Dr Mark Manulis

Academic CV (short)

since 02/2012	University of Surrey, United Kingdom *Head of Department of Computer Science (since 09/2020)* *Deputy Director of Surrey Centre for Cyber Security (since 07/2014)* *Reader (Associate Professor, since 09/2020)* *Senior Lecturer (Associate Professor, until 08/2020)*
2009 – 2012	Technische Universität Darmstadt, Germany *Assistant professor (W1 / Juniorprofessor)*
2007 – 2009	Université catholique de Louvain, Belgium *Postdoc*, UCL Crypto Group
June 2007	PhD defence with *summa cum laude* at Ruhr-Universität Bochum

Selected publications (see full list at https://scholar.google.com/citations?user=MdmQAVkAAAAJ)

- M. Manulis, C. P. Bridges, R. Harrison, V. Sekar, A. Davis: “Cyber Security in New Space”. International Journal of Information Security. Open Access. May 2020, Springer.
- N. Frymann, D. Gardham, F. Kiefer, E. Lundberg, M. Manulis, D. Nilsson: “Asynchronous Remote Key Generation: An Analysis of Yubico’s Proposal for W3C WebAuthn”. ACM SIGSAC Conference on Computer and Communications Security (ACM CCS 2020), pp.
- D. Gardham, M. Manulis: “Hierarchical Attribute-based Signatures: Short Keys and Optimal Signature Length”. 17th International Conference on Applied Cryptography and Network Security (ACNS 2019), LNCS 11464, pp. 89-109, Springer, 2019
- M. Manulis, D. Stebila, F. Kiefer, N. Denham: “Secure Modular Password Authentication for the Web using Channel Bindings”. International Journal of Information Security, 15(6):597-620, Springer, 2016
- F. Kiefer, M. Manulis: “Blind Password Registration for Two-Server Password Authenticated Key Exchange and Secret Sharing Protocols”. 19th Information Security Conference (ISC 2016), LNCS 9866, pp. 95-114, Springer, 2016
- F. Kiefer, M. Manulis: “Zero-Knowledge Password Policy Checks and Verifier-Based PAKE”. 19th European Symposium on Research in Computer Security (ESORICS 2014), LNCS 8713, pp. 295-312, Springer, 2014
- E. De Cristofaro, M. Manulis, B. Poettering: “Private Discovery of Common Social Contacts”. International Journal of Information Security (IJIS), 12(1):49-65, 2013, Springer.
- M. C. Gorantla, C. Boyd, J.M. González Nieto, M. Manulis: “Modeling Key Compromise Impersonation Attacks on Group Key Exchange Protocols”. ACM Transactions on Information and Systems Security (TISSEC), 14(4), Art. 28, 2011, ACM.

Mark Manulis