Bellare, Mihir; **Rogaway, Phillip**

Entity authentication and key distribution. (English) Zbl 0870.94019

Stinson, Douglas R. (ed.), Advances in cryptology - CRYPTO '93. 13th annual international cryptology conference, Santa Barbara, CA, USA, August 22 - 26, 1993. Proceedings. Berlin: Springer-Verlag. Lect. Notes Comput. Sci. 773, 232-249 (1994).

Summary: The authors provide the first formal treatment of entity authentication and authenticated key distribution appropriate to the distributed environment. Addressed in detail are the problems of mutual authentication and authenticated key exchange for the symmetric, two-party setting. For each we present a definition, protocol, and proof that the protocol meets its goal, assuming only the existence of a pseudorandom function.

For the entire collection see [Zbl 0856.00053].

MSC:

94A60 Cryptography

Keywords:

entity authentication; authenticated key distribution; mutual authentication