ДВФУ
ДАЛЬНЕВОСТОЧНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ

«Рекомендация NIST SP 800-90A»

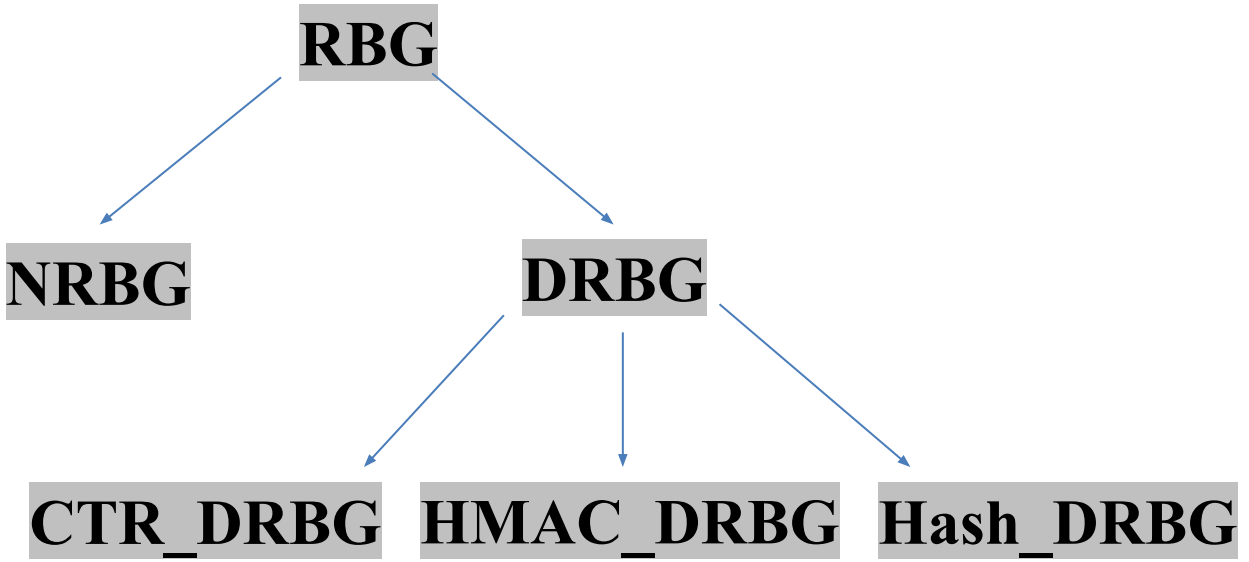
NIST SP 800-90A — («SP» — сокращение от англ. «Special Publication», «специальная публикация») — публикация Национального института стандартов и технологий с названием «Рекомендация для генерации случайных чисел с использованием детерминированных генераторов случайных битов» (англ. «Recommendation for Random Number Generation Using Deterministic Random Bit Generators»).

NIST SP 800-90A является общественным достоянием и находится в свободном доступе, так как представляет из себя исследование федерального правительства США.

NIST National Institute of Standards and Technology

Содержание рекомендации

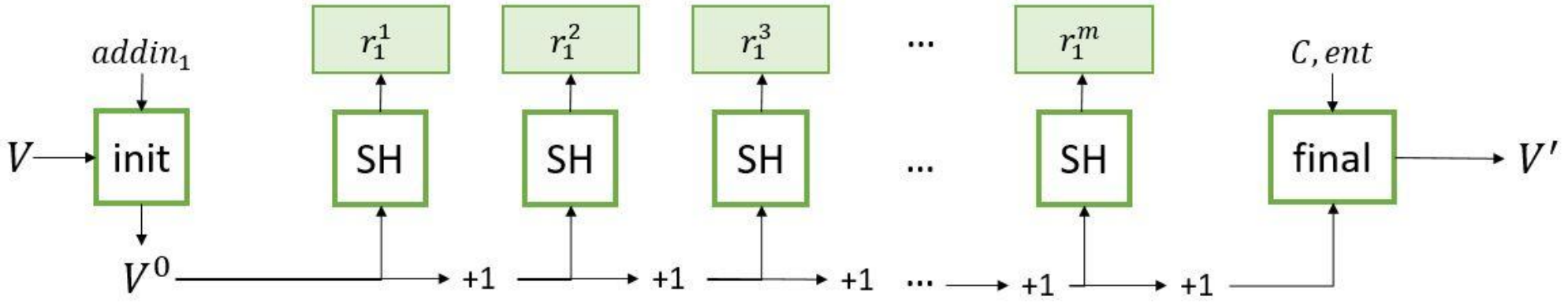
В настоящей Рекомендации определены методы генерации случайных битов, которые затем могут использоваться напрямую или преобразовываться в случайные числа, когда случайные значения требуются приложениям, использующим криптографию.



Hash_DRBG

HASH-DRBG основан на хеш-функции SH : $\{0;1\}^* \rightarrow \{0, 1\}^1$ из семейства криптографических хеш-функций SHA. Состояние имеет вид S = (V, C, cnt), где V ∈ $\{0, 1\}^{len}$ — счетчик, который хешируется для создания конечных блоков, значение которого обновляется во время каждого вызова генератора; C — константа, зависящая от порождающего элемента (англ. seed), а cnt — счетчик повторного заполнения. Счетчик cnt указывает количество запросов псевдослучайных битов с момента получения нового значения, принятого от истинно случайного генератора во время создания экземпляра или повторного заполнения.

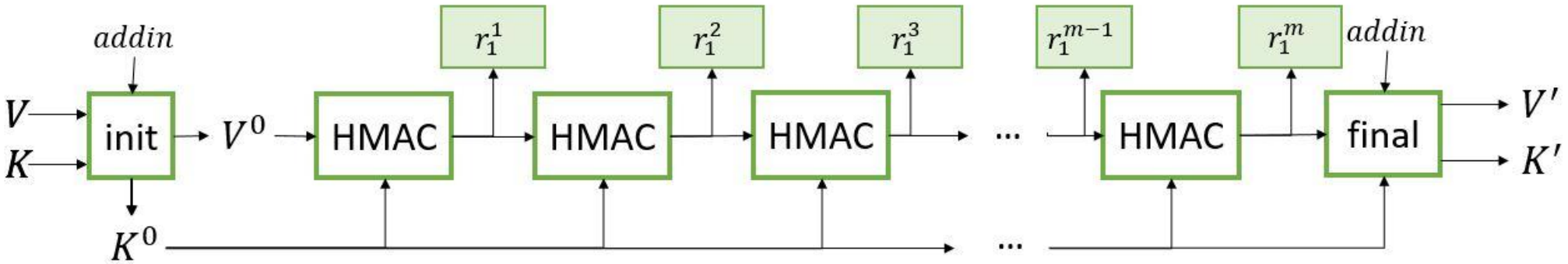
Эволюция состояния HASH-DRBG в рамках одного вызова функции generate,
с начальным состоянием S = (V, C, cnt):



HMAC_DRBG

HMAC-DRBG использует HMAC: $\{0, 1\}^l \times \{0, 1\}^* \rightarrow \{0, 1\}^l$ для генерации блоков псевдослучайного вывода. Состояние имеет вид S = (K, V, cnt), где стандарт определяет K и V как критические для безопасности переменные секретного состояния. Предполагается, что после инициализации начальным состоянием является $S_0 = (K_0, V_0, cnt_0)$, где $cnt_0 = 1$ и $K_0, V_0 \leftarrow \{0, 1\}^{len}$. Здесь $K \in \{0, 1\}^l$ используется в качестве ключа HMAC, $V \in \{0, 1\}^l$ является счетчиком, и cnt обозначает счетчик повторного заполнения.

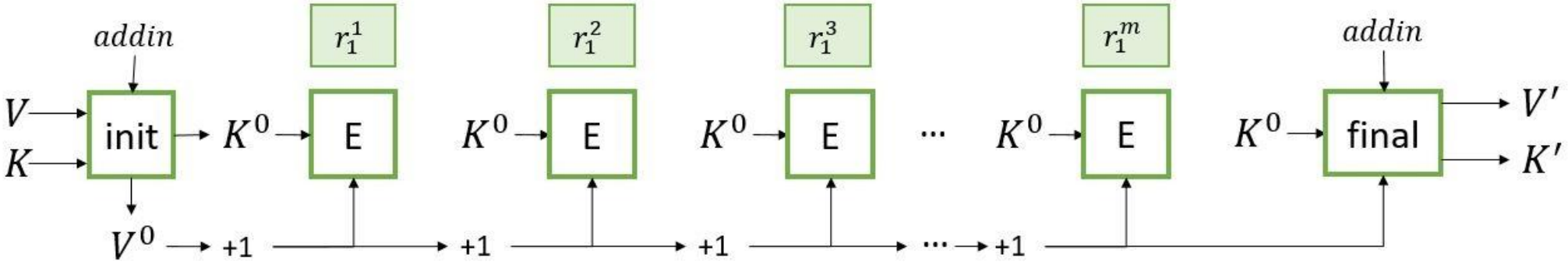
Эволюция состояния HMAC-DRBG в рамках одного вызова функции generate с начальным состоянием S = (K, V, cnt):



CTR_DRBG

Состояние имеет вид S = (K, V, cnt), где K ∈ $\{0, 1\}^k$ используется в качестве ключа для блочного шифра, V ∈ $\{0, 1\}^l$ является счетчиком, а cnt обозначает счетчик повторного заполнения. Стандарт утверждает, что K и V являются критическими переменными состояния безопасности.

Эволюция состояния HMAC-DRBG в рамках одного вызова функции generate с начальным состоянием S = (K, V, cnt):



Dual_EC_DRBG

Dual_EC_DRBG была изъята из публикации с выпуском первой редакции документа. Причиной этому стало потенциальное существование бэкдора. Бэкдор — намеренно встроенный дефект алгоритма, позволяющий получить несанкционированный доступ к данным или удалённому управлению компьютером.

10000000$

Анализ безопасности

Hash_DRBG и HMAC_DRBG имеют доказательства безопасности для генерации псевдослучайных последовательностей. Документ, подтверждающий безопасность Hash_DRBG и HMAC_DRBG цитирует попытки доказательства безопасности для Dual_EC_DRBG, высказывая, что не следует использовать CTR_DRBG, потому что это единственный генератор в NIST SP 800-90A, для которого отсутствуют доказательства безопасности.

HMAC_DRBG также имеет машинно-подтвержденное доказательство безопасности. Тезис, содержащий проверенное вычислительными методами доказательство безопасности, также доказывает, что взлом правильно реализованного экземпляра HMAC_DRBG не ставит под угрозу безопасность чисел, созданных до взлома.

Было показано, что CTR_DRBG имеет проблемы с безопасностью при использовании с определёнными параметрами, поскольку криптографы не учитывали размер блока шифра при проектировании этого генератора псевдослучайных чисел.

Примеры применения

Приведенные алгоритмы являются стандартами и используются крупными компаниями для создания собственных продуктов на их основе. Так компания Microsoft в процессе создания обновления для своего CryptoApi под названием «Cryptography API: Next Generation (CNG)» установила в качестве генератора псевдослучайных чисел по умолчанию на CTR_DRBG.
Компания Intel в инструкции RdRand для генерации случайного числа при помощи встроенного генератора случайных чисел также использует CTR_DRBG.