IADIS International Journal on WWW/Internet
Vol. 4, No. 1, pp. 55-69
ISSN: 1645 – 7641

SECURE ANONYMOUS PHYSICAL DELIVERY

Esma Aïmeur, Gilles Brassard and Flavien Serge Mani Onana *Département d'informatique et de recherche opérationnelle, Université de Montréal, C.P. 6128, Succursale Centre-Ville, Montréal (Québec), H3C 3J7 Canada*

{*aimeur, brassard, manionaf*}*@iro.umontreal.ca*

ABSTRACT

Privacy in Electronic Commerce transactions is the subject of ever increasing research. However, many challenges remain to be overcome. For example, let us consider a customer, Sir Bob, who buys anonymously a product over the Internet. Since he must receive delivery, how could his anonymity be maintained? When dealing with digital products, several solutions have already been proposed. But if Sir Bob has bought a physical product, it might seem that he must give an address for delivery. This would obviously threaten his right to privacy. Until now, the privacy of physical product delivery has not been considered seriously in the context of e-commerce. Instead, the conventional wisdom is that nothing can be done to solve this problem. In this paper, we introduce Anonymous Delivery Centres as the final step to complete our general *Blind Electronic Commerce* paradigm, which we had initiated in previous work. These centres enable Sir Bob to obtain the physical product he has bought online while keeping his identity confidential.

KEYWORDS

Privacy, Anonymous Delivery, Electronic Commerce, Cryptography, Mix-nets.

1. INTRODUCTION

During the industrial revolution, judge Thomas Cooley [1888] defined privacy as being "the right to be left alone". Since then, this definition gradually evolved to take into account other changes in the world, in particular those relating to new technologies. For instance, Westin [1967] defined privacy as the claim of individuals to determine what information about themselves is known to others, as well as when and how it is used. That definition, which is still current, means that each individual must be the master of his person and of the data that he considers private. Of utmost importance is the privacy of one's *identity*, which refers to any information that makes it possible to determine *physically* who the person is—or at least to seriously circumscribe the possibilities. This includes data such as his name, address, taxpayer number or biometric information used for access control.

Current practice in electronic commerce [Turban, King, Viehland and Lee 2006] does not emphasize privacy issues. It is usual for customers to allow merchants to collect information

about them throughout the process, or even sometimes to volunteer it in exchange for a lame offer. But too often information is collected without the customer's knowledge or approval. Indeed, the merchant can have mechanisms to get the customer's profile, which is a portrait of who he is, as well as his buying and web browsing behaviour.

Consider for instance the case of Sir Bob, a showbiz celebrity who wishes to offer an expensive engagement ring to Claudia. Despite being a star, Sir Bob would not like to see his name making the front page of tabloids! Indeed, he considers that his relation with Claudia is nobody else's business and he wants to preserve as much of his privacy as possible. (We use this example throughout under the name of *Showbiz*.) Unfortunately, if Sir Bob uses standard electronic commerce practices to buy the ring at Alice's online shop, the latter can gather information on him whether or not he so desires. She can use it for many purposes, such as the collection of statistics, data mining, creating his profile, etc. Obviously, this opens the door to several potential abuses from an unscrupulous Alice. For example, she could pool her information with other merchants and/or governments. She could also sell this information, possibly to the press. Information coming from diverse sources could be linked, resulting in the constitution of a formidable dossier on Sir Bob. This would result in a serious erosion of his privacy. Such violations are prohibited in many countries, but there is a lack of effective methods to enforce the law. This problem is exacerbated when information is used about individuals without their knowledge. Should Sir Bob have the proof that his privacy has been violated by Alice, he could complain to the proper authorities, so that justice might be served. However, no amount of "justice" can suffice to restore his privacy.

Well before the advent of electronic commerce, indeed essentially at the same time that Sir Timothy John Berners-Lee was having his first thoughts that would lead him to conceive the World Wide Web, Chaum [1981] introduced the technique of *mix-nets* to implement "untraceable electronic mail, return addresses and digital pseudonyms". Chaum's approach enabled an electronic mail system to hide the identity of email senders, yet provided the receiver with the possibility of sending back his response to the right person through an untraceable return address. With that seminal paper, Chaum initiated the study of privacy in the context of electronic communication. His approach to "transactions without identification" [Chaum 1985], amongst several other papers, continued his legendary fight against Big Brother by the introduction of different *pseudonyms* that an individual can use when he does business with different organizations. This thwarts the threat of linking records about one individual coming from different sources.

Following in Chaum's footsteps, and loosely inspired by the *Customer Buying Behaviour* model of Guttman, Moukas and Maes [1998], we have recently introduced the *Blind Electronic Commerce* paradigm [Aïmeur, Brassard and Mani Onana 2006], which aims at eliminating any information that a merchant could obtain about a customer throughout the entire electronic commerce process: while he is looking for what to buy, during optional negotiations, while he is buying and even after he has bought. We have also proposed an approach to privacy-preserving recommender systems [Aïmeur, Brassard, Fernandez and Mani Onana 2006]. Taken together with [Aïmeur, Brassard and Mani Onana 2005], these papers offer a complete and integrated proof-of-principle solution to the privacy-preserving electronic commerce conundrum, with one major exception: We had left open the issue of secure anonymous delivery of *physical* items. This is precisely the topic of the current paper, which therefore provides the final step to complete the full anonymity of the Internet buying process provided in our Blind Electronic Commerce paradigm. For this purpose, we introduce the notion of *Anonymous Delivery Centres* (ADCs). Naturally, the interest and utility of

anonymous delivery goes well beyond its application for electronic commerce. Anonymous Delivery Centres can be used in any context in which a physical delivery has to be made to a receiver who must remain anonymous.

Several different approaches can serve to design ADCs. For example, a direct physical analogue to Chaum's mix-nets can be considered, keeping in mind that Chaum's original purpose was to provide sender anonymity whereas we are interested in receiver's anonymity. Even though we discuss that possibility (Figure 2), we favour a different approach, in which an ADC consists of three main parts: the Deposit Unit, in which the merchant or his delivery agent deposits the item to be delivered, the Mix-delivery System, which is the item's *anonymizer*, and the Retrieval Unit, from which the customer or his representative (another delivery agent for instance) picks up the item. These three main parts are described in detail in Section 4, with an illustration given in Figure 3.

Using the Showbiz example, suppose that Sir Bob has anonymously bought a ring from Alice's shop over the Internet. In order to deliver the ring to Sir Bob, it would seem that Alice needs information on Sir Bob, such as address, e-mail, phone number, etc. But Sir Bob does not want to reveal any information that could threaten his privacy. In our solution to this Anonymous Delivery conundrum, the use of an ADC enables Sir Bob to protect his privacy. More detail about this example is given in Section 4.5.

We are aware that not everybody will embrace our wish for privacy. Nevertheless, we believe that privacy is a *fundamental* right for all humans, and every means to protect it should be given serious consideration. In particular, no individual should ever have to justify a wish for privacy, and such wish should never be considered suspect *a priori*. Article 12 in the *Universal Declaration of Human Rights* states that "No one shall be subjected to arbitrary interference with his privacy". No doubt our idealistic position will be considered extreme by some. Implementing it might even go against the law in some countries. But at the very least, discussing it can serve to shift the middle ground in the right direction.

After this Introduction, we review in Section 2 the notions of delivery in electronic commerce, public key cryptography and Chaum's mix-nets. In Section 3, we show how mix-nets can be adapted with minimal conceptual changes to deliver anonymously physical items, but this approach is fraught with shortcomings. Then, we present in Section 4 our proposed architecture for a secure anonymous physical delivery system. We wrap up in Section 5 with a discussion in which we conclude with perspectives for future work.

2. PRELIMINARIES

In this section, we review preliminary notions that are important to understand Anonymous Delivery Centres. Specifically, we review the (anonymous) delivery process in electronic commerce, public key cryptography and public key infrastructures, and Chaum's original mix-net architecture for the anonymous delivery of digital messages.

2.1 Delivery in e-Commerce

In general, delivery is the process of transferring an item from one party, the *Sender*, to another, the *Receiver*, through one or several *Delivery Agents*, as shown in Figure 1. A delivery agent is a company or individual that takes the item to be delivered from the sender or

from another delivery agent to the receiver or to another delivery agent. For example, if Alice wishes to send a package to Sir Bob, she may do so through a delivery company such as FedEx, DHL, UPS, etc. In the case of electronic mail, one or more entities on the Internet (Internet Service Provider (ISP), Proxy Servers, etc.) can be used to convey the e-mail from Alice to Sir Bob; each entity forwards the e-mail to the next one until the final recipient is reached. According to the traditional paradigm, the delivery process requires identification information about the receiver and sometimes also about the sender, such as their names and addresses. This information allows the delivery agent to find either the next delivery agent to which the item must be forwarded or the final receiver.

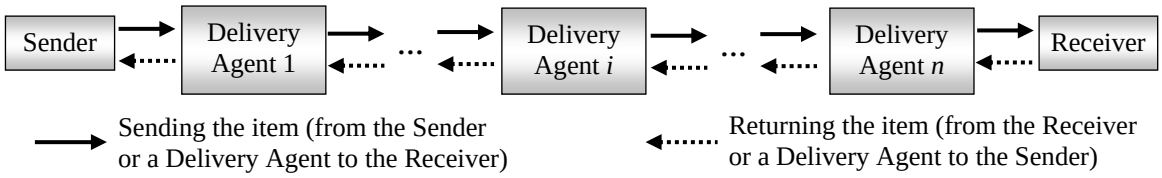

Figure 1. The delivery entities

To protect the privacy of customers in electronic commerce, *Anonymous Delivery* becomes an essential commodity. This consists in the delivery of an item from a sender to a receiver, without revealing any of the receiver's personal information or identity to the sender. The item could be digital, such as a song or piece of software, or physical, such as Sir Bob's engagement ring for Claudia. We define an *Anonymous Delivery System* as a system that supports the practice of anonymous delivery, meaning that the sender and the receiver both use the system in order to complete the delivery process in a way that guarantees the privacy of the receiver all along the delivery process.

The anonymous delivery of *digital* products has been well studied in the past [Aiello, Ishai and Reingold 2001]. It requires that the customer be able to *surf the web anonymously*, which allows him to send requests and receive responses from the merchant (including the digital good to be delivered) without being traced. If he sits in an Internet café, the product can be downloaded directly, preferably on his portable storage medium, such as a USB memory stick. More conveniently, *trusted identity proxies* can be used by the customer to recover the digital product in the comfort of his home or office. These proxies offer the possibility of surfing on the Internet without giving away personal information to other websites [Boyan 1997; Gabber, Gibbons, Kristol, Matias and Mayer 1999; etc.]. This is done by rewriting the user's request via the browser and cleaning the resulting pages that are returned to the user. However, this solution assumes that the identity proxy is indeed trustworthy, and the user's privacy depends crucially on this assumption. If no single party can be trusted, Chaum’s mix-nets can be used, as we review in Section 2.3, in which case an untraceable return address can serve to deliver the digital good.

Possible solutions to the anonymous delivery of *physical* items also depend on whether or not the customer is willing to trust a third party. Thus, we define two main types of Anonymous Delivery Systems.

2.1.1 Trust-based anonymous delivery

The anonymous delivery of *physical* goods is relatively easy provided the receiver trusts a third party. In this case, it suffices for the receiver to authorize the trusted party to pick up the

item from the sender and convey it to him. There are companies dedicated exclusively to protecting the receivers' privacy such as *ContinentalRelay* [URL1]. These companies specialize in offering anonymous maildrop and forwarding services to their customers, concerning mail, packages, postcards, voice-mail, fax and anonymous e-mail. To ensure the privacy of their customers, they provide them with such services as a private street and PO Box anonymous mail drop address, or an anonymous e-mail address. Items they receive are re-addressed and forwarded to the appropriate customers. Obviously, if that third party and the merchant are in collusion, all privacy is lost for the customer. It is therefore natural to investigate the possibility of secure anonymous physical delivery without the need to trust any specific intermediary.

2.1.2 Secure anonymous delivery

If there is no third party that the receiver is willing to trust, the anonymous delivery of physical goods becomes more challenging. In fact, it is often claimed as self-evident that the security possible in the world of digital delivery cannot be extended to the case of physical items. Nevertheless, the purpose of this paper is to introduce a *Secure Anonymous Physical Delivery System*. According to our solution, the customer's privacy can be violated only by the collusion of a significant number of *delivery agents*, so that no single entity need be trusted in particular.

2.2 Public Key Cryptosystems and Infrastructures

Public Key Distribution and Public Key Cryptosystems (PKCs) were introduced independently by Merkle [1978] and by Diffie and Hellman [1976]. Formally, a PKC consists of three efficient algorithms: a *Key-Generation Algorithm* that generates pairs of Private Key and Public Key, an *Encryption Algorithm E* that computes the ciphertext $c = E(P, m)$ for a message m, given the public key P, and a *Decryption Algorithm D* that computes the cleartext message $m = D(K, c)$ back from the ciphertext, given the private key K.

PKCs can be *probabilistic*, in which case a *randomization set R* is involved. In addition to the cleartext and public key, the encryption algorithm takes a randomly chosen element of R in order to produce the ciphertext. The decryption algorithm, on the other hand, has access only to the ciphertext and the private key to recompute the cleartext. One advantage of probabilistic PKCs is that they prevent a *guessing attack* (such as the well-known *dictionary attack*) by which one could verify if a given cleartext is correct by encrypting it with the public key and comparing the resulting ciphertext with the one whose decryption is being seeked.

Public Key Infrastructures (PKIs) have been introduced to make it possible to provide security services on the basis of PKCs. A PKI enables a security environment through a set of policies used to integrate and manage all the security parameters suitable for a great number of services, such as authentication of entities, digital signature, secure communication between entities (customers, partners, suppliers, etc.). A PKI aims at managing certificates and pairs of private and public keys, including the ability to issue, maintain, recover and revoke public key certificates. PKIs make use of Certification Authorities (CAs), which are trusted entities whose central responsibility is certifying the authenticity of users and their public keys. More precisely, a user certificate issued and signed by a CA acts as proof that the legitimate public key is associated with the user.

2.3 Chaum's Mix-Nets

Recall that the mix-nets were invented by Chaum [1981] for the primary purpose of implementing sender anonymity in electronic mail. This is based on the notion of a *mix*, which is a computer that forwards incoming messages in a special way. It waits until some number of messages have arrived, and then it outputs them one by one in random order. (Chaum's original proposal used lexicographic reordering but random reordering will be more convenient for our purpose.) As long as a transformation is applied on those messages to make them unrecognizable, this hides the correspondence between incoming and outgoing messages. This effect is amplified if we consider a sequence of mixes that implement independent random shuffles. At the end of the sequence, it is impossible to link the final outgoing messages with the original incoming messages provided at least one of the mixes stays honest and refuses to disclose the random permutation it has used. But how can the last mix know to whom each outgoing message is finally destined?

This question is answered by the use of what we call the *mix-message*. We assume that each mix, as well as the final receiver, subscribes to a public key infrastructure and that probabilistic encryption is used. At the beginning, the sender accesses all the relevant public keys, say P_A for the receiver and P_1, P_2,…, P_n for the mixes, were P_1 corresponds to the first mix and P_n to the last one. If confidentiality is desired in addition to sender anonymity, the sender encodes his message m with the receiver's public key, yielding $c = E(P_A, m)$. To this ciphertext, the sender appends the identity A of the receiver in the clear. Then, the sender successively encodes that compounded message with the public key of each mix, starting with the last. The resulting *mix-message*, which is input by the sender into the first mix, is $E(P_1, E(P_2, \ldots E(P_n, c, A)\ldots))$. One by one, each mix uses its corresponding private key to remove one encryption layer before forwarding the result to the next mix in random order. When the final mix obtains c and A, it forwards c to A, who can decrypt it by use of his private key K_A and finally recover m without being able to identify the original sender. Note that the use of probabilistic encryption makes it infeasible to link the messages coming out from a mix with those that entered it. In Chaum's original proposal, a random pad was added to messages before encrypting them with a deterministic public-key encryption scheme such as RSA [Rivest, Shamir and Adleman 1978].

3. A DIRECT PHYSICAL ANALOGUE OF CHAUM'S MIX-NETS

There is an obvious physical analogue of Chaum's mix-nets. Again, we use a fixed sequence of mixes. This is illustrated with only two mixes in Figure 2, but more mixes would be necessary to offer adequate security. Instead of manipulating digital messages, each mix manipulates physical objects. After a sufficient number of objects have been deposited, the first mix packages them in order to make them indistinguishable, it shuffles them randomly and passes them on to the second mix. Each mix in turn proceeds in the same way, including adding a layer of packaging to make sure the packages are indistinguishable even if the previous mix was dishonest and left subliminal marks on the packages. All packages become available at the same time when the last mix outputs them. This leads us to the same question

we had in our top-level description of Chaum's mix-nets: How can the last mix know to whom each package is finally destined?

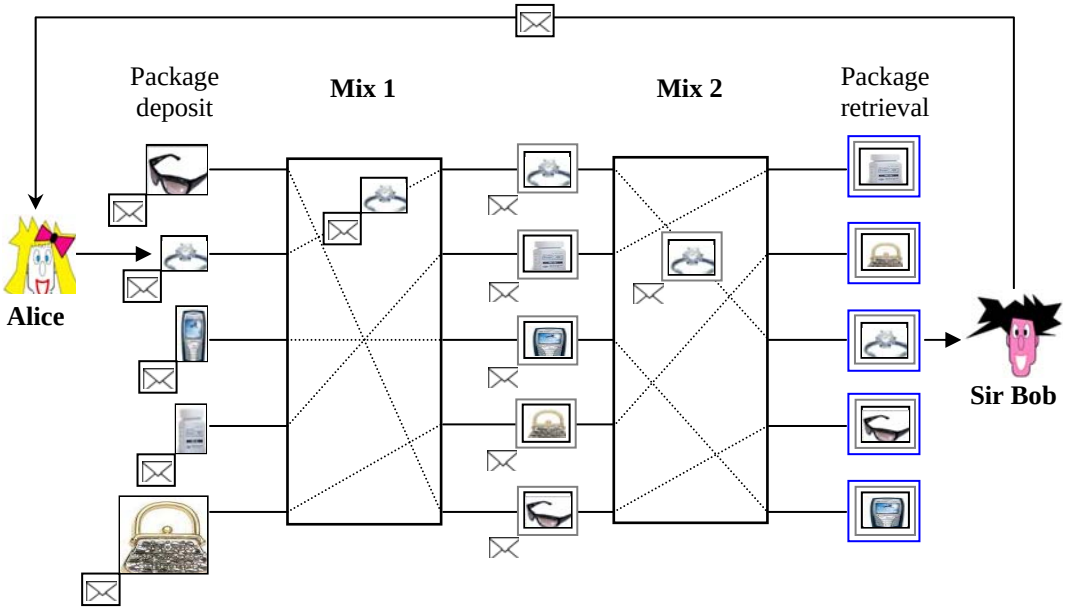

Figure 2. A direct physical analogue to Chaum's mix-nets

Recall that Chaum's solution was to have the sender prepare a mix-message that contains the identity of the receiver under multiple layers of encryptions. It seems at first that this approach is no longer possible since the entire point of the exercise is that the sender should not know the identity of the receiver! Indeed, the purpose of Chaum's mix-nets was to hide the identity of the *sender* whereas we are interested here in hiding the identity of the *receiver*. Fortunately, there is a simple solution: it is the receiver who creates the mix-message, not the sender. Once it is ready, the receiver transmits the mix-message anonymously to the sender by use of Chaum's *original* mix-net. This is possible precisely because the mix-message is digital. This is illustrated by the direct arrow going around the top from Sir Bob to Alice in Figure 2. Now, it suffices for the sender to append the receiver-prepared mix-message to the physical package when he comes to the first mix for deposit. In addition to repackaging and shuffling, each mix strips out one layer of encryption from the mix-message, so that the last mix knows to whom the multiply packaged object should be delivered.

This direct physical analogue of Chaum's mix-nets suffers from a number of drawbacks. We mention only the two most severe problems here. Firstly, a collusion of the sender with the last mix would allow the former to obtain the list of people who received packages from the batch that included his own package. This would seriously circumscribe the identity of the receiver unless the first mix waits for a very large number of packages before forwarding them to the second mix in a random order. Secondly, the prescription according to which the objects must be packaged to make them indistinguishable is not very realistic because of size and weight considerations. For instance, it is not clear how the handbag was shrunk to the size of an engagement ring after going through the first mix in Figure 2!

In order to alleviate those shortcomings but retain the advantages of secure anonymous physical delivery, we introduce now our solution to this conundrum. This solution is still inspired by Chaum's mix-nets, but also by the subsequent notion of Onion Routing [Goldschlag, Reed and Syverson 1999].

4. ANONYMOUS DELIVERY OF PHYSICAL ITEMS

An Anonymous Delivery System for physical items based directly on Chaum's mix-nets was described in Section 3, but we have seen that this approach is fraught with shortcomings. We propose below a Secure Anonymous Physical Delivery System in which the receiver's privacy is guaranteed unless several agents collude against him. We start this section by giving some definitions and notation that will be useful to understand our system.

4.1 Definitions and Notation

A *Delivery Point* is a place where the item to be delivered undergoes some transformations, for instance packaging and labelling. The sender and receiver are considered to be delivery points.

A *Delivery Agent* is an entity or an individual that carries the item to be delivered from one delivery point to another. In particular, each delivery agent constitutes a delivery point.

A *Mix-delivery System* is a network made of several delivery agents.

An *Anonymous Delivery Centre* (ADC) is a physical space dedicated to anonymous delivery. Among many possible topologies, we are considering that an ADC is composed of several compartments communicating through a horizontal rotary surface, called *H*, on which the items are placed. Each compartment belongs to a given delivery agent. The delivery agent has access to the contents of *H* for retrieval or deposit, meaning that it can pick an item from *H*, make some transformations and put it back.

A *mix-message*, *c*, is a message addressed to a Mix-delivery System, such that each delivery agent has access to at most one piece m_i of the whole message. The message m_i tells the delivery agent how to manage the item *p* being delivered. It is composed of two main parts: the action to apply on *p* (relabelling for example) and the remaining mix-message to associate with the item for the subsequent delivery agents, if any. At any moment, only the first part of the mix-message can be in the clear, meaning that only the delivery agent that possesses the item and that has been chosen by the receiver (see Section 4.2) is able to decipher this part. This is very similar to the mix-messages described in Sections 2.3 and 3.

The *Weight List*, *W*, is a list of weights acceptable in the ADC. When a merchant comes with an item for delivery, the Deposit Unit (see Section 4.3) chooses at random a type of packaging that can contain the item. The Deposit Unit fills empty spots in the package with some futile objects as necessary to obtain some weight that belongs to list *W*. We call that process *Weight-based Packing*.

Formal description of a mix-message: A mix-message *c* is a ciphertext formed from *t* cleartext messages m_1, m_2,…, m_t to be addressed to *t* delivery agents R_1, R_2,…, $R_t \in \{A_1, A_2, \ldots, A_n\}$ selected by the receiver. Message m_i is addressed to delivery agent R_i. In particular, R_t is the Target Delivery Agent from which the receiver will finally pick up the item being delivered. These messages are enciphered as follows:

- After choosing an ADC, the receiver picks in secret t delivery agents from that ADC. He obtains their respective public keys P_1, P_2,…, P_t from the ADC's public-key infrastructure.
- The receiver uses the target delivery agent's public key P_t to encipher $c_t = E(P_t, m_t, Stop = d)$, where "*Stop*" allows R_t to recognize that it has been chosen as target delivery agent by the receiver, d is a code that will be used later to recover the item and m_t could give R_t additional instructions.
- For $i = t-1$ downto 1, the receiver computes $c_i = E(P_i, m_i, c_{i+1})$, where m_i gives optional instructions to R_i about the package. The final mix-message is $c = c_1$.

The opening procedure of a mix-message proceeds in the reverse order:

- For $i = 1$ to t, delivery agent R_i uses his private key K_i to compute $D(K_i, c_i) = D(K_i, E(P_i, m_i, c_{i+1})) = (m_i, c_{i+1})$, thus getting cleartext m_i and ciphertext c_{i+1}. Cleartext m_i indicates some actions (such as relabelling) to be performed by R_i while c_{i+1} is the leftover mix-message that R_i sticks on the item for the benefit of R_{i+1} when $i < t$. Note that R_i performs this task without any need to know who R_{i+1} is. At the end, the target delivery agent R_t gets message $(m_t, Stop = d)$, keeps the item, remembers d, and waits for the retrieval process.

Delivery agents R_1, R_2,…, R_t are chosen by the receiver from the set of all delivery agents $\{A_1, A_2,\ldots, A_n\}$ in the ADC, with $t \leq n$. Of course, there can be agents sitting between R_i and R_{i+1}. Since nothing in the mix-message says explicitly who is the next active agent, all such intervening agents must use their private key to attempt deciphering the mix-message. After finding the first part to be gibberish, they let the item go undisturbed to the next delivery agent. The fact that no delivery agent has a chance to learn who is the next delivery agent designated by the receiver would make it even harder to subvert the system.

4.2 Anonymous Delivery Centre Overview

Secure Anonymous Delivery is a mechanism to facilitate the anonymous delivery of *physical* items by way of several trusted third parties, called delivery agents (see Section 4.1).

After having paid Alice for an item p, Sir Bob chooses an ADC as well as a set of t delivery agents from the ADC, he decides on optional instructions m_i for each agent R_i, and he computes the corresponding mix-message c, as explained in Section 4.1. Then, Sir Bob tells Alice his choice of ADC and he gives her c. Alice (or her delivery agent) brings the item at the Deposit Unit U of the ADC (see Figure 3) and gives it Sir Bob's mix-message c. The main role of U is to apply the Weight-based Packing process (see Section 4.1) and issue a receipt to Alice (or her delivery agent) as a proof of deposit.

The Mix-delivery System then takes control of the item. Recall that each delivery agent of a mix-delivery is associated with a delivery point. Let the set of all delivery agents in the ADC be $S = \{A_1, A_2,\ldots, A_n\}$. We assume that each delivery agent A_i takes exactly the same amount of time to act on any given item. Without loss of generality, we consider that H rotates through the delivery points according to their ordering in S. So A_1 is first to receive the item from Deposit Unit U. Now, A_1 tries to decipher Sir Bob's mix-message using his private key. If it succeeds, it applies the action required by the message, if any, and it relabels the item with the leftover mix-message, as explained in Section 4.1. If deciphering of the mix-message fails (because A_1 was *not* the first delivery agent selected by Sir Bob), then A_1 simply puts the item

back on *H*, undisturbed. The process continues, one delivery agent after another, until the item reaches Sir Bob's chosen target delivery agent R_t, which also applies any action prescribed by Sir Bob in the corresponding message m_t. At this point, the item is kept at R_t's delivery point and replaced on *H* by a fake item indistinguishable from the real one, so that no one else can notice that this package has reached its target agent. Fake packages can be identified after a while because their labels have not been modified during an entire turn, but this does not compromise the identity of the target agent. They are removed at regular interval by a garbage collector.

To retrieve item *p*, Sir Bob knows his chosen target delivery agent A_t and the code he had inserted in *Stop* = *d*. In fact, $d = f(x)$ for a public one-way function *f* and a secret input *x* known only of Sir Bob. In order to convince A_t that *p* belongs to him, he must prove his knowledge of *x*. Depending on the level of trust he has in A_t, he may wish to use a zero-knowledge protocol for this last step, before collecting the item. Instead of picking *p* by himself, he could use some new delivery agent *A*' to transfer *p* to another Anonymous Delivery Centre where the whole process (from a new *U* to a new A_t) would take place all over again. For this, he must help *A*' convince A_t about his knowledge of *x*.

4.3 Architecture of Anonymous Delivery Centres

The architecture of an Anonymous Delivery Centre (ADC) is given in Figure 3. An ADC consists of three components: the Deposit Unit, the Mix-delivery System and the Retrieval Unit.

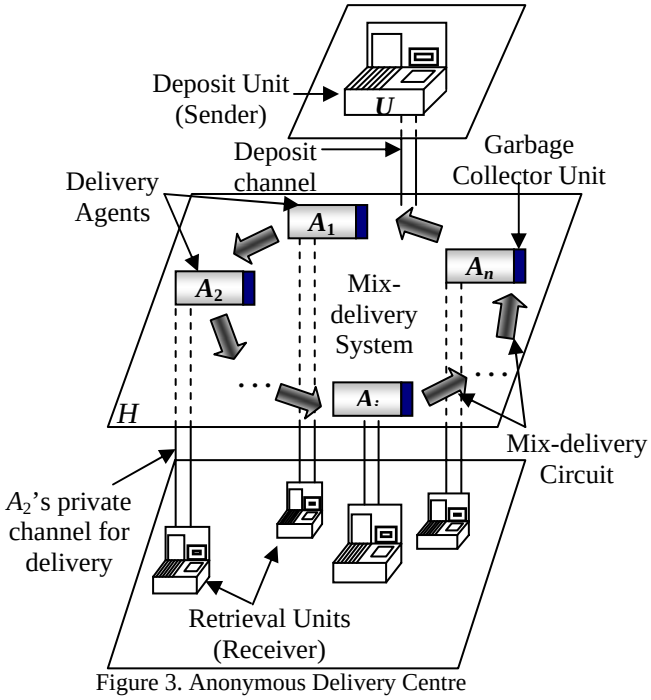

Figure 3. Anonymous Delivery Centre

The Deposit Unit is used by the Merchant or her representative to introduce the item into the ADC. There is only one Deposit Unit for any given ADC. The Mix-delivery System is defined in Section 4.1. The retrieval Unit is used by the Customer to pick up the item. In an ADC, Retrieval Units are physically separated and each delivery agent has its own. For increased security, Retrieval Units can (and should) be manufactured by different companies.

4.4 Formal Description of Anonymous Delivery Centres

Each ADC component (Deposit Unit, Mix-delivery System or Retrieval Unit) operates using an algorithm. We give the pseudo-code of these algorithms below.

DepositAlgorithm(c)

1. Ask the merchant to enter the mix-message c.
2. Open the Deposit Unit door and initialize the *timeout*.
3. Ask the merchant to put the item inside the door.
4. Close the Deposit Unit door when item is deposited or if timeout expires.
   (a) If an item has been deposited, Weight-based package it and label it with the mix-message. Transfer the labelled item to the mix-delivery system. Issue a receipt for the merchant.
   (b) If timeout has expired, cancel the operation and ask the merchant to try again later.

MixAlgorithm(c)

1. The item p, labelled c, goes from one delivery agent to another. As long as p circulates in the Mix-delivery System, each delivery agent A picks it up and tries to decipher its label c using its private key K. If unsuccessful, item p proceeds to the next agent. If successful, $D_K(c) = (m, c')$. Agent A performs task m if any. Then,
   (a) if c' is of the form $Stop = d$, the target agent R_t has been reached; it keeps the item, remembers d, and forwards an indistinguishable fake item to the next agent;
   (b) otherwise agent A relabels item p with label c' and lets it proceed to the next agent.
2. Target agent R_t waits for the retrieval connection from the customer—Execution of *RetrievalAlgorithm*(d).

RetrievalAlgorithm(d)

1. The customer (or his agent) enters the Retrieval Unit of his previously chosen target delivery agent R_t.
2. R_t asks the customer to prove knowledge of x such that $f(x) = d$.
   (a) If the verification is unsuccessful, cancel the operation and ask the customer to try again later.
   (b) If the verification is successful, then R_t transfers the item to its Retrieval Unit, opens the Retrieval Unit door and initializes a *timeout*.
   (c) R_t asks the user to pick up the item.
   (d) R_t closes the Retrieval Unit door once the item has been picked up or if timeout expires.
   (e) If timeout has expired, cancel the operation and ask the customer to try again later.

4.5 Example to Illustrate Anonymous Delivery

Coming back to our Showbiz example, Sir Bob chooses an ADC for the delivery of his engagement ring. Let us say the ADC is composed of five delivery agents A_1, A_2, A_3, A_4, A_5. Sir Bob selects three of these agents, say $R_1 = A_2$, $R_2 = A_5$ and $R_3 = A_3$. He accesses their public keys P_2, P_5, P_3, respectively, and uses them to create the mix-message $c = E(P_2, m_1, E(P_5, m_2, E(P_3, m_3, Stop = d)))$ from the cleartext $m = (m_1, m_2, m_3)$, where m_1 = "Please, forward the item", m_2 = "Please, keep the item for one day", m_3 = "Please cover the item in a brown bag", and $d = f(x)$ for some x that he has secretly selected.

Next, Sir Bob tells Alice which ADC he has decided to use, and gives her the mix-message c. Alice packages the ring. She uses *DepositAlgorithm*(c) to introduce the ring into the ADC, through the Deposit Unit.

The ring is Weight-based package by the Deposit Unit, which forwards it to A_1's delivery point. Delivery agent A_1 does not alter the package since Sir Bob did not select it as initial agent in his mix-message. More precisely, A_1 tries to decipher c, finds gibberish, and forwards the item to A_2.

The next delivery agent, A_2, computes $D(K_2, c) = D(K_2, E(P_2, m_1, E(P_5, m_2, E(P_3, m_3, Stop = d))))$ and gets message m_1 and ciphertext $c_1 = E(P_5, m_2, E(P_3, m_3, Stop = d))$. Since m_1 is meaningful, A_2 relabels the packaged ring with leftover mix-message c_1 and forwards it to the next agent (as requested in m_1) by putting it back on H.

Then, A_3 tries to decipher c_1 but he obtains gibberish since private key K_5 is required for this operation. Hence, A_3 puts the package intact back on H. Note that this occurs even though A_3 was chosen by Sir Bob as his delivery agent R_3 because its time has not yet come. Similarly, A_4 tries to decipher c_1, fails, and put the package back on H for A_5 to look at it.

Now, A_5 computes $D(K_5, c_1) = D(K_5, E(P_5, m_2, E(P_3, m_3, Stop = d)))$, obtains cleartext m_2 and ciphertext $c_2 = E(P_3, m_3, Stop = d)$, keeps the package for one day (since such are the instructions in m_2) and inserts a fake item on H to hide that fact. At a random time the next day, A_5 relabels the package with leftover mix-message c_2 and surreptitiously puts it back on H.

Having travelled one full time around the loop, the package comes back to A_1, who has no idea that this is a package it had already handled on the previous day. The outcome is the same as before and it puts it back on H. The same thing happens with A_2.

Finally, A_3 gets the package for the second time as well (not knowing this, of course). It computes $D(K_3, c_2) = D(K_3, E(P_3, m_3, Stop = d))$ and discovers it had been selected to be the target agent. Following the instructions in m_3, it puts the package in a brown bag (not knowing it contains a ring since the original packing from the Delivery Unit is still strong). Later, Sir Bob walks in the Delivery Unit of A_3 and picks up the ring by use of *RetrievalAlgorithm*(d), thanks to his knowledge of x. Sir Bob could also ask another delivery agent, A', to pick up the ring from A_3 and transfer it to another ADC, where the entire process would take place all over again.

4.6 Managing Post-Delivery

Sometimes, it is desirable that the customer could be reached after delivery. For example if there is a product recall stating that the item the customer had received for delivery is found to

be defective or even dangerous, then the ADC should have a way to reach the customer. One solution to this problem consists in using untraceable return e-mail addresses, as proposed by Chaum [1981]. The customer could also blindly query the merchant's maintenance database on a regular basis, using our blind maintenance protocol [Aïmeur, Brassard and Mani Onana 2006]. Moreover, if the customer is not satisfied with the item he received anonymously, he must be able to send it back to the merchant by use of possibly another Anonymous Delivery System, which must now hide the identity of the sender.

5. DISCUSSION AND CONCLUSION

Chaum's original concept of a mix-net [Chaum 1981] is very well adapted to its intended purpose, which is to provide *sender* anonymity for *digital* messages. However tempting it may be to translate the idea directly to provide *receiver* anonymity for *physical* products, the resulting scheme is unsatisfactory. This has prompted us to propose a slightly different approach, which draws on Chaum's ideas but is also reminiscent of the subsequent notion of Onion Routing [Goldschlag, Reed and Syverson 1999]. We have given the name of Anonymous Delivery Centre (ADC) to our architecture. Even though we believe that our solution is preferable to adapting Chaum's mix-nets directly, we acknowledge that there are still problems with it, which we offer as open questions for further research.

First of all, in Chaum's original technique of mix-nets (as well as in onion routers), the content of a given e-mail is both unknown and unalterable by the intermediaries. This translates in a potential weakness when applying this technique to the physical world in which packages can be opened, examined and sealed again. In particular, the merchant could collude with the target delivery agent and get a picture of the customer or his representative when he comes to pick up the package. This attack threatens the customer's privacy. Nevertheless, this would happen with reasonably small probability because the use of a mix-message does not reveal the target delivery agent to the merchant. In fact, no delivery agent could even predict ahead of time that it has been chosen as target!

For a more subtle threat, the merchant could collude with one or more delivery agents that open some packages as they circulate in the mix-delivery system. To overcome this threat, we need to study the technological feasibility of tamper-proof packages that cannot be opened without detection, but the issue is complicated by the fact that none of the packaging is under the control of the customer! Therefore, each agent would have to check that the previous agents have not tampered with the package. Details on this issue are beyond the scope of this paper, and we leave them for further research. We also leave for further research the procedure for detecting if a delivery agent keeps the package for itself. One solution to this problem could be the introduction of a trust environment in which customers express their trust, through global votes, in delivery agents of the ADC.

Another problem is the use of tracking devices such as Radio Frequency IDentification (RFID) tags [URL2]. The RFID technology could help track items and spy on people at a distance. According to our solution, one may imagine that each delivery agent in the ADC has some means to perform tag-killing. In this case, our solution is considered as being technology-based in the sense that the association tag/tag-killing is comparable to that of virus/anti-virus, spam/anti-spam, cryptography/cryptanalysis, etc.

Last but not least, the delivery process in some cases can be time consuming. However, this can be considered as a price to pay for privacy, as it is already the case for several other schemes (privacy-preserving data mining, oblivious transfer, etc.) that protect all or part of the customer's sensitive data.

In this paper, we have introduced the notion of an Anonymous Delivery Centre (ADC) for physical items. An ADC consists of three main components: a Deposit Unit to put items into the ADC, a Mix-delivery System to anonymize the items and a Retrieval Unit to pick up items from the ADC. We have left for future work the implementation of the first prototype of an ADC as well as a way to make sure that some delivery agents did not open the packages during the delivery process and that tracking devices cannot be used without detection.

As we admitted in the Introduction, we are aware that not everybody will embrace our wish for privacy. Some people may approve of the constitution of dossiers on their buying habits because that might increase the probability that they receive occasional relevant spams. Clearly, our position is that privacy is a non-negotiable fundamental human right and that every effort must be deployed to protect it. But in the end, the final choice belongs with each individual

ACKNOWLEDGEMENT

We are grateful to the reviewers of the IADIS conference version of this paper for their constructive comments. This paper benefited from a discussion with David Chaum, who told us he has had unpublished ideas along similar lines. The representations of Alice and Bob in Figure 2 are courtesy of Claude Crépeau.

This work is supported in part by the Natural Sciences and Engineering Council of Canada (NSERC). In addition, G.B. is supported in part by the Canadian Institute for Advanced Research (CIAR) and the Canada Research Chair Programme.

REFERENCES

Aiello, B., Ishai, Y. and Reingold, O., 2001. Priced Oblivious Transfer: How to Sell Digital Goods. *Advances in Cryptology: Proceedings of Eurocrypt 01*. Innsbruck, Austria, pp. 119–135.

Aïmeur, E., Brassard, G., Fernandez, J.M. and Mani Onana, F.S., 2006. ALAMBIC: A Privacy-Preserving Recommender System for Electronic Commerce. *ACM Transactions on Internet Technology*. To appear.

Aïmeur, E., Brassard, G. and Mani Onana, F.S., 2005. Blind Negotiation in Electronic Commerce. *Proceedings of Montreal Conference on eTechnologies*. Montréal, Canada, pp. 35–43.

Aïmeur, E., Brassard, G. and Mani Onana, F.S., 2006. Blind Electronic Commerce. *Journal of Computer Security*. To appear.

Boyan, J., 1997. The Anonymizer: Protecting User Privacy on the Web. *Computer-Mediated Communication Magazine*, Vol. 4, no. 9.

Chaum, D., 1981. Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms. *Communications of the ACM*, Vol. 24, no. 2, pp. 84–88.

Chaum, D., 1985. Security Without Identification: Transaction Systems to Make Big Brother Obsolete. *Communications of the ACM*, Vol. 28, no. 10, pp. 1030–1044.

Cooley, T., 1888. *A Treatise on the Constitutional Limitations Which Rest Upon the Legislative Power of States of the American Union*, 2nd edition. Callaghan & Co., Chicago.

Diffie, W. and Hellman, M.E., 1976. New Directions in Cryptography. *IEEE Transactions on Information Theory*, Vol. IT-22, no. 6, pp. 644–654.

Gabber, E., Gibbons, P.B., Kristol, D.M., Matias, Y. and Mayer, A.J., 1999. Consistent, Yet Anonymous, Web Access with LPWA. *Communications of the ACM*, Vol. 42, no. 2, pp. 42–47.

Goldschlag, D., Reed, M. and Syverson, P., 1999. Onion Routing for Anonymous and Private Internet Connections. *Communications of the ACM*, Vol. 42, no. 2, pp. 39–41.

Guttman, R.H., Moukas A.G. and Maes, P., 1998. Agent-Mediated Electronic Commerce: A Survey. *Knowledge Engineering Review Journal*, Vol. 13, no. 3, pp. 985–1003.

Merkle, R.C., 1978. Secure Communications over Insecure Channels. *Communications of the ACM*, Vol. 21, no. 4, pp. 294–299.

Rivest, R.L., Shamir, A. and Adleman, L.A., 1978. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, Vol. 21, no. 2, pp. 120–126.

Turban, E., King, D., Viehland, D. and Lee, J., 2006. *Electronic Commerce: A Managerial Perspective*. Prentice Hall.

Westin, A., 1967. *Privacy and Freedom*. Atheneum, New York.

[URL1] www.continentalrelay.com. Anonymous Mail Drop & Mail Forwarding Service. Accessed 15 May 2006.

[URL2] en.wikipedia.org/wiki/RFID, Radio Frequency Identification, accessed 15 May 2006.