New Generation Computing (2022) 40:47–48
https://doi.org/10.1007/s00354-022-00170-6

Preface: Special Issue on Card-Based Cryptography 2

Takaaki Mizuki[1]

Published online: 7 April 2022

I am grateful to announce that a special issue of New Generation Computing for Card-based Cryptography is released. This is the second special issue on card-based cryptography, following the first special issue which was published in Volume 39, Issue 1, April 2021.

As I wrote in Preface of the first special issue 1 year ago, 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 seven research papers that contain advanced and cutting-edge new results on the emerging research area, card-based cryptography. All the papers submitted to this special issue were reviewed in accordance with the usual rigorous standards of New Generation Computing.

In the paper, *Two Standard Decks of Playing Cards are Sufficient for a ZKP for Sudoku*, Suthee Ruangwises proposes a novel zero-knowledge proof protocol for Sudoku, one of the most popular pencil puzzles; the major advantage is that the proposed protocol works on standard decks of playing cards, implying that it is practical.

In the paper, *Card-Based Cryptographic Protocols with Malicious Players Using Private Operations*, Yoshifumi Manabe and Hibiki Ono construct secure protocols against malicious players in the private version of the card-based computation model; the key idea is to make use of envelopes as well as error correction.

In the paper, *Secure Computation for Threshold Functions with Physical Cards: Power of Private Permutations*, Takeshi Nakai, Satoshi Shirouchi, Yuuki Tokushige, Mitsugu Iwamoto, and Kazuo Ohta show that a secure computation of a threshold function can be efficiently conducted in the private model: it needs fewer cards than the trivial lower bound for the public model (where all input commitments are given at the beginning).

In the paper, *Private Function Evaluation with Cards*, Alexander Koch and Stefan Walzer implement four universal card-based protocols based on branching programs, circuits, Turing machines, and RAM machines; these are described using the sort sub-protocol, which is a useful tool formulated in this paper.

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

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

In the paper, *Card-Based ZKP for Connectivity: Applications to Nurikabe, Hitori, and Heyawake*, Léo Robert, Daiki Miyahara, Pascal Lafourcade, and Takaaki Mizuki construct card-based zero-knowledge proof protocols for three Nikoli's pencil puzzles, Nurikabe, Hitori, and Heyawake, by designing a new method for verifying the connectivity of hidden colored cells.

In the paper, *Efficient Card-Based Majority Voting Protocols*, Yoshiki Abe, Takeshi Nakai, Yoshihisa Kuroki, Shinnosuke Suzuki, Yuta Koga, Yohei Watanabe, Mitsugu Iwamoto, and Kazuo Ohta propose three-card three-input majority protocols in the private model, and then, extending the idea behind them, construct a general majority protocol which uses the same number of cards as the number of players.

In the paper, *Graph Automorphism Shuffles from Pile-Scramble Shuffles*, Kengo Miyamoto and Kazumasa Shinagawa consider a novel class of shuffles, called graph shuffles, and they show how to construct a graph shuffle protocol for any direct graph. The protocol is implementable only with pile-scramble shuffles.

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.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.