Day 1 (Monday)

Time	Presenter	Topic	Duration
7.30-9.00	Breakfast		
9.00-10.30 (chair Christof Beierle)	Christina Boura	Differential Meet-In-The-Middle Cryptanalysis (from a Dagstuhl 2022 team)	30 min
	Zahra Ahmadian	Follow-up on Differential Meet-In-The-Middle Cryptanalysis	30 min
	Virginie Lallemand	On Boomerang Attacks on Quadratic Feistel Ciphers	30 min
10.30-10.45	Coffee break		
10.45-12.15 (chair Bart Mennink)	Ritam Bhaumik	New quantum framework for symmetric modes	30 min
	Ashwin Jha	Range-Restricted Vertex Labeling and its Applications	30 min
	Stefano Tessaro	The t-wise independence of SPNs	30 min
12.15-14.00	Lunch (please be in time)		
14.00-15.30 (chair Yu Sasaki)	Patrick Derbez	A general algorithm (and associated tool) for finding efficient key-recovery strategies for differential attacks on SPN ciphers with bit-wise linear-layers	30 min
	Leo Perrin	New attacks against Griffin	30 min
	Willi Meier	Algebraic Attack on FHE-Friendly Cipher HERA Using Multiple Collisions	30 min
15.30-16.00	Cake		
16.00-16.45 (chair María Naya-Plasencia)	Akiko Inoue	On INT-RUP security analysis	15 min
	Tetsu Iwata	Key Control Security of PRF-Based KDFs; Introduction and Preliminary Cryptanalysis Results	30 min
16.45-18.00	Assigning and initializing research groups		
18.00	Dinner (please be in time)		

Day 2 (Tuesday)

Time	Presenter	Topic	Duration
7.30-9.00	Breakfast		
9.00-10.30	Research groups		
10.30-11.00	Coffee break		
11.00-12.15	Research groups		
12.15-14.00	Lunch (please be in time)		
14.00-15.30	Research groups		
15.30-16.00	Cake		
16.00-18.00	Research groups		
18.00	Dinner (please be in time)		

Day 3 (Wednesday)

Time	Presenter	Topic	Duration
7.30-9.00	Breakfast		
9.00-10.30	Research groups		
10.30-11.00	Coffee break		
11.00-12.15	Research groups		
12.15-14.00	Lunch (please be in time)		
14.00-18.00	Social event		
18.00	Dinner (please be in time)		

Day 4 (Thursday)

Time	Presenter	Topic	Duration
7.30-9.00	Breakfast		
9.00-10.20 (chair Christof Beierle)	Mridul Nandi	Six Round Feistel Is Indeed Indifferentiable Secure	50 min
	Bart Mennink	Revisiting the Indifferentiability of the Sum of Permutations (from a Dagstuhl 2022 team)	30 min
10.20-11.15	Coffee break		
11.15-12.15 (chair Mridul Nandi)	Kazuhiko Minematsu	Revisiting Vector-input MACs	30 min
	Christoph Dobraunig	Generalized Initialization of the Duplex Construction	30 min
12.15-14.00	Lunch (please be in time)		
14.00-15.30	Research groups		
15.30-16.00	Cake		
16.00-18.00	Research groups		
18.00	Dinner (please be in time)		

Day 5 (Friday)

Time	Presenter	Topic	Duration
7.30-9.00	Breakfast		
9.00-10.30	Research groups		
10.30-11.00	Coffee break		
11.00-12.15	Wrap-up status report of research groups		
12.15-14.00	Lunch (please be in time)		
14.00	Go home!		