Álvéletlen generátorok

PPKE, ITK
Csapodi Márton

Miért fontos a véletlen szám

A kriptográfia sarokköve:

- Akkor nehéz kitalálni a titkot, ha az kellően véletlen.

A 9 egy véletlen szám?

Hagyományos generátorok

Excel RAND fv. (Excel 5.0 és korábbi)

Első:

r(1) = 9821 * 0.5 + 0.211327 törtrésze

Továbbiak:

r(n+1) = 9821 * r(n) + 0.211327 törtrésze

randomize=1 az .INI file [Microsoft Excel] szekciójában:

r: rendszeróra alapján indul

Excel 5.0-nál alapértelmezett

rövid ciklus (~ 1 millió)

Hagyományos statisztikai tesztek:

- 1-esek és 0-k gyakorisága
- 00, 01, 10, 11 minták (stb.) gyakorisága
- 0, 00, 000, 0000, stb minták gyakorisága
- autokorreláció

FIPS 140: Security Requirements for Cryptographic Modules

Diehard test

stb.

Hagyományos generátorok

Excel RAND fv. (Excel 2003 és újabb)

Wichmann-Hill algoritmus

X(0), Y(0), Z(0) = 1 és 30000 közti egész

X(n) = 171 * X(n-1) mod 30269
Y(n) = 172 * Y(n-1) mod 30307
Z(n) = 170 * Z(n-1) mod 30323

r(n) = X(n)/30269.0 + Y(n)/30307.0 + Z(n)/30323.0 törtrésze

hosszú ciklus, FIPS, Diehard teszteknek megfelel

MS CryptGenRandom fv.

Kiinduló érték (seed) képzés az alábbi adatok (entropy input) összefűzésével és hash-elésével:

- The process ID of the current process requesting random data
- The thread ID of the current thread within the process requesting random data
- A 32bit tick count since the system boot
- The current local date and time
- The current system time of day information consisting of the boot time, current time, time zone bias, time zone ID, boot time bias, and sleep time bias
- The current hardware-platform-dependent high-resolution performance-counter value
- The information about the system's current usage of both physical and virtual memory, and pagefile
- The local disk information including the numbers of sectors per cluster, bytes per sector, free clusters, and clusters that are available to the user associated with the calling thread
- A hash of the environment block for the current process
- Some hardware CPU-specific cycle counters

MS CryptGenRandom fv.

- The system processor performance information consisting of Idle Process Time, Io Read TransferCount, Io Write Transfer Count, Io Other Transfer Count, Io Read Operation Count, Io WriteOperation Count, Io Other Operation Count, Available Pages, Committed Pages, Commit Limit,Peak Commitment, Page Fault Count, Copy On Write Count, etc.
- The system exception information consisting of Alignment Fix up Count, Exception DispatchCount, Floating Emulation Count, and Byte Word Emulation Count
- The system lookaside information consisting of Current Depth, Maximum Depth, Total Allocates,Allocate Misses, Total Frees, Free Misses, Type, Tag, and Size
- The system interrupt information consisting of context switches, deferred procedure call count,deferred procedure call rate, time increment, deferred procedure call bypass count, andasynchronous procedure call bypass count
- The system process information consisting of Next Entry Offset, Number Of Threads, Create Time,User Time, Kernel Time, Image Name, Base Priority, Unique Process ID, Inherited from UniqueProcess ID, Handle Count, Session ID, Page Directory Base, Peak Virtual Size, Virtual Size, PageFault Count, Peak Working Set Size, Working Set Size, Quota Peak Paged Pool Usage, QuotaPaged Pool Usage, Quota Peak Non Paged Pool Usage, etc.

MS CryptGenRandom fv.

A híváskor megadható:

- byte-ok száma
- opcionálisan további entropy bitek

r(n+1) generálása különböző Windows verziókban:

- Windows 2000-ig, alap XP: RC4 adatfolyam rejtjelező alapú
- XP SP3, alap Vista, 2003 SP2, 2008 Server: SHS based RNG (FIPS 186-2)
- Vista SP1, Windows 7: AES CTR_DRBG (NIST Special Publication 800-90)

CryptoAPI Next Generation (CNG, CryptoAPI kiváltása): BCryptGenRandom fv.

- Vista, Windows 7 és 2008 Server: választható algoritmus (FIPS 186-2, NIST SP 800-90 AES CTR_DRBG és Dual_EC_DRBG)
- Windows 10: nincs Dual_EC_DRBG

Irodalom

FIPS PUB 186-2

FEDERAL INFORMATION
PROCESSING STANDARDS PUBLICATION

2000 January 27

U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology

DIGITAL SIGNATURE STANDARD (DSS)

FIPS186-2

Van már FIPS 186-3 is (2009. június)

Digitális aláírás szabvány
Tartalmaz előírásokat véletlen számok generálására is (kulcspár)

16-18. oldal:

XKEY(1): seed

véletlen bitek (r) generálásának lépései:

XVAL(n) = XKEY(n) + XSEED(n)

r(n) = SHA-1 (IV, XVAL(n))

XKEY(n+1) = XKEY(n) + r(n) + 1

XSEED(n): opcionális további seed bitek

IV: állandó initial value

SHA-1: 160 bites lenyomat

Irodalom

NIST Special Publication 800-90

Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised)

Elaine Barker
John Kelsey

Computer Security Division
Information Technology Laboratory

COMPUTER SECURITY

March 2007

Fogalmak

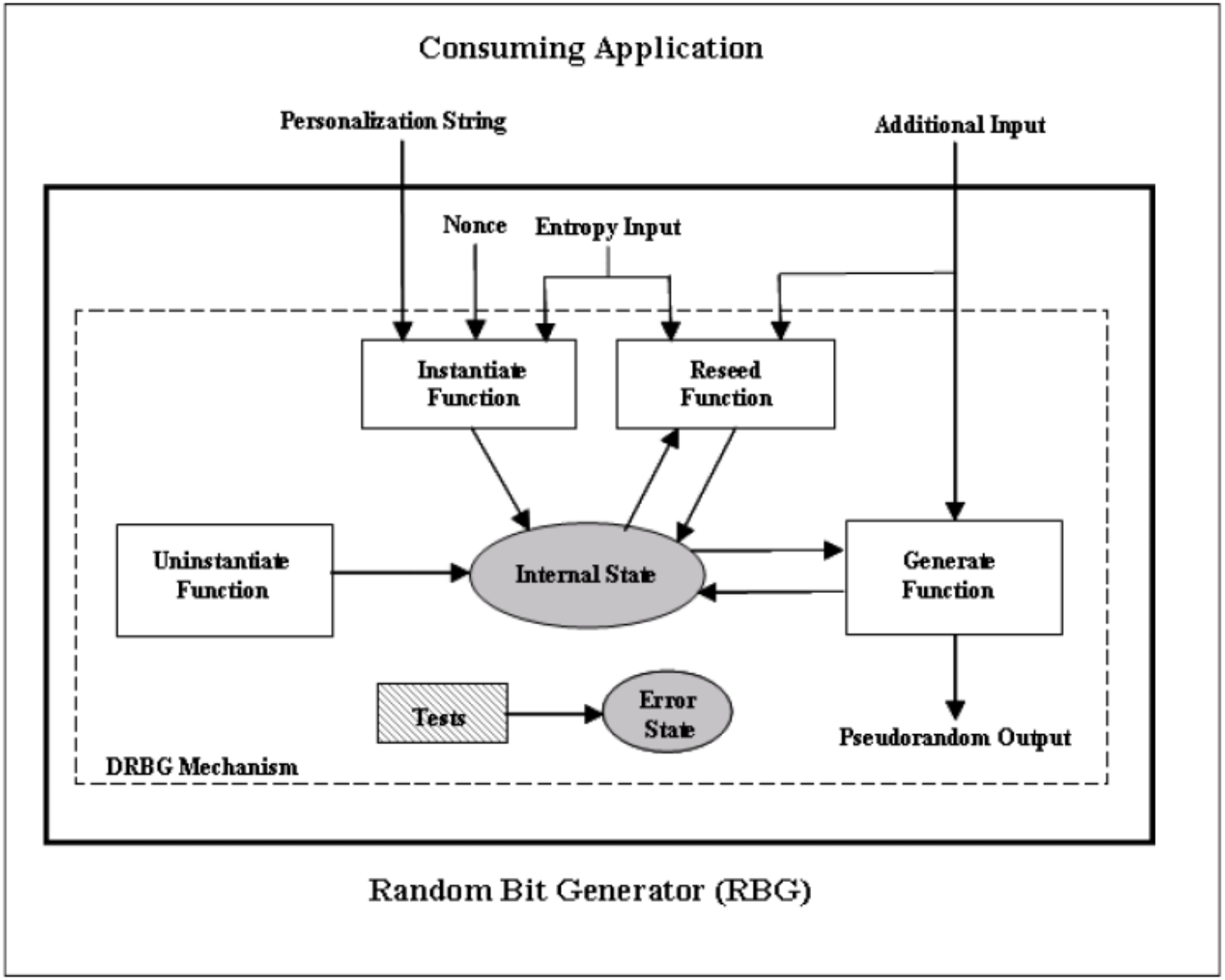
RBG - Random Bit Generator

NRBG - Non-deterministic Random Bit Generator

DRBG - Deterministic Random Bit Generator (Pseudorandom Bit Generator)

Cryptographycally Secure DRBG: csak ezzel foglalkozunk
nemcsak statisztikai tulajdonságok, hanem kriptográfiában használható

Funkcionális modell



Funkcionális modell

"Entrópia":

- magérték (seed) létrehozására
- titkos
- nem a hossza meghatározott, hanem a bizonytalansága

Egyéb bemenet:

- "nonce", személyre szabott érték, stb.
- nem feltétlenül titkos

Állapot:

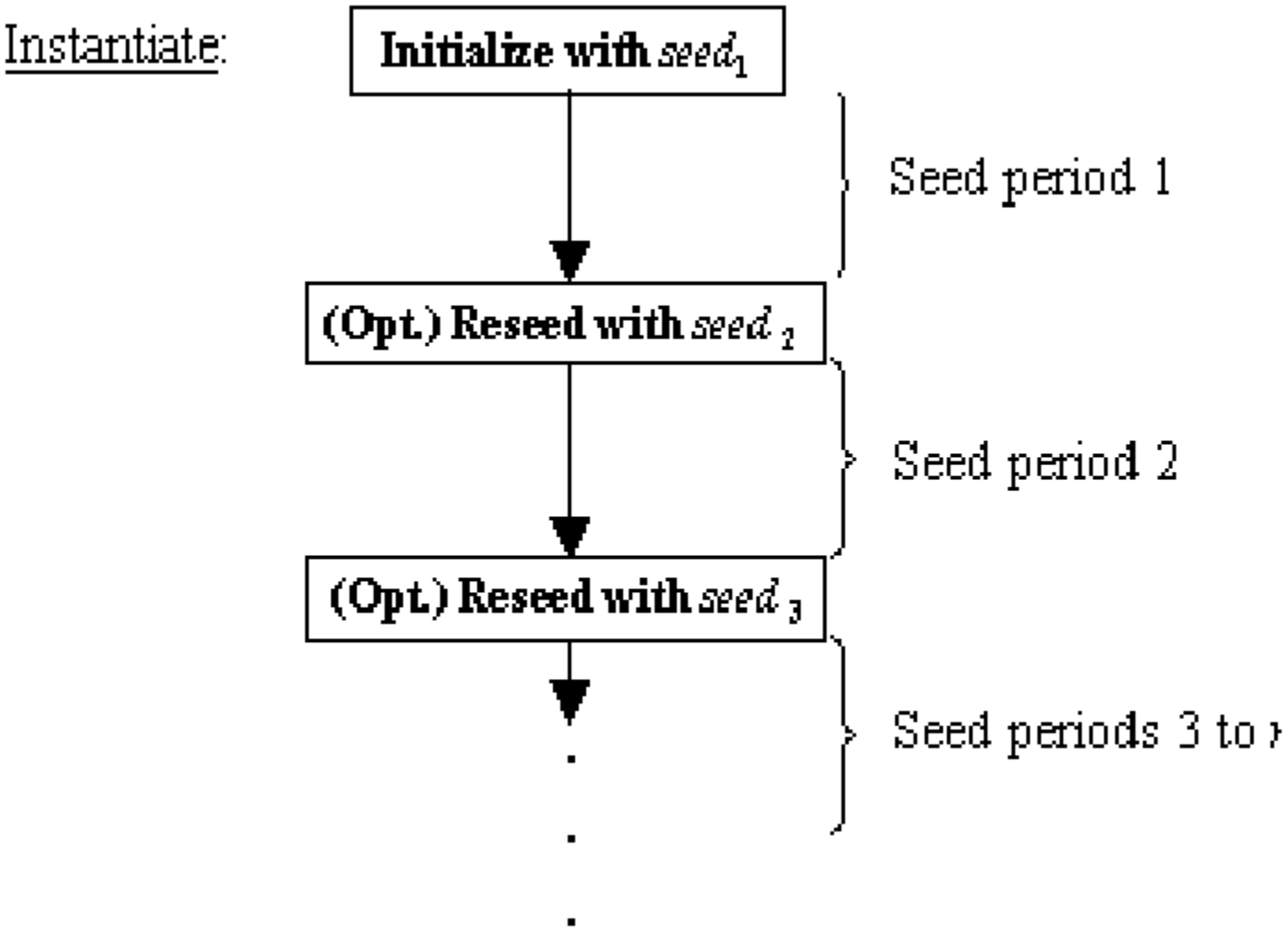
- minden belső adat, ami a következő állapot számításához kell

Műveletek:

- egyed létrehozása (instantiate)
- új magérték létrehozása (reseed)
- törlés (uninstantiate)
- gyártás (generate)

Teszt

Egyed létrehozása



Egyed létrehozása

Különböző célú véletlen számok külön egyedek lehetnek (külön seed) akkor is, ha a generálás módja azonos.

Egy egyednek lehetnek seed periódusai, ha a reseed lehetőségét kihasználjuk.

Létrejön az első állapot (titkos érték + számláló, egyéb paraméterek)

(Az állapot érték is titkos kell maradjon)

A biztonság függ:

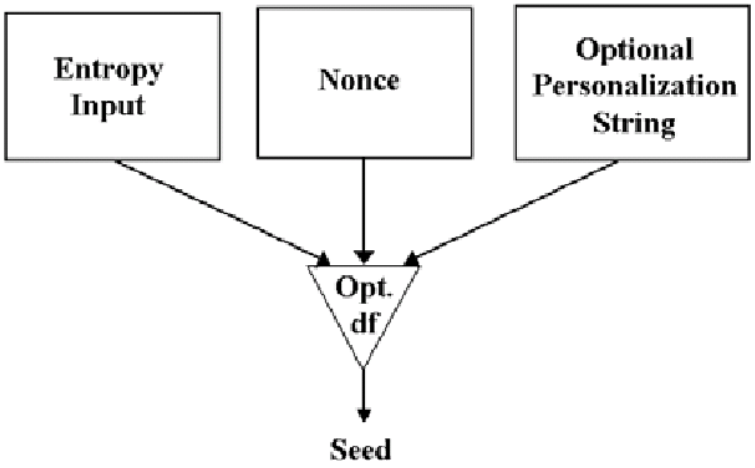
- generátortól
- egyed létrehozásától

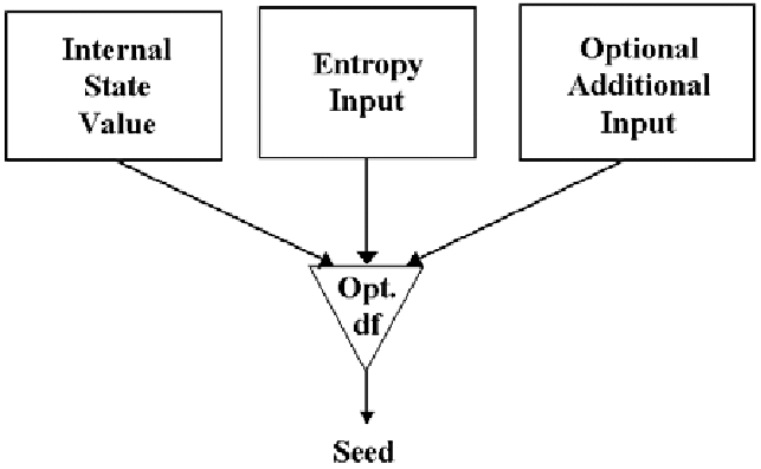
Entrópia, nonce, egyéb:

- termikus zaj a bemeneteken
- hard disk keresési idő
- rendszer óra
- felhasználó paraméterek
- hardver paraméterek
- rendszer input
- felhasználói input

Aszimmetria megszüntetése (de-skew)

Egyed létrehozása, reseed





Backtracking, prediction

Backtracking resistance:

Ismertté vált állapot alapján

- a korábbi állapotok nem állíthatók elő
- korábbi output nem különböztethető meg a véletlentől

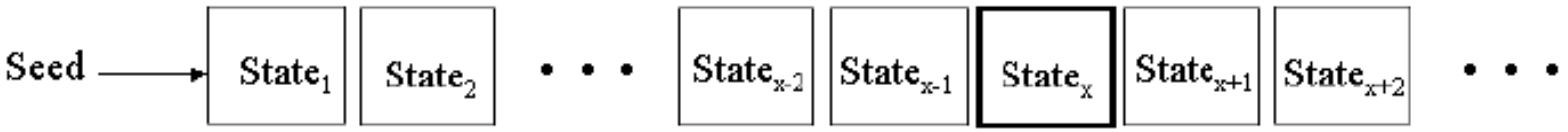
Ez mindig elvárható.

Prediction resistance:

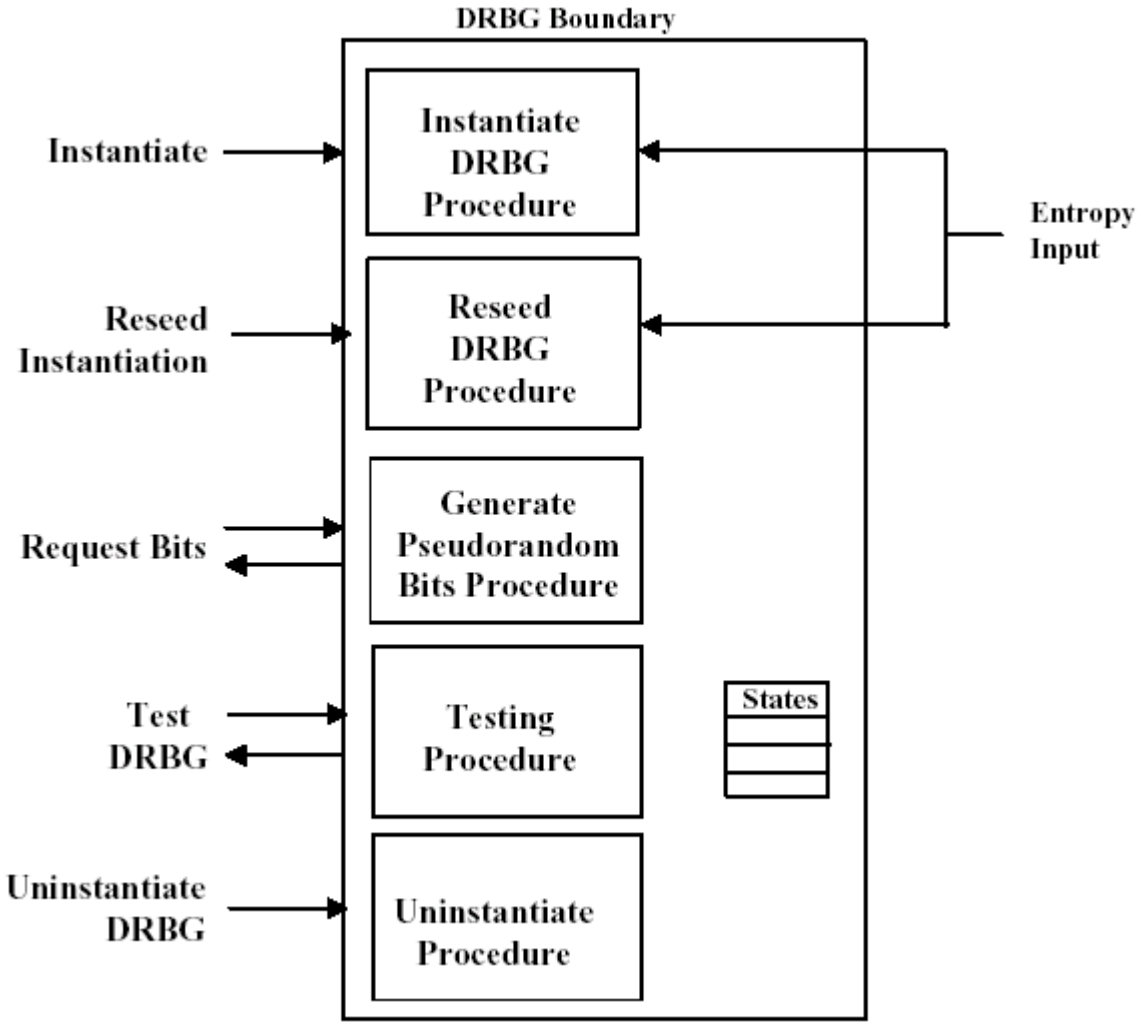
Ismertté vált állapot alapján

- későbbi állapotok nem állíthatók elő
- későbbi output nem különböztethető meg a véletlentől

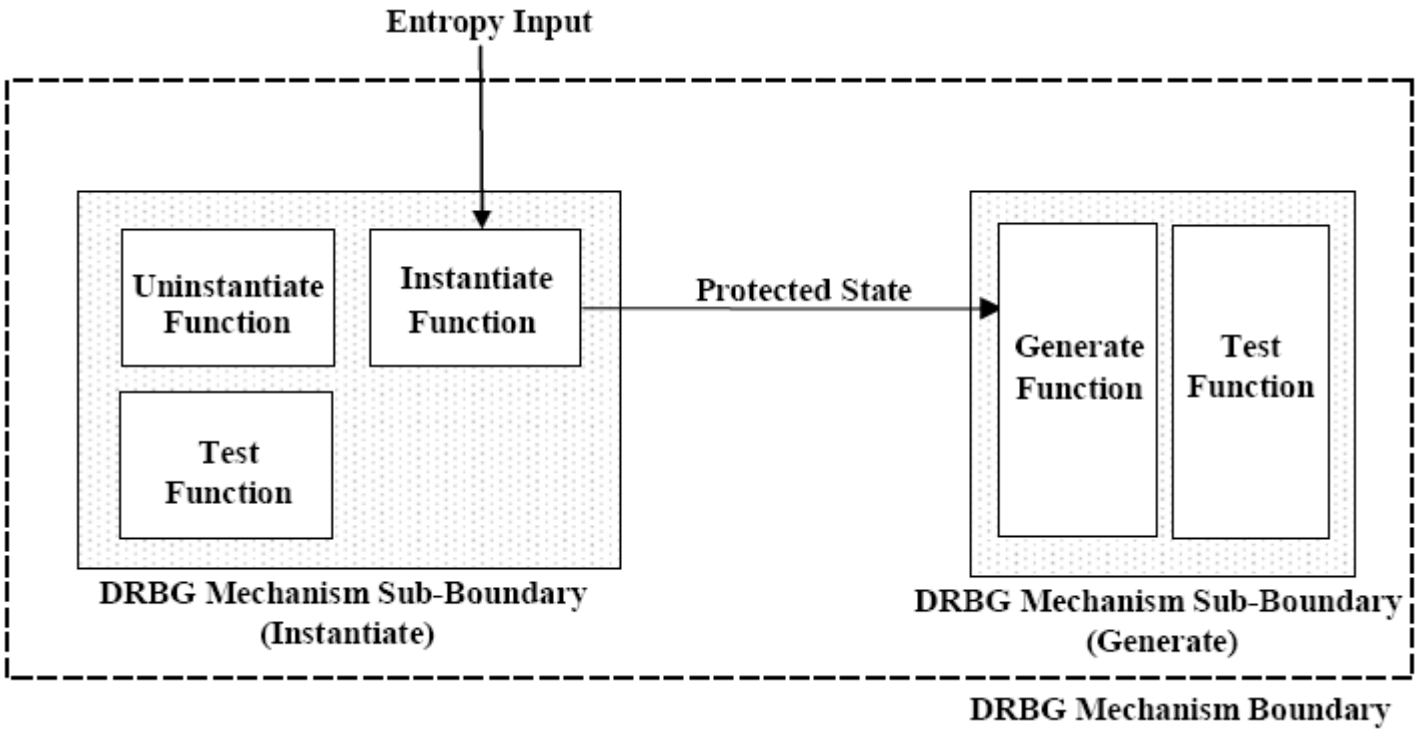
Ez nem várható el mindig. Ha szükséges, akkor reseeding kell minden alkalommal.



A generátor határai, biztonsága



A generátor határai, biztonsága



Korrekt megoldások

Alapelvek:

- erős seed
- kriptográfiailag erős generátor fv.
- állapot ne kerüljön nyilvánosságra
- bitsorozat ismerete ne okozzon problémát

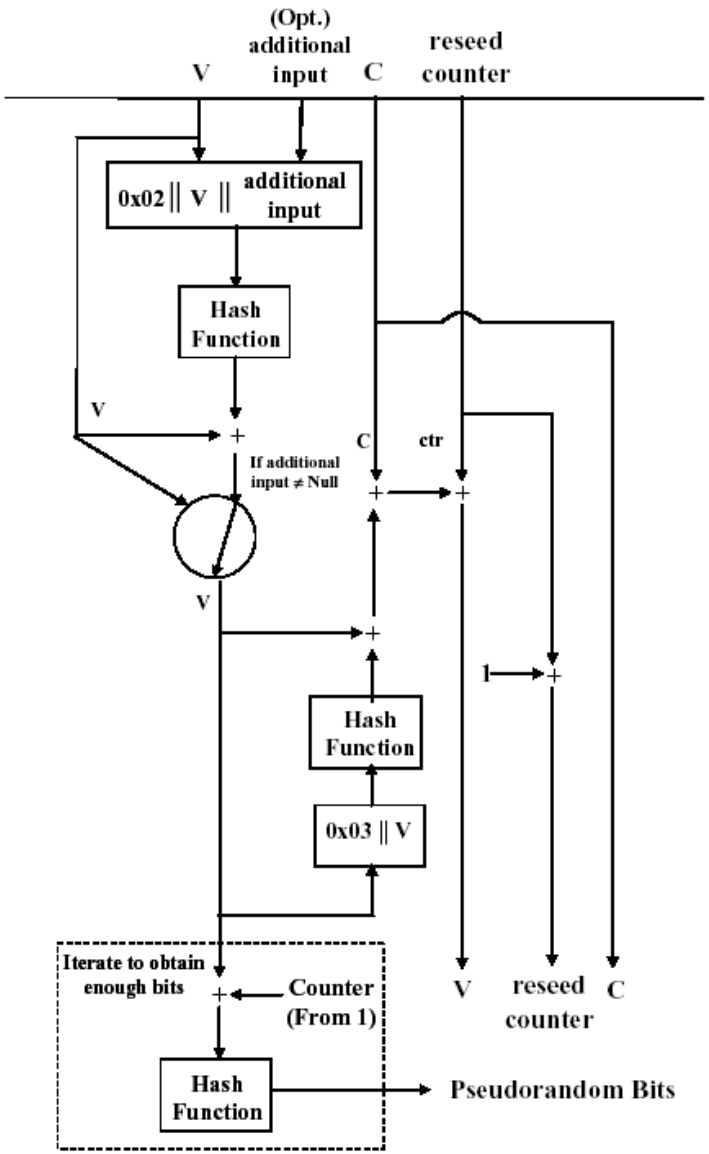
Vagyis: pl. hash alkalmazása esetén nem az output bitek leképezésével kapjuk a további biteket.

Lehetőségek:

- hash (seed | i)
- encrypt (seed | i)
- encrypt (output)
- Blum-Blum-Shub

Lehet minden ciklusban "entrópiát" hozzátenni.

Hash alapú minta

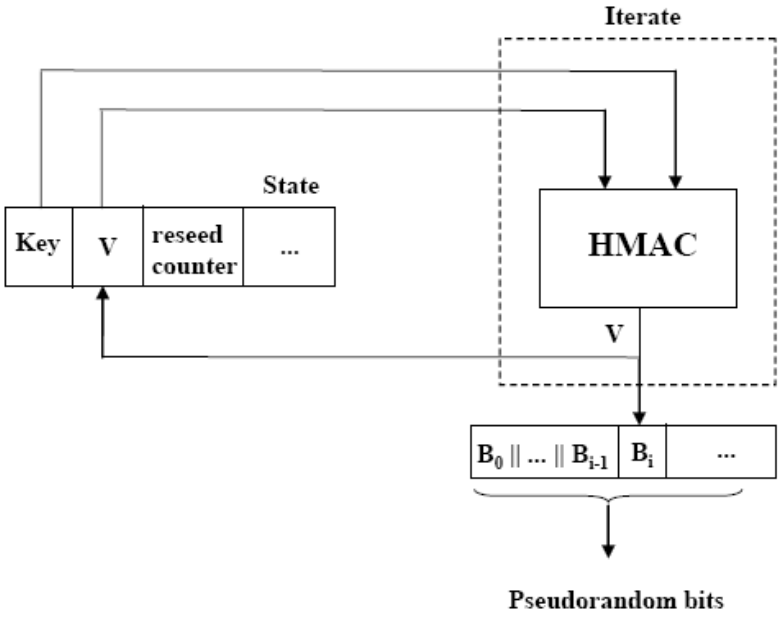


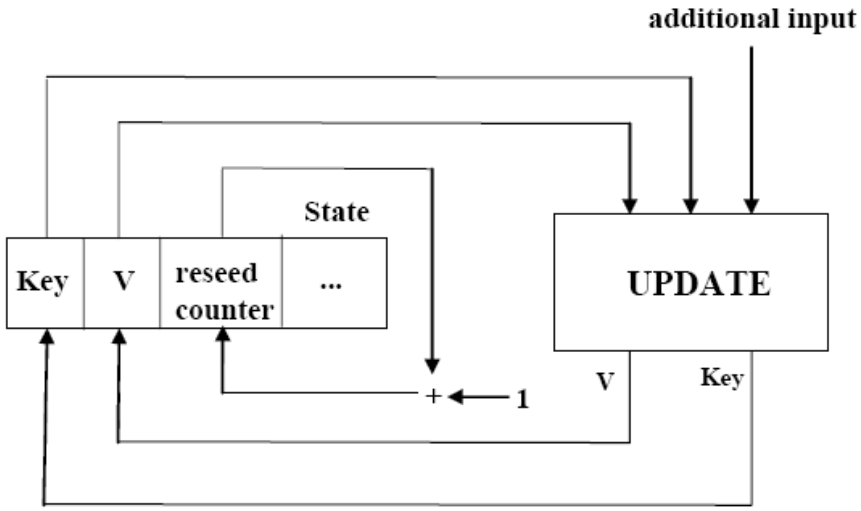
V: állapot, V_0: seed

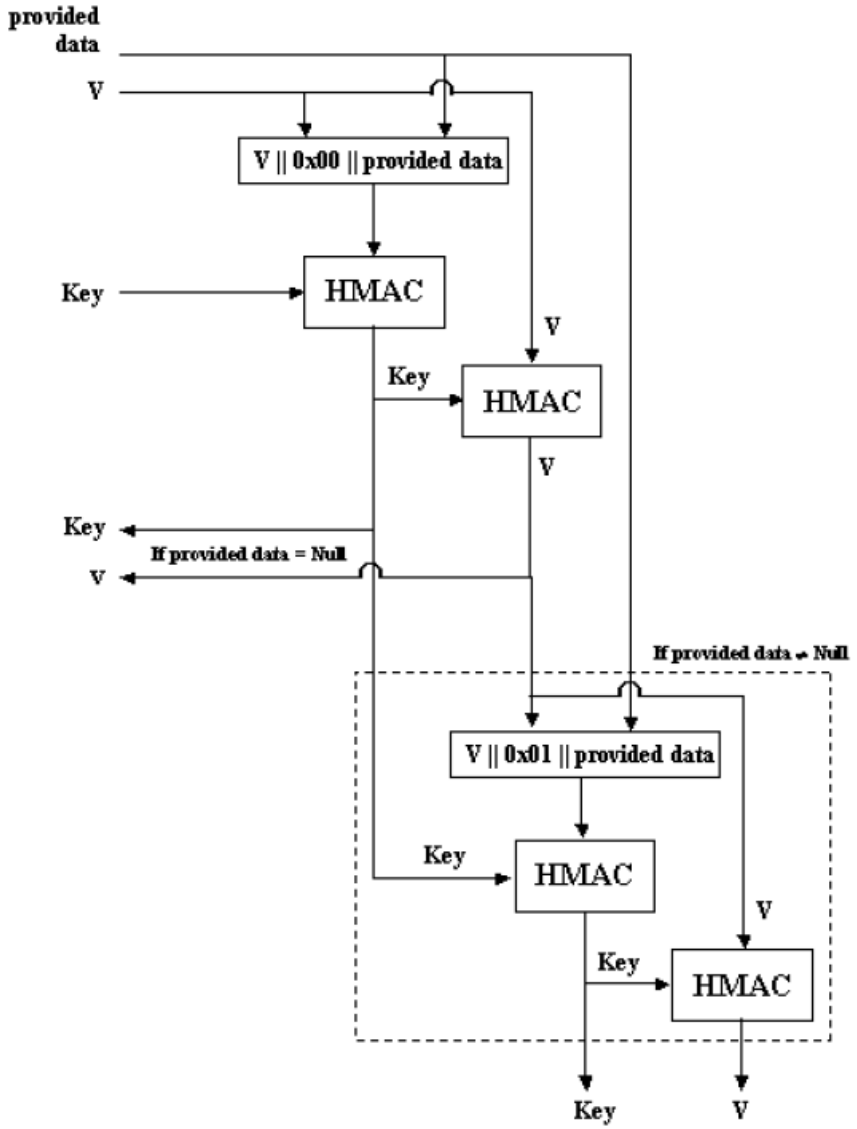
C: hash(seed)

reseed counter: számláló

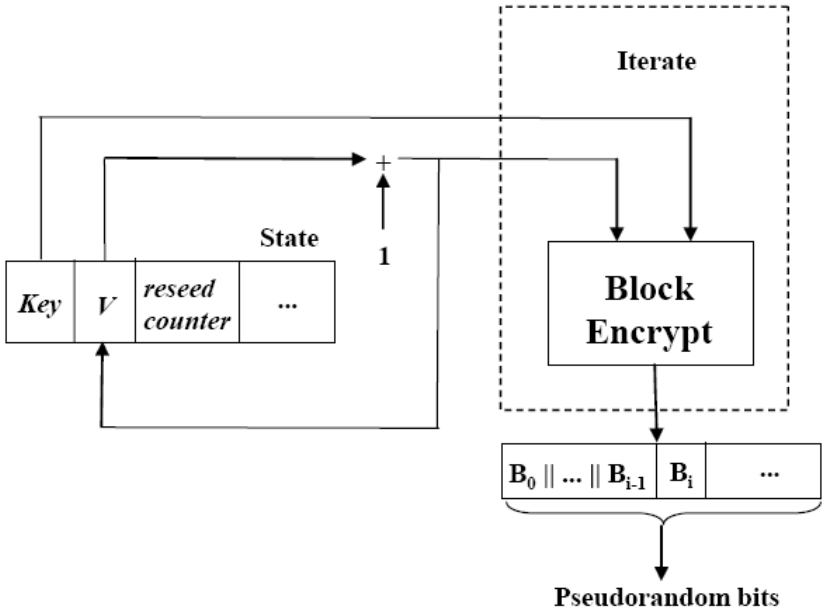
Keyed-Hash alapú minta

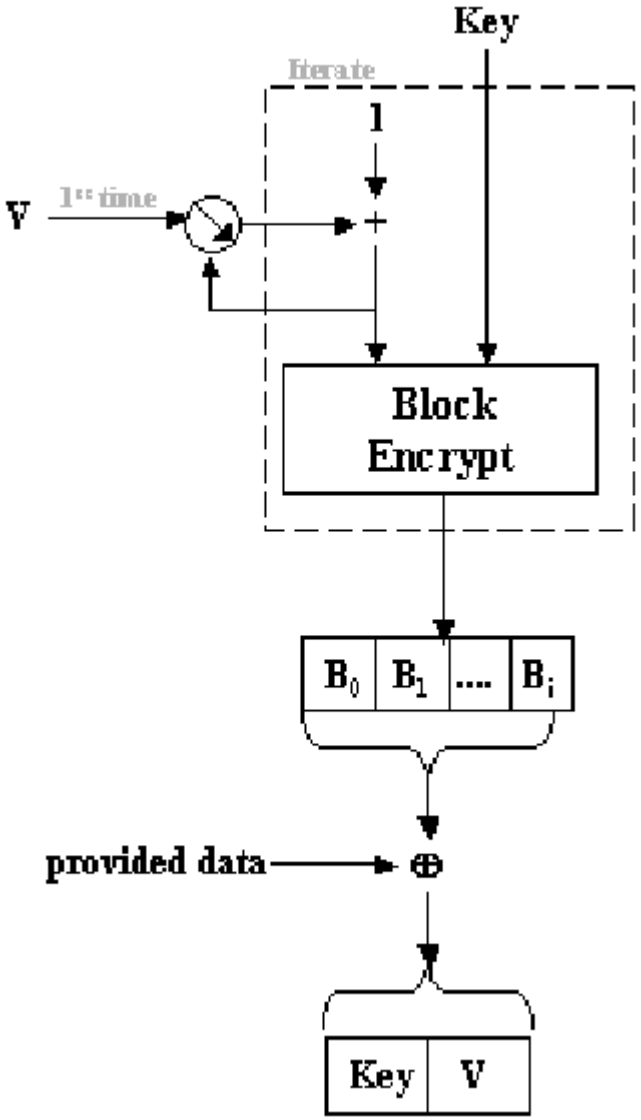


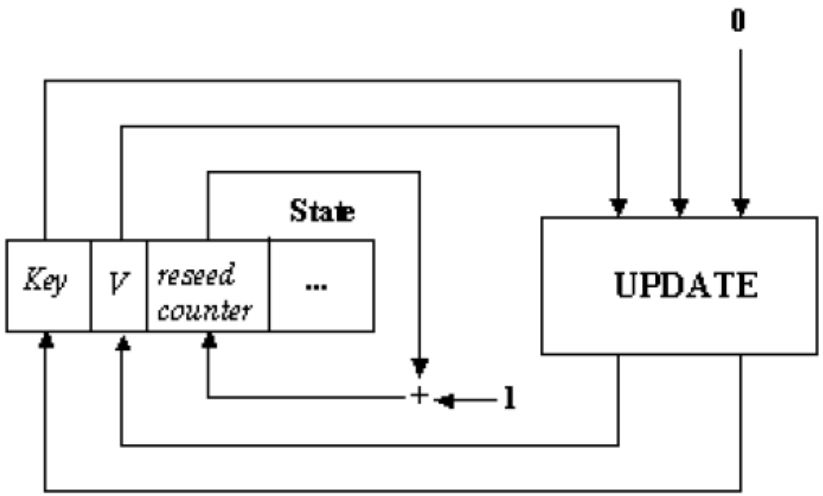




Blokk rejtjelező alapú minta







Blum-Blum-Shub generátor

The Blum-Blum-Shub PRBG is the following algorithm :

- *Generate p and q, two big Blum prime numbers.*
- $n := p \cdot q$
- *Choose $s \in_R [1, n-1]$, the random seed.*
- $x_0 := s^2 \pmod{n}$
- *The sequence is defined as $x_i := x_{i-1}^2 \pmod{n}$ and $z_i := parity(x_i)$.*
- *The output is $z_1, z_2, z_3, ...$*

where $parity(x_i)$ is defined as $R_2(x_i)$.

Let $n = p \cdot q = 7 \cdot 19 = 133$ and $s = 100$. Then we have $x_0 = 100^2 \pmod{133} = 25$. The sequence $x_1 = 25^2 \pmod{133} = 93$, $x_2 = 93^2 \pmod{133} = 4$, $x_3 = 4^2 \pmod{133} = 16$, $x_4 = 16^2 \pmod{133} = 123$ produces the output $1, 0, 0, 1$.

Problémás generátorok

MS CryptGenRandom

2007, Leo Dorrendorf et al., Hebrew University of Jerusalem and University of Haifa

Nem publikált algoritmus visszafejtése

128KByte-onként van entropy input

State kiolvasható a memóriából

Nincs backtracking resistance

Javítva:

Windows XP – Service Pack 3

Windows Vista – Service Pack 1

NIST Backdoor in Elliptical Curve DRBG

2007, Dan Shumow and Niels Ferguson, Microsoft

A görbe paraméterei lehet, hogy trükkösen vannak generálva. Ha ez igaz, akkor a trükk ismeretében az outputból a state könnyen generálható.

2013, documents released by Edward Snowden indicated that the NSA had paid RSA Security $10 million to make Dual_EC_DRBG the default in their encryption software

2014, NIST withdrew Dual EC DRBG from its draft guidance on random number generators

Problémás generátorok

PlayStation 3

2010, fail0verflow

A PS3-on futtatható kódokat hitelesítő magánkulcs megszerzése, publikálása.

Az aláírás algoritmusa (elliptic curve digital signature algorithm, ECDSA) minden aláíráshoz egyedi véletlen szám generálását igényli. Egyébként a magánkulcs előállítható.

A Sony erről megfeledkezett.

RSA publikus kulcs feltörése

2012, Lenstra, Hughes, Augier, Bos, Kleinjung, and Wachter

Néhány millió RSA publikus kulcsot (n=p*q) megvizsgálva kiderült, hogy legalább az egyik prímszám megegyezik több ezer esetben.

n1=p*q1 és n2=p*q2 esetén az lnko nem 1, hanem p. Euklideszi algoritmussal könnyen meghatározható.

Problémás generátorok

Java nonce collision

2013, Bitcoin bejelentés

Hiba a SecureRandom Java osztályban. Ismétlődések az ECDSA által igényelt véletlen számok között. A magánkulcs megszerezhető.

Ezt használta egy időben a Bitcoin Androidon. Más Bitcoinja felett lehet rendelkezni a magánkulcs megszerzésével. Több mint 50BTC veszett el. Gyorsan kijavították (nem SecureRandom-ot használ)