Revocable Privacy

Niels Feij, Henk Berendsen, Thomas de Haan

Radboud University

Revocable Privacy

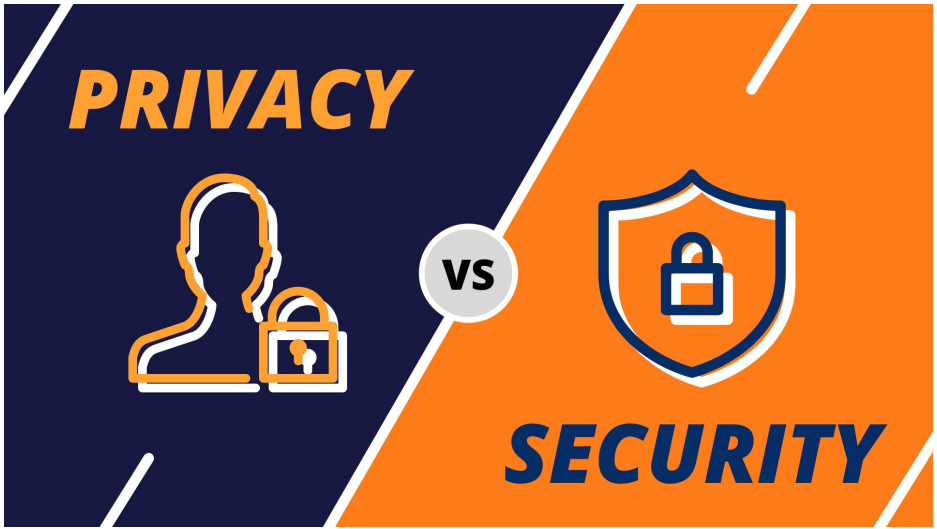
Niels Feij
Henk Berendsen
Thomas de Haan

Radboud University

Privacy versus Security

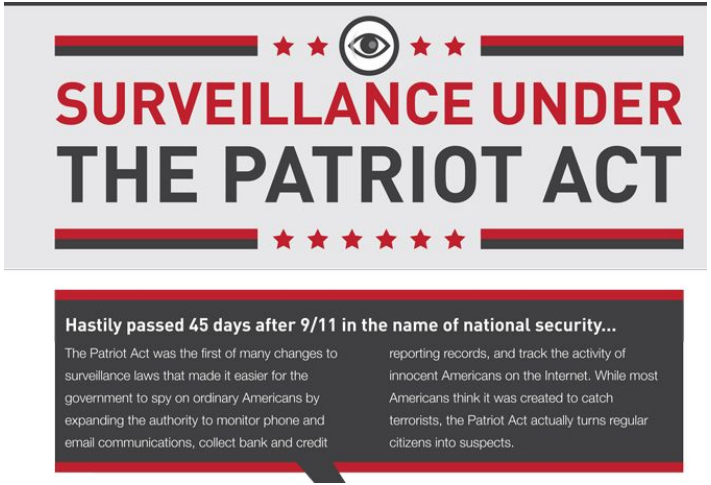
Privacy or security:

- Security and privacy are both important
- Strong security → weak privacy and vice versa
- Security seems to be winning
- Giving up privacy for tempting reasons
- Examples?



Patriot Act

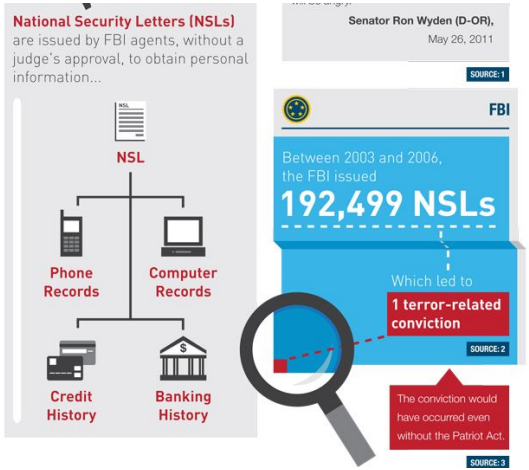
- Signed in 2001 - 45 days after 9/11



ACLU - 2014 - Surveillance under the patriot act infographic

Patriot Act

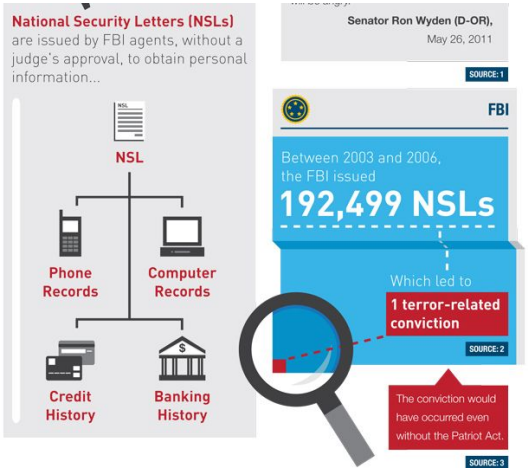
- Signed in 2001 - 45 days after 9/11
- NSLs

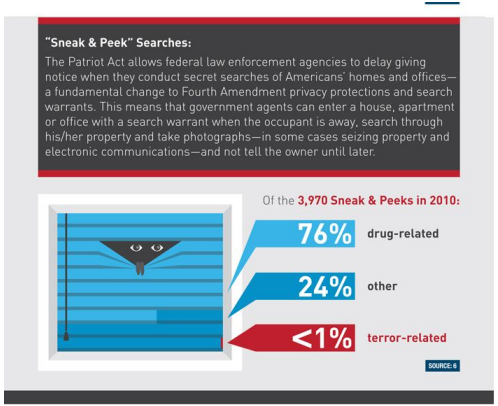


ACLU - 2014 - Surveillance under the patriot act infographic

Patriot Act

- Signed in 2001 - 45 days after 9/11
- NSLs
- Sneak & peaks

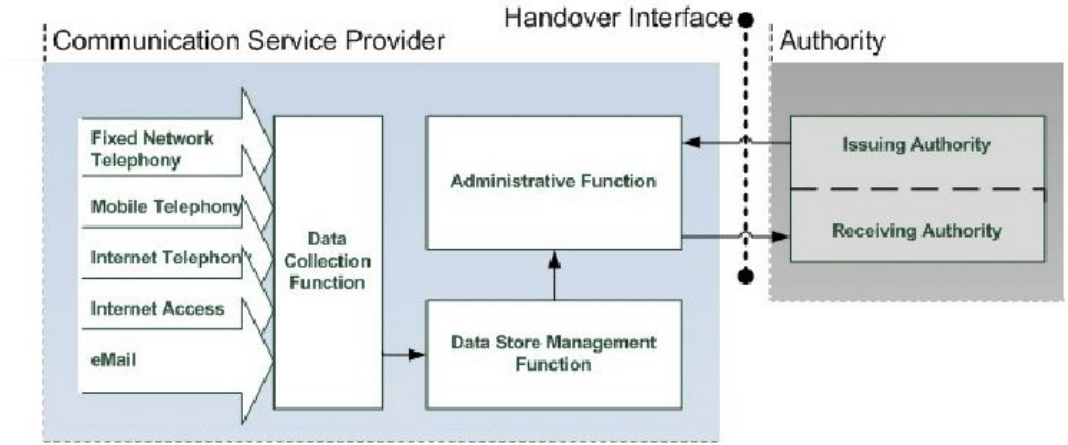




ACLU - 2014 - Surveillance under the patriot act infographic

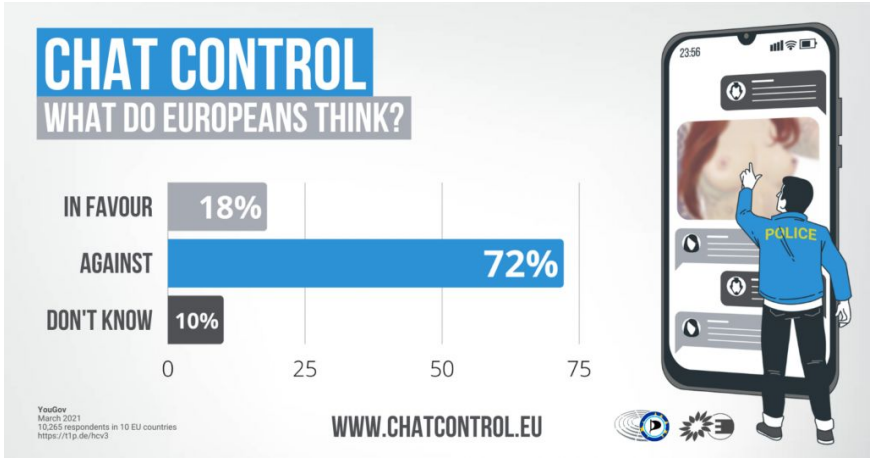
European data retention directive

- Passed in 2006 by EU
- Telecommunication metadata
- Invalidated by European court of justice in 2014
- Many countries still kept the national laws



Child sexual abuse regulation (CSAR)

- Proposed in 2022
- Fight CSAM and Online grooming
- Proposal includes a form of client side scanning
- What are risks?
- Still no decision
- Lots of backlash
- Prof. Zuiderveen Borgesius



Security & Privacy

Combining security and privacy:

- A false contradiction
- Privacy while maintaining security
- Security for companies and services
- Safe and usable platforms without giving up all privacy
- Revocable privacy

What is revocable privacy?

Definition

Property:

Data related to users who do not break any rule, is irrelevant. These users should stay anonymous as if no data was ever collected. [Lueks et al. 2016]

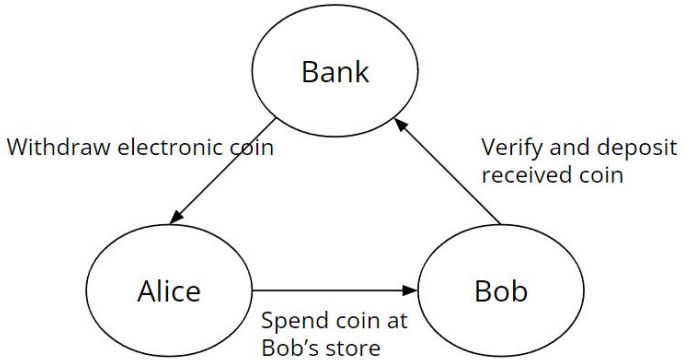
Definition:

Users of a system are guaranteed to be anonymous unless they violate a predefined rule

Digital cash

Untraceable Electronic Cash [Chaum et al.]

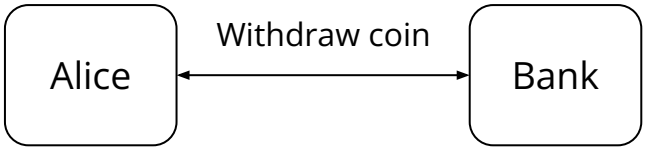
- Online cash system
- First type of cryptographic electronic currency
- Alice is fully unlinkable to Bank



Digital cash

Alice withdraws a coin:

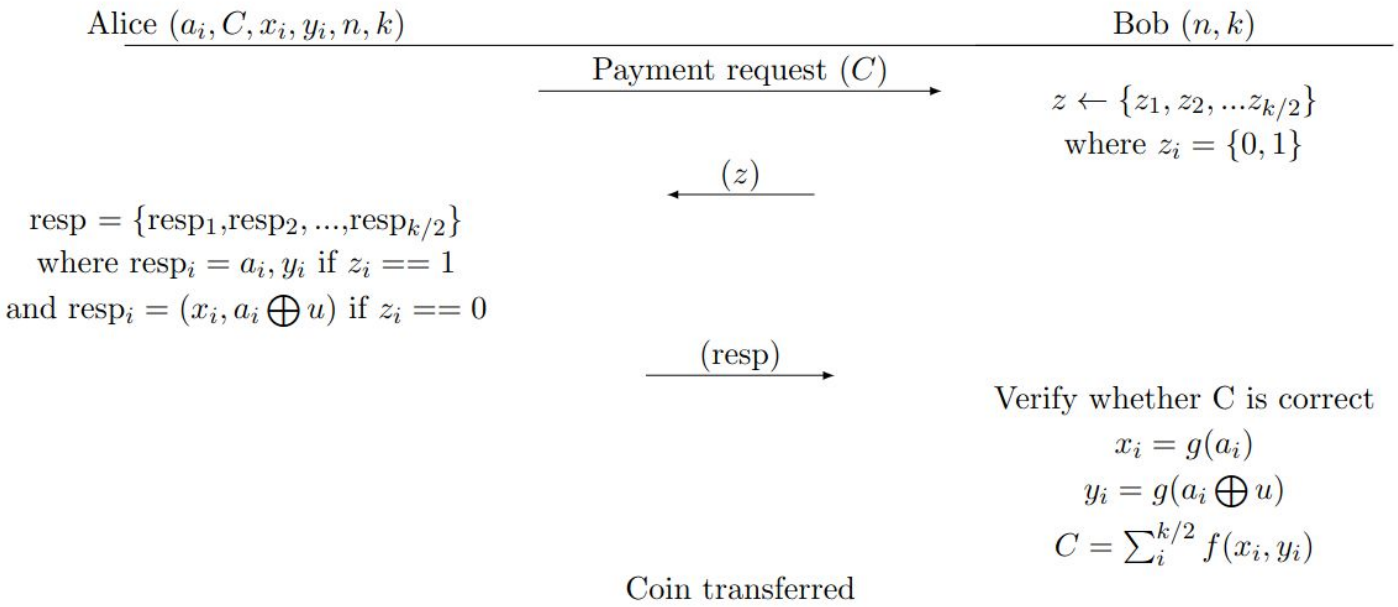
- Bank creates security parameter k
- Alice creates k times some secret variables, amongst which is a
- Functions f, g behave like random oracle
- Alice has a bank account number u
- Alice extracts coin $C = \sum_i^{k/2} f(x_i, y_i)$
- $x_i = g(a_i)$
- $y_i = g(a_i \oplus u)$



Example: Untraceable Electronic Cash

Digital cash

Alice pays Bob

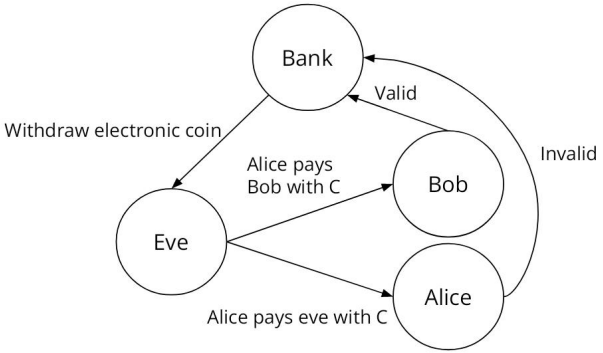


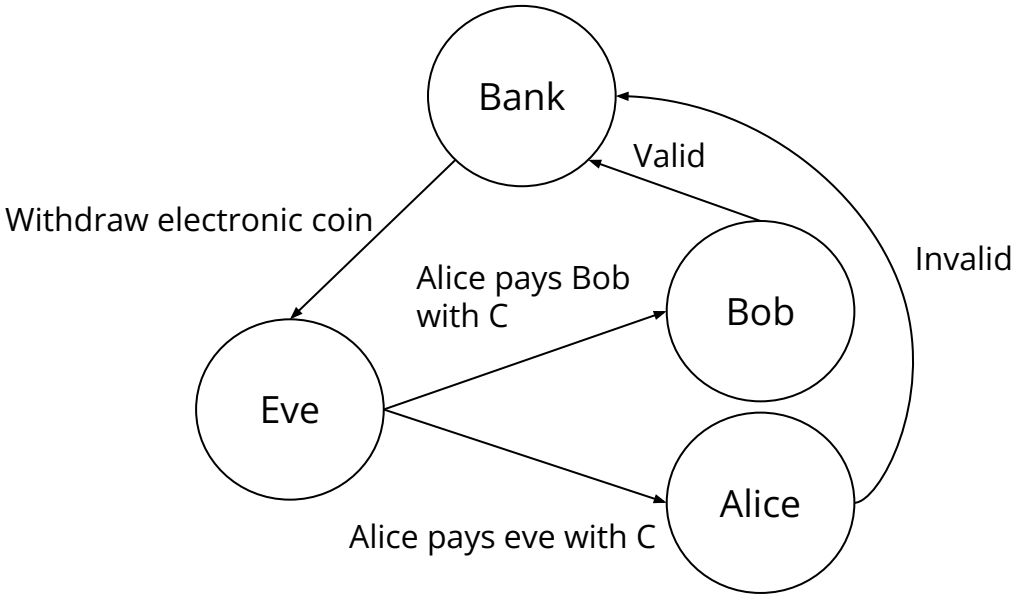
Example: Untraceable Electronic Cash

Digital cash

Multiple spending:

- Instead of Alice, Eve withdraws a coin and pays bob
- What if she spends C in another store?
- Other store will also create binary string z'
- If there exists an i such that $z'_i \neq z_i$
- The bank can find Eve's bank account : $a_i \oplus (a_i \oplus u) = u$




Bank
Valid
Withdraw electronic coin
Invalid
Alice pays Bob
with C
Bob
Eve
Alice
Alice pays eve with C

Anonymity

Different levels of anonymity:

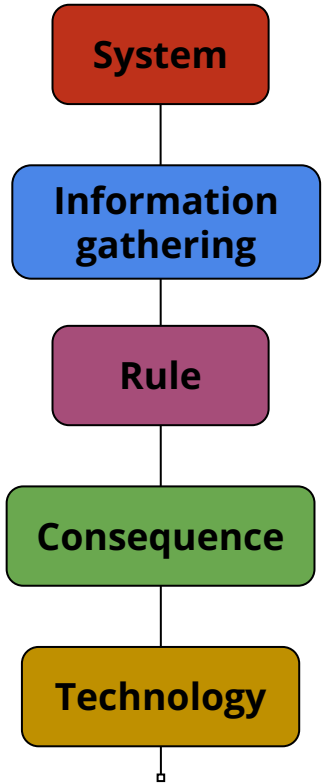
- **Fully identifiable**
  - Users full identity can be easily uncovered
- **Pseudonymity**
  - Users full identity is hidden but still linkable
- **Unlinkability**
  - User is fully anonymous and no two actions are linkable

Anonymity

Object	What level of anonymity?
- Email address (without name):	**Pseudonymity**
- Licence Plate:	**Fully identifiable**
- Anonymous bank account:	**Pseudonymity**
- Cash:	**Unlinkability**

What does it look like

1. **System with guaranteed anonymity**
2. **Method of information gathering**
3. **Rule (what constitutes misbehaviour?)**
4. **Consequence**
5. **Technology**

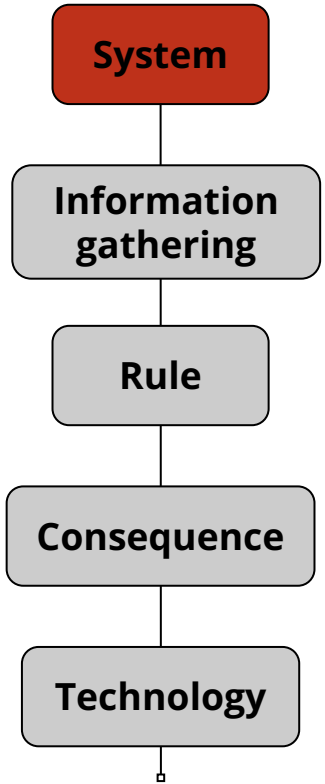


What does it look like

1. **System with guaranteed anonymity:**

- Technical vs policy
  - Function creep

- Provided anonymity
  - Pseudonymity
  - Unlinkability
  - Can be toward other users
  - Depends on method of information gathering



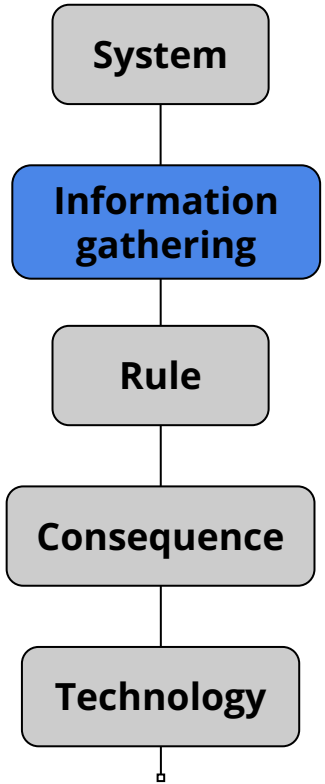
What does it look like

2. **Method of information gathering:**

- Plaintext logging
  - Identity & relevant actions stored
  - Check rules against stored data
  - Policy related
  - Third parties

- Non-interactive sensors
  - Actions and Identities are visible
  - Encrypted based on rule
  - Nothing stored in plaintext
  - Trust in key management and proper behaviour

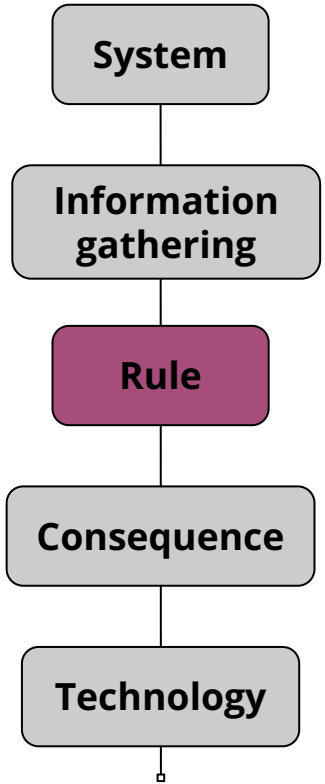
- Interactive sensors
  - User interaction
  - Fully anonymous
  - Trust in the users instead of sensor



What does it look like

3. **Rule**

- Definition of misbehaviour
- What was the rule in electronic cash?
- Pre-defined
  - Ideally known to users
  - Configurable parameters
- Multiple different classes of rules
- To be continued…

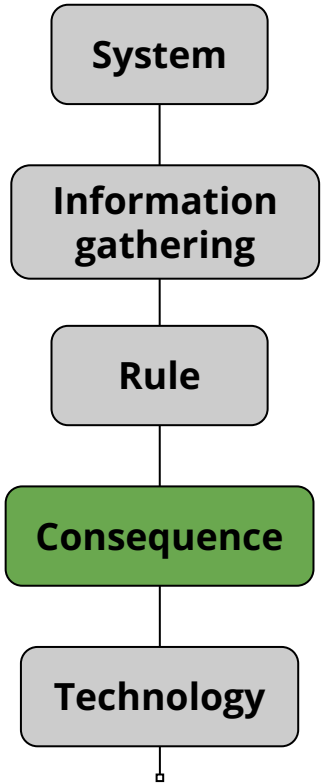


What does it look like

4. **Consequence**

- Revoking of privacy
  - Revoking privacy to the company/service
  - Revoking privacy to other users

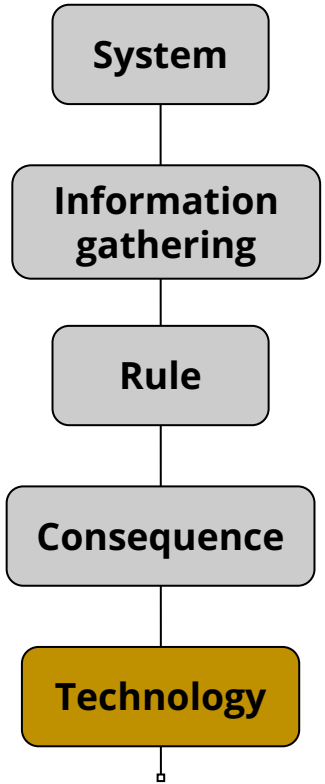
- Blocking (can anyone think of an example?)
  - Platform wide
  - Localized



What does it look like

5. **Technology**

- Actively researched
- Often cryptographic in nature
- To be continued…



The Rules

Overview of rules [Lueks et al. 2016]

Threshold Rules
If action performed ≥ k times, then …

Predicate Rules
Logical AND formula of variables
If A and B and C, then …

Decision rules
Rules with human influence
If A is offensive, then …

Complex rules
Complex data (graphs, labels) or auxiliary data

Fuzzy rules

Threshold rules

What
Threshold for actions within given period of time

When
Simple cases, relatively easy to implement

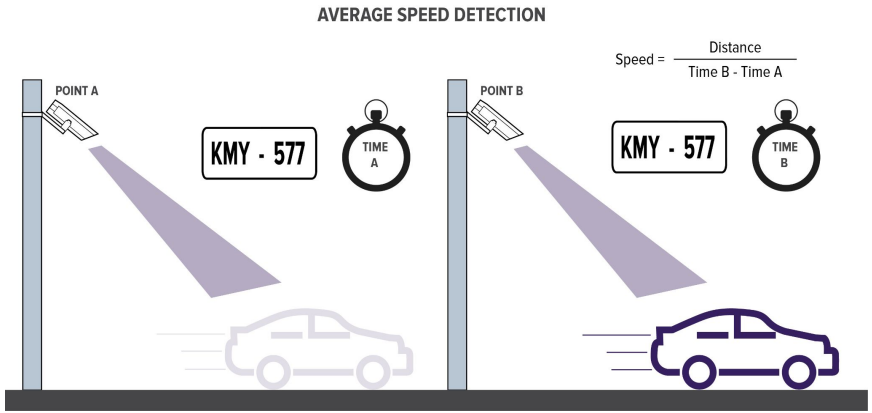
How
Distributed encryption, n-times Anonymous Credentials, Transaction based Pseudonyms

Average speed checking

Case

Police wants to identify drivers that go over the speed limit on a given route

- Information gathering: Non-interactive sensor (camera)
- Rule: No more than 1 measurement within timeframe
- Consequence: Licence plate is revealed
- Technology: Distributed Encryption



Distributed encryption

The primitive allows a recipient of a message to decrypt it only if enough senders encrypted that same message.

- Tool to implement revocable privacy [Hoepman and Galindo]
- Senders have to be trusted
- Recovering plaintext is exponential

KDE

Key-evolving Distributed Encryption [Lueks et al., 2014]

- Proposed more efficient schemes
  - to handle short time frames
  - to handle high observation numbers

Uses

- *Lagrange coefficients*
- *k-out-of-n Shamir secret sharing*

Lagrange coefficients

For a set $I \subseteq \{1, \ldots, n\}$ and field $\mathbb{Z}_q$ with $q > n$,

We define:
Lagrange polynomials $\lambda_i^I(x)$ as $\lambda_i^I(x) = \prod_{t \in I \setminus \{i\}} \frac{x - t}{i - t} \in \mathbb{Z}^*{}_q[x]$

Lagrange coefficients as $\lambda_i^I = \lambda_i^I(0)$

Then:
For any polynomial $P \in \mathbb{Z}_q[x]$ of degree at most $|I| - 1$,

$$P(x) = \sum_{i \in I} P(i)\lambda_i^I(x) \qquad P(0) = \sum_{i \in I} P(i)\lambda_i^I$$

Lagrange coefficients cont.

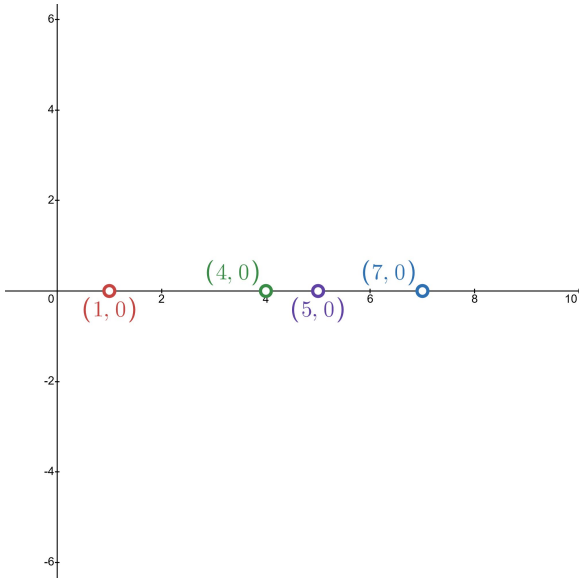
Let $I = \{1, 4, 5, 7\}$ and the field $\mathbb{Z}_{10}$ such that $q > n$ holds

For each $i \in I$ we compute the the *lagrange polynomial* $\lambda_i^I(x)$

$$\lambda_1^I(x) = \prod_{t \in I \setminus \{1\}} \frac{x-t}{i-t} = \frac{(x-4)(x-5)(x-7)}{(1-4)(1-5)(1-7)} \in \mathbb{Z}^*{}_q[x]$$

And *lagrange coefficient* λ_i^I

$$\lambda_1^I = \lambda_i^I(0) = \frac{(0-4)(0-5)(0-7)}{(1-4)(1-5)(1-7)} = 1\frac{17}{18}$$



Lagrange coefficients cont.

For any polynomial $P \in \mathbb{Z}_q[x]$ of degree at most $|I| - 1$,

$$P(x) = \sum_{i \in I} P(i)\lambda_i^I(x) \qquad P(0) = \sum_{i \in I} P(i)\lambda_i^I$$

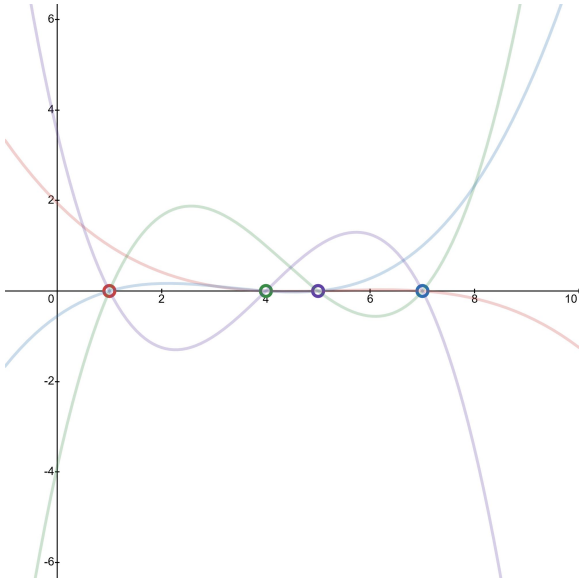
Let $P(x) = \frac{1}{2}x^3 - 2x^2 + 1$ such that $\deg(P) \leq |I| - 1$

$3 \leq 4 - 1$

Then:

$$P(x) = P(1)\lambda_1^I(1) + P(4)\lambda_4^I(4) + P(5)\lambda_5^I(5) + P(7)\lambda_7^I(7)$$

$$P(0) = P(1)\lambda_1^I + P(4)\lambda_4^I + P(5)\lambda_5^I + P(7)\lambda_7^I$$



KDE: the idea

- Let G be a cyclic group of prime order q, such that DDH is hard in G
- Let $\chi : \{0,1\}^{l_p} \rightarrow G$, an injection encoding, and χ^{-1}, the inverse such that $\chi^{-1}(\chi(p)) = p$
  - This mapping is redundant
- Every sender i is given a secret share $s_i \in \mathbb{Z}_q$ which corresponds to a *k*-out-of-*n* Shamir secret sharing of a *publically known* value: 1
- Let *f* be the corresponding degree $k-1$ secret sharing polynomial, then $f(0) = 1$ and $s_i = f(i)$

KDE: the idea cont.

Ciphertext creation

1. Sender encodes plaintext into a generator: $\chi(p) \in G$
2. Sender uses secret share to produce ciphertext share: $\alpha_i = \chi(p)^{s_i}$

Given enough of these shares for the same plaintext, the exponents can be removed, and the original ciphertext can be recovered.

How ?

- Consider a set $\{\alpha_{i_1}, \ldots, \alpha_{i_k}\}$ of shares with $I = \{i_1, \ldots i_k\}$ the set of indices
- Then there exist Lagrange coefficients $\lambda^I_{i_1}, \ldots, \lambda^I_{i_k}$ such that $\sum_{i \in I} \lambda^I_i s_i = f(0) = 1$
- So we can calculate $\alpha = \prod_{i \in I} \alpha_i^{\lambda^I_i} = \chi(p)^{\sum_{i \in I} s_i \lambda^I_i} = \chi(p)^{f(0)} = \chi(p)$

Server attack detection

Case

Server wants to detect and counter frequent fraudulent login attempts

- Information gathering: Plaintext logging (?)
- Rule: No more than *k* login attempts within timeframe *t*
- Consequence: IP address revealed
- Technology: Transaction based pseudonyms*

Transaction-based Pseudonyms [Biskup and Flegel]

Replaces personal identifiers by pseudonyms

If suspicious enough, identity can be recovered

Requires sensor to store records of events

Not truly revocable privacy, but best we've got

Predicate rules

What

- If A: Privacy secured - If B: Privacy secured - If A AND B: Privacy revoked
- Seemingly unrelated indicators

When

Often used in detecting criminal activity

How

Multiparty computation

Can you give an example?

Car frauds

Case

Tax office wants to find fraudulent car users.

Indicators:

1. Car is seen in traffic or public car park
2. Reported status of the car (work-only, not in use etc.)

- Information gathering: (non) Interactive sensor
- Rule: Both indicators must be true
- Consequence: License plate is revealed
- Technology: ???

Belastingdienst zet camera's in tegen belastingontduiker

De Belastingdienst wil automobilisten die motorrijtuigenbelasting (MRB) ontduiken vanaf volgend jaar opsporen via camerabeelden die op de openbare weg worden gemaakt. Dat blijkt uit het wetsvoorstel 'Overige Fiscale Maatregelen' dat onderdeel is van de Prinsjesdagstukken.

Decision rules

What

- Rules that include Human Decision making
- Input to this decision can be from human or automatic sensors
- More sensitive and subjective topics

When

Useful in scenarios where the rule cannot be “codified”

How

Blacklistable Anonymous Credentials (BLAC), Group signatures

Detecting child abuse

Case

Detecting child abuse by multiple authorities.

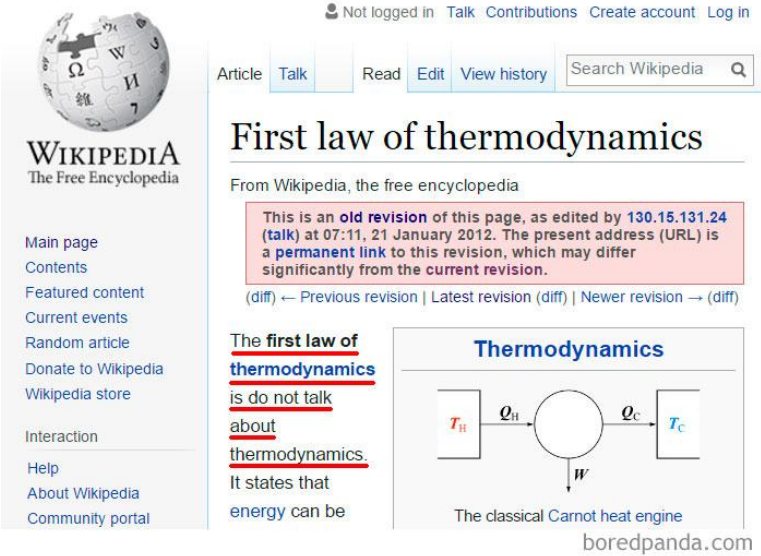
- Information gathering: Human input
- Rule: No more than *n* reports from different sources
- Consequence: Reveal child's identity
- Technology: Distributed encryption

Anonymous editing

Case

Platform wants to prevent anonymous individuals from making wrong/fake edits

- Information gathering: Human input
- Rule: No more than *n* reports by moderators
- Consequence: User is anonymously blocked
- Technology: BLAC



BlackListable Anonymous Credentials (BLAC) [Tsang et al.]

Idea

- User authenticates to Service Provider without revealing their identity
- Service Provider can deny access to misbehaving users by adding them to a blacklist

Involved parties

- User and Service Provider (SP)
- Group Manager (GM) issuing private *credentials* to users

Intuition

- User authenticates using private credential *cred*
- SP extracts *ticket* from authentication session's protocol transcript
- If user misbehaves, corresponding session's ticket is added to blacklist
- Authenticating user proves they did not generate a ticket on the blacklist

Complex rules

What

Rules that work with complex or extensive data

When

In cases of graphs, labels, large collateral information

How

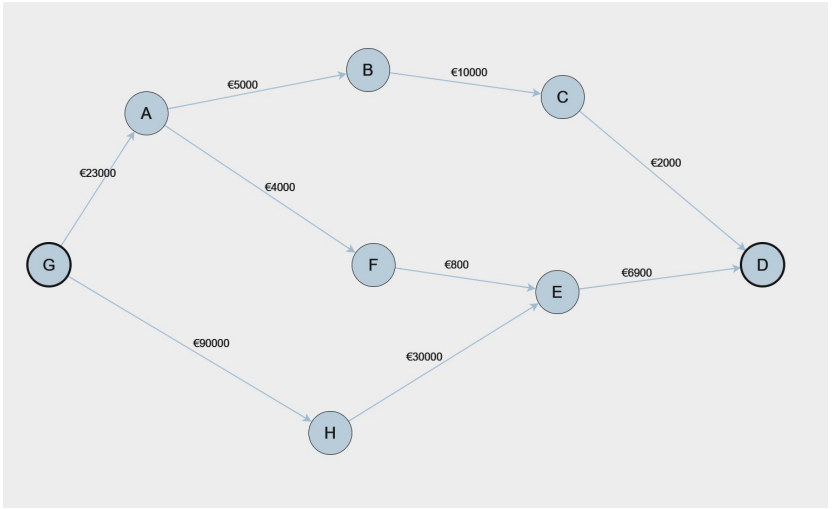
- Can be described by any (difficult to define) deterministic computer program
- Lack of techniques

Cash flow anomaly

Case

Tax authority wants to detect cash fraud

- Information gathering: Interactive sensors
- Rule: In a graph of companies (nodes) and reported money flow (edges), money flow must be consistent.
- Consequence: Nodes identity is revealed
- Technology: Multiparty Computation



Multiparty Computation

Multiple parties each have their own **private** input

Inputs used to compute a shared function of which only the output is shared

Computationally expensive

Successfully used to solve real world problems

Topic of final lecture

Privacy in practice

Is there active research on this?
Are there real world implementations in use?
Is it a known concept among big companies?
Why?

Overview of rules [Lueks et al. 2016]

Threshold Rules
If action performed ≥ k times, then …

Predicate Rules
Logical AND formula of variables
If A and B and C, then …

Decision rules
Rules with human influence
If A is offensive, then …

Complex rules
Complex data (graphs, labels) or auxiliary data

Fuzzy rules

Signal

What is Signal?

- Messenger app
  - Like Whatsapp, Facebook Messenger etc.
- Open source

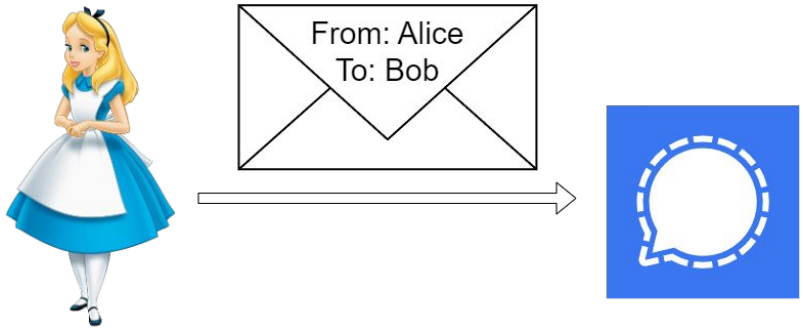
What is Signal?

- Messenger app
  - Like Whatsapp, Facebook Messenger etc.
- Open source
- Privacy friendly

Signal's current privacy features

End-To-End Encryption
Signal cannot read your messages

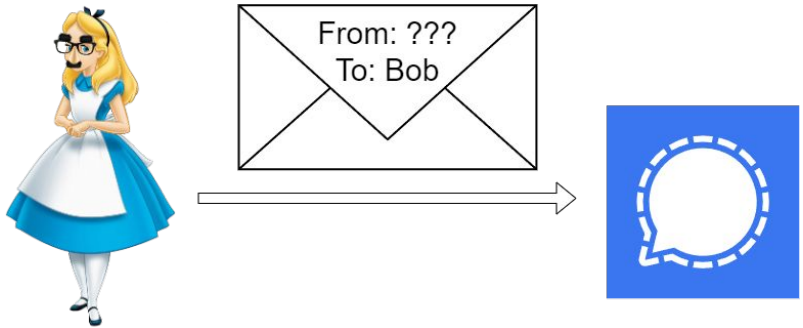
Sealed Sender
Signal does not know who the message's sender is



Signal's current privacy features

End-To-End Encryption
Signal cannot read your messages

Sealed Sender
Signal does not know who the message's sender is

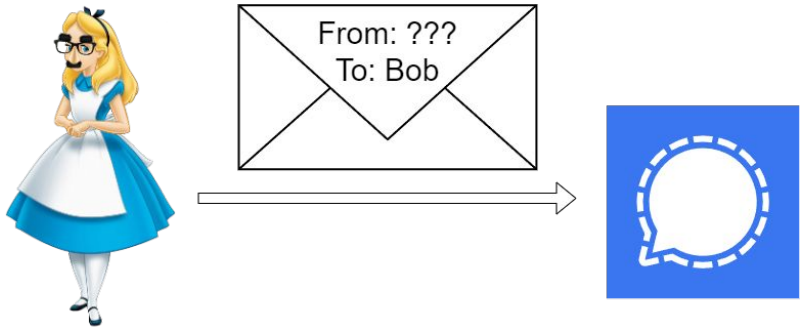


Signal's current privacy features

End-To-End Encryption
Signal cannot read your messages

Sealed Sender
Signal does not know who the message's sender is

Private Group System
Signal does not know anything about your groups



Signal's Private Group System

Signal's solution

- Group state is stored encrypted on Signal server
- Symmetric encryption key *K* known only to group members

Blackboard example

- How does Alice create a group with Bob?

Signal's Private Group System

Signal's solution

- Group state is stored encrypted on Signal server
- Symmetric encryption key *K* known only to group members

Blackboard example

- How does Alice create a group with Bob?
- What if Eve tries to modify the group state?

Signal's Private Group System

Signal's solution

- Group state is stored encrypted on Signal server
- Symmetric encryption key *K* known only to group members

Blackboard example

- How does Alice create a group with Bob?
- What if Eve tries to modify the group state?
- **Problem:** Signal cannot authenticate users because group members are encrypted!
- **Solution:** Anonymous credentials
    - Group members prove their membership without revealing their identity

Signal Groups Privacy

- Great privacy with respect to Signal ☺️
  - Signal doesn’t know who you are talking with (Sealed Sender + Private Groups)
  - Signal doesn’t know what you are talking about (E2E Encryption)

- Limited privacy with respect to other group members:
  - Phone number visible to group members
  - Other group members can easily identify you

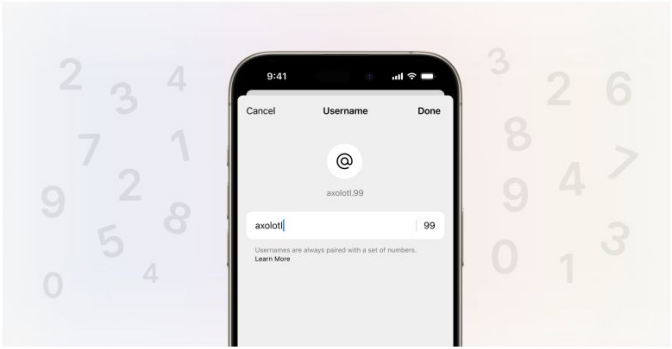
Signal: Private phone number update

New update

- Username instead of phone number
- More anonymity towards other users:
  - Choose *non-identifying* username

Keep your phone number private with Signal usernames

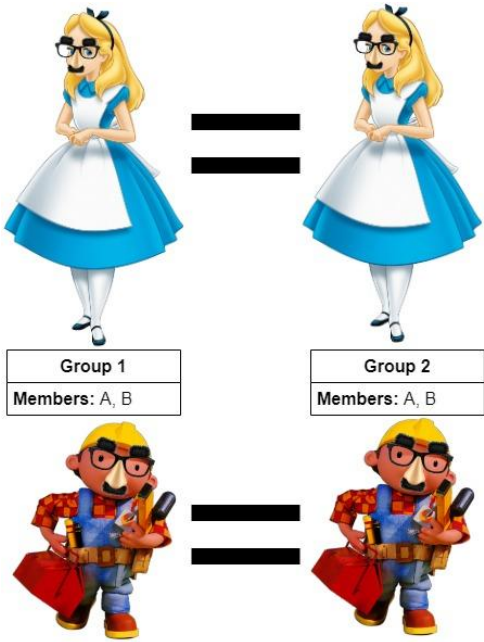
Randall Sarafa on 20 Feb 2024



Signal's mission and sole focus is private communication. For years, Signal has kept your messages private, your profile information (like your name and profile photo) private, your contacts private, and your groups private – among much else. Now we're taking that one step further, by making your phone number on Signal more private.

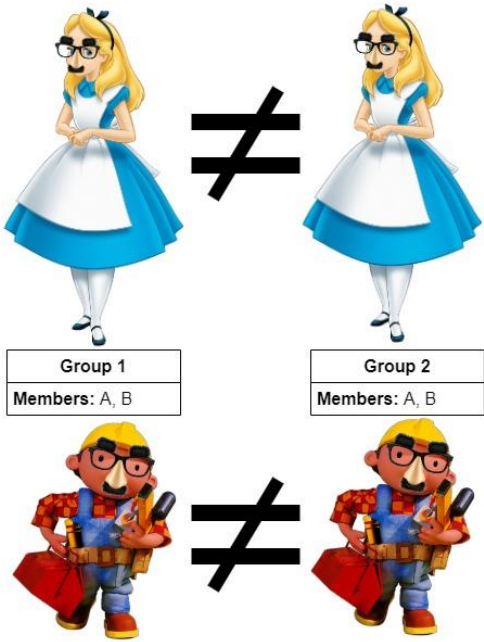
User anonymity in new update

- User achieves *pseudonymity* with respect to group members:
  - User cannot be identified by username
  - **But:** actions across groups are *linkable*
  - Link could be exploited to track the user across groups



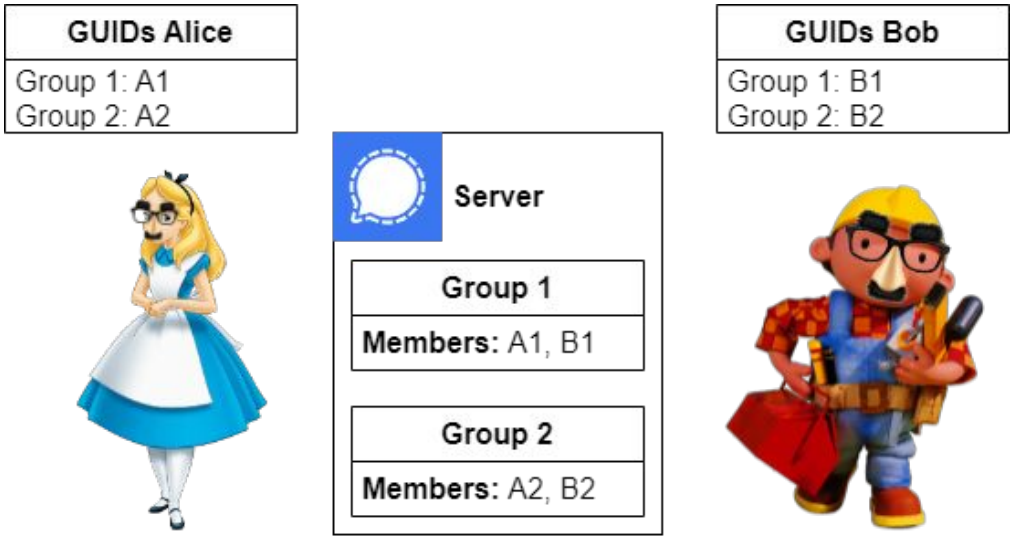
User anonymity in new update

- User achieves *pseudonymity* with respect to group members:
  - User cannot be identified by username
  - **But:** actions across groups are *linkable*
  - Link could be exploited to track the user across groups
  - Ideally, this link does not exist



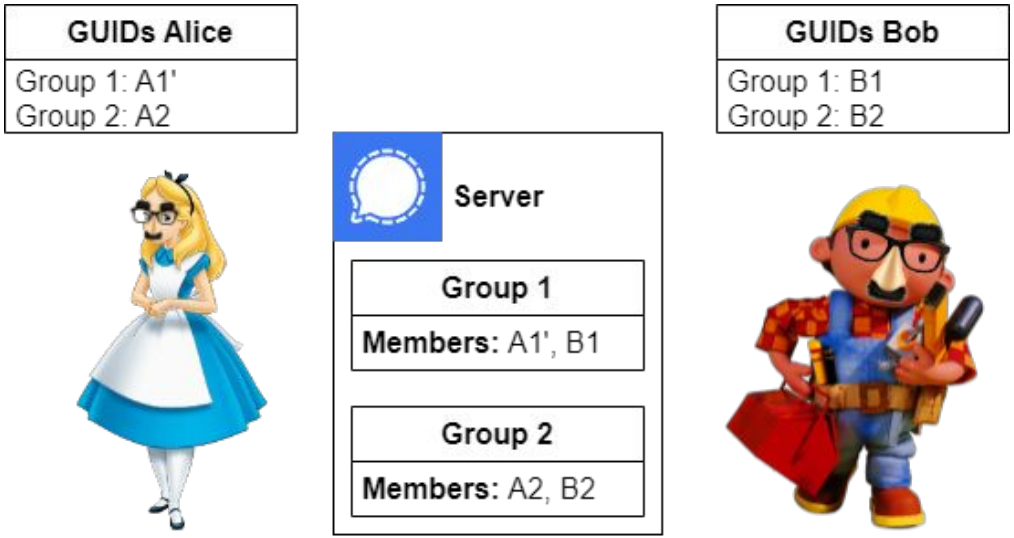
Our proposal: Signal+

- Instead of a global UID, user has a separate GUID for each group



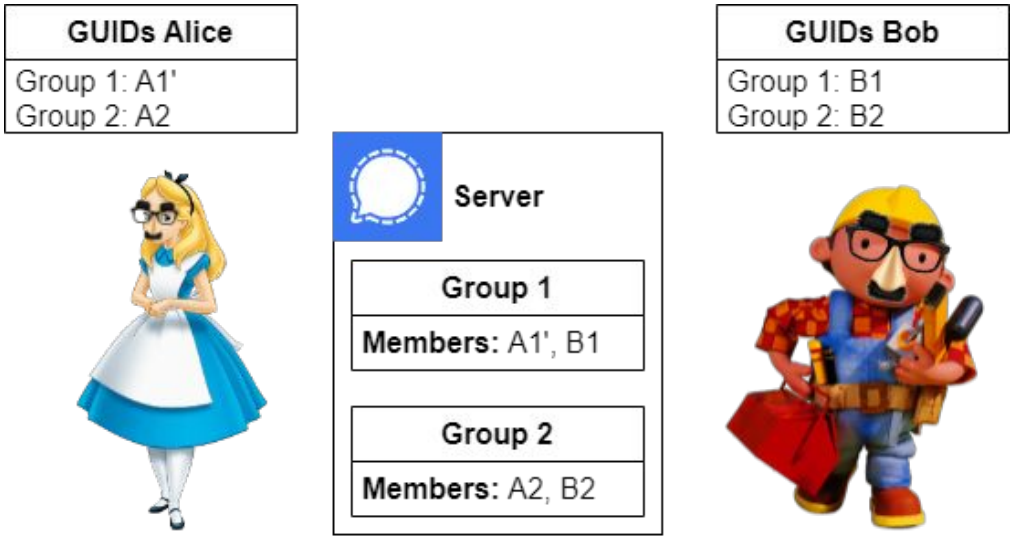
Our proposal: Signal+

- Instead of a global UID, user has a separate GUID for each group



Our proposal: Signal+

- Instead of a global UID, user has a separate GUID for each group



- Any problems if Alice wants to remove Bob from a group?

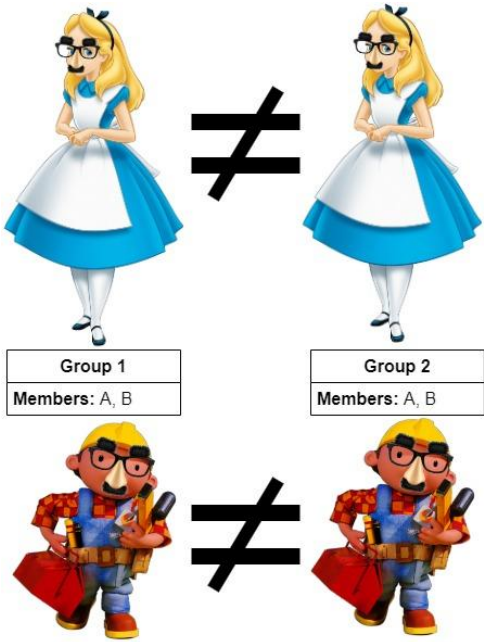
Our proposal: Signal+

Unlinkability across groups

- Instead of a fixed UID, user has a separate identity for each group
  - We call this identity the GUID
- Cross-group tracking no longer possible
- User can change identity in case of deanonymization

New challenges in Signal+

- Suppose Alice in a group with Eve
  - Alice and Eve are known by GUIDs A and E
- Eve is being malicious, so Alice wants to remove her from the group
- How can Alice remove Eve?



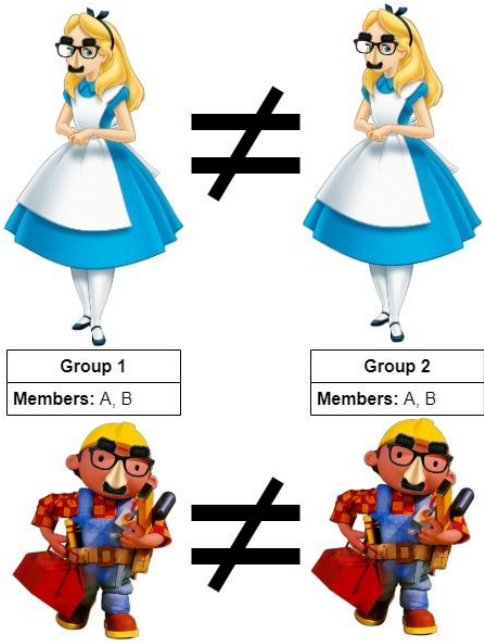
Our proposal: Signal+

Unlinkability across groups

- Instead of a fixed UID, user has a separate identity for each group
  - We call this identity the GUID
- Cross-group tracking no longer possible
- User can change identity in case of deanonymization

New challenges in Signal+

- Suppose Alice in a group with Eve
  - Alice and Eve are known by GUIDs A and E
- Eve is being malicious, so Alice wants to remove her from the group
- How can Alice remove Eve?
  - Suppose Alice removes E



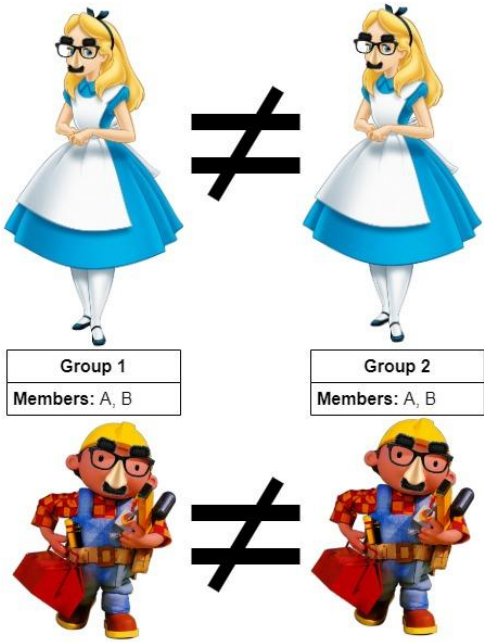
Our proposal: Signal+

Unlinkability across groups

- Instead of a fixed UID, user has a separate identity for each group
  - We call this identity the GUID
- Cross-group tracking no longer possible
- User can change identity in case of deanonymization

New challenges in Signal+

- Suppose Alice in a group with Eve
  - Alice and Eve are known by GUIDs A and E
- Eve is being malicious, so Alice wants to remove her from the group
- How can Alice remove Eve?
  - Suppose Alice removes E
  - Eve can just rejoin with a new identity!



Problem in Signal+ groups

Problem Description

- Group members only know each other's GUID
- Users can circumvent being removed from a group by changing their GUID

Solution

- We have a conflict of interests:
  - Benign users want to stay anonymous to Signal and group members
  - Signal and group members want to permanently block malicious users.
- Sounds like we need revocable privacy:
  - Rule: no more than 0 reports by group admin
  - Consequence: user is anonymously blocked from group

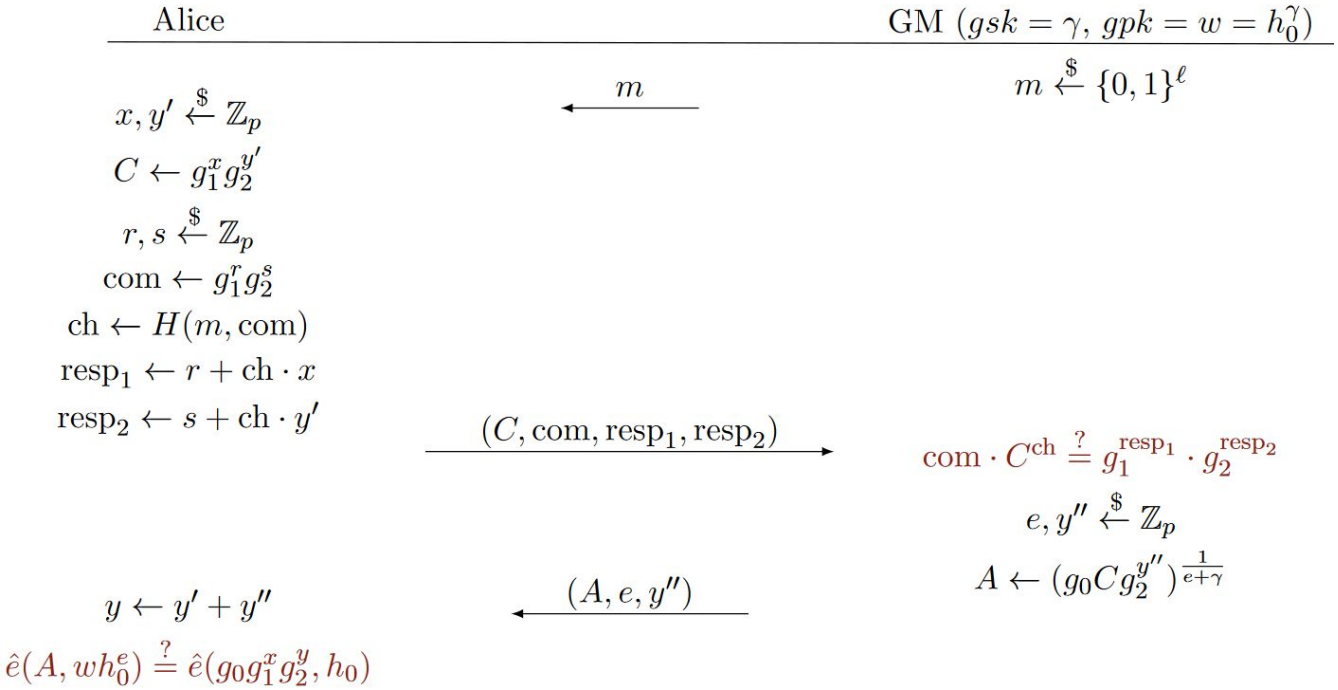
Recap of BLAC

- Involves user, Service Provider (SP) and Group Manager (GM)
- User registers with GM to obtain private credential *cred*
- SP keeps track of a blacklist of *tickets*
  - Each authentication session results in a ticket
  - Ticket can be added to blacklist if corresponding user misbehaved
- To authenticate, user proves they did not generate a ticket on the blacklist

Crypto behind BLAC: multiplicative groups

- Four multiplicative groups $\mathbb{G}, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ of order *p*
- Generators $g_0, g_1, g_2 \in \mathbb{G}_1$ and $h_0 \in \mathbb{G}_2$
- Bilinear function $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$
  - Bilinearity: $\hat{e}(A^x, B^y) = \hat{e}(A, B)^{xy}$
- Group manager has a key-pair (gsk, gpk):
  - $gsk = \gamma$ chosen randomly from $\mathbb{Z}_p$
  - $gpk = w = h_0^{\gamma}$
- User Alice has credential $cred = (A, e, x, y)$

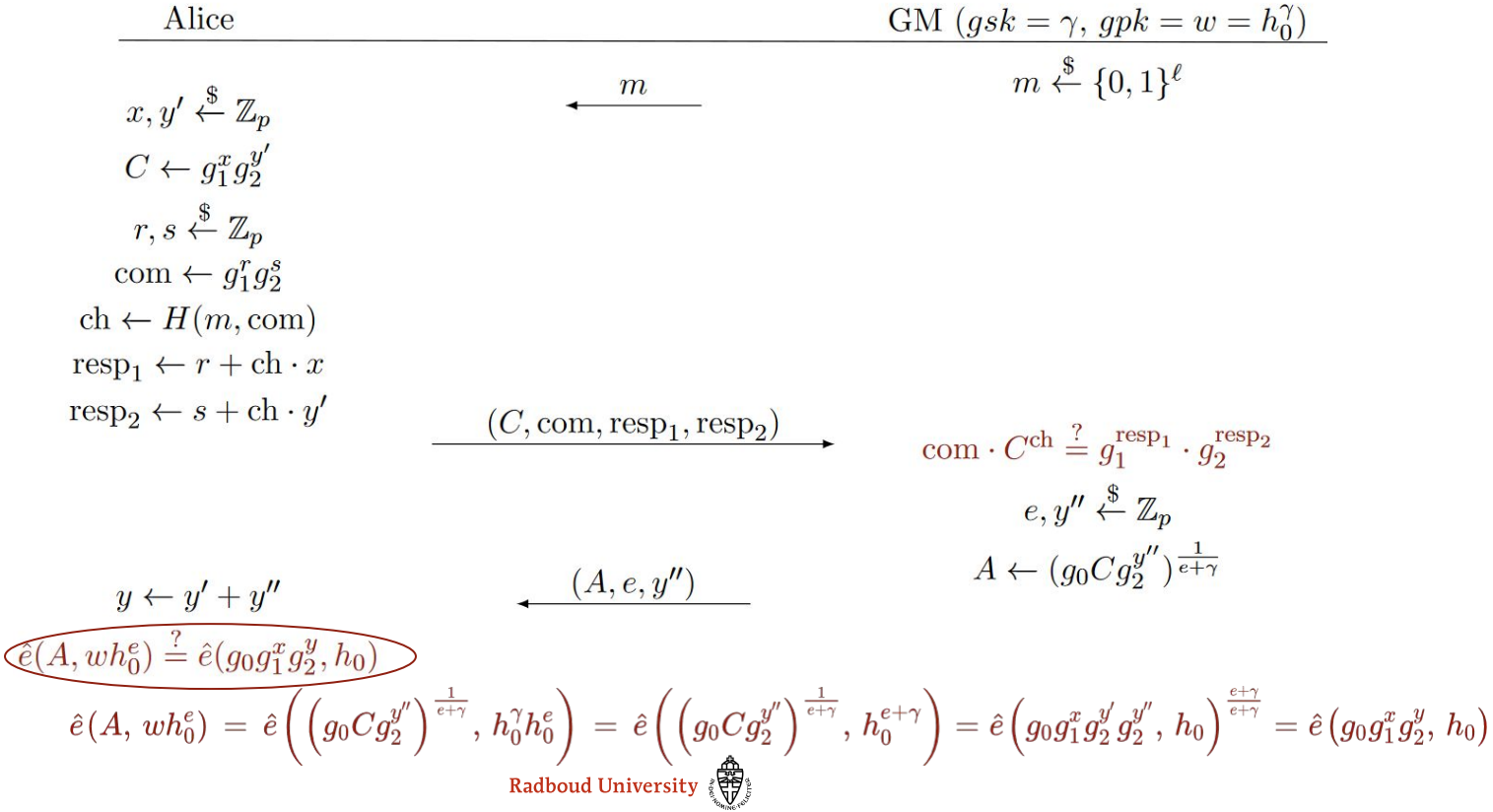
Crypto behind BLAC: issuing credentials



Crypto behind BLAC: issuing credentials

Alice		GM $(gsk = \gamma,\ gpk = w = h_0^{\gamma})$
		$m \xleftarrow{\$} \{0,1\}^{\ell}$
	$\xleftarrow{m}$	
$x, y' \xleftarrow{\$} \mathbb{Z}_p$		
$C \leftarrow g_1^x g_2^{y'}$		
$r, s \xleftarrow{\$} \mathbb{Z}_p$		
$\text{com} \leftarrow g_1^r g_2^s$		
$\text{ch} \leftarrow H(m, \text{com})$		
$\text{resp}_1 \leftarrow r + \text{ch} \cdot x$		
$\text{resp}_2 \leftarrow s + \text{ch} \cdot y'$		
	$\xrightarrow{(C, \text{com}, \text{resp}_1, \text{resp}_2)}$	$\text{com} \cdot C^{\text{ch}} = g_1^r g_2^s \cdot \left(g_1^x g_2^{y'}\right)^{\text{ch}} = g_1^r g_2^s \cdot g_1^{\text{ch}\cdot x} g_2^{\text{ch}\cdot y'} = g_1^{\text{r+ch}\cdot x} g_2^{s+\text{ch}\cdot y'} = g_1^{\text{resp}_1} \cdot g_2^{\text{resp}_2}$
		$\text{com} \cdot C^{\text{ch}} \stackrel{?}{=} g_1^{\text{resp}_1} \cdot g_2^{\text{resp}_2}$
		$e, y'' \xleftarrow{\$} \mathbb{Z}_p$
		$A \leftarrow (g_0 C g_2^{y''})^{\frac{1}{e+\gamma}}$
	$\xleftarrow{(A, e, y'')}$	
$y \leftarrow y' + y''$		
$\hat{e}(A, w h_0^e) \stackrel{?}{=} \hat{e}(g_0 g_1^x g_2^y, h_0)$		

Crypto behind BLAC: issuing credentials



Crypto behind BLAC: issuing credentials

Alice		GM $(gsk = \gamma,\ gpk = w = h_0^{\gamma})$
		$m \xleftarrow{\$} \{0,1\}^{\ell}$
	$\xleftarrow{\quad m \quad}$	
$x, y' \xleftarrow{\$} \mathbb{Z}_p$		
$C \leftarrow g_1^x g_2^{y'}$		
$r, s \xleftarrow{\$} \mathbb{Z}_p$		
$\text{com} \leftarrow g_1^r g_2^s$		
$\text{ch} \leftarrow H(m, \text{com})$		
$\text{resp}_1 \leftarrow r + \text{ch} \cdot x$		
$\text{resp}_2 \leftarrow s + \text{ch} \cdot y'$		
	$\xrightarrow{\quad (C, \text{com}, \text{resp}_1, \text{resp}_2) \quad}$	
		$\text{com} \cdot C^{\text{ch}} \stackrel{?}{=} g_1^{\text{resp}_1} \cdot g_2^{\text{resp}_2}$
		$e, y'' \xleftarrow{\$} \mathbb{Z}_p$
		$A \leftarrow (g_0 C g_2^{y''})^{\frac{1}{e+\gamma}}$
	$\xleftarrow{\quad (A, e, y'') \quad}$	
$y \leftarrow y' + y''$		
$\hat{e}(A, w h_0^e) \stackrel{?}{=} \hat{e}(g_0 g_1^x g_2^y, h_0)$		

At the end of the protocol, Alice has obtained her credential $cred = (A, e, x, y)$

Crypto behind BLAC: authentication

Scenario

- User Alice with $cred = (A, e, x, y)$ authenticates towards SP Bob
- Bob has a blacklist $BL = \langle \tau_1, \ldots, \tau_n \rangle$
  - Ticket τ_i consists of a *serial* $s_i \in \{0,1\}^\ell$ and *tag* $t_i \in \mathbb{G}$
- Hash function $H_0 : \{0,1\}^* \to \mathbb{G}$

Authentication

- Bob sends $(BL,\ m)$ with $m \xleftarrow{\$} \{0,1\}^\ell$ a random message
- Alice computes the *bases* $b_i = H_0(s_i || \text{Bob})$ and a new ticket $\tau = (s, H_0(s||\text{Bob})^x)$
- Alice proves in zero knowledge:
  1. Her credential is valid: $\hat{e}(A,\ wh_0^e) = \hat{e}\left(g_0 g_1^x g_2^y,\ h_0\right)$
  2. She is not blacklisted: $t_i \neq b_i^x$ for all i
  3. Her new ticket is valid: $t = H_0(s||\text{Bob})^x$

Applying BLAC to Signal+

Involved parties

- Signal acts as Group Manager to issue credentials to its users
- Signal acts as Service Provider to let users interact with a group

Blacklist

- Each group has a blacklist of removed users
- To link users with new GUID to the blacklist, the GUID is a BLAC ticket
  - Even with new GUID, user cannot prove they *did not* generate a blacklisted ticket
- If a user is removed from a group, their GUID is added to the blacklist

Group access management

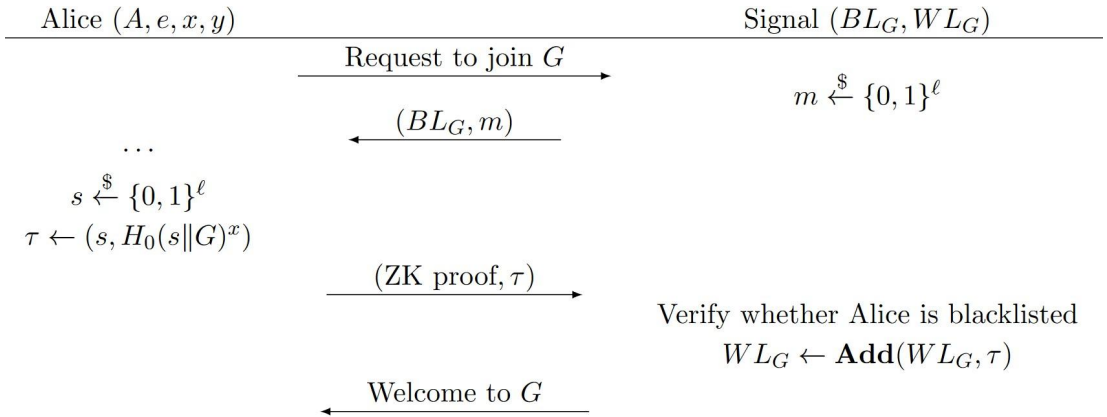
- Only group members are allowed to retrieve/modify group state
- Problem: Signal does not know identity of group members
- Solution: each group also has a **whitelist** of GUIDs:
  - User should prove to Signal that they *did* generate a whitelisted ticket

Signal+ group example

Scenario

Alice is a registered Signal user with credential $cred = (A, e, x, y)$ who wants to join group G

Joining the group



To change her identity, Alice can leave and rejoin the group

Signal+ group messaging

- Alice is now part of G, but how does she receive a group message?
  - In the context of the group, both Signal and group members do not know her UID
- Solution: Signal stores look-up table of (GUID, UID) pairs
  - To maintain unlinkability, GUIDs are hashed with a keyed hash function
  - After joining G with GUID τ, Alice asks Signal to add $(H(K_G||\tau), \text{Alice})$
- Bob sending a group message to (among others) Alice:
  1. Bob retrieves τ from WL_G
  2. Bob asks Signal to send a message to the UID corresponding to $H(K_G||\tau)$
  3. Signal uses the look-up table and forwards the message to Alice

Signal+ group example

Scenario

Bob wants to join Alice's group, and has the symmetric group key *K*

Joining the group

1. Bob anonymously authenticates towards Signal, and requests to join group
2. Ticket from this authentication session will be his GUID *B*
3. Bob has to prove he did not generate any tickets on the group's blacklist:
   - If Bob is blacklisted, authentication fails
   - Otherwise, Signal adds his GUID to the whitelist
4. Bob adds himself to the group members list

Sending group messages

- Signal maintains lookup table of hashed GUID - UID pairs
- Bob asks Signal to add *(H(K || B), Bob)*
- Group members can message Bob by computing *H(K || B)*

Signal+ group anonymity

- User's identity in a group (GUID) is a different BLAC ticket in each group
  - BLAC tickets are unlinkable and non-invertible
- Group members only know each other's GUIDs
  - Unlinkability with respect to other users is achieved
- Signal also has a lookup table of pairs $(H(K_G||\text{GUID}), \text{UID})$
  - If H is cryptographically secure, Signal cannot derive the GUID from the digest
  - Unlinkability with respect to Signal is achieved

Signal+ reflection

- Can Signal+ unlinkability be improved?
- Are there scenarios where users *can* be linked?

Q&A

References

- **[Biskup and Flegel]:** Biskup, Joachim & Flegel, Ulrich. (2000). *Transaction-Based Pseudonyms in Audit Data for Privacy Respecting Intrusion Detection.*
- **[Hoepman and Galindo]:** Hoepman, Jaap-Henk & Galindo, David. (2011). *Non-interactive Distributed Encryption: A New Primitive for Revocable Privacy.*
- **[Lueks et al. 2014]:** Lueks, Wouter & Hoepman, Jaap-Henk & Kursawe, Klaus. (2014). *Forward-Secure Distributed Encryption.*
- **[Lueks et al. 2016]:** Lueks, Wouter & Everts, Maarten & Hoepman, Jaap-Henk. (2016). *Revocable Privacy: Principles, Use Cases, and Technologies.*
- **[Tsang et al.]:** Tsang, Patrick & Au, Man Ho & Kapadia, Apu & Smith, Sean. (2007). *Blacklistable anonymous credentials: Blocking misbehaving users without TTPS.*
- **[Chaum et al.]:** Chaum, D., Fiat, A., & Naor, M. (1990). *Untraceable Electronic Cash. Annual International Cryptology Conference.*