64b/66b low-overhead coding proposal for serial links

(update 1/12/00)

Rick Walker

Agilent Laboratories, Palo Alto, CA

rick_walker@agilent.com

Richard Dugan

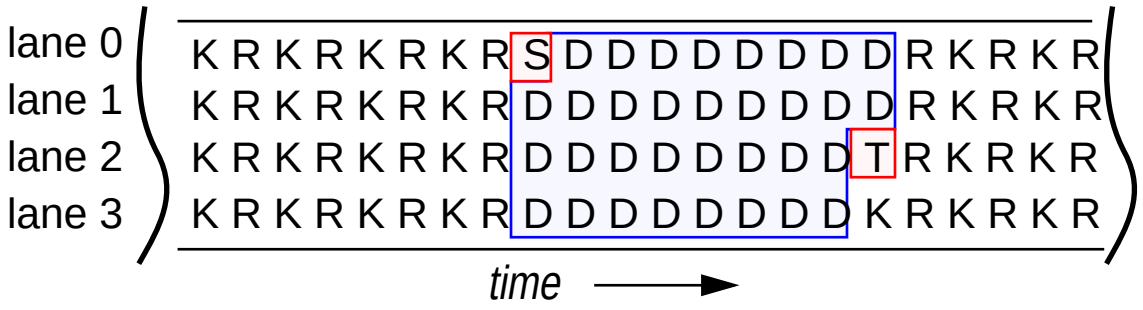
Agilent Technologies, Integrated Circuits Business Division, San Jose, CA

richard_dugan@agilent.com

Outline

- code overview (update)
- Hamming distance analysis
- scrambler analysis
- baseline wander
- summary

Building frames with HARI 10GbE mapping



S,T = SOP, EOP
K,R = control words (Z)
D = Data octets

pure data

D D
D D
D D
D D

pure control

Z Z
Z Z
Z Z
Z Z

two possible packet startings

S D
D D
D D
D D

Z S
Z D
Z D
Z D

eight possible packet endings

T Z
Z Z
Z Z
Z Z

D Z
T Z
Z Z
Z Z

D Z
D Z
T Z
Z Z

D Z
D Z
D Z
T Z

D T
D Z
D Z
D Z

D D
D T
D Z
D Z

D D
D D
D T
D Z

D D
D D
D D
D T

Overview of Code (cont.)

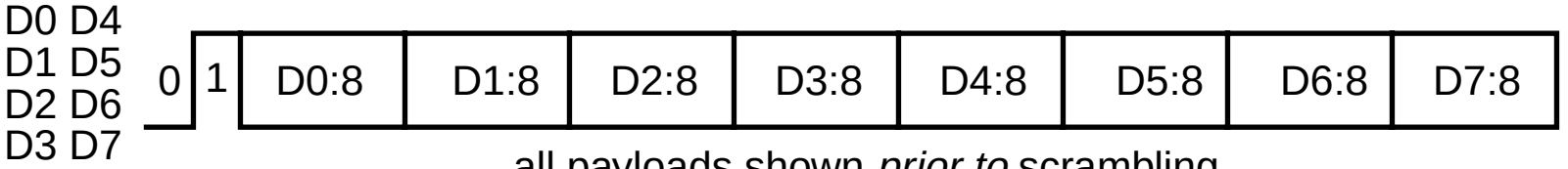
Data Codewords have “01” sync preamble

Mixed Data/Control frames are identified with a “10” sync preamble. Both the coded 56-bit payload and TYPE field are scrambled

00,11 preambles are considered code errors and cause the packet to be invalidated by forcing an error (E) symbol on the HARI output

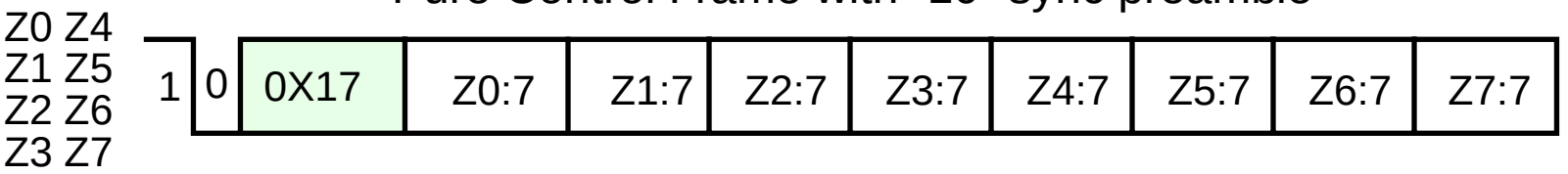
Code definition

Pure Data Frame with “01” sync preamble

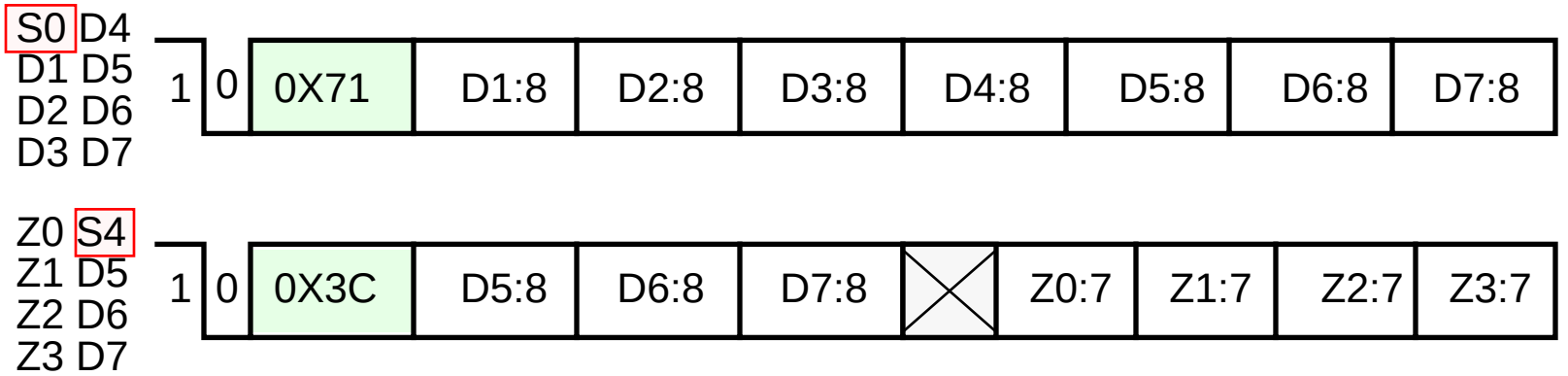


all payloads shown *prior to* scrambling

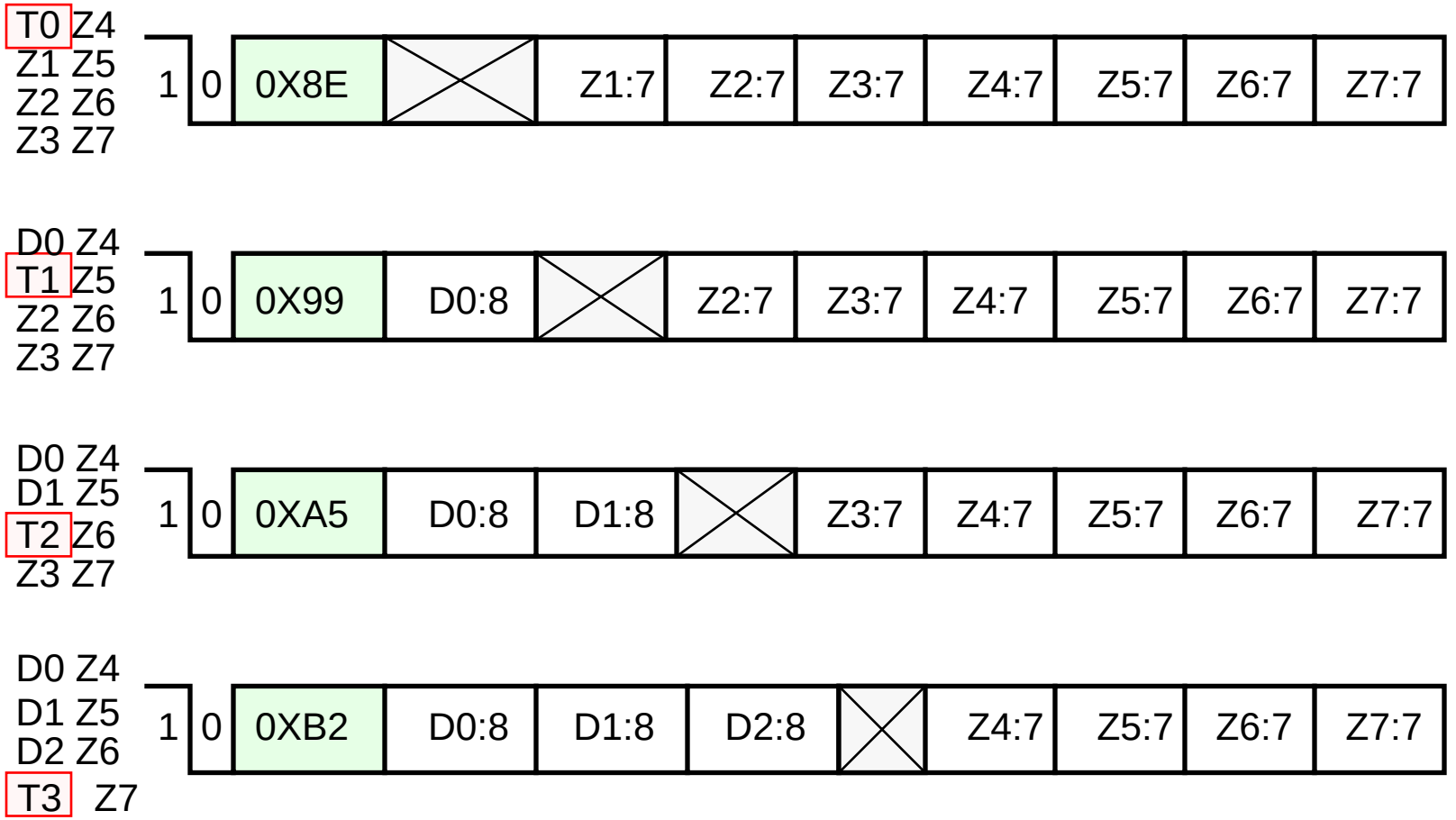
Pure Control Frame with “10” sync preamble



Mixed Data/Control Frames with “10” sync preamble

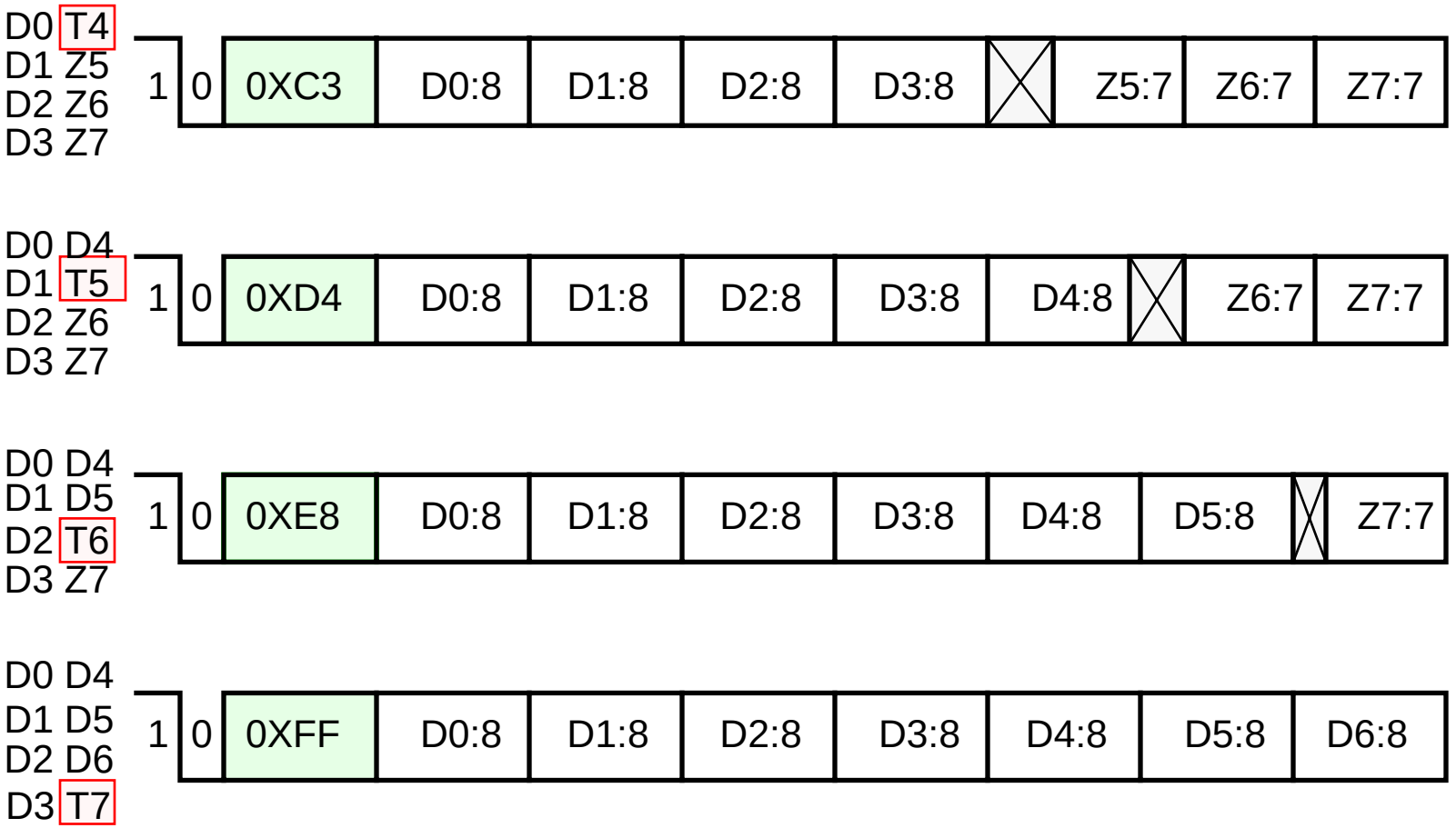


Code definition (cont.)



SOP (S) and EOP (T) are implicitly transmitted by the TYPE byte

Code definition (cont.)



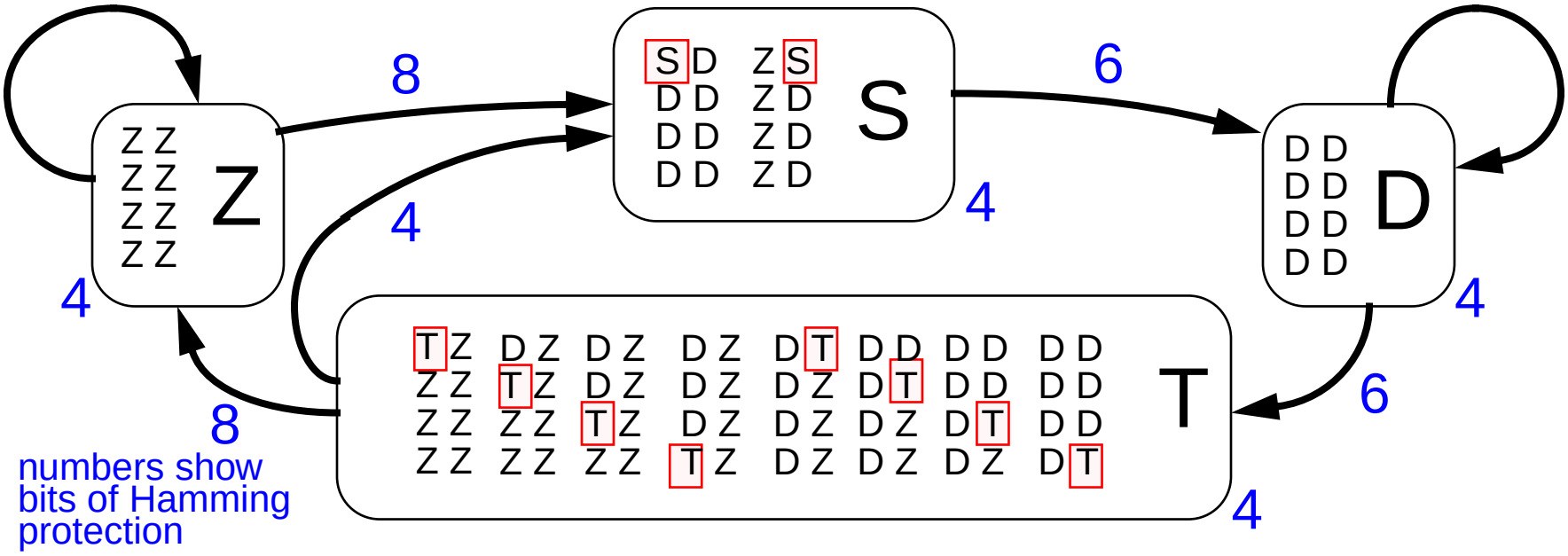
Hamming Distance

Goals and Strategies

- 4 bit Hamming protection for packet boundaries
  - ensured with a combination of TYPE byte selection and a frame-type sequencing
- 4 bit Hamming protection for control indications
  - guaranteed by 4-bit Hamming distance in the defined set of 7-bit control code mappings
- 4 bit Hamming protection for packet data
  - guaranteed by choosing a self-synchronizing scrambler that does not impair CRC32 three-bit error detection properties

Packet boundary protection

- A 2 bit error in the sync preamble can convert a packet boundary (S,T) into a Data frame (D) and vice-versa. However, all such errors violate frame sequencing rules unless another 4 errors recreate a false S,T packet (a total of six errors). Frame sequence errors invalidate the packet by forcing an (E) on the HARI output.



Control code mapping

8B/10B	name	shorthand	7-bit line code
K28.5	idle0	K	0x16
K28.1	busy idle0	Kb	0x19
K28.0	idle1	R	0x25
K23.7	busy idle1	Rb	0x2a
K27.7	start	S	encoded by TYPE byte
K29.7	terminate	T	encoded by TYPE byte
K30.7	error	E	0x43
K28.7	violate	V	0x4c
-	reserved0	-	0x70
-	reserved1	-	0x7f

- The 7-bit line codes representing 8B/10B control characters have 4-bit minimum hamming distance.

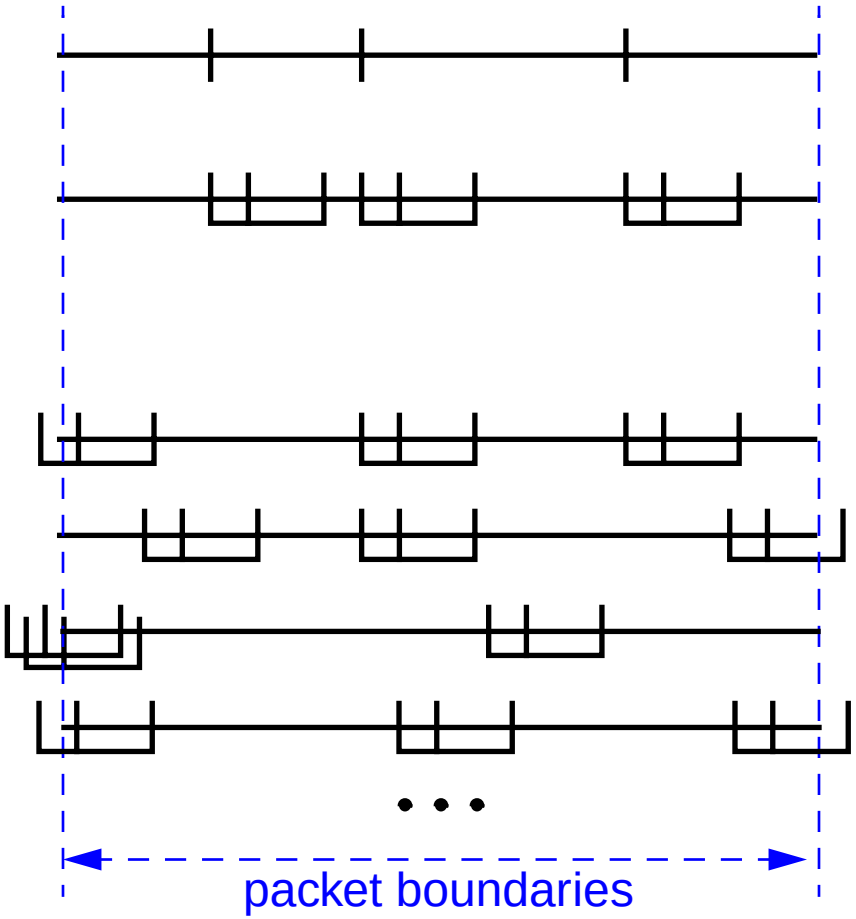
Scrambler selection

Three Criteria

- polynomial must cause no CRC32 violations under exhaustive 3-error test for all Ethernet packet sizes.
    - use a primitive trinomial to minimize interaction with CRC32
    - exhaustively analyze three-bit errors to certify scrambler performance
- polynomial tap spacings must be greater than 8 to prevent error multiplication from degrading TYPE byte Hamming protection
- polynomial order should be > 57 prevent malicious jamming and < 64 to minimize implementation complexity

Scrambler selection

CRC32 interaction with error multiplication



CRC32 is known to protect against all 1,2, and 3-bit errors in a packet

No CRC degradation occurs with error-multiplication if the scrambler and the CRC polynomial share no common factors

To certify 4-bit hamming distance for a self-synchronous scrambler, all spill-in and spill-out errors must be exhaustively checked for all packet sizes

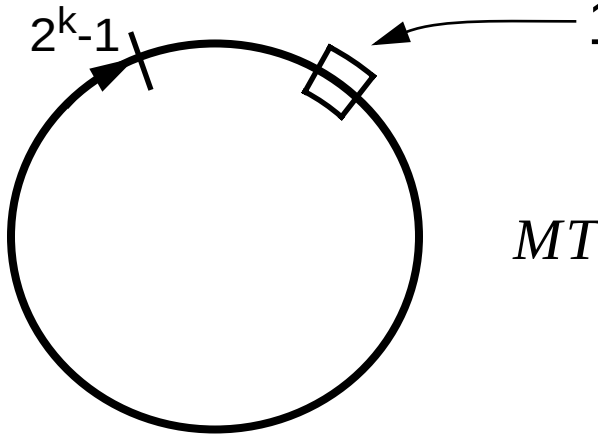
Scrambler selection

jamming probability analysis

Expected time for 64-bit run-length due to random data:

$$MTTF(random) = \frac{2^{64}}{2 \cdot 10.3GHz} \approx 29years$$

Expected time for 64-bit run-length due to jamming:



1500byte packet (26 byte overhead)
gives 94 chances to "hit" scrambler

$$MTTF(jamming) = \frac{(2^{k}-1) \bullet 1526 \bullet 8}{94 \bullet (2) \bullet 10.3GHz}$$

k=57 gives MTTF of 29 years

Candidate scrambler polynomials

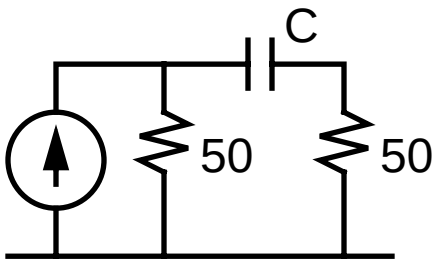
- 2 scrambler polynomials have been identified that meet all critical design criteria:

X^{58}	+	X^{19}	+	X^{0}
X^{65}	+	X^{18}	+	X^{0}

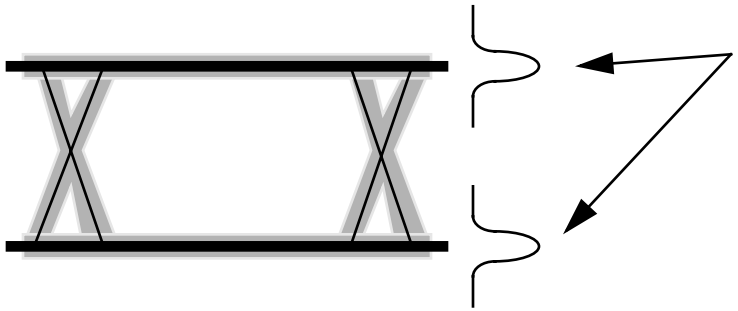
- we propose that $x^{58}+x^{19}+x^{0}$ be the “primary” choice for 64b/66b, and that $x^{65}+x^{18}+x^{0}$ be reserved as a “fallback” in case any difficulties arise upon further analysis.

The program to test CRC32 interaction is complex. These results should be considered provisional until peer reviewed. Source code is available, by request, to any interested party who wishes to help verify these findings.

Baseline Wander



A typical laser system will require a coupling capacitor at both TX and RX



Eye diagram shows Gaussian wander due to statistical fluctuation of 1's and 0's charging coupling capacitor C

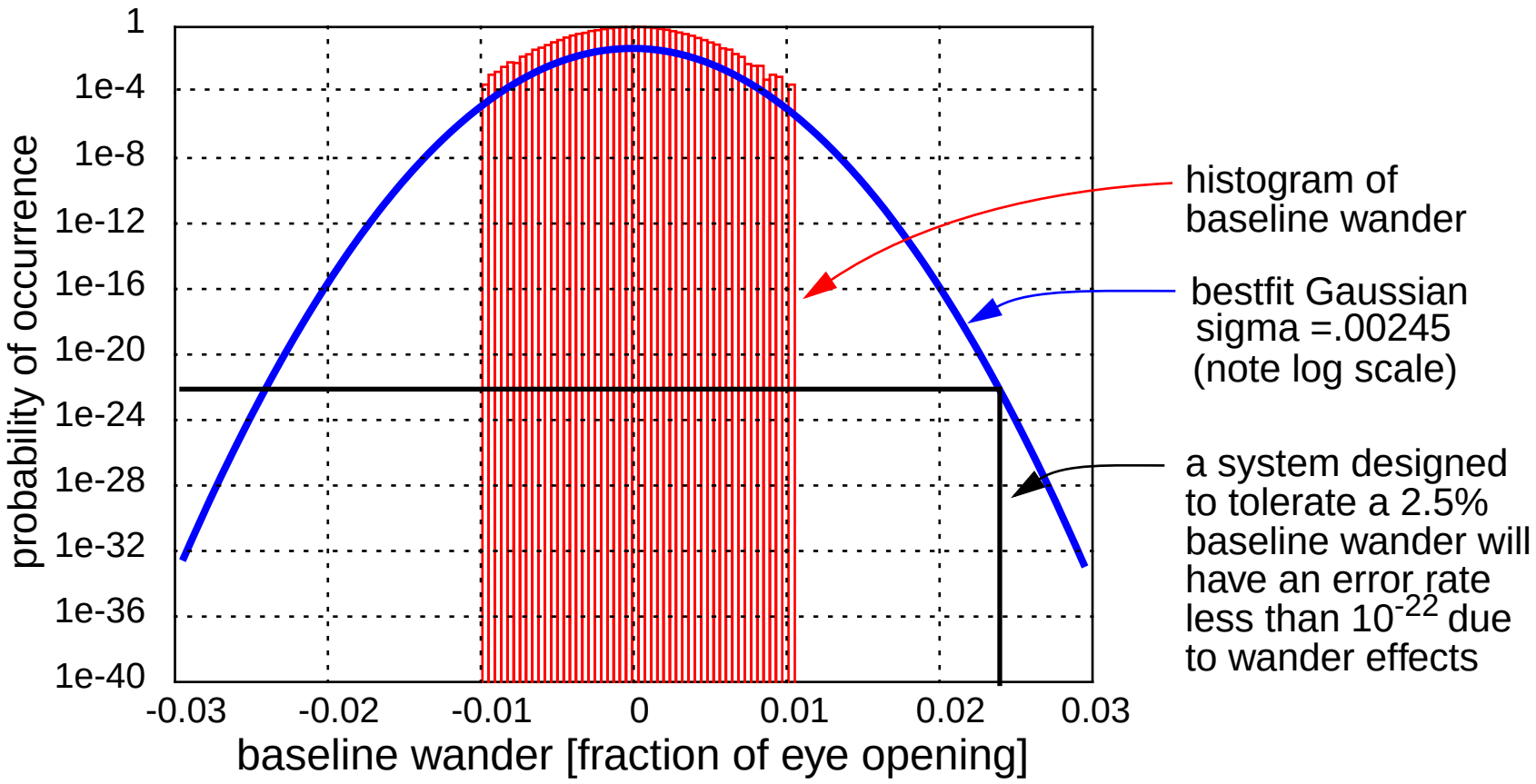
The average value of N random bits is 1/2 with a sigma of 1/sqrt(N)

A coupling capacitor can be approximately considered to be performing a moving average over N bits, where N ~= 2*PI*RC/(Tbit)

Therefore baseline wander is well approximated by a gaussian distribution with a sigma proportional to 1/sqrt(RC)

Simulated Baseline Wander

1Tb of 10.3 Gb/s scrambled data through 0.001uf and 100ohms



Conclusions

- A scrambler has been selected for 64b/66b that does not degrade the 4-bit Hamming protection of CRC32
- The self-synchronous scrambler is immune to jamming
- Overall, the 64b/66b code has 4-bit Hamming protection for packet boundaries, data bits, and control indications
- Baseline wander is well understood and easily controlled