

OpenBSD: Куда катится крипто?

Михаил Белопухов
.vantronix secure systems
mikeb@openbsd.org

Москва, 14 декабря 2013 г.

THIS AYN RANDOM NUMBER GENERATOR YOU WROTE CLAIMS TO BE FAIR, BUT THE OUTPUT IS BIASED TOWARD CERTAIN NUMBERS.

WELL, MAYBE THOSE NUMBERS ARE JUST INTRINSICALLY BETTER!



<http://xkcd.com/1277>

Генератор псевдослучайных чисел

rand (ANSI C, POSIX)

Генератор псевдослучайных чисел

rand (ANSI C, POSIX)

*rand48 (POSIX)

Генератор псевдослучайных чисел

rand (ANSI C, POSIX)

*rand48 (POSIX)

random (POSIX)

Генератор псевдослучайных чисел

rand (ANSI C, POSIX)

*rand48 (POSIX)

random (POSIX)

/dev/[au]random (Linux)

Генератор псевдослучайных чисел

rand (ANSI C, POSIX)

*rand48 (POSIX)

random (POSIX)

/dev/[au]random

arc4random (OpenBSD)

Генератор псевдослучайных чисел

rand (ANSI C, POSIX)

*rand48 (POSIX)

random (POSIX)

/dev/[au]random

arc4random в Линуксе! (libbsd)

Генератор псевдослучайных чисел

rand (ANSI C, POSIX)

*rand48 (POSIX)

random (POSIX)

/dev/[au]random

arc4random (RC4?)

Безопасность RC4

2001 Атака Флурера, Мантина и Шамира ¹

2005 Атака Кляйна ²

2013 Атака Алфардана, Бернштайна, Патерсона и др. ³

¹Weaknesses in the Key Scheduling Algorithm of RC4

²Attacks on the RC4 stream cipher

³On the Security of RC4 in TLS and WPA

Генератор псевдослучайных чисел

rand (ANSI C, POSIX)

*rand48 (POSIX)

random (POSIX)

/dev/[au]random

arc4random (ChaCha?!)

ChaCha20: Поточный шифр

<http://cr.yp.to/chacha.html>

Основан на Salsa20 (в портфолио eSTREAM)

Используется в BLAKE (финалист SHA-3)

4 цикла на байт на современных x86

Размер ключа 128 или 256 бит

Вам чачу или сальсу?

Улучшена диффузия

Улучшена скорость

IETF Crypto Forum Research Group (CFRG) заключила, что “произведенного анализа достаточно, чтобы заключить, что ChaCha является приемлемой альтернативой SALSA-20.”⁴

⁴Synopsis of CFRG discussions on new stream ciphers and MACs for TLS

Генератор псевдослучайных чисел

rand (ANSI C, POSIX)

*rand48 (POSIX)

random (POSIX)

/dev/[au]random

arc4random

libottery

Генератор псевдослучайных чисел

rand (ANSI C, POSIX)

*rand48 (POSIX)

random (POSIX)

/dev/[au]random

arc4random

goodrandom?

SSL/TLS

Шифры в стандартах SSL/TLS

RC4	SSL 2.0+
AES-CBC	SSL 3.0+
AES-GCM	TLS 1.2

SSL/TLS: Chrome

Недокументированная опция `--cipher-suite-blacklist`

```
0x0004  TLS_RSA_WITH_RC4_128_MD5
0x0005  TLS_RSA_WITH_RC4_128_SHA
0x000a  TLS_RSA_WITH_3DES_EDE_CBC_SHA
0x0032  TLS_DHE_DSS_WITH_AES_128_CBC_SHA
0xc007  TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
0xc011  TLS_ECDHE_RSA_WITH_RC4_128_SHA
```

Значения из RFC 2246

AES-GCM

Стандарт NIST шифрования с аутентификацией

AES-CTR + GHASH

NSA Suite B, SSH, TLS, IPsec, MACsec, FC-SP, WiGig

Экспериментальная поддержка в OpenBSD IPsec стеке

AES-NI и CLMUL

В Intel Westmere и более новых ЦПУ Intel и AMD

7 новых SSE инструкций

Реализация в OpenSSL и в OCF

FPU “локи” в ядре

CBC, CTR, XTS, GCM

Драфт ChaCha20-Poly1305 для TLS

Google разработали `draft-agl-tls-chacha20poly1305`

Драфт ChaCha20-Poly1305 для TLS

Google разработали [draft-agl-tls-chacha20poly1305](#)

E5-2690 2.9GHz

AES-128-GCM	131 MB/s
AES-128-GCM с AES-NI	311 MB/s
ChaCha20+Poly1305	420 MB/s

Cortex-A9 1.2GHz

AES-128-GCM	27 MB/s
ChaCha20+Poly1305	78 MB/s

Драфт ChaCha20-Poly1305 для TLS

Google разработали [draft-agl-tls-chacha20poly1305](#)

E5-2690 2.9GHz

AES-128-GCM	131 MB/s
AES-128-GCM with AES-NI	311 MB/s
ChaCha20+Poly1305	420 MB/s

Cortex-A9 1.2GHz

AES-128-GCM	27 MB/s
ChaCha20+Poly1305	78 MB/s

Chrome 32, в будущем поддержка в NSS, Firefox

Драфт Salsa20-SHA1 для TLS

RedHat и др. [draft-josefsson-salsa20-tls](#)

Ревизия	Изменения
01	убран Salsa20/12 с 128-битным ключем
02	добавлен UMAC-96
03	убран UMAC-96

Poly1305: Полиномиальная имитовставка

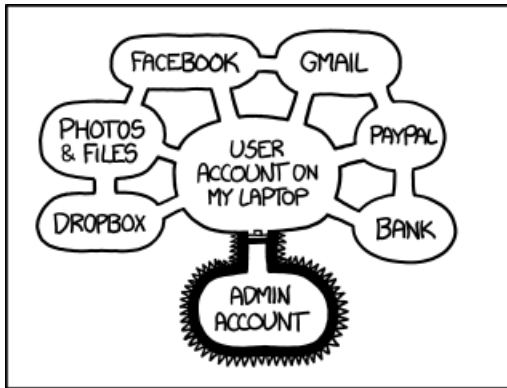
<http://cr.yp.to/mac.html>

“Poly1305 может быть объяснена в одном твите”⁵

Порядка 4 циклов на байт (не учитывая шифр)

Безопасность определяется в большей степени выбранным алгоритмом шифрования (AES, ChaCha и т.п.)

⁵Salsa20 and Poly1305 in TLS



IF SOMEONE STEALS MY LAPTOP WHILE I'M
LOGGED IN, THEY CAN READ MY EMAIL, TAKE MY
MONEY, AND IMPERSONATE ME TO MY FRIENDS,
BUT AT LEAST THEY CAN'T INSTALL
DRIVERS WITHOUT MY PERMISSION.

<http://xkcd.com/1200>

Кривые NIST

2013 Бернштайн, Ланге “Небезопасность кривых NIST” ⁶

<http://safecurves.cr.yr.to/>

⁶Security dangers of the NIST curves

Curve25519: Протокол Диффи – Хеллмана

<http://cr.yp.to/ecdh.html>

Не нарушает патентов Certicom

Исполняется за константное время

32-х байтные приватный и публичный ключи

Ed25519: Цифровая подпись EdDSA

<http://ed25519.cr.yp.to/>

Сравнима с RSA3072, NIST P-256

32-х байтные приватный и публичный ключи

64-х байтные подписи

Использует PRF (SHA512)

NIST-free криптография в OpenSSH

Поддержка в OpenBSD-current:

Шифр	<code>chacha20-poly1305@openssh.com</code>
Обмен ключами	<code>curve25519-sha256@libssh.org</code>
ЭЦП	<code>ssh-ed25519-cert-v01@openssh.com</code>

IPsec/IKEv2

Возможно использование “Private Range” в IKEv2
ChaCha20-Poly1305 в AEAD режиме для ESP

Вопросы?

If this story leaves you confused, join the club.

Bruce Schneier