MULTIPARTY UNCONDITIONALLY SECURE PROTOCOLS

(Abstract)

David Chaum[†]
Claude Crépeau[‡]
Ivan Damgård[*]

[†]*Centre for Mathematics and Computer Science*
Kruislaan 413, 1098 SJ Amsterdam, The Netherlands

[‡]*Laboratory for Computer Science, M.I.T.*
545 Technology Square, Cambridge, MA 02139, U.S.A.

[*]*Matematisk Institut, Aarhus Universitet,*
Ny Munkegade, DK 8000 Aarhus C, Danmark

Abstract

It has been shown previously how almost any multiparty protocol problem can be solved. All the constructions suggested so far rely on trapdoor one-way functions, and therefore must assume essentially that public key cryptography is possible. It has also been shown that unconditional protection of a single designated participant is all that can be achieved under that model. Assuming only authenticated secrecy channels between pairs of participants, we show that essentially any multiparty protocol problem can be solved. Such a model actually implies the further requirement that less than one third of the participants deviate from the protocol. The techniques presented do not, however, rely on any cryptographic assumptions; they achieve the optimal result and provide security as good as the secrecy and authentication of the channels used. Moreover, the constructions have a built-in fault tolerance: once the participants have sent messages committing themselves to the secrets they will use in the protocol, there is no way less than a third of them can stop the protocol from completing correctly. Our technique relies on the so called key-safeguarding or secret-sharing schemes proposed by Blakley and Shamir as basic building blocks. The usefulness of their homomorphic structure was observed by Benaloh, who proposed techniques very similar to ours.

C. Pomerance (Ed.): Advances in Cryptology - CRYPTO '87, LNCS 293, p. 462, 1988.