カードベース暗号の bib ファイル

宮原 大輝　　水木 敬明　　品川 和雅

March 18, 2026

- これは、カードベース暗号の文献を集めた bib ファイルです。
- 国際会議と論文誌は合わせて時系列順に並べています。ただし、国際会議は開催日を、論文誌は出版日・公開日を基準に並べています。
- 博士論文は（国際会議と論文誌の後の）末尾に時系列順に並べています。
- 誤り・ミス等を発見された方は編集者（miyahara[at]uec.ac.jp）までご一報ください。

References

[Boe90] Bert Den Boer. “More efficient match-making and satisfiability *The Five Card Trick*.” In: *Advances in Cryptology – EUROCRYPT’ 89*. Ed. by Jean-Jacques Quisquater and Joos Vandewalle. Vol. 434. LNCS, pp. 208–217, Heidelberg: Springer, 1990.

[CK94] Claude Crépeau and Joe Kilian. “Discreet solitary games.” In: *Advances in Cryptology—CRYPTO’ 93*. Ed. by Douglas R. Stinson. Vol. 773. LNCS, pp. 319–330, Berlin, Heidelberg: Springer, 1994.

[NR98] Valtteri Niemi and Ari Renvall. “Secure multiparty computations without computers.” *Theor. Comput. Sci.* 191.1–2, 173–183 (1998).

[NR99] Valtteri Niemi and Ari Renvall. “Solitaire zero-knowledge.” *Fundam. Inf.* 38.1,2, 181–188 (1999).

[Sti01] Anton Stiglic. “Computations with a deck of cards.” *Theor. Comput. Sci.* 259.1–2, 671–678 (2001).

[BCIK03] József Balogh, János A Csirik, Yuval Ishai, and Eyal Kushilevitz. “Private computation using a PEZ dispenser.” *Theor. Comput. Sci.* 306.1, 69–84 (2003).

[MUS06] Takaaki Mizuki, Fumishige Uchiike, and Hideaki Sone. “Securely computing XOR with 10 cards.” *The Australasian Journal of Combinatorics* 36, 279–293 (2006).

[MKS07a] Takaaki Mizuki, Yoshinori Kugimoto, and Hideaki Sone. "Secure multiparty computations using a dial lock." In: *Theory and Applications of Models of Computation*. Ed. by Jin-Yi Cai, S. Barry Cooper, and Hong Zhu. Vol. 4484. LNCS, pp. 499–510, Berlin, Heidelberg: Springer, 2007.

[GNPR07] Ronen Gradwohl, Moni Naor, Benny Pinkas, and Guy N. Rothblum. "Cryptographic and physical zero-knowledge proof systems for solutions of Sudoku puzzles." In: *Fun with Algorithms*. Ed. by Pierluigi Crescenzi, Giuseppe Prencipe, and Geppino Pucci. Vol. 4475. LNCS, pp. 166–182, Berlin, Heidelberg: Springer, 2007.

[MKS07b] Takaaki Mizuki, Yoshinori Kugimoto, and Hideaki Sone. "Secure multiparty computations using the 15 puzzle." In: *Combinatorial Optimization and Applications*. Ed. by Andreas Dress, Yinfeng Xu, and Binhai Zhu. Vol. 4616. LNCS, pp. 255–266, Berlin, Heidelberg: Springer, 2007.

[GNPR09] Ronen Gradwohl, Moni Naor, Benny Pinkas, and Guy N. Rothblum. "Cryptographic and physical zero-knowledge proof systems for solutions of Sudoku puzzles." *Theory of Computing Systems* 44.2, 245–268 (2009).

[MS09] Takaaki Mizuki and Hideaki Sone. "Six-card secure AND and four-card secure XOR." In: *Frontiers in Algorithmics*. Ed. by Xiaotie Deng, John E. Hopcroft, and Jinyun Xue. Vol. 5598. LNCS, pp. 358–369, Berlin, Heidelberg: Springer, 2009.

[CH10] Yu-Feng Chien and Wing-Kai Hon. "Cryptographic and physical zero-knowledge proof: from Sudoku to Nonogram." In: *Fun with Algorithms*. Ed. by Paolo Boldi and Luisa Gargano. Vol. 6099. LNCS, pp. 102–112, Berlin, Heidelberg: Springer, 2010.

[MKS12] Takaaki Mizuki, Michihito Kumamoto, and Hideaki Sone. "The five-card trick can be done with four cards." In: *Advances in Cryptology—ASIACRYPT 2012*. Ed. by Xiaoyun Wang and Kazue Sako. Vol. 7658. LNCS, pp. 598–606, Berlin, Heidelberg: Springer, 2012.

[MAS13] Takaaki Mizuki, Isaac Kobina Asiedu, and Hideaki Sone. "Voting with a logarithmic number of cards." In: *Unconventional Computation and Natural Computation*. Ed. by Giancarlo Mauri, Alberto Dennunzio, Luca Manzoni, and Antonio E. Porreca. Vol. 7956. LNCS, pp. 162–173, Berlin, Heidelberg: Springer, 2013.

[NMS13] Takuya Nishida, Takaaki Mizuki, and Hideaki Sone. "Securely computing the three-input majority function with eight cards." In: *Theory and Practice of Natural Computing*. Ed. by Adrian-Horia Dediu, Carlos Martín-Vide, Bianca Truthe, and Miguel A. Vega-Rodríguez. Vol. 8273. LNCS, pp. 193–204, Berlin, Heidelberg: Springer, 2013.

[CHL13] Eddie Cheung, Chris Hawthorne, and Patrick Lee. *Cs 758 project: secure computation with playing cards*, 2013.

[HST14] James Heather, Steve Schneider, and Vanessa Teague. “Cryptographic protocols with everyday objects.” *Formal Aspects Comput.* 26.1, 37–62 (2014).

[MS14a] Takaaki Mizuki and Hiroki Shizuya. “Practical card-based cryptography.” In: *Fun with Algorithms.* Ed. by Alfredo Ferro, Fabrizio Luccio, and Peter Widmayer. Vol. 8496. LNCS, pp. 313–324, Cham: Springer, 2014.

[MS14b] Takaaki Mizuki and Hiroki Shizuya. “A formalization of card-based cryptographic protocols via abstract machine.” *Int. J. Inf. Secur.* 13.1, 15–23 (2014).

[NHMS15a] Takuya Nishida, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone. “Card-based protocols for any Boolean function.” In: *Theory and Applications of Models of Computation.* Ed. by Rahul Jain, Sanjay Jain, and Frank Stephan. Vol. 9076. LNCS, pp. 110–121, Cham: Springer, 2015.

[NHMS15b] Takuya Nishida, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone. “Securely computing three-input functions with eight cards.” *IEICE Trans. Fundam.* E98.A.6, 1145–1152 (2015).

[SMS$^+$15] Kazumasa Shinagawa, Takaaki Mizuki, Jacob Schuldt, Koji Nuida, Naoki Kanayama, Takashi Nishide, Goichiro Hanaoka, and Eiji Okamoto. “Secure multi-party computation using polarizing cards.” In: *Advances in Information and Computer Security.* Ed. by Keisuke Tanaka and Yuji Suga. Vol. 9241. LNCS, pp. 281–297, Cham: Springer, 2015.

[ICM15] Rie Ishikawa, Eikoh Chida, and Takaaki Mizuki. “Efficient card-based protocols for generating a hidden random permutation without fixed points.” In: *Unconventional Computation and Natural Computation.* Ed. by Cristian S. Calude and Michael J. Dinneen. Vol. 9252. LNCS, pp. 215–226, Cham: Springer, 2015.

[MWS15] Antonio Marcedone, Zikai Wen, and Elaine Shi. *Secure dating with four or fewer cards.* Cryptology ePrint Archive, Report 2015/1031, 2015.

[SMN$^+$15] Kazumasa Shinagawa, Takaaki Mizuki, Jacob Schuldt C. N., Koji Nuida, Naoki Kanayama, Takashi Nishide, Goichiro Hanaoka, and Eiji Okamoto. “Multi-party computation with small shuffle complexity using regular polygon cards.” In: *Provable Security.* Ed. by Man-Ho Au and Atsuko Miyaji. Vol. 9451. LNCS, pp. 127–146, Cham: Springer, 2015.

[KWH15] Alexander Koch, Stefan Walzer, and Kevin Härtel. "Card-based cryptographic protocols using a minimal number of cards." In: *Advances in Cryptology—ASIACRYPT 2015*. Ed. by Tetsu Iwata and Jung Hee Cheon. Vol. 9452. LNCS, pp. 783–807, Berlin, Heidelberg: Springer, 2015.

[NNH$^+$15] Akihiro Nishimura, Takuya Nishida, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone. "Five-card secure computations using unequal division shuffle." In: *Theory and Practice of Natural Computing*. Ed. by Adrian-Horia Dediu, Luis Magdalena, and Carlos Martín-Vide. Vol. 9477. LNCS, pp. 109–120, Cham: Springer, 2015.

[Miz16a] Takaaki Mizuki. "Card-based protocols for securely computing the conjunction of multiple variables." *Theor. Comput. Sci.* 622.C, 34–44 (2016).

[NHMS16] Akihiro Nishimura, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone. "An implementation of non-uniform shuffle for secure multi-party computation." In: *ACM ASIA Public-Key Cryptography Workshop*. Ed. by Keita Emura, Goichiro Hanaoka, and Rui Zhang, pp. 49–55, New York: ACM, 2016.

[SMS$^+$16] Kazumasa Shinagawa, Takaaki Mizuki, Jacob Schuldt, Koji Nuida, Naoki Kanayama, Takashi Nishide, Goichiro Hanaoka, and Eiji Okamoto. "Secure computation protocols using polarizing cards." *IEICE Trans. Fundam.* E99.A.6, 1122–1131 (2016).

[BDDL16] Xavier Bultel, Jannik Dreier, Jean-Guillaume Dumas, and Pascal Lafourcade. "Physical zero-knowledge proofs for Akari, Takuzu, Kakuro and KenKen." In: *Fun with Algorithms*. Ed. by Erik D. Demaine and Fabrizio Grandoni. Vol. 49. LIPIcs, pp. 8:1–8:20, Dagstuhl, Germany: Schloss Dagstuhl, 2016.

[IM16] Takuya Ibaraki and Yoshifumi Manabe. "A more efficient card-based protocol for generating a random permutation without fixed points." In: *Mathematics and Computers in Sciences and in Industry (MCSI)*, pp. 252–257, 2016.

[SNN$^+$16] Kazumasa Shinagawa, Koji Nuida, Takashi Nishide, Goichiro Hanaoka, and Eiji Okamoto. "Committed AND protocol using three cards with more handy shuffle." In: *2016 International Symposium on Information Theory and Its Applications*, pp. 700–702, IEEE, 2016.

[Miz16b] Takaaki Mizuki. "Efficient and secure multiparty computations using a standard deck of playing cards." In: *Cryptology and Network Security*. Ed. by Sara Foresti and Giuseppe Persiano. Vol. 10052. LNCS, pp. 484–499, Cham: Springer, 2016.

[NTM$^+$16] Takeshi Nakai, Yuuki Tokushige, Yuto Misawa, Mitsugu Iwamoto, and Kazuo Ohta. "Efficient card-based cryptographic protocols for millionaires' problem utilizing private permutations." In: *Cryptology and Network Security.* Ed. by Sara Foresti and Giuseppe Persiano. Vol. 10052. LNCS, pp. 500–517, Cham: Springer, 2016.

[FAN$^+$17] Danny Francis, Syarifah Ruqayyah Aljunid, Takuya Nishida, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone. "Necessary and sufficient numbers of cards for securely computing two-bit output functions." In: *Paradigms in Cryptology—Mycrypt 2016. Malicious and Exploratory Cryptology.* Ed. by Raphaël C.-W. Phan and Moti Yung. Vol. 10311. LNCS, pp. 193–211, Cham: Springer, 2017.

[Han17] Goichiro Hanaoka. "Towards user-friendly cryptography." In: *Paradigms in Cryptology–Mycrypt 2016. Malicious and Exploratory Cryptology.* Ed. by Raphaël C.-W. Phan and Moti Yung. Vol. 10311. LNCS, pp. 481–484, Cham: Springer, 2017.

[UNH$^+$16] Itaru Ueda, Akihiro Nishimura, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone. "How to implement a random bisection cut." In: *Theory and Practice of Natural Computing.* Ed. by Carlos Martín-Vide, Takaaki Mizuki, and Miguel A. Vega-Rodríguez. Vol. 10071. LNCS, pp. 58–69, Cham: Springer, 2016.

[MS17] Takaaki Mizuki and Hiroki Shizuya. "Computational model of card-based cryptographic protocols and its applications." *IEICE Trans. Fundam.* E100.A.1, 3–11 (2017).

[SMS$^+$17] Kazumasa Shinagawa, Takaaki Mizuki, Jacob Schuldt, Koji Nuida, Naoki Kanayama, Takashi Nishide, Goichiro Hanaoka, and Eiji Okamoto. "Card-based protocols using regular polygon cards." *IEICE Trans. Fundam.* E100.A.9, 1900–1909 (2017).

[NNH$^+$18] Akihiro Nishimura, Takuya Nishida, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone. "Card-based protocols using unequal division shuffles." *Soft Comput.* 22, 361–371 (2018).

[HSN$^+$17] Yuji Hashimoto, Kazumasa Shinagawa, Koji Nuida, Masaki Inamura, and Goichiro Hanaoka. "Secure grouping protocol using a deck of cards." In: *Information Theoretic Security.* Ed. by Junji Shikata. Vol. 10681. LNCS, pp. 135–152, Cham: Springer, 2017.

[NSIO17] Takeshi Nakai, Satoshi Shirouchi, Mitsugu Iwamoto, and Kazuo Ohta. "Four cards are sufficient for a card-based three-input voting protocol utilizing private permutations." In: *Information Theoretic Security.* Ed. by Junji Shikata. Vol. 10681. LNCS, pp. 153–165, Cham: Springer, 2017.

[KKW+17] Julia Kastner, Alexander Koch, Stefan Walzer, Daiki Miyahara, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone. "The minimum number of cards in practical card-based protocols." In: *Advances in Cryptology—ASIACRYPT 2017*. Ed. by Tsuyoshi Takagi and Thomas Peyrin. Vol. 10626. LNCS, pp. 126–155, Cham: Springer, 2017.

[AHMS18] Yuta Abe, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone. "Five-card AND protocol in committed format using only practical shuffles." In: *ACM ASIA Public-Key Cryptography Workshop*, pp. 3–8, New York: ACM, 2018.

[SMS18] Tatsuya Sasaki, Takaaki Mizuki, and Hideaki Sone. "Card-based zero-knowledge proof for Sudoku." In: *Fun with Algorithms*. Ed. by Hiro Ito, Stefano Leonardi, Linda Pagli, and Giuseppe Prencipe. Vol. 100. LIPIcs, pp. 29:1–29:10, Dagstuhl, Germany: Schloss Dagstuhl, 2018.

[SM18a] Kazumasa Shinagawa and Takaaki Mizuki. "Card-based protocols using triangle cards." In: *Fun with Algorithms*. Ed. by Hiro Ito, Stefano Leonardi, Linda Pagli, and Giuseppe Prencipe. Vol. 100. LIPIcs, pp. 31:1–31:13, Dagstuhl, Germany: Schloss Dagstuhl, 2018.

[MUH+18] Daiki Miyahara, Itaru Ueda, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone. "Analyzing execution time of card-based protocols." In: *Unconventional Computation and Natural Computation*. Ed. by Susan Stepney and Sergey Verlan. Vol. 10867. LNCS, pp. 145–158, Cham: Springer, 2018.

[MK18] Takaaki Mizuki and Yuichi Komano. "Analysis of information leakage due to operative errors in card-based protocols." In: *Combinatorial Algorithms*. Ed. by Costas Iliopoulos, Hon Wai Leong, and Wing-Kin Sung. Vol. 10979. LNCS, pp. 250–262, Cham: Springer, 2018.

[OM18a] Hibiki Ono and Yoshifumi Manabe. "Efficient card-based cryptographic protocols for the Millionaires' problem using private input operations." In: *Asia Joint Conference on Information Security (AsiaJCIS)*, pp. 23–28, 2018.

[NHMS18] Akihiro Nishimura, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone. "Pile-shifting scramble for card-based protocols." *IEICE Trans. Fundam.* 101.9, 1494–1502 (2018).

[HNS+18] Yuji Hashimoto, Koji Nuida, Kazumasa Shinagawa, Masaki Inamura, and Goichiro Hanaoka. "Toward finite-runtime card-based protocol for generating a hidden random permutation without fixed points." *IEICE Trans. Fundam.* E101.A.9, 1503–1511 (2018).

[HSN$^+$18] Yuji Hashimoto, Kazumasa Shinagawa, Koji Nuida, Masaki Inamura, and Goichiro Hanaoka. “Secure grouping protocol using a deck of cards.” *IEICE Trans. Fundam.* E101.A.9, 1512–1524 (2018).

[WKS$^+$18] Yohei Watanabe, Yoshihisa Kuroki, Shinnosuke Suzuki, Yuta Koga, Mitsugu Iwamoto, and Kazuo Ohta. “Card-based majority voting protocols with three inputs using three cards.” In: *2018 International Symposium on Information Theory and Its Applications*, pp. 218–222, 2018.

[BDD$^+$18] Xavier Bultel, Jannik Dreier, Jean-Guillaume Dumas, Pascal Lafourcade, Daiki Miyahara, Takaaki Mizuki, Atsuki Nagao, Tatsuya Sasaki, Kazumasa Shinagawa, and Hideaki Sone. “Physical zero-knowledge proof for Makaro.” In: *Stabilization, Safety, and Security of Distributed Systems.* Ed. by Taisuke Izumi and Petr Kuznetsov. Vol. 11201. LNCS, pp. 111–125, Springer, 2018.

[OM18b] Hibiki Ono and Yoshifumi Manabe. “Card-based cryptographic protocols with the minimum number of cards using private operations.” In: *Foundations and Practice of Security.* Ed. by Nur Zincir-Heywood, Guillaume Bonfante, Mourad Debbabi, and Joaquin Garcia-Alfaro. Vol. 11358. LNCS, pp. 193–207, Cham: Springer, 2018.

[SM18b] Kazumasa Shinagawa and Takaaki Mizuki. “The six-card trick: secure computation of three-input equality.” In: *Information Security and Cryptology.* Ed. by Kwangsu Lee. Vol. 11396. LNCS, pp. 123–131, Cham: Springer, 2018.

[KM18] Yuichi Komano and Takaaki Mizuki. “Multi-party computation based on physical coins.” In: *Theory and Practice of Natural Computing.* Ed. by David Fagan, Carlos Martín-Vide, Michael O’Neill, and Miguel A. Vega-Rodríguez. Vol. 11324. LNCS, pp. 87–98, Cham: Springer, 2018.

[MHMS18] Daiki Miyahara, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone. “Practical and easy-to-understand card-based implementation of yao’s millionaire protocol.” In: *Combinatorial Optimization and Applications.* Ed. by Donghyun Kim, R. N. Uma, and Alexander Zelikovsky. Vol. 11346. LNCS, pp. 246–261, Cham: Springer, 2018.

[Shi19] Kazumasa Shinagawa. “Card-based cryptography with invisible ink.” In: *Theory and Applications of Models of Computation.* Ed. by T.V. Gopal and Junzo Watada. Vol. 11436. LNCS, pp. 566–577, Cham: Springer, 2019.

[SM19] Kazumasa Shinagawa and Takaaki Mizuki. “Secure computation of any Boolean function based on any deck of cards.” In: *Frontiers in Algorithmics*. Ed. by Yijia Chen, Xiaotie Deng, and Mei Lu. Vol. 11458. Lecture Notes in Computer Science, pp. 63–75, Cham: Springer, 2019.

[RI19] Suthee Ruangwises and Toshiya Itoh. “AND protocols using only uniform shuffles.” In: *Computer Science–Theory and Applications*. Ed. by René van Bevern and Gregory Kucherov. Vol. 11532. LNCS, pp. 349–358, Cham: Springer, 2019.

[DLM^{+}19] Jean-Guillaume Dumas, Pascal Lafourcade, Daiki Miyahara, Takaaki Mizuki, Tatsuya Sasaki, and Hideaki Sone. “Interactive physical zero-knowledge proof for Norinori.” In: *Computing and Combinatorics*. Ed. by Ding-Zhu Du, Zhenhua Duan, and Cong Tian. Vol. 11653. LNCS, pp. 166–177, Cham: Springer, 2019.

[MSMS19] Daiki Miyahara, Tatsuya Sasaki, Takaaki Mizuki, and Hideaki Sone. “Card-based physical zero-knowledge proof for Kakuro.” *IEICE Trans. Fundam.* 102.9, 1072–1078 (2019).

[OM19] Hibiki Ono and Yoshifumi Manabe. “Card-based cryptographic protocols with the minimum number of rounds using private operations.” In: *Data Privacy Management, Cryptocurrencies and Blockchain Technology*. Ed. by Cristina Pérez-Solà, Guillermo Navarro-Arribas, Alex Biryukov, and Joaquin Garcia-Alfaro. Vol. 11737. LNCS, pp. 156–173, Cham: Springer, 2019.

[LMM^{+}19] Pascal Lafourcade, Daiki Miyahara, Takaaki Mizuki, Tatsuya Sasaki, and Hideaki Sone. “A physical ZKP for Slitherlink: how to perform physical topology-preserving computation.” In: *Information Security Practice and Experience*. Ed. by Swee-Huay Heng and Javier Lopez. Vol. 11879. LNCS, pp. 135–151, Cham: Springer, 2019.

[KSK19] Alexander Koch, Michael Schrempp, and Michael Kirsten. “Card-based cryptography meets formal verification.” In: *Advances in Cryptology–ASIACRYPT 2019*. Ed. by Steven D. Galbraith and Shiho Moriai. Vol. 11921. LNCS, pp. 488–517, Cham: Springer, 2019.

[AIO19] Yoshiki Abe, Mitsugu Iwamoto, and Kazuo Ohta. “Efficient private PEZ protocols for symmetric functions.” In: *Theory of Cryptography*. Ed. by Dennis Hofheinz and Alon Rosen. Vol. 11891. LNCS, pp. 372–392, Cham: Springer, 2019.

[TMMS19] Ken Takashima, Daiki Miyahara, Takaaki Mizuki, and Hideaki Sone. “Card-based protocol against actively revealing card attack.” In: *Theory and Practice of Natural Computing*. Ed. by Carlos Martín-Vide, Geoffrey Pond, and Miguel A. Vega-Rodríguez. Vol. 11934. LNCS, pp. 95–106, Cham: Springer, 2019.

[TAS$^+$19] Ken Takashima, Yuta Abe, Tatsuya Sasaki, Daiki Miyahara, Kazumasa Shinagawa, Takaaki Mizuki, and Hideaki Sone. "Card-based secure ranking computations." In: *Combinatorial Optimization and Applications*. Ed. by Yingshu Li, Mihaela Cardei, and Yan Huang. Vol. 11949. LNCS, pp. 461–472, Cham: Springer, 2019.

[MHMS20] Daiki Miyahara, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone. "Practical card-based implementations of Yao's millionaire protocol." *Theor. Comput. Sci.* 803, 207–221 (2020).

[UMN$^+$20] Itaru Ueda, Daiki Miyahara, Akihiro Nishimura, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone. "Secure implementations of a random bisection cut." *Int. J. Inf. Secur.* 19.4, 445–452 (2020).

[TMMS20] Kodai Toyoda, Daiki Miyahara, Takaaki Mizuki, and Hideaki Sone. "Six-card finite-runtime XOR protocol with only random cut." In: *ACM ASIA Public-Key Cryptography Workshop*, pp. 2–8, New York: ACM, 2020.

[RI20a] Suthee Ruangwises and Toshiya Itoh. "Securely computing the n-variable equality function with $2n$ cards." In: *Theory and Applications of Models of Computation*. Ed. by Jianer Chen, Qilong Feng, and Jinhui Xu. Vol. 12337. LNCS, pp. 25–36, Cham: Springer, 2020.

[AIO20] Yoshiki Abe, Mitsugu Iwamoto, and Kazuo Ohta. "How to detect malicious behaviors in a card-based majority voting protocol with three inputs." In: *2020 International Symposium on Information Theory and Its Applications*, pp. 377–381, 2020.

[Yas20] Kenji Yasunaga. "Practical card-based protocol for three-input majority." *IEICE Trans. Fundam.* E103.A.11, 1296–1298 (2020).

[SMMS20] Tatsuya Sasaki, Daiki Miyahara, Takaaki Mizuki, and Hideaki Sone. "Efficient card-based zero-knowledge proof for Sudoku." *Theor. Comput. Sci.* 839, 135–142 (2020).

[RMLM20] Léo Robert, Daiki Miyahara, Pascal Lafourcade, and Takaaki Mizuki. "Physical zero-knowledge proof for Suguru puzzle." In: *Stabilization, Safety, and Security of Distributed Systems*. Ed. by Stéphane Devismes and Neeraj Mittal. Vol. 12514. LNCS, pp. 235–247, Cham: Springer, 2020.

[MO21a] Yoshifumi Manabe and Hibiki Ono. "Secure card-based cryptographic protocols using private operations against malicious players." In: *Innovative Security Solutions for Information Technology and Communications*. Ed. by Diana Maimut, Andrei-George Oprina, and Damien Sauveron. Vol. 12596. LNCS, pp. 55–70, Cham: Springer, 2021.

[SMS$^+$21] Yuto Shinoda, Daiki Miyahara, Kazumasa Shinagawa, Takaaki Mizuki, and Hideaki Sone. "Card-based covert lottery." In: *Innovative Security Solutions for Information Technology and Communications*. Ed. by Diana Maimut, Andrei-George Oprina, and Damien Sauveron. Vol. 12596. LNCS, pp. 257–270, Cham: Springer, 2021.

[SMA$^+$20] Takahiro Saito, Daiki Miyahara, Yuta Abe, Takaaki Mizuki, and Hiroki Shizuya. "How to implement a non-uniform or non-closed shuffle." In: *Theory and Practice of Natural Computing*. Ed. by Carlos Martín-Vide, Miguel A. Vega-Rodríguez, and Miin-Shen Yang. Vol. 12494. LNCS, pp. 107–118, Cham: Springer, 2020.

[TAS$^+$20] Ken Takashima, Yuta Abe, Tatsuya Sasaki, Daiki Miyahara, Kazumasa Shinagawa, Takaaki Mizuki, and Hideaki Sone. "Card-based protocols for secure ranking computations." *Theor. Comput. Sci.* 845, 122–135 (2020).

[MMMS20] Soma Murata, Daiki Miyahara, Takaaki Mizuki, and Hideaki Sone. "Public-PEZ cryptography." In: *Information Security*. Ed. by Willy Susilo, Robert H. Deng, Fuchun Guo, Yannan Li, and Rolly Intan. Vol. 12472. LNCS, pp. 59–74, Cham: Springer, 2020.

[SN21] Kazumasa Shinagawa and Koji Nuida. "A single shuffle is enough for secure card-based computation of any Boolean circuit." *Discrete Applied Mathematics* 289, 248–261 (2021).

[TMMS21] Ken Takashima, Daiki Miyahara, Takaaki Mizuki, and Hideaki Sone. "Actively revealing card attack on card-based protocols." *Nat. Comput.* 21.4, 615–628 (2021).

[MMMS21] Soma Murata, Daiki Miyahara, Takaaki Mizuki, and Hideaki Sone. "Efficient generation of a card-based uniformly distributed random derangement." In: *WALCOM: Algorithms and Computation*. Ed. by Ryuhei Uehara, Seok-Hee Hong, and Subhas C. Nandy. Vol. 12635. LNCS, pp. 78–89, Cham: Springer, 2021.

[RI21a] Suthee Ruangwises and Toshiya Itoh. "Physical zero-knowledge proof for Ripple Effect." In: *WALCOM: Algorithms and Computation*. Ed. by Seokhee Hong, Subhas Nandy, and Ryuhei Uehara. Vol. 11737. LNCS, pp. 296–307, Cham: Springer, 2021.

[DK21] Pavel Dvořák and Michal Koucký. "Barrington plays cards: the complexity of card-based protocols." In: *Theoretical Aspects of Computer Science*. Ed. by Markus Bläser and Benjamin Monmege. Vol. 187. LIPIcs, pp. 26:1–26:17, Dagstuhl: Schloss Dagstuhl, 2021.

[Miz21] Takaaki Mizuki. "Preface: special issue on card-based cryptography." *New Gener. Comput.* 39, 1–2 (2021).

[OM21a] Hibiki Ono and Yoshifumi Manabe. "Card-based cryptographic logical computations using private operations." *New Gener. Comput.* 39.1, 19–40 (2021).

[RI21b] Suthee Ruangwises and Toshiya Itoh. "Physical zero-knowledge proof for Numberlink puzzle and k vertex-disjoint paths problem." *New Gener. Comput.* 39.1, 3–17 (2021).

[Shi21] Kazumasa Shinagawa. "Card-based cryptography with dihedral symmetry." *New Gener. Comput.* 39.1, 41–71 (2021).

[NST$^+$21] Takeshi Nakai, Satoshi Shirouchi, Yuuki Tokushige, Mitsugu Iwamoto, and Kazuo Ohta. "How to solve millionaires' problem with two kinds of cards." *New Gener. Comput.* 39.1, 73–96 (2021).

[AHMS21] Yuta Abe, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone. "Five-card AND computations in committed format using only uniform cyclic shuffles." *New Gener. Comput.* 39.1, 97–114 (2021).

[KSK21] Alexander Koch, Michael Schrempp, and Michael Kirsten. "Card-based cryptography meets formal verification." *New Gener. Comput.* 39.1, 115–158 (2021).

[KW20] Alexander Koch and Stefan Walzer. "Foundations for actively secure card-based cryptography." In: *Fun with Algorithms.* Ed. by Martin Farach-Colton, Giuseppe Prencipe, and Ryuhei Uehara. Vol. 157. LIPIcs, pp. 17:1–17:23, Dagstuhl, Germany: Schloss Dagstuhl, 2020.

[RI20b] Suthee Ruangwises and Toshiya Itoh. "Physical zero-knowledge proof for Numberlink." In: *Fun with Algorithms.* Ed. by Martin Farach-Colton, Giuseppe Prencipe, and Ryuhei Uehara. Vol. 157. LIPIcs, pp. 22:1–22:11, Dagstuhl, Germany: Schloss Dagstuhl, 2020.

[MRL$^+$20] Daiki Miyahara, Léo Robert, Pascal Lafourcade, So Takeshige, Takaaki Mizuki, Kazumasa Shinagawa, Atsuki Nagao, and Hideaki Sone. "Card-based ZKP protocols for Takuzu and Juosan." In: *Fun with Algorithms.* Ed. by Martin Farach-Colton, Giuseppe Prencipe, and Ryuhei Uehara. Vol. 157. LIPIcs, pp. 20:1–20:21, Dagstuhl, Germany: Schloss Dagstuhl, 2020.

[KTMM21] Hiroto Koyama, Kodai Toyoda, Daiki Miyahara, and Takaaki Mizuki. "New card-based copy protocols using only random cuts." In: *ACM ASIA Public-Key Cryptography Workshop*, pp. 13–22, NY: ACM, 2021.

[MKMS21] Daiki Miyahara, Yuichi Komano, Takaaki Mizuki, and Hideaki Sone. "Cooking cryptographers: secure multiparty computation based on balls and bags." In: *Computer Security Foundations Symposium*, pp. 389–404, NY: IEEE, 2021.

[KMMS21] Hiroto Koyama, Daiki Miyahara, Takaaki Mizuki, and Hideaki Sone. "A secure three-input AND protocol with a standard deck of minimal cards." In: *Computer Science – Theory and Applications*. Ed. by Rahul Santhanam and Daniil Musatov. Vol. 12730. LNCS, pp. 242–256, Cham: Springer, 2021.

[MO21b] Yoshifumi Manabe and Hibiki Ono. "Card-based cryptographic protocols for three-input functions using private operations." In: *Combinatorial Algorithms*. Vol. 12757. LNCS, pp. 469–484, Cham: Springer, 2021.

[RMLM21] Léo Robert, Daiki Miyahara, Pascal Lafourcade, and Takaaki Mizuki. "Interactive physical ZKP for connectivity: applications to Nurikabe and Hitori." In: *Connecting with Computability*. Ed. by Liesbeth De Mol, Andreas Weiermann, Florin Manea, and David Fernández-Duque. Vol. 12813. LNCS, pp. 373–384, Cham: Springer, 2021.

[OM21b] Hibiki Ono and Yoshifumi Manabe. "Minimum round card-based cryptographic protocols using private operations." *Cryptography* 5.3, 17 (2021).

[AMS21] Yuta Abe, Takaaki Mizuki, and Hideaki Sone. "Committed-format AND protocol using only random cuts." *Nat. Comput.* 20.4, 639–645 (2021).

[MO21c] Yoshifumi Manabe and Hibiki Ono. "Card-based cryptographic protocols with a standard deck of cards using private operations." In: *Theoretical Aspects of Computing – ICTAC 2021*. Ed. by Antonio Cerone and Peter Csaba Ölveczky. Vol. 12819. LNCS, pp. 256–274, Cham: Springer, 2021.

[RI21c] Suthee Ruangwises and Toshiya Itoh. "Securely computing the n-variable equality function with $2n$ cards." *Theor. Comput. Sci.* 887, 99–110 (2021).

[LMM$^+$21] Pascal Lafourcade, Daiki Miyahara, Takaaki Mizuki, Léo Robert, Tatsuya Sasaki, and Hideaki Sone. "How to construct physical zero-knowledge proofs for puzzles with a "single loop" condition." *Theor. Comput. Sci.* 888, 41–55 (2021).

[Koc21] Alexander Koch. "The landscape of security from physical assumptions." In: *IEEE Information Theory Workshop*, pp. 1–6, NY: IEEE, 2021.

[IMM21] Raimu Isuzugawa, Daiki Miyahara, and Takaaki Mizuki. "Zero-knowledge proof protocol for Cryptarithmetic using dihedral cards." In: *Unconventional Computation and Natural Computation*. Ed. by Irina Kostitsyna and Pekka Orponen. Vol. 12984. LNCS, pp. 51–67, Cham: Springer, 2021.

[RI21d] Suthee Ruangwises and Toshiya Itoh. "Physical ZKP for connected spanning subgraph: applications to Bridges puzzle and other problems." In: *Unconventional Computation and Natural Computation*. Ed. by Irina Kostitsyna and Pekka Orponen, pp. 149–163, Cham: Springer, 2021.

[ITS$^+$21] Raimu Isuzugawa, Kodai Toyoda, Yu Sasaki, Daiki Miyahara, and Takaaki Mizuki. "A card-minimal three-input AND protocol using two shuffles." In: *Computing and Combinatorics*. Ed. by Chi-Yeh Chen, Wing-Kai Hon, Ling-Ju Hung, and Chia-Wei Lee. Vol. 13025. LNCS, pp. 668–679, Cham: Springer, 2021.

[Rua21a] Suthee Ruangwises. "Two standard decks of playing cards are sufficient for a ZKP for Sudoku." In: *Computing and Combinatorics*. Ed. by Chi-Yeh Chen, Wing-Kai Hon, Ling-Ju Hung, and Chia-Wei Lee. Vol. 13025. LNCS, pp. 631–642, Cham: Springer, 2021.

[MHM21] Daiki Miyahara, Hiromichi Haneda, and Takaaki Mizuki. "Card-based zero-knowledge proof protocols for graph problems and their computational model." In: *Provable and Practical Security*. Ed. by Qiong Huang and Yu Yu. Vol. 13059. LNCS, pp. 136–152, Cham: Springer, 2021.

[Rua22a] Suthee Ruangwises. "Using five cards to encode each integer in Z/6Z." In: *Innovative Security Solutions for Information Technology and Communications*. Ed. by Peter Y.A. Ryan and Cristian Toma. Vol. 13195. LNCS, pp. 165–177, Cham: Springer, 2022.

[MUH$^+$21] Daiki Miyahara, Itaru Ueda, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone. "Evaluating card-based protocols in terms of execution time." *Int. J. Inf. Secur.* 20, 729–740 (5 2021).

[RI21e] Suthee Ruangwises and Toshiya Itoh. "Physical zero-knowledge proof for Ripple Effect." *Theor. Comput. Sci.* 895, 115–123 (2021).

[TMM21] Kodai Toyoda, Daiki Miyahara, and Takaaki Mizuki. "Another use of the five-card trick: card-minimal secure three-input majority function evaluation." In: *Progress in Cryptology—INDOCRYPT 2021*. Ed. by Avishek Adhikari, Ralf Küsters, and Bart Preneel. Vol. 13143. LNCS, pp. 536–555, Cham: Springer, 2021.

[Rua21b] Suthee Ruangwises. "An improved physical ZKP for Nonogram." In: *Combinatorial Optimization and Applications*. Ed. by Ding-Zhu Du, Donglei Du, Chenchen Wu, and Dachuan Xu. Vol. 13135. LNCS, pp. 262–272, Cham: Springer, 2021.

[Koc22] Alexander Koch. "The landscape of optimal card-based protocols." *Mathematical Cryptology* 1.2, 115–131 (2022).

[Miz22] Takaaki Mizuki. “Preface: special issue on card-based cryptography 2.” *New Gener. Comput.* 40, 47–48 (2022).

[Rua22b] Suthee Ruangwises. “Two standard decks of playing cards are sufficient for a ZKP for Sudoku.” *New Gener. Comput.* 40, 49–65 (2022).

[MO22] Yoshifumi Manabe and Hibiki Ono. “Card-based cryptographic protocols with malicious players using private operations.” *New Gener. Comput.* 40, 67–93 (2022).

[NMT$^+$22] Takeshi Nakai, Yuto Misawa, Yuuki Tokushige, Mitsugu Iwamoto, and Kazuo Ohta. “Secure computation for threshold functions with physical cards: power of private permutations.” *New Gener. Comput.* 40, 95–113 (2022).

[KW22] Alexander Koch and Stefan Walzer. “Private function evaluation with cards.” *New Gener. Comput.* 40, 115–147 (2022).

[RMLM22a] Léo Robert, Daiki Miyahara, Pascal Lafourcade, and Takaaki Mizuki. “Card-based ZKP for connectivity: applications to Nurikabe, Hitori, and Heyawake.” *New Gener. Comput.* 40, 149–171 (2022).

[ANK$^+$22] Yoshiki Abe, Takeshi Nakai, Yoshihisa Kuroki, Shinnosuke Suzuki, Yuta Koga, Yohei Watanabe, Mitsugu Iwamoto, and Kazuo Ohta. “Efficient card-based majority voting protocols.” *New Gener. Comput.* 40, 173–198 (2022).

[MS22] Kengo Miyamoto and Kazumasa Shinagawa. “Graph automorphism shuffles from pile-scramble shuffles.” *New Gener. Comput.* 40, 199–223 (2022).

[KM22a] Yuichi Komano and Takaaki Mizuki. “Coin-based secure computations.” *Int. J. Inf. Secur.* 21, 833–846 (2022).

[RML$^+$22] Léo Robert, Daiki Miyahara, Pascal Lafourcade, Luc Libralesso, and Takaaki Mizuki. “Physical zero-knowledge proof and NP-completeness proof of Suguru puzzle.” *Inf. Comput.* 285, 104858 (2022).

[MK22] Takaaki Mizuki and Yuichi Komano. “Information leakage due to operative errors in card-based protocols.” *Inf. Comput.* 285, 104910 (2022).

[KTMM22] Tomoki Kuzuma, Kodai Toyoda, Daiki Miyahara, and Takaaki Mizuki. “Card-based single-shuffle protocols for secure multiple-input AND and XOR computations.” In: *ACM ASIA Public-Key Cryptography Workshop*, pp. 51–58, NY: ACM, 2022.

[RI22a] Suthee Ruangwises and Toshiya Itoh. “How to physically verify a rectangle in a grid: a physical ZKP for Shikaku.” In: *Fun with Algorithms.* Ed. by Pierre Fraigniaud and Yushi Uno. Vol. 226. LIPIcs, pp. 24:1–24:12, Dagstuhl: Schloss Dagstuhl, 2022.

[Man22] Yoshifumi Manabe. “Card-based cryptographic protocols to calculate primitives of Boolean functions: survey.” *Int. J. Comput. Softw. Eng.* 7.1, 178 (2022).

[Sug22a] Yuji Suga. “A classification proof for commutative three-element semigroups with local AND structure and its application to card-based protocols.” In: *2022 IEEE International Conference on Consumer Electronics - Taiwan*, pp. 171–172, NY: IEEE, 2022.

[HHMM22] Rikuo Haga, Yuichi Hayashi, Daiki Miyahara, and Takaaki Mizuki. “Card-minimal protocols for three-input functions with standard playing cards.” In: *AFRICACRYPT 2022*. Ed. by Lejla Batina and Joan Daemen. Vol. 13503. LNCS, pp. 448–468, Cham: Springer, 2022.

[MM23] Daiki Miyahara and Takaaki Mizuki. “Secure computations through checking suits of playing cards.” In: *Frontiers in Algorithmics*. Ed. by Minming Li and Xiaoming Sun. Vol. 13461. LNCS, pp. 110–128, Cham: Springer, 2023.

[HTS$^+$22] Rikuo Haga, Kodai Toyoda, Yuto Shinoda, Daiki Miyahara, Kazumasa Shinagawa, Yuichi Hayashi, and Takaaki Mizuki. “Card-based secure sorting protocol.” In: *Advances in Information and Computer Security*. Ed. by Chen-Mou Cheng and Mitsuaki Akiyama. Vol. 13504. LNCS, pp. 224–240, Cham: Springer, 2022.

[RI22b] Suthee Ruangwises and Toshiya Itoh. “Physical ZKP for Makaro using a standard deck of cards.” In: *Theory and Applications of Models of Computation*. Ed. by Ding-Zhu Du, Donglei Du, Chenchen Wu, and Dachuan Xu. Vol. 13571. LNCS, pp. 43–54, Cham: Springer, 2022.

[RMLM22b] Léo Robert, Daiki Miyahara, Pascal Lafourcade, and Takaaki Mizuki. “Hide a liar: card-based ZKP protocol for Usowan.” In: *Theory and Applications of Models of Computation*. Ed. by Ding-Zhu Du, Donglei Du, Chenchen Wu, and Dachuan Xu. Vol. 13571. LNCS, pp. 201–217, Cham: Springer, 2022.

[STMM22] Hayato Shikata, Kodai Toyoda, Daiki Miyahara, and Takaaki Mizuki. “Card-minimal protocols for symmetric Boolean functions of more than seven inputs.” In: *Theoretical Aspects of Computing – ICTAC 2022*. Ed. by Helmut Seidl, Zhiming Liu, and Corina S. Pasareanu. Vol. 13572. LNCS, pp. 388–406, Cham: Springer, 2022.

[DON$^+$22] Anastasiia Doi, Tomoki Ono, Takeshi Nakai, Kazumasa Shinagawa, Yohei Watanabe, Koji Nuida, and Mitsugu Iwamoto. “Card-based cryptographic protocols for private set intersection.” In: *2022 International Symposium on Information Theory and Its Applications (ISITA)*, pp. 239–243, 2022.

[RMLM22c] Léo Robert, Daiki Miyahara, Pascal Lafourcade, and Takaaki Mizuki. "Card-based ZKP protocol for Nurimisaki." In: *Stabilization, Safety, and Security of Distributed Systems*. Ed. by Stéphane Devismes, Franck Petit, Karine Altisen, Giuseppe Antonio Di Luna, and Antonio Fernandez Anta. LNCS, pp. 285–298, Cham: Springer, 2022.

[Sug22b] Yuji Suga. "How to implement non-committed card protocols to realize AND operations satisfying the three-valued logics." In: *2022 Tenth International Symposium on Computing and Networking, CANDAR 2022 - Workshops, Himeji, Japan, November 21-24, 2022*, pp. 370–374, IEEE, 2022.

[KM22b] Yuichi Komano and Takaaki Mizuki. "Physical zero-knowledge proof protocol for Topswops." In: *Information Security Practice and Experience*. Ed. by Chunhua Su, Dimitris Gritzalis, and Vincenzo Piuri. Vol. 13620. LNCS, pp. 537–553, Cham: Springer, 2022.

[KM23] Yuichi Komano and Takaaki Mizuki. "Card-based zero-knowledge proof protocol for pancake sorting." In: *Innovative Security Solutions for Information Technology and Communications*. Ed. by Giampaolo Bella, Mihai Doinea, and Helge Janicke. Vol. 13809. LNCS, pp. 222–239, Cham: Springer, 2023.

[SSM23] Masahisa Shimano, Kazuo Sakiyama, and Daiki Miyahara. "Towards verifying physical assumption in card-based cryptography." In: *Innovative Security Solutions for Information Technology and Communications*. Ed. by Giampaolo Bella, Mihai Doinea, and Helge Janicke. Vol. 13809. LNCS, pp. 289–305, Cham: Springer, 2023.

[FM22] Takuro Fukasawa and Yoshifumi Manabe. "Card-based zero-knowledge proof for the nearest neighbor property: zero-knowledge proof of ABC end view." In: *Security, Privacy, and Applied Cryptography Engineering*. Ed. by Lejla Batina, Stjepan Picek, and Mainack Mondal. Vol. 13783. LNCS, pp. 147–161, Cham: Springer, 2022.

[SM23] Kazumasa Shinagawa and Kengo Miyamoto. "Automorphism shuffles for graphs and hypergraphs and its applications." *IEICE Trans. Fundam.* E106.A.3, 306–314 (2023).

[ANW$^+$23] Yoshiki Abe, Takeshi Nakai, Yohei Watanabe, Mitsugu Iwamoto, and Kazuo Ohta. "A computationally efficient card-based majority voting protocol with fewer cards in the private model." *IEICE Trans. Fundam.* 106.3, 315–324 (2023).

[TMM23] Kazunari Tozawa, Hiraku Morita, and Takaaki Mizuki. “Single-shuffle card-based protocol with eight cards per gate.” In: *Unconventional Computation and Natural Computation.* Ed. by Daniela Genova and Jarkko Kari. Vol. 14003. LNCS, pp. 171–185, Cham: Springer, 2023.

[Rua23a] Suthee Ruangwises. “An improved physical ZKP for Nonogram and Nonogram color.” *J. Comb. Optim.* 45, 122 (5 2023).

[Sug23a] Yuji Suga. “POSTER: A card-based protocol that lets you know how close two parties are in their opinions (agree/disagree) by using a four-point Likert scale.” In: *Applied Cryptography and Network Security Workshops.* Ed. by Jianying Zhou, Lejla Batina, Zengpeng Li, Jingqiang Lin, Eleonora Losiouk, Suryadipta Majumdar, Daisuke Mashima, Weizhi Meng, Stjepan Picek, Mohammad Ashiqur Rahman, Jun Shao, Masaki Shimaoka, Ezekiel O. Soremekun, Chunhua Su, Je Sen Teh, Aleksei Udovenko, Cong Wang, Leo Yu Zhang, and Yury Zhauniarovich. Vol. 13907. LNCS, pp. 716–721, Springer, 2023.

[Sug23b] Yuji Suga. “Security considerations for the fourth data over non-committed 3-valued card-based protocols.” In: *2023 International Technical Conference on Circuits/Systems, Computers, and Communications (ITC-CSCC)*, pp. 1–4, 2023.

[SMM23] Hayato Shikata, Daiki Miyahara, and Takaaki Mizuki. “Few-helping-card protocols for some wider class of symmetric Boolean functions with arbitrary ranges.” In: *ACM ASIA Public-Key Cryptography Workshop*, pp. 33–41, New York: ACM, 2023.

[Sug23c] Yuji Suga. “A classification for commutative three-element semigroups with local XOR structure and its implementability of card-based protocols.” In: *International Conference on Consumer Electronics - Taiwan, ICCE-Taiwan 2023*, pp. 543–544, IEEE, 2023.

[Rua23b] Suthee Ruangwises. “Physical zero-knowledge proof for ball sort puzzle.” In: *Unity of Logic and Computation.* Ed. by Gianluca Della Vedova, Besik Dundua, Steffen Lempp, and Florin Manea. Vol. 13967. LNCS, pp. 246–257, Cham: Springer, 2023.

[Rua23c] Suthee Ruangwises. “Physically verifying the first nonzero term in a sequence: physical ZKPs for ABC end view and Goishi Hiroi.” In: *Frontiers of Algorithmics.* Ed. by Minming Li, Xiaoming Sun, and Xiaowei Wu. Vol. 13933. LNCS, pp. 171–183, Cham: Springer, 2023.

[MMS23] Tomoya Morooka, Yoshifumi Manabe, and Kazumasa Shinagawa. “Malicious player card-based cryptographic protocols with a standard deck of cards using private operations.” In: *Information Security Practice and Experience.* Ed. by Weizhi Meng, Zheng Yan, and Vincenzo Piuri. Vol. 14341. LNCS, pp. 332–346, Singapore: Springer, 2023.

[Nui23] Koji Nuida. “Efficient card-based Millionaires’ protocols via non-binary input encoding.” In: *Advances in Information and Computer Security*. Ed. by Junji Shikata and Hiroki Kuzuno. Vol. 14128. LNCS, pp. 237–254, Cham: Springer, 2023.

[HKL$^+$23] Samuel Hand, Alexander Koch, Pascal Lafourcade, Daiki Miyahara, and Léo Robert. “Check alternating patterns: a physical zero-knowledge proof for Moon-or-Sun.” In: *Advances in Information and Computer Security*. Ed. by Junji Shikata and Hiroki Kuzuno. Vol. 14128. LNCS, pp. 255–272, Cham: Springer, 2023.

[Gui23] Luis Guillen. “The asymmetric five-card trick: working with variable encoding in card-based protocols.” *Journal of Cryptographic Engineering* 14, 181–192 (2023).

[RMLM23] Léo Robert, Daiki Miyahara, Pascal Lafourcade, and Takaaki Mizuki. “Physical ZKP protocols for Nurimisaki and Kurodoko.” *Theor. Comput. Sci.* 972, 114071 (2023).

[TM23] Kodai Tanaka and Takaaki Mizuki. “Two UNO decks efficiently perform zero-knowledge proof for Sudoku.” In: *Fundamentals of Computation Theory*. Ed. by Henning Fernau and Klaus Jansen. Vol. 14292. LNCS, pp. 406–420, Cham: Springer, 2023.

[Rua23d] Suthee Ruangwises. “Physical zero-knowledge proofs for Five Cells.” In: *Progress in Cryptology – LATINCRYPT 2023*. Ed. by Abdelrahaman Aly and Mehdi Tibouchi. Vol. 14168. LNCS, pp. 315–330, Cham: Springer, 2023.

[Sug23d] Yuji Suga. “Relationship between AND extension and XOR extension of 3-valued input with 2-party card-based protocols.” In: *2023 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia)*, pp. 1–4, New York: IEEE, 2023.

[YTN$^+$23] Takuto Yoshida, Kodai Tanaka, Keisuke Nakabayashi, Eikoh Chida, and Takaaki Mizuki. “Upper bounds on the number of shuffles for two-helping-card multi-input AND protocols.” In: *Cryptology and Network Security*. Ed. by Jing Deng, Vladimir Kolesnikov, and Alexander A. Schwarzmann. Vol. 14342. LNCS, pp. 211–231, Singapore: Springer, 2023.

[MS23] Yoshifumi Manabe and Kazumasa Shinagawa. “Free-XOR in card-based garbled circuits.” In: *Cryptology and Network Security*. Ed. by Jing Deng, Vladimir Kolesnikov, and Alexander A. Schwarzmann. Vol. 14342. LNCS, pp. 232–248, Singapore: Springer, 2023.

[OSN$^+$24] Tomoki Ono, Kazumasa Shinagawa, Takeshi Nakai, Yohei Watanabe, and Mitsugu Iwamoto. "Single-shuffle card-based protocols with six cards per gate." In: *Information Security and Cryptology.* Ed. by Hwajeong Seo and Suhri Kim. Vol. 14562. LNCS, pp. 157–169, Singapore: Springer, 2024.

[KMNS24] Kazuki Kanai, Kengo Miyamoto, Koji Nuida, and Kazumasa Shinagawa. "Uniform cyclic group factorizations of finite groups." *Communications in Algebra* 52.5, 2174–2184 (2024).

[Rua23e] Suthee Ruangwises. "The landscape of computing symmetric n-variable functions with 2n cards." In: *Theoretical Aspects of Computing – ICTAC 2023.* Ed. by Erika Ábrahám, Clemens Dubslaff, and Silvia Lizeth Tapia Tarifa. Vol. 14446. LNCS, pp. 74–82, Cham: Springer, 2023.

[HAA24] Kyosuke Hatsugai, Kyoichi Asano, and Yoshiki Abe. "A physical zero-knowledge proof for Sumplete, a puzzle generated by ChatGPT." In: *Computing and Combinatorics.* Ed. by Weili Wu and Guangmo Tong. Vol. 14422. LNCS, pp. 398–410, Cham: Springer, 2024.

[Rua24] Suthee Ruangwises. "Verifying the first nonzero term: physical ZKPs for ABC end view, Goishi Hiroi, and Toichika." *Journal of Combinatorial Optimization* 47.4, 69 (2024).

[ESM24] Reo Eriguchi, Kazumasa Shinagawa, and Takao Murakami. "Card-based cryptography meets differential privacy." In: *Fun with Algorithms.* Ed. by Andrei Z. Broder and Tami Tamir. Vol. 291. LIPIcs, pp. 12:1–12:20, Dagstuhl, Germany: Schloss Dagstuhl, 2024.

[SKMN24] Kazumasa Shinagawa, Kazuki Kanai, Kengo Miyamoto, and Koji Nuida. "How to covertly and uniformly scramble the 15 puzzle and rubik's cube." In: *Fun with Algorithms.* Ed. by Andrei Z. Broder and Tami Tamir. Vol. 291. LIPIcs, pp. 30:1–30:15, Dagstuhl, Germany: Schloss Dagstuhl, 2024.

[ROA$^+$24] Suthee Ruangwises, Tomoki Ono, Yoshiki Abe, Kyosuke Hatsugai, and Mitsugu Iwamoto. "Card-based overwriting protocol for equality function and applications." In: *Unconventional Computation and Natural Computation.* Ed. by Da-Jung Cho and Jongmin Kim. Vol. 14776. LNCS, pp. 18–27, Cham: Springer, 2024.

[ISSM24] Yuki Ito, Hayato Shikata, Takuo Suganuma, and Takaaki Mizuki. "Card-based cryptography meets 3D printer." In: *Unconventional Computation and Natural Computation.* Ed. by Da-Jung Cho and Jongmin Kim. Vol. 14776. LNCS, pp. 74–88, Cham: Springer, 2024.

[TSSM24] Yoshihiro Takahashi, Kazumasa Shinagawa, Hayato Shikata, and Takaaki Mizuki. “Efficient card-based protocols for symmetric functions using four-colored decks.” In: *ACM ASIA Public-Key Cryptography Workshop*, pp. 1–10, New York: ACM, 2024.

[TSM24] Yuma Tamura, Akira Suzuki, and Takaaki Mizuki. “Card-based zero-knowledge proof protocols for the 15-puzzle and the token swapping problem.” In: *ACM ASIA Public-Key Cryptography Workshop*, pp. 11–22, New York: ACM, 2024.

[SMM25a] Kazumasa Shinagawa, Daiki Miyahara, and Takaaki Mizuki. “How to play old maid with virtual players.” In: *Frontiers of Algorithmics*. Ed. by Bo Li, Minming Li, and Xiaoming Sun. Vol. 14752. LNCS, pp. 53–65, Singapore: Springer, 2025.

[MS24] Yuta Minamikawa and Kazumasa Shinagawa. “Coin-based cryptographic protocols without hand operations.” *IEICE Trans. Fundamentals* E107.A.8, 1178–1185 (2024).

[OFF24] Taisei Otsuji, Peter Fulla, and Takuro Fukunaga. “NP-Completeness and physical zero-knowledge proof of Hotaru Beam.” In: *Computing and Combinatorics*. Ed. by Yong Chen, Xiaofeng Gao, Xiaoming Sun, and An Zhang, pp. 239–251, Singapore: Springer, 2024.

[HRAA24] Kyosuke Hatsugai, Suthee Ruangwises, Kyoichi Asano, and Yoshiki Abe. “NP-completeness and physical zero-knowledge proofs for Sumplete, a puzzle generated by ChatGPT.” *New Gener. Comput.* 42, 429–448 (2024).

[KM24] Yuichi Komano and Takaaki Mizuki. “Physical zero-knowledge proof protocols for Topswops and Botdrops.” *New Gener. Comput.* 42, 399–428 (2024).

[SS24] Shun Sasaki and Kazumasa Shinagawa. “Physical zero-knowledge proof for Sukoro.” *New Gener. Comput.* 42, 381–398 (2024).

[RI24] Suthee Ruangwises and Mitsugu Iwamoto. “Printing protocol: physical ZKPs for decomposition puzzles.” *New Gener. Comput.* 42, 331–343 (2024).

[TS24] Yoshihiro Takahashi and Kazumasa Shinagawa. “Extended addition protocol and efficient voting protocols using regular polygon cards.” *New Gener. Comput.* 42, 479–496 (2024).

[HKL$^+$24] Samuel Hand, Alexander Koch, Pascal Lafourcade, Daiki Miyahara, and Léo Robert. “Efficient card-based ZKP for single loop condition and its application to Moon-or-Sun.” *New Gener. Comput.* 42, 449–477 (2024).

[DOA$^+$24] Anastasiia Doi, Tomoki Ono, Yoshiki Abe, Takeshi Nakai, Kazumasa Shinagawa, Yohei Watanabe, Koji Nuida, and Mitsugu Iwamoto. “Card-based protocols for private set intersection and union.” *New Gener. Comput.* 42, 359–380 (2024).

[NIO$^+$24] Takeshi Nakai, Keita Iwanari, Tomoki Ono, Yoshiki Abe, Yohei Watanabe, and Mitsugu Iwamoto. “Card-based cryptography with a standard deck of cards, revisited: efficient protocols in the private model.” *New Gener. Comput.* 42, 345–358 (2024).

[MO24] Yoshifumi Manabe and Hibiki Ono. “Card-based cryptographic protocols with a standard deck of cards using private operations.” *New Gener. Comput.* 42, 305–329 (2024).

[Miz24] Takaaki Mizuki. “Preface: special issue on card-based cryptography 3.” *New Gener. Comput.* 42, 303–304 (2024).

[HS24] Yoshiaki Honda and Kazumasa Shinagawa. “Efficient card-based protocols with a standard deck of playing cards using partial opening.” In: *Advances in Information and Computer Security.* Ed. by Kazuhiko Minematsu and Mamoru Mimura. Vol. 14977. LNCS, pp. 85–100, Singapore: Springer, 2024.

[KNS24] Kota Kato, Takeshi Nakai, and Koutarou Suzuki. “Card-based secure sorting protocols based on the sorting networks.” In: *Advanced Informatics: Concept, Theory and Application (ICAICTA)*, pp. 1–6, NY: IEEE, 2024.

[KLM$^+$25a] Shohei Kaneko, Pascal Lafourcade, Lola-Baie Mallordy, Daiki Miyahara, Maxime Puys, and Kazuo Sakiyama. “Balance-based ZKP protocols for pencil-and-paper puzzles.” In: *Information Security.* Ed. by Nicky Mouha and Nick Nikiforakis. Vol. 15257. LNCS, pp. 211–231, Cham: Springer, 2025.

[OK25a] Shun Odaka and Yuichi Komano. “Card-based arithmetic operations and application to statistical data aggregation.” In: *Innovative Security Solutions for Information Technology and Communications.* Ed. by Luciana Morogan, Peter Roenne, and Ion Bica. Vol. 15595. LNCS, pp. 118–134, Cham: Springer, 2025.

[Shi25] Kazumasa Shinagawa. “Card-based protocols with single-card encoding.” In: *Theoretical Aspects of Computing.* Ed. by Chutiporn Anutariya and Marcello M. Bonsangue. Vol. 15373. LNCS, pp. 182–194, Cham: Springer, 2025.

[MRLM24] Daiki Miyahara, Léo Robert, Pascal Lafourcade, and Takaaki Mizuki. “ZKP protocols for Usowan, Herugolf, and Five Cells.” *Tsinghua Science and Technology* 29.6, 1651–1666 (2024).

[KLM$^+$25b] Shohei Kaneko, Pascal Lafourcade, Lola-Baie Mallordy, Daiki Miyahara, Maxime Puys, and Kazuo Sakiyama. “Secure voting protocol using balance scale.” In: *Foundations and Practice of Security.* Ed. by Kamel Adi, Simon Bourdeau, Christel Durand, Valérie Viet Triem Tong, Alina Dulipovici, Yvon Kermarrec, and Joaquín García-Alfaro. Vol. 15532. LNCS, pp. 365–376, Cham: Springer, 2025.

[TMM25] Kazunari Tozawa, Hiraku Morita, and Takaaki Mizuki. "Single-shuffle card-based protocol with eight cards per gate and its extensions." *Natural Computing* 24.1, 131–147 (2025).

[TSSM25] Kodai Tanaka, Shun Sasaki, Kazumasa Shinagawa, and Takaaki Mizuki. "Only two shuffles perform card-based zero-knowledge proof for Sudoku of any size." In: *2025 Symposium on Simplicity in Algorithms (SOSA)*, pp. 94–107, SIAM, 2025.

[Rua25a] Suthee Ruangwises. "NP-completeness and physical zero-knowledge proofs for Zeiger." In: *WALCOM: Algorithms and Computation*. Ed. by Shin-ichi Nakano and Mingyu Xiao. Vol. 15411. LNCS, pp. 312–325, Singapore: Springer, 2025.

[SN25a] Kazumasa Shinagawa and Koji Nuida. "Card-based protocols imply PSM protocols." In: *Theoretical Aspects of Computer Science*. Ed. by Olaf Beyersdorff, Michał Pilipczuk, Elaine Pimentel, and Nguyên Kim Thàng. Vol. 327. LIPIcs, pp. 72:1–72:18, Dagstuhl: Schloss Dagstuhl, 2025.

[SMM25b] Kazumasa Shinagawa, Daiki Miyahara, and Takaaki Mizuki. "How to play Old Maid with virtual players." *Theory of Computing Systems* 69.1, 13 (2025).

[IO25] Chuzo Iwamoto and Kosuke Ohara. "Card-based zero-knowledge proof for Dosun-Fuwari." *IEICE Trans. Fundam.* E108-A.9, 1206–1210 (2025).

[KM25a] Naoki Kobayashi and Yoshifumi Manabe. "Card-based cryptographic protocols for three-input functions with a standard deck of cards using private operations." In: *Data Privacy Management*. Ed. by Joaquin Garcia-Alfaro, Ken Barker, and Guillermo Navarro-Arribas. Vol. 15263. LNCS, pp. 94–111, Cham: Springer, 2025.

[Sug25] Yuji Suga. "Card protocols that allow you to switch cards to Mahjong tiles." *Journal of Information Processing* 33, 276–283 (2025).

[KM25b] Naoki Kobayashi and Yoshifumi Manabe. "Card-based secure evaluation of decision trees." In: *Risks and Security of Internet and Systems*. Ed. by Simon Collart-Dutilleul, Samir Ouchani, Nora Cuppens, and Frédéric Cuppens. Vol. 15456. LNCS, pp. 24–39, Cham: Springer, 2025.

[Rua25b] Suthee Ruangwises. "Tatami printer: physical ZKPs for Tatami puzzles." In: *Algorithms and Complexity*. Ed. by Irene Finocchi and Loukas Georgiadis. Vol. 15679. LNCS, pp. 105–118, Cham: Springer, 2025.

[OK25b] Shun Odaka and Yuichi Komano. “Card-based arithmetic operations using integer commitments and their application to statistical data aggregation.” *IEICE Trans. Fundam.* E109-A.3, 2025CIP0006 (2025).

[ORA$^+$25] Tomoki Ono, Suthee Ruangwises, Yoshiki Abe, Kyosuke Hatsugai, and Mitsugu Iwamoto. “Single-shuffle physical zero-knowledge proof for Sudoku using interactive inputs.” In: *ACM ASIA Public-Key Cryptography Workshop.* Ed. by Keita Emura and Hiraku Morita, pp. 1–8, New York: ACM, 2025.

[FISY25] Kazuhiro Fujita, Shota Ikeda, Kazumasa Shinagawa, and Kazuki Yoneyama. “Formal verification and proof of impossibility for four-card XOR protocols using only random cuts.” In: *ACM ASIA Public-Key Cryptography Workshop.* Ed. by Keita Emura and Hiraku Morita, pp. 9–16, New York: ACM, 2025.

[RS26] Suthee Ruangwises and Kazumasa Shinagawa. “Simulating virtual players for UNO without computers.” In: *Unconventional Computation and Natural Computation.* Ed. by Enrico Formenti and Luca Manzoni. Vol. 16364. LNCS, pp. 33–46, Cham: Springer, 2026.

[Rua26] Suthee Ruangwises. “Balance-based cryptography: physically computing any Boolean function.” In: *Unconventional Computation and Natural Computation.* Ed. by Enrico Formenti and Luca Manzoni. Vol. 16364. LNCS, pp. 63–72, Cham: Springer, 2026.

[MKH$^+$26] Takaaki Mizuki, Tomoki Kuzuma, Tomoya Hirano, Ririn Oshima, and Momofuku Yasuda. “Gakmoro: an application of physical secure computation to card game.” In: *Unconventional Computation and Natural Computation.* Ed. by Enrico Formenti and Luca Manzoni. Vol. 16364. LNCS, pp. 344–360, Cham: Springer, 2026.

[SN25b] Kazumasa Shinagawa and Koji Nuida. “Card-based protocols imply PSM protocols.” In: *42nd International Symposium on Theoretical Aspects of Computer Science (STACS 2025).* Ed. by Olaf Beyersdorff, Michal Pilipczuk, Elaine Pimentel, and Kim Thang Nguyen. Vol. 327. LIPIcs, pp. 72:1–72:18, Dagstuhl: Schloss Dagstuhl, 2025.

[IS26] Shota Ikeda and Kazumasa Shinagawa. “How to play Mastermind without game master.” In: *Theory and Applications of Models of Computation.* Ed. by Min Li, Mingji Xia, and Peng Zhang. Vol. 16084. LNCS, pp. 109–120, Singapore: Springer, 2026.

[ESM25] Reo Eriguchi, Kazumasa Shinagawa, and Takao Murakami. “Visualizing differentially private mechanisms with physical cards.” *Theor. Comput. Sci.* 1055, 115492 (2025).

[SN25c] Kazumasa Shinagawa and Koji Nuida. “Cyclic equalizability of words and its application to card-based cryptography.” In: *Fundamentals of Computation Theory.* Ed. by Artur Jez and Jan Otop. Vol. 16106. Lecture Notes in Computer Science, pp. 406–419, Singapore: Springer, 2025.

[Nui25] Koji Nuida. “Card-based protocol counting connected components of graphs.” *New Gener. Comput.* 43, 18 (2025).

[SK25] Takumi Sakurai and Yuichi Kaji. “General conversion scheme of card-based protocols for two-colored cards to updown cards.” In: *Emerging Security Information, Systems and Technologies (SECURWARE 2025)*, pp. 33–39, Wilmington: IARIA, 2025.

[IIS$^+$25] Shizuru Iino, Shota Ikeda, Kazumasa Shinagawa, Yang Li, Kazuo Sakiyama, and Daiki Miyahara. “Impossibility of four-card AND protocols with a single closed shuffle.” In: *Cryptology and Network Security.* Ed. by Yongdae Kim, Atsuko Miyaji, and Mehdi Tibouchi. Vol. 16351. LNCS, pp. 213–229, Singapore: Springer, 2025.

[HS25] Yoshiaki Honda and Kazumasa Shinagawa. “Efficient three-input and four-input AND protocols using playing cards with partial-open actions.” In: *Cryptology and Network Security.* Ed. by Yongdae Kim, Atsuko Miyaji, and Mehdi Tibouchi. Vol. 16351. LNCS, pp. 199–212, Singapore: Springer, 2025.

[IS25] Shunnosuke Ikeda and Kazumasa Shinagawa. “Impossibility results of card-based protocols via mathematical optimization.” In: *Information Security and Cryptology.* LNCS, Singapore: Springer, 2025.

[ITSN25] Shota Ikeda, Yoshihiro Takahashi, Kazumasa Shinagawa, and Koji Nuida. “Efficient card-based protocols for symmetric and partially doubly symmetric functions.” In: *Advances in Information and Computer Security.* Ed. by Carlos Cid and Naoto Yanai. Vol. 16208. LNCS, pp. 189–209, Singapore: Springer, 2025.

[Iwa25] Atsushi Iwasaki. “Minimum number of up-down cards for finite-time committed-AND protocol without interlocking operations.” In: *Advances in Information and Computer Security.* Ed. by Carlos Cid and Naoto Yanai. Vol. 16208. LNCS, pp. 210–226, Singapore: Springer, 2025.

[ILSM26] Shizuru Iino, Yang Li, Kazuo Sakiyama, and Daiki Miyahara. “An n-card threshold protocol is impossible.” In: *2026 IEEE 16th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 1181–1187, NY: IEEE, 2026.

[KM26] Yuichi Komano and Takaaki Mizuki. “Card-based zero-knowledge proof protocols for pancake sorting.” *IEICE Trans. Fundam.* E109.A.3, 371–382 (2026).

[Koc19] Alexander Koch. “Cryptographic protocols from physical assumptions.” PhD thesis, Karlsruhe Institute of Technology, 2019.

[Shi20] Kazumasa Shinagawa. “On the construction of easy to perform card-based protocols.” PhD thesis, Tokyo Institute of Technology, 2020.

[Miy21] Daiki Miyahara. “Basing cryptographic protocols on physical objects.” PhD thesis, Tohoku University, 2021.

[Nak21] Takeshi Nakai. “Private permutations in card-based cryptography.” PhD thesis, The University of Electro-Communications, 2021.

[Dvo21] Pavel Dvořák. “Limits of data structures, communication, and cards.” PhD thesis, Charles University, 2021.

[Abe23] Yoshiki Abe. “Physically implemented multiparty computation without randomness.” PhD thesis, The University of Electro-Communications, 2023.