BLIND SIGNATURES FOR UNTRACEABLE PAYMENTS

David Chaum

Department of Computer Science
University of California
Santa Barbara, CA

INTRODUCTION

Automation of the way we pay for goods and services is already underway, as can be seen by the variety and growth of electronic banking services available to consumers. The ultimate structure of the new electronic payments system may have a substantial impact on personal privacy as well as on the nature and extent of criminal use of payments. Ideally a new payments system should address both of these seemingly conflicting sets of concerns.

On the one hand, knowledge by a third party of the payee, amount, and time of payment for every transaction made by an individual can reveal a great deal about the individual's whereabouts, associations and lifestyle. For example, consider payments for such things as transportation, hotels, restaurants, movies, theater, lectures, food, pharmaceuticals, alcohol, books, periodicals, dues, religious and political contributions.

On the other hand, an anonymous payments systems like bank notes and coins suffers from lack of controls and security. For example, consider problems such as lack of proof of payment, theft of payments media, and black payments for bribes, tax evasion, and black markets.

A fundamentally new kind of cryptography is proposed here, which allows an automated payments system with the following properties:

(1) Inability of third parties to determine payee, time or amount of payments made by an individual.

(2) Ability of individuals to provide proof of payment, or to determine the identity of the payee under exceptional circumstances.

D. Chaum et al. (eds.), *Advances in Cryptology*

(3) Ability to stop use of payments media reported stolen.

BLIND SIGNATURE CRYPTOSYSTEMS

The new kind of cryptography will be introduced first in terms of an analogy and then by description of its parts, their use, and the resulting security properties. No actual example cryptosystem is presented.

Basic Idea

The concept of a blind signature can be illustrated by an example taken from the familiar world of paper documents. The paper analog of a blind signature can be implemented with carbon paper lined envelopes. Writing a signature on the outside of such an envelope leaves a carbon copy of the signature on a slip of paper within the envelope.

Consider the problem faced by a trustee who wishes to hold an election by secret ballot, but the electors are unable to meet to drop their ballots into a single hat. Each elector is very concerned about keeping his or her vote secret from the trustee, and each elector also demands the ability to verify that their vote is counted.

A solution can be obtained by use of the special envelopes. Each elector places a ballot slip with their vote written on it in a carbon lined envelope; places the carbon lined envelope in an outer envelope addressed to the trustee, with their own return address; and mails the nested envelopes to the trustee. When the trustee receives an outer envelope with the return address of an elector on it, the trustee removes the inner carbon lined envelope from the outer envelope; signs the outside of the carbon lined envelope; and sends the carbon lined envelope back, in a new outer envelope, to the return address on the old outer envelope. Thus, only authorized electors receive signed ballot slips. Of course, the trustee uses a special signature which is only valid for the election!

When an elector receives a signed envelope, the elector removes the outer envelope; checks the signature on the carbon lined envelope; removes the signed ballot slip from the carbon lined envelope; and mails the ballot to the trustee on the day of the election in a new outer envelope, without a return address.

When the trustee receives the ballots, they can be put on public display. Anyone can count the displayed ballots and check the signatures on them. If electors remember some identifying aspect of their ballot, such as the fiber pattern of the paper, they can check that their ballot is on display. But since the trustee never actually saw the ballot slips while signing them (and assuming every signature is identical), the trustee can not know any identifying aspect of the ballot slips. Therefore, the trustee can not know anything about the correspondence between the ballot containing