

# **2018 IEEE 31st Computer Security Foundations Symposium (CSF 2018)**

**Oxford, United Kingdom  
9 – 12 July 2018**



**IEEE Catalog Number: CFP18037-POD  
ISBN: 978-1-5386-6681-4**

**Copyright © 2018 by the Institute of Electrical and Electronics Engineers, Inc.  
All Rights Reserved**

*Copyright and Reprint Permissions:* Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

***\*\*\* This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP18037-POD
ISBN (Print-On-Demand):	978-1-5386-6681-4
ISBN (Online):	978-1-5386-6680-7
ISSN:	1940-1434

**Additional Copies of This Publication Are Available From:**

Curran Associates, Inc  
57 Morehouse Lane  
Red Hook, NY 12571 USA  
Phone: (845) 758-0400  
Fax: (845) 758-2633  
E-mail: [curran@proceedings.com](mailto:curran@proceedings.com)  
Web: [www.proceedings.com](http://www.proceedings.com)

CURRAN ASSOCIATES INC.  
**proceedings**  
.com

# 2018 IEEE 31st Computer Security Foundations Symposium **CSF 2018**

## Table of Contents

Message from the General Chair .ix.....  
Committees .xi.....  
Reviewers .xiii.....

### Session: Security Protocols 1

An Extensive Formal Analysis of Multi-factor Authentication Protocols .1.....  
*Charlie Jacomme (LSV & CNRS & ENS Paris-Saclay & Inria & Université Paris-Saclay) and Steve Kremer (LORIA, Inria Nancy-Grand Est & CNRS & Université de Lorraine)*

Composition Theorems for CryptoVerif and Application to TLS 1.3 .16.....  
*Bruno Blanchet (Inria)*

A Cryptographic Look at Multi-party Channels .31.....  
*Patrick Eugster (University of Lugano), Giorgia Azzurra Marson (Nec Laboratories Europe), and Bertram Poettering (Royal Holloway, University of London)*

Invited Paper: Secure Boot and Remote Attestation in the Sanctum Processor .46.....  
*Ilija Lebedev (Massachusetts Institute of Technology), Kyle Hogan (Massachusetts Institute of Technology), and Srinivas Devadas (Massachusetts Institute of Technology)*

Guided Design of Attack Trees: A System-Based Approach .61.....  
*Maxime Audinot (Univ Rennes, CNRS, IRISA), Sophie Pinchinat (Univ Rennes, CNRS, IRISA), and Barbara Kordy (Univ Rennes, INSA Rennes, CNRS, IRISA)*

### Session: Cryptographic Primitives

Self-Guarding Cryptographic Protocols against Algorithm Substitution Attacks .76.....  
*Marc Fischlin (Technische Universität Darmstadt) and Sogol Mazaheri (Technische Universität Darmstadt)*

Formal Security Proof of CMAC and Its Variants .91.....  
*Cécile Baritel-Ruet (UCA (Université Côte d'Azur), INRIA Sophia-Antipolis), François Dupressoir (University of Surrey), Pierre-Alain Fouque (Université de Rennes I, Rennes, France), and Benjamin Gregoire (INRIA)*

Backdoored Hash Functions: Immunizing HMAC and HKDF .105.....	
	<i>Marc Fischlin (Technische Universität Darmstadt), Christian Janson (Technische Universität Darmstadt), and Sogol Mazaheri (Technische Universität Darmstadt)</i>

## Session: Secure Computation

Computer-Aided Proofs for Multiparty Computation with Active Security .119.....	
	<i>Helene Haagh (Aarhus University), Aleksandr Karbyshev (Aarhus University), Sabine Oechsner (Aarhus University), Bas Spitters (Aarhus University), and Pierre-Yves Strub (Ecole Polytechnique)</i>
Enforcing Ideal-World Leakage Bounds in Real-World Secret Sharing MPC Frameworks .132.....	
	<i>José Bacelar Almeida (INESC TEC and Universidade do Minho, Portugal), Manuel Barbosa (INESC TEC and FCUP Universidade do Porto, Portugal), Gilles Barthe (IMDEA Software Institute, Spain), Hugo Pacheco (INESC TEC and Universidade do Minho, Portugal), Vitor Pereira (INESC TEC and FCUP Universidade do Porto, Portugal), and Bernardo Portela (INESC TEC and FCUP Universidade do Porto, Portugal)</i>
Symbolic Security of Garbled Circuits .147.....	
	<i>Baiyu Li (UC San Diego) and Daniele Micciancio (UC San Diego)</i>

## Session: Knowledge and Hyperproperties

The Complexity of Monitoring Hyperproperties .162.....	
	<i>Borzoo Bonakdarpour (Iowa State University) and Bernd Finkbeiner (Saarland University)</i>
Knowledge-Based Security of Dynamic Secrets for Reactive Programs .175.....	
	<i>McKenna McCall (Carnegie Mellon University), Hengruo Zhang (Carnegie Mellon University), and Limin Jia (Carnegie Mellon University)</i>
Assuming You Know: Epistemic Semantics of Relational Annotations for Expressive Flow Policies .189.....	
	<i>Andrey Chudnov (D. E. Shaw &amp; Co., L.P.) and David A. Naumann (Stevens Institute of Technology)</i>
KEVM: A Complete Formal Semantics of the Ethereum Virtual Machine .204.....	
	<i>Everett Hildenbrandt (University of Illinois at Urbana-Champaign), Manasvi Saxena (University of Illinois at Urbana-Champaign), Nishant Rodrigues (University of Illinois at Urbana-Champaign), Xiaoran Zhu (University of Illinois at Urbana-Champaign), Philip Daian (Runtime Verification, Inc.), Dwight Guth (Runtime Verification, Inc.), Brandon Moore (Runtime Verification, Inc.), Daejun Park (University of Illinois at Urbana-Champaign), Yi Zhang (University of Illinois at Urbana-Champaign), Andrei Stefanescu (Runtime Verification, Inc.), and Grigore Rosu (University of Illinois at Urbana-Champaign)</i>

## Session: Information Flow

- A Permission-Dependent Type System for Secure Information Flow Analysis .218.....  
*Hongxu Chen (Nanyang Technological University), Alwen Tiu (Australian National University), Zhiwu Xu (Shenzhen University), and Yang Liu (Nanyang Technological University)*
- Types for Information Flow Control: Labeling Granularity and Semantic Models .233.....  
*Vineet Rajani (Max Planck Institute for Software Systems) and Deepak Garg (Max Planck Institute for Software Systems)*
- Inductive Invariants for Noninterference in Multi-agent Workflows .247.....  
*Christian Müller (Technische Universität München), Helmut Seidl (Technische Universität München), and Eugen Zlinescu (Technische Universität München)*
- Invited Paper: Local Differential Privacy on Metric Spaces: Optimizing the Trade-Off with Utility .262.....  
*Mário Alvim (UFMG, Belo Horizonte, Brazil), Konstantinos Chatzikokolakis (CNRS, France), Catuscia Palamidessi (INRIA, France), and Anna Pazii (INRIA and Ecole Polytechnique, France)*
- Privacy Risk in Machine Learning: Analyzing the Connection to Overfitting .268.....  
*Samuel Yeom (Carnegie Mellon University), Irene Giacomelli (University of Wisconsin--Madison), Matt Fredrikson (Carnegie Mellon University), and Somesh Jha (University of Wisconsin--Madison)*

## Session: Electronic Voting

- Alethea: A Provably Secure Random Sample Voting Protocol .283.....  
*David Basin (ETH Zürich), Saša Radomirovic (University of Dundee, United Kingdom), and Lara Schmid (ETH Zürich)*
- Machine-Checked Proofs for Electronic Voting: Privacy and Verifiability for Belenios .298.....  
*Véronique Cortier (LORIA, CNRS & Inria & Université de Lorraine), Constantin Ctilin Drgan (University of Surrey), François Dupressoir (University of Surrey), and Bogdan Warinschi (University of Bristol)*

## Session: Side Channels

- Symbolic Side-Channel Analysis for Probabilistic Programs .313.....  
*Pasquale Malacaria (Queen Mary University of London, UK), MHR Khouzani (Queen Mary University of London, UK), Corina S. Pasareanu (Carnegie Mellon University, USA), Quoc-Sang Phan (Fujitsu Laboratories of America, USA), and Kasper Luckow (Carnegie Mellon University, USA)*
- Secure Compilation of Side-Channel Countermeasures: The Case of Cryptographic “Constant-Time” .328.....  
*Gilles Barthe (IMDEA Software Institute, Madrid, Spain), Benjamin Grégoire (Inria, Sophia-Antipolis, France), and Vincent Laporte (IMDEA Software Institute, Madrid, Spain)*

## Session: Security Protocols 2

A Little More Conversation, a Little Less Action, a Lot More Satisfaction: Global States  
in ProVerif .344.....  
*Vincent Cheval (Inria Nancy - Grand Est, Loria, France), Véronique  
Cortier (CNRS, LORIA, France), and Mathieu Turuani (Inria Nancy -  
Grand Est, LORIA, France)*

Automated Unbounded Verification of Stateful Cryptographic Protocols with Exclusive OR .359.....  
*Jannik Dreier (Université de Lorraine, France), Lucca Hirschi (ETH  
Zurich, Switzerland), Sasa Radomirovic (University of Dundee, UK), and  
Ralf Sasse (ETH Zurich, Switzerland)*

A Typing Result for Stateful Protocols .374.....  
*Andreas Hess (Technical University of Denmark) and Sebastian  
Mödersheim (Technical University of Denmark)*

**Author Index 389** .....