EEE5716/EEE4714 – Introduction to Hardware Security and Trust – Dr. Mark Tehranipoor

List of Oral Paper Presentations – Spring 2020 – Updated on February 11th, 2020

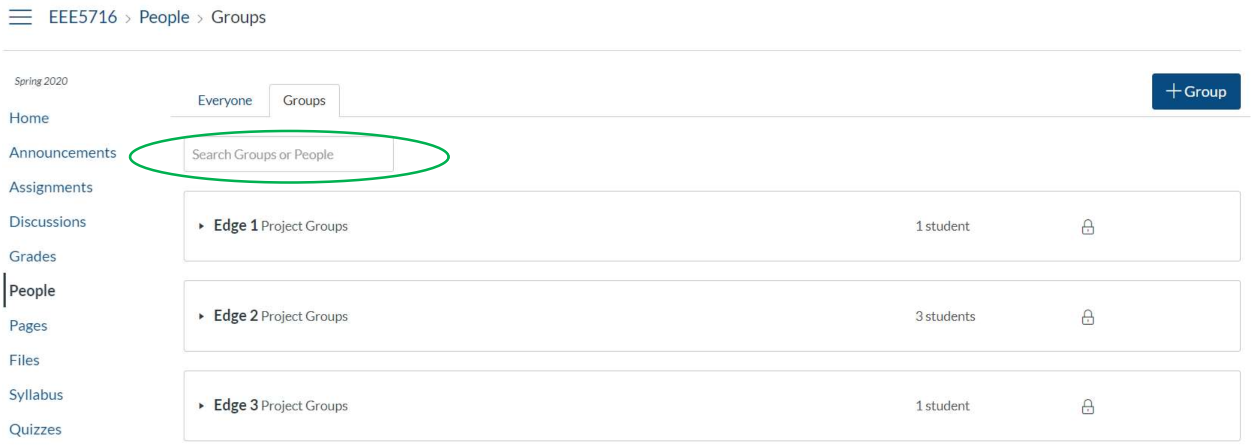
<u>Follow the announcements in Canvas and during lecture for updates.</u>

Contact the TA responsible for the project through Canvas.

Project #	Title:	TA
1	RO PUF	Dhwani
2	Arbiter PUF	Nusrat
3	Trojan Insertion	Nusrat
4	ML Attack PUF	Nitin
5	ML Class Trojan	Dhwani
6	FIFO	Nitin
7	Side-Channel	Jason
8	Modeling Risk	Jason

To find what group you are assigned:

Group Link on Canvas: https://ufl.instructure.com/courses/388274/groups#tab-44994



▸ Edge 1 Project Groups 1 student

▸ Edge 2 Project Groups 3 students

▸ Edge 3 Project Groups 1 student

EEE5716/EEE4714 – Introduction to Hardware Security and Trust – Dr. Mark Tehranipoor

List of Oral Paper Presentations – Spring 2020 – Updated on February 11th, 2020

Week		Thursday
7	**Feb-20**	**1. Group 1 (#1 RO PUF): G4:** Maiti, Abhranil, and Patrick Schaumont. "**Improved ring oscillator PUF: An FPGA-friendly secure primitive**." Journal of cryptology 24, no. 2 (2011): 375-397 **2. Group 5 (#2 Arbiter PUF): G4:** M. Majzoobi, A. Kharaya, F. Koushanfar and S. Devadas , "**Automated design, implementation, and evaluation of arbiter-based PUF on FPGA using programmable delay lines**", 2014. **Midterm Review**
8	**Feb-27**	**1. Group 2 (#1 RO PUF): G3:** A. Maiti, P. Schaumont, "**Improving the quality of a physical unclonable function using configurable ring oscillators**", Proc. IEEE Int. Conf. Field Program. Logic Appl., pp. 703-707, Aug./Sep. 2009. **2. Group 11 (#3 Trojan Insertion): G4**: R. S. Chakraborty, F. Wolff, S. Paul, C. Papachristou, S. Bhunia, "**MERO: a statistical approach for hardware trojan detection**", International Conference on Cryptographic Hardware and Embedded Systems (CHES'09), pp. 396-410, 2009. **3. Group 15 (#2 Arbiter PUF): G4:** J. Maiti et al., "**A systematic method to evaluate and compare the performance of physical unclonable functions**," In Embedded Systems Design with FPGAs, P. Athanas, D. Pnevmatikatos, and N. Sklavos (Eds.).
9	**Mar-5**	**Spring Break (No class)**
10	**Mar-12**	**1. Group 6 (#6 FIFO): UG1:G3:** Lonsing, Florian, et al. "**Unlocking the Power of Formal Hardware Verification with CoSA and Symbolic QED**." 2019 IEEE/ACM International Conference on Computer-Aided Design (ICCAD). IEEE, 2019. **2. Group 3 (#7 Side-Channel): G4 :** Kocher, P., Jaffe, J., Jun, B. et al. "**Introduction to differential power analysis.**" Journal of Cryptographic Engineering (2011) https://doi.org/10.1007/s13389-011-0006-y **3. Group 10 (#6 FIFO): G4:** Ray, Sayak, et al. "**Formal Verification of Security Critical Hardware-Firmware Interactions in Commercial SoCs."** 2019 56th ACM/IEEE Design Automation Conference (DAC). IEEE, 2019.
11	**Mar-19**	**1. Group 4 (#1 RO PUF): G4:** Tauhidur Rahman , Domenic Forte , Jim Fahrny , Mohammad Tehranipoor, **ARO-PUF: an aging-resistant ring oscillator PUF design**, Proceedings of the conference on Design, Automation & Test in Europe, March 24-28, 2014, Dresden, Germany **2. Group 20 (#3 Trojan Insertion): G3:** Shane Kelly, Xuehui Zhang, Mohammed Tehranipoor, and Andrew Ferraiuolo, "**Detecting Hardware Trojans using On-chip Sensors in an ASIC Design.**" Journal of Electronic Testing 31, no. 1 (2015): 11-26. ****SEE NEXT PAGE****

EEE5716/EEE4714 – Introduction to Hardware Security and Trust – Dr. Mark Tehranipoor

List of Oral Paper Presentations – Spring 2020 – Updated on February 11th, 2020

		3. Group 16 (#2 Arbiter PUF): G3: M. Majzoobi, A. Kharaya, F. Koushanfar and S. Devadas , "**Automated design, implementation, and evaluation of arbiter-based PUF on FPGA using programmable delay lines**", 2014.
12	**Mar-26**	**1. Group 13 (#6 FIFO): G4:** Lonsing, Florian, et al. "**Unlocking the Power of Formal Hardware Verification with CoSA and Symbolic QED.**" 2019 IEEE/ACM International Conference on Computer-Aided Design (ICCAD). IEEE, 2019. **2. Group 8 (#5 ML Class Trojan): G4:** Huang, Zhao, Quan Wang, Yin Chen, and Xiaohong Jiang. "**A Survey on Machine Learning Against Hardware Trojan Attacks: Recent Advances and Challenges.**" IEEE Access 8 (2020): 10796-10826.-. **3. Group 9 (#7 Side-Channel): (G3):** Guilley, Sylvain, et al. "**Silicon-level solutions to counteract passive and active attacks.**" Fault Diagnosis and Tolerance in Cryptography, 2008. FDTC'08. 5th Workshop on. IEEE, 2008.
13	**Apr-2**	**1. Group 7 (#1 RO PUF): G3:** A. Maiti, P. Schaumont, "**Improving the quality of a physical unclonable function using configurable ring oscillators**", Proc. IEEE Int. Conf. Field Program. Logic Appl., pp. 703-707, Aug./Sep. 2009. **2. Group 19 (#2 Arbiter PUF): G3:** Machida, T., Yamamoto, D., Iwamoto, M., & Sakiyama, K. (2015). "**A new arbiter PUF for enhancing unpredictability on FPGA**." The Scientific World Journal, 2015. **3. Group 23 (#4 ML Attack PUF): G4:** Rührmair, Ulrich, et al. "**Modeling attacks on physical unclonable functions.**" Proceedings of the 17th ACM conference on Computer and communications security. ACM, 2010.
14	**Apr-9**	**1. Group 12 (#1 RO PUF): G4:** Tauhidur Rahman , Domenic Forte , Jim Fahrny , Mohammad Tehranipoor, **ARO-PUF: an aging-resistant ring oscillator PUF design**, Proceedings of the conference on Design, Automation & Test in Europe, March 24-28, 2014, Dresden, Germany **2. Group 18 (#5 ML Class Trojan): G4:** Kulkarni, Amey, Youngok Pino, and Tinoosh Mohsenin. "**SVM-based real-time hardware Trojan detection for many-core platform.**" In 2016 17th International Symposium on Quality Electronic Design (ISQED), pp. 362-367. IEEE, 2016 **3. Group 17 (#2 Arbiter PUF): UG4:** J. Maiti et al., "**A systematic method to evaluate and compare the performance of physical unclonable functions**," In Embedded Systems Design with FPGAs, P. Athanas, D. Pnevmatikatos, and N. Sklavos (Eds.). Springer, New York, 245267
15	**Apr-16**	**1. Group 14 (#6 FIFO): G4:** Ray, Sayak, et al. "**Formal Verification of Security Critical Hardware-Firmware Interactions in Commercial SoCs.**" 2019 56th ACM/IEEE Design Automation Conference (DAC). IEEE, 2019. ****SEE NEXT PAGE****

		2. Group 21 (#3 Trojan Insertion): G3: Shane Kelly, Xuehui Zhang, Mohammed Tehranipoor, and Andrew Ferraiuolo, "**Detecting Hardware Trojans using On-chip Sensors in an ASIC Design.**" Journal of Electronic Testing 31, no. 1 (2015): 11-26. **3. Group 22 (#3 Trojan Insertion): UG3:G1:** M. Tehranipoor, F. Koushanfar, "**A survey of hardware Trojan taxonomy and detection**", IEEE Des. Test Comput., vol. 27, pp. 10-25, 2010. **EDGE Videos Due**
16	**Apr-23**	**No class** **Final Project Deliverables Due (All students)**

<u>EDGE Students:</u>

ALL EDGE STUDENTS MUST SUBMIT THEIR VIDEO SUBMISSIONS BY: APRIL 16TH

Submit video to YouTube or upload to Canvas (size is limited).

You may make the YouTube video a private link and upload the link to Canvas.

VIDEO SUBMISSIONS BY: APRIL 16TH	
Group 1	**(#8 Modeling Risk):** U. Guin, D. Dimase, and M. Tehranipoor, "**A comprehensive framework for counterfeit defect coverage analysis and detection assessment**." Journal of Electronic Testing: Theory and Applications, vol. 30, no. 1, pp. 25–40, 2014.
Group 2	**(#1 RO PUF):** Tauhidur Rahman , Domenic Forte , Jim Fahrny , Mohammad Tehranipoor, **ARO-PUF: an aging-resistant ring oscillator PUF design**, Proceedings of the conference on Design, Automation & Test in Europe, March 24-28, 2014, Dresden, Germany
Group 3	**(#6 FIFO):** Ray, Sayak, et al. "**Formal Verification of Security Critical Hardware-Firmware Interactions in Commercial SoCs.**" 2019 56th ACM/IEEE Design Automation Conference (DAC). IEEE, 2019.
Group 4	**(#7 Side-Channel):** Kocher, Paul, Joshua Jaffe, and Benjamin Jun. "**Differential power analysis.**" Annual International Cryptology Conference. Springer Berlin Heidelberg, 1999.
Group 5	**(#7 Side-Channel):** Kocher, Paul, Joshua Jaffe, and Benjamin Jun. "**Differential power analysis.**" Annual International Cryptology Conference. Springer Berlin Heidelberg, 1999.