



When Cryptography Needs a Hand: Practical Post-Quantum Authentication for V2V Communications

Geoff Twardokus



Nina Bindel



Hanif Rahbari



Sarah McCarthy



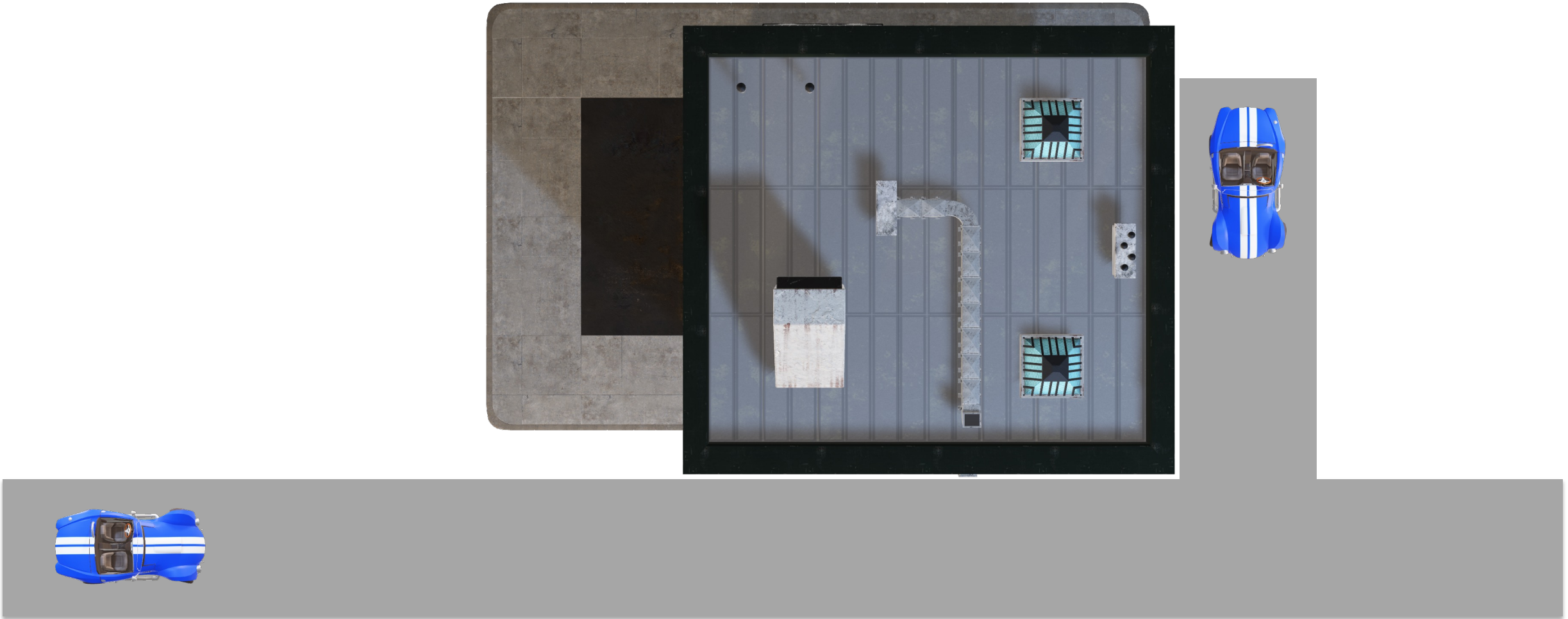
Vehicle-to-Vehicle (V2V) Communication

Direct wireless communication between vehicles for safety could **prevent 600,000 car crashes** every year¹

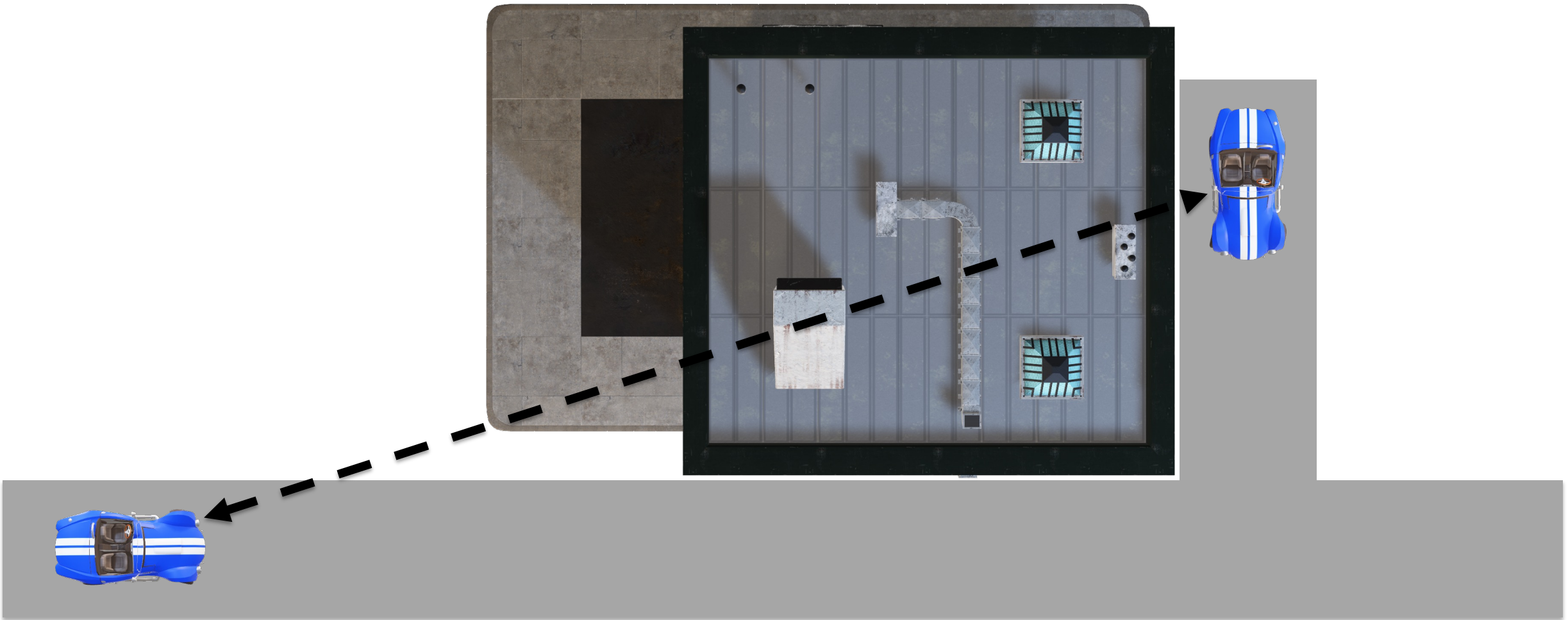
Extremely delay-sensitive (100 – 500ms)

¹National Highway Transportation Safety Administration (NHTSA), “Federal Motor Vehicle Safety Standards; V2V Communications,” Notice of Proposed Rulemaking (NPRM) for FMVSS No. 150, V2V Communications; 88 FR 80685, Nov. 2023.

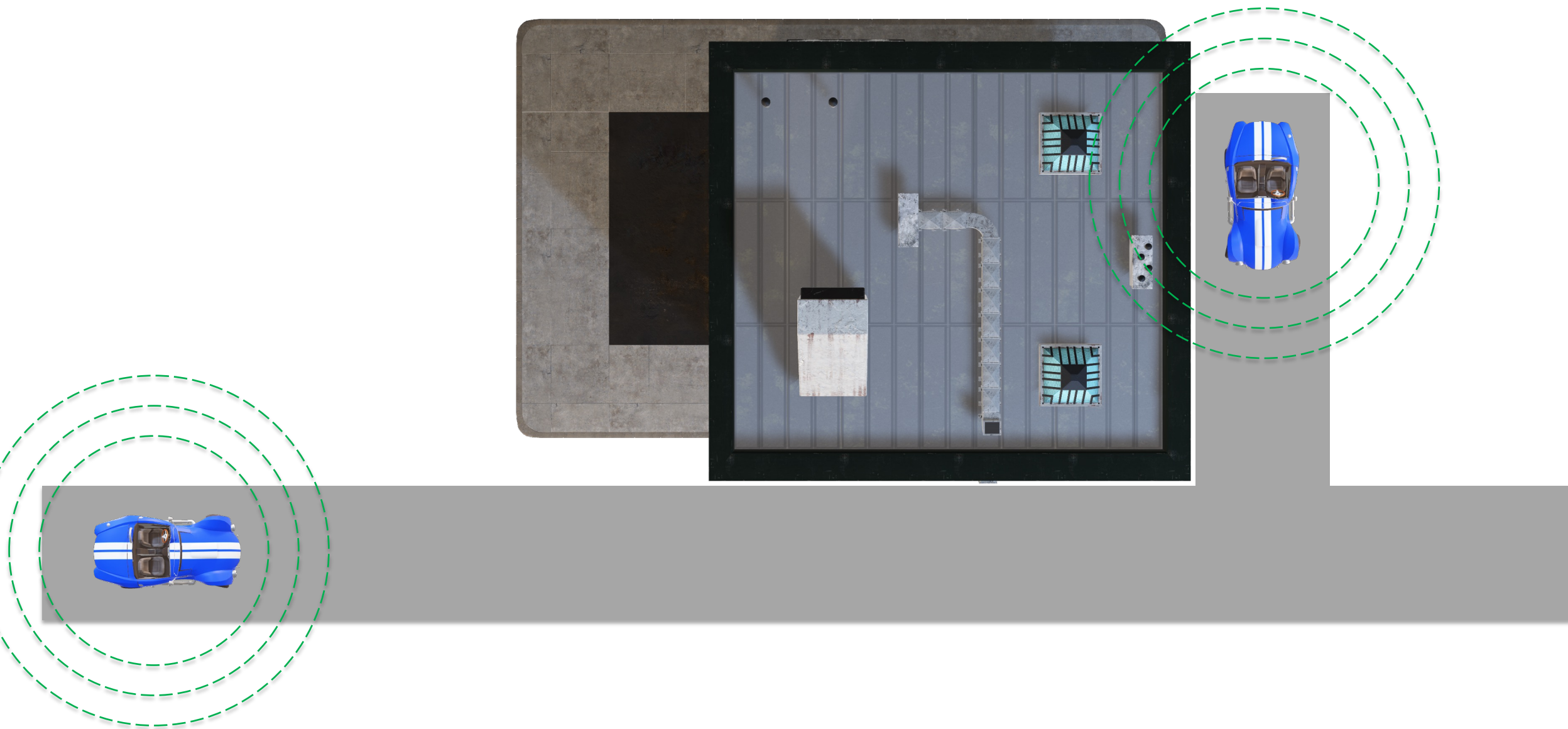
Vehicle-to-Vehicle (V2V) Communication



Vehicle-to-Vehicle (V2V) Communication



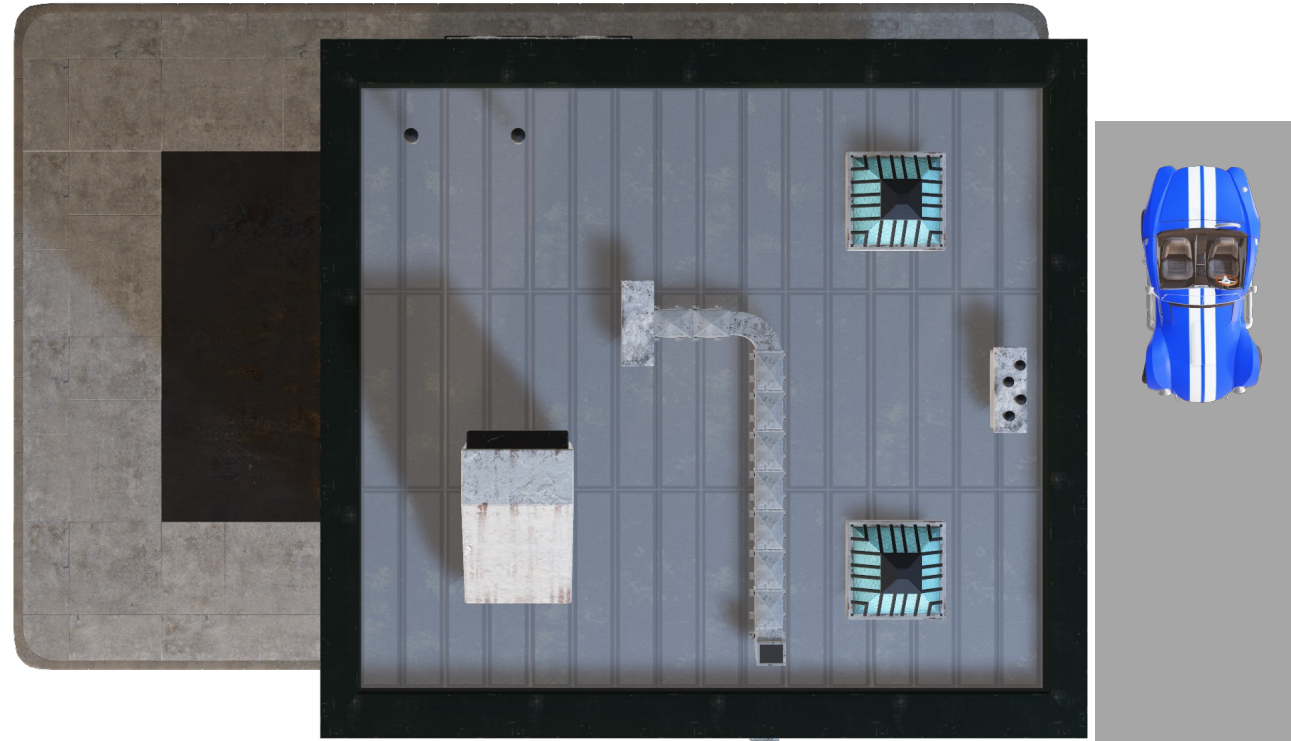
Vehicle-to-Vehicle (V2V) Communication



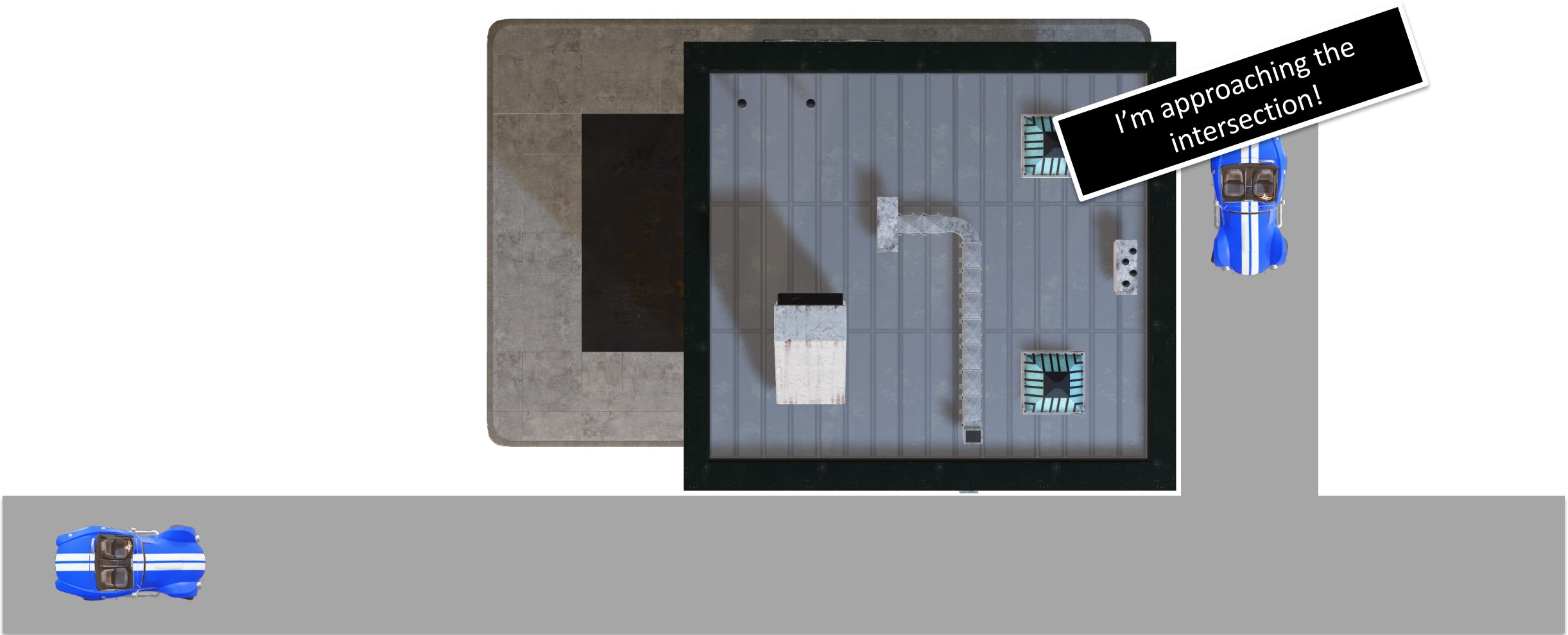
Vehicle-to-Vehicle (V2V) Communication

A Basic Safety Message (BSM)

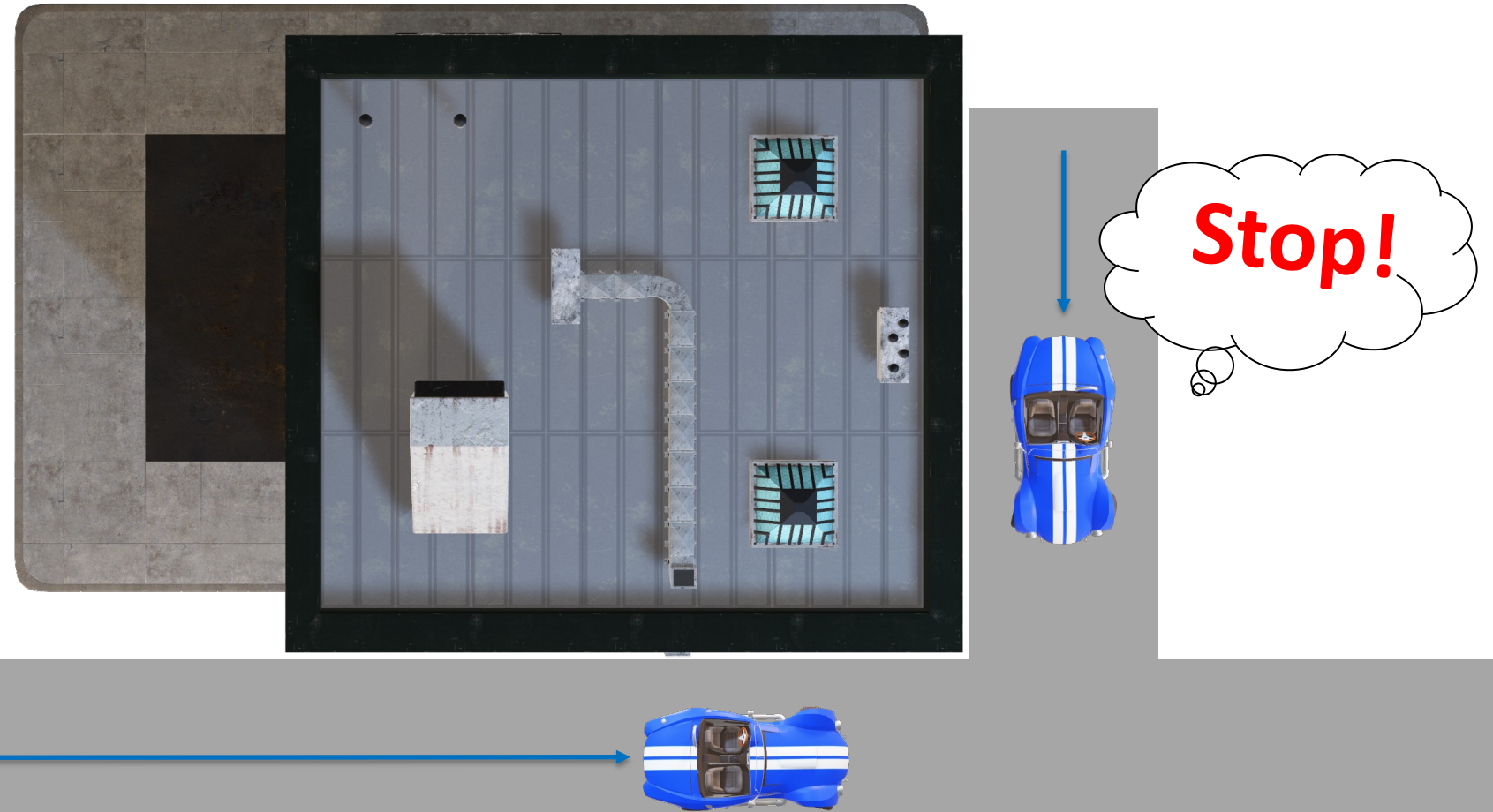
I'm approaching the intersection!



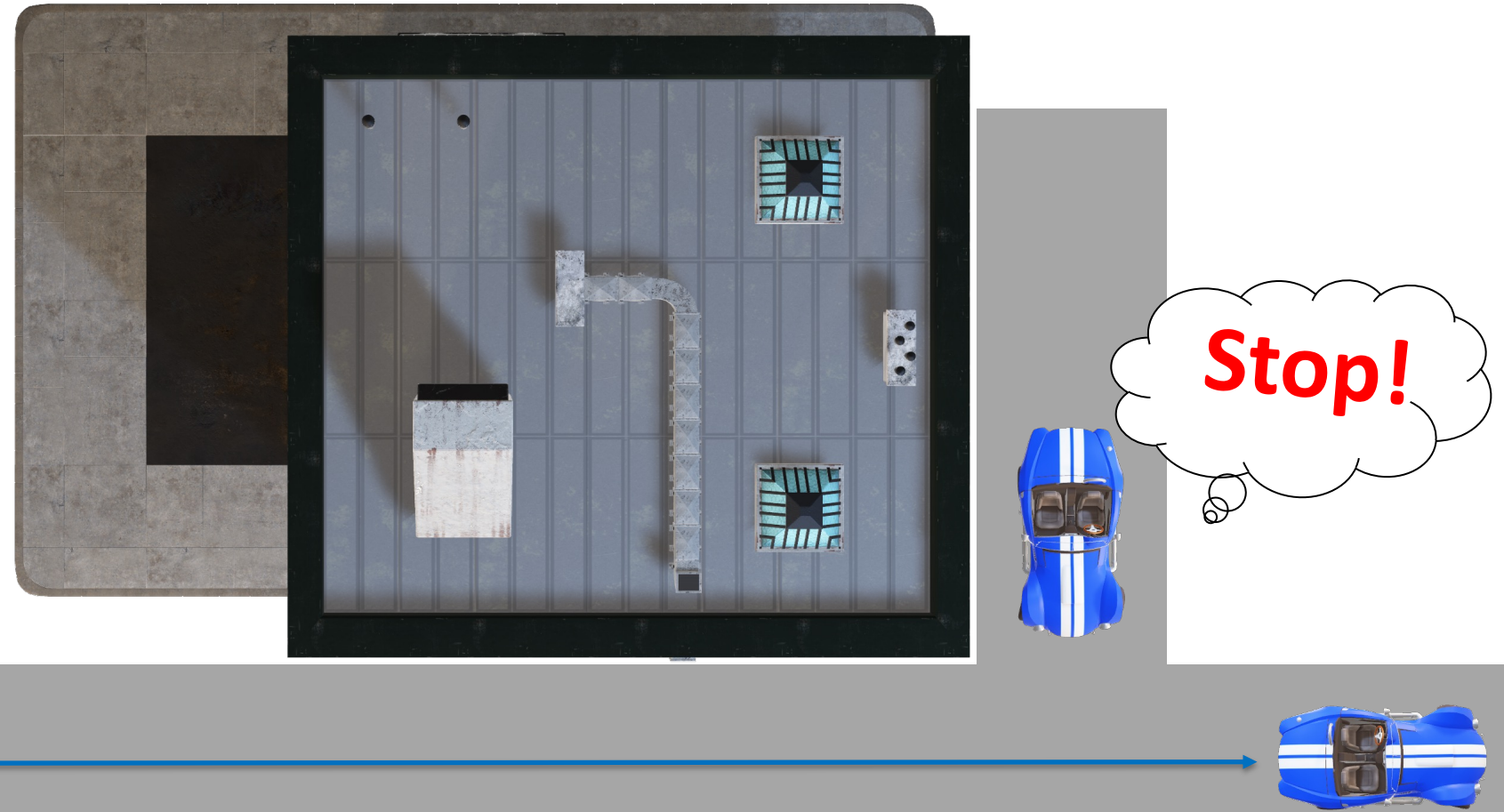
Vehicle-to-Vehicle (V2V) Communication



Vehicle-to-Vehicle (V2V) Communication



Vehicle-to-Vehicle (V2V) Communication



V2V Authentication

A Basic Safety Message (BSM)



I'm approaching the intersection!

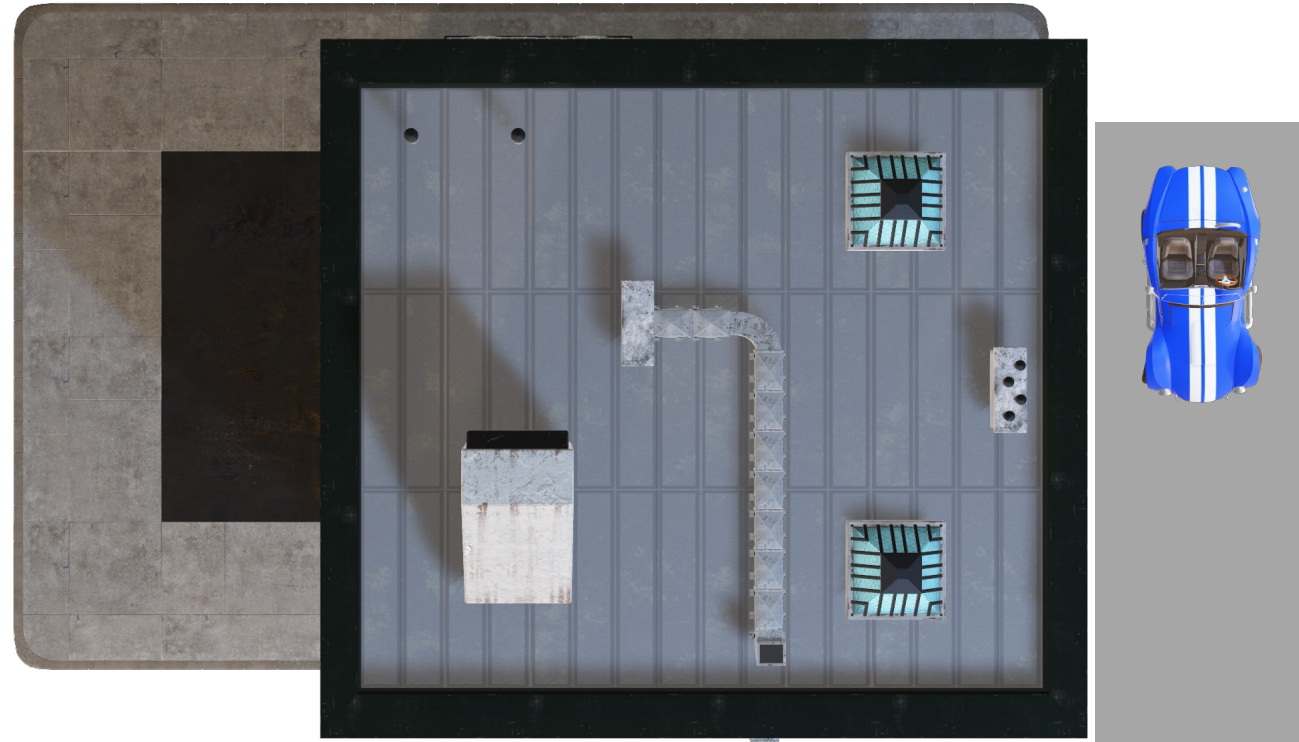


V2V Authentication

Secure Protocol Data Unit (SPDU)



SPDU



V2V Authentication

Secure Protocol Data Unit (SPDU)



SPDU



V2V Authentication

Secure Protocol Data Unit (SPDU)

BSM ("I'm approaching...")



SPDU



V2V Authentication

Secure Protocol Data Unit (SPDU)

Digital Certificate

BSM ("I'm approaching...")



SPDU



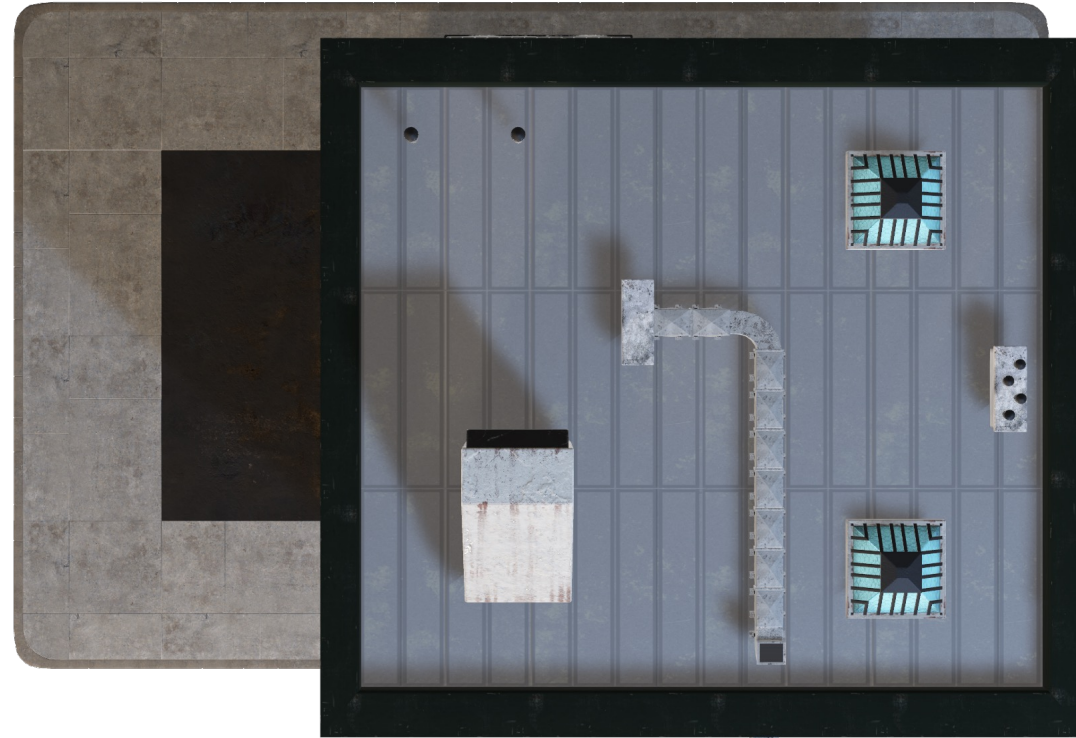
V2V Authentication

Secure Protocol Data Unit (SPDU)

Digital Certificate

BSM ("I'm approaching...")

Digital Signature (by vehicle)



SPDU



V2V Authentication

Secure Protocol Data Unit (SPDU)

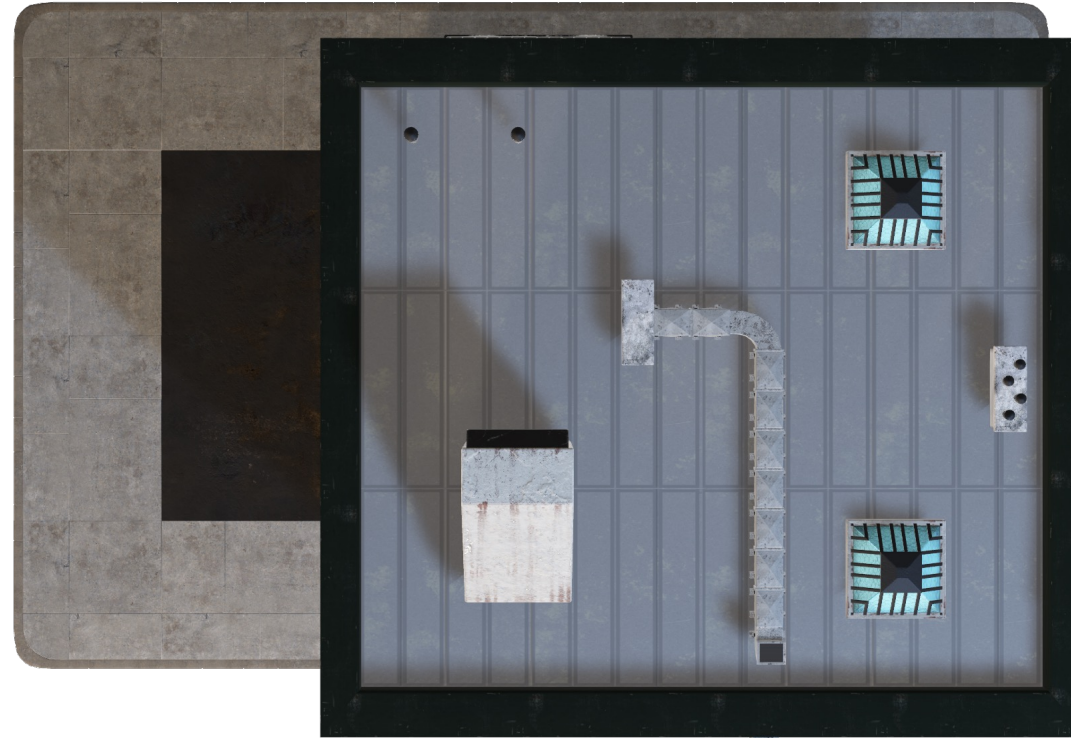
Digital Certificate

Public Key (of vehicle)

Digital Signature (by CA)

BSM ("I'm approaching...")

Digital Signature (by vehicle)



SPDU



V2V Authentication

Secure Protocol Data Unit (SPDU)

Digital Certificate

Public Key (of vehicle)

Digital Signature (by CA)

BSM ("I'm approaching...")

Digital Signature (by vehicle)



V2V Authentication

Secure Protocol Data Unit (SPDU)

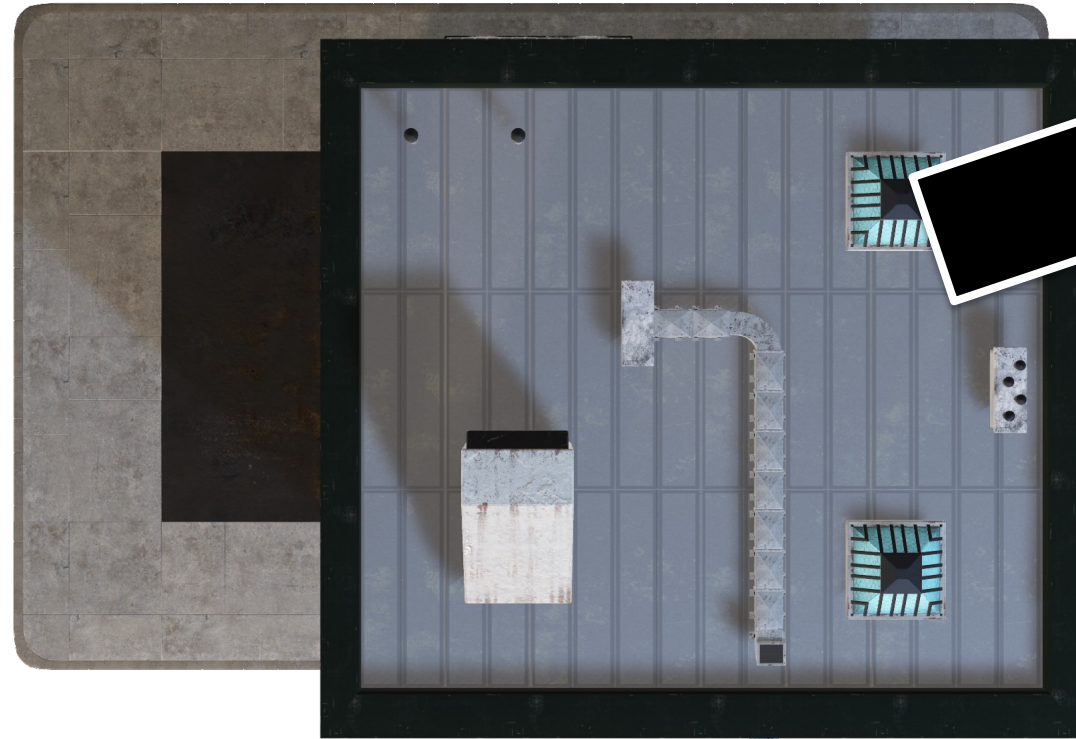
Digital Certificate

Public Key (of vehicle)

Digital Signature (by CA)

BSM ("I'm approaching...")

Digital Signature (by vehicle)



SPDU



V2V Authentication

Secure Protocol Data Unit (SPDU)

Digital Certificate

Public Key (of vehicle)

Digital Signature (by CA)

BSM ("I'm approaching...")

Digital Signature (by vehicle)

Certificate Valid?

SPDU



V2V Authentication

Secure Protocol Data Unit (SPDU)

Digital Certificate

Public Key (of vehicle)

Digital Signature (by CA)

BSM ("I'm approaching...")

Digital Signature (by vehicle)

Certificate Valid?

Signature Valid?

SPDU



V2V Authentication

Secure Protocol Data Unit (SPDU)

Digital Certificate

Public Key (of vehicle)

Digital Signature (by CA)

BSM ("I'm approaching...")

Digital Signature (by vehicle)

Certificate Valid?

Signature Valid?

Accept BSM ✓



SPDU



V2V Authentication

Secure Protocol Data Unit (SPDU)

Digital Certificate

Public Key (of vehicle)

Digital Signature (by CA)

BSM ("I'm approaching...")

Digital Signature (by vehicle)

Certificate Valid?

Signature Valid?

Accept BSM ✓



Stop!



Quantum Computers (QCs) Threaten V2V

Digital signatures in V2V use [elliptic curves \(ECDSA\)](#)

Quantum Computers (QCs) Threaten V2V

Digital signatures in V2V use **elliptic curves (ECDSA)**

QCs will break ECDSA → forge signatures, issue bogus certificates

Quantum Computers (QCs) Threaten V2V

Digital signatures in V2V use **elliptic curves (ECDSA)**

QCs will break ECDSA → forge signatures, issue bogus certificates

Good news: NIST is standardizing post-quantum (PQ) algorithms

Quantum Computers (QCs) Threaten V2V

Digital signatures in V2V use **elliptic curves (ECDSA)**

QCs will break ECDSA → forge signatures, issue bogus certificates

Good news: NIST is standardizing post-quantum (PQ) algorithms

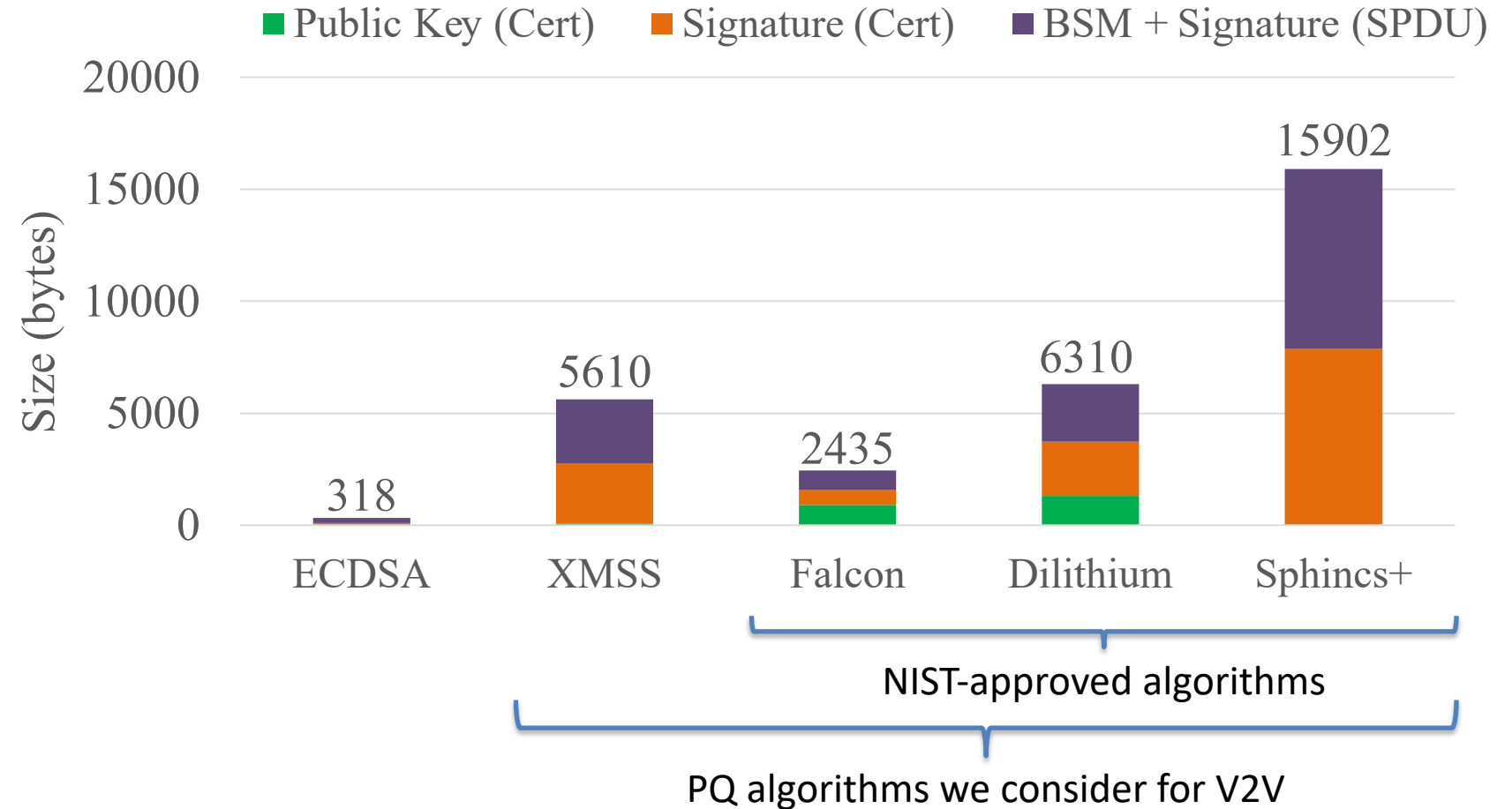
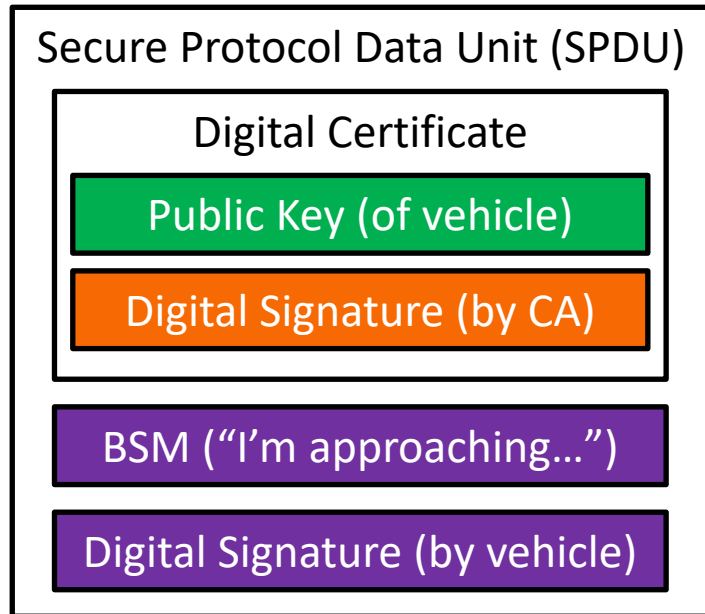
Problem: V2V protocols cannot easily adopt these PQ signatures

Why Isn't PQ “Plug-and-Play” in V2V?

- ❑ PQ signatures and keys are **much larger** than ECDSA

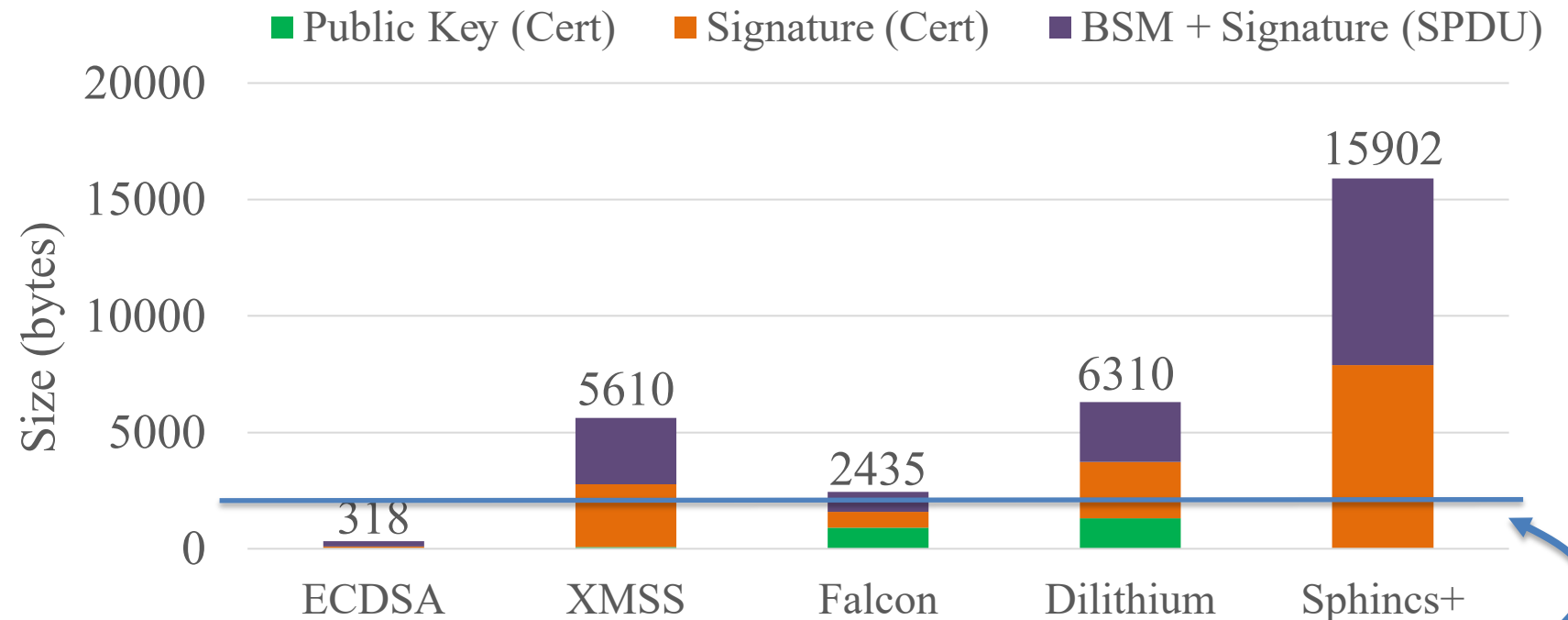
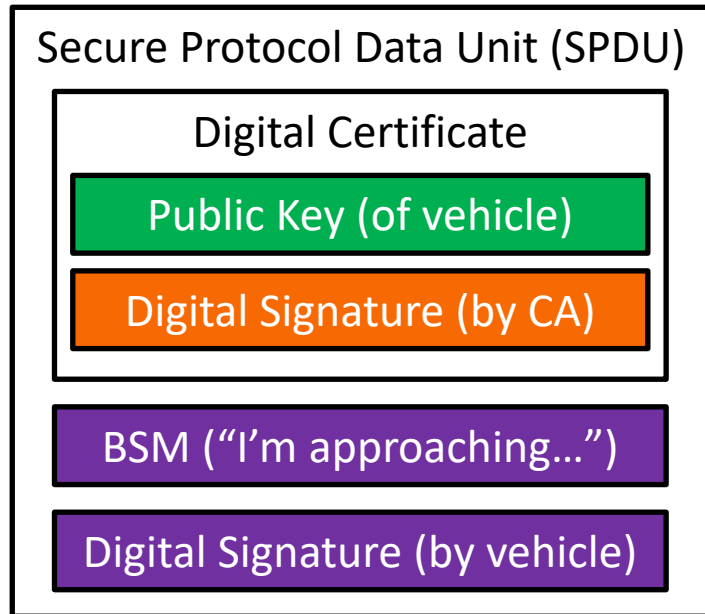
Why Isn't PQ "Plug-and-Play" in V2V?

- ❑ PQ signatures and keys are **much larger** than ECDSA



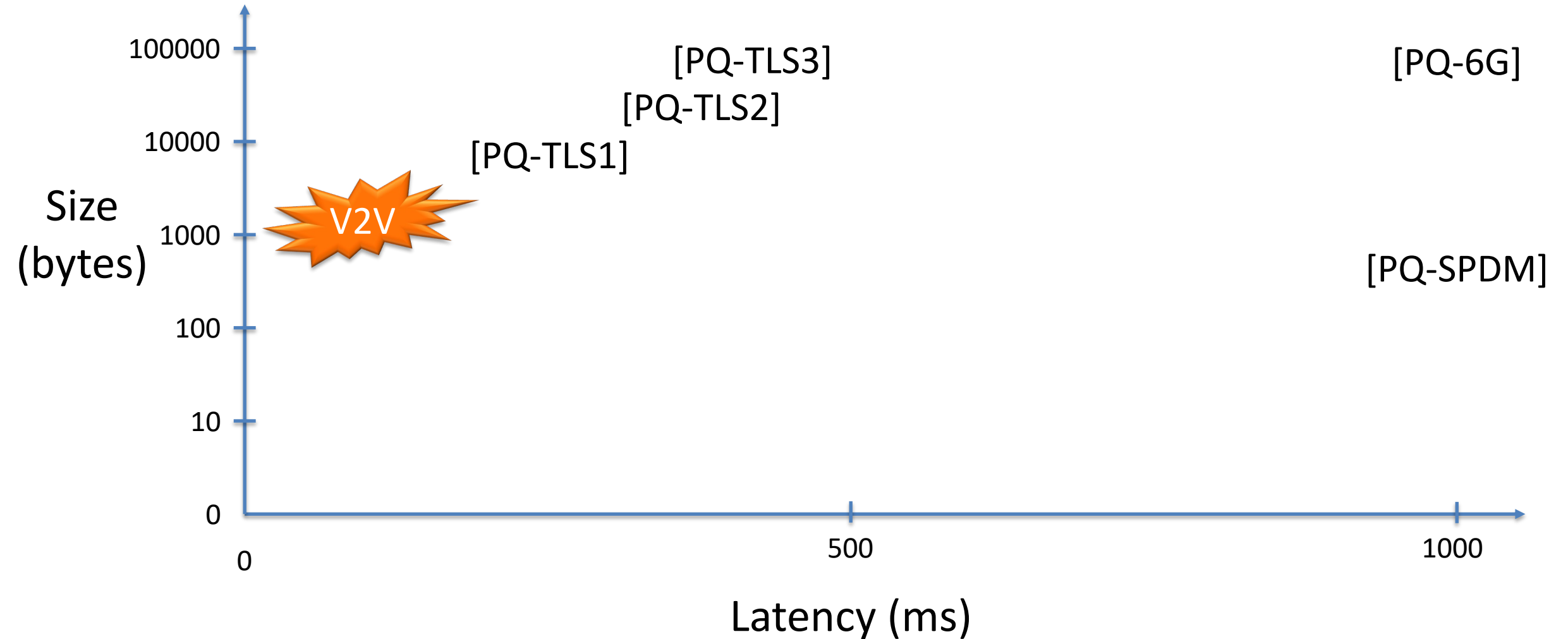
Why Isn't PQ "Plug-and-Play" in V2V?

- ❑ PQ signatures and keys are **much larger** than ECDSA



- ❑ Dedicated Short-Range Communication (DSRC) → 2,304-byte limit

V2V is (Uniquely) More Constrained



Our Contributions

Analyze quantum threat
&
Identify V2V constraints for PQC

Our Contributions

Hybrid (PQ/EC) Authentication Protocol
&
AI-based Transmission Optimization

Analyze quantum threat
&
Identify V2V constraints for PQC

Our Contributions

Hybrid (PQ/EC) Authentication Protocol
&
AI-based Transmission Optimization

Security Reduction (Proofs)
&
Extensive Experiments

Analyze quantum threat
&
Identify V2V constraints for PQC

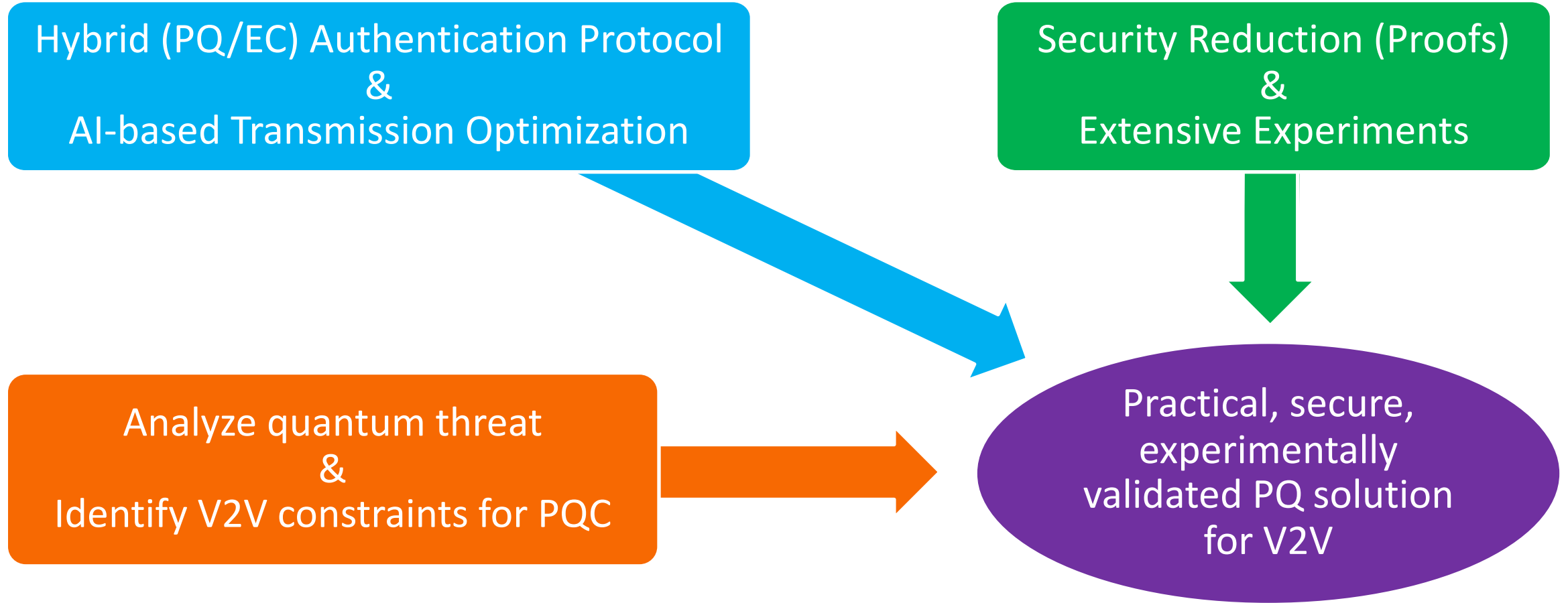
Our Contributions

Hybrid (PQ/EC) Authentication Protocol
&
AI-based Transmission Optimization

Security Reduction (Proofs)
&
Extensive Experiments

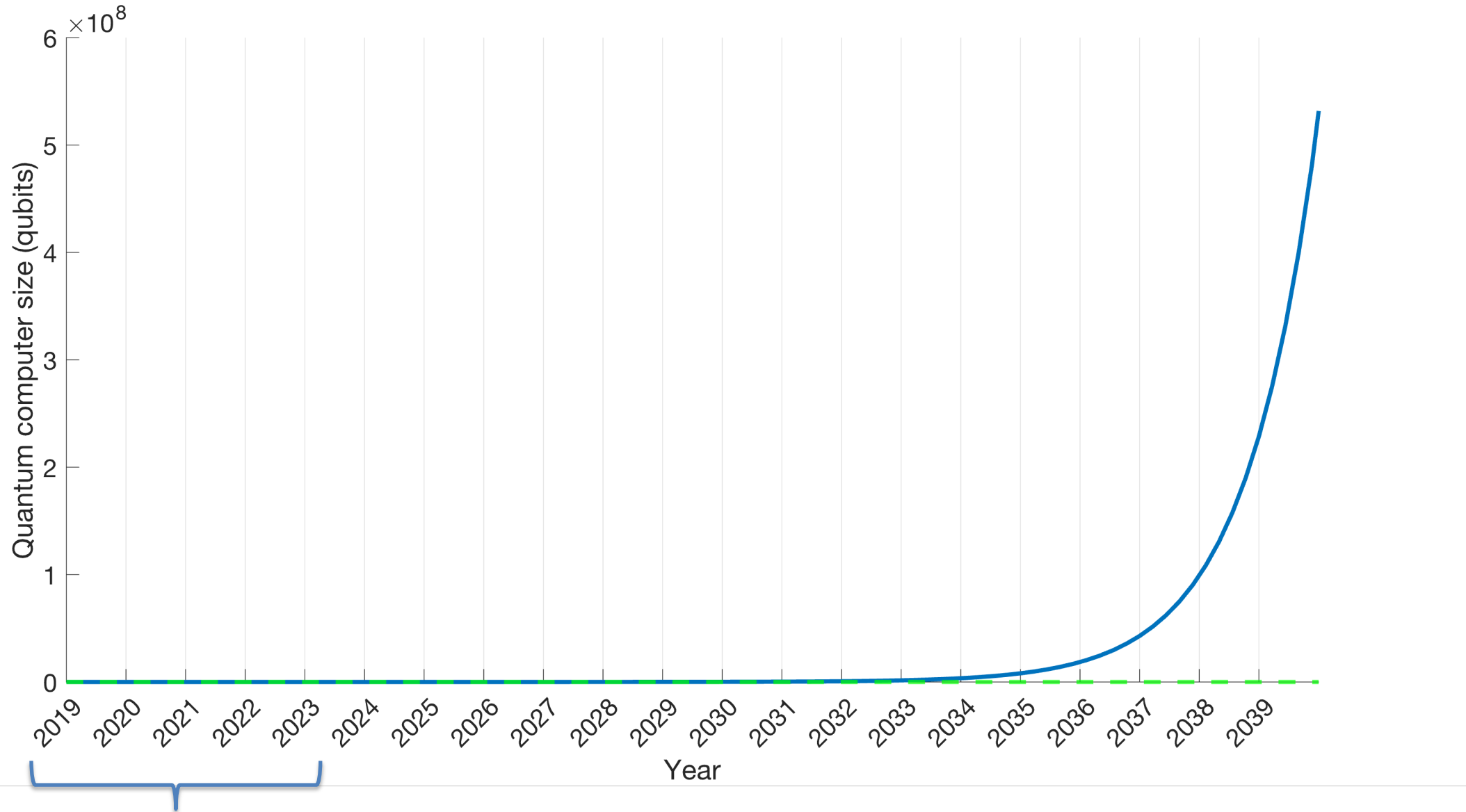
Analyze quantum threat
&
Identify V2V constraints for PQC

Practical, secure,
experimentally
validated PQ solution
for V2V

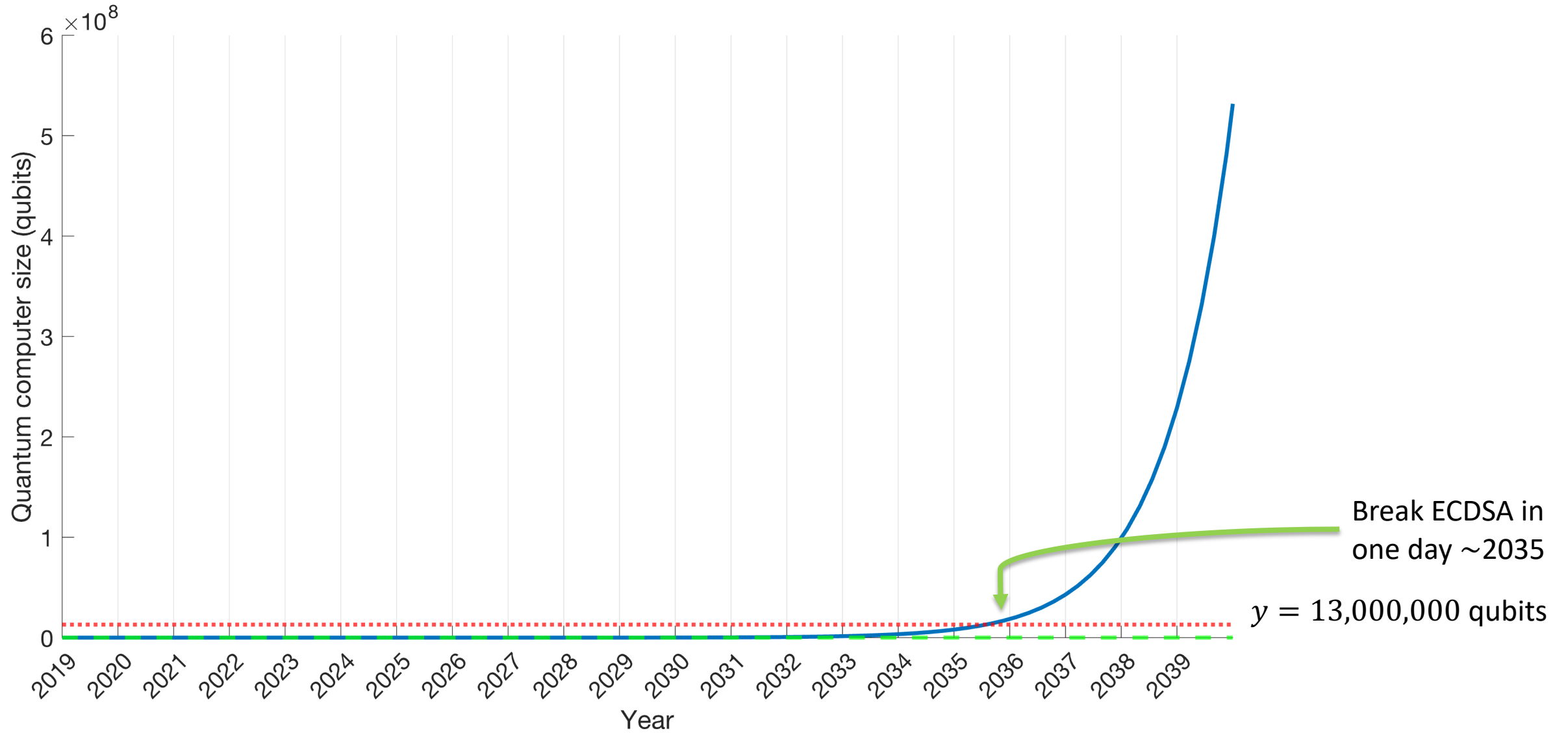


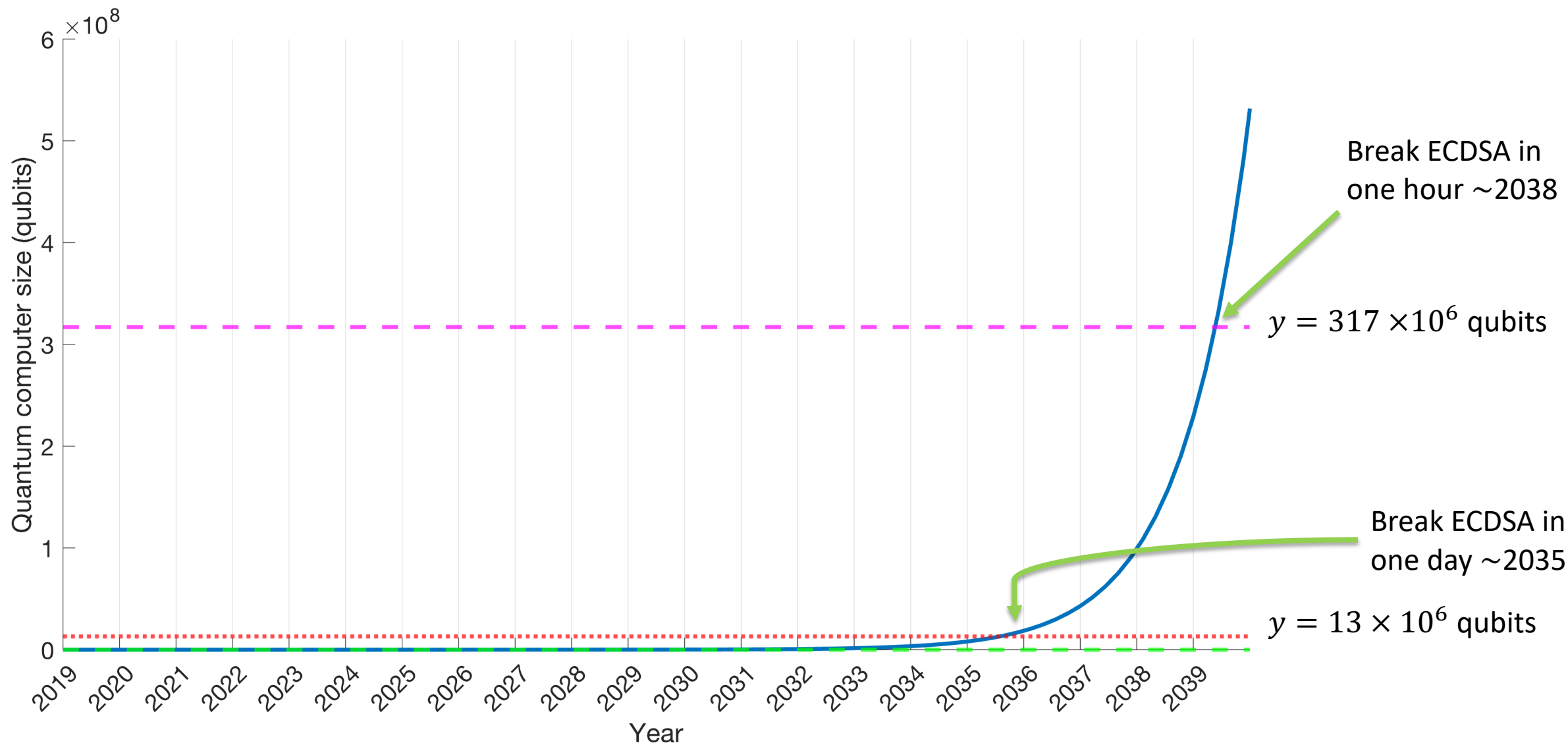
How Much PQ Do We Need *Today*?

- ❑ Quantum computers (QCs) can't break much (yet)



Extrapolation from 2019-2023 IBM data and forecast





So, Why Worry About This Now?

Unlikely to have quantum threat before ~2035

So, Why Worry About This Now?

Unlikely to have quantum threat before ~2035

Average vehicle lifetime is 12-15 years

So, Why Worry About This Now?

Unlikely to have quantum threat before ~2035

Average vehicle lifetime is 12-15 years

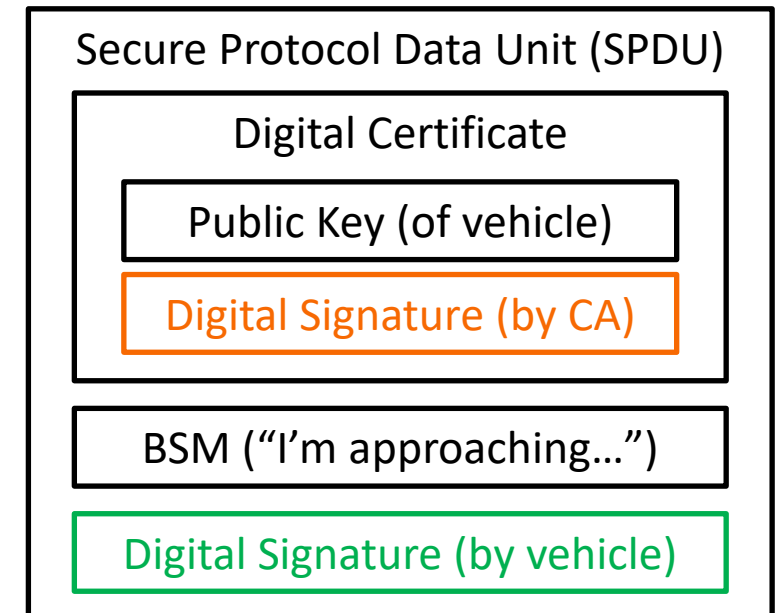
Today's V2V wireless protocols and vehicle hardware need quantum resistance

How Much PQ Security Do We Need *Now*?

- ❑ Quantum computers (QCs) can't break much (yet)
- ❑ Two critical message elements have digital signatures:

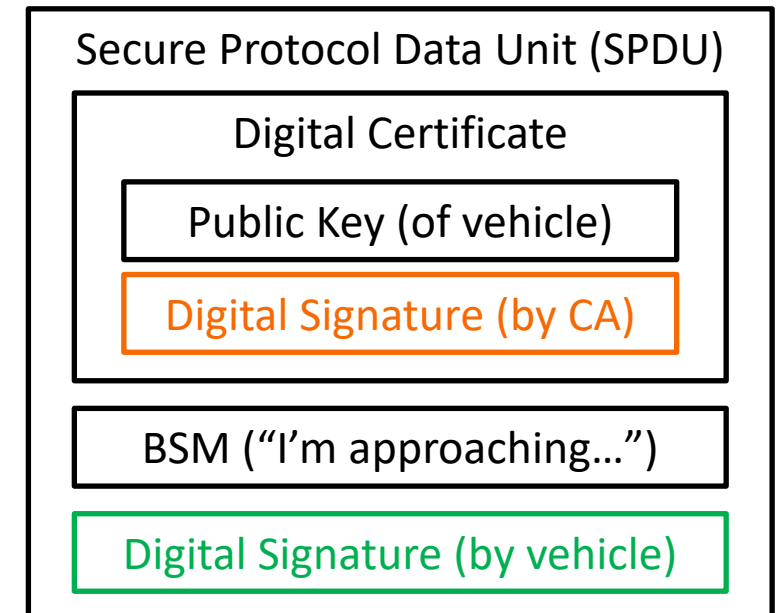
How Much PQ Security Do We Need *Now*?

- ❑ Quantum computers (QCs) can't break much (yet)
- ❑ Two critical message elements have digital signatures:
 - **Payload (BSM) signature** valid for ~30 seconds
 - **Digital certificate signature** valid for 1 week



How Much PQ Security Do We Need *Now*?

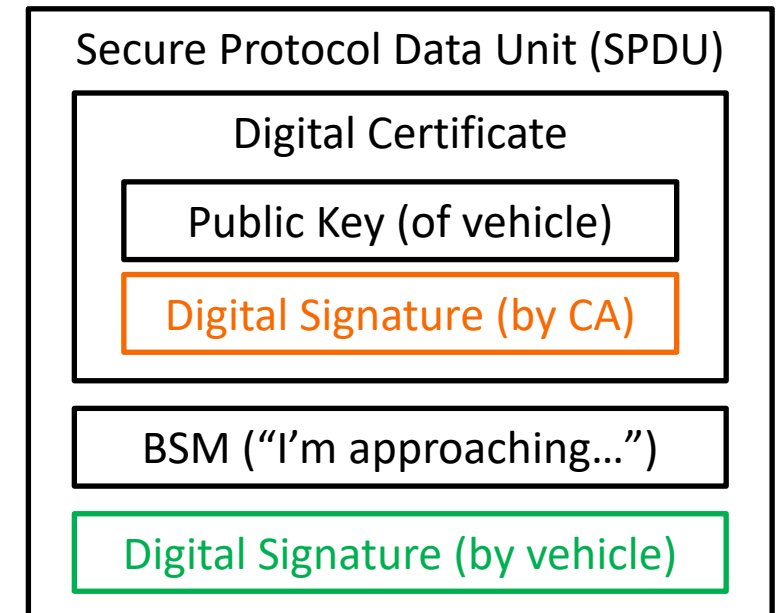
- ❑ Quantum computers (QCs) can't break much (yet)
- ❑ Two critical message elements have digital signatures:
 - **Payload (BSM) signature** valid for ~30 seconds
 - **Digital certificate signature** valid for 1 week
- ❑ Certificate forgery possible by 2035!



How Much PQ Security Do We Need *Now*?

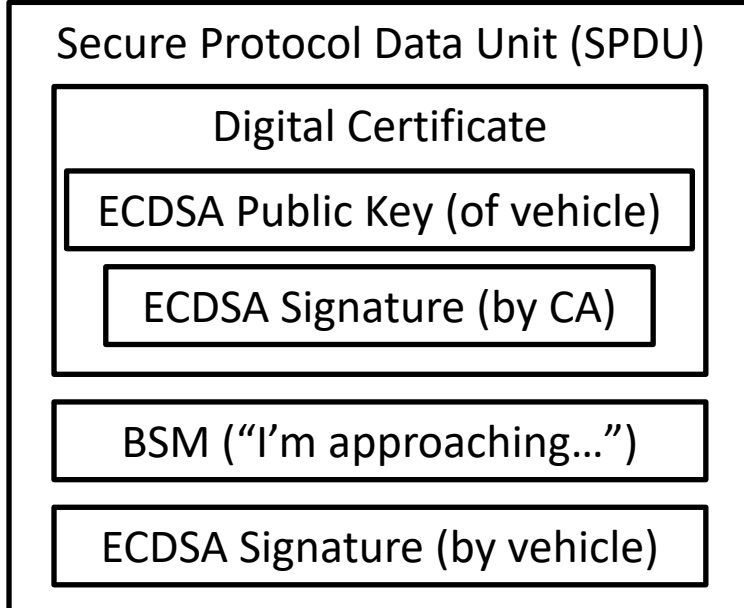
- ❑ Quantum computers (QCs) can't break much (yet)
- ❑ Two critical message elements have digital signatures:
 - **Payload (BSM) signature** valid for ~30 seconds
 - **Digital certificate signature** valid for 1 week
- ❑ Certificate forgery possible by 2035!

For the near future, focus on protecting **certificates** from quantum attacks in a **hybrid solution** for PQ V2V



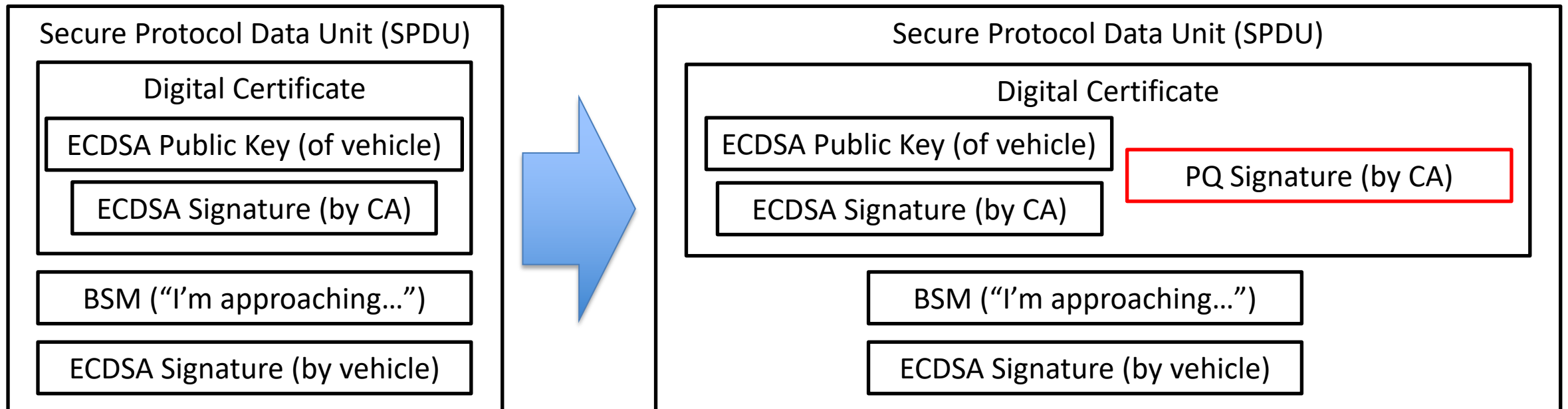
Partially Hybrid Authentication Protocol

- ❑ PQ protects what is most imminently at risk: [certificates](#)



Partially Hybrid Authentication Protocol

- ❑ PQ protects what is most imminently at risk: **certificates**
- ❑ Use PQ signature for certificate, keep EC signature for message



For Every Message, (Not) a Certificate

- ❑ Certificates are transmitted in every **fifth** SPDU
 - Certificate must be shared every 500ms

For Every Message, (Not) a Certificate

- ❑ Certificates are transmitted in every **fifth** SPDU
 - Certificate must be shared every 500ms

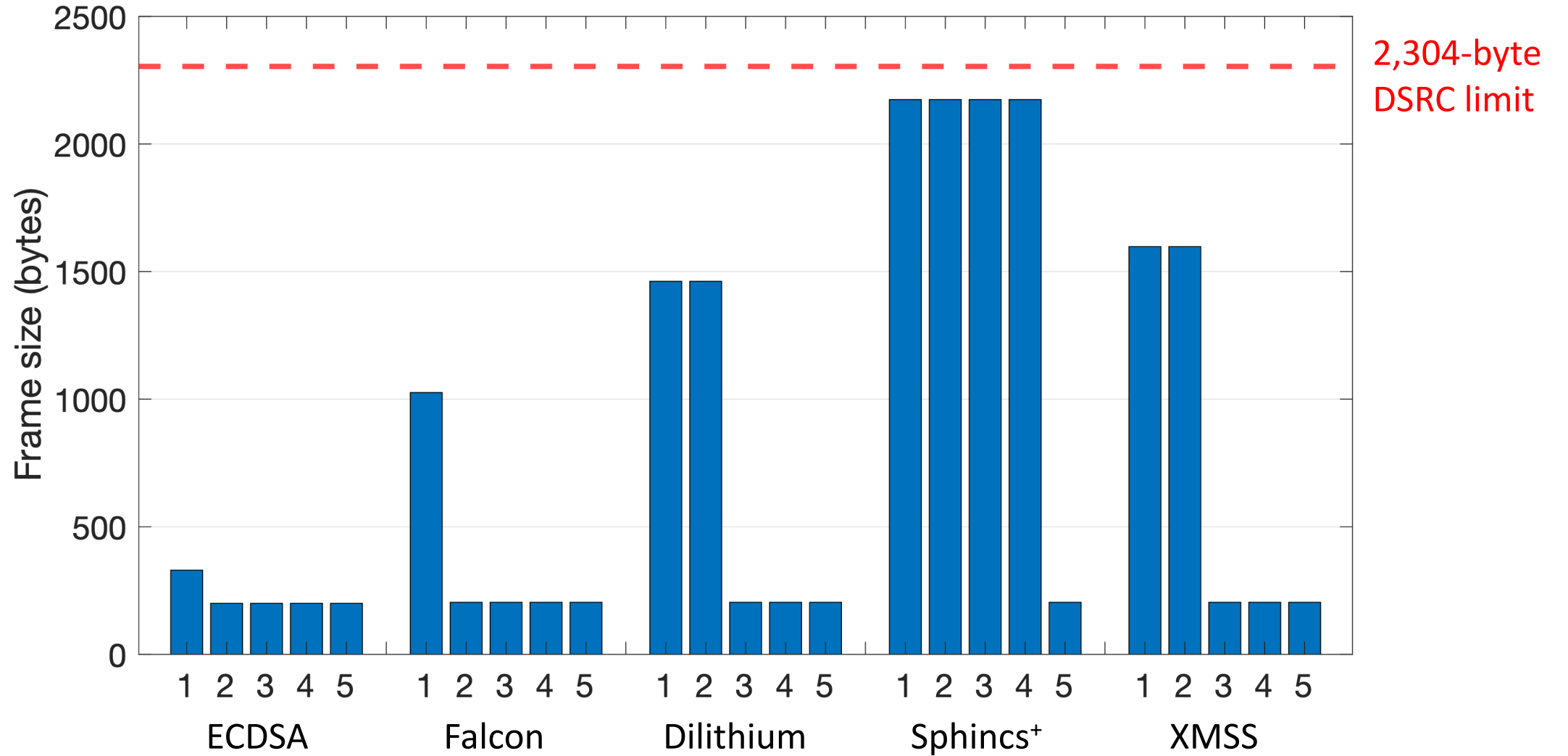
- ❑ Insight: **fragment** hybrid certificates across up to 5 SPDUs

For Every Message, (Not) a Certificate

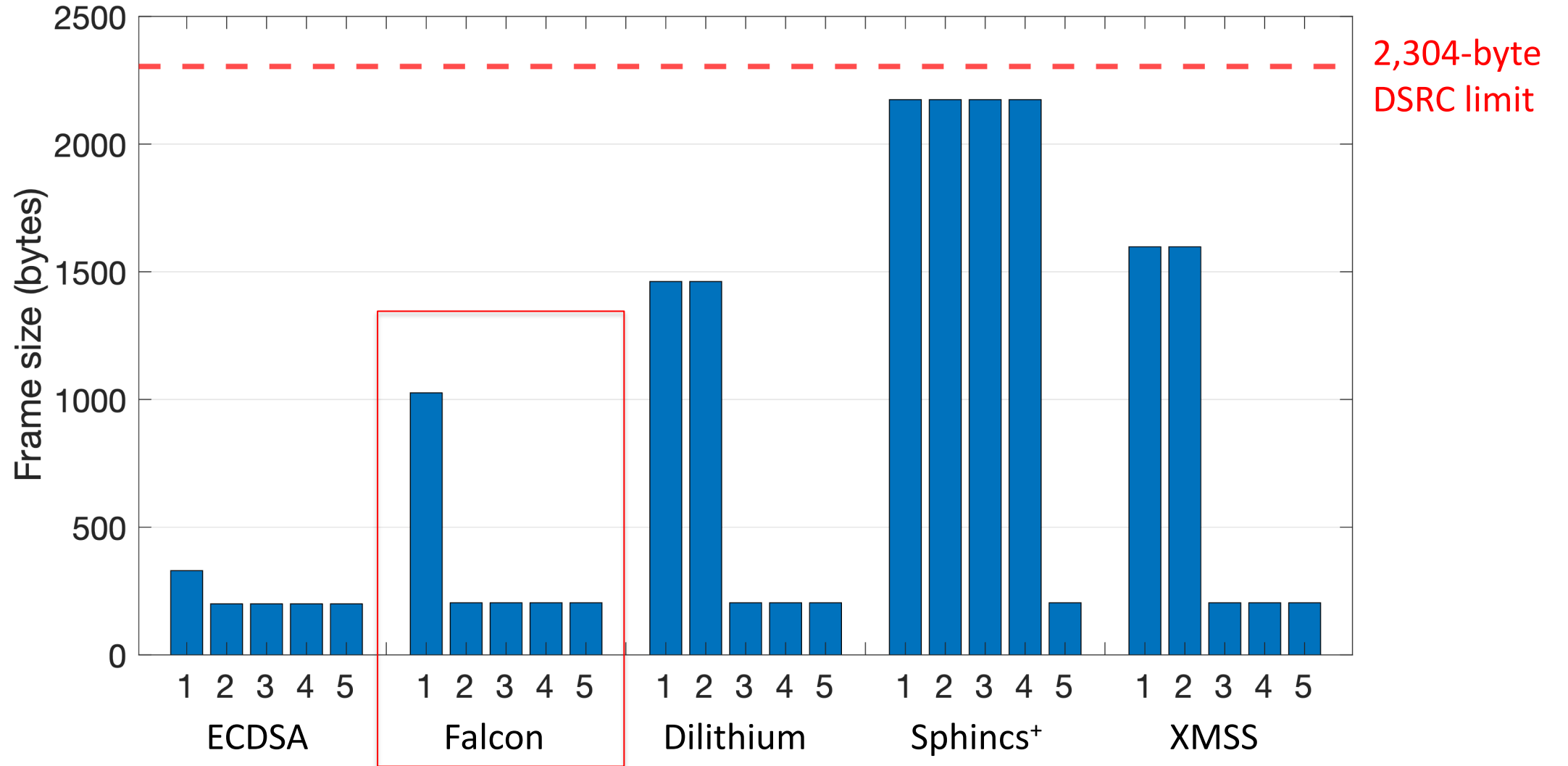
- ❑ Certificates are transmitted in every **fifth** SPDU
 - Certificate must be shared every 500ms

- ❑ Insight: **fragment** hybrid certificates across up to 5 SPDUs

- ❑ Goal: Minimize message size



“5-message cycle” for ECDSA and selected PQ algorithms



“5-message cycle” for ECDSA and selected PQ algorithms

Larger Frames → Less Reliable

- ❑ Once spectrum becomes congested, medium contention and hidden terminals in mobile network lead to **increased packet loss**

Larger Frames → Less Reliable

- ❑ Once spectrum becomes congested, medium contention and hidden terminals in mobile network lead to **increased packet loss**
- ❑ Frame Loss Rate (FLR): $\frac{\# \text{ lost frames}}{\# \text{ total frames}}$ for entire system

Larger Frames → Less Reliable

- ❑ Once spectrum becomes congested, medium contention and hidden terminals in mobile network lead to **increased packet loss**
- ❑ Frame Loss Rate (FLR): $\frac{\# \text{ lost frames}}{\# \text{ total frames}}$ for entire system

Problem (even with Falcon): In high-density scenarios (~ 100 vehicles/km), **FLR is +63%** when ECDSA replaced with *Partially Hybrid* design.



Solution: Optimize Transmissions

- Insight: $> 95\%$ of certificate transmissions are unnecessary!
 - Vehicles do not move very far in ~ 500 ms

Solution: Optimize Transmissions

- ❑ Insight: $> 95\%$ of certificate transmissions are unnecessary!
 - Vehicles do not move very far in ~ 500 ms

- ❑ Idea: send certificates **less frequently**, decrease spectrum waste

Use AI to Optimize Transmissions

- ❑ Insight: $> 95\%$ of certificate transmissions are unnecessary!
 - Vehicles do not move very far in ~ 500 ms

- ❑ Idea: send certificates **less frequently**, decrease spectrum waste

- ❑ Use **distributed** AI to dynamically adjust certificate interval

Use AI to Optimize Transmissions

- ❑ Insight: $> 95\%$ of certificate transmissions are unnecessary!
 - Vehicles do not move very far in ~ 500 ms

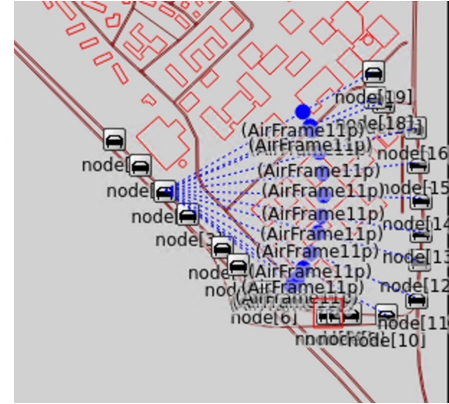
- ❑ Idea: send certificates **less frequently**, decrease spectrum waste

- ❑ Use **distributed** AI to dynamically adjust certificate interval

- ❑ Also optimize peer-to-peer certificate sharing protocol (P2PCD)

Experiments

- Extensive simulations in VEINS
 - Custom PQ-V2V module

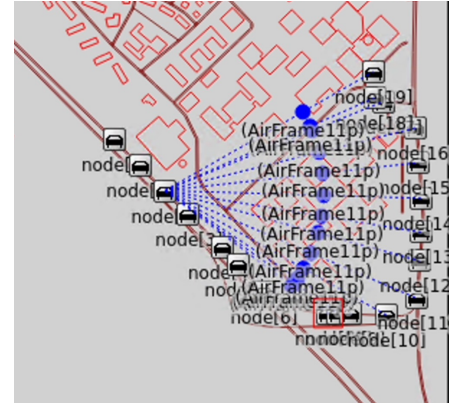


Experiments

❑ Extensive simulations in VEINS

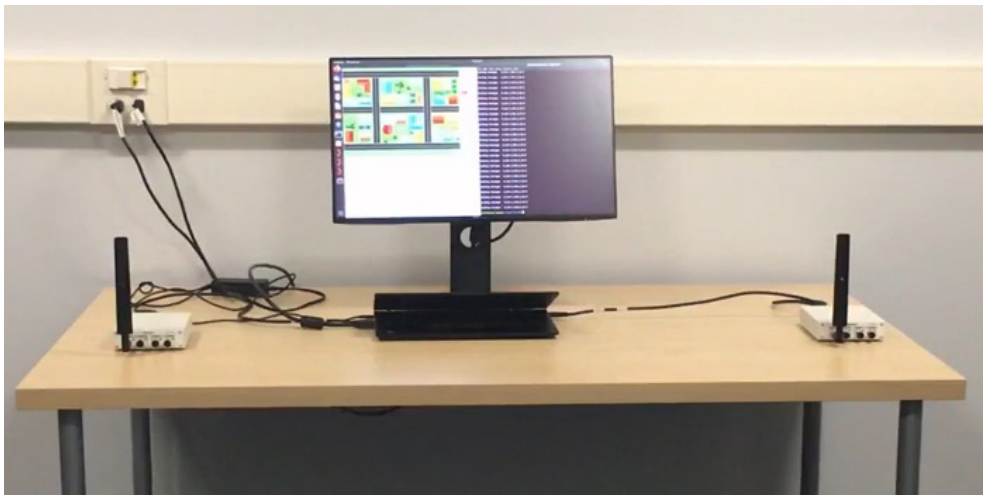
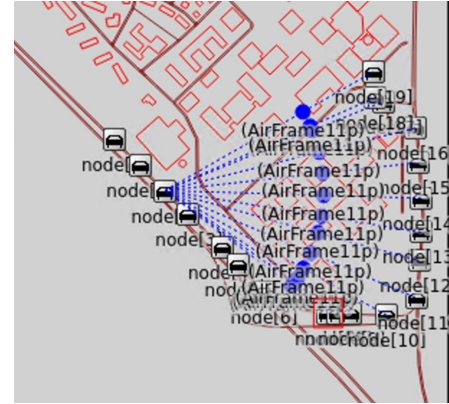
- Custom PQ-V2V module

❑ Benchmarking PQ algorithms on ARM-based V2V chipset



Experiments

- ❑ Extensive simulations in VEINS
 - Custom PQ-V2V module
- ❑ Benchmarking PQ algorithms on ARM-based V2V chipset
- ❑ USRP experiments in the lab and **on real roadways**
 - New testbed: *PQ-V2Verifier*



Experimental Results

- Combining hardware benchmarks, over-the-air measurements, and infusing data into VEINS simulations:

	Metric (vs. ECDSA)	Low-density (60 vehicles/km)	High-density (100 vehicles/km)
<i>Partially Hybrid</i>	Per-BSM delay	+0.66 ms	+0.67 ms
	Δ FLR	+29%	+61%

Experimental Results

- Combining hardware benchmarks, over-the-air measurements, and infusing data into VEINS simulations:

	Metric (vs. ECDSA)	Low-density (60 vehicles/km)	High-density (100 vehicles/km)
<i>Partially Hybrid</i>	Per-BSM delay	+0.66 ms	+0.67 ms
	Δ FLR	+29%	+61%
<i>Partially Hybrid w/ Spectrum Optimization</i>	Δ FLR	+7.9%	+7.1%

Conclusions

- ❑ Forecasted and assessed quantum risk to V2V

Conclusions

- ❑ Forecasted and assessed quantum risk to V2V
- ❑ Developed **practical, hybrid** authentication protocol

Conclusions

- ❑ Forecasted and assessed quantum risk to V2V
- ❑ Developed **practical, hybrid** authentication protocol
- ❑ Identified **Falcon** as best PQ algorithm for V2V

Conclusions

- ❑ Forecasted and assessed quantum risk to V2V
- ❑ Developed **practical, hybrid** authentication protocol
- ❑ Identified **Falcon** as best PQ algorithm for V2V
- ❑ Applied AI to optimize spectrum, improve reliability

Conclusions

- ❑ Forecasted and assessed quantum risk to V2V
- ❑ Developed **practical, hybrid** authentication protocol
- ❑ Identified **Falcon** as best PQ algorithm for V2V
- ❑ Applied AI to optimize spectrum, improve reliability
- ❑ Validated through simulations and **hardware experiments**

Key Contributions

Forecast/assessment of quantum risk

Hybrid authentication protocol

Falcon is best PQ algorithm for V2V

AI to optimize spectrum, reliability

Simulations + hardware experiments

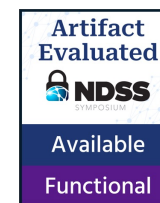
Thank You! Questions?



← Our paper



← Artifacts



Geoff Twardokus
geoff.twardokus@mail.rit.edu

Nina Bindel
nina.bindel@sandboxaq.com

Hanif Rahbari
hanif.rahbari@rit.edu

Sarah McCarthy
sarah.mccarthy@uwaterloo.ca

