FortressGB

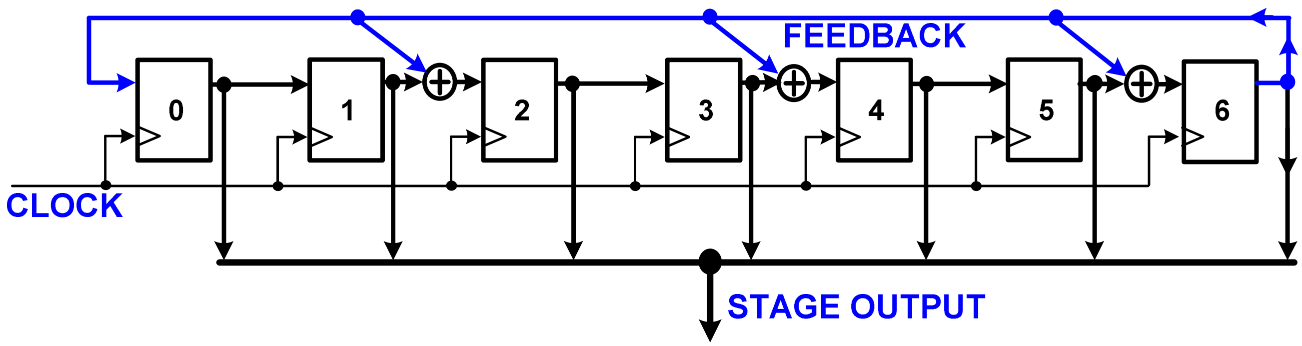
"Whitening 2 Last 32 Bit Hash Messages with a HAIFA* Inspired 64 Bit Hybrid Mersenne Prime Number LFSRs/Binary Counter"

An Efficient ZK-Crypt Artifact

* **Eli Biham & Orr Dunkelman, "A Framework for Iterative Hash Functions–HAIFA", Technion, 2006**

Patents Pending

A 7 Celled Mersenne Prime Number LFSR



MERSENNE LFSR - 7 CELL - 127 UNIQUE PSEUDO RANDOM OUTPUT STAGES

ONE TO MANY CONFIG WITH TAPS 1, 3, 5, & 6- MAX DISTANCE BETWEEN TAPS = 2

AS CLOCK PULSE RISES- INPUT SHIFTS TO OUTPUT OF EACH (FLIP-FLOP) CELL.

INITIAL CONDITION- ALL CELLS ARE SET TO ‘1’.

A 7 BIT BINARY COUNTER’S GATE COUNT IS 87 - THE 7 BIT LFSR NEEDS 51 GATES
→36/87 = 41% FEWER GATES

A 64 BIT BINARY UP COUNTER HAS MAX PROPAGATION TIME FOREVER. 12/02/09 12:12

1 A 7 Bit One to Many Mersenne Prime LFSR.vsd

Why 1 to Many Galois LFSRs for Unique Counting

LFSRs are Efficient Large Number Counters
- 40% Fewer Gates than Same Size Binary Counters
- Faster No Delays - No Ripple, No Carry
- Almost No Bias on any Bit – $2^n/2$ '1's $2^n/2-1$ '0's
- Each LFSR has 2^n-1 Unique Pseudo Random Stages

1 to Many LFSRs are "Whiter" than Many to '1's
- Less Correlated Motion Sense than Many to '1's
- More Local Pseudo-Randomness Best if Taps are not Overly Distanced from Nearest Neighbor

What About Mersenne Prime Number LFSRs

Mersenne LFSRs Have a Prime Number of Stages

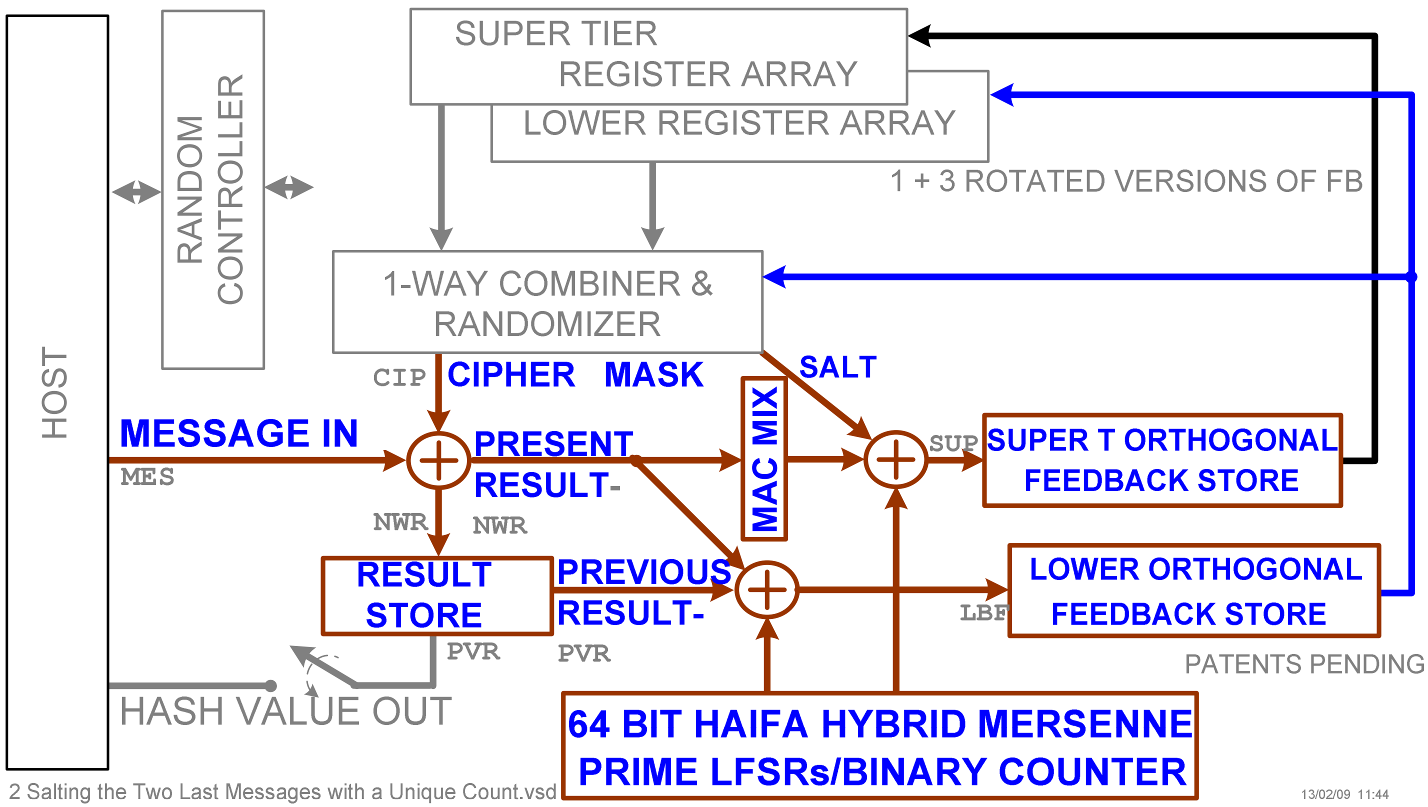
CoPrime to Each Other & Relatively Prime LFSRs can be Concatenated to one Even Length Counter

All Can be Concatenated into One Large Counter

The Few Mersennes 2,3,5,**7**,**13**,**17**,**19**,31 & 61(?)

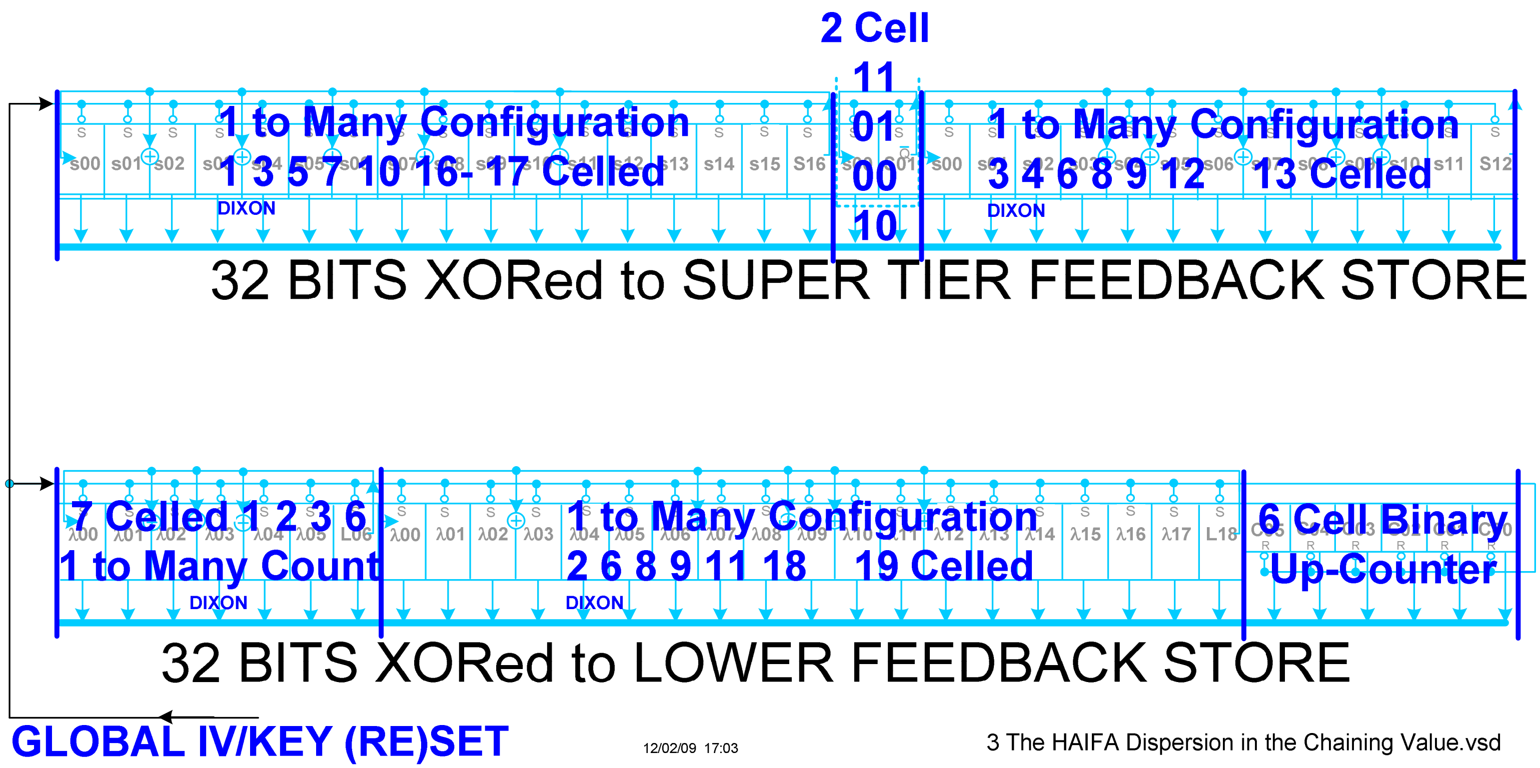
<7 Cells too Biased to '1'; 31 Bit Cells too few Taps

Mersenne was the Father of the Math of Music- This Looks Like Ultra Modern Symmetric Dissonance



M COUNTERS MAKE 64 BIT FIXED POINTS IN CHAINING VALUES

Did Eli or Orr Anticipate a 64 Bit Balanced Count



For Expansion PRFs Merkle-Damgård Looses Entropy

Unique Message Counts – from -
Super Tier FB -131,071x8191=1,073,602,561
Lwr FB - 127 x 524,287x 64 =4,261,404,736

Unique Stages in Multiple of 2 Counters = 4.58×10^{18}
~ 2^{67} Processed Data Bits

A 2^{62} Binary Counter = 4.61×10^{18} no big loss.

You Couldn't Fall Asleep in 5 Minutes Soo-

Thanks for Your (Prime- Indivisible) Attention

Thanks to Relative Prime Counters

Thanks to Eli, Orr and Hugo for Inspiration

The ZK-Crypt Design Group – FortressGB

avi, carmi,ran,tim @fortressgb.
conspiritors: nicolas t courtois, gregory v bard