A Privacy-preserving Pseudonym Acquisition Scheme for Vehicular Communication Systems

Andreas Messing
amessing@kth.se

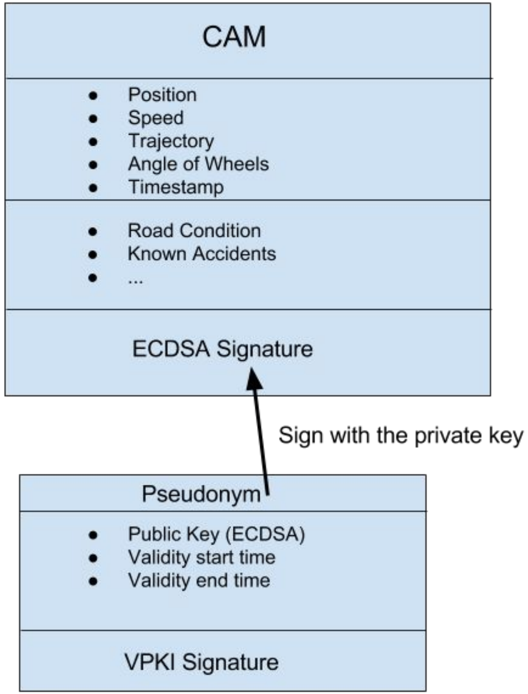
Vehicular Communication Systems

- Smart Cities
- Self-driving Transportation Systems
- Vehicle-to-Vehicle Communication
- Security and Privacy

Cooperative Awareness Message (CAM)

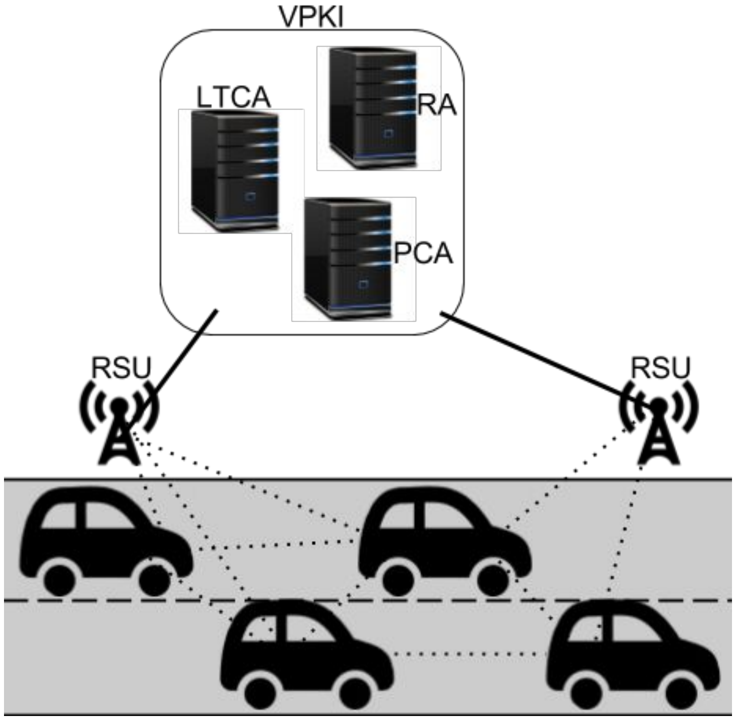
- State of the vehicle
- Environmental information
- Vehicles broadcast 3-10 CAMs per second

- Authenticity, integrity, and non-repudiation
- Pseudonym - anonymous identity
- User privacy
- Trackable during one pseudonym
- Frequently switch to a new pseudonym



Vehicular Public Key Infrastructure (VPKI)

- Root Certificate Authority (RCA)
  - Trust between regions
- Long-Term Certificate Authority (LTCA)
  - Long-Term Certificate
- Pseudonym Certificate Authority (PCA)
  - Pseudonym issuing
- Resolution Authority (RA)
  - Identity Resolution
- Road-Side Unit (RSU)



M. Khodaei, et al., “SECMACE: Scalable and Robust Identity and Credential Management Infrastructure in Vehicular Communication Systems,” in the IEEE TITS, Mar. 2018

Pseudonym Refilling Strategies

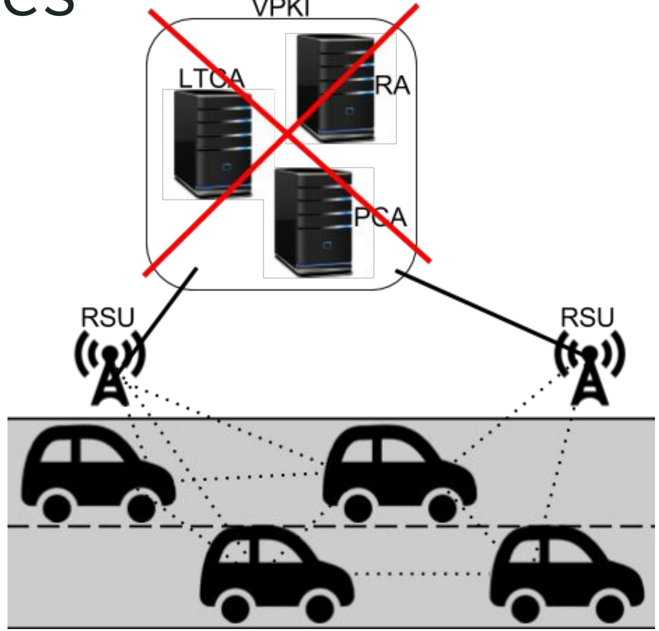
- Preloading schemes
  - Computationally costly, inefficient utilization, cumbersome revocation
- On-demand schemes
  - Efficient in utilization & revocation; effective in fending off misbehavior
  - The more frequent interactions, the more dependent on connectivity

Group Signatures

- Many private keys, one shared public key
- Privacy in the group
- Computationally expensive
- Self-signed pseudonyms

Problem Statement and Challenges

- Unavailability of the VPKI
  - No RSUs in range
  - Cellular network overloaded
  - Denial of Service attacks
- Unable to acquire pseudonyms
- Hybrid scheme[1] (baseline): issuing self-signed pseudonyms
- Vehicles without VPKI pseudonyms would “stand out in a crowd”:
  - Different pseudonym signature and timing information

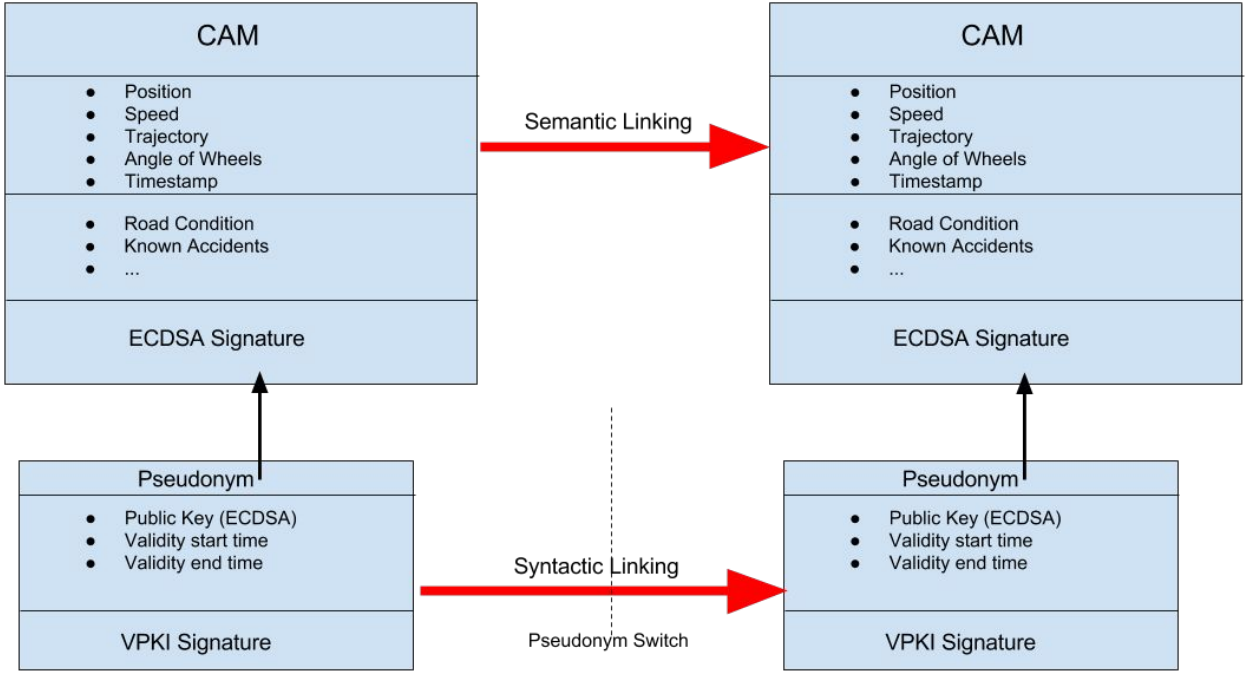


[1] G. Calandriello et al., “On the Performance of Secure Vehicular Communication Systems,” IEEE TDSC, vol. 8, no. 6, pp. 898–912, Nov. 2011.

Linking Attacks

- Linking Pseudonyms
- Syntactic Linking
  - Lifetime
  - Signature
- Solution
  - Aligned Lifetimes
  - Same Signer (PCA)

- Semantic Linking

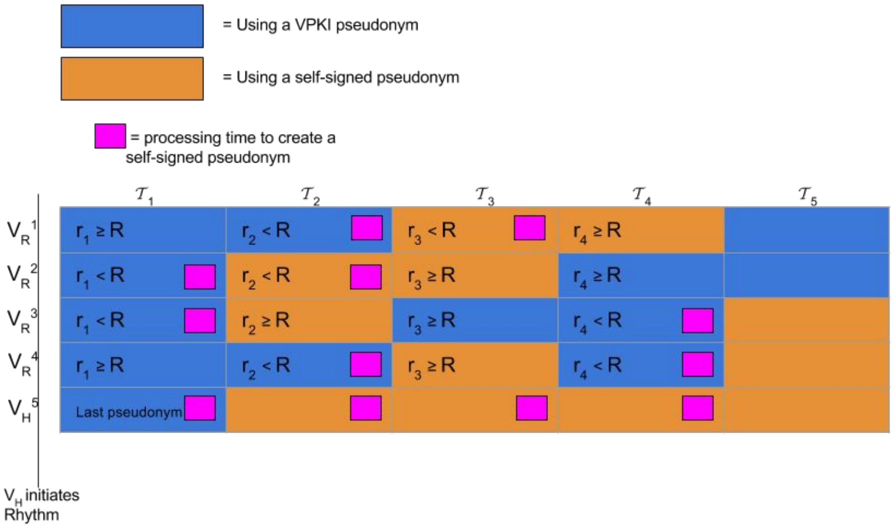


Adversarial Model

- Linking subsequent pseudonyms
- Sybil-based Attacks
- DoS attacks

Rhythm - Randomized Hybrid Scheme To Hide in a Mobile Crowd

- Add Group Manager in every region
  - Self-signed Pseudonyms
  - No Syntactic Linking protection
- Registration Phase
  - Register anonymously with GM
- Align Lifetime to VPKI Pseudonyms
  - Easily obtained information
  - Solved Syntactic Linking based on lifetime
- Solve Syntactic Linking based on signature



🟦 = Using a VPKI pseudonym

🟧 = Using a self-signed pseudonym

🟪 = processing time to create a self-signed pseudonym

	$\mathcal{T}_1$	$\mathcal{T}_2$	$\mathcal{T}_3$	$\mathcal{T}_4$	$\mathcal{T}_5$
V_R^1	🟦 $r_1 \geq R$	🟦 $r_2 < R$ 🟪	🟧 $r_3 < R$ 🟪	🟧 $r_4 \geq R$	🟦
V_R^2	🟦 $r_1 < R$ 🟪	🟧 $r_2 < R$ 🟪	🟧 $r_3 \geq R$	🟦 $r_4 \geq R$	🟦
V_R^3	🟦 $r_1 < R$ 🟪	🟧 $r_2 \geq R$	🟦 $r_3 \geq R$	🟦 $r_4 < R$ 🟪	🟧
V_R^4	🟦 $r_1 \geq R$	🟦 $r_2 < R$ 🟪	🟧 $r_3 \geq R$	🟦 $r_4 < R$ 🟪	🟧
V_H^5	🟦 Last pseudonym 🟪	🟧 🟪	🟧 🟪	🟧 🟪	🟧

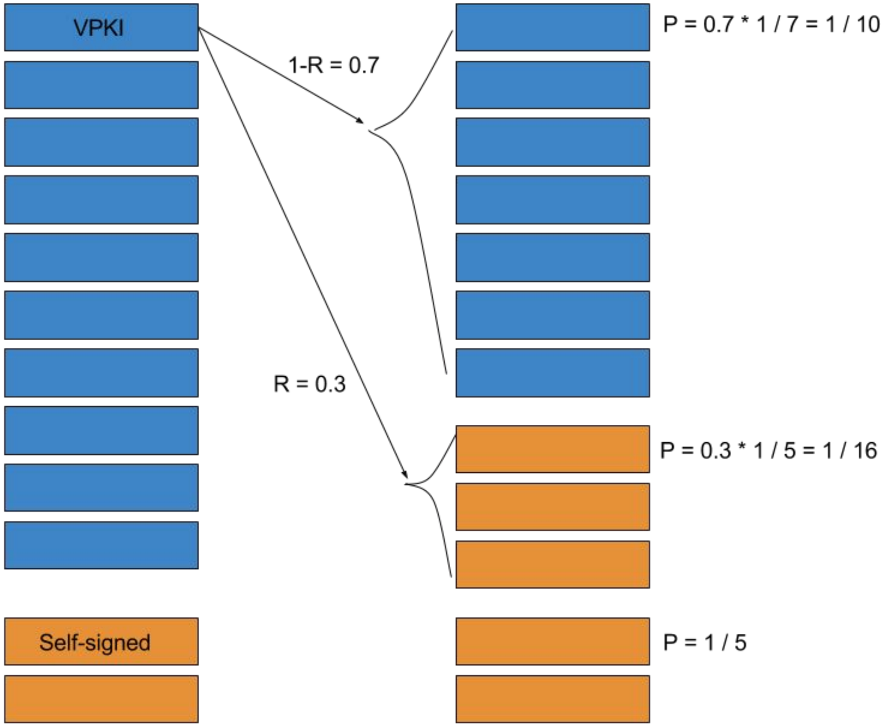
V_H initiates Rhythm

Rhythm - Syntactic Linking Based on Signature

- Every vehicle with a VPKI pseudonym randomly decides to use a self-signed pseudonym

- R = Probability of using self-signed pseudonym in next pseudonym switch

- Decreases the probability of linking a self-signed pseudonym without increasing the probability of linking a VPKI pseudonym



Security Analysis

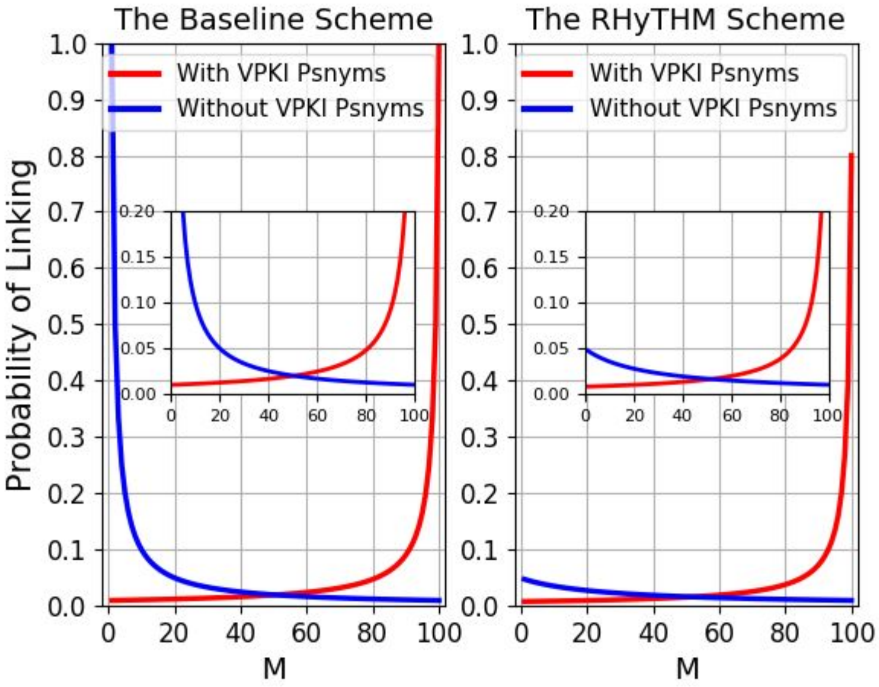
- Authenticity, integrity, and non-repudiation
  - Provided by pseudonyms
- Thwarting Sybil-based Attacks
  - Group signatures can limit the amount of valid signatures that can be made at the same time
  - Hardware Security Module (HSM) ensures signatures under one private key of a single valid pseudonym
- Thwarting Denial of Service (DoS) attack
  - Ignoring Rhythm initiation query if VPKI is reachable
  - Rhythm only lasts while the VPKI is out of reach

Privacy Analysis

- M = Number of vehicles without VPKI pseudonyms

- 100 vehicles, R = 0.2

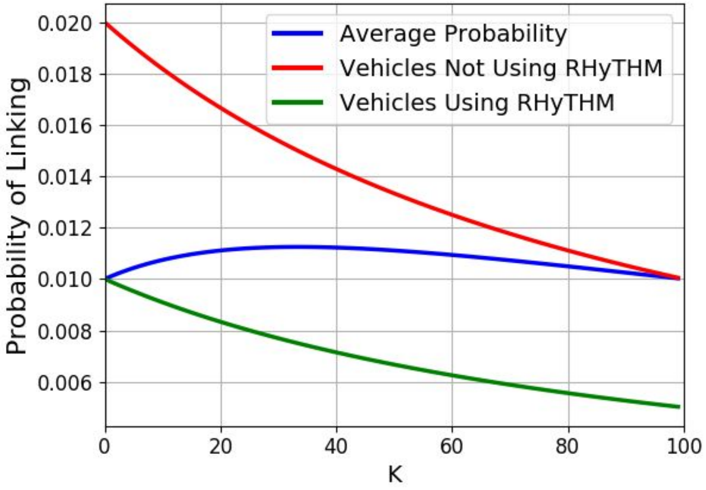
- Metric: Probability of Linking
- significant privacy enhancement
- without affecting privacy of others



Privacy Analysis

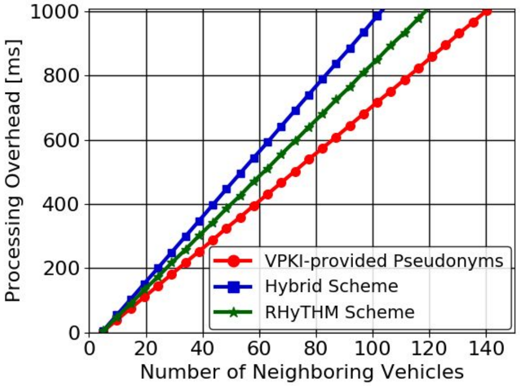
- Linking from VPKI to VPKI
- Linking from self-signed to self-signed

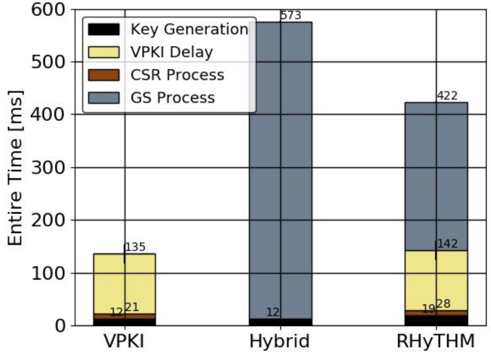
- Vehicles that do not use Rhythm gets slightly increased linkability



Performance Evaluation

- Group Signatures are more than 10x slower
- When R = 0, vehicles can handle 140 neighbors
- When R = 1, vehicles can handle 100 neighbors
- 422 - 135 = 287 ms overhead for 10 pseudonyms
  - R = 0.5
- C, OpenSSL, an implementation of short group signature: Pairings in C





Conclusion + Future Work

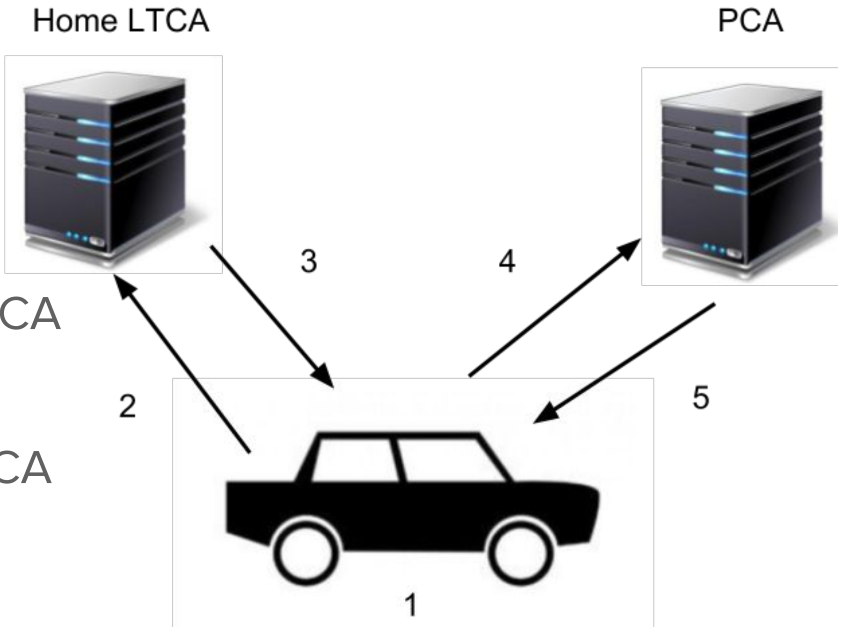
- Using Rhythm, privacy is preserved for vehicles that cannot connect to the VPKI at the cost of a reasonable computation overhead.
- The privacy of vehicles that have VPKI pseudonyms is slightly increased when using Rhythm. The privacy for those that do not use Rhythm is decreased.

- Deciding the optimal value on R is situational and is left as future work.
- How far the initialization query should propagate is left as future work.
- More incentive for vehicles to use Rhythm.

Thank you for listening!

Pseudonym Acquisition

1. Generate key pairs
2. Request token from LTCA
3. Acquire token from LTCA
4. Request a set of pseudonyms from PCA
    a. Send public keys + token
5. Acquire a set of pseudonyms from PCA



M. Khodaei, et al., “SECMACE: Scalable and Robust Identity and Credential Management Infrastructure in Vehicular Communication Systems,” in the IEEE TITS, Mar. 2018

Rhythm - Affect on Semantic Linking

- Semantic Linking is independent of the pseudonym. Rhythm should therefore be compatible with a solution to Semantic Linking.
- Initialization query in a CAM does not make that CAM more linkable.
- A solution to Semantic Linking would make the pseudonyms entirely unlinkable in the system.