Publication List

Journal Paper

1. Andrej Bogdanov, Akinori Kawachi, and Hidetoki Tanaka, "Hard Functions for Low-Degree Polynomials over Prime Fields," ACM Transactions on Computation Theory, to appear.
2. Akinori Kawachi, Takeshi Koshiba, Harumichi Nishimura, and Tomoyuki Yamakami, "Computational Indistinguishability between Quantum States and Its Cryptographic Application," Journal of Cryptology 25(3): 528–555, 2012.
3. Akinori Kawachi, Hidetoki Tanaka, and Osamu Watanabe, "Estimating the Gowers Norm of Modulo Functions over Prime Fields," IEICE transactions on Information and Systems 95-D(3): 755–762, 2012.
4. Barış Aydınlıoğlu, Dan Gutfreund, John Hitchcock, and Akinori Kawachi, "Derandomizing Arthur-Merlin Games and Approximate Counting Implies Exponential-Size Lower Bounds," Computational Complexity 20(2): 329–366, 2011. Special issue dedicated to selected CCC'10 papers.
5. Akinori Kawachi and Tomoyuki Yamakami, "Quantum Hardcore Functions by Complexity-Theoretical Quantum List Decoding," SIAM Journal on Computing, Volume 39, Issue 7, pp.2941–2969, 2010.
6. Masahito Hayashi, Akinori Kawachi, and Hirotada Kobayashi, "Quantum Measurements for Hidden Subgroup Problems with Optimal Sample Complexity," Quantum Information and Computation Journal, Vol 8, pp.345–358, 2008.
7. Andris Ambainis, Kazuo Iwama, Akinori Kawachi, Rudy Raymond, and Shigeru Yamashita, "Improved Algorithms for Quantum Identification of Boolean Oracles," Theoretical Computer Science, Vol.378, pp.41–53, 2007.
8. Akinori Kawachi and Koshiba Takeshi, "Progress in Quantum Computational Cryptography," Journal of Universal Computer Science, Vol.12, No.6, pp.691–709, 2006.
9. Akinori Kawachi and Takeshi Koshiba, "Quantum Computational Cryptography," Topics in Applied Physics, Vol.102, pp.167–184, 2006.
10. Andris Ambainis, Kazuo Iwama, Akinori Kawachi, Rudy Raymond, and Shigeru Yamashita, "Quantum Identification of Boolean Oracles," Topics in Applied Physics, Vol.102, pp.3–18, 2006.
11. Akinori Kawachi, Hirotada Kobayashi, Takeshi Koshiba, and Raymond H. Putra, "Universal Test for Quantum One-Way Permutations," Theoretical Computer Science, Vol.345 Issues 2-3 No.22, pp.370–385, 2005.
12. Kazuo Iwama, Akinori Kawachi, and Shigeru Yamashita, "Quantum Biased Oracles", IPSJ Journal, Vol.46 No.10, 2400–2408, 2005.
13. Akinori Kawachi, Hirotada Kobayashi, Takeshi Koshiba, and Raymond H. Putra, "Universal Test for Quantum One-Way Permutations," Theoretical Computer Science, Vol.345, No.2-3, pp.370–385, 2005.
14. Kazuo Iwama, Akinori Kawachi, and Shigeru Yamashita, "Quantum Sampling for Balanced Allocations," IEICE transactions on Information and Systems, Vol.E88-D No.1, pp.47–52, 2005.
15. Kazuo Iwama and Akinori Kawachi, "Compact Routing with Stretch Factor of Less Than Three," IEICE transactions on Information and Systems, Vol.E88-D No.1, pp.39–46, 2005.

16. Kazuo Iwama and Akinori Kawachi, "A New Quantum Claw-Finding Algorithm for Three Functions," New Generation Computing, 21(4), pp.319–327, 2003.

Conference Paper (Refereed)

1. Akinori Kawachi, Hirotoshi Takebe, and Keisuke Tanaka, "Symmetric-Key Encryption Scheme with Multi-Ciphertext Non-Malleability," Proceedings of the 7th International Workshop on Security (IWSEC 2012), pp.123–137, 2012.
2. Andrej Bogdanov, Akinori Kawachi, and Hidetoki Tanaka, "Hard Functions for Low-Degree Polynomials over Prime Fields," Proceedings of the 36th International Symposium on Mathematical Foundations of Computer Science (MFCS 2011), Lecture Notes in Computer Science 6907, pp.120–131, 2011.
3. Akinori Kawachi, Christopher Portmann, and Keisuke Tanaka, "Characterization of the Relations between Information-Theoretic Non-Malleability, Secrecy, and Authenticity," Proceedings of the 5th International Conference on Information Theoretic Security (ICITS 2011), LNCS 6673, pp.6–24, 2011.
4. Dan Gutfreund and Akinori Kawachi, "Derandomizing Arthur-Merlin Games and Approximate Counting Implies Exponential-Size Lower Bounds," Proceedings of the 25th IEEE Conference on Computational Complexity (CCC 2010), pp.38–49, 2010.
5. Akinori Kawachi, Keisuke Tanka, Akira Numayama and Keita Xagawa, "Security of Encryption Schemes in Weakened Random Oracles," Proceedings of the 13th International Conference on Theory and Practice of Public-Key Cryptography (PKC 2010), LNCS 6056, pp.403–419, 2010.
6. Akinori Kawachi, Keisuke Tanaka and Keita Xagawa, "Concurrently Secure Identification Schemes Based on the Worst-Case Hardness of Lattice Problems," Proceedings of the 14th Annual International Conference on the Theory and Application of Cryptology & Information Security (Asiacrypt 2008), LNCS 5350, pp.372–389, 2008.
7. Akinori Kawachi and Christopher Portmann, "On the Power of Quantum Encryption Keys," Proceedings of the 2nd International Workshop on Post-Quantum Cryptography (PQCrypto 2008), LNCS 5299, pp.165–180, 2008.
8. Akinori Kawachi, Keisuke Tanaka and Keita Xagawa, "Multi-Bit Cryptosystems Based on Lattice Problems," Proceedings of the 10th International Conference on Theory and Practice of Public-Key Cryptography (PKC 2007), LNCS 4450, pp.315–329, 2007.
9. Akinori Kawachi and Tomoyuki Yamakami, "Quantum Hardcore Functions by Complexity-Theoretical Quantum List Decoding," Proceedings of the 33rd International Colloquium on Automata, Languages and Programming (ICALP 2006), LNCS 4052, pp.216–227, 2006.
10. Andris Ambainis, Kazuo Iwama, Akinori Kawachi, Rudy Raymond, and Shigeru Yamashita, "Improved Algorithms for Quantum Identification of Boolean Oracles," Proceedings of the 10th Scandinavian Workshop on Algorithm Theory (SWAT 2006), LNCS 4059, pp.280–291, 2006.
11. Akinori Kawachi, Takeshi Koshiba, Harumichi Nishimura, and Tomoyuki Yamakami, "Computational Indistinguishability between Quantum States and Its Cryptographic Application," Advances in Cryptography – Eurocrypt 2005, LNCS 3494, pp.268–284, 2005.
12. Kazuo Iwama and Akinori Kawachi, "Approximated Two Choices in Randomized Load Balancing," Proceedings of the Fifteenth International Symposium on Algorithms and Computation

(ISAAC 2004), Lecture Notes in Computer Science 3341, pp.545–557, 2004.

13. Akinori Kawachi, Hirotada Kobayashi, Takeshi Koshiba, and Raymond H. Putra, "Universal Test for Quantum One-Way Permutations," Proceedings of the Twenty-Ninth International Symposium on Mathematical Foundations of Computer Science (MFCS 2004), Lecture Notes in Computer Science 3153, pp.839–850, 2004.
14. Andris Ambainis, Kazuo Iwama, Akinori Kawachi, Hiroyuki Masuda, Raymond H. Putra, and Shigeru Yamashita, "Quantum Identification of Boolean Oracles," Proceedings of the Twenty-First Symposium on Theoretical Aspects of Computer Science (STACS 2004), Lecture Notes in Computer Science 2996, pp.105–116, 2004.
15. Akinori Kawachi, Hirotada Kobayashi, Takeshi Koshiba, and Raymond H. Putra, "A Characterization of Quantum One-Way Permutations," Proceedings of ERATO Conference on Quantum Information Science (EQIS 2003), pp.153, 2003.
16. Akinori Kawachi, Takeshi Koshiba, Harumichi Nishimura, and Tomoyuki Yamakami, "A Quantum Trapdoor One-Way Function that Relies on the Hardness of the Graph Automorphism Problem," Proceedings of ERATO Conference on Quantum Information Science (EQIS 2003), pp.115, 2003.
17. Kazuo Iwama, Akinori Kawachi, and Shigeru Yamashita, "Quantum Sampling for Balanced Allocations," Proceedings of the Ninth International Computing and Combinatorics Conference (COCOON 2003), Lecture Notes in Computer Science 2697, pp.304–318, 2003.
18. Kazuo Iwama and Akinori Kawachi, "Compact Routing with Stretch Factor of Less Than Three," Proceedings of the Twelfth IASTED International Conference on Parallel and Distributed Computing and Systems (PDCS 2000), pp.223–228, 2000.
19. Kazuo Iwama and Akinori Kawachi, "Brief Announcement: Compact Routing with Stretch Factor of Less Than Three," Proceedings of the Nineteenth ACM Symposium on Principles of Distributed Computing (PODC 2000), p.337, 2000.

Book (Chapter)

1. Andris Ambainis, Kazuo Iwama, Akinori Kawachi, Rudy H. Putra, and Shigeru Yamashita, "Quantum Oracle Identification," Eds. Hiroshi Imai and Masahito Hayashi, Quantum Computation and Information, Springer, 2006.
2. Akinori Kawachi and Takeshi Koshiba, "Quantum Computational Cryptography," Eds. Hiroshi Imai and Masahito Hayashi, Quantum Computation and Information, Springer, 2006.

Talk

1. Akinori Kawachi, "A Computational Perspective on Pseudorandomness," The 1st ETH-Japan Workshop on Science and Computing, Invited Talk, Mar., 2012.
2. Akinori Kawachi, "Quantum Proofs for Classical Cryptography," The 5th Asia Pacific Conference in Quantum Information Science, Invited Talk, Aug., 2010.
3. Akinori Kawachi, "Pseudorandomness of the Legendre Sequences and Robust Quantum State Decoding,"International Conference on Quantum Information and Technology, Invited Talk, Dec., 2009.

4. Akinori Kawachi, "Othogonality of Boolean Functions and Quantum Computation," Workshop on Theory of Quantum Computation, Communication, and Cryptography, Invited Talk, Feb., 2006.