Postquantum Cryptography, Part 1

Because of public-key cryptography’s relevance and quantum computers’ increasingly realistic threat to this technology, it’s necessary to come up with practical and secure postquantum cryptography. This special issue aims to present the state of the art and the grand challenges in postquantum cryptography and to discuss the transition of real-world systems to the new technology.

12 Guest Editors’ Introduction: Postquantum Cryptography—State of the Art
Johannes Buchmann, Kristin Lauter, and Michele Mosca

14 The Day the Cryptography Dies
John Mulholland, Michele Mosca, and Johannes Braun

22 Postquantum Opportunities: Lattices, Homomorphic Encryption, and Supersingular Isogeny Graphs
Kristin Lauter

28 Current State of Multivariate Cryptography
Jintai Ding and Albrecht Petzoldt

37 Hash-Based Signatures: State of Play
Denis Butin

44 Code-Based Cryptography: State of the Art and Perspectives
Nicolas Sendrier

51 Cryptography Standards in Quantum Time: New Wine in an Old Wineskin
Lidong Chen
Columns
3 From the Editors
Authorship Integrity and Attacks
Gene Tsudik
88 Last Word
Attribution
Daniel E. Geer Jr.

Departments
7 Interview
Silver Bullet Talks with Kelly Lum
Gary McGraw
58 Spotlight
ACM CCS 2016 Interviews, Part 3
Ahmad-Reza Sadeghi and Shaza Zeitouni
62 Sociotechnical Security and Privacy
Privacy? I Can’t Even! Making a Case for User-Tailored Privacy
Bart P. Knijnenburg
68 Resilient Security
The Right to Digital Self-Defense
Bryan Reinicke, Jeffrey Cummings, and Howard Kleinberg
72 Education
INSuRE: Collaborating Centers of Academic Excellence Engage Students in Cybersecurity Research
Alan Sherman, Melissa Dark, Agnes Chan, Rylan Chong, Thomas Morris, Linda Oliva, John Springer, Bhavani Thuraisingham, Christopher Vatcher, Rakesh Verma, and Susanne Wetzel
79 Systems Attacks and Defenses
Internet of Things Security Research: A Rehash of Old Ideas or New Intellectual Challenges?
Earlence Fernandes, Amir Rahmati, Kevin Eykholt, and Atul Prakash
85 Conferences
Building on the Success of Building Security In
Archer Batcheller, Summer Craze Fowler, Robert Cunningham, Dinara Doyle, Trent Jaeger, and Ulf Lindqvist

Also in This Issue
57 IEEE Reliability Society Information
61 IEEE Computer Society Information

From the Editors
Authorship Integrity and Attacks
Gene Tsudik
88 Last Word
Attribution
Daniel E. Geer Jr.

IEEE Security & Privacy is copublished by the IEEE Computer and Reliability Societies. For more information on computing topics, visit the IEEE Computer Society Digital Library at www.computer.org/csdl.