Introduction to Connected Vehicle Security

Wireless & IoT Security and Privacy (WISP) Lab

Rochester Institute of Technology, NY, USA

2026

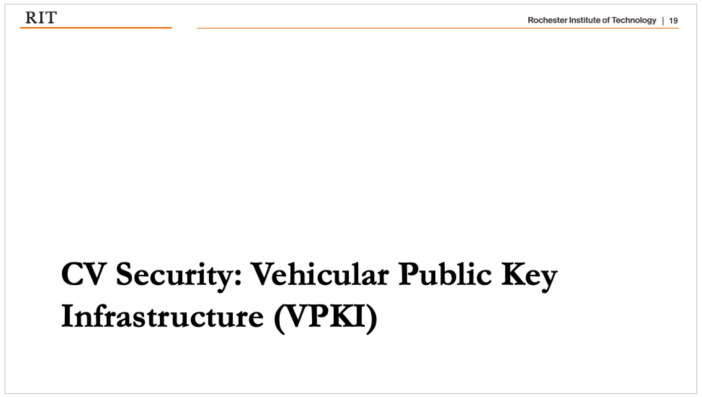
Acknowledgement: This material is based upon work supported by the National Science Foundation (NSF). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the NSF.

Overview


RIT
Rochester Institute of Technology | 3
CV Security: More Technologies, More Threats


RIT
Rochester Institute of Technology | 9
CV Security: Current and Future Protocols


RIT
Rochester Institute of Technology | 13
CV Security: Upper-layer Standards


RIT
Rochester Institute of Technology | 19
CV Security: Vehicular Public Key Infrastructure (VPKI)

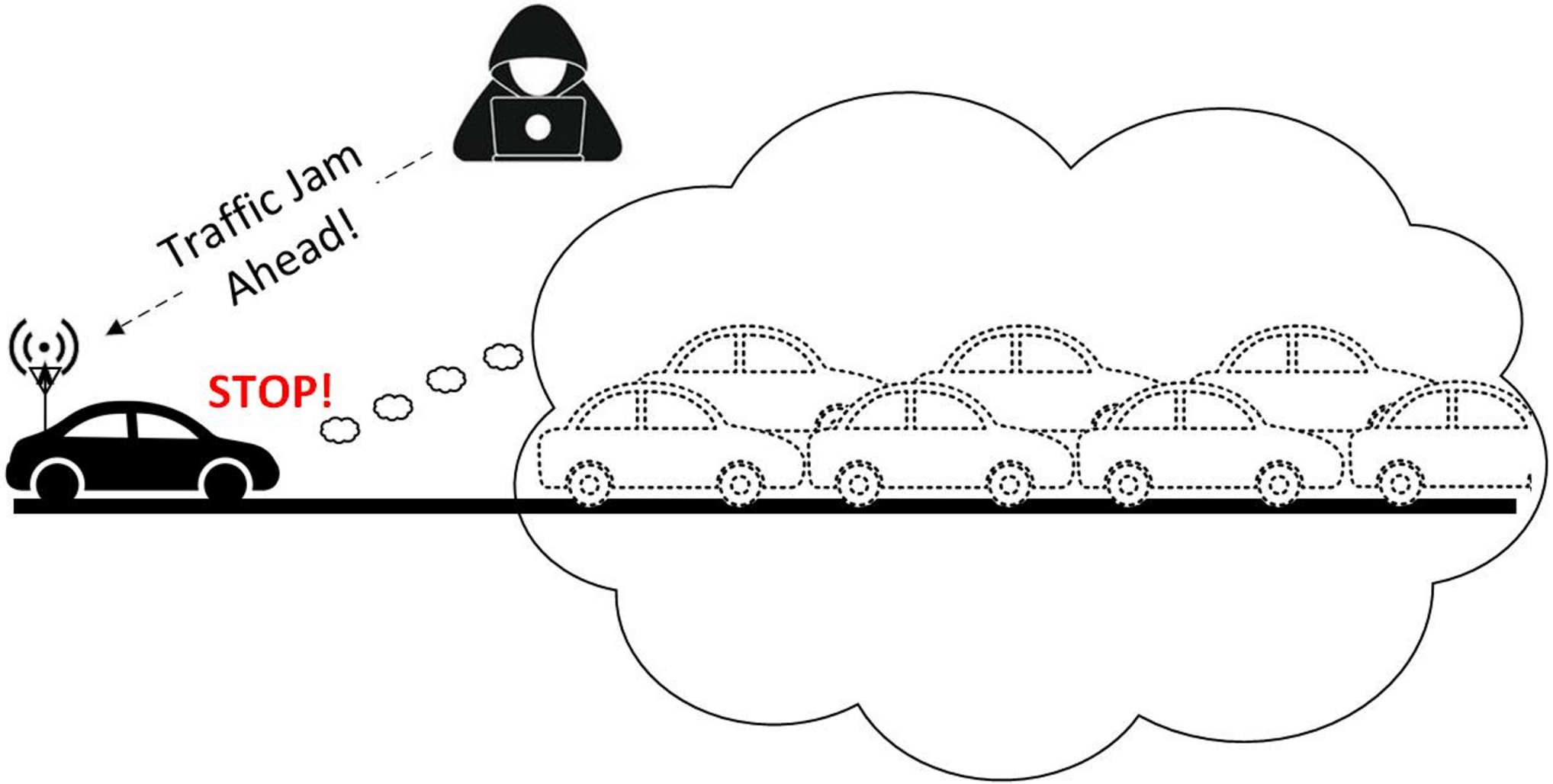

RIT
Rochester Institute of Technology | 25
CV Security: Leveraging V2N

CV Security: More Technologies, More Threats

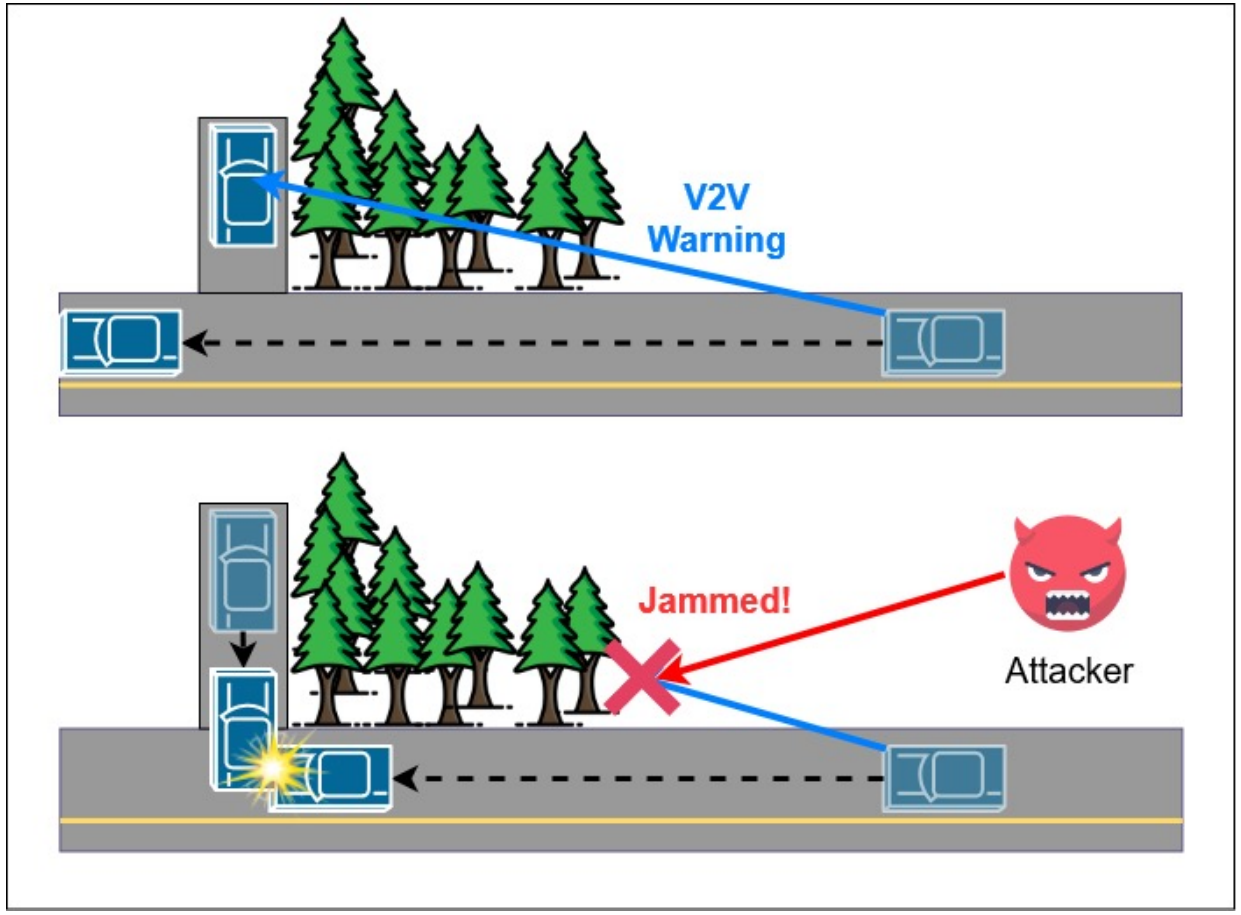
CVs Introduce New Trust Crisis

- Higher connectivity → driving decisions rely more on V2X
  - Drivers might react (swerve, stop, etc.) based on BSM contents
- Attacks against BSMs may be extremely dangerous
  - A single forged/falsified BSM could cause unnecessary, risk maneuvers
  - Denial of Service (DoS) → potential for widespread disruptions
    - Traffic gridlock, manipulation, force road closures
- Privacy considerations
  - Vehicle tracking = driver tracking

BSM Spoofing Attack



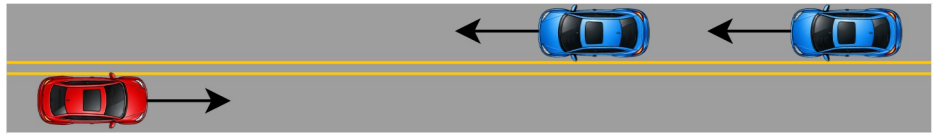
BSM Jamming (DoS) Attack



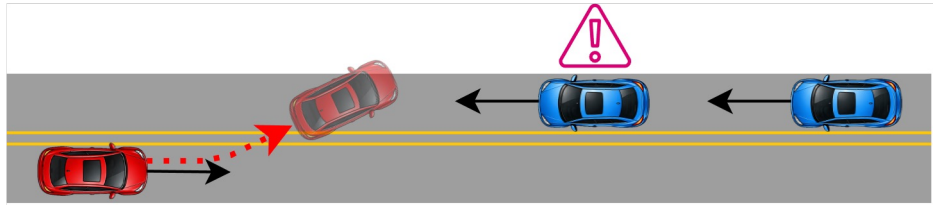
Geoff Twardokus and Hanif Rahbari, "Towards Protecting 5G Sidelink Scheduling in C-V2X Against Intelligent DoS Attacks," *IEEE Transactions on Wireless Communications* (TWC), vol. 22, no. 11, pp. 7273-7286, November 2023.

BSM Falsification Attack (Misbehavior)

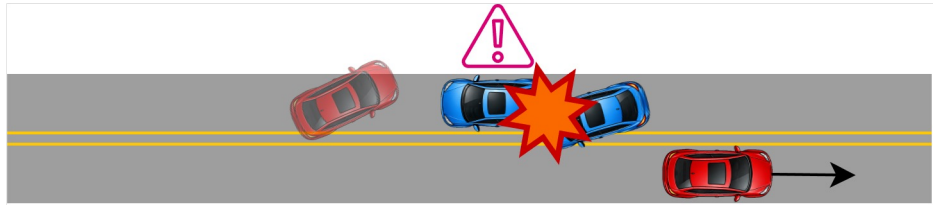
1. Attacker (red) approaches victims



2. Attacker sends false lane departure warning in a BSM



3. Oncoming victim reacts with emergency brake, causing a crash



The Pillars of V2V Trust

1. Authentication — verify messages are from trustworthy and legitimate devices with acountability
2. Integrity — verify messages are not modified between sender and receiver
3. Detect and remove misbehaving units
4. Protect privacy — no unnecessary tracking
5. Security must persist for vehicle lifetime (~15 years)

CV Security: Current and Future Protocols

V2V Security Status Quo

- Limited Scope: V2V standards cover only PHY; no built-in security
  - No authentication → replay, machine-in-the-middle attacks
  - No integrity checks → message modification/tampering attacks
  - Jamming attacks are well-known (e.g., for 802.11p) and highly effective
- Possible physical-layer security (PLS) techniques for NextGen V2X
  - Advanced capabilities (multiple antennas, intelligent surfaces)
- Security still external (3GPP: no BSM security for NR-V2X)
  - Implication: Security (encryption, authentication) pushed to upper layers

"There are no particular procedures defined for securing the NR based PC5 broadcast mode."

Cellular is Secure – Why Isn't C-V2X?

- C-V2X Sidelink skips the SIM or network attachment entirely
- Zero built-in security in Sidelink Modes (1 and 2)
  - → No SIM or network attachment
  - ∴ No authentication, integrity checking, or encryption
- However, there are privacy benefits from not having a SIM (Subscriber Identification Module)

CV Security: Upper-layer Standards

V2V Security Standards Suite (US)

- IEEE 1609.2 (rev. 2022) for secure message exchange
  - Protection from eavesdropping, spoofing, alteration, replay, …
  - New draft (P1609.2-2025) currently being finalized
- Privacy is protected with pseudonymous identification
  - CVs are anonymous to each other and outsiders, identifiable (only) by authorized linkage authorities
- 1609.2.1 (rev. 2022) – Cert. Mgmt. for End Entities
  - How to request and receive certificates on vehicles, RSUs, etc.
  - New draft (P1609.2.1-2026) current being finalized

IEEE 1609.2-2022

- Digital signatures for authentication and integrity
  - Elliptic Curve Digital Signature Algorithm (ECDSA)
- Signatures are authenticated with certificates
  - IEEE 1609.2.1
  - Requires vehicular public key infrastructure (VPKI)
- Non-US standards, such as *ETSI TS 103 097* for EU, are often based on IEEE 1609.2 with specific adjustments (like passive revocation)

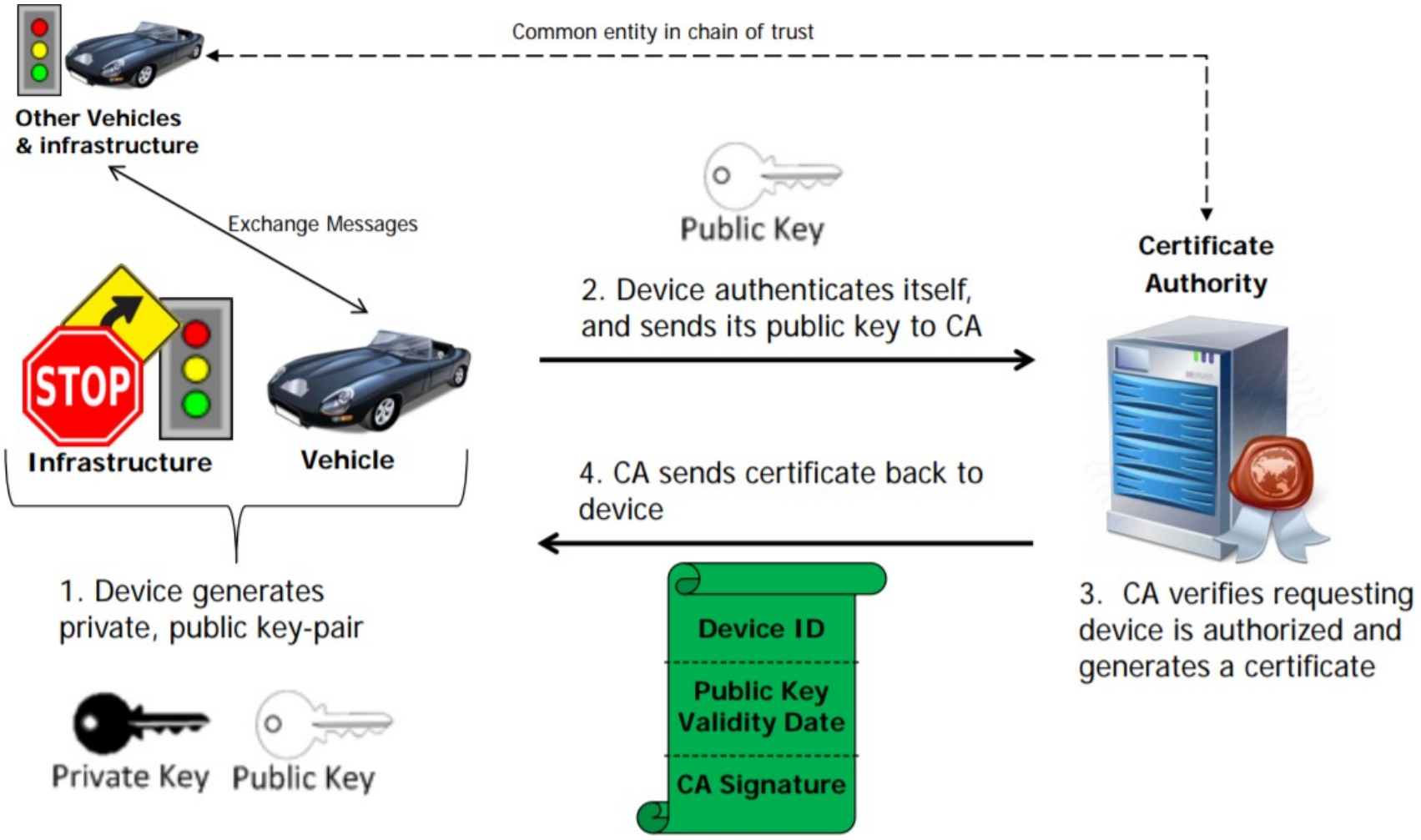
Emerging Threats

- ECDSA signatures are vulnerable to quantum attacks
- Quantum-resistant cryptography (QRC) could replace ECDSA
  - Mainstream QRC has too much overhead[1] for easy use in C-V2X
  - Crypto agility
- AI-enhanced and AI-enabled attacks and defenses
  - AI can identify new intrusions, streamline attack execution
  - Increasing use of AI for V2V performance creates vulnerabilities to poisoning, injection, and other adversarial machine learning techniques

[1]Geoff Twardokus, Nina Bindel, Hanif Rahbari, and Sarah McCarthy, "When Cryptography Needs a Hand: Practical Post-Quantum Authentication for V2V Communications," *Network and Distributed System Security Symposium* (NDSS 2024), San Diego, CA, Feb. 2024.

CV Security: Vehicular Public Key Infrastructure (VPKI)

VPKI Architecture



U.S. Department of Transportation

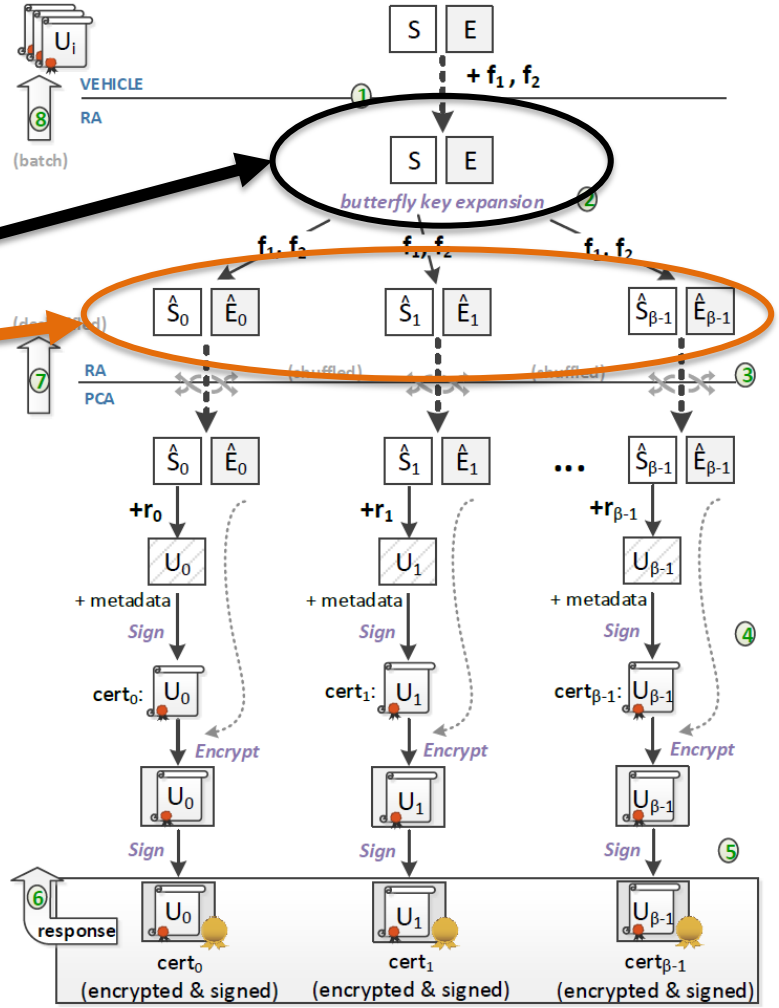
VPKI - The Problem of Scale

- ~297 million registered vehicles in the US in 2024
  - Each vehicle requires ~1,040 certificates/year
  - 100% adoption → Tsunami of 308.8 billion certificates annually!
  - This is just for vehicles – even more certs needed for V2I, V2N
  - Efforts taken to address this are untested (but promising)
    - Batch verification schemes[1], blockchain[2], and more.
- Who will manage the certificates?
  - Plans tend to be bloc- or nation-specific (E.U., U.S., China, …)
  - What about driving internationally?

[1]J. Huang et al, "ABAKA: An Anonymous Batch Authenticated and Key Agreement Scheme for Value-Added Services in Vehicular Ad Hoc Networks," *IEEE Trans. Vehicular Technol.,* vol. 60, no. 1, pp. 248–262, Jan. 2011.
[2]L. Wei et al, "Blockchain-Based Asynchronous Authentication and Key Agreement Scheme for Securing VANETs," *IEEE Trans. Dependable and Secure Computing*, vol. 23, no. 3, pp. 6964–6979, May-June 2026.

Addressing the Problem of Scale

- Instead of preloading 1,000+ keys per vehicle, preload some to derive others
- Butterfly keys use one seed keypair to derive all future keys
- Significantly reduce overhead
  - Reduce # of required key reloads
  - Make the VPKI scalable
- *Still requires managing revocation for all possible derived pseudonyms



M. A. Simplicio, E. L. Cominetti, H. K. Patil, J. E. Ricardini and M. V. M. Silva, "The Unified Butterfly Effect: Efficient Security Credential Management System for Vehicular Communications," *2018 IEEE Vehicular Networking Conference (VNC)*, 2018

Protecting Privacy in V2V

- V2V messages are broadcast and (usually) unencrypted
  - Easy to track a vehicle and its driver(s), e.g., location, behavior analysis
- Using one certificate to sign messages is bad in the long term
- 1609.2 requires pseudonym certificates instead
  - Short-term certificates derived from private-key certificate
  - Cannot be linked to vehicle's real, permanent identity
  - Pseudonym certificate rotates every 5 minutes (or can be event-driven)
- Risk: Access to multiple active identities allows "Sybil" attacks, swarming an intersection

Misbehavior and Revocation

- VPKIs must support removing vehicles from the system as needed
  - Ex: IEEE 1609.2.1 supports certificate revocation lists (CRLs)
- No single misbehavior detection algorithm, but many approaches
  1. Plausibility checks
     - Ex: if a vehicle claims moving 300 miles in ten seconds, flag as suspicious
  2. Trust and reputation management
     - Continuously increase or decrease trust in a vehicle, revoke below threshold
  3. Cooperative consensus
     - X% of vehicles in a region can vote to evict a problematic participant

CV Security: Leveraging V2N

C-V2X Network Mode Security

- V2N mode can leverage LTE/NR security mechanisms
  - Evolved Packet System Authentication and Key Agreement (EPS-AKA)
  - Authentication, integrity checking, and encryption provided
- Privacy loss from attachment to LTE network (+ added latency)
- Still vulnerable to conventional cellular attacks
  - LTE: IMSI catching, GUTI disclosure, ...
  - Privacy concerns are especially prevalent

V2N Security in NR-V2X

- Privacy is emphasized more than LTE-V2X
  - Concealed and/or encrypted identifiers
- Primary and secondary authentication
  - Support 3rd party application bootstrapping and integration
- Communication with non-cellular networks
  - Cross-technology communication (Wi-Fi, IoT, …)

Trusted Non-3GPP Access

- Allow devices to securely contact the 5G Core network via non-cellular protocols
- Centralize authentication processes in 5G Core
- Improved V2I and V2D device diversity
  - Non-cellular devices (e.g., IoT) can act as RSUs
- EAP-AKA or 5G-AKA can be used for authentication

Secondary Authentication

- AKMA – Authentication and Key Management for Applications
  - For third-party applications and 3GPP services
  - Use cellular authentication to bootstrap application-layer security/key derivation (generic bootstrapping architecture – GBA)
- Eliminate the need for massive PKI or hard-coded credentials
  - Greatly reduce complexity of VPKI design and deployment

Security Post-Mortem and Future Path

The Future of V2V Trust: VPKI vs. AKMA

VPKI: The Certificate Tsunami

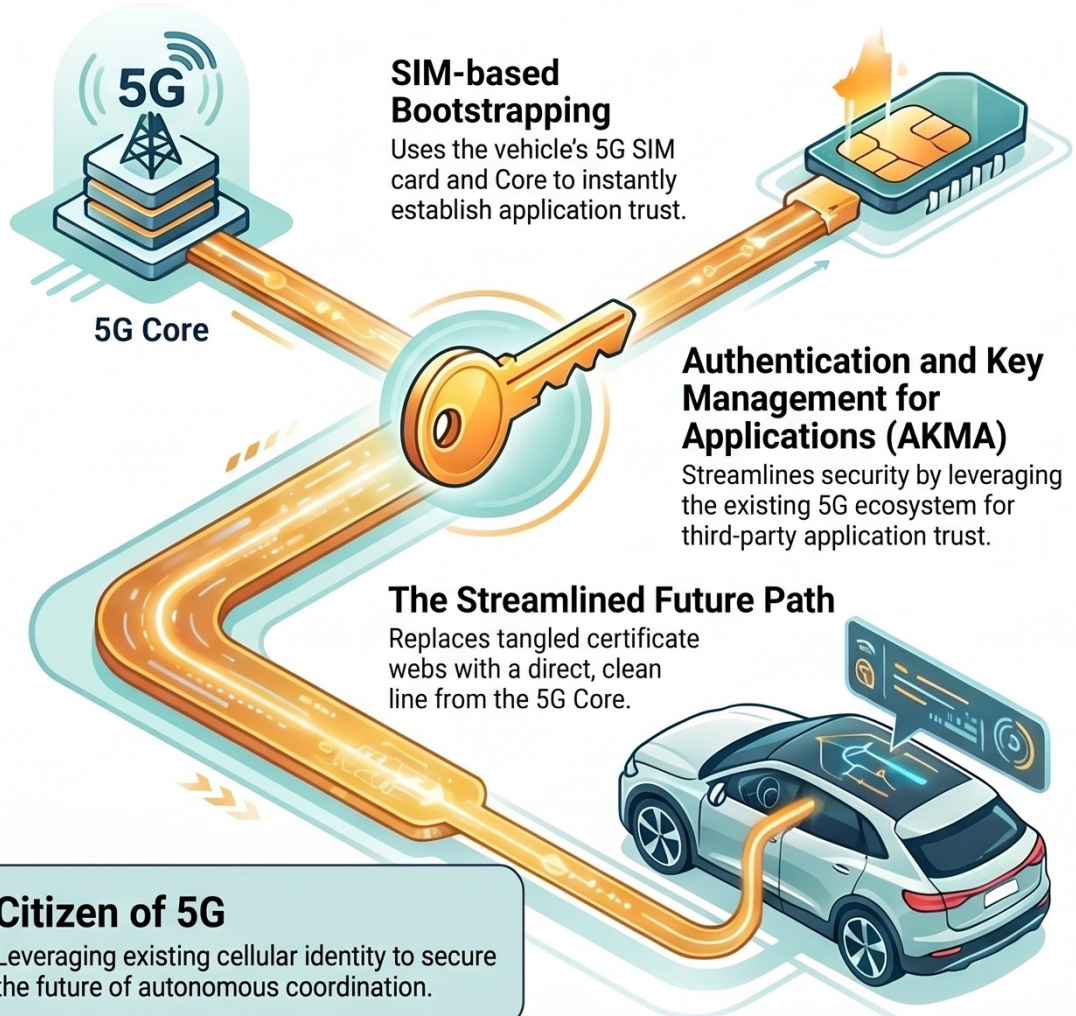
308.8 Billion
Certificates Annually
Estimated volume required to support ~297 million vehicles in the U.S. under VPKI.

The Problem of Scale
Managing massive certificate volumes and revocations creates overwhelming administrative overhead for national infrastructures.

Administrative Overhead
VPKI requires complex management of peeudonym certificates to ensure driver privacy.

Simplifying the Tsunami
AKMA eliminates the need for massive, hard-to-scale VPKI infrastructures.

AKMA: The 5G Golden Key



SIM-based Bootstrapping
Uses the vehicle's 5G SIM card and Core to instantly establish application trust.

Authentication and Key Management for Applications (AKMA)
Streamlines security by leveraging the existing 5G ecosystem for third-party application trust.

The Streamlined Future Path
Replaces tangled certificate webs with a direct, clean line from the 5G Core.

Citizen of 5G
Leveraging existing cellular identity to secure the future of autonomous coordination.

We just covered:

For questions or to provide feedback on the content, please reach out to Hanif Rahbari (hanif.rahbari@rit.edu) or Geoff Twardokus (twardokg@gvsu.edu)