Private and Efficient Set Intersection Protocol For RFID-Based Food Adequacy Check

Zakaria Gheid, Yacine Challal, Lin Chen

Private and Efficient Set Intersection Protocol For RFID-Based Food Adequacy Check

Zakaria Gheid[†], Yacine Challal[*†], Lin Chen[‡]
[*]Centre de Recherche sur l'Information Scientifique et Technique, Algiers, Algeria
[†]Ecole nationale supérieure d'informatique, Laboratoire des Méthodes de Conception des Systèmes, Algiers, Algeria
[‡]Lab. Recherche Informatique (LRI-CNRS UMR 8623), Univ. Paris-Sud, 91405 Orsay, France
Email: z_gheid@esi.dz , y_challal@esi.dz, chen@lri.fr

***Abstract*—Radio Frequency Identification (RFID) is a technology for automatic object identification that has been implemented in several real-life applications. In this work, we expand a novel relevant application of RFID tags for grocery stores, which aims to check the adequacy of food items with respect to the shoppers' personal preferences. Unlike similar works, we focus on shoppers' privacy and running time efficiency. For this aim, we propose a novel private set intersection (PSI) protocol to be used in matching the shoppers' personal preferences with the set of each item's adequate profiles that are held by the back-end server of the store. We provide a standard security proof against curious stores and malicious customers. For efficiency concern, we build our protocol without cryptographic operations, and we achieve a linear asymptotic complexity of $O(v+c)$ for communications and store-side computations, where v and c are the numbers of profiles in the store's back-end server and the shopper's list of preferences respectively. Moreover, experimental results and comparisons with state-of-the art solutions reveal the scalability of our novel PSI protocol for big market stores.**

***Index Terms*—Radio Frequency Identification (RFID), Profile Matching, Private Set Intersection.**

I. Introduction

Radio Frequency Identification (RFID) is a wireless technology that uses radio waves to identify and track objects. RFID systems consist of tags attached to the objects to be identified and readers that communicate with the tags to collect information. Owing to its advantages over barcode systems, RFID market is gaining increasing values that are expected to exceed US$18 billion by 2026 [1]. This rapid proliferation has allowed a wide range of endless applications, where commerce comes in first. For instance, Large-scale supermarkets like Walmart are attaching RFID tags to their goods to increase business revenue lost by theft or inaccurate accounting of goods [2]. Amazon Inc. has launched Amazon Go, a high-tech retail store currently in a private beta testing in Seattle, and filled a patent [3] in which they use RFID to detect when a shopper takes an item from the shelf. Then, the system adds up the item and charges the shopper's Amazon account without requiring going through a traditional check-out line. This, should improve shopping experience for customers with easier item returns.

Following this technology adoption, we introduce a novel relevant RFID-based application that we coin as FAC: Food Adequacy Check, which provides customers with information on food items whether they match their preferences or not. For instance, customers suffering from diabetes or needing a gluten-free diet, should have a detailed insight about items before buying them. Traditionally, a shopper can easily make such a check relying on product labels; nevertheless, matching a complex profile that involves several information such as age, weight, several diseases, and follows a special program as Low Carb diet [4], is a tedious task. This is highly true, if the shopper wants to match several preferences including his/her one and those of his/her family.

Accordingly, we propose (Π-FAC), a novel private and efficient set intersection protocol that we use to match customers personal preferences with items adequate profiles. We design (Π-FAC) as a multi-party computation (MPC) protocol that is implemented on customers' smartphones and the supermarket back-end server. We use passive RFID tags with no computational capability, which is the cheapest type of tag, to allow the deployment of our application with affordable cost.

We address the privacy concern of the shopper preferences against curious server, besides the privacy of the database of item profiles held by the back-end server against malicious shoppers as this may be a paid service. We provide a simulation-based security proof under the standard real/ideal paradigm [5].

For the efficiency concern, we build our protocol upon efficient matrix algebra without cryptographic operations to ensure its scalability for large supermarkets. We achieve a linear asymptotic complexity of $O(v+c)$ in communications and server side computations, where v and c are, respectively, number of profiles within the server database and the customer list of preferences. Finally, we make experimental evaluations to confirm the efficiency of our (Π-FAC) protocol compared to the hash-based private set intersection solution used in practice.

The rest of this paper is organised as follows. In Section II, we review recent literature works in Private Set Intersection field and we discuss them. In Section III, we introduce a novel RFID-based application that we name Food Adequacy Check (FAC). Then, in Section IV, we detail our novel private set intersection protocol used within FAC application for the private profile matching purpose. Next, we provide a standard security analysis of our protocol, in Section V, using the Real/Ideal paradigm. After that, we devote Section VI to evaluate the efficiency of our protocol compared to the hash-

based solution used in practice. Finally, we conclude this work by summarizing our contribution.

II. Related Work

In this section, we provide a literature survey on the private set intersection (PSI) functionality that we use to implement the Food Adequacy Check application. We focus on PSI protocols that work in the standard (plain) model, where security is only based on complexity assumptions.

Assume a client (C) and a server (V) having private sets of profiles X and Y of sizes c and v respectively. Two main approaches were used to solve PSI(X,Y), namely Oblivious Polynomial Evaluation (OPE) [8] and Oblivious Pseudo-Random Functions (OPRF) evaluation [9].

1) OPE based-PSI: In this approach, C defines a polynomial $P(.)$ such that $P(x) = 0$ for each $x \in X$, and sends to V homomorphic encryptions of the coefficients of $P(.)$. Then, V computes the encryption of $(r.P(y) + y)$ for each $y \in Y$, using homomorphic properties of the encryption system and a fresh random r. Finally, C decrypts the received cyphertexts and gets either elements of the intersection (if plaintexts match an element of X) or random values. In this approach, we find works of Freedman et al. [10], Kissner and Song [11], Dachman-Soled et al. [14] and Hazay [15]. They targeted semi-honest and malicious settings, where the most efficient construction [15] incurs $O(v+c)$ communications and $O(c + v \log\log c)$ computations, under the strong Decisional Diffie-Hellman assumption (strong-DDH).

2) OPRF-based PSI: In which V defines a random key (k) for a pseudo random function (PRF) $f_k(.)$ and computes the set $f_{ky} = \{f_k(y) : y \in Y\}$. Then, V and C executes an OPRF protocol where V inputs $f_k(.)$ and C inputs the set X and gets the set $f_{kx} = \{f_k(x) : x \in X\}$. At the end, V sends the set f_{ky} to C that evaluates $f_{kx} \cap f_{ky}$. This approach was used by Hazay and Lindell [16], Jarecki and Liu [17], Hazay and Nissim [19] and Hazay [15] to propose PSI protocols secure in the semi-honest and malicious settings. The most efficient protocol that does not require non standard assumptions [15] costs $O(v+c)$ computations under the strong-DDH assumption and $O((v + c) \log (v + c))$ under the DDH assumption.

Contrary to existing PSI protocols that rely on cryptographic schemes, we propose a novel PSI protocol based on efficient matrix algebra and secure under the mixed model of adversaries. Our protocol incurs $O(v + c)$ communications and server computations while maintaining fairness.

III. FAC: A Novel RFID-based Food Adequacy Check System

In this section, we present a novel RFID-application that aims to check the adequacy of foods to shoppers' personal preferences.

A. FAC Overview

To illustrate the FAC application, we consider a supermarket that tagged its items with RFID tags, and provides shopping carts with embedded RFID reader devices for its clients. Each client will be provided a mobile application that he/she sets up on his/her smartphone to enter information about personal food preferences that he/she wants to match. When a client enters the supermarket he/she uses the provided mobile application to connect to the supermarket wireless gateway. Then, each time the shopper takes an item from the shelf and passes it through the embedded RFID reader device, the latter reads the item tag and passes its information to the mobile application of the shopper. Once the application handles a novel arriving tag information, it sends it to the back-end server with a profile matching request. The shopper's smartphone and the back-end server start running a profile matching process using our novel private set intersection protocol (Π-FAC). This application ends-up by showing the shopper which profiles match the taken item among the set of profiles that he/she entered.

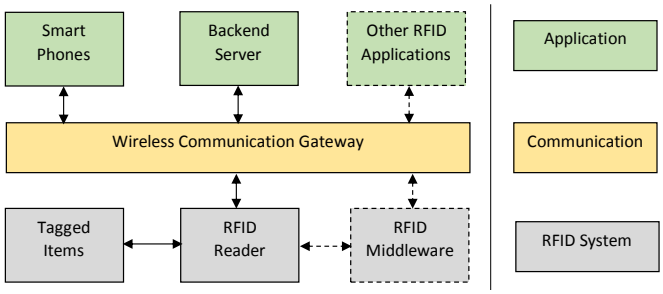


Figure 1. Architecture & Infrastructure requirements for FAC application

B. FAC Architecture

To implement the FAC application, we propose the following architecture model that is based on three layers, namely RFID system, communication, and application (Figure 1).

- **RFID system.** This is the basic layer. It consists of an RFID system with standard components. It involves passive tags put on each item of the supermarket, reader devices that can be either fixed on the shelves or embedded on shopping carts, and an RFID middleware. This latter component is not required by our FAC application, it aims to recover each tag read by a device to enable the integration of other application using the same RFID infrastructure.
- **Communication layer.** It involves a wireless communication gateway that covers the supermarket surface. It aims to interconnect the upper-layer components and ensures the communication with the RFID reader devices and the middleware.
- **Application layer.** It involves the FAC application set up on the clients' smartphones and the back-end server of the supermarket. The mobile application allows the user to input its personal preferences and connect to the back-end to run the private profile matching process using our built-in private set intersection protocol (Π-FAC).

IV. A Novel Private And Efficient Set Intersection Protocol

In this section, we present our novel private set intersection protocol as well as its design model.

A. Our Methodology

In this work, we use a matrix-based approach in which we represent the private sets of profiles as row matrices (each matrix corresponds to a private set of profiles and each row within it corresponds to a profile in the set). Then, each party obfuscates its matrix by performing a multiplication with a random matrix chosen independently from the input domain. Next, each party sends its resultant matrix to the other party to be multiplied by the other random matrix. Since, matrix product is not commutative, which is required for the correctness of the scheme, the two parties will interchange the side of the matrix product (left multiplication and right multiplication). At the end, the two resulting matrices will be checked for rows equality as each row corresponds to an original element in the set. In what follows, we give a detailed implementation of the Π-FAC protocol.

B. Protocol Design

To introduce our novel private set intersection protocol (Π-FAC), we consider a client denoted C and a back-end server denoted V having respectively $X = \{x_1, ..., x_c\}$ and $Y = \{y_1, ..., y_v\}$ sets of profiles and want to securely get the intersection between their sets. Assume for $1 \leq i \leq c$ and $1 \leq j \leq v$: x_i and $y_j \in \mathbb{R}^n$. Let $\mathbb{M}(m, n)$ denote the set of all m-by-n matrices and $\otimes$ denote the matrix multiplication operator. Let $\underline{\mathbf{M1}}$ and $\underline{\mathbf{M2}}$ denote random invertible matrices used by C and V respectively to obfuscate their sets, where $\underline{\mathbf{M1}} \in \mathbb{M}(c, c)$ and $\underline{\mathbf{M2}} \in \mathbb{M}(n, n)$. Let $\underline{\mathbf{MX}}$ and $\cup_{i>1}\underline{\mathbf{MY}_i}$ denote the private sets X and Y respectively, represented as row matrices, where $\underline{\mathbf{MX}} \in \mathbb{M}(c, n)$ and $\underline{\mathbf{MY}_i} \in \mathbb{M}(c, n)$. We present the detail of Π-FAC protocol in Algorithm 1.

Algorithm 1: Π-FAC, a Private and Efficient Set Intersection Protocol

Input : $X = \{x_1, ..., x_c\}$ C's set of personal profiles
$Y = \{y_1, ..., y_v\}$ V's set of all item profiles
Output: (For C only) $\Psi(X, Y)$: the private set intersection between X and Y
Require: $(c, n) \in \mathbb{N}^2$: $0 < c < n$
Step 1 by C
1: Generates a random invertible $\underline{\mathbf{M1}} \in \mathbb{M}(c, c)$
2: Creates $\underline{\mathbf{MX}} \in \mathbb{M}(c, n)$ with X's elements as rows
3: Computes $\underline{\mathbf{M1X}}$ = $\underline{\mathbf{M1}} \otimes \underline{\mathbf{MX}}$
4: Sends $\underline{\mathbf{M1X}}$ to V
Step 2 by V
5: Generates a random invertible $\underline{\mathbf{M2}} \in \mathbb{M}(n, n)$
6: Computes $\underline{\mathbf{M1X2}}$ = $\underline{\mathbf{M1X}} \otimes \underline{\mathbf{M2}}$
7: **for** $(i = 1; i < (v/c) + 1; i++)$ **do**
8: Creates $\underline{\mathbf{MY}_i} \in \mathbb{M}(c, n)$ with Y's elements as rows
9: Computes $\underline{\mathbf{MY2}_i}$ = $\underline{\mathbf{MY}_i} \otimes \underline{\mathbf{M2}}$
10: **end for**
11: Sends $\underline{\mathbf{M1X2}}$ and $\cup_{i>1}\underline{\mathbf{MY2}_i}$ to C
Step 3 by C
12: Computes $\underline{\mathbf{M1Y2}_i}$ = $\underline{\mathbf{M1}} \otimes \underline{\mathbf{MY2}_i}$, for each received $\underline{\mathbf{MY2}_i}$
13: For each (m, n, i) if $\underline{\mathbf{M1X2}}$[m,*] = $\underline{\mathbf{M1Y2}_i}$[n,*] and $\underline{\mathbf{M1X2}}$[m,*] $\notin \Psi(X, Y)$ then puts $\underline{\mathbf{M1X2}}$[m,*] in $\Psi(X, Y)$

V. Security Analysis

In this section, we give a security proof of our protocol using the Real/Ideal security model [5].

A. Security Model

Let Π denote a multi-party protocol executed by m participants (P_1,...,P_m) in order to evaluate a function f. Let B denote the class of adversary that may corrupt participants in Π. Let R and D denote respectively the real and the ideal executions of Π on the set of inputs w and the set of security parameters sec.

Notation 1. *Let $view_E^{\Pi}(w,sec)_i$ denote the set of messages received by the party $P_{i\in\{1,...,m\}}$ along with its inputs and outputs during the execution E of Π on the set of inputs w and security parameters sec.*

Notation 2. *Let $out_E^{\Pi}(w,sec)_i$ denote the output of the party $P_{i\in\{1,...,m\}}$ by the execution E of the protocol Π on the set of inputs w and security parameters sec. Let $out_E^{\Pi}(v,sec)$ denote the global output of all collaborating parties from the same execution of Π, where*

$$out_E^{\Pi}(w, sec) = \cup_{i=1}^{m} out_E^{\Pi}(w, sec)_i$$

During a **real execution** (R) we consider the presence of an adversary denoted A that behaves according to the class B while corrupting a set of participants $P_{i(1\leq i\leq m)}$. At the end of R, uncorrupted parties output whatever was specified in Π and the corrupted P_i outputs any random functions of their $view_R^{\Pi}(w,sec)_i$.

During an **ideal execution** (D) we consider the presence of a trusted incorruptible party denoted T, which receives the set of inputs w from all participants in order to evaluate the function f in the presence of an adversary denoted S. We assume S corrupts the same P_i as the correspondent adversary A of real execution, and behaves according to the same class B before sending inputs to T. By the end of D, uncorrupted participants output what was received from T and the corrupted P_i output any random functions of their $view_D^{\Pi}(w,sec)_i$.

Definition 1. *Let Π and f be as above. We consider Π a secure multi-party protocol if for any real adversary A having a class B and attacks the protocol Π during its execution on the set of inputs w and the set of security parameters sec, there exists an adversary S in the ideal execution having the same class B and that can emulate any effect achieved by*

A. Let $\stackrel{d}{\equiv}$ denote the distribution equality. We formalize the definition of a secure multi-party protocol Π as follows

$$\{out_R^{\Pi}(w, sec)\} \stackrel{d}{\equiv} \{out_D^{\Pi}(w, sec)\} \quad (1)$$

B. Security Proof

In what follows, we give security simulations of Π-FAC protocol using Real/Ideal paradigm. The allowed behavioural class of adversary is the mixed one, where the client (C) having a set of inputs X is actively corrupted and the server (V) having the set of inputs Y is passively corrupted.

Let A, S and T denote respectively a real adversary, an ideal adversary and a trusted third party, where A and S have the same class. Let Π denote the Π-FAC protocol (Algorithm 1), sec denote security parameters that will be presented below (Theorem 1), w denote the set of inputs $\{\underline{\mathbf{MX}}, \cup_{i>1}\underline{\mathbf{MY}_i}\}$, which are the matrix representation of the sets X and Y respectively, and $\Psi(X, Y)$ denote the private set intersection between X and Y.

Theorem 1. *Given a set of security conditions (sec) defined as $sec = \{(n, c) \in \mathbb{N}^2 : 0 < c < n\}$. Under these conditions, the protocol Π-FAC defined in Algorithm 1 is a secure multi-party protocol against an active corruption of C.*

Proof: Assume C is actively corrupted by A. Then, it can only inject fake inputs (**MA**) since aborting the protocol untimely will have no meaning. Assume C sends a fake **MA**. In this case, S can emulate A by just handling the fake **MA** and sends it to T, which performs the required computation and sends back $\Psi(X, Y)$ to C. Thereby, completing the simulation. At the end, the views of C in Ideal and Real executions are as follows

$$view_D^{\Pi}(w, sec)_C = \{\underline{\mathbf{MX}}, \Psi(X, Y)\} \quad (2)$$

$$view_R^{\Pi}(w, sec)_C = \{\underline{\mathbf{MX}}, \underline{\mathbf{M1X2}}, \cup_{i>1}\underline{\mathbf{MY2}_i}, \Psi(X, Y)\} \quad (3)$$

Otherwise, **M1X2** = **M1X** ⊗ **M2**, where **M1X** $\in \mathbb{M}(c, n)$ and **M2** $\in \mathbb{M}(n, n)$. According to security parameters (sec), we have $c < n$. This preserves well the privacy of **M2**. Thereby, **M1X2** that contains $(c \times n)$ equations opposite to $(n \times n)$ unknowns for C, will not involve meaningful information for it and can be reduced from its view. Likewise, $\cup_{i>1}\underline{\mathbf{MY2}_i}$ = $\cup_{i>1}\underline{\mathbf{MY}_i} \otimes$ **M2**, where $\underline{\mathbf{MY}_i} \in \mathbb{M}(c, n)$ and **M2** $\in \mathbb{M}(n, n)$. Then, $\cup_{i>1}\underline{\mathbf{MY2}_i}$ will contain $\alpha(c \times n)$ equations opposite to $(\alpha(c \times n)+(n \times n))$ unknowns for C, where $0 < \alpha < (v/c)+1$. This, does not involve meaningful information for it and can be so, reduced from its view. After these reductions, the view of C in real execution will be defined as follows

$$view_R^{\Pi}(w, sec)_C = \{\underline{\mathbf{MX}}, \Psi(X, Y)\} \quad (4)$$

Thus, relying on (2) and (4) we get

$$\{out_R^{\Pi}(w, sec)_C\} \stackrel{d}{\equiv} \{out_D^{\Pi}(w, sec)_C\} \quad (5)$$

On the other hand, the uncorrupted V can not be affected by the corruption of C since V does not require any output in real execution. Thus, T will simply not send it any output during ideal execution. This, means that

$$\{out_R^{\Pi}(w, sec)_V\} \stackrel{d}{\equiv} \{out_D^{\Pi}(w, sec)_V\} \quad (6)$$

Through (5) and (6), we proved by simulation that all effects achieved by a real active adversary corrupting C can also be achieved in an ideal execution. Then, Π-FAC is a secure multi-party protocol against active corruption of C (Definition 1). ■

Theorem 2. *Given a set of security conditions (sec) defined as $sec = \{(n, c) \in \mathbb{N}^2 : 0 < c < n\}$. Under these conditions, the protocol Π-FAC defined in Algorithm 1 is a secure multi-party protocol against a passive corruption of V.*

Proof: Assume V is passively corrupted. In this case, V should follow the specification of the protocol Π-FAC, yet, it is allowed to analyse all data gathered during the execution. Then, S will just handle V's input and sends it to T, which performs the required computation and sends $\Psi(X, Y)$ to C while sending nothing to V. Thereby, completing the simulation. At the end, the views of V in Ideal and Real executions are as follows

$$view_D^{\Pi}(w, sec)_V = \{\cup_{i>1}\underline{\mathbf{MY}_i}\} \quad (7)$$

$$view_R^{\Pi}(w, sec)_V = \{\cup_{i>1}\underline{\mathbf{MY}_i}, \underline{\mathbf{M1X}}\} \quad (8)$$

Moreover, **M1X** = **M1** ⊗ **MX**, where, **M1** $\in \mathbb{M}(c, c)$ and **MX** $\in \mathbb{M}(c, n)$. Then, since we defined $(0 < c)$ as security parameter (sec), we get $(c \times n) < ((c \times n)+(c \times c))$. Thus, **M1X** that contains $(c \times n)$ opposite to $((c \times n)+(c \times c))$ unknowns for V will not involve meaningful information for it and can be, so, reduced from its view. After reduction, we obtain

$$view_R^{\Pi}(w, sec)_V = \{\cup_{i>1}\underline{\mathbf{MY}_i}\} \quad (9)$$

Thus, relying on (7) and (9) we get

$$\{out_R^{\Pi}(w, sec)_V\} \stackrel{d}{\equiv} \{out_D^{\Pi}(w, sec)_V\} \quad (10)$$

On the other hand, the uncorrupted C outputs what was received from T in ideal execution, which is $\Psi(X, Y)$ according to the simulation given above and outputs what was specified in the protocol Π-FAC in real execution, which is $\Psi(X, Y)$ (Algorithm 1, Output section) . Then, we have

$$\{out_R^{\Pi}(w, sec)_C\} \stackrel{d}{\equiv} \{out_D^{\Pi}(w, sec)_C\} \quad (11)$$

Through (10) and (11) we proved by simulation that all effects achieved by a real passive adversary corrupting V can also be achieved in an ideal execution. Then, Π-FAC is a secure multi-party protocol against passive corruption of V (Definition 1). ■

Corollary 1. *Given a set of security conditions (sec) defined as $sec = \{(n, k) \in \mathbb{N}^2 : 0 < k < n\}$. Under these conditions, the protocol Π-FAC defined in Algorithm 1 is a secure multi-party protocol in the mixed model of adversary, where C is actively corrupted and V is passively corrupted.*

Proof: Corollary 1 relies heavily on the Theorem 1 and Theorem 2 proved above, while considering separately the case when the client (C) is corrupted and the case when the server (V) is corrupted. We assume that if both parties are corrupted we are not required to provide security guarantees. ■

VI. Performance Analysis

In this section, we simulate the performance of our protocol (Π-FAC) using a queueing theory model. We make experiments on the same data sets with a custom simulator built in Python and an Intel i5-2557M CPU running at 1.70 GHz and having a 4 GB of RAM.

1) Experimental scenario: We consider a large-scale supermarket that wants to provide their clients with a Food Adequacy Check (FAC) service using our private set intersection protocol (Π-FAC). In order to assess the scalability of Π-FAC, we consider the back-end server (V) receiving (N) FAC requests from different clients (C) at rate (λ) request(s) per minute according to a Poisson process: $N \sim P(\lambda)$. Assume the requests processing times (t_i) have an exponential distribution with rate (μ) requests per minute $t_i \sim exp(\mu)$. Without loss of generality, we consider fixing the number of client personal profiles to 10 profiles per client, where each profile involves 20 attributes ($\in \mathbb{R}^{20}$). Besides, we consider V having 1000 profiles of 20 attributes per item. This, results in an average range of 50 possible values for each attribute, which is highly sufficient in real applications.

For comparison purpose, we model the same above scenario, while V uses the hash-based private set intersection protocol used in practice (Section IV-A) instead of our Π-FAC protocol. For this, we use an efficient commutative hash function $H_k(x) = x^k \ mod \ p$, where k is a 32-bit security parameter and p is a 32-bit random prime.

Assume V having a FIFO service discipline with unlimited access, and operating all day long. Let $M/M/1$ denote this system using Kendall's notation [23]. We evaluate this system by varying the the number of clients requesting for FAC service (λ) in the range $\{10, 20, 50, 100, 200\}$ clients (requests) per minute. Let $mult$, add, exp and mod denote respectively one multiplication, one addition, one exponentiation and one modulo operations. Let v and c denote the number of profiles of V and C respectively, where each profile involves n attributes. To measure μ parameter, we evaluate the computational costs required by V when using Π-FAC and the hashing scheme by the following equations.

$$Cost_V^{(\Pi-FAC)} = n^2(v+c)\ mult\ + n(n-1)(v+c)\ add$$
$$Cost_V^{(hash)} = n(v+c)\ exp + n(v+c)\ mod$$

2) Results & discussion: We have made experimental evaluations by simulating two back-end servers of a supermarket handling FAC requests, while one was running Π-FAC protocol and the other was running a hash-based protocol. We used the model described in Table 1 and we evaluated the system performance for each protocol according to the number of requests (λ) through the following metrics: the usability rate (U) of the back-end server, its response time (R), the average number of clients (N) in the system, and the mean length of waiting queue (Q). Let ρ denote the intensity traffic rate. We assess the previous metrics according to the following equations and we present the results in Table 1 and Figure 4.

$$\rho = \frac{\lambda}{\mu} \quad U = \rho \quad N = \frac{\rho}{1-\rho} \quad Q = N - \rho \quad R = \frac{N}{\lambda}$$

For low arrival rates ($\lambda < 100$) results show that the server running Π-FAC was undergoing a slow intensity traffic ($\rho < 0.1$), which results in a very low probability of server overload. This claim may be confirmed by looking the low server utilization rate ($U < 10\%$), besides, the zero queue length ($Q = 0$). On the hand, the server running the hash protocol was less efficient with a usability rate of $U > 70\%$ for 50 clients per minute. This high usability tends to overload the server if more clients arrive ($\lambda > 50$), which may be confirmed by looking the increase in the number of clients waiting in the queue ($Q > 0$). Regarding response time, Π-FAC provided a high efficient and stable response ($R = 2.x$ ms) compared to the hash protocol, which was less efficient and had a significant delay each time there was an increase in the arrival rate.

For high arrival rates ($\lambda > 100$), the server running Π-FAC remained efficient with a usability rate of $U < 50\%$ for 200 clients per minute while providing a high efficient response time ($R < 4$ ms). In contrast, the server running the hash protocol was undergoing a very high intensity traffic ($\rho > 1$), which leads the system to a non-steady state and results in overloading the server with a utilization rate of $U > 100\%$. This, tended to an infinite queue length ($Q = \infty$) and an infinite response time ($R = \infty$).

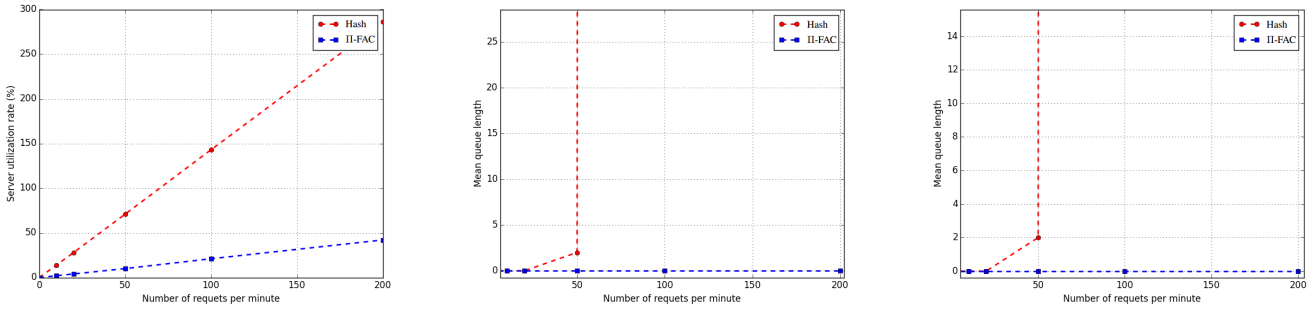
Experimental results revealed the efficiency of our Π-FAC protocol compared to the hash-based solution used in practice. This efficiency raises from the fact that our protocol involves efficient arithmetic operations (addition and multiplication) and does not require any expensive computations (modulo, exponentiation), which are involved in cryptographic methods. These performance results show the adequacy of our protocol to be used by large scale supermarkets.

VII. Conclusion

In this paper, we expanded a novel RFID-based application that aims to check whether food items matches the preferences of the shoppers, according to their personal profiles. For this, we proposed Π-FAC, a novel set intersection protocol that targets privacy and efficiency concerns while matching shoppers' preferences with item profiles that are held by the back-end server of the store. Through security analysis conducted with the standard Real/Ideal paradigm, we showed the privacy guarantees provided by Π-FAC against curious stores and malicious clients. Besides, across empirical performance analysis, we demonstrated the high efficiency of our protocol compared to the hash-based private set intersection used in practice. Evaluation results revealed the adequacy of Π-FAC to provide a private and efficient Food Adequacy Check service for large-scale stores.

Table I
EVALUATION OF A BACK-EN SERVER STORE USING M/M/1 MODEL

Fixed Parameters	Used Protocol	Client Requests (λ)/min	Running Time s	Processing Rate (μ)	Intensity Traffic (ρ)	Usability Rate (U) %	Number of Client (N) $\times$ 10^2	Queue Length (Q)	Response Time (R) ms
		10	1.29		0.02	2	2	0	2
		20	2.54		0.04	4	4	0	2
	Π-FAC	50	6.30	470	0.10	10	11	0	2.2
		100	12.79		0.21	21	26	0	2.6
v= 1000		200	25.53		0.42	42	72	0	3.6
c= 10									
n= 20		10	8.59		0.14	14	16	0	16
		20	17.28		0.28	28	39	0	19.5
	Hash	50	42.80	70	0.71	71	245	2	49
		100	86.53		1.43	143	∞	∞	∞
		200	171.66		2.86	286	∞	∞	∞



(a) Usability Rate (U) (b) Queue length (Q) (c) Response time (R)

Figure 2. Evaluation of a back-en server store using M/M/1 model

REFERENCES

[1] M. R. Das, *RFID Forecasts, Players and Opportunities 2016-2026*. IDTechEx.

[2] Walmart stores, inc. wal-mart continues rfid expansion. [Online]. Available: http://corporate.walmart.com/ [visited 04/30/2017]

[3] e. a. Puerini, Gianna Lise, "Transitioning items from a materials handling facility," US Patent, 01 08, 2015.

[4] M. L. Dansinger, J. A. Gleason, J. L. Griffith, H. P. Selker, and E. J. Schaefer, "Comparison of the atkins, ornish, weight watchers, and zone diets for weight loss and heart disease risk reduction: a randomized trial," *Jama*, vol. 293, no. 1, pp. 43–53, 2005.

[5] R. Canetti, "Security and composition of multiparty cryptographic protocols," *Journal of CRYPTOLOGY*, vol. 13, no. 1, pp. 143–202, 2000.

[6] The best of global digital marketing. case study: Hellmann's recipe cart. [Online]. Available: http://www.best-marketing.eu/case-study-hellmanns-recipe-cart/ [visited 04/30/2017]

[7] The wall street journal. whole foods aims for younger shoppers with new stores. [Online]. Available: http://www.wsj.com/articles/whole-foods-to-launch-new-outlets-1431041549 [visited 04/30/2017]

[8] M. Naor and B. Pinkas, "Oblivious transfer and polynomial evaluation," in *Proceedings of the Thirty-first Annual ACM Symposium on Theory of Computing*, ser. STOC '99. New York, NY, USA: ACM, 1999, pp. 245–254.

[9] M. J. Freedman, Y. Ishai, B. Pinkas, and O. Reingold, *Keyword Search and Oblivious Pseudorandom Functions*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 303–324.

[10] M. J. Freedman, K. Nissim, and B. Pinkas, *Efficient Private Matching and Set Intersection*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 1–19.

[11] L. Kissner and D. Song, "Privacy-preserving set operations," in *Proceedings of the 25th Annual International Conference on Advances in Cryptology*, ser. CRYPTO'05. Berlin, Heidelberg: Springer-Verlag, 2005, pp. 241–257.

[12] E. De Cristofaro, J. Kim, and G. Tsudik, *Linear-Complexity Private Set Intersection Protocols Secure in Malicious Model*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 213–231.

[13] C. Hazay and M. Venkitasubramaniam, *Scalable Multi-party Private Set-Intersection*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2017, pp. 175–203.

[14] D. Dachman-Soled, T. Malkin, M. Raykova, and M. Yung, *Efficient Robust Private Set Intersection*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 125–142.

[15] C. Hazay, *Oblivious Polynomial Evaluation and Secure Set-Intersection from Algebraic PRFs*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015, pp. 90–120.

[16] C. Hazay and Y. Lindell, "Efficient protocols for set intersection and pattern matching with security against malicious and covert adversaries," *Journal of Cryptology*, vol. 23, no. 3, pp. 422–456, 2010.

[17] S. Jarecki and X. Liu, *Efficient Oblivious Pseudorandom Function with Applications to Adaptive OT and Secure Computation of Set Intersection*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 577–594.

[18] R. Canetti and M. Fischlin, *Universally Composable Commitments*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, pp. 19–40.

[19] C. Hazay and K. Nissim, "Efficient set operations in the presence of malicious adversaries," *Journal of Cryptology*, vol. 25, no. 3, pp. 383–433, 2012.

[20] Y. Lindell and B. Pinkas, "Secure multiparty computation for privacy-preserving data mining," *Journal of Privacy and Confidentiality*, vol. 1, no. 1, p. 5, 2009.

[21] J. Vaidya and C. Clifton, "Secure set intersection cardinality with application to association rule mining," *J. Comput. Secur.*, vol. 13, no. 4, pp. 593–622, Jul. 2005.

[22] B. Pinkas, T. Schneider, and M. Zohner, "Scalable private set intersection based on ot extension," 2016.

[23] E. Gelenbe, G. Pujolle, and J. Nelson, *Introduction to queueing networks*. John Wiley & Sons, Inc., 1987, vol. 2.