Sensing with Random Encoding for Enhanced Security in Embedded Systems

10 MECO
years outgrowing the science

Georgia Tech School of Electrical and Computer Engineering

KEVIN HUTTO^ AND VINCENT MOONEY III^,&
&ASSOCIATE PROFESSOR, ^SCHOOL OF ELECTRICAL AND COMPUTER ENGINEERING
&ADJUNCT ASSOCIATE PROFESSOR, SCHOOL OF COMPUTER SCIENCE
^INSTITUTE FOR INFORMATION SECURITY AND PRIVACY
GEORGIA TECH, ATLANTA, GA 30332-0250
APRIL 23, 2021

Presented at MECO'2021 and CPSIoT'2021, Budva, Montenegro
www.embeddedcomputing.me

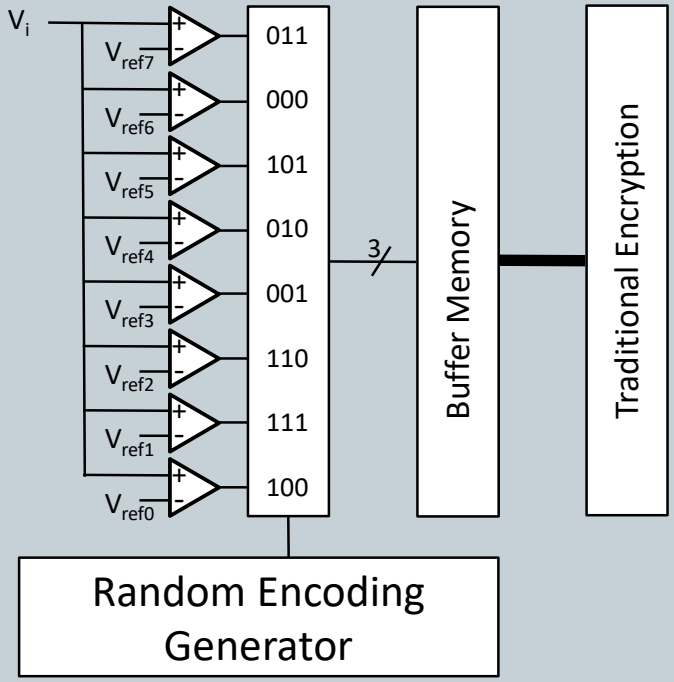
Outline

10 MECO
years outgrowing the science

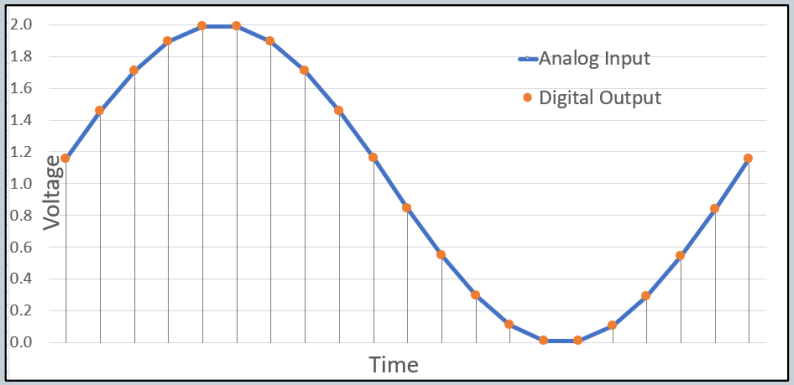
- Problem Definition
- Scenario
- Method of Encoding
- Permutation Generator
- Decoding Circuit
- Attack Resiliency and Security
- Experimental Results
- Conclusions

Problem Definition

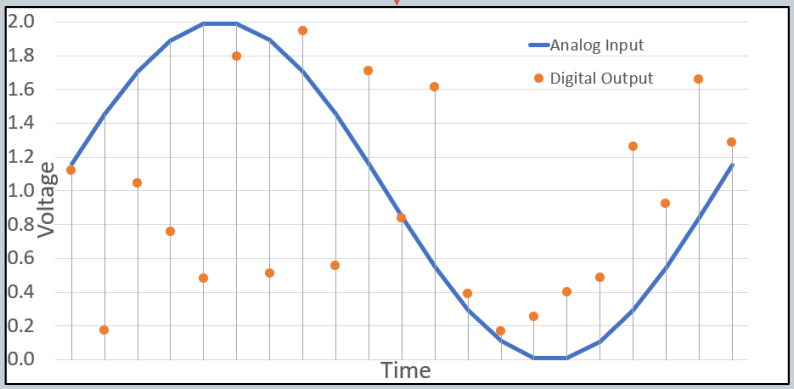
Can a **random encoding generator** be constructed to protect the contents of an ADC plaintext buffer memory from an adversary in possession of the device, memory contents, and digital logic



Random Sensing with RanCode

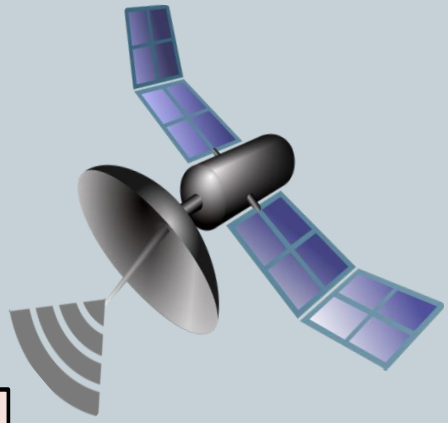


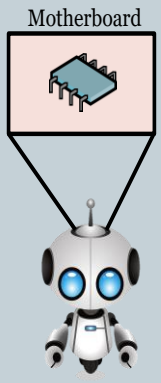
Standard ADC Encoding



Random ADC Encoding

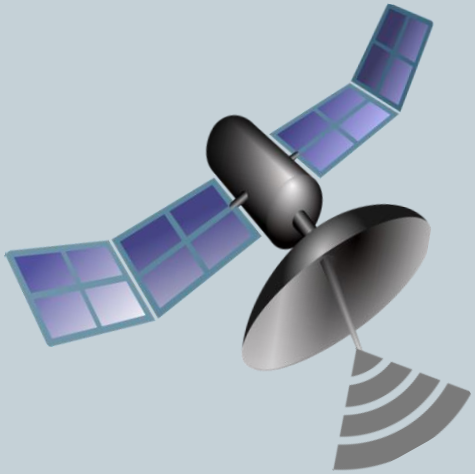
Scenario





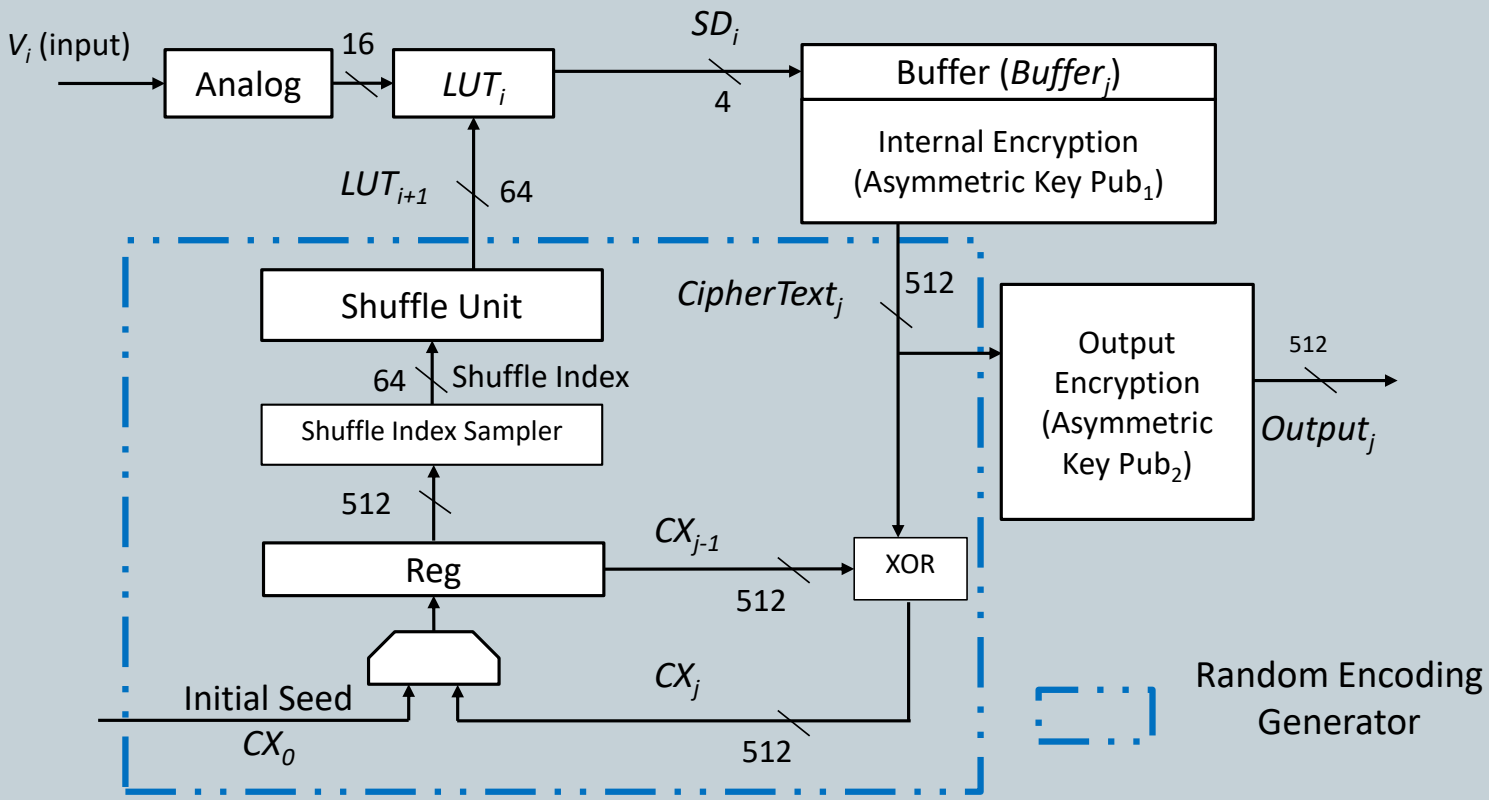
Deployed Sensor

- A satellite is communicating with a device, utilizing a frequency band unknown to an adversary
- The device has a frequency-tunable antenna receiver
- An adversary may be able to reconstruct the original waveform frequency by examining the stored data on the device, especially any such data in plaintext
- The data captured by the antenna is recorded in a manner seemingly unrelated to the received waveform



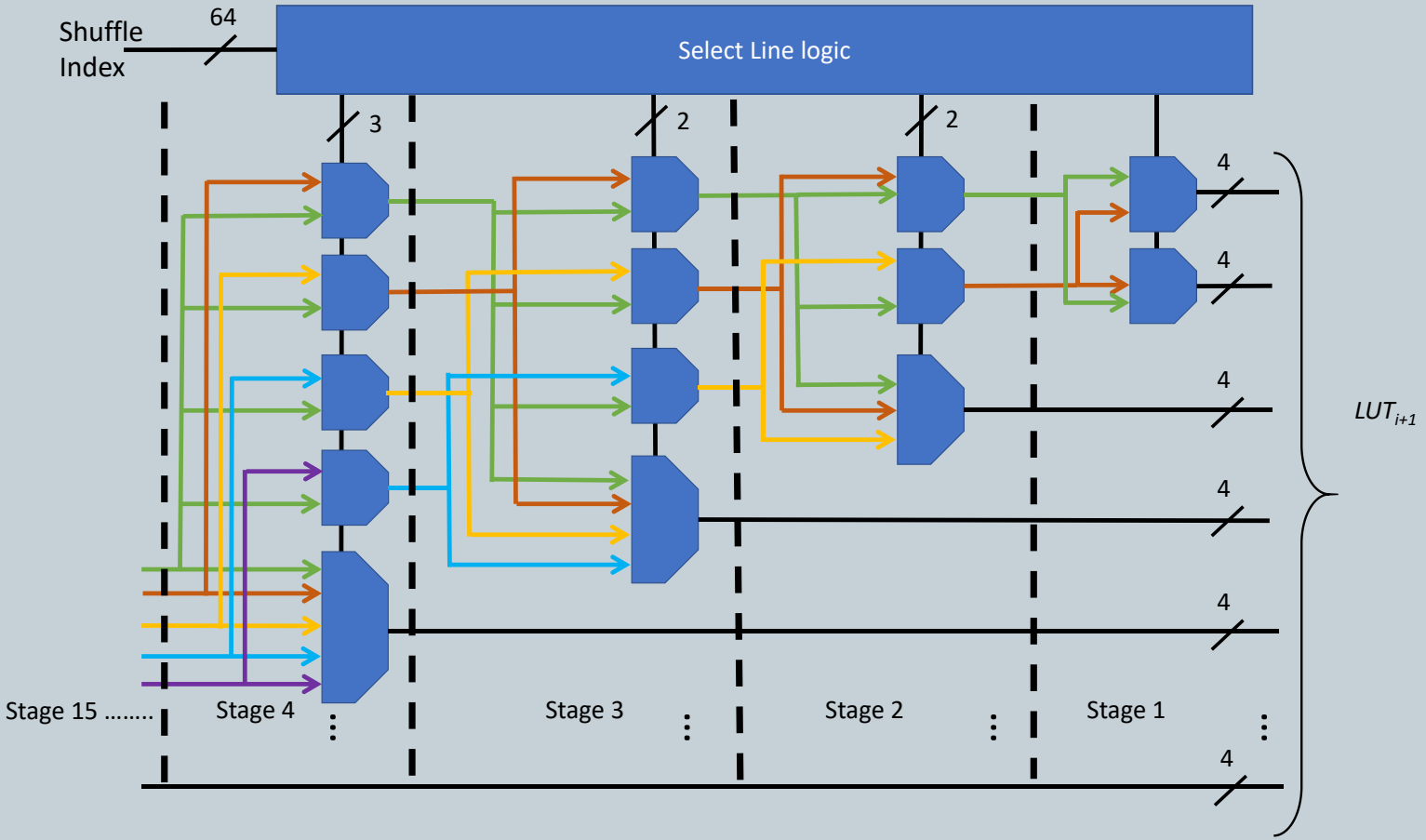
Secure Server

Method of Encoding



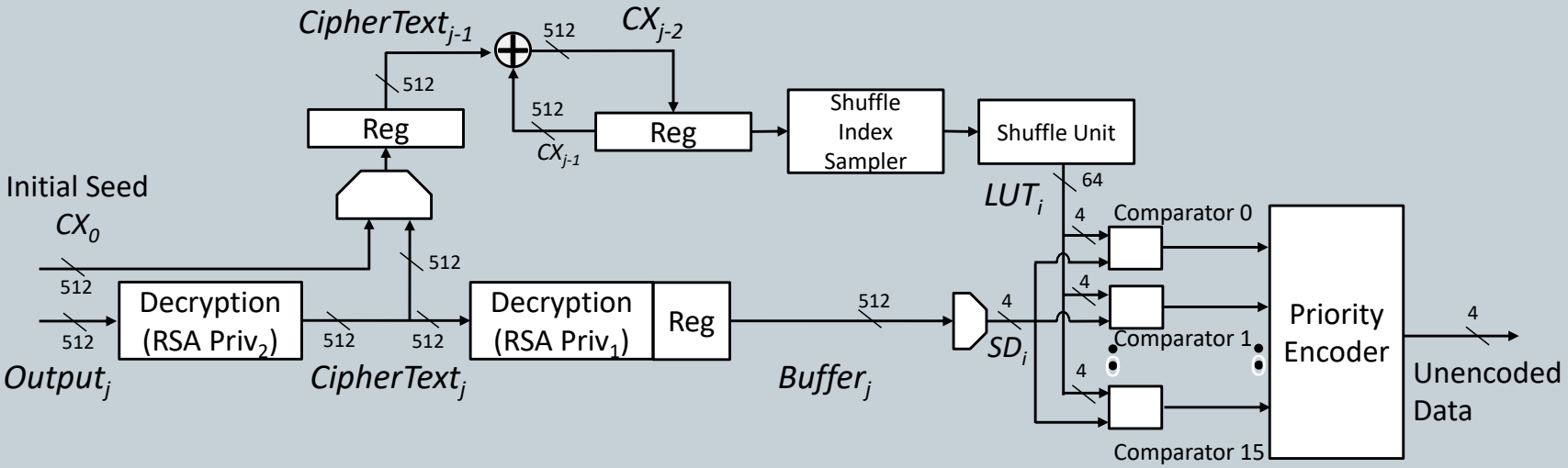
RanCode Circuit

Permutation Generator



Shuffle Unit (Hardware Implementation of Knuth Shuffle Algorithm [4][5])

Decoding Circuit



RanCode Decoder Circuit

- The decoder circuit is implemented on the secure server
- The decoder circuit interprets the sensed data and reassigns the original semantics encoded in the RanCode circuit

Attack Resiliency and Security

- Recall that our attack scenario includes microchip capture and reverse engineering
- Encodings (LUT_0 - LUT_{i-1}) generated before chip capture are not stored on the chip.
- RanCode design enables the transmission of data to a secure server over an insecure channel in real-time.
- A secure server, given the initialization vector CX_0, can utilize physically distinct circuitry to generate all encodings used by RanCode and retrieve all unencoded sampled data.
- Unencoded input values on the device cannot be determined by an adversary who reads the input buffer.

Experimental Results

	Area (Square Microns)	Area (kGE)	Max Clk
4-bit RanCode Circuit with RSA	69302	36.9	25 MHz
4-bit RanCode Circuit without RSA	6002	3.2	>400 MHz
Shuffle Unit 3-bit	1191	0.6	>550 MHz
Shuffle Unit 4-bit	2794	1.5	>400 MHz
Shuffle Unit 5-bit	8912	4.6	>150 MHz

- Written in VHDL
- Simulation results of circuit operation were conducted in ModelSim SE-64 10.6a revision 2017.03
- Synthesis was conducted in Synopsis Design Vision L-2016.03-SP5

References

- [1] D. Bayer and P. Diaconis. “Trailing the Dovetail Shuffle to Its Lair.” The Annals of Applied Probability, vol. 2, no. 2, 1 May 1992, pp. 294–313, projecteuclid.org/download/pdf_1/euclid.aoap/1177005705, 10.1214/aoap/1177005705. Accessed 5 Sept. 2020.
- [2] D. R. E. Gnad, J. Krautter, and M. B. Tahoori. “Leaky Noise: New Side-Channel Attack Vectors in Mixed-Signal IoT Devices.” IACR Transactions on Cryptographic Hardware and Embedded Systems, vol. 2019, no. 3, 9 May 2019, pp. 305–339, 10.46586/tches.v2019.i3.305-339. Accessed 8 Oct. 2020.
- [3] F. K. Jondral. “Software-Defined Radio—Basics and Evolution to Cognitive Radio.” EURASIP Journal on Wireless Communications and Networking, vol. 2005, no. 3, 1 Aug. 2005, 10.1155/wcn.2005.275. Accessed 30 Sept. 2020.
- [4] J. T. Butler and T. Sasao, "Hardware Index to Permutation Converter," 2012 IEEE 26th International Parallel and Distributed Processing Symposium Workshops & PhD Forum, Shanghai, 2012, pp. 431-436, doi: 10.1109/IPDPSW.2012.55.
- [5] D. E. Knuth. Art of Computer Programming, Volume 2: Seminumerical Algorithms, 3rd Edition. Addison-Wesley Professional, 1997, p. 192.
- [6] B. Schneier. Applied Cryptography: Protocols, Algorithms, and Source Code in C. 2nd ed., Indianapolis (Ind.), John Wiley & Sons, 2015, pp. 189-211.
- [7] “Short Burst Data Services - Beam Communications.” Beam Communications, www.beamcommunications.com/services/short-burst-data-sbd. Accessed 10 Feb. 2021.
- [8] O. Jamin. RF Receiver Architecture State of the Art. Springer International Publishing, 2014, pp. 1–38, doi.org/10.1007/978-3-319-01150-91.
- [9] NCSU 45nm FreePDKTM Process Design Kit. Electronic Design Automation, North Carolina State University. Available at: http://www.eda.ncsu.edu/wiki/FreePDK
- [10] “Gateworks Corporation - 16130 Mini-PCIe Adapter.” Iridium Satellite Communications, 22 Nov. 2019, www.iridium.com/products/16130-mini-pcie-adapter/. Accessed 31 Jan. 2021.
- [11] S. McQueen. “Freecores/BasicRSA.” GitHub, 17 July 2014, github.com/freecores/BasicRSA. Accessed 13 Jan. 2021.
- [12] A. Sedra, K. Smith, and A. Chandorkar. Microelectronic Circuits : Theory and Applications. 6th ed., New Delhi, India, Oxford University Press, 2013, pp. 1014–1017.
- [13] “Technical Capabilities | TechInsights.” Www.techinsights.com, www.techinsights.com/technical-capabilities. Accessed 12 Mar. 2021.

THANK YOU

Q&A

Kevin Hutto
khutto30@gatech.edu

Vincent Mooney
mooney@ece.gatech.edu