MOSBius-style Modular Data Conversion Chip (and Random Number Generation)

Lumut Bius Team - Project Proposal

Team Background

Our team is composed of four second year undergraduate Electrical Engineering students from ITB, Indonesia. **We have no prior IC design experience**.

Our team members consist of:

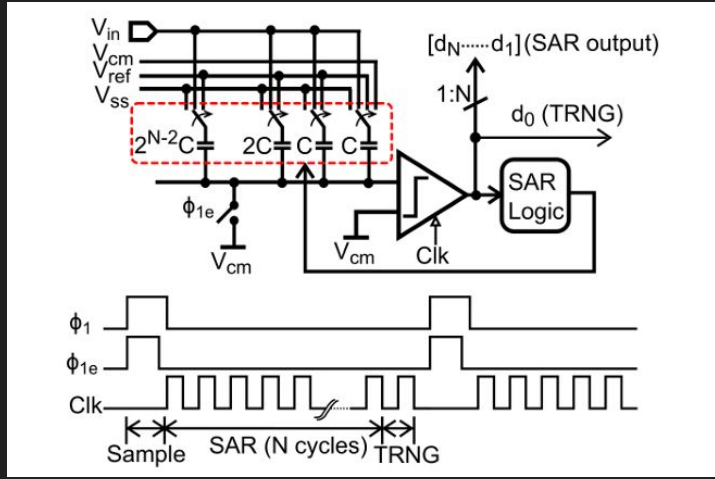
1. Andreas Adyatma Aryadeksa; element: Andreas Arya
2. Dharma Anargya Jowandy; element: AnargyaJo
3. Lionel Naythan Liu; element: Lionel Naythan Liu
4. Rizmi Ahmad Raihan; element: candrasengkala

Overview

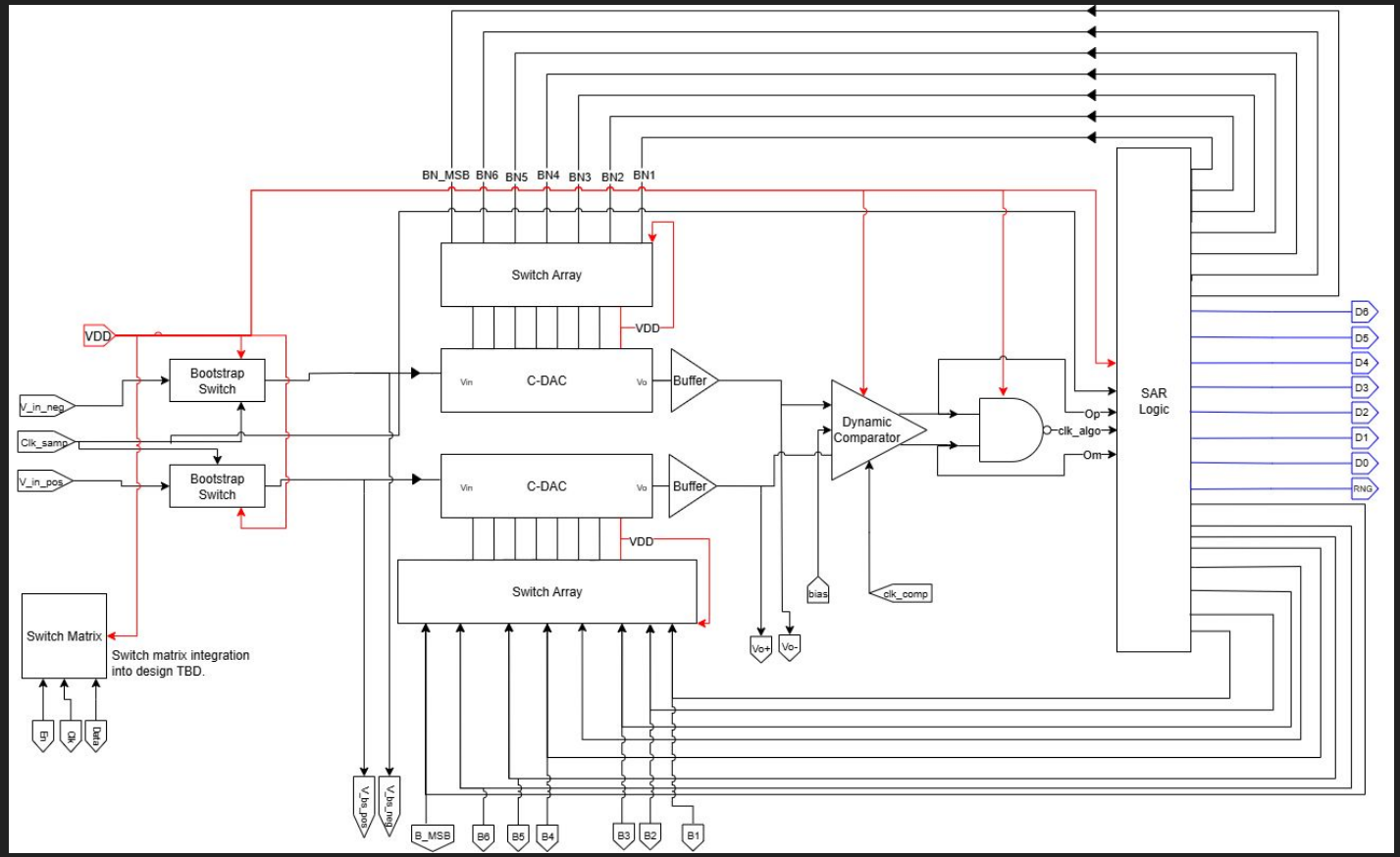
- This IC is based on IHP-AnalogAcademy's SAR ADC design. MOSBius allows the design to be made modular such allowing DAC within the ADC design to be used independently.
- This circuit runs on 3.3V (more on specifications).
- The ADC requires several clocks to operates. Clock generation will be done externally.
- Block diagram included in this file is without switch matrix integration. We plan to make one DAC operable without being hardwired to ADC.

SAR-ADC based TRNG

- Once a SAR ADC has finished quantization, the residue Vres is present at the inputs to the comparator. This residue acts as an entropy source for random number generation.
- At the end of a conversion cycle, the comparator is fired again to quantize the residue. The 1-bit quantized residue behaves as a true random sequence and no additional circuits are required.
- This TRNG system reduces ADC resolution from 8 bits to 7 bits.



Block Diagram (Top Level)



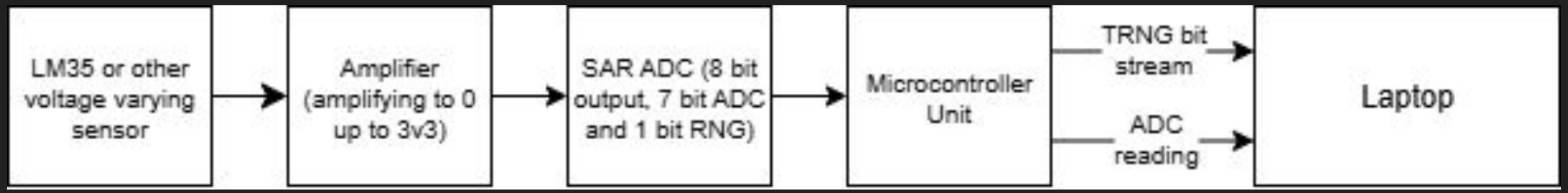
Pin List

Parameter	Value	Unit	Description
VDD	3.3	V	Supply voltage.
Data	TBD	V	Input data for switch matrix
EN	TBD	V	Enable for switch matrix
V_in_pos	0 up to 3.3	V	Positive differential input
V_in_neg	0 up to 3.3	V	Negative differential input
Clk_samp	TBD	Hz	Sampling clock
V_bs_pos	0 up to 3.3	V	Positive bootstrap switch output.
V_bs_neg	0 up to 3.3	V	Negative bootstrap switch output
B_MSB to B1	0 or 3.3	V	Digital input for DAC switch array
Vo+	0 up to 3.3	V	Positive DAC output
Vo-	0 up to 3.3	V	Negative DAC output
bias	1.65	V	Comparator bias, valued at common mode voltage
clk_comp	TBD	Hz	Comparator frequency.
D6 to D0		V	Digitial ADC output.
RNG	0 or 3.3V	V	Digital output, LSB of ADC output. RNG output

SAR-ADC Implementation

We plan to implement SAR-ADC for temperature sensor reading. We will use LM35 as the temperature analog sensor. Analog output of LM35 is converted into digital signal by SAR-ADC which is further processed by microcontrollers. The ADC also produces random number bitstream which can be collected for further encryption usage.

Block Diagram Implementation



Timeline

	Weeks									
Description	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Project Planning										
Design and Simulation										
Layout and Verification										
Post Mortem										

References

- A. Jayaraj, N. Nitin Gujarathi, I. Venkatesh and A. Sanyal, "0.6–1.2 V, 0.22 pJ/bit True Random Number Generator Based on SAR ADC," in *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 67, no. 10, pp. 1765-1769, Oct. 2020, doi: 10.1109/TCSII.2019.2949775.
- C. -C. Liu, S. -J. Chang, G. -Y. Huang and Y. -Z. Lin, "A 10-bit 50-MS/s SAR ADC With a Monotonic Capacitor Switching Procedure," in IEEE Journal of Solid-State Circuits, vol. 45, no. 4, pp. 731-740, April 2010, doi: 10.1109/JSSC.2010.2042254.
- https://github.com/IHP-GmbH/IHP-AnalogAcademy.git