

Chapter 08 Repeated Words - the Efficacy of the Filtering Media in the ZK-Crypt

We review recent results which led us to new observations on the significance of the Repeated Word, RW, 32 bit word tests and the counting of differentials.

The theoretical average number of pairs of repeated 32 bit words, RWs, in 10 million perfectly random sampling of 32 bit words from a full set of all of the possible 2^{32} 32 bit words according to a Poisson calculation is 11,632 [16]. Exhaustive tests on the ZK-Crypt, RD5 and Linux number generators have shown that the Poisson estimate is slightly higher than should be expected. The ZK-Crypt filters have been judiciously chosen, and preclude use of the 32 bit Repeated Word measure to distinguish the ZK-Crypt, or to detect a distinguishing differential in any of the 32 bit state variables.

All of our tests on 32 bit state variables produced averages which are well within the smallest Standard Deviations measured on any of the 3 "competing" number generators.

We repeat previous Repeated Word, RW, results:

Bernstein's Linux (slow- probably a combination SHA-1 and RD4)	11,623 RWs.
ZK-Crypt I	12,250 RWs,
RC4	11,625 RWs.

We conducted the following RW tests, to establish the efficacy of the combiners and permutations of the ZK-Crypt.

We generated sequences, with biased and highly internally correlated operands, in an effort to maximise the correlation of successive outputs "good" Result sequences. By locking 3 of the 4 EVNN permutation signals to constant "1", we forced almost 75% of the output of the MAJ gates in the Top and Bottom Hybrid Splash Filters. As previously explained; without locking the permutation signals, the output of the MAJ filter is highly correlated. Using our standard RW test with 100 random RWs we achieved the following results.

ZK-Crypt III (locked EVNNs)- the normal procedure Cipher Mask Result- 11,630 RWs,

ZK-Crypt III (locked EVNNs)- 2 Mask Results XORed Distance 1 - 11,634 RWs.
(where each new Result was the old t'th Result XORed to the old t+1'th Result) ,

ZK-Crypt III (locked EVNNs)- 2 Mask Results XORed Distance 7 - 11,614 RWs.
(where each new Result was the old t'th Result XORed to the old t+7'th Result),

This supports our lemma; "sampling only 'distanced' Results lowers the number of RWs".

The following intermediary results are revealing.

ZK-Crypt III (locked EVNNs) Super Tier Cipher Feedback- 12,784 RWs,
the Super Tier Cipher feedback shows trace correlation,

ZK-Crypt III (locked EVNNs) Lower Feedback (Sparse Aver 4 '1's)- 8,207,387 RWs,
almost all Lower Feedback words have less than 10 '1's;

ZK-Crypt III (locked EVNNs) Super Tier concatenated nLFSRs out 11,638 RWs,
proves to be a good and necessary primitive despite the feedback;

ZK-Crypt III (locked EVNNs) Top Tier concatenated nLFSRs out 11,640 RWs,
in the TMB sanctus sanctorum;

ZK-Crypt III (locked EVNNs) Middle Tier concatenated nLFSRs out 11,630 RWs,

in the TMB sanctus sanctorum;

ZK-Crypt III (locked EVNNs) Bottom Tier concatenated nLFSRs out 11,639 RWs,
in the TMB sanctus sanctorum;

ZK-Crypt III (locked EVNNs) MAJ Filter output 4,446,490 RWs.
with mostly strongly correlated '1's.

Each of the locked EVNN tests was executed with a time consuming count of the '1's in each index bit of tested word, to detect differentials. Good RWs always pointed to words with no differentials.

Conclusion:

Trace internal correlations in word sequences are reduced by XORing said words with a sequence of highly biased internally correlated words which are not correlated to the word with trace internal correlations.

Counting the number of '1's in individual binary variables of test words quantifies a differential, but may not detect correlations between bits in a word.

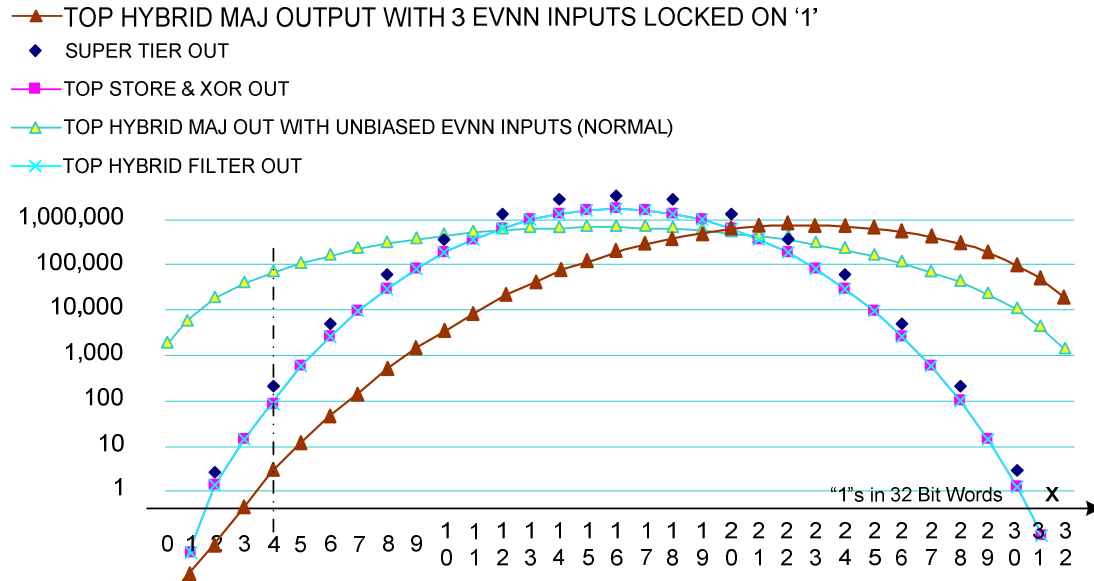
RW tests are valuable for finding differentials and correlations in word sequences.

The ZK-Crypt architecture is very robust.

Internal trace correlations typically generated about 1000 added RWs.

It will be interesting to find a π such that if we chose one index bit in all of the generated words in a test; and then change generated '1's to '0's of the chosen indexed bit with a probability of π such that the aberrated sequence will generate about 1000 added RWs.

To the previous graph of the normal dispersions of words with a given number of '1's in the 32 bit words, we have added the skewed curve of the Top Hybrid MAJ filter output with 3 EVNN inputs locked on '1'.



The Average Number of Words with X "1"s with EVNN Signals Locked and Unlocked in 10M Round Samplings
e.g., you'd find abt 6.8 Words with 4 "1"s in the output of the Top MAJ Gate with 3 EVNN signals locked on '1' ;
and about 83.2 Words with 4 "1"s in the FFs of the TOP STORE & XOR;
and 75,341 Words with 4 "1"s in the Output of the Top MAJ Gate in the Hybrid Filter;
and 166.8 words with 4 "1"s in the Output of the Super Tier (an EVNN Vector)

The above graph shows the distribution of words with 0 to 32 '1's in four classes of words in the Register Bank and Data Churn of the ZK-Crypt:

- 1) Asymptotically approaching a "perfect" random distribution of all words with no internal correlation;
- 2) Asymptotically approaching a "perfect" random distribution of all ENS (even number of '1's in a string) words with no internal correlation, equivalent to one flipped bit on half of the unconstrained occurrences;
- 3) Where each set of every fourth bit randomly has the same '1' or '0' polarity in 75% of the samples; and
- 4) Where one set of every fourth bit randomly has the same polarity 75% of the time; and the remaining three quarters of the bits are '1's in three quarters of the samples.

