GARETH T. DAVIES

Curriculum Vitae gareth.davies89@gmail.com

EMPLOYMENT

Postdoc University of Paderborn Nov 2018-present
PI: Tibor Jager
Project 'Foundations of Real-World Cryptography.'

Postdoc NTNU Trondheim Apr 2016-Nov 2018
PI: Colin Boyd & Kristian Gjøsteen
Project 'Cryptographic Tools for Cloud Security' with particular focus on deduplication.

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

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]
Focus: Non-standard definitions and constructions in provable security.

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

PUBLICATIONS

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

[5] Offline assisted group key exchange ISC 2018
C. Boyd, G. T. Davies, K. Gjøsteen and 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 and 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 and M. Toorani ePrint 2016/977

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

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

Preprints

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

EXPERIENCE

University of Paderborn — Summer 2019
(Joint) module co-ordinator for Modern Public-Key Cryptography, a Masters-level seminar.

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); Number Theory and Group Theory (2013-14).

SUPERVISED MASTERS STUDENT PROJECTS

Oblivious RAM in Practice — Spring 2019
Olav Sortland Thoresen

Secure Sharing in the Cloud — Spring 2019
Eivind Nordal Gran

Exploring libraries for homomorphic encryption — Spring 2018
Ashmitha Lokanath

Secure data sharing in the cloud — Spring 2018
Rafael Lonsky

Simulating secure cloud storage schemes — Spring 2017
Jorge Campos

Cryptographic access control for big data platforms — Spring 2017
Christoffer Viken

AWARDS AND ACTIVITIES

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

Program Committees: iPAT 2018, SAC 2019
Reviewer: EUROCRYPT, ASIACRYPT, ACNS, PETS, PKC, AsiaCCS, Passwords & others.

Successful independent application for research travel funding, Univ. Bristol Alumni, 2014.

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

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

ACADEMIC VISITS

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

REFEREES

Tibor Jager, University of Paderborn	tibor.jager@upb.de
Colin Boyd, NTNU Trondheim	colin.boyd@ntnu.no
Martijn Stam, University of Bristol	martijn.stam@bristol.ac.uk