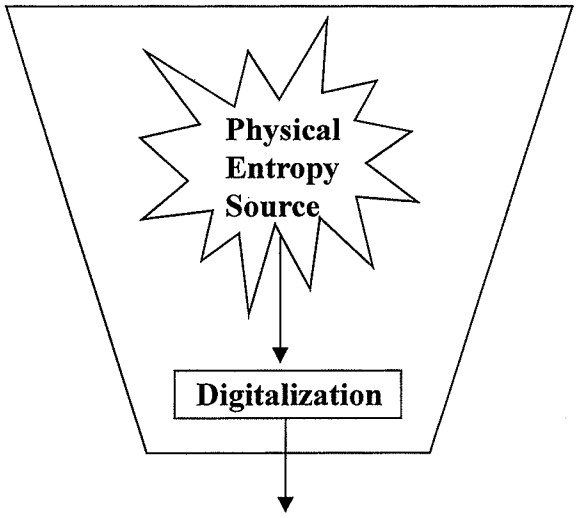
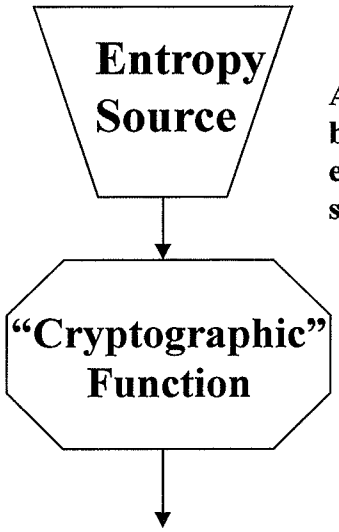
A: An Entropy Source



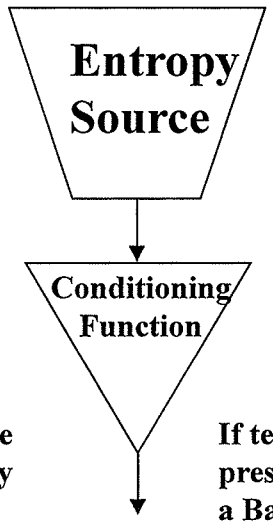
Note: The assessment has not been included here.

C: Basic NRBG with "Cryptographic" Functionality (Basic Cryptographic NRBG)



An internal state may be used to filter the entropy bits, but is not shown

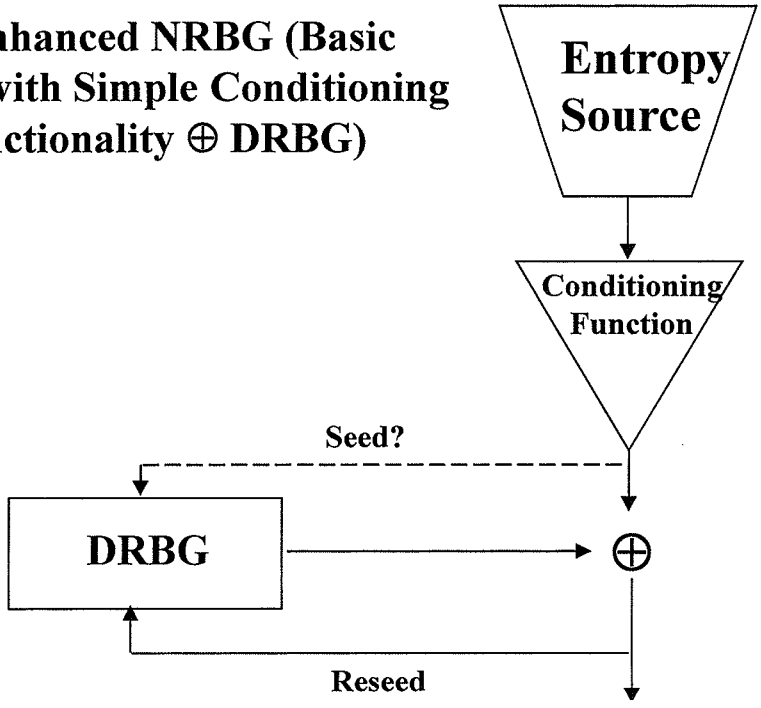
B: Simple Conditioned Entropy Functionality (Conditioned Entropy Source)



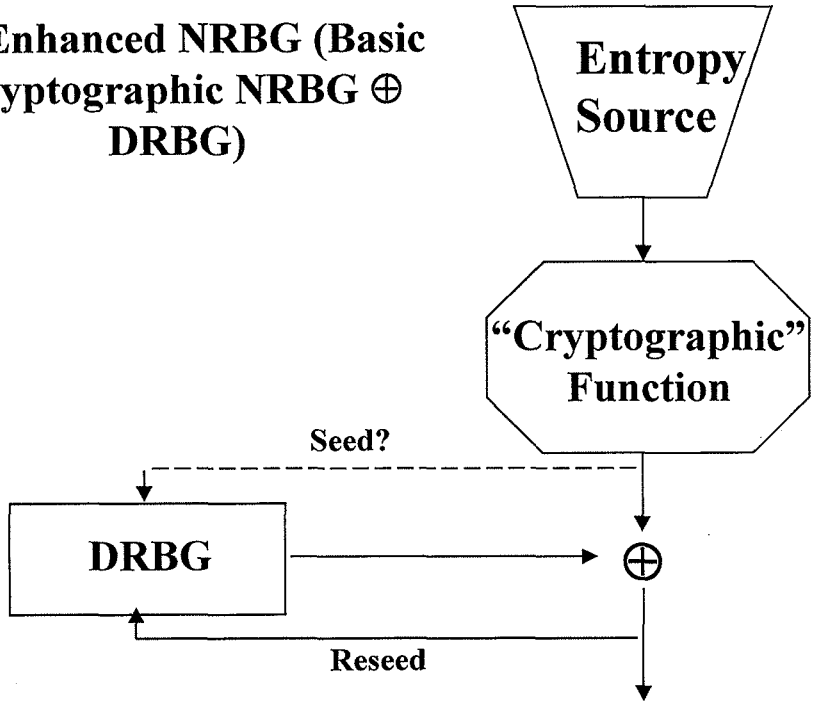
An internal state may be used to filter the entropy bits, but is not shown.

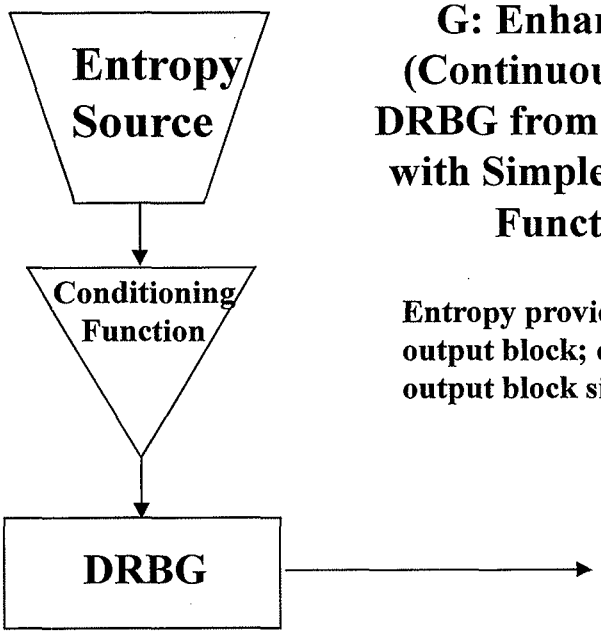
If testing and assurance are present, then this could be a Basic DRBG

D: Enhanced NRBG (Basic NRBG with Simple Conditioning Functionality ⊕ DRBG)



E: Enhanced NRBG (Basic Cryptographic NRBG ⊕ DRBG)

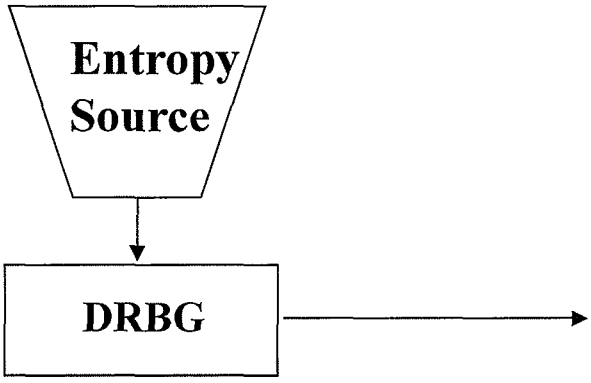




G: Enhanced NRBG (Continuously Reseeded DRBG from a Basic NRBG with Simple Conditioning Functionality)

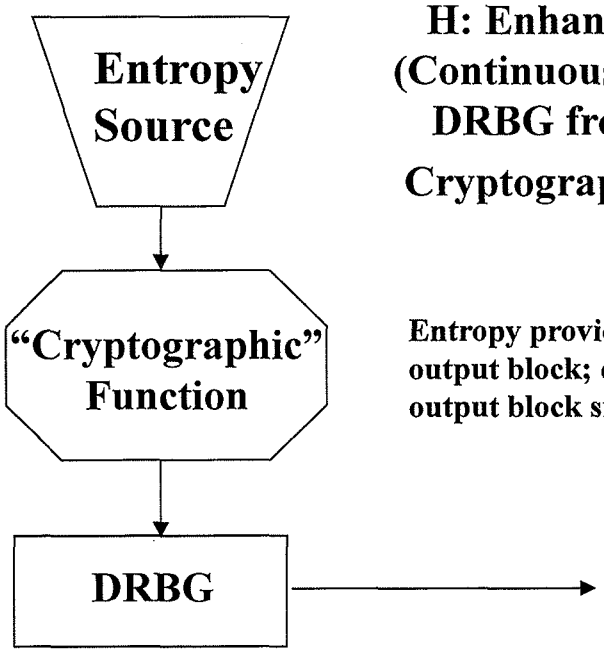
Entropy provided for each DRBG output block; entropy ≥ DRBG output block size

F: Enhanced NRBG (Continuously Reseeded DRBG from an Entropy Source)



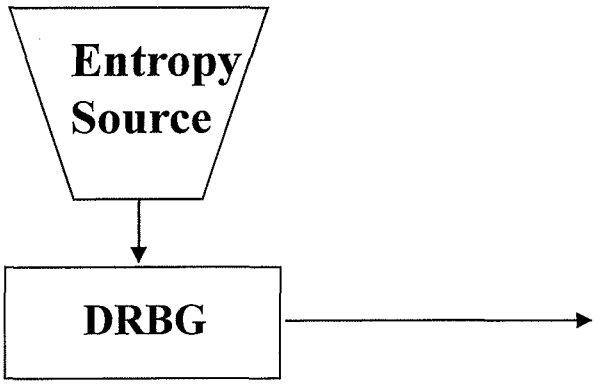
Entropy provided for each DRBG output block; entropy ≥ DRBG output block size

H: Enhanced NRBG (Continuously Reseeded DRBG from a Basic Cryptographic NRBG)



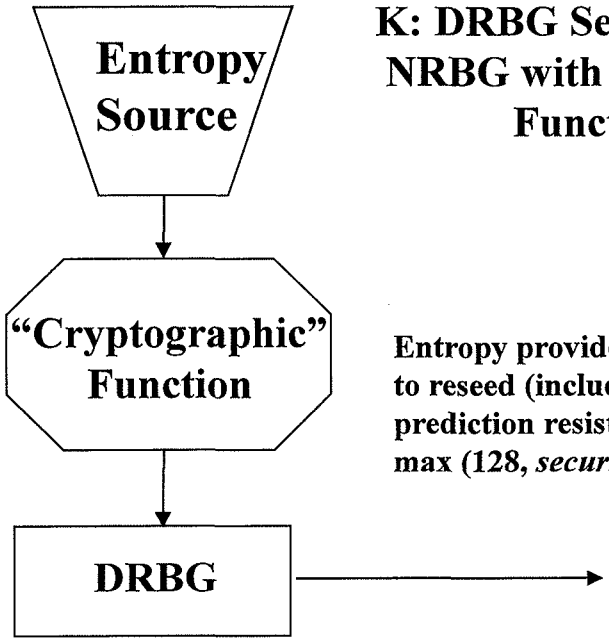
Entropy provided for each DRBG output block; entropy ≥ DRBG output block size

I: DRBG Seeded from an Entropy Source



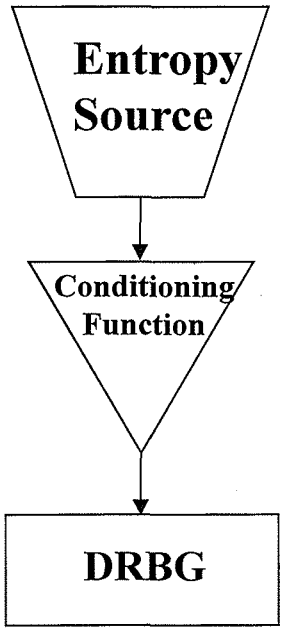
Entropy provided to instantiate and to reseed (including providing prediction resistance); entropy ≥ max (128, *security_strength*)

K: DRBG Seeded by a Basic NRBG with Cryptographic Functionality



Entropy provided to instantiate and to reseed (including providing prediction resistance); entropy ≥ max (128, *security_strength*)

J: DRBG Seeded from a Conditioned Entropy Source

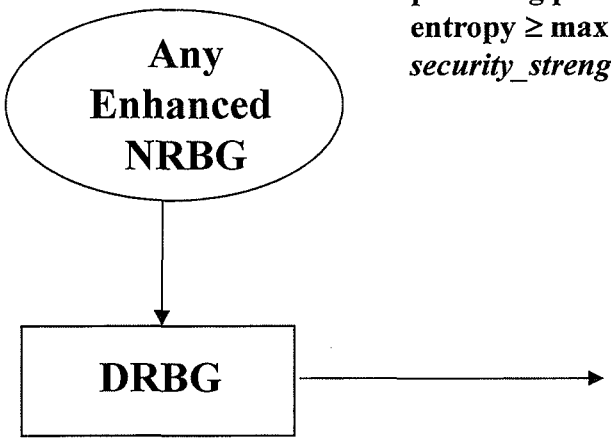


If testing and assurance are present, then the conditioned entropy source is a Basic DRBG

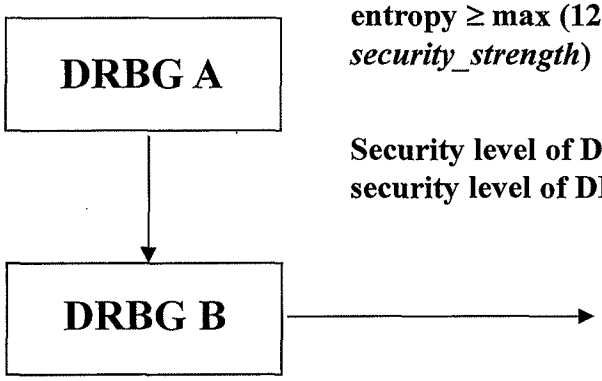
Entropy provided to instantiate and to reseed (including providing prediction resistance); entropy ≥ max (128, *security_strength*)

L: DRBG Seeded by an Enhanced NRBG

Entropy provided to instantiate and to reseed (including providing prediction resistance); entropy ≥ max (128, *security_strength*)



M: DRBG Seeded by a DRBG



Entropy provided to instantiate and to reseed (including providing prediction resistance); entropy ≥ max (128, *security_strength*)

Security level of DRBG A ≥ security level of DRBG B.

N: Approved RBG Combined with Unapproved RBG