

The Need for Being Explicit When Communicating

CFAIL 2021
August 14, 2021

Nina Bindel
Sarah McCarthy

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

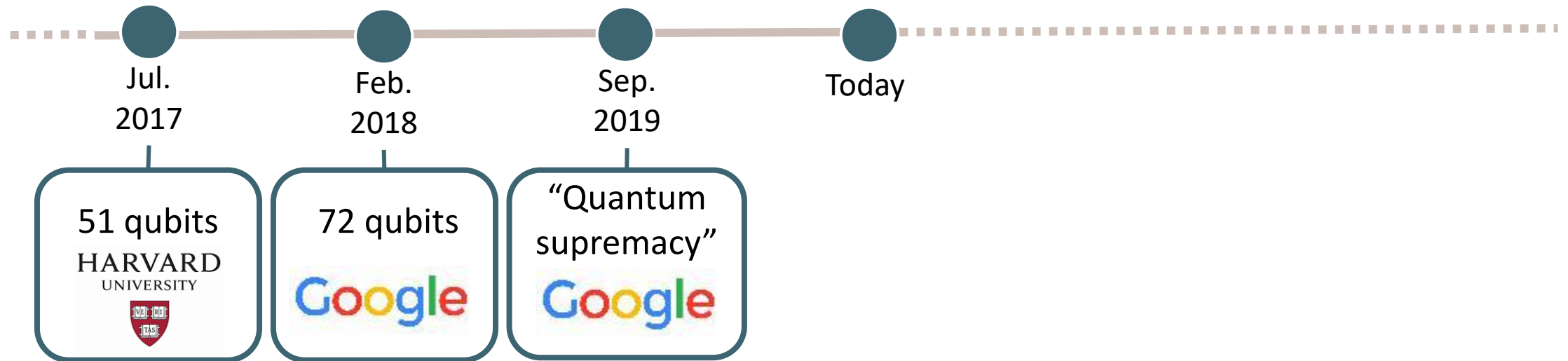
Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

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.

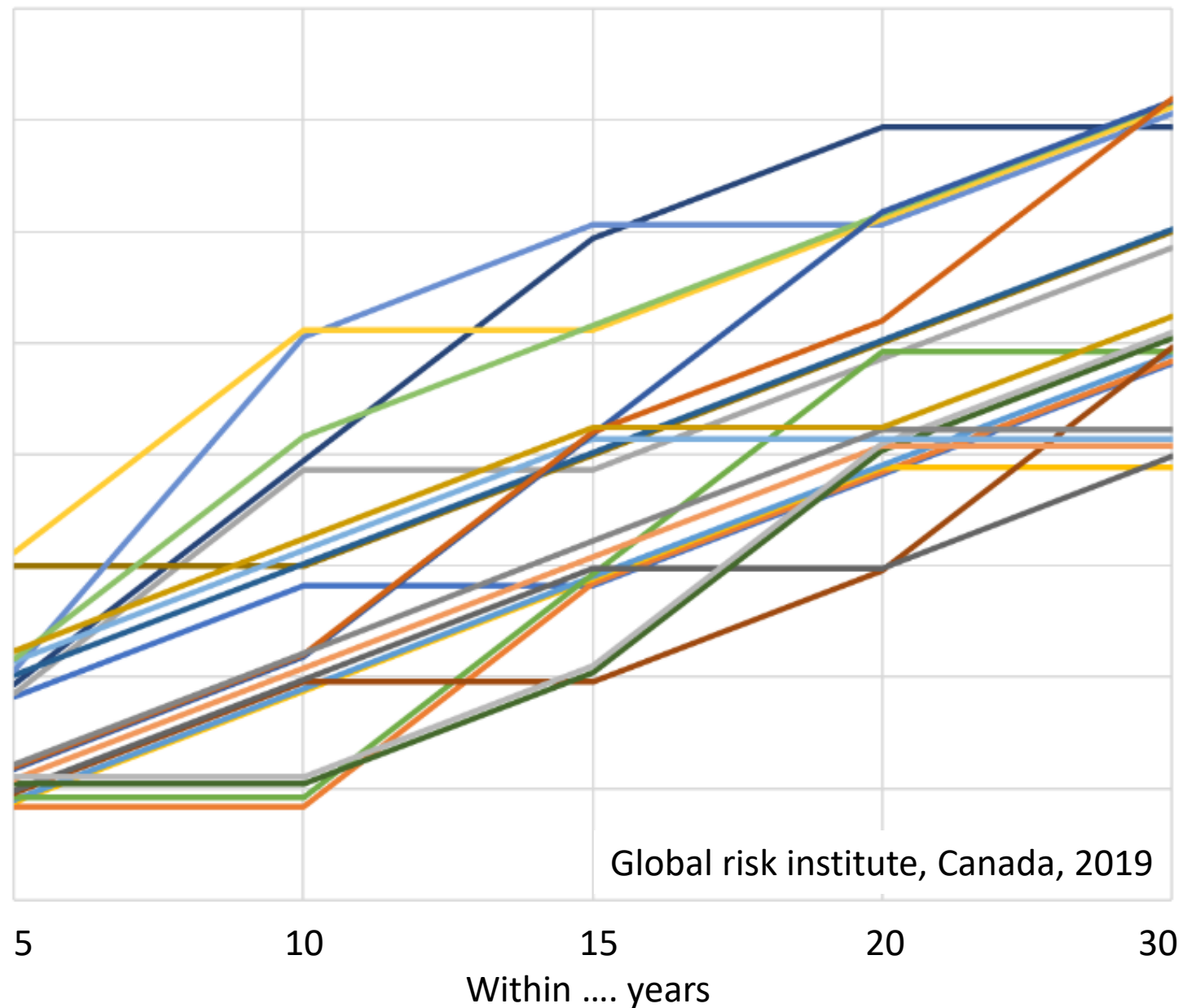
Quantum computers: State-of-the-art



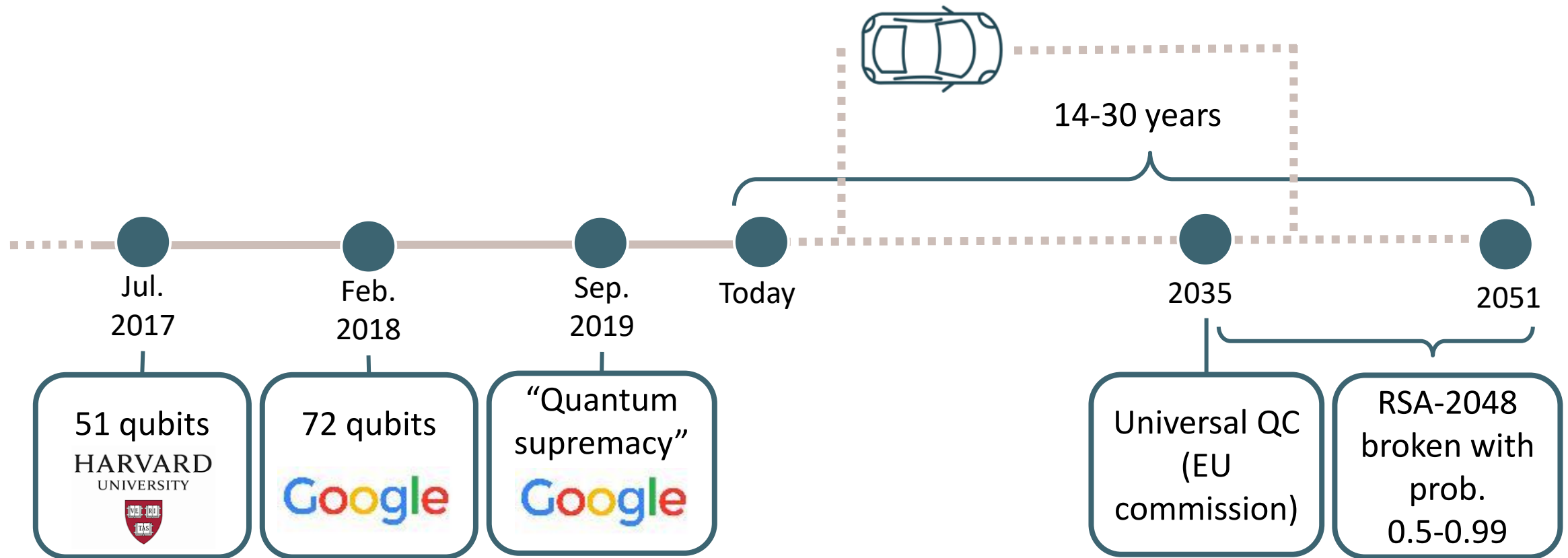
20 million qubits
needed to break RSA-2048
[GK19]


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

- Extremely likely
(> 99% chance)
- Very likely
(> 95% chance)
- Likely
(> 70 % chance)
- Neither likely not
unlikely
(~ 50% chance)
- Unlikely
(< 30% chance)
- Very unlikely
(< 5% chance)
- Extremely unlikely
(< 1% chance)

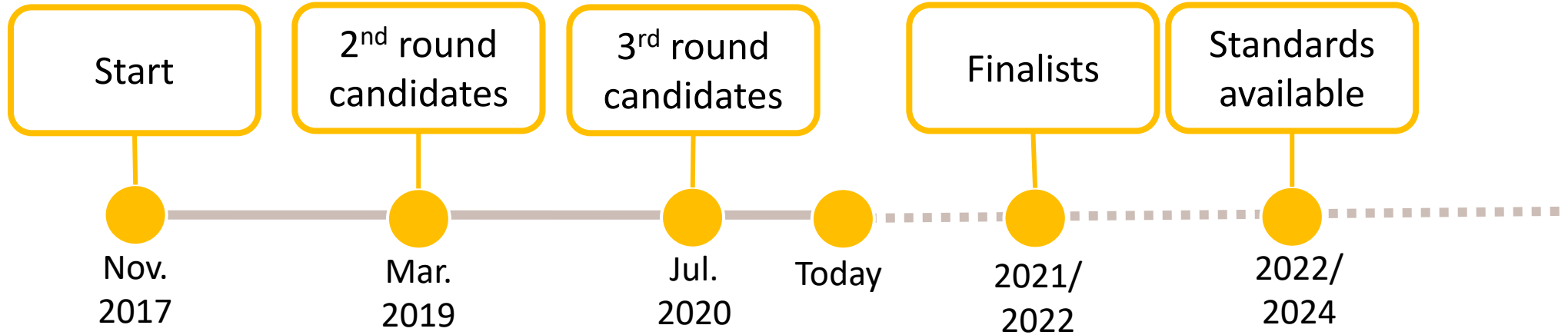


Quantum computers: State-of-the-art



Need to prepare
transition to
-secure
algorithms

NIST post-quantum standardization



PKEs/KEMs



Signatures



Lattice-based signatures:

- Falcon
- Dilithium

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

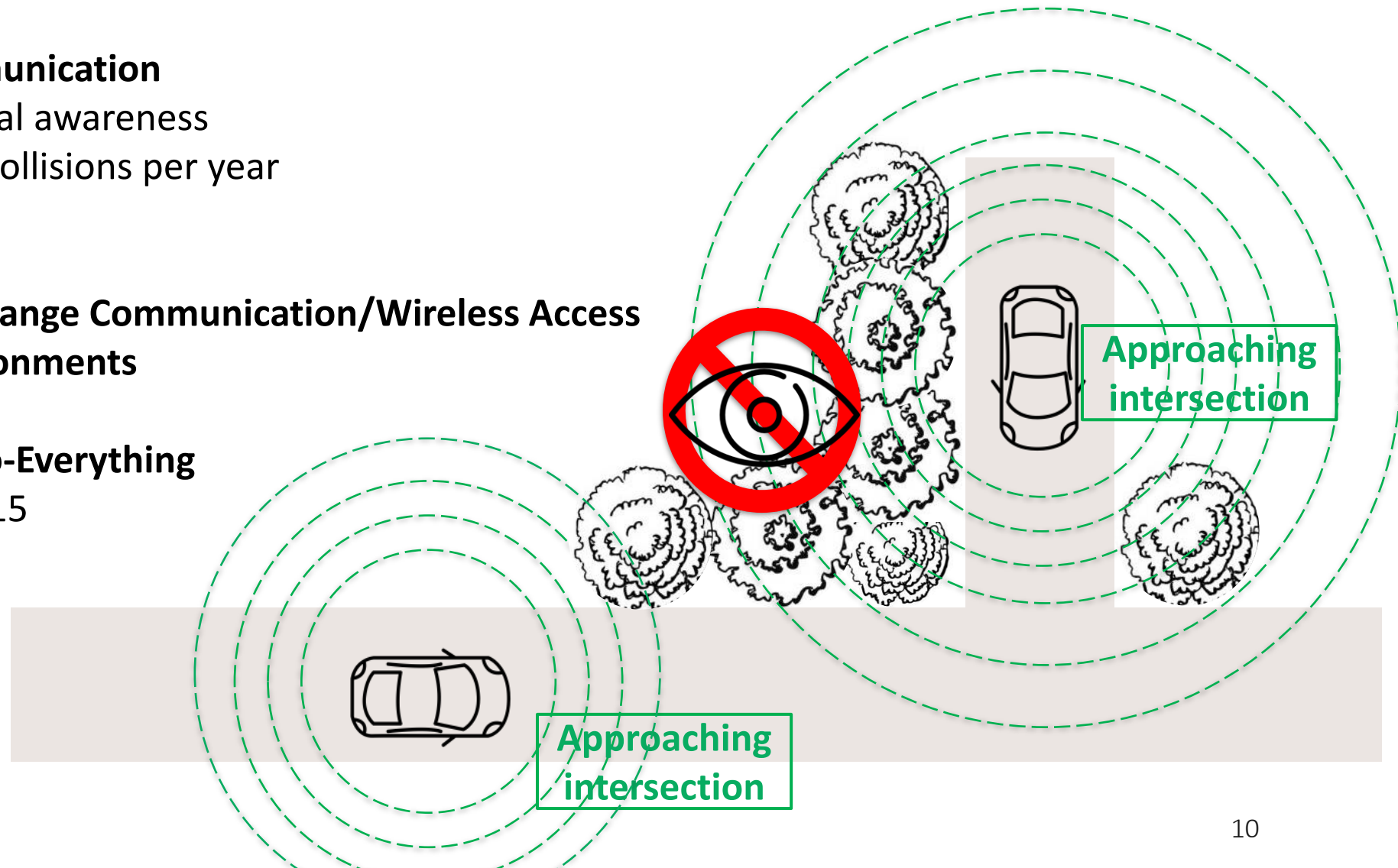
V2V Communication

Direct wireless communication

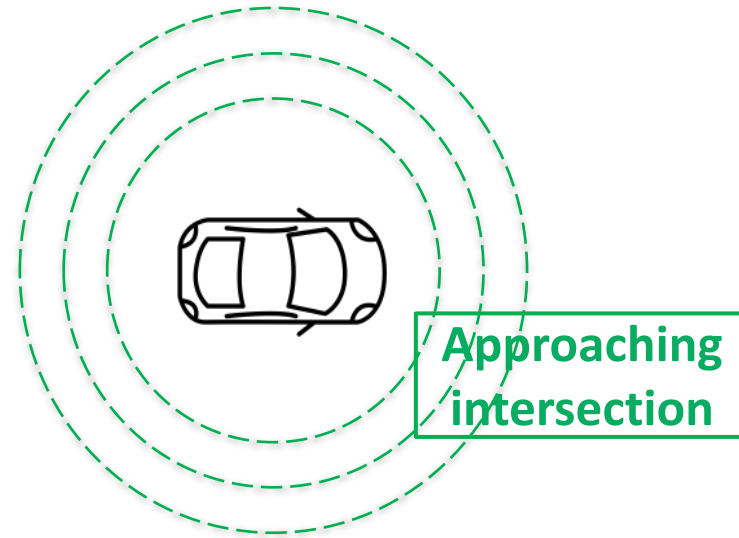
- Increases situational awareness
- Prevents 600,000 collisions per year

Described in

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

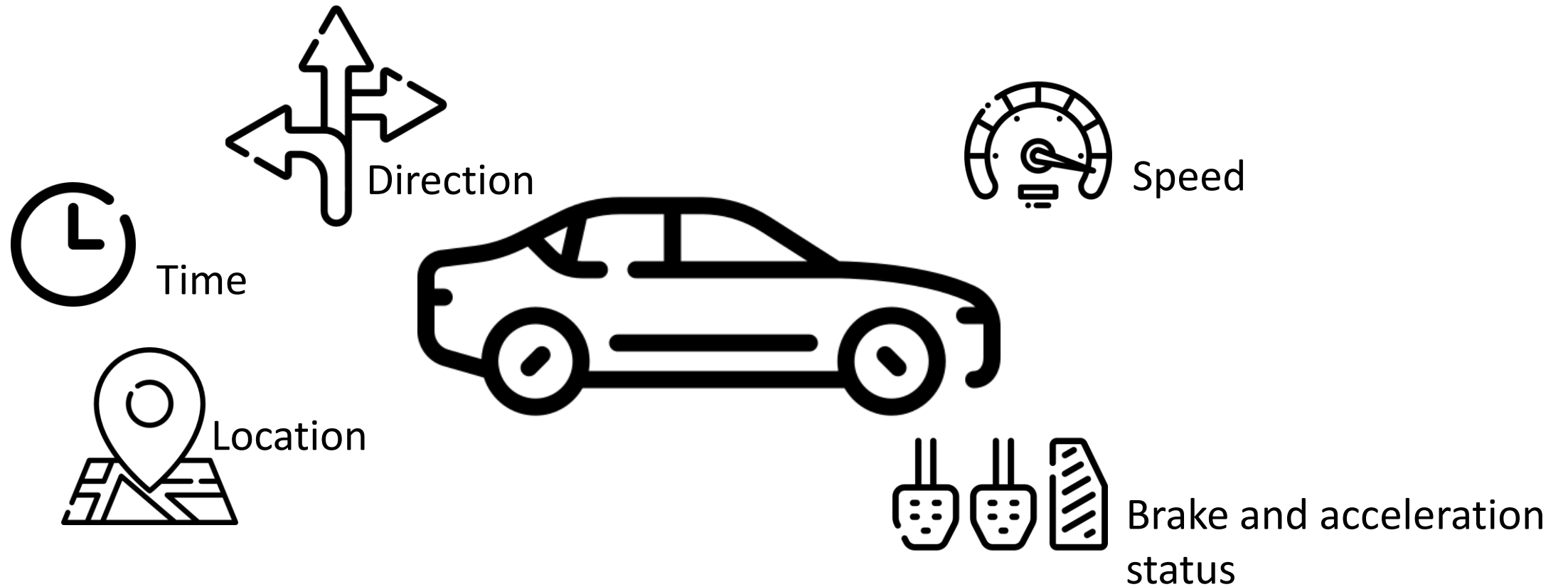


Basic Safety Messages (BSMs)



Every vehicle broadcasts 10 BSMs per second within transmission range

Information Collected in BSMs

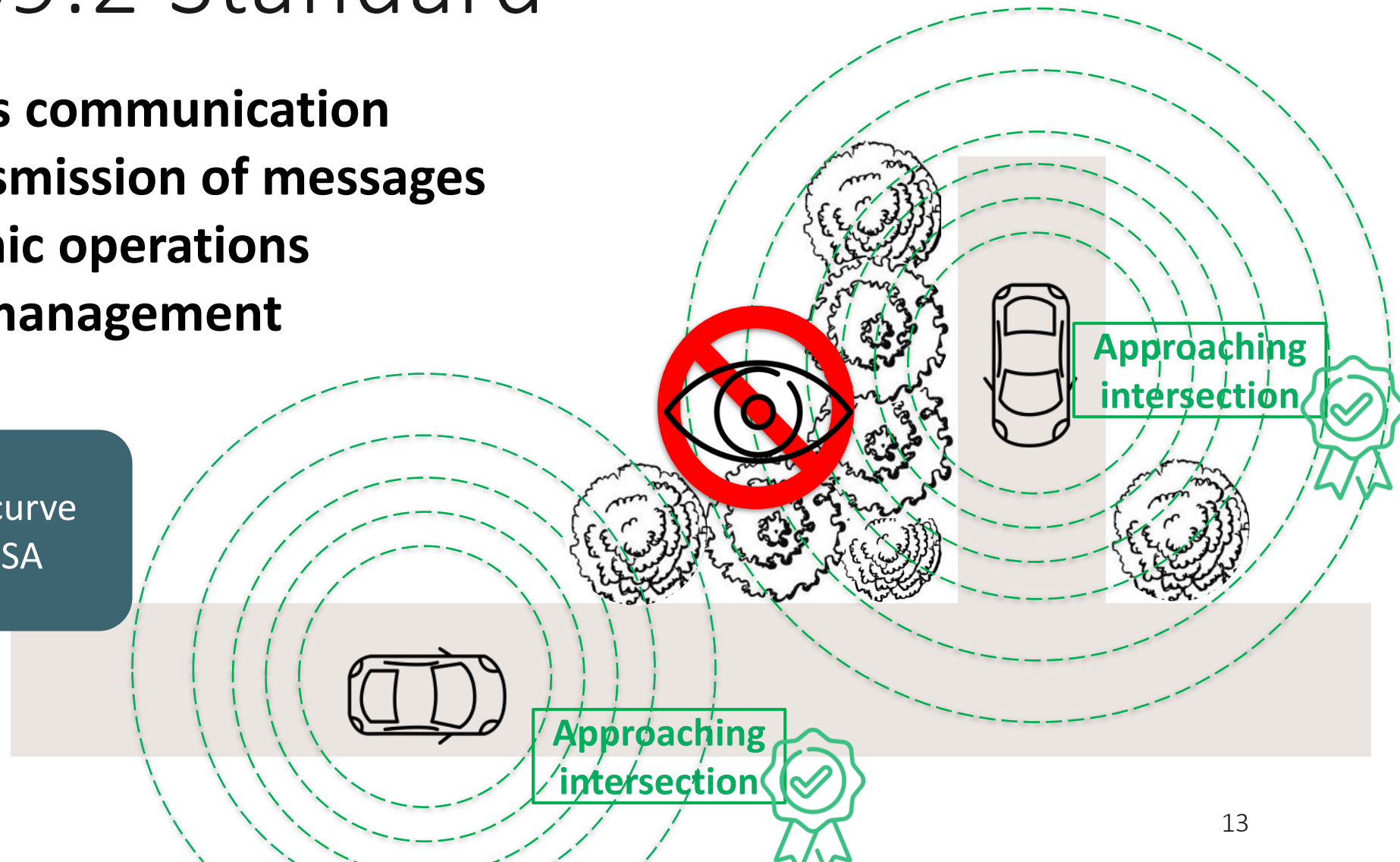


IEEE 1609.2 Standard

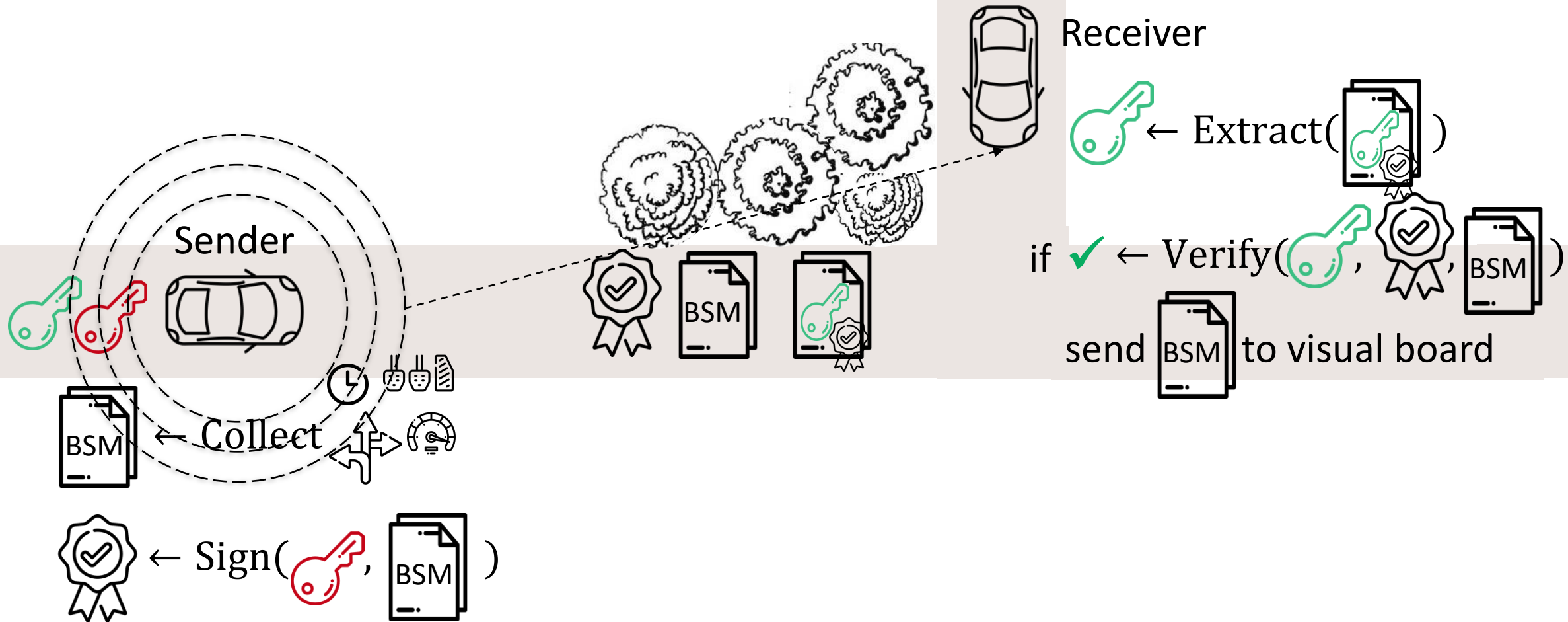
Secure wireless communication

- 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 pk_{CA}



$= \text{Sign}_{CA}(sk_{CA},$



)

User cert



Including pk_U , ID of
issuing CA

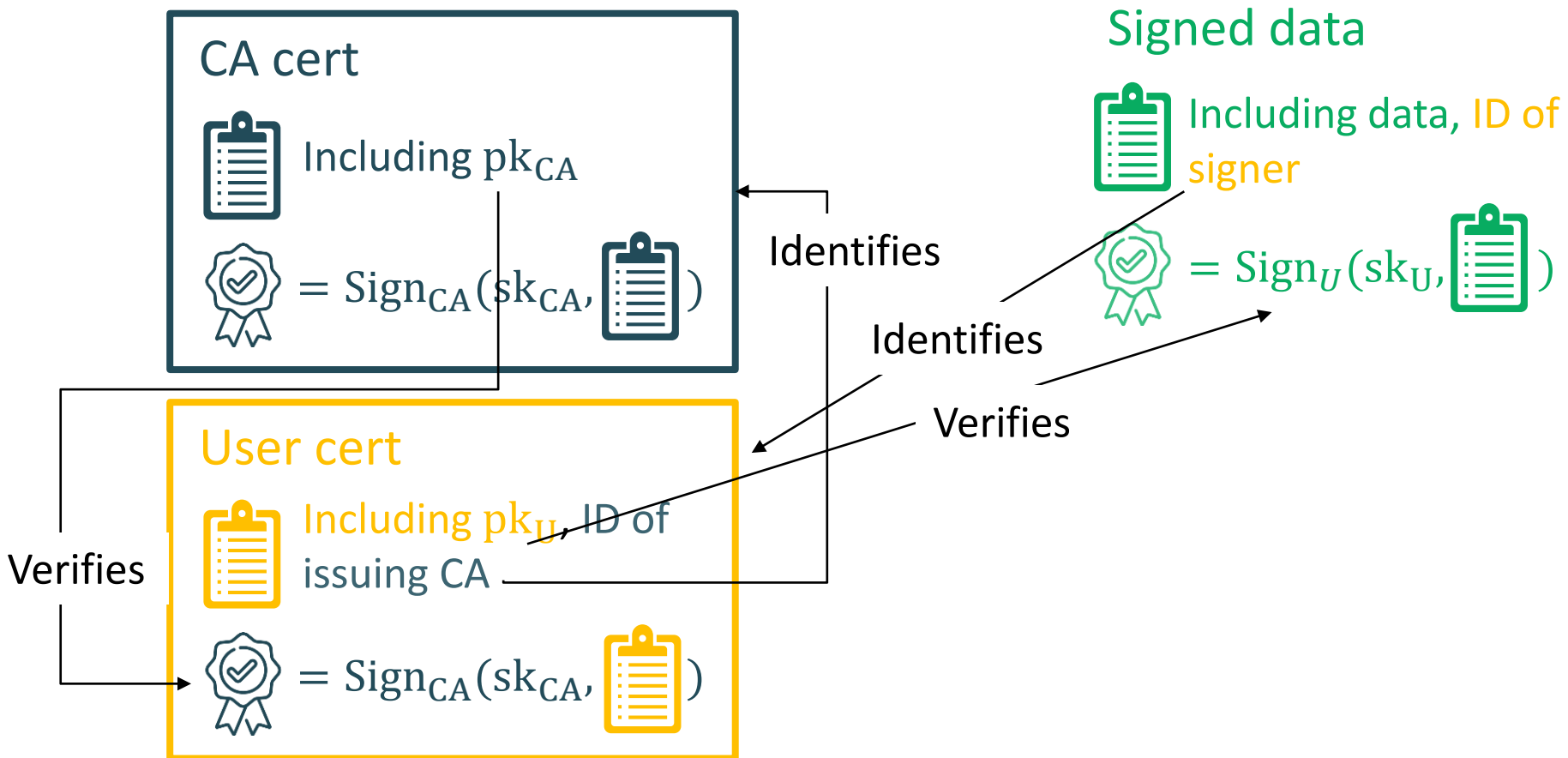


$= \text{Sign}_{CA}(sk_{CA},$



)

Explicit Certs Verification



Explicit vs Implicit Certs

CA cert



Including pk_{CA}



$= \text{Sign}_{CA}(sk_{CA}, \text{Clipboard})$

CA cert



Including pk_{CA}



$= \text{Sign}_{CA}(sk_{CA}, \text{Clipboard})$

User explicit cert



Including pk_U , ID of issuing CA



$= \text{Sign}_{CA}(sk_{CA}, \text{Clipboard})$

User implicit cert

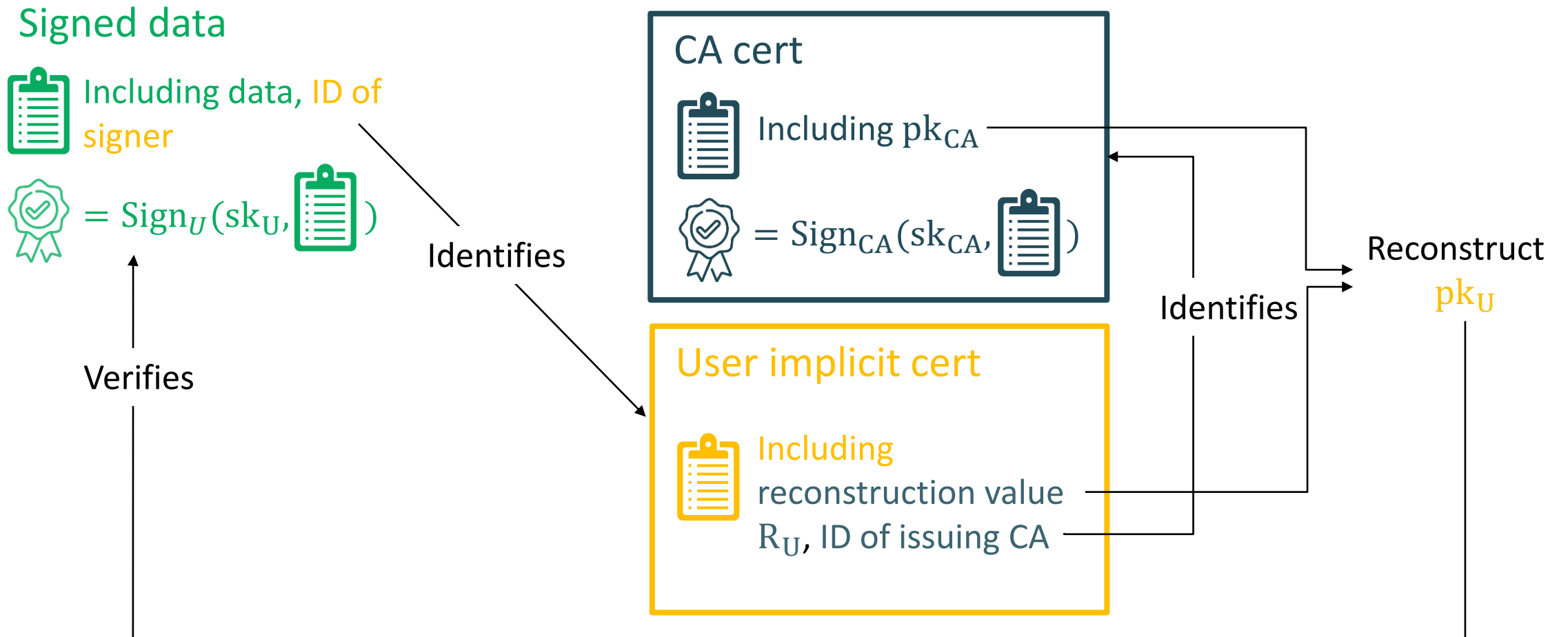


Including reconstruction value R_U , ID of issuing CA

Goal:

$$|\text{Seal}| + |pk_U| \geq |R_U|$$

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

$$\begin{aligned} sk_C &= d_C \\ pk_C &= Q_C = d_C \cdot G \end{aligned}$$

Randomness of user

$$\begin{aligned} k_U &\leftarrow_{\$} [1, \dots, n-1] \\ K_U &\leftarrow k_U \cdot G \end{aligned}$$

K_U, U

Reconstruction value

Randomness of CA

$$k_C \leftarrow_{\$} [1, \dots, n-1]$$

$$R_U \leftarrow K_U + k_C \cdot G$$

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

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

r, Cert_U

$$r \leftarrow (ek_C + d_C) \bmod n$$

ECDSA signature

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

$$sk_U = d_U \leftarrow (ek_U + r) \bmod n$$

Long-term sk of user

$$pk_U = d_U \cdot G$$

$$= ek_U G + rG = ek_U G + ek_C G + d_C G = e(K_U + k_C G) + Q_C$$

$$= eR_U + Q_C$$

CONSTRUCTION PRINCIPLES

- $|R_U| \leq |r| + |pk_U|$
- 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
 \Rightarrow CA's signature is part of the sk_U

User U

CA C

Long-term pk of CA

$$\begin{aligned} sk_C &= d_C \\ pk_C &= Q_C = d_C \cdot G \end{aligned}$$

Randomness of user

$$\begin{aligned} k_U &\leftarrow_{\$} [1, \dots, n-1] \\ K_U &\leftarrow k_U \cdot G \end{aligned}$$

K_U, U

Reconstruction value

Randomness of CA

$$\begin{aligned} k_C &\leftarrow_{\$} [1, \dots, n-1] \\ R_U &\leftarrow K_U + k_C \cdot G \end{aligned}$$

$$Cert_U \leftarrow \text{Encode}(R_U, U)$$

$$e \leftarrow H(Cert_U)$$

$r, Cert_U$



ECDSA signature

$$r \leftarrow ek_C + d_C \pmod n$$

$$e \leftarrow H(Cert_U)$$

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

Long-term sk of user

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

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

(Simplified) Falcon

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

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 $z_1 + z_2h = c \pmod q$
- 4: **return** $s = (r, z_2)$

Very small polynomial coefficients

Small polynomial coefficients

Signature coefficients larger than sk coefficients

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

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

Ensure: accept, reject

- 1: $c \leftarrow H(r||m)$
- 2: $z_1 \leftarrow c - z_2h \pmod q$
- 3: **if** $\|(z_1, z_2)\| \leq \beta$ **then return** accept
- 4: **return** reject

Large polynomial coefficients

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

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

(Simplified) Dilithium

Gen

```
01  $\mathbf{A} \leftarrow B_q^{k \times \ell}$   
02  $(s_1, s_2) \leftarrow S_\eta^\ell \times S_\eta^k$  — Very small polynomial coefficients  
03  $\mathbf{t} := \mathbf{A}s_1 + s_2$  — Learning with Errors Problem  
04 return  $(pk = (\mathbf{A}, \mathbf{t}), sk = (\mathbf{A}, \mathbf{t}, s_1, s_2))$ 
```

Sign (sk, M)

```
05  $\mathbf{z} := \perp$   
06 while  $\mathbf{z} = \perp$  do  
07  $\mathbf{y} \leftarrow S_{\gamma_1 - 1}^\ell$   
08  $\mathbf{w}_1 := \text{HighBits}(\mathbf{A}\mathbf{y}, 2\gamma_2)$   
09  $c \in B_\tau := \text{H}(M \parallel \mathbf{w}_1)$  — Somewhat small polynomial coefficients  
10  $\mathbf{z} := \mathbf{y} + c s_1$   
11 if  $\|\mathbf{z}\|_\infty \geq \gamma_1 - \beta$  or  $\|\text{LowBits}(\mathbf{A}\mathbf{y} - c s_2, 2\gamma_2)\|_\infty \geq \gamma_2 - \beta$ , then  $\mathbf{z} := \perp$   
12 return  $\sigma = (\mathbf{z}, c)$ 
```

Information about s_1 or s_2 , help recover entire sk

Signature coefficients larger than sk coefficients

Verify $(pk, M, \sigma = (\mathbf{z}, c))$

```
13  $\mathbf{w}'_1 := \text{HighBits}(\mathbf{A}\mathbf{z} - c\mathbf{t}, 2\gamma_2)$   
14 if return  $\llbracket \|\mathbf{z}\|_\infty < \gamma_1 - \beta \rrbracket$  and  $\llbracket c = \text{H}(M \parallel \mathbf{w}'_1) \rrbracket$ 
```

Most promising construction

Core idea: Combine Falcon signatures and Dilithium secret keys

User U

CA C

CA's Falcon keys
Small value to decrease element added in user's sk

$$\left\{ \begin{array}{l} g_C, F_C \leftarrow \text{KeyGen}_{\text{Falcon}} \\ h_C = g_C \cdot F_C^{-1} \\ v_C^{-1} \leftarrow_{\sigma} \mathcal{R}_q^{\ell}, f_C'^{-1} \leftarrow v_C^{-1} \cdot h_C \\ sk_C = (g_C, F_C) \\ pk_C = (h_C, f_C'^{-1}) \end{array} \right.$$

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

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

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

$$t \leftarrow A s_1 + s_2 \pmod{q}$$

User's randomness

ρ, t, U

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

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

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

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

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

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

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

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

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

User's Dilithium keys

Falcon signature

User U

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

CA C

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

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

$$\textcircled{3} \quad v_C^{-1} \leftarrow_{\sigma} \mathcal{R}_q^{\ell}, \quad f'_C{}^{-1} \leftarrow v_C^{-1} \cdot h_C$$

$$sk_C = (g_C, F_C)$$

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

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

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

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

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

$$t \leftarrow A s_1 + s_2 \pmod q$$

→ ρ, t, U

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

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

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

$$\textcircled{2} \quad (z, Z) \leftarrow F_1((c, 0, \dots, 0), g_C \cdot f'_c, f_c)$$

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

← Z, Cert_U

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

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

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

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

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

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.

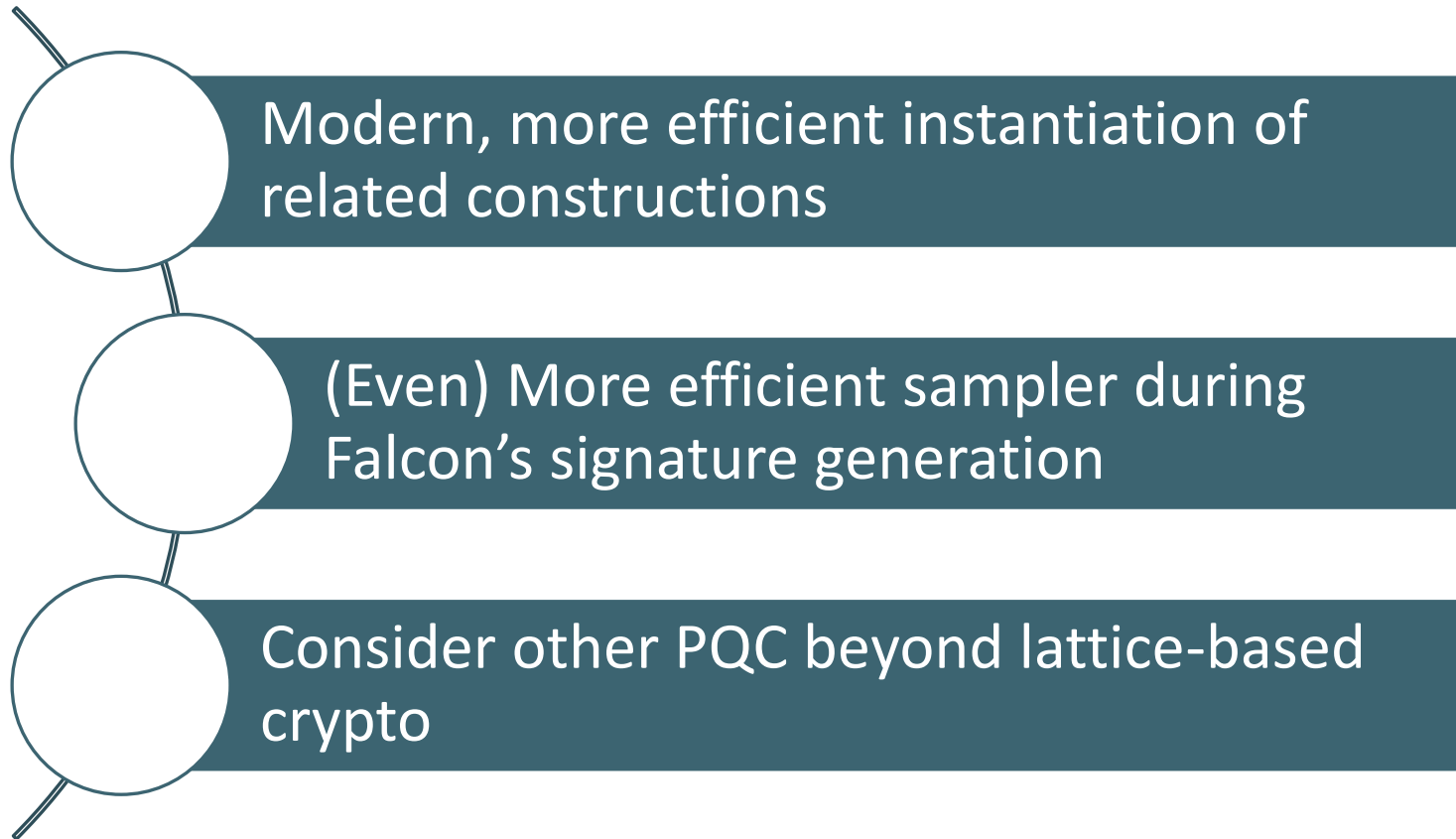
[XHGG16] Efficient identity-based signature over NTRU lattice. Jia Xie, Yu-pu Hu, Jun-tao Gao, Wen Gao. Frontiers of Information Technology & Electronic Engineering. 2016.

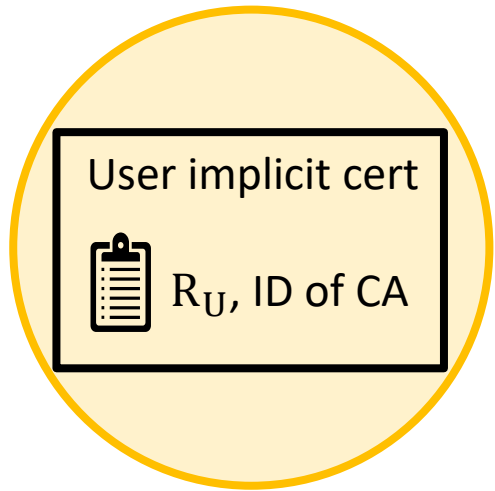
[TTTWH19] Efficient Certificate-Based Signature with Short Key and Signature Sizes from Lattices. Yuh-Min Tseng, Tung-Tso Tsai, Tung-Tso Tsai, Jui-Di Wu, Sen-Shan HUANG. INFORMATICA. 2019.

[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.

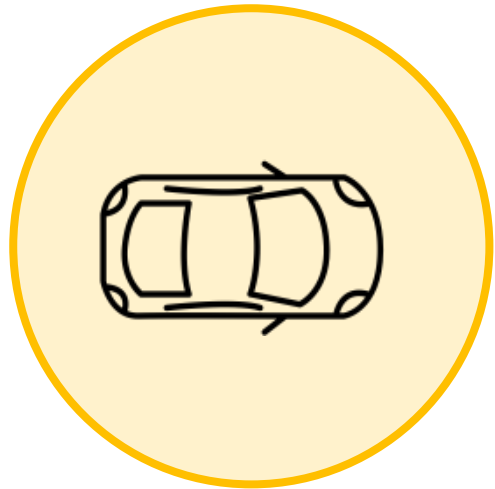
[CHLG21] Novel efficient identity-based signature on lattices. Jiang-shan Chen, Yu-pu Hu, Hong-mei Liang, Wen Gao. Frontiers of Information Technology & Electronic Engineering. 2021.

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 decrease 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

