

## Chapter 11 Testing - Searching for Weak Spots, Grobner Bases, Proprietary Tests

**Security evaluation and Testing;** :- Numerous Exhaustive Random, entropy, Auto and Cross Correlation, Bias, Feedback Orthogonality tests were standard practice, prior to our being joined by Nicolas Courtois, the known expert on finding vulnerabilities of highly diffused large variable systems.

The final Zk-Crypt design has excelled in ALL tests available, with results significantly beyond the required criteria.

Testing has progressed from Knuth's [knuth-2] semi-algorithmic programs, to Maurer's universal tests [maurer-92], nicely programmed with graphics in NIST's [fips 140], and finally in the ubiquitous series of DieHard tests [diehrd], the benchmark for Pseudo Random Numbers and commercial stream ciphers. With DieHard we developed present strategies, wherein we were able to progress from 7 step to single step highest quality random string generation.

We ran numerous Repeated Word tests which consists of repeatedly (with different initial conditions) counting how many 32 bit words are repeated in a 10 million 32 bit word sampling, [zk-a-z glos]. We counted '1's and '0's (to check for bias) on all state variables and logic variables in the 32 Bit Word Manipulator, in the deterministic Noise and the permuting signals from the Random Controller. Each result was better then the expected criteria (less repeated words then the calculated statistical probability).

With Courtois, we assiduously combed the design and the output statistics in search of local bias, timing basis for second order side channel attacks, and weak spots in general to be used in more rigorous types of classical differential and linear/correlation attacks which may include:

- Algebraic attacks with Grobner Bases,
- Algebraic attacks with improved ElimLin algorithms,
- Algebraic attacks with SAT solvers,
- Algebraic attacks with various generalized T' methods (proprietary),
- Embedding an impossible to detect trapdoor, and,
- Various other proprietary algebraic attacks.



AN ANNOTATED TYPICAL TEST REPORT GENERATED BY THE ZK-CRYPT DETERMINISTIC/RANDOM NOISE GENERATOR OPERATING IN SINGLE CLOCK MODE (NO RANDOM FM MODULATED OSCILLATOR)

Explanations & Circuit Diagrams in "The ZK-Crypt Noise Generator Design Parameter Emulator"

Statistical AIS-31 Analysis of ZK-Crypt Noise Source Date: 31.12.07; This particular test is for typical cryptographic applications, where we know that the QTA signal is a good pseudo-random, Data dependent source of pseudorandomness. Test Parameters Sampled Outputs: 10,000,000 Samples; Qta In the S/W emulator we replace random Data with an external Randomization of the (P)Random Slip. This is a normal test (takes our emulator about 30 seconds).

# of sampled '1's in test nodes: (see Drawings); (P)RandomClk 9218321 the missed pulse generator; NO RANDOM CLOCK -> frClk 0;

All of the following sampled Results are excellent- PROBABILITY OF 0.5 '1's das 4999256; 4'th Toggle 5000001; Juggle Splash 5000102;

Q8 4998231; Q7 5000576; Q6 4999784; Q4 5000252; Q5 4999784; Q3 4999325; Q2 4999325; Q1 4999498; Q0 4999498; A 4999657; C(3) 5000192; L(3) 5000358; L(4) 5000358; B 4999657; fff3 5000192; fff4 5000357; fff5 4999657; H 5005900; J 4996518;

Nibble Frequencies of 4th Toggle. 9 tests from Test # 15625 [ 0] 3 6 5 6 2 2 5 4 5 157766 [ 8] 3 5 9 8 7 3 5 6 9 155590 These numbers signify the total number of times the nibble occurred in 10M samples-all very close to the theoretical ideal of 156250 [ 1] 8 7 8 5 4 6 5 5 6 155668 [ 9] 3 7 3 4 5 3 2 5 6 152849 [ 2] 7 4 6 8 4 1 6 4 2 158879 [ 10] 5 5 0 4 4 7 5 3 4 157403 [ 3] 5 2 4 1 3 8 2 4 4 155184 [ 11] 9 7 6 3 9 8 5 5 3 157236 [ 4] 7 4 5 4 7 4 9 7 7 156386 [ 12] 4 4 7 4 5 2 5 3 2 154931 [ 5] 6 1 4 6 7 9 5 3 4 157514 [ 13] 5 4 1 3 5 8 8 6 3 158482 [ 6] 3 4 6 5 6 8 5 7 1 152967 [ 14] 4 6 4 6 4 4 5 9 10 155506 [ 7] 4 11 6 6 5 4 4 5 8 156319 [ 15] 4 3 6 7 3 3 4 4 6 157240 Demerit Results = 10.8 16.8 16.4 10.8 10.0 21.2 9.2 8.4 20.4

We consider a bad Demerit Result to be 50 or more, a failed statistic is 65 or more.

Nibble Frequencies of das Slip Toggle. 9 tests from Test # 15625 [ 0] 7 4 5 5 7 5 5 7 5 158545 [ 8] 9 4 5 3 4 8 2 2 8 157728 [ 1] 5 5 5 4 5 5 6 4 7 156095 [ 9] 4 5 4 6 2 5 6 5 3 152628 [ 2] 5 0 2 9 6 6 8 5 10 155636 [ 10] 7 3 3 4 0 3 4 3 8 157339 [ 3] 4 6 6 2 8 5 5 4 7 155726 [ 11] 2 5 8 0 6 7 3 9 3 157147 [ 4] 4 8 1 4 6 3 1 7 3 156879 [ 12] 5 4 6 7 3 3 5 7 6 155859 [ 5] 7 4 6 4 1 4 8 4 2 157065 [ 13] 8 6 7 3 8 5 5 1 0 154887 [ 6] 6 6 2 8 7 5 4 5 3 152744 [ 14] 3 5 10 7 4 5 4 7 3 155664 [ 7] 0 7 5 7 5 4 9 5 5 157014 [ 15] 4 8 5 7 8 7 5 5 7 158964 Demerit Results = 16.0 11.6 16.0 17.6 18.8 6.4 13.6 12.8 22.0

Nibble Frequencies of Juggle Splash Toggle. 9 tests from Test # 15625 [ 0] 5 8 4 3 3 2 5 10 5 159381 [ 8] 5 6 4 7 2 4 5 3 1 156199 [ 1] 5 7 6 8 8 9 5 4 5 155380 [ 9] 1 5 6 1 4 4 3 5 3 152335 [ 2] 8 2 5 1 7 7 4 7 6 156925 [ 10] 4 4 5 4 4 9 7 5 7 157756 [ 3] 6 8 4 6 6 7 5 2 6 155547 [ 11] 2 3 5 8 3 0 3 4 7 156467 [ 4] 3 6 8 7 6 5 4 2 4 156516 [ 12] 6 3 5 4 5 2 9 7 6 155395 [ 5] 7 6 9 6 2 1 5 4 6 157861 [ 13] 6 3 8 7 10 4 5 6 5 157014 [ 6] 5 5 2 2 3 6 2 3 2 152315 [ 14] 5 7 2 4 6 6 7 8 4 155529 [ 7] 4 2 2 8 3 8 5 5 5 155766 [ 15] 8 5 5 4 8 6 6 5 8 159534 Demerit Results = 11.2 12.0 13.2 18.0 17.2 22.8 8.8 14.4 10.4

Nibble Frequencies of Concatenated String ...||Juggle||4'thToggle||das||Juggle||4'thToggle||das||... 9 tests from Test # 46875 [ 0] 10 6 5 5 5 7 6 2 7 470492 [ 8] 3 1 3 6 1 4 2 4 2 470647 [ 1] 0 7 5 3 3 4 8 4 7 467549 [ 9] 6 5 5 7 9 8 2 2 11 465879 [ 2] 3 6 5 4 5 7 4 8 4 470587 [ 10] 10 6 5 2 4 2 7 6 2 469551 [ 3] 7 4 4 9 3 2 4 4 4 468537 [ 11] 2 3 7 3 6 9 5 7 7 467906 [ 4] 6 4 7 4 14 5 2 6 9 467957 [ 12] 9 3 5 4 6 6 4 1 7 467876 [ 5] 4 5 8 8 3 5 7 9 2 468758 [ 13] 4 7 5 4 3 3 4 5 2 469729 [ 6] 2 7 1 9 2 1 6 3 4 466378 [ 14] 1 3 5 5 2 4 9 8 2 466639 [ 7] 8 3 5 3 8 6 6 2 5 470190 [ 15] 5 10 5 4 6 7 4 9 5 471245 Demerit Results = 30.0 14.8 7.6 14.4 32.0 16.0 13.6 21.2 23.2

At each clock, the three binary signals are concatenated- so that the ideal number is 156250 x 3 = 468750

The 3 binary signals tested out beautifully, with only one sample run above 50 (55.2) all averages less than 15.1.

Demerit Distribution - Juggle Nibble Test: # FM Warning Triggers (> 50.0) 0 # Failed Strings (>65) 0 Count \*\* 0-25= 29813 \*\* 26-35= 1350 \*\* 36-45= 86 \*\* 46-55= 0 \*\* 56-65= 0 max= 44.0 av= 14.9



```

4th Toggle Nibble Test: # FM Warning Triggers (> 50.0) 0
                        # Failed Strings (>65) 0
Count ** 0-25= 29826 ** 26-35= 1360 ** 36-45= 57 ** 46-55= 6 ** 56-65= 0 max= 46.4 av= 14.8

das Nibble Test: # FM Warning Triggers (> 50.0) 1 Groups # 22274
                 # Failed Strings (>65) 0
Count ** 0-25= 29773 ** 26-35= 1337 ** 36-45= 133 ** 46-55= 5 ** 56-65= 1 max= 55.2 av= 15.0

```

The concatenated tests, just about the same- (remember 3 times the number of sampled bits) the BAD FILE records all of the warning signals. Here we see that there were 8 occurrences of Demerit Results more than 50, where interval between occurrences was at least 117 test sequences.

```

3 signal Nibble Test: # FM Warning Triggers (> 50.0) 8 Groups # 5302 26213 40475 60445 60562 67894 74322 89896
                     # Failed Strings (>65) 0
Count ** 0-25= 83540 ** 26-35= 9130 ** 36-45= 992 ** 46-55= 84 ** 56-65= 3 max= 60.8 av= 16.9

```

This result shows that there is a slight correlation between the three binary concatenated symbols. Despite the problem that was noticed only once in less than 1M samples the total average is still an enviable low 16.9, with the worst signal, which appeared once in 30M tests, of 60.8

Average Test Cumulative ( 61.6)/4 = 15.4 Max Test Demerit = 60.8  
 The unweighted average of the four tests is 15.4 – excellent, and the worst test (of 600,000,000 separate statistical measures was 15.4, the weighted average would be 15.9. The single worst test was 60.8.