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

Malicious Private Key Generators in Identity-Based Authenticated Key Exchange

Kazuma Wariki * Atsushi Fujioka † Taroh Sasaki † Kazuki Yoneyama ‡
Yuki Okano § Akira Nagai § Koutarou Suzuki ¶

Keywords: Identity-based authenticated key exchange, id-eCK model, Malicious private key generator.

Abstract

This paper proposes two security models in identity-based authenticated key exchange (IBAKE): the id-neCK security model captures a malicious act where an adversary can obtain the random string to generate a pair of master public and secret keys, and the id-reCK one does an act where an adversary can replace the master public key generated by the honest private key generator.

Then, we prove that both security notions are stronger than or equal to the id-eCK security [1] one, and that the id-reCK security notion is strictly stronger than the id-neCK security one. The latter means that the id-reCK security notion is the strictly strongest among three.

In addition, we prove that there exists an id-reCK secure IBAKE protocol under the asymmetric gap Bilinear Diffie–Hellman (BDH) assumption in the random oracle model (ROM). Also, we show that there exists an id-eCK secure IBAKE protocol under the asymmetric gap BDH assumption in the ROM, and that it is not id-neCK secure. These support that the id-neCK security notion is strictly stronger than the id-eCK security one under the mathematical assumption.

That is, we have the followings:

Theorem 1. When a protocol is id-neCK secure, it is id-eCK secure, also.

Theorem 2. When a protocol is id-reCK secure, it is id-neCK secure, also.

Theorem 3. There exists a protocol which is id-neCK secure but not id-reCK secure.

Theorem 4. There exists a protocol which is id-eCK secure (in the random oracle model under the assumption) but not id-neCK secure.

To prove this, we use a protocol, modifiedFSU, shown in [2] as a witness.

Theorem 5. There exists a protocol which is id-reCK secure (in the random oracle model under the assumption).

To prove this, we use a protocol, FSU, shown in [3] as a witness.

The above thorems imply that the proposed security notions are stronger than or equal to the id-eCK security one, and that the id-reCK security notion is strictly stronger than the id-neCK security one. In addition, there exists a protocol which satisfies the strongest security notion.

References

[1] H. Huang, et al, "An ID-based authenticated key exchange protocol based on bilinear Diffie-Hellman", ASIACCS09, pp. 333-342 (March, 2009).

[2] 割木 寿将, 藤岡 淳, 佐々木 太良, 鈴木 幸太郎, 富田 潤一, "IoT 機器向け ID ベース認証鍵交換と不正な PKG に対する安全性", 信学技報, Vol. 120, No. 28, pp. 55-61 (2020 年 5 月).

[3] A. Fujioka, F. Hoshino, T. Kobayashi, K. Suzuki, B. Ustaoğlu, and K. Yoneyama, "id-eCK Secure ID-based Authenticated Key Exchange on Symmetric Pairing and its Extension to Asymmetric Case", IEICE Transactions on Fundamentals, Vol. E96-A, No. 6, pp. 1139–1155 (June, 2013).

* Kanagawa University Graduate School, 3-27-1, Rokkakubashi, Kanagawa-ku, Yokohama-shi, Kanagawa 221-8686, Japan. r202170168pg@jindai.jp
† Kanagawa University, 3-27-1, Rokkakubashi, Kanagawa-ku, Yokohama-shi, Kanagawa 221-8686, Japan.
‡ Ibaraki University, 4-12-1, Nakanarusawa, Hitachi-shi, Ibaraki 316-8511, Japan
§ NTT Social Informatic Laboratories, 3-9-11, Midoricho, Musashino-shi, Tokyo 180-8585, Japan.
¶ Toyohashi University of Technology, 1–1, Hibarigaoka, Tenpaku-cho, Toyohashi-shi, Aichi 441-8580, Japan.