GARETH T. DAVIES

Curriculum Vitae gareth.davies89@gmail.com

EMPLOYMENT

Postdoc University of Wuppertal Nov 2019-Nov 2021
PI: Tibor Jager University of Paderborn Nov 2018-Oct 2019
'Theoretically-Sound Real-World Cryptography' project.

Postdoc NTNU Trondheim Apr 2016-Nov 2018
PI: Colin Boyd & Kristian Gjøsteen
'Cryptographic Tools for Cloud Security' project; focus on outsourced storage security.

Research Assistant University of Bristol Apr 2015-Mar 2016
PI: Nigel Smart
Unlinkability, secure deduplication and encryption in enterprise-level cloud storage systems.

PhD Candidate University of Bristol Oct 2011-Mar 2015
Non-standard definitions and constructions in provable security.

EDUCATION

PhD in Computer Science University of Bristol Awarded Jan 2016
Thesis: Encryption in the Presence of Key-Dependent Messages and Related-Key Attacks
Advisors: Martijn Stam and Bogdan Warinschi [Thesis]

MMath in Mathematics University of Nottingham July 2011
Thesis: The Use of Elliptic Curves for Cryptography
Advisor: Christian Wuthrich

EXPERIENCE

University of Wuppertal Winter 2019, Summer 2020
Teaching contribution to *Theoretical Foundations of Applied Cryptography*, *Provable Security* and *Communication Security for Modern Applications*.

University of Paderborn Summer 2019
(Joint) module co-ordinator for *Modern Public-Key Cryptography* and *Current Topics in IT-Security*, both Masters-level seminars. Guest lecturer for *Intro To Cryptography*.

NTNU Trondheim Spring 2017, Spring 2018
Guest Lecturer for *Information Security*; Censor for *Wireless Security*.

University of Bristol October 2011-January 2015
Teaching Assistant: *Cryptography A* (2012-15) and *Number Theory and Group Theory* (2013-14).

PUBLICATIONS

[9] Client obliviousness in oblivious parallel RAM
ICICS 2020
G. T. Davies, C. Janson, D. P. Martin
ePrint 2020/858

[8] Fast and secure updatable encryption
CRYPTO 2020
C. Boyd, G. T. Davies, K. Gjøsteen, Y. Jiang
ePrint 2019/1457

[7] Cloud-assisted asynchronous key transport with post-quantum security
ACISP 2020
G. T. Davies, H. Galteland, K. Gjøsteen, Y. Jiang
ePrint 2019/1409

[6] Security notions for cloud storage and deduplication
Best Paper, ProvSec 2018
C. Boyd, G. T. Davies, K. Gjøsteen, M. Toorani, H. Raddum
ePrint 2017/1208

[5] Offline assisted group key exchange
ISC 2018
C. Boyd, G. T. Davies, K. Gjøsteen, Y. Jiang
ePrint 2018/114

[4] Definitions for plaintext-existence hiding in cloud storage
SECPID 2018
C. Boyd, G. T. Davies, K. Gjøsteen, M. Toorani, H. Raddum
ePrint 2018/748

[3] Side channels in deduplication: trade-offs between leakage and efficiency
AsiaCCS 2017
F. Armknecht, C. Boyd, G. T. Davies, K. Gjøsteen, M. Toorani
ePrint 2016/977

[2] RKA-KDM secure encryption from public-key encryption
PKC 2014
F. Böhl, G. T. Davies, D. Hofheinz
ePrint 2013/653

[1] KDM security in the hybrid framework
CT-RSA 2014
G. T. Davies, M. Stam
ePrint 2013/567

Preprints

[10] Zero-Knowledge proof of decryption for FHE ciphertexts
C. Carr, A. Costache, G. T. Davies, K. Gjøsteen and M. Strand
ePrint 2018/026

AWARDED FUNDING

Principal Investigator for 'Key Exchange for Today's Internet', Forskningsrådet/DAAD
8,090eur (8,954usd), 2020-2021.

Recipient of independent award for research travel funding, Univ. Bristol Alumni Foundation
500gbp (831usd), 2014.

PROFESSIONAL ACTIVITIES

Lead organizer of the Secure Cloud Storage and Services workshop, Oslo, September 2017.

Program Committees: iPAT 2018, SAC 2019
Other Committees: CCS 2019 Poster Session
Reviewer: ACM CCS, EUROCRYPT, CRYPTO, ASIACRYPT, ACNS, PETS, PKC, TCC, Passwords & others.

MISCELLANEOUS

Languages: English (native), Norwegian (conversational, CEFR B1/B2), German (basic, A2)

University of Nottingham Mathematics Prize Winner 2010 for highest average grade over 3 years of all students on MMath programme.

SUPERVISED MASTERS PROJECT TITLES

ACCE for Pre-Shared Keys	2020
Oblivious RAM in Practice	2019
Secure Sharing in the Cloud	2019
Exploring Libraries for Homomorphic Encryption	2018
Secure Data Sharing in the Cloud	2018
Simulating Secure Cloud Storage Schemes	2017
Cryptographic Access Control for Big Data Platforms	2017

ACADEMIC VISITS

Christian Janson & Marc Fischlin | *TU Darmstadt*	August 2019
Colin Boyd | *NTNU Trondheim*	April 2019
Douglas Stebila | *University of Waterloo*	October 2018
Marc Fischlin | *TU Darmstadt*	June-July 2018
N. Asokan | *Aalto University*	August 2016
Krzysztof Pietrzak & Georg Fuchsbauer | *IST Austria*	October 2014
Dennis Hofheinz | *Karlsruher Institut für Technologie*	August 2013

REFEREES

Tibor Jager, University of Wuppertal	`tibor.jager@uni-wuppertal.de`
Colin Boyd, NTNU Trondheim	`colin.boyd@ntnu.no`
Martijn Stam, Simula (formerly Univ. Bristol)	`martijn@simula.no`