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.

(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

envelopes signed and the ballots made public. Thus, the trustee can not determine how anyone voted.

Functions

Blind signature systems might be thought of as including the features of true two key digital signature systems combined in a special way with commutative style public key systems. The following three functions make up the blind signature cryptosystem:

(1) A signing function s' known only to the signer, and the corresponding publically known inverse s, such that s(s'(x))=x and s give no clue about s'.

(2) A commuting function c and its inverse c', both known only to the provider, such that c'(s'(c(x)))=s'(x), and c(x) and s' give no clue about x.

(3) A redundancy checking predicate r, that checks for sufficient redundancy to make search for valid signatures impractical.

Protocol

The way these functions are used is reminiscent of the way the carbon paper lined envelopes were used in the example described above:

(1) Provider chooses x at random such that r(x), forms c(x), and supplies c(x) to signer.

(2) Signer signs c(x) by applying s' and returns the signed matter s'(c(x)) to provider.

(3) Provider strips signed matter by application of c', yielding c'(s'(c(x)))=s'(x).

(4) Anyone can check that the stripped matter s'(x) was formed by the signer, by applying the signer's public key s and checking that r(s(s'(x))).

Properties

The following security properties are desired of the blind signature system comprising the above functions and protocols:

(1) Digital signature--anyone can check that a stripped signature s'(x) was formed using signer's private key s'.

(2) Blind signature--signer knows nothing about the correspondence between the elements of the set of stripped signed matter $s'(x_i)$ and the elements of the set of unstripped signed matter $s'(c(x_i))$.

(3) Conservation of signatures--provider can create at most one stripped signature for each thing signed by signer (i.e. even with $s'(c(x_1)) \ldots s'(c(x_n))$ and choice of c, c', and x_i, it is impractical to produce s'(y), such that r(y) and $y \neq x_i$).

As is common in cryptographic work, the possibility that the same random number could be generated independently is ignored.

UNTRACEABLE PAYMENTS SYSTEM

An example payment transaction will illustrate how the blind signature systems introduced above can be used to make an untraceable payments system. The critical concept is that the bank will sign anything with its private key, but anything so signed is worth a fixed amount, say $1. The actors in the example below are a bank, a payer, and a payee. A single note will be formed by the payer, signed by the bank, stripped by the payer, provided to the payee, and cleared by the bank. The following traces the detailed steps of a single payment transaction:

(1) Payer chooses x at random such that r(x), and forms note c(x).

(2) Payer forwards note c(x) to bank.

(3) Bank signs note, i.e. forms s'(c(x)), and debits payer's account.

(4) Bank returns the signed note, s'(c(x)), to payer.

(5) Payer strips note by forming c'(s'(c(x)))=s'(x).

(6) Payer checks note by checking that s(s'(x))=x and stops if false.

(7) Payer makes payment some time later by providing note s'(x) to payee.

(8) Payee checks note by forming r(s(s'(x))) and stops if false.

(9) Payee forwards note s'(x) to bank.

(10) Bank checks note by forming r(s(s'(x))) and stops if false.

(11) Bank adds note to comprehensive list of cleared notes and stops if note already on list.

(12) Bank credits account of payee.

(13) Bank informs payee of acceptance.

Notice that by the blind signature property above, when the bank receives a note to be cleared from the payee in step (9) the bank does not know which payer the note was originally issued to in step (4). The digital signature and related conservation of signatures properties above ensure that counterfeiting is not possible.

Auditability

Extension of current practice suggests that payers receive digital receipts from payees. These receipts would include the usual description of the goods or services purchased, and the date. In addition, the receipt could also include a copy of the note. Under exceptional circumstances, such as an audit, the note would allow the payer, with the cooperation of the bank (and clearing house(s) as described below), to verify which account the note was actually deposited to.

A receipt indicating that a note was deposited to an account other than the account actually deposited to would be evidence of fraud. One dissatisfied customer of a black market could reveal a note supplied to the black market, which could then be traced to the account it ultimately ended up in. Uncleared notes reported as stolen could be included on clearing house lists and thus be prevented from being cleared; stolen notes cleared could be traced.

Receipts issued by payee to payer provide control over all outflows, and thus all flows of funds. A taxpayer could provide verifiable receipts for any expenditures needed for tax audit. Individuals could be required to keep receipts for substantial inflows, but inflow receipts maintained by organizations may be undesirable, if they could reveal the organization's patrons.

Elaborations

The simple system of the above example could be extended in various ways to provide economy of mechanism, disaggregation of services, and decentralization. For example, obvious efficiencies would result from use of multiple denomination notes. The banking and clearing house functions could be separated. There might be multiple banks; multiple clearing houses could serve different or overlapping banks. Periodic changes of the key(s) used to sign notes might increase security, increase auditability, and reduce uncertainty about the size of the money supply.

SUMMARY AND IMPLICATIONS

A new kind of cryptography, blind signatures, has been introduced. It allows realization of untraceable payments systems which offer improved auditability and control compared to current systems, while at the same time offering increased personal privacy.