Gilbert, Henri; Robshaw, Matthew J. B.; Seurin, Yannick

HB$^{\#}$: Increasing the security and efficiency of HB^{+}. (English) Zbl 1149.94334

Smart, Nigel (ed.), Advances in cryptology – EUROCRYPT 2008. 27th annual international conference on the theory and applications of cryptographic techniques, Istanbul, Turkey, April 13–17, 2008. Proceedings. Berlin: Springer (ISBN 978-3-540-78966-6/pbk). Lecture Notes in Computer Science 4965, 361-378 (2008).

Summary: The innovative HB^{+} protocol of *A. Juels* and *S. A. Weis* [“Authenticating pervasive devices with human protocols”, Lect. Notes Comput. Sci. 3621, 293–308 (2005; Zbl 1145.94470)] extends device authentication to low-cost RFID tags. However, despite the very simple on-tag computation there remain some practical problems with HB^{+}” and despite an elegant proof of security against some limited active attacks, there is a simple man-in-the-middle attack due to *H. Gilbert*, *M. J. B. Robshaw* and *H. Sibert* [“An active attack against HB^{+}: A provably secure lightweight authentication protocol”, in: IEE Electronics Letters 41, No. 21, 1169–1170 (2005)]. In this paper we consider improvements to HB^{+} in terms of both security and practicality. We introduce a new protocol that we denote random-HB$^{\#}$. This proposal avoids many practical drawbacks of HB^{+}, remains provably resistant to attacks in the model of Juels and Weis, and at the same time is provably resistant to a broader class of active attacks that includes the attack of [*H. Gilbert* et al. loc. cit.]. We then describe an enhanced variant called HB$^{\#}$ which offers practical advantages over HB^{+}.

For the entire collection see [Zbl 1133.94008].

MSC:

94A62 Authentication, digital signatures and secret sharing

Cited in **1** Review
Cited in **12** Documents

Keywords:

HB^{+}; RFID tags; authentication; LPN; Toeplitz matrix

Software:

PRESENT

Full Text: DOI