Dagstuhl Seminar **Public Key Cryptography**

Mon, Sep 26	Tue, Sep 27	Wed, Sep 28	Thu, Sep 29	Fri, Sep 30
09:00 Welcome			09:00 DBLP session	
09:15 Kenny Paterson *On the Joint Security of Signature and Encryption, Revisited*	09:15 Guiseppe Persiano *HVE with Unrestricted Queries*	09:15 Yvo Desmedt *Active Security in General Secure Multi-Party Computation via Black-Box Groups*	09:15 Antoine Joux *Cover and Decomposition on Elliptic Curves*	09:15 Pooya Farshim *Functional Encryption: Extensions and Implications*
09:50 Krzysztof Pietrzak *Commitments and Efficient Zero-Knowledge from Hard Learning Problems*	09:50 Yuval Ishai *How to Garble Arithmetic Circuits*	09:50 Stefano Tessaro *The Equivalence of the Random Oracle and the Ideal Cipher Model, Revisited*	09:50 Melissa Chase *Functional Reencryption and Collusion-Resistant Obfuscation*	09:50 Claus Schnorr *Identification and signatures based on NP-hard problems of indefinite quadratic forms*
10:30 BREAK	10:30 BREAK	10:30 BREAK	10:30 BREAK	10:30 BREAK
11:00 Thomas Holenstein *Lower Bounds for the Construction of PRGs*	11:00 Ueli Maurer *Constructive Cryptography -- A New Paradigm for Security Definitions and Proofs*	11:00 Anja Becker *Solving Hard Knapsacks*	11:00 Dominique Schröder *Security of Blind Signatures, Revisited*	11:00 Bogdan Warinschi *Game-based composition theorems for key exchange protocols*
11:35 Jörn Müller-Quade *Code obfuscation with a stateless hardware token*	11:35 Björn Tackmann *Integrity Notions for Encryption Schemes*	11:35 Vassilis Zikas *Secure Computation with Corrupted Setups*	11:35 Gregory Neven *Oblivious transfer with anonymous access control and pricing*	11:35 Yevgeniy Dodis *On the (In)security of RSA Signatures*
12:15 LUNCH	12:15 LUNCH	12:15 LUNCH	12:15 LUNCH	12:15 LUNCH
14:15 Eike Kiltz *LWE is lossy*	14:15 Dennis Hofheinz *All-But-Many Lossy Trapdoor Functions*	FREE AFTERNOON	14:15 Juan Garay *Resource-based Corruptions*	
14:50 Alon Rosen *Pseudo Random Functions and Lattices*	14:50 Tatsuaki Okomoto *Dual Pairing Vector Spaces and Functional Encryption*		14:50 Thomas Ristenpart *Careful with Composition: Limitations of Indifferentiability Framework*	
15:30 BREAK	15:30 BREAK		15:30 BREAK	
16:15 Alexander Meurer *Decoding Random Linear Codes*	16:15 Yevgeniy Dodis *Leftover Hash Lemma, revisited*		16:15 Panel Discussion: *Future Directions for Public Key Crypto*	