UNIMORE
UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA

Network-efficient authenticated pseudonym-based V2X communications with constant revocation costs

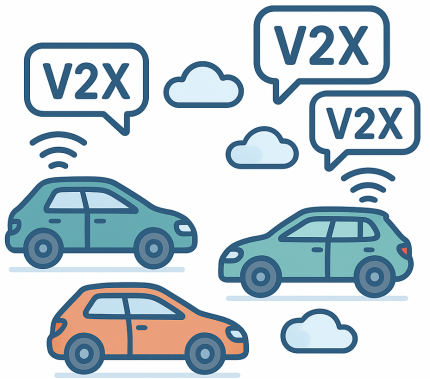
Mattia Trabucco, Giovanni Gambigliani Zoccoli, Mirco Marchetti, and Luca Ferretti
University of Modena and Reggio Emilia
Modena, Italy

23rd IEEE International Symposium on Network Computing and Applications (IEEE NCA 2025)
Lisbon (Portugal), November 5-7th 2025

Intelligent Transportation Systems communications

- Vehicles and infrastructure exchange messages for **road safety**, **traffic management**, and **enhanced mobility**
- Performance:
  - V2X beacon messages are **frequent** and **broadcast**
    → network bandwidth is the major bottleneck

every byte matters!

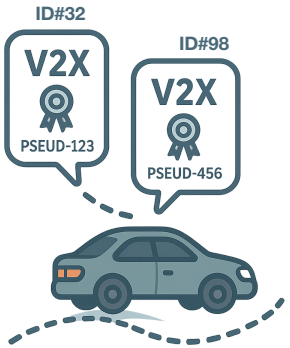


Intelligent Transportation Systems communications

- Vehicles and infrastructure exchange messages for **road safety**, **traffic management**, and **enhanced mobility**
- Performance:
  - V2X beacon messages are **frequent** and **broadcast**
    → network bandwidth is the major bottleneck
    ↳ ***every byte matters!***
- Security:
  - **Message authenticity**
  - **Conditional anonymity**
  - **Efficient revocation**
- Also, carefully balanced with: tight **latency-requirements of safety-related features**, resource constraints of wireless communication protocols, **economic costs**…

PKI-based approach: pseudonyms & linkage values

- Vehicles are provisioned with a **set of pseudonym certificates** issued by a CA
  - **Trade-off: privacy, security and scalability**
  - Full conditional anonymity not affordable in vehicular networks
- Vehicles **rotate pseudonym certificates to prevent tracking**



Protocol framework

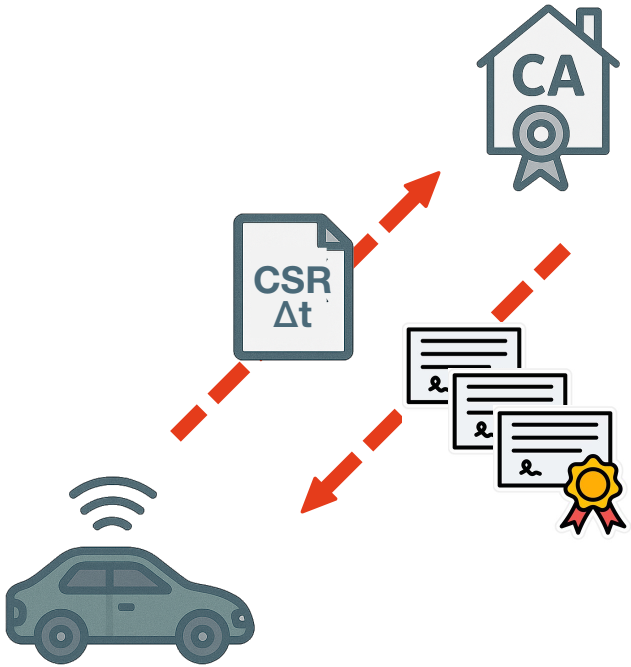
- Three sub-protocols: **pseudonym certificates release**, **revocation**, **refresh**
- Parameters:
  - CA divides time into *time periods* **t**
  - **N** is the maximum fixed number of pseudonym certificates a vehicle can obtain for each time period
  - **T** is the number of subsequent time periods for which a vehicle is requesting sets of pseudonym certificates

Pseudonym certificates release

1) **Request**: Certificate Signing Request from vehicle to CA with the number of future time periods requested Δt, $\Delta t \leq T$

2) **Generation**: the CA creates and sign N pseudonym certificates for each Δt, and sends them to the vehicle

3) **Reception**: the vehicle prepares the set of pseudonym certificates for the current time period, and stores the extra certificates for later use



Revocation

1) The **CA publishes a CRL revoking the misbehaving vehicle**

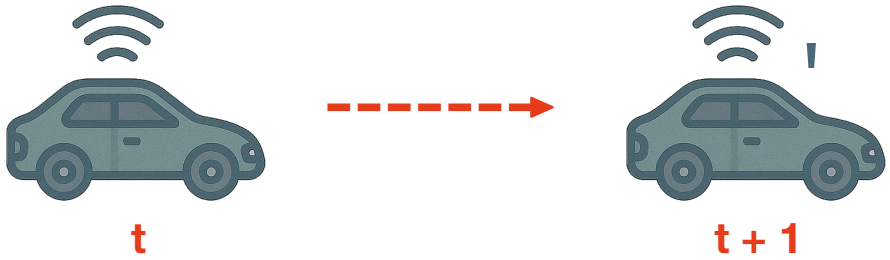
2) A vehicle can **link** all the pseudonym certificates associated with the misbehaving vehicle...

3) … and **discard V2X messages signed with a revoked key**

Refresh

At the end of each time period, the vehicle should:

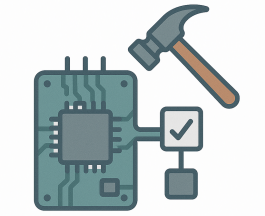
1) **prepare the new set of pseudonym certificates** for the next time period
2) **update the set of revoked pseudonym public keys** for the next time period



Weaknesses of state-of-the-art

- Revocation is not straightforward: standards include **pseudo-random indexing identifiers** within certificates (linkage values)
  - **Trade-off: smaller revocation lists vs bigger per-message overhead**

- **Pseudonym: random key pair + pseudo-random indexing identifier**
  - *Linkage value* is included in each V2X message → network bandwidth is the **major bottleneck** in vehicular networks
  - Depends on hash functions' collision resistance → resizing may be needed in the future to support higher traffic workloads and privacy guarantees



Contributions

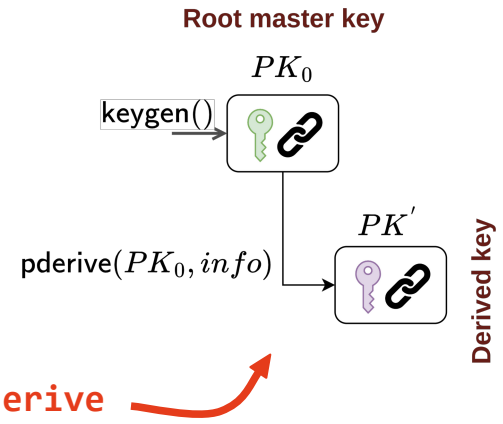
- ***What?*** *Conditionally unlinkable* **pseudo-random** keys in pseudonym certificates
- ***How?*** Pseudonym keys are derived via **Hierarchical deterministic homomorphic Key Derivation** (HKD)
  - Mostly known for deterministic wallets in the context of blockchains (see Bitcoin Improvement Proposal #32)
- ***So?***
  - No linkage values required → **reduced network overhead**
  - Revocation via single master public key → **constant network cost**

Network-efficient HKD-based protocol specification

- *Conditionally unlinkable* pseudo-random keys derived via **Hierarchical deterministic homomorphic Key Derivation (HKD)**
  - Same sub-protocols: **pseudonym certificates release**, **revocation**, **refresh**
  - Same parameters: *time periods*, **N** pseudonym certificates for each time period, **T** subsequent time periods in certificate request

HKD scheme

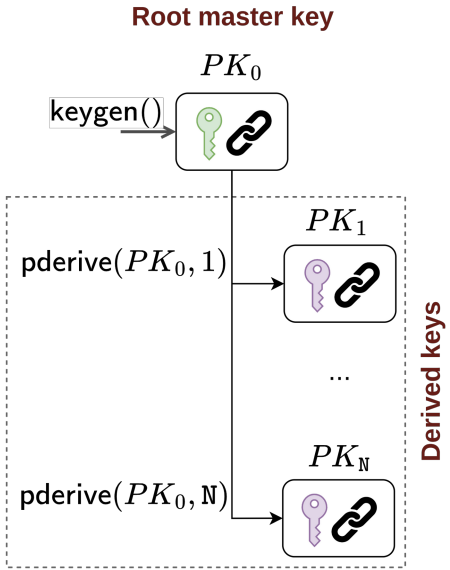
- Three routines
  - **key generation:** `⟨sk,PK⟩ ←$ keygen()`
  - **public key derivation:** `PK' ← pderive(PK,info)`
  - **secret key derivation:** `sk' ← sderive(sk,PK,info)`



Example with `pderive`

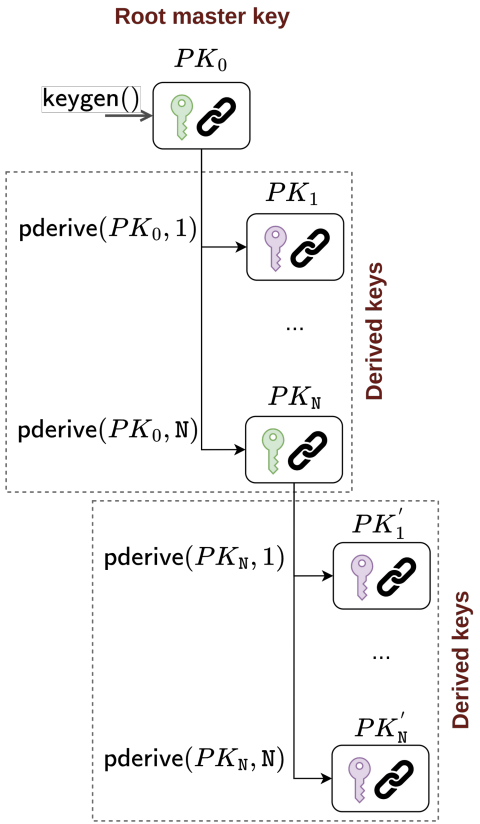
HKD scheme

- Three routines
  - **key generation:** `⟨sk,PK⟩ ←$ keygen()`
  - **public key derivation:** `PK' ← pderive(PK,`*info*`)`
  - **secret key derivation:** `sk' ← sderive(sk,PK,`*info*`)`
- Subsequent calls to **`pderive`** and **`sderive`** allows to derive several key pairs from a single master key pair



HKD scheme

- Three routines
  - **key generation:** `⟨sk,PK⟩ ←$ keygen()`
  - **public key derivation:** `PK' ← pderive(PK,`*info*`)`
  - **secret key derivation:** `sk' ← sderive(sk,PK,`*info*`)`
- Subsequent calls to **`pderive`** and **`sderive`** allows to derive several key pairs from a single master key pair
- *Hierarchical?* A derived key can be used as a master key for further derivation → **hierarchical sub-tree of derived keys** by recursively calling **`sderive`** and **`pderive`** to a derived node

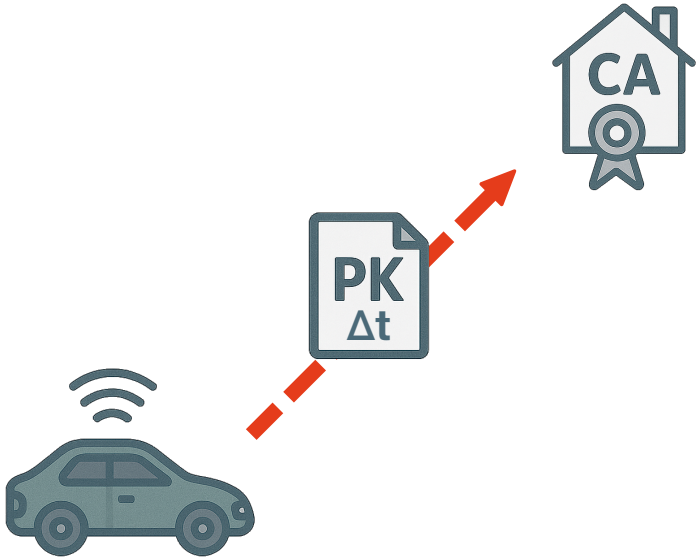


Pseudonym certificates release

1) **Request**: the vehicle sends to the CA its **master public key PK** and the number of future time periods for which is requesting pseudonym certificates Δt, $\Delta t \leq T$

2) Generation

3) Reception

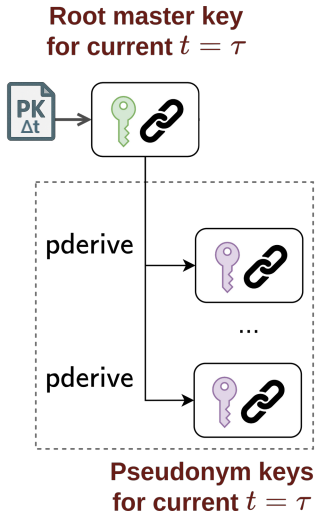


Pseudonym certificates release

1) Request

2) **Generation**: the CA derives N pseudonym public keys using `pderive`. For each subsequent time period derives the next master public key and the N pseudonym public keys. Sends the signatures back to the vehicle

3) Reception

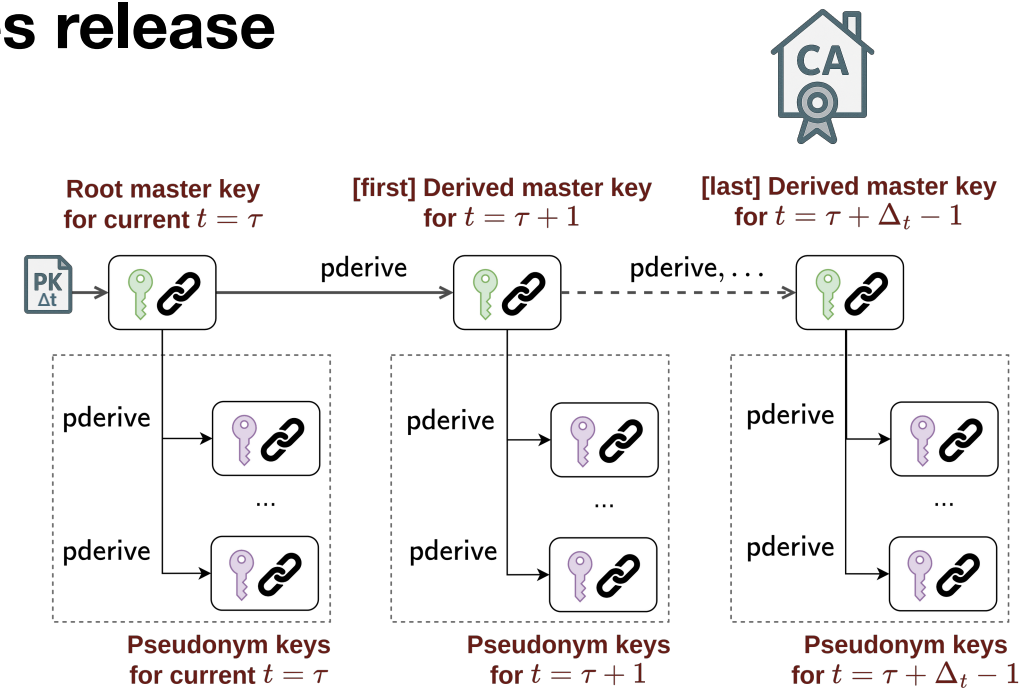


Pseudonym certificates release

1) Request

2) **Generation**: the CA derives N pseudonym public keys using `pderive`. For each subsequent time period derives the next master public key and the N pseudonym public keys. Sends the signatures back to the vehicle

3) Reception

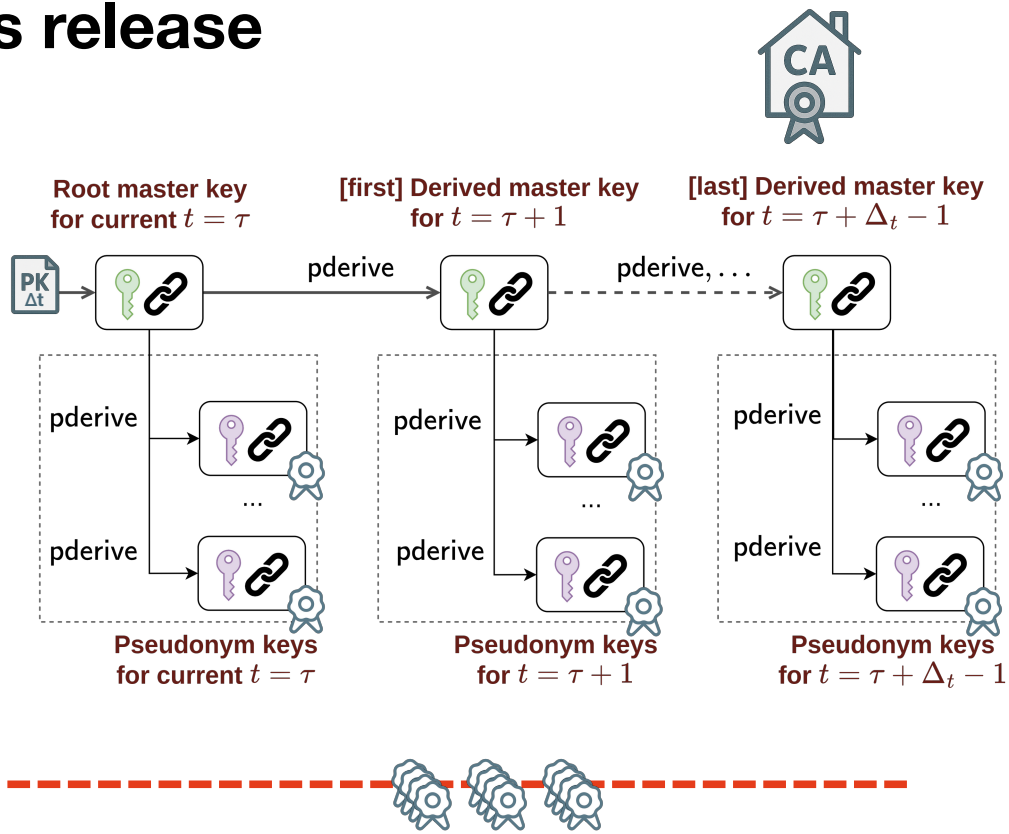


Pseudonym certificates release

1) Request

2) **Generation**: the CA derives N pseudonym public keys using `pderive`. For each subsequent time period derives the next master public key and the N pseudonym public keys. Sends the signatures back to the vehicle

3) Reception

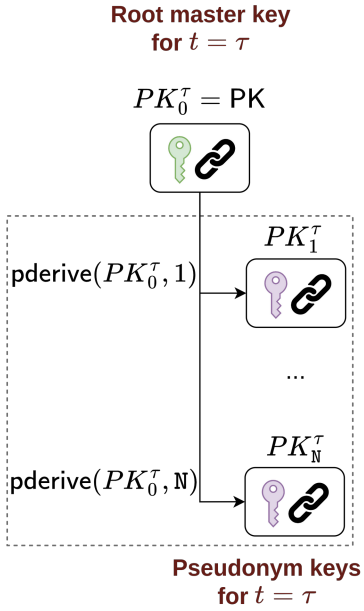


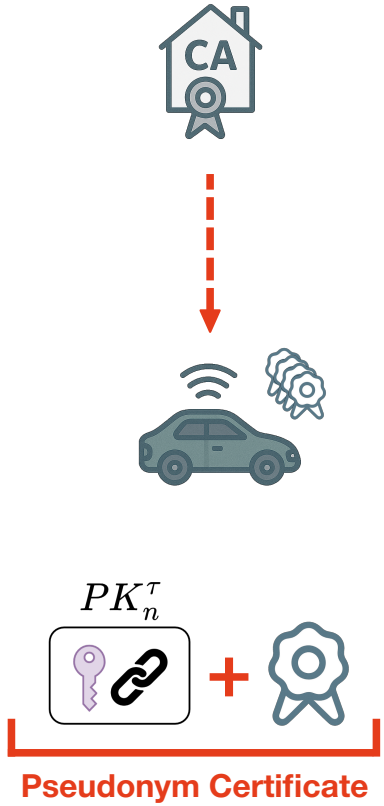
Pseudonym certificates release

1) Request

2) Generation

3) **Reception**: the vehicle derives the pseudonym public keys **only** for the current time period, creates the set of pseudonym certificates for the current time period, and stores the unused signatures for later use



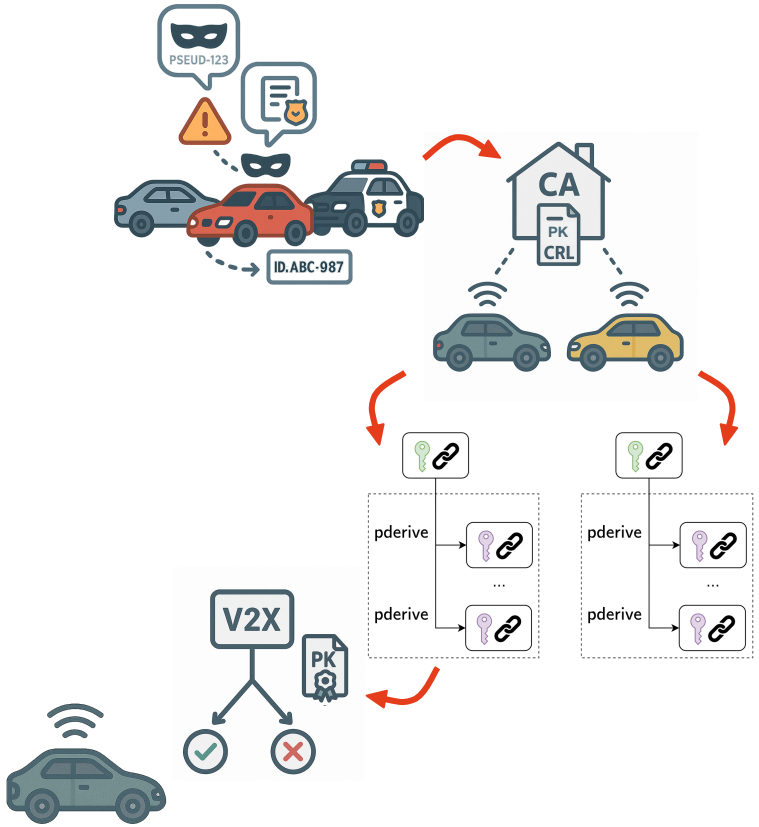


Revocation

1) The **CA revokes the misbehaving vehicle by publishing its master public key**

2) A vehicle can derive all the pseudonym public keys of the misbehaving vehicle using the **`pderive`** routine

3) Discard a received V2X message **if signed with a revoked key**

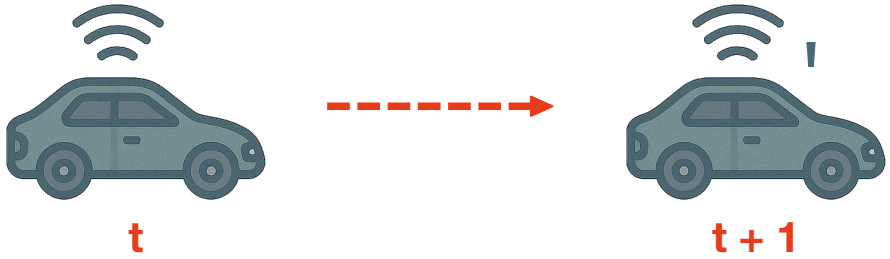


Refresh

At the end of each time period, the vehicle should:

1) **derive the master key pair** for the next time period, **derive all the pseudonym public keys** for the next time period, **create the certificates** (public key + CA signature)

2) **update the set of revoked pseudonym public keys** for the next time period



Cost evaluation: asymptotic analysis

Protocol	Procedure	Computation cost	Made by
Release	pcreq	$O(1)$	Vehicle
	pcrec	$O(\mathtt{N})$	
	pcgen	$O(\mathtt{N} \cdot \mathtt{T})$	CA
Revocation	revoke	$O(1)$ or $O(\mathtt{N})$	
	crlupdate	$O(\mathtt{N})$	Vehicle
Refresh	crtrefresh	$O(\mathtt{N})$	
	crlrefresh	$O(\mathtt{N} \cdot \mathtt{T})$	

CA is less constrained than a vehicle

Computation

Protocol	Network cost
Release	$O(\mathtt{N} \cdot \mathtt{T})$
Revocation	$O(1)$
Refresh	-

Network cost is constant!

Network

Vehicle can derive secret keys on-demand

Type of data	Storage	Storage cost
Pseudonym certificates valid in τ	$\langle crt \rangle$	$O(\mathtt{N})$
Certificates revoked by the CA in τ	$\langle crl \rangle$	$O(\mathtt{N} \cdot \mathtt{T})$
Certificate refresh material	crm	$O(\mathtt{N} \cdot \mathtt{T})$
Revocation refresh material	rrm	$O(\mathtt{N} \cdot \mathtt{T})$

Storage

Cost evaluation: analytic evaluation

Instantiation based on the ECDSA signature scheme with the NIST p-256 elliptic curve.
Standard evaluation scenario: 2.5×10^8 vehicles, N = 40 pseudonym certificates, revocation rate <1%.
Comparison against standards with explicit certificates.

	Network overhead		**Storage overhead**
	V2X message sent	**single CRL downloaded**	**10000 CRL entries**
US **SCMS** standard	Linkage value of **72 bits**	320 bits	3600 Kilobytes
Our proposal	*No extra data*	256 bits	12800 Kilobytes
	reduced network cost	**1.25× smaller**	**~3.5× larger**

Conclusions and future works

- Our novel protocol **reduces network overhead in all V2X messages**, while supporting **efficient revocation at constant network costs**.
- **Higher computational costs for key management are still affordable** in practice and there is **no computational overhead for securing communications**, all under the same cryptographic assumptions of current standards.
- **Future works:**
  - Further optimizations to allow even more efficient certificate management, such as using implicit certificates
  - Application to future V2X communication protocols based on post-quantum cryptography

UNIMORE
UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA

Q&A

Mattia Trabucco, Giovanni Gambigliani Zoccoli, Mirco Marchetti, and Luca Ferretti
↳ *mattia.trabucco@unimore.it*

23rd IEEE International Symposium on Network Computing and Applications (IEEE NCA 2025)
Lisbon (Portugal), November 5-7th 2025