# Механизмы электронной цифровой подписи: адаптация к решению актуальных задач

*Антон Гуселев и Александр Бондаренко*

Академия криптографии Российской Федерации

– PKI-Форум Россия 2021 –

# Содержание

# Схема цифровой подписи: механизм контроля целостности и подтверждения авторства

## Основные подходы:

- схема Эль-Гамаля, предложена в 1985 году
- схема Шнорра, предложена в 1990 году

## Основа стойкости:

трудная разрешимость задачи дискретного логарифмирования

## Универсальность с точки зрения выбора:

- математической структуры
- сжимающего отображения

$\Rightarrow$ «безболезненная» адаптация к противодействию новым методам анализа

## Другие схемы цифровой подписи

- RSA
  *(задача факторизации)*
- BLS
  *(задача дискретного логарифмирования в двух математических структурах)*

## Важно

правильно выбрать/построить

- простые числа (RSA)
- билинейные отображения (BLS)

# Схема Эль-Гамаля

## Национальный стандарт Российской Федерации ГОСТ Р 34.10-2012

определяет вариант схемы Эль-Гамаля, реализуемый совместно с функциями хэширования, определенными ГОСТ Р 34.11-2012.

## Национальная* стандартизация, история «адаптации»:

ГОСТ Р 34.10-94 $\xrightarrow[\text{мат. структуры}]{\text{замена}}$ ГОСТ Р 34.10-2001 $\xrightarrow[\text{хэш-функции}]{\text{замена}}$ ГОСТ Р 34.10-2012

* межгосударственная

## В международном стандарте ISO/IEC 14888-3 определены:

- (EC-)DSA – (Elliptic Curve) Digital Signature Algorithm (США)
- (EC-)KCDSA –(Elliptic Curve) Korean Certificate-based Digital Signature Algorithm
- EC-GDSA – Elliptic Curve German Digital Signature Algorithm
- EC-RDSA – Elliptic Curve Russian Digital Signature Algorithm (описана схема по ГОСТ Р 34.10-2001, который выведен из действия)*
- SM2 (Китай)

$$* \begin{cases} \text{уравнения в ГОСТ Р 34.10-2001} = \text{ГОСТ Р 34.10-2012} \\ \text{х-ф по ГОСТ Р 34.11-2012 в ISO/IEC 10118-3} \end{cases} \Rightarrow \begin{cases} \text{ГОСТ} \\ \text{в ISO/IEC} \end{cases}$$

## В международном стандарте ISO/IEC 14888-3 определены:

- (EC-)SDSA – (Elliptic Curve) Schnorr Digital Signature Algorithm
- EC-FSDSA – Elliptic Curve Full Schnorr Digital Signature Algorithm

## Национальная стандартизация

Варианты схемы Шнорра определены в национальных стандартах

- Белоруссии
- Украины
- Узбекистана
- США

## Рекомендации IETF

Описана схема EdDSA (Edwards-curve Digital Signature Algorithm)

# Новые задачи

**Задача:**

скрыть личность подписанта, но сохранить возможность верифицировать подпись

**Механизм:**

схемы групповой цифровой подписи

**Основа:**

—

**Механизм:**

схемы кольцевой цифровой подписи

**Основа:**

схема Шнорра

# Новые задачи

**Задача:**

скрыть личность подписанта, но сохранить возможность верифицировать подпись

**Механизм:**

схемы групповой цифровой подписи

**Основа:**

—

**Механизм:**

схемы кольцевой цифровой подписи

**Основа:**

схема Шнорра

# Новые задачи

**Задача:**

скрыть личность подписанта, но сохранить возможность верифицировать подпись

**Механизм:**

схемы групповой цифровой подписи

**Основа:**

—

**Механизм:**

схемы кольцевой цифровой подписи

**Основа:**

схема Шнорра

# Новые задачи

**Задача:**

скрыть содержание подписываемого сообщения от того, кто его подписывает

**Механизм:**

схемы цифровой подписи вслепую

**Основа:**

схемы Эль-Гамаля и Шнорра

# Новые задачи

**Задача:**

скрыть содержание подписываемого сообщения от того, кто его подписывает

**Механизм:**

схемы цифровой подписи вслепую

**Основа:**

схемы Эль-Гамаля и Шнорра

# Новые задачи

**Задача:**

сократить размер хранимых данных за счет «удаления» цифровых подписей

**Механизм:**

схемы агрегируемых цифровых подписей

**Основа:**

схема Шнорра

# Новые задачи

**Задача:**

сократить размер хранимых данных за счет «удаления» цифровых подписей

**Механизм:**

схемы агрегируемых цифровых подписей

**Основа:**

схема Шнорра

# Новые задачи

**Задача:**

сократить размер цифровой подписи, при сохранении «уровня стойкости»

**Механизм:**

схемы «короткой» цифровой подписи

**Основа:**

схемы Эль-Гамаля и Шнорра

# Новые задачи

**Задача:**

сократить размер цифровой подписи, при сохранении «уровня стойкости»

**Механизм:**

схемы «короткой» цифровой подписи

**Основа:**

схемы Эль-Гамаля и Шнорра

# Новые задачи

**Задача:**

обеспечить доверие к группе, при условии отсутствия доверия к одному

**Механизм:**

схемы мультиподписи

**Основа:**

схема Шнорра

**Механизм:**

пороговые схемы цифровой подписи

**Основа:**

схемы Эль-Гамаля и Шнорра

# Новые задачи

**Задача:**

обеспечить доверие к группе, при условии отсутствия доверия к одному

**Механизм:**

схемы мультиподписи

**Основа:**

схема Шнорра

**Механизм:**

пороговые схемы цифровой подписи

**Основа:**

схемы Эль-Гамаля и Шнорра

# Новые задачи

**Задача:**

обеспечить доверие к группе, при условии отсутствия доверия к одному

**Механизм:**

схемы мультиподписи

**Основа:**

схема Шнорра

**Механизм:**

пороговые схемы цифровой подписи

**Основа:**

схемы Эль-Гамаля и Шнорра

# Новые задачи

**Задача:**

использовать предварительно распределенные данные в качестве ключа проверки подписи

**Механизм:**

схемы цифровой подписи, допускающие возможность формирования ключа подписи на основе ключа проверки подписи (личностные цифровые подписи)

**Основа:**

схема Шнорра

# Новые задачи

**Задача:**

использовать предварительно распределенные данные в качестве ключа проверки подписи

**Механизм:**

схемы цифровой подписи, допускающие возможность формирования ключа подписи на основе ключа проверки подписи (личностные цифровые подписи)

**Основа:**

схема Шнорра

# Новые задачи

**Задача:**

определить права на выполнение операций

**Механизм:**

схемы атрибутных цифровых подписей

**Основа:**

—

# Новые задачи

**Задача:**

определить права на выполнение операций

**Механизм:**

схемы атрибутных цифровых подписей

**Основа:**

—

# Новые задачи

**Задача:**

отредактировать подписанное сообщение

**Механизм:**

схемы редактируемых цифровых подписей

**Основа:**

—

# Новые задачи

**Задача:**

отредактировать подписанное сообщение

**Механизм:**

схемы редактируемых цифровых подписей

**Основа:**

—

# Новые задачи

**Задача:**

недопустить возможность передачи подписанного сообщения третьей стороне

**Механизм:**

схемы цифровой подписи «хамелеон»

**Основа:**

—

# Новые задачи

**Задача:**

недопустить возможность передачи подписанного сообщения третьей стороне

**Механизм:**

схемы цифровой подписи «хамелеон»

**Основа:**

—

# Новые задачи: определение подхода к решению

- существуют различные синтезные подходы, которые могут опираться на стойкие базовые структурные элементы
- стойкий базовый структурный элемент не всегда позволяет создать стойкий механизм
- необходимо проведение всесторонних криптографических исследований, учитывающих характерные особенности «новых задач» и подходов к их решению

## Проведение исследований

Академия криптографии Российской Федерации проводит исследования по определению перспективных подходов к синтезу криптографических механизмов, в том числе подходящих для решения «новых задач»