Drive (Quantum) Safe! --Towards Post-Quantum Security for Vehicle-to-Vehicle Communications

Real World Crypto 2022
April 15, 2022

Nina Bindel

ninabindel.de

@NinaBindel

joint work with Sarah McCarthy
Geoff Twardokus
Hanif Rahbari

615,000

THE NUMBER OF MOTOR VEHICLE CRASHES PER YEAR THAT COULD BE PREVENTED USING V2V TECHNOLOGY[1]

[1] U.S. Department of Transportation, https://www.nhtsa.gov/technology-innovation/vehicle-vehicle-communication

20-30%

REDUCTION IN CONGESTION[2]

[2] On a segment of Interstate 5 freeway in the Orange County area, https://www.westernite.org/annualmeetings/15_Las_Vegas/Papers/7C-Shah.pdf

5%

REDUCTION IN CO_2 EMISSIONS[3]

[3] F. Outay, F. Kamoun, F. Kaisser, D. Alterri, A. Yasar, 2019. V2V and V2I communications for traffic safety and CO2 emission reduction: A performance evaluation. *Procedia Computer Science*, *151*, pp.353-360.

BY 2025, THERE WILL BE 100 MILLION CONNECTED CARS GLOBALLY[4]

[4] According to Communications Service Provider TIM, via https://www.ericsson.com/en/connected-vehicles

[5] S. Dongre and H. Rahbari. Message sieving to mitigate smart gridlock attacks in V2V. In Proceedings of the ACM Conference on Security and Privacy in Wireless & Mobile Networks (WiSec), 2021

BY 2025, THERE WILL BE 100 MILLION CONNECTED CARS GLOBALLY[4]

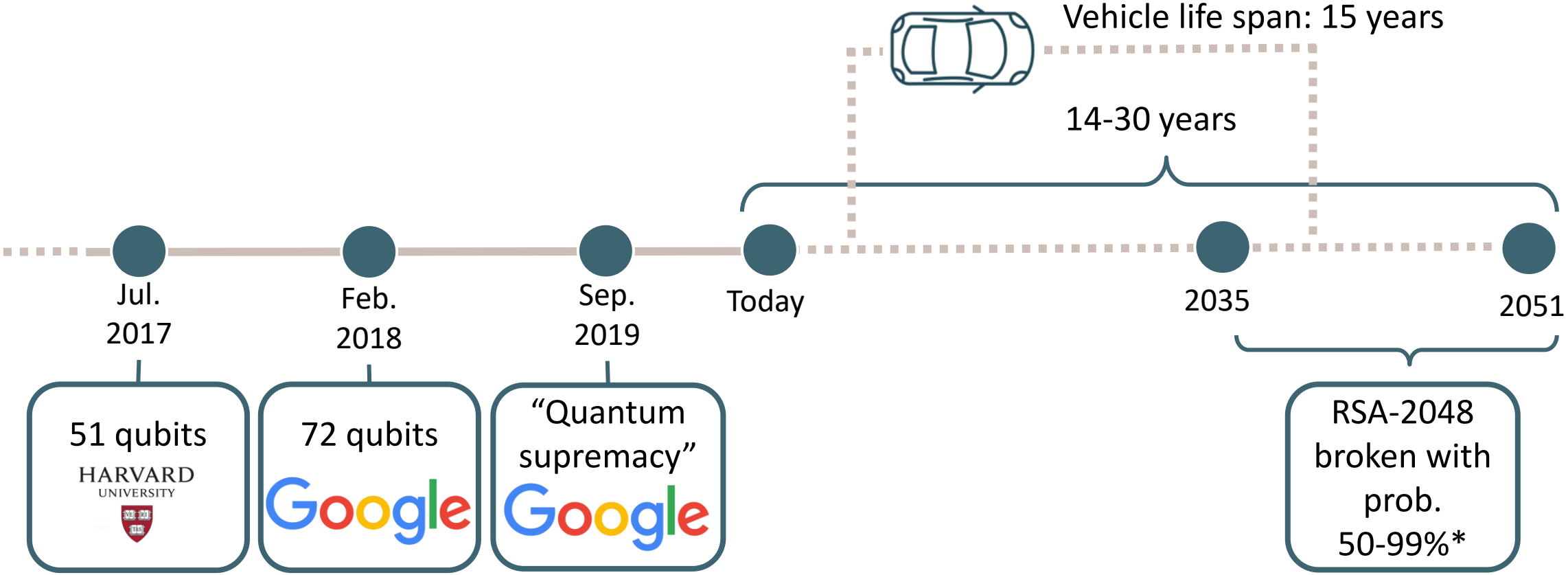
…BUT WILL THEY BE SECURE

…EVEN AGAINST QUANTUM ATTACKERS?

[4] According to Communications Service Provider TIM, via https://www.ericsson.com/en/connected-vehicles

[5] S. Dongre and H. Rahbari. Message sieving to mitigate smart gridlock attacks in V2V. In Proceedings of the ACM Conference on Security and Privacy in Wireless & Mobile Networks (WiSec), 2021

Urgency of PQ Transition for Vehicle-to-Vehicle Communication



*Global Risk Institute, Canada,2019

Outline

- Introduction to **Secure** Vehicle-to-Vehicle (V2V) Communication
- **Challenges** of Quantum-Secure V2V Communication
- Suggestion of **Standard-Compliant** Classical – Post-Quantum **Hybrid Solutions**

*All icons from flaticom.com using premium account.

Introduction to V2V Communication

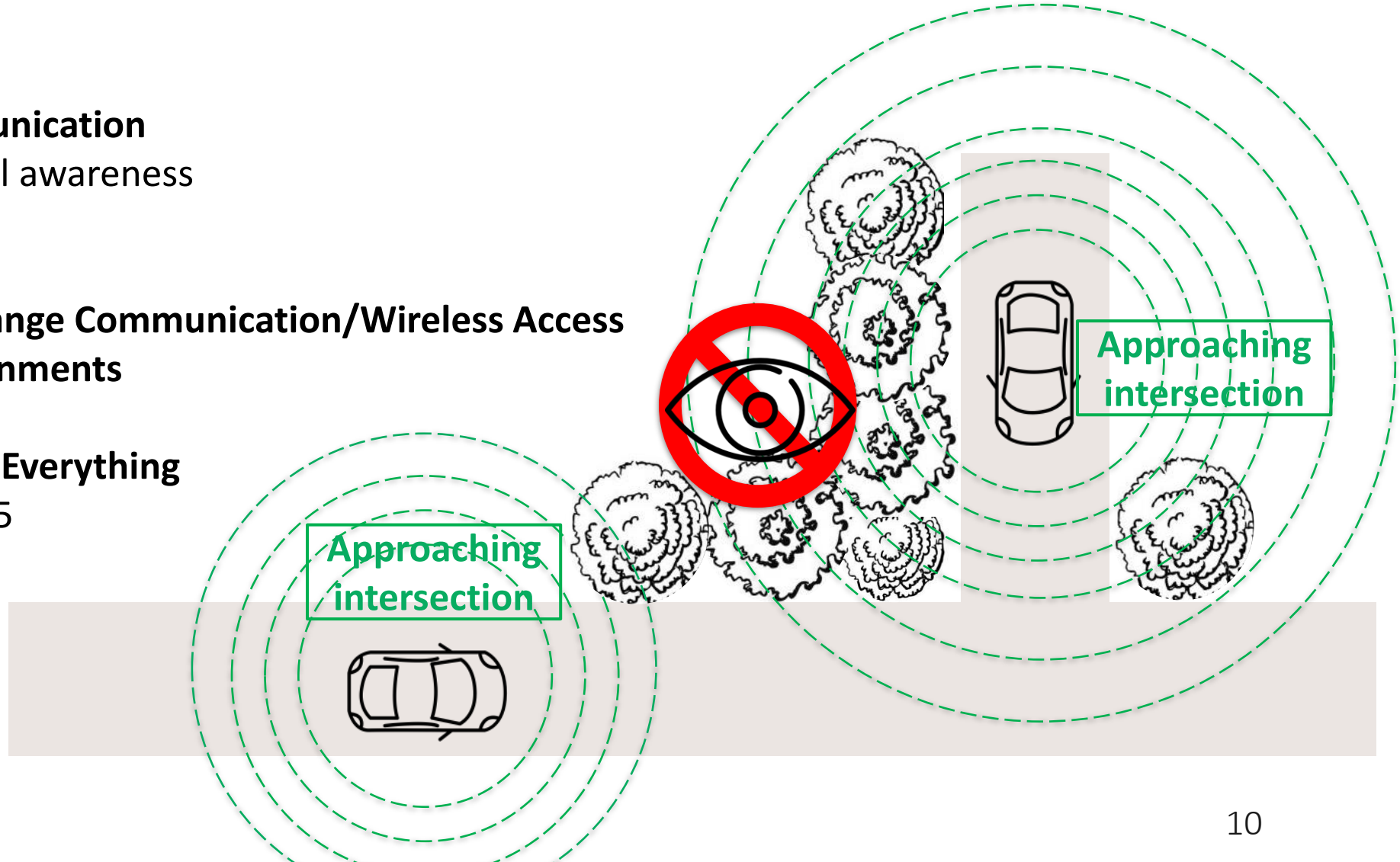
V2V Communication

Direct wireless communication

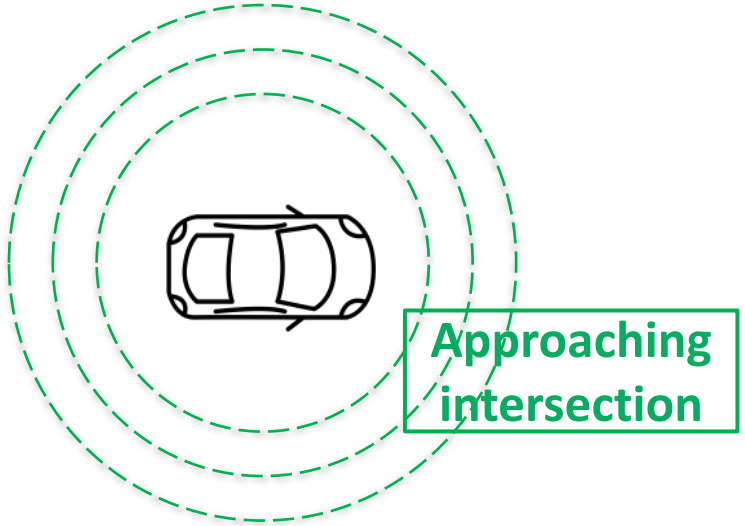
- Increases situational awareness

Described in

- **Dedicated Short Range Communication/Wireless Access in Vehicular Environments**
  IEEE 802.11p
- **Cellular Vehicle-to-Everything**
  3GPP Release 14/15



Basic Safety Messages (BSMs)



Every vehicle broadcasts 10 BSMs per second within transmission range

Direction

Speed

Time

Location

Brake and acceleration status

Introduction to **Secure** V2V Communication

IEEE 1609.2 Standard

Secure wireless communication

- secure transmission of messages
- cryptographic operations
- certificate management

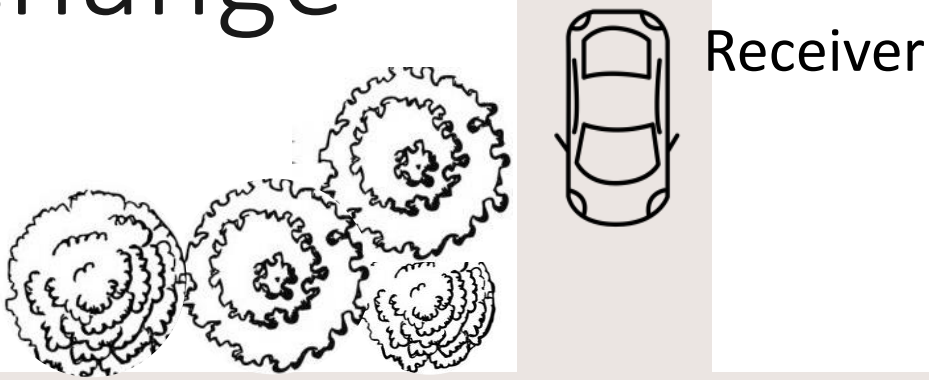
Security goal

"to protect messages from attacks such as eavesdropping, spoofing, alteration, and replay."[6]

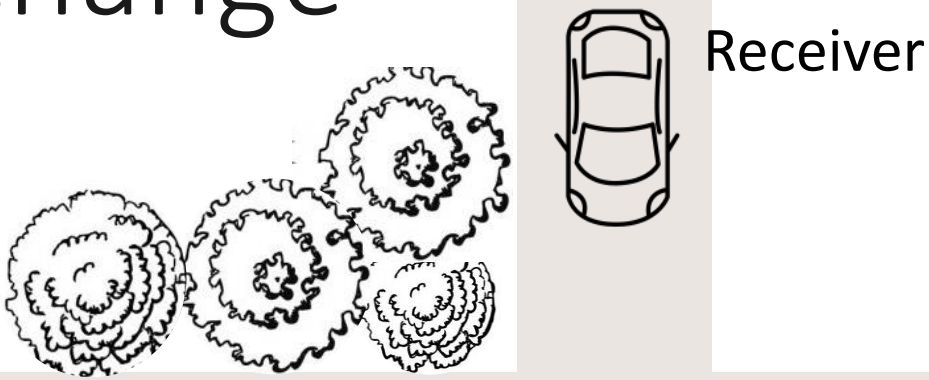
[6]IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages, IEEE Standard 1609.2, 2016.

.

Secure BSM Exchange (IEEE 1609.2)



Secure BSM Exchange (IEEE 1609.2)

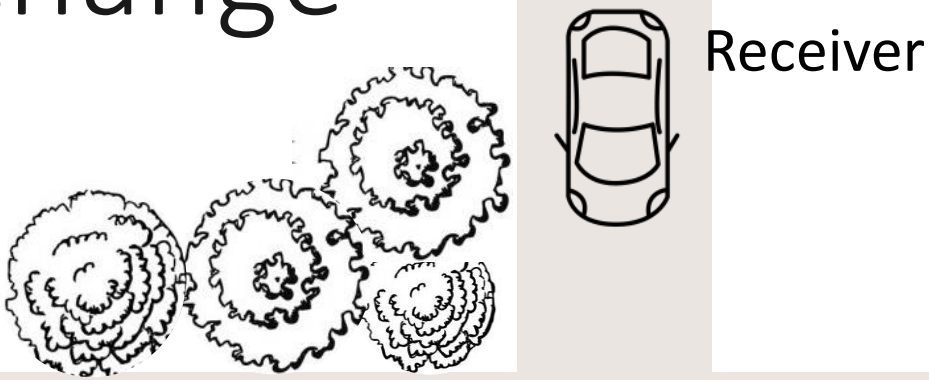


Receiver

Sender

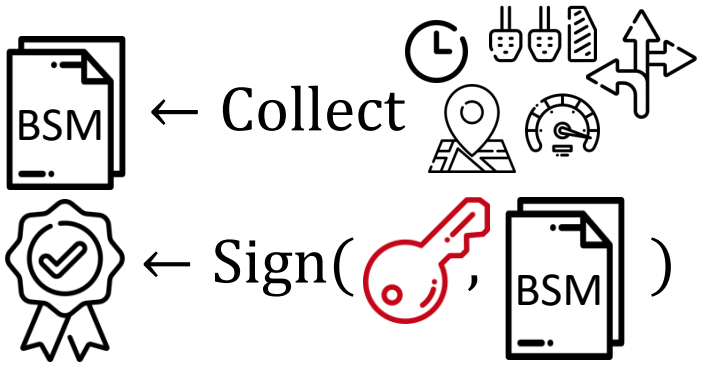
← Collect

Secure BSM Exchange (IEEE 1609.2)



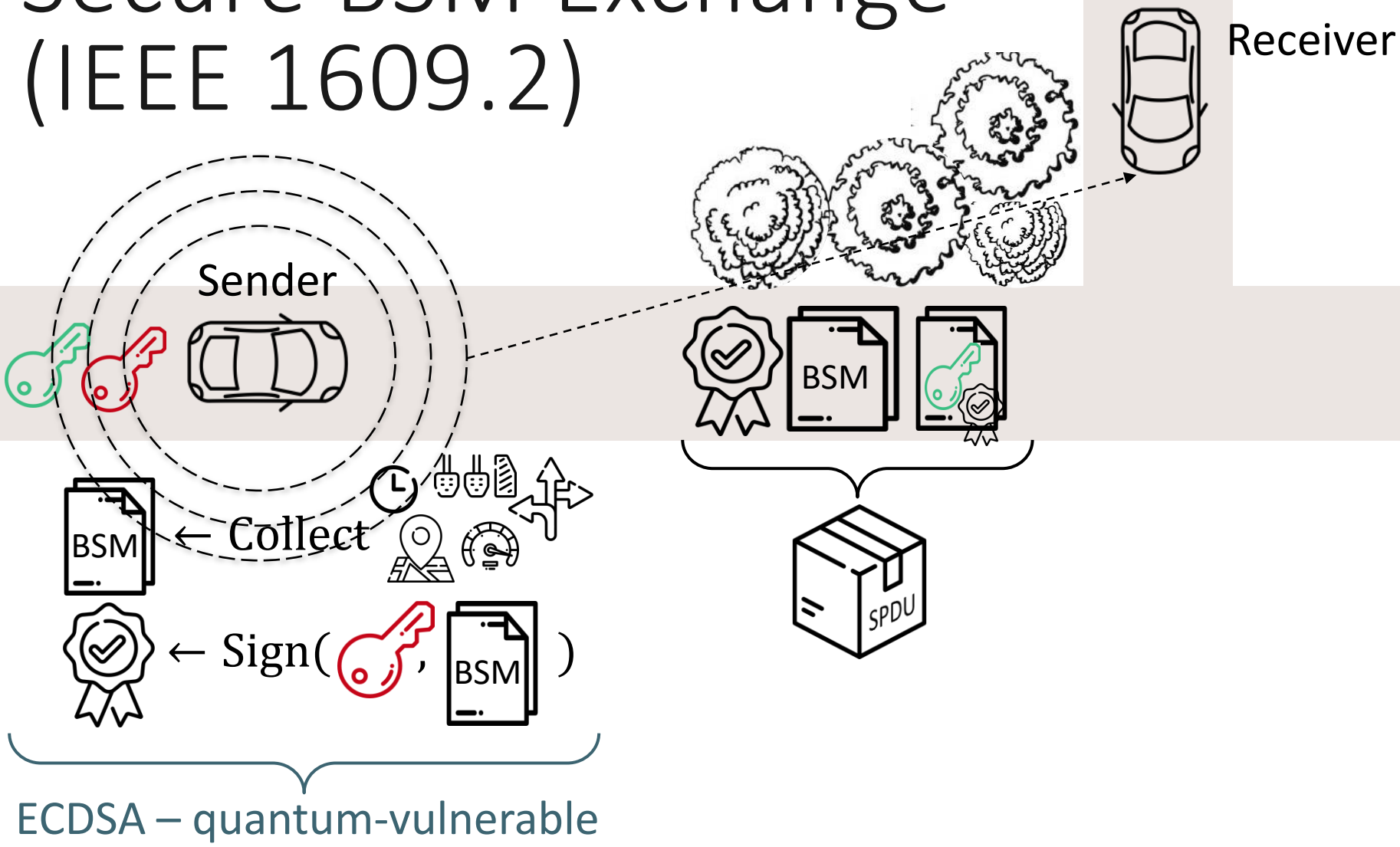
Receiver

Sender

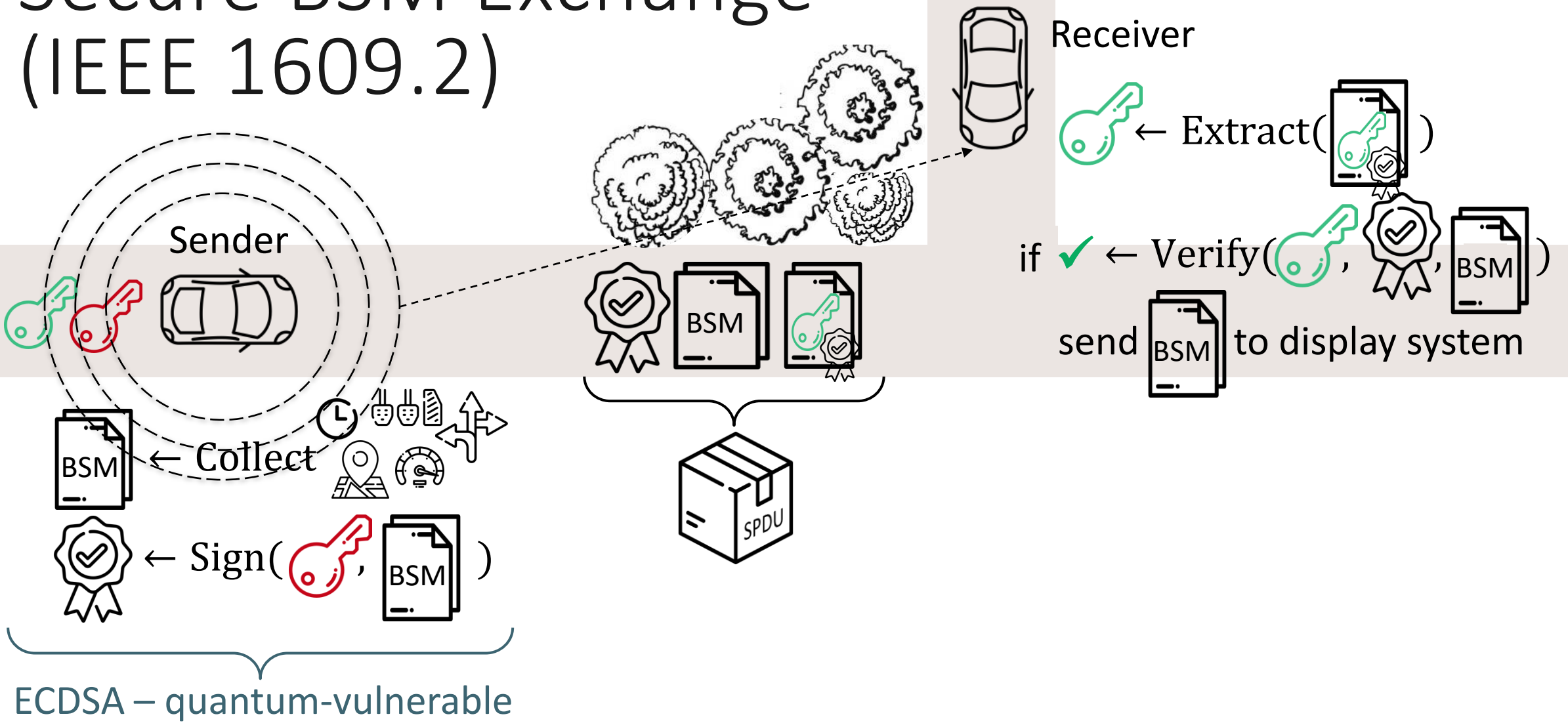


ECDSA – quantum-vulnerable

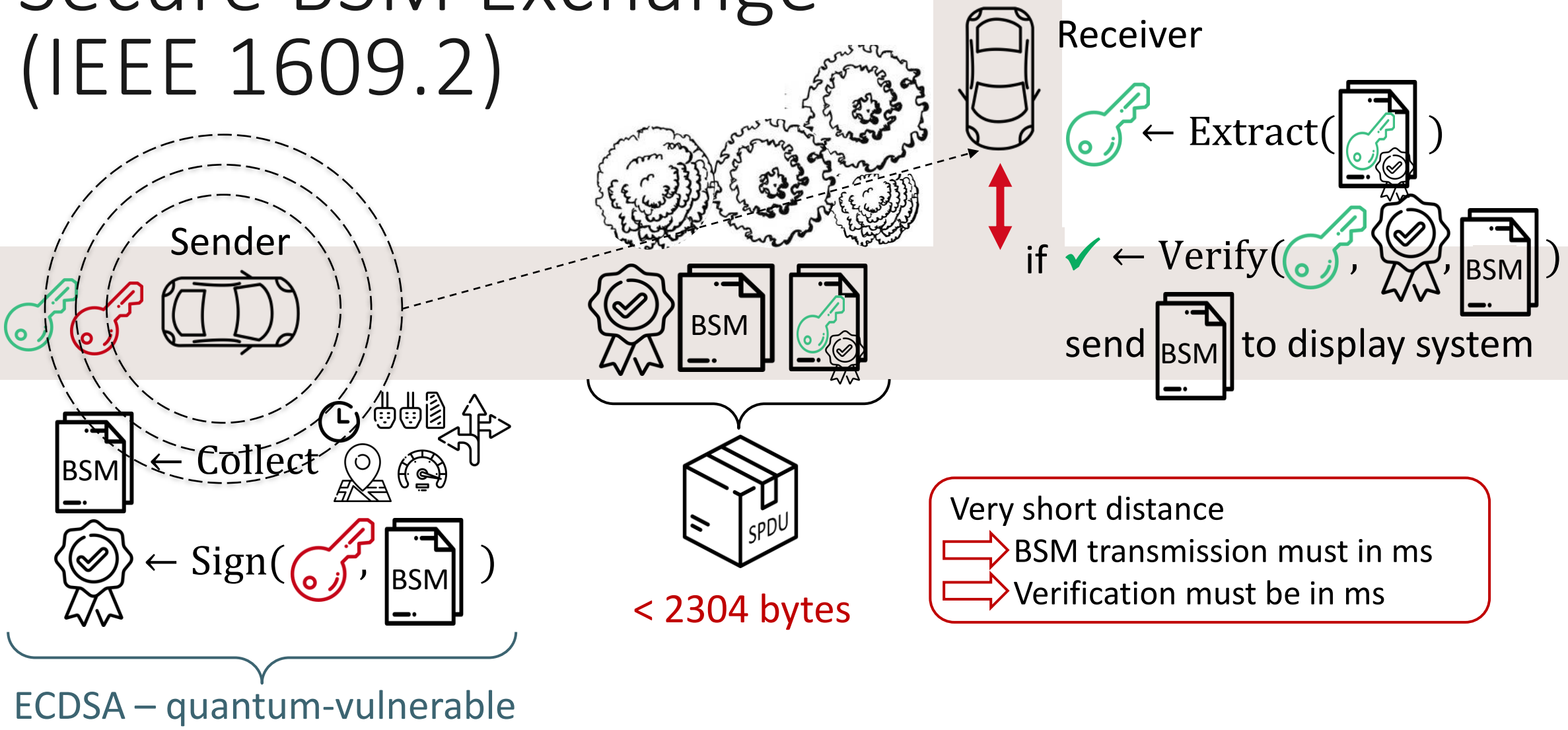
Secure BSM Exchange (IEEE 1609.2)



Secure BSM Exchange (IEEE 1609.2)

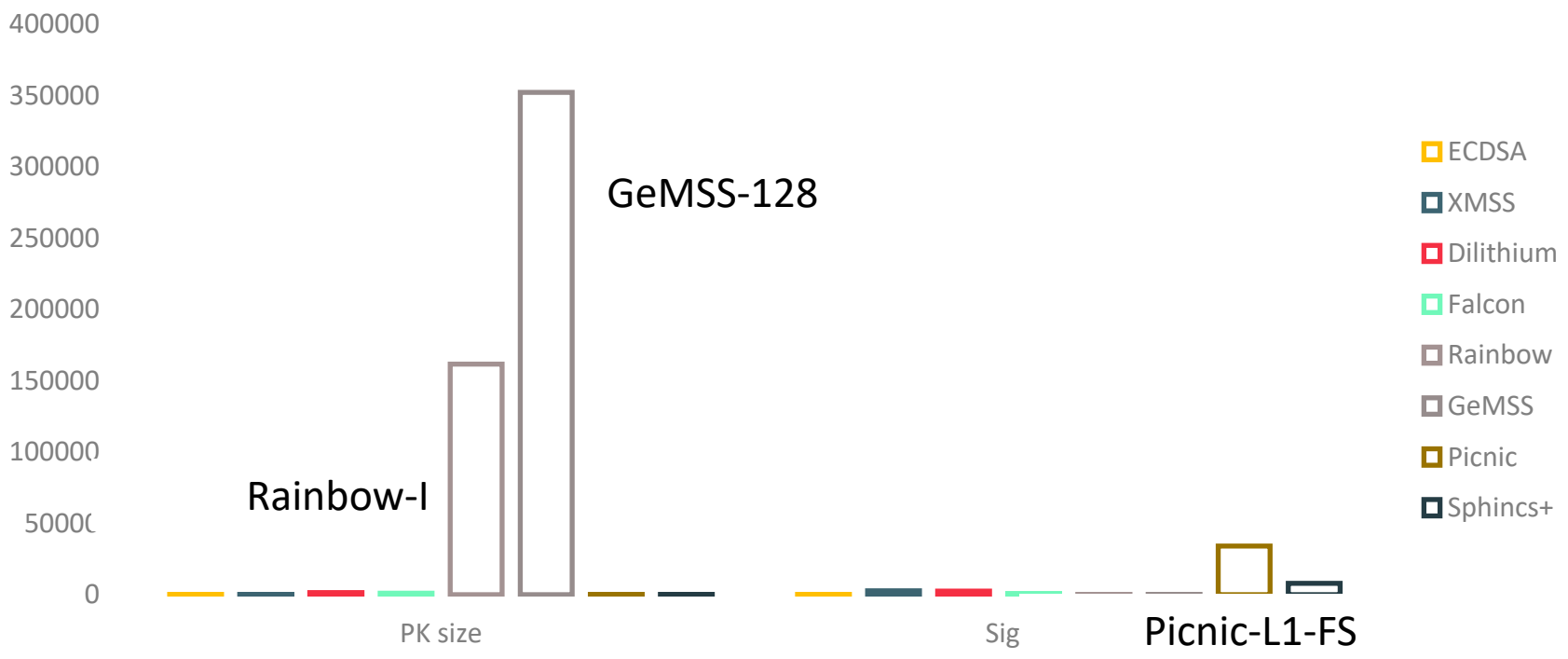


Secure BSM Exchange (IEEE 1609.2)

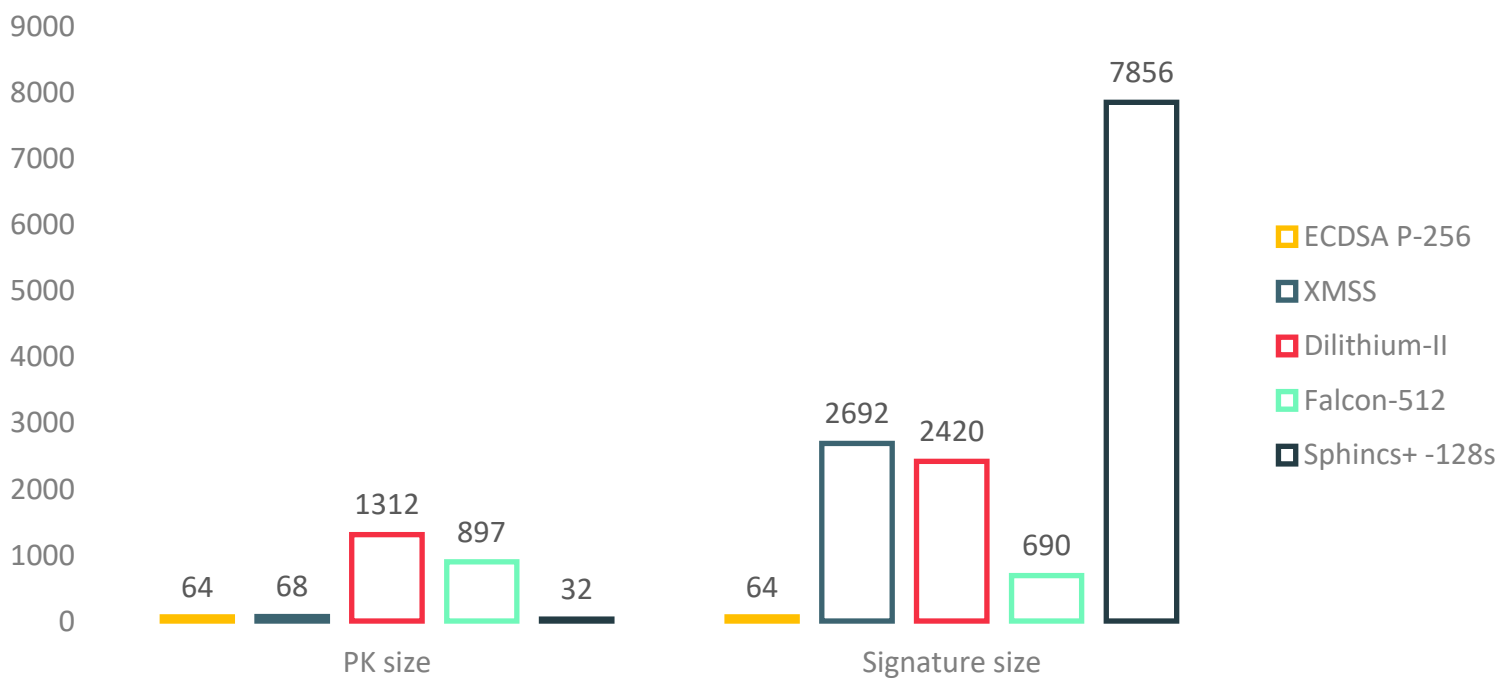


Challenges of PQ V2V Communication

Sizes of PQ Signature Candidates



Sizes of PQ Signature Candidates
(w/o Rainbow, GeMSS, Picnic)



Danger of BSM loss?

Explicit vs Implicit Certs

CA cert

Including $\mathrm{pk}_{\mathrm{CA}}$

$= \mathrm{Sign}_{\mathrm{CA}}(\mathrm{sk}_{\mathrm{CA}},$ [illegible] $)$

User explicit cert

Including pk_{U}, ID of issuing CA

$= \mathrm{Sign}_{\mathrm{CA}}(\mathrm{sk}_{\mathrm{CA}},$ [illegible] $)$

CA cert

Including $\mathrm{pk}_{\mathrm{CA}}$

$= \mathrm{Sign}_{\mathrm{CA}}(\mathrm{sk}_{\mathrm{CA}},$ [illegible] $)$

User implicit cert

Including reconstruction value R_{U}, ID of issuing CA

Explicit vs Implicit Certs

CA cert

Including $\mathrm{pk_{CA}}$

$= \mathrm{Sign_{CA}}(\mathrm{sk_{CA}},$ $)$

User explicit cert

Including $\mathrm{pk_U}$, ID of issuing CA

$= \mathrm{Sign_{CA}}(\mathrm{sk_{CA}},$ $)$

CA cert

Including $\mathrm{pk_{CA}}$

$= \mathrm{Sign_{CA}}(\mathrm{sk_{CA}},$ $)$

User implicit cert

Including reconstruction value $\mathrm{R_U}$, ID of issuing CA

Goal:

$| \quad | + |\mathrm{pk_U}| \geq |R_U|$

Explicit vs Implicit Certs

CA cert

Including $\mathrm{pk}_{\mathrm{CA}}$

$= \mathrm{Sign}_{\mathrm{CA}}(\mathrm{sk}_{\mathrm{CA}},$)

User explicit cert

Including pk_{U}, ID of issuing CA

$= \mathrm{Sign}_{\mathrm{CA}}(\mathrm{sk}_{\mathrm{CA}},$)

CA cert

Including $\mathrm{pk}_{\mathrm{CA}}$

$= \mathrm{Sign}_{\mathrm{CA}}(\mathrm{sk}_{\mathrm{CA}},$)

User implicit cert

Including reconstruction value R_{U}, ID of issuing CA

Goal:

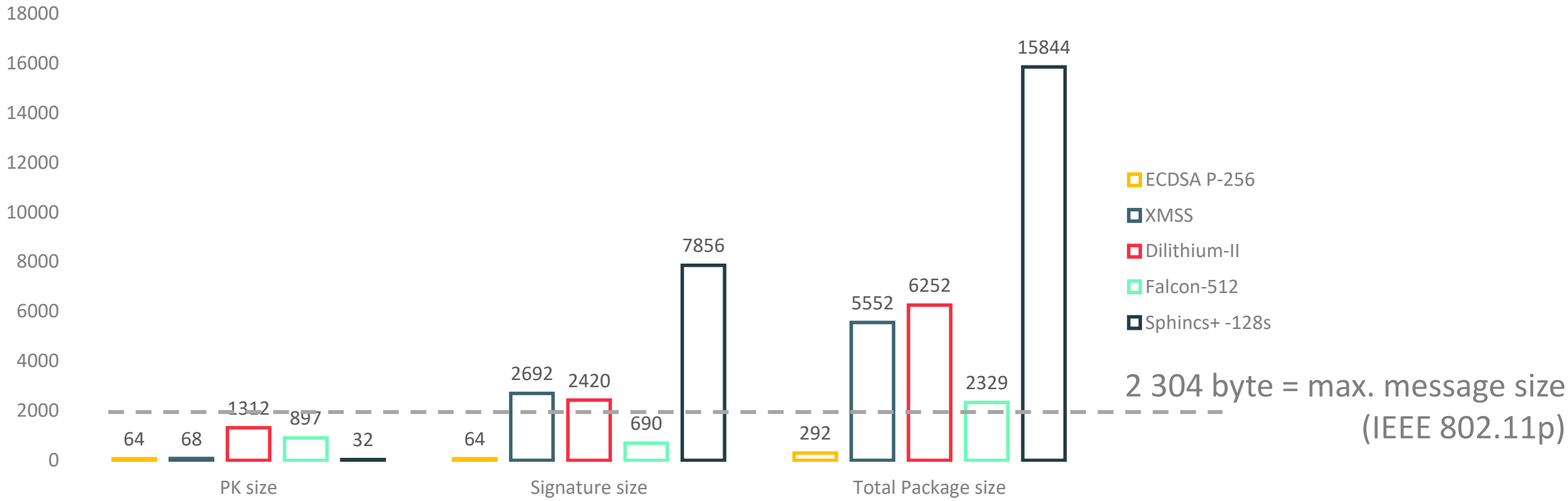
$| \quad | + |\mathrm{pk}_{\mathrm{U}}| \geq |R_U|$

Construction from elliptic curves:
Elliptic curve Qu-Vanstone scheme

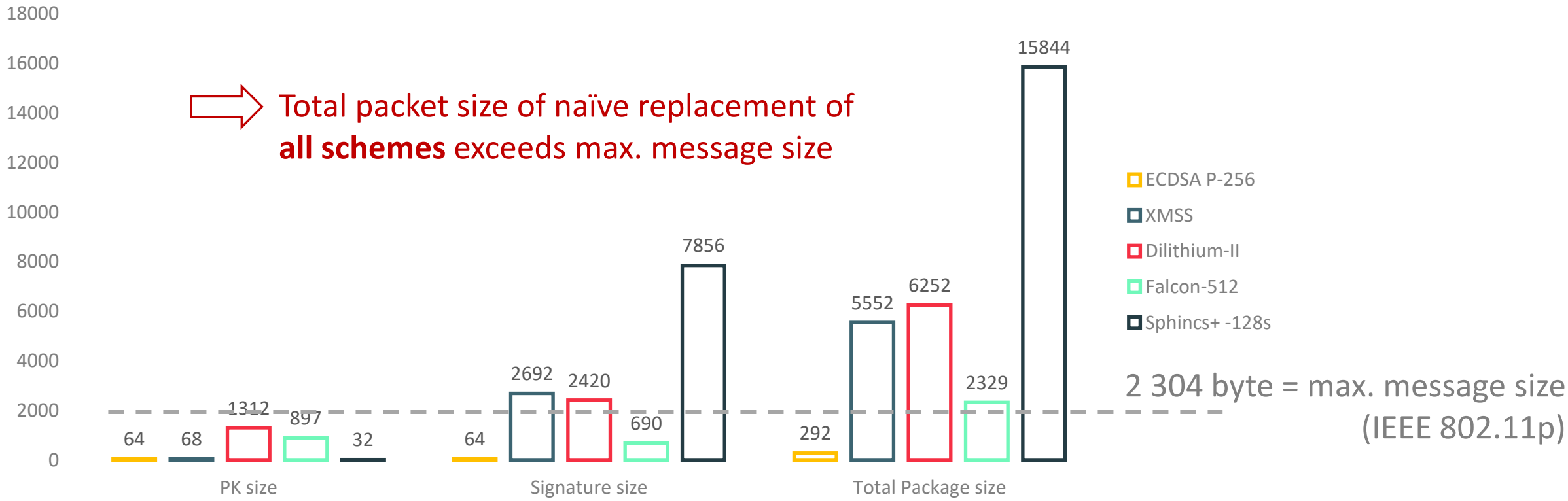
Construction from lattice/PQC:
???*

*The Need for Being Explicit When Communicating; N. Bindel & S. McCarthy; Cfail 2021

Total Package Sizes of Selected PQ Signature Candidates



Total Package Sizes of Selected PQ Signature Candidates



Standard-Compliant Classical-PQ Hybrid Solutions

Hybrid Approach Idea

Suggested by most standardization agencies, e.g. NIST, ETSI, IETF

Hybrid Approach Idea

Suggested by most standardization agencies, e.g. NIST, ETSI, IETF

S_1 - PQ

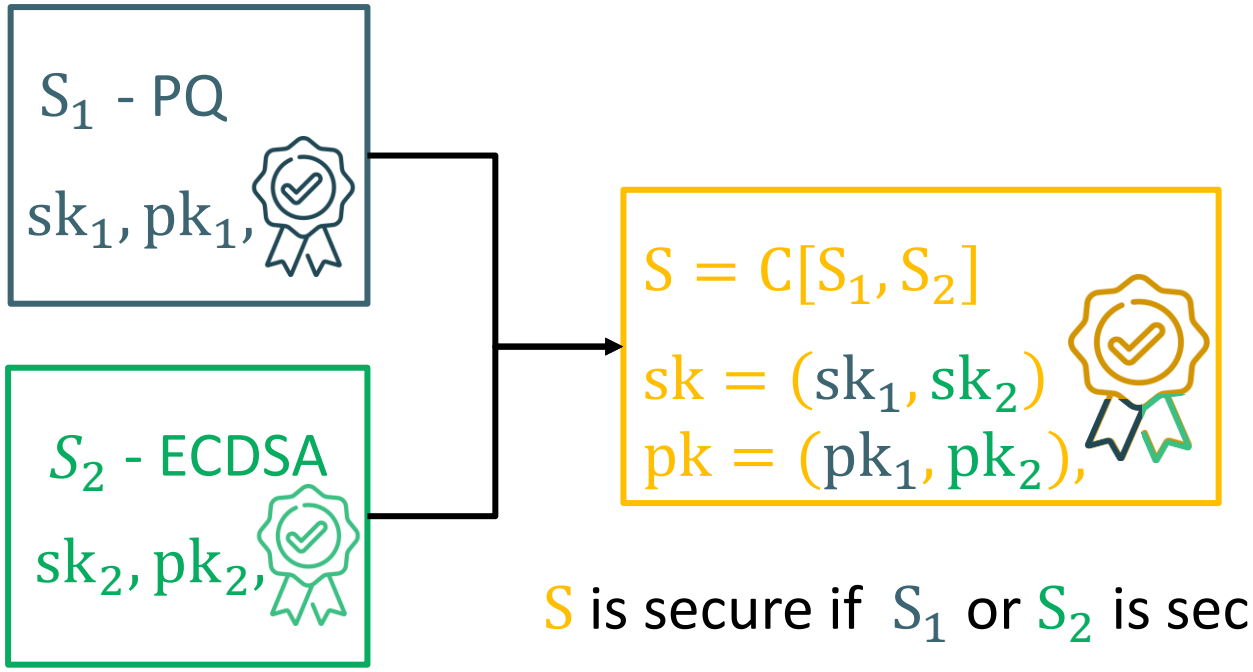
$\mathrm{sk}_1, \mathrm{pk}_1,$

S_2 - ECDSA

$\mathrm{sk}_2, \mathrm{pk}_2,$

Hybrid Approach Idea

Suggested by most standardization agencies, e.g. NIST, ETSI, IETF



S is secure if S_1 or S_2 is secure.

(SIMPLIFIED) TRUE HYBRID

Sender S

Receiver R

$\mathrm{Cert_S} = ($, $)$

$h = \mathrm{Hash}(\mathrm{Cert_S})$

PQ (Falcon)

ECDSA

Hybrid

$\mathrm{sk} = (\mathrm{sk_S^c}, \mathrm{sk_S^{pq}})$

$\mathrm{pk} = (\mathrm{pk_S^c}, \mathrm{pk_S^{pq}})$

(SIMPLIFIED) TRUE HYBRID

PQ (Falcon)

ECDSA

Hybrid

$sk = (sk_S^c, sk_S^{pq})$

$pk = (pk_S^c, pk_S^{pq})$

Sender S

$Cert_S = ($  ,  $)$

$h = Hash(Cert_S)$

Repeat every 5 BSMs:

$SPDU_1 = (BSM_1,$  ,  ,  $)$

Receiver R

$SPDU_1 \longrightarrow$ Verify  using pk_S^c from 

(SIMPLIFIED) TRUE HYBRID

PQ (Falcon)

ECDSA

Hybrid

$sk = (sk_S^c, sk_S^{pq})$

$pk = (pk_S^c, pk_S^{pq})$

Sender S

Receiver R

$Cert_S = ($, $)$

$h = Hash(Cert_S)$

Repeat every 5 BSMs:

$SPDU_1 = (BSM_1,$, , $)$

$\xrightarrow{SPDU_1}$ Verify using pk_S^c from

$SPDU_{2,3,4,5} = (BSM_i,$, $h)$

$\xrightarrow{SPDU_{2,3,4,5}}$ Verify using pk_S^c from and pk_S^{pq} from

(SIMPLIFIED) TRUE HYBRID

PQ (Falcon)

ECDSA

Hybrid

$$sk = (sk_S^c, sk_S^{pq})$$
$$pk = (pk_S^c, pk_S^{pq})$$

Sender S

Receiver R

$$Cert_S = (\, , \,)$$

$$h = Hash(Cert_S)$$

Repeat every 5 BSMs:

$$\underbrace{SPDU_1 = (BSM_1, \, , \, , \,)}_{\textbf{1 835 byte < 2 304 byte}}$$

$SPDU_1$ → Verify using pk_S^c from

$$SPDU_{2,3,4,5} = (BSM_i, \underbrace{\, , \, }_{\textbf{730 byte}}, h)$$

$SPDU_{2,3,4,5}$ → Verify using pk_S^c from and pk_S^{pq} from

Comparison of Resulting SPDUs

Design	SPDU 1	SPDU 2	SPDU 3	SPDU 4	SPDU 5
Pure ECDSA	248	144	144	144	144
True hybrid w/ Falcon	1,835	834	834	834	834

Classical and PQ security guarantees

Comparison of Resulting SPDUs

Design	SPDU 1	SPDU 2	SPDU 3	SPDU 4	SPDU 5
Pure ECDSA	248	144	144	144	144
True hybrid w/ Falcon	1,835	834	834	834	834

Classical and PQ security guarantees

Security threat due to packet loss
>>
Security threat due to signature forgeries by quantum attackers

(SIMPLIFIED) PARTIALLY PQ HYBRID

Idea:

- ECDSA pk valid for one week, changed every 5 min

⇨ sk cannot be computed even by QC

ECDSA cert

pk_S^c

$= \mathrm{sign}^{\mathrm{ECDSA}}(\mathrm{pk}_S^c)$ by a CA

PQ cert

pk_S^c

$= \mathrm{sign}^{\mathrm{PQ}}(\mathrm{pk}_S^c)$ by a CA

(SIMPLIFIED) PARTIALLY PQ HYBRID

ECDSA cert

pk_S^c

$= \mathrm{sign}^{\mathrm{ECDSA}}(\mathrm{pk}_S^c)$ by a CA

PQ cert

pk_S^c

$= \mathrm{sign}^{\mathrm{PQ}}(\mathrm{pk}_S^c)$ by a CA

Idea:

- ECDSA pk valid for one week, changed every 5 min

⇨ sk cannot be computed even by QC

- CA's (pk,sk) valid long enough to be vulnerable

⇨ CA's signature potentially forged by QC

(SIMPLIFIED) PARTIALLY PQ HYBRID

ECDSA cert

pk_S^c

$= \mathrm{sign}^{\mathrm{ECDSA}}(\mathrm{pk}_S^c)$ by a CA

PQ cert

pk_S^c

$= \mathrm{sign}^{\mathrm{PQ}}(\mathrm{pk}_S^c)$ by a CA

Idea:

- ECDSA pk valid for one week, changed every 5 min

⇨ sk cannot be computed even by QC

- CA's (pk,sk) valid long enough to be vulnerable

⇨ CA's signature potentially forged by QC

⇨ Enough to protect integrity of ECDSA keys with PQ signatures

(SIMPLIFIED) PARTIALLY PQ HYBRID

Sender S

$\mathrm{Cert_S} = (\, , \,)$

$\mathrm{h} = \mathrm{Hash}(\mathrm{Cert_S})$

$\mathrm{h^c} = \mathrm{Hash}(\,)$

$\mathrm{C_1}, \ldots, \mathrm{C_4} = \mathrm{Fragment}(\,)$

Repeat every 5 BSMs:

$\mathrm{SPDU_1} = (\mathrm{BSM_1}, \, , \, , \mathrm{C_1})$ $\xrightarrow{\mathrm{SPDU_1}}$ Verify using $\mathrm{pk_S^c}$ from

$\mathrm{SPDU_{2,3,4}} = (\mathrm{BSM_2}, \, , \mathrm{C}_i, \mathrm{h^c})$

$\xrightarrow{\mathrm{SPDU_{2,3,4}}}$ Verify using $\mathrm{pk_S^c}$ from

Check $\mathrm{pk_S^c}$ from = $\mathrm{pk_S^c}$ from

Receiver R

ECDSA cert

$\mathrm{pk_S^c}$

$= \mathrm{sign^{ECDSA}}(\mathrm{pk_S^c})$ by a CA

PQ cert

$\mathrm{pk_S^c}$

$= \mathrm{sign^{PQ}}(\mathrm{pk_S^c})$ by a CA

(SIMPLIFIED) PARTIALLY PQ HYBRID

Sender S

$\mathrm{Cert_S} = (\, , \,)$

$\mathrm{h} = \mathrm{Hash}(\mathrm{Cert_S})$

$\mathrm{h^c} = \mathrm{Hash}(\,)$

$\mathrm{C_1}, \ldots, \mathrm{C_4} = \mathrm{Fragment}(\,)$

Repeat every 5 BSMs:

$\mathrm{SPDU_1} = (\mathrm{BSM_1}, \, , \, , \mathrm{C_1})$ —$\mathrm{SPDU_1}$→ Verify using $\mathrm{pk_S^c}$ from

$\mathrm{SPDU_{2,3,4}} = (\mathrm{BSM_2}, \, , \mathrm{C}_i, \mathrm{h^c})$

—$\mathrm{SPDU_{2,3,4}}$→ Verify using $\mathrm{pk_S^c}$ from

Check $\mathrm{pk_S^c}$ from = $\mathrm{pk_S^c}$ from

$\mathrm{SPDU_5} = (\mathrm{BSM_i}, \, , \mathrm{h})$

—$\mathrm{SPDU_5}$→ Verify using $\mathrm{pk_S^c}$ from

Receiver R

ECDSA cert

$\mathrm{pk_S^c}$

$= \mathrm{sign^{ECDSA}}(\mathrm{pk_S^c})$ by a CA

PQ cert

$\mathrm{pk_S^c}$

$= \mathrm{sign^{PQ}}(\mathrm{pk_S^c})$ by a CA

Comparison of Resulting Sizes

Design	SPDU 1	SPDU 2	SPDU 3	SPDU 4	SPDU 5
Pure ECDSA					
True hybrid w/ Falcon					
Partially PQ hybrid w/ Falcon					
Partially PQ hybrid w/ Dilithium					
Partially PQ hybrid w/ Sphincs+					
Partially PQ hybrid w/ XMSS					

Comparison of Resulting Sizes

Design	SPDU 1	SPDU 2	SPDU 3	SPDU 4	SPDU 5	max. #vehicles
Pure ECDSA						183
True hybrid w/ Falcon						31
Partially PQ hybrid w/ Falcon						107
Partially PQ hybrid w/ Dilithium						54
Partially PQ hybrid w/ Sphincs+						21
Partially PQ hybrid w/ XMSS						50

Comparison of Resulting Sizes

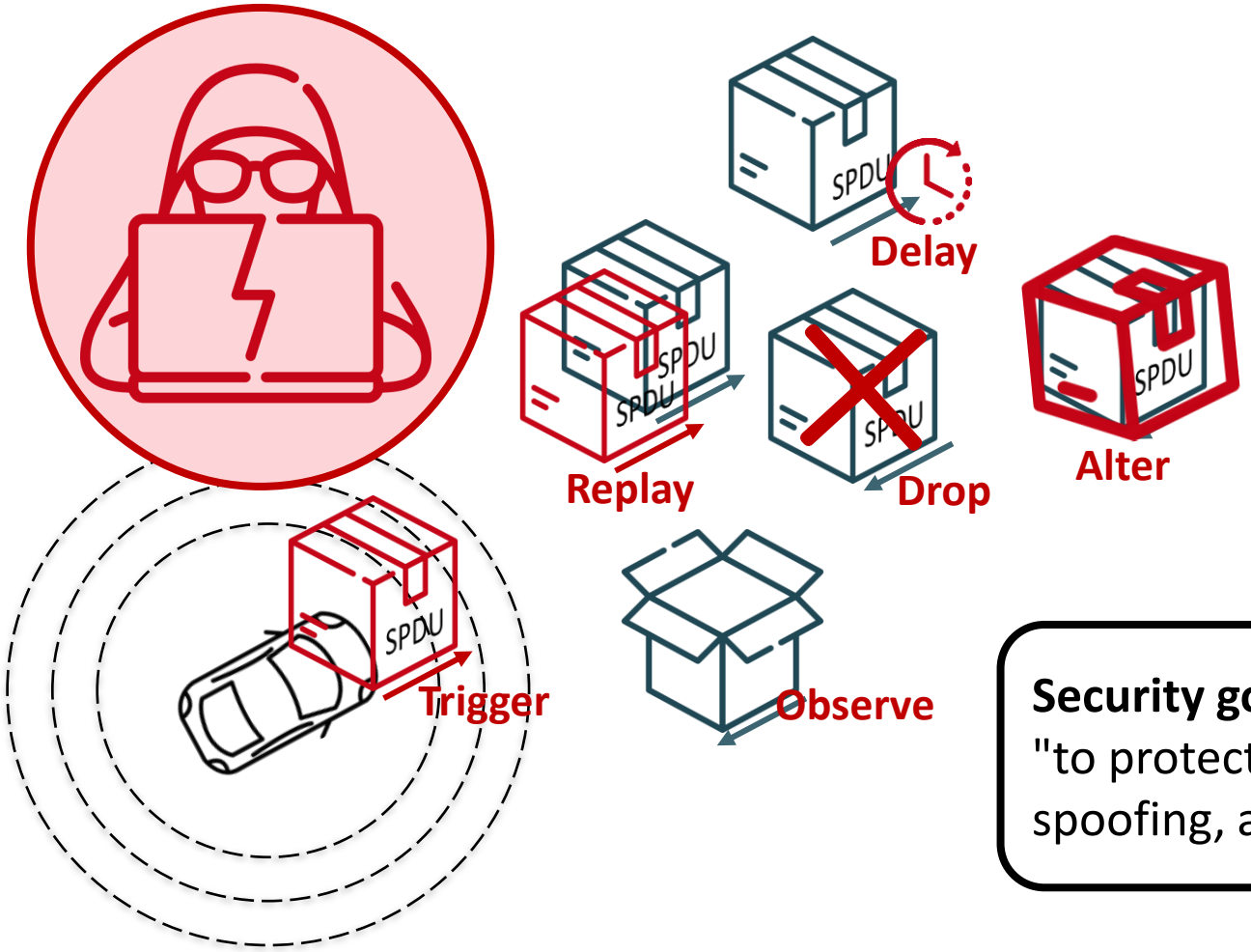
Design	SPDU 1	SPDU 2	SPDU 3	SPDU 4	SPDU 5	max. #vehicles
Pure ECDSA						183
True hybrid w/ Falcon						31
Partially PQ hybrid w/ Falcon						107
Partially PQ hybrid w/ Dilithium						54
Partially PQ hybrid w/ Sphincs+						21
Partially PQ hybrid w/ XMSS						50

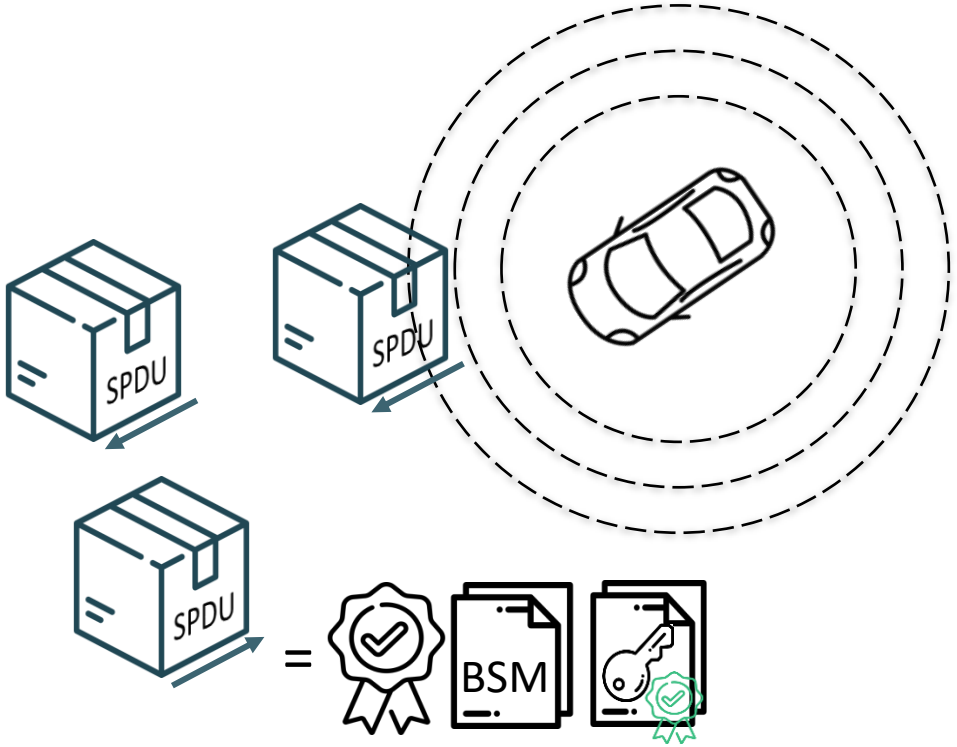
Use clever sieving algorithms to prioritize messages [DR21]

Threat Model and Limitations

Security goal
"to protect messages from attacks such as eavesdropping, spoofing, alteration, and replay.“ (IEEE 1609.2)

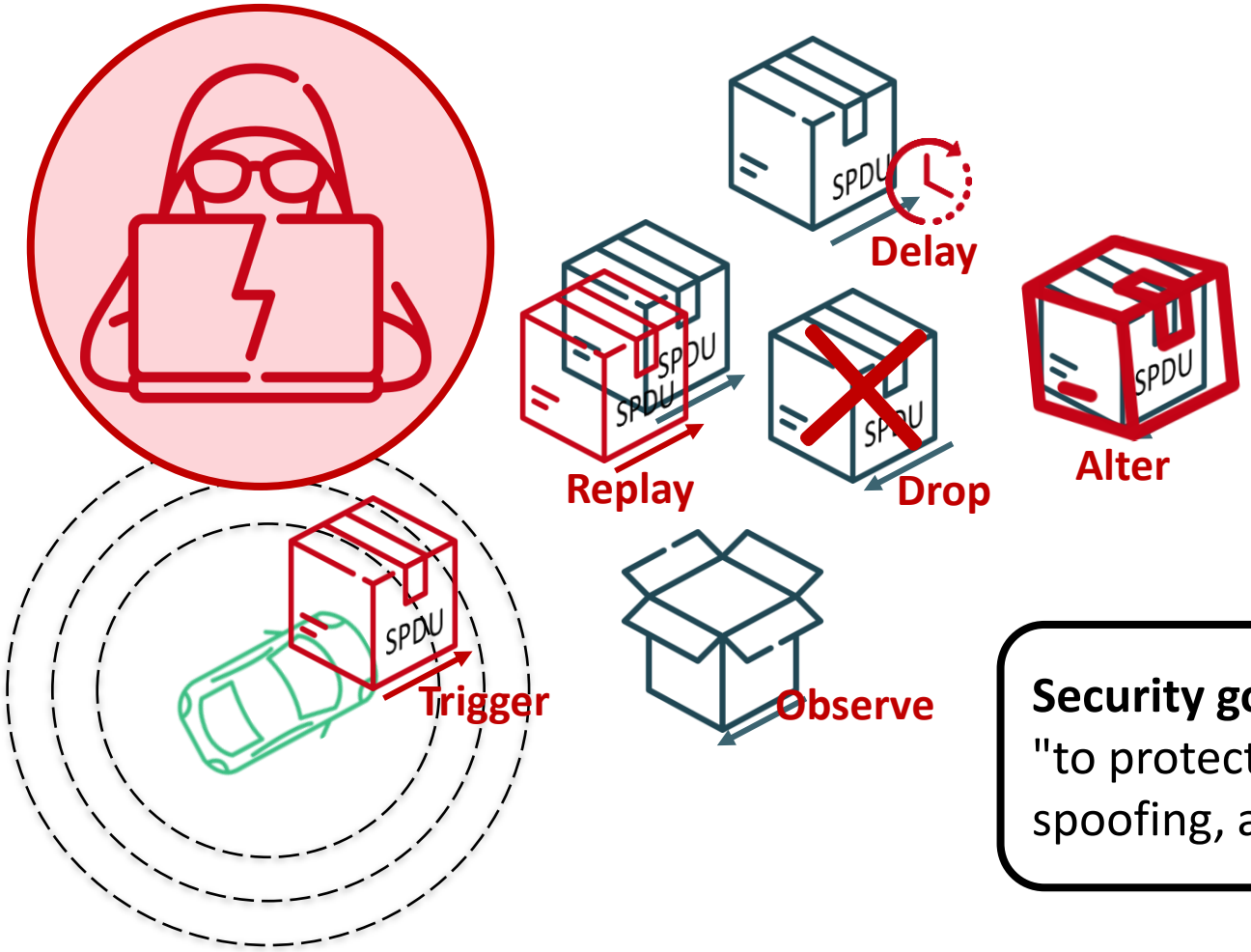
Threat Model



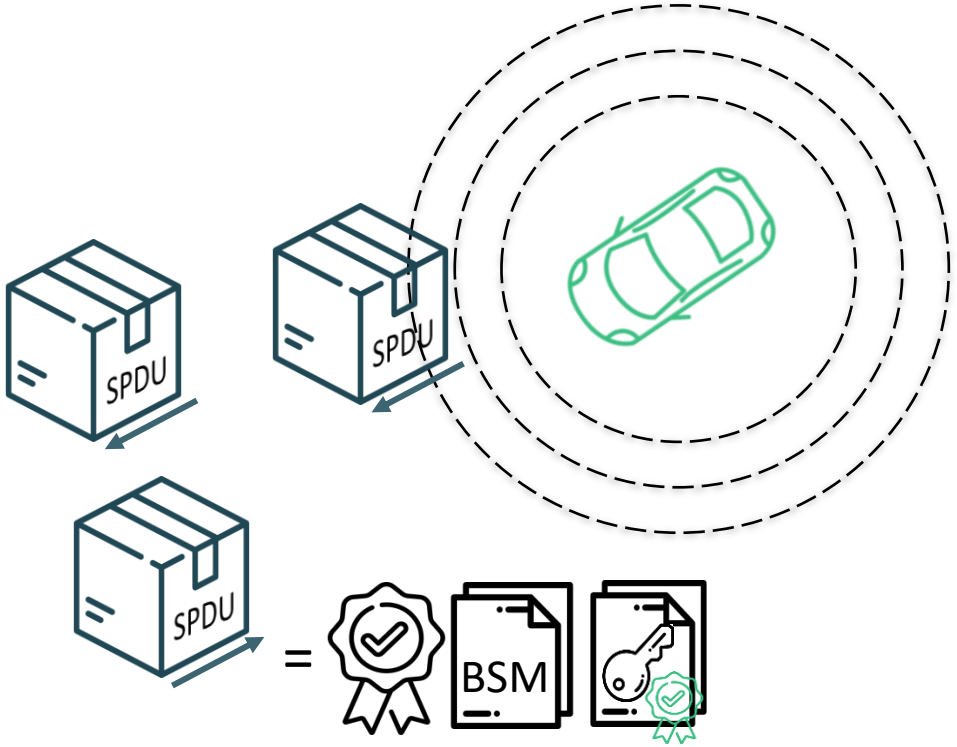


Security goal
"to protect messages from attacks such as eavesdropping, spoofing, alteration, and replay.“ (IEEE 1609.2)

Threat Model



No side-channel attacks



- CA honest
- Immediate verify of cert

Security goal
"to protect messages from attacks such as eavesdropping, spoofing, alteration, and replay.“ (IEEE 1609.2)

Summary

Summary

- **Naive swap** of ECDSA with PQ signatures is **not possible** under current standards.

Summary

- **Naive swap** of ECDSA with PQ signatures is **not possible** under current standards.
- Proposed a **practical hybrid** V2V solution that adds **PQ security** and **satisfies constraints** of standards.
- Enabled by **careful analysis of quantum power** and **tailoring** of PQ extension to the application.

Summary

- **Naive swap** of ECDSA with PQ signatures is **not possible** under current standards.
- Proposed a **practical hybrid** V2V solution that adds **PQ security** and **satisfies constraints** of standards.
- Enabled by **careful analysis of quantum power** and **tailoring** of PQ extension to the application.

- **There is still lots to do!**

Summary

- **Naive swap** of ECDSA with PQ signatures is **not possible** under current standards.
- Proposed a **practical hybrid** V2V solution that adds **PQ security** and **satisfies constraints** of standards.
- Enabled by **careful analysis of quantum power** and **tailoring** of PQ extension to the application.

- **There is still lots to do!**

THANK YOU.

Nina Bindel
ninabindel.de
nina.bindel@tu-darmstadt.de

Sarah McCarthy
cryptomccarthy.com
sarah.mccarthy@uwaterloo.ca

Geoff Twardokus
gdt5762@rit.edu

Hanif Rahbari
https://www.rit.edu/wisplab/
rahbari@mail.rit.edu

Bibliography

[BHM+17] N. Bindel, U. Herath, M. McKague, D. Stebila. Transitioning to a Quantum-Resistant Public-Key Infrastructure. PQCrypto 2017.

[BBF+19] N. Bindel, J. Brendel, M. Fischlin, B. Gonzales, D. Stebila. Hybrid Key Encapsulation Mechanisms and Authenticated Key Exchange. PQCrypto *2019.*

[BMRT21] N. Bindel, S. McCarthy, H. Rahbari, G. Twardokus. Drive (Quantum) Safe! --Towards Post-Quantum Security for Vehicle-to-Vehicle Communications. Forth coming. 2021

[KPD+18] P. Kampanakis, P. Panburana, E. Daw, D. Van Geest . The Viability of Post-quantum X.509 Certificates. Cryptology ePrint Archive: Report 2018/063.

[DR21] S. Dongre, H. Rahbari. Message Sieving to Mitigate Smart Gridlock Attacks in V2V. WiSec ’21. ACM.

[SKD20] D. Sikeridis, P. Kampanakis, M. Devetsikiotis. Post-Quantum Authentication in TLS 1.3: A Performance Study. Cryptology ePrint Archive: Report 2020/071.