YRCS 31st May 2021

There will be a flash talk session, where participants are encouraged to announce their current or recent work in the medium of a ∼2-minute presentation (with or without a slide).

09:15-	**Call goes live / Breakfast**	
09:40-09:45	**Welcome and introduction**	
09:45-10:15	Russell W. F. Lai	Subtractive Sets over Cyclotomic Rings: Limits of Schnorr-like Arguments over Lattices
10:15-10:45	David Niehues	Verifiable Random Functions with Optimal Tightness
10:45-10:55	**Break**	
10:55-11:25	Rune Fiedler	BUFFing signature schemes beyond unforgeability and the case of post-quantum signatures
11:25-11:55	Saqib A. Kakvi	Security of Standardised RSA Signatures
11:55-12:20		Flash Talks
12:20-13:05	**Lunch**	
13:05-13:35	Christoph Egger	Key-Schedule Security for the TLS 1.3 Standard
13:35-13:50	Lin Lyu	Anonymity under selective-opening attack
13:50-14:00	**Break**	
14:00-14:25	Jan P. Drees	Detection of padding side channels with machine learning
14:25-14:40	Christian Janson	Robust Channels: Handling Unreliable Networks in the Record Layers of QUIC and DTLS 1.3
14:40-15:10	Pascal Bemmann	Subversion-Resilient Public Key Encryption with Practical Watchdogs
15:10-15:20	**Break**	
15:20-15:50	Valerio Cini and Erkan Tairi	Updatable Signatures and Message Authentication Codes
15:50-16:20	Denis Diemert	More Efficient Digital Signatures with Tight Multi-User Security
16:20	**Wrap up**	

Details for the Zoom meeting have been sent via the mailing list, so if you need these sent again please get in touch via email: `davies@uni-wuppertal.de`.

Web page https://yrcs.de/

Mailing list https://www.listserv.dfn.de/sympa/info/yrcs