



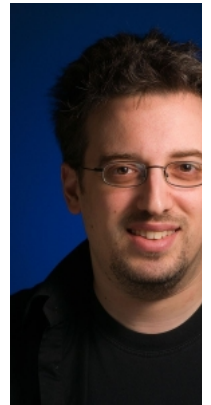
Scratch 15 января 2015 в 14:59

Curve25519, EdDSA и Poly1305: Три обделенных вниманием криптопримитива

Программирование, Криптография, Информационная безопасность

Tutorial

Есть такой очень хороший товарищ по имени Daniel Julius Bernstein. Математик, программист и спец по компьютерной безопасности. Его хэш CubeHash чуть не дотянул до третьего раунда SHA-3, а потоковый шифр Salsa20 попал в шорт лист проекта eStream. А еще он автор культовой в узких кругах криптобиблиотеки NaCl, о трех штуках из которой я бы хотел вкратце рассказать.



Curve25519

Это эллиптическая кривая и набор параметров к ней подобранных таким образом, чтобы обеспечить более высокое быстродействие (в среднем, 20-25%) и избавиться от некоторых проблем с безопасностью у традиционного ECDH.

Кривая используется $y^2 = x^3 + 486662x^2 + x$. Это — кривая Монтомгери над полем вычетов по модулю простого числа $2^{255} - 19$ (что и дало название схеме) и с базовой точкой $x=9$. Схема использует точки в сжатой форме (только X координаты), позволяя таким образом использовать "Лестницу Монтомгери", которая делает умножение точек за **фиксированно** время, избавляя нас от Timing attacks.

Curve25519 используется как обмен ключами по умолчанию в OpenSSH, I2p, Tor, Tox и даже в iOS.

Чем эта схема так хороша с точки зрения программиста?

Она очень простая и быстрая. Чтобы сгенерировать новую ключевую пару, мы подаем на вход схеме **любые** 32 случайных байта, которые закрытым ключом. Из них мы получаем 32 байта открытого ключа. Затем как обычно, обмениваемся открытыми ключами и считаем общий. Насколько именно она быстрее классического ECDH с 256битными кривыми сказать не возьмусь, зависит от реализации. Мне она нравится за устойчивость к timing attacks и за возможность использовать любые 32байтные массивы в качестве закрытых ключей.

EdDSA

Точнее, ее частный случай, Ed25519, как можно догадаться, тоже убыстренный и усиленный вариант цифровой подписи на эллиптических кривых. Используется схема Шнорра для «Скрученной кривой» Эдвардса, изобретенной, кстати, тем же Даниэлем Бернштайном в 2007 год

Используется такая вот кривая:

$$-x^2 + y^2 = 1 - \frac{121665}{121666}x^2y^2$$

которая эквивалентна кривой для Curve25519

EdDSA используется, например, в OpenBSD signify tool, чтобы подписывать образы

И так, Curve25519 и Ed25519 — примитивы на эллиптических кривых, оптимизированные по быстродействию и написанные таким образом минимизировать или вовсе исключить влияние входных данных на процесс расчета ключей/подписей.

Poly1305

Это MAC (Message authentication code), работающий совместно с AES или любым другим шифром по вашему желанию. Он считает 16 байт (128 бит) MAC, используя 256 битный ключ AES, который разделяется на два по 128 бит (k,r) и соль (nonce).

Он разбивает сообщение на блоки по 16 байт и работает с ними как с коэффициентами полинома в r по модулю простого числа $2^{130}-5$

Результат получается на 4 байта меньше, чем обычный HMAC-SHA1, не имеет проблем с безопасностью и работает быстрее.

Именно поэтому его вместе с потоковым шифром ChaCha20 использует Google вместо RC4, а так же он включен в OpenSSH, которому теперь нужно зависеть от OpenSSL

Референсная реализация всего этого в библиотеке NaCl на C, но есть порты на java и `c#`, например.

Надеюсь, после этой статьи у вас появится желание узнать об этих примитивах побольше и использовать их в ваших приложениях.

Метки: Curve25519, Ed25519, EdDSA, Poly1305, Daniel J. Bernstein

↑

+31

↓

🔖


111

👁

22,9k

💬

8



↑

149,2

↓

👤

4,8

👤

154

✉

Написать

✍

Подписать

Карма

Рейтинг

Подписчики

Алексей @Scratch

Системный архитектор, криптоманьяк

Поделиться публикацией

ПОХОЖИЕ ПУБЛИКАЦИИ

7 мая 2015 в 15:30

Реализуем ещё более безопасный VPN-протокол

↑

+32

👁

27,1k

🔖

206

💬

27

23 апреля 2015 в 16:21

Реализуем безопасный VPN-протокол

↑

+45

👁

43,2k

🔖

298

💬

56

20 января 2015 в 13:25

Встраиваем бэкдор в публичный ключ RSA

↑

+115

👁






103k

🔖

549

💬

75

ВАКАНСИИ			Мой к
	Application Security Engineer Российский квантовый центр · Москва · Возможна удаленная работа	от 150 (
	Инженер по информационной безопасности Азбука Вкуса · Москва	до 120 (
	Senior Rust Developer ICONIC · Москва	от 250 (
	Системный администратор / Devops Devmasterz · Санкт-Петербург	от 2 (
	Администратор / Сетевой инженер Хостинговые Телесистемы · Москва	от 110 000 до 150 (
Все вакансии			

Комментарии 8

Отслеживать новые в ☐ почте ☐




Greyushko 15.01.15 в 15:29

🔗

🔖

Если кому интересно, про «скрученные» кривые Эдвардса и то, как они могут использоваться в отечественных схемах подписи, вот неплохая статья.






Ответить

 **original** 15.01.15 в 15:38  



А про саму реализацию EdDSA не хотите рассказать, а то все существующие это порт с бернштейновской реализации на ассемблере? В частности требуется представление в виде Little Endian.

Ответить

 **grich** 15.01.15 в 16:42    



Есть еще библиотека с говорящим названием Tweet NaCl (угадайте автора)
Там, кажется, big-endian структуры.

Там ровно те же алгоритмы, все те же constant-time operations. Но, конечно, медленнее.
Есть порты на кучу языков, такие же лаконичные

Ответить

 **okazymyrov** 15.01.15 в 16:38  



У меня Гугл использует «The connection is encrypted and authenticated using AES_128_GCM and uses ECDHE_ECDSA as the key exchange mechanism.




Ответить

 **Scratch** 15.01.15 в 16:40    



As of February 2014, almost all HTTPS connections made from Chrome browsers on Android devices to Google properties have used the new cipher suite. Google plans to make it available as part of the Android platform in a future release.

Ответить

 **ivlad** 16.01.15 в 11:34    



Если посмотреть на все их ciphersuites, видно, что действительно есть **TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256**. Возможно, Chrome будет использовать этот сыот в каких-то ситуациях. Возможно, они когда-то понизят приоритет **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256** тогда все браузеры, у которых есть поддержка первого сыота, перейдут на второй.

Ответить

 **vasilisc** 16.01.15 в 08:03  



Как админу хочется поблагодарить этого талантливого дядьку за djbdns и qmail.

Ответить

 **vazir**  18.01.15 в 13:21    



а... с одной стороны он типа сделал qmail open-source сразу, но с такими условиями что никто не может менять ОСНОВНОЙ код и распространять, т.е. изменения в виде патчей, там аж целый портал патчей набрался. Благодаря этому недальновидному подходу (о да, умница автор просто хотел чтобы все любовались на его код, (он и в самом деле красивый), а не засоряли его). Благодаря этому подходу qmail практически мертв, и его место было занято postfix... Он одумался какое-то время назад, но поезд ушел.

Ответить

Написать комментарий

B / **U**          

Предпросмотр

Отправить

☐ Markdown

САМОЕ ЧИТАЕМОЕ

Сутки

Неделя

Месяц

Отсутствие дискриминации – это основная ценность open source

+67

16,4k

28

120

Почему мне не перезвонили?

+24

23,3k

68

68

DEFCON 17. Взлом 400 000 паролей, или как объяснить соседу по комнате, почему счёт за электричество увеличился. Часть 1

+16

6,3k

43

3

Как Microsoft спрятала целый сервер и как его найти

+3

6,1k

14

5

В чём важность $196\,884 = 196\,883 + 1$? Как это объяснить на пальцах?

+52

25,7k

119

101

claygod

Разделы

Информация

Услуги

Приложения

Профиль

Публикации

Правила

Реклама

Трекер

Хабы

Помощь

Тарифы

Диалоги

Компании

Документация

Контент

Настройки

Пользователи

Соглашение

Семинары

ППА

Песочница

Конфиденциальность



© 2006 – 2018 «TM»

[О сайте](#)

[Служба поддержки](#)

[Мобильная версия](#)

