Revocable Privacy

Privacy Seminar

Tea Coroș
Lucas van der Laan
Michiel Philipse
Elwin Tamminga
Giovanni Uchoa de Assis

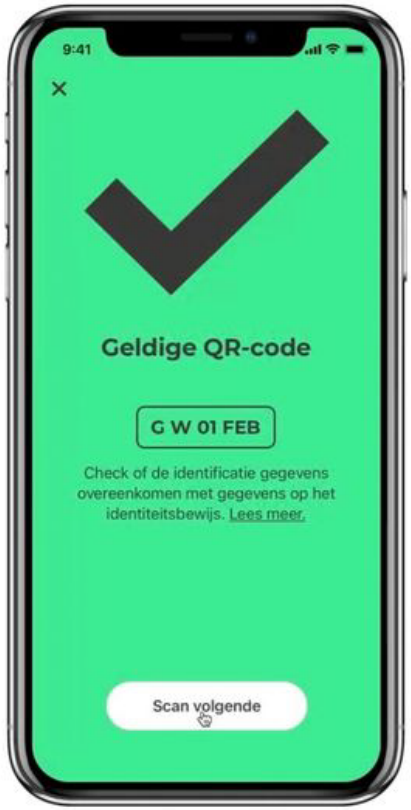
iCIS | Digital Security
Radboud University

Privacy vs Security

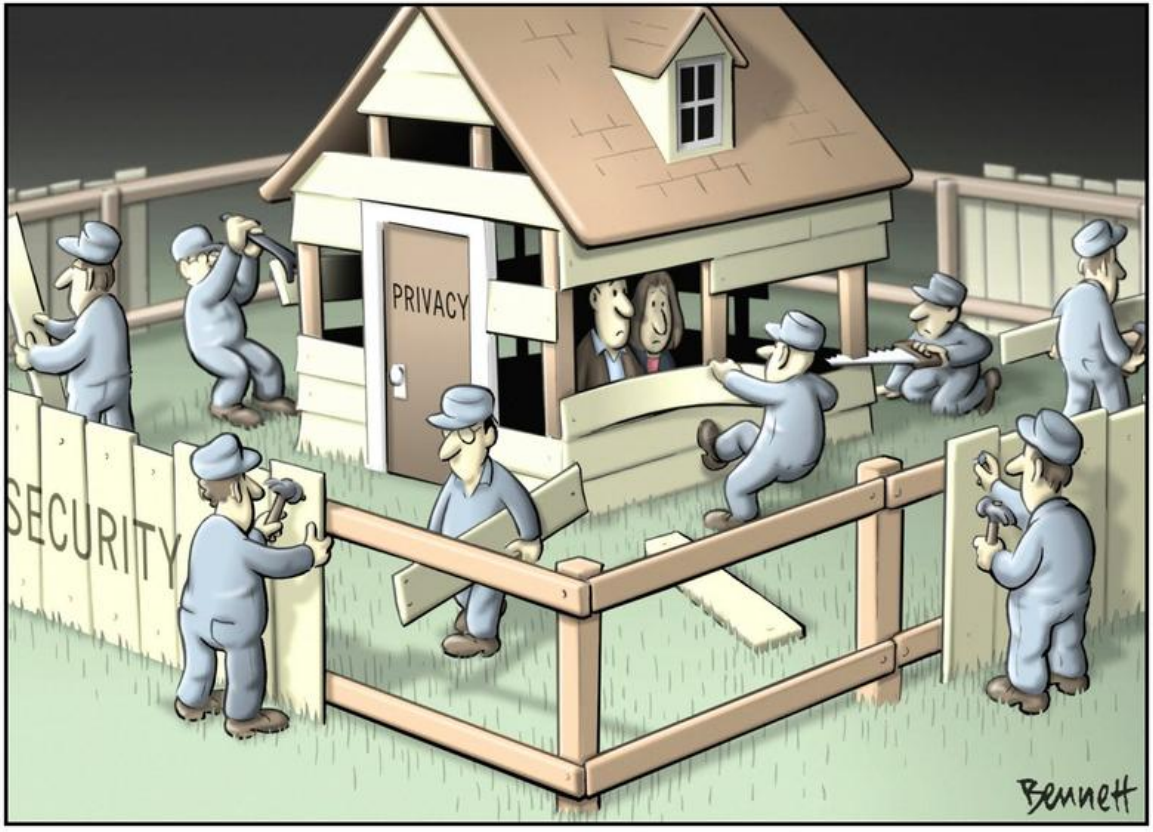
Sleepwet: 3 redenen om tegen te stemmen

Op 21 maart 2018 wordt tijdens de gemeenteraadsverkiezingen ook een raadgevend referendum gehouden. Nederland stemt dan voor of tegen de nieuwe Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv), ook wel bekend als de Sleepwet. Amnesty heeft grote zorgen over deze wet, omdat die onnodig onze privacy en vrije meningsuiting bedreigt. Ook kunnen onze gegevens in verkeerde handen terechtkomen. We willen een wet die onze veiligheid én onze mensenrechten beschermt. Daarom adviseren wij: stem tegen de Sleepwet op 21 maart. Zo roep je de regering op de wet te verbeteren.

Privacy vs Security



Privacy vs Security



Privacy and Security?

Revocable Privacy

- Privacy **AND** security
- Different levels of anonymity
- Main idea:

"Data related to people who do not violate any rules are irrelevant, and, in fact, these people should remain anonymous, as if no data on their behavior was ever collected." [4]

Revocable Privacy: Principles, Use Cases, and Technologies

Wouter Lueks[1( )], Maarten H. Everts[2], and Jaap-Henk Hoepman[1]

[1] Radboud University, Nijmegen, The Netherlands
{lueks,jhh}@cs.ru.nl
[2] TNO, Netherlands Organisation for Applied Scientific Research, The Hague, The Netherlands
maarten.everts@tno.nl

Abstract. Security and privacy often seem to be at odds with one another. In this paper, we revisit the design principle of revocable privacy which guides the creation of systems that offer anonymity for people who

Revocable Privacy: Principles, Use Cases, and Technologies

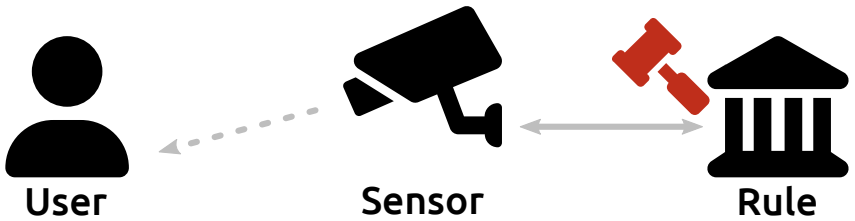
Wouter Lueks[1( )], Maarten H. Everts[2], and Jaap-Henk Hoepman[1]

"A system implements **revocable privacy** if the architecture of the system guarantees a **predefined level of anonymity** for a participant as long as she does not violate a **predefined rule**."

Abstract. Security and privacy often seem to be at odds with one another. In this paper, we revisit the design principle of revocable privacy which guides the creation of systems that offer anonymity for people who

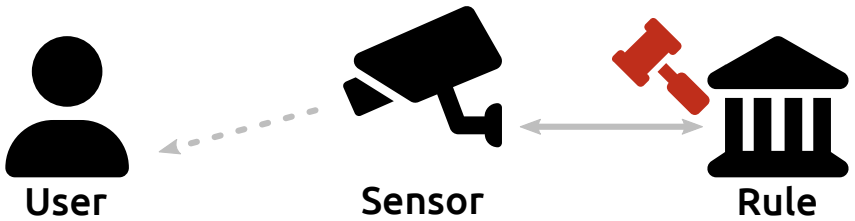
Sensors

- **Non-interactive sensors**
  - Data is simply stored
  - The system keeps track of all secret information

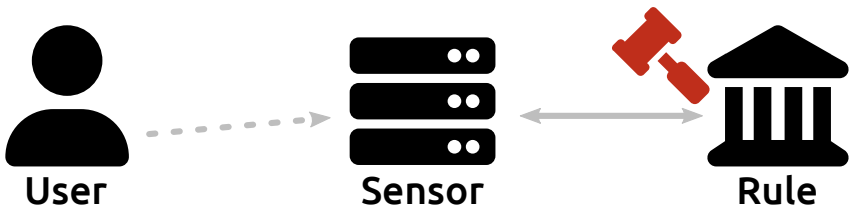


Sensors

- **Non-interactive sensors**
  - Data is simply stored
  - The system keeps track of all secret information

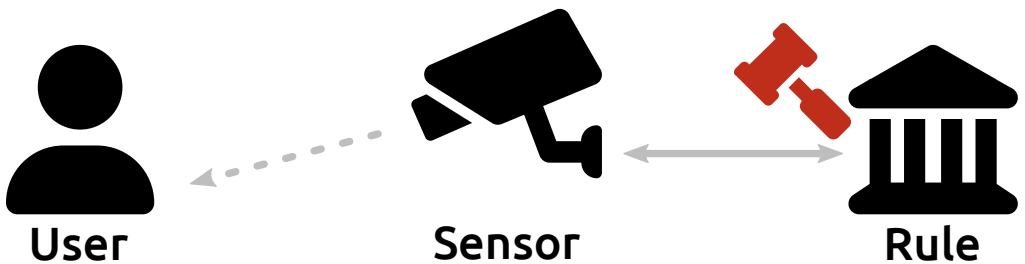


- **Interactive sensors**
  - User interacts with sensors
  - The user keeps track of some secret information



Rules

- **Threshold rules**: at most k times
- **Predicate rules**: e.g. $P \wedge Q$
- **Decision rules**: human decisions
- **Complex rules**: e.g. using graphs
- **Fuzzy rules**: e.g. using machine learning



Overview

Distributed Encryption

n-times Anonymous Credentials

Voting Protocol

Group Signatures with Distributed Management

Blacklistable Anonymous Credentials

Conclusion

Overview

Distributed Encryption

n-times Anonymous Credentials

Voting Protocol

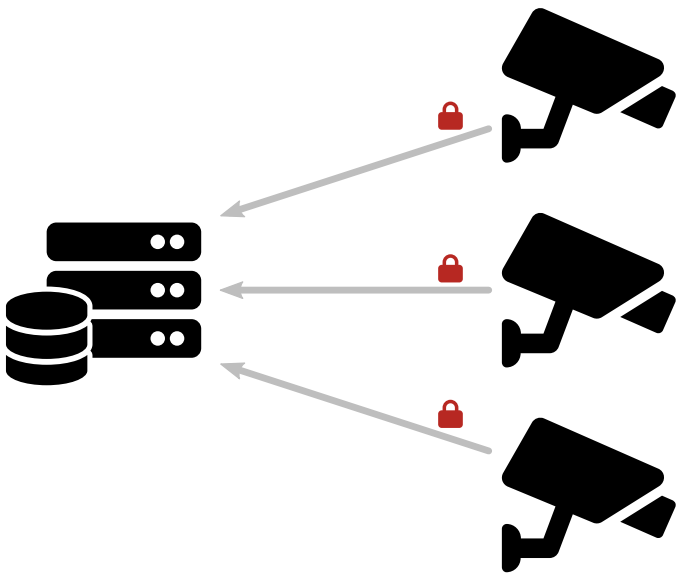
Group Signatures with Distributed Management

Blacklistable Anonymous Credentials

Conclusion

Distributed Encryption

- Sensor $\rightarrow$ Sender
- Guarantees security as long as not too many sensors are corrupted
- **Rule** $\rightarrow$ Threshold Rule
- Distributed Encryption counts the number of events
- Non-Interactive Sensors



Canvas Cutter

Use case	Sensor Type	Technique
Canvas cutters	Non-interactive	*Key-evolving Distributed encryption* [5]

- Parking places alongside highway
- Number plate recognition
- Distributed Encryption?

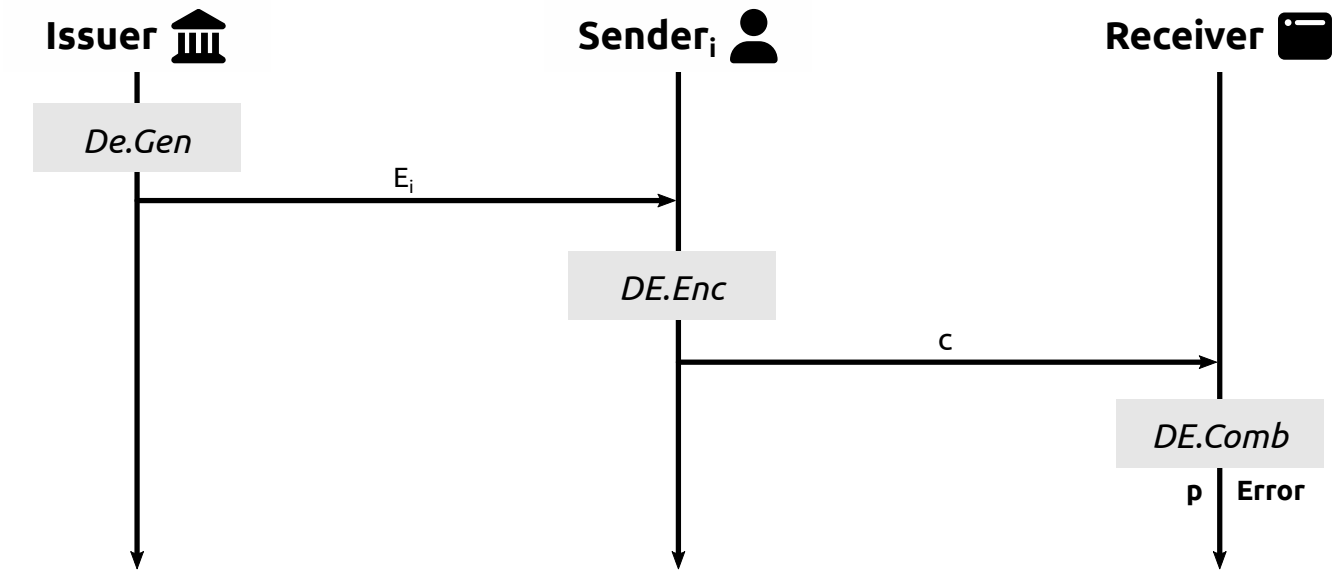
Canvas Cutter

Use case	Sensor Type	Technique
Canvas cutters	Non-interactive	*Key-evolving Distributed encryption* [5]

- Parking places alongside highway
- Number plate recognition
- Forward Secure Distributed Encryption
- Distributed Encryption inefficient

Distributed Encryption

- Share: Encrypted Encoded plaintext
- Generator $= Gen(1^l, k, n, l_p)$
- Encryption $= Enc(E_i, p)$
- Combiner $= Comb(C)$, where $C = \{c_1, .., c_k\}$

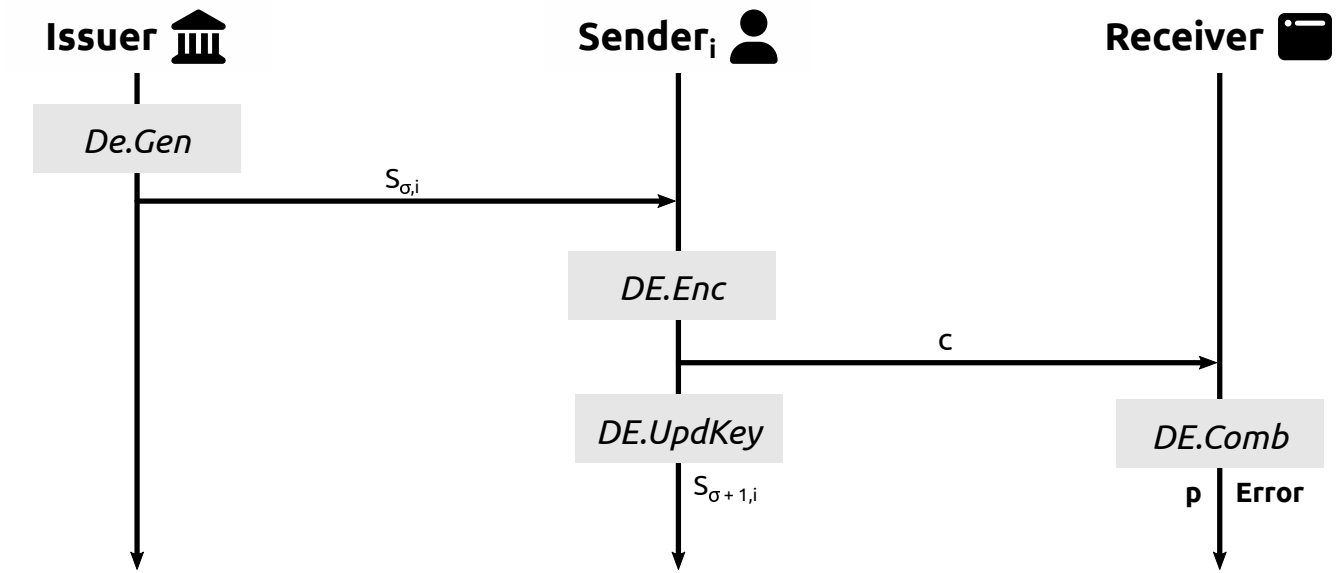


Forward Security

- Divided into epochs
- Independently updated keys
- Keys should be irrecoverably deleted

Forward Secure Distributed Encryption

- KDE (Key-evolving Distributed Encryption)
- Generator $= Gen(1^l, k, n, \boldsymbol{s}, l_p)$
- **Key Update $= \boldsymbol{UpdKey}(\boldsymbol{S_{\sigma-1,i}})$**
- Encryption $= Enc(S_{\sigma,i}, p)$
- Combiner $= Comb(C)$, where $C = \{c_1, .., c_k\}$



Canvas Cutter - Problems

- Efficiency
- What is the main problem in the combiner?

Canvas Cutter - Problems

- Efficiency
- What is the main problem in the combiner?
- It has to try all share combinations!
- So how could we fix this?

Canvas Cutter - Problems

- Efficiency
- What is the main problem in the combiner?
- It has to try all share combinations!
- So how could we fix this?
- Batched Key-evolution Distributed Encryption (BKDE)

Canvas Cutter - Problems

- Efficiency
- What is the main problem in the combiner?
- It has to try all share combinations!
- So how could we fix this?
- Batched Key-evolution Distributed Encryption (BKDE)

I Lied

Use case	Sensor Type	Technique
Canvas cutters	Non-interactive	*BKDE* [5]

Batched KDE

- Generator $= Gen(1^l, k, n, s, \mathcal{P})$
- Key Update $= UpdKey(S_{\sigma,i})$
- Encryption $= Enc(S_{\sigma,i}, P)$
- Combiner $= Comb(C_1, \ldots, C_n)$, where $C = \{c_1, .., c_k\}$

$c_{1,1}$	$c_{2,1}$	$c_{3,1}$	$c_{4,1}$	$c_{5,1}$	$c_{6,1}$
$c_{1,2}$	$c_{2,2}$	$c_{3,2}$	$c_{4,2}$	$c_{5,2}$	$c_{6,2}$
			$\vdots$		
$c_{1,p}$	$c_{2,p}$	$c_{3,p}$	$c_{4,p}$	$c_{5,p}$	$c_{6,p}$

Batched KDE

- More efficient for small-plaintexts
- Storage and time is linear to the number of plaintexts
- Generates a share for every plaintext
- We now try combinations of sensors instead of ciphertexts

Overview

Distributed Encryption

n-times Anonymous Credentials

Voting Protocol

Group Signatures with Distributed Management

Blacklistable Anonymous Credentials

Conclusion

Electronic currencies

What security/privacy properties do we want for electronic currencies?

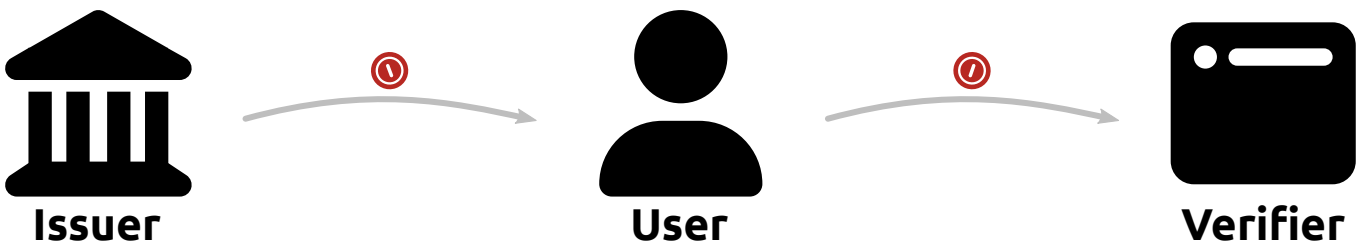
Electronic currencies

What security/privacy properties do we want for electronic currencies?

- **Soundness**: do not accept the same token multiple times
- **Anonymity**: users playing by the rules remain anonymous
- **Identification**: cheaters can be identified

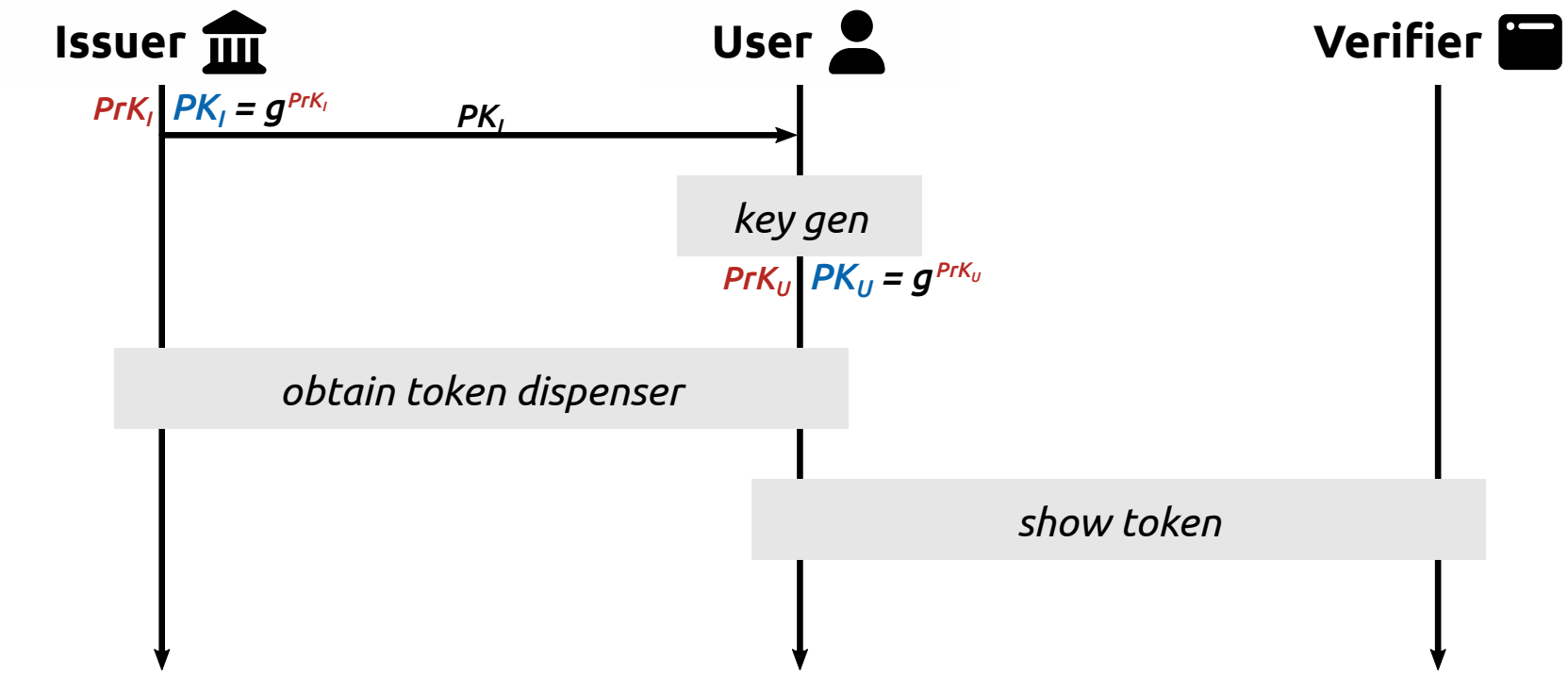
Electronic currencies

Use case	Sensor Type	Technique
Electronic currencies	Interactive	*n-times Anonymous Credentials* [1]



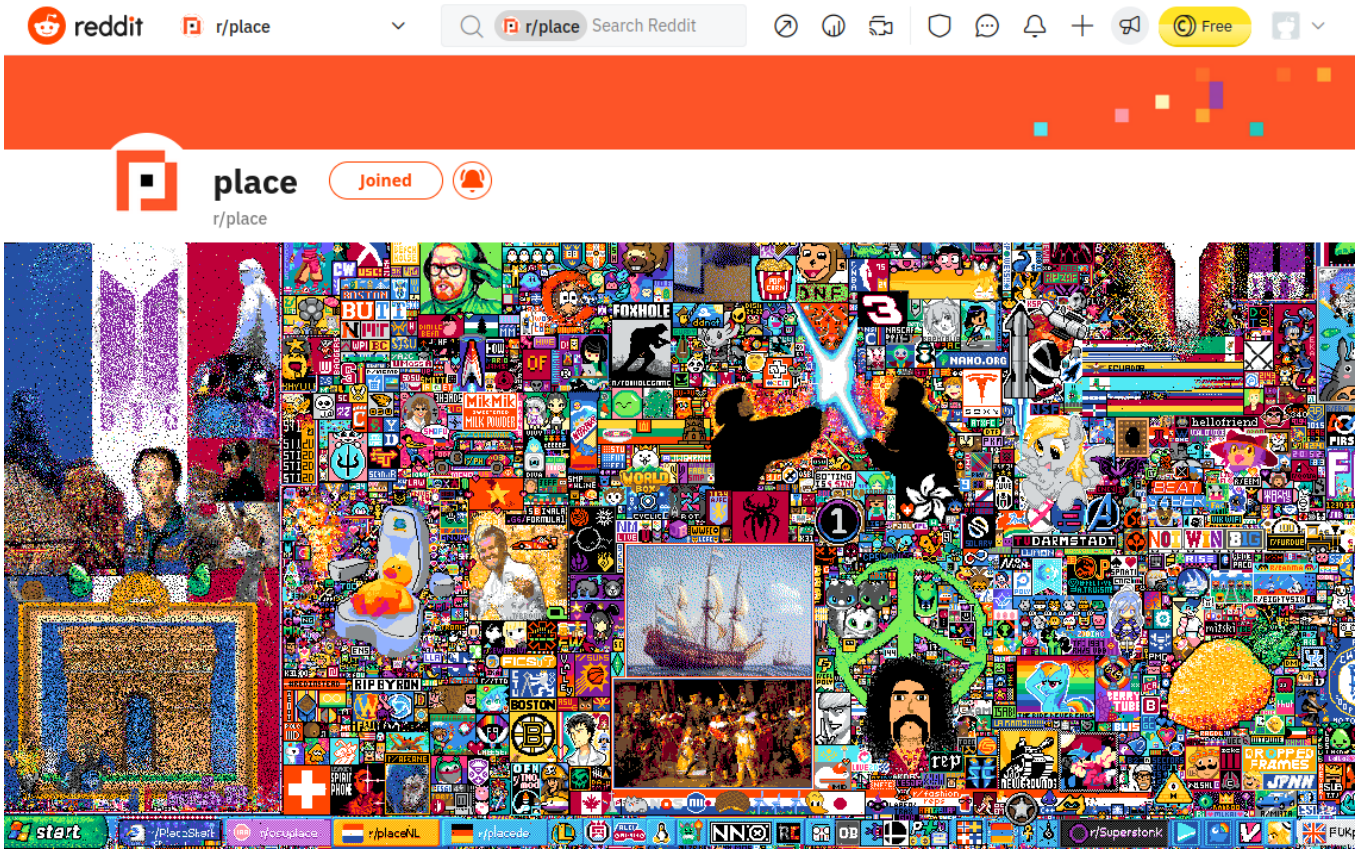
n-times Anonymous Credentials

- **Threshold rule**: a user can use a token at most once
- **Consequence**: verifier learns identity of user



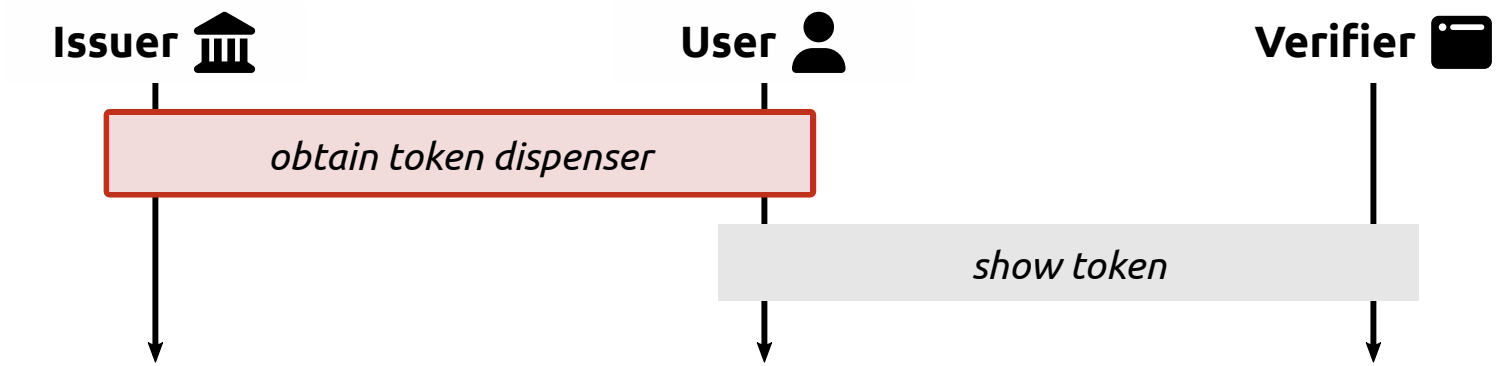
Not just for electronic currencies

- *Authorization tokens*



Obtaining token dispensers

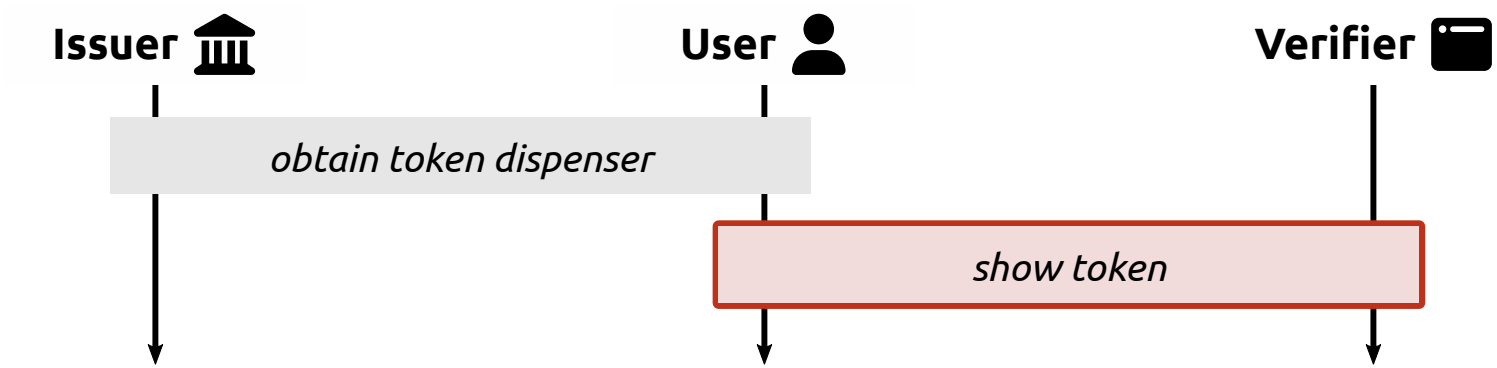
1. **Issuer** and **User** agree on random seed s
2. **Issuer** signs (PrK_U, s): $\sigma = CLsign_{PrK_I}(PrK_U, s)$
3. **User** initializes time period $T := 1$ and used token count $J := 0$
4. **User** saves dispenser $D := (PrK_U, s, \sigma, T, J)$



Showing/verifying tokens

1. **Verifier** sends random value R to **User**
2. **User** sends *token serial number* S and *double spending tag* E to V:

$$S = f_s(0, T, J) \qquad E = PK_U \cdot f_s(1, T, J)^R$$



Showing/verifying tokens

1. **Verifier** sends random value R to **User**
2. **User** sends *token serial number* S and *double spending tag* E to V:

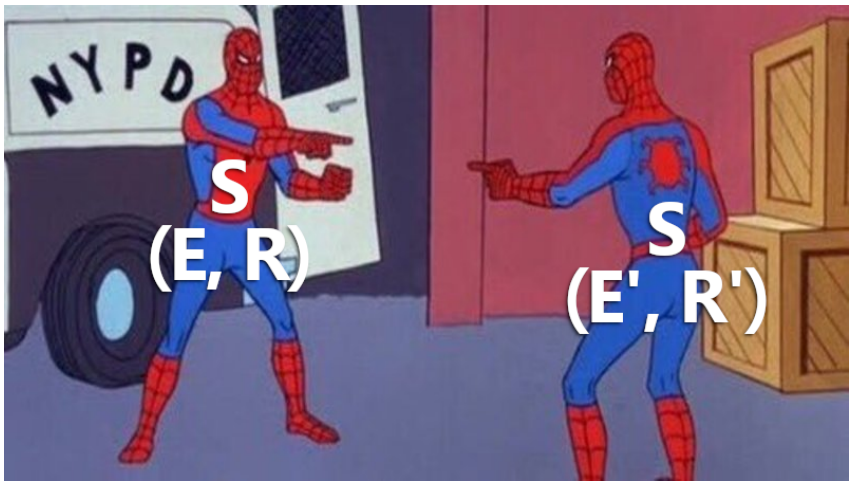
$$S = f_s(0, T, J) \qquad E = PK_U \cdot f_s(1, T, J)^R$$

3. **User** participates in *zero-knowledge proof* of knowledge of:
   - PrK_U matching PK_U
   - Seed s, with valid CL signature σ
   - S and E with $0 \leq J < n$ and current T
4. **Verifier** stores $(S, (E, R))$, **User** increments used token count J

User identification after token reuse

Two tokens with the same serial: $(S, (E, R))$ and $(S, (E', R'))$

Serial Number	Double Spending Tag	Random Nonce
$S = f_s(0, T, J)$	$E = PK_U \cdot f_s(1, T, J)^R$	R
$S = f_s(0, T, J)$	$E' = PK_U \cdot f_s(1, T, J)^{R'}$	R'



User identification after token reuse

Two tokens with the same serial: $(S, (E, R))$ and $(S, (E', R'))$

Serial Number	Double Spending Tag	Random Nonce
$S = f_s(0, T, J)$	$E = PK_U \cdot f_s(1, T, J)^R$	R
$S = f_s(0, T, J)$	$E' = PK_U \cdot f_s(1, T, J)^{R'}$	R'

Verifier can compute:

- $\sqrt[R-R']{\frac{E}{E'}} = \sqrt[R-R']{\frac{PK_U \cdot f_s(1,T,J)^R}{PK_U \cdot f_s(1,T,J)^{R'}}} = \sqrt[R-R']{f_s(1, T, J)^{R-R'}} = f_s(1, T, J)$
- $\frac{E}{f_s(1,T,J)^R} = \frac{PK_U \cdot f_s(1,T,J)^R}{f_s(1,T,J)^R} = PK_U$

User identification after token reuse

Two tokens with the same serial: $(S, (E, R))$ and $(S, (E', R'))$

Serial Number	Double Spending Tag	Random Nonce
$S = f_s(0, T, J)$	$E = PK_U \cdot f_s(1, T, J)^R$	R
$S = f_s(0, T, J)$	$E' = PK_U \cdot f_s(1, T, J)^{R'}$	R'

Verifier can compute:

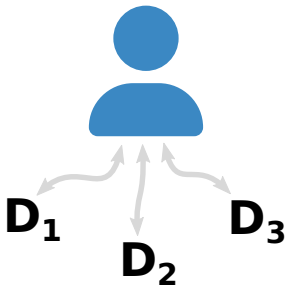
- $\sqrt[R-R']{\frac{E}{E'}} = \sqrt[R-R']{\frac{PK_U \cdot f_s(1,T,J)^R}{PK_U \cdot f_s(1,T,J)^{R'}}} = \sqrt[R-R']{f_s(1, T, J)^{R-R'}} = f_s(1, T, J)$
- $\frac{E}{f_s(1,T,J)^R} = \frac{PK_U \cdot f_s(1,T,J)^R}{f_s(1,T,J)^R} = PK_U$

Verifier now knows which user misbehaved!

Extensions

Glitch protection

Weak/strong exculpability



Tracing

Dynamic revocation

Overview

Distributed Encryption

n-times Anonymous Credentials

Voting Protocol

Group Signatures with Distributed Management

Blacklistable Anonymous Credentials

Conclusion

Remote Electronic Voting

Use case	Sensor Type	Technique
Remote electronic voting	Interactive	*Custom voting protocol* [6]

Anonymous electronic voting problems

Everyone votes anonymously and stays anonymously without any linked id

- What could go wrong?

Incredibly “secure” voting

If the voter wishes to cross off the name of the candidate it must be done with a red pen next to the ballot box.

Incredibly "insecure" voting

3. Justin Bieber Almost Gets Sent to North Korea

Justin Bieber at the 2012 Jingle Ball in Atlanta. / Chris McKay/Getty Images for Jingle Ball 2012

A restriction-less 2010 poll set up by Faxo.com to pick a destination for Justin Bieber's "My World" tour saw North Korea steal the top spot, climbing from 24th to 1st in a matter of two days. Since Kim Jong-Il put the kibosh on Western music in North Korea, instituted rigid travel regulations, and made the Internet off-limits for most of the country, the result was head-scratching at best.

Votebots

About 374.000.000 results (0,35 seconds)

https://buyvotescontest.com › ...

Buy online contest votes, buy poll votes, buy contest votes ...

The best service for selling votes in contests and voting, we will win any contest for you. Buy contest votes, get votes, **buy online votes**, buy poll votes.

https://buyvotespoll.com

Buy Votes to Win Any Contest - Buy Online Poll Votes Fast

We are a specialized **online poll voting** company delivering fast & bulk **votes** for all. **online** contests from past 7 years. Get **online votes**, **buy poll votes**, ...

https://voteseller.com

Vote Seller: Buy Online Vote service in 2022

Want to win any **online** contest, Voteseller can help you, We have expertise team who can priovide faster **online vote** service in affordable price.

https://www.buyonlinecontestvotes.com

Buy Bulk Contest Votes to win Online Poll & Facebook Contest ...

Win **Online Poll** & Facebook **Voting** Contest with BOCV.With over 7 Years of experience, we are specialized in **Online Voting** & deliver fast & bulk **votes** for any ...

https://buyvotesservice.com › Blog

Buy Votes For Contest & Win Your Online Voting Contest Votes.

We, buyVotesservice, are the leading service providers for **online** contest **voting**. We use unique IP and realistic profiles to **vote** in your contest. With our ...

https://onlinepollservice.com

Buy votes for online contest

We will help you win and get the right amount of **votes** for your contest. If you **buy votes online** in our service.

Voting Protocol - Properties

Eligibility: Only eligible voters should be able to vote.

Uniqueness: Only one vote per voter should be counted.

Voting Protocol - Properties

Vote Privacy: No one should be able to link any ballot to the voter...

Voting Protocol - Properties

Vote Privacy: No one should be able to link any ballot to the voter...unless anonymity has been revoked!

Revocable Anonymity: It should be possible for an authorised entity (or collaboration of entities) to reveal the identity of any single voter by linking their vote.

Voting Protocol - Properties

Vote Privacy: No one should be able to link any ballot to the voter...unless anonymity has been revoked!

Revocable Anonymity: It should be possible for an authorised entity (or collaboration of entities) to reveal the identity of any single voter by linking their vote.

- What kind of rule?

- Threshold
- Predicate
- Decision
- Complex
- Fuzzy

Voting Protocol - Properties

"It should not be possible for a voter to prove how they voted or even if they are voting"

- Why?

Voting Protocol - Properties

"It should not be possible for a voter to prove how they voted or even if they are voting"

- Why?

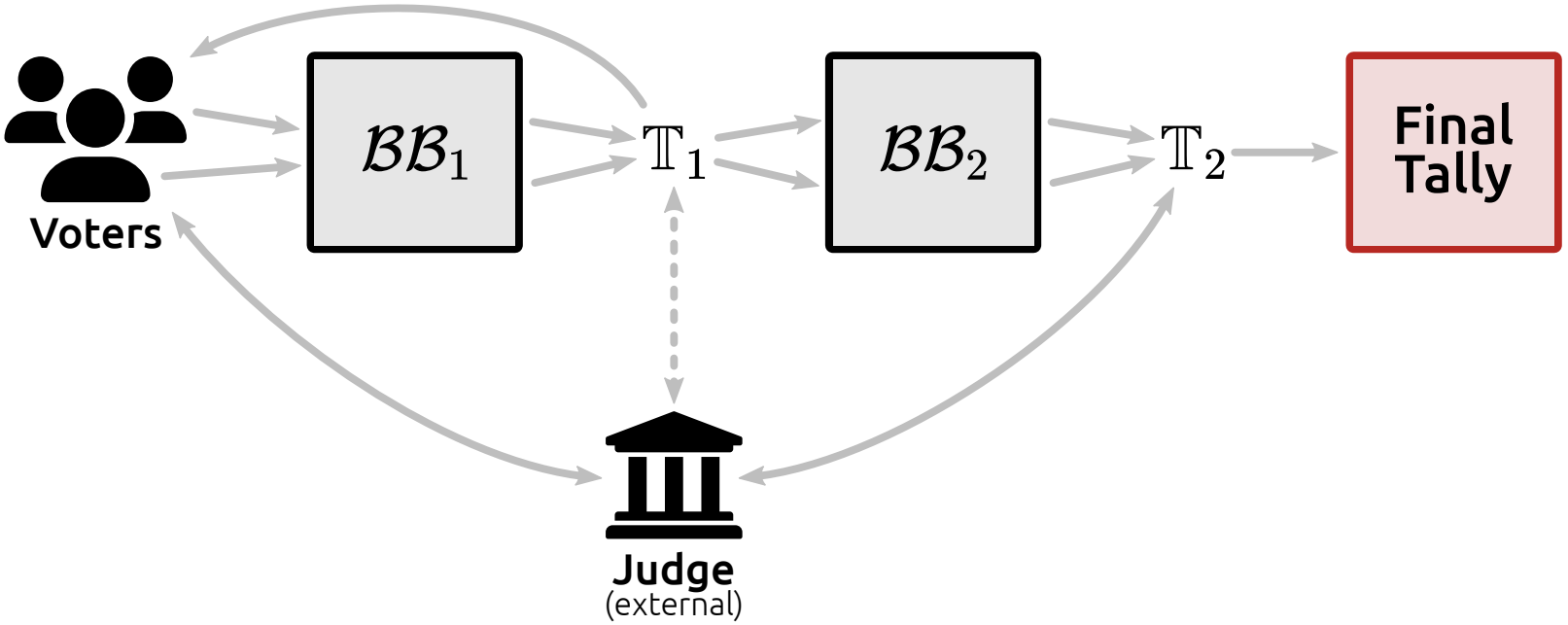
Coercion-Resistance (voter interference, bribery, vote selling)

How does it work?

A protocol consisting of four stages:

1. Ballot Validity Tokens
2. Encrypted Vote Posting
3. Validity Checking
4. Tallying

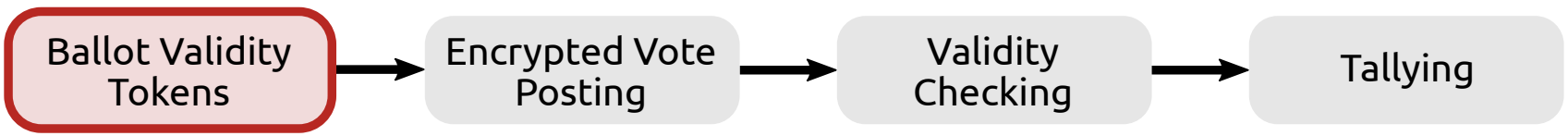
Scheme



$\mathbb{T}_1$: First-round talliers
$\mathbb{T}_2$: Second-round talliers

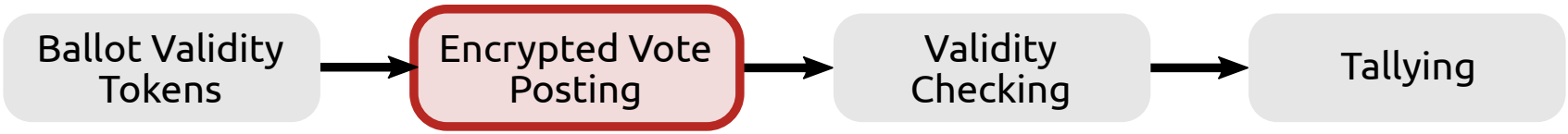
Stage 1: Ballot Validity Tokens

- The voter (Alice) registers in person with $\mathbb{T}_1$
- Alice receives:
  - a new public/private keypair
  - a random number of values δ_i with a designated verifier signature
- Only one signature is valid
- The valid δ value for Alice with her name is stored by $\mathbb{T}_1$



Stage 2: Encrypted Vote Posting

- Alice encrypts her vote v using the public key of $\mathbb{T}_2$
- She calculates the Generalised Proof of Equality of Discrete Logarithms (G-PEQDL)
- She encrypts[1] the encrypted vote, proof and her public key with the public key of $\mathbb{T}_1$ and posts it to $\mathcal{BB}_1$

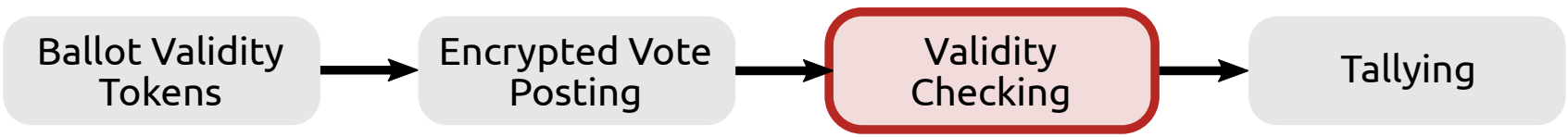


[1] Altogether the following tuple is encrypted: $\langle v_{\mathbb{T}_2}, \text{Sign}_A(\text{G-PEQDL}), \delta, \text{pub}_A \rangle$

Stage 3: Validity Checking

The first-round talliers $\mathbb{T}_1$ removes the first layer of encryption of each vote on $\mathcal{BB}_1$. The tallier then checks her vote and proof.

1. Re-encrypt $v_{\mathbb{T}_2}$ with a random factor β
2. Encrypt Alice's public key using the joint public key for both sets of talliers $\text{pub}_{\mathbb{T}}$ and the Judge's public key $\text{pub}_{\mathbb{J}}$
3. Generate a hash and post to $\mathcal{BB}_2$

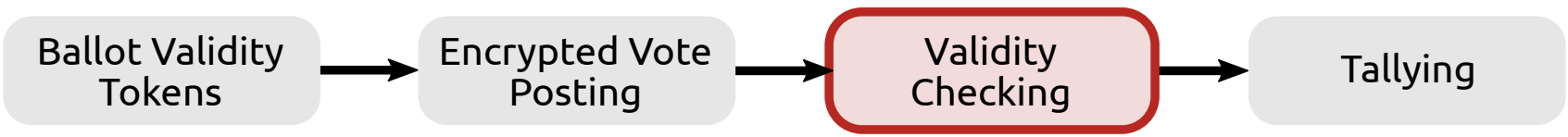


Stage 3: Validity Checking

The first-round talliers $\mathbb{T}_1$ removes the first layer of encryption of each vote on $\mathcal{BB}_1$. The tallier then checks her vote and proof.

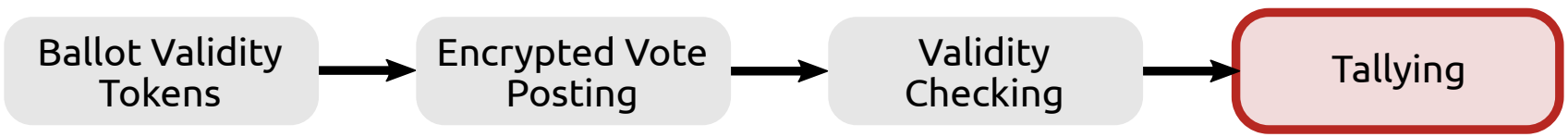
1. Re-encrypt $v_{\mathbb{T}_2}$ with a random factor β
2. Encrypt Alice's public key using the joint public key for both sets of talliers $\text{pub}_{\mathbb{T}}$ and the Judge's public key $\text{pub}_{\mathbb{J}}$
3. Generate a hash and post to $\mathcal{BB}_2$

$\mathbb{T}_1$ cannot see Alice's vote!



Stage 4: Tallying

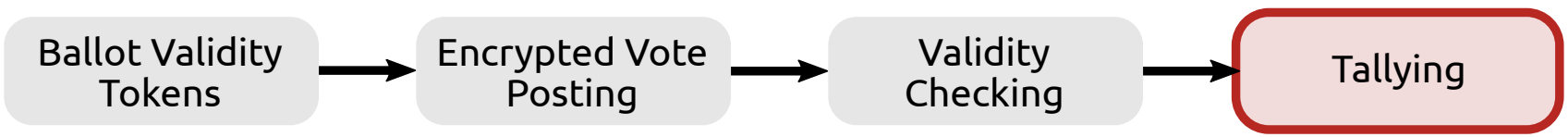
The second-round talliers $\mathbb{T}_2$ can now check if the votes are valid by checking the hash.
A quorum of talliers jointly decrypt a product of the votes giving the resulting tally.



Stage 4: Tallying

The second-round talliers $\mathbb{T}_2$ can now check if the votes are valid by checking the hash.
A quorum of talliers jointly decrypt a product of the votes giving the resulting tally.

Anonymity Revocation
A quorum of members of the anonymity tallier group $\mathbb{T}$ need to collude to get $\text{pub}_{\mathbb{J}}(\text{pub}_A)$. The Judge can then get the voter's identity pub_A.



Overview

Distributed Encryption

n-times Anonymous Credentials

Voting Protocol

Group Signatures with Distributed Management

Blacklistable Anonymous Credentials

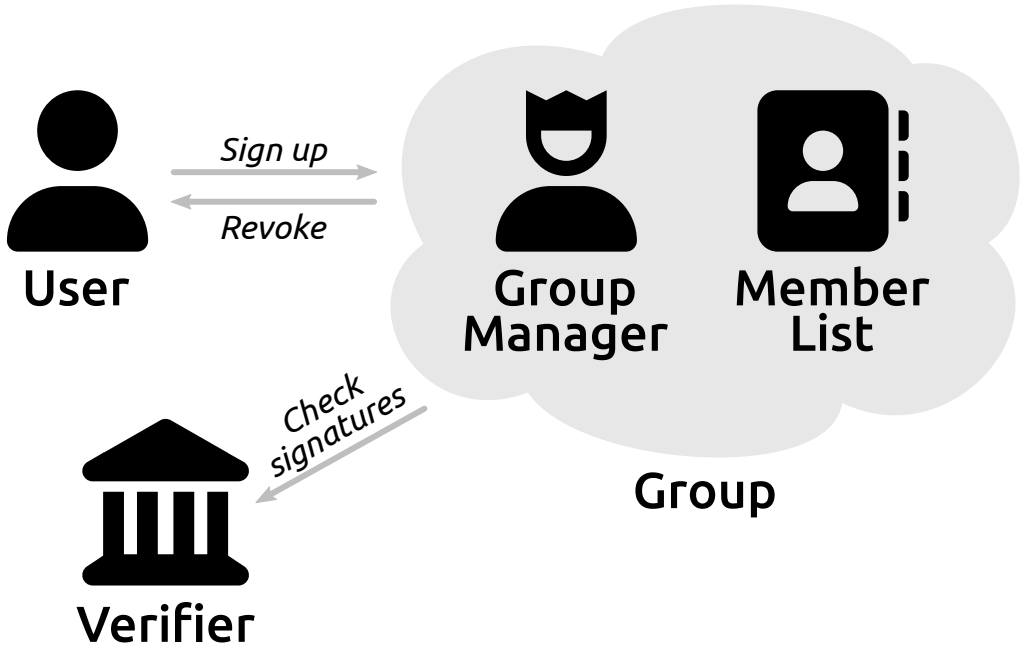
Conclusion

Group Signatures

- Group member signs message for the whole group
- Anonymity for members
- Signature can be verified

Group Signatures with Distributed Management

- Only members of the group can sign messages
- Receiver can verify that it is a valid group signature, but cannot discover which group member made it
- If necessary, the person who signed the message is revealed to all



Why use this?

- Multiple tracking agents
  - Need for t moderators for revealing an identity
  - Not ONE trusted third party
- Members who follow the rules remain anonymous

Should we use interactive or non-interactive sensors?

Why use this?

- Multiple tracking agents
  - Need for t moderators for revealing an identity
  - Not ONE trusted third party
- Members who follow the rules remain anonymous

Should we use interactive or non-interactive sensors?

What kind of rule could this be?

- Threshold
- Predicate
- Decision
- Complex
- Fuzzy

What could we use this for?

What could we use this for?

Deanonymizing comments

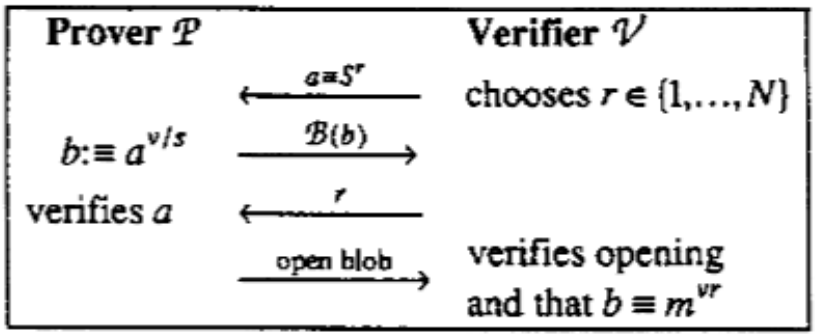
What could go wrong?

What could go wrong?

- Good moderation is necessary
- The group needs to agree on what behavior is unacceptable

Group Signature Protocols

- Most use RSA
- Undeniable signatures
- Configuration is generally linear with the nr. of group members
- Group manager



Deanonymizing comments

Use case	Sensor Type	Technique
Deanonymizing comments	Interactive or Non-interactive	*Group Signatures with Distributed Management* [2]

Overview

Distributed Encryption

n-times Anonymous Credentials

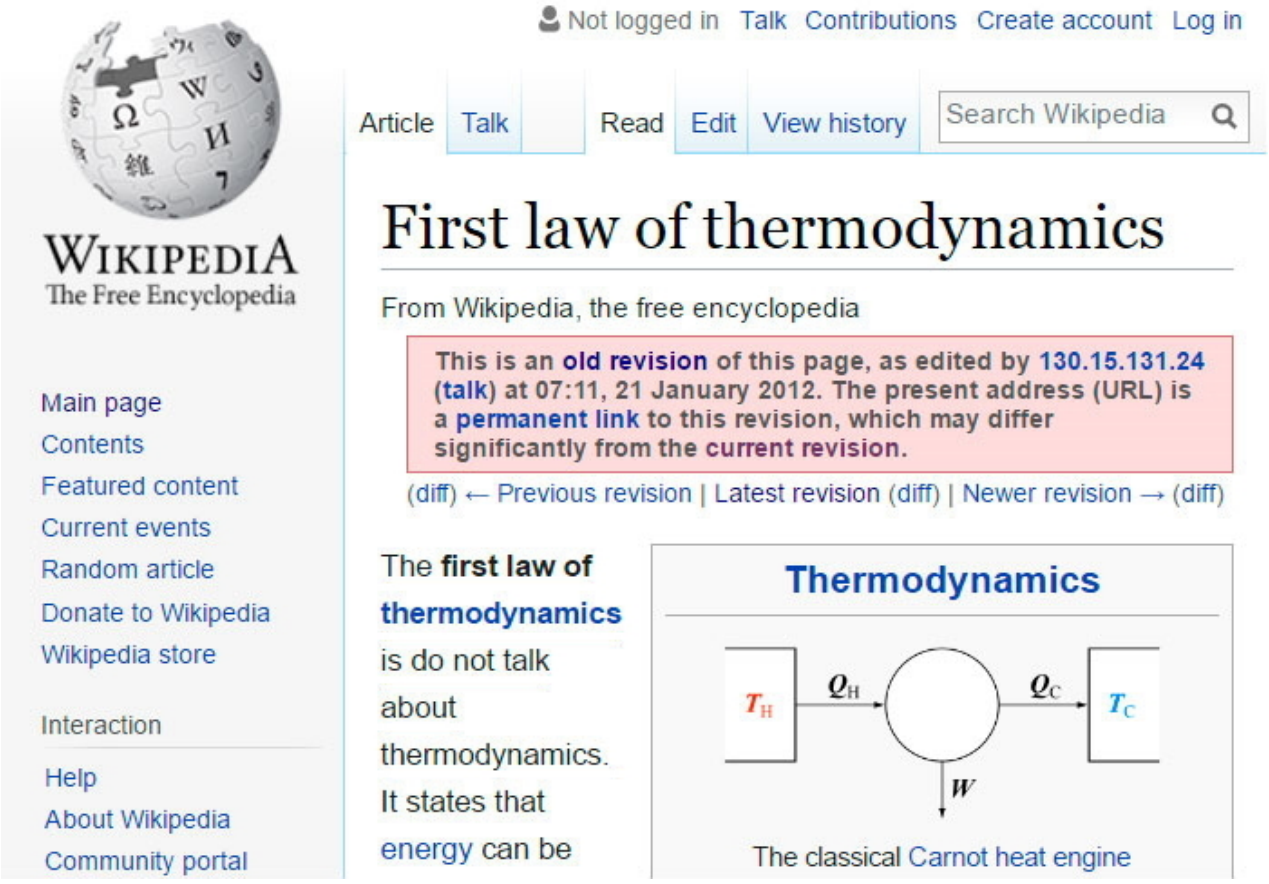
Voting Protocol

Group Signatures with Distributed Management

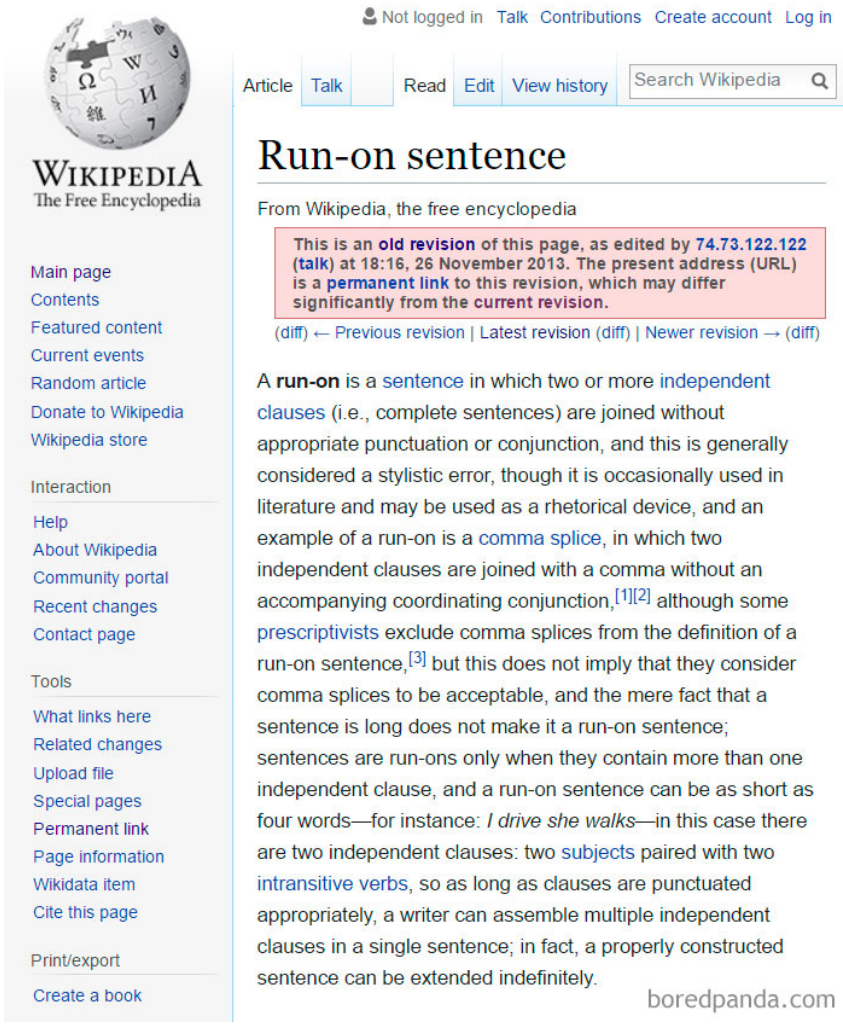
Blacklistable Anonymous Credentials

Conclusion

Blocking anonymous editing: Example 1



Example 2



Not logged in Talk Contributions Create account Log in

Article Talk Read Edit View history Search Wikipedia

WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools
What links here
Related changes
Upload file
Special pages
Permanent link
Page information
Wikidata item
Cite this page

Print/export
Create a book

Run-on sentence

From Wikipedia, the free encyclopedia

This is an old revision of this page, as edited by 74.73.122.122 (talk) at 18:16, 26 November 2013. The present address (URL) is a permanent link to this revision, which may differ significantly from the current revision.

(diff) ← Previous revision | Latest revision (diff) | Newer revision → (diff)

A **run-on** is a sentence in which two or more independent clauses (i.e., complete sentences) are joined without appropriate punctuation or conjunction, and this is generally considered a stylistic error, though it is occasionally used in literature and may be used as a rhetorical device, and an example of a run-on is a comma splice, in which two independent clauses are joined with a comma without an accompanying coordinating conjunction,[1][2] although some prescriptivists exclude comma splices from the definition of a run-on sentence,[3] but this does not imply that they consider comma splices to be acceptable, and the mere fact that a sentence is long does not make it a run-on sentence; sentences are run-ons only when they contain more than one independent clause, and a run-on sentence can be as short as four words—for instance: *I drive she walks*—in this case there are two independent clauses: two subjects paired with two intransitive verbs, so as long as clauses are punctuated appropriately, a writer can assemble multiple independent clauses in a single sentence; in fact, a properly constructed sentence can be extended indefinitely.

boredpanda.com

Example 3

Not logged in Talk Contributions Create account Log in

Article Talk Read View source More Search Wikipedia

WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools
What links here
Related changes
Upload file

List of serial killers by number of victims

From Wikipedia, the free encyclopedia

This is an old revision of this page, as edited by 88.236.55.132 (talk) at 15:50, 7 December 2012. The present address (URL) is a permanent link to this revision, which may differ significantly from the current revision.

(diff) ← Previous revision | Latest revision (diff) | Newer revision → (diff)

This list is incomplete; you can help by expanding it.Please do not expand the list by killing people.

A serial killer is a person who murders two or more people, in two or more separate events over a period of time, for primarily psychological reasons.[1] There are gaps of time between the killings, which may range from a few hours to many years. This list shows serial killers from the 20th century to present day by number of victims (list of serial killers by victim before 1900). In many cases, the exact number of victims assigned to a serial killer is not known, and even if that person is convicted of a few, there can be the possibility that he/she killed many more.

boredpanda.com

Example 4

Niet aangemeld Overleg Bijdragen Account aanmaken Inloggen

WIKIPEDIA
De vrije encyclopedie

Artikel Overleg | Lezen Bewerken Brontekst bewerken Geschiedenis | Doorzoek Wikipedia

Hoofdpagina
Vind een artikel
Vandaag
Etalage
Categorieën
Recente wijzigingen
Nieuwe artikelen
Willekeurige pagina

Informatie
Gebruikersportaal
Snelcursus
Hulp en contact
Doneren

Hulpmiddelen
Links naar deze pagina
Gerelateerde wijzigingen
Bestand uploaden
Speciale pagina's
Permanente koppeling
Paginagegevens
Deze pagina citeren
Wikidata-item

Afdrukken/exporteren
Boek aanmaken

Kevin Bacon

Kevin Norwood Bacon (Philadelphia (Pennsylvania), 8 juli 1958) is een Amerikaans filmacteur. Hij won een Golden Globe voor zijn rol in *Taking Chance*. Verder won hij meer dan 15 andere acteerprijzen, waaronder een Blockbuster Entertainment Award voor *Hollow Man*.

Bacon kreeg in 2003 een ster op de Hollywood Walk of Fame.

Inhoud [verbergen]
1 Biografie
2 Films
3 Bacongetal
4 Trivia
5 Externe link

Biografie [bewerken | brontekst bewerken]

Bacon maakte zijn filmdebuut in *Animal House* van John Landis, waarin hij Chip Diller speelde.

Hij trouwde in 1988 met actrice Kyra Sedgwick, die hij op de set van *Lemon Sky* ontmoette. Samen kregen ze in 1989 zoon Travis en in 1992 dochter Sosie Ruth. Naast het acteren speelt Bacon samen met zijn broer Michael in de band *Bacon Brothers*, die verschillende albums uitbracht.

Films [bewerken | brontekst bewerken]

Filmografie als acteur

Jaar	Titel	Rol	Opmerkingen
1978	*Animal House*	Chip Diller	
1979	*Starting Over*	Man (jong stel)	
1979	*The Gift*	Teddy	Televisiefilm

Kevin Bacon

Kevin Bacon in 2014

Algemene informatie	
Volledige naam	Kevin Norwood Bacon
Geboren	Philadelphia, 8 juli 1958
Land	Verenigde Staten
Werk	
Pseudoniem	The Bacon Brothers, Kevin Bacon III
Jaren actief	1978-
Beroep	Acteur

What do we want?

What do we want?

Revoke rights with Anonymity

Solutions?

- Trusted Third Parties?

TTPs

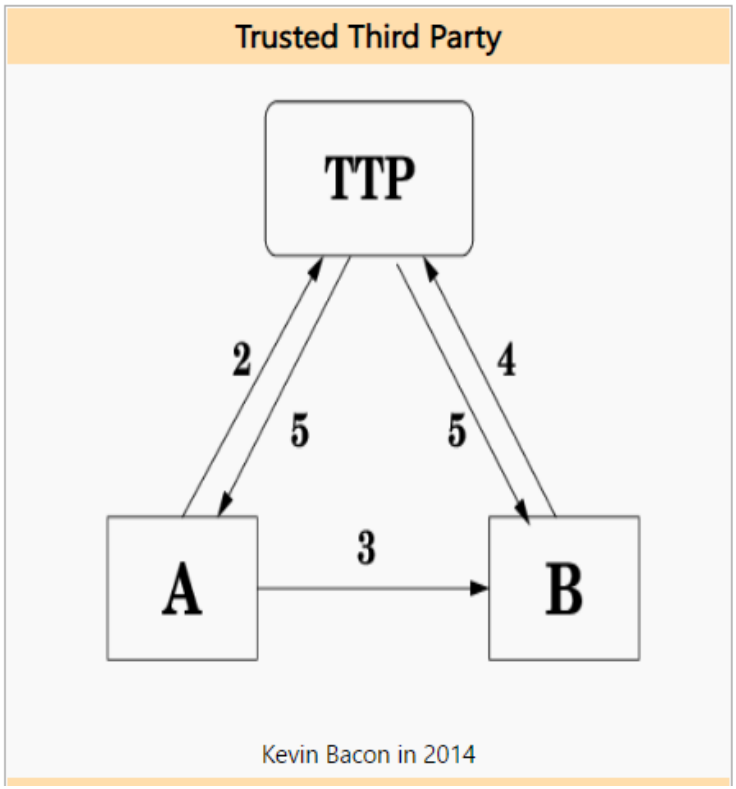
Neither A or B know who each other are.

Kevin Bacon

Kevin Norwood Bacon (Philadelphia (Pennsylvania), 8 juli 1958) is een Amerikaans filmacteur. Hij won een Golden Globe voor zijn rol in *Taking Chance*. Verder won hij meer dan 15 andere acteerprijzen, waaronder een Blockbuster Entertainment Award voor *Hollow Man*.

Bacon kreeg in 2003 een ster op de Hollywood Walk of Fame.

Inhoud [verbergen]



NO!!

TRUSTED Third Parties.
Relies on TRUSTing a third party

$\Rightarrow$ *they CAN deanonymize the users*

$\Rightarrow$ *they CAN abuse your trust*

Solutions?

- Trusted Third Parties?
- Distributed encryption?

Example 5: Non-interactive?

UFC 133

From Wikipedia, the free encyclopedia

UFC 133 is an upcoming mixed martial arts event to be held by the Ultimate Fighting Cha expected to take place on August 6, 2011 at the Wells Fargo Center in Philadelphia, Pen

On April 5, 2011 it was revealed that this event would be a landmark in MMA history, host to host seven main card bouts as opposed to the usual five.

Bouts in the works include:

- Heavyweight bout: Optimus Prime vs. Megatron
- Light Heavyweight bout: He-Man vs. Skeletor
- Middleweight bout: Wolverine vs. Magneto
- Welterweight bout: Spider-Man vs. Green Goblin
- Lightweight bout: Mario vs. Wario
- Featherweight bout: Ash Ketchum vs. Gary Oak
- Bantamweight bout: Bugs Bunny vs. Elmer Fudd

Solutions?

- Trusted Third Parties?
- Distributed encryption?
  $\rightarrow$ *Must be interactive*

Solutions?

- Trusted Third Parties?
- Distributed encryption?
- n-times anonymous credentials?

Example 5: What's the threshold?

UFC 133

From Wikipedia, the free encyclopedia

UFC 133 is an upcoming mixed martial arts event to be held by the Ultimate Fighting Cha expected to take place on August 6, 2011 at the Wells Fargo Center in Philadelphia, Pen

On April 5, 2011 it was revealed that this event would be a landmark in MMA history, host to host seven main card bouts as opposed to the usual five.

Bouts in the works include:

- Heavyweight bout: Optimus Prime vs. Megatron
- Light Heavyweight bout: He-Man vs. Skeletor
- Middleweight bout: Wolverine vs. Magneto
- Welterweight bout: Spider-Man vs. Green Goblin
- Lightweight bout: Mario vs. Wario
- Featherweight bout: Ash Ketchum vs. Gary Oak
- Bantamweight bout: Bugs Bunny vs. Elmer Fudd

Solutions?

- Trusted Third Parties?
- Distributed encryption?
- n-times anonymous credentials?
  $\rightarrow$ *No objective threshold*

Solutions?

- Trusted Third Parties?
- Distributed encryption?
- n-times anonymous credentials?
- Custom voting protocol?

Solutions?

- Trusted Third Parties?
- Distributed encryption?
- n-times anonymous credentials?
- Custom voting protocol?
- Group signatures?

Solutions?

- Trusted Third Parties?
- Distributed encryption?
- n-times anonymous credentials?
- Custom voting protocol?
- Group signatures?

→ *If necessary, the person who signed the message is revealed to all*

Solutions?

- Trusted Third Parties?
- Distributed encryption?
- n-times anonymous credentials?
- Custom voting protocol?
- Group signatures?
- BLAC?

Recap: What do we want?

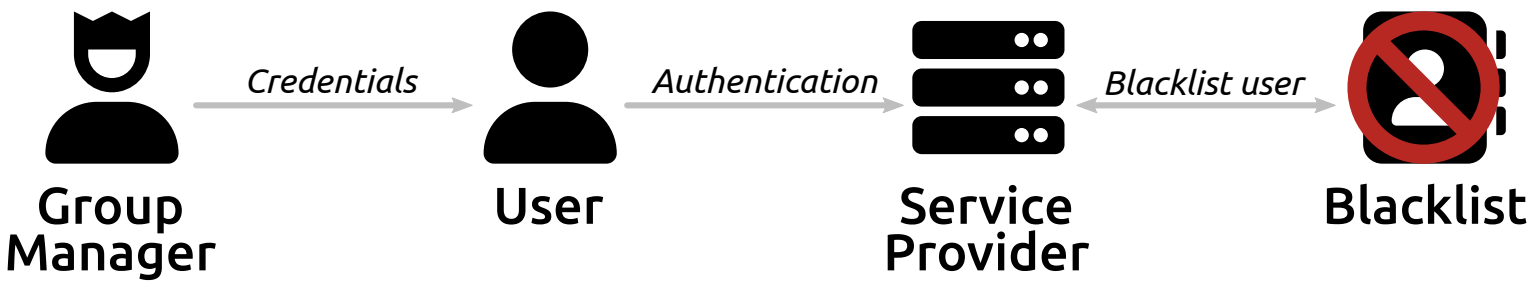
- Preserve anonymity
- interactive
- Decision rules
- Wikipedia decides
- No TTPs!!! (not enough anonymity)

BLAC is the new Black

- **BL**acklistable
- **A**nonymous
- **C**redentials

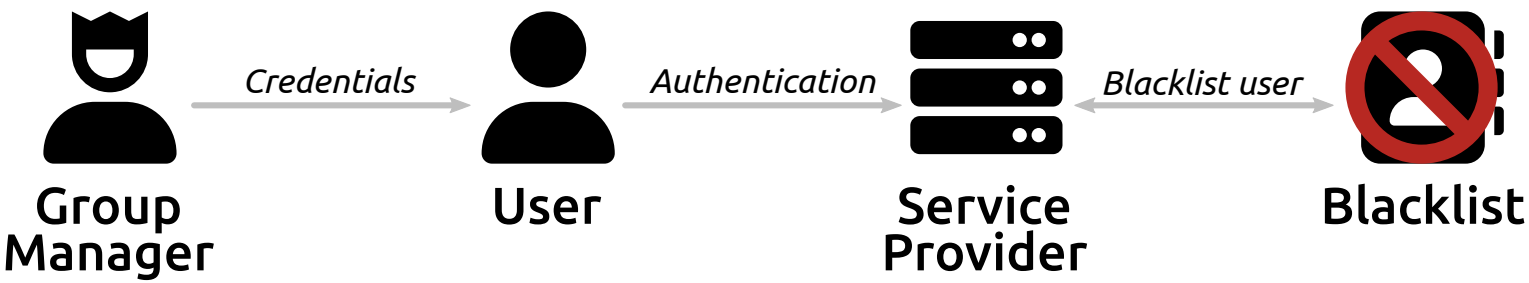
BLAC model

1. Setup
2. Registration
3. Authentication
4. Blacklist Management



BLAC model

- Group Manager $\neq$ TTP. only enrolls
- Service Provider does blacklisting
- No one ever learns user info
- Store tickets



Security Notions

- Mis-authentication Resistance
- Blacklistability
- Anonymity
- Non-frameability

What do we want?

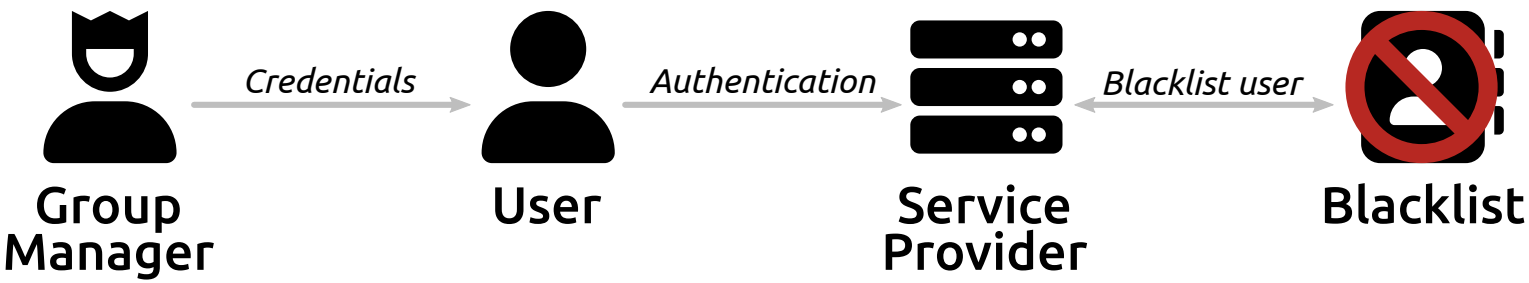
- Preserves anonymity ✓
- interactive ✓
- Wikipedia decides ✓
- Subjective thresholds ✓
- No TTPs!!! (not enough anonymity) ✓

Example of how it works

Nagasaki

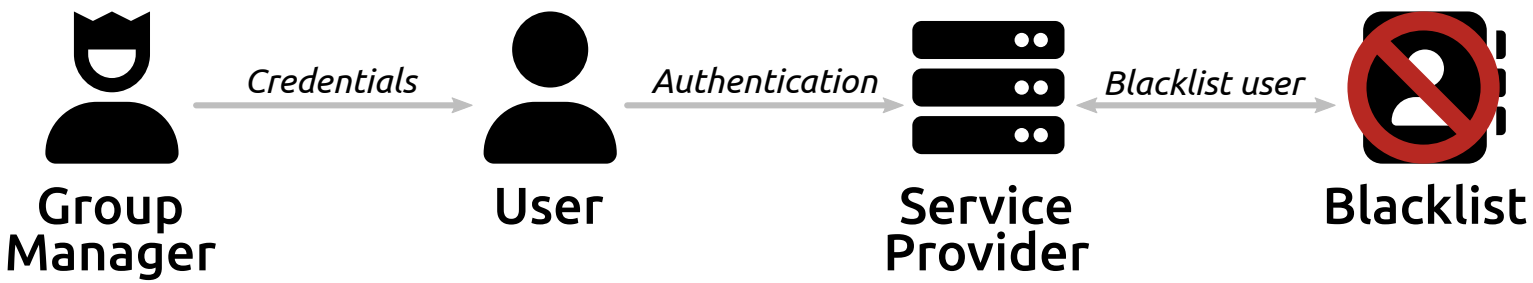
From Wikipedia, the free encyclopedia

Nagasaki (Japanese: 長崎, "Long Cape") is a Japanese port city that was founded by the Portuguese in the late 16th century and unfounded by the United States on August 9, 1945.



Blocking anonymous editing

Use case	Sensor Type	Technique
Blocking anonymous editing	Interactive	*Blacklistable Anonymous Credentials* [7]



Overview

Distributed Encryption

n-times Anonymous Credentials

Voting Protocol

Group Signatures with Distributed Management

Blacklistable Anonymous Credentials

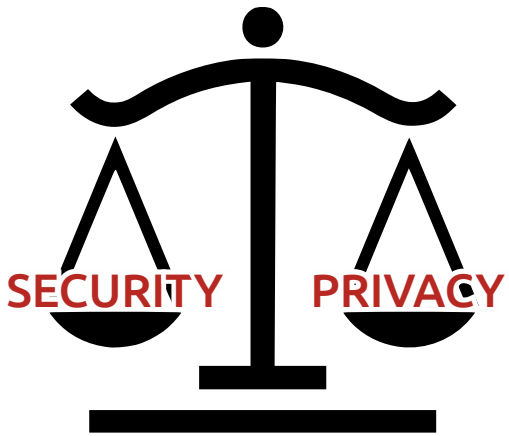
Conclusion

Summary

Use case	Sensor Type	Technique
Canvas cutters	Non-interactive	*Distributed encryption* [3]
Electronic currencies	Interactive	*n-times Anonymous Credentials* [1]
Electronic voting	Interactive	*Custom voting protocol* [6]
Deanonymizing comments	Interactive or Non-interactive	*Group Signatures with Distributed Management* [2]
Blocking anonymous editing	Interactive	*Blacklistable Anonymous Credentials* [7]

Conclusion

- Security **AND** Privacy
- However, not all complex rules have existing techniques
- There is still a lot to be done in regards to Revocable Privacy



Disclaimer

No wikipedia pages were harmed during the making of this presentation.

Thanks for your attention!

- Any questions?

References I

[1] Jan Camenisch et al. 'How to Win the Clonewars: Efficient Periodic n-Times Anonymous Authentication'. In: CCS '06. Alexandria, Virginia, USA: Association for Computing Machinery, Jan. 2006, pp. 201–210. ISBN: 1595935185. DOI: 10.1145/1180405.1180431.

[2] David Chaum and Eugène van Heyst. 'Group signatures'. In: *Workshop on the Theory and Application of of Cryptographic Techniques*. Springer. 1991, pp. 257–265.

[3] Jaap-Henk Hoepman and David Galindo. 'Non-interactive distributed encryption: a new primitive for revocable privacy'. In: *Proceedings of the 10th annual ACM workshop on Privacy in the electronic society*. 2011, pp. 81–92.

References II

[4] Wouter Lueks, Maarten H. Everts and Jaap-Henk Hoepman. 'Revocable Privacy: Principles, Use Cases, and Technologies'. In: *Privacy Technologies and Policy*. Ed. by Bettina Berendt et al. Cham: Springer International Publishing, 2016, pp. 124–143. ISBN: 978-3-319-31456-3.

[5] Wouter Lueks, Jaap-Henk Hoepman and Klaus Kursawe. 'Forward-Secure Distributed Encryption'. In: *Privacy Enhancing Technologies*. Ed. by Emiliano De Cristofaro and Steven J. Murdoch. Cham: Springer International Publishing, 2014, pp. 123–142. ISBN: 978-3-319-08506-7.

References III

[6] Matt Smart and Eike Ritter. 'Remote Electronic Voting with Revocable Anonymity'. In: *Information Systems Security*. Ed. by Atul Prakash and Indranil Sen Gupta. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 39–54. ISBN: 978-3-642-10772-6.

[7] Patrick P. Tsang et al. 'Blacklistable Anonymous Credentials: Blocking Misbehaving Users without Ttps'. In: *Proceedings of the 14th ACM Conference on Computer and Communications Security*. CCS '07. Alexandria, Virginia, USA: Association for Computing Machinery, 2007, pp. 72–81. ISBN: 9781595937032. DOI: 10.1145/1315245.1315256. URL: https://doi-org.ru.idm.oclc.org/10.1145/1315245.1315256.