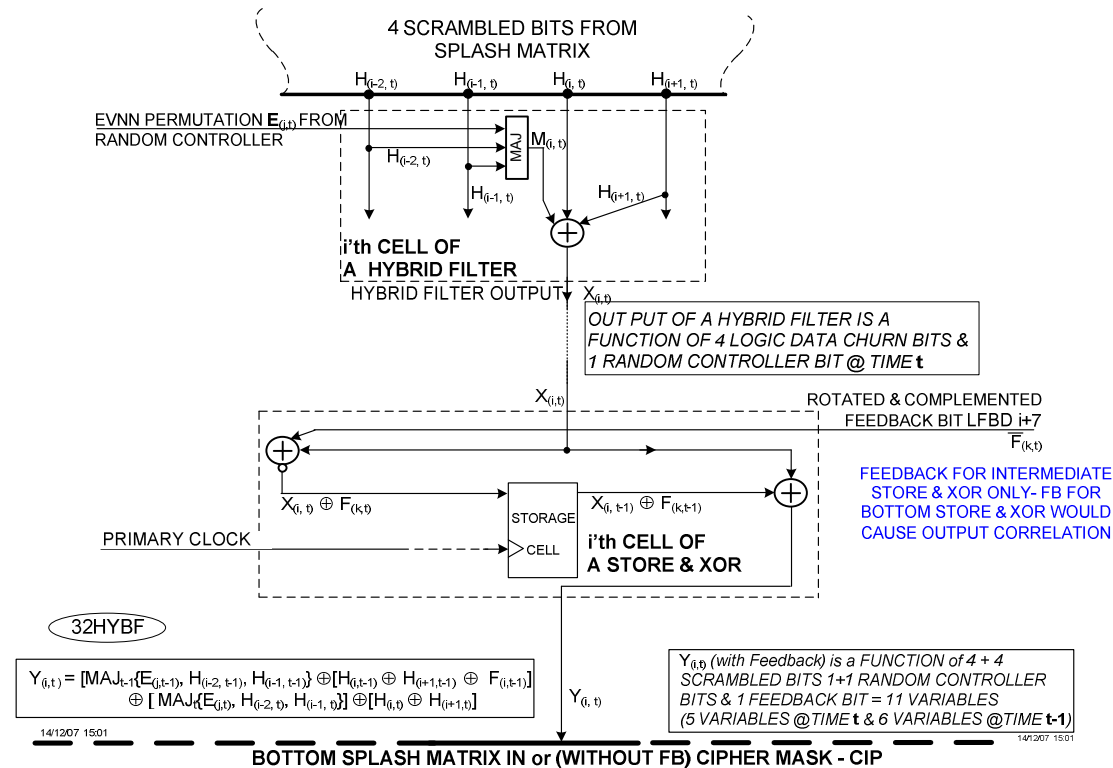


## Chapter 04 Hybrid & Correlation Filters<sup>1</sup>

### Debiasing, Diffusing, Delinearizing and Decorrelating in One Filter

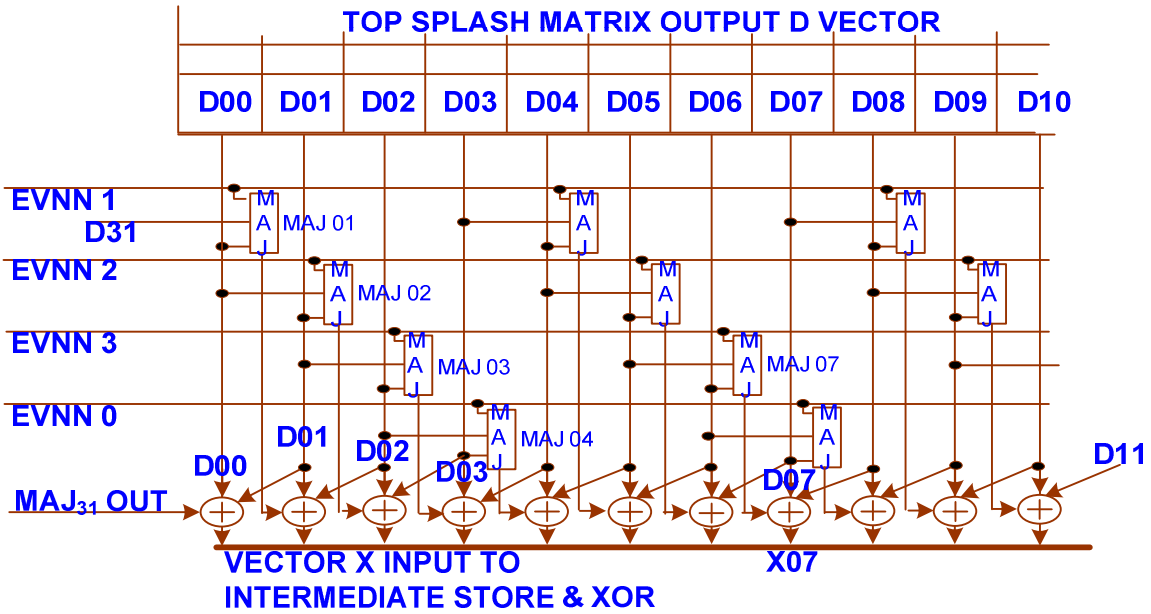
The following figure typifies ZK-Crypt proprietary hybrid diffusing, delinearizing, debiasing and decorrelating of - four scrambled near neighbor data bits; one permutation bit; and one feedback bit; into one output binary variable. The 32 bit hybrid filters, in similar configurations, are strategically placed before each of the Top, Intermediate and Bottom Store & XOR correlation immunizers. The top hybrid filter is found in the 4 Tier combiner of the Register Bank, and the other two precede the Intermediate and Bottom Store & XORs.



**Fig. 1: Combining, Diffusing, Correlation Immunizing & Debiasing in the Data Churn**

The Store & XOR cell serves as a classical correlation immunizer, while it doubles the number of variables in the output equations. The feedback bit,  $F_{(k,t)}$ , is a function of the "present output", so that it is stored to be output as  $F_{(k,t-1)}$  on the next clock. In our analyses in the next section, we only "count" the diffusive variables appearing during a present clock cycle (1st degree), not the cumulative effect (higher degrees) from all of the previous clock cycles. We will see that two clock cycles "down", every memory variable in the Word Manipulator's equations carries a "history" of all the previous variable values, starting from the cipher initialization. Note that  $Y_{(i,t)}$  is a function of 11 variables.

<sup>1 1</sup> References in Chapter 1



$$MAJ_{07} \text{ OUT} = MAJ[(EVNN \ 7 \ \text{mod} \ 4), D05, D06]$$

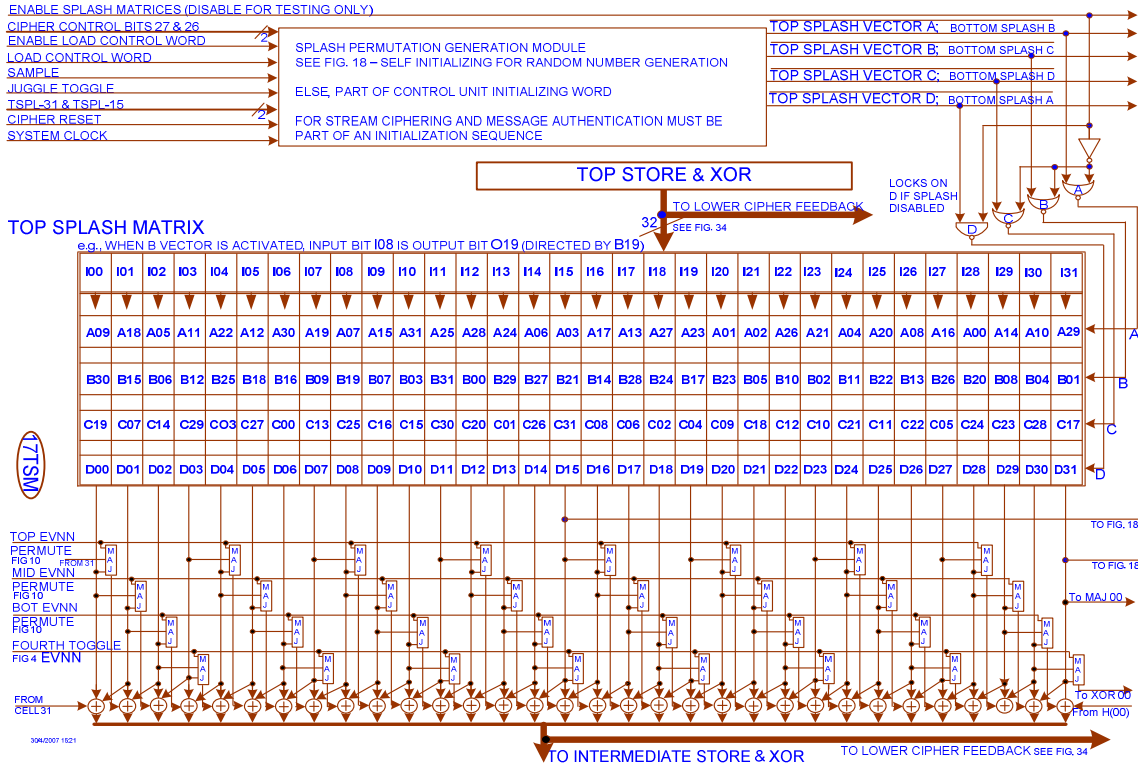
**EVNNFORC**

$$X07 = MAJ[EVNN \ 3, D05, D06] \oplus D07 \oplus D08$$

21/7/2008 15:07

**Fig. 2: Each Hybrid Filtered Outputs is a Function of 5 Inputs**

Obviously, three of four EVNN permutations cause random displacement into at least one of the MAJ filters, such that the Cipher Mask is a pseudo random result of a one-way function.



**Fig. 3: Efficient Hybrid Filtering between Top & Intermediate Store & XOR**



In Fig. 3, each of the EVNN signals strongly biases every fourth MAJ gate output. The output of the MAJ filters therefore is an unbiased strongly correlated string. The XORED sum of two near Splash Matrix neighbor bits inputs an ENS string into the Hybrid Filter.

The input to the Intermediate Store & XOR filter is a debiased string with a very slight residual correlation. The (classic) Intermediate Store & XOR filter typically reduces the residual correlation thereby generating a non-distinguishing Repeated Word merit number.