FortressGB

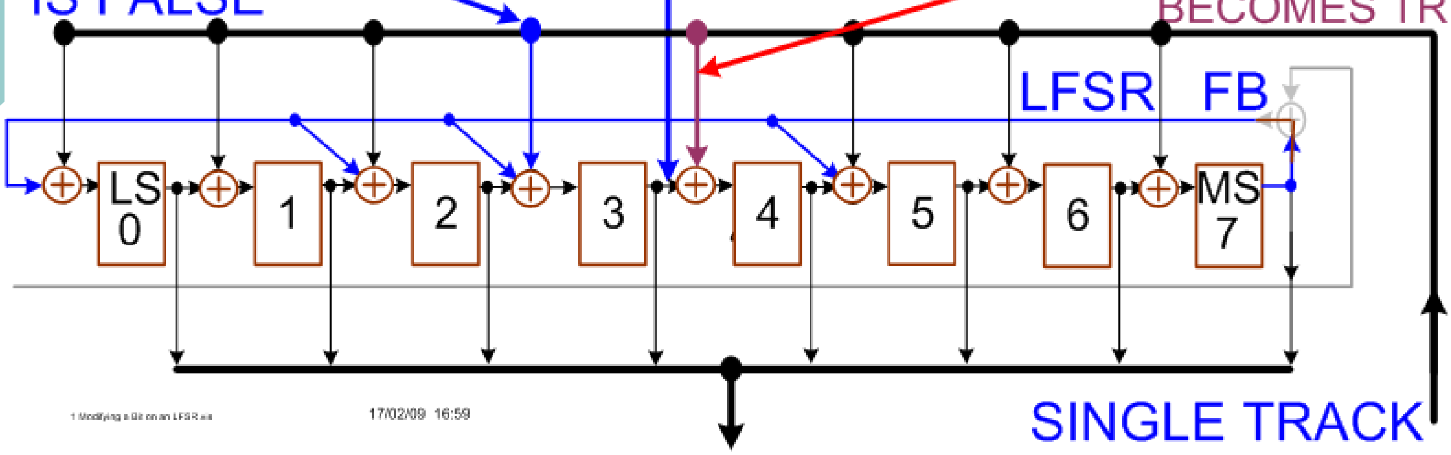
"Precluding Message Modification with Two 32 Bit Orthogonal Feedback Tracks" an Important ZK-Crypt Artifact

THE HACKER'S DELIGHT

ON THE NEXT CLOCK THIS OUTPUT WILL BE FALSE

IF THIS HASHED FB BIT IS FALSE

BUT IF THIS FB BIT IS THEN FALSE THE LFSR STAGE BECOMES TRUE NEXT CLK

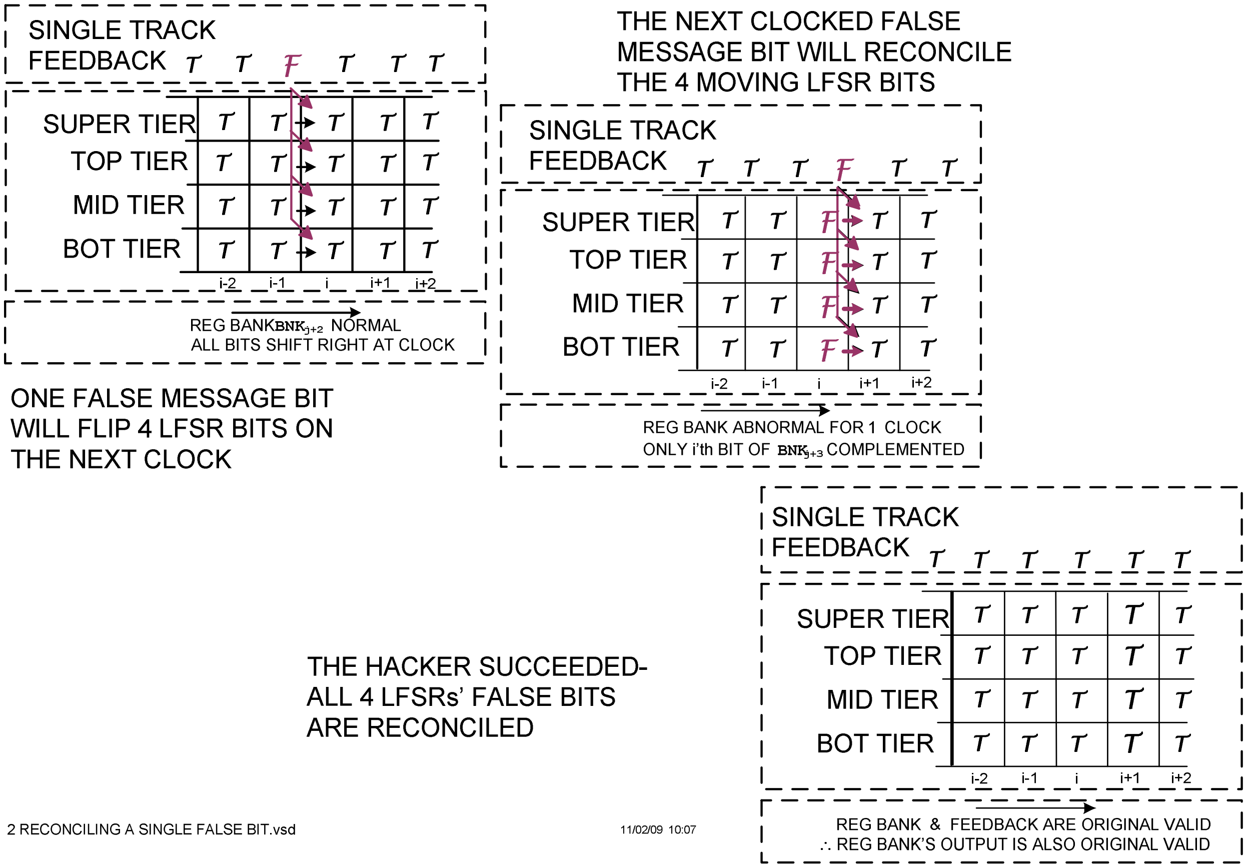


PARALLEL OUTPUT

SINGLE TRACK HASH/MAC FEEDBACK

WE ASSUME THE HACKER CAN CHANGE FB BITS AT WILL

Single Track FB Corrupting & Reconciling
4 Tiers of Simultaniously Clocked LFSRs



SINGLE TRACK FEEDBACK T T F T T T

SUPER TIER	T	T	T	T	T
TOP TIER	T	T	T	T	T
MID TIER	T	T	T	T	T
BOT TIER	T	T	T	T	T
	i-2	i-1	i	i+1	i+2

REG BANK$\mathbf{BNK}_{j+2}$ NORMAL
ALL BITS SHIFT RIGHT AT CLOCK

ONE FALSE MESSAGE BIT
WILL FLIP 4 LFSR BITS ON
THE NEXT CLOCK

THE NEXT CLOCKED FALSE
MESSAGE BIT WILL RECONCILE
THE 4 MOVING LFSR BITS

SINGLE TRACK FEEDBACK T T T F T T

SUPER TIER	T	T	F	T	T
TOP TIER	T	T	F	T	T
MID TIER	T	T	F	T	T
BOT TIER	T	T	F	T	T
	i-2	i-1	i	i+1	i+2

REG BANK ABNORMAL FOR 1 CLOCK
ONLY i'th BIT OF $\mathbf{BNK}_{j+3}$ COMPLEMENTED

SINGLE TRACK FEEDBACK T T T T T T

SUPER TIER	T	T	T	T	T
TOP TIER	T	T	T	T	T
MID TIER	T	T	T	T	T
BOT TIER	T	T	T	T	T
	i-2	i-1	i	i+1	i+2

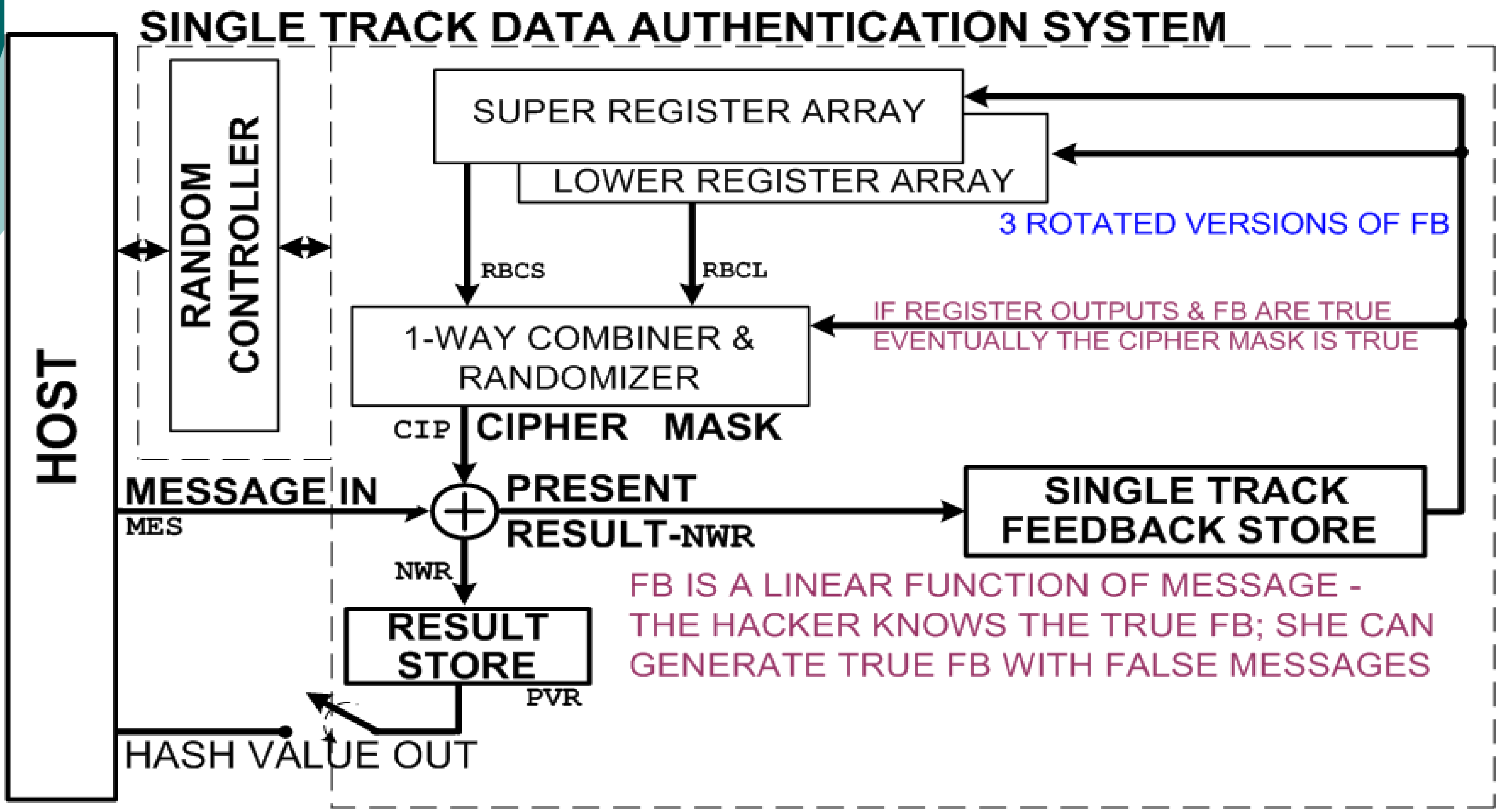
REG BANK & FEEDBACK ARE ORIGINAL VALID
∴ REG BANK'S OUTPUT IS ALSO ORIGINAL VALID

THE HACKER SUCCEEDED-
ALL 4 LFSRs' FALSE BITS
ARE RECONCILED

2 RECONCILING A SINGLE FALSE BIT.vsd

11/02/09 10:07

Hacking a Single Track Feedback



FB IS A LINEAR FUNCTION OF MESSAGE - THE HACKER KNOWS THE TRUE FB; SHE CAN GENERATE TRUE FB WITH FALSE MESSAGES

3 Single Track Feedback on Present Result.vsd

18/02/09 10:39

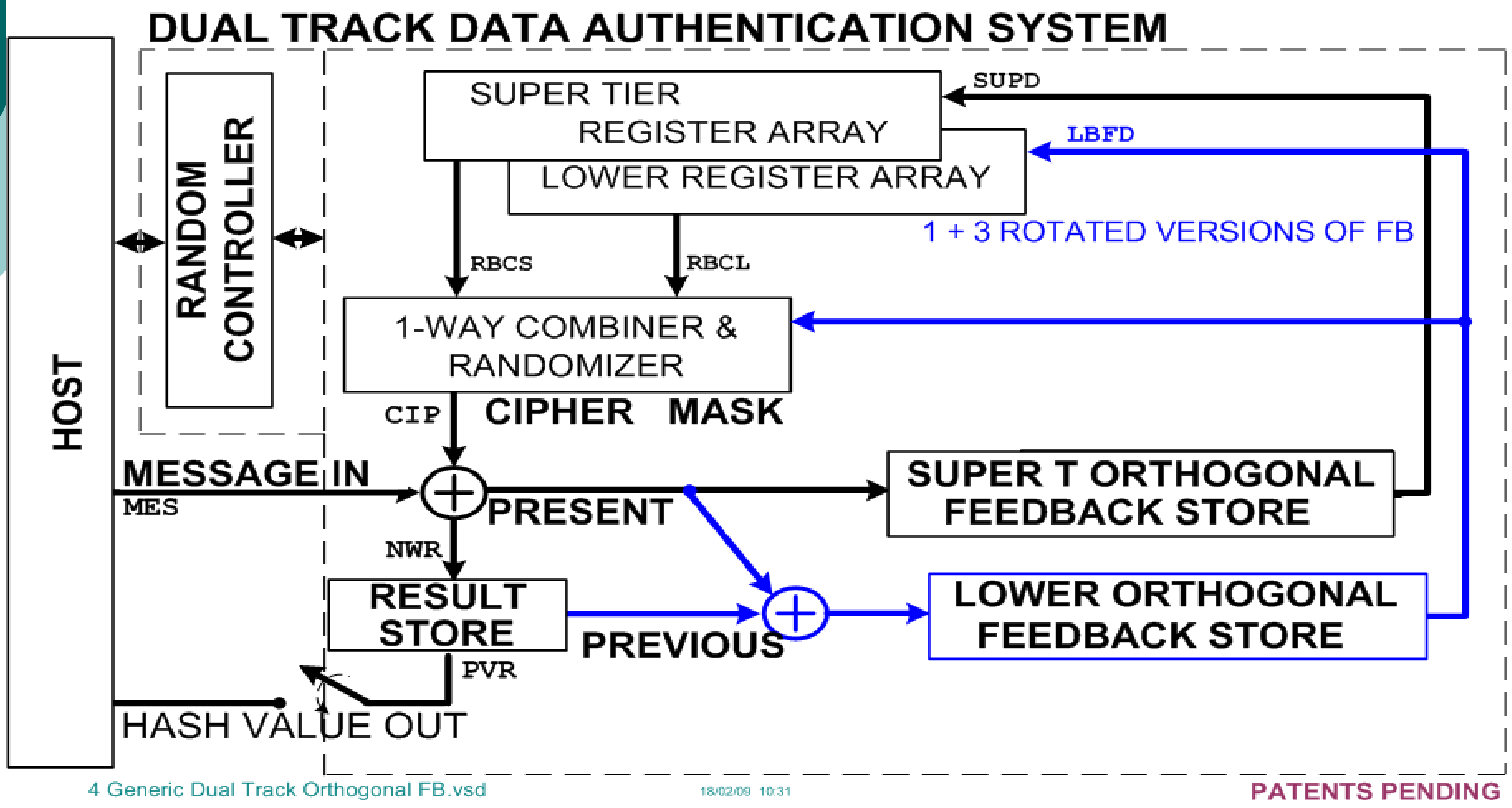
Max-Did you ever hear of Orthogonal Feedbacks?

We define two linear affected Message streams as Orthogonal

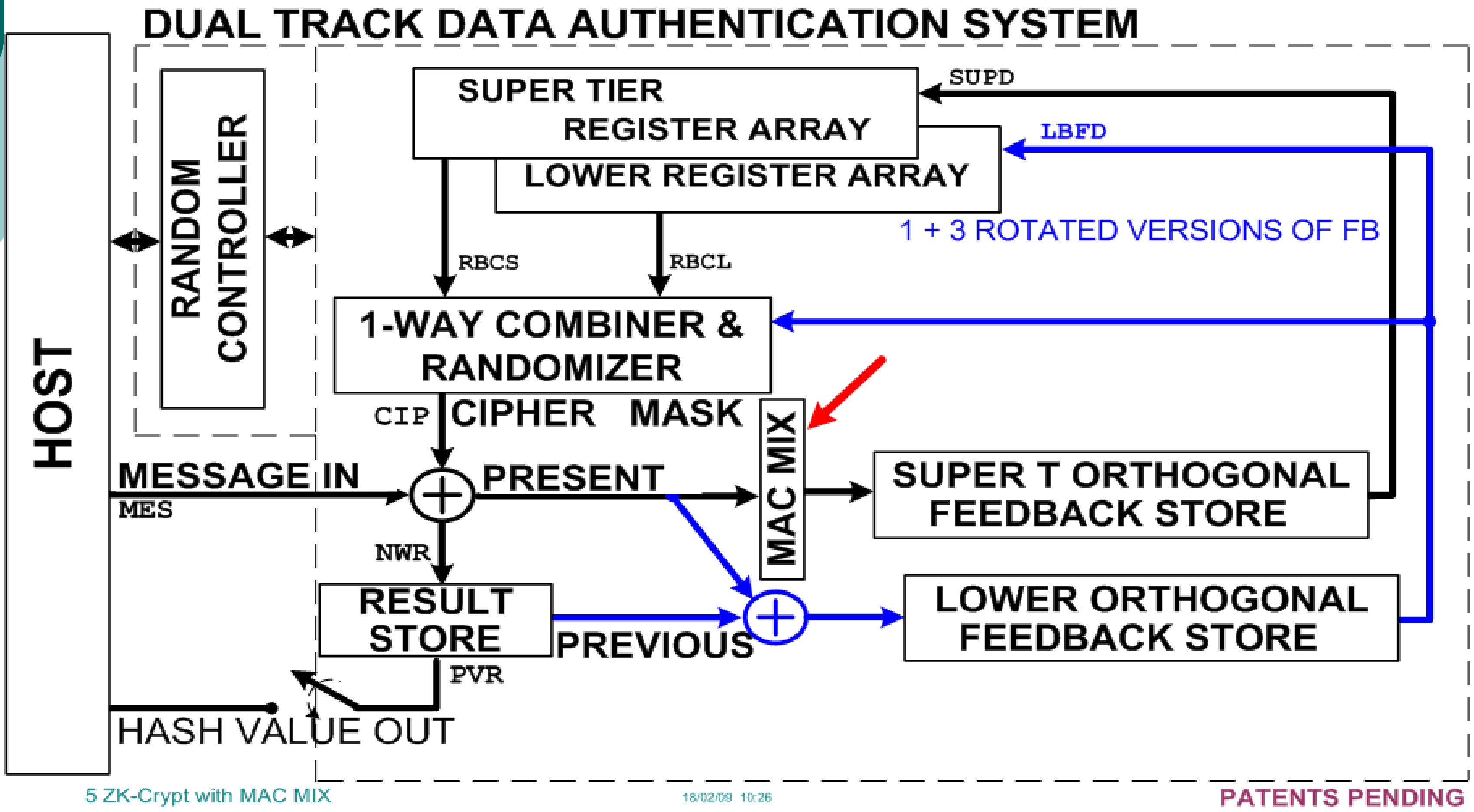
iff a sequence of Message words causes one FB stream to successfully corrupt and reconcile one cascading data section (eg, in the ZK-Crypt the Register Bank LFSRs)

and same Message word simultaneously irreconcilably corrupts a second cascading section in the Hash/MAC device (eg, in the ZK-Crypt, parts of the Register Bank & also to the Data Churn)

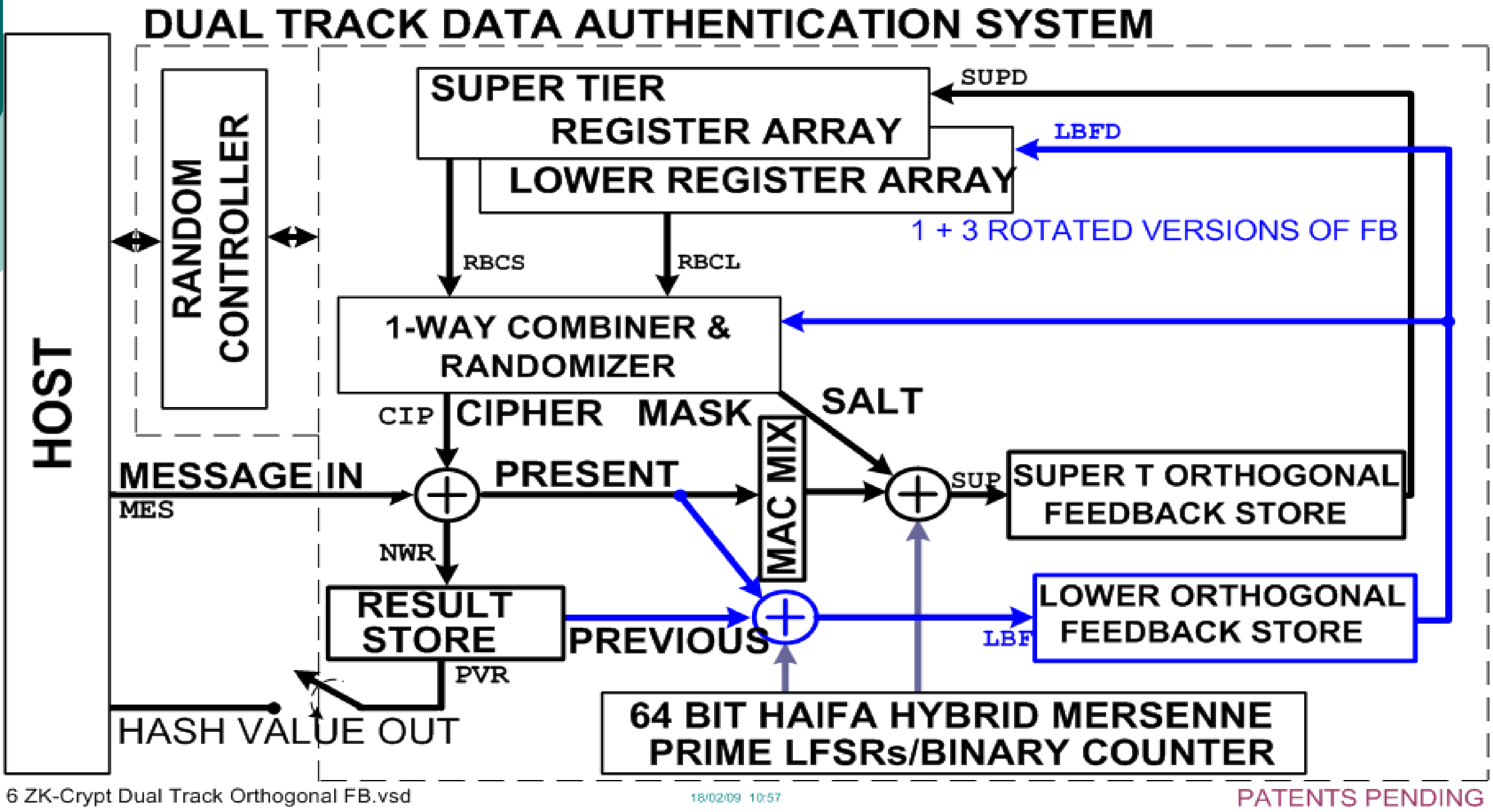
Generic Dual Track Orthogonal FB Streams


DUAL TRACK DATA AUTHENTICATION SYSTEM
HOST
RANDOM CONTROLLER
SUPER TIER REGISTER ARRAY
LOWER REGISTER ARRAY
SUPD
LBFD
1 + 3 ROTATED VERSIONS OF FB
RBCS
RBCL
1-WAY COMBINER & RANDOMIZER
CIP
CIPHER MASK
MESSAGE IN
MES
PRESENT
SUPER T ORTHOGONAL FEEDBACK STORE
NWR
RESULT STORE
PREVIOUS
LOWER ORTHOGONAL FEEDBACK STORE
PVR
HASH VALUE OUT
4 Generic Dual Track Orthogonal FB.vsd
18/02/09 10:31
PATENTS PENDING

Dual Track with MAC MIC Decorrelator

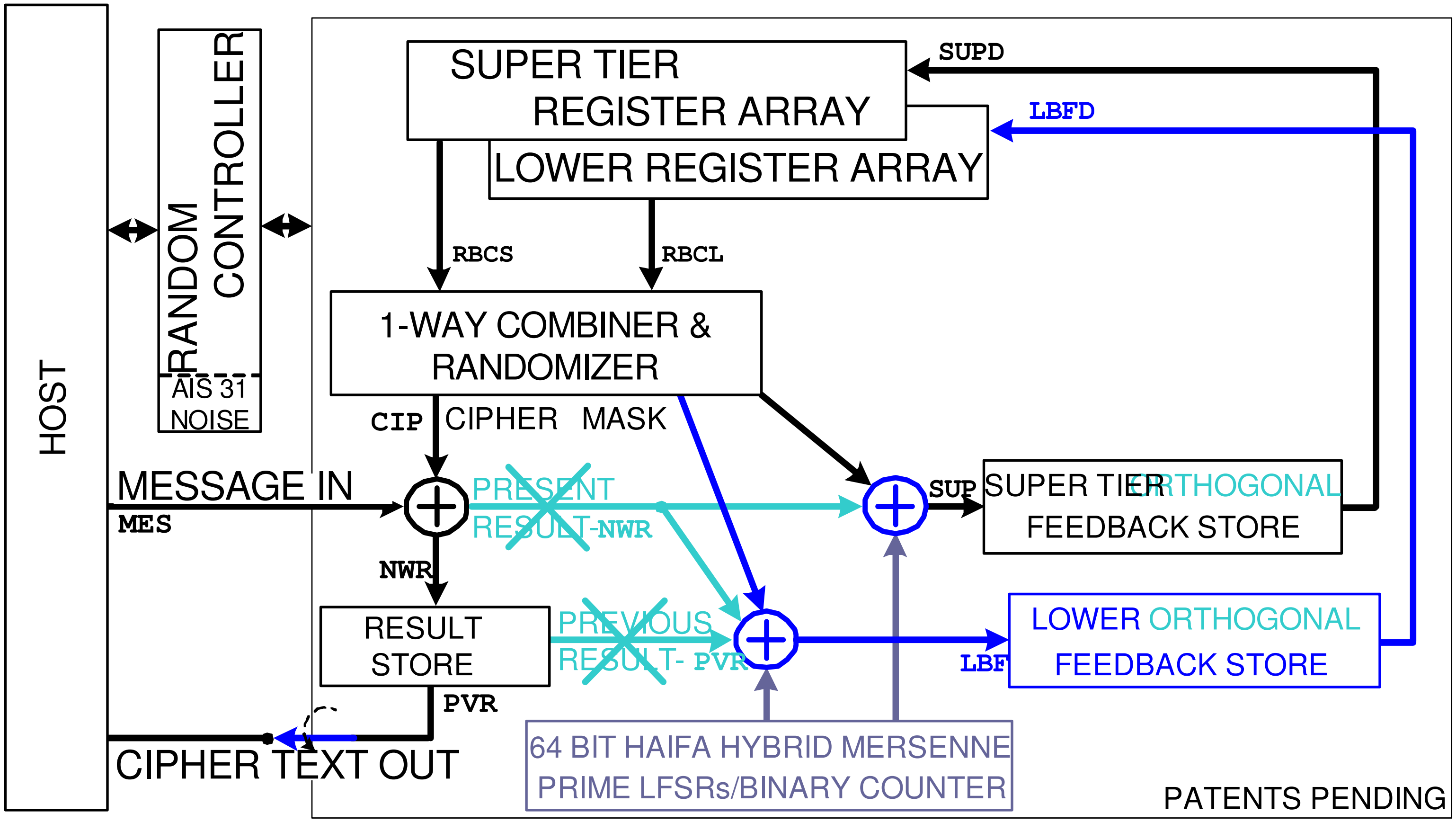


After 4 Clocks If
The SALT is False We Know Randomizer is Corrupted
If by Fluke SALT is True We Know LWR FB is False – Chap 5


DUAL TRACK DATA AUTHENTICATION SYSTEM
HOST
RANDOM CONTROLLER
SUPER TIER REGISTER ARRAY
LOWER REGISTER ARRAY
SUPD
LBFD
1 + 3 ROTATED VERSIONS OF FB
RBCS
RBCL
1-WAY COMBINER & RANDOMIZER
CIP
CIPHER MASK
SALT
MAC MIX
MESSAGE IN
MES
PRESENT
SUP
SUPER T ORTHOGONAL FEEDBACK STORE
NWR
RESULT STORE
PREVIOUS
LBF
LOWER ORTHOGONAL FEEDBACK STORE
PVR
HASH VALUE OUT
64 BIT HAIFA HYBRID MERSENNE PRIME LFSRs/BINARY COUNTER
6 ZK-Crypt Dual Track Orthogonal FB.vsd
18/02/09 10:57
PATENTS PENDING

HI Diffusion Hash PRF → Best of Breed HI Speed Stream Cipher

DUAL TRACK CIPHER FB - JUST THROW THE MAC MODE SWITCH AFTER KEY /IV LOAD



5 ZK-Crypt Ciphering with Dual Track & Mersenne FB.vsd 11/02/09 17:30

Expand Don't Compress -
the We can get you on the right tracks.

Thanks to Orr for Taking Aim at a Moving Target -

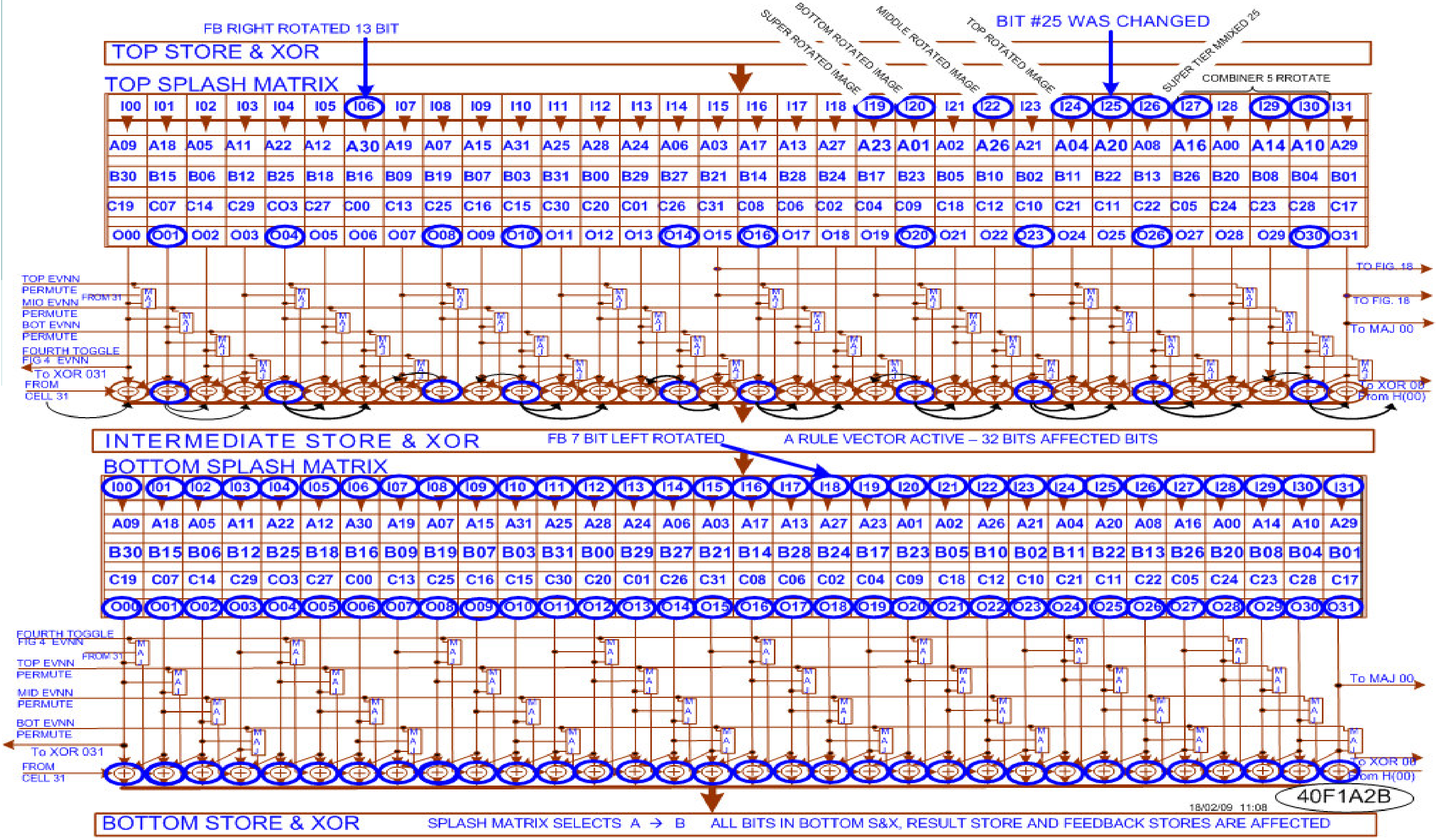
Thanks to all of you for listening-

The ZK-Crypt Design Group – FortressGB

avi, carmi, ran, tim @fortressgb.com

conspiritors: nicolas T courtouis & gregory V bard

Expand Don't Compress -



TOP SPLASH MATRIX

I00	I01	I02	I03	I04	I05	I06	I07	I08	I09	I10	I11	I12	I13	I14	I15	I16	I17	I18	I19	I20	I21	I22	I23	I24	I25	I26	I27	I28	I29	I30	I31
A09	A18	A05	A11	A22	A12	A30	A19	A07	A15	A31	A25	A28	A24	A06	A03	A17	A13	A27	A23	A01	A02	A26	A21	A04	A20	A08	A16	A00	A14	A10	A29
B30	B15	B06	B12	B25	B18	B16	B09	B19	B07	B03	B31	B00	B29	B27	B21	B14	B28	B24	B17	B23	B05	B10	B02	B11	B22	B13	B26	B20	B08	B04	B01
C19	C07	C14	C29	CO3	C27	C00	C13	C25	C16	C15	C30	C20	C01	C26	C31	C08	C06	C02	C04	C09	C18	C12	C10	C21	C11	C22	C05	C24	C23	C28	C17
O00	O01	O02	O03	O04	O05	O06	O07	O08	O09	O10	O11	O12	O13	O14	O15	O16	O17	O18	O19	O20	O21	O22	O23	O24	O25	O26	O27	O28	O29	O30	O31

BOTTOM SPLASH MATRIX

I00	I01	I02	I03	I04	I05	I06	I07	I08	I09	I10	I11	I12	I13	I14	I15	I16	I17	I18	I19	I20	I21	I22	I23	I24	I25	I26	I27	I28	I29	I30	I31
A09	A18	A05	A11	A22	A12	A30	A19	A07	A15	A31	A25	A28	A24	A06	A03	A17	A13	A27	A23	A01	A02	A26	A21	A04	A20	A08	A16	A00	A14	A10	A29
B30	B15	B06	B12	B25	B18	B16	B09	B19	B07	B03	B31	B00	B29	B27	B21	B14	B28	B24	B17	B23	B05	B10	B02	B11	B22	B13	B26	B20	B08	B04	B01
C19	C07	C14	C29	CO3	C27	C00	C13	C25	C16	C15	C30	C20	C01	C26	C31	C08	C06	C02	C04	C09	C18	C12	C10	C21	C11	C22	C05	C24	C23	C28	C17
O00	O01	O02	O03	O04	O05	O06	O07	O08	O09	O10	O11	O12	O13	O14	O15	O16	O17	O18	O19	O20	O21	O22	O23	O24	O25	O26	O27	O28	O29	O30	O31