Wang, Huaxiong; Pieprzyk, Josef

Shared generation of pseudo-random functions. (English) Zbl 1058.94017


This is a continuation of the idea of S. Micali and R. Sidney [Lect. Notes Comput. Sci. 963, 185–196 (1995; Zbl 0868.94030)] for shared generation of a pseudo-random function \( f \) among \( n \) players such that \( u \) of the players can compute \( f(x) \) while \( t \) or fewer of them do not do it, for each input \( x \). To study this problem, the notion of a ramp access structure is introduced and discussed. The main results are obtained for a special case of these objects, so-called \( (t, u, n) \) ramp access structures with \( (t, u, n) \) cumulative maps, which for \( t = u - 1 \) form the \( (u, n) \) threshold access structures with \( (u, n) \) cumulative maps studied by Micali and Sidney. For the minimal \( (t, u, n) \) cumulative maps lower and upper bounds are derived. The paper has been crowned with an algorithm that designs a \( (t, u, n) \) cumulative map as the solution of a special case of the set-cover problem. This construction achieves the optimum bound by a factor of at most \( u \ln 2 \).

Reviewer: Jerzy Żurawiecki (Lublin)

MSC:

94A62 Authentication, digital signatures and secret sharing
94A60 Cryptography

Keywords:
cryptography; pseudo-random functions; secret sharing; access structure; cumulative maps; resilient collection of sets; set-cover problem

Full Text: DOI

References: