APOD: Anonymous Physical Object Delivery

Elli Androulaki and Steven Bellovin

Columbia University
{elli,smb}@cs.columbia.edu

Abstract. Delivery of products bought online can violate consumers' privacy, although not in a straightforward way. In particular, delivery companies that have contracted with a website know the company selling the product, as well as the name and address of the online customer. To make matters worse, if the same delivery company has contracted with many websites, aggregated information per address may be used to profile customers' transaction activities. In this paper, we present a fair delivery service system with guaranteed customer anonymity and merchant-customer unlinkability, with reasonable assumptions about the threat model.

1 Introduction

A lot of work has been done over the last 25–30 years on privacy for networking and paying for products. Here, we address privacy concerns from the delivery of products to the buyers. Delivery of purchases made online is usually performed by a courier company who has contracted with the website selling the product (merchant). Based on the current product delivery infrastructure and a plausible threat model, we propose a privacy-preserving product system.

Privacy Concerns. Product delivery raises many privacy concerns, primarily deriving from information the delivery company acquires from the merchant. As noted, the delivery company is usually under contract to the seller. Given the (usually) long-term monetary relationship between the two, the delivery company knows the following: *(a)* the type of products the merchants sell; *(b)* the name and shipping address of the person the product is for. This person may or may not be the one who bought the product; *(c)* the exact object shipped, if it is fragile or of great value.

Certainly, the courier company knows the person to whom the product is delivered, as well as the type of the product. In addition, since the same delivery company may serve a variety of other websites, the former may obtain a very good approximation of the transaction profile of consumers who often make purchases online.

Our Contribution. In this paper, we will introduce a privacy-preserving delivery system based on package-routing through multiple courier companies, where,

- the courier company knows at most the merchant or the type of the product shipped, but not the recipient.
- there is no way for the merchant to recover the address of the intended recipient without collaborating with more than one courier company.

I. Goldberg and M. Atallah (Eds.): PETS 2009, LNCS 5672, pp. 202–215, 2009.

We emphasize on the fact that our system is deployable. Our threat model is based on the powers of any current real-world delivery system entities. For the purposes of our protocols, we made use of blind ([C81], [CL02], [O06]) and group ([CS97]) signatures as well as of blind group signature schemes ([LR98]).

Organization. In the following section we provide a brief overview of our system entities and requirements with a particular focus on privacy definition and threat model. Sections 3 and 4 present in detail our delivery protocol and discuss many deployability and security issues related to it.

2 System Architecture

As in all currently-deployed e-commerce systems, the most important entities are:

- **Merchants**, who are the entities who maintain a website selling a particular product or series of products. A broader definition of merchants may include websites like Amazon or EBay, where a large variety of products is sold.
- **Customers**, who buy one more products from merchants.
- **Delivery Companies** (DCs), which are the courier companies paid by a merchant to deliver the product to an address specified by the customer. Delivery companies maintain a number of *mail stations* (MSs) on their own, while (if necessary) making use of the mail stations of other DCs. Although affiliated with DCs, in the following sections MSs will constitute separate entities.

For anonymity purposes, we extend the current delivery system with a central **Anonymous Physical Object Delivery Administration** (APODA), which is the manager of our Anonymous Physical Object Delivery (APOD) system. It authorizes the DCs and their mail stations to participate in the APOD, maintains the APOD website, etc. Merchants who need to send something anonymously may do it through any of the DCs which have contracted with APOD. As we will show in a later section, a part of the DC's payment goes to the APODA, who then distributes the payments among the rest of the nodes in the system according to the services they provided.

2.1 System Requirements

Privacy is the main focus in our system and defining it is critical. According to a general privacy definition [SS07], ***Privacy*** *is the right of an entity (normally a person), acting on its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share information about itself with others.* In the context of product delivery service (and assuming that no identity is revealed through the online payment procedure), privacy requires that the merchant should not be able to learn his customer's address, unless authorized by the latter. In addition, the DC should not be able to link any particular package destination address to the merchant who authorized the package's shipment.

Other requirements of our system, which basically derive from the nature of the system we want to enhance, are the following:

- *Package Delivery to Intended Recipients.* We require that the package shipped is delivered to the legal recipient of the package.
- *Package Tracing.* We require that a customer who has requested anonymous delivery of her online purchases is able to trace her packages without any information related to her or the item shipped being leaked. In addition, we require that merchant is able to trace the status of the delivery of the product, without acquiring any information regarding the intended package recipient. Tracing the package from both merchant and customer is especially important when the package has not been delivered within the estimated time.
- *Fairness.* Delivery Companies and mail stations involved are only paid when they perform their service correctly.
- *Proof of Delivery/Accountability.* We require that there can exist an undeniable proof of receipt issued by the anonymous recipient when she receives the package. Although unforgeable, this "receipt" should carry no identification or location-related information. In addition, in case of delivery failure, there should be possible to trace the misbehaving party.

2.2 Adversarial Model

Our goal is to create a realizable system. Thus, we require that our entities have the abilities and powers of the corresponding entities in real systems.

Each **Merchant** is interested in maintaining his clientele, which implies that he is trusted to perform his functional operations correctly. However, we assume that he is "curious", namely he may try to combine information he possesses to reveal his customers' identities. A merchant may also collaborate with the DC he has paid to learn the recipient's address.

We make similar assumptions regarding **Delivery Companies**' powers . In particular, although "honest" in their functional operations, it is likely that a DC would collaborate with a merchant it has contracted with to reveal the recipient of a particular package[1]. The reason for the latter assumption is the following: the DC's primary concern is to maximize its profit and thus to get paid for the services it has provided. Because of this strong monetary DC-dependence on the merchant, DCs are motivated — if requested — to provide the latter with all the recipient-related information its *mail stations* possess. Collusion between two DCs, however, is considered to be highly unlikely.

Anonymous Physical Object Delivery System(APOD) consists of several independent or semi-dependent *mail stations* (MSs) which are associated with one of the DCs as well as affiliated with an administration authority (APODA). We generally assume that MSs are independent if they belong to a different DC, while there is a chance of sharing the information they possess when they are part of the same company. More specifically, each MS: *(a)* possesses its own secret authorization/identification information (digital and group membership signature keys), *(b)* forwards mail towards their

[1] It is easy to see how this model is applied in real world if we consider the fact the employees in a DC may not trick any client directly, since they will lose their job, while they may try to combine information the company has obtained legally to draw their own conclusions.

destination by contacting at most the MS the package came from and the MS the mail is forwarded to, and, *(c)* may provide the information it possesses to the central authority of the same DC.

As mentioned before, for practical purposes we include in the design of the DC system an central administration station APODA, which handles payment and authorization matters. As such, it provides a valid MS with certificates (keys etc.). In our threat model, only the payment section of APODA is online and obtains no further information regarding the system unless compelled by a privileged authority such as a judge.

2.3 Payments for Anonymous Routing vs. Anonymous Product Delivery

Our anonymous delivery system has many similarities with PAR [ARS+08], a payment system specially designed for the Tor anonymity network [DMS04]. In particular, APODand PAR are similar in terms of threat models and goals.

1. (Goals) In both cases the goal is accountable and fair packet/package delivery through a group of nodes/MSs with guaranteed sender/merchant - receiver/recipient unlinkability. Another similar goal is the user-anonymity w.r.t. the other communication party: PAR (Tor) requires *sender anonymity w.r.t. the receiver*, while in APOD we require *recipient anonymity w.r.t. the merchant*.
2. (Adversarial Model) In both cases we deal with a local adversary, i.e. an adversary that may not control all the nodes/MSs in a user-chosen[2] delivery path. As in PAR (Tor), path nodes can only observe the traffic of their path neighbors and collaborate with other nodes which may or may not be part of the same path. Similarly, in our APOD MSs may observe the package-flow from/to their path neighbors and collaborate only with mail stations of the same DC which may or may not be part of the path of a particular package. For APOD, we explicitly rule out "active attacks" such as attaching a GPS-based tracking device to the packages.

3 Privacy Preserving Delivery Systems

In what follows, we will assume that each customer has completed her transactions with the merchants anonymously, i.e., no identification information has leaked through product browsing or payment procedure.

As mentioned before, APOD is coordinated by an offline administration authority, the APODA. Delivery companies (DCs) which participate in the APOD obtain membership credentials from the APODA. In a similar way, APODA issues authorization credentials to the *mail stations* (MSs) that offer their services to the APOD. Therefore, the APODA is the coordinator of two groups: (a) the DC group (APODA-DC) and (b) the MS group (APODA-MS) of the participating DCs and MSs respectively. We need to emphasize that, although DC group members may own some or all of the MSs in the APODA-MS group, no package may be provided anonymous delivery unless authorized by a DC group member.

[2] *User* for PAR (Tor) is the sender, while for the APOD *user* is the recipient.

Each Merchant is in agreement with one or more DCs. In particular, each merchant is a member of the Mgroup (DC-M) of one or more DCs.

The customer chooses one among the DCs that have contracted with the merchant and are part of the APODA-DC group. Then, the merchant uses his DC membership credentials to issue a blind ticket T to the customer. The customer uses T to log in to APOD's website anonymously and to choose the MSs she wants her package to go through. She then collaborates with the APODA to issue one blind *package-coin (*pcoin*)* per MS in the path with serial numbers of her choice. Serial numbers in this case serve as package tracking numbers. The client uses the information contained in the website to encrypt triplets of

(package-coin, tracing-info, next-destination)

with each path station's public key. She then interacts with the merchant to get a proof-receipt of the final form of the label which the latter will attach to the product.

Within the delivery process, each path MS decrypts the part of the package-label corresponding to it, revealing the package coins (pcoins) as well as the MS to forward the package to. In addition, each MS uploads the tracing information to the APODA site, so that both the merchant and the client are informed of the package delivery status. We note that no piece of label-information provided to each path MS carries merchant/client identification information.

To assure that only the intended recipient of the product may receive the package, the customer and the merchant agree on a secret PIN number whose endorsed hash is added to the overall packet label. The endorsement is basically created by the DC in collaboration with the merchant in a way that it reveals no information regarding which exactly DC of the APODA-DC group has produced it.

To enforce that each station forwards the packet towards the right direction, package-coins (pcoins) are accompanied by receipts which MSs will only get from the next path station after the latter receives the package. As pcoins with their receipts will later be used for the distribution of payments among the path MSs, there is a strong motivation for MSs to do their job properly.

3.1 Building Blocks

In this section, we describe the definition and security of the group, blind, and blind group signatures. See [CL02], [JLO97], [KY05] and [LR98] respectively.

Group Signature Schemes (GSS). In a typical GSS, there is a group manager (GM), the group-members, who act as signers (let each be S) and produce signatures on behalf of the group. The procedures supported are the following:

- $(\mathsf{gpk}, \mathsf{gsk}) \leftarrow \mathsf{GS.Setup}(1^k)$. This algorithm generates a group public key gpk and the GM's secret group information gsk .
- $\langle \mathsf{usk}_\mathsf{S}, \mathsf{JLog}_\mathsf{S} \rangle \leftarrow \mathsf{GS.Join}(\mathsf{gpk})[\mathsf{S}, \mathsf{GM}(\mathsf{gsk})]$. When this interactive join procedure ends, an S obtains a secret signing key usk_S, and the GM (group manager) logs the join transcript in the database D.
- $\sigma \leftarrow \mathsf{GS.Sign}(\mathsf{gpk}, \mathsf{usk}_\mathsf{S}, m)$. This algorithm generates a group signature on a message m.

- $\langle \top/\bot \rangle \leftarrow \mathsf{GS.Verify}(\mathsf{gpk}, m, \sigma)$. This is a verification algorithm.
- $\mathsf{MS} \leftarrow \mathsf{GS.Open}(\mathsf{gsk}, \sigma, D)$. With this algorithm the GM determines the identity of the group member who generated the signature σ.

Security Properties: (a) Anonymity. Given a signature and two members, one of whom is the originator, the adversary can identify its originator among the group members no better than randomly. *(b) Unforgeability.* The adversary cannot produce a valid group signature without owning group membership information. *(c)Non-framability.* The adversary cannot create a valid group signature that opens to another group member.

Blind Signature Scheme (BSS). In a typical BSS, there are signers (let each be S) who produce blind signatures on messages of users (let each be U). The procedures supported are the following:

- $(pk_{\mathsf{S}}, sk_{\mathsf{S}}) \leftarrow \mathsf{BS.KeyGen}(1^k)$. This is a key-generation algorithm that outputs a public/secret key-pair $(pk_{\mathsf{S}}, sk_{\mathsf{S}})$.
- $\langle \top/\bot,\ \sigma/\bot \rangle \leftarrow \mathsf{BS.Sign}(pk_{\mathsf{S}})[\mathsf{S}(sk_{\mathsf{S}}),\ \mathsf{C}(m)]$. At the end of this interactive procedure, the output of the S is either *completed* or *not-completed* and the output of U is either the signature (σ) or a failure sign ($\bot$).
- $\langle \top/\bot \rangle \leftarrow \mathsf{BS.Verify}(m, \sigma, pk_{\mathsf{S}})$ is a verification algorithm.

Security Properties: Apart from *Unforgeability*, *Blindness* is the most important security property of blind signature schemes: S does not learn any information about the message m on which it generates a signature σ.

We make use of GSS to instantiate the APODA-MS group, where the APODA is the group manager and the MSs who participate in the APOD are the group members.

Blind Group Signature Scheme (BGS). In a typical group signature scheme we can identify the group manager(GM), who maintains the BGS group administration information, the group-members who produce group signatures on users' messages. For now we will assume that a user U, has requested group member S to produce a signature on message m. The procedures supported are the following:

- $(\mathsf{bgpk}, \mathsf{bgsk}) \leftarrow \mathsf{BGS.Setup}(1^k)$. This algorithm generates a group public key bgpk and the GM's secret administration information bgsk .
- $\langle \mathsf{usk}_{\mathsf{S}}, bcert_{\mathsf{S}}, \mathsf{BJLog}_{\mathsf{S}} \rangle \leftarrow \mathsf{BGS.Join}(\mathsf{bgpk})[\mathsf{S}, \mathsf{GM}(\mathsf{bgsk})]$. When this interactive join procedure ends, S obtains her secret signing key $\mathsf{usk}_{\mathsf{S}}$, her membership certificate $bcert_{\mathsf{S}}$, and the GM logs the join transcript in the database D.
- $\sigma \leftarrow \mathsf{BGS.Sign}(\mathsf{bgpk})[\mathsf{S}(\mathsf{usk}_{\mathsf{S}}), \mathsf{U}(m)]$, where U obtains a signature on m.
- $\langle \top/\bot \rangle \leftarrow \mathsf{BGS.Verify}(\mathsf{bgpk}, m, \sigma)$. This is a verification algorithm run by a verifier.
- $\mathsf{S} \leftarrow \mathsf{BGS.Open}(\mathsf{bgsk}, \sigma, D)$. This algorithm is run only by GM and determines the identity of the S which generated the signature σ.

Security Properties: They combine the properties of group and blind signature schemes: *Anonymity*, *Unforgeability*, *Non-framability*, *Undeniable Signer Identity* towards the group manager, *Signatures' Unlinkability* and *Blindness*.

We make use of BGS in two cases: to instantiate the APODA-DC group — where APODA is the GM and the DCs participating in APOD are the group members — and to instantiate the M-group — where a DC is the GM and the merchants-clients of that DC are the group members.

Notation: We will use BSig_y (BSig_y^x) for blind (group x) signatures and Sig_y (Sig_y^x) for regular (group x) digital signatures of y.

3.2 Protocol Description

Anonymous Delivery System's Administration (APODA) makes the required setup (if any) for the two groups it manages (see subsection 3.1 for preliminaries):

- the APODA-DC group, which is instantiated through a blind group signature scheme and
- the APODA-MS group, which is realized through a plain group signature scheme.

Therefore, the APODA executes BGS.Setup and GS.Setup to obtain:

$$(\mathsf{bgpk}^{\mathsf{APODA-DC}}, \mathsf{bgsk}^{\mathsf{APODA-DC}}) \text{ and } (\mathsf{gpk}^{\mathsf{APODA-MS}}, \mathsf{gsk}^{\mathsf{APODA-MS}}).$$

In addition, for payment purposes, APODA executes BS.KeyGen to generate a blind signature key pair $(\mathsf{pk}_{\mathsf{APODA}}, \mathsf{sk}_{\mathsf{APODA}})$ and defines two hashes: a $\mathsf{pcoin}(H_{\mathsf{pcoin}})$ and a PIN (H_{PIN}) - related. The APODA publishes her public keys and the hashes:

$$\mathsf{bgpk}^{\mathsf{APODA-DC}}, \mathsf{gpk}^{\mathsf{APODA-MS}}, \mathsf{pk}_{\mathsf{APODA}}, H_{\mathsf{pcoin}} \text{ and } H_{\mathsf{PIN}}.$$

Delivery Companies (DCs) acquire membership in the group of companies participating in the APOD. More specifically, each delivery company DC_i collaborates with the APODA in a BGS.Join procedure to issue a blind group signature key-pair $(\mathsf{bgpk}_{\mathsf{DC}_i}^{\mathsf{APODA-DC}}, \mathsf{bgsk}_{\mathsf{DC}_i}^{\mathsf{APODA-DC}})$.

To manage all of its participating merchants, DC_i groups them together in a blind group signature group (see subsection 3.1), the $\mathsf{DC}_i - \mathsf{M}$. Therefore, DC_i performs the appropriate setup (BGS.Setup) to generate the corresponding blind group signature administration information:

$\mathsf{bgpk}^{\mathsf{DC}_i - \mathsf{M}}, \mathsf{bgsk}^{\mathsf{DC}_i - \mathsf{M}}$. DC_i publishes $\mathsf{bgpk}^{\mathsf{DC}_i - \mathsf{M}}$.

Mail stations (MSs) acquire membership in the APODA-MS group by interacting with the APODA in GS.Join protocol to issue $(\mathsf{gpk}_{\mathsf{MS}_i}^{\mathsf{APODA-MS}}, \mathsf{gsk}_{\mathsf{MS}_i}^{\mathsf{APODA-MS}})$, which enables each MS MS_i to sign a quantity on behalf of the APODA-MS group in an indistinguishable way. Each MS_i also runs EC.UKeyGen procedure to issue a public encryption key pair $(pk_{\mathsf{MS}_i}^e, sk_{\mathsf{MS}_i}^e)$.

Each *Merchant* M_j is a member of the group of clients (M-group) of one or more DCs he has contracted with. Let DC_i be one of these DCs. To obtain membership, M_j collaborates with the DC_i's central authority in BGS.Join protocol to issue a blind group signature key-pair $(\mathsf{bgpk}_{\mathsf{M}_j}^{\mathsf{DC}_i - \mathsf{M}}, \mathsf{bgsk}_{\mathsf{M}_j}^{\mathsf{DC}_i - \mathsf{M}})$. M_j also runs EC.UKeyGen protocol to create a public encryption key pair $(pk_{\mathsf{M}}^e, sk_{\mathsf{M}}^e)$.

Customer C has preestablished a pseudonymous account with the merchant, which we assume carries no C-identification information ($\mathsf{P_C}$, $\mathsf{secret}_{\mathsf{P_C}}$). Although out of the scope of this paper, we may consider $\mathsf{P_C}$ as a pseudonym such as the ones introduced in [LRSW99].

In what follows we will assume that a customer C collaborates anonymously with a merchant M_j, while M_j has contracted with the Delivery Company DC_i.

Package Label Preparation Procedure. There are four main phases in preparing the label which will be attached to each package sent anonymously: merchant-client interaction, DC-client interaction, APOD-client interaction and merchant client interaction:

Merchant-Client Interaction. M_j and C agree on a number PIN , which will serve as an authentication code between the two. M_j hashes the PIN into

$$\mathsf{PIN}_h = H_{\mathsf{PIN}}(\mathsf{PIN}||date)$$

in order to use it later as part of the barcode on top of the product. Final MS will only hand out the package to a person who demonstrates knowledge of PIN . Finally, M_j interacts with C — through $\mathsf{P_C}$ — such that the latter obtains a blind credential from M_j, $\mathsf{cred_b}$. $\mathsf{cred_b}$ is a blind signature of M_j on a random number N_r of C's choice

$$\mathsf{cred_b} = \mathsf{BSig}^{\mathsf{DC}_i - \mathsf{M}}_{\mathsf{M}_j}(N_r),$$

where $\mathsf{DC}_i - \mathsf{M}$ denotes the M-group of DC_i. M_j does not know the final form of $\mathsf{cred_b}$. However, anyone can confirm $\mathsf{cred_b}$'s validity as having derived by a valid DC_i's customer.

Client-Delivery Company Interaction. C uses $\mathsf{cred_b}$ to enter DC_i's website anonymously. DC_i's M-group administrator evaluates $\mathsf{cred_b}$ (BGS.Verify) and updates the statistics regarding merchant M_j. Here we need to note that according to the group signature attributes (see 3.1) DC_i, as the M-group administrator is the only entity, who using BGS.Open procedure, can identify the merchant who produced a $\mathsf{DC}_i - \mathsf{M}$ group signature. C — through her $\mathsf{cred_b}$ — collaborates with DC_i to obtain a blind endorsement on PIN_h:

$$\sigma_{\mathsf{PIN}_h} = \mathsf{BSig}^{\mathsf{APODA-DC}}_{\mathsf{DC}_i}(\mathsf{PIN}_h),$$

where $\mathsf{APODA-DC}$ denotes the DC group of APODA. In addition, C establishes a one time use anonymous account with DC_i to enter APOD's website

$$A_{\mathsf{C}} = (\mathsf{BSig}^{\mathsf{APODA-DC}}_{\mathsf{DC}_i}(N_A), N_A).$$

Client-APODA *Interaction.* Customer C logs in to APOD's website using A_{C}. The APODA verifies A_{C}'s validity (BGS.Verify), updates DC_i's statistics (BGS.Open) and allows C to browse in APOD's website to choose the route of her package. For each intermediate stop of the path she chooses, C:

1. collaborates with APOD to issue:

   $$(pc_1, r_1), (pc_2, r_2), \ldots, (pc_m, r_m),$$

   where $pc_k = \mathsf{BSig}_{\mathsf{APODA}}(H_{\mathsf{pcoin}}(r_k)), k = 1 \ldots m$ are the receipt enabled package-coins (pcoins). Receipt parts (r_k) are chosen by C and their hashes will serve as packet tracking numbers.

2. creates merchant-related package tracing parts: $mt_1, mt_2, \ldots, mt_m$, where

$$mt_k = Enc_{\mathsf{M}_j}(K)||Enc_K\{1||\mathsf{Sig}_{\mathsf{P_C}}(N_k)\}, i = 1, \ldots, m.$$

   Namely mt_k are pseudonym-signed random numbers(N_k), encrypted under M_j's public key. "1" is used for merchant to realize whether an uploaded tracing number is referring to him.
3. combines the pcoins, their receipts and merchant package-tracing parts in groups of

$$Msg_k = \{\mathsf{pcoin}(stop_k), receipt(stop_{k-1}), mt(stop_k), stop_{k+1}\}$$

   where

$$receipt(stop_{k-1}) = Enc_{pk^e_{stop_{k-1}}}(K)||Enc_K(r_{k-1})$$

   is encrypted with (k-1)-stop's public key. The Msg for the last stop f, contains, additionally, $\mathsf{pcoin}(stop_f)$'s receipt in a PIN -encrypted form: $Enc_{\mathsf{PIN}}(receipt(stop_f))$. All Msg-s are encrypted with the public encryption keys each MS acquires from APOD's administration authority into $barcode_{stop_k} = Enc_{pk^e_{stop_k}}(Msg_k)$.

Merchant-Client Interaction. C, as $\mathsf{P_C}$, sends all barcodes and σ_{PIN_h} to the merchant M_j. M_j hashes and digitally signs (S.Sign) the entire barcode sequence into

$$\sigma_{barcodes} = \mathsf{Sig}_{\mathsf{M}_j}(H_{\mathsf{proof}}(barcodes, \sigma_{\mathsf{PIN}_h}))$$

and sends it to C ($\mathsf{P_C}$) as a proof of what the former attaches to the packet to be sent out. C verifies the $\sigma_{barcodes}$'s validity and sends a verification response email with a notification of the first mail stop of the path: $\mathsf{Sig}_{\mathsf{P_C}}(stop_1, date)$.

Shipment. Merchant M_j prints out stickers for each of the barcodes as well as for the σ_{PIN}, which he attaches to the package to be sent anonymously. He then delivers the package to the first station of the path. For label integrity purposes, both parties, M_j and $stop_1$, exchange signed hashes of the encrypted route of the packet sent out:

$$\mathsf{Sig}_{\mathsf{M}_j}(H(barcodes, \sigma_{\mathsf{PIN}_h})) \text{ and } \mathsf{Sig}^{\mathsf{APODA-MS}}_{stop_1}(H(barcodes, \sigma_{\mathsf{PIN}_h})).$$

While the package moves from one MS to the other, each MS decrypts the barcode which corresponds to it. In this way, the next package destination is revealed along with the pcoin. Pcoins(pc_k-s) contained in each barcode are checked for validity (BS.Verify), while their serial is uploaded in the database of the APOD along with the merchant tracing parts (mt-s). In this way, C may track her package delivery status (by checking whether each serial number has been uploaded and thus reached its destination). At the same time, receipt parts of each barcode are sent back to the path predecessors of each station as a proof that the package was properly delivered. Merchant tracing parts (mt-s) are uploaded on APOD's website; M_j may then attempt to decrypt them using his secret decryption key. We note that M_j can only see the tracing numbers uploaded on the APOD website and not the particular MSs who uploaded them. To avoid any path recovery attacks based on the time each mt-s are uploaded, path MSs may randomize the time interval between the package arrival time and the corresponding mt-upload.

When the package reaches the final stop — where C picks her package up the last pcoin serial is uploaded. To obtain the package, C should provide the PIN agreed upon with the merchant. Non invertibility property of hash functions guarantees that only C is able to provide that number. A value different from H_{PIN} and a pre-agreed hash of the PIN ($H_{\mathsf{PIN\_received}}$) is then signed with MS's MS group signature uploaded to APOD's website:

$$\mathsf{Rec}_{\mathsf{Del}} = \mathsf{Sig}_{\mathsf{MS}_k}^{\mathsf{APODA-MS}}(H_{\mathsf{PIN\_received}}(\mathsf{PIN})).$$

M_j records $\mathsf{Rec}_{\mathsf{Del}}$ as proof that the package was properly delivered. At the same time, PIN reveals the receipt for the pcoin provided in the last stop. If no one comes to pick the package up within 10 days of its arrival at the last stop, the latter returns the packet to the MS it received it from.

Payment. The merchant charges the customer for the anonymous delivery service. The price may include the services of the upper bound of number of MSs that can be included in the anonymous path. DC_i charges the merchant in proportion to the merchant-signed endorsements the former receives from customers in the client-DC_i interaction phase. In a similar vein, the APODA charges the DC_i at each valid client-APODA interaction. The aggregated payments the APODA receives are distributed among the different MSs in proportion to the valid pcoins and receipts they present to the APODA.

4 System Considerations

In this section we will provide a brief presentation of how our requirements are satisfied.

Privacy. Privacy in our system consists of two parts: (a) *Recipient Anonymity* against the merchant and the delivery companies the latter has contracted with, and (b) *Sender-Recipient Unlinkability* against any delivery company or the APODA.

During the label preparation procedure, *Recipient Anonymity* is preserved through the combination of the anonymity provided by $\mathsf{P_C}$ and the unlinkability property guaranteed by the *Blindness* property of blind (group) signatures. In particular, a customer C uses her $\mathsf{P_C}$ pseudonym to browse the merchant's website, an (unlinkable to $\mathsf{P_C}$) anonymous account $\mathsf{cred_b}$ to browse to the DC's website and an (unlinkable to $\mathsf{cred_b}$) account A_{C} to visit APODA's website. The information each entity possesses at the stage of the label preparation is the following:

- the *merchant* M knows $\mathsf{P_C}$, the product $\mathsf{P_C}$ wants to have anonymously delivered, and that he provided $\mathsf{P_C}$ a blind $\mathsf{cred_b}$.
- the *delivery company* DC_i (as the manager of its M-group) knows that $\mathsf{cred_b}$ has interacted with M and that it provided $\mathsf{cred_b}$ with a blind A_{C}.
- the APODA knows that that A_{C} has interacted with DC_i and the MSs A_{C} has requested info for, which may finally be added to the delivery path or not. However, APODA has no information regarding M.

It is obvious that there is no recipient (customer) identification information known to any of the entities participating in the label preparation procedure. *Sender-Recipient*

Unlinkability is also satisfied at this stage. Since timing is not an issue here, the merchant can not be linked to a particular A_{C}.

Customer Anonymity is preserved throughout the package delivery procedure. No C-identification information is contained in the label attached to the product. For the delivery of the product at the final stop, C only needs to demonstrate knowledge of PIN.

As far as the *Sender-Recipient Unlinkability* requirement is concerned, the information attached to the package, $(\sigma_{\mathsf{PIN}}||barcode_1||\ldots||barcode_m)$, has been created by the customer and cannot be linked to any of $\mathsf{cred_b}/A_{\mathsf{C}}$ accounts the latter used to create the label. However, each MS in the path knows both the exact form of the label attached to the package and its delivery path neighbors. In our threat model, MSs from the same DC may collaborate by comparing package labels, so they recover a package's path. Although we consider this case highly unlikely as it is not cost effective, the severity of this attack is considerably decreased by the following:

- M_j may attach the barcodes in any order. Although this would require extra computation power in each stop, as each MS will have to go through the entire label to detect the barcode which refers to it, no MS — except for the first and the last — will be able to find its place in the path.
- C is the one choosing the entire path. She can easily choose the first and final stops[3] to be from different DCs.

Even in cases where the aforementioned scenario cannot be avoided, the most a DC may learn is the location of the final stop of a particular package without knowing the corresponding it to particular merchant or recipient. For completeness, we will refer to different types of collaborations between entities in our system. Although collaborations involving APODA or more than one DCs are not included in our threat model — since there is no direct monetary dependence between the merchant and APODA or other DCs — we refer to them as they may occur in the extreme case where a Judge has requested information about the recipient of a particular package.
a. M-DC_i (or DC_i-APODA): Because of $\mathsf{cred_b}$ (A_{C}) blindness, M-DC_i (DC_i-APODA) collaboration will reveal nothing more than what DC_i (APODA) knows.
b. any M-APODA collaboration: The APODA knows the MS – (mt-s/$\mathsf{Rec_{Del}}$) uploads correspondence, while M knows the (mt-s/$\mathsf{Rec_{Del}}$) – $\mathsf{P_C}$ correspondence. Thus M-APODA collusion may lead to complete package path recovery.

Depending on the privacy level we need to enforce, one way to avoid this attack scenario is via authorized-anonymous MS-logins(uploads) to APODA's website, using unlinkable-blind credentials ([SSG97]). Payments can be made through another type of blind coins, issued in response to each valid pcoin-receipt upload; these may be deposited unlinkably by MSs in person. Delivery proofs $\mathsf{Rec_{del}}$s may have the form of

$$\mathsf{Rec_{del}} = \mathsf{BSig_{APODA}}(H_{\mathsf{PIN}\_received}(\mathsf{PIN})),$$

[3] We refer to the stops of these path positions, since they would link the sender (merchant) to a particular recipient (location wise).

where the signature is produced blindly by the MS-APODA collaboration and uploaded anonymously by the final path MS. In this way, M-APODA attempts at package path recovery will fail.

Package Delivery to Intended Recipients. It is satisfied through the non-invertibility attribute of hash functions. In this way, only the legal recipient of the package, i.e., the one who interacted with the merchant, is able to demonstrate knowledge of PIN . To avoid any attack on any party's behalf to link a package to a particular $\mathsf{Rec}_{\mathsf{del}}$ upload, the final path MS uploads a pre-agreed hash of the PIN as opposed to the PIN itself.

Package Tracing. Package tracing is satisfied through the uploads of the pcoins' serials and the mt-s to the APOD's website. A merchant may visit that site anytime to collect the mt-s which refer to him. The customer may trace her package delivery status by checking on the serial numbers uploaded.

Fairness-Accountability. Fairness is satisfied in our system since, if a MS does not forward the package towards the right direction, it will never receive his pcoin receipt and will thus not be paid. pcoin receipts serve accountability as well, as they provide a proof of proper delivery of the package to the next path MS. Invalid pcoin-receipt pairs may be resolved through APODA, which will request the cooperation of all nodes to recover the full path corresponding to a package label and, thus, the misbehaving MS.

We note that we assume a customer does not deliberately provide invalid pcoin-receipt pairs, as it would only affect the payment distribution within the MSs, while she — having already paid the merchant — will have no monetary motive. On the other hand, the PIN requirement for the final package delivery guarantees that no customer can falsily claim failure of the delivery process.

5 Related Work

As mail service is not a new concept, anonymous package delivery has been addressed in the past by several companies.

iPrivacy [S01] guarantees anonymous ecommerce activity, including anonymous delivery service. However, in iPrivacy the delivery company already knows the address of the recipient. The consumer provides the merchant with a special code number which corresponds to his address in iPrivacy's databases. iPrivacy then uses extra physical boxes, each with different address for the package to be sent to different locations prior to its final destination. Recipient anonymity in this case is physically vulnerable, while the iPrivacy company may link a merchant to a particular address.

ContinentalRelay [CON07] is another company guarranteing anonymous package delivery. However, in this case anonymity is guarranteed from the merchant (sender) but not from the delivery company itself: customers pay a monthly fee to maintain a fake Australian address. Every package sent to this imaginary mailbox is then forwarded to the customer's real address. However, this solution may be more expensive and inconvenient, as some mail carrier services will not deliver to a mailbox.

Kushik Chatterjee in [C08] has also suggested a patent for efficient anonymous package delivery service. In particular, Chatterjee suggested a system where the physical

address of the recipient is identified within the delivery system with an identification number, which is what sender attaches to the mail sent. Thus recipient's physical address is concealed from the sender but not from the delivery company.

Tor[DMS04] and other onion routing protocols[SGR97] as well as PAR[ARS+08] can also be considered as part of the related work in this paper as described in section2.3.

6 Conclusion

In this paper, we presented a real-world applicable delivery service protocol for online purchases with guaranteed merchant-customer unlinkability and recipient anonymity w.r.t. the merchant and/or the delivery companies involved. Our protocols utilise similar techniques to the Tor[DMS04] anonymity network and support package tracing and mail delivery proof. As opposed to currently deployed anonymous delivery techniques, recipient's address is concealed even from the company paid to perform the delivery.

Acknowledgment

The authors would like to thank the anonymous referees for their valuable comments and suggestions and Google Inc. for subsidizing this work.

References

[ARS+08] Androulaki, E., Raykova, M., Srivatsan, S., Stavrou, A., Bellovin, S.M.: PAR: Payment for anonymous routing. In: Borisov, N., Goldberg, I. (eds.) PETS 2008. LNCS, vol. 5134, pp. 219–236. Springer, Heidelberg (2008)

[C81] Chaum, D.L.: Untraceable electronic mail, return addresses, and digital psuedonyms. Communications of the ACM (1981)

[C08] Chatterjee, K.: System and method for anonymous mail delivery services (2008)

[CL02] Camenisch, J., Lysyanskaya, A.: A signature scheme with efficient protocols. In: Cimato, S., Galdi, C., Persiano, G. (eds.) SCN 2002. LNCS, vol. 2576, pp. 268–289. Springer, Heidelberg (2003)

[CON07] Protect your privacy with your own offshore private maildrop (1999-2007)

[CS97] Camenisch, J., Stadler, M.: Effcient group signature schemes for large groups. In: Kaliski Jr., B.S. (ed.) CRYPTO 1997. LNCS, vol. 1294, pp. 410–424. Springer, Heidelberg (1997)

[DMS04] Dingledine, R., Mathewson, N., Syverson, P.: Tor: The second-generation onion router. In: Proceedings of the 13th USENIX Security Symposium (August 2004)

[JLO97] Juels, A., Luby, M., Ostrovsky, R.: Security of blind digital signatures (extended abstract). In: Kaliski Jr., B.S. (ed.) CRYPTO 1997. LNCS, vol. 1294, pp. 150–164. Springer, Heidelberg (1997)

[KY05] Kiayias, A., Yung, M.: Group signatures: Provable security, efficient constructions and anonymity from trapdoor-holders. In: Dawson, E., Vaudenay, S. (eds.) Mycrypt 2005. LNCS, vol. 3715, pp. 151–170. Springer, Heidelberg (2005)

[LR98] Lysyanskaya, A., Ramzan, Z.: Group blind digital signatures: A scalable solution to electronic cash. In: Hirschfeld, R. (ed.) FC 1998. LNCS, vol. 1465, pp. 184–197. Springer, Heidelberg (1998)

[LRSW99] Lysyanskaya, A., Rivest, R., Sahai, A., Wolf, S.: Pseudonym systems (Extended abstract). In: Heys, H.M., Adams, C.M. (eds.) SAC 1999. LNCS, vol. 1758, pp. 184–199. Springer, Heidelberg (2000)

[O06] Okamoto, T.: Efficient blind and partially blind signatures without random oracles. In: Halevi, S., Rabin, T. (eds.) TCC 2006. LNCS, vol. 3876, pp. 80–99. Springer, Heidelberg (2006)

[S01] Smith, J.M.: Iprivacy white paper (2001)

[SGR97] Syverson, P.F., Goldschlag, D.M., Reed, M.G.: Anonymous connections and onion routing. In: IEEE Symposium on Security and Privacy, Oakland, California, pp. 44–54, 4–7 (1997)

[SS07] Smith, R., Shao, J.: Privacy and e-commerce: a consumer-centric perspective. Electronic Commerce Research 7(2), 89–116 (2007)

[SSG97] Syverson, P.F., Stubblebine, S.G., Goldschlag, D.M.: Unlinkable serial transactions. In: Proceedings of Financial Cryptography, pp. 39–55. Springer, Heidelberg (1997)