Group Signatures
Concepts, Applications*, and new Advances**

Anja Lehmann

IBM Research – Zurich

*Zone Encryption with Anonymous Authentication for V2V Communication.
J Camenisch, M Drijver, A Lehmann, G Neven, P Towa

**Group Signatures with Selective Linkability. PKC 2019
L Garms, A Lehmann

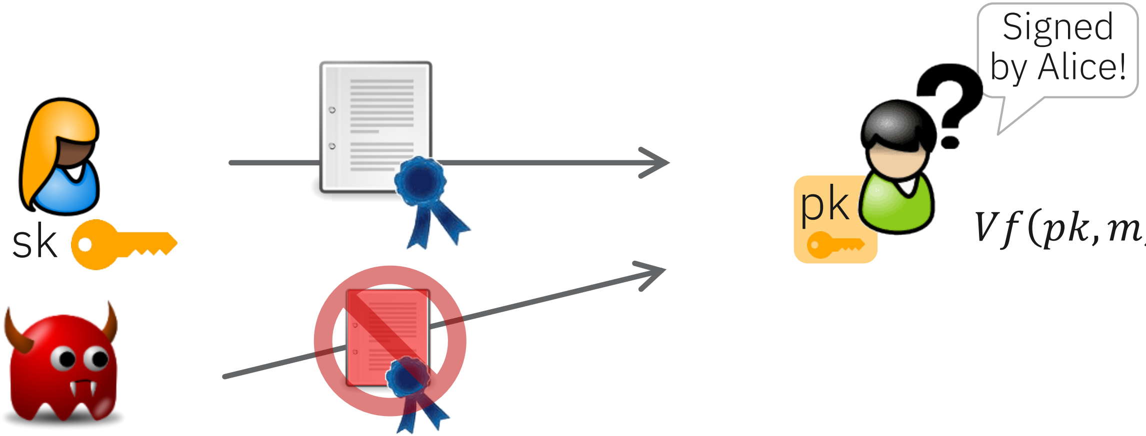
Roadmap

- Introduction to Group Signatures
  - Setting & Security Properties
  - Schemes
  - Similar Concepts
    - Anonymous Credentials
    - Direct Anonymous Attestation (DAA)
    - Enhanced Privacy ID (EPID)
- Group Signatures & V2X Communication
- Group Signatures with Selected Linkability for V2Cloud

Standard Signatures

$KGen(1^\tau) \rightarrow sk, pk$

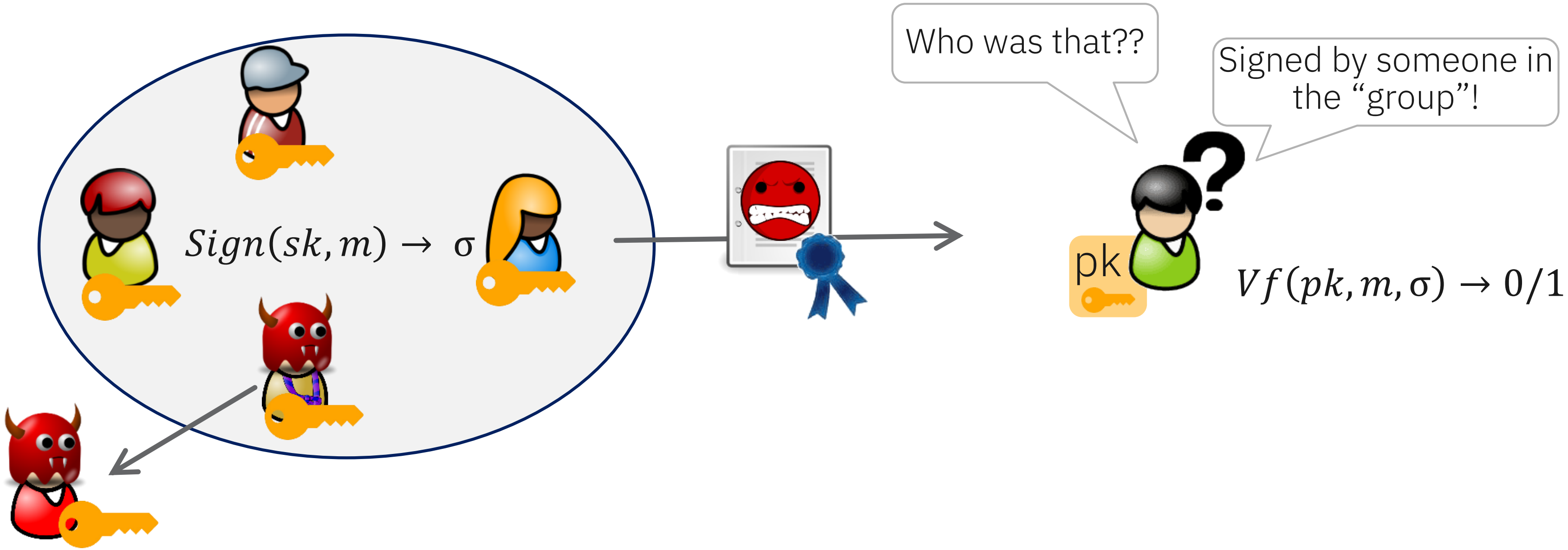
$Sign(sk, m) \rightarrow \sigma$



$Vf(pk, m, \sigma) \rightarrow 0/1$

- Security property: unforgeability
- Important primitive for strong authentication:
  - Server-side authentication, certified updates, eID cards, ...
- Bad for privacy – “leaks” the identity of the signer
  - Membership based online newsportal, vehicle-to-vehicle (V2V) communication, IoT,...

Group Signatures | Naive Approach

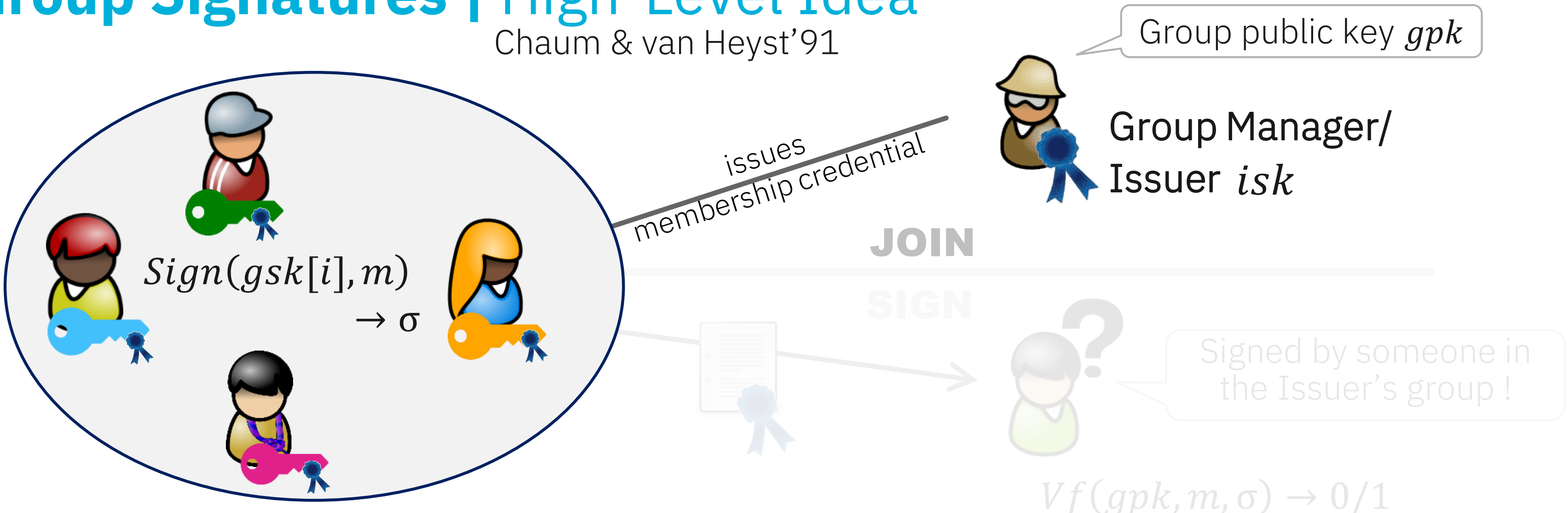


- Privacy ✓ : Doesn't leak any information about signer
- Security ✗ : Access to "group" not controlled

  No way to reveal signer in case of abuse (bug or feature?)

Group Signatures | High-Level Idea

Chaum & van Heyst’91

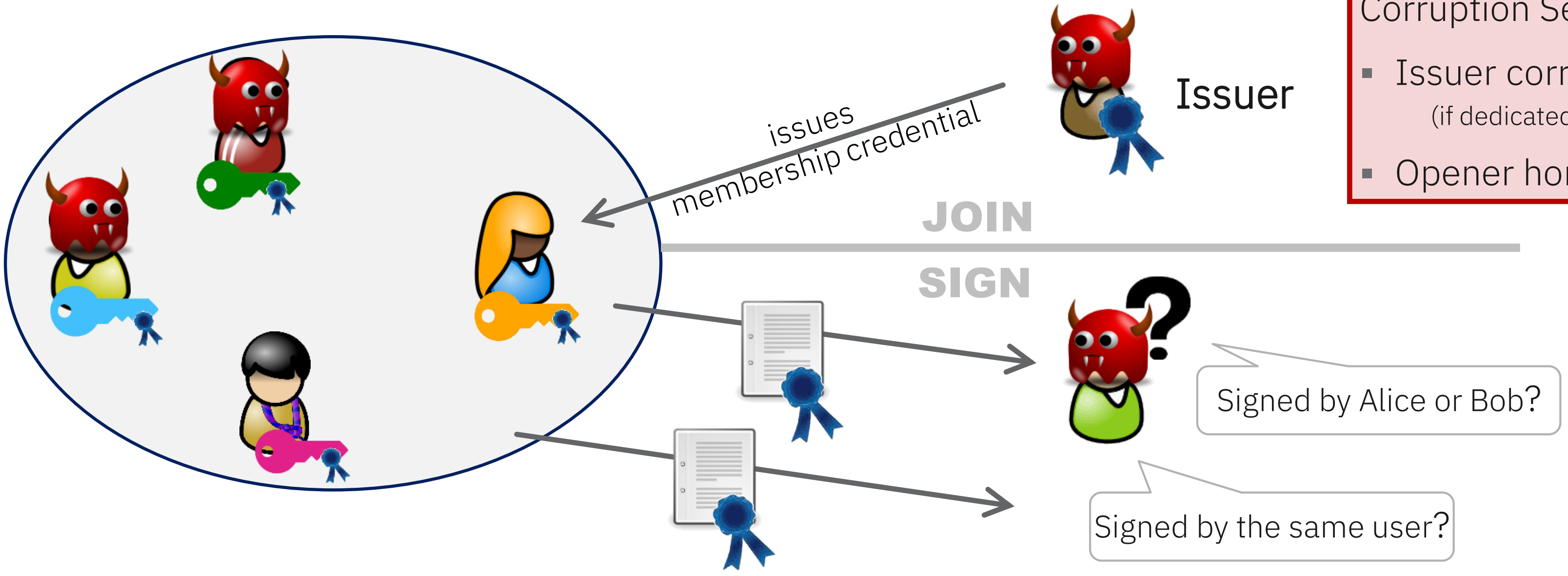


- Variants:
  - Static vs dynamic groups
  - Issuer = opener vs dedicated opener
  - Verifiable Opening

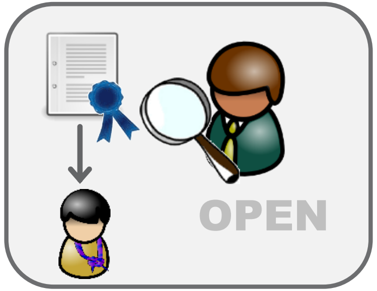
Group Signatures | Anonymity

Corruption Setting

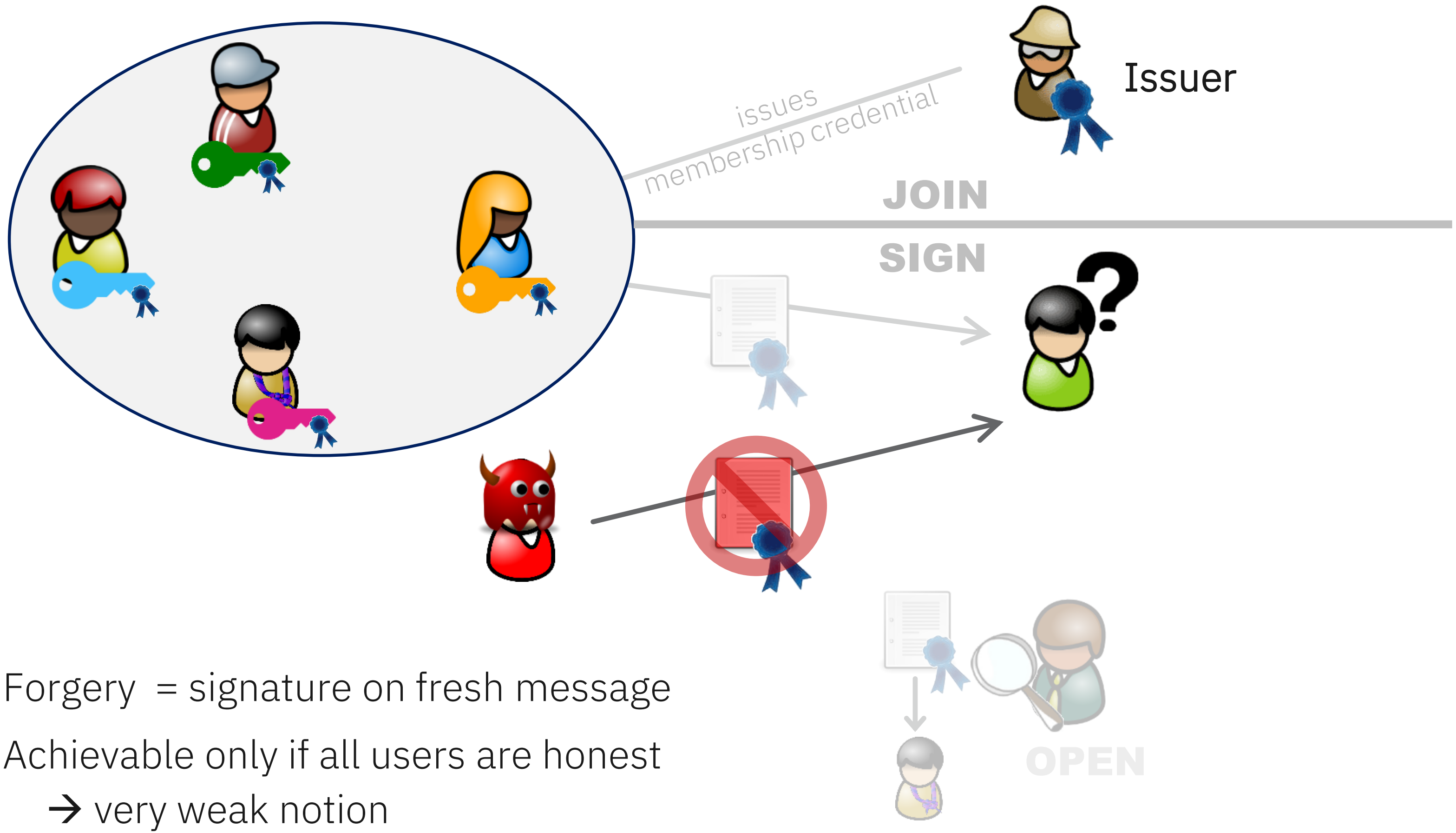
- Issuer corrupt*
  (if dedicated entity)
- Opener honest



- Signatures don't leak info about signer
  – Unlinkability of signatures
- Full/CCA anonymity: access to Opener

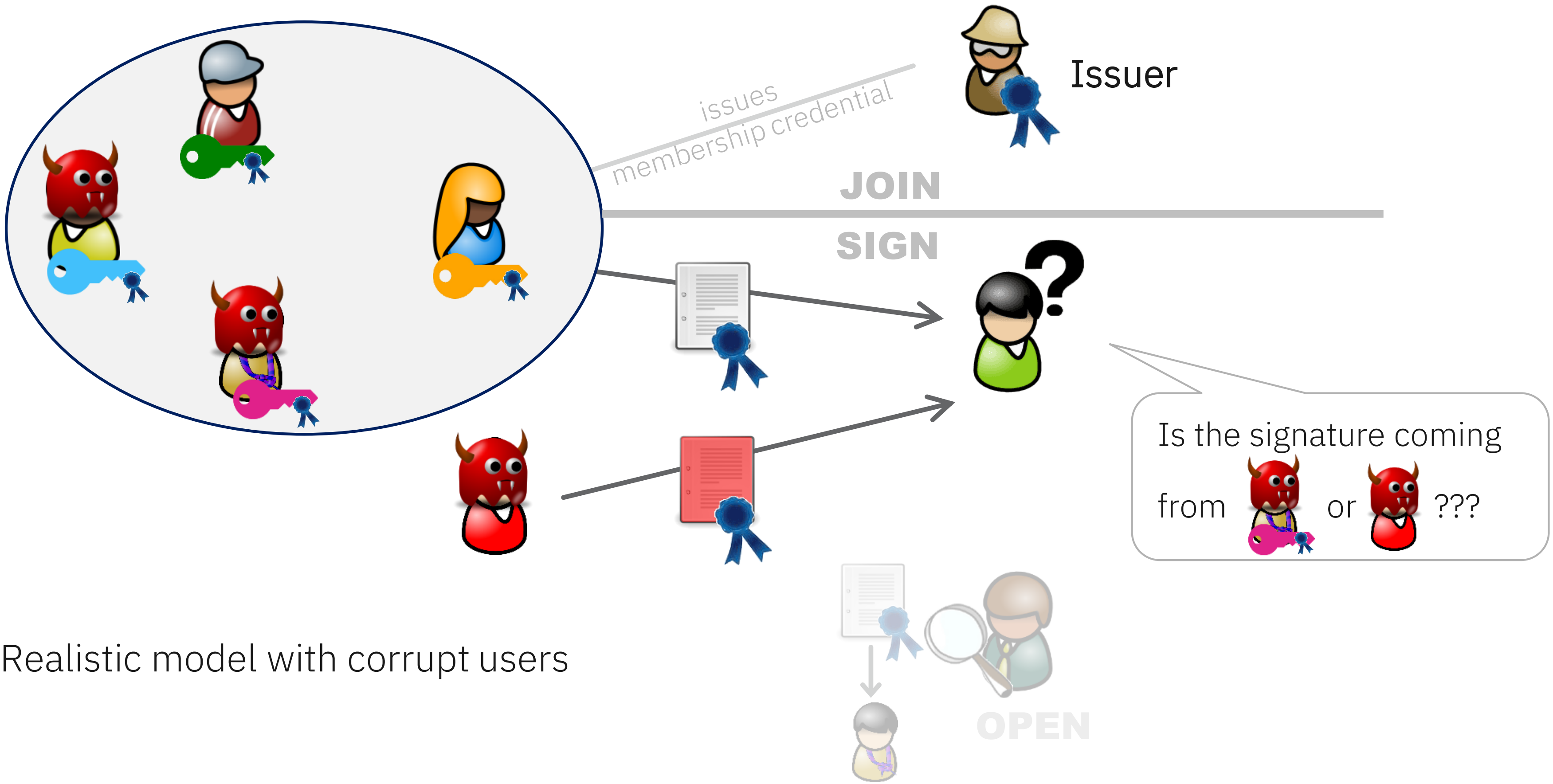


Group Signatures | Unforgeability (Naïve Approach)



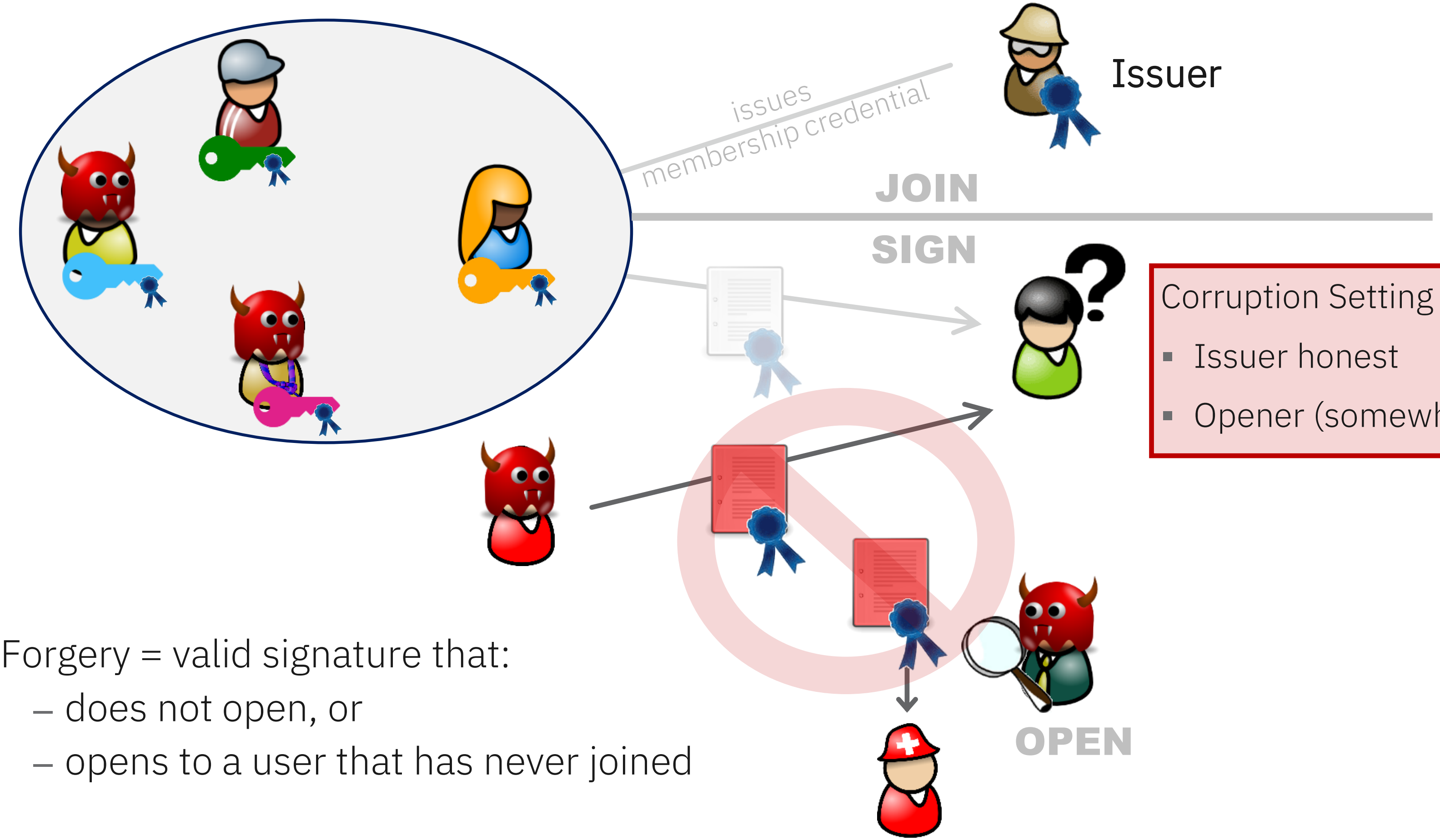
- Forgery = signature on fresh message
- Achievable only if all users are honest
  → very weak notion

Group Signatures | Unforgeability



- Realistic model with corrupt users

Group Signatures | Unforgeability (Traceability)

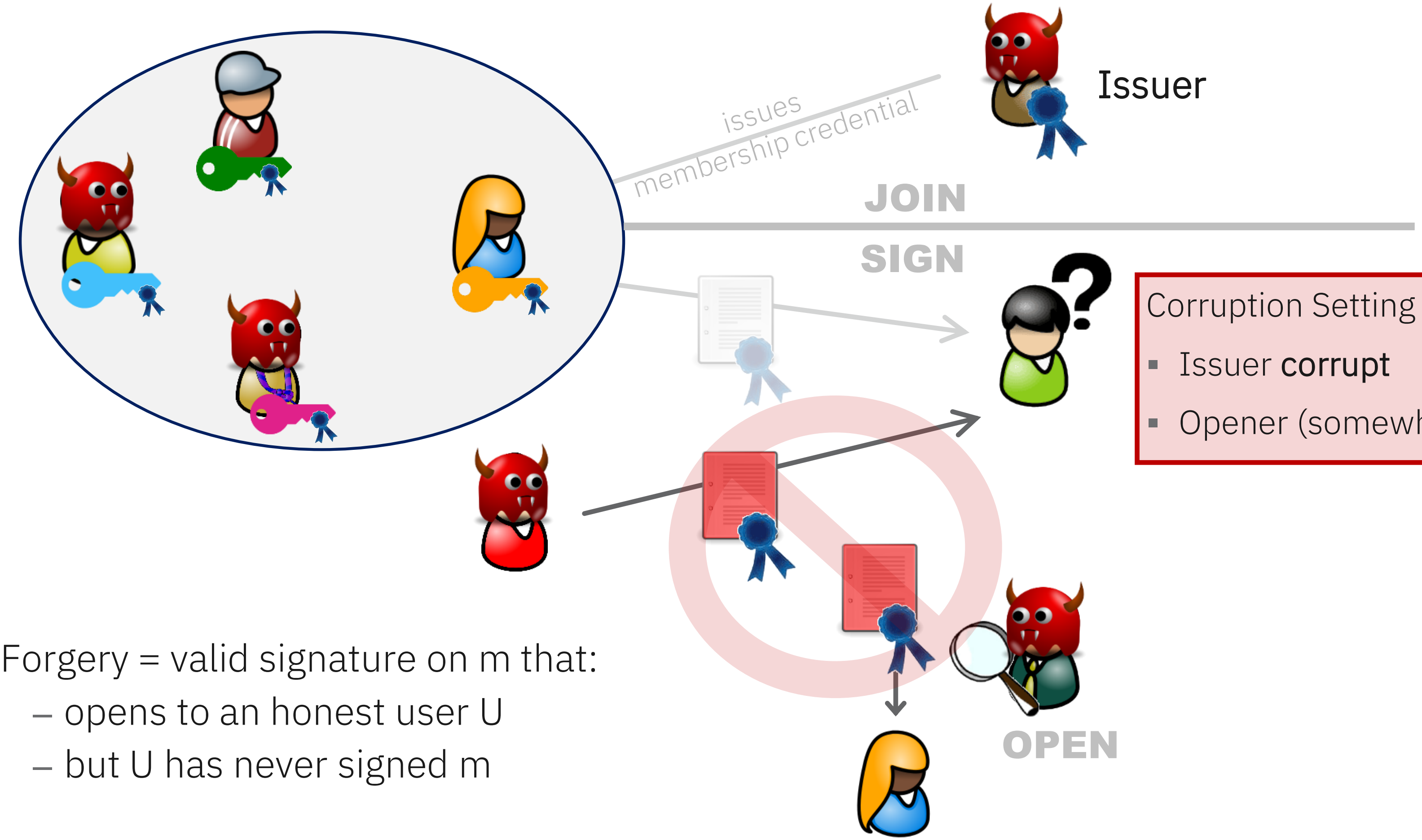


Corruption Setting

- Issuer honest
- Opener (somewhat) corrupt

- Forgery = valid signature that:
  – does not open, or
  – opens to a user that has never joined

Group Signatures | Non-Frameability



Corruption Setting
- Issuer **corrupt**
- Opener (somewhat) corrupt

- Forgery = valid signature on m that:
  - opens to an honest user U
  - but U has never signed m

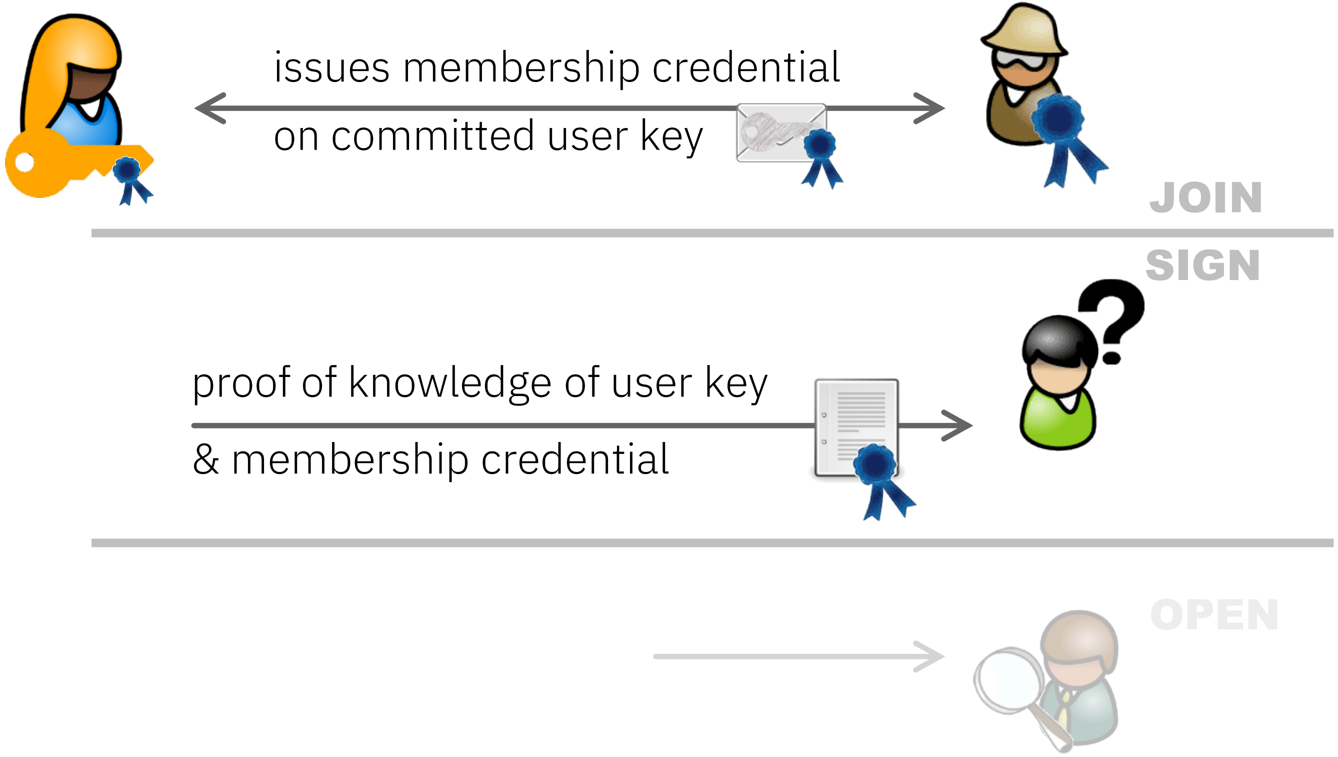
Group Signatures | Security Properties

Bellare, Shi, Zhang, '05

	Anonymity	Traceability	Non-Frameability
Issuer	Corrupt*	Honest	Corrupt**
Opener	Honest	Corrupt*	Corrupt

- *Only when Issuer ≠ Opener
- ** Only for **dynamic** group signatures. Issuer honest in static ones.
- Traceability + Non-frameability = unforgeability

Group Signatures | Schemes



Group Signatures | Schemes

$SIG.KGen(1^\tau) \rightarrow ssk, spk$

$upk = PKGen(usk) \longrightarrow$

$\longleftarrow cred = Sign(ssk, upk)$

$isk = ssk$

Choose random usk

$gsk[i] = (usk, cred)$

JOIN

SIGN

$$\pi = NIZK \left\{ \begin{array}{l} usk, upk, cred\colon Vf(spk, cred, upk) = 1 \wedge \\ upk = PKGen(usk) \end{array} \right\}(m)$$

$gpk = spk$

$\xrightarrow{m, \sigma = \pi}$

Group Signatures | Schemes

$ENC.KGen(1^\tau) \rightarrow esk, epk$

$SIG.KGen(1^\tau) \rightarrow ssk, spk$

$\xrightarrow{upk \,=\, PKGen(usk)}$

$\xleftarrow{cred \,=\, Sign(ssk,\, upk)}$

$isk = ssk$

Choose random usk

$gsk[i] = (usk, cred)$

JOIN

SIGN

$$\pi = NIZK\left\{ \begin{array}{l} usk, upk, cred\!: Vf(spk, cred, upk) = 1 \wedge \\ upk = PKGen(usk) \wedge \ C = Enc(epk, upk) \end{array} \right\}(m)$$

$C = Enc(epk, upk)$

$\xrightarrow{m,\, \sigma \,=\, (\pi,\, C)}$

$gpk = spk, epk$

OPEN

$\xrightarrow{m,\, \sigma \,=\, (\pi,\, C)}$

$\xleftarrow{upk \,=\, Dec(esk,\, C)}$

$osk = esk$

Group Signatures | Schemes

$ENC.KGen(1^\tau) \rightarrow esk, epk$

$SIG.KGen(1^\tau) \rightarrow ssk, spk$

- Non-Frameability: PKGen hiding

$upk = PKGen(usk)$ →

← $cred = Sign(ssk, upk)$

$isk = ssk$

Choose random usk

$gsk[i] = (usk, cred)$

JOIN

SIGN

$$\pi = NIZK \left\{ \begin{array}{l} usk, upk, cred\text{: } Vf(spk, cred \\ upk = PKGen(usk) \wedge \boldsymbol{C = Enc(epk, up} \end{array} \right.$$

- Anonymity: ZK of NIZK & CCA security of ENC

$\boldsymbol{C = Enc(epk, upk)}$

$m, \sigma = (\pi, \boldsymbol{C})$ →

OPEN

$\boldsymbol{m, \sigma = (\pi, C)}$ →

← $\boldsymbol{upk = Dec(esk, C)}$

$\boldsymbol{osk = esk}$

- Traceability: Unforgeability of SIG & Soundness of NIZK

Group Signatures | Schemes

Bellare, Micciancio, Warinschi‘03

- Sign & Encrypt & Prove most common approach, mainly differ in signature scheme
  - Signatures on committed messages $cred = Sign(isk, upk) = "Sign(isk, usk)"$
  - Efficient proofs of knowledge of a signature
  - Instantiations: CL‘01 (strong RSA), CL‘04 (LRSW), BBS‘04 (q-SDH), PS‘16 (q-MSDH-1)

- Opening flexible: verifiable decryption, threshold decryption
- Disadvantage: opening increases signature size, yet is hardly needed

- More compact group signatures: GetShorty (Bichsel et al, SCN’10)
  - Join creates user-specific opening secret at Issuer/Opener
  - To open, Issuer/Opener iterates through all opening secrets & test against signature
  - Disadvantage:
    - Opening gets very expensive (feature?)
    - Issuer = Opener (inherently weaker security guarantees)

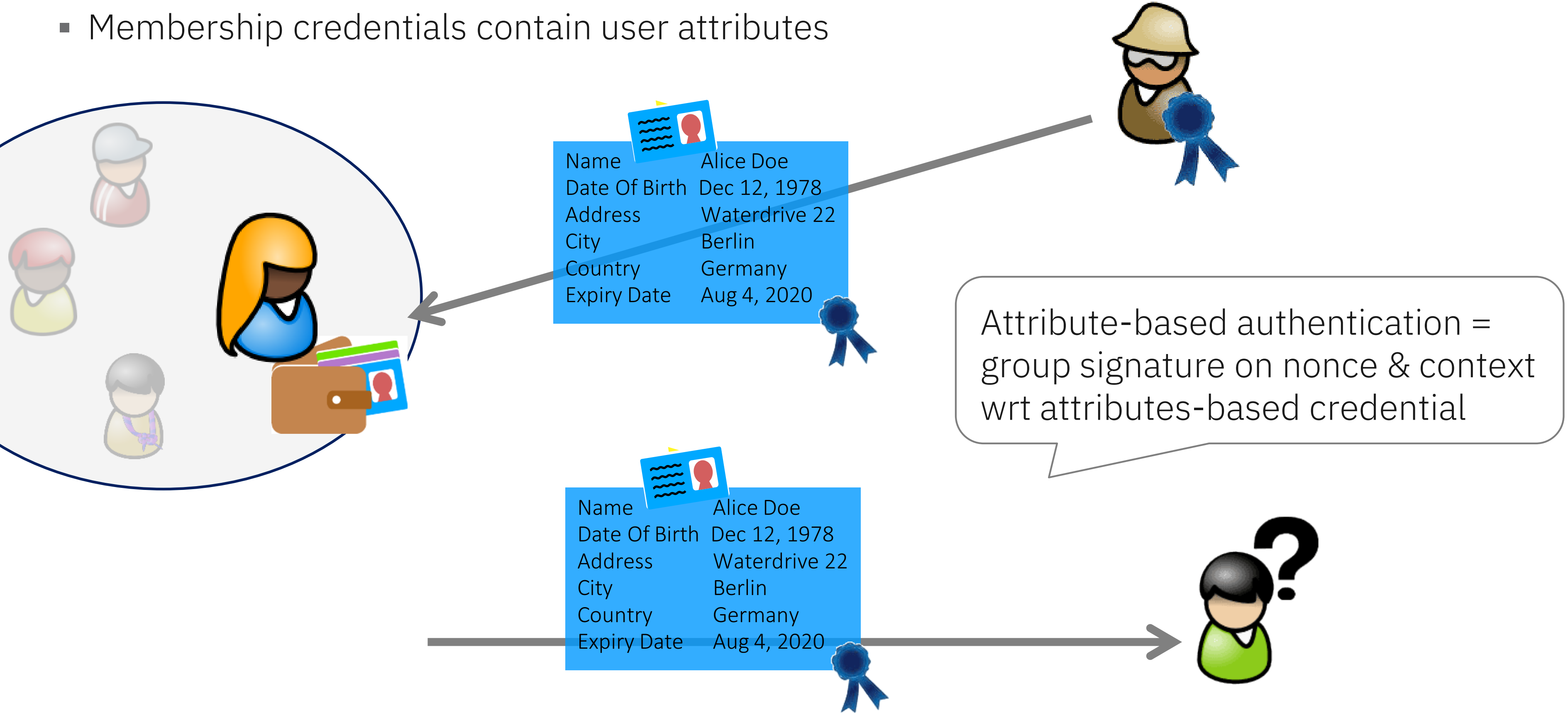
Roadmap

- Introduction to Group Signatures
  - Setting & Security Properties
  - Schemes
  - Similar Concepts
    - Anonymous Credentials
    - Direct Anonymous Attestation (DAA)
    - Enhanced Privacy ID (EPID)
- Group Signatures & V2X Communication
- Group Signatures with Selected Linkability for V2Cloud

Anonymous Credentials

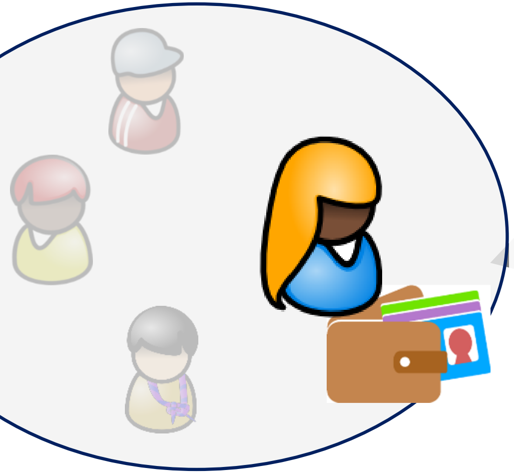
Envisioned by Chaum in 1981,
first full scheme by Camenisch & Lysyanskaya in 2001

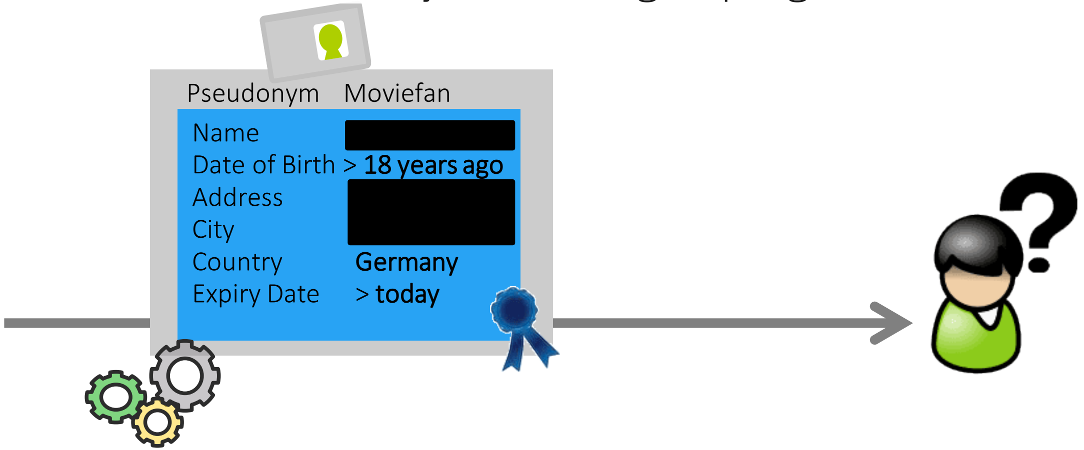
- Membership credentials contain user attributes



Anonymous Credentials

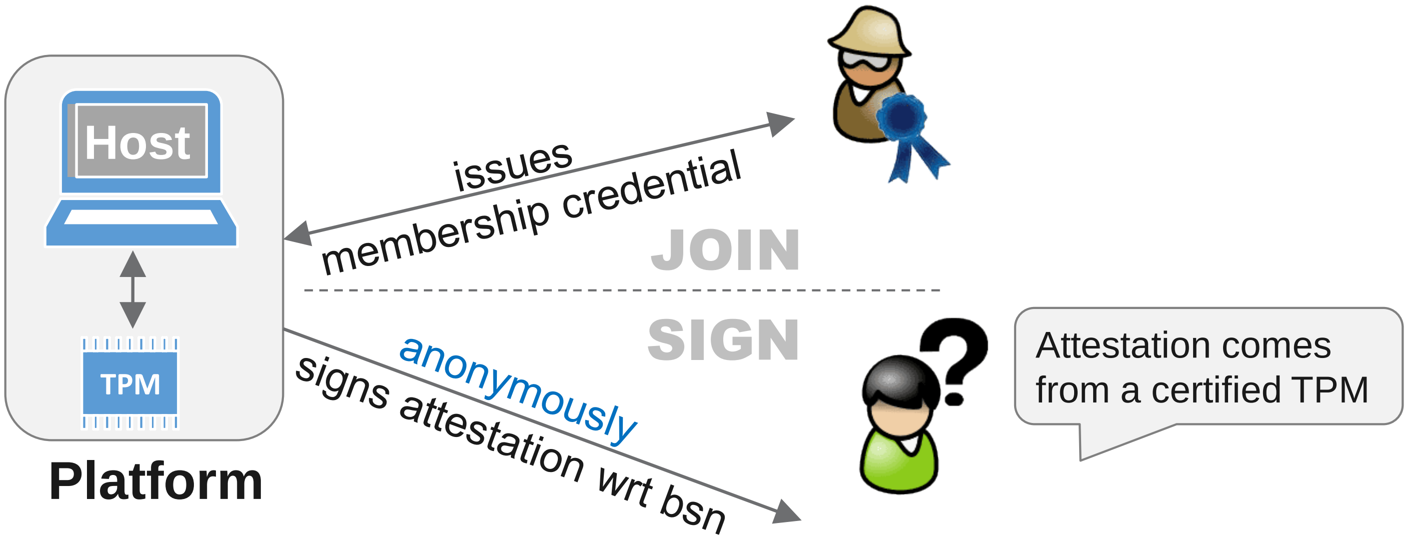
- Membership credentials contain user attributes
  - User can selectively disclose each attribute
  - User can prove predicates over the attributes, e.g., “I'm over 18”
  - Revocation of credentials (issuer/verifier-driven)
  - User-controlled linkability via pseudonyms
    → Unlinkable authentication as default, linkability as an option
  - Construction very similar to group signatures (CL/BBS/PS-based)





Direct Anonymous Attestation (DAA)

- Hardware-based attestation using a Trusted Platform Module (TPM)
  - Secure crypto processor creates, stores, uses cryptographic keys
  - Makes anonymous remote attestations of host status
- Split between host & TPM → shift heavy computations to host
- Unlinkability steered via “basename” and pseudonyms. No Opener.



Direct Anonymous Attestation (DAA)

- Standardized in TPM1.2 (2004) & ISO/IEC 20008-2
  - RSA-based by Brickell, Camenisch, Chen
  - Developed for Trusted Computing Group (TCG) = industry group that standardizes TPM

- Revised TPM2.0 (2014)
  - Elliptic curve & pairing based
  - Flexible API to support different protocols
  - TPM part & protocols ISO standardized

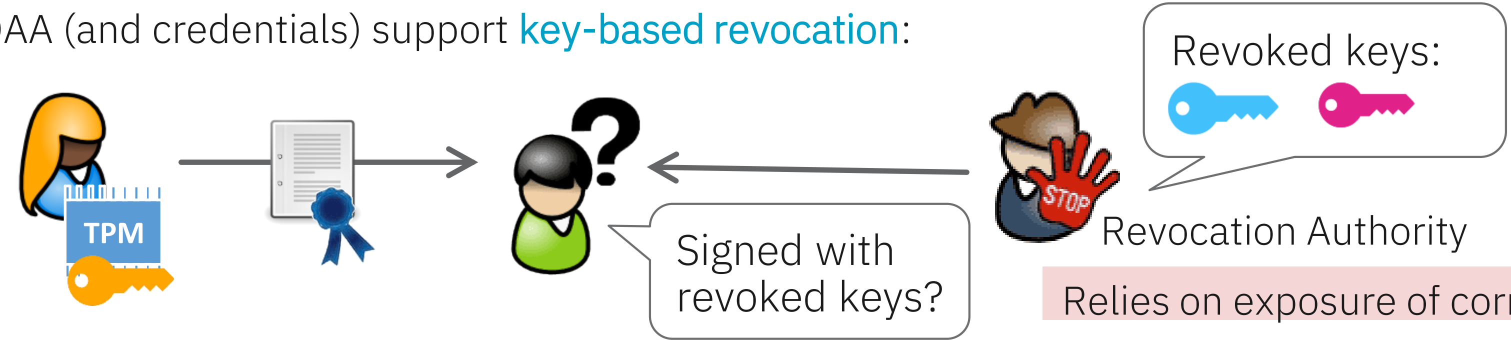
- Over 500 million TPMs sold

- Standardized DAA has a number of security issues
  - All security models & schemes had issues (ISO scheme is trivially forgeable) [CDL16a, CDL16b]
  - TPM interfaces had inherent security problems [CCD+17]
  - TPM assumed fully trusted. Subversion-resilient DAA [CDL17]

Enhanced Privacy ID (EPID)

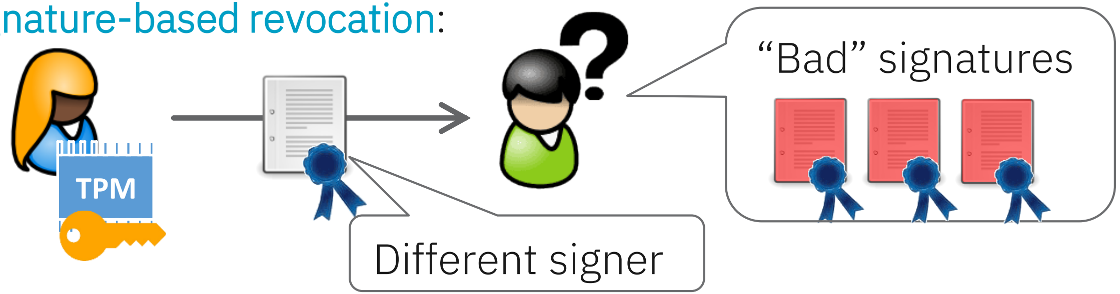
- DAA-variant used for attestation on Intel's SGX
  - Without host/TPM split
  - Signature-based revocation

- DAA (and credentials) support key-based revocation:



Relies on exposure of corrupted keys

- Signature-based revocation:



Proof scales linearly in #revoked users

Comparison

	Group Signature	Credentials	DAA	EPID
Opener				
Pseudonyms				
Attributes				
Revocation			Key-based	Signature-based
TPM Anchor				All on TPM

Comparison

	Group Signature	Credentials	DAA	EPID
Opener				
Pseudonyms				
Attributes				
Revocation			Key-based	Signature-based
TPM Anchor				All on TPM

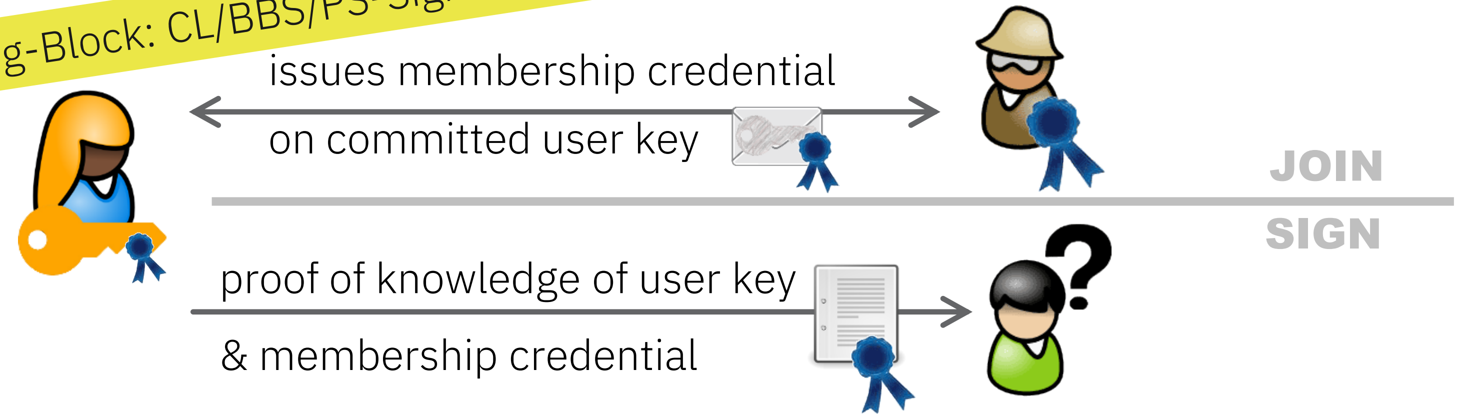
- Opener vs. pseudonyms has not only impact on privacy but also on unforgeability
- Every new combination of features requires new security model

- Attributes: can encode validity, i.e., make creds short-lived = alternative to revocation

Comparison

	Group Signature	Credentials	DAA	EPID
Opener				
Pseudonyms				
Attributes				
Revocation			Key-based	Signature-based
TPM Anchor				All on TPM

Same Core Building-Block: CL/BBS/PS-Signature



Roadmap

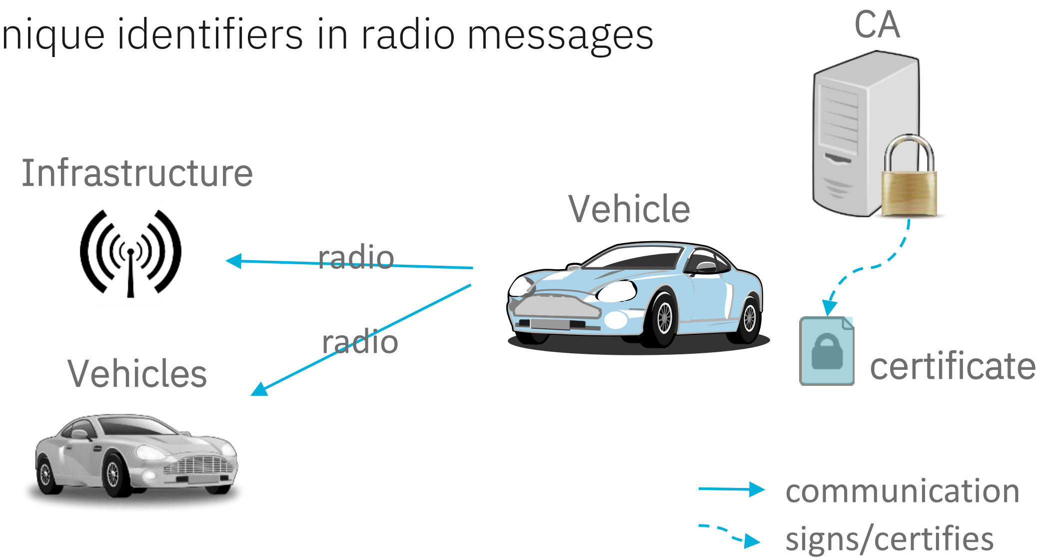
- Introduction to Group Signatures
  - Setting & Security Properties
  - Schemes
  - Similar Concepts
    - Anonymous Credentials
    - Direct Anonymous Attestation (DAA)
    - Enhanced Privacy ID (EPID)

- Group Signatures & V2X Communication

- Group Signatures with Selected Linkability for V2Cloud

Vehicle-to-Vehicle (V2V) Authentication

- Short-range radio communication between vehicles (V2V) and infrastructure (V2I)
  - position, speed,... for collision avoidance, road & traffic conditions
  - first roll-out in 2019(?), expected mandatory in new vehicles in near future
- Requirements:
  - **security:** authenticate real vehicles to exclude attacker trying to disrupt traffic
  - **privacy:** cannot track vehicles by unique identifiers in radio messages
- V2V/V2I (=V2X)
  - low communication bandwidth (300 Bytes max)
  - high message frequency (1-10 msg/vehicle/second)



Current C-ITS Security Architecture

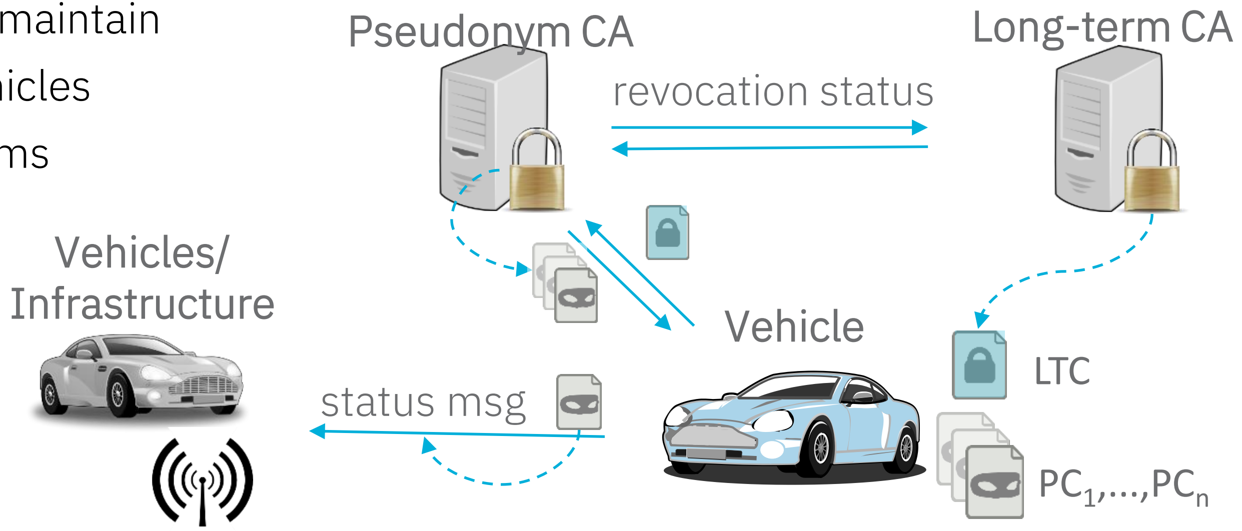
- C-ITS: Cooperative Intelligent Transport Systems
  - Standardization in CEN and ETSI
- C-ITS Platform established by European Commission in 2014
  - Cooperative framework incl. national authorities, C-ITS stakeholders and the Commission
  - Develop a shared vision on the interoperable deployment of C-ITS in the EU

Current C-ITS Security Architecture with Pseudonym CA

- Vehicles receive short-term pseudonym certificates (100/week), switch every 5min
- Authenticate messages via pseudonym certificates

Neither optimal for privacy nor security:

- Pseudonym CA is security/privacy bottleneck & expensive to maintain
- High storage costs for vehicles
- Limited pool of pseudonyms



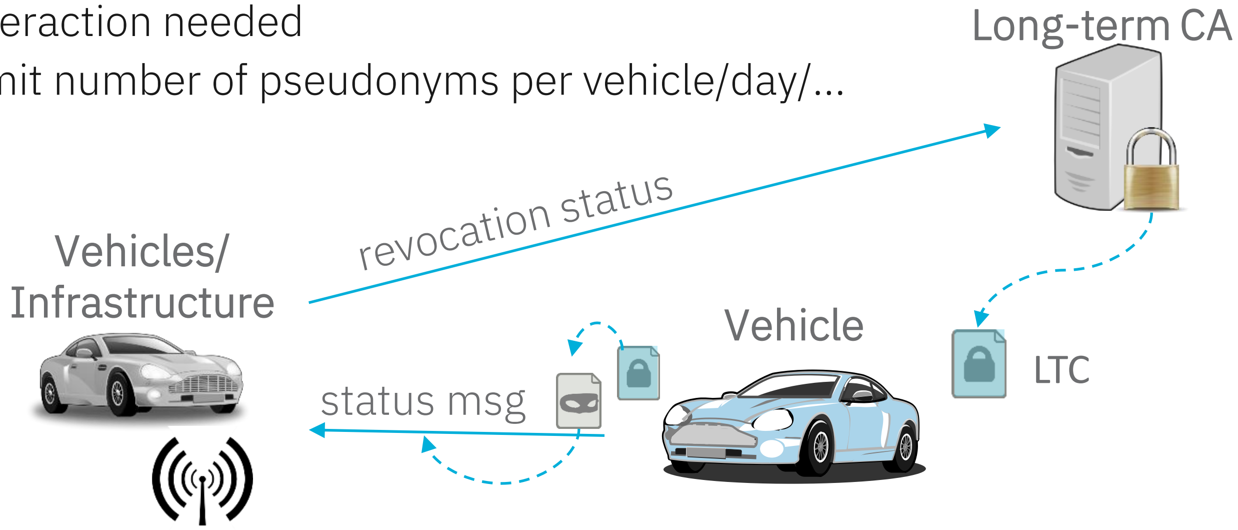
Group Sigs/Credentials: Optimal Privacy and Security

security

- Different key ("credential") in each vehicle, can be individually revoked
- Offline authority (or multiple) can de-anonymize signatures

privacy

- Vehicles can locally self-certify pseudonyms
  - no server interaction needed
  - optionally limit number of pseudonyms per vehicle/day/…



Group Sigs/Credentials: Optimal Privacy and Security

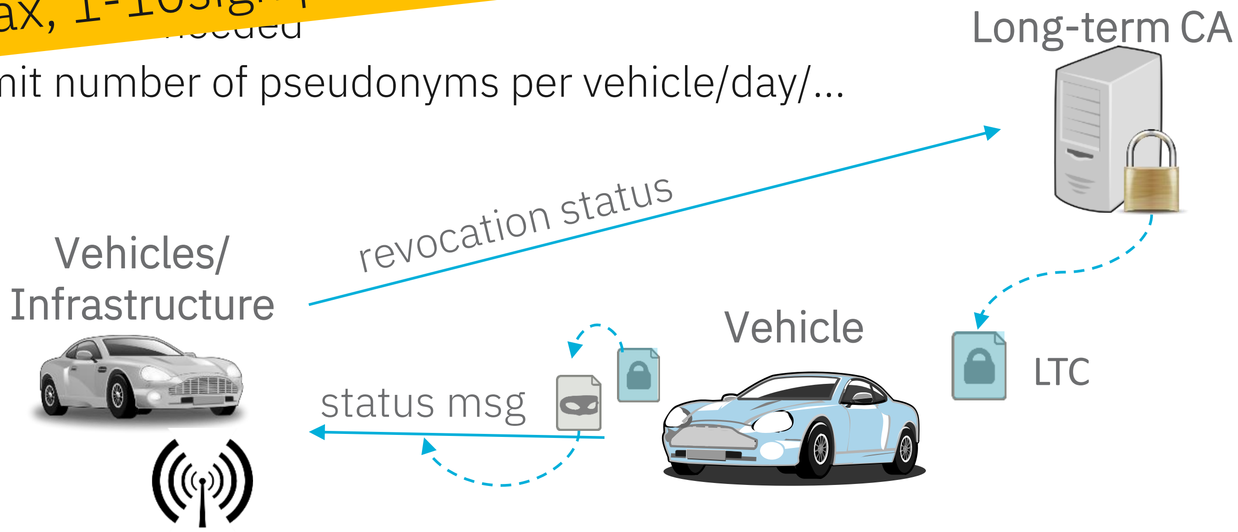
security

- Different key ("credential") in each vehicle, can be individually revoked
- Offline authority (or multiple) can de-anonymize signatures

privacy

  - optionally limit number of pseudonyms per vehicle/day/…

Main challenge: efficiency & bandwidth & revocation
(300 Bytes max, 1-10sign per vehicle/sec)



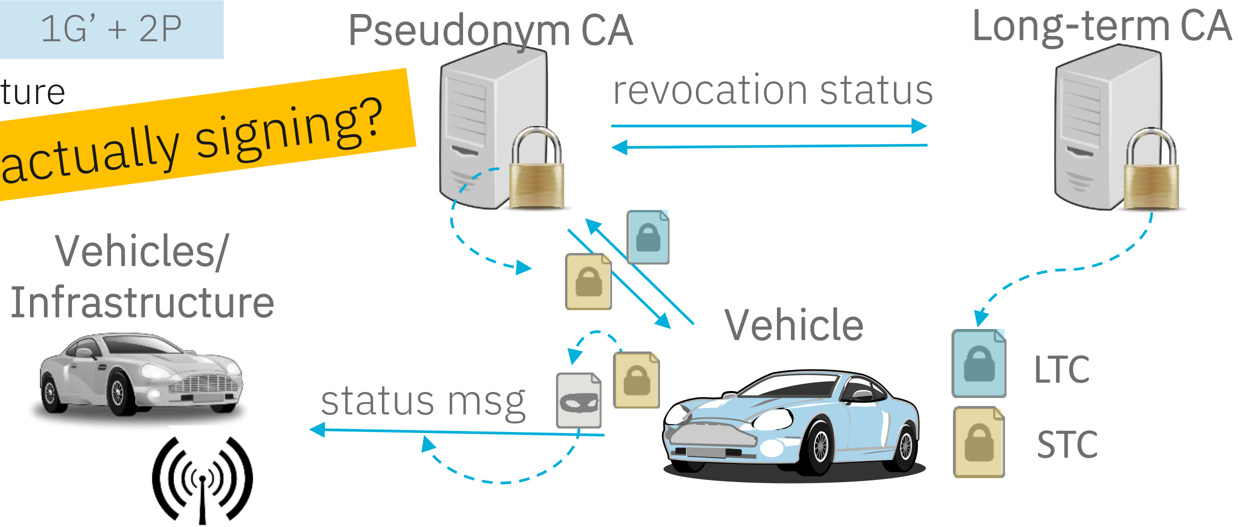
V2X Communication via Group Signatures

- Our approach:
  - Long-term conventional certificate (revocation is easy)
  - Short-lived group membership credentials incl attribute =validity epoch, e.g, week
  - Compact sigs: GetShorty + PS group signatures + attribute

Sig Size	Signing	Verification
2G + 3Zp	1G	1G' + 2P

BLS381: 176 Byte per signature

Wait .... what are we actually signing?



V2X Communication via Group Signatures

- Regular position beacon messages, broadcasted 1–10 times per second
  - Cooperative Awareness Messages (CAMs)
  - Dynamic information: position, speed, and heading
  - Static information: length, width, and sensor accuracy
- Signed with privacy-preserving (group/pseudonym) signature but broadcast in plaintext

Group Signature cannot guarantee privacy when messages are already identifying!

V2X Communication via Group Signatures & Encryption

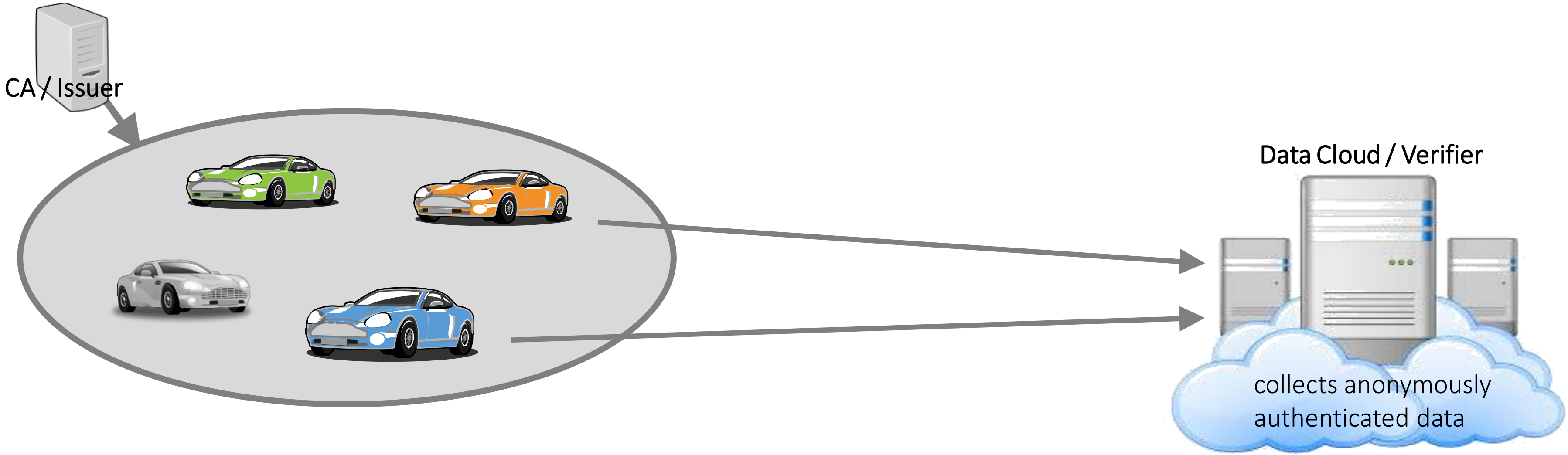
- Privacy-preserving V2X communication needs encryption!
- New Approach: Zone Encryption with Anonymous Authentication [CDLNT19]
  - Vehicles exchange short-lived & geo-local *symmetric* AE keys
  - Use (compact) group signatures for authenticated key-exchange
  - Send CAMs encrypted with AE keys (w/o group signature)
  - Legitimate vehicles can decrypt, but no passive eavesdropping & mass surveillance

Roadmap

- Introduction to Group Signatures
  - Setting & Security Properties
  - Schemes
  - Similar Concepts
    - Anonymous Credentials
    - Direct Anonymous Attestation (DAA)
    - Enhanced Privacy ID (EPID)
- Group Signatures & V2X Communication
- Group Signatures with Selected Linkability for V2Cloud

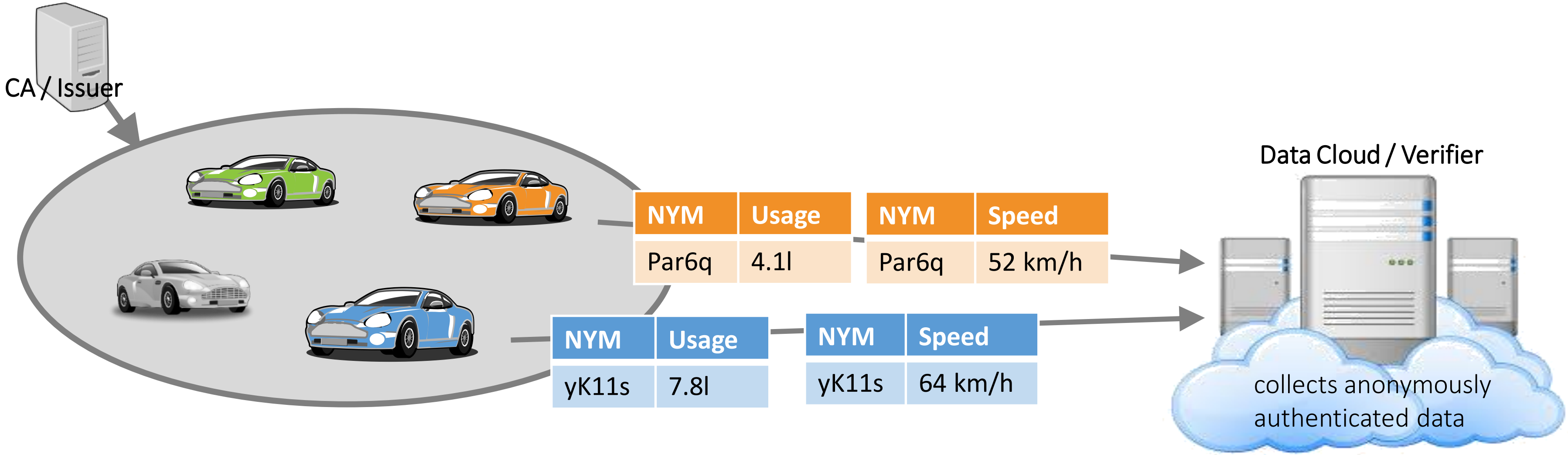
Vehicle-to-Cloud Communication

- V2Cloud communication: updates, diagnostics, services (e.g., insurance)
  - Less resource critical (via 4/5G, Wifi), less frequent
- Collection of sensor, driver data – general statistics, user-specific services
  - Data usage often not clear at time of collection
  - Requirements: authenticity & privacy



Vehicle-to-Cloud Communication with Group Signatures

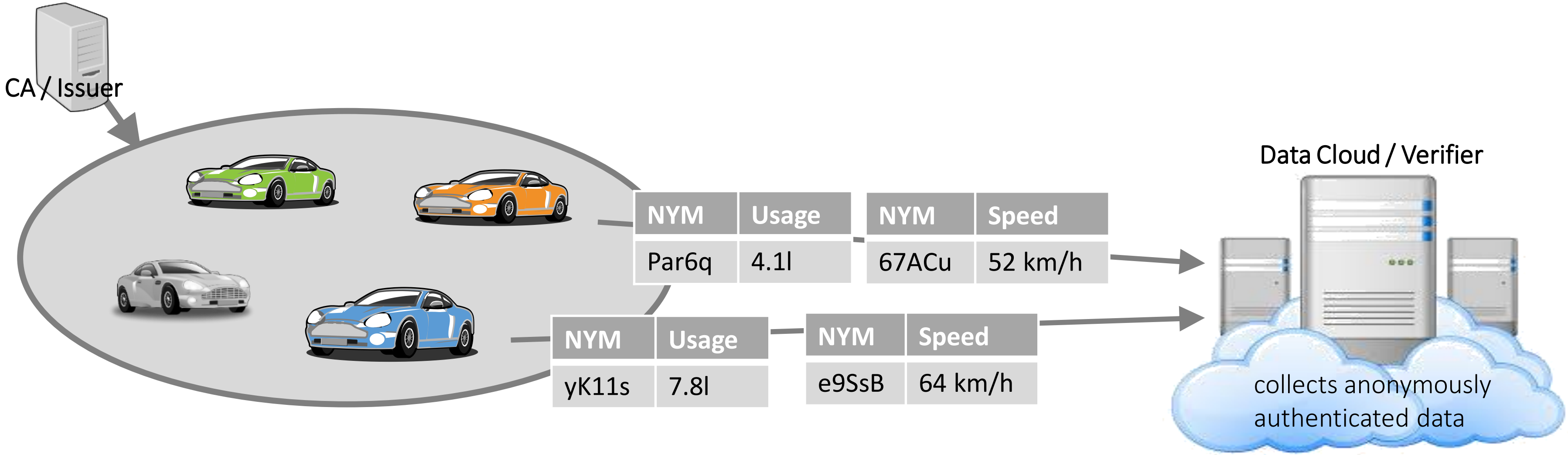
- Which variant to control privacy vs utility?
  - **Opening** not suitable – too invasive and inefficient. Might have to open all signatures
  - **User-controlled linkability (pseudonym)** too inflexible:
    - Decision about linkability must be done at the moment the data is disclosed
    - No option to selectively correlate data later on → bad tradeoff between privacy and utility
    - Static pseudonyms allow inference attacks



Group Signatures with Selective Linkability [GL19]

- Extends group signatures to allow for selective linkability after the data is collected
  - Data is fully unlinkable and anonymous when its collected
  - Selective subsets can be correlated in a consistent manner later on
  - Linkability is created through a dedicated entity → the converter

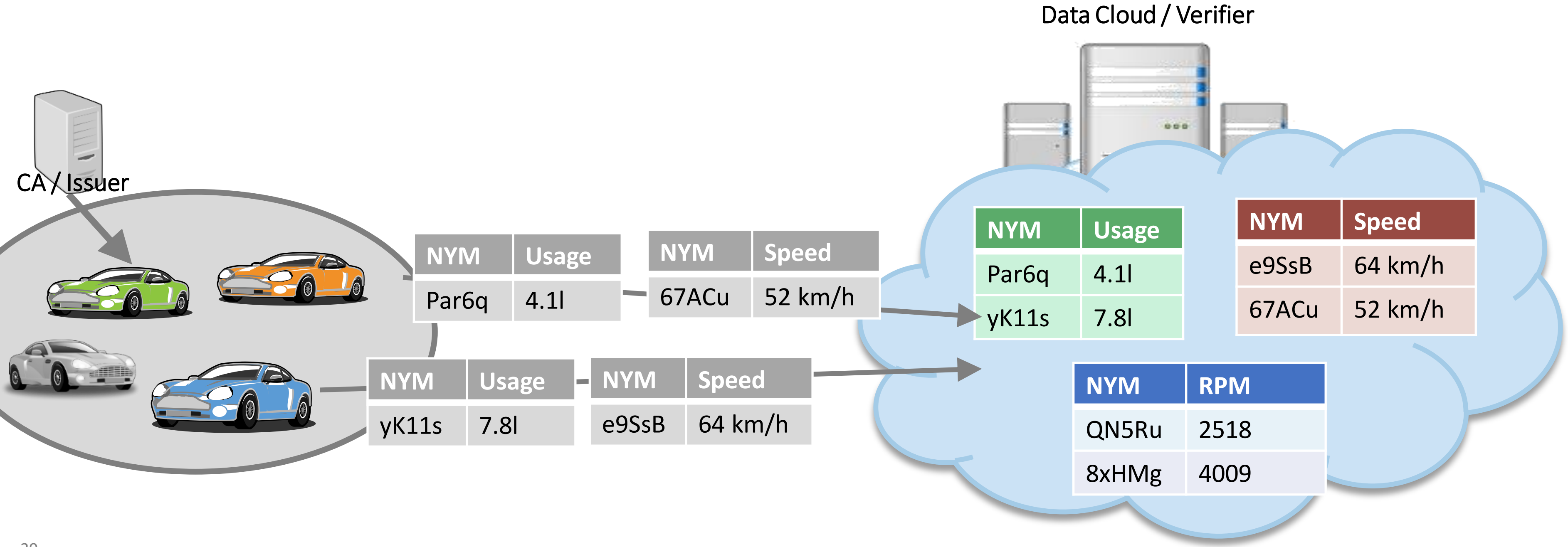
Optimal privacy when data is collected while preserving the full utility of the data



Group Signatures with Selective Linkability | Sign

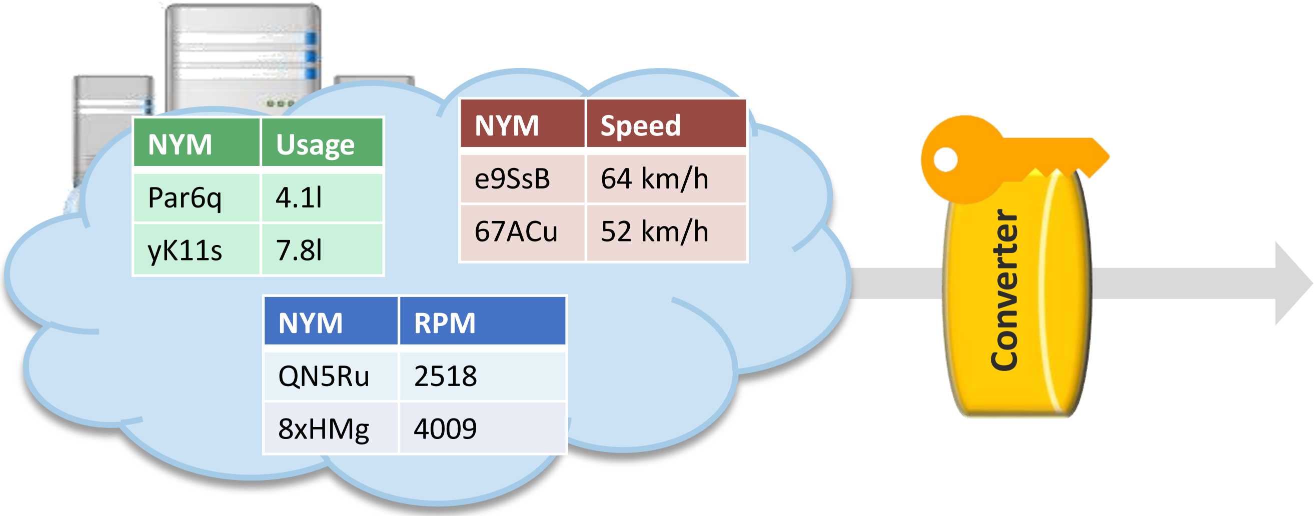
- Data is collected in unlinkable, authenticated snippets
- Group signatures with fresh pseudonyms for every message

→ Cloud is assured that only legitimate data gets uploaded & full privacy is preserved



Group Signatures with Selective Linkability | Convert

- Only required sub-sets of the data are made linkable w.r.t. to join-specific pseudonym
- Converter transforms pseudonyms into consistent representation
  - **Obliviousness**: converter learns nothing about pseudonyms / messages it transforms
  - **Non-transitivity**: different conversion requests cannot be linked



NYM	Usage
Par6q	4.1l
yK11s	7.8l

NYM	Speed
e9SsB	64 km/h
67ACu	52 km/h

NYM	RPM
QN5Ru	2518
8xHMg	4009

query: speed & usage

NYM	Speed	Usage
GDA12	64 km/h	7.8l
0tU5r	52 km/h	4.1l

Summary

- Group signatures: privacy-preserving authentication
- Many variants & extensions exist:
  - Opener, pseudonyms, attributes, hardware-based, revocation, ...
  - Anonymous Credentials, DAA, EPID
- Defining security for group signatures requires a lot of care
- Group signature cannot guarantee privacy when messages are already identifying!

Thanks! Questions?

anj@zurich.ibm.com