

# A New Privacy-Friendly Loyalty Program

## *GlassJar*

<https://github.com/thisisneena/glassjar>

**Neena Dugar, Christie Hong, Annie Wang**

{ndugar, cshong, anniew}@mit.edu

Instructor: Ronald Rivest, Yael Kalai

6.857 Computer & Network Security

May 16, 2018

## Contents

<b>1</b>	<b>Introduction</b>	<b>2</b>
<b>2</b>	<b>Past Works</b>	<b>2</b>
<b>3</b>	<b>Objective</b>	<b>3</b>
<b>4</b>	<b>Principals</b>	<b>3</b>
4.1	Customers . . . . .	4
4.2	Vendors . . . . .	4
4.3	Third-Party . . . . .	4
<b>5</b>	<b>Our Security Schematic</b>	<b>4</b>
5.1	Customer & Vendor . . . . .	5
5.1.1	Registering with Vendor . . . . .	5
5.1.2	Earning Loyalty Points . . . . .	5
5.1.3	Querying Loyalty Points . . . . .	6
5.1.4	Spending Loyalty Points . . . . .	6
5.2	Vendor & Third Party . . . . .	7
5.2.1	Differential Privacy . . . . .	7
<b>6</b>	<b>System Guarantees</b>	<b>8</b>
<b>7</b>	<b>Usability</b>	<b>8</b>
<b>8</b>	<b>Limitations</b>	<b>9</b>
<b>9</b>	<b>Conclusion</b>	<b>9</b>

# 1 Introduction

Today, loyalty programs are ubiquitous. Many of us partake in loyalty programs on a daily basis, from turning our loyalty points into free drinks at coffee shop, to exchanging points for miles on our next trip with a major airline, to even exchanging points for cash at our local supermarket. These schematics exist for vendors to reward loyal customers, buttress the company's reputation, and potentially increase their customer base. More importantly, vendors implement loyalty programs to keep customers coming back to spend more money, and collect individualized data for targeted ads.

Existing loyalty card schemes function by collecting significant amounts of personal user data, in exchange for some small benefits to the customer. Typically, customers are unaware of the degree of information being collected by companies, and there are little to no guarantees placed on the security of their data. Moreover, privacy guarantees are usually vague and poorly communicated.

While in most cases this is a symbiotic relationship between vendor and customer, in recent light, there have been many security problems arising with these loyalty programs.

Popular retailer, Target, hit the headlines in 2012 when Target exposed a teen girl's pregnancy, before she even knew herself. Target's statistician, Andrew Pole, "identified 25 products that when purchased together indicate a woman is likely [to be] pregnant." With the data collected from customer purchasing histories, Target was able to identify a pregnant teen before she even knew she was pregnant. Pole could "estimate her due date to within a small window" and began sending advertisements to the pregnant teen with coupons for "maternity clothing, nursery furniture, and diapers" all timed at very "specific stages of her pregnancy" [4].

Moreover, pharmacy retailers, CVS and Walgreens, were exposed of marketing and transacting data containing "not only the name and dosage of the drug and the name and address of the doctor, but also the patient's address and Social Security number" to third party vendors. While the names of the customers were removed or encrypted, third party vendors who purchased these data sets from CVS and Walgreens were still able to trace back the original customers and send them targeted coupons and samples associated to the customers' prescription history [3].

Clearly, there is not only a security problem between vendor and third party, but also a transparency issue between customer and vendor. Firstly, customers are unaware of the level of sharing that occurs with every transaction they make with their loyalty programs. There is a severe lack of control on the customer's end, and more importantly there is no assurance of privacy. Hence, we propose a new privacy-friendly loyalty program, GlassJar, that heightens transparency between customer and vendor, and guarantees personal data anonymity and security when vendors market their data to third parties.

## 2 Past Works

A few existing systems have been proposed to deal with the privacy issue in loyalty cards. In particular, we examined "An Advanced, Privacy-Friendly Loyalty System" by Milutinovic et al. and "Privacy-Preserving Loyalty Programs" by Blanco Justicia and Domingo-Ferrer. Milutinovic et al. cite a lack of existing research into this area, which makes it a particularly interesting topic for investigation.

Both past works take a decentralized approach to favour the customers' privacy, utilizing partially blind signatures [1, 5]. Taking this approach stores loyalty points on the customer's

end, and the vendor essentially receives little to no data about the customer's purchases. These loyalty schematics provide increased anonymity, and allow for more granular privacy control. They give the customer greater clarity on what data is being shared with the company, and allow the customer to better understand the consequences [1, 5]. However, these loyalty schemes have been reduced to no more than a stamp card that one may receive to get their "10th coffee for free!"

This leads to an even greater problem: because the vendor receives little no data from their customers with these loyalty schemes, there is little incentive for vendors to actually implement the decentralized approach. Despite the security these schematics provide for the vendor's customers, because there is reduced profitability from the vendors end, these designs do not set precedence for companies to better their loyalty programs.

None of the existing works employ differential privacy in their system designs. Thus, in the following sections we will explore the concept of transparency, distribution of loyalty points, as well as incorporation of differential privacy in our loyalty program security scheme, GlassJar.

### 3 Objective

Loyalty card schemes allow customers to receive benefits (such as discounts, special pricing, vouchers) in exchange for information on their spending habits. This data allows vendors to provide targeted ads/incentives for their customers, and have a greater understanding of their customer base (particularly with regards to seasonal trends). The loyalty card has an additional goal of encouraging the user to make more purchases, and become a returning customer. We highlight the following goals for GlassJar:

- **Confidentiality:** The personal data of the customer, and their purchase history should not be available to a malicious third-party. However, the vendor should be able to obtain this information if the customer agrees to share it.
- **Integrity:** A malicious customer or vendor should not be able to forge loyalty points or purchases. A customer cannot delete data they have already shared.
- **Availability:** It's important that the data is highly available to the vendor, since they are likely to want to use it to make marketing decisions. The customer should also be able to see a history of what data they have shared.
- **Controlled Linkability:** A customer should be able to decide whether their purchase history should be linked to their loyalty card account on a case-by-case basis.
- **Transparency:** A customer should have a strong understanding of what data they are giving to the vendor.

### 4 Principals

There are three principals relevant to this security policy for loyalty. Mainly, there is the customer and vendor. The customer purchases products from the vendor, while the vendor provides the products for the customers. Additionally, more often than not, there are third-parties looking to obtain the vendor's data for their own purposeful analysis.

## 4.1 Customers

Customers are one of the main principals in this discussion of loyalty card schemes. They should be able to gain perks through their purchases, but also be aware of the data they are sharing with the vendor. Furthermore they should have the option to maintain a certain degree of privacy about their purchases. Customers should:

1. Be able to choose whether a given purchase can be linked with their account or not
2. Receive perks even if he/she chooses not to be associated with a certain purchase they made
3. Receive extra perks if he/she chooses to associate their information with a certain purchase
4. Receive targeted advertisements and/or incentives based on their shopping habits if they choose to share their information
5. Be able to see a history of the information he/she has shared with the vendor

## 4.2 Vendors

Vendors utilize loyalty card schemes to retain customers with targeted advertisements and perks. The vendor also communicates with third-party vendors to gain more capital by marketing their customers data. Vendors should:

1. Only be able to view data that their customers have chosen to share
2. Export a "safe" version of the data they've collected to third-party vendors that is differentially private

Vendors have many **stores** which function as the main contact point between the customer and the vendor. In our design, we assume these are brick-and-mortar stores, though our design could easily be extended to online stores.

## 4.3 Third-Party

Third-parties are typically vendors that purchase data from other vendors to gain insight into market shares, customer bases, and essentially gain valuable data analysis. The third-party vendor is looking for access to useful statistics, and are willing to pay large sums of money for accurate statistics that would potentially help them make future business decisions.

# 5 Our Security Schematic

This security policy relies on the following mechanisms: authentication, signature scheme, differential privacy, and encryption.

## 5.1 Customer & Vendor

Between the customer and vendor we utilize encryption, signature scheme, and authentication to control how much information the customer chooses to share with the vendor, and distribute the correlating loyalty points.

### 5.1.1 Registering with Vendor

When the customer creates an account, they generate a public-private key pair and a random loyalty number (with which they will be identified to the system). Realistically this will be generated by the vendor's system then assigned to each customer. The customer then broadcast their loyalty number, biographical information and public key to the vendor (via the store) and the vendor retains this information in their local databases.

### 5.1.2 Earning Loyalty Points

To ensure ultimate transparency between customer and vendor, our schematic asks the customer after *each* purchase whether or not they'd like to share their itemized purchase history with the vendor. Depending on the customer's answer, he or she will be allocated a certain amount of loyalty points. If the customer chooses to share their purchase history, he/she will be rewarded more loyalty points than not doing so.

In the case in which the customer chooses to not disclose their purchase history, the vendor will instead receive the total amount spent by the customer instead. However, to fully ensure privacy, we add some noise to the amount of spent, such that the vendor cannot figure out what items were bought, as unique prices or purchase of a singular item, could disclose the exact product a customer purchased. In our implementation, the "noise" is randomly drawn from a triangle distribution of width  $k = 1$ , where  $k$  is optionally changeable. In Section 8 *Limitations*, we discuss this notion further.

The following is a schematic for customers earning loyalty points by purchasing products at a vendor's store.

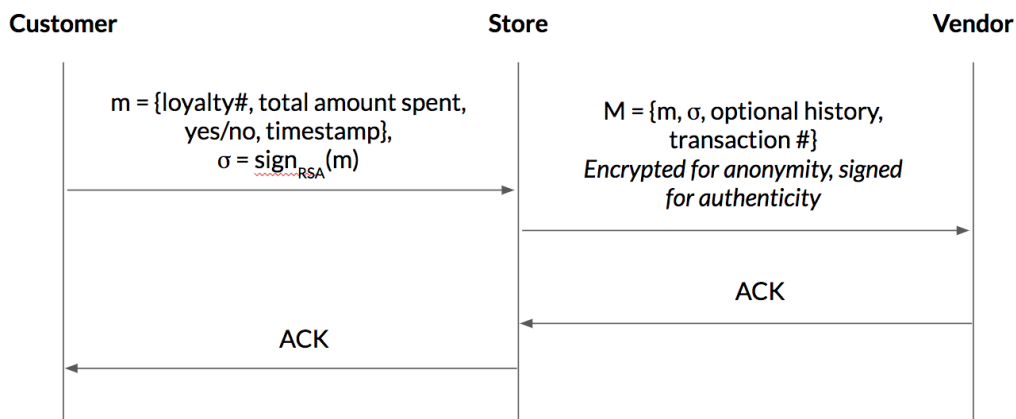


Figure 1: Purchasing Schematic

We utilize RSA signatures from customer to store, as seen in *Figure 1* to ensure that the transaction was actually made by said customer. The store checks that the timestamps of the message falls within a certain bound of the current time to ensure that the signature

sent is reliable. Furthermore, the message sent between store and vendor are tagged with a transaction number generated by the store, to ensure no adversarial customer can gain more points by resending the same message multiple times. This message sent between store and vendor is encrypted for anonymity and signed for authenticity to ensure that no adversary can manipulate or eavesdrop on the message. We send acknowledgements back from vendor to store to customer to complete the purchase transaction.

### 5.1.3 Querying Loyalty Points

In the case in which a customer would like to know how many loyalty points they have, we have the following querying schematic:

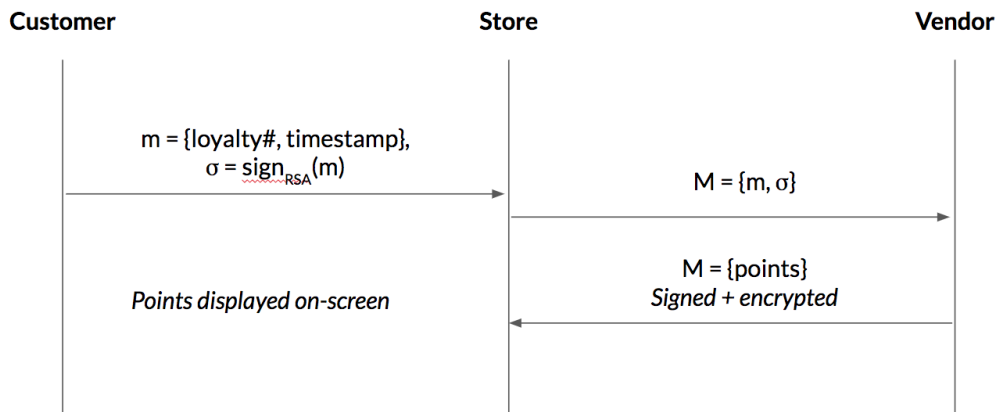


Figure 2: Querying Schematic

As before, the customer submits their loyalty number to the store using a RSA signature for authentication, and a timestamp; then the store forwards this signed message to the vendor. The vendor then matches the loyalty number in their database, and sends back to the store the number of points collected by the customer, which is then displayed on the store's kiosk screen for the customer. The vendor signs and encrypts this message such that no adversary could manipulate or eavesdrop on the number of loyalty points.

### 5.1.4 Spending Loyalty Points

When spending loyalty points, we once again must use signature schemes, encryption, and authentication to ensure that no adversary can come in the middle and attempt to manipulate the amount of points to spend. We do this in the following way:

The customer gives the store his/her loyalty number, along with the amount of points to swap for cash. The message is signed using a RSA signature to ensure that no adversary manipulates the message. The store then sends the loyalty number, the amount of points, the signature, and a transaction number - all signed and encrypted - to ensure that no adversary can decrypt and manipulate this request. The unique transaction number is to prevent a malicious customer from double-spending their points. The store then converts the points to some cash discount, and sends back to the store the transaction number, discounted amount, and signs it; thus completing the transaction.

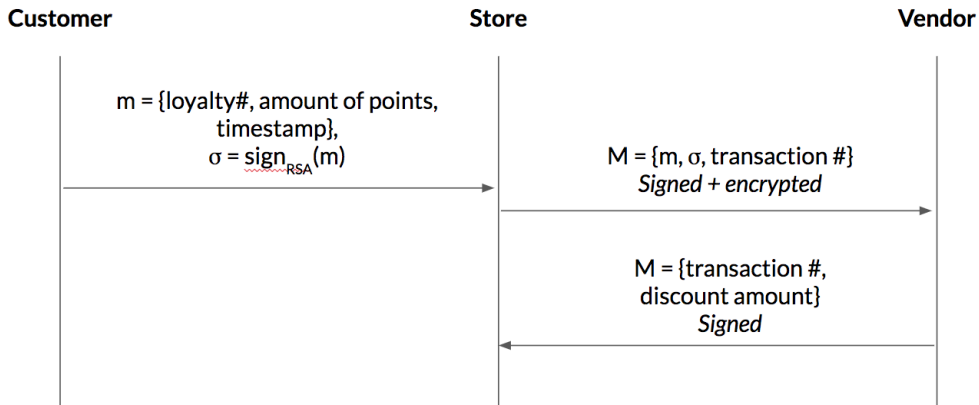


Figure 3: Spending Schematic

## 5.2 Vendor & Third Party

Transaction of data between vendors and third-parties are beneficial to both parties as the vendor makes more profit, and the third-parties gain some analytical edge. However, it is incredibly important that vendors uphold their customers' privacy with the data sets that are marketed. Thus, our design schematic for GlassJar allows third parties to purchase differentially private statistics - i.e. statistics that protect identification of individual customers, without diminishing accuracy and value of the data.

### 5.2.1 Differential Privacy

Differential privacy's ultimate goal is to provide a means to maximize the accuracy of queries from a database whilst minimizing the chances of identifying its records - or in this case, a customer's sensitive data.

In GlassJar protocol, we utilize a Laplacian mechanism such that the differential privacy mechanism is randomized. The Laplacian mechanism adds controlled Laplacian noise to the function that we want to compute based off the number of queries. The schematic is the following:

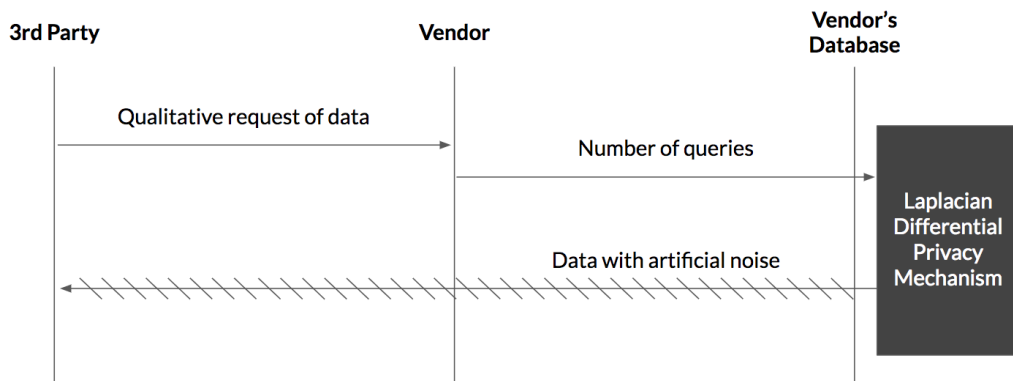


Figure 4: Sharing Data Schematic

A third party requests our vendor for some qualitative data. For example, our third party is



a produce vendor who is interested in bringing a store into Cambridge. They request from our vendor, a large conglomerate retailer, some customer data regarding produce purchases in the past year. Based off this qualitative data, the vendor then sends a series of queries to their database, in which we deploy a Laplacian Differential Privacy Mechanism and return back to the third party the data requested with some artificial noise. The amount of noise will depend on the number of queries the vendor will make on the database [2].

In our prototype, we implemented simple counting queries, with added Laplace noise under the following scheme:

$$q'_i = q_i + \text{Lap}\left(\frac{k}{n\epsilon}\right)$$

where  $k$  is the number of queries,  $n$  is the size of the dataset, and  $\epsilon$  is the differential privacy parameter[6]. We arbitrarily set  $\epsilon$  as  $\ln 2$ , however this is adjustable by the vendor.

While the data may have artificial noise, it's crucial to note that Laplacian differential privacy schemes add *controlled* noise, such that the value in the data is not destroyed and can still be used for valuable analytics [2].

## 6 System Guarantees

GlassJar is a two-pronged schematic: RSA signatures and encryption, as well as Laplacian differential privacy. Thus, we make the following guarantees:

- **Confidentiality:** RSA signatures and encryption ensure no adversary, customer, or store employee can manipulate or forge the data sent between customer and vendor.
- **Integrity:** The integrity of loyalty points is verified by RSA signatures, encryptions, and transaction numbers. As long as the store and vendor are not corrupt, each loyalty point acquisition, query, and expenditure is trustworthy.
- **Availability:** Data that has been acknowledged to be shared by the customers is all highly accessible to the vendor.
- **Controlled Linkability:** With each purchase, customers are able to decide whether or not to share their itemized purchase history with the vendor, or merely share the aggregate cost.
- **Transparency:** With every transaction, the customer will be aware of whether or not he/she is sharing his/her itemized purchased history with the vendor. By varying the rewards based on sharing/not sharing, the customer is implicitly aware that their data has value.

## 7 Usability

GlassJar provides a secure solution for loyalty card schematics. GlassJar emphasizes transparency, but unlike past works, our use of signature schemes and encryptions/authentications allows the loyalty points to be stored on the vendor's end. This additionally allows vendors to collect data that customer's willfully released, and for vendors to continue sending targeted ads with *only* data that has been knowingly sent. This creates incentive for the vendors to employ this scheme and raises awareness in customers about the value of their data.

Furthermore, GlassJar provides a more secure transaction of data between third parties and vendors. With differentially privatized data, not only will vendors still profit in these transactions, but third parties will additionally still gain valuable insight into potential markets. This protects the vendor's customers, and buttresses vendor goals to keep their customers safe, happy, and returning to their businesses.

Ultimately, in day-to-day use, GlassJar will be fairly similar to existing loyalty programs, but will provide much stronger security guarantees to all parties.

## 8 Limitations

In our current prototype implementation, we ask the customer to enter the message and signature in plaintext form. In reality, this would be done by scanning a QR code which would be able to transfer this information very quickly. However, we felt that this was out of the scope of the prototype.

Our prototype implementation employs a simple Laplacian differential privacy scheme for counting queries. [6] We did not implement a full querying scheme with differential privacy between the vendor and the third party because we did not implement a full database system in our prototype system. In a non-prototype implementation, we would implement a more sophisticated multi-query differential privacy system, such as PMW or BLR. Given a lack of real data, it would have been very difficult to evaluate any of these privacy mechanisms against each other, and as a result we decided to opt for the simplest solution[6].

Furthermore, in 5.1.2 *Earning Loyalty Points* we discussed our implementation of "noise," utilizing a triangle distribution of width  $k=1$ . For  $k$  to be completely optimized, we must know the inventory and pricing of the stock of the store. This is the only way to ensure that the noise added truly blurs a customer's purchase should he/she not wish to disclose to the company what he/she bought.

A major point of concern with this design is the fidelity of the store. We are building this system under the assumption that the store is trustworthy. We are trusting that the store will pass on the correct message between the vendor and customer without tampering with it. For example, if a customer decides not to share their complete transaction data on a specific purchase, the store could easily ignore the yes/no part of the message sent from the customer and send the entire transaction data to the vendor anyway. However we don't anticipate this to be a significant problem as most of the process will be automated and abstracted away from the workers. Furthermore we don't expect most workers to have the technical knowledge to dive into the system and tamper with it.

## 9 Conclusion

In this paper we presented GlassJar: a loyalty schematic using authentication, signature scheme, differential privacy, and encryption, to provide customers with a more transparent loyalty program, as well as protect customer privacy from third party vendors. GlassJar beats competing loyalty programs because we still preserve vendors receiving customer data, as well as marketing this data to other third parties; thus, maintaining the original profitability of these schemes.

GlassJar sets precedence for a more secure and transparent relationship between vendors and its customers - a principle we hope more loyalty programs will start to adopt in the future.

## References

- [1] Blanco-Justicia, Alberto, and Josep Domingo-Ferrer. "*Privacy-Preserving Loyalty Programs.*" Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance Lecture Notes in Computer Science, 2015, pp. 133–146., doi:10.1007/978-3-319-17016-9\_9.
- [2] Dwork and Roth. "*The Algorithmic Foundations of Differential Privacy.*" Foundation and Trends in Theoretical Computer Science Vol.9, Nos 3-4(2014) 211-407, 2014, pp. 30-36, doi: 10.1561/0400000042.
- [3] Freudenheim, Milt. "*And You Thought a Prescription Was Private.*" The New York Times, The New York Times, 8 Aug. 2009, [www.nytimes.com/2009/08/09/business/09privacy.html](http://www.nytimes.com/2009/08/09/business/09privacy.html).
- [4] Lubin, Gus. "*The Incredible Story Of How Target Exposed A Teen Girl's Pregnancy.*" Business Insider, Business Insider, 16 Feb. 2012, [www.businessinsider.com/the-incredible-story-of-how-target-exposed-a-teen-girls-pregnancy-2012-2](http://www.businessinsider.com/the-incredible-story-of-how-target-exposed-a-teen-girls-pregnancy-2012-2).
- [5] Milutinovic, Milica, et al. "*An Advanced, Privacy-Friendly Loyalty System.*" IFIP Advances in Information and Communication Technology Privacy and Identity
- [6] Vadhan, Salil. "*Lecture 11- Differential Privacy.*" 6.889 New Developments In Cryptography. Massachusetts Institute of Technology, Massachusetts. 3 May. 2011.