

BLIND SIGNATURE SYSTEM

David Chaum

Department of Computer Science
University of California
Santa Barbara, CA 93106

ABSTRACT

An untraceable payments system based on an extension of public key cryptography, called blind signatures, has been presented previously by the author. The existence of such blind signature systems was not demonstrated. An actual set of implementable functions is presented in the present work which have the blind signature property, and for which the **blindness of the signature is proved without any assumptions about computational infeasibility**. In terms of the simple payments system previously presented, this means that even a conspiracy between the bank and payee can learn nothing from their participation in the payments protocol about the identity of the payer.

Several extensions over the simple payments system are also presented. Previously only payer anonymity was provided. A new protocol allows payee anonymity. A combination of the two protocols can even allow mutual anonymity. A subtle threat could be perpetrated by the bank in the previous protocols; new cryptographic protocol extensions are presented that can protect payers and payees from such fraud by the bank.

SESSION IV
APPLICATIONS

