

# GARETH T. DAVIES

<https://gareth-t-davies.github.io/>

gareth.davies89@gmail.com

## Curriculum Vitae

### EMPLOYMENT

---

<b>Postdoc</b>	University of Wuppertal	Nov 2019–present
PI: Tibor Jager	University of Paderborn	Nov 2018–Oct 2019
'Theoretically-Sound Real-World Cryptography' project.		
<b>Postdoc</b>	NTNU Trondheim	Apr 2016–Nov 2018
PI: Colin Boyd & Kristian Gjøsteen		
'Cryptographic Tools for Cloud Security' project; focus on outsourced storage security.		
<b>Research Assistant (Postdoc)</b>	University of Bristol	Apr 2015–Mar 2016
PI: Nigel Smart		
Unlinkability, secure deduplication and encryption in enterprise-level cloud storage systems.		
<b>PhD Candidate</b>	University of Bristol	Oct 2011–Mar 2015
Non-standard definitions and constructions in provable security.		

### QUALIFICATIONS

---

<b>PhD in Computer Science</b>	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		[ <a href="#">Thesis</a> ]
<b>MMath in Mathematics</b>	University of Nottingham	July 2011
Thesis: The Use of Elliptic Curves for Cryptography		
Advisor: Christian Wuthrich		

### TEACHING EXPERIENCE

---

University of Wuppertal	Winter 2019–present
Teaching contribution to <i>Theoretical Foundations of Applied Cryptography</i> , <i>Provable Security</i> and <i>Communication Security for Modern Applications</i> .	
University of Paderborn	Summer 2019
(Joint) module co-ordinator for <i>Modern Public-Key Cryptography</i> and <i>Current Topics in IT-Security</i> , both Masters-level seminars. Guest lecturer for <i>Intro To Cryptography</i> .	
NTNU Trondheim	Spring 2017, Spring 2018
Guest Lecturer for <i>Information Security</i> ; Censor for <i>Wireless Security</i> .	
University of Bristol	October 2011–January 2015
Teaching Assistant for <i>Cryptography A</i> (2012–15) and <i>Number Theory and Group Theory</i> (2013–14).	

## AWARDED FUNDING

---

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

Recipient of independent award for research travel funding (STSM)  
1,250eur (1,398usd), E-COST IC1306, 2016.

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

Co-author of proposal 'Foundations of Secure Storage for Encrypted Instant Messaging' joint with Tibor Jager. For administration reasons, partly funded with Jager as sole PI (PhD student's supervisor)  
318,840eur (376,070usd), Deutsche Forschungsgemeinschaft, 2021-2024.

## PROFESSIONAL ACTIVITIES

---

Lead organizer of the [Secure Cloud Storage and Services workshop](#), Oslo, September 2017.

Lead organizer of the 3rd [Young Research Cryptography Seminar](#), Wuppertal, May 2021.

Program Committees: SAC 2019, CT-RSA 2022, iPAT {2018,2020,2021}

Other Committees: ACM CCS 2019 Poster Session

Reviewer: ACM CCS, IEEE S & P, EUROCRYPT, CRYPTO, ASIACRYPT, PETS, PKC, TCC and 15+ others

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

## 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.

## PUBLICATIONS

---

- [10] Symmetric key exchange with full forward security and robust synchronization ASIACRYPT 2021  
C. Boyd, G. T. Davies, B. de Kock, K. Gellert, T. Jager, L. Millerjord [ePrint 2021/702](#)
- [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

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

## REFEREES

---

Tibor Jager | *University of Wuppertal*

[tibor.jager@uni-wuppertal.de](mailto:tibor.jager@uni-wuppertal.de)

Colin Boyd | *NTNU Trondheim*

[colin.boyd@ntnu.no](mailto:colin.boyd@ntnu.no)

Martijn Stam | *Simula (formerly Univ. Bristol)*

[martijn@simula.no](mailto:martijn@simula.no)