

Appendix 2 Dual Track Feedback - Proof of Preclusion of Message Modification

ZK-Crypt Feedback

As was shown in previously in the ZK-Crypt II, using a classic Data Authentication attack method, an adversary can find a sequence of Message Words that can start with the insertion a first false Message Word, and subsequently not leave any trace of falsification of the subsequent states of the Random Controller, the Register Bank, or the Data Churn. Here we prove that by generating two very different feedbacks, each affecting uncorrelated pseudo-random sequences, we obviate finding a sequence of Message Words that can insert a first false Message Word and can provably not leave any trace of falsification in the subsequent states of the Random Controller, the Register Bank, or the Data Churn.

Dense linear feedback degrades random statistics. In the ZK-Crypt II Cipher Mode, we were only able to recirculate sparse feedback (an average of four '1's).

With the dense SuperMIX transformed feedback to the Super Tier in the Register Bank, we believe that we have solved the dense feedback anomaly with uncorrelated feedback, such that the output of the Super Tier serves to randomize all variables in the Data Churn in both Cipher and MAC modes of operation.

The MAC MIX Reverse Nibble Displacement Transformation

The MAC MIX transformation in Fig. Appx-3 is efficient in multi-metal layer silicon (standard in security and microcontroller chips), and not difficult to implement in firmware [zk-ccc Fig. 34MMX]. Each nibble (a half byte) is reversed (close linked without long metal link propagation delays). The input to the MAC MIX in the ZK-III is the Present Result, simply the Message Word XORed to the Cipher Mask.

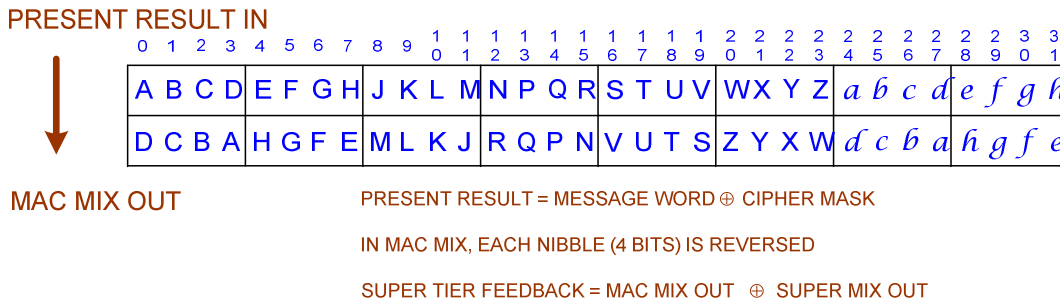


Fig. Appx-3[15]: MAC MIX Nibble Displacement.

Example 1– Two Tracks with the Same Two Cycle TMB Tiers Reconciling Input

The top two vectors of Fig. Appx-4 show how four fraudulent Lower Feedback bits at the first clock cycle are reconciled to a true value in the second clock cycle, as happened in the TMB tiers. If the same four complemented bits were input into the MAC MIX filter, we would see the output as depicted in the bottom two vectors. Four original false bits would "leave" 8 unreconciled bits in the Super Tier.

Here, Message Word MES_{i-2} (Lower Feedback, $LFBD_{i-1}$) index bits 4, 9, 19 and 26 are complemented, causing the complementations **E', K', V'** and **c'**. This complements bits 4, 9, 19 and 26 in the TMB Tiers, and bits 7, 10, 16 and 25 in the Super Tier. In the next clock the complemented $LFBD_i$ feedback index bits 5, 10, 20 and 27 complement (and reconcile) the complemented bits, **E', K', V'** and **c'** as they move into the 5th, 10th, 20th and 27th cells of the TMB Tiers.

Simultaneously, if the MAC MIX displacement filter had received the same input in the second clock cycle, complemented index bits 5, 10, 20 and 26 would be displaced to the 6th, 9th, 23rd and 24th cells of the MAC MIX output. In addition, the MAC MIX complemented index bits from the first clock 7, 10, 16 and 25 shift to index positions 8, 11, 17 and 26 on the second clock. A total of 8 bits in the Super Tier would be complemented by 4 fraudulent bits that were reconciled in the TMB Tiers.

A FALSE (COMPLEMENTED) BIT IN THE J'TH BIT OF THE 3 TIER TMB REGISTER BANK IS RECONCILED BY THE J+1'TH (COMPLEMENTED) FALSE BIT IN THE NEXT CLOCK

1) THE 1ST FALSE LINEAR FEEDBACK ← 1ST VALID FEEDBACK ⊕ 4 FALSIFYING "1" BITS

A B C D E F G H J K L M N P Q R S T U V W X Y Z a b c' d e f g h

2) THE 2ND CONTRIVED WORD TO RECONCILE THE 4 FALSIFIED BITS NOW SHIFTED 1 STEP TO THE RIGHT

φ A B C D E F G H J K L M N P Q R S T U V W X Y Z a b c' d e f g

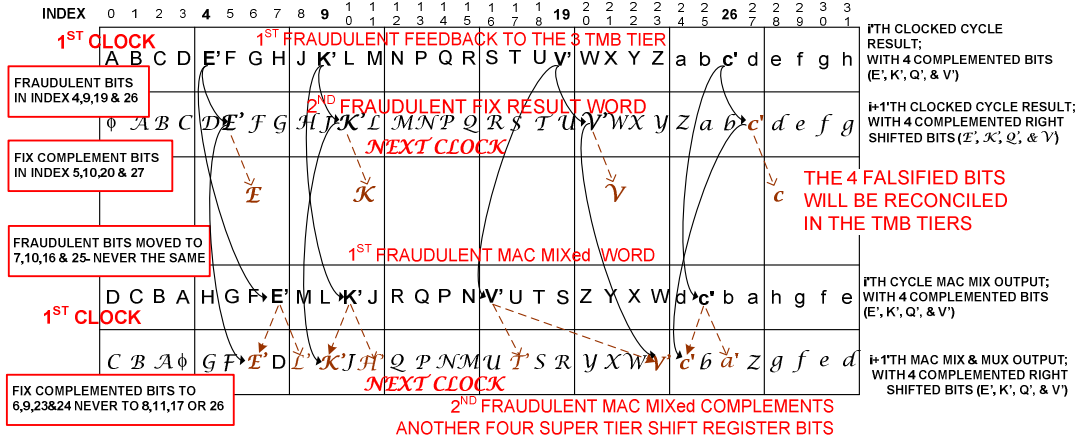


Fig. Appx-4[15]: Complementeds Bits Input into the MAC MIX Filter and the Lower FB Store

Example 2 – The Two Tracks with the Real Two Cycle Reconciling Input

Note, however, that the complemented 4, 9, 19 and 26 index bits from the Message Word, NWR, of the first false cycle are stored in the Result Store, to be output, PVR, at the second reconciling cycle. (See Fig.xxx Appx-6). The Previous Result, PVR and the second fraudulent reconciling Message Word are XOR summed to produce the reconciling Lower Feedback (the second falsified feedback word). The Adversary knows that the reconciling TMB Tier Lower Feedback bits are the first false bits shifted one bit to the right (the first false D-Word vector divided by 2 where the LS bit is by definition true).

As in Appendix A-

- 1) All false or most probably false variable words are designated in **Bold**, e.g., **CIP_{j+1}**. We underline provably false variables, e.g., MES_{j+1}.
- 2) Often we cannot prove that a single word variable is false (or true), but we can prove that the composite expression is false, where we underline the expression, e.g., CIP_x ⊕ MES_x.
- 3) We deal with "false value vectors" where '1's designate false bits and '0's signify the true original bits.

For the first two cycle feedbacks, only generated false bits emanate from the first two false Message Words, as all 32 Bit Word Manipulator variables are in a true state, for the 0'th and 1'st cycles. Remember from Appendix A, a Result false vector of a present Message Word (Cipher Mask ⊕ Message Word), is "XORed into" a tier after two cycles; i.e., one cycle to load into a Feedback Store, a second cycle to XOR into TMB Tiers.

Explicitly, these are the only false value vectors that can falsify and rectify the TMB Tiers: (Fig.xxx Appx-6)

I MES₀ = NWR₀ = LFB₀; as the Cipher Mask, CIP and Previous NWR, (PVR), are true, where the Message Word, MES₀, is an "auspicious" false word that defines a unique subsequent rectifying word, which returns the TMB Tiers to a true state. There are many such auspicious words.

II LFB₁ = LFB₀ ⊕ MES₁; from **I**, the Lower Feedback false value vector, LFB₀ ≡ MES₀ and as the Cipher Mask, CIP₁ is still true, MES₁ is the second Present Result false vector,

III LFB₁ = LFB₀ / 2 = MES₀ / 2; the single valued second false LFB vector is a right shift of the first Lower Feedback vector; else first false shifted bits cannot be re-complemented, e.g., made true. Note that the left hand bits in all TMB Tiers are true, because the MS

bits of all nLFSRs in the previous cycle were true; as the auspicious first false word was chosen so as not to complement MS bits of the nLFSRs.

IV $\underline{LFB}_1 = \underline{MES}_0 / 2 = \underline{MES}_0 \oplus \underline{MES}_1$; we have proved that $(\underline{MES}_0 / 2)$ is the only possible reconciling feedback word, in II & II; and we proved that $\underline{MES}_0 \oplus \underline{MES}_1$ represents the false value i'th Lower Feedback vector as CIP_0 and CIP_1 are both true, as the LFB feedback is active, XORed into the TMB Tiers, 2 clocks later.

V $\underline{MES}_1 = \underline{NWR}_1 \neq \underline{LFB}_1$; as the Result Store outputs the false \underline{MES}_0 , and from equation II, as addition and subtraction are identical in modulo 2 arithmetic-

VI $\underline{MES}_1 = \underline{LFB}_0 \oplus \underline{LFB}_1 = \underline{MES}_0 \oplus \underline{MES}_0 / 2$; the false bits in the contrived Message Word.

The falsified and reconciled results:

$\underline{TMB}_0 = \underline{LFB}_0 = \underline{MES}_0$; \underline{TMB}_0 , the first false value superimposed into the TMB Tiers-

where the false right shift value that is moving into the TMB registers - $\underline{TMB}_0 / 2 = \underline{TMB}_1$

$\underline{TMB}_1 \oplus \underline{LFB}_1 = \underline{MES}_0 / 2 \oplus \underline{LFB}_1 = \underline{LFB}_1 \oplus \underline{LFB}_1 = 0$ (Reconciled)

Following the above equations where the false index bits of Fig. Appx-4, are 4, 9, 19 and 26:

I (0000 1000 0100 0000 0001 0000 0010 0000); $\underline{MES}_0 = \underline{LFB}_0$

\oplus

II (0000 0100 0010 0000 0000 1000 0001 0000); $(\underline{MES}_0) / 2 = \underline{LFB}_1$

=

VI (0000 1100 0110 0000 0001 1000 0011 0000); \underline{MES}_1 generates TMB reconciliation.

The Previous Result, \underline{PRV} , is XORed into the Lower Feedback, \underline{LFB} , but not into the Super Map Feedback, \underline{SUP} , as depicted in Fig. Appx-6.

Remember- the false Message Words were generated 2 cycles before being summed into the tiers.

What happens, simultaneously to the Super Tier:

\underline{SUP}_0 , the first false vector is a function of the Present Result, only, as the SuperMIX feedback is irrelevant; it will be affected by \underline{MES}_0 two cycles later; and as the and as CIP_0 is true, the Present Result false vector, $\underline{PRV}_0 = \underline{MES}_0$

VII $\underline{SUP}_0 = f_{\text{MMX}}[\underline{MES}_0] = \underline{STO}_0$; \underline{STO}_0 is the first falsified vector superimposed into the Super Tier (the MAC MIX filtered NWR Present Results),

\underline{SUP}_1 , the next false vector is a function of the Present Result only, as the SuperMIX feedback is still true as it will be affected by \underline{MES}_1 two cycles later; and as CIP_1 is true, the Present Result false vector, $\underline{PRV}_1 = \underline{MES}_1$

VIII $\underline{SUP}_1 = f_{\text{MMX}}[\underline{MES}_1]$; as the Cipher Mask, CIP_1 , was still true when the second false (reconciling the TMB Tier) Message was generated, then the SuperMIX output was also true, and the second Super Tier false feedback vector would be the f_{MMX} transform on the second false Message Word,

and the falsified bits simultaneously generated with the TMB reconciliation-

IX $\underline{STO}_1 = \underline{STO}_0 / 2 \oplus \underline{SUP}_1$; \underline{STO}_0 moved one bit to the right is XORed to the second MMX 'd feedback. In this example \underline{STO}_1 is not all zeroed,

i.e., $\underline{STO}_0/2 \neq \underline{SUP}_1 \neq \underline{STO}_1 \neq 0$.

VII (0000 0001 0010 0000 1000 0000 0100 0000); $SUP_0 = STO_0 = f_{MMX} [MES_0]$,

VIII (0000 0011 0110 0000 1000 0001 1100 0000); $SUP_1 = f_{MMX} [MES_1]$,

\oplus

(0000 0000 1001 0000 0100 0000 0010 0000); $\underline{STO}_0/2$, shifting \underline{STO}_0 ,

=

IX (0000 0011 1111 0000 1100 0001 1110 0000); $\underline{STO}_1 = \underline{STO}_0/2 \oplus \underline{SUP}_1 \neq 0$.

The example shows a case where a false MES_0 is followed by (the only possible) TMB Tier reconciling MES_1 which leaves 12 random false traces in the Super Tier.

This disparate feedback feature is doubly important, as the dual track feedback obviates simple simultaneous logic manipulation of the Super Tier and the TMB tiers. It shows that we affect separate uncorrelated pseudo-random functions in disparate ways, at each clock cycle.

Note that a false Message Word index bit 12 would cause an internal feedback error in the top left nLFSR in the Register Bank. The false feedback would falsify bits 0,3,4,6,9 and 10 in the nLFSR at the next clock cycle, see Fig. 5 and Table 1. This aberration would be unique to one nLFSR. Subsequent simultaneous reconciliation of this single register and the whole Register Bank with MAC feedback would be impossible. If we skip the optional check, the test is generic, e.g., nLFSRs could be any length.

Proving that the two step reconciliation of the TMB Tiers leaves behind a false value in the Super Tier, proves also there will be a false output from the Register Bank Combiner, RBC. We assume that at least either the Top or Intermediate Store & XOR output values are immediately false. (If both Store & XORs are true - the proof in the following rigorous proof **Step V**, shows that the attack fails sooner than expected.)

Following falsification and reconciliation of the Register Bank, true feedback must be sustained to both the Super Tier and the TMB Tiers, else the condition of the Register Bank and eventually the Random Controller would obviate short term reconciliation. We will prove that there is no Message Word generated feedback that can sustain the Register Bank in a true condition for more than two cycles, following reconciliation.

As our intention is/was to find, even with lowest probability, an attack that could succeed, we choose to falsify and reconcile in two successive clock cycles. Reconciling in a third, fourth or up to the 12th cycle is possible, but lowers any chance of reconciling the Register Bank for even one clock cycle. It is easily shown that delayed reconciliation has a very low chance of success as:

- a) MES_0 could include fewer false bits, lest a false bit complements an MS nLFSR feedback bit;
- b) as TMB tiers are randomly clocked; therefore it is less likely that affected tiers be clocked simultaneously would be less likely;
- c) at the first delayed reconciliation cycle the Super Tier feedback includes false feedback from the Data Churn (not only from the Result/Feedback Processor); so that,
- d) the Super Tier will be further convoluted, with the more distinct possibility that the Super Tier will transmit false signal bits to the Top Control Unit of the Random Controller.

Assuming that the adversary successfully reconciled the TMB Tiers, he would have completed the equivalent of **Step V**, and would proceed to **Step VI** in the following rigorous proof. All delayed false Message Words that can be generated are equivalent to one of a reduced subset of the $2^{31}-1$ possible words; e.g., FFFF FFFC can only be one clock shift delayed to become 7FFF FFFA without flipping the MS nLFSR internal feedback and FFFF FFFE cannot be delayed for even one clock cycle. FFFF FFFC is a Message Word that is in the search subset of all 2^{32} possible words.



The above nine step algorithm is formalized in the flow chart of Fig. Appx-5. Remembering that index bit 31, the MS bit, cannot be flipped, progressing from 2 to $2^{32}-2$, when incrementing by 2, we perform an exhaustive search of all the possible flipped words. If the result, $BADFALSWRD = 0$, the program proves the efficacy of the ZK-Crypt III feedback strategy for repulsing the classic Message Modification attack in a two step procedure. This proves that there is no combination of false flipped bits in a ZK-Crypt Message Word that can be reconciled in two cycles, in both the Super Tier and the TMB Tiers.

Note the "Optional Check" in Fig. Appx-5 is valid for the defined length configurations of the ZK-Crypt nLFSRs. Eliminating testing of Message Words that would trigger false nLFSR feedback, shortens the generic test by a factor of 32. The generic test takes less than 10 minutes; the option is irrelevant. The search proved exhaustively over all of the $2^{31}-1$ possible complemented feedback word pairs, that there is no falsified word pair that simultaneously complements and reconciles both the TMB Tiers and the Super Tier in the ZK-Crypt III.

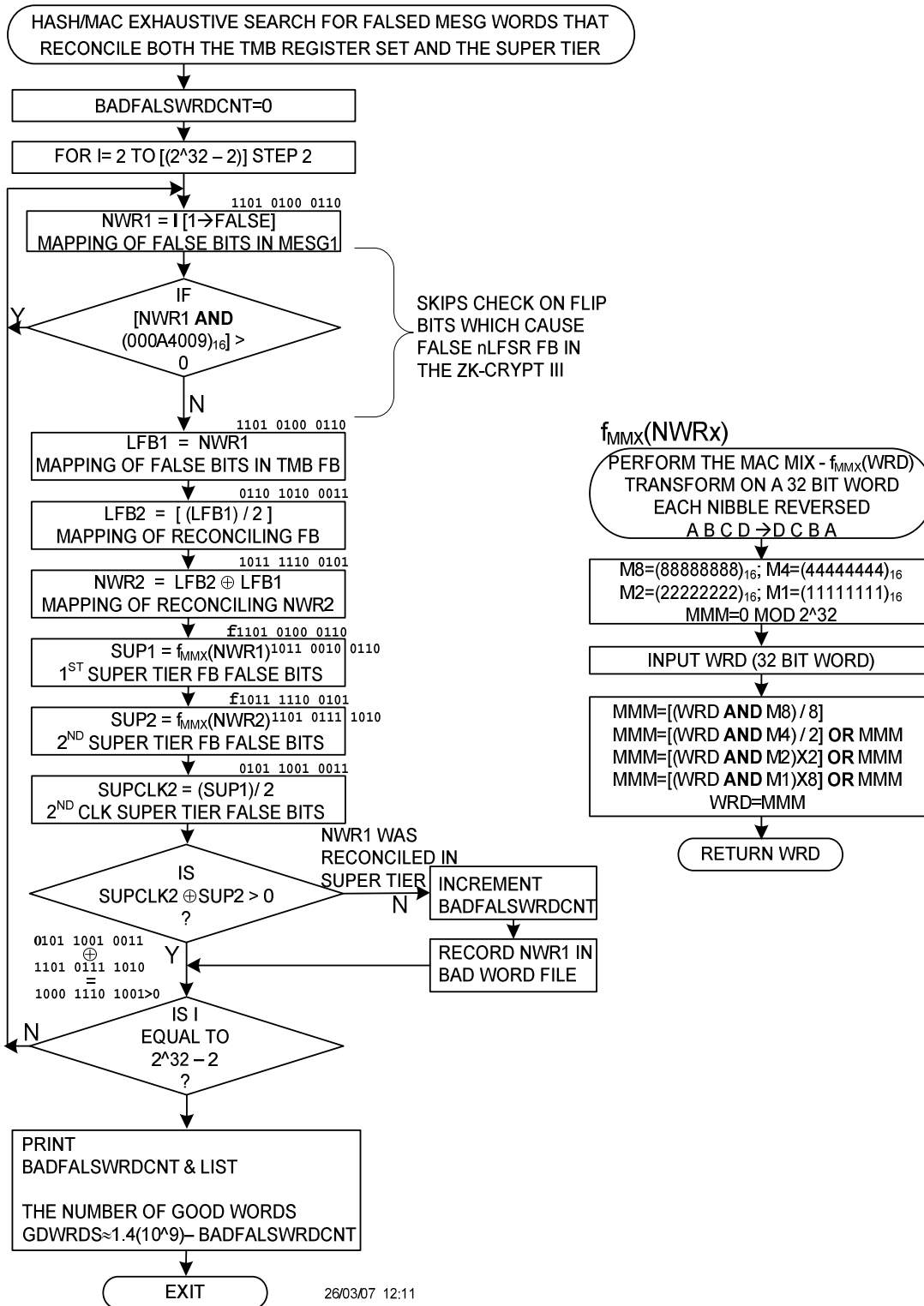


Fig. Appx-5[15]: No Single Cycle False Word Reconciliation in the ZK-Crypt III Register Bank

As BADFALSWRDCNT=0; there is always a difference between the only word that can reconcile the TMB Tiers, and the only single word that could reconcile Super Tier, in the single step false/reconcile clock sequences.

Fig. Appx-6 depicts the ZK-Crypt III MAC Feedback mode in its entirety, including the additional 24 bit Counter Mask feeding the Super Tier, as used in Data Authentication, only.

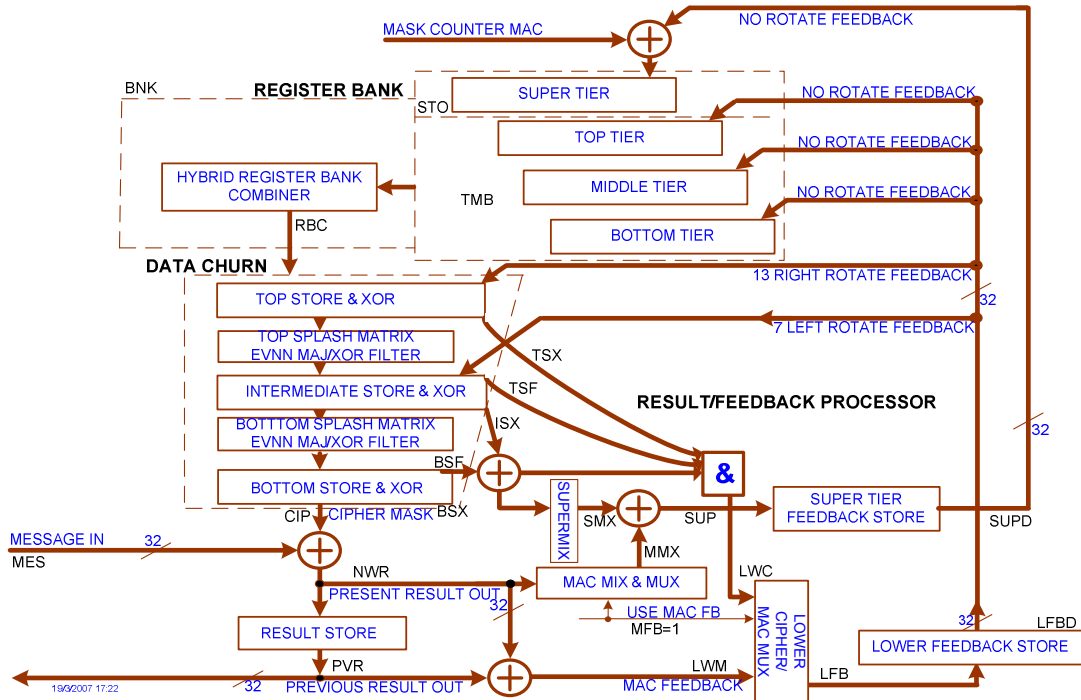


Fig. Appx-6[15]: The ZK-Crypt III Dual Track Feedback Strategy (see new enhanced design)

The SuperMIX Transform is Active in both the Ciphering and the MAC Processes

The SuperMIX displacement is similar to the MAC MIX displacement transformation, with the exception that the reverse nibbled output is eight bit right rotated. The 8 bit shift slightly increases silicon real estate, but decorrelates the shared inputs of the SuperMIX feedback from the non-linear Lower Cipher feedback function.

THE SUPERMIX ROTATES EACH INPUT NIBBLE 8 CELLS TO THE RIGHT & ALSO REVERSES THE BITS OF EACH OUTPUT NIBBLE

INPUT	A	B	C	D	E	F	G	H	J	K	L	M	N	P	Q	R	S	T	U	V	W	X	Y	Z	<i>a</i>	<i>b</i>	<i>c</i>	<i>d</i>	<i>e</i>	<i>f</i>	<i>g</i>	<i>h</i>
$f_{NR\&SHIFT}$ OUTPUT	<i>d</i>	<i>c</i>	<i>b</i>	<i>a</i>	<i>h</i>	<i>g</i>	<i>f</i>	<i>e</i>	D	C	B	A	H	G	F	E	M	L	K	J	R	Q	P	N	V	U	T	S	Z	Y	X	W

AS WOULD AFFECT THE JKLM & NPQR NIBBLES

INPUT	J	K	L	M	N	P	Q	R	S	T	U	V	W	X	Y	Z
OUTPUT	D	C	B	A	H	G	F	E	M	L	K	J	R	Q	P	N

Fig. Appx-7[15]: The SuperMIX Transform

The SuperMIX displacement does not affect the two clock cycle MAC TMB Tier reconciliation process, as the non-valid SMX is XORed to the Super Tier two cycles after the reconciliation cycle.

In Cipher Mode the SuperMIX supplies dense cipher feedback, decorrelated from the sparse Lower Cipher (TMB) Feedback.

We show that with the SuperMIX/ MAC MIX filters, there is provably no chance of short term forging of a false MAC Message Word in the ZK-Crypt III.

Analyzing a Fraudulent Word Attack on the ZK-Crypt III

In the following analysis, we prove that a 2 step fraudulent word reconciliation strategy for the ZK-Crypt III does not work because the TMB and the Super Tiers of the Register Bank cannot be sustained in the short term in a valid state. Invalid Lower Feedback corrupts both the TMB Tiers and the Data Churn and would obviate reconciliation, as will be seen. One random word XORed to the Super Tier can always reconcile the tier's condition for one clocked step. If a false bit or bits corrupts MS bit(s) of one or any nLFSRs in the TMB Tiers, reconciliation is impossible, as the tiers would have non-equal false vectors obviating future false Message Word reconciliation.

Reviewing the feedback variables in the ZK-Crypt III, remembering that these equations relate to false word vectors; e.g., if $CIP_x=0$, all bits of CIP_x are true.

The MAC MIX output, MMX_x , is the f_{MMX} transformation of the Present Result, NWR of Figure Appx-3;

$$A) \quad \underset{\text{Generated Feedback}}{MMX_x} = \underset{\text{EMMX Filtered Present Result}}{f_{MMX}} [CIP_x \oplus MES_x]; \text{ } MMX_x \text{ is true if } CIP_x \oplus MES_x, \text{ the Present Result, is true;} \\ \text{else } MMX_x \text{ is a pseudo-random number.}$$

The SuperMIX output SMX_x is the f_{SMX} transformation of the XORed sum of the output of the Intermediate Store & XOR, ISX_x , and the output of the Bottom Splash EVNN MAJ/XOR filter, BSF_x .
 BSX_x , the output of the Bottom Store & XOR is by definition, the Cipher Mask, $CIP \equiv BSX_x$.

$$B) \quad \underset{\text{SuperMIX Output}}{SMX_x} = \underset{\text{fSMX Filtered Input}}{f_{SMX}} [ISX_x \oplus BSF_x]; \text{ the } SMX_x \text{ is true if the sum, } ISX_x \oplus BSF_x, \text{ is true.;} \\ \text{else, } SMX_x \text{ is a pseudo-random number.}$$

C) The Super Tier Feedback, SUP_x , may be true, only if the sum, $MMX_x \oplus SMX_x$, is true.

D) RBC_x , the Register Bank Combiner, is provably true, only if the Register Bank's, (BNK_x 's) all four tiers' (3 in the TNB and 1 in the STO) outputs are true.

E) ISX_x & BSF_x are provably true, only if RBC_x and the Top and Intermediate Store & XOR outputs are true, TSX_x and ISX_x respectively.

Proof that False Message Words cannot be Inserted in a Valid MAC Sequence Causing the Register Bank to be Reconciled in the Short Term

This proof encompasses the proof that the classic Fraudulent Word Attack cannot succeed, as shown in Appendix A for the Single Track ZK-Crypt II feedback.

In order to prove that the Register Bank cannot be reconciled in the short term, we must assume that the Adversary is extremely lucky, in Steps III to VI. Then, in Step VII we can prove that such an improbable "lucky" scenario does not exist.

Start:

We assess the situation at the j 'th word, prior to the adversary's first attack word.

– All is well – the ZK-Crypt III is processing a valid Message; and all variables are true.

The Register Bank BNK_j is true, therefore the combiner output, RBC_j is true.

Top Store output TSX_j is true; Intermediate Store output ISX_j is true; and,
Bottom Store output $BSX \equiv CIP_j$ is true.

The Message Word = MES_j is true; the Present Result = NWR_j is true;
the Previous Result = PRV_j is true; the generated and Stored Feedback $LFB_j = LWM_j$ and,
 $LFBD_j$ are the true original "historic" values.

There are many conditions involved in the choice of an "auspicious" word in **Step I**. There are many j 'th words, and in each of the candidate j 'th words and there are up to 2^{28} candidate false Message Words. An adversary who knows the device and its contents can easily find illusive solutions (if they exist) to **Steps I to V**, but to no avail. We will prove that there is no auspicious word that will lead to a successful attack on the Register Bank, therefore the specific choice is irrelevant.

In the following, variables that are provably false appear in **Bold and** are underlined; e.g., $(CIP_{j+1} \oplus \underline{MES_{j+1}})$. Variables that we assume, but do not prove are false appear in **Bold** face type, but are not underlined, e.g., CIP_n . Instants where we suspect that both variables in a composite variable are false, where we can prove that the composite is false, we underline the whole composite function:

$$\text{e.g., } (\underline{CIP_{j+3} \oplus MES_{j+3}}) .$$

Other words are assumed to be true (if only for argument's sake), and are not emboldened.

Step I – The adversary chooses an "auspicious" falsifying Message Word, $\underline{MES_{j+1}}$.

The generated Lower, LFB_{j+1} , feedback is provably false-

$$\underline{LFB_{j+1}} = (CIP_{j+1} \oplus \underline{MES_{j+1}}) \oplus CIP_j \oplus MES_j, \text{ and also the -}$$

Generated Lower FB Present Result NWR Previous Result

$$\underline{SUP_{j+1}} = f_{MMX}[CIP_{j+1} \oplus \underline{MES_{j+1}}] \oplus f_{SMX}[ISX_{j+1} \oplus BSF_{j+1}] \text{ is false.}$$

Generated Super Tier FB fMMXed Present Result on NWR fSMXed Filtered Input

$LFBD_{j+1}, TMB_{j+1}, STO_{j+1}, RBC_{j+1}, TSX_{j+1}, ISX_{j+1}, BSX_{j+1}$ & SMX_{j+1} are true .

The first false feedbacks are "waiting to" be stored into Feedback Stores, $LFBD$ & $SUPD$.

Step II – The adversary calculates a Message Word, $\underline{MES_{j+2}}$ that generates Lower Feedback to complement the one bit rotated to the right fraudulent bits in the TMB Tiers. This reconciliation word will reconcile the TMB Tiers to a true state and provably falsify the Super Tier. (Fig. Appx-5.) The Adversary has no degree of freedom in his choice of $\underline{MES_{j+2}}$.

The generated feedbacks-

$$\underline{LFB_{j+2}} = CIP_{j+2} \oplus \underline{MES_{j+2}} \oplus CIP_{j+1} \oplus \underline{MES_{j+1}} \text{ is false we know that it isn't the original}$$

Generated Feedback Present Result Previous Result

as it must reconcile false bits; and,

$$\underline{SUP_{j+2}} = f_{MMX}[CIP_{j+2} \oplus \underline{MES_{j+2}}] \oplus f_{SMX}[ISX_{j+2} \oplus BSF_{j+2}] \text{ is also provably false.}$$

Generated Super Tier FB fMMX Present Result = NWR fSMX Filtered Input

$TMB_{j+2}, STO_{j+2}, RBC_{j+2}, TSX_{j+2}, ISX_{j+2}, BSX_{j+2}$ & SMX_{j+1} are provably still true .

$\underline{LFBD_{j+2}}$ is false as $\underline{LFB_{j+1}}$ was false .

$\underline{SUPD_{j+2}}$ is false as $\underline{SUP_{j+1}}$ was false .

$\underline{LFBD_{j+2}}$ and $\underline{SUPD_{j+2}}$ are "waiting" to falsely complement the Register Bank and the Data Churn.

$\underline{LFB_{j+2}}$ is "waiting" to follow $\underline{LFBD_{j+2}}$ to reconcile the TMB Tiers to a true value.

$\underline{SUP_{j+2}}$ is "waiting" to follow $\underline{SUPD_{j+2}}$ to further falsify the Super Tier.

Step III – In the following steps a MAC adversary must guess Message Words (MES 's) that will compensate for a false Previous Result and/or false Present and/or Previous Cipher Masks, in order to generate a true Lower Feedback, LFB , to sustain the TMB Tiers (two clocks hence).

In this step, $SUPD_{j+2}$ was XORed into the **STO** (Fig. Appx-6), thereby corrupting the Super Tier- and LFB_{j+2} was XORed into the **TMB** and Data Churn, corrupting with an auspicious word- LFB_{j+3} , $SUPD_{j+3}$, TMB_{j+3} , STO_{j+3} , RBC_{j+3} , TSX_{j+3} , ISX_{j+3} , CIP_{j+3} , MMX_{j+3} & SMX_{j+3} are either assumed or proved false,

and we assume (as the MES_1 was chosen auspiciously) that the TMB can and will be reconciled on the next clock cycle.

The generated feedbacks-

$$LFB_{j+3} = (\underbrace{CIP_{j+3}}_{\text{Present Result}} \oplus \underbrace{MES_{j+3}}_{\text{Previous Result}}) \oplus CIP_{j+2} \oplus \underbrace{MES_{j+2}}_{\text{Previous Result}} \text{ is true,}$$

as the "guessed" Message Word MES_{j+3} probably compensates two false variables.

The Super Tier Feedback-

$$SUP_{j+3} = \underbrace{f_{MMX}}_{\text{Generated Super Tier FB}} [CIP_{j+3} \oplus MES_{j+3}] \oplus \underbrace{f_{SMX}}_{\text{fSMX Filtered Input}} [ISX_{j+3} \oplus BSF_{j+3}]$$

is a random number. With extreme luck it will reconcile the Super Tier's in the 5'th step.

SUP_{j+3} is not the valid feedback, it is the assumed feedback that will reconcile.

LFB_{j+3} is false as LFB_{j+2} was false.

LFB_{j+3} is "waiting" to reconcile the variables in the TMB Tiers, TMB, to a true state.

$SUPD_{j+3}$ is "waiting" with a number that provably cannot reconcile the Super Tier into a true state.

LFB_{j+3} is "waiting" with true Feedback, to "sustain" the TMB Tiers in a true state.

Step IV – In this step, reconciling feedback is XORed into the TMB Tiers, thereby recovering all TMB variables into a true state. The reconciling feedback further corrupts the Data Churn. We have proved, logically and with an exhaustive search that the Super Tier Feedback is not reconciled, so that the BNK and the Data Churn are both false. (See Fig. Appx-5.) The MAC adversary will continue guessing compensating words to generate "historic" original LFBs.

In this step, LFB_{j+3} was XORed into the **TMB** and Data Churn, thereby reconciling the TMB .

The $SUPD_{j+3}$ was XORed into the **STO** thereby further randomizing the Super Tier.

$SUPD_{j+4}$, STO_{j+4} , RBC_{j+4} , TSX_{j+4} , ISX_{j+4} , CIP_{j+4} , MMX_{j+4} & SMX_{j+4} are assumed false, and TMB_{j+4} , LFB_{j+4} are true.

$$LFB_{j+4} = (\underbrace{CIP_{j+4}}_{\text{Present Result}} \oplus \underbrace{MES_{j+4}}_{\text{Previous Result}}) \oplus (\underbrace{CIP_{j+3}}_{\text{Present Result}} \oplus \underbrace{MES_{j+3}}_{\text{Previous Result}}) \text{ is true,}$$

as the "guessed" Message Word MES_{j+4} probably compensates three false variables.

The Super Tier Feedback-

$$SUP_{j+4} = \underbrace{f_{MMX}}_{\text{Generated Super Tier FB}} [CIP_{j+4} \oplus MES_{j+4}] \oplus \underbrace{f_{SMX}}_{\text{fSMX Filtered Input}} [ISX_{j+4} \oplus BSF_{j+4}]$$

SUP_{j+4} is a random number. With extreme luck we assume that it is the true Super Tier feedback which can sustain the Super Tier in a valid state in Step VI.

LFB_{j+4} is true as LFB_{j+3} was true and is waiting to sustain TMB to a true state.

$SUPD_{j+4}$ is random and "waiting" with, a low probability to reconcile the STO_{j+5} .

LFB_{j+4} is "waiting" with true Feedback, to "sustain" the TMB Tiers in a true state in Step VI.

Step V – In this step the TMB remains true, the STO is reconciled by a lucky $SUPD_{j+4}$, Super Tier feedback. The Data Churn remains false. The Result Store (Previous Result) remains false. We "know" that the adversary was very lucky. The MAC adversary will continue guessing compensating words to generate "historic" original LFBs.

If $SUPD_{j+4}$ does not reconcile STO_{j+5} , the attack fails here, as $SUPD_{j+4}$ is single valued for MES_1 .

In this step, LFB_{j+4} was XORed into the **TMB** and Data Churn, sustaining a true TMB ,

and pseudo-random $SUPD_{j+4}$ was XORed into and "luckily" reconciled the **STO** . Now the BNK and RBC are true. If on the next cycle RBC is still true, TSX will be true. (If LFB and RBC are true for 3 more cycles, consecutively, TSX, ISX and BSX are reconciled).

TSX_{j+5} , ISX_{j+5} , CIP_{j+5} , MMX_{j+5} & SMX_{j+5} we assume are false,

TMB_{j+5}, STO_{j+5}, RBC_{j+5} are true, as the random SUP (we assumed) reconciled the Super Tier.
LFB_{j+4} & SUPD_{j+4} were assumed to be true, to sustain a valid Register Bank.

And the Lower Feedback

$$\text{Generated Feedback } LFB_{j+5} = \underbrace{(CIP_{j+5} \oplus MES_{j+5})}_{\text{Present Result}} \oplus \underbrace{(CIP_{j+4} \oplus MES_{j+4})}_{\text{Previous Result}} \text{ is true,}$$

as the "guessed" Message Word **MES_{j+5}** compensates at least one false variable.

The Super Tier Feedback-

$$\text{Generated Super Tier FB } SUP_{j+5} = f_{MMX} [CIP_{j+5} \oplus MES_{j+5}] \oplus f_{SMX} [ISX_{j+5} \oplus BSF_{j+5}]$$

is a random number. With extreme luck we assume it will sustain true STO_{j+7} in step 7.

LFB_{j+5} is true as LFB_{j+4} was true and is "waiting" to sustain TMB to a true state in step 6.

SUPD_{j+5} is "waiting" with a number we assume (improbably) will reconcile STO in step 6.

LFB_{j+5} is "waiting" with true Feedback, to sustain the TMB Tiers in a true state in step 7.

Step VI – In this step the TMB remains true, a true STO is sustained by a lucky SUPD_{j+5}, Super Tier feedback.

The Data Churn, except for the TSX remains false. The Result Store (Previous Result) remains false. We "know" that the adversary was very lucky. The MAC adversary will continue guessing compensating words to generate "historic" original LFBs.

In this step, LFB_{j+5} was XORed into the TMB and Data Churn, thereby sustaining a true TMB, and pseudo-random SUPD_{j+5} was XORed into and "luckily" reconciled the STO. The BNK and RBC remain true. As the RBC_{j+5} and LFB_{j+5} are true for a second time, TSX will be true. (If LFB and RBC are true for 1 more cycle, ISX and BSF will be reconciled).

ISX_{j+6}, CIP_{j+6}, MMX_{j+6} & SMX_{j+6} are false,

TMB_{j+6}, STO_{j+6}, RBC_{j+6} & TSX_{j+6}, are true, as the random SUP again reconciled the Super Tier.

We assume again that SMX_{j+6} is false; later we will prove that it must be false;

LFB_{j+6} & SUPD_{j+6} are assumed to be true,

And the Lower Feedback

$$\text{Generated Feedback } LFB_{j+6} = \underbrace{CIP_{j+6}}_{\text{Present Result}} \oplus \underbrace{MES_{j+6}}_{\text{Present Result}} \oplus \underbrace{CIP_{j+5}}_{\text{Previous Result}} \oplus \underbrace{MES_{j+5}}_{\text{Previous Result}} \text{ is true,}$$

as the "guessed" Message Word **MES_{j+6}** compensates three false variables.

The Super Tier Feedback-

$$\text{Generated Super Tier FB } SUP_{j+6} = f_{MMX} [CIP_{j+6} \oplus MES_{j+6}] \oplus f_{SMX} [ISX_{j+6} \oplus BSF_{j+6}]$$

SUP_{j+6} is a random number. With extreme luck we assume it might reconcile STO in **Step VIII**.

LFB_{j+6} is true as LFB_{j+5} was true and is "waiting" to sustain TMB to a true state in **Step VII**.

SUPD_{j+6} is "waiting" with a number we assume will sustain a true STO in **Step VII**.

LFB_{j+6} is "waiting" with true Feedback, to sustain the TMB Tiers in a true state in **Step VIII**.

Step VII – In this step the TMB remains true with a luckily guessed Message Word^{*}, the STO is again reconciled by a lucky SUPD_{j+5}, Super Tier feedback. The Data Churn is true, except for BSX=CIP which remains false. ISX and BSF are true as RBC, TOP and ISX are true. The Result Store (Previous Result) remains false. We will question if the adversary could have been very lucky. We also see, also, that the attack could not work, without the anomalies which we will show.

In this step, LFB_{j+6} was XORed into the TMB and Data Churn, thereby sustaining a true TMB, and pseudo-random SUPD_{j+6} was XORed into and "luckily" reconciled STO. The BNK and RBC remain true. As the RBC_{j+6} and LFB_{j+6} were true for a third time, both TSX and ISX are true.

CIP_{j+7} = BSX_{j+7} is still false, and we have an anomaly with MMX_{j+6} & SMX_{j+6}.

TMB_{j+6}, STO_{j+6}, RBC_{j+6}, TSX_{j+6}, ISX_{j+7}, BSF_{j+7} & SMX_{j+7} are true, as SUP once again reconciled the Super Tier ISX_{j+7} is true, making BSF_{j+7} true so that SMX_{j+7} is now true.

And the Lower Feedback can always be contrived:

$$\text{Generated Feedback } LFB_{j+7} = \underbrace{(CIP_{j+7} \oplus MES_{j+7})}_{\text{Present Result}} \oplus \underbrace{(CIP_{j+6} \oplus MES_{j+6})}_{\text{Previous Result}} \text{ is true,}$$

where the Present Result cannot be true, if the Previous Result was not true.

The Super Tier Feedback can no longer be true-

$$\text{Generated Super Tier FB } \mathbf{SUP}_{j+7} = \underbrace{f_{\text{MMX}}[\mathbf{CIP}_{j+7} \oplus \mathbf{MES}_{j+7}]}_{\text{fMMX Present Result on NWR}} \oplus \underbrace{f_{\text{SMX}}[\text{ISX}_{j+7} \oplus \text{BSF}_{j+7}]}_{\text{fSMX Filtered Input}} \text{ where both } \text{ISX}_{j+7} \text{ \& } \text{BSF}_{j+7} \text{ have been reconciled and are true.}$$

If $f_{\text{SMX}}[\text{ISX}_{j+7} \oplus \text{BSF}_{j+7}] = \text{SMX}_{j+7}$ is true, and SUP_{j+7} were true, then

$$f_{\text{MMX}}[\mathbf{CIP}_{j+7} \oplus \mathbf{MES}_{j+7}] \text{ and } [\mathbf{CIP}_{j+7} \oplus \mathbf{MES}_{j+7}] = \text{NWR}_{j+7} \text{ would also be true.}$$

$\mathbf{CIP}_{j+6} \oplus \mathbf{MES}_{j+6} = \mathbf{PVR}_{j+7}$ is by definition false-

then, $\mathbf{LFB}_{j+7} = \text{NWR}_{j+7} \oplus \mathbf{PVR}_{j+7}$,

the valid feedback to sustain the TMB could not also be simultaneously true.

Despite the aforesaid, let's assume that it was possible to maintain the Register Bank in a true sequence, obviously with false Message Words, as the Previous Result would constantly be false-

The generated feedback at the final tail word step can only be-

$$\text{Generated Feedback } \mathbf{LFB}_T = (\underbrace{\mathbf{CIP}_T \oplus \mathbf{MES}_T}_{\text{Present Result}}) \oplus (\underbrace{\mathbf{CIP}_{T-1} \oplus \mathbf{MES}_{T-1}}_{\text{Previous Result}}) \text{ is again true.}$$

The T'th Message Word should be a meaningful Tail not the random \mathbf{MES}_T , necessary to compensate for false \mathbf{MES}_{T-1} .

$$\text{Generated Feedback } \mathbf{LFB}_T = \underbrace{\mathbf{CIP}_T}_{\text{Present Result}} \oplus \mathbf{MES}_T \oplus \underbrace{\mathbf{CIP}_{T-1} \oplus \mathbf{MES}_{T-1}}_{\text{Previous Result}} \text{ where } T > j+7.$$

A true Tail word would obviously have generated, \mathbf{LFB}_T , a false feedback.

In the tag process (see Appendix C) all Messages Words after the T'th word are, by definition, "all zeroes". The adversary has no degree of freedom. If Message Words are equal to zero, then Cipher Mask values constitute Previous and Present Results.

The first MAC Feedback Scramble is false-

$$\text{Generated Feedback } \mathbf{LFB}_{T+1} = \underbrace{\mathbf{CIP}_{T+1} \oplus [00\dots0]}_{\text{Present Result}} \oplus \underbrace{\mathbf{CIP}_T \oplus \mathbf{MES}_T}_{\text{Previous Result}} = \underbrace{\mathbf{CIP}_{T+1}}_{\text{Present Result}} \oplus \underbrace{\mathbf{PRV}_T}_{\text{Previous Result}}$$

as the Tail word was false;

but the second MAC Feedback Scramble would be true, as false feedback corrupts two cycles later-

$$\text{Generated Feedback } \mathbf{LFB}_{T+2} = \underbrace{\mathbf{CIP}_{T+2}}_{\text{Present Result}} \oplus \underbrace{\mathbf{CIP}_{T+1}}_{\text{Previous Result}}$$

now $\mathbf{LFB}_{T+2} = \mathbf{LFB}_{T+1}$ is false,

the third MAC Feedback Scramble feedback is false, as \mathbf{LFB}_{T+1} is inserted into \mathbf{BNK}_{T+3} , corrupting \mathbf{RBC}_{T+2} and the Data Churn-

$$\text{Generated Feedback } \mathbf{LFB}_{T+3} = \underbrace{\mathbf{CIP}_{T+3}}_{\text{Present Result}} \oplus \underbrace{\mathbf{CIP}_{T+2}}_{\text{Previous Result}}$$

at this stage, \mathbf{BNK}_{T+4} remains false as true \mathbf{LFB}_{T+2} feedback cannot reconcile a false Register Bank.

Conclusion: In the ZK-Crypt III, sustaining the Register Bank in a valid state following the insertion of a false Message Word is not possible.

The Super Tier feedback track logically obviates adversarial Message Words from simultaneous logic manipulation of the Super Tier and the TMB tiers.