First Advanced Encryption Standard Candidate Conference,
Ventura, CA, August 20-22, 1998

SAFER+

Cylink Corporation’s Submission for the Advanced Encryption Standard

CYLINK

Principal submitter:

Cylink Corporation, Sunnyvale, CA 94086
(represented by **Dr. Lily Chen**)

Inventors of algorithm:

James L. Massey (Prof. *emeritus*, ETH Zurich, Switzerland)
Prof. Gurgen H. Khachatrian (Academy of Sciences, Armenia)
Dr. Melsik K. Kuregian (Academy of Sciences, Armenia)

Owner of algorithm:

Cylink relinquishes all proprietary rights to SAFER+ and consigns this algorithm to the **public domain**.

The Background of SAFER+

• SAFER+ is based on the existing SAFER family of ciphers, which comprises the ciphers SAFER K-64, SAFER K-128, SAFER SK-64, SAFER SK-128, and SAFER SK-40.

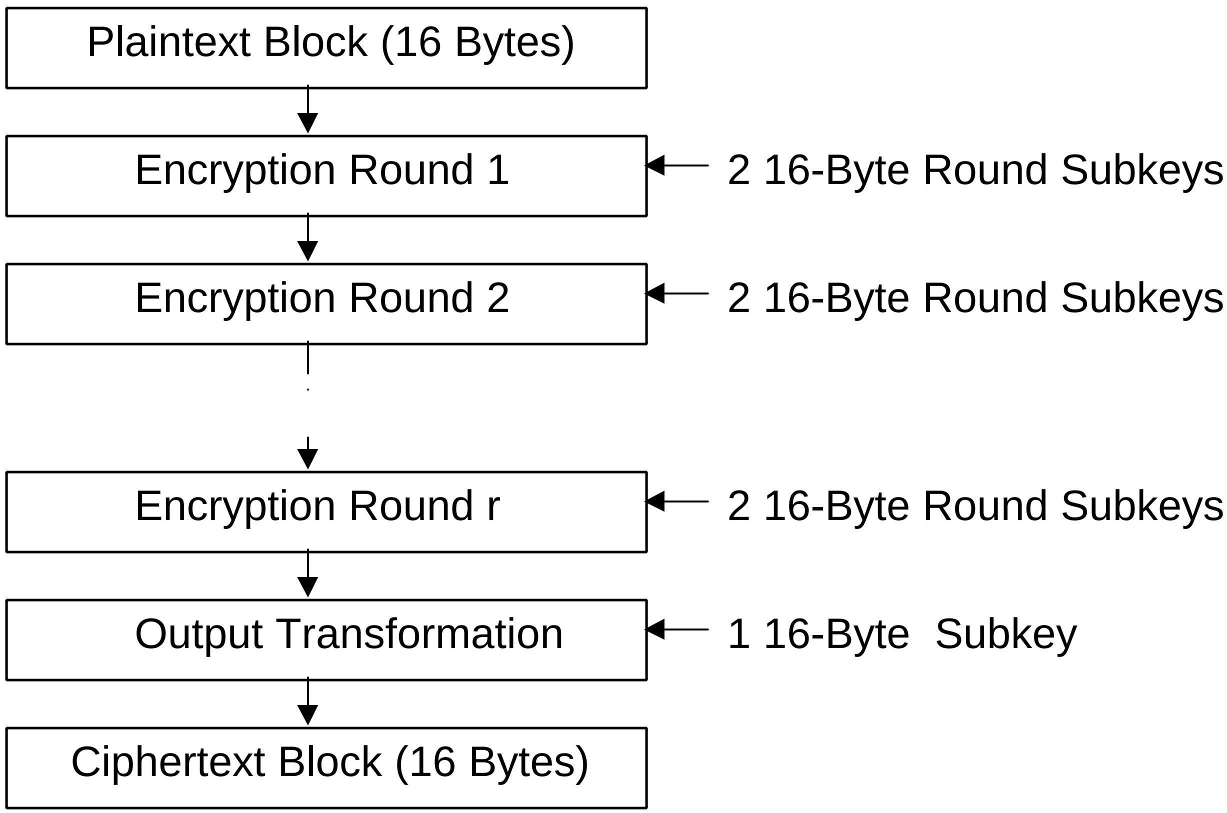
• The block size of all the ciphers in the existing SAFER family is 64 bits, while the key length is 40 or 64 or 128 bits as indicated in the name of the cipher.

• The ciphers in the existing SAFER family are non-proprietary ciphers and were designed by Prof. James L. Massey of the ETH Zurich (Swiss Federal Institute of Technology, Zurich) at the request of Cylink Corporation.

•The first of these ciphers, SAFER K-64, was publicly announced at the Dec. 9--11, 1993, Fast Software Encryption workshop in Cambridge, England. The other ciphers in the SAFER family differ from SAFER K-64 only in their key schedules and in the number of rounds used.

• The name "**SAFER**" was originally chosen by Massey as an acronym for "**Secure And Fast Encryption Routine**".

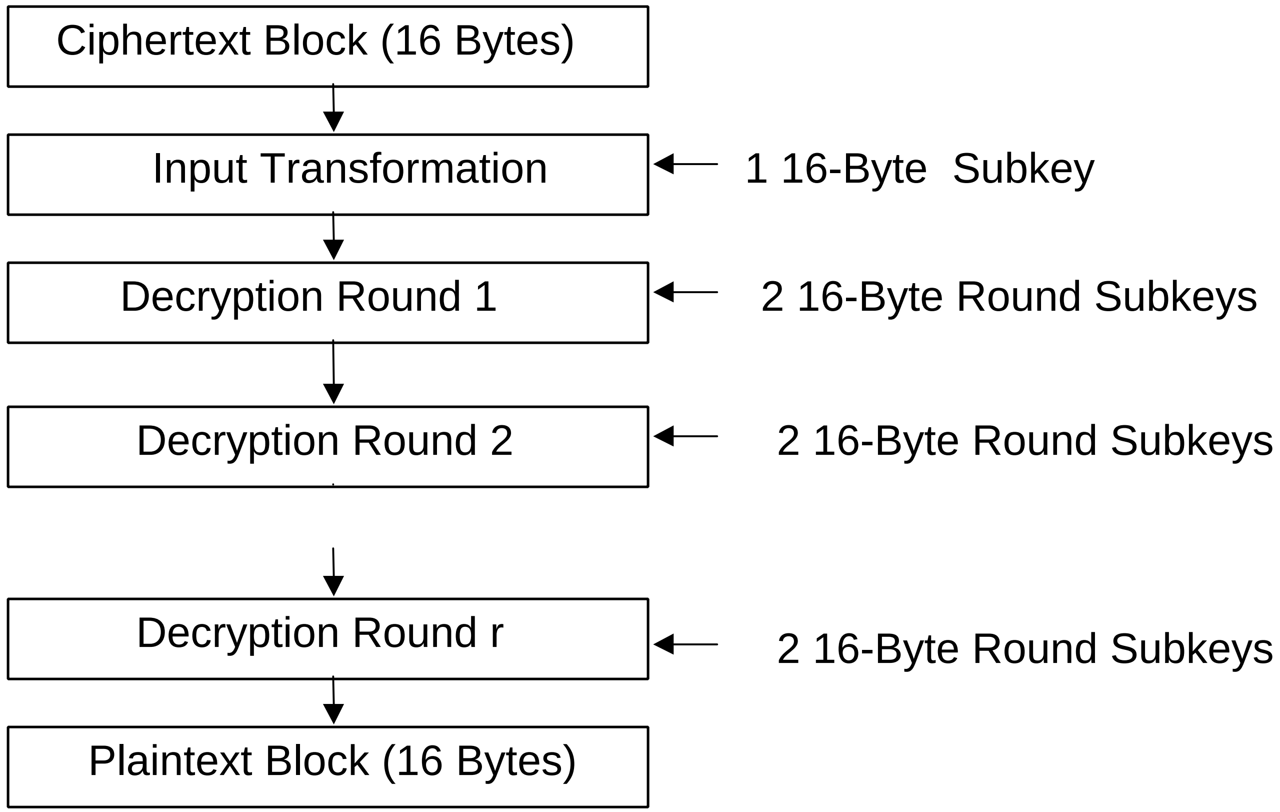
SAFER+ Encrypting Structure



Key Length	128 bits	192 bits	256 bits
Number of Rounds	8	12	16

CYLINK

SAFER+ Decrypting Structure

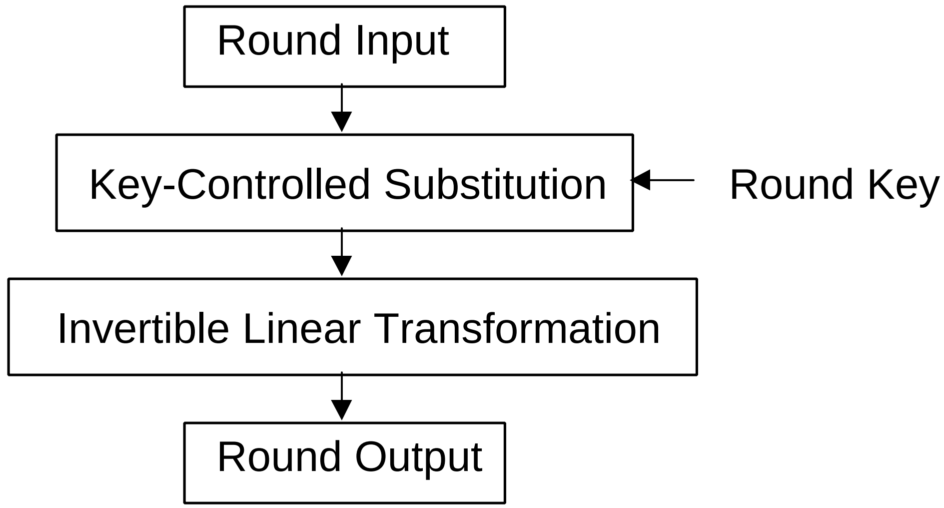


- A decryption round is very similar to, but not identical with, an encryption round.
- The input transformation is very similar to, but not identical with, the output transformation.

CYLINK

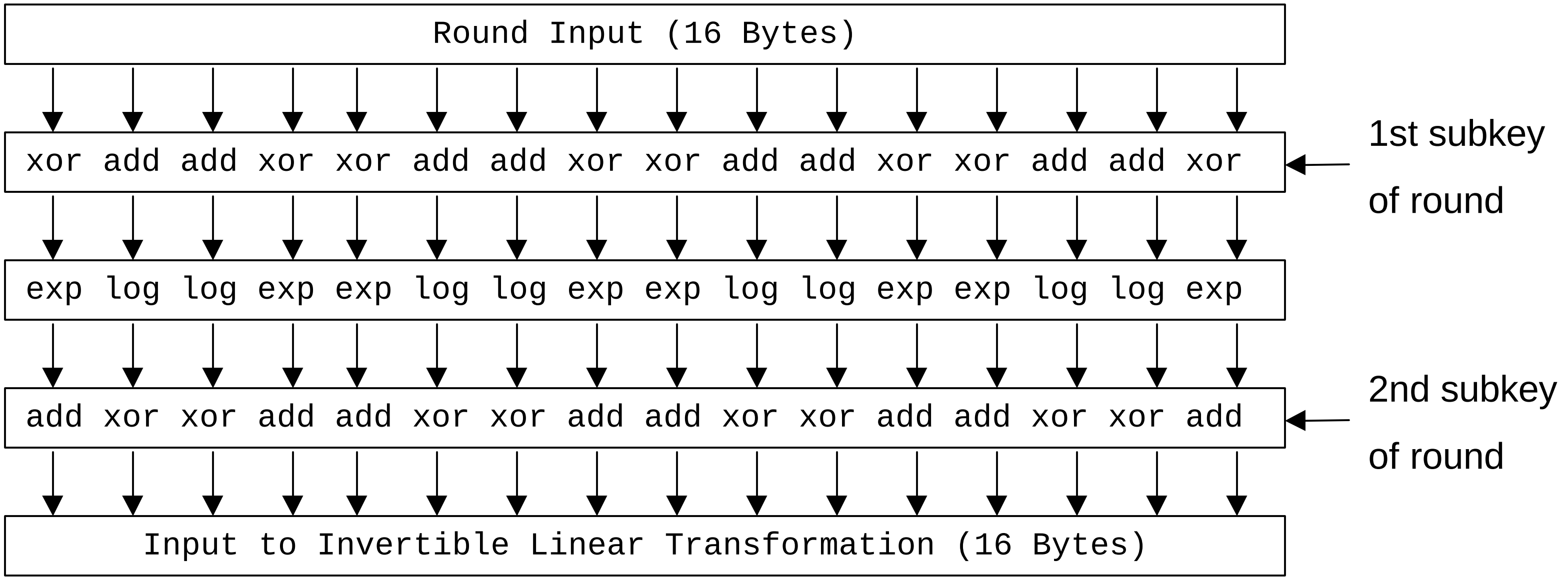
SAFER+ Round Structure

SAFER+ is neither a Feistel Cipher nor a substitution-permutation cipher,but is rather a **substitution/linear-transformation cipher**.



The Key-Controlled Substitution provides for **confusion**.
The Invertible Linear Transformation provides for **diffusion**.

The SAFER+ Key-Controlled Substitution



"xor" denotes bit-by-bit modulo-two addition of bytes.
"add" denotes modulo-256 addition of bytes.

"exp" denotes the function exptab(x) = 45^X modulo 257
with the convention that exptab(128) = 0.

"log" denotes the function logtab(x) = $\log_{45}(x)$
with the convention that logtab(0) = 128.

CYLINK

The SAFER+ Invertible Linear Transformation

y = xM in modulo-256 arithmetic where

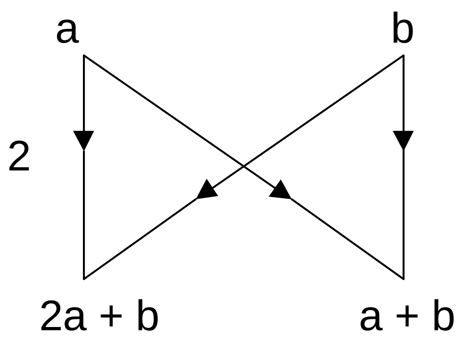
$$M = \begin{bmatrix}
2 & 2 & 1 & 1 & 16 & 8 & 2 & 1 & 4 & 2 & 4 & 2 & 1 & 1 & 4 & 4 \\
1 & 1 & 1 & 1 & 8 & 4 & 2 & 1 & 2 & 1 & 4 & 2 & 1 & 1 & 2 & 2 \\
1 & 1 & 4 & 4 & 2 & 1 & 4 & 2 & 4 & 2 & 16 & 8 & 2 & 2 & 1 & 1 \\
1 & 1 & 2 & 2 & 2 & 1 & 2 & 1 & 4 & 2 & 8 & 4 & 1 & 1 & 1 & 1 \\
4 & 4 & 2 & 1 & 4 & 2 & 4 & 2 & 16 & 8 & 1 & 1 & 1 & 1 & 2 & 2 \\
2 & 2 & 2 & 1 & 2 & 1 & 4 & 2 & 8 & 4 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 4 & 2 & 4 & 2 & 16 & 8 & 2 & 1 & 2 & 2 & 4 & 4 & 1 & 1 \\
1 & 1 & 2 & 1 & 4 & 2 & 8 & 4 & 2 & 1 & 1 & 1 & 2 & 2 & 1 & 1 \\
2 & 1 & 16 & 8 & 1 & 1 & 2 & 2 & 1 & 1 & 4 & 4 & 4 & 2 & 4 & 2 \\
2 & 1 & 8 & 4 & 1 & 1 & 1 & 1 & 1 & 1 & 2 & 2 & 4 & 2 & 2 & 1 \\
4 & 2 & 4 & 2 & 4 & 4 & 1 & 1 & 2 & 2 & 1 & 1 & 16 & 8 & 2 & 1 \\
2 & 1 & 4 & 2 & 2 & 2 & 1 & 1 & 1 & 1 & 1 & 1 & 8 & 4 & 2 & 1 \\
4 & 2 & 2 & 2 & 1 & 1 & 4 & 4 & 1 & 1 & 4 & 2 & 2 & 1 & 16 & 8 \\
4 & 2 & 1 & 1 & 1 & 1 & 2 & 2 & 1 & 1 & 2 & 1 & 2 & 1 & 8 & 4 \\
16 & 8 & 1 & 1 & 2 & 2 & 1 & 1 & 4 & 4 & 2 & 1 & 4 & 2 & 4 & 2 \\
8 & 4 & 1 & 1 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 1 & 2 & 1 & 4 & 2
\end{bmatrix}$$

The matrix **M** is based on the Pseudo-Hadamard Transform (PHT) used in the original SAFER family of ciphers.

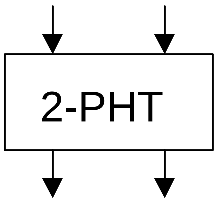
The 2-PHT has the matrix

$$H_2 = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$$

which corresponds to the "butterfly"

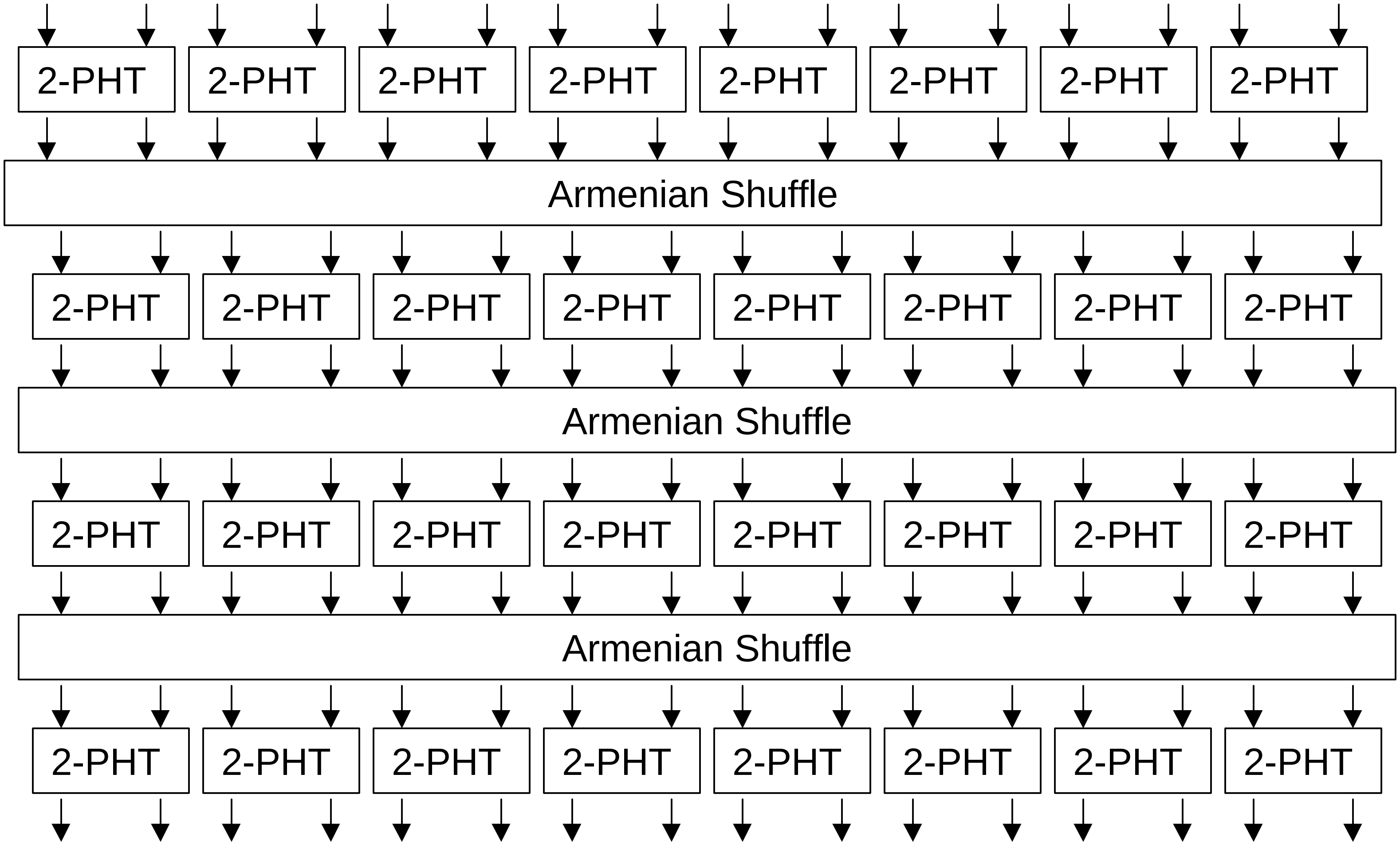


which we denote as



Note that the inverse matrix is $H_2^{-1} = \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix}$

The matrix **M** can be realized as



where the “Armenian Shuffle” is the coordinate permutation:

9 12 13 16 3 2 7 6 11 10 15 14 1 8 5 4

CYLINK

If, as in the original SAFER family, the “Hadamard Shuffle”

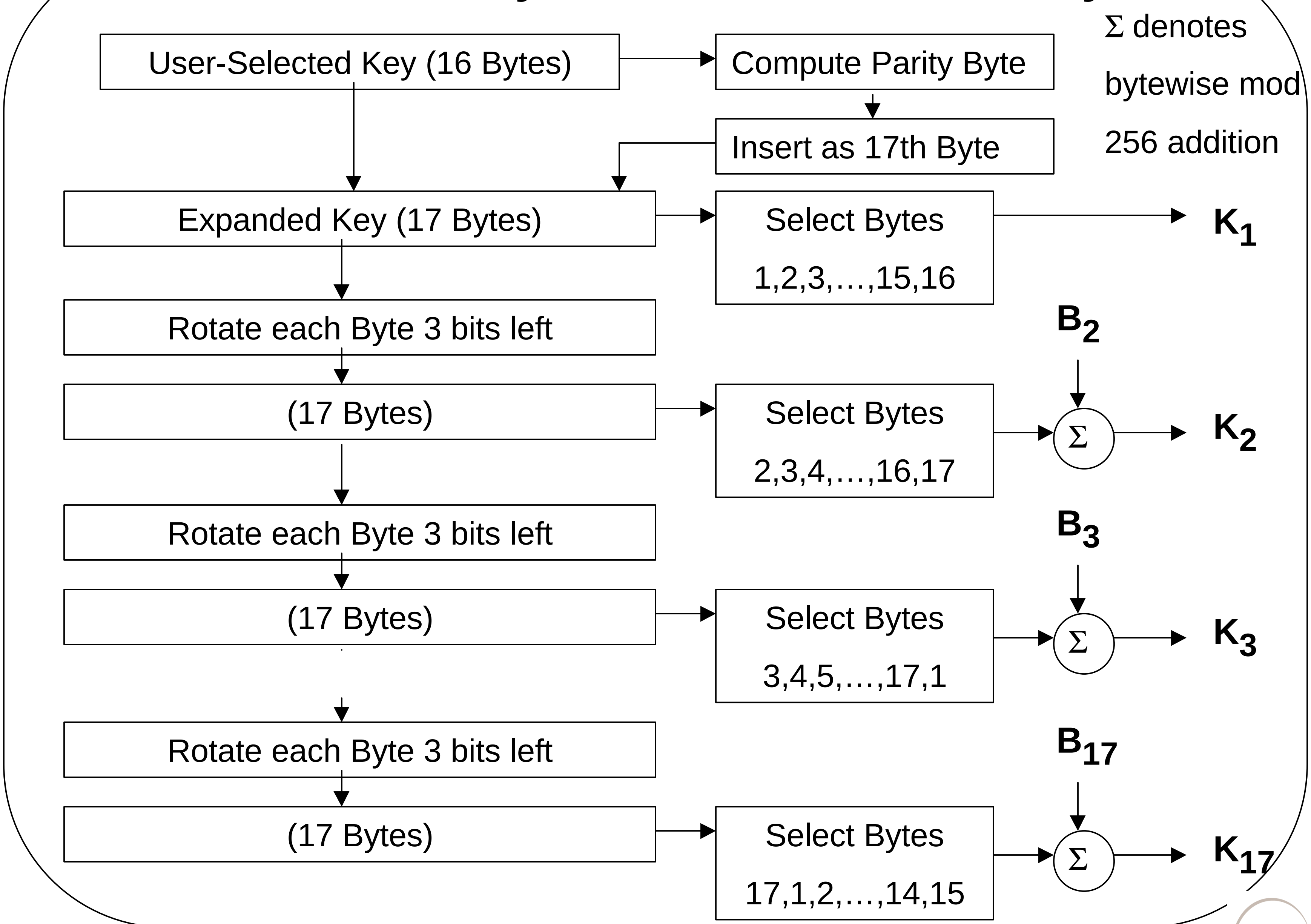
1 3 5 7 9 11 13 15 2 4 6 8 10 12 14 16

(which is that used in the usual Walsh-Hadamard transformation) had been used, the resulting linear transformation would have the matrix

$$\begin{bmatrix}
16 & 8 & 8 & 4 & 8 & 4 & 4 & 2 & 8 & 4 & 4 & 2 & 4 & 2 & 2 & 1 \\
8 & 4 & 8 & 4 & 4 & 2 & 4 & 2 & 4 & 2 & 4 & 2 & 2 & 1 & 2 & 1 \\
8 & 4 & 4 & 2 & 8 & 4 & 4 & 2 & 4 & 2 & 2 & 1 & 4 & 2 & 2 & 1 \\
4 & 2 & 4 & 2 & 4 & 2 & 4 & 2 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 \\
8 & 8 & 4 & 4 & 4 & 4 & 2 & 2 & 4 & 4 & 2 & 2 & 2 & 2 & 1 & 1 \\
4 & 4 & 4 & 4 & 2 & 2 & 2 & 1 & 2 & 2 & 2 & 2 & 1 & 1 & 1 & 1 \\
4 & 4 & 2 & 2 & 4 & 4 & 2 & 1 & 2 & 2 & 1 & 1 & 2 & 2 & 1 & 1 \\
2 & 2 & 2 & 2 & 2 & 2 & 2 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
8 & 4 & 4 & 2 & 4 & 2 & 2 & 1 & 8 & 4 & 4 & 2 & 4 & 2 & 2 & 1 \\
4 & 2 & 4 & 2 & 2 & 1 & 2 & 1 & 4 & 2 & 4 & 2 & 2 & 1 & 2 & 1 \\
4 & 2 & 2 & 1 & 4 & 2 & 2 & 1 & 4 & 2 & 2 & 1 & 4 & 2 & 2 & 1 \\
2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 \\
4 & 4 & 2 & 2 & 2 & 2 & 1 & 1 & 4 & 4 & 2 & 2 & 2 & 2 & 1 & 1 \\
2 & 2 & 2 & 2 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 1 & 1 & 1 & 1 \\
2 & 2 & 1 & 1 & 2 & 2 & 1 & 1 & 2 & 2 & 1 & 1 & 2 & 2 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{bmatrix}$$

with slower diffusion and less resistance to differential cryptanalysis.

SAFER+ Key Schedule for 128 bit key



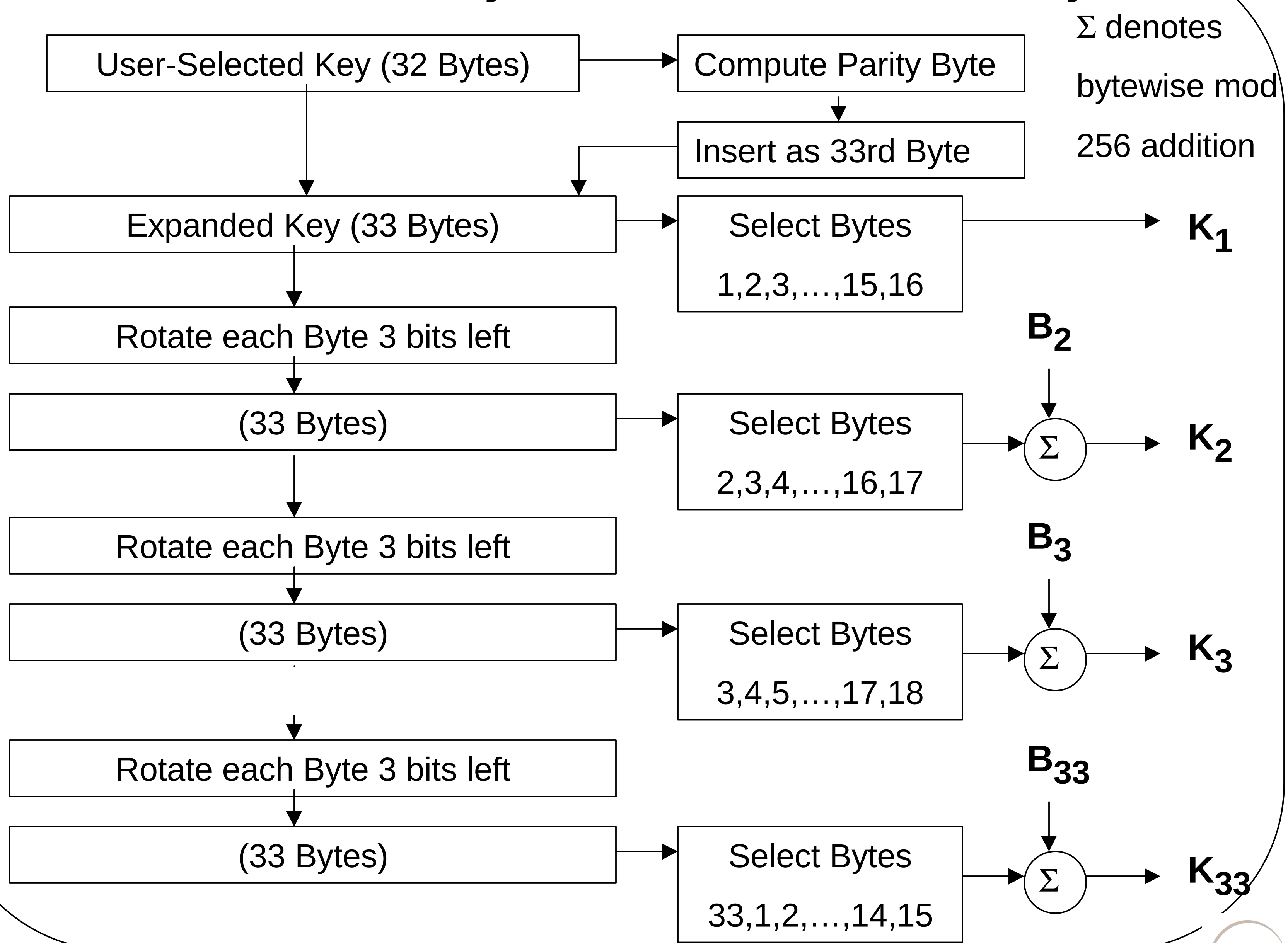
CYLINK

The use of the parity Byte and of the progressive rotation in selecting Bytes was suggested by Dr. **Lars Knudsen** (Univ. of Bergen, Norway).

The **bias words** B_2, B_3, … B_{17} are computed by "double exponentiation" with the function exptab(.) and are as follows:

70	151	177	186	163	183	16	10	197	55	179	201	90	40	172	100
236	171	170	198	103	149	88	13	248	154	246	110	102	220	5	61
138	195	216	137	106	233	54	73	67	191	235	212	150	155	104	160
93	87	146	31	213	113	92	187	34	193	190	123	188	153	99	148
42	97	184	52	50	25	253	251	23	64	230	81	29	65	68	143
221	4	128	222	231	49	214	127	1	162	247	57	218	111	35	202
58	208	28	209	48	62	18	161	205	15	224	168	175	130	89	44
125	173	178	239	194	135	206	117	6	19	2	144	79	46	114	51
192	141	207	169	129	226	196	39	47	108	122	159	82	225	21	56
252	32	66	199	8	228	9	85	94	140	20	118	96	255	223	215
250	11	33	0	26	249	166	185	232	158	98	76	217	145	80	210
24	180	7	132	234	91	164	200	14	203	72	105	75	78	156	53
69	77	84	229	37	60	12	74	139	63	204	167	219	107	174	244
45	243	124	109	157	181	38	116	242	147	83	176	240	17	237	131
182	3	22	115	59	30	142	112	189	134	27	71	126	36	86	241
136	70	151	177	186	163	183	16	10	197	55	179	201	90	40	172

SAFER+ Key Schedule for 256 bit key



Design Principles for SAFER+

- **Encrypting structure** – faster diffusion than for substitution-permutation cipher.
- **Byte orientation** – during encryption and decryption, all operations are on bytes.
- **Group operation at round input** – “perfect secrecy” with a “one-time key”.
- **Use of 2 additive group operations on bytes** -- takes advantage of each’s strength.
- **Confusion via well-defined nonlinear functions** – no “suspicious-looking” tables.
- **Fast-diffusing linear transformation** – via the PHT and the Armenian shuffle.
- **Scalability** – Bytes can be made to 2 or 4 (or even 16) bit characters for study.
- **Biases in key schedules** – eliminates “weak keys”.
- **Parity word and selections in key schedules** – diversity in round subkeys.
- **Number of rounds** – chosen for security with a margin of safety.

CYLINK

Strength of SAFER+ against Differential Cryptanalysis

• An exhaustive study of SAFER+ has shown that all 5-round characteristics have probability significantly smaller than

$$2^{-128}$$

(but that this is not the case for only 4 rounds).

• SAFER+ with six or more rounds (but not fewer) is secure against differential cryptanalysis.

• For a desirable margin of safety, we have chosen 8 rounds for SAFER+ with the 128-bit key schedule. This also has the effect that each byte of the user-selected key affects every byte position within the round keys exactly once. (This is also true for the 192-bit and 256-bit key schedules.)

CYLINK

Strength of SAFER+ against Linear Cryptanalysis

• Linear cryptanalysis is a very effective general attack against ciphers in which the round sub-keys are inserted by modulo-two addition, but is in general a weak attack against ciphers in which the round sub-keys are inserted by addition modulo a larger modulus.

• The attack by linear cryptanalysis on an r-round cipher requires finding an r - 1 round Input/Output (I/O) sum with substantial imbalance.

• Harpes' procedure for finding effective homomorphic I/O sums, which is the only practical procedure known, cannot find an I/O sum with non-zero imbalance for one-and-one-half rounds of SAFER+. We believe that there is no homomorphic I/O sum whatsoever with non-negligible imbalance for one-and-one-half rounds of SAFER+, i.e., SAFER+ is already secure against linear cryptanalysis after only two-and-one-half rounds.

• The 8 rounds of SAFER+ (with a 128-bit key) provide an enormous margin of safety against an attack by linear cryptanalysis.

Computational Efficiency of SAFER+ in Software

(Independent block encryptions -no latency)

ANSI C with 200 MHz Pentium Platform:

- SAFER+ with 128 bit key (8 rounds) – about 18.2* megabits/s of encrypted data and about 15.3 microseconds to run the key schedule.

- SAFER+ with 192 bit key (12 rounds) – about 12.3* megabits/s of encrypted data and about 28.6 microseconds to run the key schedule.

- SAFER+ with 256 bit key (16 rounds) – about 9.3* megabits/s of encrypted data and about 45.7 microseconds to run the key schedule.

Assembly on 8-bit Processors of the MCS 51 family with 16 MHz clock:

- SAFER+ with 128 bit key (8 rounds) – about 25.6 kilobits/s of encrypted data.
- SAFER+ with 192 bit key (12 rounds) – about 16.9 kilobits/s of encrypted data.
- SAFER+ with 256 bit key (16 rounds) – about 12.7 kilobits/s of encrypted data.

*Improved implementation of August 1998.

CYLINK

Computational Efficiency of SAFER+ in Hardware

(Independent block encryptions - no latency)

Simulated hardware implementation in VERILOG HDL using Synplify tools:

- Synplify and MAX+Plus II
- ALTERA chip with speed grade:-3 (80 MHz)
- System clock: 62 MHz.

Results were as follows:

- Number of Synopsys cells 62,000
- Encryption and decryption rate for 128-bit key SAFER+ 58.9 megabits/s

We believe that both the software and hardware efficiencies will be increased substantially as more programming experience and design experience are obtained for SAFER+.

CYLINK

Advantages of SAFER+

- A proven track record of security
- Speed and simplicity
- Transparency
- Flexibility of Use
- Flexibility of Environment

Limitations of SAFER+

- No proof of complete security
- Encryption/Decryption Dissimilarity