

Chapter 06 Configuring Tandem and Concatenated ZK-Engines

Future applications anticipate many applications which can efficiently use more than one ZK-Crypt on the CPU chip. With two engines, and programmable feedback connections, double length word processes are possible for maximum security 64 bit word operations, or alternately with one or two CPUs on the same silicon substrate, two standard or proprietary processes may operate simultaneously. We also show an interesting low power concatenation of n engines concatenated to operate on $n \times 32$ words to accommodate anticipated more than 20 Gb/s transmission protocols; which fabs tell us are in preparation.

In all secured hardware applications, we assume that the only degree of freedom that an adversary has is his ability to alter the incoming Message. In the final NIST application we will include our graphic proof of robustness against an attack where an adversary might attempt to use the L/H Engine to allow acceptance a 2nd preimage modified Message in the ostensibly standalone R/H engine. This obviously is not a viable attack method, but is designed to show that even when we double the attacker's degrees of freedom, he is unable to compromise the ZK-Crypt.

In classical hashing procedures, initial conditions are not secret, and the adversary, working with a software emulator knows all. As seen in previous attacks, the knowledgeable adversary could always modify Messages to generate a Lower Feedback reconciling feedback, but by doing so, would have lost all control of the chaining value of the ZK-Crypt Engine.

Side by Side Pairs

NIST Specs ostensibly specify authentication of previously encrypted data. This eminently fits two side by side normal (non-shared feedbacks). One engine (or pair of engines) can be configured for deciphering and the second for Data Authentication. Aside from the initialization phase, and reading the tag, the input to both engines is the same. While inputting the same data to both engines, only the decipher engine is read. At the end of file, only the Data Authenticator output is read.

In this configuration, there is no interaction between the two engines; stored encrypted data is deciphered and authenticated transparently.

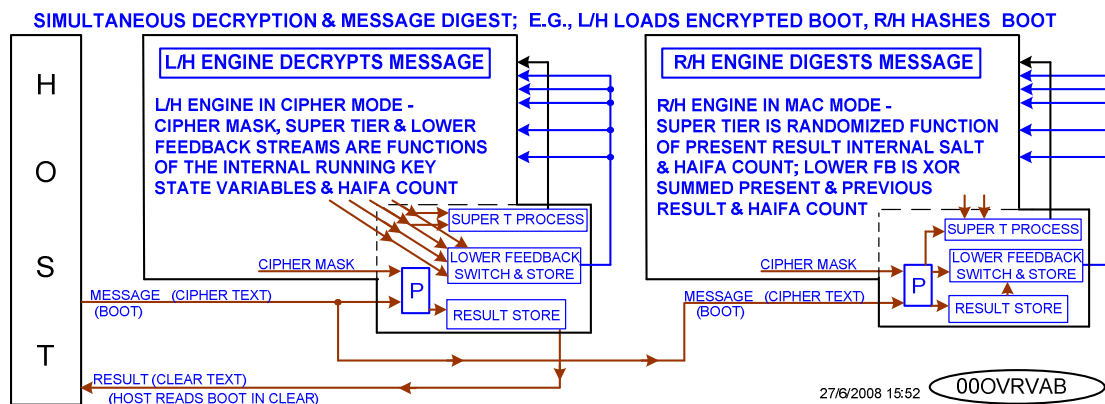


Fig. 1: Concurrent Decryption & Hashing: L/H Decrypts Text; R/H Hashes Same Encrypted Text

Similarly, the L/H engine can encrypt clear text transparently as the CPU moves data from the memory store, wherein the encrypted data is loaded, one clock later, into the R/H engine. The R/H engine simultaneously digests "effectively salted" encrypted data, with one clock latency. We consider this to be more secure, in the event that the data is not confidential, as visual inspection is often an additional desired mode of authentication.

Twined Pairs Operating on Double Words

For both Cipher and MAC Mode operation on double words, Lower Feedbacks are swapped via the R/H Lower Feedback Switch and Store, and likewise the R/H Lower Feedback is fed into the L/H engine. To reduce CPU

processing, a 64 bit DMA configuration can manage insertion of Messages and simultaneous sampling of the Result. Assuming DMA input and output, speed is doubled, and cryptocomplexity is exponentially increased.

Fig. 2 depicts twin paired ZK-Crypt engines, en/decrypting (feedbacks are function of internal binary variables) 64 bit words, with swapped Lower Feedback streams. We will prove the robustness of this configuration on the next phase.

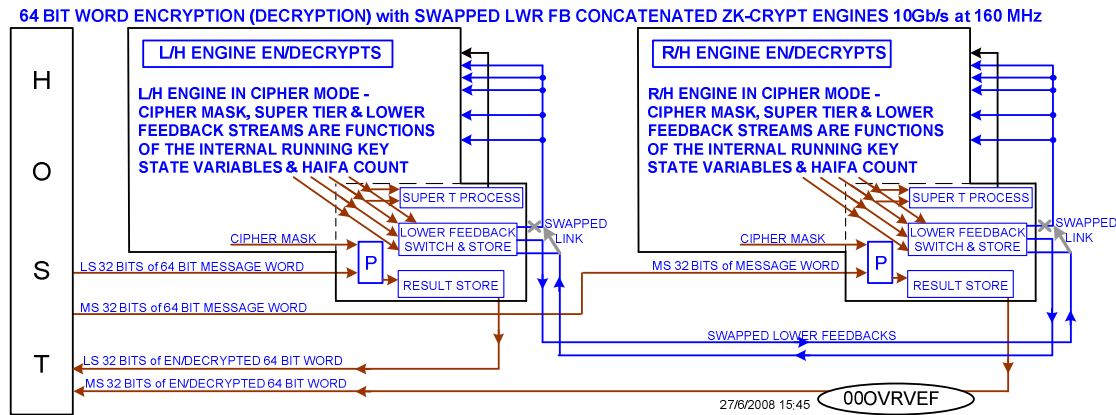


Fig 2: 64 Word En/Decryption; with Swapped Lower Feedback

B000VRVEF

In both implementations, the LS 32 bit of the Message Word is input into the L/H engine, and the R/H accepts the MS 32 bits.

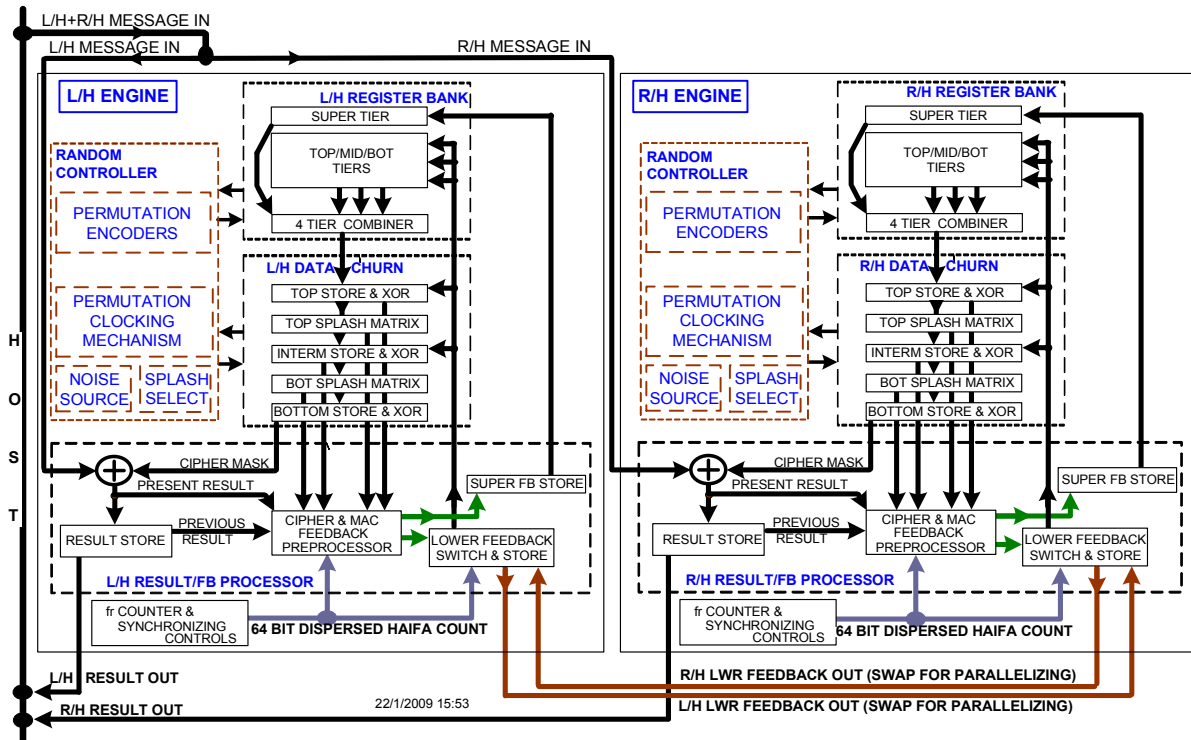


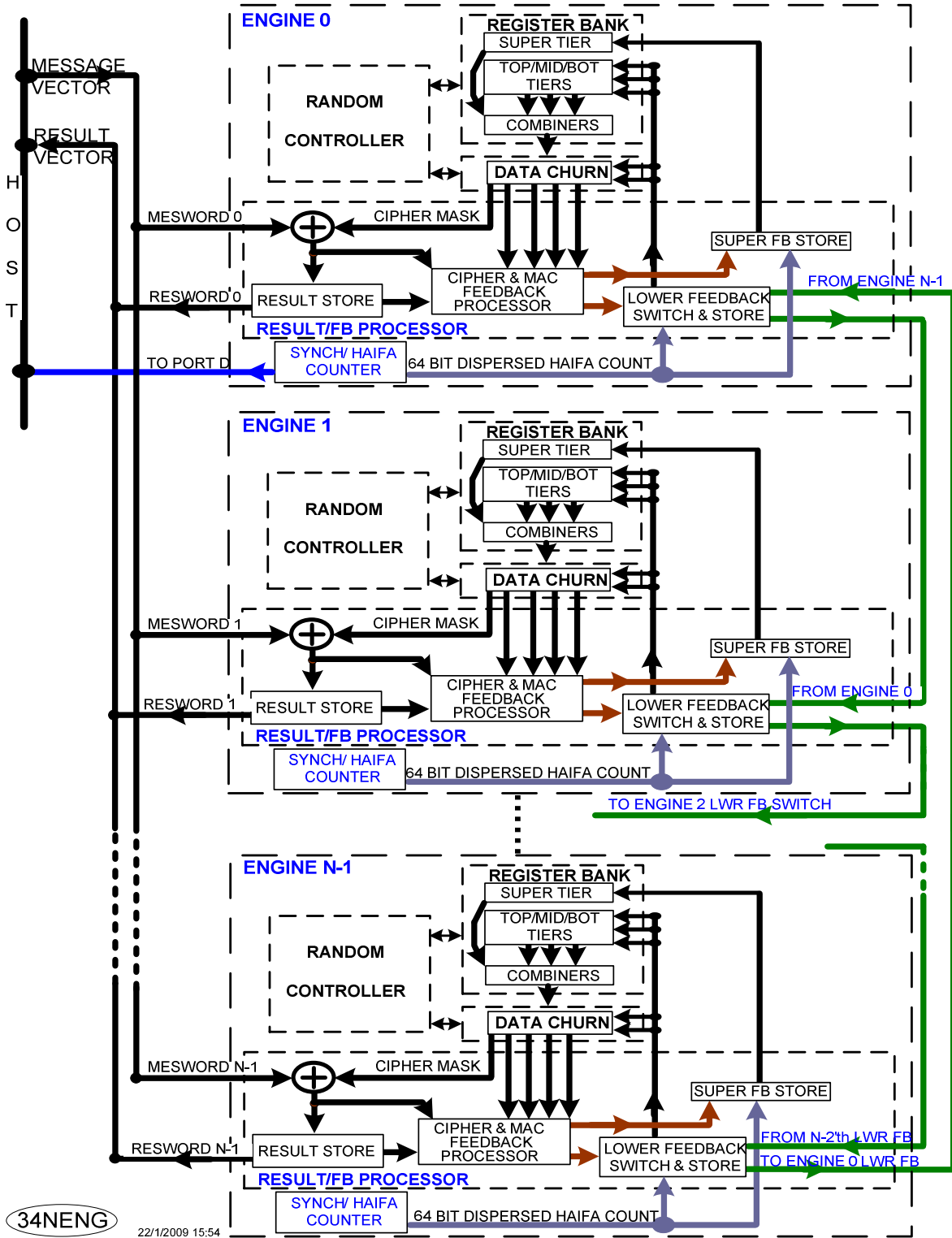
Figure 3: 2 Concatenated ZK-Crypt Engines for very Hi-Security and Doubled Speed



n Engine Concatenations

The following concatenation is designed for highest security **n** Message Word Data Authentication and/or **n** Message Word Stream Ciphering. The Lower Feedbacks are rotated to near neighbors; except for the **n-1**'th engine whose feedback is circulated to the **0**'th engine. Simultaneously, the HAIFA Counter indelibly "marks" both feedback tracks to preclude hash collisions.

False Lower and Super Tier Feedback is generated on the first instance that a false Message Word is input. Two Primary Clocks later, the false bits cause a false Cipher Mask in the next Lower Feedback receiving engine, which affects the Lower Feedback and the Super Tier Feedback immediately. The false Lower Feedback ripple irreconcilably affects all **n** engines after $2(n-2)$ Primary Clock pulses.



34NENG

22/1/2009 15:54

Figure 4: n ZK-Crypt Engine Concatenation for Very Low Power Dual Mode Acceleration