

Module MA-INF 1313	Topics in Theoretical Cryptography				
Workload 270 h	Credit points 9 CP	Duration 1 semester	Frequency every year		
Module coordinator	Prof. Dr. Joachim von zur Gathen				
Lecturer(s)	Prof. Dr. Joachim von zur Gathen, Dr. Michael Nüsken				
Classification	Programme M. Sc. Computer Science		Mode Optional	Semester 3.	
Technical skills	Gain deeper understanding in a special area of cryptography close to current research.				
Soft skills	Oral presentation (in tutorial groups), written presentation (of exercise solutions), team collaboration in solving homework problems, critical assessment.				
Contents	One varying, advanced topic related to current research in theoretical cryptography, e.g. • elliptic curve cryptography, or • quantum cryptography				
Prerequisites	Required: MA-INF 1103 – Cryptography and one further course in cryptography like The Art of Cryptography or eSecurity.				
Format	Teaching format	Group size	h/week	Workload[h]	CP
	Lecture	60	4	60 T / 105 S	5.5
	Exercises	30	2	30 T / 75 S	3.5
	T = face-to-face teaching; S = independent study				
Exam achievements	Written exam (graded)				
Study achievements	Successful exercise participation (not graded)				
Forms of media					
Literature	Research articles				