Перспективные механизмы цифровой подписи в России и мире

Антон Гуселев

Технический комитет по стандартизации
«Криптографическая защита информации»
— (ТК 026) —

– PKI-Форум Россия 2019 –

ГОСТ Р 34.10-2012

На территории Российской Федерации действует 1* стандарт, определяющий процедуры формирования и проверки цифровой подписи.

- вариант обобщенной схемы Эль-Гамаля
- основа стойкости – трудная разрешимость задачи дискретного логарифмирования в группе точек эллиптической кривой (а также трудоемкость поиска коллизии и второго прообраза для функции хэширования определяемой ГОСТ Р 34.11-2012)

Международный стандарт

ISO/IEC 14888-3 (EC-RDSA) + ISO/IEC 10118-3 (Streebog)

Область применения схемы подписи обширна, уровень ее стойкости высок, однако... есть к чему стремится

** **На самом деле их 2***

Межгосударственный стандарт ГОСТ 34.10-2018, определяет аналогичный механизм

Что уже сделано

Первоочередная задача:

Увеличить скорость реализации процедур формирования и проверки подписи

✓ Рекомендации по стандартизации Р 50.1.114-2016

Использование кривых в скрученной форме Эдвардса = увеличение скорости

(Некоторые) направления развития

Узкоспециализированные практические области, *где удобней применять «альтернативные» варианты схем подписи*

- Формирования ключей «в обратную сторону»
  (ключ подписи формировать на основе ключа проверки)
- Обеспечение анонимности субъекта, при сохранении доверия к сформированной подписи
  (криптовалюты? – а куда же без них)
- Уменьшение длин параметров при сохранении уровня стойкости
  (технические ограничения)

Шаг за шагом: Формирование ключей «в обратную сторон»

Что это дает?

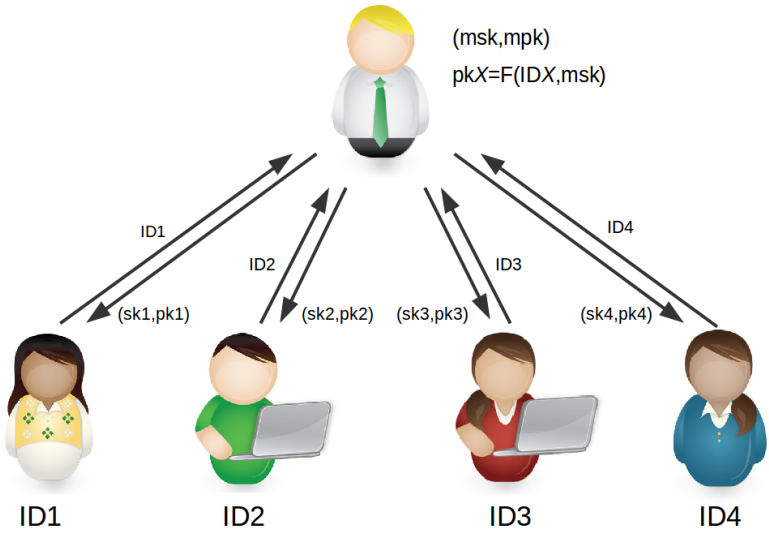
В качестве ключа проверки подписи можно использовать осмысленную (а не случайную) информацию

В 1984 году А. Шамир предложил использовать личностную информацию (ФИО, email, телефон) в качестве ключа проверки подписи $\Longrightarrow$
$\Longrightarrow$ **личностная криптография (подпись)**

Сегодня область можно значительно расширить:
ключи проверки = серийные номера датчиков, сенсоров и т.п. $\Longrightarrow$

~~**Личностная**~~ **криптография (подпись), основанная на использовании идентификаторов**

Формирование ключей «в обратную сторон»
Идея



Формирование ключей «в обратную сторон»
Как реализовать?

- Использовать схему RSA
  - – *Не подходит для практического применения*
- Использовать схему Шнорра
  - – *Размер подписи*
  - \+ *Эффективная реализация*
- Использовать билинейные отображения
  (спаривания точек эллиптической кривой)
  - – Раньше были проблемы...
    спаривались только точки суперсингулярной (не очень хорошей) кривой
  - \+ Теперь проблем меньше...
    кривых подходящих для реализации спариваний больше
    (ISO/IEC 15946-5 – Cryptographic techniques based on elliptic curves – Elliptic curve generation,
    IETF Pairing-Friendly Curves draft-yonezawa-pairing-friendly-curves-00)
  - \+ *Размер подписи*

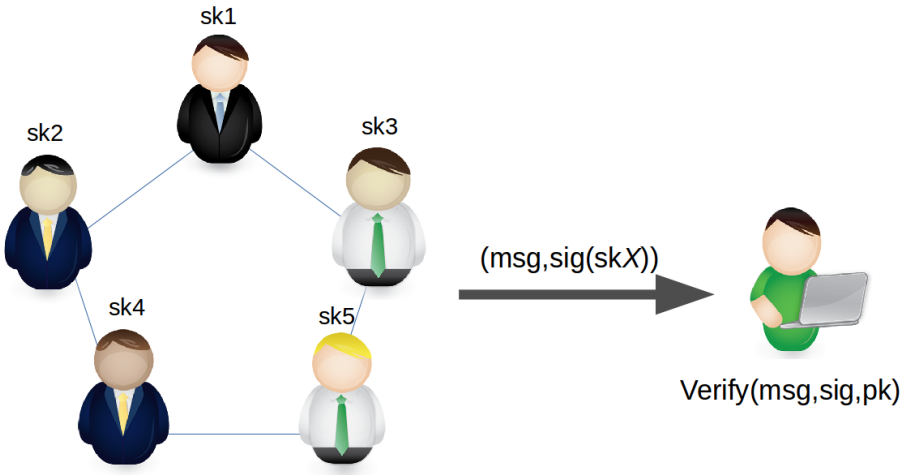
На основе билинейных отображений

- ISO/IEC 14888-3: Digital signatures with appendix – Discrete logarithm based mechanisms
- IETF RFC 7859 Identity-Based Signatures for Mobile Ad Hoc Network (MANET) Routing Protocols

На основе схемы Шнорра

- ISO/IEC 29192-4: – Lightweight cryptography – Mechanisms using asymmetric techniques

Шаг за шагом:
Обеспечение анонимности
Идея



Шаг за шагом: Обеспечение анонимности Реализация

Вопрос:

Можно ли узнать, кто автор подписи?

- Групповые подписи – да, но нужно позвать доверенное лицо
- Кольцевые подписи – нет, автор всегда неизвестен

Что лежит в основе?

Не совсем классические принципы: RSA, дискретное логарифмирование, билинейные отображения

Стандартизация:
ISO/IEC 20008-2 – Anonymous digital signatures – Mechanisms using a group public key

Шаг за шагом: Уменьшение длины (подписи)

Используем:

- Схему Шнорра (меньше Эль-Гамаля на 25%)
- билинейные отображения (меньше Эль-Гамаля на 50%)

Стандартизация (билинейные отображения):
IETF BLS Signature Scheme draft-boneh-bls-signature-00

!!! Появление квантового вычислителя поставит под угрозу большинство существующих криптографических механизмов !!!

Самые ожидаемые бои XXI века:

Гровер and Саймон vs симметричная криптография

Шор vs асимметричная криптография

1997 год	П. Шор – квантовые алгоритмы факторизации и дискретного логарифмирования в мультипликативной группе
2003 год	Варианты алгоритма Шора для решения задачи дискретного логарифмирования в группе точек эллиптической кривой

Как же победить?

Разработать новые механизмы стойкие к новым атакам
(или вспомнить старые)

(**постквантовая криптография**) = (использовать задачи «неразрешимые» как с использованием квантового вычислителя, так и классических методов)

Наиболее перспективными считаются задачи:

- теории решеток
- теории кодирования
- теории многочленов от многих переменных
- теории изогений эллиптических кривых

  и ...
- *инвертирования однонаправленной функции*

Все математические задачи достаточно хорошо изучены и почти все имеют долгую (не совсем успешную[†] и поэтому угасающую) криптографическую историю.

Угроза применения квантового вычислителя раздула угасающее пламя...

Однако сомнения остались:

NIST решил провести конкурс по выбору постквантовых криптографических механизмов. Стойкость почти всех конкурсантов основана трудноразрешимых задачах

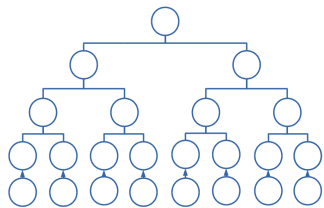
... ждем результатов

[†]По разными причинам: эффективные методы криптоанализа, слишком длинные параметры

... а как же задача инвертирования однонаправленной функции.

Утверждены 2 отраслевые рекомендации IETF со схемами постквантовой подписи на основе итеративного применения функции хэширования.

- RFC 8391 – XMSS: eXtended Merkle Signature Scheme
- RFC 8554 – Leighton-Micali Hash-Based Signatures



Схемы две, а базовый принцип один

СПАСИБО ЗА ВНИМАНИЕ!

Вопросы?