

Re: Good enough for crypto?

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-12/0362.html>

From: r.e.s. (r.s_at_XXmindspring.com)

Date: 12/06/03

Date: Sat, 06 Dec 2003 03:56:32 GMT

"Scott Wilber" wrote ...

>> "Scott Wilber" wrote ...

>>> "r.e.s." wrote ...

>>>> "Scott Wilber" wrote ...

>>>>> "r.e.s." wrote ...

>>>>>> "Scott Wilber" wrote ...

>>>>>>> "r.e.s." wrote ...

>>>>>>>> "Scott Wilber" wrote ...

>>

>>>>>>>>> *The autocorrelation function of a non-deterministic sequence will
>>>>>>>>> always decrease with increasing order. The decrease will either
>>>>>>>>> be monotonic or the function will oscillate, and the amplitude of
>>>>>>>>> the oscillations will decrease monotonically. This is proved by
>>>>>>>>> proving the behavior of the generalized autocorrelation function
>>>>>>>>> of the random process, including its measurement device
>>>>>>>>> – something I will not try to show in this setting.*

>>>>>>>>>

>>>>>>>>>> *To the best of my knowledge, this theorem on non-deterministic
>>>>>>>>>> sequences is original and has never been published before. But,
>>>>>>>>>> its a big world and if anyone has seen this before, I would like
>>>>>>>>>> to know.*

>>

>>>>>>>>> (To Scott:)

>>>>>>>>>

>>>>>>>>>> *Your "theorem" isn't true, as this counterexample shows:*

>>>>>>>>>>> $Y_i = aX_0 + bX_{i+1}$ ($a, b \neq 0$) ($i = 0, 1, 2, \dots$),

>>>>>>>>>>> *where X_0, X_1, X_2, \dots are nondegenerate iid on $\{0,1\}$.*

>>>>>>>>>>> *The autocorrelation function for the Y -sequence is*

>>>>>>>>>>> $R(0) = 1, R(k)(k > 0) = 1/(1 + b^{**2}/a^{**2}) = \text{constant}$.

>>>>>>>>>>>

>>>>>>>>>>> *The theorem relates specifically and only to non-deterministic
>>>>>>>>>>> sequences as is clearly stated. No inference may be made from this
>>>>>>>>>>> concerning deterministic generators.*

>>>>>>>>>>>

>>>>>>>>>>>> *Eh? The Y -sequence *is* non-deterministic.*

>>>>>>>>>>>>

>>>>>>>>>>>>> *Perhaps I missed the invention of algorithmic true random number*

sci.crypt: Re: Good enough for crypto?

>>>> *generators. What is the source of entropy in this generator?*
>>>>
>>>> *Your snideness is uncalled for.*
>>>> *Do you understand what nondegenerate iid random variables are?*
>>>>
>>>> *If you thought my response was snide and you didn't like it, why do*
>>>> *you think it is OK to reply in the same way?*
>>>>
>>>> *I *didn't* reply the same way. Your reference to a sum of iid*
>>>> *random variables first as being deterministic, and then again*
>>>> *as being an "algorithmic TRNG", suggested you really didn't*
>>>> *understand what they are, so I asked -- directly.*
>>>>
>>>> *Your iid sequence is a mathematical abstraction. A real, physical*
>>>> *generator, which is what I am referring to, does not spit out iid*
>>>> *random variables. The theorem relates to either continuous numbers,*
>>>> *or more typically to binary digits directly produced by a hardware*
>>>> *true random number generator. The ACF of this real sequence of bits*
>>>> *^^^^*
>>>> *can be fully described and hence its behavior over all orders.*
>>>>
>>>> *You say "this" real sequence, but of course there is no specific*
>>>> *sequence of bits. An ACF relates to a *mathematical abstraction**
>>>> *-- a probabilistic model for such sequences -- otherwise theorems*
>>>> *& proofs don't even pertain.*
>>>>
>>>> *You stated a would-be theorem about the autocorrelation functions*
>>>> *of non-deterministic sequences, without otherwise qualifying those*
>>>> *sequences. The counter-example is to what you stated.*
>>>>
>>>> *This is reminiscent of discussions*
>>>> *that confuse a "theoretical" OTP with its "realizations"*
>>>> *in practice.*
>>>>
>>>> *--r.e.s.*
>>>>
>>>> *Please educate me.*

I'll try to answer each of your questions.

> *Why is the Y-sequence non-deterministic*

It's non-deterministic because each Y_i is a non-degenerate random variable, i.e. a random variable whose distribution is not completely concentrated on a single value. IOW, it can't be a constant (with probability 1), which would have made it effectively deterministic.

> *and where do the iid random variables come from?*

sci.crypt: Re: Good enough for crypto?

They're ingredients in the usual type of random process model in which 'autocorrelation', 'variance', 'expected value', etc, are on a common probabilistic footing.

> *Again, what is their source of entropy?*

Shannon entropy is *by definition* a specific function of the relevant probability distribution — its very definition requires a probabilistic model. The entropy of a random variable is the entropy of that random variable's probability distribution; so, since X_i is distributed on $\{0,1\}$, with one of those values having probability p (say), its entropy is $p \log(1/p) + (1-p) \log(1/(1-p))$ (= 1 bit iff $p = 1/2$).

> *BTW, a theoretical ACF is not a probabilistic model, but is an exact equation that will predict the measured values of the modeled system.*

The autocorrelation function I refer to is the usual one (modulo normalization factors) in random process models — it's the expected value of a particular function of random variables in the probabilistic model.

In the (esp. engineering) literature, authors sometimes fail to distinguish between the ACF and an ACF-*estimator*. Actually it's even more confused than that, since there are three different things to be distinguished:

- (1) the ACF as described above (or its equivalent),
- (2) an *estimator* of that ACF (which is itself a sample-based random quantity — hopefully convergent to the ACF in (1)), and
- (3) the *estimated* ACF (which is the estimator as numerically "realized" in a given sample, and is specific to that sample).

> *It is only the measurements that are probabilistically distributed,*
> *and this distribution will converge to the predicted values if the*
> *model is accurate.*

To say "measurements are probabilistically distributed" is to imply that there's a probabilistic model for these measurements; specifically, in a random process model, particular measured values are regarded as "realizations" of random variables.

—r.e.s.