Tempest

ACADEMY

Conference

2023

Segurança em comunicações veiculares (V2X)

Prof. Dr. Marcos A. Simplicio Jr.
Universidade de São Paulo (USP)

01 Contexto: comunicações veiculares

02 Desafios de segurança e privacidade

03 Soluções -- foco: IEEE 1609 (EUA)
Gestão de certificados & processamento de assinaturas

04 Considerações finais

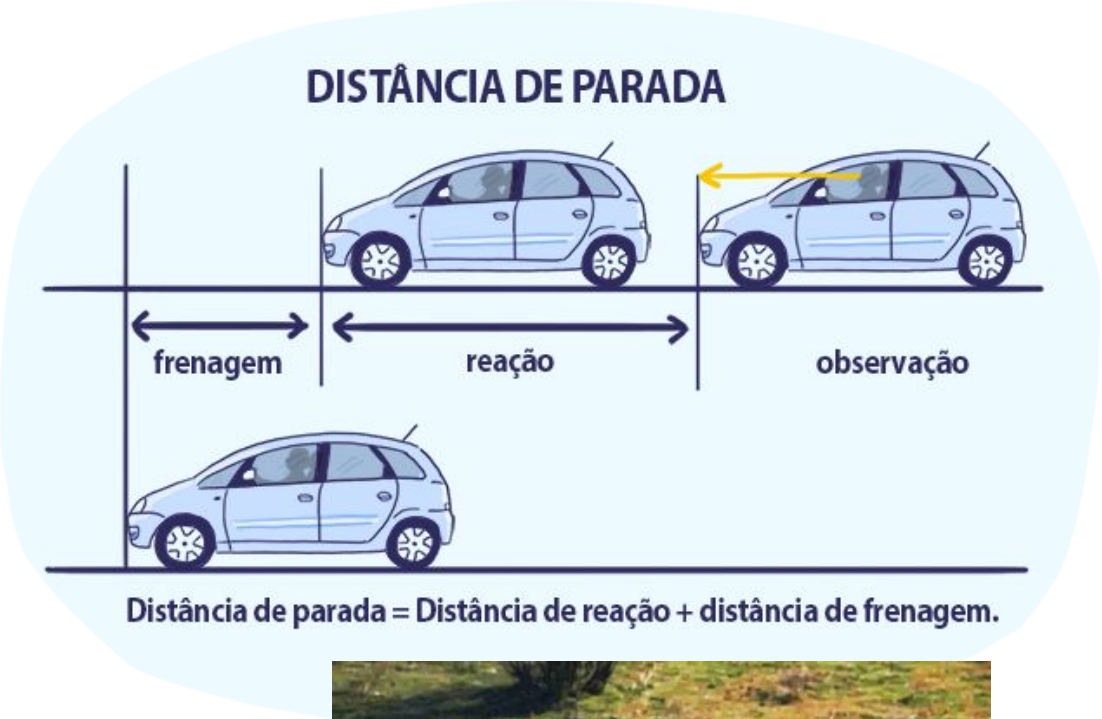
Agenda

- Contexto: comunicações veiculares
- Desafios: segurança e privacidade
- Soluções na literatura (foco: IEEE 1609 - EUA)
  - Gestão de certificados: emissão com chaves borboleta
  - Gestão de certificados: revogação com CRLs e ACPC
  - Processamento de assinaturas digitais: verify-on-demand
- Considerações finais

Marcos quem?

- Em suma:
  - Pesquisador na área de cibersegurançae criptografia desde 2007
  - Professor associado na Universidade de São Paulo (USP) desde 2011
  - Vice coordenador da Comissão Especial em Segurança da Informação e de Sistemas Computacionais (CE-Seg) da Sociedade Brasileira de Computação (SBC)
- Experiência com redes veiculares:
  - Motorista desde 2015 (sim, demorei…)
  - Parceria com a LG Electronics de 2017 – 2021: publicações, patentes, padrões, …
    - Várias ideias discutidas junto ao 5G Automotive Association (5GAA)
    - 2 soluções incluídas no padrão IEEE 1609.2.1-2022: UBK e ACPC

Contexto: desafios técnicos ao volante



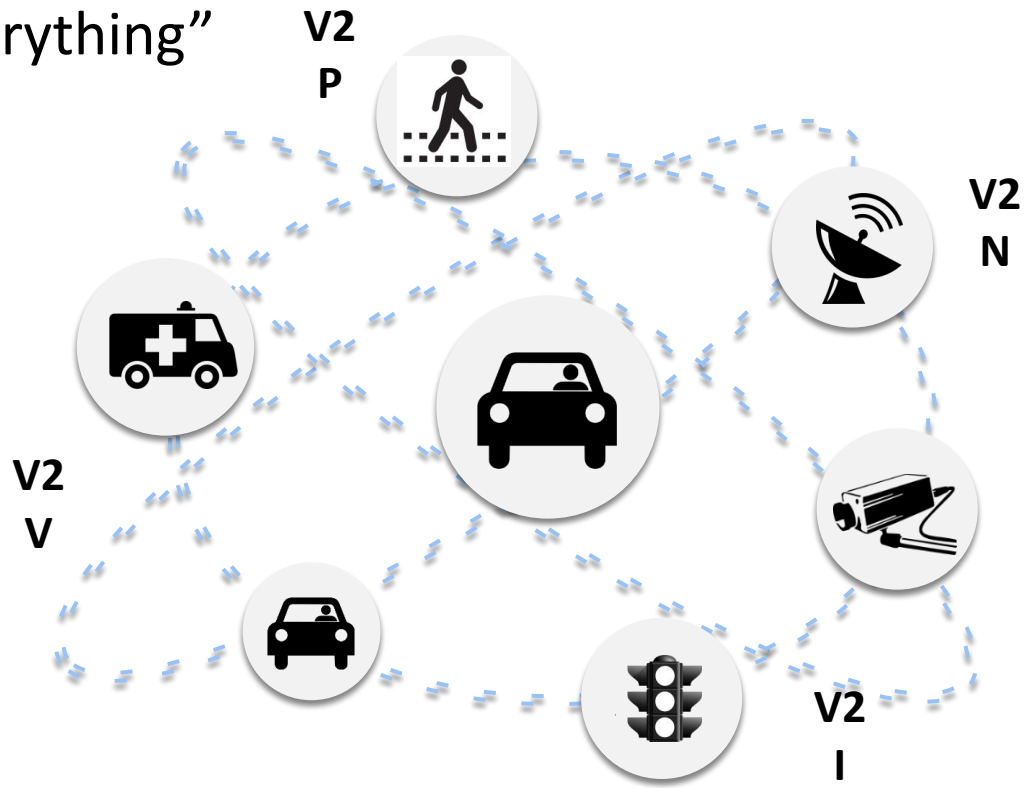
Contexto: desafios com pessoas ao volante

Av. Brigadeiro Faria Lima c/ Av. Juscelino Kubitschek, São Paulo/SP, 02/02/2017

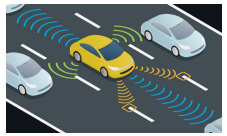
Qualquer estrada, qualquer lugar do Brasil, **/**/****

Solução: Comunicações veiculares (V2X)

- Veículo-Veículo, Veículo-Infraestrutura, Veículo-Pedestres, Veículo-rede…
  - “Vehicle-to-Everything”



Solução: Comunicações veiculares (V2X)



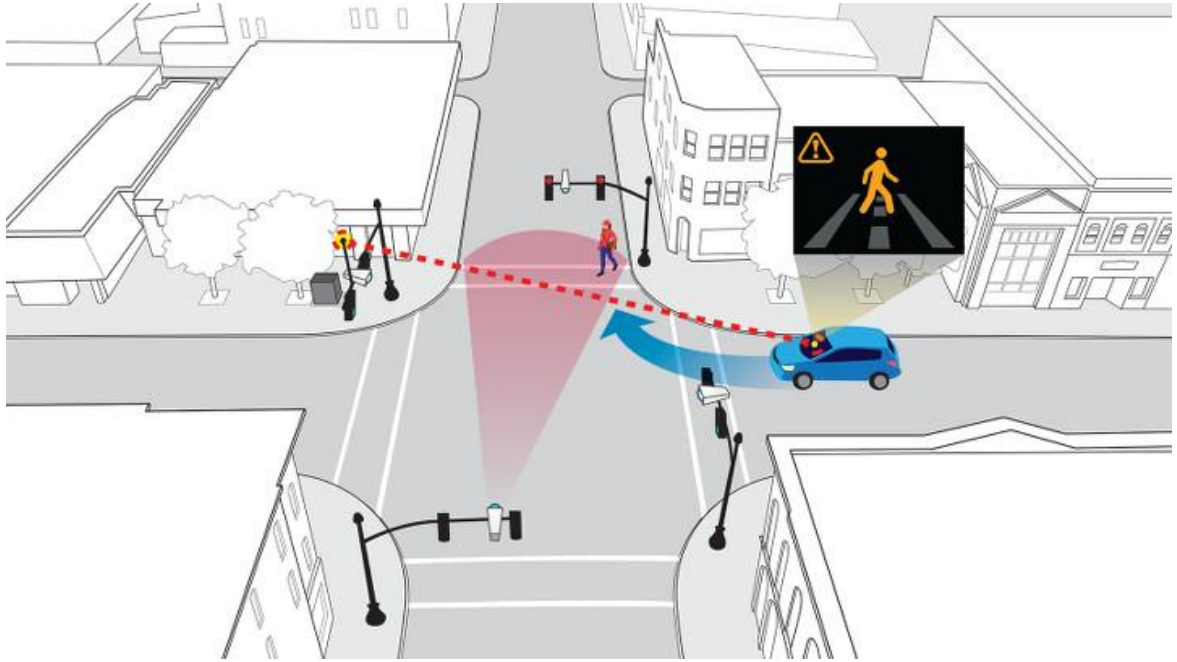
- Mensagens enviadas periodicamente: comumente, 10 por segundo
  - *US*[1]*: Basic safety messages* (**BSM**); EU[2]: *Cooperative Awareness Messages* (**CAM**)
    - Posição, velocidade, direção, (des)aceleração, frenagem, dimensões do veículo, ...
  - *Decentralized Environmental Notification Message* (**DENM**)
    - Obras na pista, pista molhada, desvio, velocidade máxima, ...

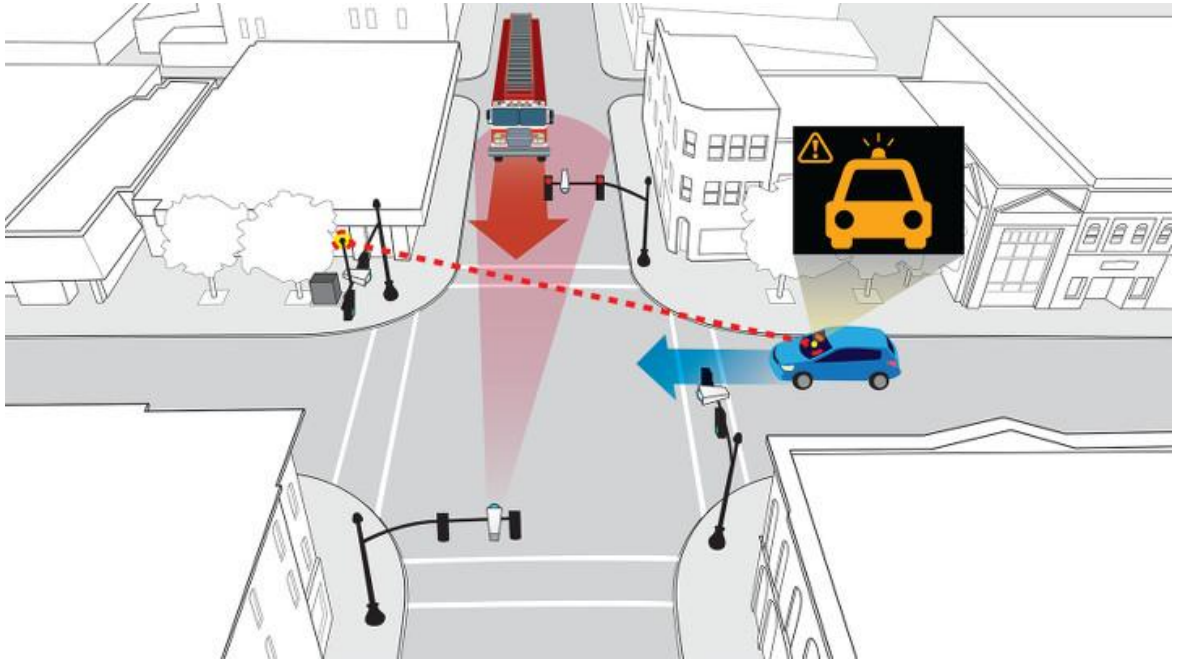
- Processadas por computador de bordo
  - Detecção de potenciais situações de risco: **alerta a motorista**, ou **ação (semi) autônoma** para reduzir tempo de reação (~1s para motorista atento)
  - Objetivo: **evitar acidentes** e **aumentar eficiência** de transportes

- Importante para veículos autônomos
  - “Visão além do alcance”: vai além de câmera e sensores de distância locais

Principais padrões: [1] IEEE 1609.2.1 -2022; [2] ETSI C-ITS standards

Solução: Comunicações veiculares (V2X)

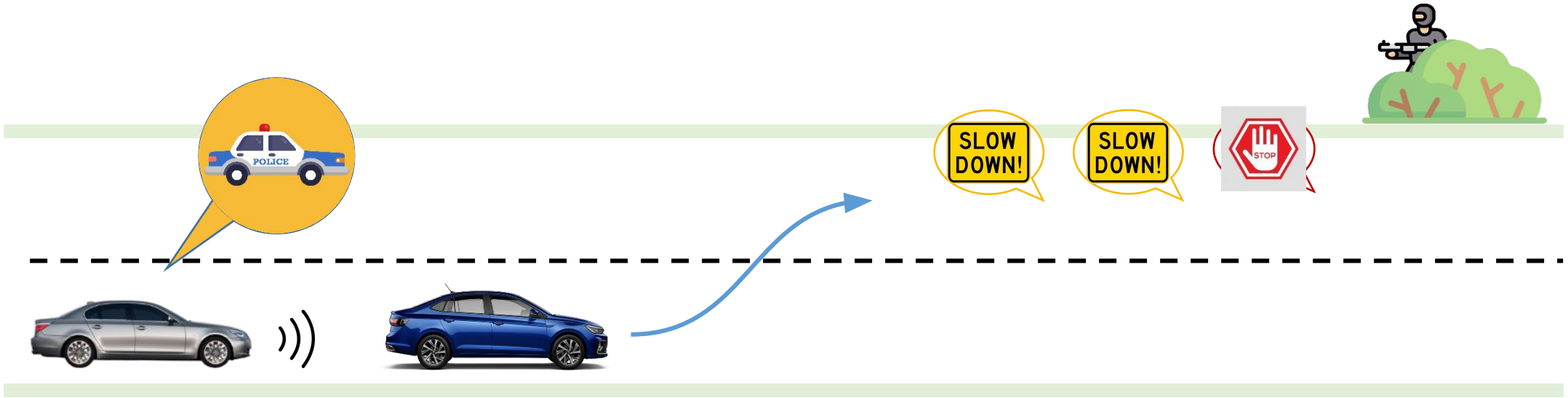




https://www.topgear.com.ph/news/technology-news/honda-volkswagen-v2x-communication-intersections-a2578-20181007

Segurança e Privacidade em V2X

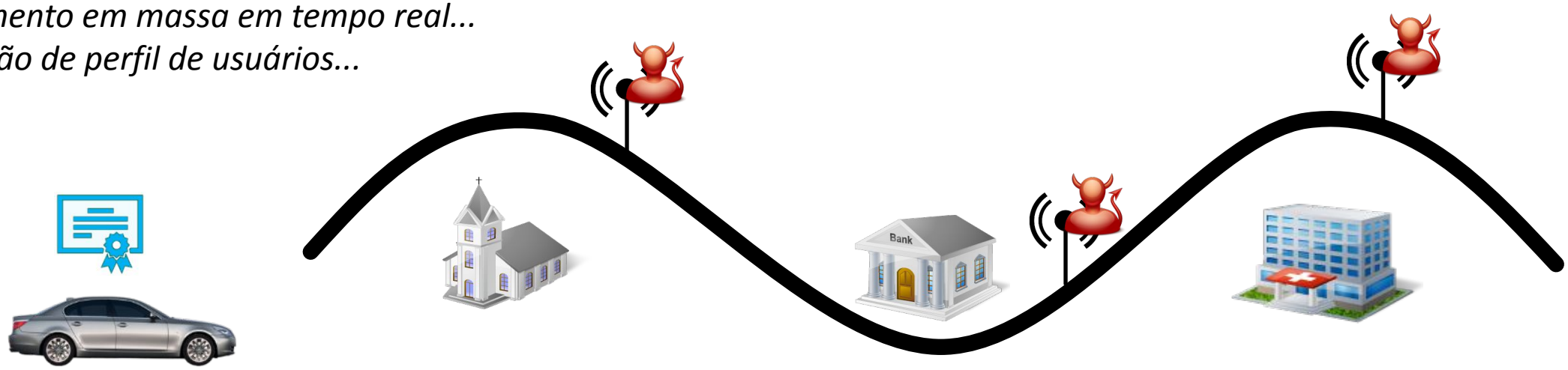
- Risco: poluição com mensagens falsas
  - **Vantagens indevidas**: personificação de veículos de emergência; imitação de vários veículos (semáforos inteligentes)
  - **Ações criminosas**: redução de velocidade para facilitar roubo, ...
  - **Vandalismo/terrorismo**: frenagem brusca, velocidade máxima falsa, ...



Segurança e Privacidade em V2X

- Vehicular Public Key Infrastructure (**VPKI**)
  - **Autenticidade**: **mensagens assinadas** por veículos autorizados
    - Certificados digitais gerenciados por HSM embarcado em veículo
  - **Privacidade**: riscos se for sempre usado o mesmo certificado...

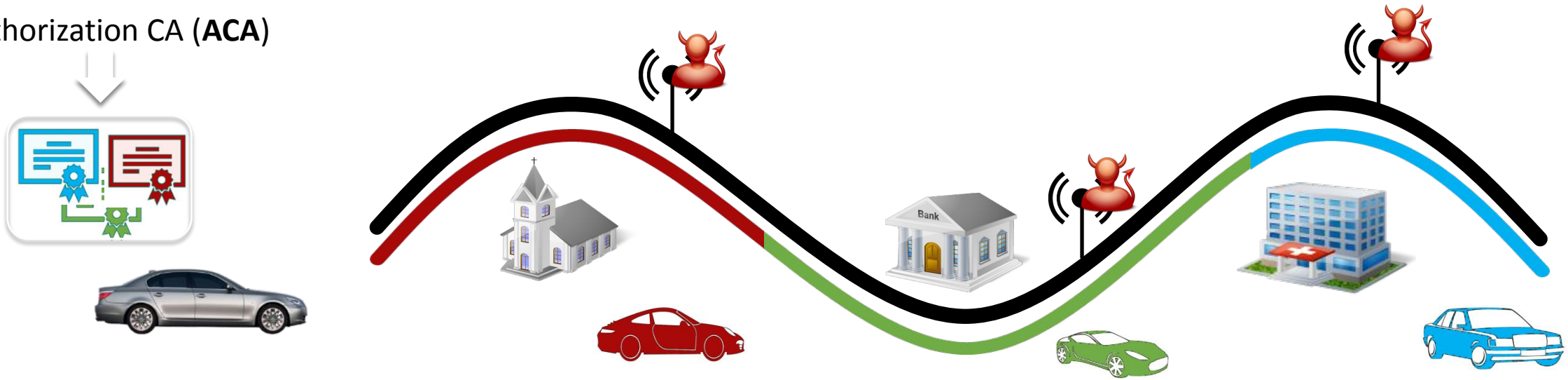
Rastreamento em massa em tempo real...
Construção de perfil de usuários...
...



Segurança e Privacidade em V2X

- Vehicular Public Key Infrastructure (**VPKI**)
  - **Autenticidade**: **mensagens assinadas** por veículos autorizados
  - **Privacidade**: certificados contêm pseudônimos
    - **Curta validade** (e.g., 1 semana); não identificam dono do veículo
    - **Múltiplos certificados** válidos simultaneamente: revezamento por veículo
    - Certificado + privacidade **revogados** em caso de mau comportamento

Authorization CA (**ACA**)



O custo da segurança...

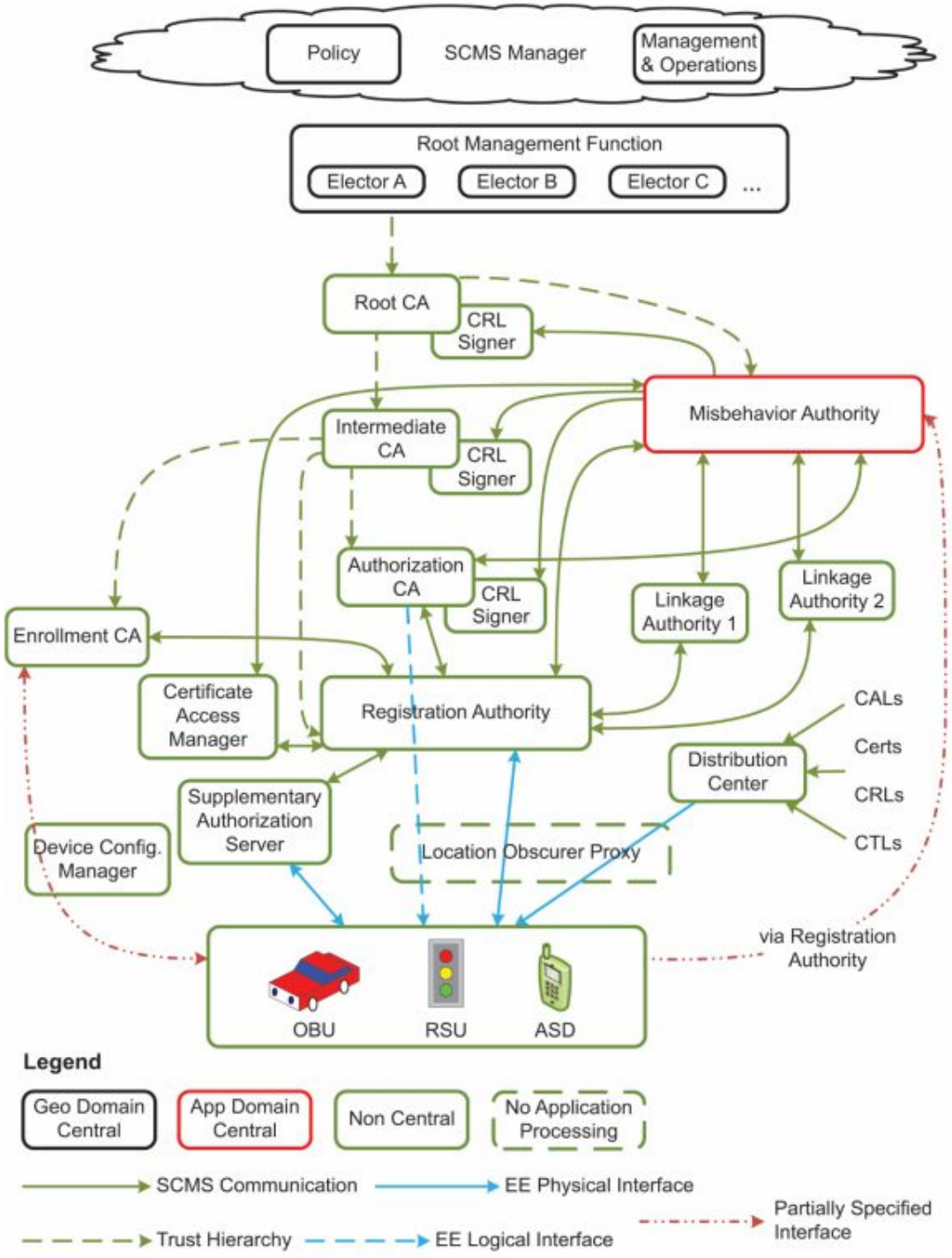
- Custo anual de manter tal VPKI:
  - #veículos em operação nos EUA em 2022: 286M (https://www.statista.com/)
  - #certificados por veículo: 100 certs/semana * 52 semanas/ano = 5200
  - Total: emissão e gestão de **1.5 trilhões de certificados/ano**

- Comparação: Let's Encrypt, "*the world's largest certificate authority*"
  - Lançado em Abril/2016
  - Fevereiro/2020: celebrou a emissão de 1 bilhão de certificados
    - letsencrypt.org/2020/02/27/one-billion-certs.html

 Otimizações são essenciais: **emissão** e **revogação** de certificados

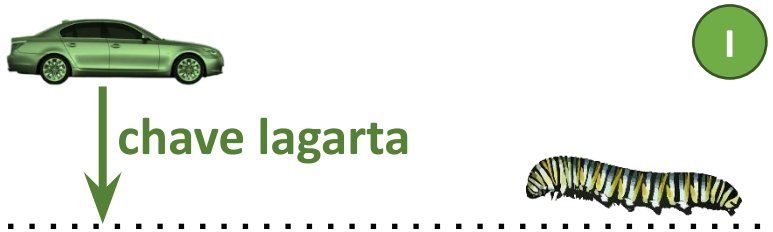
Padrão IEEE 1609: SCMS

- SCMS: Security Credential Management System
  - IEEE Std 1609.2.1-2022
- Desenvolvido em cooperação com o *United States Department of Transportation* (USDOT)
  - Principal padrão americano
- Foco desta apresentação



SCMS: Emissão de certificados

- Expansão de chaves “borboleta”: homomorfismo



Veículo

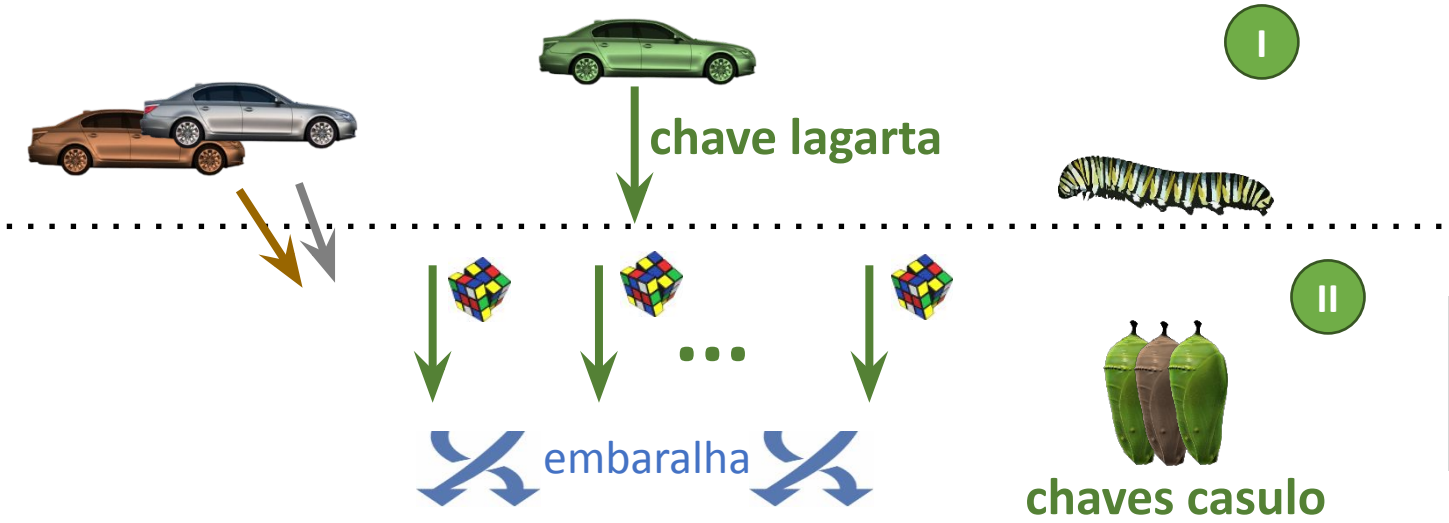
r, ***U*** = *r*•*G*

Registration Authority (RA)

Authorization CA (ACA)

SCMS: Emissão de certificados

- Expansão de chaves “borboleta”: homomorfismo



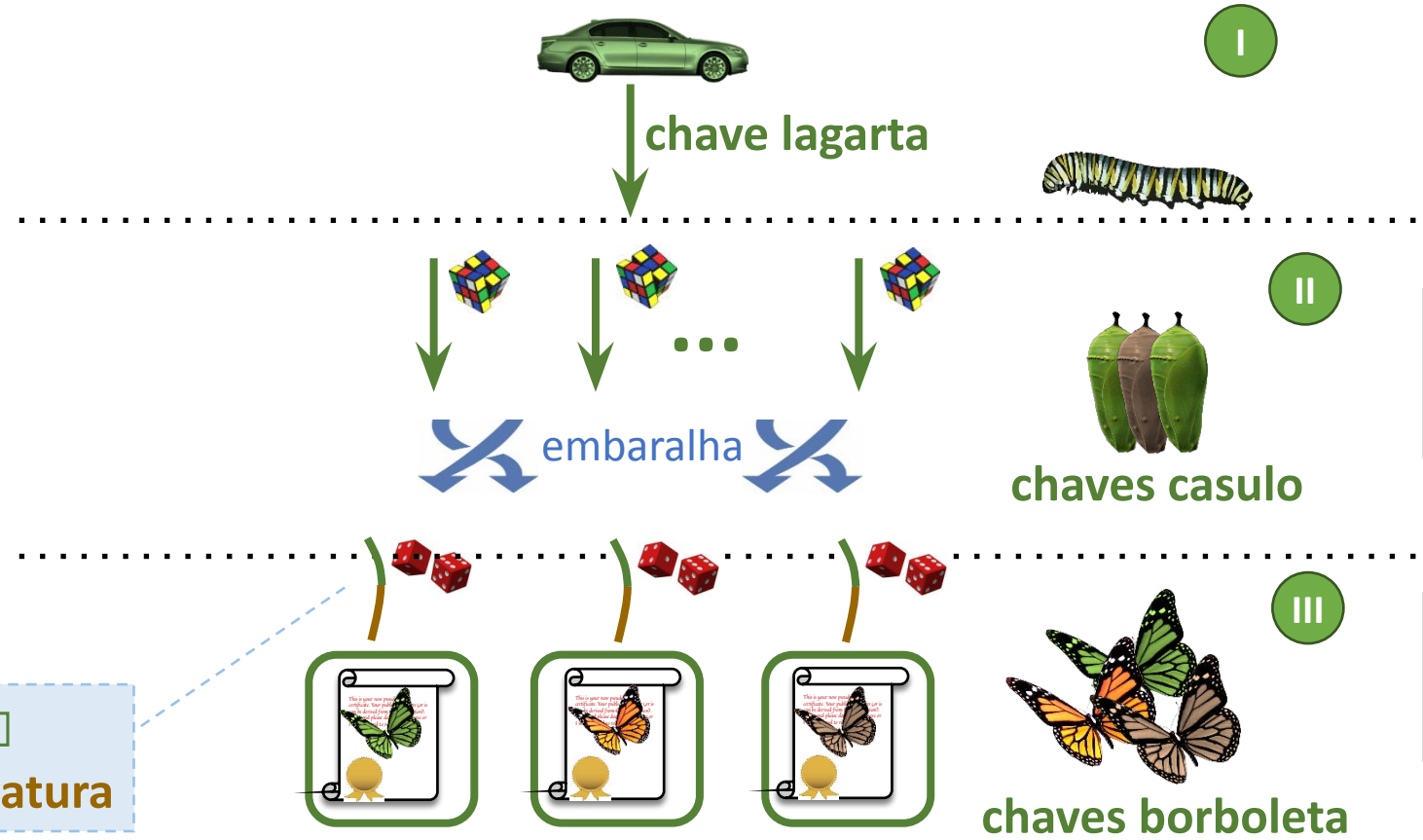
Veículo — $r, U = r \bullet G$

Registration Authority (RA) — $C_i = U + f(i) \bullet G$

Authorization CA (ACA)

SCMS: Emissão de certificados

- Expansão de chaves “borboleta”: homomorfismo



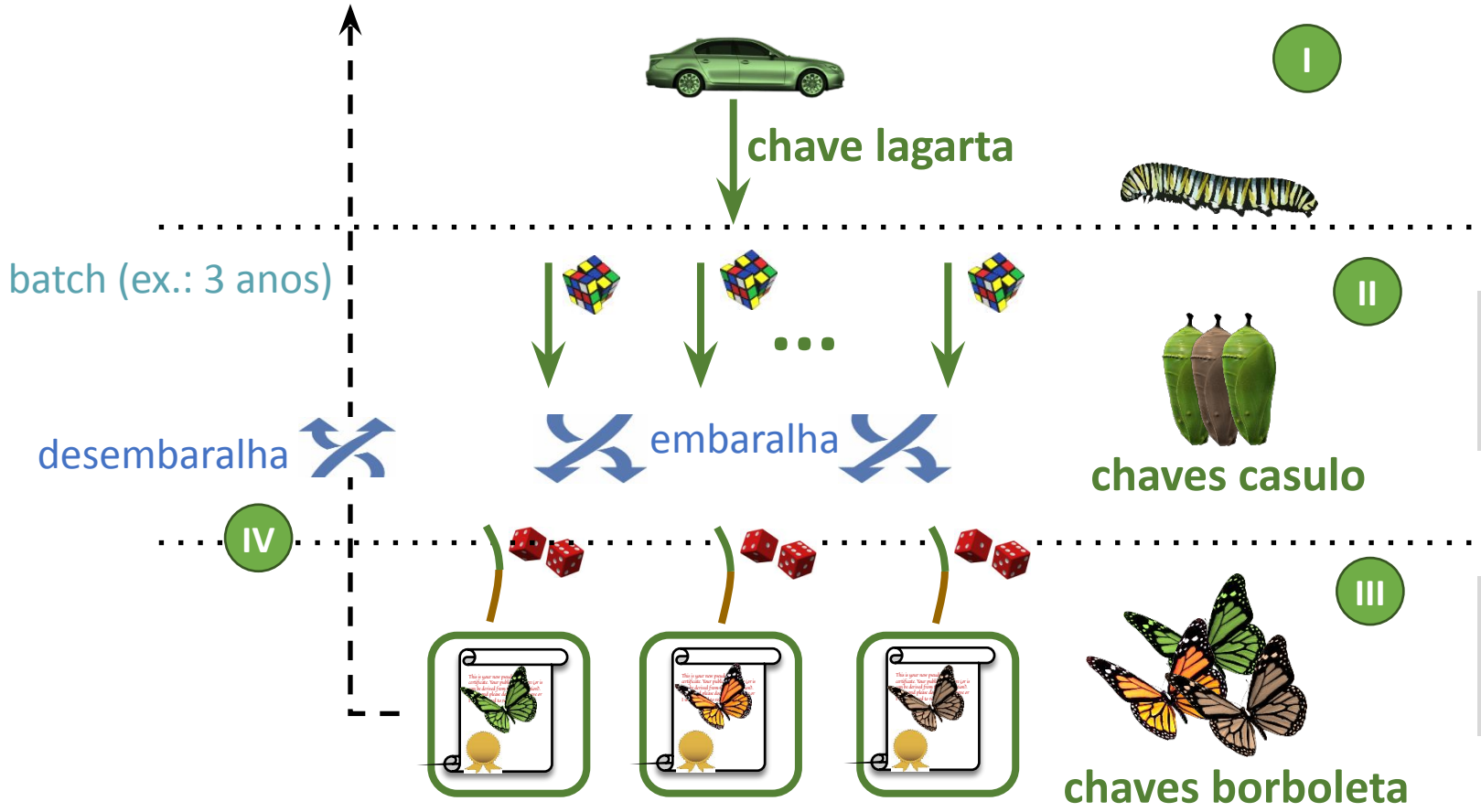
Veículo $r, U = r \bullet G$

Registration Authority (RA) $C_i = U + f(i) \bullet G$

Authorization CA (ACA) $B_i = C_i + s_i \bullet G$
$cert_i = (B_i, sig)$
$Enc(C_i, [s_i, cert_i])$

SCMS: Emissão de certificados

- Expansão de chaves “borboleta”: homomorfismo



Veículo

$r, U = r \bullet G$

Registration Authority (RA)

$C_i = U + f(i) \bullet G$

Authorization CA (ACA)

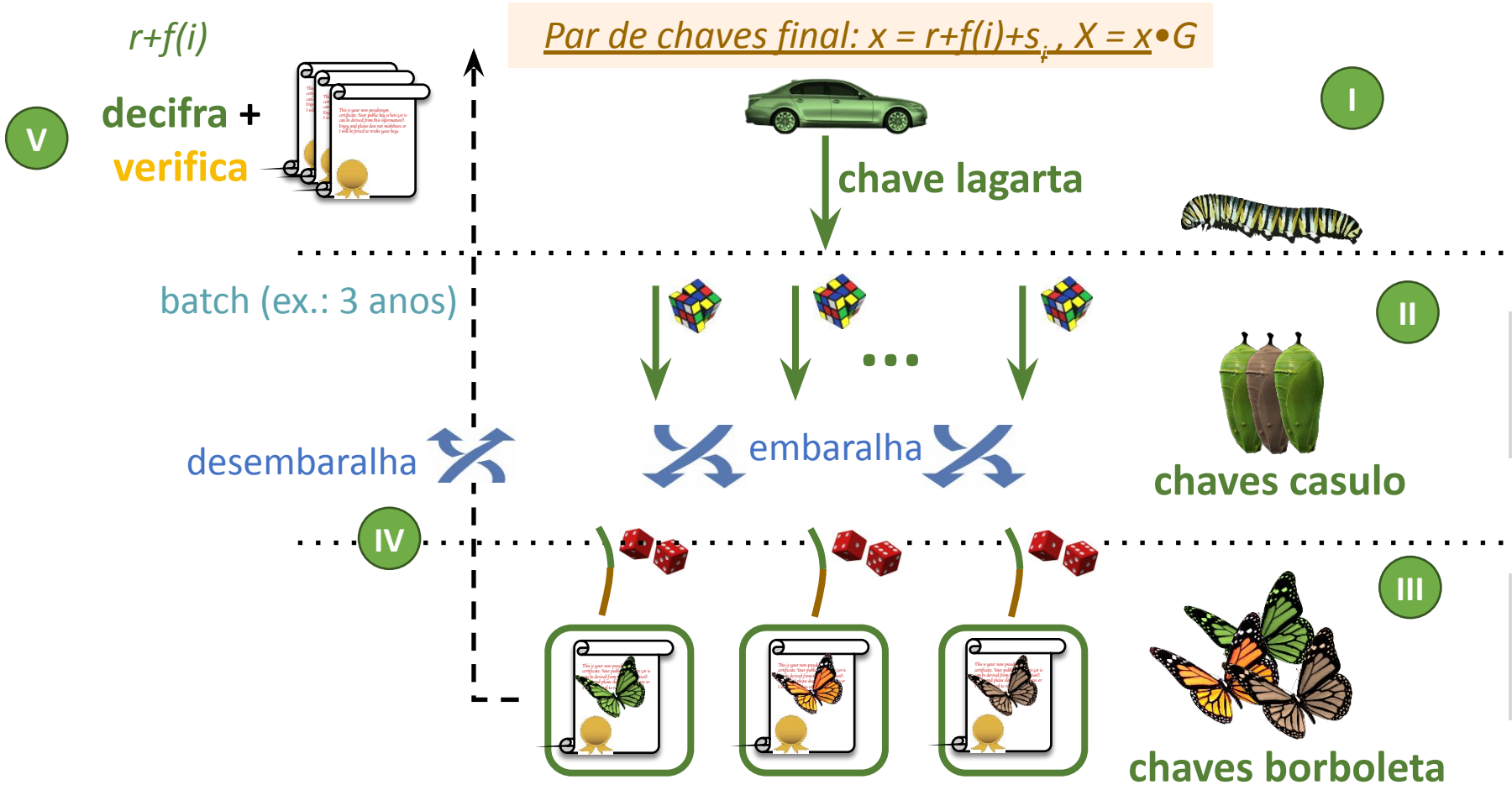
$B_i = C_i + s_i \bullet G$

$cert_i = (B_i, sig)$

$Enc(C_i, [s_i, cert_i])$

SCMS: Emissão de certificados

- Expansão de chaves “borboleta”: homomorfismo



Veículo

$r, U = r \bullet G$

Registration Authority (RA)

$C_i = U + f(i) \bullet G$

Authorization CA (ACA)

$B_i = C_i + s_i \bullet G$

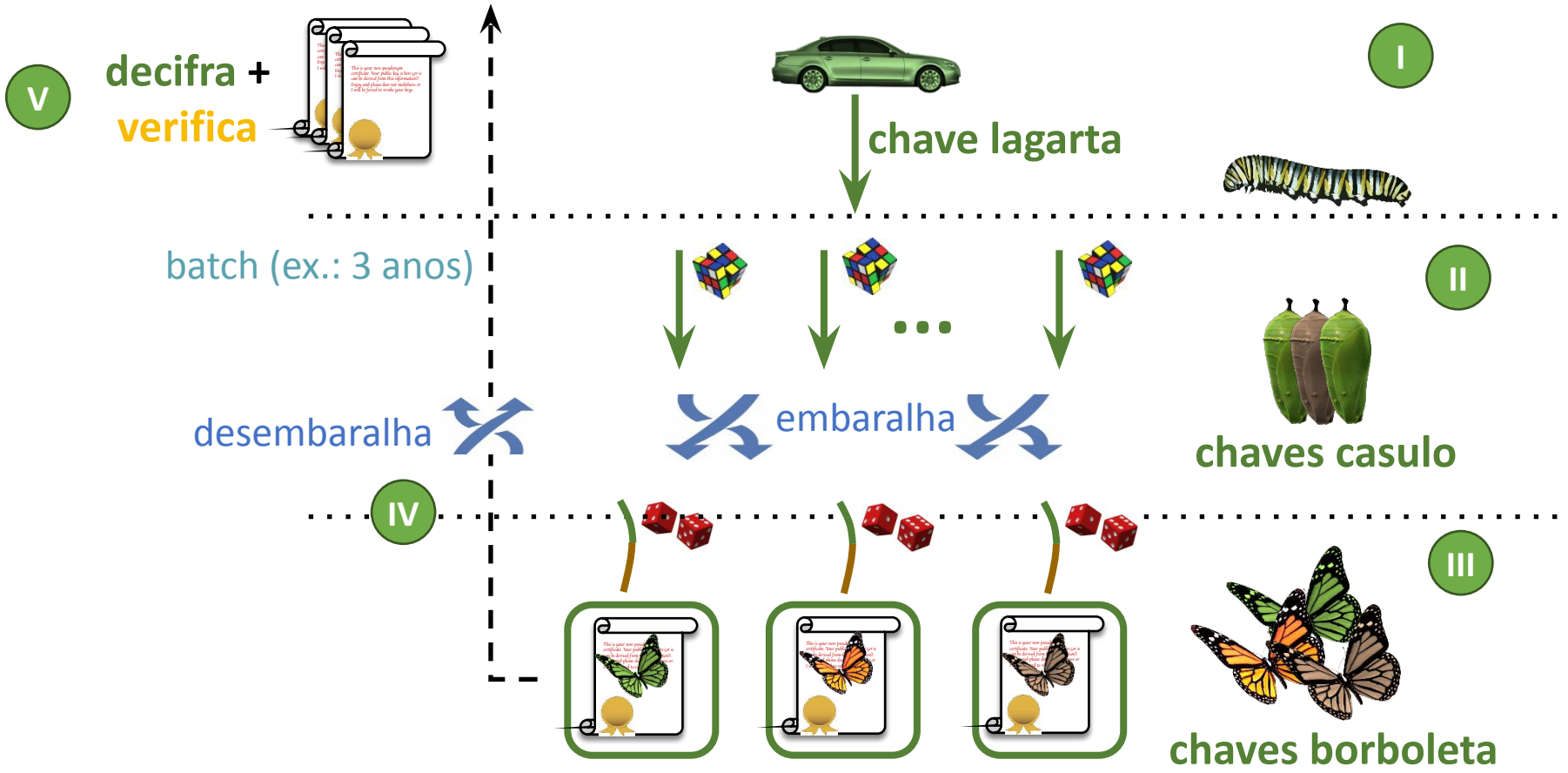
$cert_i = (B_i, sig)$

$Enc(C_i, [s_i, cert_i])$

SCMS: Emissão de certificados

- Expansão de chaves “borboleta”: privacidade

Privacidade via separação de deveres



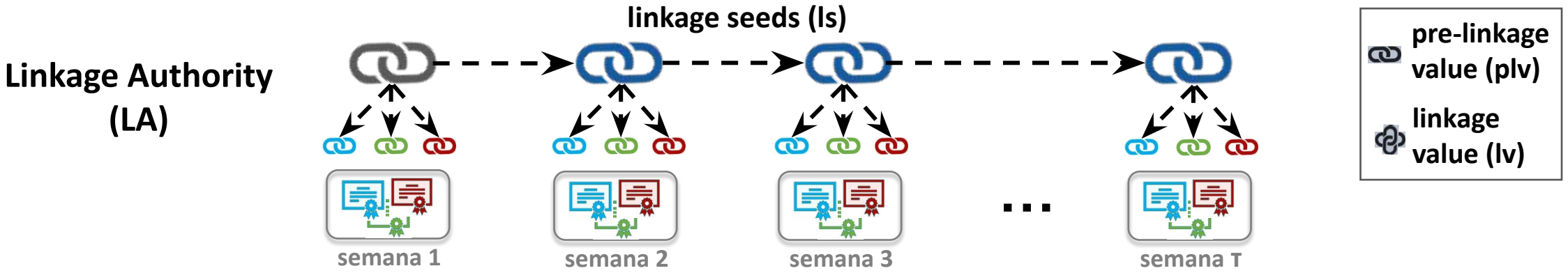
Veículo: único que sabe todos os seus certificados

RA: enxerga veículos, mas não seus certificados

ACA: sabe certificados, mas não os veículos

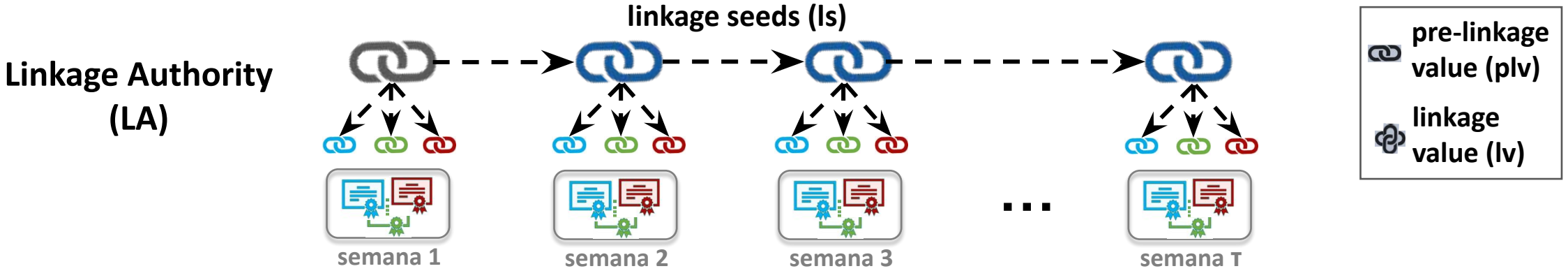
Revogação via linkage values: CRLs

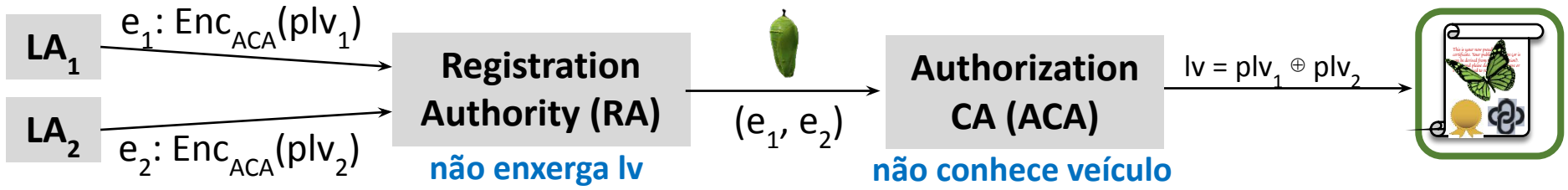
- Emissão de Certificate Revocation Lists (CRLs)
  - **1 única entrada** permite revogar **vários certificados** de um mesmo veículo
  - Linkage values (lv) inseridos nos certificados por ACA: $lv = plv_1 \oplus plv_2$



Revogação via linkage values: CRLs

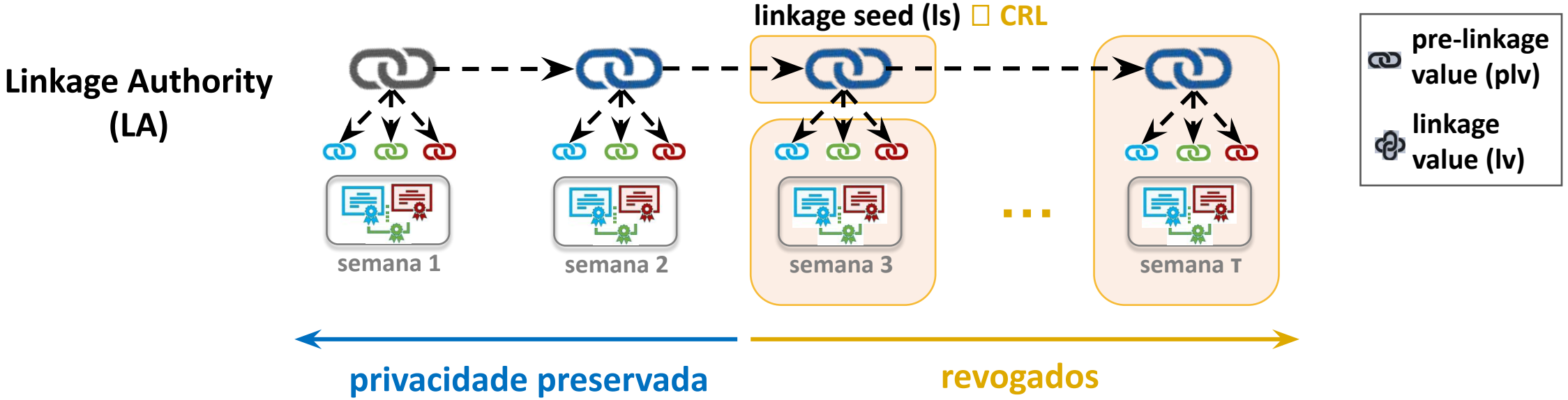
- Emissão de Certificate Revocation Lists (CRLs)
  - **1 única entrada** permite revogar **vários certificados** de um mesmo veículo
  - Linkage values (lv) inseridos nos certificados por ACA: $lv = plv_1 \oplus plv_2$





Revogação via linkage values: CRLs

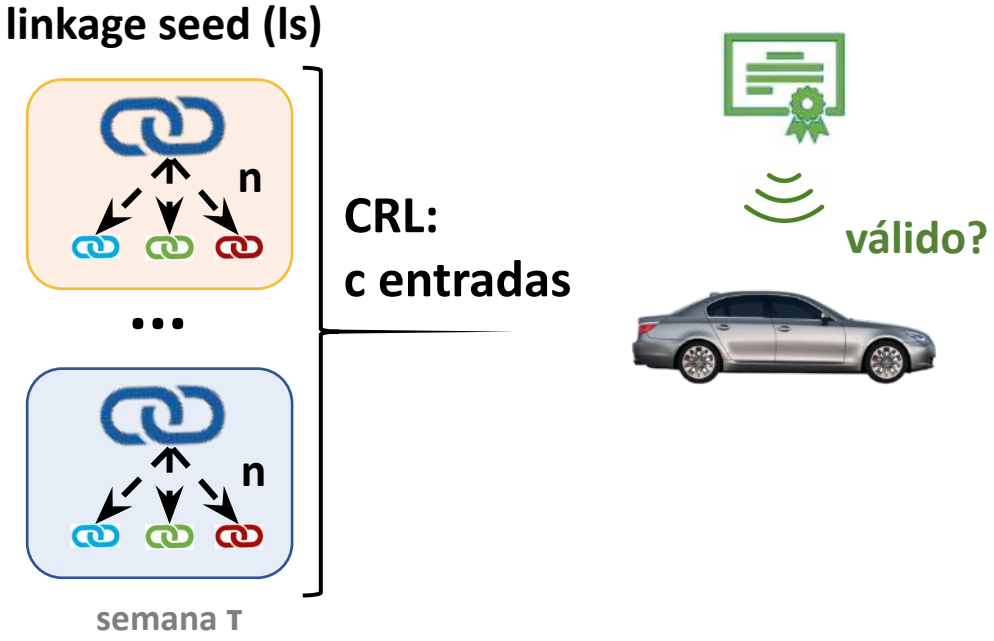
- Emissão de Certificate Revocation Lists (CRLs)
  - **1 única entrada** permite revogar **vários certificados** de um mesmo veículo
  - Linkage values (lv) inseridos nos certificados por ACA: $lv = plv_1 \oplus plv_2$



□ verificação de status de revogação de cada certificado: cálculo de várias derivações (hashes) p/ cada entrada na CRL

Revogação via linkage values: CRLs

- Emissão de Certificate Revocation Lists (CRLs)
  - **1 única entrada** permite revogar **vários certificados** de um mesmo veículo entradas na CRL (**linkage seeds**) permitem **calcular lv** revogados



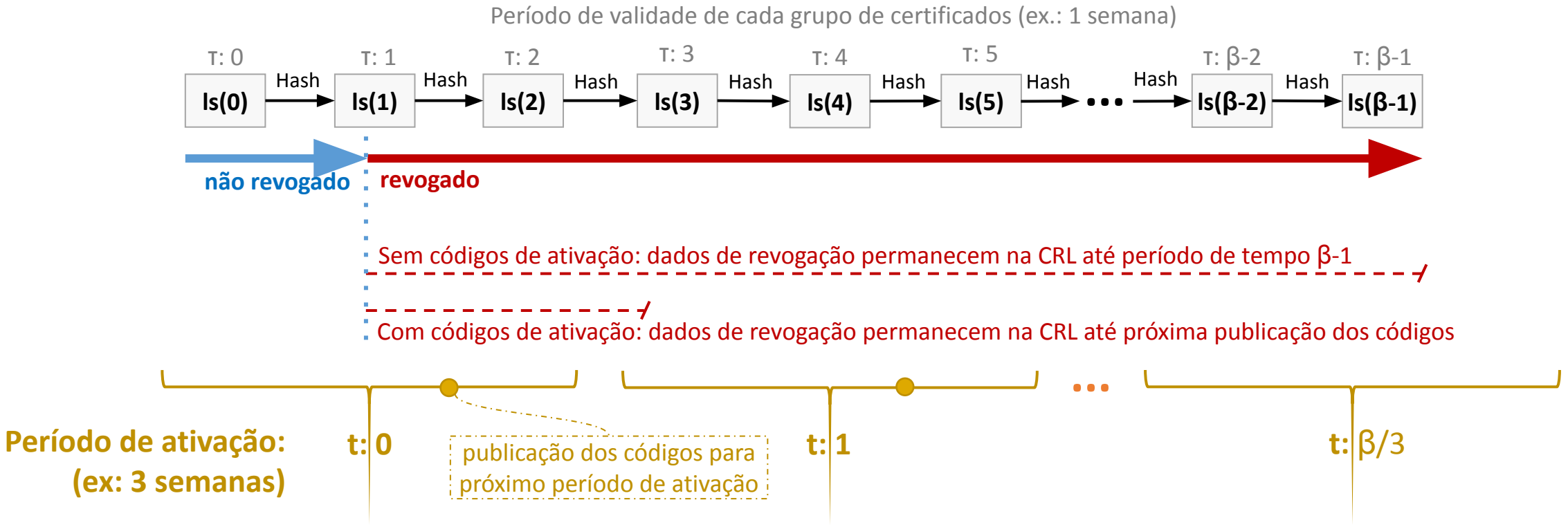
Se **n certificados por semana**, custo da verificação é:

- **Sob demanda**: **O(c·n) derivações** por certificado verificado
- **Pre-computação**, usando tabelas de busca (**LUTs**): LUT de **tamanho O(c·n)**; 1 lookup por certificado verificado

... e podem ser vários certificados recebidos por segundo...

Revogação via ACPC

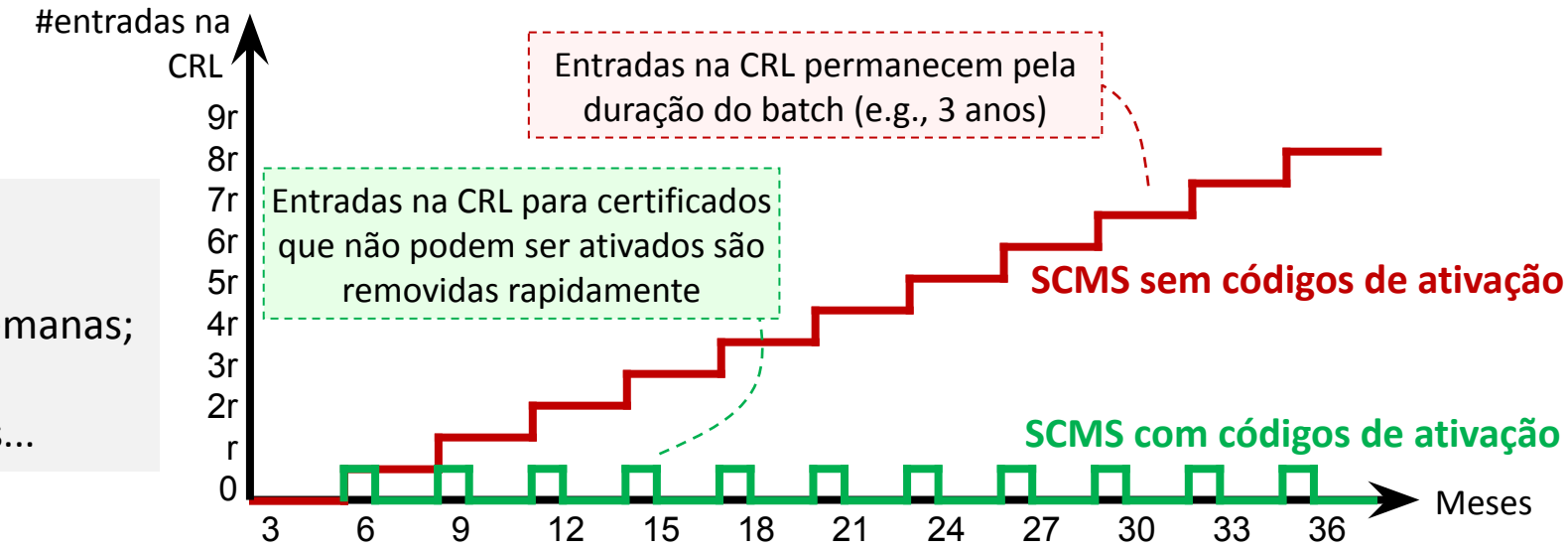
- Activation Codes for Pseudonym Certificates (ACPC)
- Certificate Access Manager (CAM): periodicamente publica "**códigos de ativação**", necessários para **decifrar certificados de pseudônimo**



Revogação via ACPC

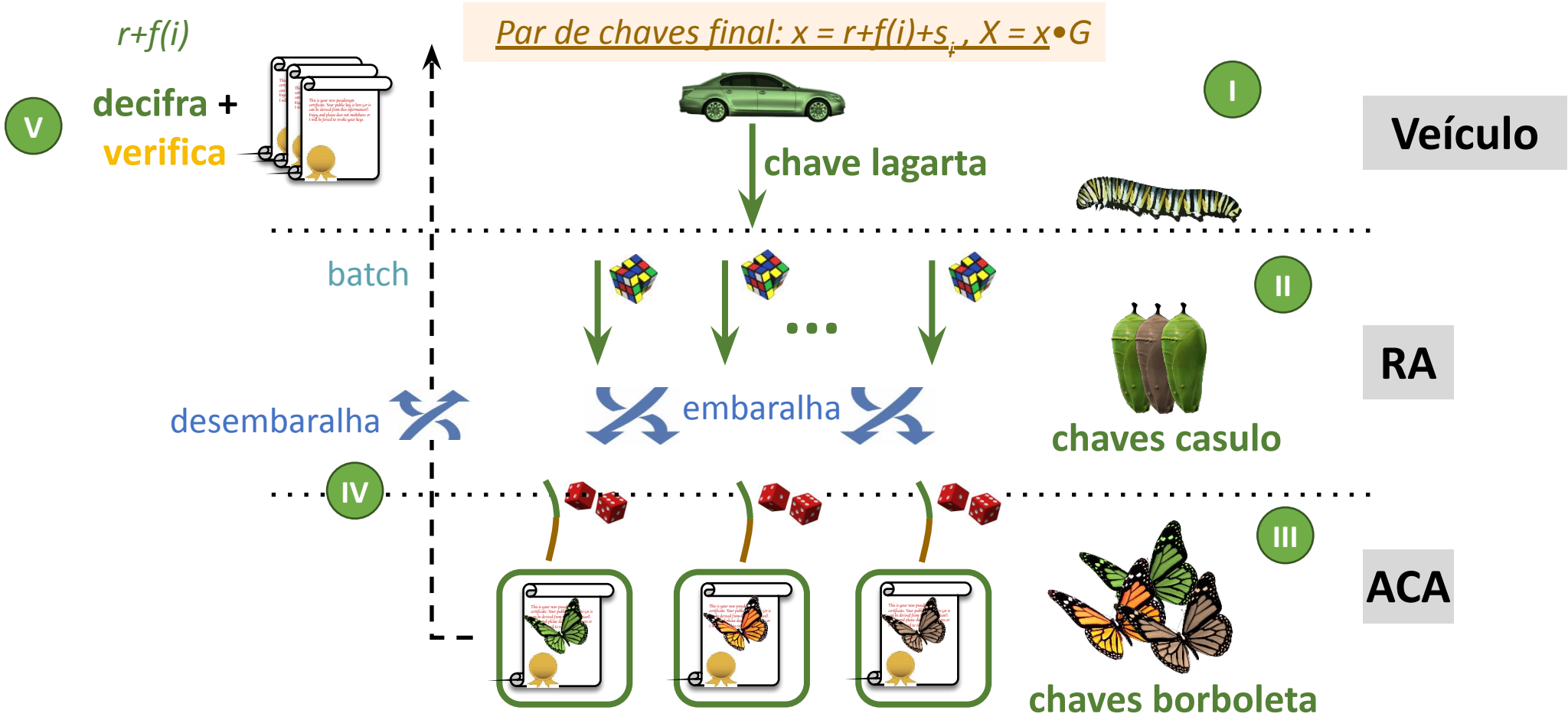
- Activation Codes for Pseudonym Certificates (ACPC)
- Certificate Access Manager (CAM): periodicamente publica "**códigos de ativação**", necessários para **decifrar certificados de pseudônimo**
  - **Reduz a necessidade/custo de CRLs**: mantém só certificados válidos em campo!
  - Permite emissão de batches de certificados p/ **vida útil** do veículo!

<u>Cenário de exemplo:</u>
- r veículos revogados a cada 3 meses;
- códigos de ativação publicados a cada 3 semanas;
- batches de certificados duram 3 anos
  - com ACPC, 3 anos e 30 anos são parecidos...



Revogação via ACPC: emissão

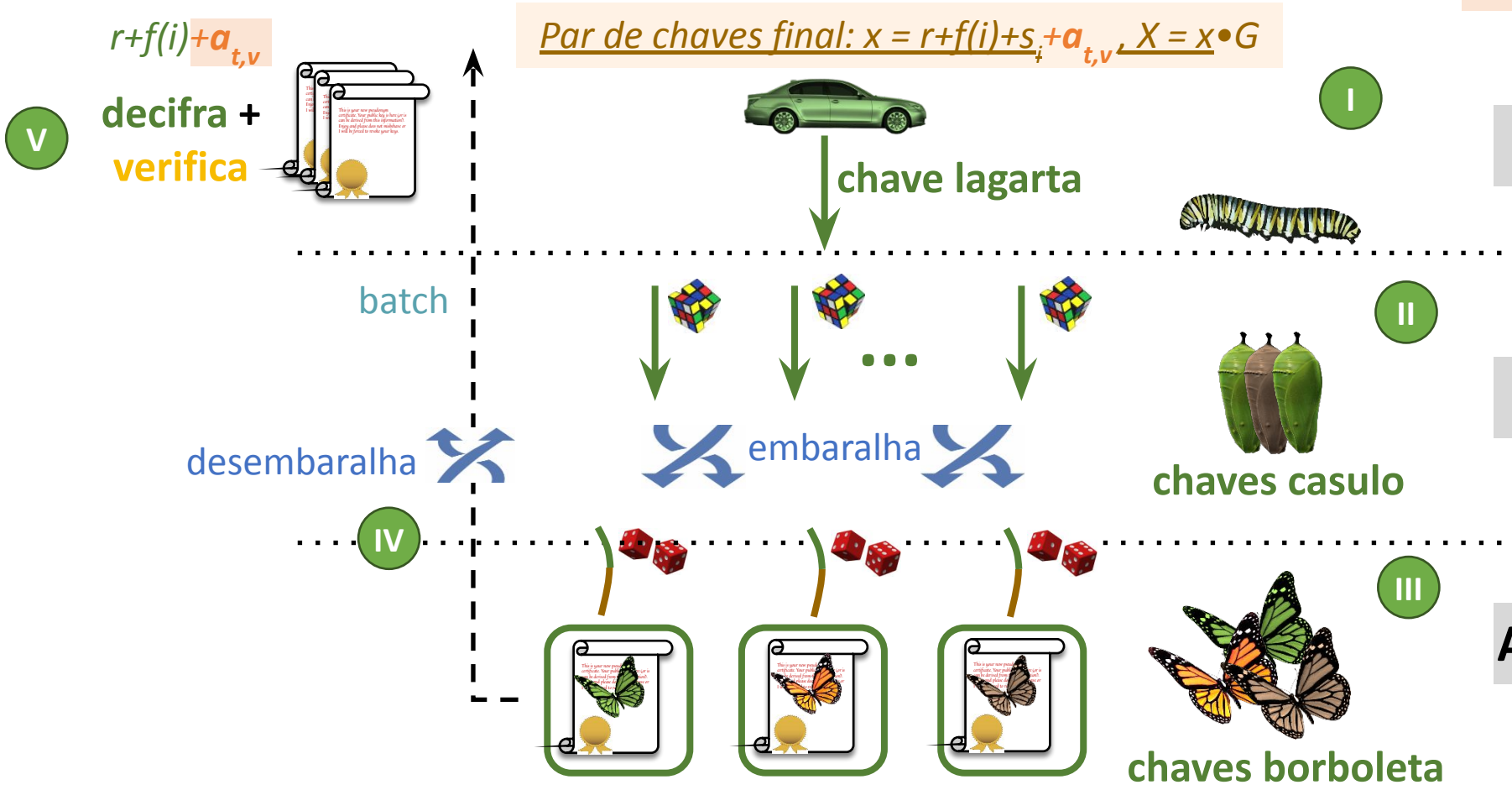
- **Recap**: expansão de chaves "borboleta"



Revogação via ACPC: emissão

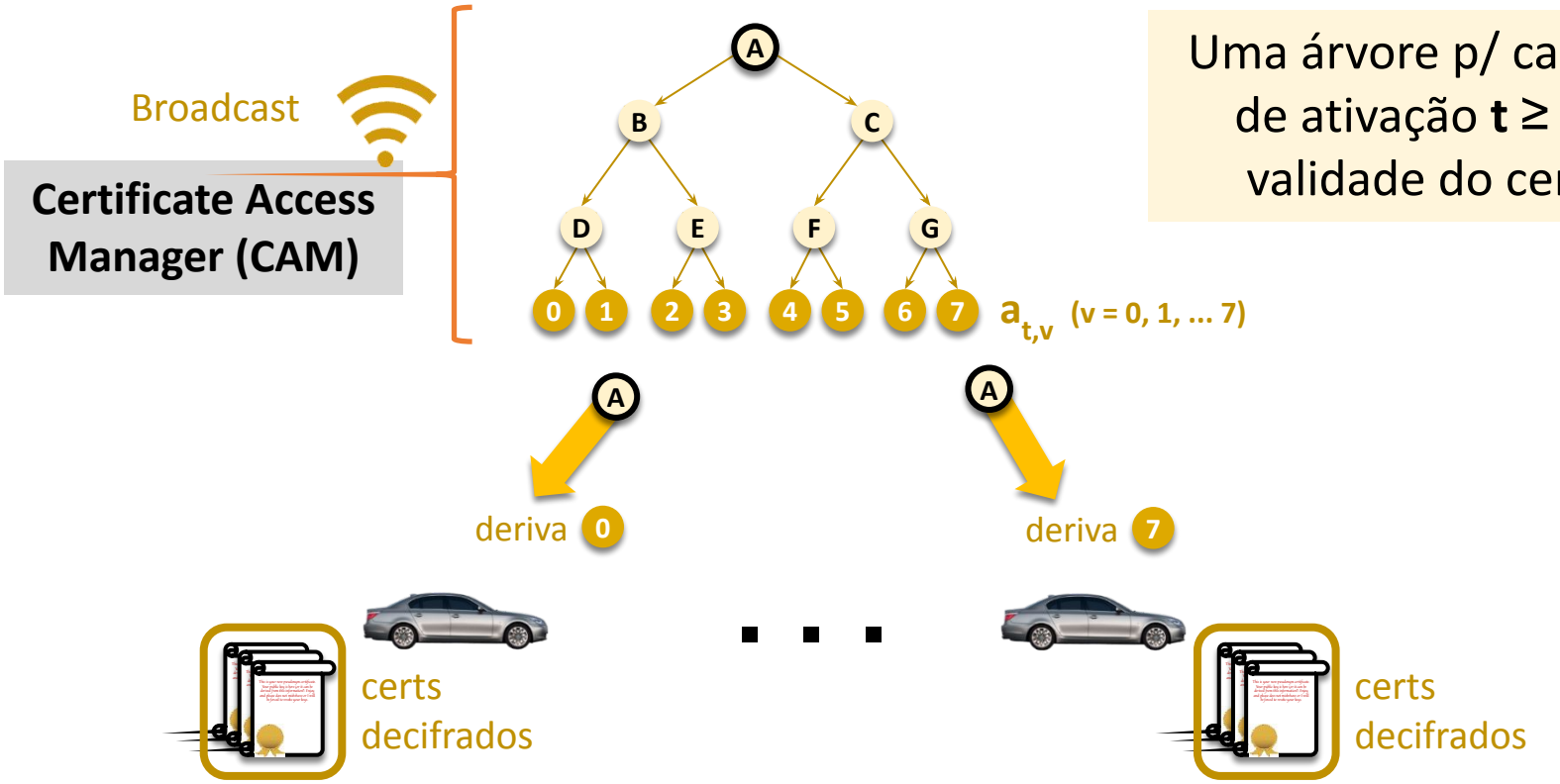
- Expansão de chaves “borboleta + ACPC

CAM insere códigos de ativação no processo de emissão de certificados: apenas CAM conhece códigos que permitem sua decifração



Revogação via ACPC: operação

- Códigos de ativação ($a_{t,v}$): derivados de árvore de ativação
  - Nenhuma revogação: broadcast da raíz

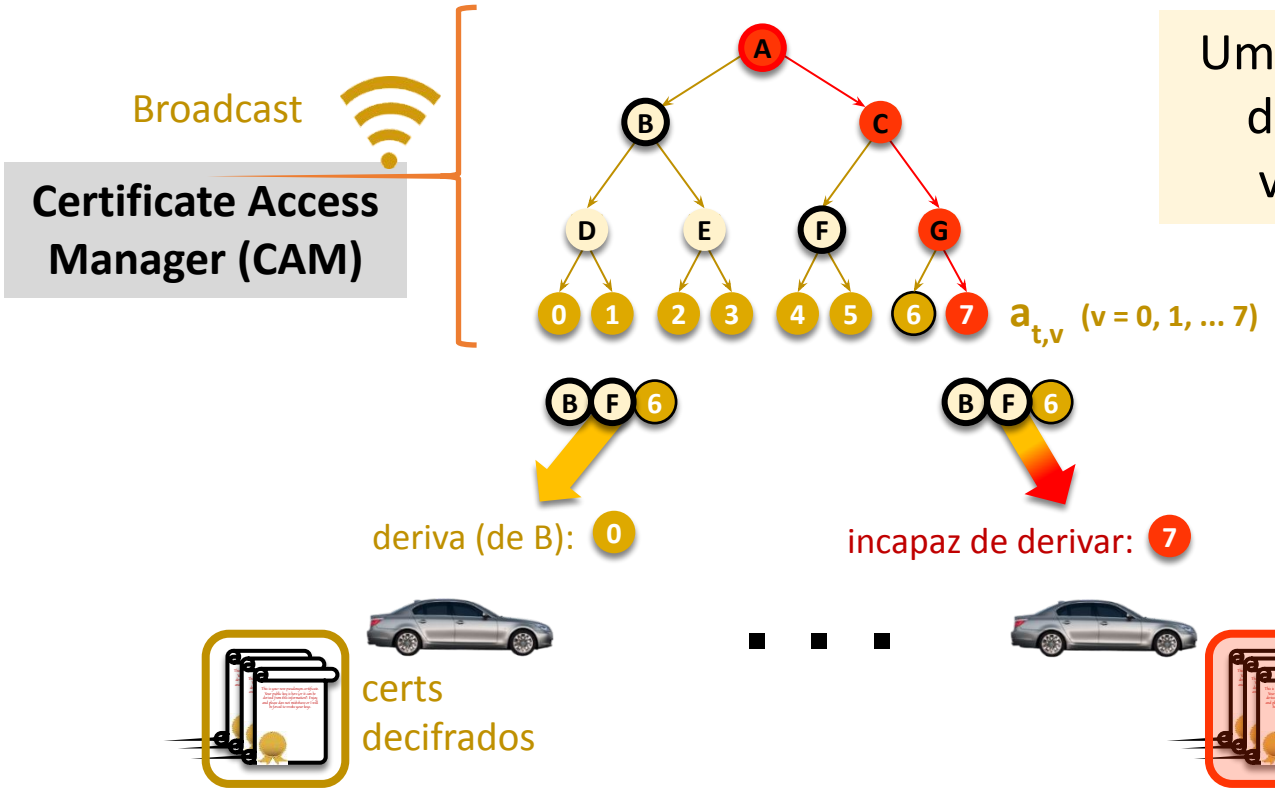


Uma árvore p/ cada período de ativação **t** ≥ prazo de validade do certificado

Ex. simplificado:
árvore para 8 veículos

Revogação via ACPC: operação

- Códigos de ativação ($a_{t,v}$): derivados de árvore de ativação
  - Revogação: broadcast não inclui ancestrais de nós revogados

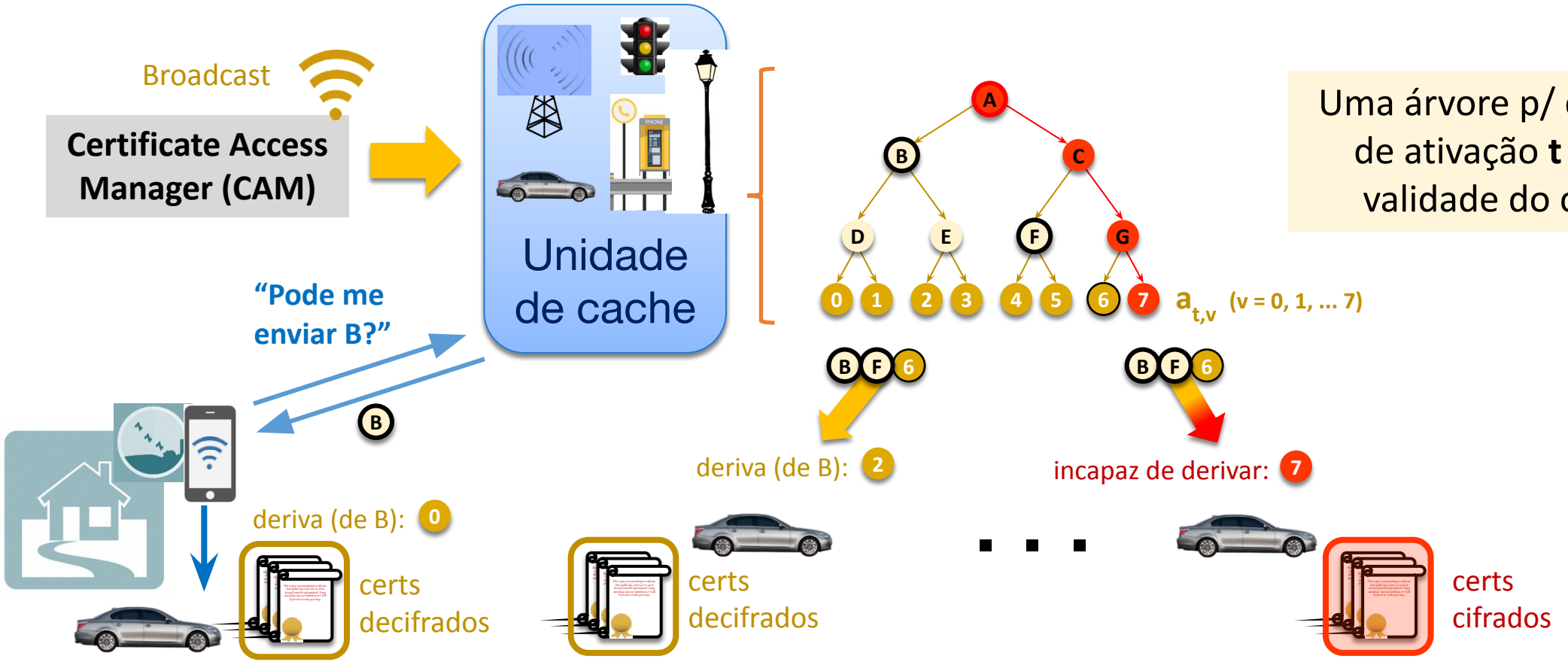


Uma árvore p/ cada período de ativação **t** ≥ prazo de validade do certificado

Ex. simplificado:
árvore para 8 veículos

Revogação via ACPC: operação

- Códigos de ativação ($a_{t,v}$): derivados de árvore de ativação
  - Distribuição também suporta **caching** e **unicast**, em adição a broadcast

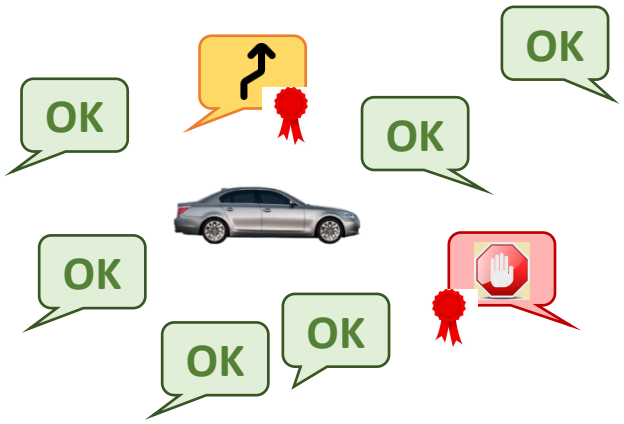


Operação: verificação de assinaturas

- Cada veículo envia **10 mensagens assinadas** por segundo
  - Cada veículo pode receber de **milhares de mensagens assinadas** por segundo!
  - **Custos de verificação** podem ser problemáticos: mensagens críticas (e.g., que podem evitar acidentes) devem ser **processadas em até 20 ms**

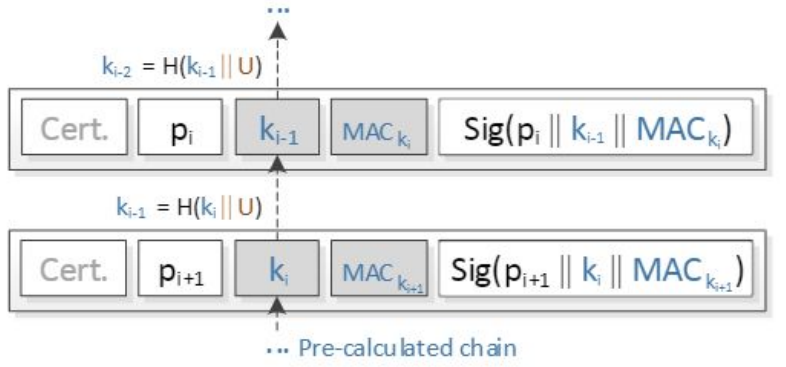
Operação: Verify-on-demand (VoD)

- Cada veículo envia **10 mensagens assinadas** por segundo
  - Cada veículo pode receber de **milhares de mensagens assinadas** por segundo!
  - **Custos de verificação** podem ser problemáticos: mensagens críticas (e.g., que podem evitar acidentes) devem ser **processadas em até 20 ms**
- Solução: **verify-on-demand**
  - Assinatura só é **verificada se mensagem leva a alguma ação**: assume-se autenticidade de mensagens “menos relevantes”



Operação: Verify-on-demand (VoD)

- Cada veículo envia **10 mensagens assinadas** por segundo
  - Cada veículo pode receber de **milhares de mensagens assinadas** por segundo!
  - **Custos de verificação** podem ser problemáticos: mensagens críticas (e.g., que podem evitar acidentes) devem ser **processadas em até 20 ms**
- Solução: **verify-on-demand**
  - Assinatura só é **verificada se requer alguma ação**: autenticidade de mensagens menos "relevantes" é ignorada
  - Pode exigir **verificação de um curto histórico**: e.g., predição de rota
    - **Verificação em batch**: ganhos de até 50%
    - **Encadeamento de mensagens** (TESLA): mensagens carregam MAC e a chave MAC do antecessor (verificação de N mensagens requer 1 assinatura + N-1 MACs)



Considerações finais

- V2X: diversos desafios de segurança e privacidade
  - **Emissão e revogação de certificados**
  - **Assinatura e verificação de mensagens**
  - Potencializados pela elevada **escala** e requisitos de **tempo real**
- Tema de pesquisa e padronização no mundo: IEEE/SCMS, ETSI/C-ITS
  - Ainda em desenvolvimento: contribuições são sempre possíveis!
- Testes sendo realizados no mundo: potencializado pelo 5G
  - Ex.: procure por “Cellular V2X” (C-V2X) no seu buscador favorito

Obrigado

Merci

THANK YOU

Danke

감사해요

Obrigado

Merci

THANK YOU

Danke

감사해요

Tempest

ACADEMY

Conference