An Energy-Efficient Random Number Generator for Stochastic Circuits

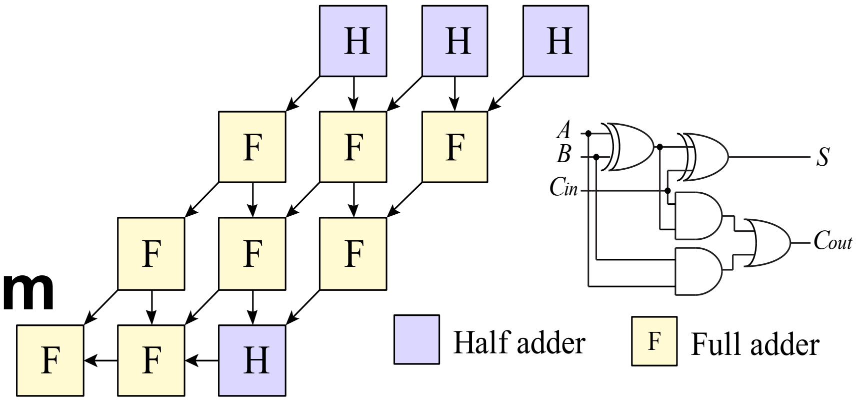
Kyounghoon Kim[1], Jongeun Lee[2],
Kiyoung Choi[1]

Seoul National University[1]
UNIST[2]

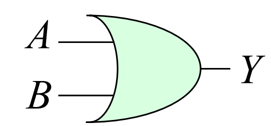
Stochastic computing (SC)

- A (pseudo) random bit stream
- SC uses the probability of 1's
- Advantages
  - Very small hardware footprint
    - Multiplication → AND gate
    - Compound arithmetic
  - High fault tolerance
  - Bit-level massive parallelism

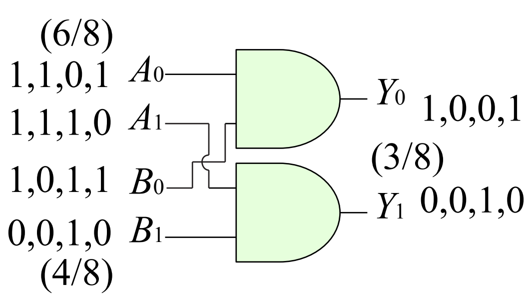
Ex)1,0,0,1,0,0,1,0 (3/8)

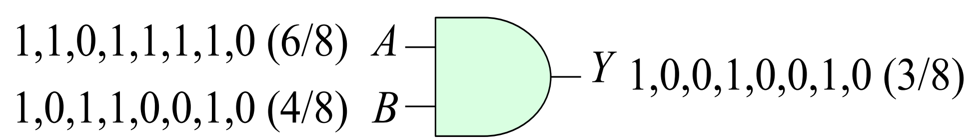


< Multiplication >



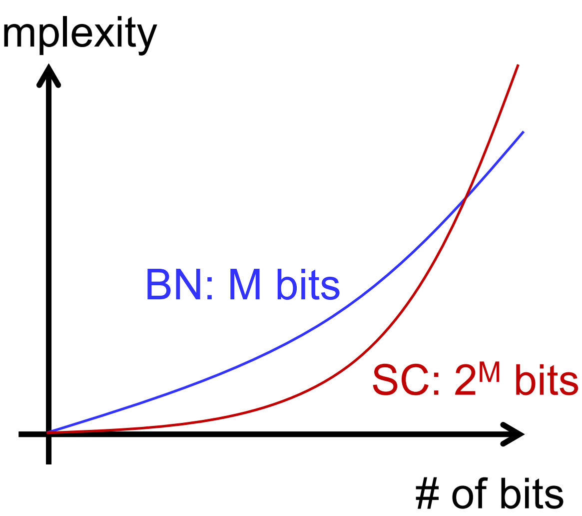
$y=a+b - ab$





Stochastic computing (SC)

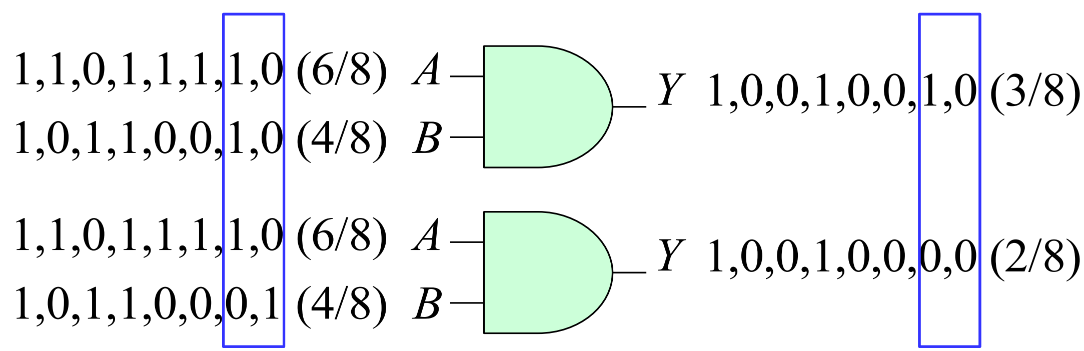
- **Disadvantage**
  - **Exponential complexity**
    - **For same resolution**
    - **Conventional binary logic (BN) : M bits**
    - **Stochastic logic (SC) : 2^M bits**
  - **Random bit generation**
  - **Error from probability**
    - **Approximate computation**



011 (BN)

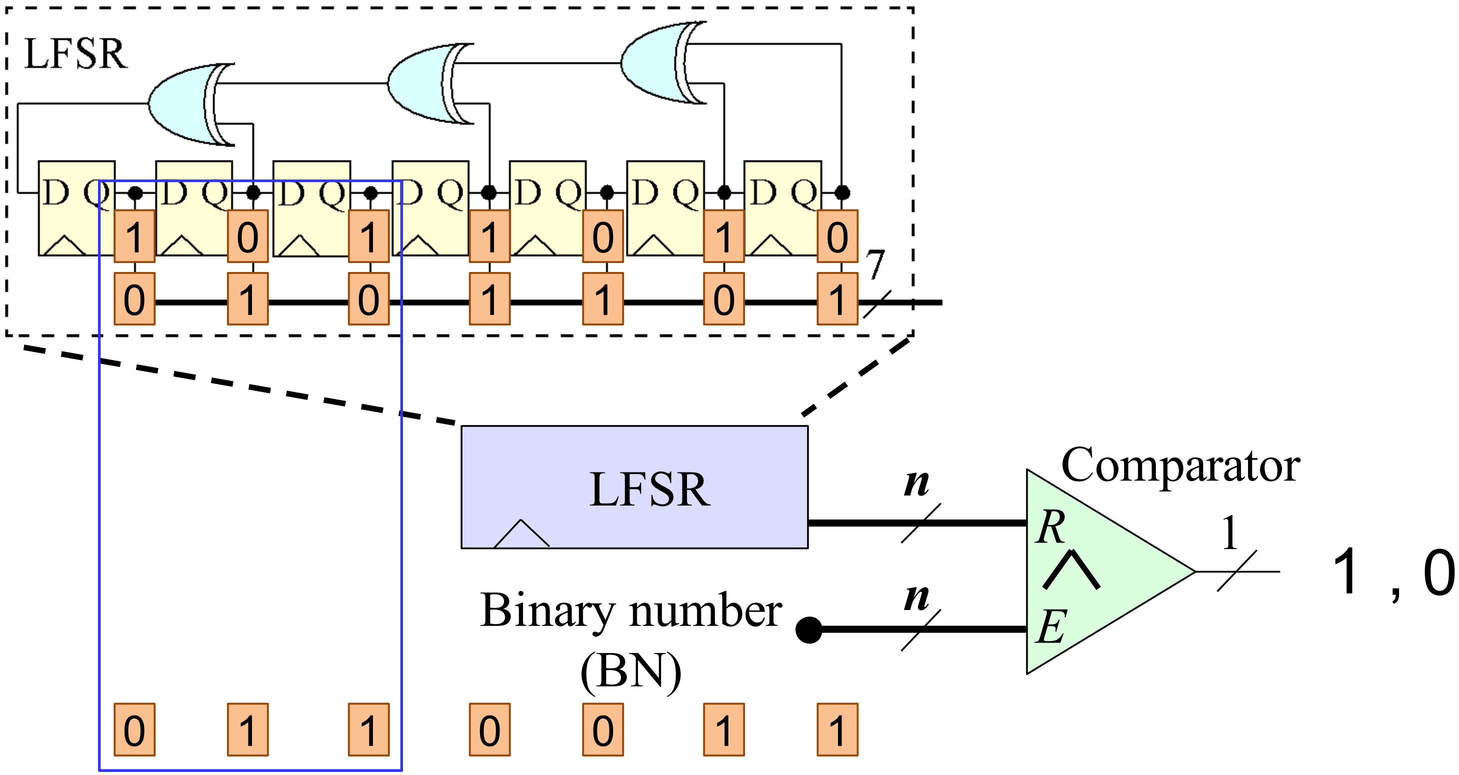
Randomizer

1,0,0,1,0,0,1,0 (SN)



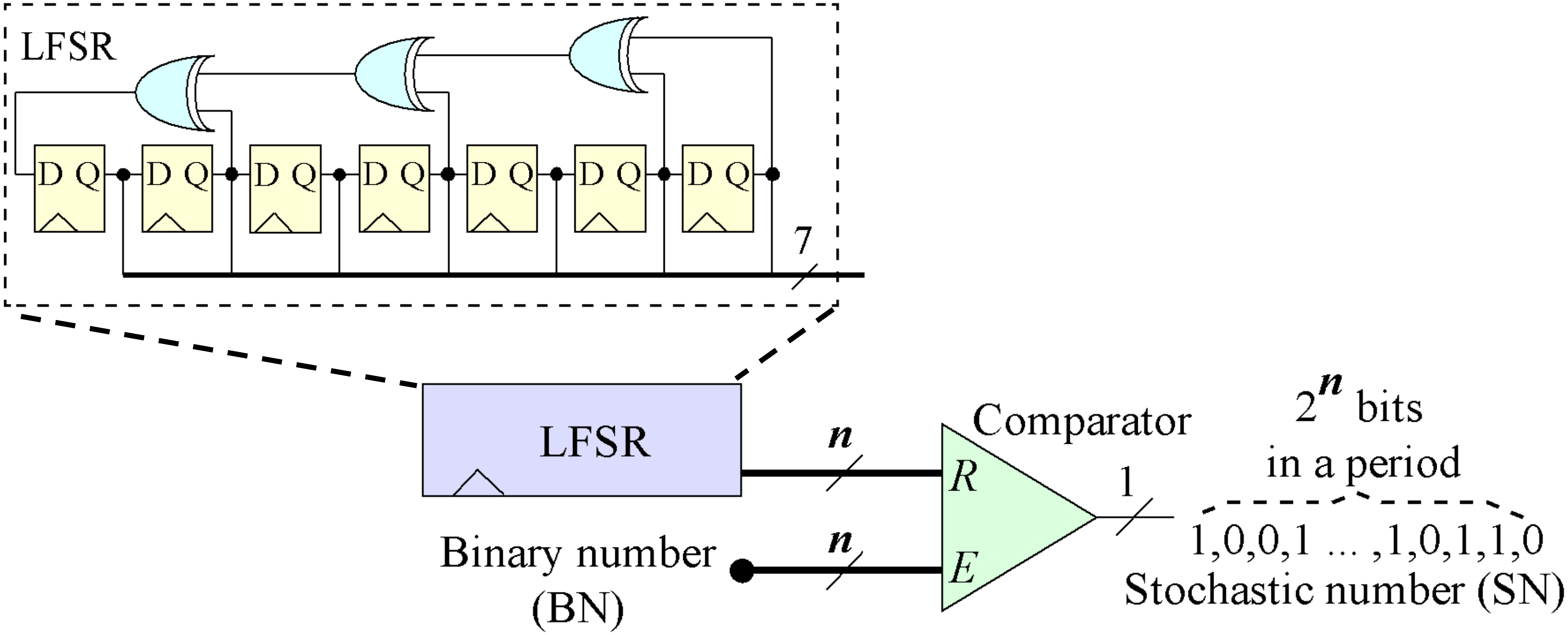
Introduction to SNG

- **Stochastic number generator (SNG)**
  - **Binary number (BN) to stochastic number (SN)**
  - **Linear feedback shift register (LFSR)**



Shortcomings of Conventional SNG

- Single stochastic bit
  - Activating the entire SNG circuit including the LFSR
    - Ex) 512 activation for 512-bit stream
  - Energy consumption



Long bit-stream!

Shortcomings of Conventional SNG

- **Inaccurate random number generation**
  - Ex) Generating SC 2^5 bits by using 10-bit LFSR
- **Progressive precision (PP) in SC**
  - Precision can be dynamically changed

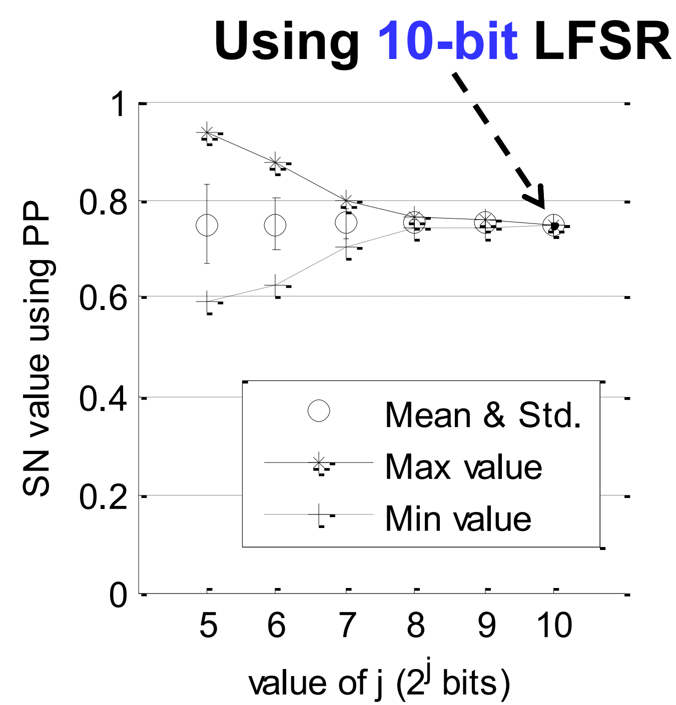
Ex) Generating SC 0.75 value

2^5 24/32 = 0.75

2^8 192/256 = 0.75

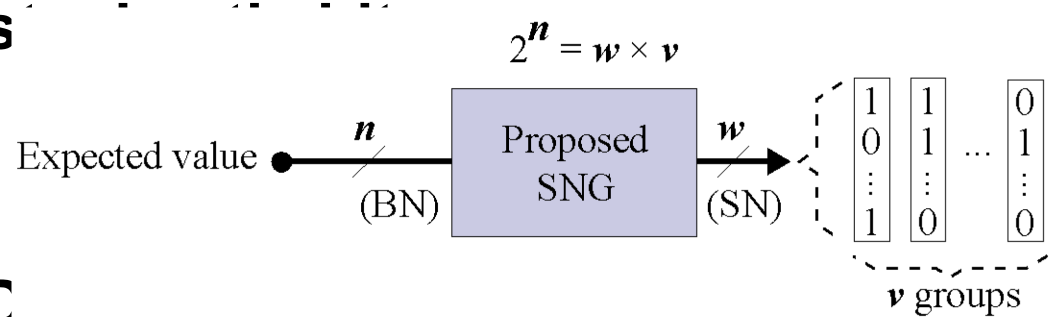
2^{10} 768/1024 = 0.75

< Progressive precision >

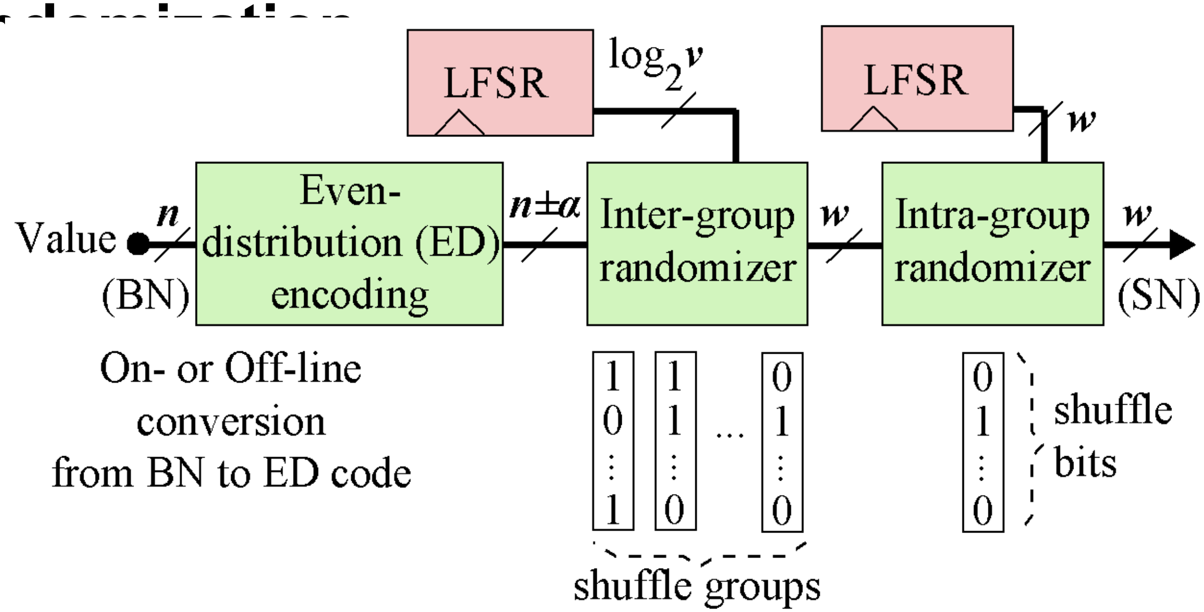


Overview of Proposed SNG

- Proposed Scheme
  - Generating a single s
    - → Shuffling 1s

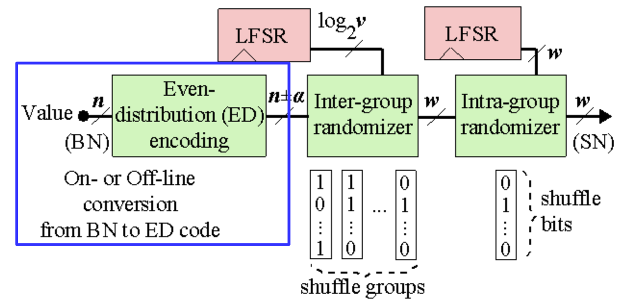


- Components
  - Even-distribution (ED
  - Inter-group randomization
  - Intra-group rar



Even-distribution (ED) encoding

- **Total weights:** $\sum_{j=0}^{k} 2^j b$
- **Difference of the number of 1s between groups**
  - $\max_{i \in v} \boldsymbol{g_i} - \min_{i \in v} \boldsymbol{g_i} \leq b$
  - $2^k b - \sum_{j=0}^{k-1} 2^j b = b$
- **Worst case error:** $\lfloor b/2$
- **Encoding**
  - **Saturation**
  - **Digit**
  - **Group**
  - **Ex) 237, 76**



Decimal L: 237

ED Code: 1-10-010 (Compact)
100-10-010 (Fixed length)

Saturation digit	Digit index	Group ID 0	1	2	3	4	5	6	Weight (b=3)
1	11	1	1	1	1	1	1	1	24
0	10	1	1	α					12
0	01			1	1	1	1	1	6
	00			1	1	1	1	1	3
	Group index	000	001	010	011	100	101	110	

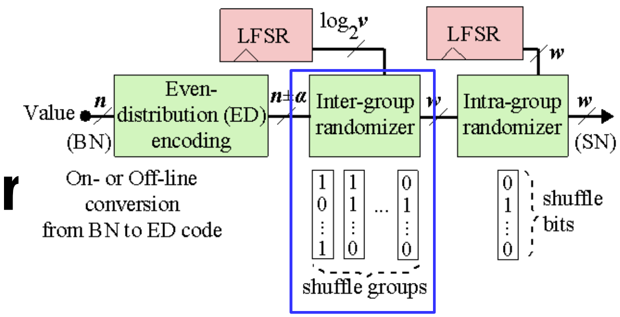
Decimal L: 76

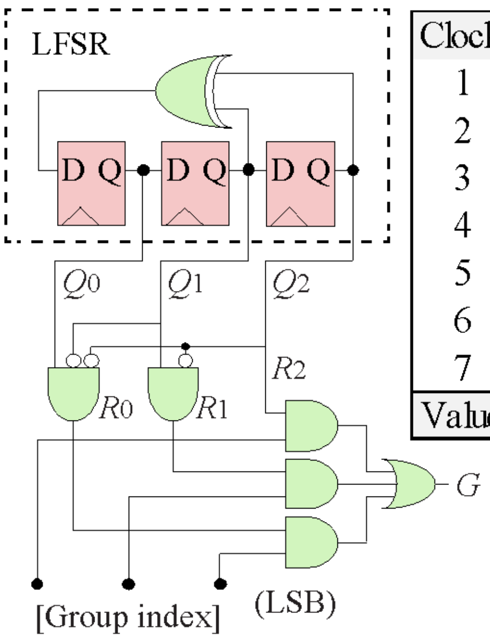
ED Code: 01-01-0001 (Compact)
010-01-0001 (Fixed length)

Saturation digit	Digit index	Group ID 0	1	2	3	4	…	14	Weight (b=1)
0	11								8
1	10	1	1	1	1	1	…	1	4
0	01	1	α						2
	00		1	1	1	1		1	1
	Group index	0000	0001	0010	0011	0100	…	1110	

Inter-group Randomization

- **Sequence of the groups**
  - **scrambled in inter-group randomizer**
  - **Group index, digit index, saturation**

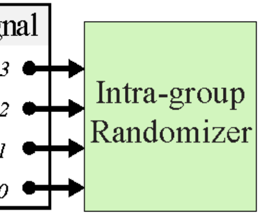




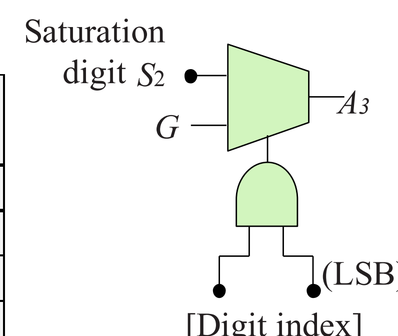
Clock	Q_0	Q_1	Q_2	R_0	R_1	R_2	G
1	0	0	1	0	0	1	0
2	1	0	0	1	0	0	0
3	0	1	0	0	1	0	1
4	1	0	1	0	0	1	0
5	1	1	0	0	1	0	1
6	1	1	1	0	0	1	0
7	0	1	1	0	0	1	0
Value	4/7	4/7	4/7	1/7	2/7	4/7	2/7

Group index	0	1	0

	Group ID								
	2	3	0	4	1	5	6		
G	0	0	1	0	1	0	0	Weig.	Signal
	1	1	1	1	1	1	1	24	A_3
			1		1			12	A_2
	1	1		1		1	1	6	A_1
	1	1		1		1	1	3	A_0
Clock	1	2	3	4	5	6	7		

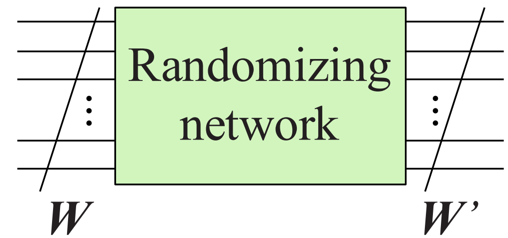


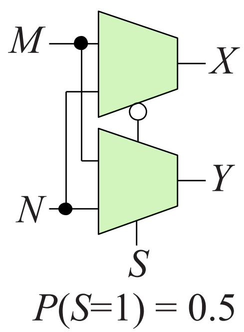
Row index of α				Output signal
11	10	01	00	
G	S_2	S_2	S_2	A_3
$\sim G$	G	S_1	S_1	A_2
$\sim G$	$\sim G$	G	S_0	A_1
$\sim G$	$\sim G$	$\sim G$	G	A_0

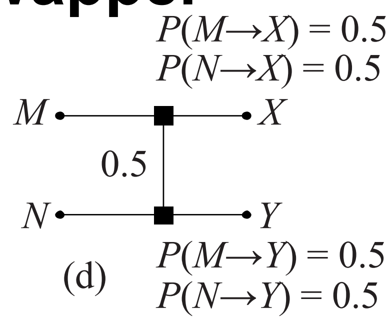


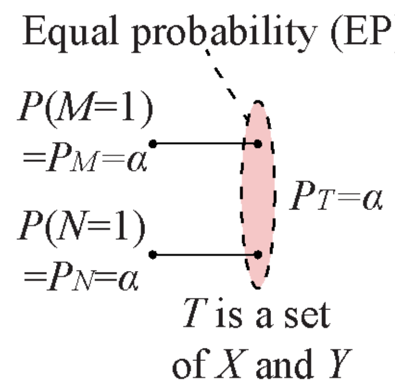
Intra-group Randomization (1/2)

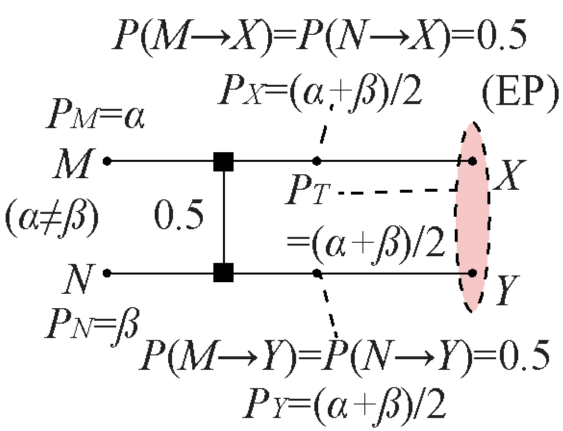
- **Proposed building block for bit shuffling**
  - **Equal probability (EP) set**
  - **Two input signals and swapper**
  - **Two EP sets and swapper**

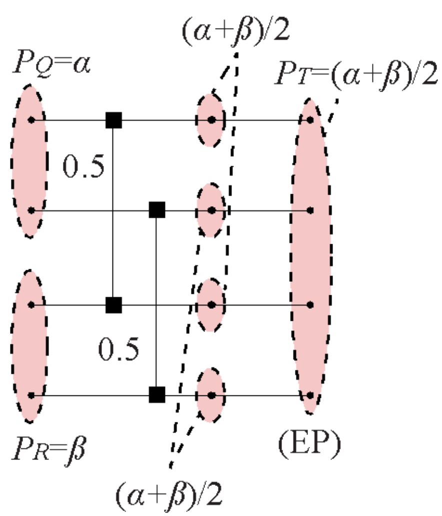


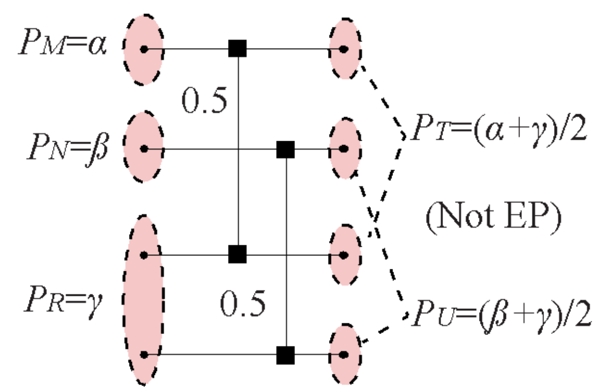








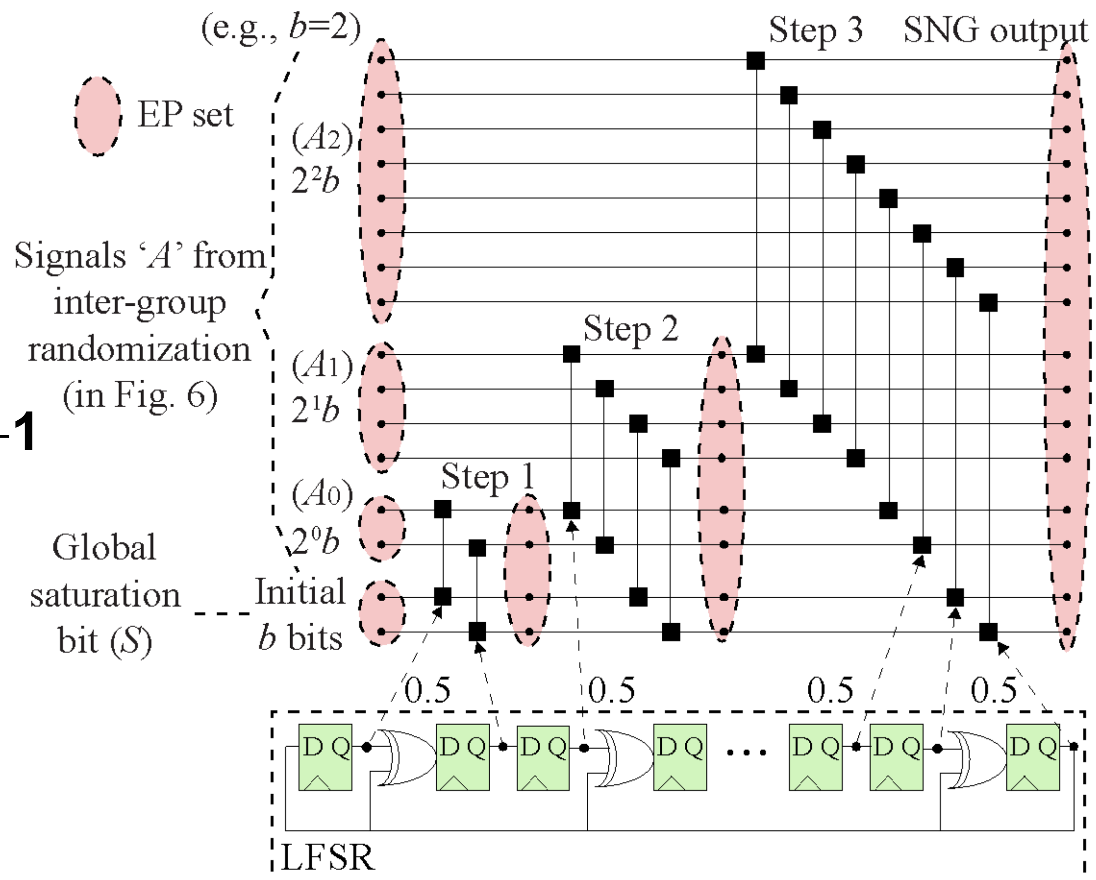




Intra-group Randomization (2/2)

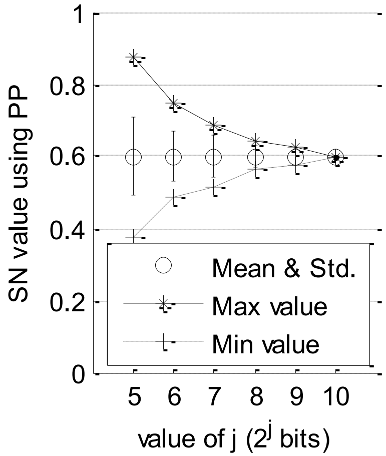
- **Randomizing network**
  - **Scrambled by using the intra-group randomizer**
  - **Global saturation bit**

$$\begin{cases} \text{if } L \geq (b \cdot v)\text{, then } L \leftarrow (L - b \cdot v),\ S \leftarrow 1 \\ \text{otherwise, } L \leftarrow L,\ S \leftarrow 0 \end{cases}$$

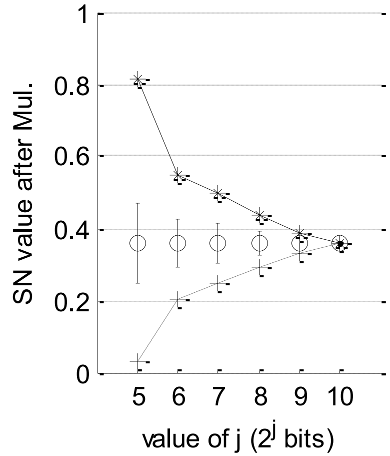


Experimental Result

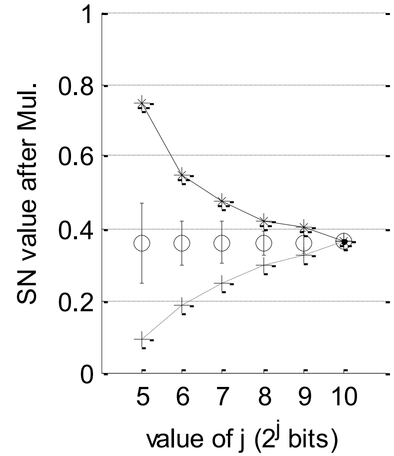
- **Accuracy** of generated stochastic bit stream



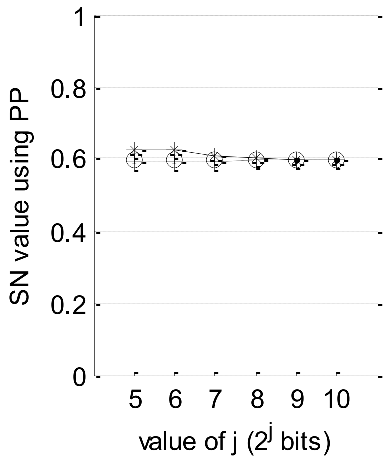
<Conventional SNG>
[1] (Mul.)>



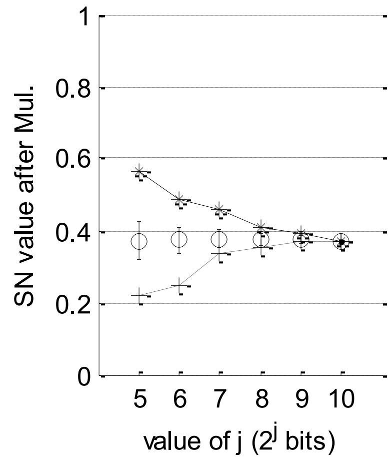
<Conv. SNG (Mul.)>



<Shared SNG



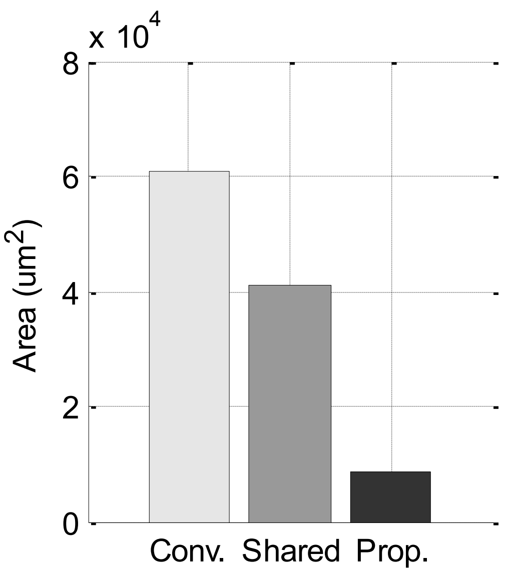
<Proposed SNG>
(Mul.)>

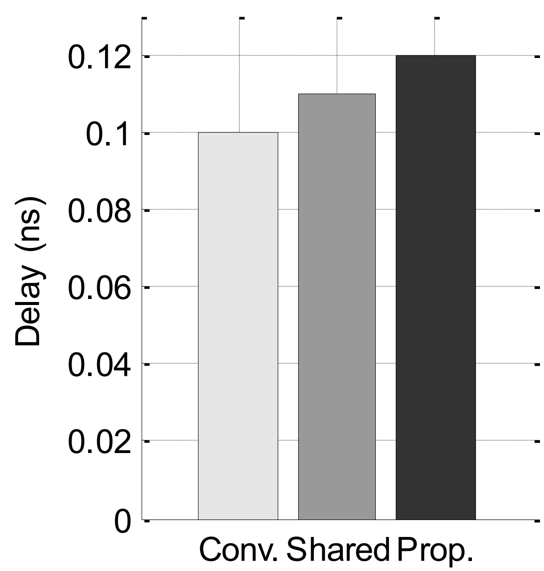


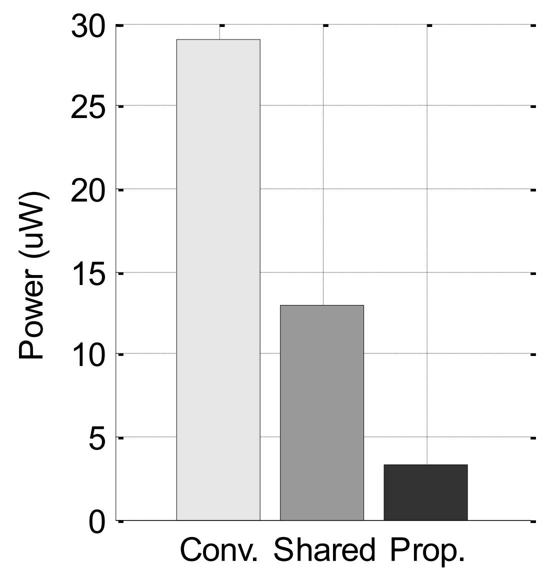
<Prop. SNG

Experimental Result

- **Area, critical path delay, power**

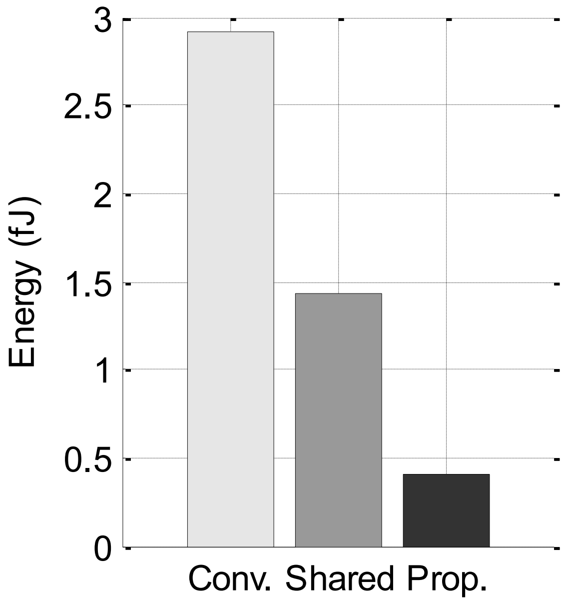


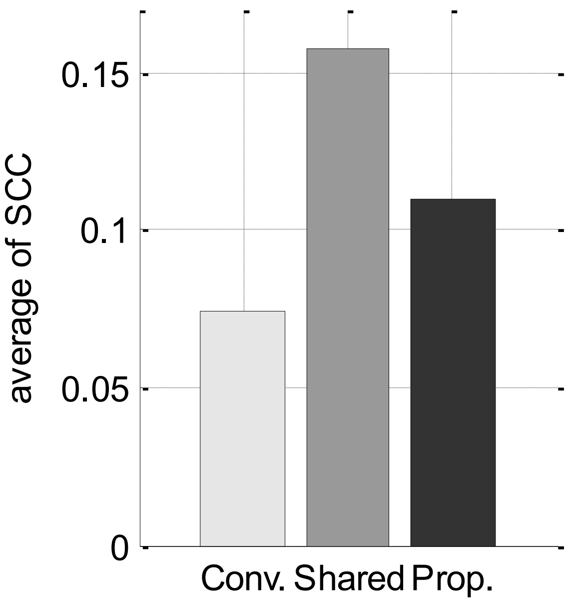




Experimental Result

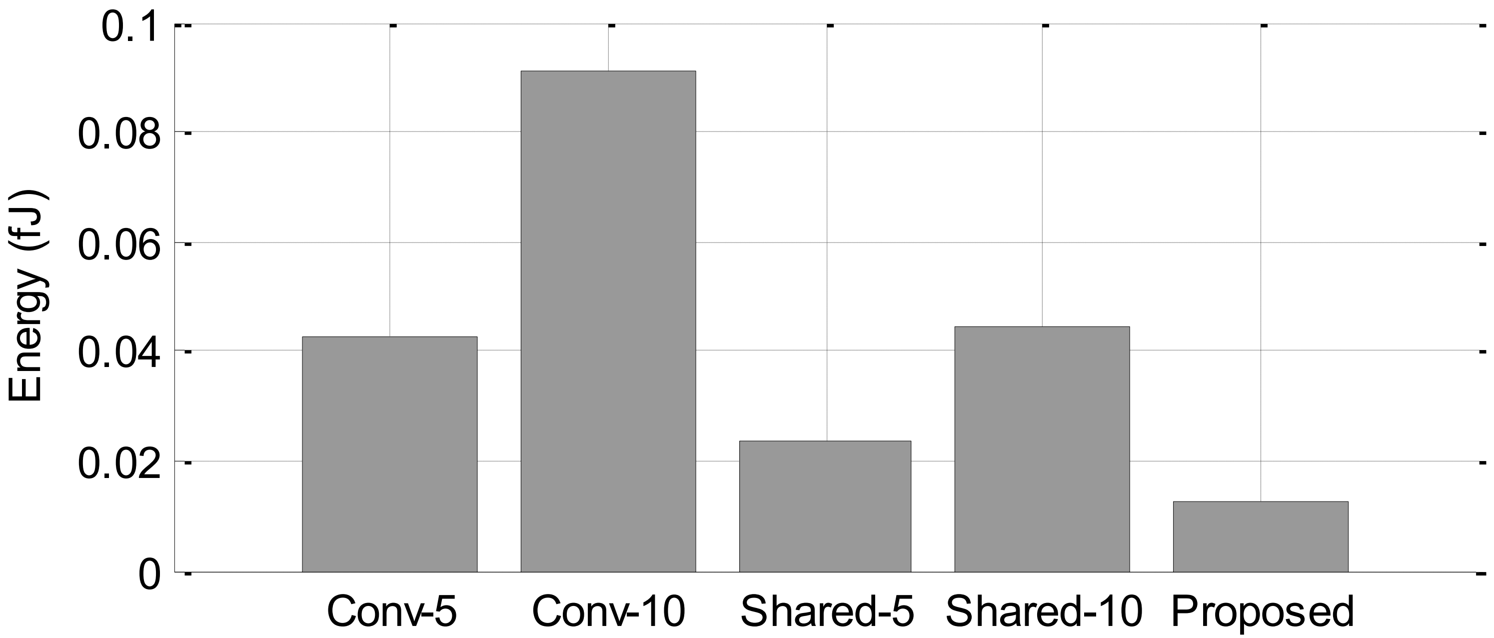
- **Energy and SC correlation (SCC)**





Experimental Result

- **Energy** to generate 2^5 bits
  - Conventional & previous work
    - With 5-bit LFSR
    - With 10-bit LFSR
  - Proposed



Conclusion

- **Stochastic computing requires random bit streams**
  - **It incurs area and energy overhead**
- **We proposed area- and energy-efficient SNG**
- **Experimental results**
  - **our SNG outperforms the existing approaches in terms of area, power, energy, and accuracy**

Thank you

Q&A