Towards Secure and Accurate Targeted Mobile Coupon Delivery

JINGHUA JIANG1,2, YIFENG ZHENG2,3, XINGLIANG YUAN2,3, ZHENKUI SHI2,3, XIAOLIN GUI1, CONG WANG2,3, AND JING YAO1,2

1School of Electronic and Information Engineering, Xi’an Jiaotong University, Xi’an 710049, China
2Department of Computer Science, City University of Hong Kong, Hong Kong
3City University of Hong Kong Shenzhen Research Institute, Shenzhen 518057, China

Corresponding authors: X. Gui (xlgui@mail.xjtu.edu.cn); C. Wang (congwang@cityu.edu.hk).

This work was supported in part by the Research Grants Council of Hong Kong under Project CityU 138513 and Project CityU 11276816, in part by the National Natural Science Foundation of China under Project 61572412 and Project 61472316, in part by the Innovation and Technology Commission of Hong Kong under ITF Project ITS/307/15, an AWS Education Research Grant, and in part by the Science and Technology Project of Shaanxi Province under Grant 2016ZDJC-05.

ABSTRACT This paper presents our research on secure and accurate targeted mobile coupon delivery. Our goal is to enable the secure delivery of targeted coupons to eligible users equipped with mobile devices, whose behavioral profiles accurately satisfy the targeting profile defined by the vendor. Our design well preserves user privacy, and further provides the strict security guarantee of vendor protection, by verifying user’s eligibility for a coupon without revealing the vendor’s targeting profile. We first show a basic approach which can effectively address the challenges posed by secure and accurate targeted coupon delivery, via properly leveraging Yao’s garbled circuits. In order to achieve practical performance for resource-limited mobile devices, we then present our proposed design, which imposes lightweight workload on the user side, via properly bridging together homomorphic encryption and Yao’s garbled circuits. We implement a preliminary user-side prototype and deploy it on an Android smartphone to evaluate the performance. Extensive experimental results demonstrate that our proposed design achieves practical performance for mobile devices.

INDEX TERMS Targeted coupon delivery, user privacy, vendor protection, mobile, behavioral targeting.

I. INTRODUCTION

Online advertising via behavioral targeting is becoming increasingly prevalent. Behavioral targeting enables vendors to customize their messaging service based on the collected information about users’ behavior, such as geographic location, browsing histories, and purchase behaviors. Meanwhile, behavioral targeting also benefits users as they can enjoy more personalized services and have less exposure to information that is at odds with their interests [1]. Among others, one practical application of behavioral targeting is targeted coupon delivery [1]–[3], where vendors take into account users’ behavior information and intend to provide coupons to certain users who are likely to become loyal routine customers.

Despite the promising benefits, collecting user’s personal behavior information for targeting also raises privacy concerns [4]–[6]. Besides, targeted coupon delivery poses additional challenges beyond those demanded by targeted advertising. First, to prevent coupon exploitation attacks, coupons must be delivered to eligible users whose behavioral profiles accurately satisfy the vendor’s targeting profile [2]. Second, during the process of targeted coupon delivery, non-eligible users should learn nothing about the vendor’s targeting profile other than their non-eligibility. Otherwise, non-eligible users may attempt to take advantage of the information they learn to obtain targeted coupons [2], [3]. In order to protect user privacy and guarantee vendor protection, it is of critical importance to ensure that security must be embedded in the design for targeted coupon delivery service from the very beginning.

While there has been extensive research on privacy-preserving targeted ad delivery in the literature, little work has been done for secure targeted coupon delivery. Prior work aimed at achieving secure targeted coupon delivery either exposes the targeted coupons to a portion of non-eligible users [2], or leaks sensitive information about the vendor’s targeting profile to non-eligible users [3]. To our best knowledge, privacy-preserving behavioral targeting for targeted coupon delivery is still challenging, and to design a secure, accurate, and practical targeted coupon delivery...
delivery system, especially for resource-limited mobile devices, remains to be fully explored.

In this paper, we propose our research on secure and accurate targeted mobile coupon delivery. Our goal is to ensure that targeted coupons are delivered to eligible users whose behavioral profiles accurately satisfy the vendor’s targeting profile, while preserving user privacy and providing vendor protection. We first formulate secure and accurate targeted coupon delivery as a secure two-party computation problem, and provide a basic approach by properly leveraging the cryptographic primitive—Yao’s garbled circuits. In the basic approach, the vendor sends coupon and targeting profile in a protected form to the user. Then, a blind eligibility test protocol based on Yao’s garbled circuits is initiated between the user and the vendor, so as to securely test whether the user is eligible for a particular coupon. The basic approach ensures that during the process of targeted coupon delivery, no information about user’s behavioral profile is disclosed to the vendor, while the coupon and targeting profile of the vendor are protected against non-eligible users.

Although the basic approach can effectively address the security challenges faced by targeted coupon delivery, it is not practically suitable for mobile devices. Particularly, it suffers from critical efficiency issues for users, as the transmission and evaluation of the garbled circuit per targeted coupon delivery may consume intensive resources of mobile devices. In order to support secure and accurate targeted mobile coupon delivery in a mobile-friendly manner, we propose to build our design by shifting most workload of behavioral targeting to the vendor side while still achieving privacy preservation.

To this end, we modify the basic model a bit and consider a setting in which an additional party called crypto service provider (CSP) is available. In particular, the CSP does not collude with the vendor and users, and assists the vendor to perform blind eligibility test. We are aware that such a non-colluding two-server model is commonly adopted in the literature to facilitate various security-aware applications, e.g., privacy-preserving ridge regression [7], database queries [8], matrix factorization [9], and near-duplicate detection [10]. By properly bridging together the techniques of homomorphic encryption and garbled circuits, our proposed design provides the security guarantees required by targeted coupon delivery. Meanwhile, lightweight workload is imposed on the user. Specifically, the user only needs to submit her encrypted behavioral profile to the vendor. When a new coupon is available, the vendor performs blind eligibility test which produces small ciphertext metadata. Then the vendor simply pushes down the coupon ciphertext along with the ciphertext metadata, from which only eligible users can extract the key for coupon decryption. Our contributions can be summarized as follows.

- We propose a design for secure and accurate targeted mobile coupon delivery, which imposes lightweight workload on users’ mobile devices.
- We implement a preliminary user-side prototype on the Android platform, and test it on a real smartphone. Extensive experiments show that our design achieves practical performance on mobile devices.

The rest of this paper is organized as follows. We first present our problem statement in Section II. Then, we briefly introduce some cryptographic primitives in Section III, followed by the detailed design of secure and accurate targeted mobile coupon delivery in Section IV. We give performance evaluation in Section V, followed by the description of related work in Section VI. Finally, we conclude the whole paper in Section VII.

II. PROBLEM STATEMENT
A. SERVICE MODEL

Fig. 1 illustrates the basic model of our proposed secure targeted mobile coupon delivery service. We consider two primary parties: the user and the vendor. The user maintains a private behavioral profile on her mobile device, and wants to enjoy personalized coupon delivery service, while keeping her behavioral profile confidential. The vendor wants to perform accurate user targeting via taking into account user behavior, and deliver targeted coupons only to eligible users, so as to prevent coupon exploitation attacks. In particular, targeted coupons are required to be delivered to users whose behavioral profiles accurately satisfy the targeting profile specified by the vendor.

![Figure 1. The illustration of our service model.](image)

Following existing work [2], [3], we consider the user’s behavioral profile \(u\) as an \(n\)-dimensional vector, i.e., \(u = \{u_i\}_{i=1}^n\), where each element \(u_i\) is an integer that may refer to the value of some attribute such as the number of times specific websites have been visited, number of times of different geo-locations that have been visited, and number of similar products purchased in the past month [1], [2]. Likewise, the targeting profile \(v\) is also represented as an \(n\)-dimensional vector, i.e., \(v = \{v_i\}_{i=1}^n\), which characterizes the behavior of users that the vendor targets. The eligibility requirement for the user to obtain a particular coupon is that the distance (e.g., squared Euclidean distance) between the behavioral profile \(u\) and the targeting profile \(v\) is within a threshold \(\epsilon\), i.e., \(\text{Dist}(u, v) \leq \epsilon\). Our goal is to enable secure and accurate delivery of targeted coupons to eligible users whose behavioral profiles strictly satisfy the distance metric.
B. SECURITY THREATS AND GOALS
Being aimed at secure and accurate targeted mobile coupon delivery, our design will consider the protection for both the user and the vendor. Specifically, our design aims to provide the following security guarantees:

1) USER PRIVACY
No information about the user’s private behavioral profile is disclosed to the vendor throughout the targeted coupon delivery process, unless a coupon is redeemed by the user. More precisely, the behavioral profile and eligibility status of the user are both protected against the vendor during the process of targeted coupon delivery.

2) VENDOR PROTECTION
The coupon and targeting profile of the vendor should be protected against non-eligible users during the process of targeted coupon delivery. More precisely, from the information provided by the vendor, a user either learns that she is eligible to obtain a particular coupon, or learns nothing beyond her non-eligibility.

Similar to prior work [2], [3], we do not consider the protection of the user’s behavioral profile when she redeems a coupon, since: (1) Revealing the eligibility of a user who chooses to redeem a coupon is inevitable at the point of redemption in practice; (2) The result of coupon redemption could be beneficial to the vendor to improve the targeting service. Note that user authentication is not the focus of this work, and it can be handled by various orthogonal mechanisms such as passwords and digital certificates [11]. Meanwhile, we assume that the communication channel is secure, which can be achieved via a secure transportation protocol such as SSL.

III. CRYPTOGRAPHIC PRIMITIVES
A symmetric encryption scheme SE is a pair of algorithms (ES, DS). The encryption algorithm ES takes as input a key $K \in \{0, 1\}^k$ and a message $M \in \{0, 1\}^*$, and outputs a ciphertext $C$. We denote this encryption by $C \leftarrow ES_K(M)$. The decryption algorithm DS takes as input a key and a ciphertext $C$, and outputs a message $M$. We denote this decryption as $M \leftarrow DS_K(C)$. An asymmetric encryption scheme AE is a pair of algorithms (EA, DA). The encryption algorithm EA on input a public key $pk$ and a message $M \in \{0, 1\}^*$ outputs a ciphertext $C$. This encryption is written as $C \leftarrow EA_{pk}(M)$. The decryption algorithm DA takes as input a secret key $sk$ and a ciphertext $C$, and outputs a message $M$. This decryption is denoted as $M \leftarrow DA_{sk}(C)$.

A. YAO’S GARBLED CIRCUITS
Yao’s garbled circuits enables two parties to jointly compute an arbitrary function $\text{fun}(a, b)$ on their respective inputs $a$ and $b$, without leaking any information about their inputs beyond what is implied by the function output [12], [13]. In particular, one party, referred to as generator, first prepares a garbled version of a circuit that computes $\text{fun}(\cdot, \cdot)$. Then, the generator provides the other party, referred to as evaluator, with the garbled circuit and the garbled input $\hat{a}$ corresponding to $a$. The evaluator then obliviously obtains the garbled input $\hat{b}$ corresponding to $b$, via running a 1-out-of-2 oblivious transfer ($OT^2$) protocol with the generator. After this, the evaluator can evaluate the garbled circuit by using $\hat{a}$ and $\hat{b}$ as inputs, so as to obtain the result of $\text{fun}(a, b)$.

B. ADDITIVELY HOMOMORPHIC ENCRYPTION
An asymmetric encryption scheme $HE = (EH, DH)$ with a key pair $< pk, sk >$ is additively homomorphic if it has the following property: $EH_{pk}(m_1 + m_2) = EH_{pk}(m_1) \cdot EH_{pk}(m_2)$, where the public key $pk$ is used to encrypt a message and the secret key $sk$ is used to decrypt a ciphertext.

IV. DESIGN OF SECURE AND ACCURATE TARGETED MOBILE COUPON DELIVERY
In this section, we present our proposed design for secure and accurate targeted mobile coupon delivery. We start with a basic approach which builds on garbled circuits. We analyze its security guarantee and discuss the limitation. Then we present our proposed design, which takes into account both security and user cost efficiency.

A. BASIC APPROACH
1) OVERVIEW
In this basic approach, the vendor first sends the encrypted coupon and targeting profile in protected form to the user. Then, a blind eligibility test protocol is initiated between the user and the vendor to securely test whether the user is eligible for the particular coupon, i.e., whether the distance between the user’s behavioral profile and the vendor’s targeting profile is within a certain threshold. During the protocol execution process, the user’s behavioral profile and the vendor’s targeting profile are kept private against each other. Besides, the vendor is oblivious to the eligibility test result. After the blind eligibility test, an eligible user can obtain the coupon encryption key and further decrypt the encrypted coupon. Otherwise, the user learns nothing beyond her non-eligibility for that particular coupon.

We support such a kind of eligibility test, our main idea is to initiate a secure two-party computation protocol between the vendor and the user, based on Yao’s garbled circuits. Form a high-level perspective, the vendor prepares a garbled circuit for the user, who acts as an evaluator to perform evaluation of the garbled circuit. If the distance between the user’s behavioral profile and the vendor’s targeting profile is within the threshold, the evaluation outputs the coupon encryption key, which can be used to decrypt the encrypted coupon later. Otherwise, the evaluation outputs a dummy key, and the decryption of the coupon ciphertext will fail.

2) PROTOCOL
We now present the detailed protocol for our basic approach. Let $\text{Sig}()$ be some digital signature scheme
detailed protocol proceeds as follows: (e.g., RSA-based signature). As illustrated in Fig. 2, the garbled circuit design in our basic approach.

FIGURE 2. High-level description of our basic approach.

3) SECURITY ANALYSIS

The security of the above basic approach is straightforwardly guaranteed by that of Yao’s garbled circuits, the formal proof of which could be found in [13]. First, the user’s behavioral profile and the vendor’s targeting profile are well protected against each other during the process of blind eligibility test. Second, as the garbled circuit is executed on the user side, the evaluation result is not disclosed to the vendor. Third, only the eligible user can obtain the key for coupon decryption while non-eligible user is prevented from recovering the coupon. Therefore, the above basic approach well preserves user privacy and provides vendor protection simultaneously.

Remark: The above basic approach ensures that targeted coupons are only delivered to eligible users whose behavioral profiles strictly satisfy the distance metric, in a privacy-preserving manner. On the other hand, it requires the user to actively interact with the vendor per targeted coupon delivery. Besides, the transmission and execution of garbled circuit may consume intensive resources of mobile devices. Therefore, from the perspective of cost efficiency for mobile devices, the basic approach is not necessarily suitable for secure and accurate targeted mobile coupon delivery.

B. PROPOSED DESIGN

To support secure and accurate targeted mobile coupon delivery with as little user cost as possible, we propose to build a customized garbled circuit based design that securely shifts most workload of behavioral targeting to the vendor side. In the literature, we observe that the non-colluding two-server model is commonly used to facilitate privacy-preserving computation in various application scenarios, e.g., privacy-preserving ridge regression [7], privacy-preserving database queries [8], privacy-preserving matrix factorization [9] and privacy-preserving near-duplicate detection [10]. Inspired by those work, we modify the basic model a bit and build our proposed design under the non-colluding two-server model. In particular, a third party called crypto service provider (CSP) that does not collude with the vendor or users is introduced to assist in the blind eligibility test.

From a high level point of view, the main workflow in our proposed design is as follows. Initially, the user only needs to send her encrypted behavioral profile to the vendor. Then, when a new coupon is available, a protocol based on customized garbled circuit design is initiated between the vendor and the CSP to perform blind eligibility test. The protocol outputs some ciphertext metadata on the vendor side. In the literature, we observe that the non-colluding two-server model is commonly used to facilitate privacy-preserving computation in various application scenarios, e.g., privacy-preserving ridge regression [7], privacy-preserving database queries [8], privacy-preserving matrix factorization [9] and privacy-preserving near-duplicate detection [10]. Inspired by those work, we modify the basic model a bit and build our proposed design under the non-colluding two-server model. In particular, a third party called crypto service provider (CSP) that does not collude with the vendor or users is introduced to assist in the blind eligibility test.

From a high level point of view, the main workflow in our proposed design is as follows. Initially, the user only needs to send her encrypted behavioral profile to the vendor. Then, when a new coupon is available, a protocol based on customized garbled circuit design is initiated between the vendor and the CSP to perform blind eligibility test. The protocol outputs some ciphertext metadata on the vendor side, from which only those eligible users can extract the coupon encryption key $K$ and successfully decrypt the coupon ciphertext, while a non-eligible user will obtain a dummy key $K'$ and fail in coupon decryption.

4) When an eligible user chooses to redeem the recovered coupon, the vendor checks the validity of the redeemed coupon by verifying the signature $\sigma$, and the $UID$ of the redeeming user.

FIGURE 3. The garbled circuit design in our basic approach.

(e.g., RSA-based signature). As illustrated in Fig. 2, the detailed protocol proceeds as follows:

1) The vendor first produces the ciphertext $C_M$ for a coupon $M$: $C_M = ES_K(M||UID||Nonce||\sigma)$, where $K$ is the encryption key, $UID$ specifies the user, $Nonce$ is a fresh random number per encrypted coupon delivered to the user, and $\sigma = Sig_{vendor}(M||UID||Nonce)$ is the signature indicating that the encrypted coupon delivery has been digitally signed by the vendor.

2) The vendor then prepares a garbled circuit as depicted in Fig. 3. The garbled circuit takes as input the garbled values of the user’s behavioral profile $u$, the vendor’s targeting profile $v$, the coupon encryption key $K$, a dummy key $K'$, and the threshold $\epsilon$, denoted as $\hat{u}$, $\hat{v}$, $\hat{K}$, $\hat{K'}$, and $\hat{\epsilon}$, respectively. Subsequently, the vendor sends the coupon ciphertext $C_M$, the garbled circuit, and the garbled inputs $\hat{v}$, $\hat{K}$, $\hat{K'}$ and $\hat{\epsilon}$ to the user.

3) Upon receiving the data, the user runs a 1-out-of-2 oblivious transfer protocol with the vendor to obtain the garbled input $\hat{u}$ of her behavioral profile $u$. Then, based on the garbled circuit and the garbled inputs $\hat{u}$, $\hat{v}$, $\hat{K}$, $\hat{K'}$ and $\hat{\epsilon}$, the user evaluates the garbled circuit. At the end of evaluation, an eligible user will obtain the coupon encryption key $K$ and successfully decrypt the coupon ciphertext, while a non-eligible user will obtain a dummy key $K'$ and fail in coupon decryption.
Specifically, our protocol includes the following phases.

work under the non-colluding two-server model [7], [9], [10].

To recover user’s behavioral profile, we will use inside the garbled circuit. To avoid decryption within the circuit, the user’s eligibility status. After the blind eligibility test, the vendor simply pushes down the coupon ciphertext and the resultant ciphertext metadata to the user. From the ciphertext metadata, an eligible user then efficiently extracts the correct coupon encryption key for coupon decryption, while a non-eligible user will recover a dummy key and thus fail in coupon decryption.

1) DESIGN RATIONALE
The challenge facing us is how to perform blind eligibility test over encrypted user’s behavioral profile at the vendor side, while preventing the vendor from knowing the eligibility status of the user. To tackle this challenge, our main idea is to let the CSP provide the vendor with a garbled circuit inside which the user’s behavioral profile is recovered and eligibility test is conducted. The evaluation of the garbled circuit by the vendor outputs a masked coupon encryption key which is generated by the CSP for each user per garbled circuit evaluation. More precisely, if the user’s behavioral profile accurately satisfies the targeting profile, then from the vendor’s public key, an eligible user recovers this key and can extract the coupon encryption key from ciphertext, via computing . On the other hand, a non-eligible user recovering is not able to correctly extract from , and thus will fail in coupon decryption.

2) PROTOCOL
With the above design rationale, we are now ready to present the details of our proposed protocol. As described above, the encrypted user’s behavioral profile needs to be recovered inside the garbled circuit. To avoid decryption within the circuit for the recovery of user’s behavioral profile, we will use additively homomorphic encryption and random masking to protect user’s behavioral profile, inspired by existing security work under the non-colluding two-server model [7], [9], [10]. Specifically, our protocol includes the following phases.

a: SYSTEM SETUP
The CSP generates a key pair < pkCSP, skCSP > of some additive homomorphic encryption scheme HE = (E, D) (e.g., the Paillier cryptosystem), and publishes the public key pkCSP. Each user also generates a key pair < pku, sku > of some asymmetric encryption scheme AE = (EA, DA) (e.g., the RSA cryptosystem). Besides, the vendor provides the CSP with the specification of the garbled circuit, such as the dimension of targeting profile, and the length of the coupon encryption key .

b: SECURE TARGETED COUPON DELIVERY
As illustrated in Fig. 4, our protocol then supports secure and accurate targeted mobile coupon delivery as follows. First, each user sends her encrypted behavioral profile to the vendor.

When a new targeted coupon is available, the vendor first encrypts the coupon to produce the coupon ciphertext as generated by the CSP under the user’s public key, an eligible user recovers this key and can extract the coupon encryption key from , via computing . On the other hand, a non-eligible user recovering is not able to correctly extract from , and thus will fail in coupon decryption.

1) The vendor generates a random mask and produces the obscured ciphertext of user’s behavioral profile as based on the homomorphic addition property. Then, the vendor sends to the CSP.

2) Upon receiving , the CSP decrypts it using the secret key skCSP, and obtains the masked user’s behavioral profile as Then, the CSP generates two fresh random values and prepares a garbled circuit which is depicted in Fig. 5. The garbled circuit takes as input the garbled values of the masked user’s behavioral profile , the random mask , the vendor’s targeting profile , the random values and , the coupon encryption key , and the threshold , denoted as , and respectively. Then, the CSP sends the garbled circuit, and the garbled values to the vendor.
The garbled circuit in our proposed design.

3) The vendor runs the oblivious transfer protocol with with CSP to obtain the garbled values $\hat{s}$, $\hat{v}$, $\hat{K}$, and $\hat{\epsilon}$. Then, based on the garbled circuit and the garbled inputs $\hat{u}$, $\hat{s}$, $\hat{v}$, $\hat{R}_0$, $\hat{R}_1$, $\hat{K}$, and $\hat{\epsilon}$, the vendor performs circuit evaluation and obtains the result $\hat{R}_i \oplus \hat{K}$.

4) The CSP further sends encrypted $R_0$ under the user’s public key, i.e., $C_{R_0} = \text{EA}_{pk}(R_0)$, to the vendor.

After the execution of blind eligibility test, the vendor sends the coupon ciphertext $C_M$ along with the ciphertext metadata $\{R_1 \oplus K, C_{R_0}\}$ to the user. If a user is eligible, the ciphertext metadata received by her is $\{R_0 \oplus K, C_{R_0}\}$, and thus she can recover the correct coupon key $K$ for the decryption of the coupon ciphertext. Otherwise, she will obtain $\{R_1 \oplus K, R_0\}$ and is not able to recover the correct coupon key $K$. Note that as before in the basic approach, the validity of a redeemed coupon by the eligible user will be verified by the signature $\sigma$ and the UID of the redeeming user.

C. FURTHER INVESTIGATION ON EFFICIENCY IMPROVEMENT

As analyzed above, the proposed design ensures strong user privacy and vendor protection. Meanwhile, it only requires the user to upload encrypted behavioral profile for the use in the remaining workload of secure behavioral targeting on the vendor side. And the user later just receives the coupon ciphertext along with some small ciphertext metadata. Thus, our proposed design imposes lightweight workload for users equipped with mobile devices. On the vendor side, the vendor performs blind eligibility test for each user against the targeting profile of each coupon, based on the customized garbled circuit design. As the number of users grows large, the performance on the vendor side may not scale well.

To speed up the secure behavioral targeting process on the vendor side, an intuitive idea would be to reduce the number of users whose encrypted behavioral profiles engage in blind eligibility test against the targeting profile. This can be achieved if a pre-processing step can be introduced to efficiently filter a number of non-eligible users. Then, blind eligibility test based on the customized garbled circuit design only needs to be performed over a relatively small candidate set of users. The trade-off here is that the vendor will be aware of the non-eligibility status of those filtered users. If such a trade-off between security and performance is allowed,
we show below how to enable secure and efficient filtering of a number of non-eligible users, before the blind eligibility test is triggered.

Our basic idea is to properly leverage the locality-sensitive hashing (LSH) technique to support secure and efficient similarity test between the user’s behavioral profile and the vendor’s targeting profile. The LSH technique hashes high-dimensional data points in such a way that close data points collide with much higher probability than distant ones [16]. Roughly speaking, two data vectors are very likely to be similar if their LSH values are equal.

Based on the LSH technique, our mechanism design for user filtering is mainly aimed at ensuring that all eligible users are still able to obtain the targeted coupons, while protecting their behavioral profiles and eligibility status against the vendor. To ensure that eligible users will not be filtered out, we may resort to LSH algorithms without false negatives [17], [18]. Meanwhile, due to the inevitable existence of false positives in LSH [10], the vendor is prevented from reliably guessing the eligibility status of a user who is not filtered out and thus resides in the candidate set for blind eligibility test. Next, we describe in detail how to properly leverage LSH for secure and efficient user filtering.

A strawman approach is to let the user send the hash value of her behavioral profile’s LSH value, i.e., \( \text{Hash}(\text{LSH}(u)) \), to the vendor for equality testing. However, this would also enable the vendor to directly do equality testing between the LSH values across different users, and lead to direct similarity leakage. To address this issue, a viable approach is to share a secret key \( k_u \) between the vendor and each user. Then, the user sends \( \text{PRF}(k_u, \text{LSH}(u)) \) to the vendor for equality testing, where \( \text{PRF} \) is a secure pseudorandom function. In this case, the vendor is prevented from directly comparing the LSH values of different users. To further prevent the vendor from directly comparing the LSH values of the behavioral profiles potentially updated by the same user, we can resort to the following enhancement. In particular, we can let the user send \( \{\text{salt}, \text{PRF}(k_u, \text{LSH}(u))||\text{salt}\} \) to the vendor, where \( \text{salt} \) is a randomly-chosen value per update of the behavioral profile. To detect a match of LSH values between \( u \) and \( v \), the vendor first computes \( \text{PRF}(k_u, \text{LSH}(v)||\text{salt}) \), and then tests equality with \( \text{PRF}(k_u, \text{LSH}(u)||\text{salt}) \). As randomness is introduced between each update of the behavioral profile within the same user, the vendor is prevented from directly comparing the LSH values at different update points. Such a mechanism design only requires the vendor to perform the simple operations of LSH hashing, \( \text{PRF} \), and equality testing, which can be efficient for user filtering before the relatively expensive blind eligibility test is initiated.

V. EXPERIMENT

A. IMPLEMENTATION

We implement a preliminary system prototype for our proposed design in Java. Our user-side prototype is deployed on an Android smartphone Samsung Galaxy S4. Our vendor-side/CSP-side prototype is deployed on a desktop PC which is equipped with a two-core 2.7 GHz processor and 8.0 GB RAM. For cryptographic primitives, we use the Paillier library\(^1\) for additively homomorphic encryption, and the RSA-1024 for asymmetric encryption.\(^2\) To prove the concept of our garbled circuit based customized design, we rely on ObliVM-lang [19], the state-of-the-art programming framework for secure multi-party computation, for protocol implementation and performance test. Besides, we set the bit length of the coupon encryption key \( K \) to 128 as in AES-128. Without loss of generality, we use the number \( n \) of dimensions ranging from 10 to 60 as example cases in our experiments, so as to thoroughly evaluate the performance. We remark that such a setting is reasonable and has the same order of magnitude as in prior work [2] and real-world user targeting applications (e.g., Facebook uses 98 personal data points for user targeting [20]).

B. PERFORMANCE EVALUATION

We now investigate the performance overheads at the user, the vendor, and the CSP. Our performance evaluation will be conducted in three aspects: computation, bandwidth, and energy. All the results are averaged over 10 runs.

1) COMPUTATION CONSUMPTION

We first report computation cost at the user, the vendor, and the CSP, respectively.

a: USER SIDE

The computation overheads on the user consist of the generation of an asymmetric key pair, the encryption of her behavioral profile, and the extraction of the coupon key from the ciphertext metadata. Note that we do not report the time required to decrypt a coupon ciphertext, as the operation is standard AES decryption and its time also depends on the coupon size.

Firstly, we measure the key generation time on the user side, which turns out to be 390 msec. Note that this is a one-time cost during system setup. Secondly, Fig. 6 shows the time of encrypting the user’s behavioral profile \( u \), for a varying number of the profile dimensions. As expected, the encryption time linearly grows in the number of profile dimensions. Particularly, when the number of profile dimensions \( u \) varies from 10 to 60, the encryption time ranges from 322.2 msec to 1330.8 msec. Note that the user only needs to encrypt her behavioral profile once even for the delivery of multiple targeted coupons. New encryption of the behavioral profile takes place only when the behavioral profile is updated after a certain time period.

Finally, to extract the coupon decryption key from the ciphertext metadata \( \{R, K, C_{K^\perp}\} \) pushed down by the vendor, the user only needs to perform one operation of

---

\(^1\)http://www.csee.umbc.edu/~kunliu1/research/Paillier.html

\(^2\)Other additively homomorphic encryption schemes and asymmetric encryption schemes may also be used.
RSA decryption and one 128-bit XOR operation. In our test, one RSA decryption operation takes 4.1 msec, while the 128-bit XOR operation only takes $10^{-5}$ msec, which is negligible. Hence, the total time of extracting the coupon decryption key from the ciphertext metadata is only about 4.1 msec, which is also independent of the dimension of the user’s behavioral profile. Overall, our proposed design achieves practical computation performance on the user side.

**b: VENDOR SIDE**

Regarding the vendor side, the computation overhead comes from the process of blind eligibility test. In the blind eligibility test, the vendor needs to generate the random mask, add the encrypted mask to the encrypted user’s behavioral profile, and engage in a garbled circuits based protocol with the CSP.

Firstly, we measure the time of generating one element of the random mask $s$, which turns out to be 0.03 msec. Therefore, the total time of generating the random mask ranges from 0.3 msec to 1.8 msec, when the number of the user’s behavioral profile dimensions varies from 10 to 60. Secondly, the operation of adding one element of the random mask to one encrypted element of the user’s behavioral profile requires one Paillier encryption and one operation of Paillier ciphertext multiplication. In our test, the time taken by one Paillier encryption and one operation of Paillier ciphertext multiplication is 10 msec and 0.004 msec, respectively. Hence, the total time of adding the encrypted random mask to the encrypted user’s behavioral profile is $n \times 10,004$ msec. When $n$ varies from 10 to 60, the total time ranges from 100.04 msec to 600.24 msec. Finally, we measure the time required to perform the garbled circuits based protocol on the vendor side. When $n$ varies from 10 to 60, the time ranges from 88.2 msec to 151.1 msec.

Fig. 7 illustrates the total computation cost of the vendor in the process of blind eligibility test. It can be observed that the computation cost depends on the dimension of the coupon’s targeting profile/user’s behavioral profile. When the profile dimension varies from 10 to 60, the total computation cost of the vendor performing blind eligibility test ranges from 188.54 msec to 753.14 msec.

**2) BANDWIDTH CONSUMPTION**

Bandwidth is a kind of precious resources for mobile devices, especially when they operate in cellular networks [21]. Therefore, we now report the user’s bandwidth cost. Recall that the user first needs to send the encrypted behavioral profile $C_u$ to the vendor, where $C_u$ is an $n$-dimensional vector.
Each element of $C_u$ is a Paillier ciphertext. Therefore, the size of the encrypted behavioral profile is $n \times z$ bytes, where $z$ is the size of one Paillier ciphertext. In our test, $z$ is 256 bytes. When $n$ increases from 10 to 60, the bandwidth consumed by this part ranges from 2.5 KB to 15 KB. When the user receives the coupon ciphertext $C_M$ from the vendor, she also receives some extra ciphertext metadata, i.e., the masked coupon key $R_i \oplus K$ and the encrypted mask $C_{R_0}$. Obviously, the size of $R_i \oplus K$ is 16 bytes, which is equal to the 128-bit coupon key. Regarding $C_{R_0}$, it is actually a RSA ciphertext which consumes 256 bytes in our test. Therefore, the bandwidth overhead of the user for the delivery of each targeted coupon for the user is only 272 bytes.

3) ENERGY CONSUMPTION

Considering that battery energy is one of the most precious resources of mobile devices [22], we also measure the energy cost on the user side in our proposed design. In our energy test, we resort to Power Tutor 2 Pro [23], a diagnostic tool which can be used for the analysis of system and App power usage. We measure the energy cost due to computation and communication, respectively.

We first report the energy cost due to computation on the user side. We note that the energy consumed by the extraction of the coupon encryption key from the ciphertext metadata is negligible, so we focus on the energy consumed by the encryption of the user’s behavioral profile. Fig. 8 shows the energy cost of encrypting the user’s behavioral profile for a varying number of the profile dimensions. It can be observed that the energy consumed by the encryption of a user’s behavioral profile is positively correlated with the number $n$ of profile dimensions. Particularly, when $n$ varies from 10 to 60, the corresponding energy cost grows from 33.2 mJ to 196.5 mJ.

Fig. 9 further shows the energy cost of uploading the encrypted user’s behavioral profile to the vendor, also for a varying number of profile dimensions. It can be observed that the energy consumed by the transmission of user’s encrypted behavioral profile does not fluctuate too much. Particularly, for different values of $n$ (10 $\leq n \leq$ 60), the energy cost fluctuates around 3.7 J.

In order to help readers get a sense of what the above energy cost implies, we provide the amount of energy consumed by playing a 10-minute audio as a reference example. Specifically, it takes about 10 J energy to play a 10-minute audio. Note that for a large value of $n$ ($n = 60$), the total energy taken by the encryption and transmission of user’s behavioral profile is only 4.72 J. Therefore, our proposed design achieves affordable energy cost on the mobile device.

VI. RELATED WORK

Our work provides secure and accurate targeted mobile coupon delivery service via private targeting of user behavior. In the literature, previous work focusing on secure behavioral targeting based applications can be broadly divided into two categories: (i) work on secure targeted ad delivery, and (ii) work on secure targeted coupon delivery. Most existing work falls in the first category. Our work falls in the second category, where little work has been done.

A. SECURE TARGETED AD DELIVERY

A lot of work has been proposed for the delivery of targeted ads to users with the preservation of user privacy (e.g., [24]–[27], to list a few). In [24], Toubiana et al. propose Adnostic, which executes behavioral targeting on the user side. In particular, the ad-network in Adnostic sends a few randomly chosen ads to the user’s device, which then selects the ads most relevant to the user’s behavioral profile for display. They also propose a private billing scheme based on homomorphic encryption and zero-knowledge proof, enabling the ad-network to charge advertisers correctly without learning the ad view history of a particular user. In [25], Guha et al. propose Privad, which achieves user privacy mainly through anonymization based approach. In particular, they introduce a third party between the ad-network and users, so as to anonymize users’ click/view behavior against the ad-network, while still supporting billing based on the resultant click/view report. Backes et al. propose ObliviAd [26], which relies on secure hardware (i.e., secure processor) deployed at the ad-network to support oblivious targeted ad delivery. A very recent work by Jiang et al. [27]
leverages the technique of private stream searching (PSS) to enable users to retrieve targeted ads that match their behavioral profiles, without disclosing personal behavior information.

Most of existing work on secure targeted ad delivery only considers user privacy. These techniques are not directly applicable to address more challenging security requirements in targeted coupon delivery, where both user privacy and vendor protection should be considered [2], [3].

B. SECURE TARGETED COUPON DELIVERY

Little work has been done for secure targeted coupon delivery. Prior work either exposes targeted coupons to a portion of non-eligible users, or suffers from information leakage of the vendor’s targeting profile. In [2], Partridge et al. propose PiCoDa, which performs behavioral targeting on the user side. They leverage the LSH technique to test whether the user’s behavioral profile approximately matches the vendor’s targeting profile. Specifically, users can obtain the key for coupon decryption, if their behavioral profiles have the LSH value matched with that of the vendor’s targeting profile. Due to the existence of false positives in LSH, their design would expose the coupons to a portion of non-eligible users, which might violate the vendor’s interests. Similar to [2], Rane and Uzun [3] also performs behavioral targeting on the user device. However, they adopt a different solution which applies error-correcting codes to the encoding of the user’s behavioral profile and the vendor’s targeting profile. Despite being free of the problem of false-positives, their design reveals some information about the vendor’s targeting profile.

Different from prior work, our proposed design properly bridges together the techniques of homomorphic encryption, random masking, and garbled circuits, ensuring that targeted coupons are accurately delivered to eligible users only, while achieving user privacy and vendor protection. In a word, our proposed design achieves the security strengths that prior studies do not afford.

There are some other work combining homomorphic encryption and garbled circuits for applications like secure biometric identification [28]–[30], secure ridge regression [7], and secure in-network near-duplicate detection [10]. Their target problems are considerably different from secure and accurate targeted mobile coupon delivery that we study.

VII. CONCLUSION AND FUTURE WORK

We studied the problem of secure and accurate targeted mobile coupon delivery. Our research is aimed at enabling the delivery of targeted coupons to eligible users whose behavioral profiles accurately satisfy the targeting profile defined by the vendor, while preserving user privacy and providing vendor protection. We first showed a basic approach which is built on the proper usage of garbled circuits. It satisfies the stringent security requirements of secure and accurate targeted coupon delivery, yet suffers from the cost efficiency issue for users equipped with mobile devices. We then proposed a design which securely shifts most workload of private behavioral targeting to the vendor side, without sacrificing the security guarantees. We implemented a preliminary system prototype for our proposed design, and conducted thorough experiments for performance evaluation. The results demonstrated that our proposed design can achieve practical performance for mobile devices.

One interesting future work is to extend our proposed design under different security models, e.g., malicious users and malicious CSP. Malicious users might attempt to collect coupons in an illegitimate manner by faking the behavioral data. Such a threat can be handled via a set of orthogonal approaches such as trusted computing technology and data commitments [2]. A malicious CSP can corrupt the computation in two ways: it may provide a garbled circuit for the wrong function and may incorrectly perform decryption over the homomorphic ciphertexts received from the vendor. The former issue can be handled via standard techniques for verifying garbled circuits [31], [32]. The latter issue can be handled via standard techniques which require the CSP to prove in zero knowledge to the vendor that homomorphic decryption was done correctly.

ACKNOWLEDGEMENTS

Jinghua Jiang and Yifeng Zheng contributed equally to this work.

REFERENCES


XINGLIANG YUAN received the B.E. degree from the Nanjing University of Posts and Telecommunications, Nanjing, China, in 2008, the M.S. degree from the Illinois Institute of Technology, Chicago, IL, USA, in 2009, and the Ph.D. degree from the City University of Hong Kong, Hong Kong, in 2016. He is currently a Research Fellow with the Department of Computer Science, City University of Hong Kong. His research interests include cloud computing security, mobile security, and multimedia security.

ZHENKUI SHI received the B.E. degree from the Southwest University of Science and Technology, Mianyang, China, in 2007, and the M.S. degree from the University of Electronic Science and Technology of China, Chengdu, China, in 2010. He is currently pursuing the Ph.D. degree with the Department of Computer Science, City University of Hong Kong, Hong Kong. His research interests include network security, mobile privacy and security, and targeted advertising.

XIAOLIN GUI received the B.E., M.E., and Ph.D. degrees from Xi’an Jiaotong University, Xi’an, China, in 1988, 1993, and 2001, respectively. He is currently a Professor and the Deputy Dean with the School of Electronic and Information Engineering, Xi’an Jiaotong University. His research interests include secure computation in open network systems, data privacy, and the Internet of Things.

CONG WANG received the B.E. and M.E. degrees in electrical and computer engineering from Wuhan University, Wuhan, China, in 2004 and 2007, respectively, and the Ph.D. degree in electrical and computer engineering from the Illinois Institute of Technology, Chicago, IL, USA, in 2012. He was with the Palo Alto Research Center in 2011. He is currently an Assistant Professor with the Department of Computer Science, City University of Hong Kong, Hong Kong. His current research interests include on cloud computing security.

JING YAO received the B.E. degree from Shaanxi Normal University, Xi’an, China, in 2009 and 2012, respectively. She is currently pursuing the Ph.D. degree with the School of Electronic and Information Engineering, Xi’an Jiaotong University, and with the Department of Computer Science, City University of Hong Kong, Hong Kong. Her research interests include cloud computing security, outsourcing storage security, and data privacy.

JINGHUA JIANG received the B.E. degree from Xi’an Jiaotong University, Xi’an, China, in 2010. He is currently pursuing the Ph.D. degrees with the School of Electronic and Information Engineering, Xi’an Jiaotong University, and with the Department of Computer Science, City University of Hong Kong, Hong Kong. His research interests include cloud computing security, multimedia security, mobile security, and targeted advertising.

YIFENG ZHENG received the B.E. degree in information engineering from the South China University of Technology, Guangzhou, China. From September to December 2013, he studied at Zhejiang University, Hangzhou, China. He is currently pursuing the Ph.D. degree with the Department of Computer Science, City University of Hong Kong, Hong Kong. His research interests include cloud computing security and multimedia security.