



## Chapter 05: Dual Track Orthogonal Feedback

### *The ZK-Crypt Obviates Contrived Word Hash Fraud*

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

TO BE REVISED

DUAL FEEDBACK MAC AUTHENTICATION  
WITH THE MAC MIX ANTI-COLLISION PERMUTATION

SINGLE STEP 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

SUBMITTERS: CARMİ GRESSEL  
NICOLAS T. COURTOIS  
GREGORY V. BARD  
AVI HECHT  
RAN GRANOT

JANUARY 2009 DRAFT



## The ZK-Crypt Obviates Contrived Word Hash Fraud

Note: The following study was made previous to increasing the HAIFA/Page Synch/Phase Detect counter to a 56 bit counter with 64 bit pseudo random dispersion to the Lower and Super Tier Feedback Stores.

In keyed and unkeyed MAC and Hash authentication schemes, Message Words are "digested" and diffused into the ZK-Crypt engine. The final Message Digest should be an output that is in reality unique for only one meaningful Message string. The potential danger in an unkeyed engine is that an adversary may know both the message string and the subsequent Tag (hash output) and easily construct an identical function where he would learn all internal values and be able to alter a small number of bits in a message so as not to change the final Tag. We prove the ZK-Crypt architecture inherently averts illicit attempts to contrive Message Words, even if the adversary were able to maintain valid parts of sequences in any components of the ZK-Crypt for a precious few clocks. To understand this explanation, the reader is advised to first become acquainted with the referenced [zk-algo] and [zk-ccc] documents; respectively the formal algorithms, and the circuit, block & concept drawings of the ZK-Crypt. Relevant drawings have been copied into the Appendices.

If we assume that omnipotent adversaries know the engine and all values in the 407 ZK-Crypt MAC variables, they will attempt to contrive meaning closely related false Message Words that generate valid MAC Feedback so that subsequent Register Bank sequence variables will be identical to the original valid sequence. In the Single Track Feedback strategy previously used, theoretically such an adversary could have temporarily maintained the Register Bank in a valid condition, albeit there was provably no way that the hacker could simultaneously restore all of the Stores in the Data Churn and Result word to a valid state. This would not have enabled False Message Insertion, but we considered it a sign of a potential weakness. The Single Track feedback was a linear transformation, which insured massive diffusion, and satisfactory statistics. We will show how our addition of a second non-linear, innovative displacement feedback track proactively prevents false message insertion thereby simultaneously enhancing outputs which generate "ideal" statistical results, e.g., DieHard, Repeated Words, etc.

We show that a contrived sequence of Message Words designed to first compromise and then maintain a valid condition in the TMB (Top, Middle & Bottom Tier) Bank, irrefutably alters the values in the Super Tier, and vice versa. The "uncontrollable" Super Tier's contents not only affect the Data Churn, but also affect the Top Control Unit, which ultimately, via the Slip Pulses, and the random shift register activators additionally contaminates the TMB Tier Bank. Typically, after another small number of clocks cycles, all other variables in the ZK-Crypt Engine are compromised. We know that an astute adversary can generate contrived words, to generate valid feedback when he is able calculate Cipher Masks and Result words, and knows the licit Feedback sequence.

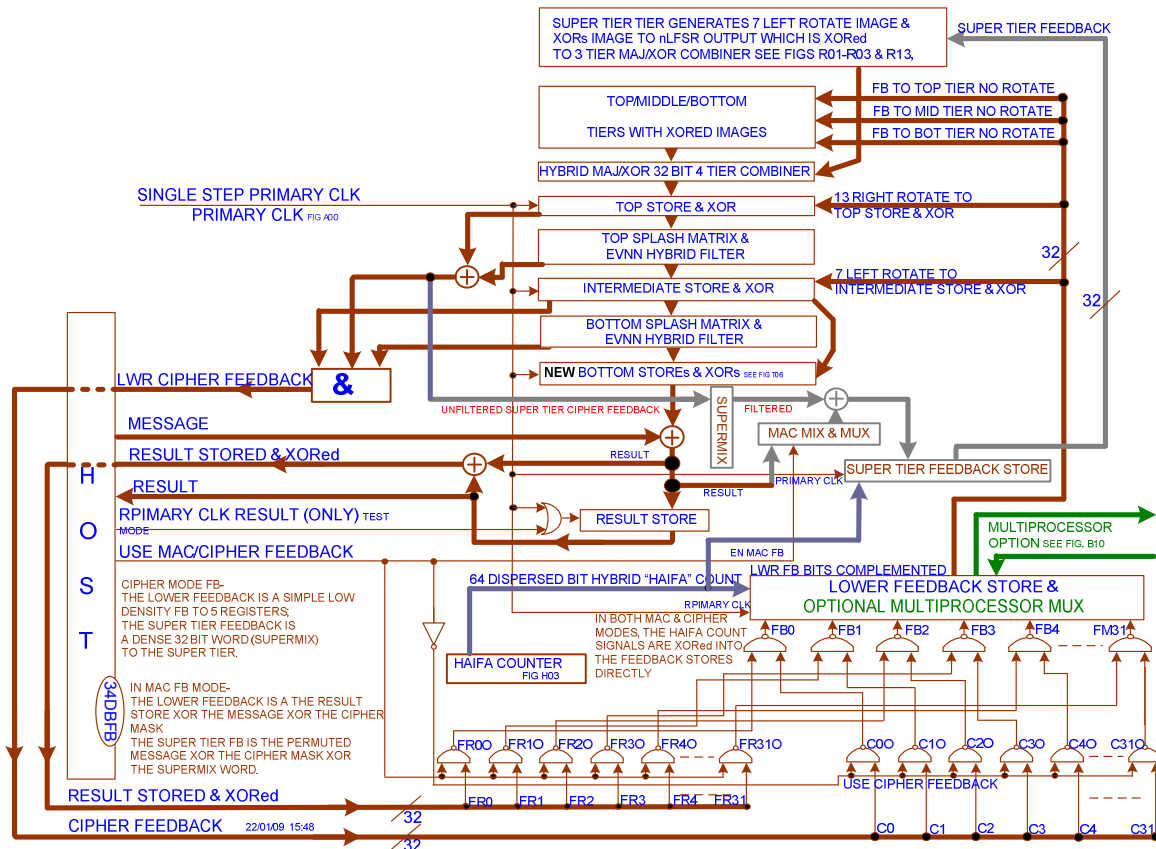
In addition, we have assumed that an omnipotent adversary may find a method to cause an inverse of a stage (as in a block cipher), and could have a method to generate sections of a false message string that could be concatenated, such that at the final message blocks, the internal variables would be in a valid condition, (similar to the fixed point attacks with block ciphers). The inspiration came from the HAIFA [haifa] Framework indexing method to avert relocatable sections of hash chain values (in our case the "running key" values); we XOR the output of the 24 bit Mask Counter to the Super Tier Feedback vector, leaving a unique trace in the engine at every masking step. The "unique" count-index internally tags each engine stage in a way that obviates relocation or duplication of strings.

In the first phase of the demonstration, in Table 1, we will assume that any bits can be complemented (and the aberrations can be locally rectified) in a Message, and in any Message. In the second phase, Table 2, we show that because of the random values which become dispersed in the Super Tier, the omnipotent adversary can only maintain valid values in the TMB Tier bank for a limited duration of the Message Digestion, as the uncontrollable Super Tier contents affect the Data Churn, and the Top Control Unit, which alters Slip signals and (P)Random sequence changes to the TMB Tier Bank.

## Feedback Loops

There are two distinct modes of feedback: a) the Cipher Mode, where our interest is to raise crypto-complexity. As the Cipher Masks are a function of the internal running key only, the masks are not affected by unpredictable Message Words, (else the message receiver would be unable to decipher); and b) MAC mode, where every bit of each message must diffuse into every ZK-Crypt engine variable. In this document, we are interested in the MAC mode, as we demonstrate the immunity of the ZK-Crypt to fraudulent word attacks, where we show that a single changed bit in one Message Word will invalidate any tag digest.

In the following Fig. 00FB we see two diverse feedback loops, the simpler Lower Feedback Word and the more convoluted Super Tier Feedback Word.xxx



**Figure F02- The Dual Orthogonal Track Feedback Strategy**

The Dual Track Feedback in the ZK-Crypt generates two different modes of MAC feedback to avert pre-image collisions in the Register Bank, by recording an amplified trace of toggled (False) Message bits in the Super Tier.

### The Lower Feedback

The Lower Feedback loop feeds 5 registers as depicted in Figs. B01. In Cipher Mode, the lower feedback is a sparse function (on the average only four "1" bits) of intermediate values in the Data Churn. [This value is not used in the MAC Mode.]

[Appendix 1 Fig. 00FLWR] depicts the elements of the ZK-Crypt TMB Tier (Lower Feedback Store) feedback scheme. The Register Bank, which includes the TMB and Super Tiers combined in the Hybrid Register Bank Combiner, outputs a random word which undergoes, in the Data Churn, further manipulations, varied linear and non-linear permutations and receives feedback (rotated) from the



Lower Feedback Store. The Bottom Store & XOR, the last component in the Data Churn trail, outputs a 32 bit random word, the Cipher Mask (CM).

In the MAC mode, see Table 1-

At each clock cycle a Message Word ( $MS_{n-1}$ ) is XORed to the Cipher Mask ( $CM_{n-1}$ ), and is Stored in the Result Store ( $CXM_{n-1}$ ). (In Cipher Mode the Message is thus encrypted). In MAC Lower Feedback, the Feedback Word is the present Message Word XORed to the present Cipher Mask XORed to the present value in the Result Store, which is the previous Message Word XORed to the previous Cipher Mask;

e.g.,  $CXM_{n-2} \oplus CXM_{n-1}$ . It is easily seen that if one bit is falsely complemented in either the (n-2)'th or (n-1)'th Message word said complemented bits would "contaminate" bits in at least two of the TMB registers, and in both the Top and Intermediate Store & XORs.

We assume that the adversary has chosen a word that meets the criteria for "pinpointing" those bits that can be altered without affecting the Random Controller, or the MS cells of any of the tiers' One to Many type nLFSRs, e.g., the tier activation signals, FT, FM, and FB are stable for two critical clock periods, that the tiers will "hold" uncontaminated values for only one clock cycle. Here we assume that the tier activators are stable for the two critical clocks; conditions that can be met by an astute adversary.

All non-linear feedback shift registers (nLFSRs) in the TMB Tier Bank have the same structure, see [zk-ccc Figs. 19TL – 24TR]. They receive random clock activation (with a probability of more than 5/6 at any clock) and receive random aberrating Slip Pulses XORed to their internal feedback on the average of about once in 5 or 6 clocks. We note that an astute adversary will probably find an interval when the Random Controller would not be aberrated by the feedback from the TMB Tier Bank, by the Super Tier, or the output of the Top Splash Matrix, so that the conditions in the TMB Tier Bank will be stable during the first few clock cycles of the attack; [we show that all other components of the device will be totally compromised].

Note that our adversary knows the received Cipher Mask word, he knows the contents of the Result Store, and he remembers what the valid feedback word is, so that as long as the Random Controller is not contaminated, the TMB Tier Bank can receive valid feedback at every clock, maintaining the TMB Tier Bank in a licit sequence.

The Host (in this analysis, an assumed omnipotent adversary) inputs a string of Message Words which would be identical to the original string, except where where he replaces a sub-string of Message Words, with a string of contrived Message Words, which (were there not the second feedback track) could leave the 96 variable bits of the Top, Middle and Bottom Tiers (only) without trace of the fraud.

The two first "fraudulent" Message Words constitute a first word that would complement designated bits in the TMB Tier Bank and a second word that would retrieve (reverse the complementation) in the TMB Tier Bank tiers, where each designated bit would have shifted one cell to the right. After these first "contaminating" words, four Stored words (from the four Store & XOR correlation immunizers) would have been corrupted. Each corrupted stored word output further corrupts lower stores. In the single track configuration, three of the four corrupted Stored words could be "cleansed"- one after another, by three consecutive valid output words from the Hybrid Register Bank Combiner. We will show that this play does not work in the dual track configuration, because every complemented bit in the first word leaves a trace in the Super Tier, which irretrievably corrupts, at each clock, the values in the Data Churn, and eventually affects the Random Controller. We will also show that a Message word cannot be contrived that can both return the Result Store and the Lower MAC Feedback to valid values; and what is more important, even without the Super Tier Feedback, **the Result Store is contaminated completely at the first falsifying clock cycle, and cannot be reconciled at any subsequent clock cycle without contaminating the TMB Tier Bank.**

We review the reconciliation scheme in the TMB Tier Bank, as depicted in Table 1, for 12 bits. In Table 2 we demonstrate the interactive contamination of the Super Tier and Data Churn.

Note, we are only interested in tracing bits that have been aberrated,  $\mathcal{F}$ .

- At the 0<sup>th</sup> Clock, all variables in the ZK-Crypt are in the valid  $\mathcal{T}$  (true) sequential state.
- At the 1<sup>st</sup> Clock, 3 bits of the depicted string from the Message Word, MS, are (fraudulently) flipped, and processed into  $MAC_{t-2}$  to be loaded into the Lower Feedback Store. No other variables are affected.
- At the 2<sup>nd</sup> Clock, a correcting Message Word is generated, both to negate superfluous false bits in the Result Store, and to pinpoint complementing "fix" bits in the TMB Tier Bank. The corrupting word is output by the Lower Feedback Store, to be "enjoined" on the next clock cycle to the TMB Tier Bank and to the Super Tier.
- At the 3<sup>rd</sup> Clock the TMB Tier Bank is "pinpoint" contaminated. A Message Word is contrived, as the adversary knows ("remembers") the MFB from the valid sequence, he knows the value of the previous result, and he "reads" the corrupted value of the Cipher Mask. The Lower Feedback Store outputs the "fix" word that complements the shifted  $\mathcal{F}$  bits in their new positions. The three  $\mathcal{F}$  bits in the Message Word complemented three disbursed bits in the Super Tier nLFSRs. The output dispersion is amplified by the 7 Left rotation of the XORed Super Tier image, and corrupts output bits from the Hybrid Tier Combiner which are different from toggled bits from the TMB Tier Bank.
- At the 4<sup>th</sup> Clock, the TMB Tier Bank is retrieved to the valid state. The TMB Tier Bank (only) can be kept in a licit sequence for additional clocks, as the adversary knows the sequence of valid feedback words that he must contrive by changing the Message Words that must be fed into the TMB Tier Bank. The adversary knows that if the Slip signals are not corrupted, and the (P)Random Clock stream is unchanged, he can maintain the TMB Tier Bank in the valid sequence. From the changes of Message Words contrived in Table 1 inserted in Table 3, it is easily seen that after a maximum of 12 clock cycles, corrupted bits will start "arriving" in an nLFSR MS feedback bit, "corrupting" the Top Control Unit in the Random Controller see [zk-ccc Figs. 28SL, 29SR and 13TCU], and the whole device, via the  $Q_{TA}$  debiaser. Note that at this clock, all of the "Stores" in the Store & XOR registers are contaminated; **most completely diffused is the Result Store.**
- After the 4<sup>th</sup> aberrant clock, a fraudulent Message Word string can maintain the TMB Tier Bank, only until the Top Control Unit contaminates at least one tier of the TMB Tier Bank.

## The Super Tier Reverse Nibble Feedbacks

In MAC mode, the Super Tier receives feedback sampled from two intermediate values in the Data Churn, and also receives the Cipher Mask encoded Message Word, filtered respectively by the SuperMIX and the MAC MIX.

This two track permuted dense feedback also solves the well know problem of degraded correlation statistics encountered when recycling dense feedback in cipher blocks.

We assume that the adversary has chosen a word that meets the criteria for "pinpointing" those bits that can be altered without affecting the Random Controller, or the MS cells of any of the tiers' One to Many type nLFSRs, e.g., the tier activation signals, FT, FM, and FB are stable for two critical clock periods, so that the working together TMB tiers will "hold" uncontaminated values for only one clock cycle. Here we assume that tier activators when receiving the first word are all equal to "1" ( $FT_n=FM_n=FB_n=1$ ); that in the general case the TMB tiers are toggled identically; where in the following

exposition,  $TT_n$ ,  $MT_n$  &  $BT_n$  are the values in the tiers prior to XORing the  $MFB_{n-1}$  Feedback into the  $n$ 'th output.

We demonstrate in Table 1 on 10 bit strings how the Message had to be complemented, in order to be retrieved. We only care about true or false (complemented) bits. We know that a false bit in the output of the hybrid Register Bank Combiner always causes false bits in the Bottom Store & XOR (the output of which is the Cipher Mask). We show how a sequence of Message Words can be contrived to maintain the TMB Tier Bank in a valid state, identical to the original valid sequence.

In Tables 1 and 2, we are only interested in knowing if an active bit is the original bit,  $\mathcal{T}$ , true, or if it is a complemented bit,  $\mathcal{F}$ , false. The arrow symbol ( $\rightarrow$ ) point to those bits of the 10 bit string which are true or false; if their values are changed or are not changed from the valid sequence values, respectively.

The Dual Track Feedback system works because:

- 1) A bit flip in the TMB Tier Bank caused by flipped bits in the Message Word (MS), can only be rectified by flipping the Right Hand adjacent register cell (to where the flipped bit will reside on the next clock). Changing two consecutive bits in the Message Word changes consecutive bits in the TMB tier Bank, but never changes corresponding right hand consecutive bits in the Super Tier.
- 2) The Result Store "remembers" a complemented bit from the previous Clock, and outputs the bit on the next clock. This superfluous bit must be negated by a second Message Word, whilst it also generates the second "fix" complemented bit to retrieve the valid condition in the TMB Tier Bank. Every flipped bit in a Message Word scatters complementing bits in the Super Tier, that are unaffected by the value in the Result Store. This means that in order to alter one index bit in the TMB Tiers, three Message bits must be changed causing only two toggles in the TMB Tiers, and 3 toggles in the Super Tier.
- 3) An  $\mathcal{F}$  bit in the Super Tier is linearly reflected in at least one false output bit from the Register Bank combiner (combining the Super Tier and the TMB Tier Bank) thereby preventing valid sequences in the TMB Tier Bank from "cleaning up" the four Stores in the Data Churn.
- 4) Complementing either one of the nLFSR (MS) Super Tier feedback cells immediately generates uncontrollable randomization of the whole device, (a most likely event). Corrupted output from the Register Bank Combiner which is sampled in the Data Churn and input into the SuperMIX filter cannot be rectified by a fraudulent Message Word. Corrupt data is permuted by the SuperMIX filter; XORed to the MAC MIX filtered Result and thereby further randomizes the contents of the Super Tier.
- 5) The MAC MIX filter reflects corruption of the RESULT; the Lower Feedback Store reflects, in addition, corruption of the RESULT STORE, the SUPERMIX reflects (one clock earlier) two intermediate values in the Data Churn.
- 6) Feedback bits from the Super Tier affect all stages of the Top Control Unit (Fig. 13), which translate quickly into toggles in the Random Controller, and into the TMB Tier Bank.
- 7) The Message Word is hardwired to zero, during the entire tagging procedure to prevent subsequent attempts to affect contrived tags.

An example follows in Table 1 where 3 bits out of 12 Message Word bits are toggled. We show that an attempt to left an indelible trace in the Super Tier, and can only estimate the drastic changes in the Hybrid Filter.

0'th Clock – All is well	1st Clock
	Contaminating 3 bits in Message Word
$CM_{t-3} \rightarrow TTTT TTTT TT$ ; Bottom Store & XOR	$CM_{t-2} \rightarrow TTTT TTTT TT$ ; Bottom Store & XOR
$MS_{t-4} \rightarrow TTTT TTTT TT$ ; Real MSG	$MS_{t-3} \rightarrow TFFT FTIT TT$ ; Contaminating MSG
$CXM_{t-3} \rightarrow TTTT TTTT TT$ ; MS $\oplus$ CM Pres Result	$CXM_{t-2} \rightarrow TFFT FTIT TT$ ; MS $\oplus$ CM Pres Result
$CXM_{t-4} \rightarrow TTTT TTTT TT$ ; Previous Result	$CXM_{t-3} \rightarrow TTTT TTTT TT$ ; Previous Result
$MAC_{t-3} \rightarrow TTTT TTTT TT$ ; $CXM_{n-1} \oplus CXM_n$	$MAC_{t-2} \rightarrow TFFT FTIT TT$ ; $CXM_{n-1} \oplus CXM_n$
$MFB_{t-3} \rightarrow TTTT TTTT TT$ ; Lower FB Store Out	$MFB_{t-2} \rightarrow TTTT TTTT TT$ ; Lower FB Store Out
$NEWTMBT_{t-2}=MFB_{t-3} \oplus TMBT_{t-2} \rightarrow TTTT TTTT TT$	$NEWTMBT_{t-1}=MFB_{t-2} \oplus TMBT_{t-1} \rightarrow TTTT TTTT TT$
Next Clock- Register Values not Contaminated	Next Clock- Register Values not Contaminated
2nd Clock	3rd Clock Bottom Store&XOR is Contaminated!!
Lower FB Store Outputs Contamination	MAC <sub>t</sub> is Proper FB, the Adversary Knows
$CM_{t-1} \rightarrow TTTT TTTT TT$ ; Bottom Store & XOR	$CM_t \rightarrow$ A Random Variable; Bottom S&X-Learned
$MS_{t-2} \rightarrow TFFF FTIT TT$ ; Repairing MSG	$MS_{t-1} = CM_{t-1} \oplus CXM_{t-2} \oplus MAC_{t-1}$ ; False Contrived MSG
$CXM_{t-1} \rightarrow TFFF FTIT TT$ ; MS $\oplus$ CM Pres Result	$CXM_t = MS \oplus CM$ ; Pres unTrue Result
$CXM_{t-2} \rightarrow TFFT FTIT TT$ ; Previous Result	$CXM_{t-1} \rightarrow TFFF FTIT TT$ ; Previous Fixing Result
$MAC_{t-1} \rightarrow TFFF FTIT TT$ ; $CXM_{n-1} \oplus CXM_n$	MAC <sub>t</sub> $\rightarrow$ Know from valid sequence; Given
$MFB_{t-1} \rightarrow TFFT FTIT TT$ ; Lower FB Store Out	$MFB_t \rightarrow TFFF FTIT TT$ ; Lower FB Store Out
$NEWTMBT_t=MFB_{t-1} \oplus TMBT_t \rightarrow TFFT FTIT$	$NEWTMBT_{t+1}=MFB_t \oplus TMBT_{t+1} \rightarrow TTTT TTTT TT$
On Next Clock- Complemented Bits Enter the TMB REGBANK	On Next Clock– TMB Tier Bank values Right Shifted & TMB Tier Band Value is "DE"Contaminated
In order to attempt "Clean" the 3 Top Stores, For the 3rd, 4th, and 5th Clocks the Adversary "Remembers" Previous Result $CXM_{n-1}$ , Learns the $CM_n$ , the received Bottom Store & XOR Knows TrueMAC <sub>n</sub> from the valid sequence	$MS_n = CM_n \oplus CXM_{n-1} \oplus MAC_n$ ; False MSG  $CXM_n = CM_n \oplus MS_n$ by definition- the untrue Result for the Next Clock
It is necessary to generate 3 True NEWTMBTs, but the 4th cannot "fix" the Result Store, and output a valid feedback value.	
At 4 <sup>th</sup> 5 <sup>th</sup> CLK Bot S&XOR is still Contaminated!!	At the 6th Clock in a successful single track feedback configuration, only the Previous Result would have remained false & the one more contrived MSG could not finalize the false sequence. As shown in Table 3 from the 2nd clock on, the Super Tier generates false feedback to itself, and maintains the Data Churn in a constant random state.
$CM_{t+1} \rightarrow$ A random value; Bottom S&X-Learned	$CM_{t+3} \rightarrow$ Not True as the Previous Result is random.
$MS_t \rightarrow$ Contrived; False Contrived MSG	$MS_{t+2} \rightarrow$ The Last Contrived MSG in the failed attempt
$CXM_{t+1} \rightarrow MS \oplus CM$ ; Pres unTrue Result	$CXM_{t+3} \rightarrow$ The last failed Result in the attempt
$CXM_t \rightarrow$ Previous Fixing Result	$CXM_{t+2} \rightarrow$ The Previous Fixing Result
$MAC_{t+1} \rightarrow$ From the known sequence; Known True	$MAC_{t+3} \rightarrow$ Known True – Given
$MFB_{t+1} =$ The Previous MAC; Lower FB Store Out	$MFB_{t+3} \rightarrow$ Lower FB Store Out
$NEWTMBT_{t+2}=MFB_{t+1} \oplus TMBT_{t+2} \rightarrow TTTT TTTT$	$NEWTMBT_{t+4}=MFB_{t+3} \oplus TMBT_{t+4} \rightarrow TTTT TTTT$

Table 1- Inserting a False Message Word; maintaining the TMB Tier Register Bank in a valid state

**Super Tier Contamination caused by a False Message Sequence (Page 2) which temporarily does not affect stages in the Top, Middle & Bottom Register Bank Tiers. Inputs from Table 1**

0'th Clock – All is well	1st Clock
Bottom Store & XOR output is the Cipher Mask	Contaminating 3 bits in the Message Word
$CM_{t-3} \rightarrow TTTT TTTT TT$ ; Bottom Store & XOR	$CM_{t-2} \rightarrow TTTT TTTT TT$ ; Bottom Store & XOR
$MS_{t-3} \rightarrow TTTT TTTT TT$ ; Real MSG	$MS_{t-3} \rightarrow TFFT FTTT TT$ ; Contaminating MSG
$CXM_{t-3} \rightarrow TTTT TTTT TT$ ; $MS \oplus CM$ Pres Result	$CXM_{t-2} \rightarrow TFFT FTTT TT$ ; $MS \oplus CM$ Pres Result
$MMIX_{t-4} \rightarrow TTTT TTTT TT$ ; $f_{nr}(CXM_{t-3})$	$MMIX_{t-2} \rightarrow TFFT TTTT TT$ ; $f_{nr}(CXM_{t-2})$
$SFB_{t-3} \rightarrow TTTT TTTT TT$ ; $MMIX_{t-4}$	$SFB_{t-2} \rightarrow TTTT TTTT TT$ ; $MMIX_{t-3}$
$NEWST_{t-2}=SFB_{t-3} \oplus ST_{t-2} \rightarrow TTTT TTTT TT$	$NEWST_{t-1}=SFB_{t-2} \oplus ST_{t-1} \rightarrow TTTT TTTT TT$
Next Clock- Super Tier is not Contaminated	Next Clock- Register Value is not Contaminated
2nd Clock	3rd Clock Bottom STORE & XOR Contaminated!!
Lower FB Store Outputs Contamination	
$CM_{t-1} \rightarrow TTTT TTTT TT$ ; Bottom Store & XOR	$CM_t \rightarrow$ A random value ; Bottom S&X
$MS_{t-2} \rightarrow TTF TFF TT$ ; Repairing MSG	$MS_{t-1} \rightarrow$ Random contrived; False Contrived MSG
$CXM_{t-1} \rightarrow TTF TFF TT$ ; $MS \oplus CM$ Pres Result	$CXM_t \rightarrow$ A random value; Pres unTrue Result
$MMIX_{t-1} \rightarrow TFFT TTF TT$ ; $f_{nr}(CXM_{t-1})$	$MMIX_t \rightarrow$ Random FB Next Clock; $f_{nr}(CXM_t)$
$SFB_{t-1} \rightarrow TFFT TTF TT$ ; $MMIX_{t-2}$	$SFB_t \rightarrow TFFT TTF TT$ ; $MMIX_{t-1}$
	$ST_{t+1} \rightarrow TTF TTT FT$ ;
$NEWST_t=SFB_{t-1} \oplus ST_t \rightarrow TFFT TTF TT$	$NEWST_{t+1}=SFB_t \oplus ST_{t+1} \rightarrow TTF TTF FT$
On Next Clock- Complemented Bits Enter the HYBRID REGISTER BANK COMBINER	Five toggle bits in the Super Tier, as opposed to 3 original toggles in the TMB Tier Bank
At the fourth clock, SFB further randomizes the known status of the Super Tier.	At the 5th Clock all Super Tier FBs and values are random.
$CM_{t+1} \rightarrow$ Random Cipher Mask;	
$MS_t \rightarrow$ Random Contrived MSG	
$CXM_{t+1} \rightarrow$ Random Result	
$MMIX_{t+1} \rightarrow$ Permuted Random Result ; $f_{nr}(CXM_{t+1})$	
$SFB_{t+1} \rightarrow$ Random FB; $MMIX_t$	
$ST_{t+2} \rightarrow$ Super Tier Segment $TTF TTF FT$	
$NEWST_{t+2}=SFB_{t+1} \oplus ST_{t+2} \rightarrow$ Completely Random	

Table 2- Demonstrating False Word corruption of the Super Tier

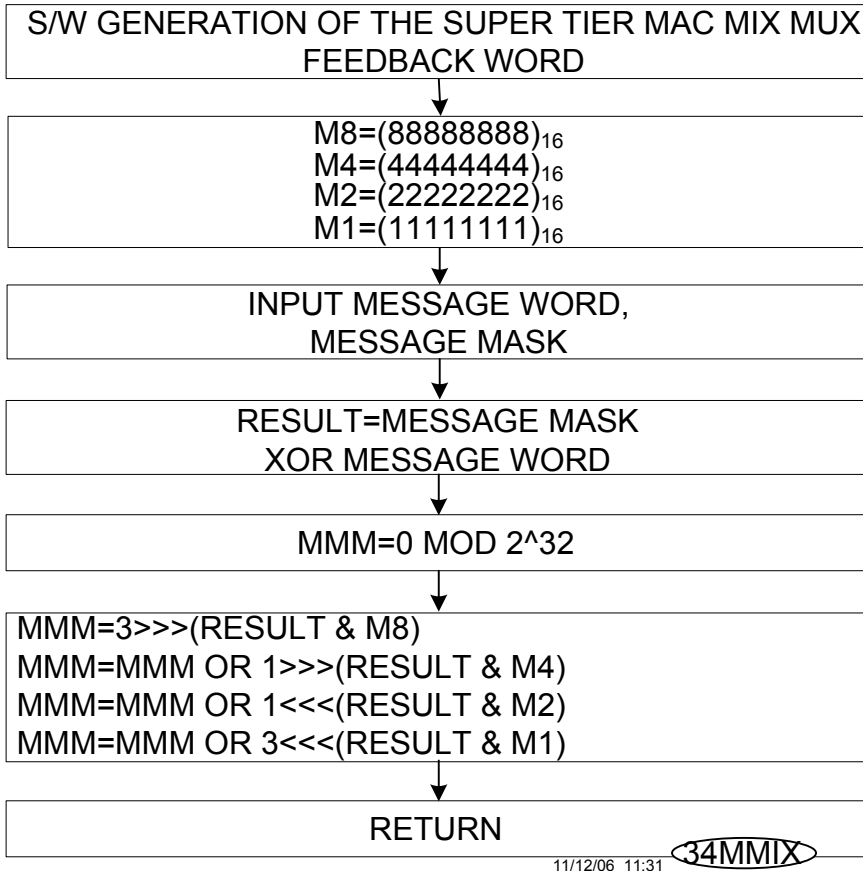


Fig. xxx The MAC MIX Transformation (Software)

References:

- [haifa] E. Biham & O. Dunkelman, A Framework for Iterative Hash Functions, NIST Hash Forum 2006, August, 2006, Santa Barbara.
- [zk-ccc] C. Gressel, A. Hecht, N.T. Courtois, G.V.Bard, ZK-Crypt Circuit Concept Drawings, FortressGB, [www.fortressgb.com](http://www.fortressgb.com), London & Omer, January 2009.
- [zk-code] A. Hecht, ZK-Crypt C Code Simulator, FortressGB, [www.fortressgb.com](http://www.fortressgb.com), London & Omer, January 2009.
- [zk-algo] A. Hecht, O. Dunkelman<sup>1</sup>, C. Gressel, ZK-Crypt Algorithmic Specification, FortressGB, [www.fortressgb.com](http://www.fortressgb.com), London & Omer, January 2009.
- [zk-a-z glos] C. Gressel, O. Dunkelman<sup>1</sup>, The A-Z Guide to the ZK-Crypt, An annotated glossary, eSTREAM website, vers 3, December 30, 2006.
- [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, December 30, 2006.

<sup>1</sup> The eSTREAM Versions