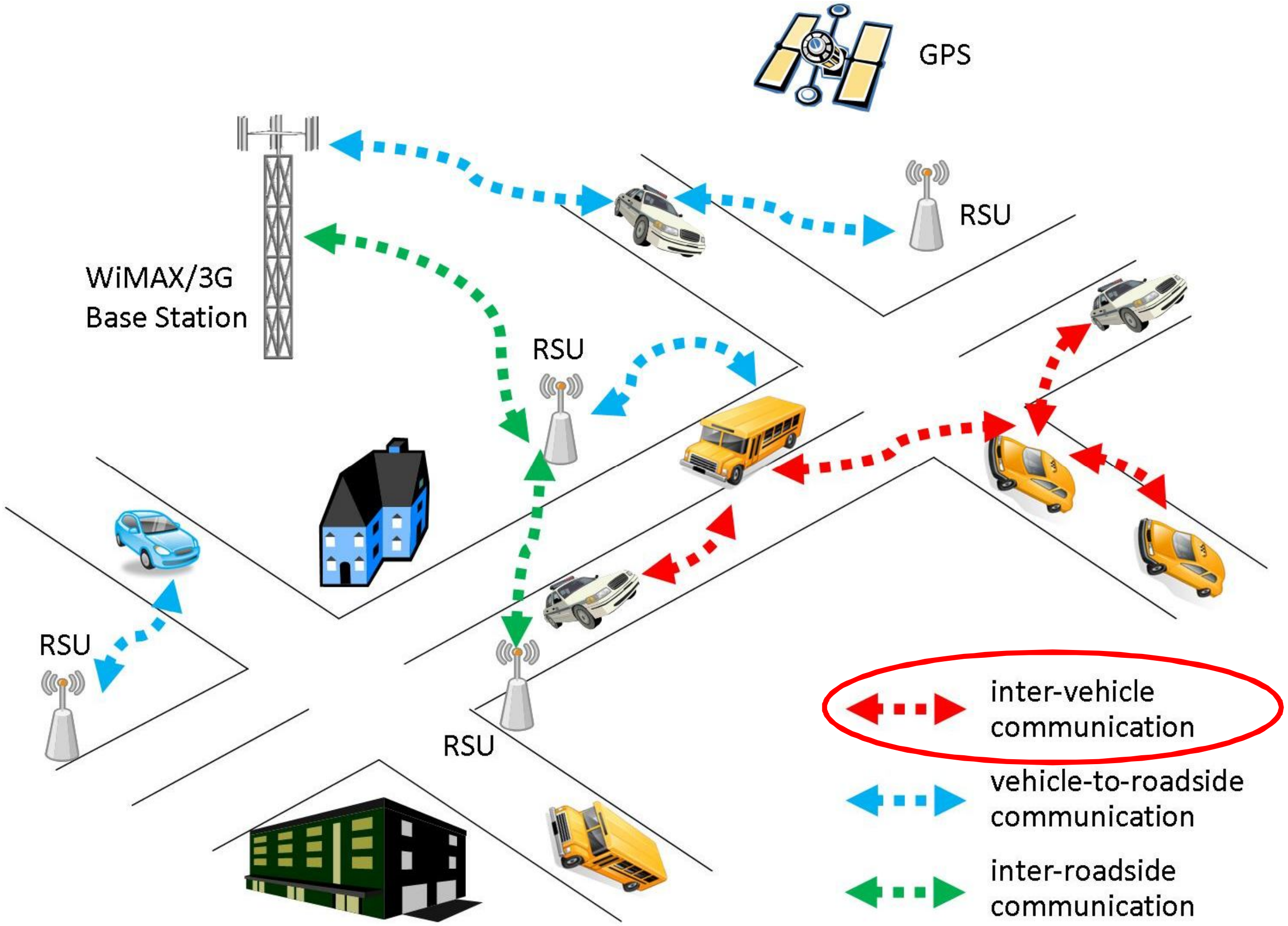
UNIVERSITY OF TWENTE.

Secure and Privacy-Preserving Broadcast Authentication for IVC

Liting Huang

IVC / VANET (Vehicular Ad-hoc Network)

watch video



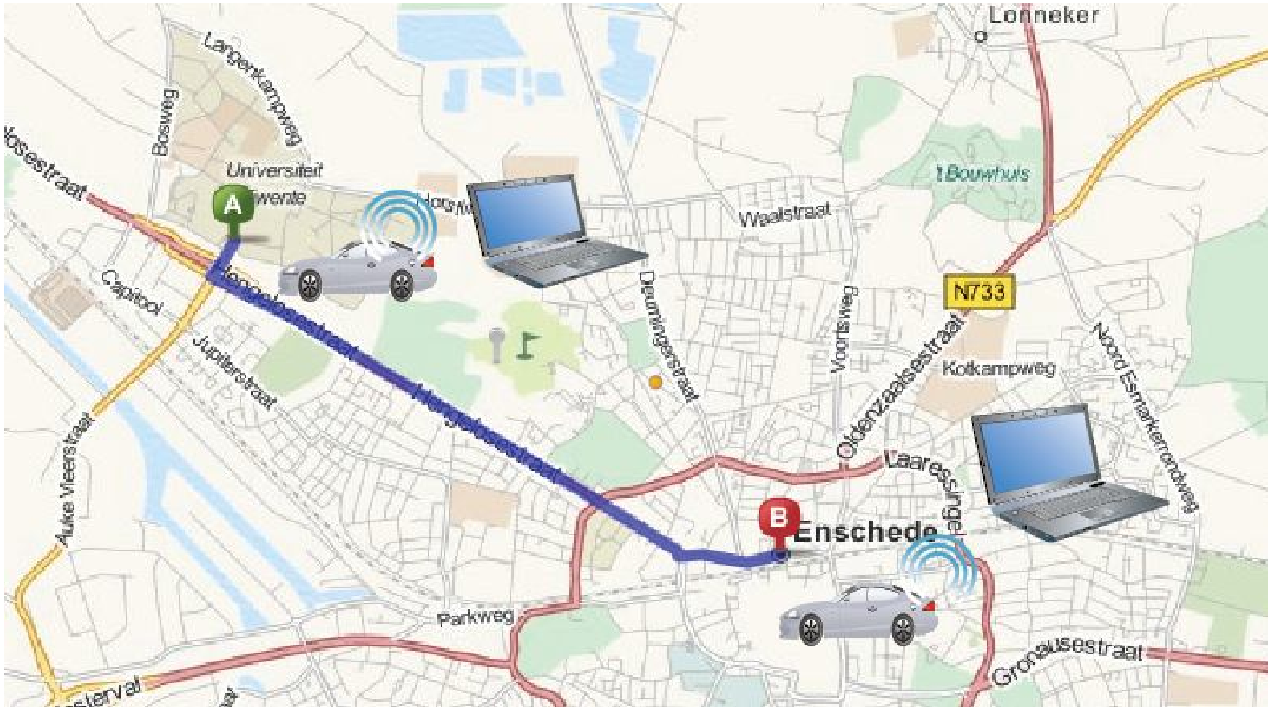
inter-vehicle communication

vehicle-to-roadside communication

inter-roadside communication

Motivation

- Why Broadcast Authentication needed?
- Why Privacy Protection needed?
  - Tracking Problem



Ultimate Privacy Protection - Attribute Authentication

- Attribute Authentication
  - No Identity, No Pseudonym
  - Show an attribute or several attributes
- What is Attribute?

Attribute Name	Attribute Value
Vehicle type	{Car, bus, motor-cycle}
Vehicle role	{Public, private, emergency, police}
Vehicle key	200-bit integer

Requirements For “Secure and Privacy-Preserving Broadcast Authentication” Protocols

- Basic Requirements

Message Authentication Without Originator Verification	Attribute Authentication	Privacy Protection	Strong Unlinkability
One-hop Broadcast Authentication	Small Size	Low Computation Overhead	Independent Authentication

How Previous Solutions Fulfill the Requirements

Schemes	Message Authentication Without Originator Verification	Attribute Authentication	Privacy Protection	Unlinkability	One-hop Broadcast Authentication	Independent Authentication
PKI+	●		●	Flexible	●	●
ECPP	●		●	Flexible	●	●
Hybrid	●	○	●	Flexible	●	●
SeVeCom	●	○	●	Flexible	●	●
V-tokens	●		●	Flexible	●	●
Sun’s IDB	●		●	Flexible	●	●
Kamat’s IDB	●		●	Flexible	●	●
SRAAC	●		●	Flexible	●	●
GSIS	●		●	High	●	●

How Previous Solutions Fulfill the Requirements

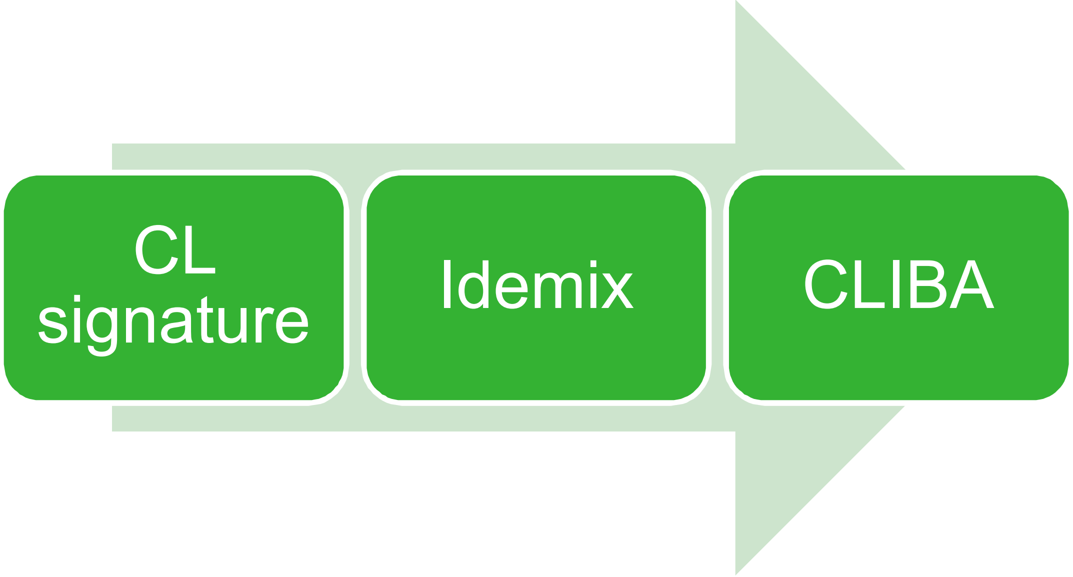
- How about performance?

Generally speaking, the size of the authentication information is less than 200 bytes. The computation time is less than 50 ms on a low efficiency machine (with CPU clock frequency less than 1.6 GHZ and single core)

	Small Size	Low Computation Overhead
All Schemes	●	●

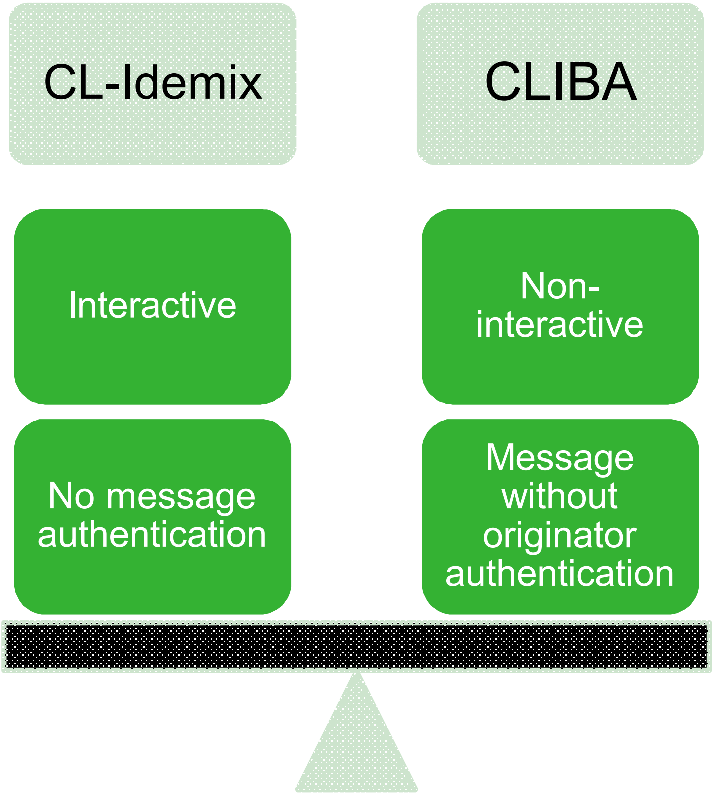
CLIBA (Our Scheme)

- CLIBA : "CL-Idemix based Broadcast Authentication"



CLIBA

- The changes from CL-Idemix to CLIBA



CL-Idemix

CLIBA

Interactive

Non-interactive

No message authentication

Message without originator authentication

Preliminaries (Ctd.)

- Safe prime p, q

  $p = 2p' + 1$,$q = 2q' + 1$, p’ and q’ are also primes
- Special RSA modulus

  n=pq , with p, q safe primes

$$\phi(n) = 4p'q'$$

- Consider the set of quadratic residues modulo n, $QR_n \subseteq Z_n^*$, the size of the set is $\frac{1}{4}\phi(n) = p'q'$

CL Signature

- private key: p, q
- public key: $\{a, b, c\} \in QR_n, n$
- Signature generation

  For message m, choose a prime e, a random number v, and compute

$$A = (a^m b^v c)^{e^{-1} mod\, p'q'}\ mod\ n$$

The signature is (A, e, s)

- Signature verification

  Check that

$$A^e = a^m b^s c$$

- For many messages m_1, …, $m_{L,}$

$$A^e = a_1^{m_1} \ldots a_L^{m_L} b^v c$$

Idemix

- Attributes are the messages m_1, …, m_L in CL signature
- The certificate (A, e, v)

$$A^e = \frac{Z}{{a_1}^{m_1} {a_2}^{m_2} \ldots {a_l}^{m_l} b^v} \qquad (CL:\ A^e = \mathrm{a}_1^{m_1} \ldots \mathrm{a}_L^{m_L} b^v c)$$

Preliminaries : Schnorr’s Identification Scheme

- Non-interactive Schnorr’s Identification

➢ Step1 . P->V :

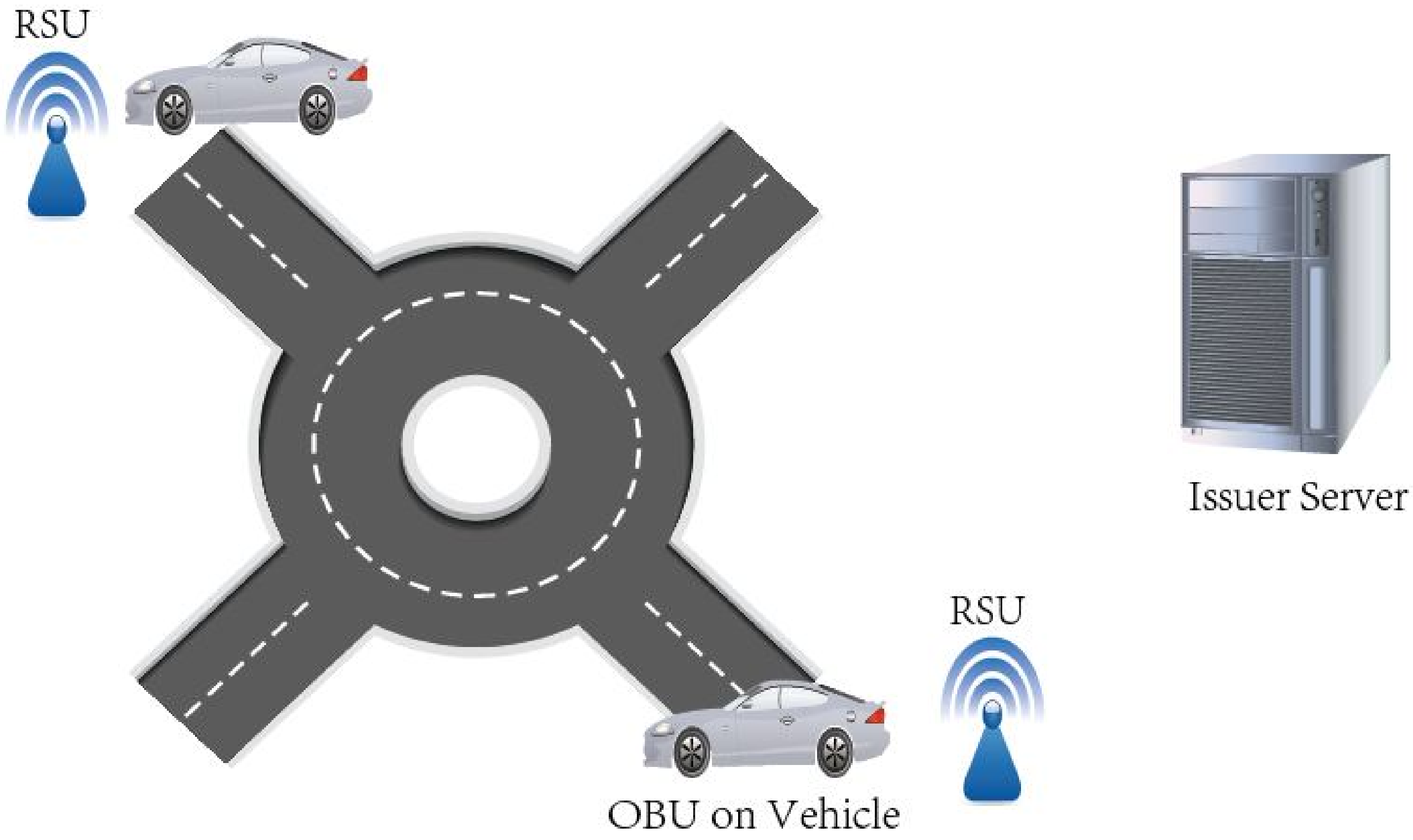
$$c = H(g^r), \qquad s = r + cm$$

➢ Step2. V:

$$t = g^s y^{-c},$$

verify $H(t) == c$

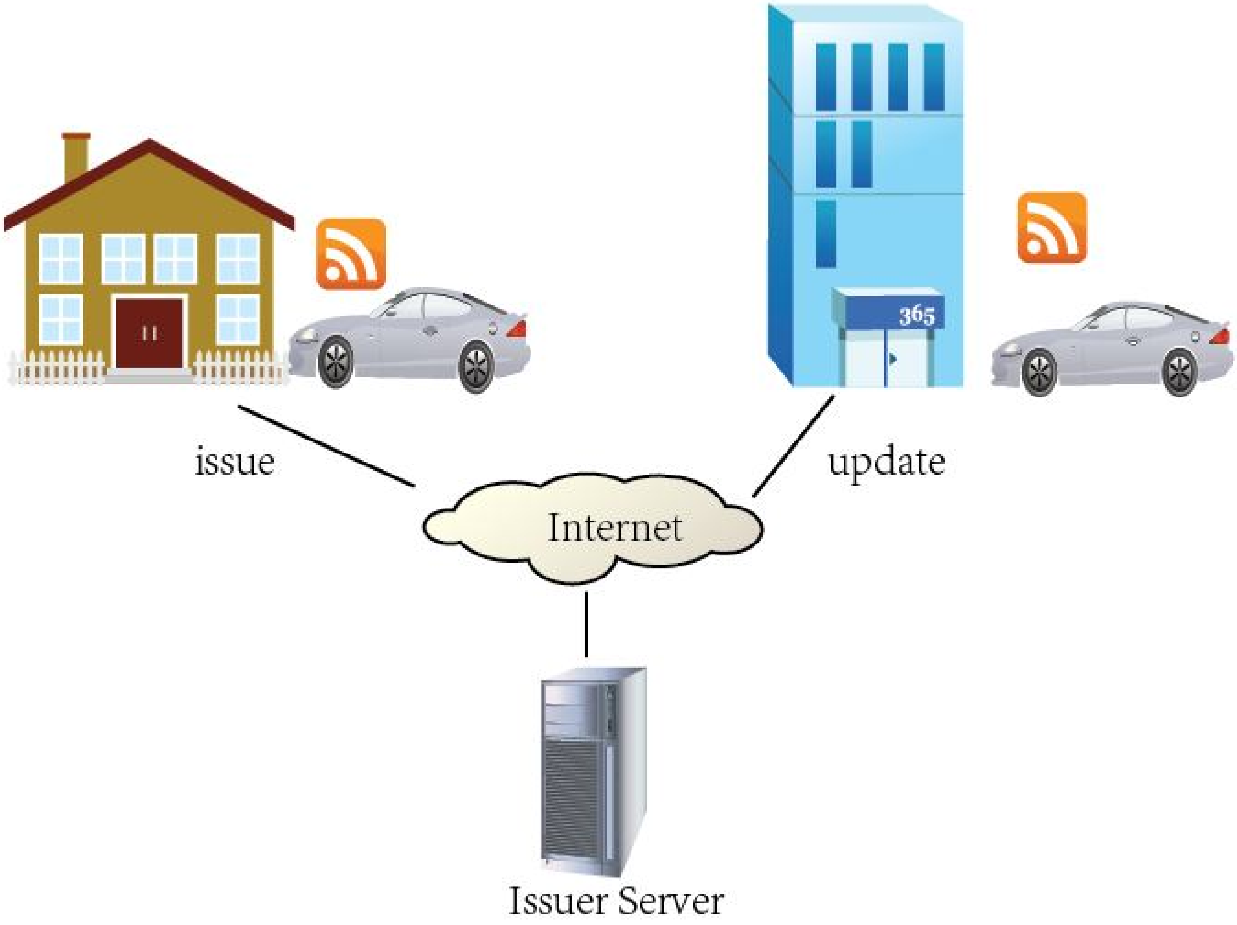
CLIBA System Structure



CLIBA Phases – System Setup

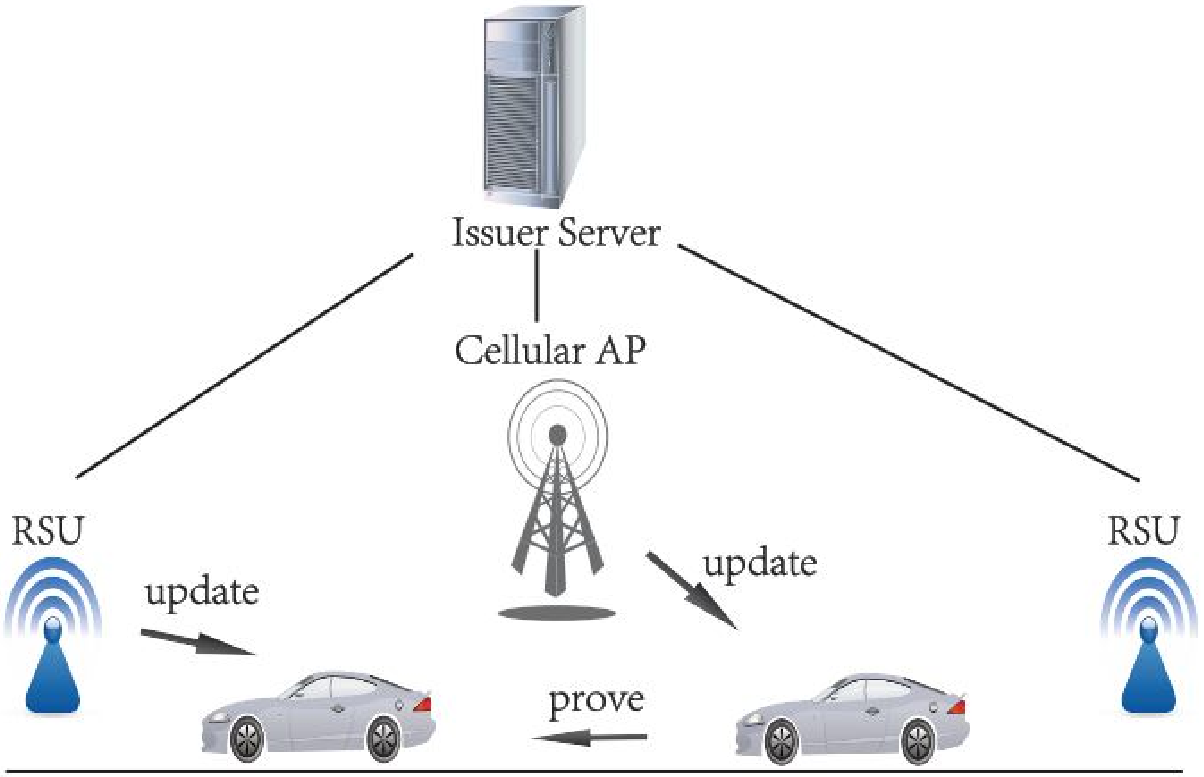
- The issuer generate system parameters randomly
- The issuer select random keys for the underlying CL-Idemix system

CLIBA Phases - Issuance



CLIBA Phases - Issuance

- Issue Without Wifi



CLIBA Phases - Issuance

- Known attributes (A_k) vs Hidden attributes (A_h)

A_k

- vehicle type = car
- vehicle role = private

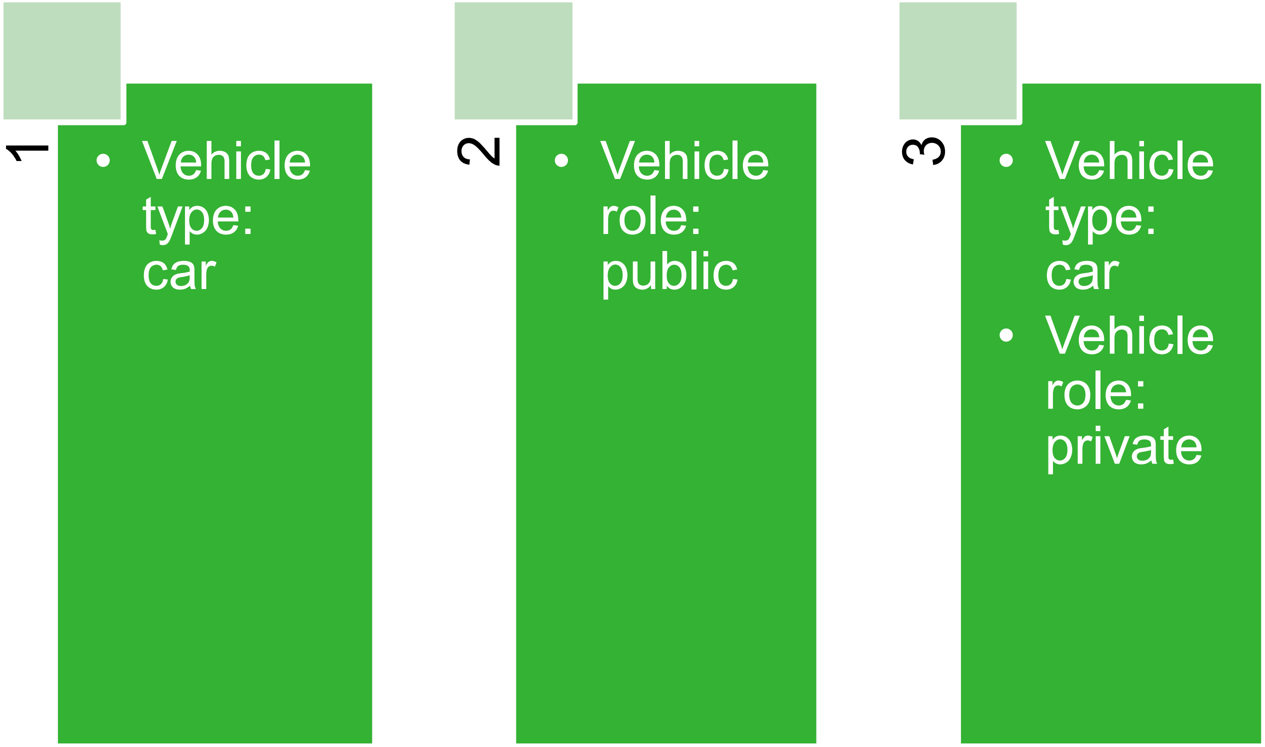
A_h

- Signing key = 0xABCDEF0134590234580ED05803200

EXAMPLE

CLIBA Phases - Verification

- Attribute authentication -- Collective show of attribute values



1

- Vehicle type: car

2

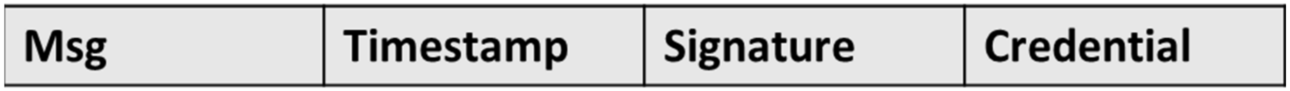
- Vehicle role: public

3

- Vehicle type: car
- Vehicle role: private

CLIBA Phases - Verification

- message format



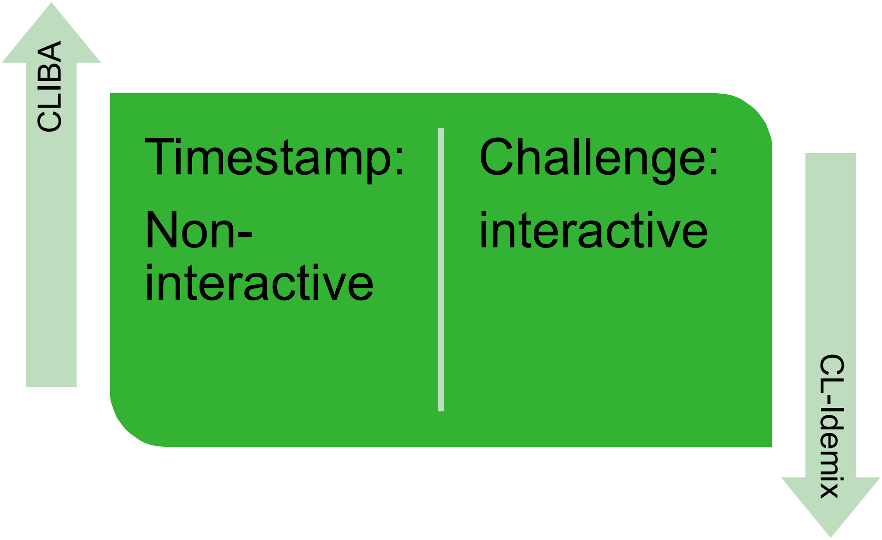
Msg	Timestamp	Signature	Credential

- The message signature $\delta = M^{m_s}$

M = { Msg, Timestamp }

m_s : signing key of the vehicle

Verification – Make the Verification Non-interactive



CLIBA

Timestamp:

Non-interactive

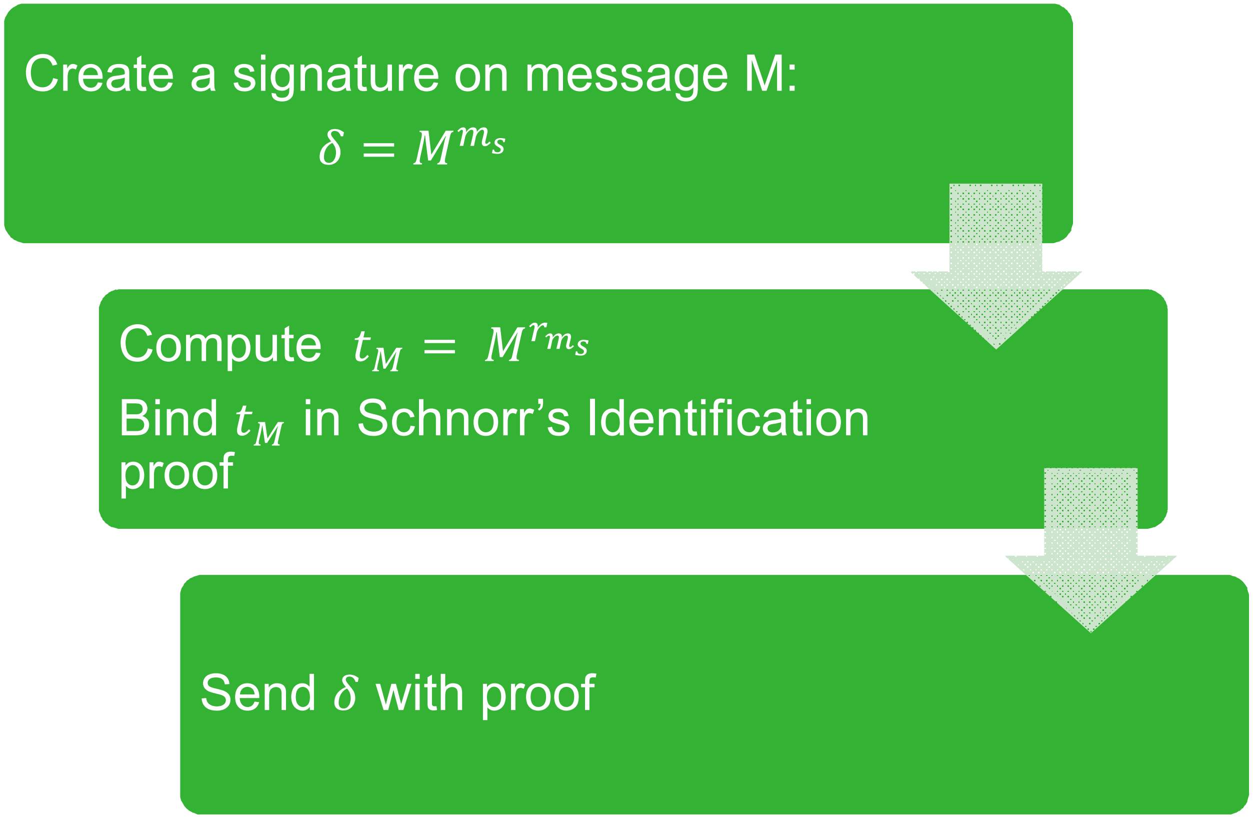
Challenge:

interactive

CL-Idemix

Verification - How to Integrate Message Authentication

- For Prover



Create a signature on message M:

$$\delta = M^{m_s}$$

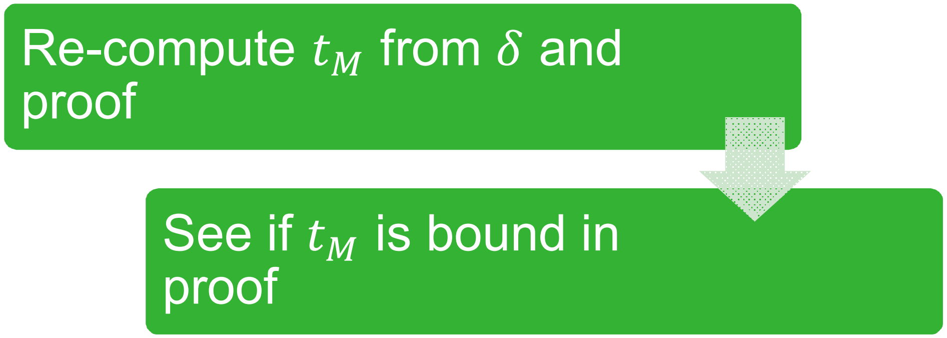
Compute $t_M = M^{r_{m_s}}$

Bind t_M in Schnorr’s Identification proof

Send δ with proof

Verification - How to Integrate Message Authentication

- For Verifier



Re-compute t_M from δ and proof

See if t_M is bound in proof

CLIBA Demo

- Live demo

Performance Issues

- Machine: PC with Core i3 CPU (frequency of 2.13 GHz), and 4GB RAM

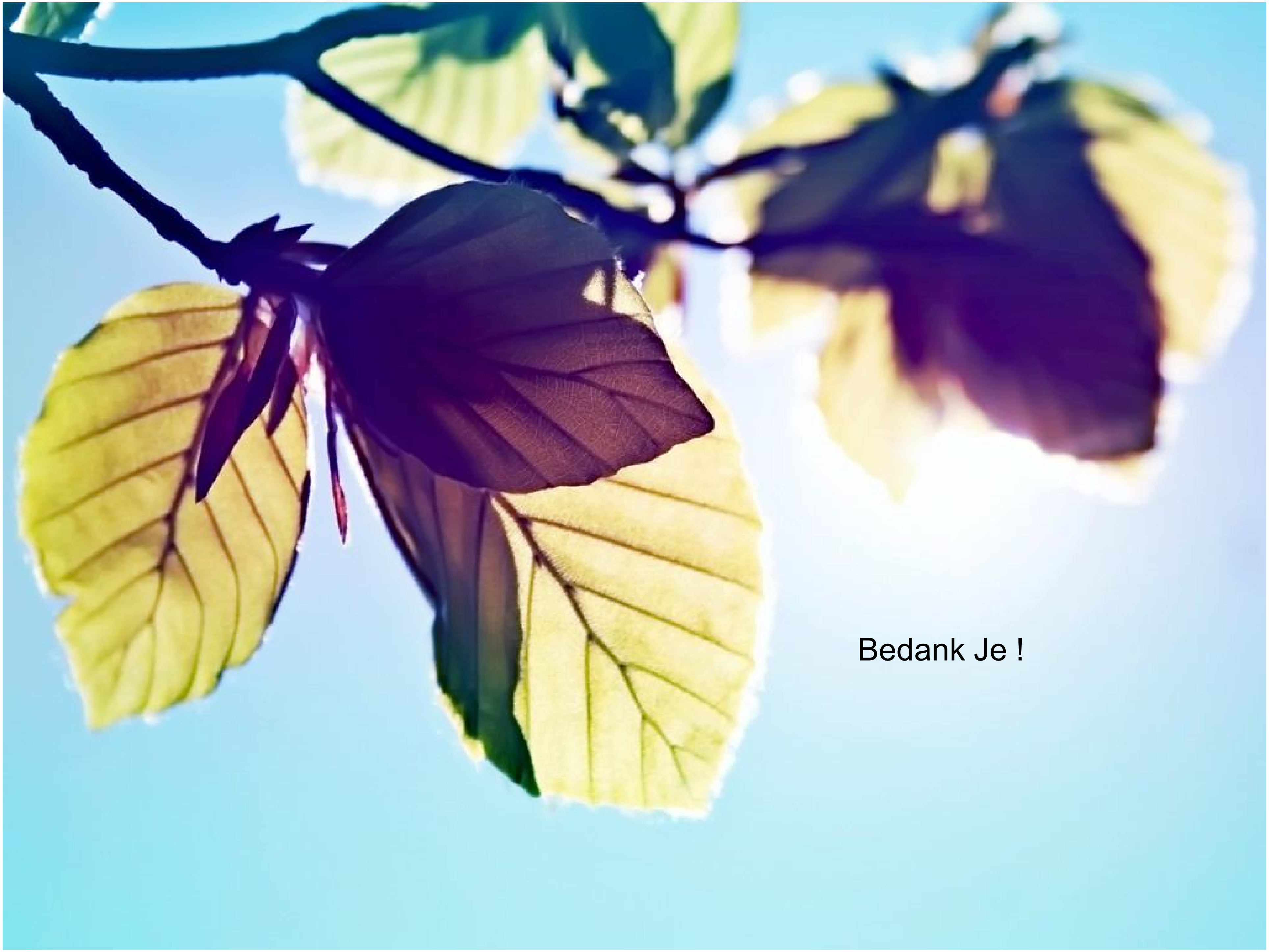
Scenario	Number of Bases in Credential	Process	Average Time	Authentication Information Size
1	2	Sign	64.5ms	1800B
1	2	Verify	45.8ms	-
2	7	Sign	71.5ms	2070B
2	7	Verify	52.4ms	-

CLIBA Conclusion

- Fulfills all basic requirements except the computation time and information size
- Computation time only satisfies signing
- Information size unacceptable

CLIBA Conclusion – Future Work

- Verification speed up
- Authentication information size reduction



Bedank Je !