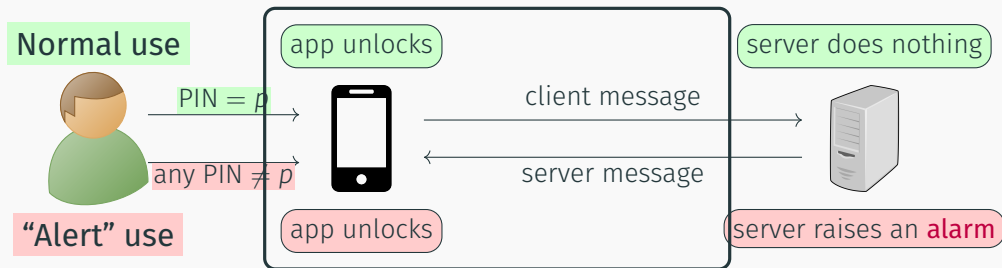
- PINs capture the **distinction of compromising people or their devices**.
- Multiple PINs model that the abducted person knows they have been abducted: **they can decide which PIN to use**.

REALISM: CONFIDENTIALITY



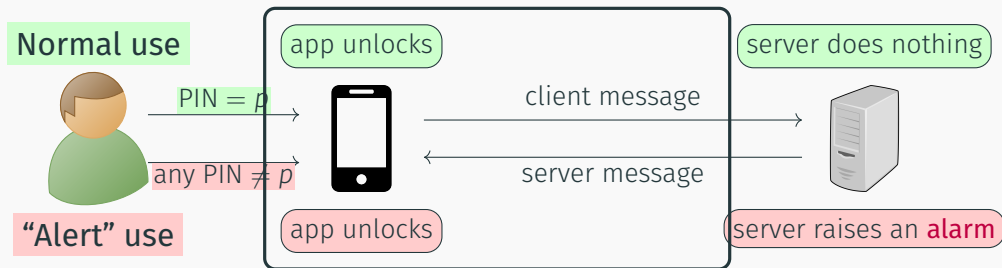
- “They wanted to know who was funding these protest.” (P49)

REALISM: CONFIDENTIALITY



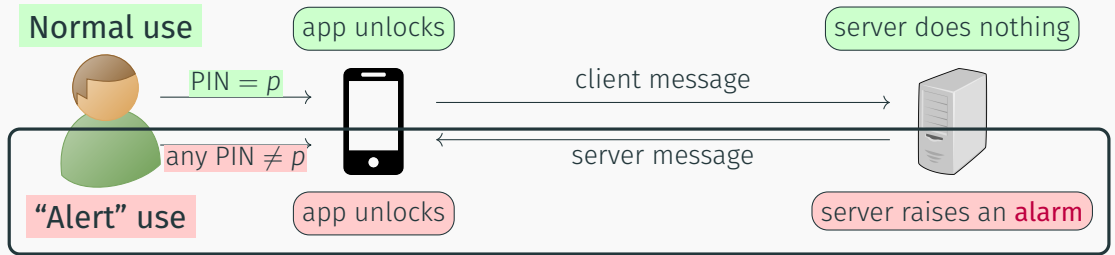
- “They wanted to know who was funding these protest.” (P49)
- P61 shared how the interrogators had told them: “**We are going to ask you questions and you’re going to answer us**; this is not a police station so they might not find you.”

REALISM: CONFIDENTIALITY



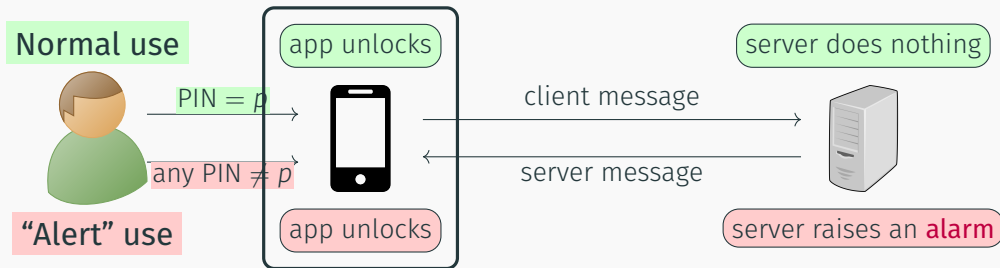
- “They wanted to know who was funding these protest.” (P49)
- P61 shared how the interrogators had told them: “**We are going to ask you questions and you’re going to answer us**; this is not a police station so they might not find you.”
- We exploit the abductors’ goal to access information: **at least one message must reach the server, without** that message the phone **does not unlock** and access is impossible.

REALISM: ALERT



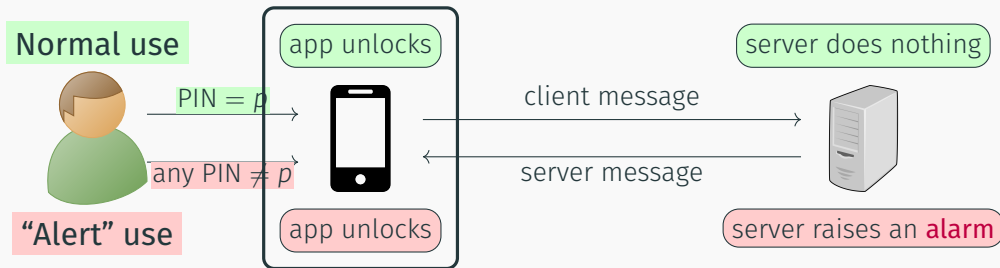
The security goal for abductees was to make their **disappearance publicly known**: *"I think that is the only thing that saved me."* (P51)

REALISM: BLINDNESS



- All expressed the same fear: **they would be killed if they did not cooperate with their abductors**: *"if I do anything now to upset these guys, I'm dead."* (P60)

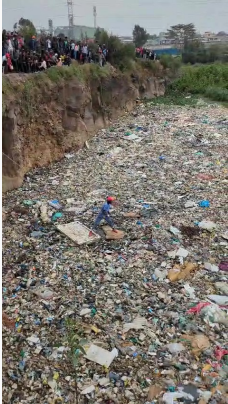
REALISM: BLINDNESS



- All expressed the same fear: **they would be killed if they did not cooperate with their abductors**: *"if I do anything now to upset these guys, I'm dead."* (P60)
- The app unlocks in both cases: abductees would cooperate regardless, and abductors would not notice any difference.

LAST THOUGHTS!

MISSING PROTESTERS



*“Over the weekend, **five bodies were retrieved from swamps and quarries**, people who had been missing since the first protests and most with bullet wounds. Bodies of missing protesters have also been found in some morgues” (FN5, July 2024).*

Figure 9: Community search for bodies in dumpsite swamp, July 2024 (photo by author).

THANK YOU!

Game KIND-AtC-AB $_{\mathcal{S}, \mathcal{K}, \text{ABOM}}(1^\lambda, \mathcal{A})$

IND-CPA-AtC-AB $_{\mathcal{S}, \mathcal{H}, \text{ABOM}}(1^\lambda, \mathcal{A})$

```
1: //  $\text{ps}_1$  is real personal secret,  $\text{ps}_0$  is random
2:  $\text{ps}_1 \xleftarrow{\$} \mathcal{S}$ ;  $\text{ps}_0 \xleftarrow{\$} \mathcal{S} \setminus \{\text{ps}_1\}$ ;  $k_1, k_0 \xleftarrow{\$} \mathcal{K}$ 
    $\text{ps}_1 \xleftarrow{\$} \mathcal{S}$ ;  $\text{ps}_0 \xleftarrow{\$} \mathcal{S} \setminus \{\text{ps}_1\}$ ;  $k_1 \xleftarrow{\$} \mathcal{K}$ 
3:  $(\text{ds}, \text{ss}) \leftarrow \text{GeneralSetup}(1^\lambda, k_1, \text{ps}_1)$ 
4:  $\text{win}_{\text{cm}}, \text{win}_{\text{sm}} \leftarrow \text{false}$ 
5:  $d \xleftarrow{\$} \{0, 1\}$ 
6:  $\sigma \leftarrow \mathcal{A}(k_d)^{\{\text{REQUEST}, \text{RESPONSE}, \text{GETKEY}, \text{CLEAR}\}}$ 
    $\sigma \leftarrow \mathcal{A}^{\{\text{REQUEST}, \text{RESPONSE}, \text{GETKEY}, \text{CLEAR}, \text{ENC}\}}$ 
7: if  $\text{win}_{\text{cm}} \vee \text{win}_{\text{sm}}$  : return 1
8:  $\text{ds} \leftarrow \text{Clear}(\text{ds})$ 
9:  $b \xleftarrow{\$} \{0, 1\}$ 
10:  $\text{dtct}, \text{recv} \leftarrow \text{false}$ 
11:  $(b', d') \leftarrow \mathcal{A}^{\text{DETECT, ENC}}(\sigma, \text{ds}, \text{ps}_b)$ 
12: if  $d = d' \wedge \neg \text{recv}$  : return 1
13: if  $b = 0 \wedge \text{recv} \wedge \neg \text{dtct}$  : return 1
14: if  $b = b'$  : return 1
15: return 0
```

Oracle CLEAR()

```
1:  $\text{ds} \leftarrow \text{Clear}(\text{ds})$ 
```

Oracle REQUEST()

```
1:  $(\text{ds}, \text{cm}) \leftarrow \text{Request}(\text{ds}, \text{ps}_1)$ 
2:  $\mathcal{C} \leftarrow \mathcal{C} \cup \{\text{cm}\}$ 
3: return cm
```

Oracle RESPONSE(cm)

```
1:  $(\text{acc}, \text{ss}, \cdot, \text{sm}) \leftarrow \text{Response}(\text{ss}, \text{cm})$ 
2: if  $\text{acc} \wedge \text{cm} \notin \mathcal{C}$  :  $\text{win}_{\text{cm}} \leftarrow \text{true}$ 
3:  $\mathcal{Z} \leftarrow \mathcal{Z} \cup \{\text{sm}\}$ 
4: return sm
```

Oracle GETKEY(sm)

```
1:  $(\text{acc}, \text{ds}, \cdot) \leftarrow \text{GetKey}(\text{ds}, \text{sm})$ 
2: if  $\text{acc} \wedge \text{sm} \notin \mathcal{Z}$  :  $\text{win}_{\text{sm}} \leftarrow \text{true}$ 
```

Oracle DETECT(cm)

```
1:  $(\text{acc}, \text{ss}, \text{dtct}', \text{sm}) \leftarrow \text{Response}(\text{ss}, \text{cm})$ 
2: if  $\neg \text{acc}$  : return  $\perp$ 
3:  $\text{recv} \leftarrow \text{true}$ 
4:  $\text{dtct} \leftarrow \text{dtct} \vee \text{dtct}'$ 
5: return sm
```

Oracle ENC(m_0, m_1)

```
1: if  $|m_0| \neq |m_1|$  : return  $\perp$ 
2: return  $\mathcal{H}.\text{Enc}(k_1, m_d)$ 
```

Claim 1 Consider KIND-AtC-AB as defined in Definition 4. Model “confidentiality” as KIND security. Then KIND-AtC-AB correctly responds to security needs of some organisers and frontliners in Kenya in 2024.

Talk by Simone Colombo

Eurocrypt: Real-World Security session,
Tuesday 12 May, 14:30-15:50

REFERENCES I

- [Bla12] Jean-François Blanchette. **Burdens of proof: Cryptographic culture and evidence law in the age of electronic documents**. MIT Press, 2012.
- [Bre00] John Brewer. **Ethnography**. Open University Press, 2000.
- [Bri24] British High Commission Nairobi. **Joint statement by Ambassadors and High Commissioners in Kenya on public protests**. Accessed: 2025-05-29. 2024. URL: <https://www.gov.uk/government/news/joint-statement-by-ambassadors-and-high-commissioners-in-kenya-on-public-protests>.
- [Gee98] Clifford Geertz. **Deep hanging out**. 1998.

- [Ken24] Kenya National Commission on Human Rights. **Statement on the Recent Surge of Abductions/Enforced Disappearances in Kenya**. Accessed: 2025-07-01. 2024. URL: <https://www.knchr.org/Articles/ArtMID/2432/ArticleID/1213/Statement-on-the-Recent-Surge-of-AbductionsEnforced-Disappearances-in-Kenya>.
- [Ken25] Kenya National Commission on Human Rights. **KNCHR Update on the 25th June 2025 Demonstrations**. Accessed: 2025-07-01. 2025. URL: <https://www.knchr.org/Articles/ArtMID/2432/ArticleID/1230/KNCHR-UPDATE-ON-THE-25TH-JUNE-2025-DEMONSTRATIONS>.

- [MBNP24] Larry Madowo, Stephanie Busari, Catherine Nicholls, and Sugam Pokharel. **Kenya's president calls protests 'treasonous' after police fire live rounds at demonstrators**. Accessed: 2025-06-29. 2024. URL: <https://edition.cnn.com/2024/06/25/africa/kenya-protests-tax-rises-intl>.