Munilla, J.; **Peinado, A.**

HB-MP: a further step in the HB-family of lightweight authentication protocols. (English)

Zbl 1118.68015
Comput. Netw. 51, No. 9, 2262-2267 (2007).

Summary: A family of lightweight authentication protocols has been developed since Hopper and Blum proposed the HB protocol in 2001. In 2005, the HB^+ protocol was proposed as an improvement of the original HB to overcome the weakness against active attacks. Later, several authors have successfully applied new attacks to both HB and HB^+, resulting in a new modification known as HB^{++}. Again, this protocol has been cryptanalyzed and a new protocol has been presented by Piramuthu in 2006. This kind of protocol is especially suitable for RFID systems in which every tag has to be authenticated by the reader. Taking into account security and performance aspects, we present in this paper a new protocol, named HB-MP, derived from HB^+, providing a more efficient performance and resistance to the active attacks applied to the HB-family.

MSC:

68M10 Network design and communication in computer systems
68P25 Data encryption (aspects in computer science)
94A62 Authentication, digital signatures and secret sharing

Keywords:

RFID; low-cost cryptography; authentication; HB protocol

Software:

HB-MP

Full Text: DOI