конференция РусКрипто

Ежегодная международная научно-практическая конференция

«РусКрипто'2022»

Что подписано ключом, то не вырубишь...

10 лет действующим национальным стандартам электронной подписи и хэш-функции

С.В. Гребнев QApp
Г.Б. Маршалко ФСБ России
Д.В. Матюхин ФСБ России
В.И. Рудской ТК 26
В.А. Шишкин Криптонит

У криптографов юбилей каждый год

- Приказами Федерального агентства по техническому регулированию и метрологии от 7 августа 2012 г. №№ 215-ст, 216-ст утверждены национальные стандарты ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» и ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования» с датой введения в действие 1 января 2013 г.
- Стандарты разработаны Центром защиты информации и специальной связи ФСБ России с участием ОАО «ИнфоТеКС»
- ГОСТ Р 34.10-2012 отличается от ГОСТ Р 34.10-2001 дополнительным вариантом выбора параметров и использованием хэш-функций по ГОСТ Р 34.11-2012 вместо ГОСТ Р 34.11-94
- Функции хэширования, впоследствии ставшие ГОСТ Р 34.11-2012, впервые представлены широкой общественности на РусКрипто’2010

Схема подписи ГОСТ Р 34.10-2012

- ГОСТ Р 34.10-94, 2001, 2012 определяют *один и тот же* вариант *обобщённой схемы Эль-Гамаля:*
  - Параметры: q – простое, $G = \langle P \rangle_q, R: G \setminus \{e\} \to \{0, \dots, q-1\}$, хэш-функция h
  - Выработка ключей: $d \in_R \{1, \dots, q-1\}$ – ключ подписи (секретный), $Q = dP$ – ключ проверки подписи (открытый)
  - Выработка подписи сообщения M: $k \in_R \{1, \dots, q-1\}, r = R(kP), s = rd + kh(M) \bmod q$, подпись – (r, s)
  - Проверка подписи сообщения M: подпись принимается $\Leftrightarrow R\big((sh(M)^{-1} \bmod q)P - (rh(M)^{-1} \bmod q)Q\big) = r$

ГОСТ Р 34.10-	94	2001	2012
q, битов	255-256		255-256, 509-512
G	подгруппа $GF(p)^*$, p – простое 510-512 или 1021-1024 бита	подгруппа $E\big(GF(p)\big) = \{y^2 = x^3 + ax + b\} \cup \{O\}$, p – простое, $p^t \not\equiv 1 \bmod q, t = 1, \dots, B$, $\#E\big(GF(p)\big) \neq p, a \neq 0, b \neq 0$	
B	–	31	31, 131
R	$\bmod q$	x-координата точки кривой $\bmod q$	
h	ГОСТ Р 34.11-94		ГОСТ Р 34.11-2012

ГОСТ Р 34.10-2012: криптоанализ

- Теоретическое обоснование в модели с защищенным модулем (Варновский, 2008)
- Анализ безопасности конкретных вариантов кривых, используемых в документах по стандартизации (Алексеев и др., 2018)
- Общие методы криптоанализа: параллельный метод поиск коллизий (van Oorschot, Wiener, 1994) - выбранные размеры параметров не позволяют говорить о возможности применения метода в обозримое время

ГОСТ Р 34.10-2012: реализация (теория)

- Оптимизация реализации умножения алгоритмическими методами (Гребнев, Дыгин 2013; Гребнев, 2016)
- Оптимизация реализации через представление в виде скрученной кривой в форме Эдвардса (Алексеев и др., 2014)
- Оптимизация программной реализации (Бородин, Рыбкин, 2014)
- Оптимизация аппаратной реализации (Родионов, 2014)

ГОСТ Р 34.10-2012: реализация (практика)

Базовые механизмы

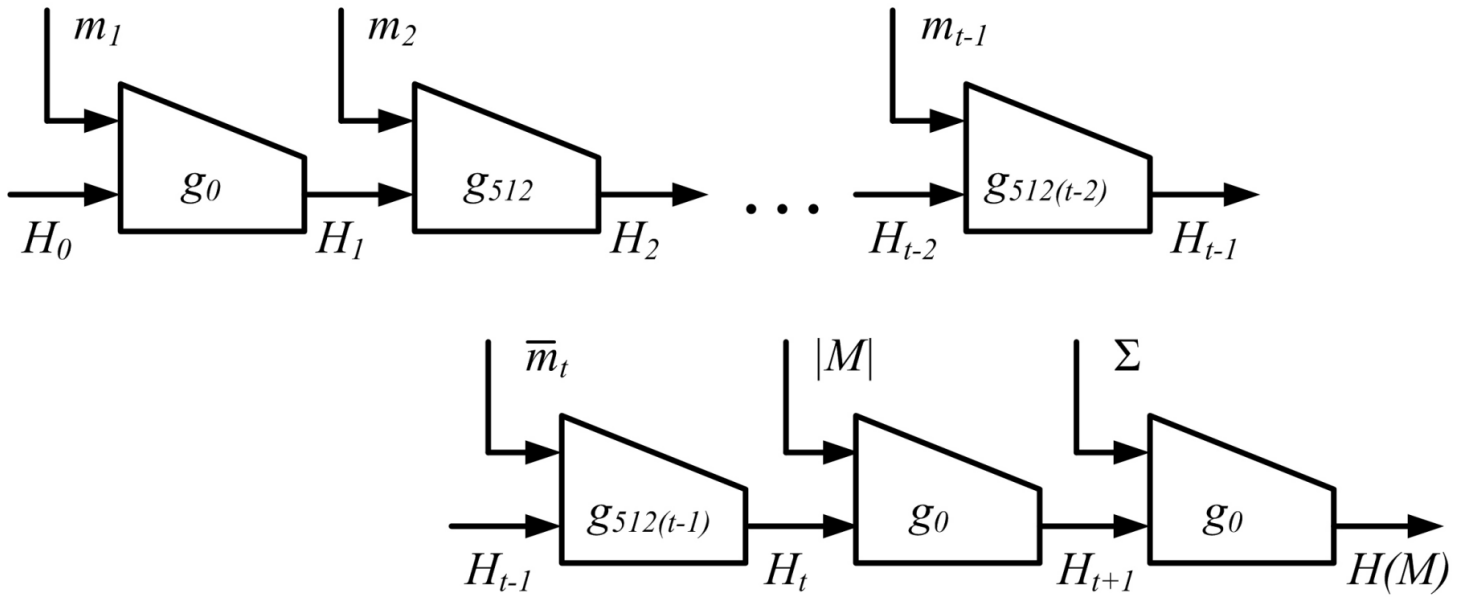
Р 1323565.1.020-2020 (TLS 1.2)
Р 1323565.1.024-2018 (Параметры ЭК)
Р 1323565.1.033-2020 (XML)
Р 1323565.1.025-2019 (CMS)
Р 50.1.115-2016 (Общий ключ из пароля)
Р 50.1.113-2016 (Сопутствующие алгоритмы)
Р 1323565.1.025-2019 (Выработка общего ключа)
Р 1323565.1.023-2018 (X.509)
Р 1323565.1.030-2020 (TLS 1.3)
Р 50.1.110-2016 (PKCS# 15)

Прикладные механизмы

Р 1323565.1.016-2018 (оффлайновая аутентификация)
Р 1323565.1.015-2017 (EMV-сертификаты)
Р 50.1.112-2016 (Транспортный контейнер PKCS#8, PKCS #12)
Р 1323565.1.018-2018 (Контрольно-измерительные устройства)
Р 1323565.1.013-2017 (SPC-F2)
Р 1323565.1.028-2019 (Контрольно измерительные устройства)

ГОСТ Р 34.11-2012: хэш-функции «Стрибог»

- Конструкция Меркля-Дамгорда с "подхэшированием" длины и суммы блоков сообщения
- Функция сжатия на основе конструкции Миягучи-Принеля, зависящая от номера блока
- Базовый XSL-шифр с длиной блока 512 бит (12.5 итераций)
- Длина хэш-кода 256 или 512 бит



Общий вид

ГОСТ Р 34.11-2012: криптоанализ

- Более **20** работ в рецензируемых изданиях (конструкция в целом, функция сжатия, структурные элементы, реализации)
- **Нет результатов, свидетельствующих о невыполнении изначально предъявленных разработчиками требований к стойкости**
- Открытый конкурс работ по исследованию хэш-функции (2014-2015, streebog.info)
- Наилучший результат — алгоритм построения второго прообраза хэш-функции «Стрибог-512» для сообщения длины 2^x блоков, $0 < x < 179$, с трудоёмкостью $x2^{513-x}$ вызовов функции сжатия (Guo et al., 2014, первая премия конкурса)
- Седов, 2015: доказательство стойкости к построению коллизии и прообраза в модели идеального шифра (вторая премия конкурса)
- Наибольшее известное число раундов блочного шифра, при котором трудоёмкость построения коллизии функции сжатия меньше универсальной оценки – 9.5 (Wang et al., 2013)

ГОСТ Р 34.11-2012: реализация (теория)

- Широкий спектр работ по оптимизации программных реализаций (Бородин, Рыбкин, 2014; Казимиров, Смышляев, 2013; Лебедев, 2012)
- Компактное представление структурных элементов (Бирюков и др., 2016)

ГОСТ Р 34.11-2012: реализация (практика)

Базовые механизмы

Р 1323565.1.006-2017 (PRF)
Р 1323565.1.020-2020 (TLS 1.2)
Р 1323565.1.033-2020 (XML)
Р 1323565.1.025-2019 (CMS)
Р 1323565.1.022-2018 (KDF)
Р 50.1.115-2016 (Общий ключ из пароля)
Р 50.1.113-2016 (Сопутствующие алгоритмы)
Р 1323565.1.035-2020 (ESP)
Р 1323565.1.023-2018 (X.509)
Р 1323565.1.030-2020 (TLS 1.3)

Прикладные механизмы

Р 1323565.1.016-2018 (оффлайновая аутентификация)
Р 1323565.1.019-2018 (контрольно-кассовая техника)
Р 1323565.1.011-2017 (оффлайновая проверка PIN)
Р 1323565.1.003-2017 (S3G)
Р 1323565.1.028-2019 (Контрольно измерительные устройства)

ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012 на международном уровне

- ГОСТ Р 34.10-2012:
  - международный стандарт ISO/IEC 14888-3:2018 (схема подписи EC-RDSA)
  - межгосударственный стандарт ГОСТ 34.10-2018
  - IETF RFC 7091
- ГОСТ Р 34.11-2012:
  - международный стандарт ISO/IEC 10118-3:2018 (хэш-функции STREEBOG-512, STREEBOG-256)
  - межгосударственный стандарт ГОСТ 34.11-2018
  - RFC IETF 6986
- Рекомендация Коллегии Евразийской экономической комиссии от 12.03.2019 N 9 «О перечне стандартов и рекомендаций в области информационной безопасности, применяемых в рамках реализации цифровой повестки Евразийского экономического союза»

ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012 и квантовые компьютеры

- ГОСТ Р 34.10-2012:
  - Алгоритм Шора в теории: $O(\log N)$ кубитов и $O(\log^3 N)$ групповых операций
  - Для DLOG в подгруппе $E(GF(p))$ (Roeteller et al.,2017, Haner et al. 2020) :
    - для q длины 256 бит ~2500 кубитов и $\sim 2^{34}$ гейтов
    - для q длины 512 бит ~5000 кубитов и $\sim 2^{37}$ гейтов
  - Реализация на практике с учетом шумов - несколько миллионов кубит
- ГОСТ Р 34.11-2012:
  - Вычислительная сложность поиска коллизии – BHT-алгоритм (Brassrad, Hoyer, Tapp) $- O\left(2^{\frac{n}{3}}\right)$ вызовов функции
  - $\sim 2^{86}$ и $\sim 2^{171}$ вызовов хэш-функции, количество гейтов зависит от сложности реализации хэш-функции
  - Количество кубит: для сообщения M требуется |M|+1536 кубит (Денисенко, Рудской, РусКрипто'2022)

Есть ли подпись после подписи?

Отдельные области применения требуют наличия схем подписи, обладающих специфическими свойствами

- Подпись вслепую для протоколов электронного голосования (Алексеев и др, завтра с утра)
- Короткая подпись для маркировки групп товаров (Гуселев, тогда же)
- Постквантовые схемы подписи
  - Рабочая группа ТК 26 «Постквантовые криптографические механизмы»
  - Подпись, основанная на функции хэширования (Гуселев, 2019; Булычев и др., 2020)