The Need for Being Explicit When Communicating

CFAIL 2021
August 14, 2021

Nina Bindel
Sarah McCarthy

UNIVERSITY OF WATERLOO
IQC Institute for Quantum Computing

OUTLINE

Transition to Quantum-Secure Algorithms

The Use of Certificates in Vehicle-to-Vehicle (V2V) Communication

Explicit vs Implicit Certificates

Constructing Implicit Certificates

Implicit Certificates From Lattices

Potential future directions

Shor‘s quantum algorithm

Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

Peter W. Shor†

Abstract

A digital computer is generally believed to be an efficient universal computing device; that is, it is believed able to simulate any physical computing device with an increase in computation time by at most a polynomial factor. This may not be true when quantum mechanics is taken into consideration. This paper considers factoring integers and finding discrete logarithms, two problems which are generally thought to be hard on a classical computer and which have been used as the basis of several proposed cryptosystems. Efficient randomized algorithms are given for these two problems on a hypothetical quantum computer. These algorithms take a number of steps polynomial in the input size, e.g., the number of digits of the integer to be factored.

3

Quantum computers: State-of-the-art

Jul. 2017 — 51 qubits
HARVARD UNIVERSITY

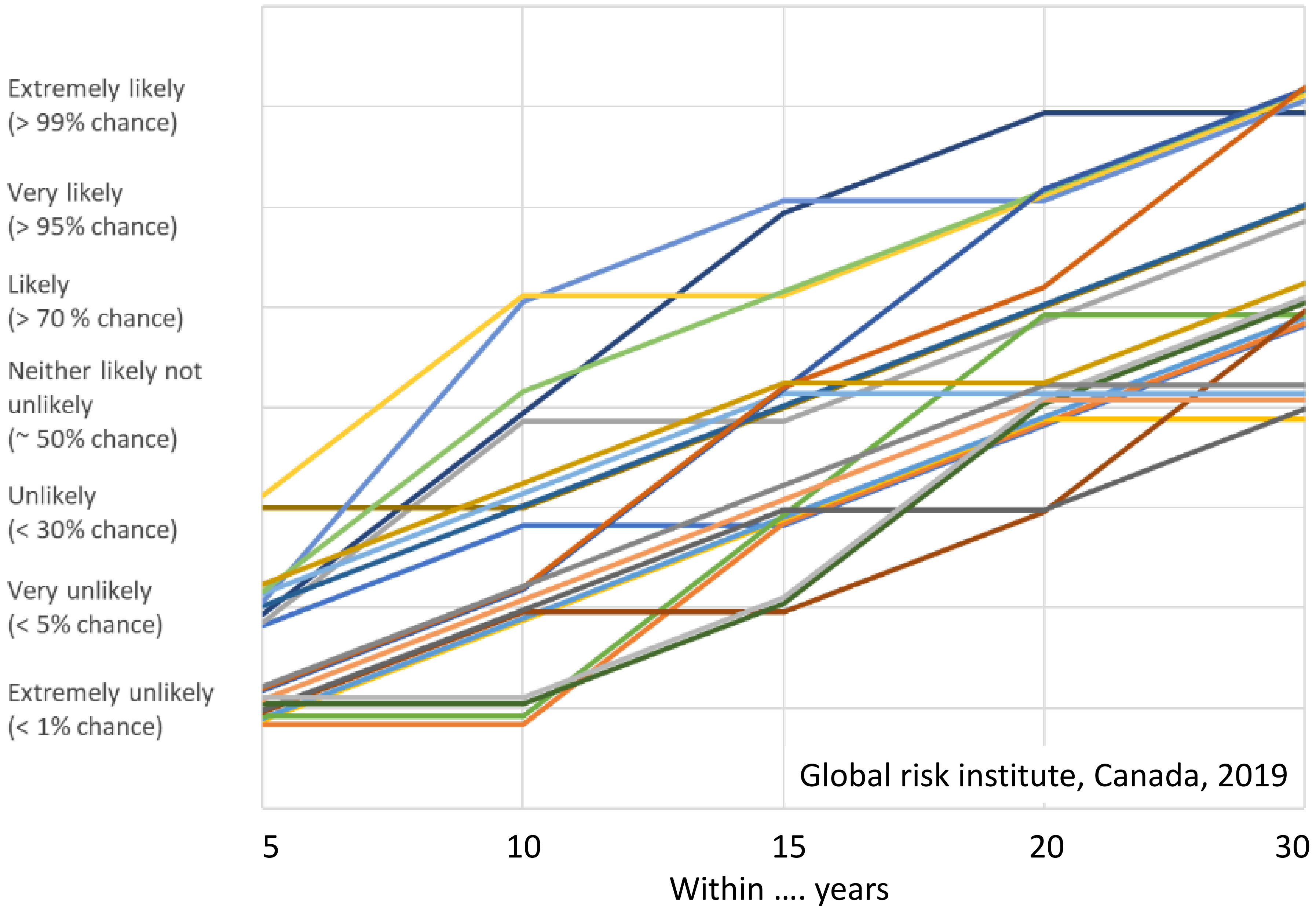
Feb. 2018 — 72 qubits
Google

Sep. 2019 — "Quantum supremacy"
Google

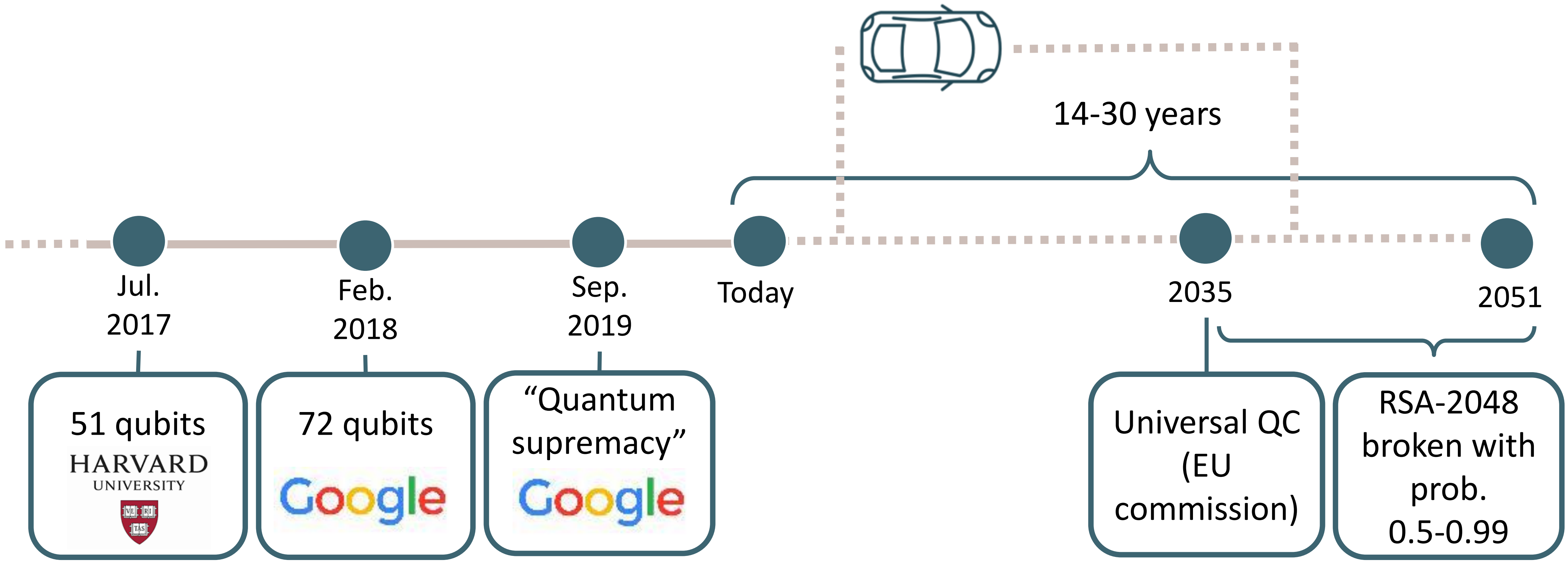
Today

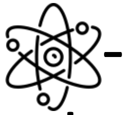
20 million qubits needed to break RSA-2048 [GK19]

Expert opinions about likelihood of a quantum computer able to break RSA-2048 in 24 hours

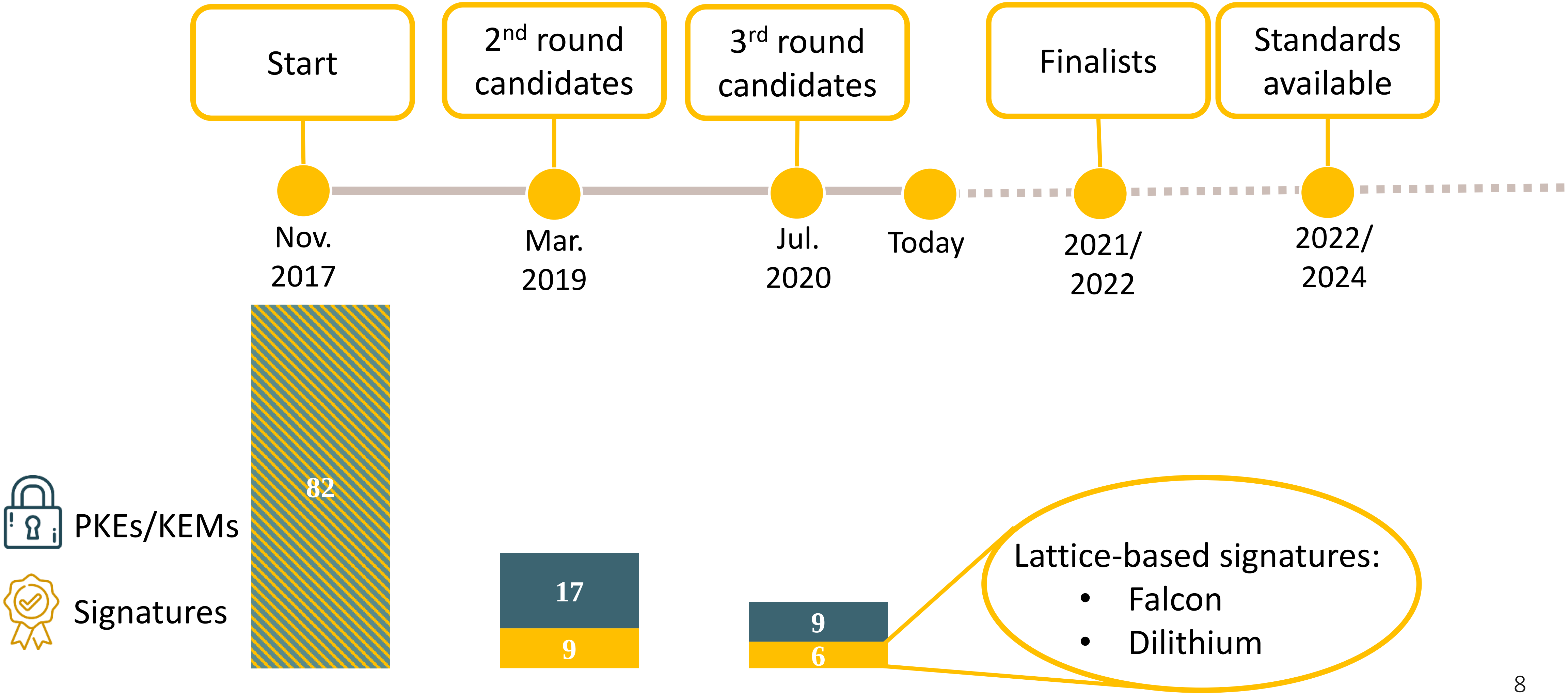


Quantum computers: State-of-the-art



Need to prepare transition to -secure algorithms

NIST post-quantum standardization



OUTLINE

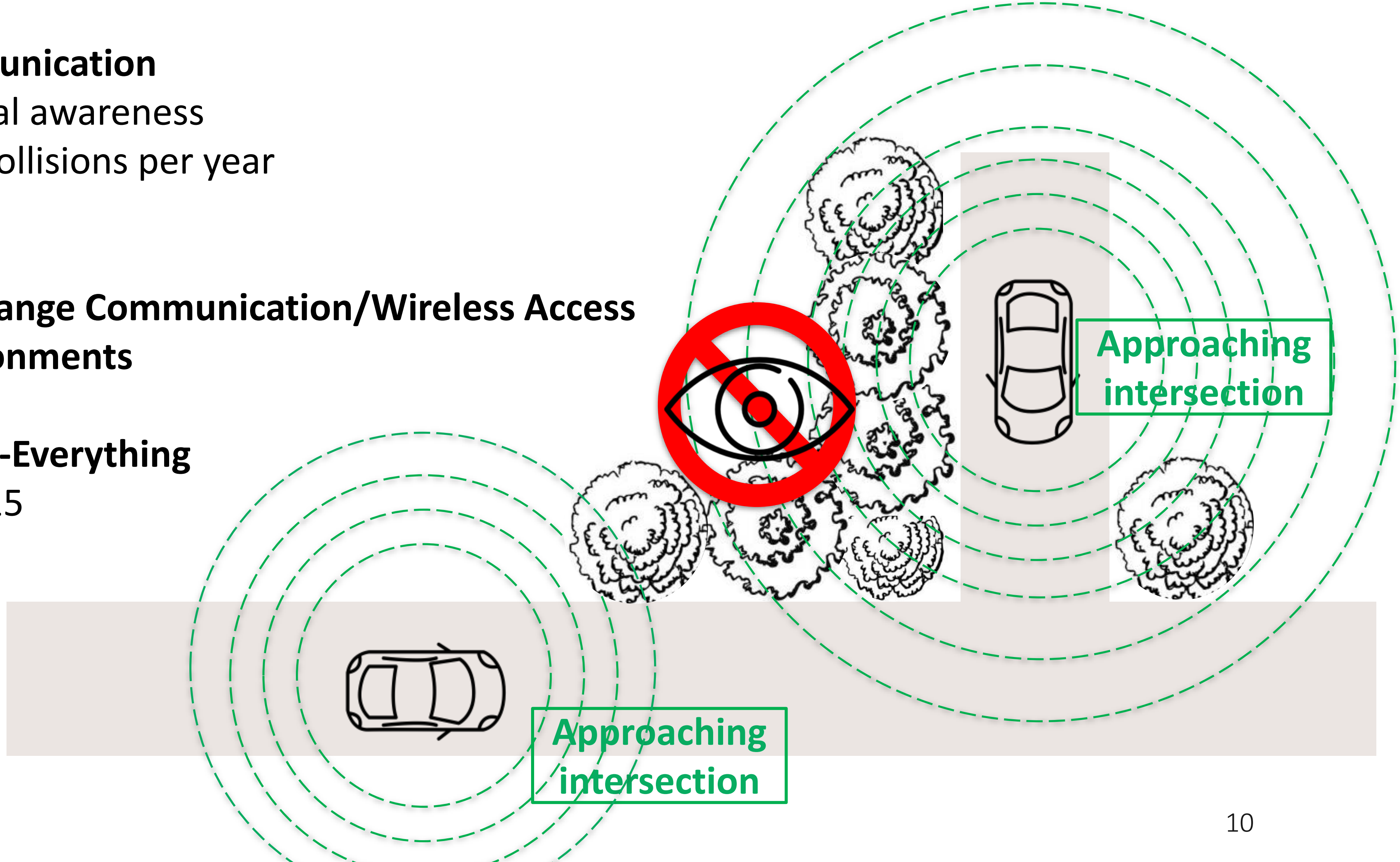
V2V Communication

Direct wireless communication

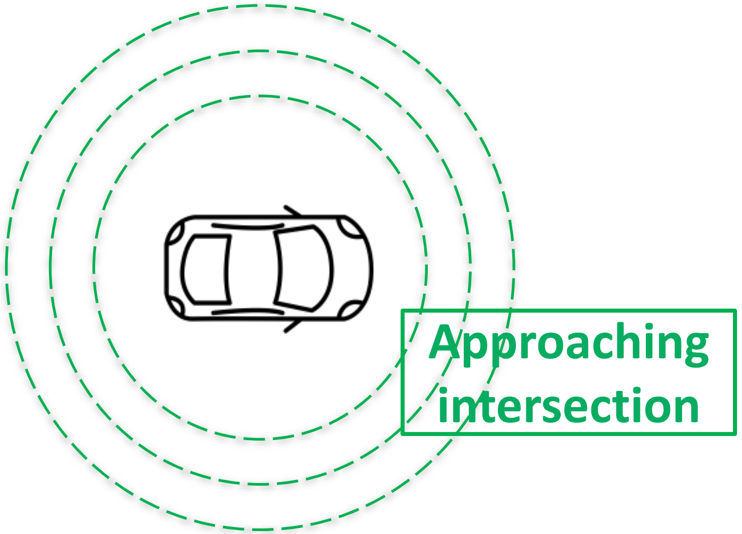
- Increases situational awareness
- Prevents 600,000 collisions per year

Described in

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

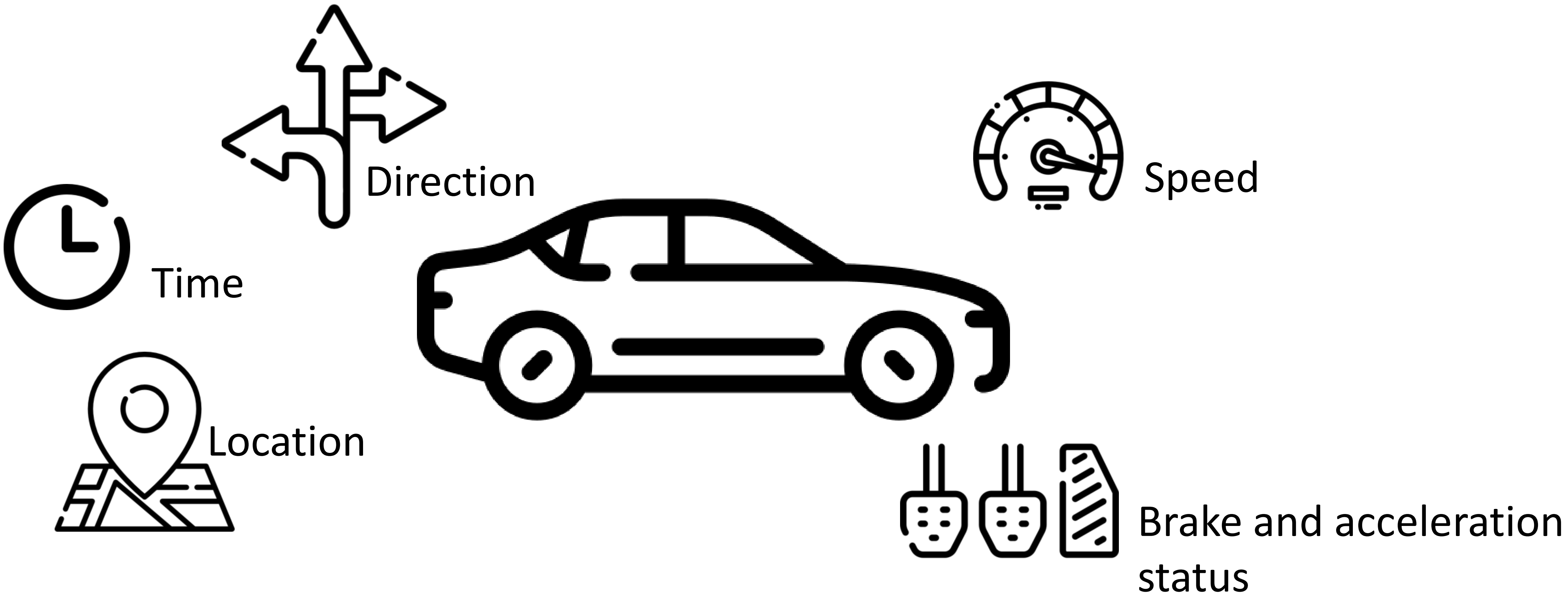


Basic Safety Messages (BSMs)



Every vehicle broadcasts 10 BSMs per second within transmission range

Information Collected in BSMs

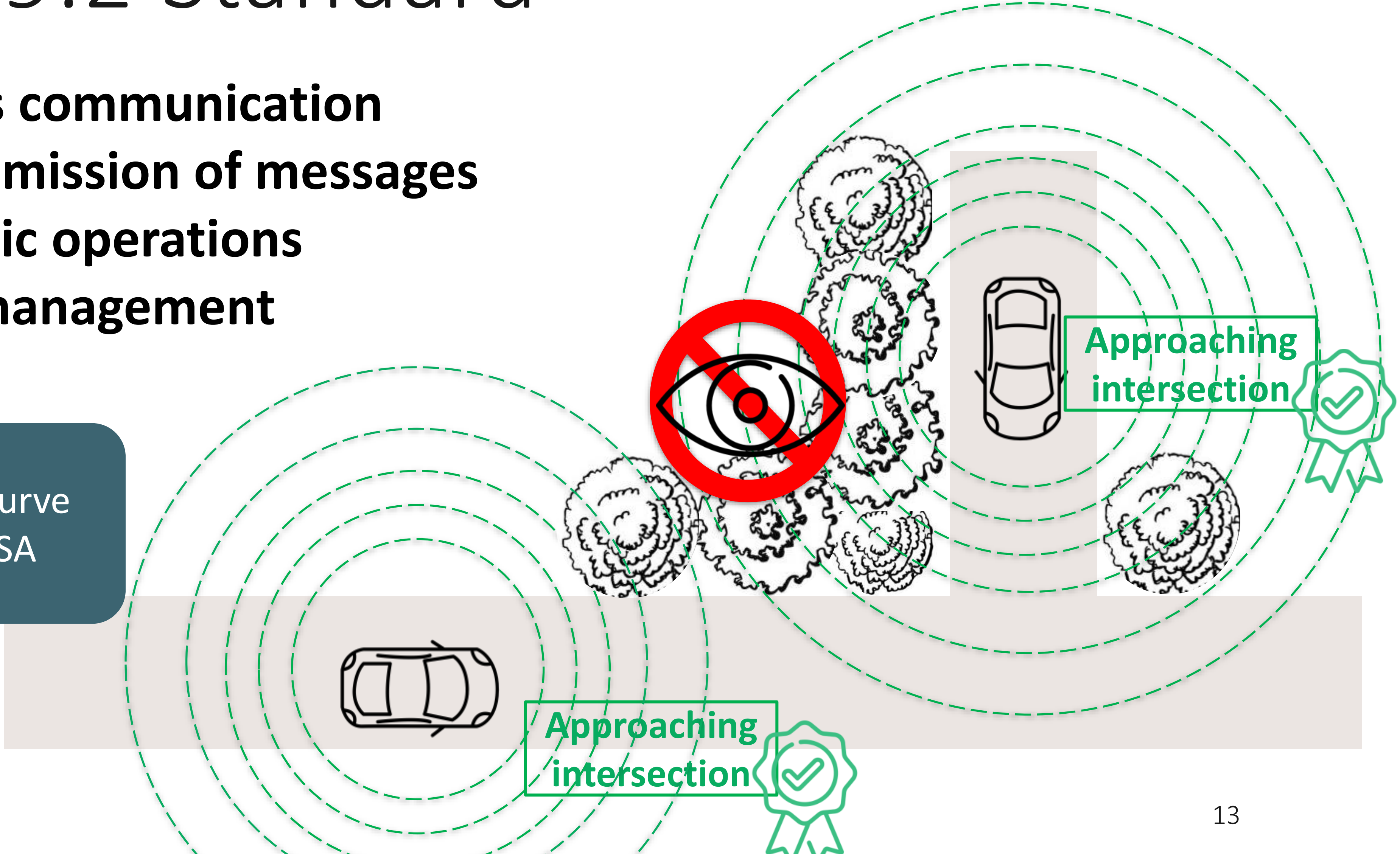


IEEE 1609.2 Standard

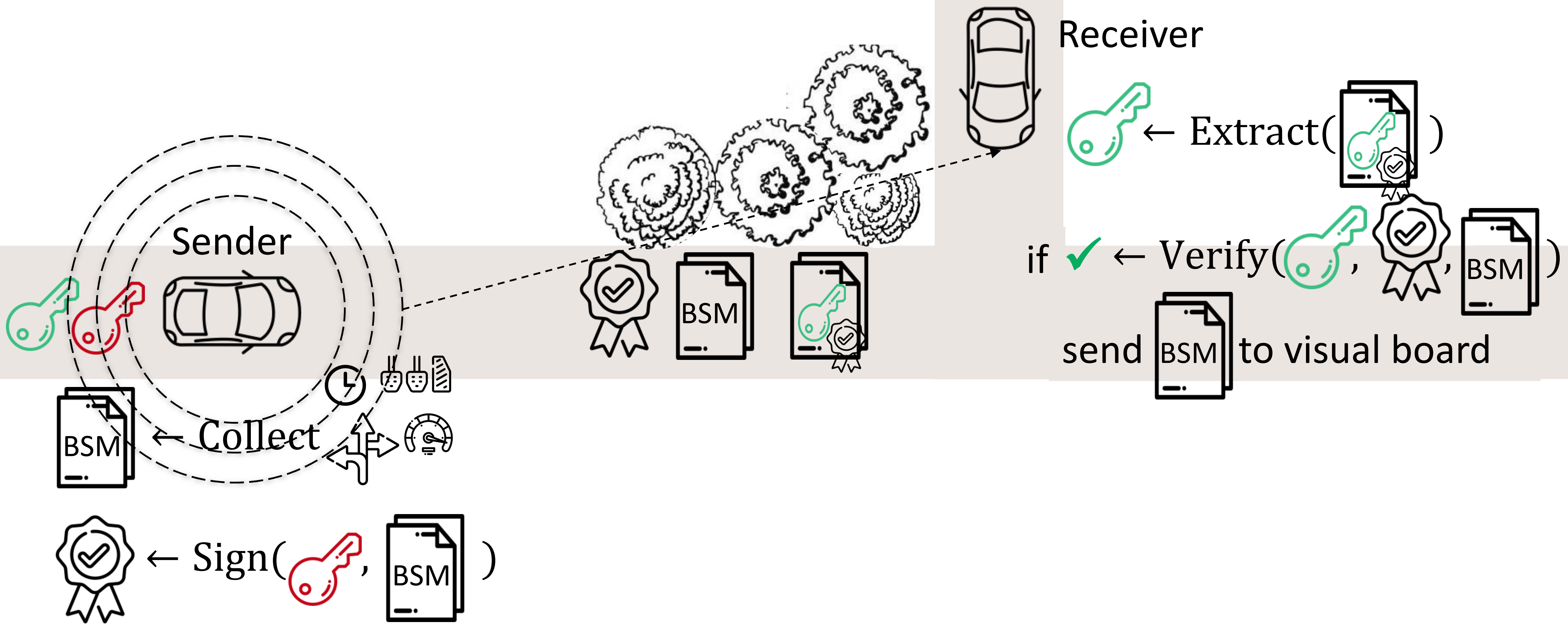
Secure wireless communication

- **secure transmission of messages**
- **cryptographic operations**
- **certificate management**

Based on elliptic curve crypto, e.g. ECDSA



Secure BSM Exchange



OUTLINE

Transition to Quantum-Secure Algorithms

The Use of Certificates in Vehicle-to-Vehicle (V2V) Communication

Explicit vs Implicit Certificates

Constructing Implicit Certificates

Implicit Certificates From Lattices

Potential future directions

Explicit Certs

CA cert

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

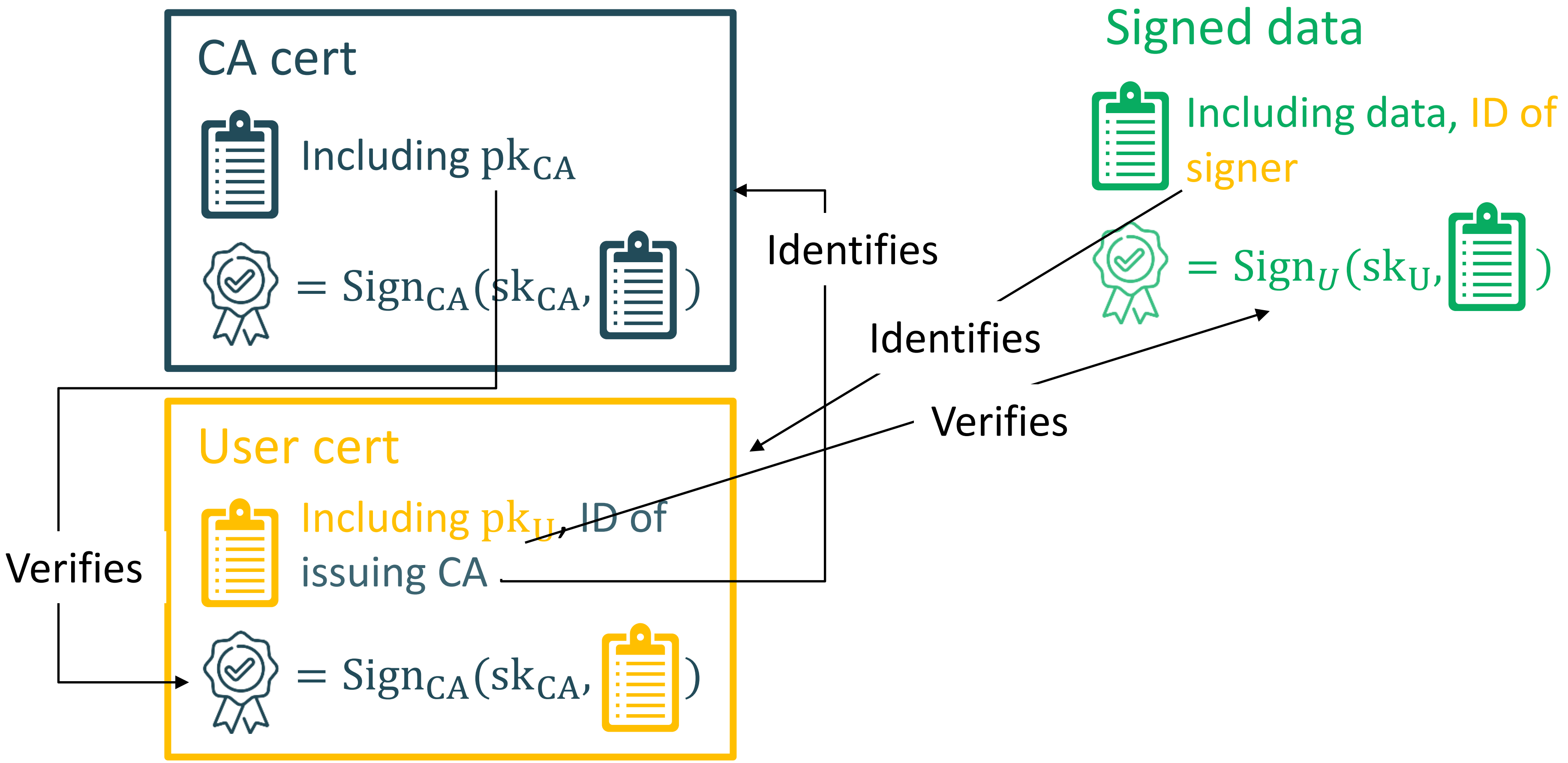
 $= \mathrm{Sign}_{\mathrm{CA}}(\mathrm{sk}_{\mathrm{CA}},$  $)$

User cert

 Including pk_{U}, ID of issuing CA

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

Explicit Certs Verification



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 $\mathrm{pk_{CA}}$

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

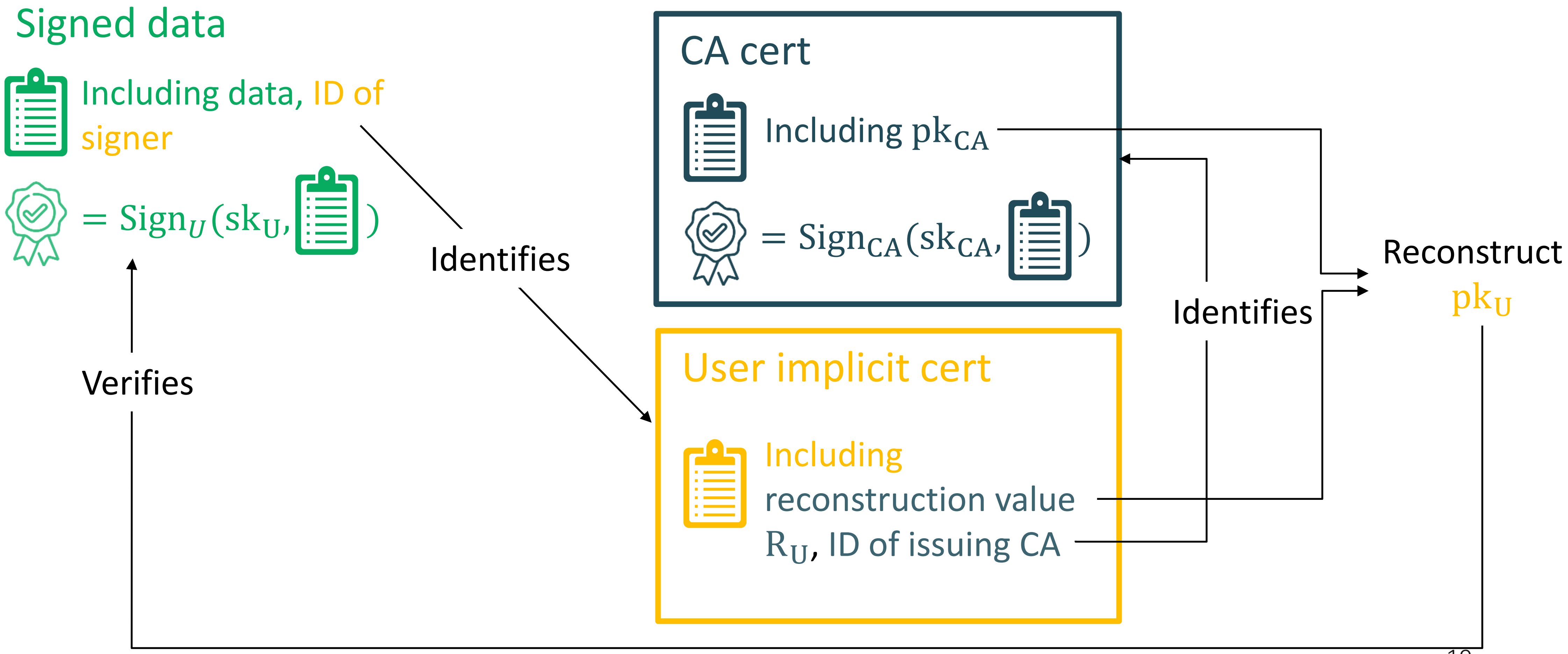
User implicit cert

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

Goal:

$\left|\ \right| + |\mathrm{pk_U}| \geq |R_U|$

Implicit Certs Verification



OUTLINE

- Transition to Quantum-Secure Algorithms
- The Use of Certificates in Vehicle-to-Vehicle (V2V) Communication
- Explicit vs Implicit Certificates
- Constructing Implicit Certificates
- Implicit Certificates From Lattices
- Potential future directions

ELLIPTIC CURVE QU-VANSTONE IMPLICIT CERT

User U | **CA** C

Long-term pk of CA

$sk_C = d_C$

$pk_C = Q_C = d_C \cdot G$

Randomness of user

$k_U \leftarrow\!\!\$ \; [1, ..., n-1]$

$K_U \leftarrow k_U \cdot G$

$\xrightarrow{K_U, U}$

Randomness of CA

$k_C \leftarrow\!\!\$ \; [1, ..., n-1]$

$R_U \leftarrow K_U + k_C \cdot G$

Reconstruction value

$\mathrm{Cert}_U \leftarrow \mathrm{Encode}(R_U, U)$

$e \leftarrow H(\mathrm{Cert}_U)$

$r \leftarrow ek_C + d_C \mod n$

ECDSA signature

$\xleftarrow{r, \mathrm{Cert}_U}$

$e \leftarrow H(\mathrm{Cert}_U)$

$sk_U = d_U \leftarrow ek_U + r \mod n$

Long-term sk of user

$$
\begin{aligned}
\mathrm{pk_U} &= \mathrm{d_U} \cdot G \\
&= ek_U G + rG = ek_U G + ek_C G + d_C G = e(K_U + k_{CG}) + Q_C \\
&= eR_U + Q_C
\end{aligned}
$$

CONSTRUCTION PRINCIPLES

- $|R_U| \le |r| + |pk_U|$
- Only U is able to compute sk_U
- Everyone is able to compute pk_U from pk_C and R_U
- sk_C is kept secret
- U is not able to generate its own certs

⇨ CA's signature is part of the sk_U

User U | **CA** C

Long-term pk of CA:

$sk_C = d_C$

$pk_C = Q_C = d_C \cdot G$

Randomness of user:

$k_U \leftarrow\$ [1, ..., n-1]$

$K_U \leftarrow k_U \cdot G$

$\xrightarrow{K_U, U}$

Randomness of CA:

$k_C \leftarrow\$ [1, ..., n-1]$

Reconstruction value:

$R_U \leftarrow K_U + k_C \cdot G$

$\mathrm{Cert}_U \leftarrow \mathrm{Encode}(R_U, U)$

$e \leftarrow H(\mathrm{Cert}_U)$

ECDSA signature:

$r \leftarrow ek_C + d_C \mod n$

$\xleftarrow{r, \mathrm{Cert}_U}$

$e \leftarrow H(\mathrm{Cert}_U)$

Long-term sk of user:

$sk_U = d_U \leftarrow ek_U + r \mod n$

$$pk_U = d_U \cdot G$$
$$= ek_U G + rG = ek_U G + ek_C G + d_C G = e(K_U + k_{CG}) + Q_C$$
$$= eR_U + Q_C$$

OUTLINE

(Simplified) Falcon

Algorithm 1 Sign$_{\text{Falcon}}$

Require: $sk = g, -f, G, F, m$

Ensure: (r, z_2)

1: $r \leftarrow_\$$

2: $c \leftarrow H(r||m)$

3: $(z_1, z_2) \leftarrow f_1(c, sk)$ such that $z_1 + z_2 h = c \mod q$

4: **return** $s = (r, z_2)$

Very small polynomial coefficients

Small polynomial coefficients

Signature coefficients larger than sk coefficients

Algorithm 2 Verify$_{\text{Falcon}}$

Require: $pk = h = gf^{-1} \mod q, m, s = (r, z_2)$

Ensure: accept, reject

1: $c \leftarrow H(r||m)$

2: $z_1 \leftarrow c - z_2 h \mod q$

3: **if** $||(z_1, z_2)|| \leq \beta$ **then return** accept

4: **return** reject

NTRU problem ⇒ Information about g or f, help recover entire sk

Large polynomial coefficients

Problem of using signature in sk

- without needing signature in reconstruction of pk
- without using large elements

(Simplified) Dilithium

<u>Gen</u>

$\mathbf{A} \leftarrow R_q^{k\times\ell}$

$(\mathbf{s}_1, \mathbf{s}_2) \leftarrow S_\eta^\ell \times S_\eta^k$ — Very small polynomial coefficients

$\mathbf{t} := \mathbf{A}\mathbf{s}_1 + \mathbf{s}_2$ — Learning with Errors Problem

$\mathbf{return}\ (pk = (\mathbf{A}, \mathbf{t}), sk = (\mathbf{A}, \mathbf{t}, \mathbf{s}_1, \mathbf{s}_2))$

⇨ Information about s_1 or s_2, help recover entire sk

<u>Sign(sk, M)</u>

$\mathbf{z} := \perp$

$\mathbf{while}\ \mathbf{z} = \perp\ \mathbf{do}$

$\quad \mathbf{y} \leftarrow S_{\gamma_1 - 1}^\ell$

$\quad \mathbf{w}_1 := \mathsf{HighBits}(\mathbf{A}\mathbf{y}, 2\gamma_2)$

$\quad c \in B_\tau := \mathsf{H}(M \,\|\, \mathbf{w}_1)$

$\quad \mathbf{z} := \mathbf{y} + c\mathbf{s}_1$ — Somewhat small polynomial coefficients

$\quad \mathbf{if}\ \|\mathbf{z}\|_\infty \geq \gamma_1 - \beta\ \text{or}\ \|\mathsf{LowBits}(\mathbf{A}\mathbf{y} - c\mathbf{s}_2, 2\gamma_2)\|_\infty \geq \gamma_2 - \beta,\ \mathbf{then}\ \mathbf{z} := \perp$

$\mathbf{return}\ \sigma = (\mathbf{z}, c)$

<u>Verify$(pk, M, \sigma = (\mathbf{z}, c))$</u>

$\mathbf{w}_1' := \mathsf{HighBits}(\mathbf{A}\mathbf{z} - c\mathbf{t}, 2\gamma_2)$

$\mathbf{if}\ \mathbf{return}\ [\![\|\mathbf{z}\|_\infty < \gamma_1 - \beta]\!]\ \mathbf{and}\ [\![c = \mathsf{H}(M \,\|\, \mathbf{w}_1')]\!]$

Signature coefficients larger than sk coefficients

Pseudocode from 3rd round Dilithium submission, Fig. 1

Most promising construction

Core idea: Combine Falcon signatures and Dilithium secret keys

User U | **CA C**

CA's Falcon keys:

$g_C, F_C \leftarrow \mathsf{KeyGen}_{\text{Falcon}}$

$h_C = g_C \cdot F_C^{-1}$

$v_C^{-1} \leftarrow_\sigma \mathcal{R}_q^\ell,\ f_C'^{-1} \leftarrow v_C^{-1} \cdot h_C$

$sk_C = (g_C, F_C)$

$pk_C = (h_C, f_C'^{-1})$

Small value to decrease element added in user's sk

User U:

$\rho \leftarrow_\$ \{0,1\}^{256}$

$A \in \mathcal{R}_q^{k \times \ell} \leftarrow \text{Expand}(\rho)$

$(s_1, s_2, e_U) \leftarrow_\$ \mathcal{S}_\eta^\ell \times \mathcal{S}_\eta^k \times \mathcal{S}_\eta^\ell$

$t \leftarrow As_1 + s_2 \mod q$

User's randomness

$\xrightarrow{\rho, t, U}$

CA C:

CA's randomness

$r \leftarrow_\$ \{0,1\}^{128}$

$= R_U$

$\text{Cert}_U \leftarrow \text{Encode}(\rho, t, r, U)$

$c \leftarrow F(r||\text{Cert}_U)$

Falcon signature

$(z, Z) \leftarrow F_1((c, 0, ..., 0), g_C \cdot f_C', f_C)$

s.t. $z + Z \cdot v_C^{-1} = (c, 0, ..., 0) \cdot v_C^{-1}$

Instead of $z + Zh = (c, 0, \ldots, 0)$

$\xleftarrow{Z, \text{Cert}_U}$

User U:

$(\rho, t, r, U) \leftarrow \text{Cert}_U$

$c \leftarrow F(r||\text{Cert}_U)$

$v_C^{-1} \leftarrow h_C^{-1} \cdot f_C'^{-1}$

$sk_U = (s_1 + Z \cdot v_C^{-1} + z\, e_U)$

$pk_U = t + A \cdot c \cdot h_C^{-1} \cdot f_C'^{-1}$

User's Dilithium keys

Falcon signature

User U | **CA** C

Can we find v_c such that $f_C{}'$ is small?

Not while the NTRU problem is hard, as

$$f_C' = v_C \cdot g_C^{-1} \cdot F_C$$

⇨ a small f_C' would leak the secret

$$g_C, F_C \leftarrow \mathsf{KeyGen}_{\mathrm{Falcon}}$$
$$h_C = g_C \cdot F_C^{-1}$$
3
$$v_C^{-1} \leftarrow_\sigma \mathcal{R}_q^\ell, \quad f_C'^{-1} \leftarrow v_C^{-1} \cdot h_C$$
$$sk_C = (g_C, F_C)$$
$$pk_C = (h_C, f_C'^{-1})$$

$$\rho \leftarrow_\$ \{0,1\}^{256}$$
$$A \in \mathcal{R}_q^{k\times\ell} \leftarrow \mathrm{Expand}(\rho)$$
$$(s_1, s_2, e_U) \leftarrow_\$ \mathcal{S}_\eta^\ell \times \mathcal{S}_\eta^k \times \mathcal{S}_\eta^\ell$$
$$t \leftarrow As_1 + s_2 \mod q$$

$\xrightarrow{\rho, t, U}$

$$r \leftarrow_\$ \{0,1\}^{128}$$
$$\mathrm{Cert}_U \leftarrow \mathrm{Encode}(\rho, t, r, U)$$
$$c \leftarrow F(r \| \mathrm{Cert}_U)$$
2
$$(z, Z) \leftarrow F_1((c, 0, \dots, 0), g_C \cdot f_C', f_C)$$
$$\text{s.t. } z + Z \cdot v_C^{-1} = (c, 0, \dots, 0) \cdot v_C^{-1}$$

Trade-off between input and output size:

The larger the coefficients of the input, the larger the coefficients of the input

⇨ the larger the signature

$\xleftarrow{Z, \mathrm{Cert}_U}$

$$(\rho, t, r, U) \leftarrow \mathrm{Cert}_U$$
$$c \leftarrow F(r \| \mathrm{Cert}_U)$$
$$v_C^{-1} \leftarrow h_C^{-1} \cdot f_C'^{-1}$$
1
$$sk_U = (s_1 + Z \cdot v_C^{-1} + z\, e_U)$$
$$pk_U = t + A \cdot c \cdot h_C^{-1} \cdot f_C'^{-1}$$

While smaller, not small enough:

Dilithium parameters would probably be so large that there is no efficiency benefit in using this construction compared to explicit certs.

… and why it fails

OUTLINE

Transition to Quantum-Secure Algorithms

The Use of Certificates in Vehicle-to-Vehicle (V2V) Communication

Explicit vs Implicit Certificates

Constructing Implicit Certificates

Implicit Certificates From Lattices

Potential future directions

Related primitives and results

Certificate-less signatures: user's private key constructed from a partial master private key and secret value of user

Certificate-based signature: signing requires a user cert signed by the CA

ID-based signatures: Public key constructed from user ID

Approx. signature sizes

[TH15] 84,437 bytes

[TTTWH19] 10,895 bytes

[XHVCL20] 1,400-1,700 bytes

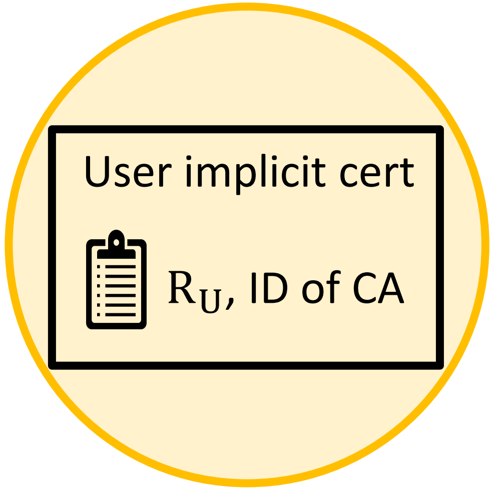
[XHGG16] 6,000-7,000 bytes

[CHLG21] 15,000 bytes

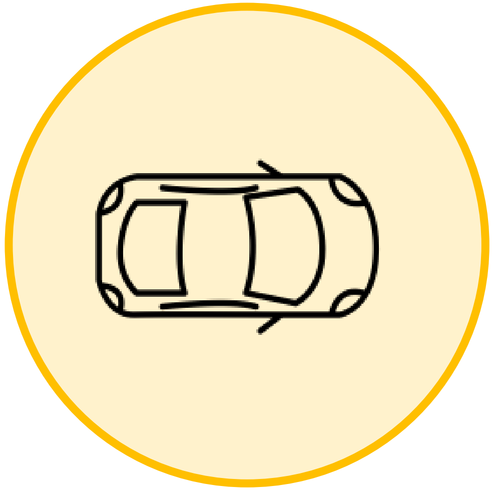
[TH15] Certificate-less and certificate-based signatures from lattices. Miaomiao Tian, Liusheng Huang. Security and Communication Networks. 2015.
[XHGG16] Efficient identity-based signature over NTRU lattice. Jia Xie, Yu-pu Hu, Jun-tao Gao, Wen Gao. Frontiers of Information Technology & Electronic Engineering. 2016.
[TTTWH19] Efficient Certificate-Based Signature with Short Key and Signature Sizes from Lattices. Yuh-Min Tseng, Tung-Tso Tsai, Tung-Tso Tsai, Jui-Di Wu, Sen-Shan HUANG. INFORMATICA. 2019.
[XHVCL20] Efficient NTRU Lattice-Based Certificate-less Signature Scheme for Medical Cyber-Physical Systems. Zhiyan Xu, Debiao He, Pandi Vijayakumar, Kim-Kwang Raymond Choo, Li Li. Journal of Medical Systems. 2020.
[CHLG21] Novel efficient identity-based signature on lattices. Jiang-shan Chen, Yu-pu Hu, Hong-mei Liang, Wen Gao. Frontiers of Information Technology & Electronic Engineering. 2021.

Future Directions

- Modern, more efficient instantiation of related constructions
- (Even) More efficient sampler during Falcon’s signature generation
- Consider other PQC beyond lattice-based crypto



- Constructing implicit certificates from lattices inherently difficult
- Major break-through needed to decreases sizes of current constructions to be used in applications



- Use explicit or implicit-explicit ECDSA-Falcon certificates in V2V communication

Thanks to John Schanck for fruitful discussions, in particular about the hardness of the NTRU problem.

This research is funded by
- NSERC, RGPIN-2016-05146
- NRC, program 927517
- Public Works and Government Services Canada

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing
nina.bindel@uwaterloo.ca

THANKS.