International Journal of Business Quantitative Economics and Applied Management Research
Volume-6, Issue-8, 2020 ISSN No: 2349-5677

USE OF MULTIPARTY COMPUTATION FOR MEASUREMENT OF AD PERFORMANCE WITHOUT EXCHANGE OF PERSONALLY IDENTIFIABLE INFORMATION (PII)

Varun Chivukula
University of California, Berkeley
Varunvenkatesh88@berkeley.edu

Abstract

The digital advertising ecosystem, particularly in auction-based platforms using real-time bidding (RTB), increasingly relies on large-scale data collection for performance measurement. Traditionally, this data exchange involves the use of personally identifiable information (PII), which raises significant privacy concerns. This paper explores the potential for applying multiparty computation (MPC) to evaluate user-based randomized control trials (RCTs) for ad performance measurement in a manner that ensures privacy preservation by not exchanging PII. We investigate how MPC can facilitate collaborative analysis among multiple stakeholders in the advertising ecosystem—advertisers, demand-side platforms (DSPs), supply-side platforms (SSPs), and publishers—while maintaining user confidentiality. Additionally, the paper delves into the specific challenges, benefits, and practical applications of MPC in this context, providing insight into how privacy-preserving methods can enhance the efficacy of A/B testing and other experimental ad measurement methodologies [1][2].

Keywords: Privacy-enhancing technologies, causal inference, digital ad platforms, auction-based RTBs, data encryption, randomized control trials (key words)

I. INTRODUCTION

The growing complexity of digital advertising platforms, especially those using auction-based models like real-time bidding (RTB), has brought significant advancements in ad targeting and performance measurement [3][4]. These platforms operate through a variety of interconnected entities—advertisers, DSPs, SSPs, publishers, and ad exchanges—all of which collect and exchange large amounts of data to optimize ad delivery. This data often includes PII used to assess ad performance and adjust bidding strategies based on user behaviours, demographics, and interests [5].

RCTs, considered the gold standard in experimental design, are widely employed in digital advertising to assess the causal impact of ad exposure on user behavior, such as conversions and purchases [6]. However, the reliance on PII raises significant privacy concerns, especially with stringent regulations like the GDPR and CCPA. Multiparty computation (MPC), a cryptographic

technique enabling multiple parties to compute functions over private data without revealing individual inputs, offers a promising solution [7][8].

II. AUCTION-BASED DIGITAL ADVERTISING AND RCTS

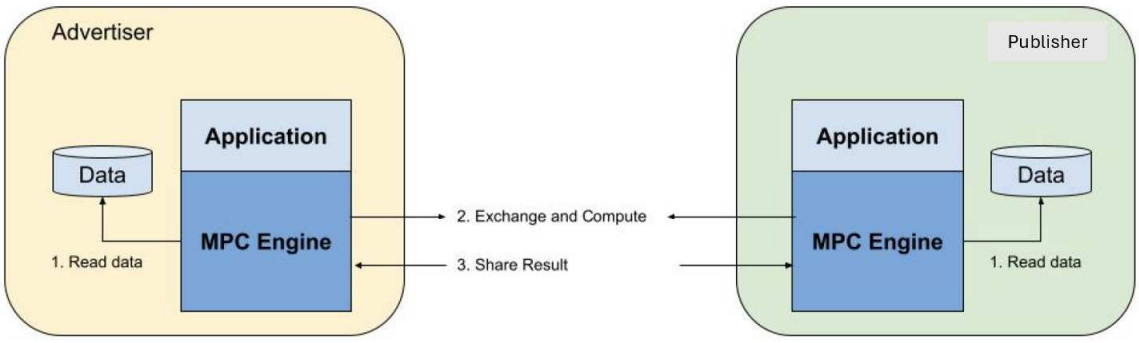
In RTB systems, advertisers bid on ad impressions in real time based on user-specific information such as browsing history and demographic data [9]. RCTs are used to evaluate the impact of different ad strategies by randomly assigning users to treatment or control groups [10]. For example, treatment groups may view a specific ad creative, while control groups receive a generic ad. Accurate performance measurement, such as click-through rates and conversions, often require aggregating data across stakeholders without compromising user privacy [11].

Typically, the results of RCTs are aggregated across various participants in the ecosystem—advertisers, DSPs, and publishers—all of whom have different pieces of user-level data. The ability to measure ad performance while maintaining the confidentiality of users' personal data is crucial for ensuring compliance with privacy laws and maintaining consumer trust.

III. MULTIPARTY COMPUTATION AND PRIVACY-PRESERVING RCTS

MPC enables collaborative computation over private data without exposing individual inputs [12]. Techniques such as secret sharing and homomorphic encryption allow stakeholders to securely evaluate RCTs without exchanging PII [13][14]. For example, advertisers can measure conversion rates by securely aggregating impression and click data from DSPs and publishers [15]

Multiparty computation (MPC) allows multiple parties to collaboratively compute a function over their private data without revealing the individual inputs of each party. This makes MPC particularly suitable for contexts like digital advertising, where multiple stakeholders need to share results without exposing sensitive user information. Illustrative schematic below



Key techniques used in MPC include:

- **Secret Sharing**: In secret sharing, data is split into multiple "shares," which are distributed to different parties. Each party holds a share of the data and cannot reconstruct the original

information. Through coordinated computations, the parties can compute the desired function on the data without revealing individual inputs.

- **Homomorphic Encryption**: This allows computations to be carried out on encrypted data, producing encrypted results that can be decrypted only by an authorized party. Homomorphic encryption preserves privacy because the data is never exposed in an unencrypted form during the computation process.
- **Secure Multi-party Summation:** Secure summation protocols allow the aggregation of data, such as impressions or conversion rates, across different parties without revealing the individual contributions of each party.

By using MPC, ad platforms can evaluate user-based RCTs on a larger scale, performing operations like comparing treatment and control group outcomes (e.g., clicks, conversions) without the need to exchange PII.

Here is an illustration of such a computation for scenario where A and B hold value where each want to know whether their values are greater than the other without sharing their own value
In this abstract, we focus on a single solution to the problem of comparing two private values while preserving privacy. Assume:

- A holds i
- B holds j
- Both values satisfy $1<i , j<10$

The goal is to design a protocol that determines whether $i<j$ ensuring this is the only information exchanged (aside from each party knowing their own value).

Define:

- M: the set of all N-bit nonnegative integers.
- QN: the set of all bijections (1-1 and onto functions) from M to M.
- Ea: A's public key, generated by selecting a random element from QN .

The protocol proceeds as follows:

1. **Initialization by B**
   - B selects a random N-bit integer x and computes k=Ea(x).
2. **B Sends a Value to A**
   - B sends k−j+1 to A.
3. **A's Computations**
   - A computes: yu=Da(k−j+u),for u=1,2,…,10, Where Da is the decryption function corresponding to Ea
4. **Prime Generation and Modular Reduction by A**
   - A generates a random prime p with N/2-bit size.
   - Computes: zu=yu mod p,for all u
   - Checks if all zu differ by at least 2 modulo p.
   - If not, generate a new p and repeats until the condition is satisfied

5. **A Sends Results to B**
   - A sends B:
     - The prime p.
     - Numbers: z1,z2,…,zi,zi+1,zi+1+1,…,z10+1interpreted modulo p.
6. **B Determines the Relationship**
   - B inspects the j-th number (not counting p) in the list received from A.
   - Decides:
     - i⩾j if the number equals x mod p
     - i<j otherwise.
7. **B Communicates the Result**
   - B informs A whether i<j or i⩾j.

IV. MPC FOR EVALUATING USER-BASED RCTS IN AUCTION-BASED AD PLATFORMS

In auction-based digital advertising platforms, multiple stakeholders (e.g., advertisers, DSPs, SSPs, and publishers) need to evaluate the performance of ads, often via randomized experiments. By utilizing MPC, the participants in a randomized control trial can collaborate to evaluate the effectiveness of different ad exposures (e.g., ad creatives, targeting strategies) while ensuring that individual user data remains private.

1. Secure Randomization and Assignment to Treatment Groups

One of the first steps in conducting an RCT is the randomization of users into treatment and control groups. Traditionally, this randomization process may involve the sharing of user-level information (e.g., which users are assigned to which group). Using MPC, the randomization process can occur securely, where the assignment of users to groups is conducted in such a way that no party learns any individual's group assignment.

For example, using secret sharing, each participant in the ad ecosystem can contribute to a randomized decision process without revealing user identifiers. The outcome of this randomization (i.e., which users are assigned to treatment vs. control groups) is kept private until the analysis phase.

2. Measurement of Ad Performance Metrics Without PII Exchange

Once the users are assigned to treatment and control groups, ad performance metrics (e.g., CTR, conversions, ROAS) must be measured across both groups. MPC enables this process by allowing multiple parties to contribute their data to an aggregated calculation without revealing individual-level data.

For instance, an ad exchange may measure the number of impressions shown to users, while a DSP measures clicks, and a publisher tracks conversions. Using MPC protocols, each party can securely contribute to the aggregated performance statistics—such as the overall number of conversions in the treatment and control groups—without any participant gaining access to the others' user-level data.

3. Causal Inference and Statistical Analysis Without PII

After collecting the relevant data from treatment and control groups, causal inference techniques (e.g., comparing conversion rates) can be applied to assess the effectiveness of the ad strategy. MPC allows for secure, collaborative computation of these statistics without the exchange of PII. By applying cryptographic methods, participants can jointly calculate differences in conversion rates between groups or perform A/B testing analyses while keeping user-level information encrypted.

The result is a robust analysis of ad performance, including statistical tests of significance, that respects user privacy while still providing actionable insights.

V. CHALLENGES AND LIMITATIONS

While MPC offers a promising solution, it faces several challenges:

- **Computational Complexity**: MPC protocols are resource-intensive and may delay real-time ad performance evaluation [16][17].
- **Scalability:** As the number of stakeholders grows, coordinating secure computations becomes increasingly difficult [18].
- **Data Compatibility:** Variations in data storage formats across stakeholders may hinder interoperability [19].

VI. CONCLUSION

MPC provides a powerful tool for evaluating RCTs in auction-based digital advertising platforms without exposing PII. Despite challenges like computational complexity and scalability, it holds significant potential for enabling privacy-preserving collaboration among advertisers, DSPs, and publishers. Future research should focus on optimizing MPC protocols and validating their efficacy through empirical studies across industries such as healthcare, finance, and digital marketing [20][21].

REFERENCES

1. Andrew C. Yao, “Protocols for Secure Computations (Extended Abstract).”
2. Shamir, A., Rivest, R., Adleman, L., “Mental Poker.” Technical Report LCS/TR-125, MIT, April 1979.
3. David Chaum, Ivan Damgård, Jeroen van de Graaf, “Multiparty Computations Ensuring Privacy of Each Party's Input and Correctness of the Result.”
4. Ben-Or, M., Goldwasser, S., Wigderson, A., “Completeness of Secure Two-Party Protocols.”
5. Gentry, C., “A Fully Homomorphic Encryption Scheme.”
6. Hardt, M., Papadimitriou, C., “Privacy-Preserving Ad Targeting: A Review.”
7. Jarecki, S., Shmatikov, V., “Secure Computations on Outsourced Data.”
8. David Evans, Vladimir Kolesnikov, Mike Rosulek, “A Pragmatic Introduction to Secure Multiparty Computation.”

9. Tadelis, S., "The Economics of Digital Advertising."
10. LeFevre, K., et al., "Scalable Secure Computation Protocols for Privacy-Preserving Analysis."
11. Fung, B., et al., "Data Anonymization for Privacy-Preserving Data Sharing."
12. Zhang, L., & Zhang, X., "Efficient Algorithms for Privacy-Preserving Data Analysis."
13. Chaudhuri, K., et al., "Cryptographic Approaches to Big Data Privacy."
14. Papadimitriou, C., et al., "The Future of Privacy in Online Advertising."
15. Hardt, M., et al., "Practical Approaches to Privacy-Preserving Computation."
16. Zhang, X., "Scaling Secure Computations for Digital Advertising Platforms."
17. Gentry, C., "Efficiency in Homomorphic Encryption for Practical Applications."
18. Papadimitriou, C., "Coordinating Privacy in Distributed Systems."
19. Evans, D., "Interoperable Cryptographic Protocols for Big Data."
20. Shmatikov, V., "Advancing Privacy in Programmatic Advertising."
21. Goldwasser, S., "Applications of Cryptography in Ad Tech."