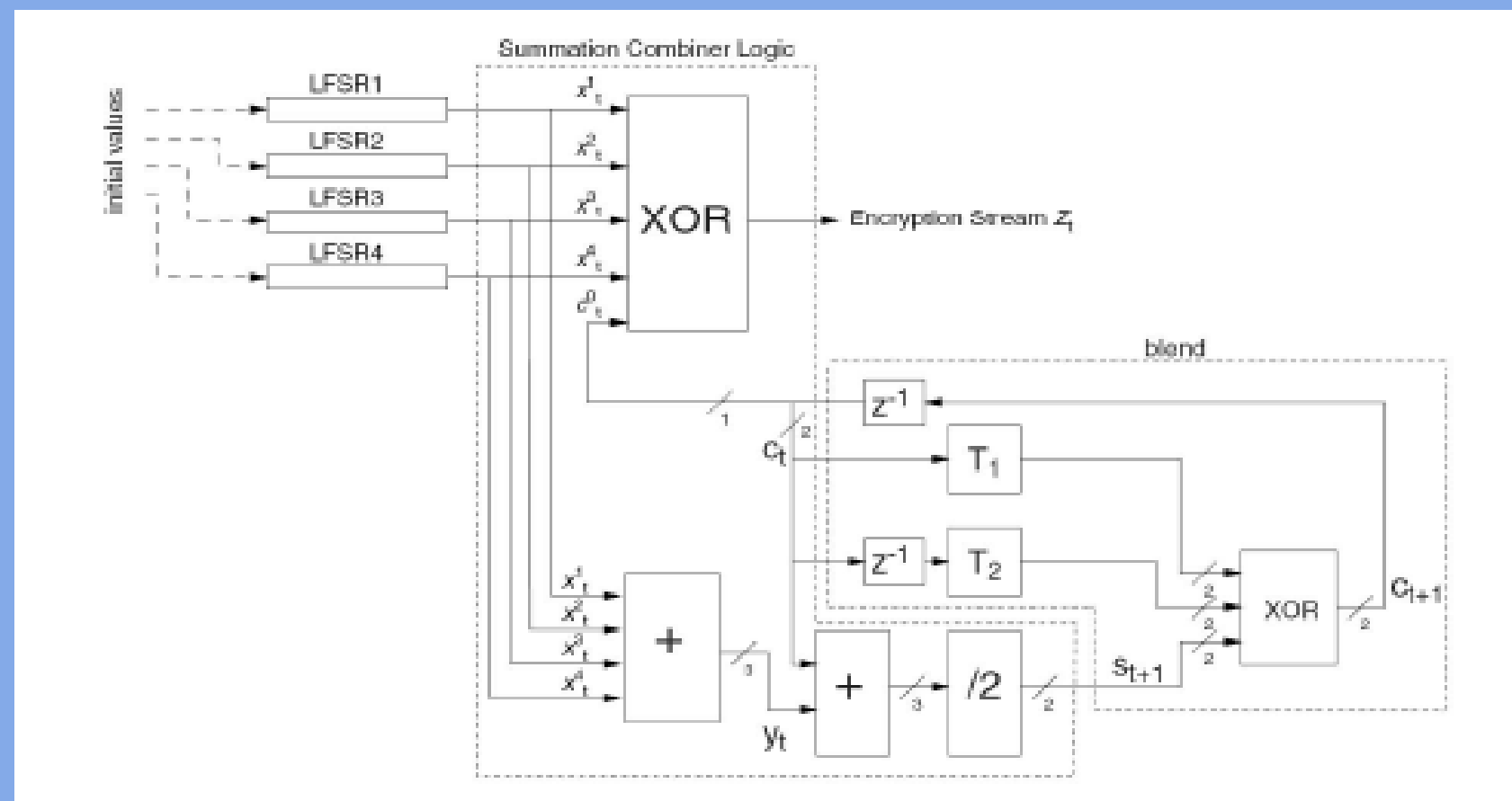


Bluetooth(E0) Cipher



E0 Cipher Design

LFSR Number	LFSR Length	LFSR Feedback Polynomial
1	25	$t^{25} + t^{20} + t^{12} + t^8 + 1$
2	31	$t^{31} + t^{24} + t^{16} + t^{12} + 1$
3	33	$t^{33} + t^{28} + t^{24} + t^4 + 1$
4	39	$t^{39} + t^{36} + t^{28} + t^4 + 1$

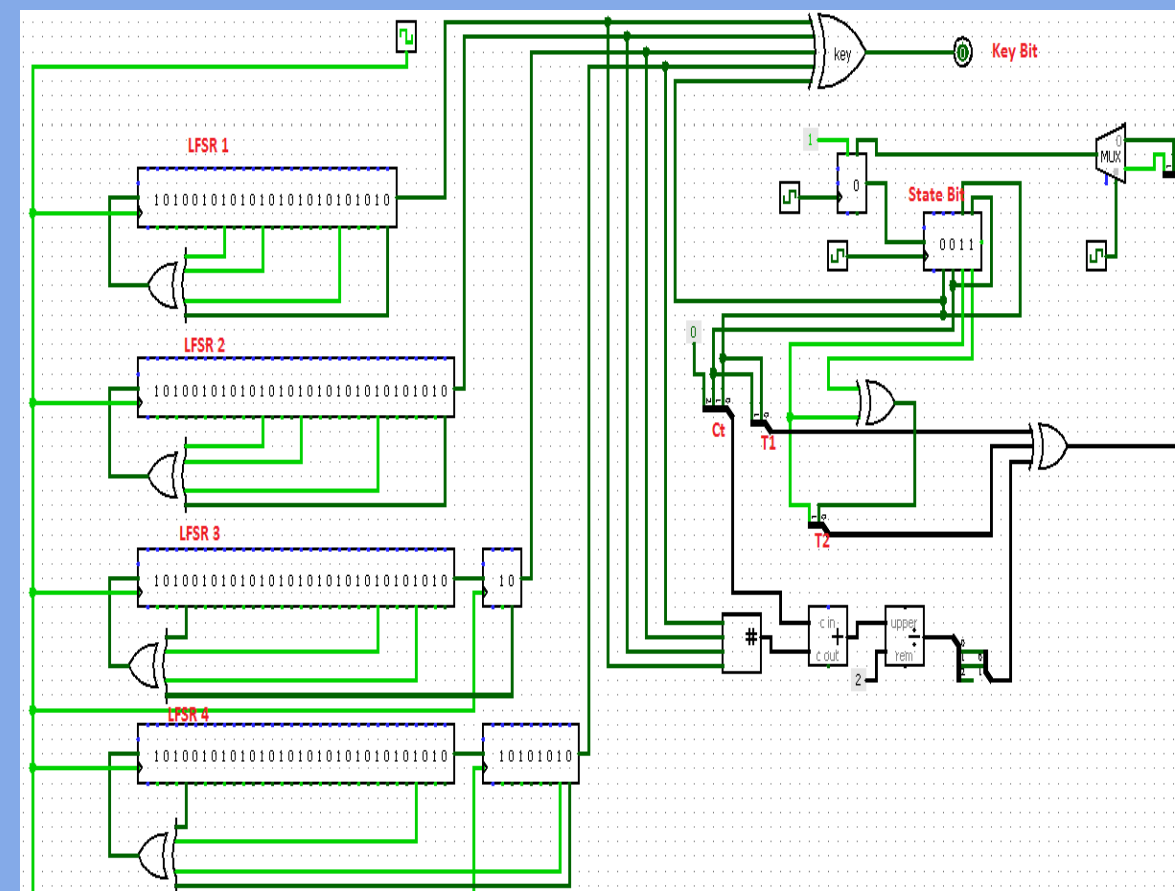
Feedback Polynomial

$$c_{t+1} = \begin{bmatrix} c_{t+1}^0 \\ c_{t+1}^1 \end{bmatrix} = s_{t+1} \oplus T_1[c_t] \oplus T_2[c_{t-1}]$$

Calculation of State bits

$$T_1 : (x_1, x_0) \mapsto (x_1, x_0),$$
$$T_2 : (x_1, x_0) \mapsto (x_0, x_1 \oplus x_0),$$

Calculation of T1 and T2



Simulation design in LOGISIM

Bluetooth Version	Speed	Compatibility
Bluetooth v1.0 and v1.0B	< 0.7 MBPS	Yes
Bluetooth v1.1	< 0.7 Mbps	Yes
Bluetooth v1.2	0.7 Mbps	No
Bluetooth v2.0 + EDR	2.1 Mbps	No
Bluetooth v2.1 + EDR	24 Mbps	No
Bluetooth v3.0 + HS	24 Mbps	No

Compatibility with Bluetooth Versions

Initializing LFSR's	0.004838 ms
CUDA malloc	243.0138 ms
CPU to GPU copy	0.006840 ms
GPU calculation	0.029884 ms
GPU to CPU copy	4.000000 ms
Total Time for key generation	0.664239 ms

Analysis of execution time in CUDA

==3010== Profiling result:						
Time(%)	Time	Calls	Avg	Min	Max	Name
98.38%	658.87us	1	658.87us	658.87us	658.87us	LFSR_SHIFT(int*, int*, int*, int*, int*)
1.02%	6.8480us	5	1.3690us	1.1520us	1.6320us	[CUDA memcpy DtoH]
0.60%	4.0000us	5	800ns	736ns	960ns	[CUDA memcpy HtoD]
==3010== API calls:						
Time(%)	Time	Calls	Avg	Min	Max	Name
97.12%	64.846ms	5	12.969ms	6.9340us	64.813ms	cudaMalloc
1.20%	799.29us	83	9.6290us	711ns	376.60us	cuDeviceGetAttribute
1.16%	776.87us	10	77.686us	7.1470us	667.87us	cudaMemcpy
0.19%	127.56us	5	25.512us	5.9390us	94.682us	cudaFree
0.15%	101.07us	1	101.07us	101.07us	101.07us	cuDeviceTotalMem
0.13%	86.235us	1	86.235us	86.235us	86.235us	cuDeviceGetName
0.03%	19.931us	1	19.931us	19.931us	19.931us	cudaLaunch
0.01%	5.7840us	5	1.1560us	235ns	4.4320us	cudaSetupArgument
0.01%	4.5910us	2	2.2950us	1.1680us	3.4230us	cuDeviceGetCount
0.00%	2.3000us	2	1.1500us	987ns	1.3130us	cuDeviceGet
0.00%	1.2150us	1	1.2150us	1.2150us	1.2150us	cudaConfigureCall

Profiling Result

CUDA	C
0.664 ms	32 ms

Execution time for 200 bits

CUDA	C
0.333 Mbps	0.0062 Mbps

Communication Speed

```
C:\Users\SYSTEM-2\documents\visual studio 2010\Projects\cipher_text\Debug\...
Initial value of LFSR
LFSR1 <25> 1100100000111111010010
LFSR2 <31> 0100110101011101101110100111
LFSR3 <33> 0001110010000000001010011011000001
LFSR4 <39> 001011000111110001010110001111000101110
After initial 200 iteration
LFSR1 <25> 000000001100111100110100
LFSR2 <31> 11100110100101001100100110011000
LFSR3 <33> 00001010101001110000000101111100000
LFSR4 <39> 011000111000000111110100110100001101111
After generating 200 key bits
LFSR1 <25> 10001101101011001111111111
LFSR2 <31> 11010111010010111010000111111111
LFSR3 <33> 00000011011010001101011000011010111
LFSR4 <39> 100001100111110011110111001101110010010
200 KEY bits
0 0 0 0 1 1 0 0 0 0 0 0 0 0 0 1 0 1 1 1 0 0 1 1 0 0 1 1 1 0 0 0 1 0 0 1 1 1 1 0
0 0 0 1 1 0 0 0 0 0 0 0 1 0 1 0 0 0 1 0 0 0 0 1 0 0 0 1 1 0 0 0 0 0 0 1 1 0 0 1
1 0 0 1 0 1 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 1 1 1 1 1 1 0 0 1 0 1 1 1 1 0 1
1 1 0 0 0 0 0 0 1 1 0 1 1 1 0 1 0 1 1 1 1 1 0 0 0 1 0 0 1 0 1 1 1 1 1 0 1 0 1 0
1 0 0 1 1 0 1 0 1 1 1 1 1 0 0 1 0 0 0 0 1 1 1 1 0 0 0 1 0 0 1 0 1 1 1 1 0 1 0 1 0
INPUT DATA
Helloooo.....
Hiii.....!!!!!!
I m Reshma Sanghariyat..
Bye ....???
ENCRYPTED DATA
NeB      8t_G1B-7%e(!G45yL@t;J'  ?fJcP!t+.<^<i<L<H#J! :e7-\t6+Δ 8
DECRYPTED DATA
Helloooo.....
Hiii.....!!!!!!
I m Reshma Sanghariyat..
Bye ....???
```

Output of CUDA code

```
C:\Users\SYSTEM-2\Documents\Visual Studio 2010\Projects\seq2\Debug\seq2....
Initial value of LFSR's
LFSR1 <25> 110010000011111101010010
LFSR2 <31> 0100110101011101101110100111
LFSR3 <33> 000111001000000000101000110110000001
LFSR4 <39> 001011000111110001010110001111000101110
After Initial 200 iterations
LFSR1 <25> 110010000011111101010010
LFSR2 <31> 0100110101011101101110100111
LFSR3 <33> 000111001000000000101000110110000001
LFSR4 <39> 001011000111110001010110001111000101110
After generating 200 key bits
LFSR1 <25> 1001010011001000010010101
LFSR2 <31> 1000110101000101011001101010011
LFSR3 <33> 00011011111110010101100101110101
LFSR4 <39> 110100011101101000101101101100100100101
200 KEY bits
1 0 1 0 0 1 0 1 0 1 1 1 1 0 0 1 0 1 0 0 0 1 0 0 0 1 0 0 1 1 0 1 1 1 1 0 1 0 0 0 1 1 0
0 0 0 1 1 1 0 0 0 0 0 0 1 0 1 0 1 1 1 0 0 0 0 1 1 0 0 0 1 0 0 1 0 0 1 0 0 1 1 1 1 0
0 0 1 1 1 0 1 1 1 1 0 1 1 0 1 0 1 1 0 0 1 0 0 1 1 1 1 1 1 0 1 0 1 1 1 1 0 0 0 0 1
0 0 0 1 0 0 1 1 0 0 1 1 1 1 1 1 0 1 1 0 0 1 0 0 1 0 1 0 0 0 1 0 0 1 1 1 1 0 1 0
0 1 1 0 1 0 1 0 1 0 0 1 0 1 0 0 0 1 0 1 1 1 0 1 0 1 0 1 1 0 0 0 1 0 1 0 0 1 1 0
Time Require to intializing LFSR's :0.022484 ms
total time for Sequential code :32.673420 ms_
```

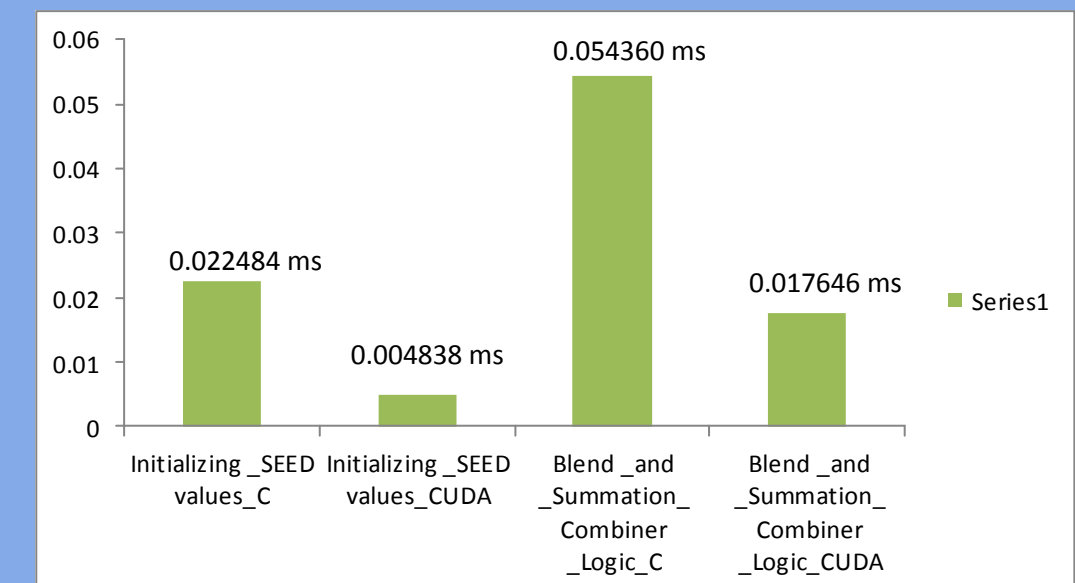
Output of C code

Conclusion

In real time application of Bluetooth Communication, communication speed is 0.7 to 2.1 Mbps. Whereas in CUDA we will get communication speed is **0.33 Mbps** which is very less compare to actual Bluetooth communication. Here, we conclude that we can replace lower version of Bluetooth communication hardware with our software code (CUDA code).

Guided By
Prof. Darshana Upadhyay

Prepared by
Reshma Sanghariyat (11bce127)
Darshil Patel(11bce070)



Module wise Comparison

