Endo, Kosei; **Kunihiro, Noboru**

On the security proof of an authentication protocol from Eurocrypt 2011. (English)

Zbl 1417.94094

Yoshida, Maki (ed.) et al., Advances in information and computer security. 9th international workshop on security, IWSEC 2014, Hirosaki, Japan, August 27–29, 2014. Proceedings. Berlin: Springer. Lect. Notes Comput. Sci. 8639, 187-203 (2014).

Summary: This paper discusses the security of one of authentication protocols proposed by *E. Kiltz* et al. [Eurocrypt 2011, Lect. Notes Comput. Sci. 6632, 7–26 (2011; Zbl 1281.94083); J. Cryptology 30, No. 4, 1238–1275 (2017; Zbl 1386.94096)]. Kiltz et al. claimed that the protocol is secure against active attacks. However, they did not give rigorous security proof and just mentioned that the scheme would be secure. In this paper, we introduce a new problem that is as hard as the learning parity with noise problem and prove the active security of the protocol under the assumption that the problem is hard. By combining our result with that of *P. Rizomiliotis* and *S. Gritzalis* [Revisiting lightweight authentication protocols based on hard learning problems. In: WiSec, ACM, 125–130 (2013)], we obtain complete proof of the Man-in-the-Middle (MIM) security of the protocol.

For the entire collection see [Zbl 1312.68014].

MSC:

94A62 Authentication, digital signatures and secret sharing
68M12 Network protocols

Keywords:

RFID; authentication protocol; LPN problem; HB-Family

Full Text: DOI