Uncoercible e-Bidding Games

M. Burmester (burmester@cs.fsu.edu)*

Florida State University, Department of Computer Science, Tallahassee, Florida 32306-4530, USA

E. Magkos (emagos@unipi.gr)*

University of Piraeus, Department of Informatics, 80 Karaoli & Dimitriou, Piraeus 18534, Greece

V. Chrissikopoulos (vchris@ionio.gr)

Ionian University, Department of Archiving and Library Studies, Old Palace Corfu, 49100, Greece

Abstract. The notion of *uncoercibility* was first introduced in e-voting systems to deal with the coercion of voters. However this notion extends to many other e-systems for which the privacy of users must be protected, even if the users wish to undermine their own privacy.

In this paper we consider uncoercible *e-bidding* games. We discuss necessary requirements for uncoercibility, and present a general uncoercible e-bidding game that distributes the bidding procedure between the bidder and a tamper-resistant token in a verifiable way. We then show how this general scheme can be used to design provably uncoercible e-auctions and e-voting systems. Finally, we discuss the practical consequences of uncoercibility in other areas of e-commerce.

Keywords: uncoercibility, e-bidding games, e-auctions, e-voting, e-commerce.

* Research supported by the General Secretariat for Research and Technology of Greece.

1. Introduction

As technology replaces human activities by electronic ones, the process of designing electronic mechanisms that will provide the same protection as offered in the physical world becomes increasingly a challenge. In particular with Internet applications in which users interact remotely, concern is raised about several security issues such as privacy and anonymity. Privacy usually refers to the protection of sensitive information from other parties (eavesdroppers). However there are cases when privacy extends to the owner of the information, in the sense that the owner should not be able to undermine his/her privacy, e.g. by selling the information to information-buyers, or by giving it to coercers.

The notions of *receipt-freeness* and *uncoercibility* were first introduced to deal with *vote-selling* and the *coercion* of voters in e-voting systems (Benaloh and Tuinstra, 1994a; Okamoto, 1997; Sako and Killian, 1995; Hirt and Sako, 2000; Magkos et al., 2001). These notions are similar in many respects, however there are also subtle differences. With receipt-freeness the voter is the adversary: the voter should not be able to convince a third party of the value of the vote, even if the voter wants to (e.g. for a reward). With uncoercibility, the adversary is a coercer: the coercer should not be able to extract the true value of the vote from the voter, even if the voter is forced to (e.g. threatened). In fact receipt-freeness is stronger than uncoercibility, in the sense that there are e-systems which are uncoercible but not receipt-free (e.g. (Benaloh and Tuinstra, 1994a; Canetti et al., 1997; Canetti and Gennaro, 1996)). This is because, although a voter can succeed in fooling a coercer (uncoercibility), the voter can also sell the vote by

pre-committing to the random choices made during the encryption of the vote (see (Hirt and Sako, 2000) for such an attack).

However the concepts of uncoercibility and receipt-freeness have been used interchangeably in the literature. In this paper, for simplicity, we shall assume that uncoercibility extends to receipt-freeness. In particular, users can also be self-coercers, i.e. information sellers. We believe that this interpretation is also semantically correct.

1.1. Uncoercibility and e-auction systems

The notion of uncoercibility applies to every electronic transaction which involves sensitive private data that may be traded. Examples are digital cash, key escrow (key revocation) in payment systems, electronic campaign finance (see Section 6 for an analysis). Uncoercibility becomes increasingly important with electronic transaction systems that can be manipulated by some powerful authority (e.g. a "Mafia", a political party, a government, a financial institution, etc). Examples of such systems in e-commerce are e-auctions.

With auctions one has to deal with collusions of bidders, who conspire not to outbid each other, so as to lower the winning bid. Such collusions are known as *rings*. In the physical world, *public* auctions (bids are public during the auction) are more vulnerable to rings than *private* auctions (bids are secret until the end of the bidding period). This is because with private auctions, a ring member can deviate from the collusion and outbid the others, to acquire the auctioned item at a price slightly greater than the collusive price (Klemperer, 1999; Mead, 1987).

However with private e-auctions (e.g. (Viswanathan et al., 2000; Magkos et al., 2000)) the bids are encrypted with the public key of the auctioneer (for secrecy), and the encryptions are sent to the auctioneer via an open network (e.g. the Internet). For verifiability, the encryptions are posted on a bulletin board. In this case, ring members can prove to the collusion (the coercer) the content of their encrypted bids. This is because with public-key encryptions the plaintext M (the bid), can be checked for correctness by encrypting it with the public key of the receiver (using the same randomness, if a probabilistic encryption is used) and then comparing the result $E(M)$ with the (publicly observed) ciphertext C: we must have $C = E(M)$. Even if the identity of the bidder is protected, e.g. as in (Sakurai and Miyazaki, 2000), all ring members can prove to the collusion that their bids were different from the winning bid. A ring member who cannot prove this, will be exposed to the collusion. Consequently, collusions in e-auctions are harder to deal with.

From our discussion above the need for uncoercibility in e-auctions is obvious: if ring members are not able to prove their bid to a coercer, then the bidders will be discouraged from forming rings. Thus the auction will be free of collusions.

1.2. Current solutions for Resolving Uncoercibility

The solutions for uncoercibility presented so far in the literature involve e-voting systems. Depending on the model used, two basic premises are made:

– the existence of *voting booths* (e.g. (Benaloh and Tuinstra, 1994a; Okamoto, 1997)),

– the existence of *untappable channels* (e.g. (Sako and Killian, 1995; Hirt and Sako, 2000; Franklin and Sander, 2000).

Voting booths and untappable channels are primitives. Voting booths require that the voter can, (*i*) vote without being observed and, (*ii*) communicate with the system authorities without being tapped. Untappable channels are a weaker primitive: they only require that the voter can communicate without being tapped.

All e-voting systems assume the first requirement of voting booths, that is, that voters can vote (and in particular, encrypt their vote) without being observed. We shall call this, the *virtual booth* assumption.

Voting booths and untappable channels can be quite cumbersome to implement, particularly for Internet applications with geographically distributed users. Therefore solutions based on these primitives are mainly of theoretical interest.

1.3. Our approach

We consider uncoercibility in the more general context of e-bidding games in which bidders bid on-line for items selected from a list. The winner is then determined by the rules of the game. We shall also assume the existence of virtual booths: this is essentially a physical requirement, and it is hard to see how one can do without it (Hirt and Sako, 2000). However we shall replace the untappable channel require-

ment by the more practical requirement of tamper-resistant tokens such as smartcards.

To achieve uncoercibility we shall distribute the bidding procedure between the bidder and the token in a verifiable way. We do not exclude the possibility that the bidder and the coercer can co-operate (and in particular, agree on some bid) *before* the bidding starts. Thus in our model, uncoercibility is *perfect* (Benaloh and Tuinstra, 1994b).

1.4. Organization

The rest of this paper is organized as follows. In Section 2 we discuss the requirements for uncoercibility in e-bidding games. In Section 3 we present a general uncoercible e-bidding game. This scheme is used in Section 4 to design a practical uncoercible e-auction system, and in Section 5 to design a practical uncoercible e-voting system. Finally, in Section 6 we consider the practical consequences of uncoercibility in other areas of electronic commerce.

2. Requirements for Uncoercibility in e-Bidding Games

We discuss several requirements that are necessary for uncoercibility in e-bidding games. These are general and will not depend on the particular aspects of the system used. First we define our model.

The main players are the *bidders*, the *Bidding Authorities* and the *Coercer*. In addition, there is a list of *items* I and a set of *Rules*. A *Bulletin Board* is used as a primitive. This is a public broadcast channel with memory. Only intended bidders can write to a designated area on the Bulletin Board, while no party can erase any information from it. An e-bidding game has essentially three phases:

ENCRYPTION. Each bidder selects and then encrypts a bid from list I.
POSTING. The encryptions are posted on the Bulletin Board.
TALLYING. The Bidding Authorities decrypt the encrypted bids and post the results on the Bulletin Board for verification. The winner is then declared, based on the Rules of the game.

The Coercer is the adversary. The Coercer wants to find out the value of a selected bid. The Coercer can:

- coerce, or co-operate with the bidder, *before* and *after* the bidding, but not *during* the bidding;
- tap the communication channel that links the bidder to the Bidding Authorities;
- co-operate with some of the Bidding Authorities (but no more than a certain threshold).

The bidder must reveal to the Coercer any information requested. The bidder may give false information (lie) and get away with the lie, provided the Coercer cannot prove that it is false. We do not exclude the possibility that the Coercer is the bidder (see our earlier remark on

self-coercing). In this case, the bidder does not only want to find out the value of the bid, but also to be able to prove it to an information buyer.

For uncoercibility, the communication channel linking the bidder to the Bidding Authorities must be:

1. *Private*: so that the Coercer cannot get the bid by eavesdropping.

2. *Receipt-free*: so that it is not possible for the bidder, the Coercer, the Bidding Authorities, or anybody else, to get a receipt for a submitted bid.

3. *Authenticated*: so that the Coercer cannot submit a bid on behalf of the bidder.

We shall now discuss the requirements for uncoercibility, by analyzing the security aspects of the communication channel, in the context of e-bidding games.

2.1. Private Channels with Probabilistic Encryption

All bids must be encrypted for privacy. Observe that *symmetric-key* encryption (Schneier, 1996) cannot be used because the Coercer can extract the secret encryption key from the bidder and unmask the encrypted bid. So *public-key* encryption must be used. The bids are encrypted with the public key of the Bidding Authorities. The encryption must be *probabilistic* (Goldwasser and Micali, 1984), i.e. randomness must be used during the encryption, otherwise the encryption constitutes a receipt for the bid.

2.1.1. Threshold Cryptography

The Bidding Authorities share the private decryption key, and decrypt the encrypted bids in a distributed way, using *threshold cryptography* (Desmedt, 1994). That is, they jointly decrypt the encrypted bids without explicitly reconstructing the private decryption key. In this way uncoercibility is not undermined by a Coercer who succeeds in corrupting some of the Bidding Authorities (less than the threshold).

2.2. Receipt-free Channels with Distributed Randomness

If the bidder chooses the randomness of the encrypted bid, then this randomness will constitute a receipt. Even worse, since in our model we allow for prior co-operation between bidder and Coercer, the Coercer may select the randomness on behalf of the bidder, and insist that the bidder use it. Later, the Coercer will demand a proof (Okamoto, 1997).

If the randomness of the encrypted bid is chosen by a tamper-resistant token, and not the bidder, then too much trust is placed on the token: the bid's secrecy will be broken if the Coercer gets control of the token. On the other hand, a solution which involves a number of tokens will not scale well.

Distributing the randomness between the bidder and the token seems to be the only practical solution. However, since the final encrypted bid will contain randomness unknown to the bidder, the bidder must be convinced that it is indeed an encryption of the original bid, i.e. that the token has not altered it. As a consequence, the token must prove to the bidder that the encryption is correct. This proof must be *non-transferable*, otherwise it would constitute a receipt, when combined

with the bid and the randomness of the bidder. For this purpose we shall use an *interactive zero-knowledge proof system* (Goldwasser et al., 1984). With such proofs the verifier learns no more than strictly necessary, that is, the correctness of the encryption (one bit). Zero-knowledge proofs are on-line proofs which can be simulated off-line. Therefore their transcripts have no off-line value to the adversary, since they cannot be used as part of a receipt.

2.2.1. Untappability of The Bidder-Token Channel

This channel must be protected in a physical way. The Coercer should not be able to tap it: otherwise the Coercer can get the partial encryption of the bidder and thus unmask the encrypted bid. We can do without this untappability assumption if we assume that the distributed encryption of the bid takes place in the virtual booth.

2.2.2. Bidder/Item Ratio

If this ratio is considerably low, e.g. if there are many items and few bidders, then the chances that a particular item is selected may also be low. If this item has been tagged, then uncoercibility may be undermined. For instance, the bidder could easily sell his bid by committing to it before the final decrypted results get published.

2.3. Authenticated Channels with Bulletin Boards

For authentication, the encrypted bids are digitally signed by the bidders. The signatures are posted on the Bulletin Board.

3. A General Uncoercible e-Bidding Game

In this Section we present a general uncoercible e-bidding game. We only give a high level description which will serve as our model. This shall be used in the following sections to design practical e-auctions and e-voting systems which are provably uncoercible. First we define the tools for this game.

- Probabilistic Homomorphic Encryptions. Let $\oplus$ be an operation on the message space and $\otimes$ an operation on the cipher space. A probabilistic encryption e is *homomorphic* if: for all messages x, y, and randomness r_1, r_2, there exists a random string r such that,
$$e_r(x \oplus y) = e_{r_1}(x) \otimes e_{r_2}(y).$$

- Tamper-Resistant Tokens (e.g. smartcards). These should be capable of randomizing input data, and digitally sign data on behalf of their owner (a bidder). To prevent the Coercer from using the token on behalf of the bidder, the token incorporates proper authentication mechanisms (e.g. biometric identification).

We shall also assume the existence of virtual booths, so that bidders can encrypt their bid without being observed.

Protocol

The uncoercible e-bidding game has four distinct phases: *Encryption*, *Blinding*, *Posting* and *Tallying*.

1. ENCRYPTION (in a virtual booth). Each bidder B selects a bid i from the list I, and randomness r_1, to encrypt i with the probabilistic encryption e. Let $e_{r_1}(i)$ be the encryption. The bidder inputs this to the token –see Fig. 1, Step 1.

Figure 1. A General Uncoercible e-bidding Game

2. BLINDING. The token randomizes the input $e_{r_1}(i)$, without changing the value of the bid i. This is achieved by "multiplying" $e_{r_1}(i)$ by $e_{r_2}(u)$, where r_2 is the token's randomness and u is the *neutral* element of the message space. The token outputs the encrypted bid $e_r(i) = e_{r_1}(i) \otimes e_{r_2}(u)$ together with a digital signature $Sig_B(e_r(i))$ of $e_r(i)$ (the operation $\otimes$ will be specified later in Section 4 and Section 5 when we consider applications) –Fig. 1, Step 2.

The bidder has to be convinced that the token's output is correct, i.e. that $e_r(i)$ is the encryption of i. The problem is that the bidder must be convinced without finding out the token's randomness r_2, otherwise uncoercibility will be undermined. For this purpose the token proves correctness to the bidder by using an interactive zero-knowledge proof system. That is, the token proves to the bidder in zero-knowledge that: for the given encryptions $e_r(i)$, $e_{r_1}(i)$, there exists a random string r_2

such that: $e_r(i) = e_{r_1}(i) \otimes e_{r_2}(u)$. The particular zero-knowledge protocol employed will depend on the operation $\otimes$. For this general setting we can use a zero-knowledge protocol for NP languages (Goldreich et al., 1991).

3. Posting. If the proof of correctness is valid, then the bidder B posts the encrypted bid $e_r(i)$ together with the signature $Sig_B(e_r(i))$ on the Bulletin Board –Fig. 1, Step 3.

4. Tallying. The Bidding Authorities (BAs) jointly decrypt the encrypted bids, post the results on the Bulletin Board, and declare a winner according to the Rules of the game –Fig. 1, Step 4. The results are posted in such a way that there is no direct link between the final results and the encrypted bids.

This game is uncoercible if we assume that the Coercer cannot control *both* the bidder and the token. Indeed the randomness of the bidder and the token are needed to unmask the encryption. Note that we do not make any physical untappability assumptions about the communication channel between the bidder and the Bidding Authorities. This could be an open channel such as the Internet.

In the following sections we will show how this general e-bidding game can be used to design provably uncoercible e-auctions and e-voting systems.

4. Application 1: An Uncoercible Private e-Auction

The protocol we propose satisfies most of the requirements for secure e-auctions, as well as uncoercibility. These are:

- *Secrecy:* All bids remain secret until the end of the bidding period.
- *Unforgeability:* No one can impersonate a bidder, or alter/eliminate a bid.
- *Verifiability:* All bidders can verify that the highest bid wins.
- *Uncoercibility:* No bidder can prove that a particular bid has been submitted.

For encryption we use the ElGamal public-key encryption scheme (ElGamal, 1985). This is a probabilistic multiplicative homomorphic scheme. Below we briefly describe it.

Let p, q be large primes such that $q \mid (p-1)$, Z_p^* be the multiplicative group of integers $\{x : 1 \leq x \leq p-1\}$ modulo p, G_q be the subgroup of Z_p^* of order q, and g a generator of G_q. To get a secret key, choose a random number $s : 1 \leq s \leq q-1$. The corresponding public key is (p, g, h), where $h = g^s \bmod p$. All operations of the ElGamal encryption are modulo p, so for simplicity in the sequel we shall drop the operator "mod$p$".

The encryption of a message $m \in Z_p^*$ is $(x, y) = (g^r, h^r m)$, where $r : 1 \leq r \leq q-1$ is random. To decrypt the ciphertext (x, y), compute

$m = y/x^s$, where s is the private key. We clearly have,

$$\begin{aligned} e_{r_1}(m_1) \cdot e_{r_2}(m_2) &= (g^{r_1}, h^{r_1} m_1) \cdot (g^{r_2}, h^{r_2} m_2) \\ &= (g^{r_1+r_2}, h^{r_1+r_2}\, m_1 \cdot m_2) \\ &= (g^r, h^r m) \;=\; e_r(m), \end{aligned}$$

where $r = r_1 + r_2$ and $m = m_1 \cdot m_2$. So the encryption is homomorphic. The security of the ElGamal encryption is reduced to the difficulty of solving the *Diffie-Hellman problem*[1] (Diffie and Hellman, 1976).

PROTOCOL

1. ENCRYPTION. Each bidder B selects a bid i from the list of bidding prices $I \subset \{1, 2, \ldots, p-1\}$, and a random $r_1 : 1 \leq r_1 \leq q-1$, to encrypt i with the public key h of the Auctioneers (the Bidding Authorities). Let $e_{r_1}(i) = (g^{r_1}, h^{r_1} i)$ be the encryption. The bidder inputs $e_{r_1}(i)$ to the token –see Fig. 2, Step 1.

Figure 2. An Uncoercible Private e-Auction

[1] In this problem one has to compute $z = g^{ab}$, given $x = g^a$ and $y = g^b$ in G_q, but not the exponents a, b. It is considered to be a hard problem.

2. Blinding. The token now contributes its own randomness. It selects a random $r_2 : 1 \leq r_2 \leq q-1$, and computes $e_{r_2}(1) = (g^{r_2}, h^{r_2})$. It then computes the product: $e_{r_1}(i) \cdot e_{r_2}(1) = e_r(i)$, where $r = r_1 + r_2$. The token outputs $e_r(i)$ to the bidder, together with a digital signature $Sig_B(e_r(i))$ on the encrypted bid (Fig. 2, Step 2). For uncoercibility, the token must prove to the bidder that its contribution $e_{r_2}(1) = (x, y)$, say, is an encryption of 1. For this purpose the token uses the Chaum-Petersen interactive zero-knowledge proof of discrete logarithms (Chaum and Pedersen, 1993). This proof can be used to confirm that the numbers $x, y, g, h \in G_q$ are related by $log_g x = log_h y$. This is equivalent to: $(x, y) = (g^{r_2}, h^{r_2})$, which is an encryption of 1. Observe that the bidder can compute $e_{r_2}(1)$ by taking $e_r(i)/e_{r_1}(i)$.

3. Posting. If the proof of correctness is valid, then the bidder B posts the encrypted bid $e_r(i)$ together with the signature $Sig_B(e_r(i))$ on the Bulletin Board (Fig. 2, Step 3).

4. Tallying. The Auctioneers jointly decrypt the encrypted bids by using a threshold decryption protocol (Pedersen, 1991) (without explicitly reconstructing the private key s: in this way, the same public key can be used for future auctions). After decryption, the winning bid is determined by the rules of the auction, and posted on the Bulletin Board. For verification the Auctioneers post a list E of the encrypted bids $e_r(i)$, as well as a list L of the decrypted bids i, in random order (e.g. lexicographical). The Auctioneers also post a *non-interactive* zero-knowledge proof π, which proves that the list L contains only those bids whose encryptions are in the list E, without revealing the connection

between $e_r(i)$ and i (Fig. 2, Step 4). Such proof for ElGamal has been described in (Abe, 1998).

Theorem. If the Decision Diffie-Hellman problem[2] *is hard and if the Coercer does not control both the bidder and the token, then the proposed e-auction protocol is uncoercible.*

Proof. Suppose that the Coercer and the bidder can jointly prove that $e_r(i)$ is the encryption of the bid i. This means that they can prove that $e_{r_2}(1) = e_r(i)/e_{r_1}(i) = (x, z)$, say, is an encryption of 1. This holds if and only if: $\log_g x = \log_h z = r'$, say. If they can prove this, they can also check that $z = h^{r'} = (g^s)^{r'} = g^{sr'} = DH_g(x, h)$,[2] since $h = g^s$ and $x = g^{r'}$.

We now will use the Coercer and bidder as a subroutine to design an algorithm that will solve the Decision Diffie-Hellman (DDH) problem. Let (x, y, z) be an instance of the DDH problem, with $y = h$ the public key of the Bidding Authorities. Input (x, z) to the Coercer and bidder as an "encryption" of 1. If the Coercer and bidder succeed in proving that (x, z) is actually an encryption of 1, then we must have $z = DH_g(x, y)$. We therefore have an algorithm which solves the DDH problem. The case when the Coercer and the token can jointly prove that $e_r(i)$ is the encryption of i is similar, and omitted.

[2] The Diffie-Hellman operator DH_g is defined by $DH_g(g^a, g^b) = g^{ab}$. The problem of recognizing whether $z = DH_g(x, y)$, where $x, y, z \in G_q$, is called the *Decision Diffie-Hellman problem* (Diffie and Hellman, 1976).

5. Application 2: An Uncoercible e-Voting System

This is based on the voting system of Cramer, Gennaro and Schoenmakers (Cramer and Schoenmakers, 1997), which uses a variant of the ElGamal encryption that is additively homomorphic.

We use the same notation as in Section 4, with groups Z_q^*, G_q, parameters p, q, g, and public encryption key $h = g^s$ for the Voting Authorities, with s the secret decryption key. For this system the votes v are either 1 or -1. We assume that the total number of voters ℓ is less than q. The encryption of v is: $e_r(v) = (g^r, h^r G^v)$, with $r : 1 \leq r \leq q-1$, random and G a fixed generator of G_q. We have,

$$\begin{aligned} e_{r_1}(v_1) \cdot e_{r_2}(v_2) &= (g^{r_1}, h^{r_1} G^{v_1}) \cdot (g^{r_2}, h^{r_2} G^{v_2}) \\ &= (g^{r_1+r_2}, h^{r_1+r_2}\, G^{v_1+v_2}) \\ &= (g^r, h^r G^v) \;=\; e_r(v), \end{aligned}$$

where $r = r_1 + r_2$ and $v = v_1 + v_2$. For decryption we first compute: $h^r G^v / (g^r)^s = G^v$, where s is the decryption key, and then get v by comparing G^v to G and G^{-1}.

Protocol

1. Encryption. Each voter V selects a vote $v \in \{1, -1\}$, a random number $r_1 : 1 \leq r_1 \leq q - 1$, and computes the encryption $e_{r_1}(i) = (g^{r_1}, h^{r_1} G^v)$. This is input to the token.

2. BLINDING. The token computes $e_{r_2}(0) = (g^{r_2}, h^{r_2})$, where $r_2 : 1 \leq r_2 \leq q-1$ is random, and outputs the product: $e_{r_1}(v) \cdot e_{r_2}(0) = e_r(v)$, $r = r_1 + r_2$, together with a proof of correctness as in Section 4.

3. POSTING. If the encrypted bid $e_r(v)$ is correct, then the voter V posts it together with the signature $Sig_V(e_r(i))$ on the Bulletin Board. V also posts a proof of validity, i.e., that the vote v belongs to the set $\{-1, 1\}$. This proof is constructed *jointly* by the voter V and the token (such a proof is given in (Magkos et al., 2001)).

4. TALLYING. The Voting Authorities multiply all the encrypted votes to get the encrypted tally:

$$(X, Y) = (\prod_{i=1}^{\ell} g^{r_i}, \prod_{i=1}^{\ell} h^{r_i} G^{v_i}) = (g^{\sum r_i}, h^{\sum r_i} G^T), \quad T = \sum_{i=1}^{\ell} v_i.$$

T is the difference between the number of yes (1) and no (-1) votes. The Voting Authorities jointly decrypt the tally, as in Section 4, to get $G^T = Y/X^s$. Finally T is determined by using $O(\ell)$ modular multiplications.

This scheme is uncoercible provided the Diffie-Hellman Decision problem[2] is hard –this follows from (Magkos et al., 2001).

6. Discussion: The Impact of Uncoercible Communication in e-Commerce

The notion of uncoercibility has numerous applications in e-commerce. In this paper we introduced the notion of uncoercibility for private e-auctions and described a general scheme for uncoercible e-bidding games. This scheme was used to design provably uncoercible e-bidding games over the Internet.

In general uncoercibility is a prerequisite for all electronic transactions for which the privacy of the transactions must be protected from external coercion or self-coercion. For the rest of this Section we will consider some typical scenarios where uncoercible communication could be of some importance.

6.1. Anonymous e-Cash

Anonymous e-cash can be used for financial transactions that have to be unconditionally untraceable (Chaum, 1985; Chaum, 1982). Untraceable means that e-cash withdrawals cannot be associated with their subsequent deposit. This is achieved by using *blind signatures*[3] in which randomness is used during a cash withdrawal. The randomness is selected by the customer. However, the customer could be coerced by a "Maffia", a Bank, or some other organization, to reveal how the e-cash was spent. Alternatively, a self-coercing customer could choose

[3] Blind Signatures are the electronic equivalent of signing carbon-paper lined envelopes. A user seals a slip of a paper inside such an envelope, which is later signed on the outside. When the envelope is opened, the slip will bear the carbon image of the signature.

the randomness in a particular way to prove later the nature of the transaction. In an *uncoercible* e-cash protocol such attacks would not be possible.

6.2. Key escrow in payment systems

Key escrow (or key recovery) mechanisms have gained much attention recently as many governments try to protect society[4] from criminals who use encryption to block access to evidence of crime (for a taxonomy of key escrow systems see (Denning and Branstad, 1996)). However if encryption is used for legitimate payment transactions, then Law Enforcement Agencies should not have access to the plaintext. As a result, there is a need to develop an *uncoercible* infrastructure for such transactions.

6.3. Electronic campaign finance

In the political stage, candidates may extort donations from potential donors, by threatening with punitive treatment or indifference (Franklin and Sander, 2000). On the other hand, influence-buying donors may wish to prove to a candidate that they have made a donation. An *uncoercible* protocol would allow donors to contribute to a candidate's campaign without being able to prove the donation.

[4] There is obviously a conflict of interest between the Law Enforcement Agencies and individual citizens, or organizations. Several cryptographic protocols have been proposed to address this issue. These focus on fairness (Micali, 1993) and equitability (Burmester et al., 2001). The former deals with abuses by citizens, the latter with abuses by both citizens and Law Enforcement Agencies.

References

Abe, M. (1998). "Universally Verifiable Mix-net with Verification Work Independent of the Number of Mix-servers." In *Advances in Cryptology - EUROCRYPT '98*. Berlin: Springer-Verlag, LNCS 1403, 437-447.

Benaloh, J. and D. Tuinstra. (1994a). "Receipt-free Secret Ballot Elections." In *26th Annual ACM Symposium on the Theory of Computing*, 544-553.

Benaloh, J. and D. Tuinstra. (1994b). "Uncoercible Communication." Computer Science Technical Report TR-MCS-94-1, Clarkson University.

Burmester, M., Y. Desmedt, and J. Seberry. (1998). "Equitable Key Escrow with Limited Time Span (or How to Enforce Time Expiration Cryptographically)." In *Advances in Cryptology - ASIACRYPT '98*. Berlin: Springer-Verlag, LNCS 1514, 380-391.

Canetti, R., C. Dwork, M. Naor, and R. Ostrovsky. (1997). "Deniable Encryption." In *Advances in Cryptology - CRYPTO '97*. Berlin: Springer-Verlag, LNCS 1294, 90-104.

Canetti, R. and R. Gennaro. (1996). "Uncoercible Multiparty Computation." In *37th IEEE Symposium on the Foundations of Computer Science - FOCS '96*, 462-471.

Chaum, D. (1982). "Blind Signatures for Untraceable Payments." In *Advances in Cryptology - CRYPTO '82*. New York: Plenum Press, 199-203.

Chaum, D. (1985). "Security Without Identification: Transaction Systems to Make Big Brother Obsolete." *Communications of the ACM*, 28(10), 1030-1044.

Chaum, D. and T. Pedersen. (1993). "Wallet Databases with Observers." In *Advances in Cryptology - Crypto '92*. Berlin: Springer-Verlag, LNCS 740, 89-105.

Cramer, R., R. Gennaro, and B. Schoenmakers. (1997). "A Secure and Optimally Efficient Multi-Authority Election Scheme." In *Advances in Cryptology - EUROCRYPT '97*. Berlin: Springer-Verlag, LNCS 1233, 103-118.

Denning, D. and D. Branstad. (1996). "A Taxonomy of Key Escrow Encryption Systems." *Communications of the ACM*, 39(3), 34-40.

Desmedt, Y. (1994). "Threshold Cryptography." *European Transactions on Telecommunications*, 5(4), 449-457.

Diffie, W. and M. Hellman. (1976). "New Directions in Cryptography." *IEEE Transactions on Information Theory*, 22(6), 644-654.

ElGamal, T. (1985). "A Public-key Cryptosystem and a Signature Scheme Based on Discrete Logarithms." *IEEE Transactions on Information Theory*, 31(4), 469-472.

Franklin, M. and T. Sander. (2000). "Commital Deniable Proofs and Electronic Campaign Finance." In *Advances in Cryptology - ASIACRYPT '2000*. Berlin: Springer-Verlag, LNCS 1976, 373-387.

Goldreich, O., S. Micali, and A. Widgerson. (1991). "Proofs that Yield Nothing but their Validity, or all Languages in NP have Zero-Knowledge Proof Systems." *Journal of the ACM*, 38, 691-729.

Goldwasser, S. and S. Micali. (1984). "Probabilistic Encryption." *Journal of Computer and System Sciences*, 28, 270-299.

Goldwasser, S., S. Micali, and C. Rackoff. (1989). "The knowledge Complexity of Interactive Proof Systems." *Siam Journal on Computing*, 18, 186-208.

Hirt, M. and K. Sako. (2000). "Efficient Receipt-Free Voting Based on Homomorphic Encryption.", In *Advances in Cryptology - EUROCRYPT '2000*. Berlin: Springer-Verlag, LNCS 1807, 539-556.

Klemperer, P. (1999). "Auction Theory, A Guide to the Literature." *Journal of Economic Surveys*, 13.

Magkos, E., M. Burmester, and V. Chrissikopoulos. (2000). "An Equitably Fair Online Auction Scheme." In *1st International Conference on Electronic Commerce and Web Technologies - EC-WEB '2000*, Berlin: Springer-Verlag, LNCS 1875, 72-84.

Magkos, E., M. Burmester, and V. Chrissikopoulos. (2001). "Minimal Requirements for Receipt-Freeness in Electronic Elections without Physical Assumptions about the Communication Channel." In *1st IFIP I3E Conference*, Zurich. Kluwer Academics, 683-693.

Mead, W. (1987). "Natural Resource Disposal Policy: Oral Auction Versus Sealed Bids." *Natural Resources Journal*, 7, 195-224.

Micali, S. (1993). "Fair-Public-key Cryptosystems." In *Advances in Cryptology - CRYPTO '92*. Berlin: Springer-Verlag, LNCS 740, 113-139.

Okamoto, T. (1997). "Receipt-Free Electronic Voting Schemes for Large Scale Elections." In *Workshop of Security Protocols 97*. Berlin: Springer-Verlag, LNCS 1163, 125-132.

Pedersen, T. (1991). "A Threshold Cryptosystem Without a Trusted Party." In *Advances in Cryptology - EUROCRYPT '91*. Berlin: Springer-Verlag, LNCS 547, 522-526.

Sako, K. and J. Killian. (1995). "Receipt-Free Mix-Type Voting Schemes-A Practical Solution to the Implementation of Voting Booth." In *Advances in Cryptology - EUROCRYPT '95*. Berlin: Springer-Verlag, LNCS 921, 393-403.

Sakurai, K. and S. Miyazaki. (2000). "An Anonymous Electronic Bidding Protocol Based on New Convertible Group Signature Scheme." In *5th Australasian Conference for Information Security and Privacy - ACISP '2000*. Berlin: Springer-Verlag, LNCS 1841, 385-399.

Schneier, B. (1996). *Applied Cryptography, Second Edition: Protocols, Algorithm and Source Code in C*. New York: John Wiley and Sons.

Viswanathan, K., C. Boyd, and E. Dawson. (2000). "A Three Phased Schema for Sealed Bid Auction System Design." In *5th Australasian Conference for Information Security and Privacy - ACISP '2000*. Berlin: Springer-Verlag, LNCS 1841, 412-426.