Desafios e oportunidades de pesquisa na adoção de criptografia pós-quântica em redes veiculares

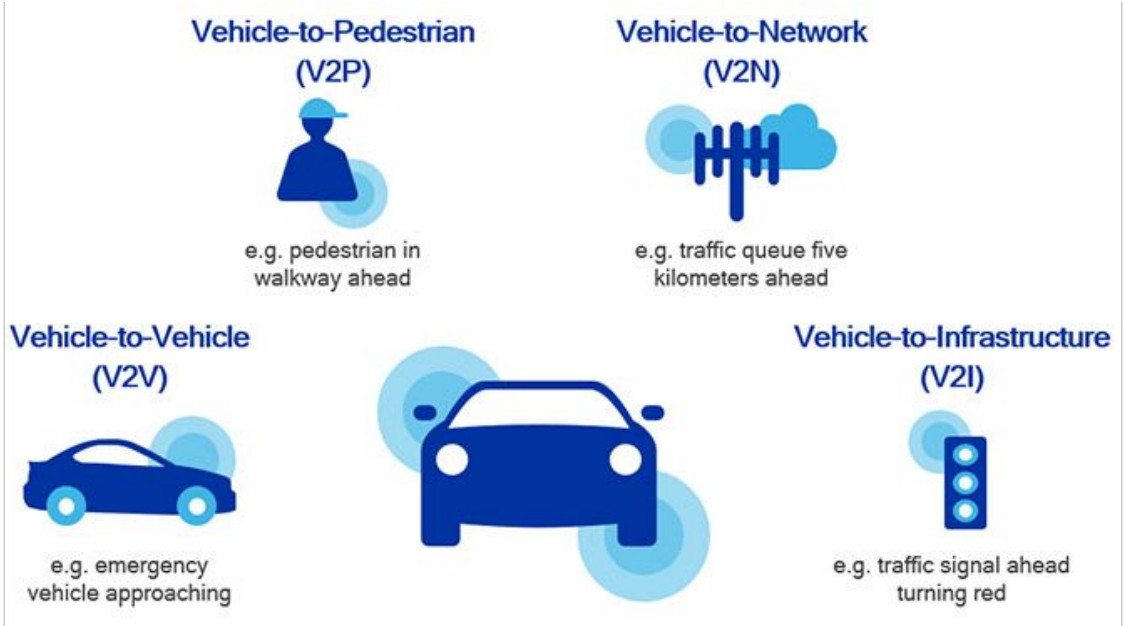
Caio Teixeira[1], Marco A. A. Henriques[1]

[1]DCA/FEEC - Unicamp

Foco do trabalho

- Estágio preliminar
- Não apresenta resultados parciais/completos
- Objetivo:
  - Alavancar mais pesquisa na área
  - Incentivar colaboração

Contexto: Comunicações *V2X*



Fonte: *The path to 5G: Paving the road to tomorrow's autonomous vehicles*, Qualcomm

Mensagens de Cooperação

Mensagens curtas (de 400B a 2KB) e enviadas com frequência alta (≈ 100ms).

Componentes: Dados de velocidade e posição, identificação, etc.

Autenticação é fundamental!

Segurança em redes veiculares

Todas mensagens de coordenação incluem uma assinatura e, opcionalmente, um certificado.

Todos padrões atuais utilizam o algoritmo ECDSA (baseado em curvas elípticas).

Requisito adicional: múltiplas identidades para evitar rastreamento.

Pseudônimos

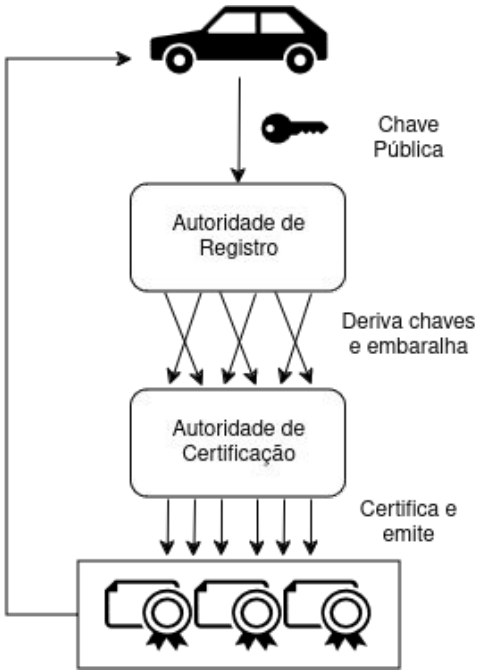
Múltiplos certificados referentes ao mesmo veículo.

- Alta rotatividade (minutos) e baixo tempo de vida (uma semana) evitam rastreamento;
- Todos pseudônimos devem ser devidamente certificados por uma autoridade certificadora.

Butterfly Key Expansion[1] (BKE)

Derivação de múltiplos certificados a partir de uma única chave pública.

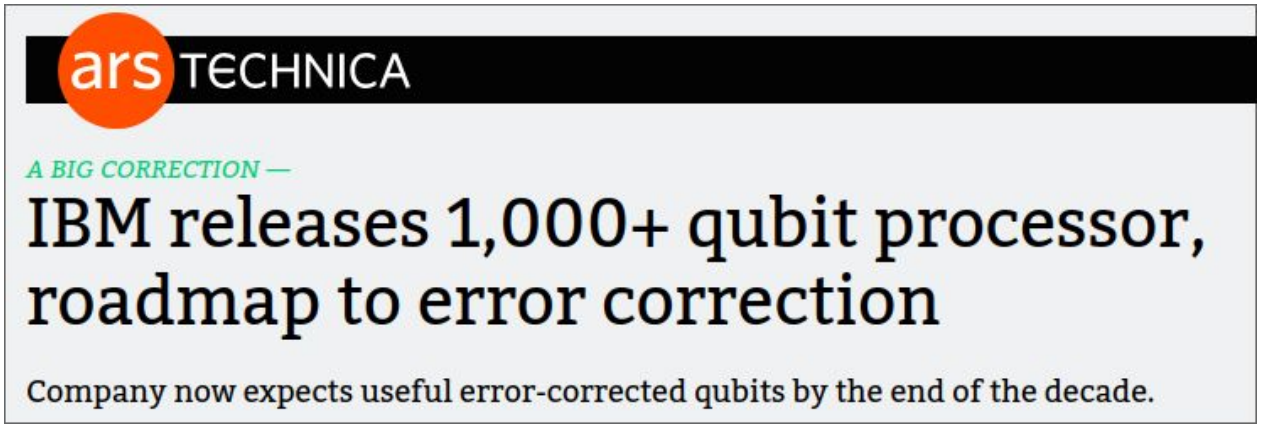
Possibilitado pela propriedade de homomorfismo sobre adição de pontos em curvas elípticas.



[1] Brecht, B. et al. (2018). A Security Credential Management System for V2X Communications.

Desafios pós-quânticos

ECDSA não é seguro diante de um computador quântico, devido ao algoritmo de Shor[2].



[2] Shor, P. (1994). Algorithms for quantum computation: discrete logarithms and factoring.

Desafios pós-quânticos

Esquemas pós-quânticos padronizados são muito mais custosos, e não suportam homomorfismo sobre adição.

ECDSA	**64 bytes**
FALCON	666 bytes
CRYSTALS-Dilithium	2420 bytes
SPHINCS+	17088 bytes

Comparação de tamanhos de assinatura de algoritmos padronizados

Propostas de pesquisa

1. **Avaliação do impacto no canal ao se adotar esquemas pós-quânticos**
   a. Qual a densidade de dispositivos suportada por cada algoritmo? Em quais cenários seria apropriado seu uso?
   b. Avaliação de novos algoritmos pós-quânticos sob avaliação do NIST

Propostas de pesquisa

2. **Segurança pós-quântica com menor tempo de validade**
   a. Precisamos de apenas uma semana por pseudônimo → requisitos de segurança menores;
   b. Algoritmos pós-quânticos mais flexíveis podem podem ter seus parâmetros reduzidos, mantendo a segurança mínima necessária (ex. XMSS e LMS).

Propostas de pesquisa

3. ***Butterfly Key Expansion* pós-quântico**
   a. Buscar algoritmos que apresentam homomorfismo sobre adição[3];
   b. Avaliar se pseudônimos podem ser derivados a partir de algoritmos pós-quânticos que utilizam árvores de Merkle.

[3] Barreto, P., Ricardini, J., Simplicio, M., and Patil, H. (2018). qSCMS: Post-quantum certificate provisioning process for V2X.

Propostas de pesquisa

4. **Métodos indiretos de redução de assinaturas e certificados no sistema**
   a. Autenticação por blocos de mensagem[4];
   b. Divulgação de certificados sob demanda (*Peer-to-peer Certificate Distribution*).

[4] Cominetti, E. L., Silva, M. V. M., Simplicio, M. A., Kupwade Patil, H., and Ricardini, J. E. (2023). Faster verification of V2X basic safety messages via Message Chaining.

Obrigado!

Caio Teixeira
caio@dca.fee.unicamp.br

Marco A. A. Henriques
maah@unicamp.br

ERICSSON

Slides extras

Padrões de comunicação veicular

Comunicação por interfaces de rede sem fio:
Dedicated Short-Range Communications (DSRC)

- Padronizada em 2010, em uso em diversos países
- Apenas para comunicações por proximidade

Padrões de comunicação veicular

Comunicação por interfaces de rede celular:
Cellular V2X (C-V2X)

- Mais recente, busca superar limites do DSRC
- Possibilita aplicações usando comunicação via rede

Padrões para camadas superiores

Estados Unidos

- **Comunicação:** *Wireless Access in Vehicular Environments* (WAVE)
- **Infraestrutura de Segurança:** *Security Credential Management System* (SCMS)
- **Mensagens de Cooperação:** *Basic Safety Message* (BSM)

Padrões para camadas superiores

Europa

- **Comunicação:** *Intelligent Transport Systems G5* (ITS-G5) & *Collaborative ITS* (C-ITS)
- **Infraestrutura de Segurança:** C-ITS *Security Management*
- **Mensagens de Cooperação:** *Coordination and Awareness Message* (CAM)

BKE com curvas elípticas

Seja $f(x)$ uma função pré-determinada, K uma chave pública e k uma chave privada do ECDSA, e G seu ponto gerador.

Podemos derivar novas chaves públicas calculando:

$$K'_i = K + f(i) \cdot G$$

E a chave privada correspondente será $k'_i = k + f(i)$.