О применении схемы ECQV для защиты интеллектуальных транспортных систем

Диана Кирюхина

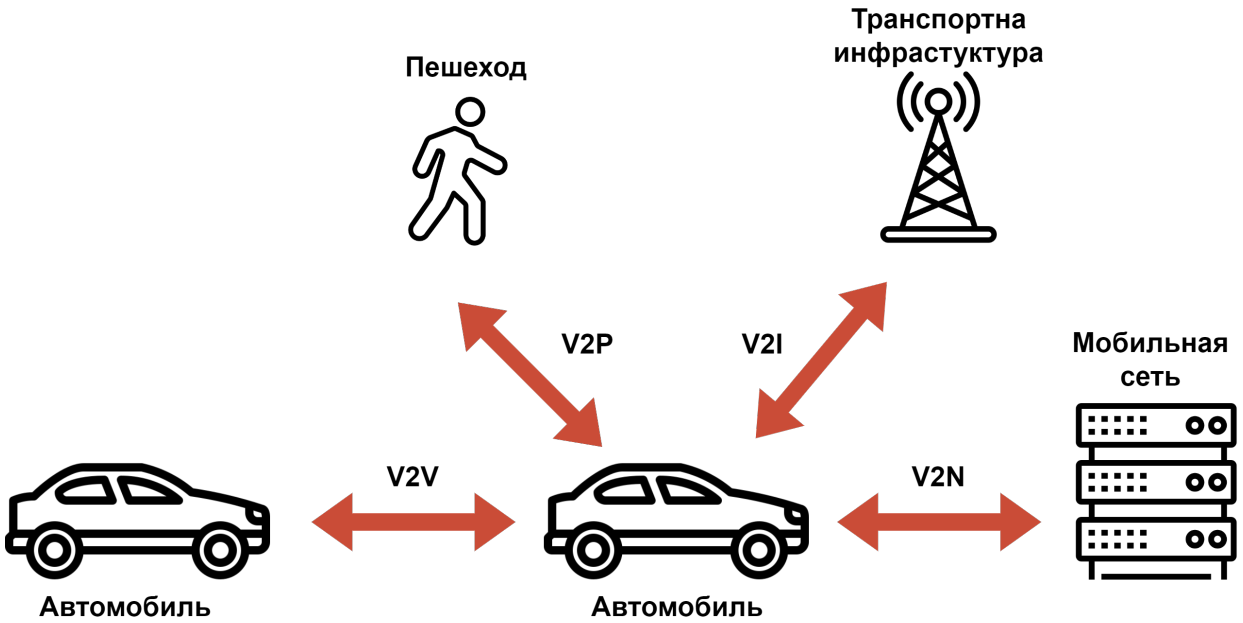
ООО «СФБ Лаб»

РусКрипто’2024
21 марта 2024

Diana.Kiryukhina@sfblaboratory.ru

Интеллектуальная транспортная система

Технология V2X



V2X (Vehicle-to-Everything) – технология связи, которая объединяет дорожную инфраструктуру, транспорт, участников движения в информационную систему.
Включает в себя: V2V, V2P, V2I, V2N

Где развивается V2X?

V2X в России

Идет активное развитие

- Ведется разработка бортовых устройств (БУ), базовых станций
- Проводятся тестовые запуски автомобилей с БУ
- Разрабатывается нормативная база (ГОСТ Р 70982-2023)

Защита данных в V2X

Защищенное взаимодействие в V2X

СФБ ЛАБ

- Передача открытых данных (местоположение, скорость, ...)
  ⇒ **нужна защита целостности**
- Передача чувствительных данных
  ⇒ **нужна защита конфиденциальности и целостности**
- Большое количество участников движения
  ⇒ **большой объем передаваемых данных**
- Быстрая смена положения участников движения
  ⇒ **нужна высокая пропускная способность**

Криптография в V2X

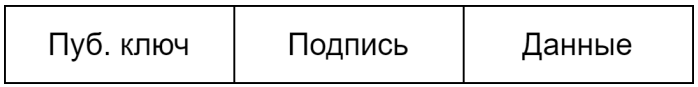
IEEE 1609.2-2022
Wireless Access in Vehicular Environments Security Services for Application and Management Messages

1. Схемы подписи сообщений (ECDSA)
2. Схемы с явными или неявными сертификатами (ECDSA или ECQV)
3. Асимметричное шифрование сообщений (ECIES)

Отличие явных от неявных сертификатов

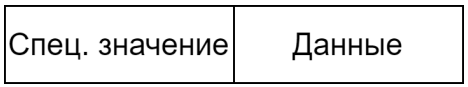
СФБ ЛАБ

Явный сертификат



Проверяющая сторона за счёт публичного ключа из сертификата и публичного ключа УЦ проверяет валидность сертификата.

Неявный сертификат



Проверяющая сторона за счёт публичного ключа УЦ восстанавливает публичный ключ сертификата из **спец. значения**.

Схемы с неявными сертификатами **НЕ** стандартизованы в России!

Сравнение битовых длин параметров

Схема	Подпись	Пуб. ключ	Итог
ГОСТ, ECDSA	$2\lambda = 512$	$\lambda \approx 256$	$3\lambda \approx 768$
Подпись Шнорра	$1.5\lambda = 384$	$\lambda \approx 256$	$2.5\lambda \approx 640$
ECQV (с подписью Шнорра)	$\lambda = 256$	0	$\lambda = 256$

Размер сертификата ECQV меньше в 3 раза!

Схема подписи неявных сертификатов ECQV

Схема ECQV

D. Brown, R. Gallant and S. Vanstone

Provably secure implicit certificate schemes

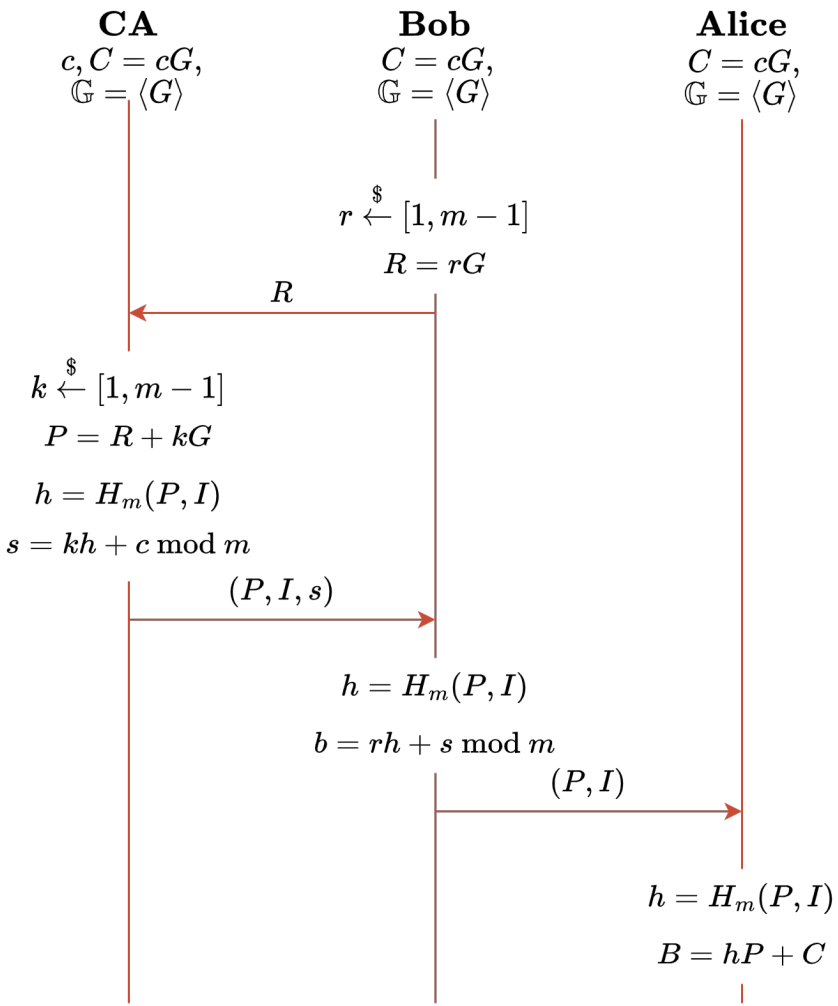
2001

SEC 4

Elliptic Curve Qu-Vanstone Implicit Certificate Scheme (ECQV)

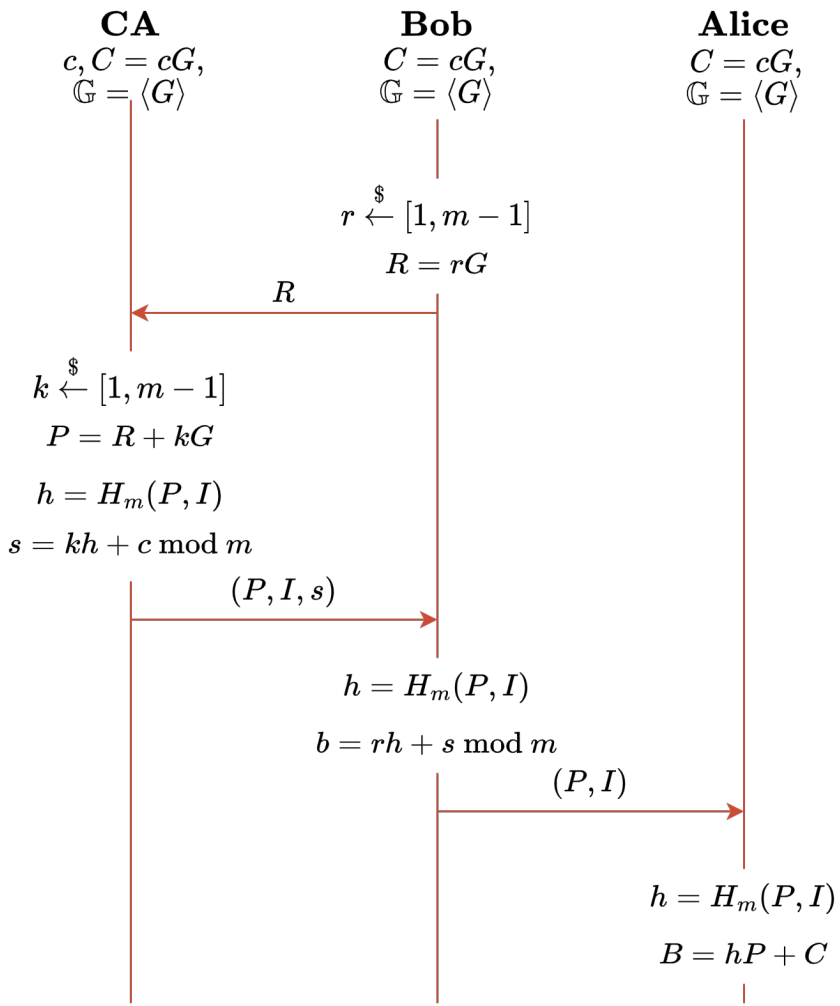
2013

Схема ECQV



- (P, I) – сертификат:
  - P – спец. значение
  - I – метаданные
- B, b – публ. и секр. ключи Боба
- C, c – публ. и секр. ключи УЦ
- $H_m(.)$ – хэш-функция, принимает блок байтов, выдает значение из $[0, m-1]$

ECQV с отечественными криптоалгоритмами



- $H_m(.)$ – хэш-функция «Стрибог» с взятием выхода по модулю m
- Эллиптические кривые согласно ГОСТ 34.10-2018 и Р 1323565.1.024-2019

Доказательство стойкости ECQV

Доказательство стойкости ECQV

В [BGV01] получены *асимптотические* оценки.
Для практики важны «конкретные» [Bel98]
– зависимость вероятности успеха противника от его ресурсов.


[BGV01] D. Brown, R. Gallant and S. Vanstone
Provably secure implicit certificate schemes
2001


[Bel98] M. Bellare
Practice-Oriented Provable-Security
1998

Требования к схеме

Нарушитель НЕ может:

1. изготовить валидный сертификат без участия УЦ (модели EF-ICS, EF-mICS)
2. восстановить секретный ключ валидного сертификата (модели KRC-ICS, KRC-mICS)

Подделка сертификата

СФБ ЛАБ

Модель EF-ICS

- Нарушитель A:
  - на вход получает публичный ключ $\mathbf{CA}$
  - может взаимодействовать с оракулами $\mathbf{CA}$ и $\mathbf{H}$
- Задача: выдать поддельный валидный сертификат и секретный ключ от него

Ресурсами A являются:

- $q_{\mathbf{CA}}$ – количество запросов к $\mathbf{CA}$
- $q_{\mathbf{H}}$ – количество запросов к $\mathbf{H}$
- t – время работы (число операций)

Восстановление ключа сертификата

СФБ ЛАБ

Модель KRC-ICS

- Нарушитель A:
  - на вход получает публичный ключ $\mathbf{CA}$
  - может взаимодействовать с оракулами $\mathbf{CA}$, $\mathbf{Bob}$
- Задача: выдать секретный ключ к действующему сертификату

Ресурсами A являются:

- $q_{\mathbf{CA}}$ – количество запросов к $\mathbf{CA}$
- $q_{\mathbf{Bob}}$ – количество запросов к $\mathbf{Bob}$
- t – время работы (число операций)

Многопользовательские модели

По аналогии с EF-ICS и KRC-ICS определяются **многопользовательские** (**m**ulti-user) модели EF-**m**ICS и KRC-**m**ICS.

Противник взаимодействует со многими УЦ и многими пользователями.

Используемые предположения

Для моделей KRC-ICS и KRC-mICS (определение ключа):

- Вычислительная сложность дискретного логарифмирования

Используемые предположения

Для моделей KRC-ICS и KRC-mICS (определение ключа):

- Вычислительная сложность дискретного логарифмирования

Для моделей EF-ICS и EF-mICS (подделка):

- Вычислительная сложность дискретного логарифмирования
- Хэш-функция – случайный оракул

Основа доказательства

D. Brown, R. Gallant and S. Vanstone

Provably secure implicit certificate schemes

2001

M. Bellare, G. Neven

New Multi-Signature Schemes and a General Forking Lemma

2005

Стойкость ECQV в EF-mICS

Теорема

Вероятность успешной подделки ограничена

$$\mathrm{Adv}^{\text{EF-mICS}}_{\text{ECQV}}(t, q_{\mathbf{CA}}, q_{\mathbf{H}}) \leq d \cdot \sqrt{\left(\mathrm{Adv}^{\mathrm{DL}}_{\mathbb{G}}(t') + \frac{2q_{\mathbf{CA}}}{m} + \frac{1}{m}\right) \cdot \left(q_{\mathbf{H}} + q_{\mathbf{CA}} + 1\right)},$$

где

- $t' \approx t$ – вычислительные ресурсы противника,
- $q_{\mathbf{CA}}$ – число запросов к различным УЦ,
- $q_{\mathbf{H}}$ – число запросов к $\mathbf{H}$ (на практике, $q_{\mathbf{H}} \approx t$),
- d – число УЦ,
- m – порядок группы $\mathbb{G}$,
- $\mathrm{Adv}^{\mathrm{DL}}_{\mathbb{G}}$ – вероятность успешного решения задачи дискретного логарифмирования.

Стойкость ECQV в KRC-mICS

Теорема

Вероятность восстановления секретного ключа действующего сертификата

$$\mathrm{Adv}_{\mathrm{ECQV}}^{\text{KRC-mICS}}(t, q_{\mathbf{CA}}, q_{\mathbf{Bob}}) \leq \mathrm{Adv}_{\mathbb{G}}^{\mathrm{DL}}(t') + \frac{1}{m-1},$$

где

- $t' \approx t$ – вычислительные ресурсы противника,
- m – порядок группы $\mathbb{G}$,
- $\mathrm{Adv}_{\mathbb{G}}^{\mathrm{DL}}$ – вероятность успешного решения задачи дискретного логарифмирования.

Вероятность успеха противника в модели KRC-mICS **НЕ увеличивается** с ростом числа пользователей!

Атаки на ECQV

Атака в модели EF-mICS

Строим поддельный сертификат за счёт нахождения **второго прообраза** хэш-функции.

Нарушитель знает сертификат (P, I) и ключ b.
Подбирает P', I', при которых $H(P', I') = H(P, I)$.
Предъявляет подделку (P', I') и знает её ключ b.

Вероятность успеха

$$p_{\mathrm{SP}} \approx \frac{t}{m},$$

t – вычислительные ресурсы противника,
m – порядок группы, $m \approx 2^{256}$.

Метод ρ-Полларда

Вычисляем секретный ключ сертификата или формируем подделку за счёт решения задачи дискретного логарифмирования.

Вероятность успеха

$$p_\rho \approx \frac{t^2}{2m},$$

t – вычислительные ресурсы противника,
m – порядок группы.

Сравнение оценок

В моделях KRC-ICS и KRC-mICS (определение ключа сертификата) оценки **точные**.

В моделях EF-ICS и EF-mICS (подделка сертификата) оценки далеки от точных, как и для большинства схем, доказательство которых основано на «Лемме о разветвлении» (Forking Lemma).

Заключение

1. Схемы с неявными сертификатами (в т.ч. ECQV) позволяют сократить объём передаваемых данных в 3 раза , что важно для V2X

Заключение

1. Схемы с неявными сертификатами (в т.ч. ECQV) позволяют сократить объём передаваемых данных в 3 раза , что важно для V2X
2. Возможно применение ECQV с отечественными криптомеханизмами

Заключение

1. Схемы с неявными сертификатами (в т.ч. ECQV) позволяют сократить объём передаваемых данных в 3 раза , что важно для V2X
2. Возможно применение ECQV с отечественными криптомеханизмами
3. Для ECQV получены «конкретные» оценки стойкости (вместо асимптотических), а также рассмотрены конструктивные методы анализа

Благодарю за внимание!

Диана Кирюхина

ООО «СФБ Лаб»

РусКрипто’2024

21 марта 2024

Diana.Kiryukhina@sfblaboratory.ru