113學年度 晶片安全設計 – 課程大綱與須知.

2025 Feb

PUF security
AN ememory COMPANY

上課資訊 .

- 課程名稱: 晶片安全設計
- 課程目標: 從晶片安全設計及密碼學算法的介紹出發，導入硬體密碼學算法引擎的RTL實作課，能學習到的數位設計流程。
- 上課時間: 週五9:00~12:00
- 課程地點: 資電館104/台達館219 (上機課程)
- 助教時間: 助教群駐場解惑，無強制出席，有需要才來哦!
- 上課內容: 投影片 教材為主。

上課資訊 (cont.) .

- **一人一組，而且需要 coding 的能力才有辦法通過。**
- **嚴禁抄襲任何資源，一旦助教發現一律0分計算!**
- 考評方式: (correctness, style, efficiency)
  1. 期中Lab-1 SHA compressor: 30%
  2. 期中Lab-2 SHA engine: 40%
  3. 期末Lab-3 FPGA : 30%

上課資訊 (cont.) .

- FPGA 開發版
  1. Urbana (real digital) https://www.realdigital.org/hardware/urbana
  2. Basys 3 (digilent) https://digilent.com/reference/programmable-logic/basys-3/start

113學年度 課程大綱 .

Date	w	Content	host	作業	Location
2月21日	1	學期內容介紹。 晶片安全介紹	MY		資電館202
2月28日	2	AES演算法介紹 (線上課程) SHA演算法介紹 (線上課程)			放假
3月7日	3	Linux 指令介紹; RTL 語言設計 (Introduction, RTL & test bench語法) RTL 語言設計 (Combinational Logic: blocking);	CW		台達館219
3月14日	4	RTL 語言設計 (Sequential Logic: non-blocking)	Danny		台達館219
3月21日	5	RTL 語言設計 (FSM: moore, mealy) (架構)	Danny		台達館219
3月28日	6	RTL 語言設計 (Test Bench: input, DUT, output, compare)	CY	Lab1/compressor	台達館219
4月4日	7	PKC演算法介紹 (線上課程)			放假
4月11日	8	RTL 語言設計 (Digital Flow and Synthesis)	CY	Lab2/SHA2 with padding	台達館219
4月18日	9	期中報告 Lab1	助教群		台達館219
4月25日	10	補教周/助教時間(null)	助教群		台達館219
5月2日	11	硬體安全設計與操作	MY		台達館219
5月9日	12	期中報告 Lab2 (SHA2 with padding)	助教群		台達館219
5月16日	13	FPGA 進行設計開發與驗證。	Balance	Lab3/SHA2 FPGA	台達館219
5月23日	14	助教時間	助教群		台達館219
5月30日	15	Entropy Introduction; 抗攻擊設計 (線上課程)			放假
6月6日	16	期末報告 Lab3 (FPGA)	助教群		台達館219

Online Course .

Content	
AES 演算法介紹 (線上課程)	https://youtu.be/3vZGFPihoEA https://youtu.be/cYqnPpFF8fU https://youtu.be/eYLfBk7jp70
Hash 演算法介紹 (線上課程)	https://youtu.be/oQuOlxY8Ykw https://youtu.be/9Xovj3nqII8
PKC 演算法介紹 (線上課程)	https://youtu.be/4bdERnRse38 https://youtu.be/KjewKoEjZPA
Entropy Introduction - Static Entropy/Dynamic Entropy 抗攻擊設計 from IP to SoC (線上課程)	https://youtu.be/XPQ0SzDQtf8 https://youtu.be/II09c9o7S1Y

參考資料 .

書目:

1. Introduction to Hardware Security and Trust (2012, Springer)
2. Hardware Security - A Hands-on Learning Approach (2018, Elsevier)
3. Understanding Cryptography: A Textbook for Students and Practitioners (2010, Springer)

網頁:

Verilog 從放棄到有趣 :: 2018 iT 邦幫忙鐵人賽 (ithome.com.tw)