Christian Rechberger - DTU Orbit (23/12/2017)

Rechberger, Christian
crec@dtu.dk

Department of Applied Mathematics and Computer Science - Associate Professor

Cyber Security

Publications:

Design and analysis of cryptographic algorithms
Publication: Research › Ph.D. thesis – Annual report year: 2017

Secure Block Ciphers - Cryptanalysis and Design
Publication: Research › Ph.D. thesis – Annual report year: 2017

Design and Analysis of Symmetric Primitives
Publication: Research › Ph.D. thesis – Annual report year: 2016

MiMC: Efficient encryption and cryptographic hashing with minimal multiplicative complexity
Publication: Research - peer-review › Article in proceedings – Annual report year: 2016

Practical Low Data-Complexity Subspace-Trail Cryptanalysis of Round-Reduced PRINCE
Publication: Research - peer-review › Article in proceedings – Annual report year: 2016

Analyzing Permutations for AES-like Ciphers: Understanding ShiftRows
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015

Ciphers for MPC and FHE
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015

Linear Distinguishers in the Key-less Setting: Application to PRESENT
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015

Practical Attacks on AES-like Cryptographic Hash Functions
State-Recovery Analysis of Spritz

The Rebound Attack and Subspace Distinguishers: Application to Whirlpool


Rotational Rebound Attacks on Reduced Skein

The LOCAL attack: Cryptanalysis of the authenticated encryption scheme ALE

Improved cryptanalysis of the block cipher KASUMI

Bicliques for Preimages: Attacks on Skein-512 and the SHA-2 Family

Narrow-Bicliques: Cryptanalysis of Full IDEA

On security arguments of the second round SHA-3 candidates

PRINCE - A Low-Latency Block Cipher for Pervasive Computing Applications: Extended Abstract

A 3-Subset Meet-in-the-Middle Attack: Cryptanalysis of the Lightweight Block Cipher KTANTAN
Bogdanov, A. & Rechberger, C. 2011 In : Lecture Notes in Computer Science. 6544, p. 229-240
Biclique cryptanalysis of the full AES
Bogdanov, A., Khovratovich, D. & Rechberger, C. 2011 In : Lecture Notes in Computer Science. 7073, p. 344-371
Publication: Research - peer-review › Conference article – Annual report year: 2011

Improved Meet-in-the-Middle Cryptanalysis of KTANTAN
Publication: Research - peer-review › Conference article – Annual report year: 2011

Advanced meet-in-the-middle preimage attacks: First results on full tiger, and improved results on MD4 and SHA-2
Guo, J., Ling, S., Wang, H. & Rechberger, C. 2010 In : Lecture Notes in Computer Science. 6477, p. 56-75
Publication: Research - peer-review › Conference article – Annual report year: 2010

Cryptanalysis of the 10-Round Hash and Full Compression Function of SHA3-3-512
Publication: Research - peer-review › Conference article – Annual report year: 2010

Rebound Attacks on the Reduced Grøstl Hash Function
Publication: Research - peer-review › Conference article – Annual report year: 2010

Rotational Rebound Attacks on Reduced Skein
Publication: Research - peer-review › Article in proceedings – Annual report year: 2010

Second-Preimage Analysis of Reduced SHA-1
Rechberger, C. 2010 In : Lecture Notes in Computer Science. 6168, p. 104-116
Publication: Research - peer-review › Conference article – Annual report year: 2010

Cryptanalysis of Vortex
Publication: Research - peer-review › Article in proceedings – Annual report year: 2009

Grøstl Addendum
Publication: Research › Other contribution – Annual report year: 2009

Projects:

Trusted Cryptography
Kölbl, S., Rechberger, C., Knudsen, L. R., Mödersheim, S. A., Johansson, T. & Rijmen, V. 01/12/2013 → 12/12/2016
Project: PhD

Trusted Cryptography
Project: PhD
Design and Analysis of Symmetric Primitives
01/09/2012 → 19/11/2015
Project: PhD

Block Cipher Cryptanalysis
Alkhzaimi, H. A., Knudsen, L. R., Rechberger, C., Johansson, T. & Preneel, B. K. B.
15/11/2010 → 04/03/2015
Project: PhD

Cryptanalysis of Some Lightweight Symmetric Ciphers
01/01/2010 → 22/03/2013
Project: PhD

Activities:

New Directions in Cryptography
Rechberger, C. (Panel member)
7 Dec 2012
Activity: Talks and presentations › Conference presentations

New meet-in-the-middle attacks in symmetric cryptanalysis
Rechberger, C. (Keynote speaker)
30 Nov 2012
Activity: Talks and presentations › Conference presentations

PRINCE - A Low-latency Block Cipher for Pervasive Computing Applications
Rechberger, C. (Invited speaker)
21 Nov 2012
Activity: Talks and presentations › Conference presentations

Related-key and Biclique cryptanalysis of AES
Rechberger, C. (Invited speaker)
18 Oct 2012
Activity: Talks and presentations › Conference presentations

Yet another cryptanalysis of the AES
Rechberger, C. (Invited speaker)
27 Sep 2012
Activity: Talks and presentations › Conference presentations

The SHA-3 Competition
Rechberger, C. (Keynote speaker)
21 Sep 2012
Activity: Talks and presentations › Conference presentations

Cryptanalytic ideas for SHA and AES
Rechberger, C. (Keynote speaker)
11 Aug 2012
Activity: Talks and presentations › Conference presentations

Narrow-Bicliques: Cryptanalysis of Full IDEA
Rechberger, C. (Speaker)
17 Apr 2012