SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

New Post-Quantum Digital Signature Scheme based on MinRank Problem

Bagus Santoso * Yasuhiko Ikematsu† Shuhei Nakamura ‡ Takanori Yasuda §

Keywords: MinRank problem, Signature scheme

Abstract

In Asiacrypt 2001, Courtois [1] proposed the first three-pass zero-knowledge identification (ID) scheme based on the MinRank problem. However, in Courtois' basic ID scheme, the cheating probability, i.e., the success probability of cheating prover, is 2/3, which is larger than half. Based on our modification [3] of Curtois' ID scheme into a three-pass ID scheme with cheating probability of 1/2, we propose a new digital signature scheme based on MinRank problem. Our scheme is constructed based on the Fiat-Shamir paradigm for post-quantum lossy ID scheme which are proposed by Kiltz et al. at Eurocrypt 2018 [2]. Therefore, our scheme also inherits the provable security under chosen message attacks against quantum adversaries.

References

[1] Nicolas T. Courtois. Efficient zero-knowledge authentication based on a linear algebra problem minrank. In ASIACRYPT, pages 402–421. Springer, 2001.

[2] Eike Kiltz, Vadim Lyubashevsky, Christian Schaffner. A Concrete Treatment of Fiat-Shamir Signatures in the Quantum Random-Oracle Model. In EUROCRYPT 2018, pages 552-586. Springer, 2018.

[3] Bagus Santoso, Yasuhiko Ikematsu, Shuhei Nakamura and Takanori Yasuda. MinRank Based Three-Pass Identification Scheme with Half Cheating Probability. In Computer Security Symposium (CSS) 2021.

* Department of Computer and Network Engineering, The University of Electro-Communications, 1-5-1 Chofugaoka, Chofu, Tokyo 182-8585, Japan (Email: santoso.bagus@uec.ac.jp)

† Institute of Mathematics for Industry, Kyushu University 744, Motooka, Nishi-ku, Fukuoka 819–0395, Japan. ikematsu@imi.kyushu-u.ac.jp

‡ Department of Liberal Arts and Basic Sciences, Nihon University, 1-2-1 Izumi-cho, Narashino, Chiba 275-8575, Japan. nakamura.shuhei@nihon-u.ac.jp

§ Institute for the Advancement of Higher Education, Okayama University of Science, 1-1 Ridaicho, Kitaku, Okayama 700-0005, Japan (Email: tyasuda@bme.ous.ac.jp)