Date	Lecture	Topic	HW Out	HW Due
Jan 17	1	Introduction to design of secure and reliable computer and communication systems		
Jan 22	2	Fault models and error models		
Jan 24	3	Attack models. Passive and active attacks. Weak and strong fault injection attacks	1	
Jan 29	4	Introduction to finite fields		
Jan 31	5	Extensions of finite fields		
Feb 5	6	Rings of polynomials over finite fields	2	1
Feb 7	7	Linear spaces over finite fields		
Feb 12	8	Hamming codes, extended Hamming codes		
Feb 14	9	BCH codes		
Feb 19	10	Analysis of hardware complexities of encoding and decoding		
Feb 21	11	Design of reliable memories with Hamming codes and BCH codes		
Feb 26	12	Self checking checkers		
Feb 28	13	Midterm review		
Mar 5	14	Midterm exam		
Mar 7	15	Arithmetical AN-codes		
Mar 19	16	Design of reliable arithmetical devices		
Mar 21	17	Reed Solomon codes		
Mar 26	18	Linear feedback shift registers		
Mar 28	19	Reliable and secure computer systems in the presence of passive attacks based on BCH and Reed Solomon codes		
Apr 2	20	Non-linear robust codes with uniformly distributed error detecting capabilities		
Apr 4	21	Encoding and decoding for robust codes		
Apr 9	22	Design of secure memories and secure communications by robust codes		
Apr 11	23	Design of secure cryptographical devises resistant to fault injection attacks by robust codes		
Apr 16	24	Algebraic Manipulation Detection (AMD) codes for detection of strong fault injection attacks		
Apr 23	25	Bounds and constructions for optimal AMD codes		
Apr 25	26	Hardware implementations of encoding and decoding for AMD codes		
Apr 30	27	Applications of AMD codes for design of secure hardware resistant to strong fault injection attacks		
May 2	28	Final exam		