



*The A to Z GUIDE to the ZK-Crypt*

AN ANNOTATED GLOSSARY & SUPPORT REFERENCE

FOR THE NIST SHA3 CONTEST & FOR COVENTURER DUE DILIGENCE

*ZK-CRYPT–THE 9.5K GATE SYMMETRIC PERIPHERAL FOR BEST OF BREED*

DUAL TRACK FEEDBACK HASH/MAC AUTHENTICATION  
WITH THE MAC MIX ANTI-COLLISION PERMUTATIONS

SINGLE STEP DUAL TRACK FEEDBACK 32 BIT STREAM CIPHERING  
WITH PAGE SYNCHRONIZATION

AIS 31 COMPATIBLE TRUE RANDOM NUMBER GENERATION  
WITH A RANDOM FREQUENCY MODULATED CLOCK  
AND ON-LINE ENTROPY MONITORING

all with LOW POWER, 32 BIT SINGLE STEP HIGH DIFFUSION  
3 GIGA BITS/SECOND at 100 MHz OPERATION

**REVISION - LOWERING CURRENT CONSUMPTION AND INCREASING SPEED**

AUTHORS: CARMİ GRESSEL  
AVI HECHT  
NICOLAS T. COURTOIS  
GREGORY BARD  
RAN GRANOT  
ORR DUNKELMAN \*

\* eSTREAM CO-SUBMITTER

Reference for "Understanding the ZK-Crypts- Ciphers for (Almost) all Reasons"

January 2009 Revision

A Reference Glossary.

Detailed drawings in the "ZK-Crypt Circuit - Concept Drawings" [zk-ccc]

<p><b>2 of 3 Majority, aka MAJ Function</b></p>	<p>The MAJ function outputs a "1" iff either 2 or 3 inputs are ones and a "0" iff either 2 or 3 of the inputs are zeroes.</p> <p>The MAJ function reduces bias iff 2 of three inputs are unbiased. The non-linear MAJ function is more robust under analysis than the linear 3 input XOR function, iff all three input signals are unbiased but slightly correlated. Typically, the MAJ output leaves traces of input bias.</p> <p>The MAJ function uses half the number of gates used by the comparable 3 in XOR function, and typically has less propagation delay.</p> <p>The 2 of 3 MAJority gate is used in high security computing to obviate false outputs caused by malfunction of one of three parallel operating computing devices. In a high security encryption system, 3 low-power ZK-Crypt engines could be operated in parallel wherein only a result where at least 2 of the 3 engines agree would be accepted Read by the Host. See [zk-ccc- Figs.T4 &amp; T5]</p>
<p><b>32 Bit Word Manipulator</b></p>	<p>The 32 Bit Word Manipulator includes the Register Bank, with the Hybrid Combiner and the Data Churn. The other two main modules are the Result/Feedback Processor and the Random Controller. [zk-ccc- Figs.A01 &amp; A02]</p>
<p><b>AIS 31 &amp; AIS 20</b></p>	<p>The BIS (German IT Standard Organization) standards for True Random Number Generators, TRNG (AIS 31); and for pseudo-random post processors (AIS 20) which receive colored random signals from a physical noise source specified in AIS 31. The AIS 31 specification explicitly demands proof of a reasonable state of randomness from the output(s) of the autonomous physical noise source before and while the TRNG generates statistically fairly uniform distributed random numbers (described by AIS31). The suggested statistical test of the output is a distance form an ideal measure of demerit, on strings of nibbles (4 bit strings). In the ZK-Crypt we also implement a test to prove constantly changing phase differences between the driving oscillator signal, <b>fr</b>, and the more stable, Host Clock, the Primary Clock; i.e., we count the number of <b>fr</b> pulses in the last positive Primary Clock pulse.</p> <p>The ZK-Crypt Noise Source consists of a random Frequency Modulated unstable ring oscillator, regulated by a random controller. See Oscillator.</p> <p>The Stream Cipher, driven by the 4 output deterministic Noise function, amply qualifies to be an excellent AIS 20 Deterministic Random Number Generator.</p>
<p><b>Biased bits</b></p>	<p>Pseudo-random string generators potentially combine devices and functions which generate specific bits in a string, or possibly all bits in a pseudo-random binary string with a predisposition to either one or zero. Herein, the principal method used is to XOR uncorrelated or poorly correlated pseudo-random bits to output less biased (debiased) bits.</p>
<p><b>Bijection</b></p>	<p>In a function <math>f</math> where <math>X \rightarrow Y</math> is one to one, i.e., each bit or nibble from <math>X</math> is imaged in a single bit or nibble of <math>Y</math> then <math>f</math> is called a bijection. The Splash Matrices and the Biham Serpent S Box used in the ZK-Crypt are bijections. DES S Boxes are not bijections. See Serpent S Box.</p>
<p><b>Birthday Attack</b></p>	<p>The birthday statistical problem asks what is the chance on a given day that two children in a classroom of <math>n</math> children will have the same birthday, assuming that births are evenly distributed over <math>H=365</math> days. The number of children in the class for the probability to be half is 22.4 from the approximation:</p> $n(0.5) \approx 1.2 \times H^{0.5}.$ <p>What is the chance of collision of a reliable random distribution with a Hash/MAC Tag/Hash value of <math>n</math> bits, a dispersion of <math>2^n</math> tags; e.g., <math>n=256</math>, <math>H=2^{256}</math>, <math>H^{0.5}=2^{128}</math>;</p> <p>on an average of about once in <math>n \approx 1.2 \times 2^{128} \approx 4 \times 10^{38}</math> attempts for two arguments <math>x_1</math> and <math>x_2</math>, the tag of <math>x_1</math> will equal the tag of <math>x_2</math>, a collision.</p> <p>To generate a collision using the Birthday Attack, a fraudster might generate a fair word file, <math>M</math>, and a fraudulent file, <math>M'</math>. Then generating variations of both files with the same meaning with equivalent words, insertions and deletions of commas, and blank lines, until she finds two files with the same Tag/Hash values. She presents one to be signed, and later replaces the equivalent of <math>M</math></p>

	with M'.
<b>Brown, Top, Middle &amp; Bottom</b>	The Brown signals activate the XOR summing of the rotated concatenation of the nLFSR pairs in the TMB Tiers. Each signal is pseudo-randomly active with a probability of about 69%, at each Primary Clock cycle. Internally, the BRN signals regulate the Brown Signals. See Tiers.
<b>Chaining Value</b>	The intermediate value that is hashed with a next input block of the message string to produce the next intermediate (chaining) value. Conventionally the input block is larger and is compressed into a smaller chaining value; wherein typically the last chaining value is the "hash-value".  In the ZK-Crypt MAC or Hash, the 32 Message Block input (assuming a single 32 bit standalone engine) is expanded into a 554 bit chaining value, which includes all binary state variables in the Random Controller, the Register Bank, the Data Churn, the Result/Feedback Processor and the 64 bit HAIFA Counter. (For a parallel paired ZK-Crypt, the chaining value is doubled.)  Compare this to conventional hash devices, where the chaining value is a compression, typically the same length as the hash value.
<b>Cipher Feedback</b>	Use of linear feedback in any pseudo-randomizing function must be used judiciously; else adversaries are able to find revealing correlations between sequences of masks. To reduce the correlation caused by normal single track feedback, the ZK-Crypt engine "recycles" two versions of feedback: 1) a sparse version to the Top, Middle and Bottom Tiers, and to the Top and Intermediate Store & XOR,; i.e., the Lower Feedback; 2) a dense rotated and reverse nibble version to the Super Tier; the Super Tier Feedback. [zk-ccc- Fig. F02] The addition of the separate Super Tier feedback produced enhanced DieHard statistics.
<b>Cipher Mask; Cipher Text</b>	The pseudo-random output of the 32 bit Word Manipulator. In the TRNG mode the Cipher Mask is the output of the ZK-Crypt; in the Cipher Mode the Cipher Mask is XORed to a clear text Message Word, to output the resulting word of Cipher text; and, in Data Authentication mode the Tag/Hash value is a concatenation of MAC mode output Cipher Masked Message words. [zk-ccc- Figs.A01 & F02]
<b>Clock Modes, Single/Dual Clock Mode</b>	There are two modes of clocking the ZK-Crypt; 1) for deterministic operation, the clocking functions are either the Host initiated Primary Clock or a synchronized derivative thereof. The (P)Random Clock drives the Control Units, and the Random Controller generated clock signals to the TMB Tiers are "occasional" missing clock signals; e.g., typically 1/12 and 1/6 missed clock, respectively. 2) for True Random Number Generation (non-deterministic) Dual Clock Mode, clocking functions are activated by the Noise Source, which is randomly driven by the FM Oscillator. (Config bit 24 = 0). See Oscillator, Dual Track Feedback. See [zk-ccc- Figs.N00, N04- N07].
<b>Collision</b>	The unexpected occurrence where a second data file and the original hash/MAC encoded data file have identical hash/tag values. A collision may be accidentally or fraudulently contrived, e.g., a modified Message where a criminal changes the amount of money in a transaction file.  We widen the scope of possible collisions to include instances where only 372 bits of the chaining value need be identical to cause a collision. The attacker is free to contrive a Message that would compensate for the false HAIFA count output diffused into the orthogonal feedback streams. We prove that this is impossible for the first $2^{62}$ Messages.  Meaningful collisions are extremely hard to generate in good HASH OR MAC functions.
<b>Complement</b>	In the binary sense, one complements zero, and zero complements one, as affected by a semiconductor inverter, i.e., a NOT gate.
<b>Confusion</b>	Shannon's original definition of permutation rules, e.g., enciphering transformations that complicate the determination of how the statistics of ciphertext depend on the statistics of plaintext.
<b>Control Units, Top, Middle &amp; Bottom</b>	Three hardware pseudo-random functions in the Random Controller driven by the (P)Random Clock, and pseudo-randomized by data from the 32 Bit Word Manipulator. Each Control Unit is loosely correlated to the tiers of the Register Bank; wherein the outputs of all three are encoded in the Permutation Encoder of the Random Controller.
<b>Correlation</b>	A measure of mutual relationship between two signals, e.g., when one clock is a derivative (e.g., divided by 4) of a second clock, the correlation of one clock to the other is the ratio of the frequencies, 4 to 1. In stream cipher parlance, a nonlinear function F is m-order correlation-immune if the mutual information between the output variable and any subset of m input variables is zero

	(statistically independent). We differentiate between auto correlation, wherein there is a discernable relation between bits in a word; e.g.; every fourth bit in the outputs of the 2 of 3 MAJ filters have the same value with a probability of 0.75. Auto correlation of 32 bit words is best measured with the Repeated Word Test; e.g., if two bits are always the same value, there is a half sized pool of numbers, and twice the number of repeated words. If bit a and bit b in the same word are with high probability of same polarity, there is inter-word correlation, which is easily detected by the Repeated Word Test.
<b>Correlation Immunity</b>	We say that an output is correlation immune, or maximum correlation immune, if practically no information is leaked from the input (either the stage of an nLFSR or a Message word) to the output, (either the mask output or to the XORed Message to mask output).
<b>Corrupt</b>	Because of the high diffusion in the ZK-Crypt, a single bit change in a valid Message affects, in the first clock, the equations of more than 140 state variables in 32 Bit Word Manipulator, and all of the variables in the Cipher Mask, in a way that cannot be reconciled.
<b>Cryptanalysis; Cryptanalysts Cryptographers</b>	<p>Cryptanalysis is the sister of cryptography in the science of cryptology that deals with analyzing what cryptographers design, to find weaknesses or attributes that lead to finding weaknesses, in the processing of learning the secrets of a cipher A Cryptanalyst, as Nechtaval in Contemporary Cryptology defines succinctly, "is a would-be intruder into a cryptosystem".</p> <p>A reasonable analog of cryptographers and cryptanalysts, and their particular priorities can be found in a riddle in Royt's Mother Goose Rhymes, circa 1930; "What is it that Dutch children like making that English children like breaking?" Answer: toys. How times have changed!</p>
<b>Data Churn</b>	<p>That part of the ZK-Crypt which processes the unpredictably rotated and MAJ/3XOR filtered combined output from the four 32 bit tiers of the Register Bank.</p> <p>The churning operations consist of two pseudo-randomly stepped 4 rule (Splash) Matrix displacements; Random Controller's (EVNN) MAJ regulated diffusion of two Matrix bit outputs XORed to two other Matrix bit outputs; and three Store &amp; XOR decorrelation filters. The output of the Data Churn is the Bottom Store &amp; XOR/Cipher Mask See [zk-ccc- Figs. A01, R13 &amp;T1].</p>
<b>Debias</b>	In pseudo-random functions the binary output strings typically locally have a tendency to either "1" or "0". The balance of "1"s and "0"s are generally improved if two uncorrelated signals are XORed to produce a third output signal. XORing two uncorrelated biased bits typically is the most cost effective way of reducing bias. See Biased Bits.
<b>Digest (verb) Digest, Message Digest (nouns)</b>	<p>We call the process of pseudo-randomly compressing a stream of Message Words into the variables of the ZK-Crypt a digesting sequence.</p> <p>The output Tag/Hash value is also called a Message Digest of the input Message Words. See Tag.</p>
<b>Diffusion</b>	<p>The affect of one variable on a number of dependent variables, such that it causes a linear and/or a non-linear change of output in a plurality of dependent variables; preferably affecting disparate sources of change.</p> <p>The ZK-Crypt's unique structure guarantees rapid and massive diffusion of every single complemented variable.</p> <p>Note the diffusion analysis [zk-secure app 4] of the ZK-Crypt where a minimum of 144 state variable equations are effected by a single flipped bit in a Message Word.</p>
<b>Divide and Conquer or the Meet in the Middle Attack</b>	<p>The process of parsing a function into parts that are loosely interactive, where all of (generally the smaller) part's stages are mapped into memory and the second larger section exhaustively tested against each combination of the memory mapped generally smaller part, such that in practice only the number of trials of the larger part are relevant.</p> <p>The ZK-Crypt Cipher is "susceptible" to a Divide and Conquer attack, as the controller has 61 internal binary variables and 10 variable inputs, and the 32 Bit Word Manipulator has 288 (cipher) binary variables and 10 external inputs.</p>
<b>DPA Differential Power Analysis</b>	The name given by Kocher et al in "Cryptography Research International" for refined side channel attacks. The CRI methods are primarily based on monitoring aberrations of chip power to learn secret cryptographic keys. The ZK-Crypt submitters have extensive successful experience

<b>(Attack)</b>	defending public key designs from side channels previous to CRI's first issued patents, and have written patented algorithms which accelerate and preclude side channel attacks. See Side Channel.
<b>Dual Track Feedback</b>	Conventional feedback procedures are shunned in RNG designs because of inferior statistics, generally attributed to forced correlation of output stages (the cipher masks); despite the fact that judicial feedback potentially increases crypto-complexity.  In the ZK-Crypt, in both the Cipher Feedback and the MAC Feedback modes the feedback sources and permutations of each of the feedback words are diverse, and affect different portions of the Register Bank and Data Churn in grossly different ways. The MAC mode feedback streams are orthogonal. See [zk-ccc Figs. B01, & F02], Cipher Feedback and MAC Feedback.
<b>Engine</b>	We refer to the interacting modules, i.e., the Random Controller, the 32 Bit Word Manipulator and the Result/Feedback Processor as the Engine. See [zk-ccc Fig. A01]
<b>Entropy</b>	In the random binary string context, a comparative measure of confusion or divergence from a predictable sequence, or a part thereof. Simply stated, entropy signifies a degree of "unpredictability".  Entropy is only one (possible) measure of true randomness.  For long lasting proof of entropy in random number generation; (where the processing and compressing of a noise source is valid and the subsequent processor may be weak) reference the AIS 31 Standard Noise Source "on-line measurements". The ZK-Noise Source (AIS 31 compliant) generates 4 serial streams of "on-line monitored entropy", to drive the Cipher module which is a Deterministic Random Number generator. The ZK-Crypt phase differential test proves wandering phase difference between the Primary Clock and the random FM Clock, and typically reduces the necessary large number of AIS 31 "Tests of Demerit".
<b>Even Number String ENS</b>	A binary string in a Word consisting of an even number of binary bits, wherein the number of "0" bits is an even number, and, conversely, the number of "1" bits is also an even number; e.g., a 32 bit Word with 14 one bits and 18 zero bits in any permutation would be an Even Number String. Obviously, only one half of the possible $2^{32}$ bit combinations are Even Number Strings.  If any 32 bit word, X, is bit wise displaced into a second 32 bit Word, Y, where the result R is X XOR Y; R is always an Even Number String. The output of a triple ENS string 3XOR input is and ENS. The output of a triple ENS string 3XOR input is and ENS. The output of a triple ENS string MAJ input may or may not be an ENS.  Each of the XORed tier rotational permutations outputs ENSs only.  See Odd Number String, ONS. .
<b>EVNN, MAJ Regulators</b>	See [zk-ccc Figs. T3 & T4]. There are four regulating vectors of Splash Matrix output MAJ gates, where each vector activates 8 indexed interspersed MAJ combiners. Each EVNN regulated MAJ combiner diffuses two Splash Matrix output bits into an XOR of the central indexed Splash bit; alongside the adjacent right hand Splash output bit.  Three EVNN selects are debiased signals emanating from the TOP, MID and BOT Control Unit Configuration outputs; the EVNN Fourth Toggle vector is controlled directly by the Random Clock module of [zk-ccc Figs. 4x.]
<b>Exhaustive Search Brute Force</b>	A well designed stream cipher is most efficiently compromised (the secret key extracted) by conducting an orderly exhaustive or brute force search, over all, or most of the possible range of secret keys. The ZK-Crypt SHA3 submission is for cipher key lengths from 160 to 768 bits. Key extensions are arbitrary- wherein only the first four key words are loaded directly into ZK-Crypt engine, and all additional words are "hashed" into the engine via the Message Word input. Any exhaustive key search attack would be unfeasible.
<b>FB, Feedback</b>	In a closed loop system, any of a variety of functions which recycle an output value into a function that will have an affect on an input value. See LFSRs, Lower Feedback, Super Tier Feedback, Cipher Feedback, and MAC Feedback.
<b>Finite State Machine, FSM</b>	A sequencing controlling mechanism consisting of combinational logic, a clock and memory elements determining a finite number of states wherein a given input state causes a transition to a defined output state. The ZK-Crypt can be operated by the FortressGB designed hardware FSM with extended functionality necessary for most efficient single step direct memory access functions, which are not included in the present core, see the proposed concept in [zk-ccc Fig. A03].

	<p>It is anticipated that most first generation implementations will be operated directly from the Host Interface described in [zk-ccc Fig. A00], without an FSM.</p>
<p><b>fr</b> <b>2fr</b></p>	<p><b>fr</b> is the shaped output of the randomly frequency modulated ring oscillator AIS-31 compatible noise source used for driving the ZK-Crypt in TRNG mode. <b>2fr</b> is the real output of the oscillator, prior to being divided by 2 and "shaped" by a toggle flip flop. See [zk-ccc- Figs.N00 – N07].</p>
<p><b>Flip-Flop (FF) – Types D, T &amp; SR</b></p>	<p>An electronic memory cell, capable of maintaining two stable output states, one or zero on outputs Q and Q NOT. Synchronous (clock activated) flip-flops used in the ZK-Crypt, are Data (D type) and Toggle (T type). In the D flip-flop, the input at the D connection appearing immediately before an activating clock cycle is Sampled and transferred to the output, Q. In the T (Toggle) flip-flop configuration, the output is a polarity change from the previous output. When the T input is a one, and a clock signal activates the flip-flop, the previous polarities of Q and Q NOT are reversed. Clock activation is activated by a rise in the voltage of the clock signal, denoted in the figures by a direct connection of the input to the clock connection; or by the fall in voltage of the input clock signal, denoted by a small circle adjacent to the clock input connection of the flip-flop. SR flip-flops are asynchronous devices, as they are activated at pseudo-random instants, and not stepped by a system Primary Clocking device. An activation voltage on the S input causes a stable one (a set) on the output, Q. Activation of the R input (often marked CLR or Clear), causes a stable zero (a reset) on the output, Q. Flip-flops have an optional second output Q Not, symbolized by a Q under a horizontal dash. A D type flip-flop, with the inverted Q NOT output connected to its D input, toggles the output, at each activating clock signal. D, T and SR flip-flops are used in Stream Ciphers and Random Number Generators. Emulation of such devices is immediate in software implementations.</p> <p>Synchronizing large strings of flip-flops is often an arduous task, and designers take the easier way out by adding an Enable input, which means that the flip-flop is internally activated, despite the fact that it does not sense changing data on its input. Energy can be reduced by about 35% if flip-flops are only clocked when they are logically driven. This is facilitated by fine tuning the synchronization of the logic gated clock trees.</p> <p>All ZK-Crypt binary variables are stored in flip-flops. Flip-flops account for almost one half of the electronic gates.</p> <p>In non-secured difficult to test systems, the standard test method, JTAG, is to execute a serial scan of all flip-flops, which entails an additional minimum of two gates on every flip-flop. Fortress' experience has been that reputable manufacturers do not allow scanning procedures in secured modules. Simple probes can often divulge all hidden secrets. The ZK-Crypt and similar devices are easily tested with tailored test sequences, because of the constant interaction of virtually all gates and variables.</p>
<p><b>HAIFA</b></p>	<p>"A Framework for Iterative Hash Functions" suggested by Eli Biham and Orr Dunkelman, designed essentially to strengthen conventional hash devices based on block ciphers. The framework included "salt" aberrations, similar to IVs or non-secret encryption keys as seen in the ZK-Crypt and a counter which extends the normal compressed chain value.</p> <p>The HAIFA counter consists of a concatenation of Mersenne prime LFSRs lengths 7, 13, 17 and 19, an extended 2 celled LFSR, and a six bit binary up-counter.</p> <p>In the ZK-Crypt, outputs bits of the 64 bit HAIFA Counter are disbursed and linearly summed into the Super Tier and Lower Feedback words. The essential purpose of the HAIFA counter is to prevent multiple collisions, and herded sections of data with replicated sections of data. [zk-ccc- Figs. H0-H03B].</p>
<p><b>Hash</b></p>	<p>A Hash function is typically an efficient one-way compression of longer binary strings into fixed length strings, typically called hash-values (for hashes, keyed hashes or MACs), or tags (typically for keyed hashes or MACs). In such data authentication systems, a user must be reasonably assured that any change in the binary input string, large or small, will render a false hash value. Typically, hash functions do not involve secrets, are publicly known, and a potential attacker knows fully the process of compression. The hash value, to be checked against the single value previously known hash value of the original binary string, is designed to reasonably assure a user of the authenticity of the data. A hash function, in which a secret key is used to initiate the apparatus, enables a user who knows both the secret key and the true hash-value to determine the</p>

	<p>integrity and, with a level of assurance, the origin of the "hashed" data. An apparatus with a secret key is typically classified as a MAC, a Message Authentication Code; or an HMAC, a Hashed MAC.</p>
<p><b>Hybrid Filter</b></p>	<p>Diffusing Non-Linear component configurations (MAJ, CARRY and AND) typically exaggerate the input bias. The XORed bias of a result of two inputs is typically less biased than either of the input bits, only assuming that there is no noticeable correlation between the inputs. The 2 of 3 MAJ filter typically lengthens string lengths; e.g., if an output bit is a '1', with a probability of about 0.73, the next near neighbor output bit will be a '1'.</p> <p>A single cell of the Hybrid Filter which accepts 4 variable bits from the Splash Matrix diffused output is a MAJ/XORed result caused by 4 bits from the input of the Splash Matrix, and one of 4 bits inputs from the Random Controller. Both Top &amp; Bottom Splash Matrix - Hybrid Filters are input into correlation immunizing Store &amp; XOR filters. See [zk-ccc Figs T3-T5].</p>
<p><b>Images of nLFSR Outputs</b></p>	<p>In the first designs the XORed outputs of the TMB pairs of nLFSRs showed blatant signs of auto correlation. Intuitively this is easy to understand, as more than half of the bits advancing from left to right retain the same value. Bits between taps in One to Many nLFSRs always retain the same value, and on one half of the clock signals, the internal SR feedback (Slip XOR MS cell output) is a zero, thereby increasing the occurrence of the <math>t</math> i'th bit being the same as the <math>t+1, i+1</math>'th bit. DieHard and other tests sensed this correlation, but the Repeated Word test were the most obvious and sensitive test for this type of correlation.</p> <p>The first solution was to generate a Brownian motion type Image, where bits from each tier would go from right to left, each with a different displacement. The Images (like the new Images) were XOR combined to their progenitor nLFSR pairs to produce the tier output. Statistics were appreciably improved. Subsequently, instead of the random "Brownian" movement, each Register Tier output was left rotated a different odd number of stages; i.e., more compact hardware and especially software implementation. In the ZK-Crypt the TMB Images are randomly combined to the progenitor nLFSRs.</p>
<p><b>Initial Value, IV Initial Vector</b></p>	<p>Starting from an identical initial condition, in Cipher Mode, the Cipher Mask generates a single valued deterministic sequence. An adversary who could record a cipher text transmission and could learn the value of the deciphered clear text could record the sequence of secret masked values, and later decipher all data sent using the same secret key. Hence, after loading secret keys, we encode a "nonce", a one-time value per message as an IV, such that the given data is uniquely encoded. See nonce. See [zk-ccc- Fig. B06].</p>
<p><b>Intractable</b></p>	<p>The assumption that accurate estimation or prediction is unfeasible using known methods. With 382/764 binary variables (single or concatenated engine), and secret keys up to 368/768 bits long, compromising the ZK-Crypt is considered an intractable exercise.</p>
<p><b>Least Significant, LS &amp; Most Significant, MS, LFSR &amp; nLFSR representation</b></p>	<p>In normal binary representations, the Least Significant, LS, bit (lowest power bit) is on the right hand side, and the Most Significant, MS, bit (highest power bit) is on the left hand side of the binary word.</p> <p>Circuit diagrams, including binary counters and shift register representations in the literature typically depict signal inputs with movement oriented from left to right, with the output and MS bit on the right. In typical descriptions in the literature, and in this document, cells of registers and counters are numerated from left to right, where the LS cell is on the left, and the MS cell on the right. In the tier, counter and shift register representations in this document, the LS bit, denoted the zero bit, is on the left, and the MS bit of an <math>n</math> bit device, denoted the <math>n-1</math>'th bit of the device is the rightmost bit.</p>
<p><b>Linear Feedback Shift Register – LFSR</b></p>	<p>A clocked shift register device assembled from D type flip-flops with feedbacks taps drawn from defined pairs of flip-flops in the register, or in a second class, with XORs placed between flip-flops of the registers.</p> <p>There are two general classes of LFSRs, One to Many, (Galois) and Many to One (Fibonacci). In a Many to One sequence, outputs from a plurality of taps from a shift register are XORed to the output of the feedback flip-flop which is returned to the input of the first "left hand" flip-flop. In a One to Many configuration, the output of the last flip-flop of the register is fed into specific XOR gates (taps) placed between register flip-flops and also fed into the first leftmost flip-flop.</p> <p>The LFSR is a linear device, as for each configuration of the LFSR, a given word on the outputs of each of the registers, leads to a next defined output of the register, such that the <math>n</math> bit word sequences are cyclically repeated, when the clock is continuously clocked. An all zero word is the</p>

	<p>unacceptable sequence in an LFSR configuration, as 0 XOR 0 equals zero. At the all zero stage the LFSR is stuck in a sequence syndrome (Stuck on Zero Syndrome) of zero in and zero out. The only input to an LFSR is the clock or stepper.</p> <p>An n bit LFSR has a cyclic sequence of <math>2^n - 1</math> bits. An observer who learns a string of 2n bits of the sequence can recreate the whole sequence and can compute the configuration of the LFSR.</p> <p>Different feedback configurations from same length maximum sequence length registers produce all of the same elements of the sequence, but in a different sequential order.</p> <p>Adjacent stages of One to Many LFSRs appear to have more "local" entropy than adjacent stages of Many to One LFSRs, to an observer who has no knowledge of the generating LFSR devices.</p>
<p><b>Lower Feedback, Lower Feedback Register</b></p>	<p>In the ZK-Crypt, the recycled Lower Feedback word is XORed without rotation into the TOP, MID and BOT tiers of the Data Register Bank, and with 13 right and 7 bit left rotation into the Top and Intermediate Store &amp; XOR registers. See [zk-ccc Figs. B01 &amp; F02].</p>
<p><b>MAC (or Hash Feedback</b></p>	<p>As opposed to Cipher Feedback strategy wherein feedback must be used judiciously, for Data Authentication coding, massive diffusion and extremely strong (absolute) correlation between the "Message" and the previous and future states of the encoding device is mandatory.</p> <p>Therefore the Hash or MAC feedback stored in the Lower Feedback Store is the XOR sum of the Present and Previous Cipher Mask XORed to the XOR sum of the Present and Previous Message Word.</p> <p>In the previous ZK-Crypt II this feedback is recirculated to all tiers of the Register Bank and to the Top and Intermediate Store &amp; XORs.</p> <p>In the ZK-Crypt, the Super Tier Hash or MAC feedback consists of a MAC MIX version of the Message Feedback XORed to the SuperMIX transformation of two internal Data Churn words. See [zk-ccc Figs. B01 &amp; F02].</p>
<p><b>MAC Message Authentication Code</b></p>	<p>MAC or HMAC, Message Authentication Coding or more exact Data Authentication Coding is a secret keyed one way function process for uniquely compressing a large concatenation of binary words into a shorter binary string, a Tag/Hash value. The Tag/Hash value is a unique trace on the contents, such that the chance of two inputs causing an identical Tag/Hash value, a collision, caused by an adversary or fault, is practically non-existent. See [zk-ccc- Figs.31HMAC].</p>
<p><b>MAC MIX</b></p>	<p>The <math>f_{MMM}</math> transformation where each nibble's bits are reversed, <math>WXYZ \rightarrow ZYXW</math>.</p> <p>The <math>f_{MMM}[x]</math> is used in Data Authentication in the ZK-Crypt Super Tier Feedback track to thwart Message modifications which produce valid Tag/Hash values.</p> <p>If we designate the 32 word input bits to the MAC MIX transformation- [ABCD EFGH JKLM NPQR STUV WXYZ abcd efgh];</p> <p>then the MMX displacement affected by the <math>f_{MMX}</math>- <math>f_{MMX}[ABCD EFGH JKLM NPQR STUV WXYZ abcd efgh]</math> outputs the displacement- MMX=[DCBA HGFE MLKJ RQPN VUTS ZYXW dcba hgfe].</p> <p>See [zk-ccc Fig. F11].</p> <p>In the previous ZK-Crypt II, contrived Message Words in the linear Lower MAC feedback loop could completely control the feedback words recycled to the Top, Middle and Bottom Tiers and to the Data Churn, such that in certain instances the status of their nLFSRs and their data stores can be reconciled to a valid condition following a fraudulent Message word.</p> <p>In the ZK-Crypt, the MAC MIX scatters both the fraudulent Message Word's false bits and the modified word's complemented bits intended to reconcile the aberrations in the lower tiers and the Data Churn in the Super Tier's feedback. Such an action serves to amplify the aberrations of the first fraudulent word in the Data Churn.</p> <p>The four bit transformation <math>WXYZ \rightarrow ZYXW</math> is doubly relevant as the Feedback Vectors typically relate to moving bits, e.g., in nLFSRs, such that the Z bit in the first clock cycle affects the left most</p>

	cell of the present nibble, and at the next clock cycle affects the right most cell of the adjacent nibble.
<b>MAJority Function</b>	See 2 of 3 Majority function. (First entry in the table).
<b>Many to One nLFSR &amp; LFSR aka Fibonacci</b>	<p>The conventional configuration of maximum length feedback registers, wherein pairs of tapped junctions between flip-flops are XORed together to produce the feedback signal. See also One to Many nLFSRs. In some designs these shift register configurations are referred to as Fibonacci, no relation to the rabbit propagation function. The Control Unit shift registers are aberrated by random slip pulses.</p> <p>The nLFSRs in the TMB Control Units are Many to One, . See [zk-ccc- Figs. P02-P04]</p>
<b>Mask Cipher Mask</b>	<p>The pseudo-random, deterministic, intractably unpredictable output of the Bottom Store &amp; XOR Non-Linear Correlation-Immunizing Combiner is the mask which encrypts the Message Word into cipher text when XORed to the plain text Message word and decrypts the cipher text when XORed to the cipher text. The Mask encodes the message in Data Authentication.</p> <p>The Mask is generated by the running key. In the MAC feedback mode, the Mask XORed to the Message is recycled into the Register Bank, and is diffused into subsequent Masks. See [zk-ccc- Fig. A01].</p>
<b>Mask Decorrelator Shifter</b>	To insure that the Cipher Mask would have minimal internal correlation, two buffers were added, relevant to testing wherein it was found that the final output should be a result of a "back dated" internal intermediate Data Churn Value, and a Last Result. [zk-ccc Fig T06]
<b>Mask\HAIFA\ Page Counter</b>	<p>The Mask/Page/HAIFA Counter is a 64 bit combination Mersenne prime LFSRs/6 bit –of the 10 bit up-counter used to salt the Super and Lower Feedback Stores. The 10 bits of the up-counter can be read on Port D.</p> <p>In the Cipher Mode the counter's comparator transmits interrupts at Page Ends. The counter can be read on Port D. The page count is used for indexing packets transmitted over varied delay channels, wherein packets may not arrive in proper order.</p> <p>In both MAC and Cipher mode, the 64 bit output of the counter is dispersed and XOR summed into both the Super Tier and the Lower Feedback stores, to provably preclude collisions. See [zk-ccc- Figs. H03-H04]</p> <p>In the TRNG mode the Counter records the number of <b>fr</b> (autonomous oscillator) pulses recorded in the first half of each Primary (sampling) Clock cycle. If the recorded number is different on sequential Primary Clock intervals, we are assured that there is a wandering random phase difference between the <b>fr</b> clock and the Primary Clock, the ultimate source of entropy in the noise source. Only six bits of the counter are active in the TRNG mode, as it is doubted that the <b>fr</b> oscillator will not be accelerated to more than 10 times the frequency of the Primary Clock. See [zk-ccc- Figs.B08 &amp; H00].</p>
<b>Message Word, message</b>	We refer to a typically longer than 32 bit data input operand as a message (small "m"). We conventionally refer to the 32 bit operand that is encrypted for transmission and decrypted at reception, (typically XORed to the Cipher Mask) as a Message Word, (capital"M").
<b>Multipermutation</b>	A concept for designing hashes based on many pseudorandom function building blocks, causing massive diffusion in the state space [Vaudenay] and C. Schnorr. We say that the ZK-Crypt is an extension of the original 1995 concept.
<b>Multi-Step Mode</b>	<p>An option in the FortressGB FSM, wherein a Host defined number of unread Sampled operations (scrambles) is performed, prior to a read-out Sample which is returned to the Host. See Wait &amp; Read.</p> <p>Circuit concept in [zk-ccc- Fig. A03].</p>
<b>NFIX Gate</b>	<p>The FortressGB implementation of the de Bruijn nLFSR configuration, where a string of n-1 LS zeroes forces a "1" into the feedback function. The NFIX gate senses and outputs a "1", if the n-1 LS outputs of an n bit nLFSR are zero. If the MS bit of the nLFSR is a "1", the next stage of the nLFSR will be the all "0" value. If the MS bit is a "0" the next stage will be "0"s interspersed with "1"s at the output of each feedback tap. This increases the length of an uninterrupted cycle to include the <b>n</b> all zero stage, with a perfect balance of "0"s and "1"s.</p> <p>The NFIX gate has been removed from the nLFSRs in the Register Bank, as it is redundant in normal use where Lower and Super Tier Feedbacks are hardwired, and the Global Key/IV (Re)set automatically loads an MS '1' into all nLFSRs. In the Register Bank the NFIX propagation would have been in the critical propagation path, degrading maximum throughput.</p>

	<p>It is valuable in the nLFSRs of the TMB Control Units, which may, in some instances sustain a long sequence of all zeroes.</p> <p>See Stuck on Zero.</p>
<b>nLFSRs</b>	<p>The so called nLFSRs in the Register Bank which receive linear and non-linear feedback should now be called pseudo linear feedback shift registers, as their internal feedback mechanism no longer defines a sequence of stages in said registers; e.g., the Lower and Super Tier 32 bit feedback is a more dominant mask on the stages of the so called shift registers.</p> <p>The nLFSRs in the Random Controller are true non-linear feedback registers, dominated by the non-linear Slip and NFIX functions. See non Linear Feedback Shift Registers.</p>
<b>Nonce</b>	<p>A nonce is a value used only once. The IV used in a cipher should be a nonce. A counter is an acceptable paradigm for a nonce. We suggest using true random numbers, generated by the users as part of the initialization process.</p>
<b>Non-linear Functions (in the ZK-Crypts)</b>	<p>The AND function is the simplest non-linear function, where the change of a single input into the AND logic gate may or may not change the gate output. The Carry (adder) gate is often used in older ciphers, but not in the present ZK-Crypt offering. The non-linear MAJ function is the ubiquitous non-linear module in the ZK-Crypts. Non-linear functions MAJ and Carry exaggerate bias of input bits, in their outputs.</p> <p>The MAJ filter is the principal non-linear function in the ZK-Crypts. The non-linearity of the ZK-Crypt nLFSRs is provided by Slips, random Imaging, and erratic clocking.</p>
<b>Noise Source</b>	<p>In Cipher and MAC modes, the quadruple outputs of the ZK-Crypt permutation clocking mechanism is a deterministic noise source with measured statistics, remotely affected by the Register Bank binary variables.</p> <p>True Random Number Generators consist of two essential parts (see AIS 31 standard), a noise source and a post processor, wherein the Noise Source injects "entropy", aka unpredictability, into the post processor.</p> <p>To be compliant to the AIS 31 standard, a noise source must include a test mechanism that proves, on-line while generating random strings, that the source generates acceptable random distributions of 4 bit nibbles.</p> <p>The ZK-Crypt noise source has two modes of operation. In deterministic, Single Clock operation all clock steppers operate at frequencies which are derivatives of the Host supplied Primary Clock. In TRNG Dual Clock mode, the phase differences between a randomized Frequency Modulated oscillator and the Host supplied Primary Clock, sampled after random delays, is the source of physically generated random noise and the clocking of the Top, Mid and Bot Control Units. See [zk-ccc- Figs.N01 &amp; N04-N06].</p>
<b>Nonlinear Feedback Shift Registers, nLFSRs</b>	<p>Linear Feedback Shift Register configurations where the logic state of the cells is not the only condition that determines the next value of the register. The linear logic that affects the ZK-Crypt nLFSRs in Cipher and MAC mode includes the Slip signals; erratic tier and Image clocking; and dense unpredictable feedback. [zk-ccc- Figs. P02-P04, R01-R02 &amp; R04-R09].</p>
<b>Odd Number String, ONS</b>	<p>In a string with an even number of bits; e.g., a 32 bit word, with an odd number of "1" bits, and conversely an odd number of "0" bits. See ENS.</p>
<b>One to Many nLFSR aka Galois nLFSR</b>	<p>Conventional linear and non-linear feedback shift registers in the literature are configured as many to one feedback shift registers, where pairs of taps are drawn from junctions between flip-flops, and the modulo 2 sum of the outputs serves as the principal feedback into the "left hand", LS, flip-flop. The main drawback to the Many to One "Fibonacci" configuration is that each stage of the output of the nLFSR or LFSR is a shifted copy (exceptional correlation) of the previous stage, with the exception of the feedback bit fed into the left hand memory cell.</p> <p>In each of the one to many configuration ZK-Crypt Register Bank nLFSRs there is a minimum of 6 XOR gates inserted between the shift register memory cells. Therefore, during the "movement" of a bit moving "from left to right" through the nLFSR, its value would be complemented an average of at least three times. [zk-ccc- Figs. R01-R02 &amp; R04-R09]</p>

<p><b>Orthogonal Feedback</b></p>	<p>We define two or more data authentication feedback streams as orthogonal if a sequence of Message Words causes one stream to successfully corrupt and reconcile one section of tiers in the Register Bank, the second feedback stream simultaneously irreconcilably corrupts another section of the Register Bank for every possible corrupting Message Word. [zk-secure app 2]</p>
<p><b>Oscillation, Oscillators</b></p>	<p>In the binary context, an indefinite length undulation between "0" and "1" with respect to time, with a quasi-stationary period between changes of polarity. The Primary Clock is the Host's regulated derivative of the CPU's system clock. In the Dual Clock TRNG mode, a second uncorrelated clock oscillator is generated by an odd (and constantly changing) number of inverters (NOT gates) joined together in a ring, operative to oscillate at a varying frequency, uncorrelated to the Primary Clock frequency. The period of a ring oscillator clock cycle is a function of the propagation delays of the inverters. The propagation delays are functions of the device temperature and the fluctuating supply voltage. In the FM ZK-Crypt oscillator, the number of inverters is randomly increased and reduced, causing a very unstable frequency, and a "wandering" phase difference between the Primary Clock and signals generated by the unstable frequency. See [zk-ccc- Figs.N06-7].</p>
<p><b>Page, Page Equality</b></p>	<p>In normal transmission of data over noisy channels, sender and receiver are synchronized at relevant intervals. The intervals whence both sender and receiver's modules will interrupt the flow of data will be a predefined number of words, which we call a page, and which in some instances may be a frame of data transmitted on the Internet. See [zk-ccc Figs. B08, H00 &amp; concept in C04-5].</p> <p>At the beginning of a page the sender transmits, and the receiver typically checks the page number against the Mask (Synch) Counter. In a software transmission, or in an internet transmission where pages are not properly decrypted in real time, and or when pages are sent on arbitrary paths, and pages may not be received in the proper sequence, the receiver may store a transmission in memory, in a proper order; to be decrypted later.</p> <p>The Synch Comparator triggers the interrupt when the "Page Equality" designated number of Least Significant bits in the Target Register equals the same Least Significant bits of the Mask Counter.</p> <p>The page sizes are between 4 bits long (16 masks → 16 x 32= 512 bits of encrypted data in a page) to 10 bit long (1024 masks → 32K bits of encrypted data in a page). The Mask Counter is connected to a Port in the Host, such that at each page end a transmitter precedes the next page of encrypted data with the total or a reasonably large portion of the total Word count number in the Mask Counter.</p>
<p><b>Parallelizing ZK-Crypt engines</b></p>	<p><b>n</b> ZK-Crypt engines can be parallelized to linearly increase word size and exponentially increase cryptocomplexity, without increasing energy per processed bit. The hardware link between adjacent cores is the Lower Feedback stream. For <b>n=2</b>, Lower Feedbacks are swapped; e.g., the generated left hand Lower Feedback stream is switched into the R/H Lower Feedback stream, and vice versa. See [zk-ccc- Figs.B10-11] for paired and <b>n</b> concatenated engines respectively.</p>
<p><b>Permutations</b></p>	<p>Permutations are regulated by pseudo-random functions and generators which include:</p> <ul style="list-style-type: none"> <li>The 11 of 12 (P)Random Clock (aka the missing pulse Pseudo (P)Random Clock);</li> <li>The Splash Matrix Stepper; and</li> <li>The Top, Middle and Bottom Control Units.</li> <li>The Permutation Encoder</li> <li>11 non-linear feedback shift registers</li> </ul> <p>The permutations include:</p> <ul style="list-style-type: none"> <li>The MAC MIX Result Displaced FB to the Super Tier;</li> <li>The SuperMIX Displaced FB to the Super Tier;</li> <li>The Right and Left nLFSR Slips;</li> <li>The pseudo-random activation of Tiers;</li> <li>The pseudo-random Image XOR of Tiers' outputs;</li> <li>The pseudo-random XORing of a Tier's concatenated nLFSRs' output Image to itself;</li> <li>The pseudo-random Splash displacements;</li> <li>Missing Clock activation of the Control Units &amp; with Alternate permutations</li> <li>The MAJ diffusions of two left hand adjacent Splash output bits to the principal Splash output bit</li> <li>The non-linear 4 Tier Hybrid MAJ/XOR combiner;</li> <li>The bias balancing of the principal Splash output bit to its</li> </ul>

	<p>right hand adjacent Splash output bit;  The XOR combining of the last two EVNN outputs; and  The Top, Intermediate and Bottom Store &amp; XORs  The XOR combining of the last two Result words to be fed back into the three tiers;  and more.</p>
<p><b>Primary Clock</b></p> <p><b>(P)Random Clock → Pseudo-Random in Cipher &amp; MAC Mode</b></p>	<p>The Primary Clock is the only step controller in any Single Clock deterministic mode of operation. It drives the (P)Random Clock generator.</p> <p>All outputs of the (P)Random Clock module are synchronized to the Primary Clock in both modes of operation.</p> <p>The (P)Random Clock only directly drives the TMB Control Units which pseudo-randomly trigger slip pulses, select EVNN permutations, and select how and which tiers are activated at a given step.</p> <p>Each of the TMB Tiers is clocked erratically about 84.7% of the Primary Clock pulses. At a given clock cycle, only one of the TMB Tiers may be disabled.</p> <p>[zk-ccc- Fig. P08]</p>
<p><b>Pulse</b></p>	<p>A short aberration of a quasi-stationary signal, hence a short interval of "1", over a signal that was typically binary "0". In the ZK-Crypt deterministic mode, all pulses (we call them signals) that activate random logic are synchronized to the Primary Clock and are single value during each whole Primary Clock period. The clock pulses that drive memory and other flip flops, are half Primary clock periods.</p>
<p><b>Random Controller</b></p>	<p>In Single Clock mode, the (pseudo) Random Controller receives binary feedback signals from 8 nLFSRs in the Register Bank, and two signals from the output of the Top Splash Matrix. The Random Controller includes a deterministic Noise Source which drives the three included Control Units which feed the permutation encoding logic.</p> <p>See [zk-ccc- Figs. A01&amp; P01].</p>
<p><b>Random Number Generator, RNG, True RNG, TRNG &amp; Deterministic RNG</b></p>	<p>A (binary) Random Number Generator, RNG, is a device that generates strings of unpredictable binary bits, which when concatenated into longer strings remain virtually unpredictable, even in those instances where an observer knows the precise logic implementation (hardware or software).</p> <p>Silicon fabs are striving to meet the German AIS 31 Noise Source Standard for True Random Number Generation. The German regulators divide a TRNG in two; a Noise Source, and a post processing Deterministic Random Number Generator, DRNG; e.g., a stream cipher. They assume that the DRNG design may be compromised. They assume that if the Noise Source drives said DRNG, the TRNG will be a dependable generator, if its components do not age excessively and are provably functioning properly. We demonstrate that the all digital, random FM modulated FortressGB noise source is virtually immune to varied Host sampling frequencies, ageing and biased clocks.</p> <p>Therefore, as unpredictable random numbers are increasingly important in cryptography, they now demand that said post processors "receive" streams of binary redundant entropy, which is statistically monitored on line.</p>
<p><b>Random Hashing</b></p>	<p>Using the ZK-Crypt as a one way function, typically for authenticating passwords, where an intruder learns little from stored hash values, and the verifier automatically hashes the incoming value, and checks against the stored hash value. An attacker who outputs the hashed files will find it difficult to invert the information.</p>
<p><b>Reconcile</b></p>	<p>The first classic attack on a hash is to modify a Message Word, knowing that the modification will flip state variable bits. The attacker will be able to estimate which bits were flipped, and will try to reconcile by flipping the faulty bits to the original valid state. We call the process reconciliation.</p>
<p><b>Register Bank</b></p>	<p>The Register Bank is the complex of 8 unique pseudo-randomly driven nLFSRs organized in four tiers in the 32 bit Word Manipulator. The three TMB Tiers each include a pseudo-randomly activated rotated output (an "Image") of the tier's nLFSR pair's output. A tier's output is either the XOR sum of the Image and the register pair's output, or the concatenated nLFSR pair's output only. See [zk-ccc- Fig. A02 for use with Rationales zk-secure ch 1].</p>
<p><b>Register Bank Store</b></p>	<p>In a configuration wherein the Register Bank "rains down" metastable changing data to the Data Churn, for a period immediately following a clock tick; causing the Data Churn to consume a fairly constant amount of wasted current prior to the Bank's arriving at a final stable value. The Register Bank Store, [zk-ccc T06], isolates the Register Bank from the Data Churn for one clock cycle,</p>

	<p>shortening the settling time necessary for the Cipher Mask to assume its final value, preferably in less than a single Primary Clock period.</p>
<p><b>Repeated Word Distinguisher</b></p>	<p>A test of the random distribution of 32 bit words in a large set of consecutive samples. Typical tests check the distribution of nibbles and bytes. Daniel Bernstein first suggested testing a series of 10 million samples, each test in the series starting at a different initial condition. Experience has shown that other standard rigorous tests do not detect poor distribution of 32 bit words. We benchmarked the ZK-Crypt against Bernstein's tests on the Linux RND (a combination of SHA/AES generator) and our own generated RD5 files.</p> <p>How many repeated words may we expect to find in each test? First we will take the naïve approach- because of the large size, and the very low probability of expected finding a number in the 10M sample; the chance of finding a pair is one half the chance of finding a specific number.</p> <p>If there are <math>2^{32}</math> different numbers in a 32 bit word, and we sample 10 million words, the chance of finding a particular word is <math>1/429,497</math> or finding the same word at least twice is about one in 859. Ten million divided by 859 gives us the approximate number words that appear twice 11,641. (Obviously there should be a few less.) Note that these tests were done testing random distribution of the Pseudo Random Function, without the randomizing affect of hashing in of uncorrelated Message Words. Testing on uncorrelated, non-trivial hashed messages gave remarkably better results.</p> <p>A better representation that leads to understanding why we constantly found fewer RWs -  <math display="block">\#RW = (\text{Number of candidate RWs}) / (\text{Probability of any word's occurrence}) = (n(n-1)/2) / (2^{32})</math> </p> <p>This assumes that finding any one of the <math>2^{32}</math> words in any of the n test words is equiprobable. In the equation (n-1) hints that finding two identical output words juxtaposed - is equiprobable. This provably not so. Last tests generated an average of <math>\#RW = 11,613</math> hint that for the first 12,600 Messages (400K bits), a RW will never be found as:  <math display="block">\#RW \text{ with non-trivial hashed in Messages} = (n(n-12600)/2) / (2^{32}) = 11,613</math> </p> <p>The Repeated Word test detects internal correlations in words; in the ZK-Crypt Hybrid MAJ filter, every fourth indexed MAJ gate has the same polarity input, meaning that, on the average <math>\frac{3}{4}</math> of the eight gates' output will be same polarity. The same test, run repeatedly on the ZK-Crypt, with EVNN inputs to the MAJ filter locked on "1", averaged 11,633 pairs and triplets with a relatively small variance. However, if we XORed adjacent Results words (word X and X+1), we found on the average 4 more repeats, but when we XORed the X and X+7 words, we found 17 less words. Conclusion- there is a trace correlation between pairs of Result words, but no measured correlation between distanced words.</p> <p>Repeats on the outputs of the Hybrid MAJ gates were astronomical, close to 2M out of 10M samplings on the same tests. Interesting to note that there were no differentials on any of the MAJ outputs.</p> <p>Bernstein's testing on the Linux RNG function, and our measures on RD5 yielded about 11,623 repeats.</p> <p>The ZK-Crypt submission with colored spectrum Messages (as opposed to all zero Message inputs on all previous checks achieved a new low of 11,613 RWs.</p> <p>New interesting conjectures on the meaning of Repeated Words are included in the NIST submission. Expect new results.</p>
<p><b>Result/Feedback Processor</b></p>	<p>That component of the ZK-Crypt engine that Processes the 3 function Results and generates the Super Tier and Lower 32 bit feedback streams. See [zk-ccc-Fig.B01]. The Processor also integrates the "salting" HAIFA counter results into both FB streams.</p> <p>In MAC mode, the Lower FB is the XOR sum of a previous Result (the Cipher Mask XORed to a Message) XORed to a present Result; wherein the Super Tier feedback is a "salt" internally generated word XORed to a reverse nibbled present Result word.</p>

	In Stream Ciphering the Result is the XOR sum of the Message and the Cipher Mask. The Lower FB is a sparse function, and the Super Tier FB is a reversed nibble dense FB.
<b>Reversed Nibble</b>	A nibble with bits A, B, C&D, [ABCD], input is reversed nibble transformed to sequence [DCBA]). In the MAC MIX, each reversed nibble is output unrotated; e.g., the LS reversed nibble remains in the LS position. In the SuperMIX, each reversed nibble is 8 bit right rotated See MAC MIX and SuperMIX.
<b>S Box, Serpent Bijective Biham S Box</b>	The Biham Serpent bijective S Box is included in the SuperMIX transformation to delinearize and decorrelate the 32 bit Super Tier Feedback stream. Each of 8 nibble slices in the input defines a one to one (bijective) transformation of the input (one of 16 nibbles) to a single valued four bit output. Each S Box nibble is reversed. DES S Boxes are not bijective.
<b>Salt</b>	Any aberrating pseudo random function that introduces additional unpredictability into an incoming Message Word or a Result word. Often it is a keyed variable that is XORed onto an incoming Message Word, or "last minute received" IV, which would make an adversary's task intractable in a given time frame. See IV, HAIFA Counter, Scramble, Dual Track Feedback.
<b>Scramble</b>	The Scramble function in the ZK-Crypt is a simple diffusion mechanism which we use to maximize cryptocomplexity of initialization (precluding weak keys) prior to ciphering, prior to Message Digesting, and prior to Hash Value/Tag generation, and to enable increased security in constrained hardware. Simply stated, a single scramble is a single Primary Clocked procedure in MAC Mode, with the Message Word input and the Result output to the Host locked to zero. In the Wait and Read cipher or hash, the engine is Scramble cycled a defined number of times before the Host inputs a Message Word one cycle before the Host may read a Result. See Multi-Step Mode, Wait & Read
<b>Side Channel Attack</b>	A variety of methods to monitor cryptographic algorithms to learn embedded secrets, via radiation, physical probing, and the present most popular analyzing of input voltage aberrations. DPA, differential power analysis, is the commonly used name given by Kocher et al in "Cryptography Research International" for refined side channel attacks. The CRI methods are primarily based on monitoring aberrations of chip power to learn secret cryptographic keys. The ZK-Crypt submitters have extensive successful experience defending public key designs from side channels previous to CRI's first issued patents, and have written patented algorithms which accelerate and preclude side channel attacks. See DPA.
<b>Single Step RNG/SCE &amp; MAC</b>	The principal modes of operation wherein at each Primary Clocked cycle a 32 bit Message is introduced and/or a Result is drawn. This is the only mode of operation in the eSTREAM rendition. See RFU Multi-Step Mode.
<b>Slip Sequence &amp; Slip Signal</b>	A slip in an nLFSR sequence is a pseudo-random displacement (slip) of one n bit output word from one location in the sequence of $2^{PPPP}$ words to another unique word in the sequence. The aberration is caused by an externally generated binary "1" Slip signal which complements the normal nLFSR feedback for one clock cycle. Overly frequent occurrences of the Slip signal, e.g., an average of one in four Slip signals, causes short term bias on the nLFSR output. Any residual bias is typically exaggerated by the MAJ combining functions.
<b>Software ZK-Crypt</b>	FortressGB supplies an unoptimized generic software C program with test vectors compliant with the eSTREAM submission. FortressGB has also implemented a "software friendly" configuration of the ZK-Crypts, wherein the Splash Matrix pseudo random displacements are nullified; e.g., only the "straight through" displacement is locked in. All remaining ZK-Crypt manipulations are easily executed using standard software functions, e.g., AND, OR, XOR, NOT, Rotate and Shift. This facilitates efficient interoperability of legacy devices and hardware implementations. The statistical output is still very good (slightly degraded); the crypto-complexity may not be affected.
<b>Sparse Feedback, Lower Cipher FB</b>	The Sparse Feedback function used in the Lower Cipher Feedback (is a non-linear function which recycles an average of four "1" bits in each word into five memory stores. There are three versions of the feedback, non-rotated, 13 right rotated, and 7 left rotated; each of which serves to increase diffusion. In the ZK-Crypt, the dense Super Tier Cipher feedback masks the effect of the Sparse Feedback in the TMB Tiers. See [zk-ccc- Fig.F00].
<b>Splash Matrix</b>	In the ZK-Crypt, each Splash Matrix is a rule set of 4 displacement permutations on an input word. In the ZK-Crypt the rule is selected by a five input pseudo-random variable function, the Splash Selector. Three of the four rules displace input bits to output bits in a pseudo-random permutation. The fourth rule is a "straight through displacement", where the input word is identical to the output word. See [zk-ccc Figs. T3 & T4].
<b>Splash Selector</b>	The Splash Selector receives five variable binary inputs into the function which pseudo-randomly selects (at each Primary Clock Sample) which displacement rules are exercised in the Top and Bottom Splash Matrices. The Selector's inputs are one variable from the Random Controller, two included memory variables (previous select), and two data dependent values from the Data Churn.

	See [zk-ccc- Fig. P06].
<b>Store &amp; XOR (Filter)</b>	A combination of a memory cell (a D-Flip Flop) and an XOR gate, wherein the present clocked input bit is XORed to the previous input bit, i.e., the present input bit is stored in the memory, to be output and XORed to the new input bit at the next clock cycle. Observing the outputs of a single Store & XOR cell, forms a logical barrier, making it difficult to estimate previous inputs. Rueppel calls such a function a correlation immunizer. See [zk-ccc- Fig. T1].
<b>Stream Cipher Encoder, SCE</b>	<p>Stream ciphers are symmetric encryption devices. As defined by Rueppel in (out of print) <u>Analysis and Design of Stream Ciphers</u>; "stream ciphers divide the plain unencrypted text into characters and encipher each character with a time-varying function whose time-dependency is governed by the internal state of the stream cipher. After each character that is enciphered, the device changes state according to some rule. Therefore, two occurrences of the same plaintext-character will usually not result in the same ciphertext character."</p> <p>In most conventional stream ciphers, characters are binary bits, and the time dependency is a function based on a plurality of Many to One type LFSRs, where a combined output of the plurality of LFSRs is XORed bit by bit to a message stream, which is first encrypted by the encryption stream, and subsequently decrypted by XORing each binary bit in another functionally identical device, using the same secret initializing key.</p> <p>In the ZK-Crypt stream cipher the feedback shift registers are typically non-linear feedback shift registers based on One to Many LFSRs, and the cipher characters are 32 bit words.</p>
<b>Stuck on Zero</b>	<p>Stuck on Zero is the malfunction that occurs in conventional LFSRs, when for some reason the output of all memory cells in the shift register are fixed at zero. With the shift register in such a state, the feedback (and consequently the LFSR) is "stuck" at zero, as at each clock all memory cells remain at binary "0".</p> <p>If the NFIX gate senses that the n-1 LS bits are zero; it outputs a "1". Then, if the MS bit of the nLFSR is a "1", the next stage of the nLFSR will be the all "0" value. This completes the pseudo-random sequence which now includes an equiprobable all zero element.</p> <p>Conversely, if the MS bit is a "0" the next stage will be a single LS "1" followed by "1"s in the outputs of all of the nLFSR feedback taps.</p> <p>Note if a stream of slip pulses ("1"s) is constantly received at the stage where all cells are zeroes, the nLFSR will remain "stuck on 0000....0000".</p> <p>The NFIX gates have been removed from the Reg. Bank nLFSRs, as it is virtually impossible that an nLFSR that receives Left or Right Slip permutation signals, and/or parallel Lower or Super Tier feedback can be "stuck on zero". This may happen to the nLFSRs in the TMB Control Units.</p>
<b>Super Tier</b>	<p>An additional tier was added to the ZK-Crypt I to balance the output of the Register Bank. The Top, Middle and Bottom (TMB) Tiers are input into a MAJ filter, whose Image and output are XORed to the output of the Super Tier, in a mode that masks the contents of the three TMB Tiers. The Super Tier receives dense (an average of 16 "1"s in a 32 bit word) uncorrelated feedback both in Cipher Mode and MAC mode. In MAC Mode, the Super Tier also receives, XORed to the parallel feedback, the output from the 24 bit Mask Counter. This may prevent copying and relocating running key values.</p> <p>The output of the Super Tier nLFSR pair is hardwire XORed to its 7 left rotated Image, always; e.g., not pseudo-randomly XORed like the TMB Tiers. See [zk-ccc R01-R03].</p>
<b>Super Tier Feedback</b>	<p>The Super Tier, in the ZK-Crypt accepts a dense (average of 16 "1"s) feedback word. The SuperMIX nLFSRs are clocked, and incorporate feedback at every Primary Clock cycle. (Sparse Feedback is recycled into the TMB tiers and the Data Churn, in cipher mode, where, randomly, two or three tiers are simultaneously clocked and enabled to combine feedback).</p> <p>In the MAC mode of operation, the Super Tier receives the MAC MIXed message affected feedback XORed to the SuperMIX output; obviating weaknesses related to message modifications. See [zk-ccc- Fig. F02].</p>
<b>SuperMIX</b>	The Super MIX is a nibble (one half of a byte) displacement transformation on the feedback vector to the Super Tier; derived from the XORed outputs of the Intermediate Store & XOR and the lower Splash Matrix EVNN MAJ/XOR filter. This nibble reversal and subsequent 8 bit right rotation of

	<p>the nibble obviates a correlation between the originating feedback vector and the vector to the Super Tier. This permutation improved statistics.</p> <p>Algorithmically, the SuperMIX nibble displacement transformation:  <math>(ABCD) \rightarrow 8 \gg \gg (DCBA)</math> See [zk-ccc- Fig. F11]</p>
<b>Synch Counter</b>	See Mask Counter. Originally the Counter was only used for synchronizing message transmissions. Now it serves to prove wandering phase differences between the Primary Clock and the fr FM oscillator signals in TRNG generation, and also as a nonce input to each MAC word digest.
<b>Tag/Hash value</b>	<p>We use the term, Tag/Hash value, to describe the output of the MAC compression function.</p> <p>The Tag/Hash value is the (securely) saved prover of authentication of a MAC file. We say that the one-way MAC diffusion/compression of the file data into the 404 MAC variables is a digestion. The final Tag/Hash value output is a "signature" of message digestion generated by the ZK-Crypt engine in MAC mode, wherein the input Message Word is the all zero word. See [zk-ccc- B06].</p>
<b>Tenets, Basic of the ZK-Crypt</b>	<p>The design strategy of the ZK-Crypt engines was based on the following four tenets, which have been supported by vigorous testing, and mathematical proofs.</p> <p>Large scale diffusion, wherein each binary state variable is an immediate function of at least three preferably disparate state variables, leads to intractable algebraic cryptocomplexity; unbiased binary and word state variables; and to a stark reduction of state variable autocorrelation.</p> <p>XOR summing of two or more slightly biased binary structures; i.e., bits, nibbles bytes or 32 bit words, results in less predictable, less biased output; if and only if there is no or very little detectable cross correlation between the structures; i.e., one structure may show strong signs of autocorrelation.</p> <p>Judicious use of conventional and tailored non-linear and linear artifacts to simultaneously control: the levels of autocorrelation and bias within binary structures; and the acute reduction of cross correlation between linear combined binary structures.</p> <p>The Dual (2x32 bit) Track Orthogonal Feedback permuted streams are linearly combined into interacting state variables thereby amplifying the affects of both the randomized increments of the Message counter and the irreconcilable modifications of Message Words; the resulting increased diffusion effects proven preclusion of Collision and Message Modification attacks and effective resistance to Pre-Image attacks.</p>
<b>Tier Combiner, 4 Tier Combiner</b>	<p>In the ZK-Crypt the word outputs of the Top, Middle and Bottom tiers are Majority Function, MAJ, combined together, with a shifted Image and XORed together into a combined ENS output.</p> <p>This ENS TMB output is then XORed to the ENS output of the Super Tier. See [zk-ccc Fig. 11S2].</p>
<b>Tier, Top, Middle &amp; Bottom (TMB) and Super Tier</b>	<p>In the ZK-Crypt a Tier is one of the five random logic formations in the Register Bank.</p> <p>Each tier consists of two unlike nLFSRs concatenated, and a 1, 3, 5 or 7 bit left-rotated Image of the output of the nLFSR pair.</p> <p>The TMB tiers' Images are pseudo-randomly activated. If the rotated Image is not activated, the tier output is the concatenated output of the pair of nLFSRs. If the rotated Image is active, the tier output is the concatenated output of the nLFSR pair XORed to the Image.</p> <p>The Super Tier's Image is always active. Therefore, the Super Tier's output is always the concatenated output of the Super Tier nLFSR pair XORed to the Super Tier's Image.</p> <p>The Super Tier is clocked at every Primary Clock pulse.</p> <p>At each Primary Clock pulse either two or three of the TMB Tiers' nLFSR pairs are activated. The unactivated tier is selected pseudo-randomly, with a probability of about 64%. The paired nLFSR output XORed to its Image outputs a pseudo-random ENS.</p> <p>The TMB receive Left and Right Slip signals from the Random Controller. Each Slip will be enacted on the average of about once every seven Primary Clock cycles.</p>

	All tiers are aberrated by feedback; the TMB tiers receive FB from the Lower Feedback Store, and the Super Tier receives from the Super Tier Store. In MAC mode the Super Tier's FB vector is XORed to the output of the 24 bit counter. [zk-ccc- Figs. R01-R11].
<b>Toggle</b>	A complementary change of a binary signal, i.e., a change of a one to a zero or a change of a zero to one.
<b>True Random Number Generators TRNG</b>	Random Number Generators are often deterministic devices initialized with a secret seed. The German BIS' AIS 31 specification defines a TRNG as a device with a testable reasonably good Markov chain analog noise source driving an AIS 20, deterministic "entropy" compression scrambling device. The random FM autonomous oscillator driving the post processing Permutation Encoder and 32 Bit Word Manipulator is compliant with both the rigorous AIS 31 and less rigorous AIS 20 spec.
<b>Wait &amp; Read equivalent to Multiple Rounds</b>	For greatly increased security without increasing hardware. The Wait and Read command cycles the ZK-Crypt engine for n ( $n \leq 64$ ) Scramble cycles, designated in the 6 bit counter set in Port A. The last cycle is a Read command, wherein the Result is read onto fast Port C, and the value of the Message is Read into the engine from input Port B. Wait & Read is equivalent to multiplying the number of rounds in a block cipher. In MAC mode Hash Value/Tag Wait & Read, the Message input is locked on zero. The Message is input one cycle before the Read to Host. [zk-ccc- Fig.A03]
<b>Work Factor</b>	The approximate number of computational trials using a given method, necessary, on the average to compromise a cryptographic process. Compromising Single DES on random data, using brute force guessing, has an average work factor of $2^{55PP}$ . Diffie estimates that a work factor of $2^{128}$ will be adequate so long as full scale quantum computing is not available. [diffie99]
<b>ZK-Crypt</b>	The abbreviated name of the herein described method and device, operative to generate Random Number Words and Sequences, to encrypt and decrypt streams of binary words, and to validate the unaltered status of a stream or file of binary data, with very close to Zero Knowledge leakage from the Register Bank, Sanctus SanctoUm, when operated properly in a prescribed manner. The ZK-Crypt is the subject of three patent applications; the Random Controller/Data Manipulator architecture, the AIS 31 compatible Noise FM methodology, and the correlation immunizing Feedback Strategy. [zk-fbpat1,2 & 3]



References:

- [diffie99] W. Diffie & S. Landau, "Privacy on Line: The Politics of Wiretapping and Encryption", first ed. February, 1999
- [haifa] E. Biham & O. Dunkelman, A Framework for Iterative Hash Functions, NIST Hash Forum 2006, August, 2006, Santa Barbara.
- [zk-ccc] ZK-Crypt Circuit Concept Drawings, eSTREAM Phase II Evaluation, FortressGB, London & Omer, March 2007.
- [zk-code] A. Hecht, ZK-Crypt C Code Simulator, vers3, eSTREAM website, vers 3, March 2007.
- [zk-algo] A. Hecht, O. Dunkelman, ZK-Crypt Algorithmic Specification, eSTREAM website, vers 3, March 2007.
- [zk-fbpat1] PCT Application WO2005/101975, Architecture, April 24, 2005.
- [zk-fbpat2] PCT Application, PCT/IL/2006/000627, Noise, May 25, 2006.
- [zk-fbpat3] US Patent Application 60/84612, Feedback, September 7, 2006.
- [zk-secur] O. Dunkelman, A. Hecht, The ZK-Crypt Security Analysis, eSTREAM website, vers 3, January 2007.
- [zk-undr] C. Gressel, O. Dunkelman, A. Hecht, Understanding the ZK-Crypts – Ciphers for (almost) all Reasons, eSTREAM website, March 2007.