New Generation Computing (2021) 39:1–2
https://doi.org/10.1007/s00354-021-00127-1

NEW GENERATION COMPUTING

Preface: Special Issue on Card-Based Cryptography

Takaaki Mizuki[1]

Published online: 17 March 2021

I am very pleased to present this special issue of New Generation Computing for Card-Based Cryptography. The research field of card-based cryptography, which performs cryptographic tasks using a deck of physical cards, has been developing rapidly over the past several years. This special issue consists of six research papers that contain advanced and cutting-edge new results on the emerging research area, card-based cryptography.

In the paper, *Physical Zero-Knowledge Proof for Numberlink Puzzle and k Vertex-Disjoint Paths Problem*, Suthee Ruangwises and Toshiya Itoh propose a card-based zero-knowledge proof protocol for a popular pencil puzzle, Numberlink; the key technique used there can also be applied to k vertex-disjoint path problem.

In the paper, *Card-Based Cryptographic Logical Computations Using Private Operations*, Hibiki Ono and Yoshifumi Manabe introduce three new operations, private random bisection cuts, private reverse cuts, and private reveals, by which they provide efficient card-minimal protocols for elementary computations such as AND and XOR as well as more general constructions.

In the paper, *Card-based Cryptography with Dihedral Symmetry*, Kazumasa Shinagawa proposes a novel kind of cards, called the dihedral cards, by which he designs several important protocols suitable especially for multi-valued computations; he also constructs a framework capturing a wide range of types of physical cards.

In the paper, *How to Solve Millionaires' Problem with Two Kinds of Cards*, Takeshi Nakai, Yuto Misawa, Yuuki Tokushige, Mitsugu Iwamoto, and Kazuo Ohta reveal the power of a new operation, called the Private Permutation, for the first time by proposing efficient protocols that solve Millionaires' problem.

In the paper, *Five-Card AND Computations in Committed Format Using Only Uniform Cyclic Shuffles*, Yuta Abe, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone construct efficient and practical card-based protocols, i.e., five-card committed-format AND protocols using only uniform cyclic shuffles.

In the paper, *Card-Based Cryptography Meets Formal Verification*, Alexander Koch, Michael Schrempp, and Michael Kirsten comprehensively deal with protocols

✉ Takaaki Mizuki
mizuki+cardbasedngc@tohoku.ac.jp

[1] Cyberscience Center, Tohoku University, Sendai, Japan

working on a (commercially available) standard deck of playing cards, and provide non-trivial results such as a card-minimal AND protocol and lower bounds on the number of cards together with a technique based on the formal program verification.

All the papers submitted to this special issue were reviewed in accordance with the usual rigorous standards of New Generation Computing. All the accepted papers happened to be extended ones from the earlier versions presented at several prominent conferences: Every paper was substantially expanded from such a preliminary version, containing a lot of new findings and materials.

I would like to thank the authors for their contributions to this issue. I also thank the anonymous reviewers for reviewing the papers and appreciate the dedicated efforts and hard work of the board members listed below. My special thanks go to Editor-in-Chief Masayuki Numao and Area Editor Ayumi Shinohara for giving me this opportunity and their encouragement, as well as Springer for their professional support and collaboration.