FortressGB

" A Hybrid Filter Diffuses 11 Disparate State Variables into One Binary Output Variable in One Clock Cycle"

an Important ZK-Crypt Artifact

1 Message bit diffuses to more than 200 state variables on the 1st round

Follow Basic Tenets, Using Multipermutations, Orthogonal FBs, non-LINs & Decorrelators then Test to Prove no Bias, no Impossible Differential

Basic Tenets

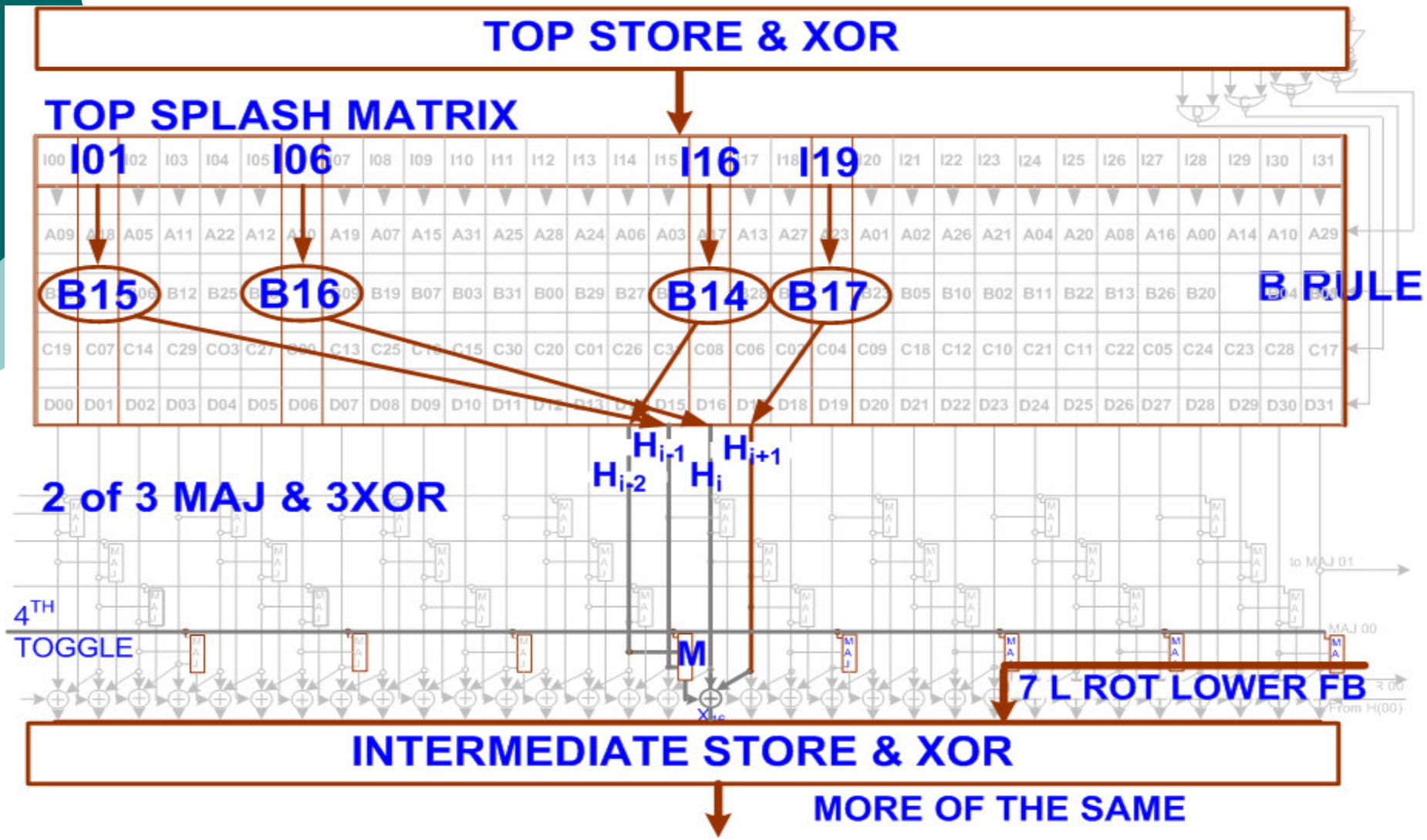
Massive Diffusion into State Variables

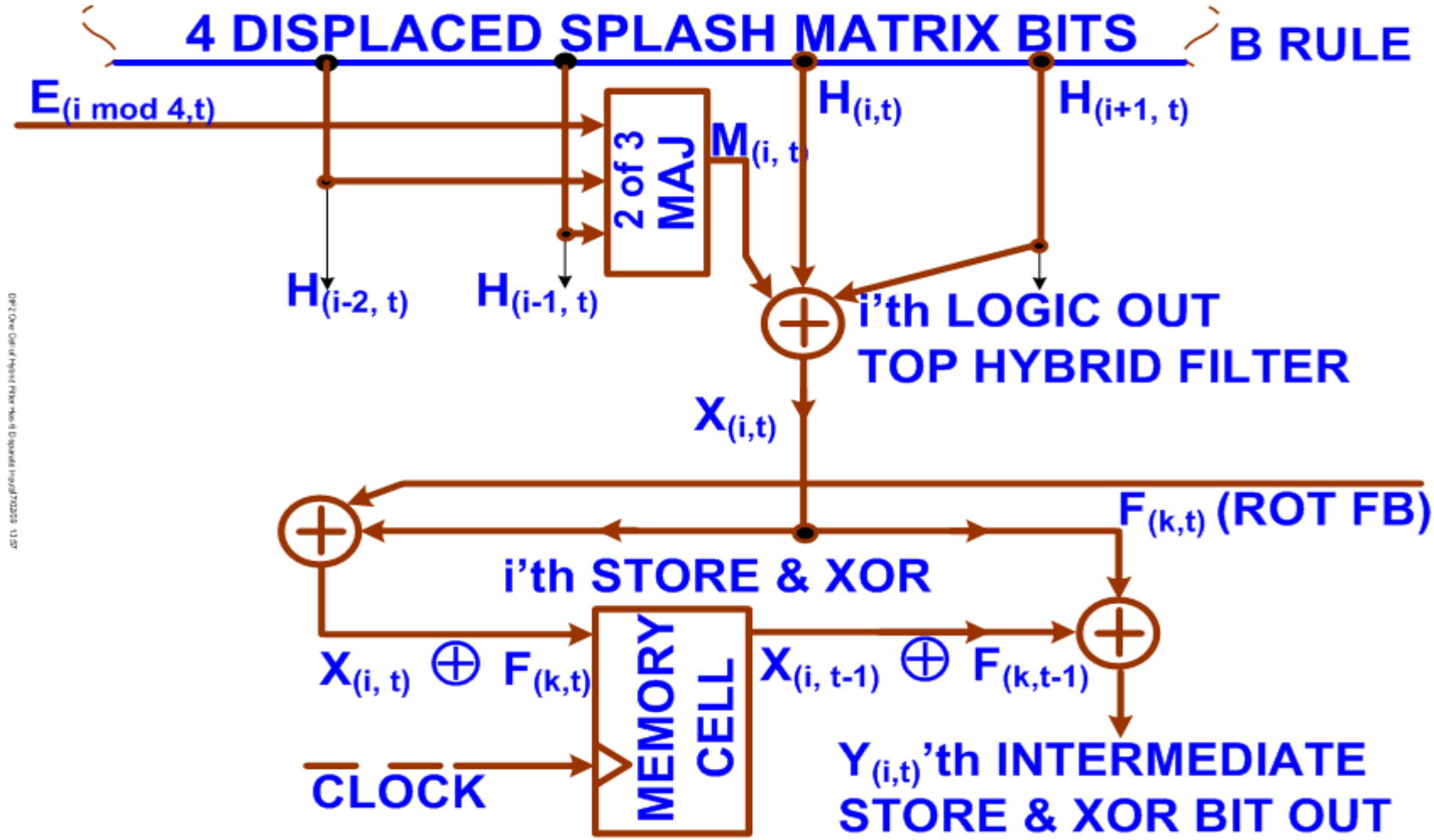
XOR Uncorrelated Words to Remove Differentials

Smart Combi Non-Lin & Linear to Reduce Correlations

Dual Track Orthogonal FB Precludes Message Modifiers

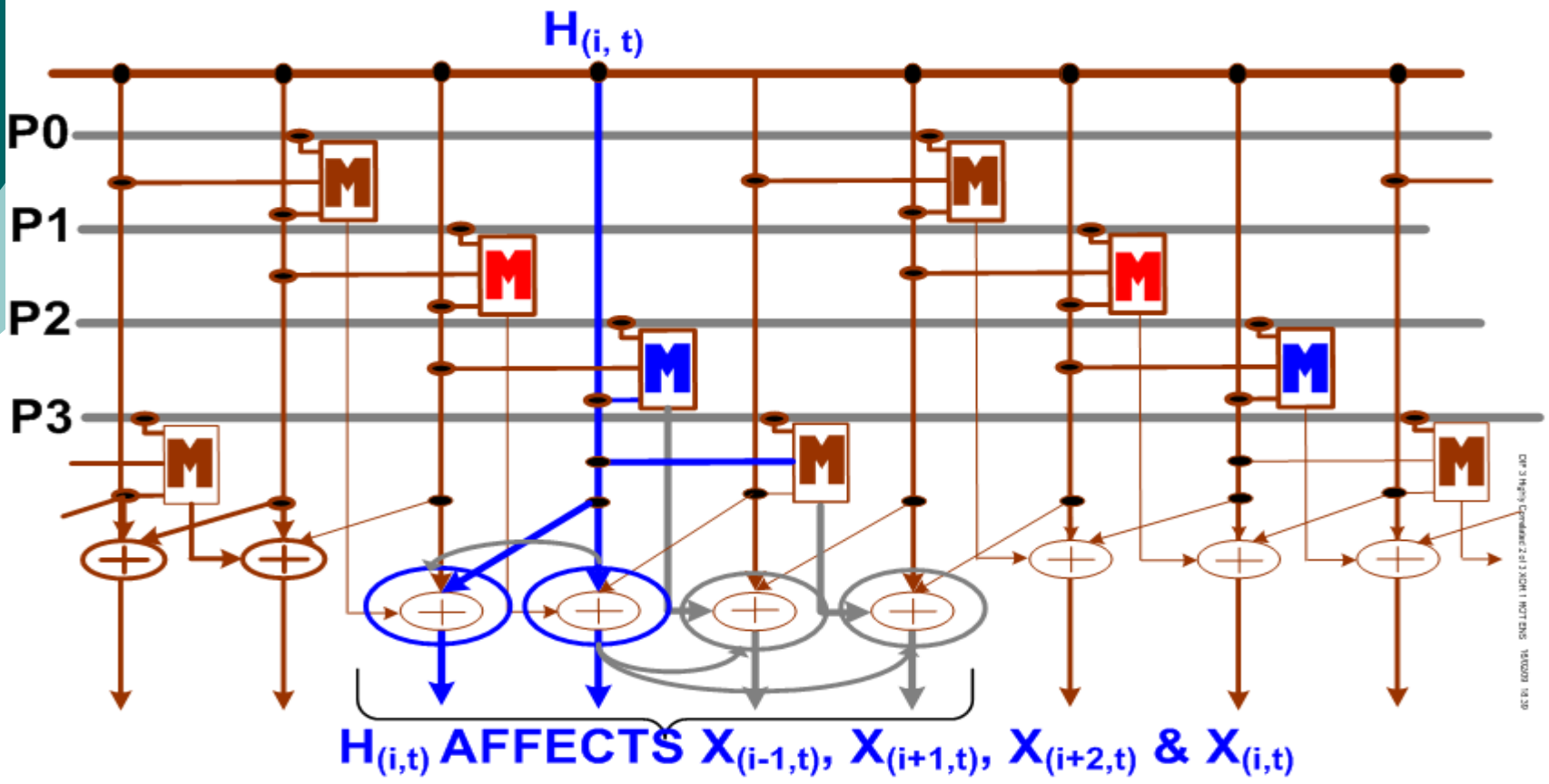
The Environment -Top Half of the Data Churn





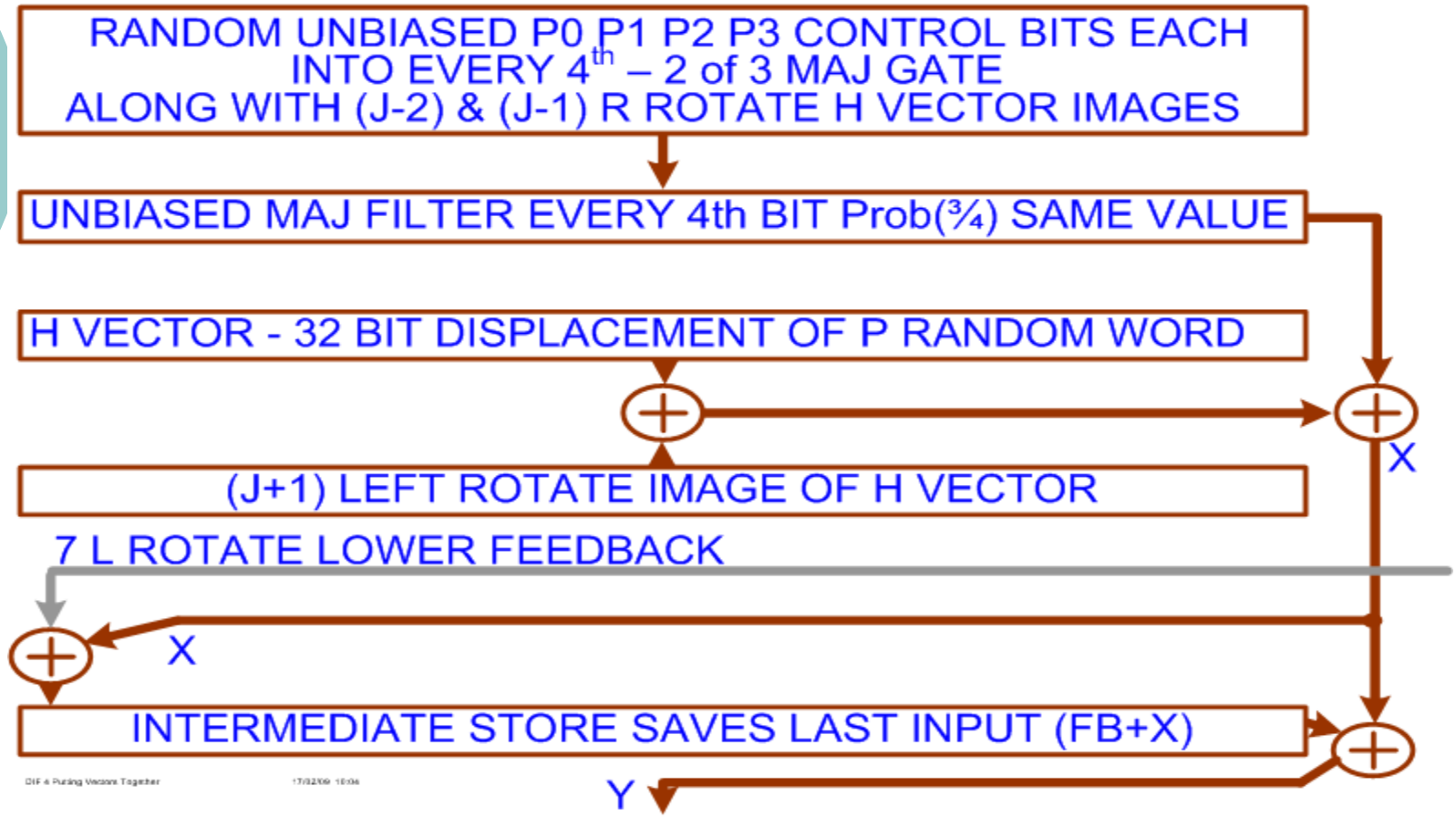
$$Y_{(i,t)} = [MAJ_{t-1}\{E_{(j,t-1)}, H_{(i-2,\,t-1)}, H_{(i-1,\,t-1)}\} \oplus [H_{(i,t-1)} \oplus H_{(i+1,t-1)} \oplus F_{(i,t-1)}] \oplus [MAJ_{t}\{E_{(j,t)}, H_{(i-2,\,t)}, H_{(i-1,\,t)}\}] \oplus [H_{(i,t)} \oplus H_{(i+1,t)}]$$

2 of 3 MAJ Vector Obviously not strongly Correlated to Linear Pseudo Random Outputs



Px's FORCE Prob(¾) EVERY 4th MAJ to ITS OWN SAME VALUE

Combining H rot 1 ⊕ H ⊕ Highly Correlated MAJ OUT
the 3 vectors slightly biased maybe loosely correlated
X ⊕ Lower FB is Decorrelated in Store & XOR



FortressGB

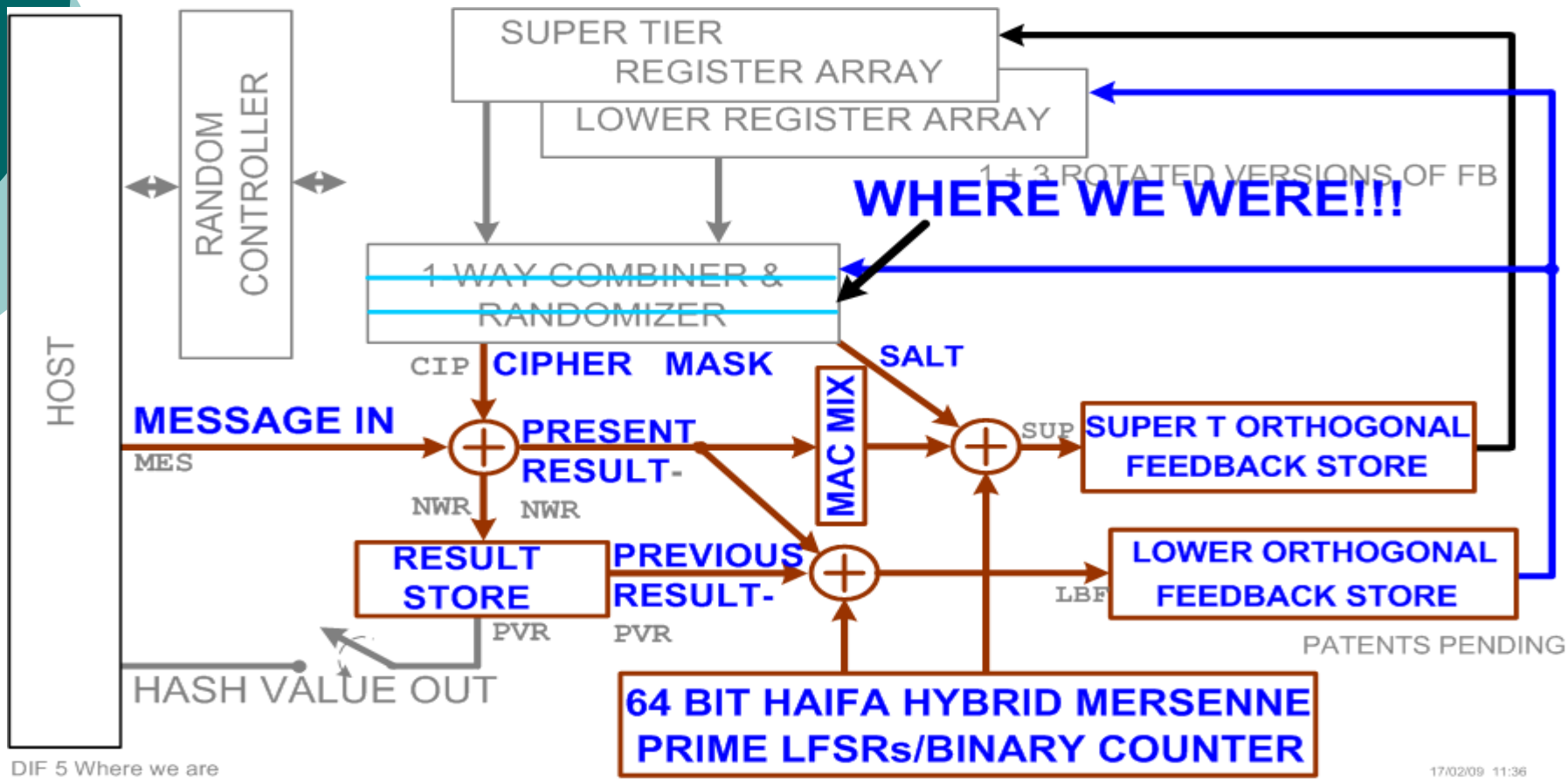
Thx for your attention

carmi, avi, ran, tim @fortressgb.com

Cosubmitters:

Nicolas T. Courtois
Gregory V. Bard

FortressGB


HOST
RANDOM CONTROLLER
SUPER TIER REGISTER ARRAY
LOWER REGISTER ARRAY
1 + 3 ROTATED VERSIONS OF FB
WHERE WE WERE!!!
1 WAY COMBINER & RANDOMIZER
CIP
CIPHER MASK
SALT
MESSAGE IN
MES
PRESENT RESULT-
NWR
NWR
MAC MIX
SUP
SUPER T ORTHOGONAL FEEDBACK STORE
RESULT STORE
PREVIOUS RESULT-
PVR
PVR
LBF
LOWER ORTHOGONAL FEEDBACK STORE
PATENTS PENDING
HASH VALUE OUT
64 BIT HAIFA HYBRID MERSENNE PRIME LFSRs/BINARY COUNTER
DIF 5 Where we are
17/02/09 11:36

10 Bits from the Register Stored Diffuse into 25 bits of the Intermediate Store & XOR & into 32 bits in the Bottom Store & XOR