New Generation Computing (2024) 42:303–304
https://doi.org/10.1007/s00354-024-00280-3

NEW GENERATION COMPUTING

PREFACE

Special Issue on Card-Based Cryptography 3

Takaaki Mizuki[1]

Published online: 30 August 2024
© The Author(s), under exclusive licence to The Japanese Society for Artificial Intelligence and Springer Nature Japan KK, part of Springer Nature 2024

I am pleased to announce the release of a special issue of New Generation Computing dedicated to card-based cryptography. This is the third special issue on this topic, following the successful ones published in Volume 39, Issue 1 (April 2021) and Volume 40, Issue 1 (April 2022).

Card-based cryptography is a very unique type of computing where we can perform cryptographic tasks using a deck of physical cards. The research area of card-based cryptography has developed rapidly over the last decade. This special issue consists of nine research papers that present advanced and innovative new results in this area. All papers submitted to this special issue have been peer-reviewed according to the usual rigorous standards of New Generation Computing.

In the paper, *Card-Based Cryptographic Protocols with a Standard Deck of Cards Using Private Operations*, Yoshifumi Manabe and Hibiki Ono use a standard deck of cards to construct card-minimal AND, XOR, and copy protocols based on private operations, by which any Boolean function can be securely computed. They also deal with private input operations as well as asymmetric cards.

In the paper, *Printing Protocol: Physical ZKPs for Decomposition Puzzles*, Suthee Ruangwises and Mitsugu Iwamoto propose the printing protocol, by which we can physically verify solutions of decomposition puzzles. They use it to construct zero-knowledge proof protocols for Five Cells and Meadows.

In the paper, *Card-based Cryptography with a Standard Deck of Cards, Revisited: Efficient Protocols in the Private Model*, Takeshi Nakai, Keita Iwanari, Tomoki Ono, Yoshiki Abe, Yohei Watanabe, and Mitsugu Iwamoto design a three-card AND protocol, a three-card OR protocol, and a two-card XOR protocol using a standard deck of playing cards in the private model, followed by an efficient three-input majority protocol.

In the paper, *Card-Based Protocols for Private Set Intersection and Union*, Anastasiia Doi, Tomoki Ono, Yoshiki Abe, Takeshi Nakai, Kazumasa Shinagawa, Yohei Watanabe, Koji Nuida, and Mitsugu Iwamoto design several card-based protocols

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

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

for performing Private Set Intersection (PSI) and Private Set Union (PSU) by considering both the shuffle-based model and the private-permutation-based model.

In the paper, *Physical Zero-Knowledge Proof for Sukoro*, Shun Sasaki and Kazumasa Shinagawa construct a card-based zero-knowledge proof protocol for Nikoli's pencil puzzle, Sukoro, by using a method for verifying the connectivity condition in the non-interactive setting.

In the paper, *Physical Zero-Knowledge Proof Protocols for Topswops and Botdrops*, Yuichi Komano and Takaaki Mizuki construct card-based zero-knowledge proof protocols for one-player card games, Topswops and Botdrops, by introducing new encodings for integers.

In the paper, *NP-Completeness and Physical Zero-Knowledge Proofs for Sumplete, a Puzzle Generated by ChatGPT*, Kyosuke Hatsugai, Suthee Ruangwises, Kyoichi Asano, and Yoshiki Abe first show the NP-completeness of Sumplete, a pencil puzzle, which was created with the help of ChatGPT. They then construct a card-based zero-knowledge proof protocol for Sumplete.

In the paper, *Efficient Card-Based ZKP for Single Loop Condition and Its Application to Moon-or-Sun*, Samuel Hand, Alexander Koch, Pascal Lafourcade, Daiki Miyahara, and Léo Robert design an efficient card-based method for verifying the single-loop condition by revisiting the previous work. They apply this method to constructing a zero-knowledge proof protocol for Moon-or-Sun, a pencil puzzle.

In the paper, *Extended Addition Protocol and Efficient Voting Protocols Using Regular Polygon Cards*, Yoshihiro Takahashi and Kazumasa Shinagawa use regular polygon cards to construct a new efficient protocol for securely adding two integers and they propose two voting protocols.

I would like to express my sincere gratitude to the authors for their valuable contributions to this issue. I am also indebted to the anonymous reviewers for their careful evaluation of the submitted papers. The dedicated efforts of the board members listed below are greatly appreciated. My special thanks go to Editor-in-Chief Yutaka Matsuo, Area Editor Ayumi Shinohara, and Editor Haruka Murakami for their invaluable support, and to Springer for their professional assistance and cooperation.

Editorial Members
Guest Editors-in-Chief
Takaaki Mizuki (Tohoku University, Japan)
Board Members
Goichiro Hanaoka (AIST, Japan)
Pascal Lafourcade (University Clermont Auvergne, France)
Yoshifumi Manabe (Kogakuin University, Japan)

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