8.7 Prediction Resistance and Backtracking Resistance

~~Each of the DRBGs specified in Section 10 has been designed to provide prediction resistance and backtracking resistance when observed from outside the DRBG boundary, given that the observer does not know the seed, or any key or state values.~~

Figure 7 depicts the sequence of DRBG states that result from a given seed. Some subset of bits from each state are used to generate pseudorandom bits upon request by a user. The following discussions will use the figure to explain backtracking and prediction resistance. Suppose a compromise occurs at $State_X$.

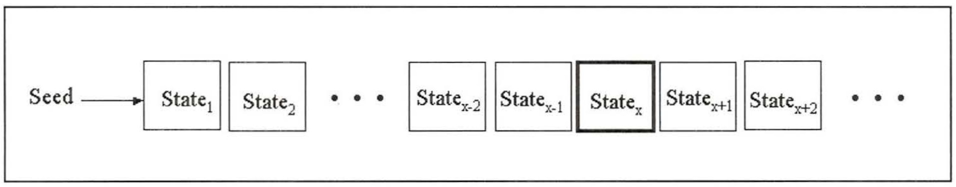

Figure 7: Sequence of DRBG States

Backtracking Resistance: *Backtracking resistance means that a compromise of the DRBG state has no effect on the security of prior outputs.* ~~If a compromise of $State_X$ occurs, *backtracking resistance* provides assurance that the output sequence resulting from states *before* $State_X$ remains secure.~~ That is, an adversary who is given access to all of~~any subset of~~ that prior output sequence cannot distinguish it from random, and as a consequence, the adversary cannot determine any bit of that prior output sequence that ~~the adversary~~he has not already seen. ~~In other words, *a compromise has no effect on the security of prior outputs.*~~

For example, suppose that an adversary knows $State_x$ ~~and also knows the output bits from $State_1$ to $State_{x-2}$.~~ Backtracking resistance means that:

a. The output bits from $State_{x-1}$ and before cannot be distinguished from random.
b. Unknown output bits from $State_{x-1}$ and before cannot be predicted.
c. Neither $State_{x-1}$ nor previous states can be recovered.

~~$State_{x-1}$ and its output bits cannot be determined from knowledge of $State_x$ (i.e., $State_x$ cannot be "backed up"). In addition, since the output bits from $State_1$ to $State_{x-2}$ appear to be random, the output bits for $State_{x-1}$ cannot be predicted from the output bits of $State_1$ to $State_{x-2}$.~~

Backtracking resistance can be provided by ensuring that the state transition function of a DRBG is a one-way function, or by regenerating an additional DRBG state from pseudorandom outputs at the end of each DRBG request.

Prediction Resistance: *Prediction resistance means that a compromise of the DRBG state has no effect on the security of future DRBG outputs.* ~~If a compromise of $State_X$ occurs,~~

Comment [jmk1]: This is not really consistent with what we define below. Backtracking and prediction resistance are only defined there for state compromises. What is being described in this paragraph is a property we always require of RBG outputs—that the current output not leak information about prior or later outputs.

Formatted

Formatted: Bullets and Numbering

Formatted

Formatted

Comment [ebb2]: This makes the definition very convoluted.

Comment [ebb3]: Need to define.

Comment [ebb4]: We already update the state once.

~~*prediction resistance* provides assurance that the output sequence resulting from states *after* the compromise remains secure.~~ That is, an adversary who is given access to all of, ~~any subset of~~ the output sequence after the compromise cannot distinguish it from random, and as a consequence, ~~an adversary~~he cannot predict any bit of that future output sequence that the adversary has not already seen. ~~In other words, *a compromise has no effect on the security of future outputs.*~~

For example, suppose that an adversary knows $State_x$: ~~and also knows the output bits from $State_{x+2}$ to $State_{x-n}$.~~ Prediction resistance means that:

a. The output bits from $State_{x+1}$ forward cannot be distinguished from an ideal random bitstring by the attacker.
b. Unknown output bits from $State_{x+1}$ forward cannot be predicted by the attacker.
c. Neither $State_{x+1}$ nor any future states can be recovered by the attacker.

~~$State_{x+1}$ and its output bits cannot be predicted from knowledge of $State_x$. In addition, because the output bits from $State_{x+2}$ to $State_{x-n}$ appear to be random, the output bits for $State_{x-1}$ cannot be determined from the output bits of $State_{x-2}$ to $State_{x-n}$.~~

Formatted: Bullets and Numbering

Formatted

Formatted

Formatted

Prediction resistance can be provided only by ensuring that a DRBG is effectively reseeded between DRBG requests. That is, an amount of entropy sufficient to support the security level of the DRBG (i.e., for *strength* bits of security, *entropy* = **max** (128, strength)) must be added to the DRBG in a way that ensures that knowledge of the current~~previous~~ DRBG state doesn't allow an adversary any useful knowledge about future DRBG states or outputs. Note that inserting less than the required amount of entropy may improve the security of the DRBG, but does not guarantee prediction resistance.