Imperial College
London

IMPERIAL COLLEGE LONDON

DEPARTMENT OF COMPUTING

Cookieless future in attribution modelling

Analysis on the Interoperable Private Attribution attack space

and development of a technical prototype

Author:

Antonius Strauch

Supervisor:

Yves-Alexandre de Montjoye

Submitted in partial fulfillment of the requirements for the MSc degree

in Computing of Imperial College London

August 2022

Abstract

It is undoubtedly that online advertising has a place on the Internet, helping to finance various free-of-charge services. However, the underlying mechanisms for web tracking of users and performance measurement of advertising allow for the high vulnerability of privacy. Therefore, discussions are increasingly focused on how online advertising can work in a privacy-preserving manner. This report looks at three proposals for possible attribution systems from Apple, Google, and Meta/Mozilla designed to avoid third-party cookies. First, a summary of the current state of knowledge about proposal development and the main differences in the technical design choices. The focus is put on privacy and utility considerations regarding the protocols. Herewith the main differences in the protocols are worked out. For example, Apple proposes a very privacy-oriented but functionally one-sided concept. In contrast, Google's and Meta/Mozilla's protocols provide increased utility to the industry but remain with debatable design choices harming privacy and security. Second, an analysis of the IPA's attack space reveals a potential security threat to the protocol, which enables a malicious server within the MPC to leak sensitive user data. This way, the intended privacy preservation of the protocol can be bypassed. Lastly, the first functioning prototype of the IPA proposal is developed to facilitate future discussions on the concept by providing the full source code of the protocol's logic and and demonstration environment.

Remark

On August 12th, 2022, Ben Savage, software engineer at Meta, announced a new update on the Interoperable Private Attribution (IPA) proposal for cookieless. Compared to the former proposal, directional changes to the system architecture are proposed. With it comes a simplified research prototype for performance testing of the multi-party computing architecture. We strongly support the update as it positively contributes to the discussion and brings clarity. Moreover, we value the areas of improvement as they reflect the concerns we raise in this report:

- **Attribution request** - Adtechs could flexibly formulate precise attribution queries using the event's metadata, which subverted privacy partially. The update defines breakdown keys, which are set with the event registry limiting the adtech's flexibility.

- **Differential privacy and privacy budgeting** - the implementation of differential privacy lacked a precise definition. The update details the concept. Every attribution request will be differentially private utilising (1) noise applied to the result by breakdown key and (2) a maximum contribution of a single match key per request.

- **MPC architecture** - the MPC's architecture was not clearly defined leading security threats. The update provides an improved concept removing the leader server from MPC and explaining the helper server's algorithm for processing shared secrets.

- **MPC threat model** - previously the threat model was honest-but-curious meaning that every party must be trusted to adhere to the protocol. The new update provides an improved threat model so that no single malicious party could leak information.

Overall, the new update validates our work and its relevancy for the current discussion. However, this report is based on the IPA proposal published on January 5th, 2022 including discussions thereafter. The same is true for the developed prototype. We feel confident, that our work still contributes with an overview on the cookieless attribution discussion and a fully functional IPA prototype, which could easily be updated given the applied clean architecture. Furthermore, we offer an approach to analyzing the IPA attack space. Lastly, all information on Apple's and Google's protocols is based on the latest available updates at the time of the report's submission.

Acknowledgement

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Almost 63% of the global population uses the Internet today, which has grown even more significantly due to covid-19 [4]. Free-to-use online services such as google.com and facebook.com remain one of the driving forces for mass adoption since there are no direct costs for the user. Nevertheless, the user still has indirect costs by passing on his or her private data, which advertisers can use for profiling and targeted advertising. Accordingly, there is an increasing public discourse on user privacy in the face of tracking and the collection and storage of sensitive data by advertising companies [5, 6, 7]. In the past, this discourse focused on creating transparency about tracking mechanisms and discussing possible defence mechanisms. More and more, new regulations (e.g., GDPR) have protected the right to one's data resulting in 71% of all countries having any data protection and privacy legislation [8]. The impact has also been considered and evaluated in research. However, the optimal approach to protect user privacy while not harming the ad industry is missing. Therefore, new tracking mechanisms are constantly being brought to the fore to achieve privacy preservation in online advertising.

Online marketing remains one of the critical revenue streams on the Internet [9]. Google, Facebook and independent ad exchanges and networks connect advertisers and publishers to work together to sell products online. Attribution modelling is a field in online advertisement focusing on performance measurement and user journey tracking. Commonly, multiple events map the user journey on the Internet including the interaction with advertisement (i.e., source events) and the conversion (i.e., trigger event), e.g., product purchase. The technological challenge in this process is to track a user correctly to be able

to attribute relevant source events to the actual trigger event. Currently, the collected data in this process facilitate user profiling due to cross-site information and transparent user behaviour.

Due to increasing pressure from regulators and the interest in an industry-compatible solution, Apple, Google and Meta/Mozilla have each presented a proposal to remedy the situation. The main focus is to avoid third-party cookies in tracking and reduce the amount of information about an individual user to prevent profiling altogether. In this context, different attribution systems are proposed, which differ in their architecture and technical modification, thus causing different privacy and utility considerations. This project aims to contribute to current research and these new developments in three ways: First, the project provides a summary of the three proposals to bring transparency to the industry's intend for a cookieless future. Here we compare the proposals key design choices and discuss privacy and utility considerations. Second, we analyze the attack space of the Meta/Mozilla proposal and identify a potential security risk in the system. Third, the project presents a running technical prototype of the Meta/Mozilla protocol for demonstration and increased understanding on the mode of operation and technical design. The focus is put on the Meta/Mozilla proposal as it is the most recent addition to the discussion and incorporates feedback based on the work of Apple's and Google's work. In general, this work is intended to provide a foundation for understanding cookieless attribution systems and to enable further research on them.

Chapter 2

Background

2.1 Literature Review

The following chapter provides an overview of web tracking and data privacy research. For this purpose, the focus is primarily on the period of the last ten years in order to describe the relevant research and development in the immediate vicinity. We have derived four major research trends, which also provide chronological representation of the development of the content of this topic. These trends demonstrate how the focus in research arose and shifted to respond to growing concerns.

2.1.1 Transparency on tracking techniques and stakeholders' roles

Research from 2012 onwards mainly focused on raising awareness of the potential data privacy issue of web tracking. The aim was to create transparency about current tracking mechanisms and to shed light on the actors in the industry. Mayer and Mitchell [10] researched third-party tracking technologies such as third-party cookies[1], fingerprinting[2], and supercookies[3] and the price users pay to use free online content and highlighted the conflicting areas of tracking efforts with the prevailing regulation. They also provided a summary of the current user's control mechanisms (e.g., opt-out cookies, blocking), concluding that it is seen as somewhat problematic to bypass tracking as a non-advanced internet user. Further research [11, 12, 13] added more detailed explanations and large-

---

[1]Type of identifier (i.e., any data) stored in your client from a different domain then the visited website.

[2]Client-specific identity based on software and hardware configurations, which can be read out in communication with a web server.

[3]Commonly locally stored and persistent tracking identifier.

scale studies on fingerprinting techniques and implications on browser regulations and data privacy protection at this time. Takano et al. [14] designed and implemented a third-party tracking visualizer to raise awareness regarding web tracking. They concluded that a tool for web tracking visualization helps to increase how users perceive the invasion of privacy. In contrast, Agarwal et al. [15] argued that users are more concerned by misplaced or suggestive advertisements than the potential threat of being tracked on the internet. Hamed and Ayed [16] furthermore developed a privacy scoring model as a Firefox add-on to evaluate the user's privacy risk and the associated trackers while browsing the web. In testing their add-on, they provided insight into the correlation between user's behaviour and tracking. They identified the risk of omnipresent trackers (e.g. Facebook), which have multiple touchpoints with the user and can link the behaviour back to personal data from social media channels. Martin [1] offered a different perspective on the research field, providing regulators with insight into the stakeholders of web tracking and assessing their relative responsibility to respect user privacy [Figure 2.1]. She further categorized the actors in terms of data depth and relationship to the end user and sees ad networks as a problem for potential surveillance actors [Figure 2.2].
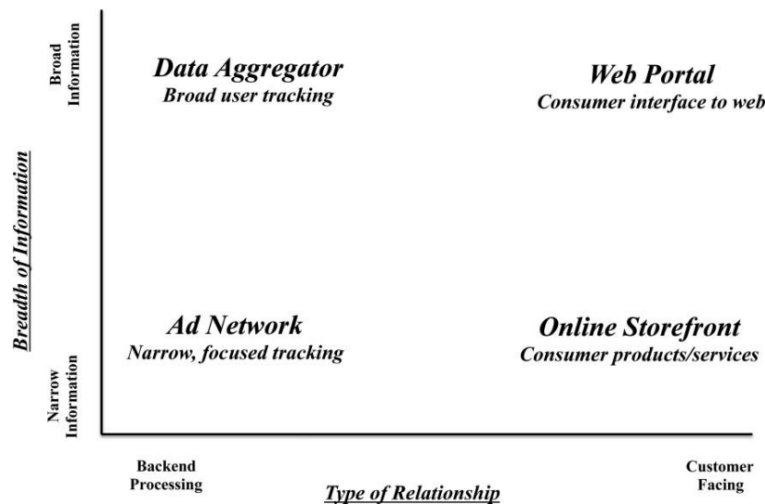
Figure 2.1: Categorizing actors online by the breadth of information and relationship with users [1].

She concludes that client-facing web portals and associated data aggregators are mainly responsible for any law enforcement for privacy regulation, while the actual knowledge creation and risk of user profiles is with the ad networks. Gill, Erramilli et al. [17]
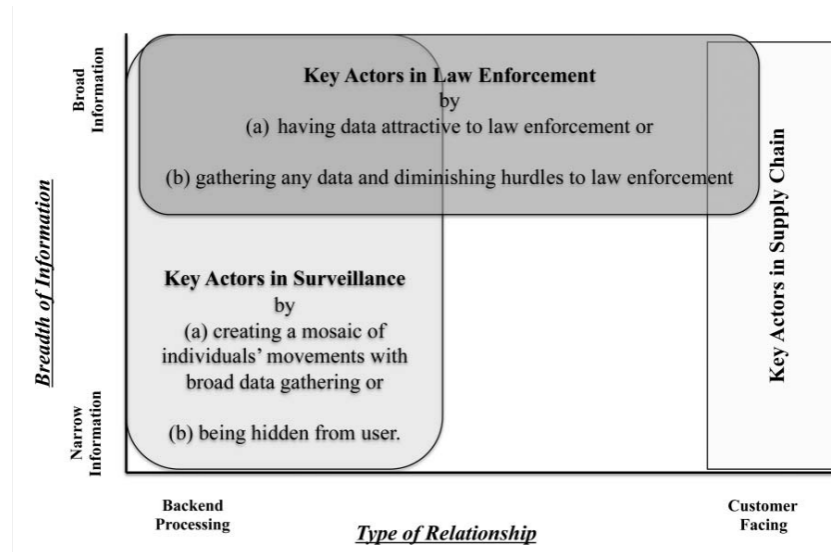
Figure 2.2: Roles and obligations online by type of online tracking actor
[1].

investigated data collection and its economics, concluding that it is critical that most of
the revenue is with a limited number of advertising stakeholders but also pointed out that
this revenue is generated and split across many users.

2.1.2 Detection and defense against web tracking

Once the scientific foundation regarding tracking techniques and dynamics was estab-
lished, the focus shifted to recognizing tracking from the user's perspective and effectively
defending against it. With their paper, Castell-Uroz et al. [18] provided a tutorial on
detecting web tracking via network measurements using a new open-source large-scale
framework. In the experiment, the tool scraped contents of the 100,000 most popular
websites based on Alexa's list, concluding that 28% of the websites had no third-party-
tracking mechanisms incorporated. In contrast, the remainder included one or more track-
ing resources. Furthermore, they only found a few tracking resources within the top 100
websites (e.g., www.google.de), given that these websites operate first-party-tracking. Yu,
Macbeth, et al. [19] designed and tested a browser extension where users collectively
identify sensitive data transfers to third-party domains, which are then blocked. They
proposed this approach as an alternative to the prevailing technique of blocklists, as they
argued that those have limited coverage, especially when new trackers appear and hence
would require high manual maintenance. Cozza, Guarino, et al. [20] designed and im-

plemented a prototype for a hybrid approach to blocklist defending. They trained and deployed a machine learning model to automatically categorize functional and malicious JavaScripts and HTTP requests to update a blocklist accordingly. While the prototype still had drawbacks compared to the performance of alternative systems, they showed that the complete software solution would likely provide high usability and efficiency while maintaining the model's accuracy. Le, Fallace et al. [21] provided a detection approach which monitors JavaScript calls by the browser and compares them to the original website code. By doing this, they could bypass efforts of code obfuscation of trackers, which allowed them to discover fingerprinting mechanisms in 10% of the test websites. Building upon their earlier study, Castell-Uroz et al. [7] also published a novel approach to discovering fingerprinting code across domains of the most popular websites and accurately identified a vast amount of new trackers and tracking resources so far unknown to most common blocklists. An large-scale study summarizing the areas of research identified so far was published by Bujlow et al. [13] The work describes a comprehensive overview of all types of tracking, means of detection and their implications on user privacy. Furthermore, the study lists a range of defence tools and techniques and describes their application.

2.1.3 Adaption of regulatory and its impact on web tracking

With growing concern and increasing interest in protecting user privacy [22], two counter-movements emerged to oppose web tracking. Tightening legal regulations on data privacy and a tighter corset of browser/ad blocker requirements increasingly limit online advertising efforts. This sparked academic discourse on the legal limits of online advertisement and analyses of the impact of new regulations on web tracking. Narayanan et al. [23] looked into the risk of large data sets as a thread to re-identify individual users. They concluded the with the need to collect data on users but stressed the importance of privacy-preserving measures for protection. They identified clear directions for developing legal foundations for the privacy-protecting use of data. Narayanan et al. also argued for close cooperation between practitioners and policymakers to increase transparency on risks and innovation in rulemaking. Motivated by the trend of stricter privacy requirements, Budak, Goel et al. [24] investigated the relevance of such threats to retailers and publishers primarily focused on display advertisement. They found that the free publisher services experience increasing pressure if ad revenue would decrease. In contrast, retailers are less

at risk as their traffic is mostly not dependent on display ads. Another study from Samarasinghe and Mannan [25] investigated the impact of new data privacy legislation on a global scale to understand how web tracking was affected differently in different countries. With an open-source web measurement framework and 56 local machines, they analyzed scripts and Cookies from 2050 URLs. They found that the ability for web tracking was influenced by prevailing data privacy regulations, censorship and speed of the internet in a country. Nevertheless, more importantly, they concluded that solid data privacy regulations do not hinder web tracking immensely. In May 2018, the European Union ratified the General Data Protection Regulation, which introduced, among others, user consent on third-party cookies. Since then, research started to look into the impact of this regulation on web tracking behaviour. Jakobi et al. [26] researched the data collected by web trackers compared to the legal requirements and discussed potential structural consequences of adapting to the current law. They concluded that the introduction of GDPR reduced web tracking efforts only a little, as the consent was still relatively opaque to the user. They argue that to protect users and to conform to the law, an agent system, an autonomously acting software to negotiate and consent privacy settings for the user, would be required but lacks current research. Another study from Urban, Tatang et al. [27] analyzed how information sharing between online advertising companies was affected by GDPR using graph analysis on client-side ID synching. They measured a 40% decline in third-party interactions and information sharing when GDPR was introduced but recognized this as a temporary effect only. Also, they concluded that the amount of data collected and the overall tracking efforts did not decrease, keeping the web tracking industry relatively unaffected. Kretschmer et al. [28] conducted a survey on GDPR's impact and found that overall transparency on data processing in web services has increased. They also argued that further improvement is required as services lack most policy's requirements or hide relevant information behind unnecessarily complex consent designs. Kretschmar et al. [28] further stressed the importance of balancing the regulation with its economic impact on the industry to evaluate a policy's effectiveness. Amarasekara et al. [29] summarized a set of data privacy compliant tracking methods given the new legal landscape. The main objective was to help practitioners adjust their tracking implementation as they argued that e-commerce could be negatively affected if further policies ignored industry needs.

2.1.4 Next generation of web tracking and data privacy preservation

Until 2020 research focused on a sound academic basis for web tracking techniques, the discussion on the best possible defence against such techniques and the understanding of the influence of the tightening legal and browser regulatory landscape for increased data privacy. In response to those trends, research started to focus on balancing the increasing privacy demands with the industry's response through new web tracking and data storage techniques. Data aggregators like Google and Baidu announced anonymization of data sets to reduce the link to the individual to comply with data privacy policies. Deusser, Passmann and Strufe [30] analyzed this approach in their paper to understand the effectiveness of generalization of data in order to increase data privacy. They analyzed representative browsing sessions with local analytics data and cross-website tracking. They concluded that current techniques (e.g., data coarsening) result in pseudonymized data only, which allows for re-identification. Hence, no client or web domain information could be stored for effective privacy preservation. Papadogiannakis et al. [6] looked into techniques which did not rely on cookies given the newly introduced GDPR consent, which allows users to refuse the tracking. They found that techniques like first-party ID leaking or synchronizing and fingerprinting are common "no-cookie" techniques. More importantly, they argue that any consent banner introduced by GDPR sets misleading user expectations for higher privacy as those "no-cookie" techniques are applied even before any consent is registered. Chen, Ilia et al. [5] investigated first-party cookies, which are set through a proxy by third-party domains, bypassing browser regulations. They concluded that 98% of Alexa's 10,000 websites implement this technique, which makes many of the prevailing privacy countermeasures (i.e., ad blockers) inadequate for privacy preservation requiring further research to design new tracking defence. Research of Cassel et al. [31] focused on mobile web tracking, which became increasingly important, with more than half of all website visits originating from a mobile device. They conducted a large-scale web measurement study, which analyzed website visits through desktop and mobile to measure the tracking efforts of each visit. They found that mobile and desktop tracking ecosystems are similar, even though mobile website visits received fewer tracking requests overall. Furthermore, they concluded that the same web trackers were active in either of the environments. However, Yang and Yue [32] had slightly different findings. They con-

ducted a similar study and tested 23,000 websites in mobile and desktop environments with their self-developed framework. Their results show that mobile web tracking has slightly different characteristics and 10% of web trackers were mobile-specific. Also, they argued that mobile web tracking could become more severe regarding data privacy as user interaction is more frequent through mobile devices. Hence a more detailed picture of the user's behaviour could be constructed. Further research by Krupp, Hadden and Matthews [33] looked into user tracking through mobile applications. They advocated to open up the focus of research to the mobile operating systems to increase transparency on tracking in this domain. Pestana et al. [34] and Servan-Schreiber et al. [35] further conducted research to develop prototypes on inherently privacy-preserving ad networks balancing increasing data privacy and industry requirements.

In summary, research in data privacy at the intersection of web tracking followed four broad trends over the last decade. The associated research has shaped the today's discourse on privacy in online advertisement. It is apparent that most research still stresses the need for increased privacy standards. Nevertheless, the dialogue more and more includes the perspective of the industry, which might facilitate joint solutions.

2.2   Status quo in attribution modelling

The Internet is populated with various forms of advertisements and product placements, such as display or search advertisements. However, a user commonly does not see the infrastructure behind the advertisement, which coordinates the alignment of advertiser's (i.e., buy-side) and publisher's (i.e., sell-side) interests.

For this communication, different modes of operation exist, spanning from highly partner-driven and manual ad networks (i.e., direct advertisement) to highly automated modes (i.e., programmatic advertising) [36]. Whereas the first enables targeted collaboration between advertisers and publishers the latter implements a bidding process of aggregated ad resources through a single marketplace. For example, affiliate marketing commonly relies on strong partnerships and the people involved, hence is rather direct. Compared to this, display or search advertisement is usually settled through a central platform (e.g., Google AdSense). Attribution modelling in this picture frames the whole advertisement
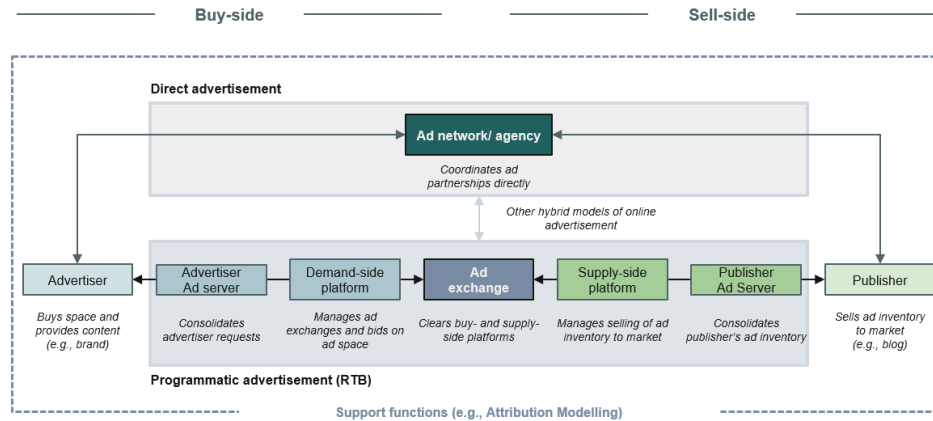
Figure 2.3: Overview on modes of online advertisement and involved stakeholders.

ecosystem and facilitates the process by providing data on the conversion on user journeys. It ensures that successes such as purchases, clicks or registrations can be attributed to a single online marketing channel or publisher and their corresponding advertising space. It furthermore helps to provide a performance-based measurement of the advertisement or performance-based remuneration of a publisher's effort. In essence, with attribution modelling, the marketer tries to understand a user's journey along different events until the user eventually converts to a given product. Interactions with advertisements such as ad view or clicks are referred to as source events. In contrast, conversions such as a purchase or a registration for a platform are referred to as trigger events. The match of two or more corresponding source and trigger events is called the attribution, which provides insight into the ad campaign of a marketer. The correct assignment of relevancy of source events to have led to a trigger event requires a rule- or data-based attribution model [37]. It determines the extent to which one or multiple source events have contributed to the achievement of a trigger event. Rule-based attribution arranges the source events in a predefined relevance, for example, the last click, first click, and time-to-conversion. Data-based attribution considers user behaviour and conversion type and calculates relevance based on additional factors (e.g., product type, product value, the time between interactions). The implementation of attribution modelling requires different tracking mechanisms to constantly re-identify the user across websites. The mechanisms can be characterized along (1) which user data is collected, (2) how it is stored and (3) how it is transmitted in the event of a conversion [10, 13]. First, collected data always has the

purpose of uniquely identifying the user. For this, identifiers (e.g., Click-ID, View-ID) are assigned to the user, or the interaction is uniquely described (e.g., Campaign-ID, Timestamp). Second, this data is usually stored persistently in the browser accessible across sessions. (i.e., cookies, local storage, cache). So each source event creates and stores data according to the underlying definition of the adtechs attribution requirements. Third, when the user converts, this data is transmitted to the advertising network to perform the attribution. It is either done directly in the source code of the conversion page (i.e., client-sided) or transmitted to the network by the advertiser's web server after conversion (i.e., server-side). These characteristics of web tracking (i.e., data, storage, transmission) allow for different tracking forms. Probably the most common form of tracking occurs using third-party cookies, which are set by a partner of the visited website, mostly in the absence of the user's awareness [10]. This way, various information can be added to the cookie (e.g., user's prior page visits), which facilitates interest-based profiling. Due to the far-reaching profiling possibility and vulnerability to privacy, two regulatory directions formed as a counter. First, the legal regulatory tightened the existent frameworks the with laws such as the ePrivacy Directive in 2011 [38], regulating the processing of personal data and protecting privacy, or the GDPR in 2016 [39], regulating the responsibility of obtaining consent to collect and store user data. Second, the browsers themselves began to protect their users from unwanted tracking and targeting. For this purpose, the browsers implemented technical functions to control these mechanisms, such as blocking third-party cookies altogether [40, 41, 42]. In this field of conflicting interests between industry, which aims for a technically feasible solution in attribution modelling and the legal and browser-side requirements, with tightening frameworks for higher data privacy standards comes the idea of cookieless attribution modelling. In essence, it describes an idea which aims to provide a tracking mechanism for attribution modelling without the need for third-party cookies stored in the browser. In addition, the concept aims to be fully privacy-preserving by reducing cross-site information to avoid user profiling.

Chapter 3

Cookieless future in attribution modelling

The proposals discussed in this paper focus on measuring advertisement performance through privacy-preserving attribution modelling. In this context, a system allows matching source and trigger events to track a user's conversion without storing any third-party cookies. Restricting cookies set by parties other than the current website are especially in focus as users likely would not know about their existence and the inherent data stored. By avoiding third-party cookies, privacy preservation is granted by reducing cross-site information of a user not to be able to profile its behaviour. Nevertheless, developing systems that satisfy both the requirements of the advertisement industry and the data privacy needs comes with a trade-off. Systems which endorse privacy by design might potentially lead to a limited utility of that system [43]. Striking the right balance between the usability of data and the need for data protection is currently a challenge for the community. To this end, the three proposals are developed and discussed by developers, representatives of the community and industry under the leadership of the World Wide Web Consortium (i.e., W3C). We discuss the three concepts in the following.

3.1 Overview of proposals

Starting in 2019, Apple, Google, and Facebook have gradually submitted their attribution modelling proposals to the W3C for public discussion [44, 45, 46]. At first glance [Figure 3.1], the companies seem to have different intentions with the proposed protocols if the

scope, attribution level and attribution setup are compared. Apple, not as dependent on advertising revenues and an advocate for data privacy in its software and hardware [47], is developing a straightforward concept with little room for manoeuvre for the advertiser. With PCM, they focus primarily on a clearly defined area of application, which only takes ad clicks as source events and generates event-level reports for web-to-web and app-to-web attribution. They have been the earliest to the market, and a further extension of the concept is expected. Google, with its strong Google Chrome browser with 65% [48] in market share and an extensive ad network focuses on client-sided attribution while simultaneously trying to enable highly flexible advertiser use cases. The joint effort of Meta and Mozilla is a rather unusual alliance [49], with Meta being a highly ad-driven business and Mozilla's privacy-oriented browser. Leveraging large internet footprints (e.g., facebook.com), they propose a server-sided attribution system promising high flexibility for the advertising industry, adaptability of the system and robust data protection measures.
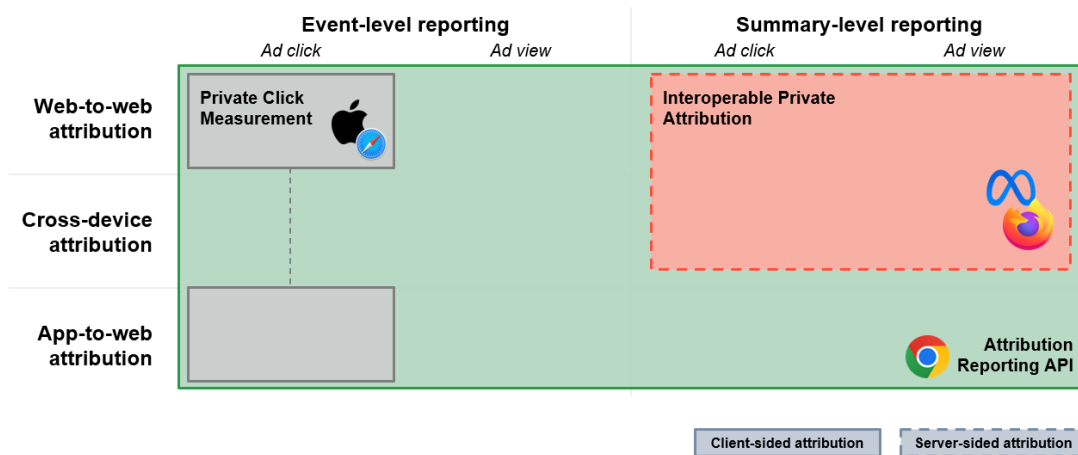
Figure 3.1: Key differences in the technical design of the cookieless attribution proposals from Apple, Google and Meta/Mozilla.

3.2 Mode of operation

In the following, we will provide a brief overview of the proposal's mode of operation. Further technical details are addressed thereafter. In the explanation, five stakeholders play a more or less vital role in the concepts: the client represents the user and its browser, the publisher (e.g., *example.blog.com*) and advertiser (e.g., *example.shop.com*) are the respective source and destination domains of any user navigation based on advertisement

interaction, the adtech (e.g., *example.adtech.com*) represents any ad company (i.e., ad network) commonly facilitating online advertisement efforts for its associated publishers and advertisers, and an external processing environment for data aggregation across clients.

3.2.1   Private Click Measurement (PCM)

In May 2019, Apple was the first to propose a new technology for privacy-preserving attribution modelling through its open-source web engine, WebKit. They also published a testing environment to collect industry and W3C community feedback for improvement. The primary motivation was to prove that ad performance measurement does not require knowledge about the individual but only about the conversion process [50]. With the proposed system architecture, Apple published a simple attribution model centred around the browser in the conversion process in interaction with the publisher and advertiser websites. The adtech has no part in the system, hence cannot easily support any website with attribution modelling directly. The main process is summarised below based on the latest updates to the technology [44, 51, 52]. PCM's scope includes an app-to-web application, which is not described separately but can be treated similarly to the web-to-web solution.
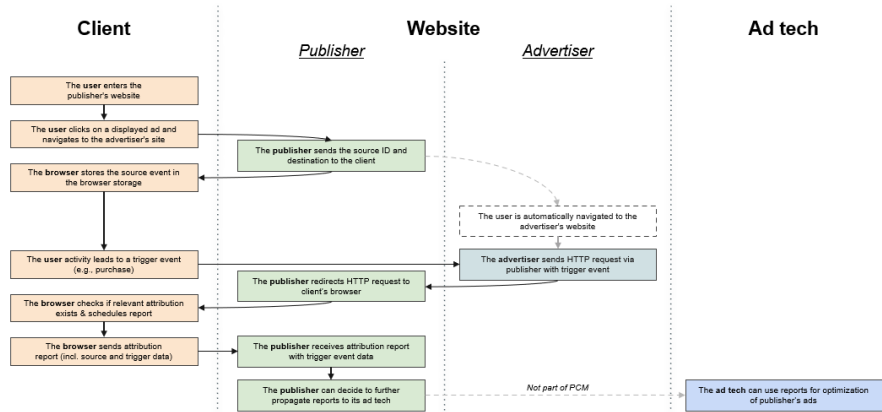
Figure 3.2: Mode of operation of the Private Click Measurement (PCM) proposal by Apple published in May 2019.

Source events are registered when a user enters a website (e.g., *example.blog.com*) and clicks on an ad, which navigates him or her to the corresponding advertiser (e.g., *example.shop.com*). For this, the publisher must modify its web source code to call the PCM

API every time a user interacts with the ad link. The registration of source events based on ad view (i.e., views) is not in the concept's scope. Upon API call, the client creates a source event using the provided information from the website (e.g., destination domain) and stores the event in the browser's cache. The source event's destination and the actual destination from the navigation must match for the source event to be valid. The user then continues searching the internet until converting on (e.g., *example.shop.com*). This interaction results in an HTTP redirect[1] from the advertiser to all associated publishers. This way, the client is notified and registers a trigger event. Every trigger event attempts attribution within the client based on the stored source events. For this, the client tries to match the source events data of the publisher and advertiser's domain with the corresponding trigger data. Suppose a pair of source and trigger events is found. In that case, the client prepares an event-level report by combining the event data and schedules a delayed delivery of the report to the publisher. The publisher can then use the received event-level report for its use cases (e.g., managing campaigns via adtech).

3.2.2   Attribution Reporting API (ARA)

In May 2021, Google Chrome published the Attribution Reporting API, two concepts on event-level and summary-level reporting. It is part of Google's Privacy Sandbox, a collection of proposals to facilitate cross-site ad use cases without requiring third-party cookies [53]. In addition, Google introduced a running test environment to help the community understand the proposal and collect feedback for the development. Furthermore, they submitted two brief proposals for further advancements in app-to-web and cross-device attribution. These are not considered in the following, given their current development status. A brief overview of ARA's mode of operation is explained below based on the latest developments [54, 55, 56].

As with PCM, the user searches the web and interacts with an advertisement on a publisher website (e.g., *example.blog.com*), which has its source code modified for the client's ARA API. When the client loads the code, it sends an HTTP GET request[2] to the specified attribution destination (e.g., *example.adtech.com*), which defines a source event to be

---

[1]HTTP response type redirecting an initial HTTP GET request to a new domain.
[2]HTTP method to fetch data from a web server to the requesting client.

stored within the client. A trigger event is registered if the client, e.g., buys a product on an advertiser's website (e.g., *example.shop.com*). The advertiser notifies the adtech about the conversion, which will return a trigger event to the client's storage. When the trigger event is received, the client attempts attribution. It will compare all source events to the trigger event trying to match the event's adtech (e.g., *example.adtech.com*) and advertiser (e.g., *example.shop.com*).
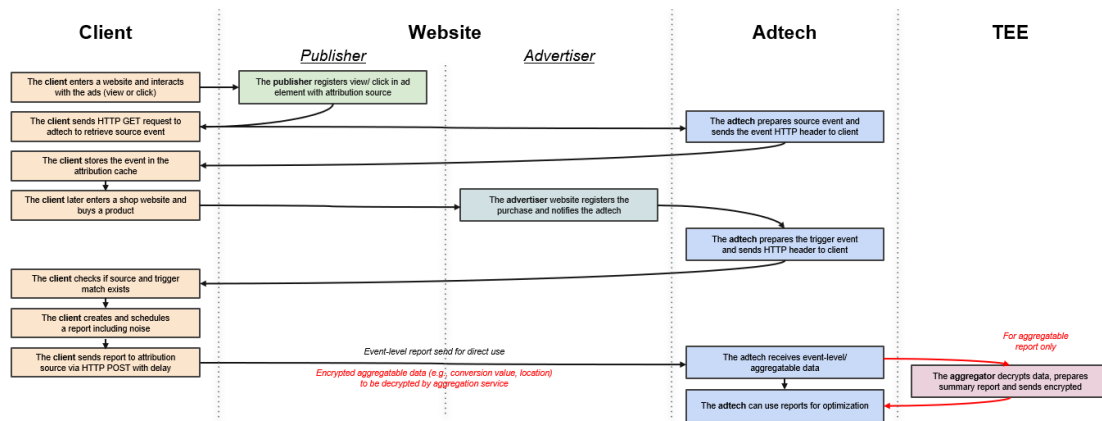
Figure 3.3: Mode of operation of the Attribution Reporting API (ARA) proposal by Google published in May 2021.

Upon attribution, the client merges the source and trigger event information, prepares the event-level report and schedules the send-out. ARA further adds noise and delay to the attribution report, increasing privacy through uncertainty regarding the user's data. The report is then sent to the adtech specified in the event. The summary-level report is created differently as it requires data across clients. With each event registration, the event will require the definition of aggregation keys (e.g., location, product category) in the website's source code. The adtech can use these to add further details to an event, which is then used to cut the data accordingly for aggregation (e.g. preparation of histograms). Upon attribution, the aggregatable information is included in the event-level report. However, the contents of the aggregatable information are encrypted and obfuscated. For the summary-level report, the adtech requests aggregation by sending the event-level reports to an external processing environment. The data is decrypted and aggregated based on the aggregation keys. Further noise is added before send-out back to the adtech.

3.2.3 Interoperable Private Attribution (IPA)

In January 2022, Mozilla and Meta jointly published a draft of the Interoperable Private Attribution proposal for public discourse and feedback [57]. Building on feedback from PCM and ARA, the proposal aims for a privacy-preserving attribution with enhanced industry utility. The key design revolves around two main concepts different from ARA and PCM. First, a central identifier (i.e., match key) is used to identify a client in attribution. Second, an external processing environment for attribution and aggregation[3]. The current draft of the IPA is summarised below based on the latest discussions [57, 46].
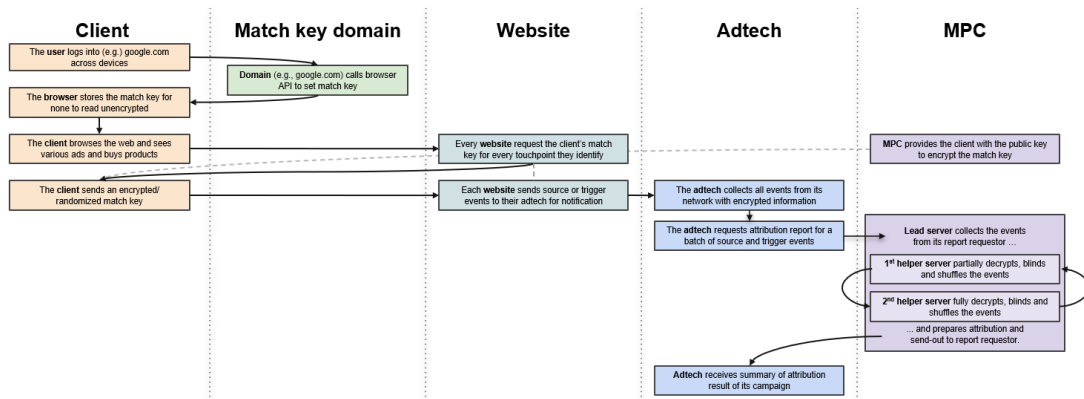
Figure 3.4: Mode of operation of the Interoperable Private Attribution (IPA) proposal by Meta/Mozilla published in January 2022.

The client identifier is provided by any contributing domain, which uses the browser's IPA API to write a match key to the client's storage. This match key is accessible to anyone using IPA; however, only revealed via the read-only browser's API in ciphertext. The client browses the web and interacts with an advertisement on any publisher (e.g., *example.blog.com*) or converts on any advertiser (e.g., *example.shop.com*). Again, the websites must incorporate the required IPA API call in the website's source code to enable event registration. Upon registry, the obfuscated match key is fetched and bundled with the event data. The website stores the event or shares it with any associated adtech (e.g., *example.adtech.com*). This way, the adtech collects source and trigger events across clients, publishers and advertisers. Attribution can be requested by sending a batch of events to

---

[3]Refer to chapter 3 on 'External processing environment' for more information.

the external processing environment. For this, a source query consisting of events from one publisher but several advertisers or a trigger query (vice versa) is created. In the external processing environment, the input data is decrypted to match the source and trigger events based on their match key. Finally, the summary-level report is prepared by aggregating the events (e.g., a sum of purchase values). The report is then sent to the attribution requestor with additional noise added to the result to increase the client's privacy.

3.3 Key design choices

The following will provide a deep dive into the technical specifications of each proposal based on common key design choices. Based on these designs, Apple, Google and Meta/ Mozilla try to ensure that privacy and security requirements are met and a functional attribution is realised. Figure 3.5 provides a summary of the technical details per design element, which are further described.

Key design choices	Description	PCM	ARA	IPA
Client- vs. server-side attribution	Design of the system architecture for the attribution and identification	Client instance as identifier, event attribution based on matching source/ destination domain	Client instance as identifier, event attribution based on matching destination and adtech domain	Match key as identifier, server-side attribution based on event's match key
Coarse event data	Reduction of private data by defining a data structure and limiting the input bits for source and trigger events	Source event with 8-bit source ID Trigger event with 4-bit trigger data (optional: 6-bit priority)	Source event with 64-bit ID and expiry, priority Trigger event with 3-bit (clicks) or 1-bit (view) trigger value	Trigger event with 8-bit conversion value
Event storage	Design of data ownership and duration of data storage in the attribution system	Events are stored with the client locally Data is stored max. 7 days, then automatically deleted	Events are stored with the client locally Data is stored max. 30 days, then automatically deleted	Events are stored with the adtech externally No limitation to data storage duration
Cryptographic protocols	Encryption mechanisms of the system for data-in-transit, storage and use	Encryption of data-in-transit with HTTPS protocol	Encryption of data-in-transit with HTTPS protocol and HPKE encryption of aggregatable data for use in TEE	Encryption of data-in-transit with HTTPS protocol Encryption of data-in-use with homomorphic mechanism to allow for data manipulation in MPC
External processing environment	System architecture for aggregation of event data across clients in the system		Trusted execution environment hung up with adtech in cloud-environment requiring validation of codebase from external auditor	Multi-party computing entity (min. 4 separate servers), which co-process the event data limiting knowledge per server to protect privacy
Differential privacy	Adding uncertainty to the result of the attribution to further reduce re-identifying individual's information		Send out of event-level report with fully randomized trigger value and reporting window given probability p. Further noise added in data aggregation in TEE	Fixed amount of randomized noise added to result summary report
Reporting delay	Reduction of information by delaying the send-out of the report to decouple an event from its registration	Event-level report is delayed by min 24h to 48h or until the browser is running again	Event-level report is delayed by 1h or 2/7/30 days and summary report by max 1h or until client is active again	
Rate limits	Limitation of the systems usage by any party to further reduce data leakages of user's information		100 attributions per <source, adtech, 30days>;. Further limits on reporting origins per <source, destination> per source event and attribution	Privacy Budget per website/ match key limiting number of queries and blocking queries if no budget is left

Figure 3.5: Summary of technical specifications per key design choice of the cookieless attribution modelling protocols PCM, ARA and IPA.

3.3.1 Client- vs. server-side attribution

The primary purpose of the proposals is to replace third-party cookies. However, any means of client identification is required to match the user's interaction with advertisements and the eventual conversion. The type of identifier depends on the decision where attribution is processed. If the attribution is done client-side, within the browser, the client's association with an event must not be transferred. The client itself remains the

identifier. If the attribution is done server-side, the event data is processed externally, where the association to a client is required for attribution.

PCM and ARA run client-side attribution. Hence, the browser has only its events in storage. Trigger events are matched with source events by comparing the event's attribution source (e.g., *example.blog.com* in PCM) and the destination (e.g., *example.shop.com*). The source and trigger event in scope will be attributed if there is a single match. The most recent or the highest priority match is selected if multiple matches exist. A result could be, e.g., *'Source ID 1234 on example.blog.com has led to a purchase on example.shop.com by client ID 9999'*. ARA's summary-level report is processed externally but will have been attributed client-side by this time.

IPA proposes a server-side attribution. For this, Meta/ Mozilla offer to use one or multiple locally stored match keys. Any IPA-contributing domain that can identify a user across devices (e.g., facebook.com) can set a client-specific key upon user identification after login. The match key will then be stored in the client. The corresponding key can be fetched using the client's API by specifying the match key provider (e.g., *facebook.com*). When fetched, the match key is randomised and encrypted[4] before being sent to the adtech. Each repeated API call will reveal a differently randomised key, thus obscuring the user's identity. The event data is sent to the MPC for attribution returning the count of conversions and the sum or average of the provided trigger values. A result could be, e.g., *'In query 15, 4 conversions were attributed with 200 GBP in revenue.'*), which is sent back to the adtech's context.

Privacy and security considerations

The client's data must be anonymised or pseudonymised to reduce the re-identification risk. Anonymized data has no identifier on an entry level, whereas pseudonymised data has an identifier that cannot be linked to a client directly but across data entries. To break anonymisation, one must find significant patterns in the data set that potentially reveal an identity[5]. To break pseudonymisation, one must only find the real identify behind a pseudonym and would then know all related data entries. PCM and ARA propose client-side attribution that creates anonymised event data. The annonymizatio can be bypassed

---

[4]Refer to chapter 3 on 'Cryptographic protocol' for more information.
[5]Refer to chapter 3 on 'Data coarsening' for more information.

by the website, if any identifier is added such as a client's fingerprinting. IPA's match key is a pseudonym, which is obfuscated for publisher, advertiser and adtech but must be revealed in the MPC. Any adversary could try to attack the MPC and would be able to get to the identifiable event data, which creates a privacy risk. Protecting measures are applied to match keys to keep them secure, which will be discussed in the following. Another privacy risk arises from using event-level reports, as in ARA and PCM. Although the information transmitted is coarse[6], the event-level report reveals cross-site details on a single user with another website. For example, the report receiver could learn the publisher and advertiser website in a conversion. This event-level information is not directly linkable with other event-level reports, hence does not readily suffice to build a user profile. However, it opens an attack space for an adversary trying to collect and connects those reports. Further research is required on the potential threat through event-level reports in ARA and PCM.

Utility considerations

All three proposals create a system that inherently solves attribution, taking this task away from adtech. Thus, an adtech theoretically does not need to understand which source event belongs to which conversion. Hence, the client's identity can remain hidden. However, the utility for the industry is limited in all three protocols as the current proposals have a simple approach to attribution modelling in general. The use of last touch attribution is one of the multiple modes to recognise a publisher's contribution to conversion. More sophisticated partnerships (e.g., based on time a client interacts with certain content) between publishers and advertisers could not be applied within any of the protocol's systems.

3.3.2 Data coarsening

Data coarsening or categorical data in a data set helps to limit the entropy of a single entry to anyone observing the data. Effectively information is grouped for a selected attribute to obfuscate the uniqueness of an individual. For example, a particular purchase price might be unique in a data set, whereas a related price range provides less entropy to that user. All protocols coarse the data collected upon event registration by limiting the number of bits allowed, which are allowed in the event objects. Figure 3.6 references an

---

[6]Refer to chapter 3 on 'Data coarsening' for more information.

exemplary JSON dictionary for source and trigger events for each protocol. The names of the variables are standardised for better comparison of the data types but may differ from the original proposals.
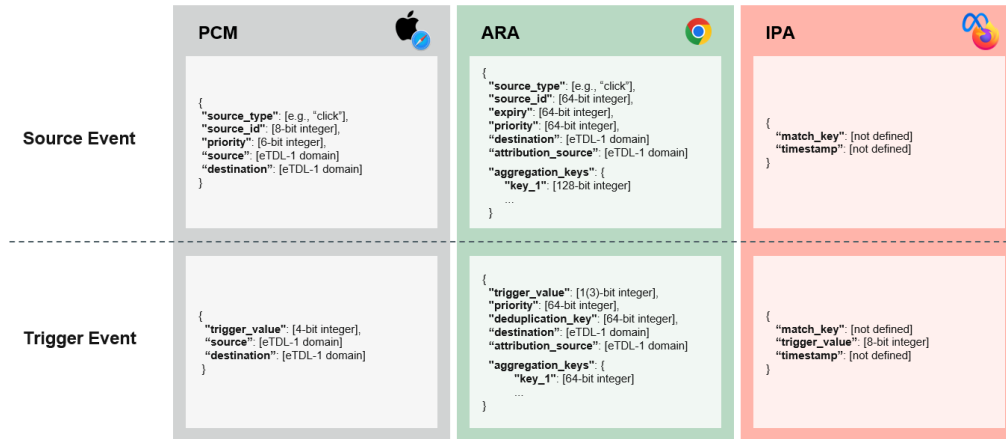

Figure 3.6: Overview on source and trigger event data in an exemplary JSON dictionary per cookieless attribution protocol PCM, ARA and IPA.

PCM proposes a source event consisting of a categorical string (i.e., *source_type*, currently only ad clicks supported), an 8-bit integer referencing a *source_id* and an 8-bit integer referencing *priority* of an event in the attribution. The trigger event comes with a 4-bit *trigger_value* providing additional detail to the conversion. Furthermore, both events come with two eTLD+1 domains[7] for the publisher and advertiser.

ARA defines the source event with a string for *source_type*, 64-bit *source_id*, *priority* and *expiry*. The latter defines the remaining time until the source event loses its validity for attribution. In addition, the trigger event has a 1-bit (ad views) or 3-bit (ad clicks) *trigger_value* and a 64-bit integer as *deduplicate_key* to avoid double-attribution of an event. It also includes two eTLD+1 domains for the advertiser and the adtech (i.e., *destination* and *attribution_source*. Furthermore, ARA's events can include *aggregatable_keys*, which is a collection of categorical keys (e.g., 'geoLocation') and their encrypted values (e.g., UK) for aggregation of events in the summary-level report.

IPA defines the source event with an encrypted *match_key* as identifier and a *timestamp*. One part of the *match_key* is the identifier, and the other part is shared encryption details needed to decrypt the key later. In the report, we use 'match key' as a synonym for the

---

[7]Refers to same-site contexts on an effective top-level domain (eTLD+1). For example, 'example.blog.com' is the eTLD, whereas 'example.blog.com' is the eTLD+1.

identifier only unless stated otherwise. The entropy of the *match_key* is not defined. The trigger event will further add an 8-bit *trigger_value*. Across the protocols, data on *priority*, *expiry* and *deduplicate_key* will only be used in the attribution process and are not shared in the report, hence do not increase entropy in the event data.

Privacy and security considerations

There is a misconception that coarse data will necessarily lead to sufficient anonymisation [30, 58]. Combining multiple attributes might have enough entropy to produce sufficiently precise data in an attribution report. Therefore, the risk could be that sufficiently accurate information about a user can be included leading to re-identification. All protocols limit the data points on a user drastically compared to no limitations using third-party cookies. PCM offers relatively low entropy given the bits associated with a single client through the event data. Per pair of source and destination domain, the source event has an entropy of 2^8 (i.e., *source_id*) and the trigger event an entropy of 2^4 (i.e., *trigger_value*). Hence, both event types seem unlikely to identify a user in a sufficiently large data set. Compared to this, ARA offers a rather high entropy environment. The source event provides entropy of 2^{65} (i.e., 64-bit *source_id* + 1-bit *source_type*) per pair of advertiser and adtech, which might be sufficient to identify a user after attribution. The trigger event is restricted to 2^1 or 2^3 entropy given the *trigger_value*. This is needed as a high-entropy source and trigger event would facilitate cross-site knowledge on a user. *Aggregation_keys* are high entropy data types. However, since this data is encrypted, any entropy should not necessarily be problematic if the aggregation process is secure. IPA only sends summary- instead of event-level reports, hence no exact user data is revealed directly. Furthermore, setting URLs to eTLD+1 domains also coarses potential domains and prevents using targeted URLs for re-identification. Otherwise, specific domains (e.g., *client1.example.blog.com*) could be registered to track individuals directly.

Utility considerations

Commonly in attribution modelling, many different data points on a single user are collected. It helps the advertiser to reliably attribute the user's events, even with unexpected legal and browser regulations or ad blockers. This data is no longer needed if attribution is done via any proposed API. However, the advertiser would also use all the collected

data to detail user and ad campaign insights for performance measurement. The protocols enable a simple ad performance measurement given the provided information. But, for example, the remuneration of a publisher based on generated revenue might already be problematic with the setup of the PCM. For this, the advertiser would require, e.g., the corresponding respective purchase price of a product, which is referenced through a 4-bit *trigger_value*. ARA and IPA make this possible with the summary reports. With a targeted query for a specific publisher or ad campaign, the aggregated revenue for a particular publisher can be obtained. However, this is only one use case of an advertiser. Further research on understanding the advertiser's limitations given coarse data must be conducted.

3.3.3   Event storage

Event storage is relevant as it indicates who controls event data. It is critical to understand the metadata it is stored with and the time the data is kept. Both might further facilitate user profiling. Metadata is all additional data of a session (e.g., conversion). They cannot be stored in the event itself and are therefore not part of an attribution. However, metadata can be stored with the events and are thus conditionally associable.

In PCM, event registration and storage are the responsibility of the browser. The client receives all event data within the website's source code upon event registration for storage. The website cannot add additional metadata to the event as the data is stored internally. The data is kept until it is used for attribution or exceeds a maximum of 7 days. PCM further allows the client to disable attribution tracking fully.

In ARA, the client is responsible for event registration and storage but involves the adtech defined in the website's source code. Thereby, the adtech defines the event's data and returns the event for storage with the client. The data is stored until it is used for attribution or exceeds a maximum of 30 days. ARA also allows the user to disable the attribution API. IPA partially proposes a different approach. The event registration also happens in the client based on the website's source code. It includes fetching the encrypted match key and creating the event based on the provided data. The event is then sent to server-side storage (i.e., website or adtech), allowing for the addition of further metadata (e.g., geography, email as of checkout, etc.) of the publisher or advertiser. Currently, IPA does not define an expiry for the stored event data.

Privacy and security considerations

As PCM and ARA manage event data client-side, they retain complete control over it and can limit which data is collected in the browser. ARA involves the help of an adtech to register events. Hence all data might be stored server-side and can be enriched with the website's metadata. The privacy risk is limited as long as no client identifier can be associated with the events. But if the entropy of the event data was sufficiently high, adtechs might be able to match an event with a resulting event-level report. Furthermore, both proposals limit the storage time of historical events, further reducing the risk of user profiling. By storing the event data server-side, IPA allows metadata side-by-side with the events. Hence, the adtech can create overly precise queries to request attribution (e.g., *Request attribution for events for example.blog.com from the UK with conversions by user1@email.com*). This way, detailed attribution results can be requested, helping to identify an individual within the summary-level report. In addition, the data is stored with the adtech and is not in control and not restricted by any expiry. Moreover, in IPA, event registration is not subject to any controlling mechanism, such as the client. Hence, any adversary could forge fake events and send them to the external processing environment. The adversary's knowledge of the fake events might undermine aggregation efforts[8].

Utility considerations

IPA offers a significant advantage over the other proposals by allowing the adtech to create individual attribution queries from the metadata context. Different data cuts and the corresponding attribution result should satisfy a variety of the industry's use cases. PCM does not provide any additional metadata within the client storage; hence the advertiser is limited to the output of the corresponding event-level report. ARA combines client-side storage with sufficiently rich reports by implementing summary reports. However, the aggregation has to be considered in the website's source code during event registration, making the system less flexible than IPA. Another utility aspect is the system's adoptability by publishers and advertisers. Since PCM does not allow support by adtechs, it requires a manual implementation of the event-relevant data in the source code of the page, which is usually automated.

---

[8]Refer to chapter 4 for more information.

3.3.4   Cryptographic protocol

Cryptography measures ensure privacy and security requirements in systems where different applications communicate and share data. Above all, appropriate mechanisms are used to authenticate interacting parties and ensure secrecy and immutability of the message [59]. The scope of cryptography methods in distributed systems can be divided into three areas: data-in-transit, data-in-use and data-at-rest [60].

PCM encrypts all data-in-transit with Hypertext Transfer Protocol Secure (i.e., HTTPS). HTTPS applies the TLS protocol for encryption on top of the commonly used HTTP protocol, which provides relevant web-functionality to send and receive data (e.g., HTTP GET or POST method)[61]. The TLS protocol secures data transfer via three steps: First, the two parties follow a protocol for mutual authentication and definition of encryption parameters in the communication. Second, using asymmetric cryptography (e.g., RSA, Elliptic Curve Diffie-Hellman), a shared session key is created based on each party's private and public key pair (Figure 3.7). Third, using symmetric encryption, the communication is encrypted using the newly created session key and decrypted using each individual's private key [62]. HTTPS to protect web communication is a widely used cryptographic measure for most websites and provides solid security and privacy guarantees [63]. For data-in-use and data-at-rest, no information is provided in the protocol.
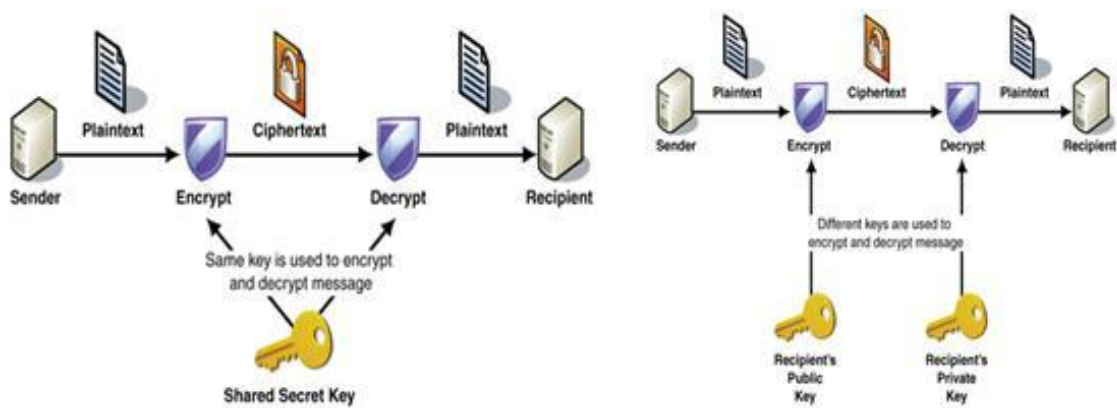

Figure 3.7: Symmetric and asymmetric encryption [2].

ARA encrypts data-in-transit using HTTPS. Furthermore, it is proposed to encrypt the aggregatable information sent to the adtech using a public key from the aggregation service.

The protocol currently does not detail the encryption mechanism other than using Hybrid Public Key Encryption[9]. For data-in-use and data-at-rest, no information is provided.

IPA also encrypts data-in-transit using HTTPS. For data-in-use, IPA proposes that the client encrypts the match key, which is then used in the external processing environment. By design, the external processing environment must be able to perform arithmetic operations on the original match key while the data remains partially encrypted[10]. It limits the knowledge the external server can learn from the data it processes. Encryption algorithms usually produce ciphertexts, which are indistinguishable from a random number making it unfavourable to conclude the data. Any change to the encrypted value would change the original value unrecognisably. IPA proposes three components for the encryption: First, homomorphic encryption to encrypt the data while ensuring editability through arithmetic operations [64, 65]. Currently, the protocol does not specify a certain algorithm but discusses, e.g., ElGamal encryption as an option[11]. Second, randomisation of the encryption in the client. It ensures, subsequent API calls to fetch the match key do not result in the same ciphertext. Third, threshold encryption, which is a distributed public key generation. This way, two parties jointly create a public key for encryption, which can only be decrypted using both parties' private keys, which is required in the external processing environment[12]. For data-at-rest, no information is provided in the protocol. A detailed example on how the encryption including all three components might look like is provided in the *Analysis of the IPA attack space*.

Privacy and security considerations

HTTPS is state-of-the-art for encrypting communication on the web, which is why any potential problems (i.e., man-in-the-middle-attack [66]) are primarily known and not specific to any proposal. However, HTTPS only protects data transfers, not data-in-use or data-at-rest. For this, every web server or client is responsible for the sufficient security of the underlying infrastructure. It is currently not detailed in the protocol and remains an open question in developing the protocols. Considering IPA's homomorphic encryption

---

[9]Standardised protocol for the joint use of symmetric and asymmetric encryption, as in TLS encryption.
[10]Refer to chapter 3 on 'External processing environment' for more information.
[11]Refer to chapter 4 for more information.
[12]Refer to chapter 3 on 'External processing environment' for more information.

mechanism, research has not reached a conclusive opinion on the security and efficiency of the mechanisms [67, 68]. It is critical to the IPA that the encryption mechanism and its associated parameters are carefully selected as it empowers the use of the match key and the external processing environment. Also it must be ensured that brute-force attacks cannot break the randomisation of the client. A thorough evaluation on the applied encryption is needed as soon as the protocol provides more detail. In general, the security of symmetric and asymmetric encryption methods depends on the complexity of the underlying mathematical function. Accordingly, the security of each algorithm must be considered as a function of the computing power of the adversary [64]. However, the proposals provide little information on the applied encryption mechanisms. A discussion of the algorithms will therefore be part of future research.

Utility considerations

The choice of the suitable encryption methodology should have minor relevance in the context of the utility. It is essential that encryption per se protects data efficiently and that the correctness of data is granted. However, as long as a selected mechanism work from an algorithmic and privacy standpoint, the industry will likely not object. IPA's use of homomorphic encryption mechanisms could lead to bottlenecks in the performance of the external processing environment. Fully homomorphic methods, which allow any arithmetic operation on the ciphertext, tend to be computationally expensive [65]. This issue should be reconsidered based on a future update of the proposal.

3.3.5   External processing environment

Increased insight into attribution reports requires a system to collect event data across-client. Using any statistical analysis (e.g., averages, sums) to generate an output of the data shall thereby feasibly protect an individual's privacy. For this, an external processing environment is needed that everyone can trust to provide such summary-level reports in a privacy-preserving and secure manner. The ARA and IPA protocols discuss two different designs, whereas PCM does not offer summary-level reports.

ARA lets the adtech operate an privacy-preserving aggregation service individually. The approach involves a combination of a Trusted Execution Environment (TEE) with an open-source code and an independent external coordinator (Figure 3.8).
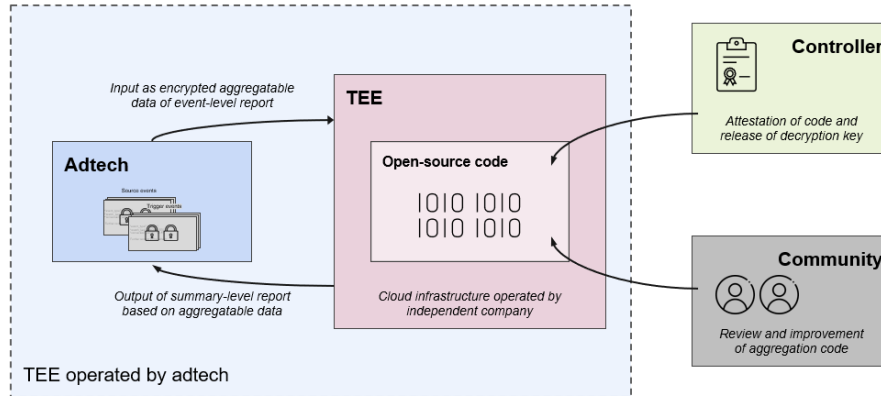
Figure 3.8: Illustration of ARA's TEE with open-source code and external controller.

TEE describes a system where any source code runs in complete isolation, protected by software and hardware mechanisms. Essentially, it guarantees the authenticity of the code and, therefore, the result by hiding the execution of the process and data unobservably for any party [69]. It is proposed to deploy the TEE using an external cloud service (e.g., AWS Nitro) to provide an independent hardware infrastructure. The code will be open-source to invite everyone to check on the aggregation process, granting full transparency regularly. An external controller is required for the encryption management and as a controlling instance of the TEE. The controller provides the client with the public key for encryption of the aggregatable data and attests to the validity of the current source code of the TEE. In executing an attribution request, the controller will provide the private keys for the decryption to the TEE if its source code is valid. The TEE will then run the code to decrypt the aggregatable data, aggregate the information and prepare the summary-level reports.

IPA proposes using a Multi-Party Computing Environment (MPC) for attributing events and preparing the summary-level reports. The MPC is essentially a distributed network of servers where each server processes a single input component independently of one another. As a result, it is assumed that data can be decrypted and processed without each server learning too much of its underlying database [70]. IPA currently plans for three servers to process the data collected with distinct tasks. It is discussed whether the servers are operated by one or multiple non-profit organisations to reduce any risk of collusion.

The *Leader Server* receives the event batch provided by the attribution requestor (e.g.,
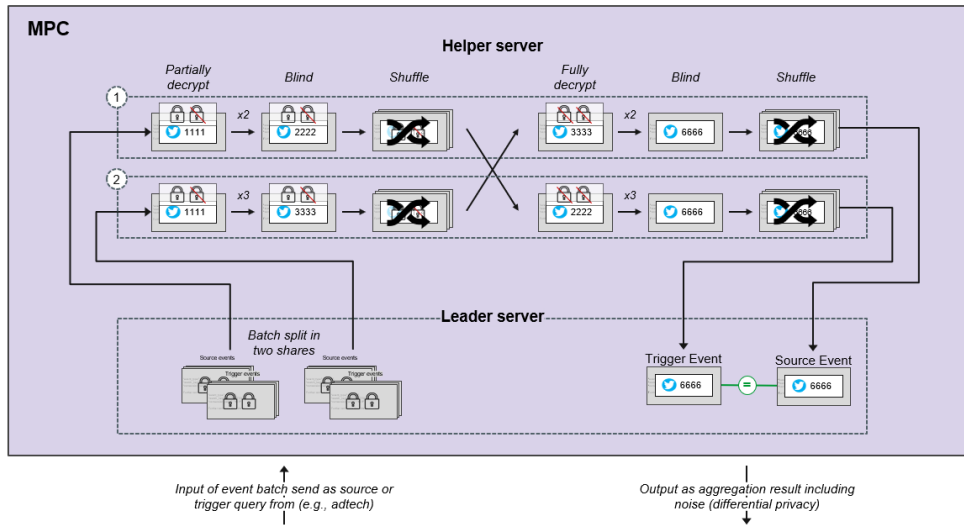
Figure 3.9: Illustration of MPC setup with the leader and two helper servers.

adtech), splits the data set and passes it to the two *Helper Servers*. The helper servers serve two essential purposes: First, they provide an API to the client, who can fetch the public key for match key encryption. Second, they serve to prepare the data for subsequent attribution. For this purpose, each helper server applies three separate functions to its current data set - decryption, blinding and shuffling. Each helper server takes its batch and removes its part of the encryption of the match key, given the applied threshold encryption. The match keys are then modified with a blinding factor per helper server. Any arithmetic function can be applied given homomorphic encryption, which is currently not further specified in the proposal (i.e., Figure 3.9 uses multiplication for illustration). The blinding factor changes with every request from the adtech, hence remains non-deterministic. Match keys that were previously identical remain identical, but the now decrypted user identity is obfuscated for any observer unaware of the blinding factors. Lastly, the order of the events in the data set is shuffled randomly to remove any causality. The helper servers then swap their data sets and repeat the process. Given that each helper server processes each match key, they are fully decrypted, twice blinded and shuffled in order. The leader server then combines the data sets of the helper servers, attributes the events based on the matching match keys and prepares the summary-level report. The protocol states that the MPC is PRIO-conform, a privacy and security standard for data aggregation that provides robustness to any system. Assuming that all servers are non-malicious, the system should

sufficiently protect the client's anonymity and limit the information revealed to the aggregated result [71]. Furthermore, it is planned that not only match keys will be processed by the MPC but also trigger values and timestamps, which are relevant for meaningful attribution. Currently, the attribution result is a count of conversions but should be extended to include the, e.g., sum of purchase prices as well. However, an event's purchase price can be unique to re-identify a specific user interaction. Hence, upon event registration, the event's numerical data must be obfuscated so that the MPC cannot learn anything from the data it processes.

Secret share 1	1234
Secret share 2	-1224
Actual trigger value	10

Table 3.1: Exemplary secret shared trigger value to be incorporated in the event data for numerical values.

The protocol intends to solve this by using secret shared values. For example, the advertiser will split the trigger value of an event into two secret shares (Table 3.1): The first share will be any random value generated during event registration. The second share will be the difference between the trigger value and the first secret share. Those two components will be encrypted and added to the event body. It is currently not defined if the advertiser creates two events carrying one part of the share each. Somehow the two shares must be disassociated to protect the underlying trigger value from any observer. The shares will be summed up across the attributed events in the MPC, resulting in the original trigger value.

Privacy and security considerations

By providing summary-level reports to the adtech, increased infrastructural complexity is inevitably added to the whole attribution system. Assuming that the external environments function as intended, they demand some degree of trust, which otherwise opens up attack spaces for any adversary. TEE requires a central coordinator for encryption and code validation. This bears the risk that either the entity or an external adversary can abuse the encryption to view the event data. Also, the operator of the cloud infrastructure must be trusted by the system to have no economic interest in viewing the event data. Under the premise that any abuse of the operator would be noticed and harm the com-

pany, abuse is unlikely. Nevertheless, all adtechs worldwide would have to believe in the trustworthiness of, e.g., AWS Nitro (Amazon, USA) or would likely demand a local counterpart for the cloud infrastructure not to store data on another continent. As every adtech operates its aggregation service, the risk of a single point of failure for the ARA protocol is partially mitigated. The situation is different here in the IPA protocol. The MPC must also be trusted. Based on the distribution of tasks to individual components, complete privacy preservation is expected to be guaranteed so that no client identity is ever revealed. However, the current setup assumes no malicious server, a threat model one could argue not to be sufficiently secure[13]. Since the MPC is the heart of the protocol processing all attribution data, we expect a more critical requirement for security. In general, technical details on the MPC remain opaque. For example, the attribution with secret shared values is essential to the protocol's utility, but few details are provided. We expect significant protocol detailing, as the full IPA is based on the MPC operation.

Utility considerations

Overall, from an industry perspective, it is relevant that the summary-level report exists, as it seems to be the only viable option for an information-rich report on an attribution without too detailed private information. Hence ARA and IPA provide a solution which is likely favoured over the approach of PCM. Furthermore, the approach of ARA to implement a TEE for each adtech seems rather complex from an implementation standpoint and creates barriers for entry to use the API. As both systems are semi-trusted entities, which still require a central controlling entity, it is opaque why the external processing environment should be split across several adtechs rather than a central entity. The approach of the IPA with the MPC, if it is working fully privacy-preserving, seems easily adapted for any adtech.

3.3.6 Differential privacy

Differential privacy is a privacy-preserving technique used in aggregated statistics to add random noise to any result. The aim is to provide noisy output so that the information in this dataset cannot be distinguished from the information in the same dataset when a particular user is removed [71, 72]. A randomising algorithm will make two decisions:

---

[13]Refer to chapter 4 for more information.

First, a biased coin will be flipped, which decides with probability p if the underlying data will be noised. Second, a randomised value of that data item is selected instead of or added to the data. This relationship is defined as follows, where $M()$ is the randomising algorithm applied to the data set D, D' is the same data set with one entry removed and $S \in range(M)$:

$$\frac{P(M(D) = S)}{P(M(D') = S)} \leq e^{\epsilon}$$

The lower the probability that S can be derived equally from the two data sets, the higher must $epsilon$ be. ϵ-differential-privacy describes the mathematical property to quantify privacy-loss applied to a data set by the algorithm. Epsilon is a metric to describe the loss of privacy given a slight change to the data set [72]. The smaller Epsilon, the higher the guaranteed privacy in the data set (i.e., $\epsilon = 0$), resulting in zero accuracies in the data set). The proposals discuss different approaches to differential privacy based on the underlying reporting type. In general, the protocols provide limited details on the proposed approach to differential privacy but intend to build a robust framework in the future. Epsilon is a parameter selected by the protocol developers, which is required to evaluate differential privacy implications.

PCM does not implement any differential privacy measures.

ARA proposes two means of differential privacy. For event-level reports, they will send k-randomized responses. Upon registration of a source event, the client will randomly decide if the source event will lead to a randomised response if attributed. If so, a fully randomised event-level report (e.g., trigger_value) will be created and shared with the recipient. It can also include the decision to send zero or multiple fake reports. The report provides the probability of a randomised event-level report for increased transparency. Summary-level reports are noised as part of preparing the report in the aggregation service. The statistical result is noised and scaled proportionally depending on the selected $epsilon$ and the remaining contribution budget per aggregatable key. Every source event will have a contribution budget per aggregatable key, limiting the number of occurrences of this event in the aggregation statistic. The contribution of this source event is blocked if the budget is exceeded. The budget will be refreshed for every 30 days.

In IPA, differential privacy is added within the MPC. Two components will be applied: First, a fixed amount of noise will be added to every aggregated statistic (e.g., noise

added to the sum of purchase values). It provides reasonable uncertainty to every report independent of the analysed batch size sent by the adtech. Hence, the larger the batch provided to the MPC, the better the noise-to-signal ratio in the resulting report. Second, IPA also uses a privacy budget as a metric to scale any additional noise applied to the summary-level report. This privacy budget is applied per match key. For every query sent, a specific budget amount will be deducted from every match key. If the budget of a match key is exceeded, no further aggregation will be executed in the given epoch (i.e., not yet defined). Moreover, it is planned that an adtech can consume its privacy budget to reduce applied noise in a query.

Privacy and security considerations

In general, the consensus in research is that differential privacy represents a solid mechanism to provide data protection guarantees [72, 73, 23]. Assuming that Epsilon is set correctly for the corresponding use case, it should be challenging to reconstruct an individual's identity from an aggregated result. However, there are limits, for example, given sensitive attribution requests. The problem is especially with non-counting queries, which do not only summarise counts in histograms but apply any statistical functions to numerical values. A query such as, e.g., *maximum value*, *mean* or *sum* is especially affected by unbound ranges of numerical values [73, 71]. The statistical output would likely hold sensitive information, which might reveal an individual. The proposed frameworks are still in very early stages and require further detailing to be evaluated. The concept of a privacy budget helps to limit repeated requests on a single match key, exposing its information and identity. For a budget to be applied meaningfully, the scope of the budget (e.g., per match key, per entity) must be carefully defined. For example, in IPA, a budget per business entity is explored to prevent an adtech from creating dozens of websites, sharing the event data and hence being able to overuse the privacy budget for a single source event.

Utility considerations

Uncertainty in data is likely an unpopular topic in the online advertisement industry, as less accurate data can lead to less accurate decisions. Hence, the protocols must carefully balance the trade-off between differential privacy and the corresponding accuracy loss in the data. Moreover, noise that does not scale with the number of events sent for attribution

will inevitably lead to an unfair competitive advantage for larger adtechs. Smaller adtechs, compared to larger companies, will likely collect less data, hence will have more noise in the resulting attribution reports. IPA's proposal to consume the privacy budget of a website to keep noise in resulting output low is desirable. The idea of consuming more privacy budget to reduce applied noise seems favourable. It gives an adtech the flexibility to manage the noise to a certain extent resulting in increased utility for the industry. For example, queries with high accuracy requirements could thus be kept as accurate as possible.

3.3.7   Reporting delay

One piece of information that comes with each event registration is the timestamp. In event-level reports, this could allow the recipient to know about a user's cross-site activity. For example, if a report is sent directly after attribution, that timestamp would almost equal the trigger event's timestamp, becoming a proxy for an identifier. The advertiser could enrich the report with its conversion metadata (e.g., location, user name). It would allow us to gain knowledge about a conversion that is intended to be visible on a summary level.

PCM sends event-level reports, hence requiring reporting delay to disassociate the report from previous user activity. The concept proposes a time window of 24 to 48 hours, out of which a random time delay is selected to schedule the report. If the browser is not running as the report is due, the report is shared on its earliest occasion.

ARA also plans on delaying its event-level reports but differentiates between attributions based on ad views and ad clicks. For source events from ad views, the report is sent one hour after the expiry of the source event. In ARA, expiry is an optional value with a default of 30 days. There will be three reporting windows for source events from ad clicks (i.e., 2, 7 and 30 days) randomly assigned to a source event upon registry. Upon event attribution within an assigned reporting window, the report is sent at the end of that window. As with PCM, the client will randomly send any reports due while the client is inactive when the browser becomes active again.

IPA does not provide event-level reports. Hence no artificial reporting delay is required. But nondeterministic delay is created as the adtech must collect a certain number of events to send this batch for attribution.

Privacy and security considerations

Overall it seems relevant to decouple any information about time from the attribution report, especially in event-level reports. The decision to determine the time delay based on the source event's registry is reasonable. If the trigger event registry was the dependent, a link between the event-level report and trigger event could be approximated, and conversion metadata could be attached to the report. In IPA, an adtech could control the collection time of event data by forging fake events to fill the missing data in the batch for send-out. It would allow for short turnaround times of attribution after event registration. The collection time is not a privacy measure per se, hence bypassing it does not threaten the current design choice. However, the adtech receives source and trigger events immediately after registration. Suppose a user clicks on an ad and buys the corresponding product instantly. The source and trigger event will be created and sent to the adtech quickly. Given the similar timestamps, the events might be linked, revealing cross-site information on a user.

Utility considerations

In today's attribution efforts, time to conversion is an important metric used to evaluate the relevancy of a user's interaction with an advertisement before they decide to buy a product [37]. Introducing uncertainty increases the difficulty of correctly remunerating a publisher for its role in the user's sales journey. Furthermore, the time lag also reduces the possibility of testing advertising campaigns and controlling and optimizing them with real-time feedback, which is a critical component of an adtech or advertiser.

3.3.8   Rate limits

With every additional query, more information about an individual is leaked incrementally. Whereas differential privacy reduces the privacy risk corresponding to a single query, rate limits introduce further privacy protection over the sum of all queries. Thereby, a maximum threshold of leaked information can be defined.

PCM and IPA do not apply rate limits in their attribution system. ARA proposes three rate limits applied to both event- and summary-level reports for the client's reporting window of 30 days. First, a reporting origin limit restricts the number of unique adtech domains in source events with the same pair of publisher and advertiser domains to a hun-

dred events or ten successful attributions. Suppose a client stores a hundred events from *example.blog.com* defining *example.shop.com* as the destination and different adtechs as attribution source. Every additional source event with a new adtech will not be stored in the client. Otherwise, an advertiser could deterministically coordinate event registration with several adtechs to gain additional entropy. Second, a reporting cooldown will further restrict attributions for client events with equal source, destination and adtech domain to a hundred. This limit further reduces the maximum data revealed from a single client. Third, the number of unique advertiser domains defined in the pending source events of an adtech is limited to 100. For example, a client stores a hundred source events of an adtech from *example.blog.com* pointing to different advertisers. Every new source event from the same adtech referring to a new advertiser will exceed the client's limit and is not stored. This is done to limit further the insight a single adtech can gain on the browsing history of a single client.

Privacy and security considerations

An upper boundary for a user's data leakage in the overall attribution process seems reasonable as a safety net in general. It ensures that the entire knowledge anyone can learn is restricted to a well-defined maximum. IPA tries to create the same effect of a maximum leakage threshold with its privacy budget in differential privacy. Further research must evaluate the configuration of the rates selected, possibly via simulation. The current thresholds are an arbitrary starting point and must be fine-tuned.

Utility considerations

Rate limits per se should not limit the quality of the attribution systems. However, the limits may affect the operation of attribution modelling differently depending on the size of an adtech. A larger network, which partners with more publishers and advertisers, might query larger amounts of data. It could run up against limits in the attribution, which remain to be investigated.

3.4 Interim conclusion

We looked at the three proposals for devising attribution modelling solutions that did not require the use of third-party cookies. The proposals have advantages and disadvantages

regarding privacy, security and utility, based on the current design choices. However, we think that none of the proposals has offered a solution that sufficiently balances all stakeholders' interests.

Apple's PCM provides a basic yet effective solution to enable attribution and protect privacy. With client-sided attribution and the exclusion of adtech and any external aggregation service, the protocol offers an almost trivial architecture and, thus, a simple implementation. The focus is on, and control is with the client trying to limit the revealed data points as much as possible. However, the protection of the user is strongly accompanied by the loss of functionality in attribution. Publishers and advertisers will find it difficult to do online marketing efficiently without the direct assistance of an adtech, leaving much of the effort to individual sites. Furthermore, the available attribution data is limited to only a count and a categorical trigger value of ad clicks. The attribution modelling logic is based on last touch- or priority-based attribution. This severely limits the extent performance measurement can be done. We assume this results in a setback for the industry compared to their requirements. In the future, we recommend testing if the send-out of event-level reports is reasonably privacy-preserving or if an unjustifiable amount of information is leaked compared to summary-level reports. Especially since only delay but no noise is applied to the individual's data.

Google's ARA takes a functionally broad approach and offers event-level and summary-level reports after client-sided attribution. By separating attribution in the client and later aggregation in the TEE, they ensure that the sensitive information around the client never leaves its instance. Thus, all data processed outside the client is not directly identifiable, which is an advantage for privacy and utility since summary-level reports allow macro insights into any advertising campaign. However, ARA allows for detailed data in the reports, firstly through a relatively high entropy in the source event on the event level and secondly through an unlimited number of aggregation keys in the summary-level report. It is not yet clear whether the diversity of data makes it possible to re-identify individual users or to create profiles and how the corresponding protective measures (e.g., delay, noise, rate limits) counteract this. Compared to IPA, the external TEE seems less critical in

its role for aggregation as the data has no associated client identifier. But, as the TEE will be able to observe data in plain, it learns everything provided, hence must be evaluated carefully. Details on the setup are awaited.

Meta/ Mozilla's IPA protocol focuses entirely on preparing summary-level reports and the associated measures to protect the sensitive match key. Unlike its predecessors, IPA proposes an industry-focused approach to attribution with a relatively strong position of the websites/adtech and a simple browser API. Flexible attribution queries in the context of the conversion's metadata should ensure the utility of the industry. However, those queries also allow very targeted requests to the MPC, which requires a well-balanced approach to aggregation and differential privacy to safeguard any individual in the data. Moreover, the concept brings an increased degree of complexity since the identifier is removed from the private browser environment and is always associated with sensitive data. The main focus of the IPA is on the MPC, which handles attribution and aggregation simultaneously. This is a somewhat opaque setup of several servers that process the data collected without learning private information. Although the developers aim for high security and privacy requirements in the MPC, details on the actual implementation are missing. In general, we see that the concept is still in its infancy, compared to PCM and ARA, making it difficult to assess the protocol conclusively. Further research should focus on further evaluation of the MPC to identify possible weaknesses in privacy and security.

In summary, all proposals are still in development and improvement, and none has found a sufficiently balanced solution between privacy, security and utility along the key design choices. ARA and IPA have promising protocols, which might develop into sufficiently functional attribution systems meeting privacy requirements. However, further development of the protocols is needed. Especially some technical details in the proposals are sparsely revealed or not conclusively defined. Further research or industry simulations with the existing tools (i.e., PCM and ARA) could contribute to the ongoing discussion and serve as feedback for the development. In the following, we will focus on the IPA protocol specifically. This protocol is currently under intense discussion, as it is the most recent addition to the cookieless attribution discussion, which only exists as a concept.

Below, we analyze the attack space of the IPA and describe the first running prototype that we have developed based on the protocol.

Chapter 4

Analysis of the IPA attack space

The previous consideration of the IPA was primarily focused on privacy and utility aspects. Assuming that the selected privacy measures are generally sufficient to meet the privacy requirements, considering the system's security seems reasonable. In order to maximize utility, any adversary (e.g., adtech) could decide to attack the system to gain information not intended to be revealed, which would undermine the protocol's purpose. In the following, we will derive an attack space of the IPA, which helped us to identify a potential threat to the protocol. Hence, we will explain the mode of operation of our identified threat and discuss its consequences and underlying technical details. Furthermore, we will discuss potential mitigation and limitations to the threat to further improve the protocol. Particular focus was placed on the MPC, which had already been identified in the previous review as a somewhat opaque and possibly error-prone design.

4.1 Derivation of an attack space

This section will derive an attack space relevant to the IPA protocol. It is meant as a structured approach to analyzing potential attacks on the current version of the proposal. As the protocol is a set of multiple stakeholders and assumptions, a structured approach seems needed to identify flaws of the current protocol.

4.1.1 Threat model

Analyzing potential threats to an information system, especially with multiple stakeholders, can be viewed as a function of trust given to each party in that system. It requires

looking at multiple scenarios for each party to identify the extent of data leakage considering a certain trust level. Threats external to the system, such as attacking a database or intercepting server communications, are not considered in this analysis for simplification. These represent relevant risks but are not system-specific per se. The following three trust levels can be considered:

First, trusted parties in a system follow the protocol as intended. They learn whatever the protocol provides them; however, they would not actively seek to reveal any exception case beyond that. Such parties are not considered in the analysis because any system with only trusted parties would be considered inherently protected against internal attacks.

Second, semi-trusted or honest-but-curious parties are also within the bounds of what is possible under the specifications of the protocol. However, unlike before, the parties exploit edge cases trying to learn as much as possible about the underlying data, which was not actively protected in the first place. For example, an adtech could strongly refine the request to the MPC based on the adtech's metadata of the conversion, e.g., 'All source and trigger events from coffee.blog.com (publisher) and coffee.shop.com (advertiser) with geography equal to "UK" in the last three days. The adtech would not harm the protocol and still might be able to learn detailed information about an anonymous individual, which is meant to be prevented in the proposal. Countermeasures like differential privacy are intended to limit such data leakage. In the following, we do not consider honest-but-curious parties as an analysis would depend on the proposed countermeasures provided and their detailed design assumptions, which are still relatively opaque.

Third, malicious parties follow protocol but may choose to deviate if it is advantageous by running unintended processes. It might enable them to bypass privacy-preserving measures while learning sensitive information. Furthermore, malicious adversaries might decide to collude with one or multiple other parties in the system. Any cross-party communication, which is not intended by the protocol, could help to reveal secret information, e.g., private keys of cryptography mechanisms, which could ultimately undermine the system's integrity. The following shows the IPA attack space for malicious parties in the system.

4.1.2 Definition of an attack space

We decided to outline the whole space of possible collusion between one or two parties to identify a possible attack on the IPA protocol assuming a malicious party. We explicitly

decided not to consider collusion by three or more parties because we assume that (a) each additional malicious party should be considered unlikely, (b) with each additional malicious party, the system is easier to undermine, but an analysis result only gains limited significance, and (c) in a majority malicious system security measures are unlikely to take any effect. Furthermore, the proposals are not a solution to mechanisms such as fingerprinting or IP address tracking [24]. Given those, the entire attribution system could be undermined, a challenge that must be considered in general. We have entered all the already known security threats in the IPA attack space to identify known vulnerabilities and possible collusion. However, it also gave us a view of previously unconsidered areas of the attack space (Figure 4.1).

Figure 4.1: Threats of maliciously (non-) colluding stakeholders in the IPA protocol.

So far, four vulnerabilities are known to the proposal [57], which allows to re-identify the original match key of a client. Those could be linked back to the metadata collected by adtech resulting in cross-site information and the potential to profile the user. Unilateral and bilateral blinding reveal describe attacks we have identified as potential threats to the MPCs security, which will be discussed in the next chapter. Two attacks are possible if the adtech colludes with the leader or helper server:

- **Known Event Cardinality** - The adtech could forge many fake events with the same encrypted match key as the one to be revealed. The helper server would then be able to observe the decrypted and twice blinded batch of match keys with a single match key that stands out due to its frequency in the data set.

- **Known Secret Shared Value** - The adtech could forge a single fake event with the same encrypted match key as the one to be revealed. Suppose the fake event's secret share (e.g., the trigger value) was communicated to the helper server. In that case, it could identify the fake event in the decrypted and twice blinded batch of match keys, hence finding the targeted match key. The secret shared value likely has high entropy to sufficiently protect the secretly shared trigger values, leading to potentially unique values in a selected batch of events.

One attack is possible if the match key provider colludes with the leader or helper server:

- **Known Linear Relationships** - Homomorphic decryption and blinding operations preserve an arithmetically linear relationship by definition. As the match key provider knows original identifiers, it could forge fake events, which are linearly related to the identifier to be revealed. This relationship is unchanged throughout the MPC process. Hence the helper server could identify the same relationship in its blinded values which might lead to the re-identification of the targeted match key.

One attack is possible if both the helper servers collude with each other:

- **Joint Blinding** - As both helper servers run the whole data processing, including decryption, blinding and shuffling, they would jointly have all knowledge to re-identify every matching key.

We assume that the client/browser does not become malicious for the consideration below. It would neglect any privacy interest of the browser and cause tremendous image damage should a browser subvert its users. Furthermore, we focus primarily on an attack of the MPC driven by two reasons. First, the MPC seemed questionably designed in the previous review and thus potentially offers an attack surface. Second, the MPC is the only point in the system that sees the identities decrypted and thus represents a sensitive point.

In the following, we will focus on the unilateral blinding reveal a potentially new threat to the MPC.

4.2   Unilateral blinding reveal

The attacks on the protocol identified so far required the collusion of two parties to subvert the system. The security risk inherent in this cannot be neglected but requires a corresponding effort that can create a deterrent effect. Accordingly, an attack on the IPA that could be perpetrated by one party alone would be all the more critical. Below we describe such an attack and its consequences. We also address possible mitigation and limitations of our consideration to improve the proposal further.

4.2.1   Mode of the attack

In the identified attack, the leader server may be able to leak the identity of any match key while running a regular attribution request. This attack is assumed to work without collusion or anyone noticing. Such a security risk is especially critical since the entire system must trust the leader server not to turn malicious or that it was taken over.

The mathematical basis

For illustrating the attack, the mathematics behind homomorphic encryption (i.e., Elgamal encryption) in combination with blinding must be understood to arrive at the fully decrypted and twice blinded match keys. For this, Rescorla [74], CTO at Firefox, has worked out an overview of how this might look in the context of the IPA protocol. Note that Rescorla's explanation simplifies calculations by using integers and exponential notation to explain the basic properties of the approach. The encryption will be based on elliptical curve cryptography, which is significantly more difficult to compute by an adversary, hence more secure. Helper servers A and B have a pair of private keys A and public key g^A, whereas g is public knowledge.

$$[A, g^A] \quad and \quad [B, g^B]$$

The MPC provides a combined public key of the two helper servers (i.e., threshold encryption) by multiplying the single public keys, which results in $g^A * g^B = g^{A+B}$. It allows no single helper server to read a secretly shared message alone. For every API call to fetch a match key, the client creates a private random value R and a public value g^R. It then computes the encryption factor $g^{(A+B)^R} = g^{R(A+B)}$ using the joint public key, which encrypts

the match key I. This encrypted match key and the client's public value g^R is then secretly shared with the API caller.

$$[g^R, I * g^{R(A+B)}]$$

Later, helper server A receives its batch with encrypted match keys (respectively, helper server B) for processing. For this, it (1) calculates its decryption factor based on its private key and the client's public value, (2) removes its encryption from the match key and (3) blinds the resulting match key value pair with its factor B_A.

$$(1) \quad (g^R)^A = g^{RA}$$

$$(2) \quad \frac{I * g^{\cancel{RA}} * g^{RB}}{g^{\cancel{RA}}} = I * g^{RB}$$

$$(3) \quad [(g^R)^{B_A}, (I * g^{RB})^{B_A}]$$

Note that blinding is done by applying an arithmetic operation (i.e., here exponentiation) to match key I. After shuffling, helper servers B takes over and repeats the same processing with its blinding factor B_B. The result is the fully decrypted and twice blinded match key $I^{(B_A)(B_B)}$, which will be used for attribution and aggregation.

$$(1) \quad ((g^R)^{B_A})^B = g^{(RB)(B_A)}$$

$$(2) \quad \frac{I^{B_A} * g^{(RB)\cancel{(B_A)}}}{g^{(RB)\cancel{(B_A)}}} = I^{(B_A)}$$

$$(3) \quad (I^{(B_A)})^{(B_B)} = I^{(B_A)(B_B)}$$

The leader's attack

In the protocol, the registration of any event is not tied to an actual event (e.g., ad click or ad view) or any authentication of a publisher or advertiser. Hence, everyone within the IPA system can forge events which look alike. To create a fake event, the adversary fetches the publicly available encryption key $[g, g^{(A+B)}]$, generates a random secret S and selects a match key J to create the fake event.

$$[g^R, I * g^{(A+B)^R}]_{legit}$$

$$[g^S, J * g^{(A+B)^S}]_{fake}$$

Any external spectator should be unable to distinguish the match keys since a match key from a single client is always randomized differently given the random secret R or S. In the regular IPA process, the adtech would send a batch of legit events (Table 4.1) to the leader server with a request for attribution.

Event type	Match key	Timestamp	Trigger value	
SOURCE	1000	00:00	-	*legit*
SOURCE	1011	01:20	-	*legit*
TRIGGER	1000	02:00	100	*legit*

Table 4.1: Exemplary event batch sent to the leader server. The data is simplified and shown in plain text for illustration.

If the leader server is malicious, it forges a fake event and adds it to the adtech's batch. By doing this, nobody will notice the fake event as the adtech receives, in return, an aggregated attribution only, and the helper servers would not know the original batch size. The leader server will require to re-identify its fake event later on. Hence, it creates a batch of fake events similar in size to the original batch (Table 4.2). Re-identification might also be accomplished through known event cardinality or a known secret shared value.

Event type	Match key	Timestamp	Trigger value	
SOURCE	2222	00:00	-	*fake*
SOURCE	2222	11:11	-	*fake*
SOURCE	2222	22:22	-	*fake*

Table 4.2: Exemplary event batch of fake events created by the leader server. The data is simplified and shown in plain text for illustration.

This way, the leader server has a batch of legit events (Table 4.1) and a batch of fake events (Table 4.2) for send-out to the helper servers. The helper servers take on the event processing as described before, resulting in:

$$[I^{(B_A)(B_B)}]_{legit} \quad and \quad [J^{(B_A)(B_B)}]_{fake}$$

The leader server would receive both processed batches from the helper servers. Since the

events were divided into fake and legit events before and since all fake events have the exact match key, the leader server will re-identify the fake events easily (Table 4.3).

Event type	Match key	Timestamp	Trigger value	
SOURCE	4000	00:00	-	*legit*
TRIGGER	4000	02:00	100	*legit*
SOURCE	4044	01:20	-	*legit*

Event type	Match key	Timestamp	Trigger value	
SOURCE	8888	22:22	-	*fake*
SOURCE	8888	11:11	-	*fake*
SOURCE	8888	00:00	-	*fake*

Table 4.3: Exemplary batches of fully decrypted, twice-blinded and shuffled events. Combined blinding factor for both helper servers of four assumed for simplification.

The leader server would know the fake match key J and now has identified $J^{(B_A)(B_B)}$ as the corresponding blinded version. This way, it should be able to derive the blinding factor $(B_A)(B_B)$ of the two helper servers. If this was possible, any twice blinded legit match key defined as $I^{(B_A)(B_B)}$ could be re-identified to I by implication of this attack. Hence, the leader server could potentially reveal the client's match key, given the described attack.

A similar attack (i.e., Bilateral Blinding Reveal), even though more complex as two parties are involved, could be run by one of the helper servers colluding with the adtech. The adtech would be responsible for creating the fake events and communicating the known match keys to the helper server. The helper server would re-identify the fake events among the actual events. In this scenario, the re-identification must be managed through a known secret shared value or event cardinality. It is assumed that the adversary does not control the leader server, hence has no control over the split of the original event batch.

4.2.2   Consequence and mitigation

Finding an attack on a system helps in that the underlying protocol can be refined and becomes more secure. However, it is necessary to discuss the consequences of the attack to determine the urgency of mitigation.

Consequences

Due to the attack, the leader server can uncover all sent match keys in the batch for each request of an adtech. The fact that a client's real identity is visible outside the client contradicts the protocol's purpose. One could argue that the pseudonym alone is not as valuable for the leader server. However, as long as the match key for an individual remains constant and can be linked to the match key provider, the lead server consistently collect data and create a user profile, which includes preferences for purchase prices and purchase times at least. Furthermore, it could conclude the duration of a user's conversion cycle using the timestamp of the first source event and the final trigger event. Because the leader server communicates with the adtech, it can identify this adtech with every request. The provided match key will likely be unique per client given a high entropy value and assuming that the adtech likely uses few match key providers only. Furthermore, the data could be shared with either the match key provider or the adtech. The former would mean that the pseudonymity of the match key could be removed entirely based on the shared knowledge of the match key. Recall that the match key provider is a log-in platform, presumably with a more extensive personal data profile that could complement the purchasing behaviour profile accordingly. The latter has the advantage of linking the leaked data with the knowledge of relevant metadata of the adtech. The entire conversion data (e.g., payment method, email address) could be assigned to an identity.

Mitigation

Although the attack has profound consequences for the system, the solution of it should not be complicated. Unless the leader can get the values of the match keys after decryption and blinding, he will not be able to re-identify the fake events and, thus, any other events. Thus, the introduction of a separate aggregating party would make sense. This party would receive the data from the helper server directly, attribute it, aggregate it and send it to the adtech. The leader would be removed from this step, hence will have a view of the processed data.

The bilateral blinding reveal seems to be more difficult to be mitigated as the helper server is the closest to the processed data with no other party having any influence. Nevertheless, each additional helper server in processing the data in the MPC would weaken the

probability of a successful attack. For example, suppose that four helper servers would now process a batch of 100 events previously processed by two helper servers. It would mean that a malicious helper server's actual decrypted and twice-blinded sub-batch would result in 25 events instead of 50. Out of these, the fake events must be re-identified to break the applied blinding factor resulting in the remaining events being actual match key leaks. However, this mitigation might not be feasible as every new helper server increases the complexity of the MPC, resulting in new security risks and decreased performance.

Overall, it seems helpful to introduce any prevention of fake events from being generated. As in the previous attacks, fake events are the gateway for attacks since the adversary can define them as wished. Further research is required in this area. Moreover, the existence of the leader server should be reconsidered, as the introduced merit of randomly split input for the helper servers does not outweigh the introduced security risk. Nevertheless, the helper servers retain an excessively critical role in the MPC. Since they have access to unencrypted match keys, they will be the linchpin of any attack. Further research should reduce the dependence of system security on a single helper server.

4.2.3   Limitations

It should be noted that the proposal and the MPC are designed for an honest-but-curious threat model. The proposal aims to build a robust protocol to protect against malicious parties. However, this does not have to be included in the design necessarily. Thus, aggravations of the attack space may not have been considered by the author so far to keep the concept more straightforward. Moreover, any details about the MPC are kept vague and leave room for interpretation. A more detailed description is needed to re-evaluate the attack space. For example, the blinding of the match keys assumes that all match keys of a batch are blinded with the same factor, which is possible due to the current understanding of the applied homomorphic encryption scheme [74]. If the blinding would create the same random value for the exact match key but uses a different random function for a different match key, the attack would be mitigated. Furthermore, it does not seem conclusively certain whether the leader server runs attribution and aggregation after the helper servers have processed the match keys. It would mitigate the risk of unilateral blinding reveal as described but would not solve for the bilateral blinding reveal.

Chapter 5

Development of an IPA prototype

In the following chapter, we will provide an overview of the IPA prototype developed as part of the project. The focus will be on the objective for the decision to develop the prototype, the technical implementation of the application, identification of opaque design choices and evaluation of the resulting prototype.

5.1 Motivation of the prototype

The research on the cookieless attribution modelling proposals indicated three aspects, which generally led to the decision to build a prototype source code of the IPA protocol. First, a well-balanced cookieless attribution approach requires input and feedback from various perspectives, i.e., developers, researchers, regulators and industry experts. Second, PCM and ARA have a running protocol application, whereas IPA is a proposal draft only. Third, the definition of MPC in the IPA generally seemed somewhat vulnerable and could be further clarified utilising a prototype. Considering all three, we perceived that a comprehensive and clean written source code for demonstration would facilitate the IPA development with new feedback. Moreover, it would increase understanding of the technical design choices and allow testing of the protocol not only on the concept level. The development of the project's prototype aimed for:

- **Adaptability** - the prototype aims to provide a solid foundation for the future source code of the upcoming IPA protocol. The prototype should be extendable so that any changes in the protocol can be incorporated easily to develop the application in parallel to the proposal incrementally.

- **Completeness** - the prototype aims to cover the most relevant technical details to the extent described in the public proposal. Assumptions for implementation might be simplified but should be addressed in the prototype for a full overview of the underlying protocol.

- **Accessibility** - the prototype should be accessible for demonstration and to look at the technical details for all potential interest groups to easily understand and use the protocol in an individual test case.

- **Robustness** - the prototype must deliver the provided functionality reliably and consistently with clear exception and error handling to avoid malfunction and breakdown.

5.2 Technical details

This section will cover how we thought about translating the prior described IPA protocol into a functioning prototype. It follows a summary of the tech stack applied summarised in the front end, back end and deployment. It will discuss the proposal's current limitations and the technical key design choices. The corresponding code repository will be provided.

5.2.1 Technical implementation

The technologies used to develop the prototype can be roughly divided along the roles in the protocol. The client, the match key provider and the websites represented the IPA's front end. The Adtech and the MPC are the back end components and contain most of the protocol's logic. The individual components of the tech stack are described below.

Front end

The front end comprises the client's representation, the match key provider and the publisher and advertiser domains. The adtech is visualised with a front end as well, but only for the purpose of demonstration. The content seen here, will not be available to the public. The implementation was kept rather simple, as it is meant to illustrate the IPA's overall setup and provide code examples for implementation on the web. The implementation of the IPA will happen in the browser or any participating website/ adtech directly. We generally utilised HTML5 for webpage setup, CSS library for basic styling and JavaScript
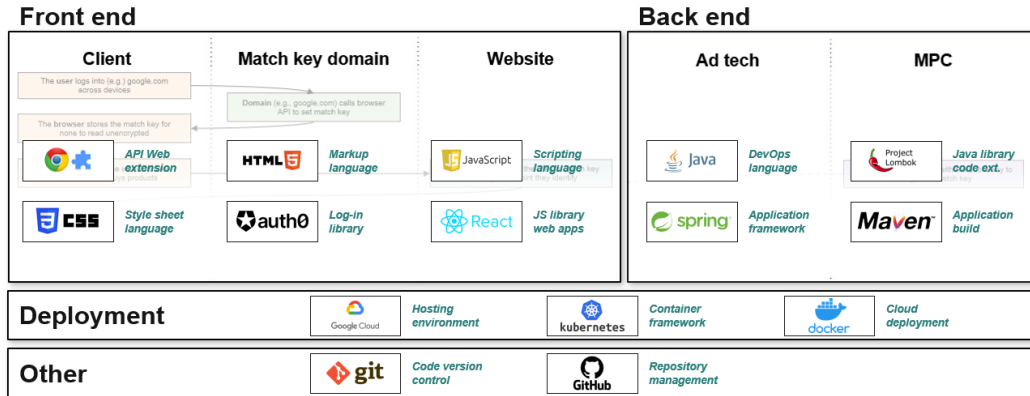
Figure 5.1: Technology stack for the development of the IPA prototype.

through the React framework for web applications. This setup enabled us to easily implement the required basic front end. For the client, we built a chrome extension to mimic the browser API, which any browser will need to implement if IPA is supported. Chrome was chosen as the browser infrastructure due to the extensive user base and the comprehensive documentation for developing an extension. The client implements two APIs (a) for setting a match key to the local storage and (b) fetching an encrypted match key for registration of an event (i.e., *contentscript.js*). Here, it furthermore implements the background call to the MPC to retrieve the required encryption details (e.g., public key) for the match key. The extension implements a simple popup with a list of domains that have currently stored a match key in the browser and the functionality to clear the storage (i.e., *popup.js, popup.html*). Further configurations of the extension, including metadata (e.g., description) and permissions, are defined in the *manifest.json*. The match key provider website implements the client API call to set a match key for client storage. For this, a simple web page is created with a log-in (i.e., *pages/index.js*). The log-in is needed to identify the user to set a consistent match key across devices. For the authentication we leveraged the Auth0 identity platform, which provides a simple, reliable and secure login API (i.e., *pages/api/auth/[...auth0].js*). Upon log-in the match key provider calls its web server (i.e., more details in the backend description) to store the user credentials. Here, either a newly generated or an existent match key will be returned, which is passed on to the client. The exemplary publisher or advertiser domain mimics any domain which will have ads displayed or will be the point of final conversion. Upon click on the displayed

button, the client's API is called to fetch the encrypted match key, which is packed in the event object defined in the web page's source code. The website then forwards the object to the adtech's web endpoint.

Back end

The back end includes the setup of the required web server of the MPC, the adtech and the match key provider, and the corresponding functionality. Four key technologies were used to build the back end. First, we choose to implement the back end using Java to increase the source code's re-usability. As it is one of the standard programming languages, especially regarding software development, we assumed that any further code development was facilitated. Second, we leveraged the annotation-based java library Lombok, which automatically implements functionality for model objects like getter and setter functions to keep the source code clean and simple. Other standard Java libraries were implemented on a need basis. Third, for the overall application development, we opted for Java Spring Boot, a framework built on top of the Spring framework. It offers a simplified setup and auto-configuration of the required dependencies to run a (web-) application and is highly integrated with Java. Furthermore, Spring Boot simplified endpoint definition and cross-server communication, which is extensively required in the protocol. Lastly, we used Apache Maven to manage and build the back end application. Special attention was given to the code structure of the back end.

We intended to create a simple but reusable code for everyone to understand and to pick up if needed. Furthermore, as the back end keeps most of the protocol's logic, we assumed it would be subject to change in the future, requiring a high degree of flexibility. Given that, the code structure is based on the software design principle for clean architecture by Martin [3]. The primary purpose of this design principle is the best possible separation of dependencies in the code. For this, the development is based on four distinct layers of the code. Changes outside of a specific layer do not affect the layer itself. The core is described by entities and use cases. Entities are data structures or objects used in the application, which are at the core of the logic and least likely to change. Use cases implement the logic of how entities are processed and encapsulate the application's functionality. They can be accessed using a single output and input interface. Interface adapters represent a bridging layer to translate data formats from the core to any form that is needed by any outside
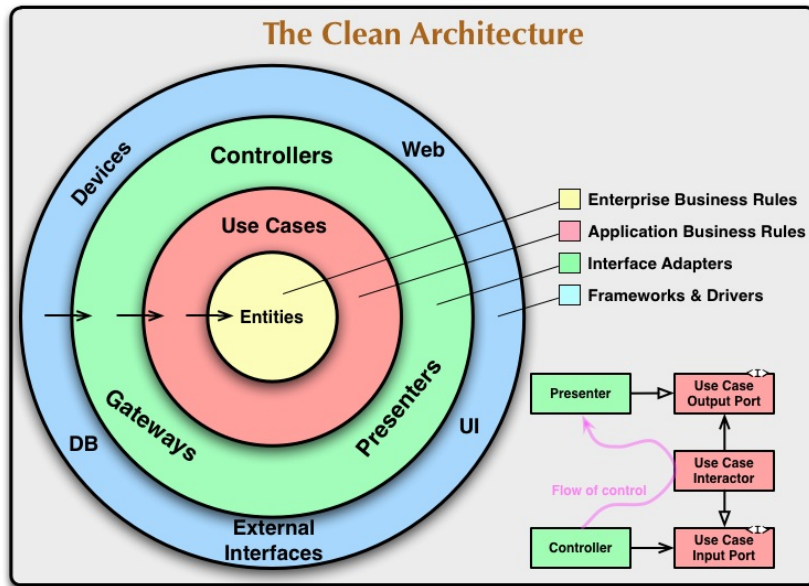
Figure 5.2: Software design principle - "The Clean Architecture" [3]

tool or application. The last layer structures the implementation of the application and manages the application's outward and inward communication.

Deployment

The prototype is deployed to give everyone unrestricted access to a basic demonstration of the IPA protocol without requiring them to set up a *localhost*. For our hosting and deployment of the application, we have created required build and deployment scripts (i.e., *build_backend.sh, build_frontend.sh, deploy_ipa.sh*). The build scripts essentially creates a docker container. The deploy script then pushes the container into the Google Cloud Platform (GCP) artifact registry, where it is finally deployed using Kubernetes. First, GPC is an infrastructure-as-a-service providing us with the complete management of the web servers, including, e.g., server startup, load balancing and HTTPS certification. Second, Kubernetes is a framework from Google for container management to facilitate automated software development and deployment. Third, we use Docker to containerise applications, which is the encapsulation of the application to minimise dependencies on any operating system. All the technologies used are standard in the industry, so we assume that the source code of the prototype can be easily used.

Furthermore, the project used Git/ Github as a version control system.

5.2.2 Limitations of the prototype

For the prototype, we aimed at the best possible first implementation of the current proposal to create a solid starting point for further development. Therefore, addressing the areas where the present prototype differs from the proposal is necessary. The points where the prototype differs from the proposal and the points where the proposal provides insufficient information will help guide further development. For this consideration, the earlier described key design choices are used to pinpoint relevant deviations between protocol and prototype:

Client- vs. server-sided attribution

The proposal provides an extension that multiple match keys can be queried in the client simultaneously and attributed to an event to increase the attributability of an event. So far, this has not been implemented in the prototype, as this consideration has been discussed more intensively. It must be noted that the implementation of the client via an extension is an interim solution. The client APIs must be integrated into the actual browser to guarantee the complete security of the match keys. Furthermore, the attribution report is limited to the number of conversions and does not include aggregation of the trigger value. Since the protocol does not clearly define how secret shared values are passed privately in an event, it has not been included. Moreover, it is proposed that the domains of all source or trigger events in a request batch are the same (i.e., source and trigger query) to restrict event selection. It is not clarified who will validate that a request meets these requirements. Lastly, the prototype has not implemented any epoch to reset match keys or privacy budgets as the protocol is not clearly defined.

Data coarsening

The protocol currently does not provide a fixed size of bits allocated to the representation of the match key (i.e., match key is a value between $0 - 100$). Hence, the prototype sets the match key size arbitrarily. In addition, the trigger value is not part of the event data. This is primarily for simplification of the prototype and could be added, assuming details on the secret shared values were provided.

Event storage

Currently, the prototype's adtech does not collect any further metadata about its source or trigger events. It is intentionally left out as it is not defined in the protocol and will be decided by the adtech. Also, the event registration currently is implemented using buttons for registration. This is not the case in a real-life scenario as events can be registered automatically given the user interaction (e.g., ad impression). Also, the registration on the publisher or advertiser website could be implemented dynamically (i.e., iframes[1]) in control of the adtech, which is allowed by the protocol but not relevant to the attribution process. The prototype currently sets no minimum batch size before an attribution can be requested. This is intended by the protocol but is left out to simplify the use of the prototype.

Cryptographic protocol

The homomorphic encryption mechanism applied to the match key and processed in the MPC is based on simple arithmetic operations and the use of a pair of private and public key[2]. The encryption details for the MPC are set constant, but can be configured (i.e., *resources/application.yml*). Furthermore, the client's randomising factor is a value between $1 - 5$ (i.e., *contentscript.js*). The prototype does not intend to provide any means of security. Instead, it intends to illustrate the mechanism by communicating critical encryption factors between the parties and by showing the required functionality of each party. Furthermore, the actual encryption mechanism, as well as its configuration, is not detailed in the protocol.

External processing environment

The prototype currently has a separate MPC web server, managing the leader and helper servers. Since there were tasks (e.g., preparation of the joint threshold public key of the helper servers) which were not associated with any role, these were allocated to a central web server. Clarification of the MPC architecture and its functionality is required. Also, the minimum batch size is currently not restricted and requires definition, as it likely becomes

---

[1]Abbreviation for inline frame, which is an HTML tag used to embed another HTML context on the current website. Commonly used to automatically display advertisement coordinated by an adtech on the publisher's website.

[2]See chapter 4 for more information on the applied basic encryption mechanism.

too easy to re-identify a client in small batches even after aggregation. Furthermore, the blinding mechanism is sparsely defined. The prototype currently implements a random blinding factor per helper server per request. However, details on the blinding factor generation and the applied arithmetic function are required. The processing of secret shared values in the MPC is also not defined. It is unclear which algorithm is used to process the data between the helper servers involving secret shares. Lastly, it must be mentioned that the current deployment of the MPC does not reflect the intended setup. It is planned to have one or more independent companies running the MPC's servers for the separation of concerns.

Differential Privacy

Differential privacy as a key protocol design remaining untouched in the prototype. The provided information on the implementation of noise to the aggregation result has been high-level only. Also, the application of differential privacy requires a budget per match key to restrict the data leakage of a single user to a threshold. The protocol describes that the MPC will be responsible for keeping a state of the remaining budget per match key across several requests. This is an area where further details are required. Implementing such a database seems contradictory as the MPC would be required to recognise the same match key across requests.

IPA does not include any specification on reporting delay or rate limits. Hence, no separate limitations are being discussed.

5.2.3   Prototype and code availability

The IPA prototype is deployed and can be accessed online via the following websites. Note that the adtech and MPC components are not directly accessible via domain as it runs in the background upon attribution request.

- `https://simulation.v3e.org` - represents the landing page of the master project with links to the corresponding websites of the simulation; no IPA-specific functionality is provided

- `https://simulation.v3e.org/matchkeyprovider` - represents the match key provider, which calls the client API to set an identifier to the client storage upon user log-in

- `https://simulation.v3e.org/pub` - represents an exemplary publisher domain, which will call the client API to fetch the encrypted match key and will register and send a source event to the adtech

- `https://simulation.v3e.org/adv` - represents an exemplary advertiser domain, which will call the client API to fetch the encrypted match key and will register and send a trigger event to the adtech

- `https://simulation.v3e.org/adtech` - represents the adtech collecting all event data of its associated publisher and advertiser domains, requests attribution with the MPC and will receive responses

The source code of the IPA prototype implementation can be obtained from `https://github.com/effectLX/msc_ipa_prototype`. Here the full implementation of the front end, back end and deployment are provided as described before. The structure of the code largely echoes the stakeholders in the protocol. Please refer to the included *README.md* for instructions on how to set up the prototype locally, if needed.

5.3   Usage of the prototype

The prototype can be used in a real-life simulation using the deployed web application. For this, the bare navigation between the publisher's and advertiser's website will create source and trigger events, which will be propagated to the adtech. As soon as ten (i.e., current assumption of the prototype) events have been stored with the adtech, the attribution request will be sent to the MPC, which will return the corresponding result. The client API call can be implemented on any website to simulate a publisher or advertiser website. For this, the following code must be included to *FETCH* the match key from the client in your website's source code. It requires the chrome extension to be set up with the client.

```
1 let data = { type: "FETCH", text: urlToPostMessage };
2     window.postMessage(data, "*");
```

If this code is executed in the browser, a fetch request will be posted between the windows to the client asking to return the match key. *urlToPostMessage* specifies the current website (i.e., locally it is *http://localhost:3000/*). The client will return the match key by posting a *RETURN_KEY* message, which must be caught in the website's context. For this, include the corresponding event listener in the web page's source code.

```
1  useEffect (() => {
2     window.addEventListener("message", handleMessageEvent);
3     return () => {
4       window.removeEventListener("message", handleMessageEvent);
5     };
6   }, []);
7
8   const handleMessageEvent = async (event) => {
9     if (event.source !== window) return;
10
11    // Receive match key from client
12    if (event.data.type && event.data.type === "RETURN_KEY") {
13      const encryptedData = event.data.text;
14      registerEventWithAdtech(encryptedData);
15    }
16  };
```

The *RETURN_KEY* message's body will provide the encrypted match key to register an event with the associated adtech (i.e., *urlToFetch*) for storage. For this, the event body must be defined, including the encrypted match key, and an HTTP POST must be sent.

```
1  let registerEventWithAdtech = (encryptedData) => {
2     let data = JSON.parse(encryptedData);
3
4     let event = {
5       type: "SOURCE",
6       matchKey: data.encryptedMatchKey,
7       clientKey: data.clientKey,
8       timestamp: moment().toISOString(),
9     };
10
11    const requestOptions = {
12      method: "POST",
```

```
13        headers: { "Content-Type": "application/json" },
14        body: JSON.stringify(event),
15      };
16
17      fetch(urlToFetch, requestOptions).catch((error) => {
18        console.error(error);
19      });
20    };
```

Further, the prototype can be set up locally by running the application on a *localhost*. Here, the adtech or MPC endpoint to request attribution can be reached direclty with a JSON file of event objects. This way, the whole front end simulation is skipped, and the back end can be tested in isolation. For this, an HTTP POST must be sent like in the following example:

```
1 POST http://localhost:8080/attribution
2 Accept: application/json
3 Content-Type: application/json
4
5 [
6   {
7     "type": "SOURCE",
8     "matchKey": "1234",
9     "clientKey": "10",
10    "timestamp": "2022-08-31T10:00:00"
11  },
12  {
13    "type": "TRIGGER",
14    "matchKey": "1234",
15    "clientKey": "20",
16    "timestamp": "2022-08-31T11:00:00"
17  },
18 ]
```

To call the MPC endpoint directly with a batch of events, the data must comply with the MPCs requirements. Hence, the timestamp must match the Java's LocalDateTime format. The match key must be encrypted and randomised using the MPC's public key and an individual random value R. And the client value (i.e., g^R) must be derived from the

MPC's encryption factor g and the client's random value R.

5.4   Evaluation of the prototype

The prototype's goal was to develop a working source code based on the IPA proposal to drive discussion and improvement of the protocol. For this, objectives were defined to guide the development of the source code. In the following, we will briefly discuss the quality of the prototype along these objectives.

- **Adaptability** - In the development, we generally focused on the back end and less on the front end. Since the MPC is the heart of the protocol and the front end is likely implemented differently in the future, this focus seemed reasonable. For example, we have decided to build a chrome extension which simulates the browser's API only. This will be replaced in the future as it merely mimics the IPA API, which will be built into the browser directly. For the back end, we decided to build a clean source code based on the principle of clean architecture. In retrospect, the decision was beneficial, as it allowed new findings from the proposal to be easily implemented in the code throughout development. The flexibility created herewith will also be positive for subsequent further developments. The proposal will bring adaptations that can be easily implemented based on our architecture, which will keep the prototype up to date. The entire tech stack of the prototype is primarily composed of technologies that are largely considered an industry standard. Thus, the hurdle to using the source code should be as low as possible.

- **Completeness** - In general, a complete and working prototype has been developed based on the current IPA protocol. It provides a detailed understanding of the mode of operation of the protocol covering all roles involved along the IPA process. However, not all specifics of the protocol were implemented, which was elaborated in the limitations. This is because the protocol is still insufficiently defined in many places and is rather the first idea of a concept. With the idea of providing a first functioning prototype as close as possible to the actual protocol, assumptions on undefined specifications were avoided (e.g. Differential Privacy). It is assumed that the code could be developed as soon as the limitations are resolved conceptually.

- **Accessibility** - The prototype is accessible as a deployed web application and a local setup. Both have advantages which suit specific use cases. First, the deployed web application can be used by anyone who wants to test or demonstrate the prototype in a real scenario. It can be accessed by going onto `https://simulation.v3e.org`, which provides all relevant links. This demonstration allows us to experience the IPA protocol as it is currently intended, which might be especially useful as a start to understand the protocol's working. Moreover, this can be further advanced by incorporating the IPA API calls to any other website to let them communicate with the client extension. Second, the local setup helps anyone dive into the technical details of the IPA protocol. This local setup can be accessed via `https://github.com/effectLX/msc_ipa_prototype`. Here the installation of the local IPA is explained, which then allows the building of specific test cases on key designs of the protocol, such as the MPC.

- **Robustness** - We have tried to build a robust prototype using clean architecture, which helped avoid errors in the first place. Furthermore, we have added basic error handling to the prototype to reduce unknown edge cases of the prototype and avoid unwanted crashes of the tool. As this is a prototype only, there is still room for further improvement. We have added one exemplary test (i.e., *BlindEventTest.java*) to showcase that the back end's functionality can be easily tested. Here, the prototype can be further improved to offer a complete test coverage as soon as the functionality of the IPA is finalised and the prototype evolves.

In general, we think the prototype is of solid quality, ensuring that it can contribute to future work on the IPA protocol. Especially with this report, we think the provided source code is beneficial for demonstrations and further development.

Chapter 6

Conclusion and future work

In the following, we comment on this project's legal and ethical considerations. Then we provide a summary of the key findings of this report. Finally, briefly discuss what we see as essential topics for future work to further research on cookieless attribution.

6.1   Legal and ethical considerations

The technical details of PCM, ARA and IPA summarised in the report are based on the published and publicly discussed proposals. The intellectual property belongs to the companies mentioned above and the developers behind them. We do not claim the architecture and design choices of the aforementioned protocols. As of submission of this report, the latest state of the published proposals has been used as a reference. In addition, and to the best of our knowledge, we have included the community's ongoing discussions based on these published proposals. We do not claim to have fully considered all discussions that are not part of the official proposals. A prototype of the IPA protocol was developed during the project. We do not claim that the source code is ready for production. The current state of the prototype is only for demonstration and testing of the protocol. Using the source code and creating a production-ready application is the sole responsibility of Meta and Mozilla and their respective developers. Finally, aspects concerning protecting the individual's privacy regarding legal requirements have been considered throughout this report.

6.2 Conclusion

This report includes four contributions we hope will support future research. First, we summarised a brief overview of the existing state of research in web tracking. Second, we described the three most relevant proposed solutions for attribution modelling without third-party cookies and approached the technical design choices in a structured way. Third, we analysed the current attack space of the IPA proposal and identified potential security risks. Finally, we developed and deployed a first working IPA prototype for demonstration.

We identified four general trends in the research published since 2010. First, the research focused on creating transparency about tracking mechanisms and stakeholders in web tracking. Second, the limited possibilities an individual has to detect and avert web tracking were analysed and discussed. Third, the rising changes to the legal landscape to curb privacy loss and its impact on web tracking were investigated. Fourth, the research focused on finding new tracking solutions balancing the user's privacy and the industry's utility. The research published to date highlights a stringent pathway for today's debate around privacy-preserving tracking and reinforces the discussion on cookieless attribution.

We identified the common key design choices in the system architectures of the cookieless attribution protocols. Those allowed us to have a brief privacy and utility discussion at the level of the individual design choices between the proposals. It became apparent that PCM offers a simple solution that prioritises privacy but severely limits the options available to the advertising industry. ARA and IPA offer a starting point for privacy- and utility-promising systems based on either client- or server-sided attribution. However, further clarification is needed, especially on the external processing environments in the discussion, to evaluate the extent to which privacy and security can be guaranteed. Generally, the protocols provide limited information on technical details (i.e., PCM and ARA) or are still in early-phase discussions of the overall design (i.e., IPA).

We have analysed the attack space of the IPA protocol and identified an attack (i.e., "Unilateral Blinding Reveal") on the system. In our opinion, a malicious leader server could

expose the pseudonymous identity behind the data of an adtech's request by interspersing fake evens in the regular attribution process, bypassing the blinding effort. It would undermine the protocol's goal of obfuscating information and facilitating user profiling. Mitigation and limitations based on this attack are discussed.

We have developed the first working prototype of the IPA protocol. The aim was to complement the already existing test environments for PCM and ARA with the IPA prototype to increase the systems' comparability. The prototype primarily demonstrates and simulates the protocol and should contribute to increased understanding. The prototype was developed as closely as possible to the protocol. It allowed us to identify specific gaps in the description of the system, where further clarification of Meta/ Mozilla is needed. The high reusability and adaptability of the source code should allow adjusting the prototype for future discussions.

Overall, the three concepts are openly discussed and aligned across the proposal's authors, which is an asset for the discussion. In our opinion, any solo efforts by regulators, browsers, or the industry should be avoided. Otherwise, one side's interests might be shortchanged, leading to unsatisfactory results. Furthermore, it must be stressed that these proposals are a piece of a puzzle in the overall discussion on privacy preservation in online advertisement. The protocols will not stop potential privacy loss through tracking mechanisms such as fingerprinting or IP address tracking. A joint effort of new tracking mechanisms with improved legal and browser regulations is needed.

6.3 Future work

In support of the ongoing discussions on the development of cookieless attribution, we see the following research areas as targeted additions: First, an in-depth analysis of the current design choices would be helpful. In particular, a conclusive opinion on privacy preservation via client- vs server-sided attribution and the final setup of the external processing environment (i.e., TEE vs MPC) would be helpful. Second, given provided details on the implementation of differential privacy in ARA and IPA, a data-driven evaluation could be conducted to optimally tune the degree of noise depending on the aggregation of

the data. Third, a detailed analysis of the attack space on PCM and ARA would be conceivable. Those proposals are already advanced but could still contain security risks that have not yet been identified. Likewise, the IPA attack space analysis could be reevaluated when an update of the proposal is published. Fourth, a comprehensive view of the limitations of future attribution, given the application of the three proposals, is worthwhile. For this purpose, the three existing prototypes would lend themselves to be applied in real-world scenarios.

List of references

[1] Martin K. Data Aggregators, Consumer Data, and Responsibility Online: Who is Tracking Consumers Online and Should They Stop. The Information Society. 2015 01;32. DOI:10.1080/01972243.2015.1107166. pages VI, 4, 5

[2] Ahmed RK, Mohammed IJ. Developing a New Hybrid Cipher Algorithm using DNA and RC4. International Journal of Advanced Computer Science and Applications. 2017;8(10). DOI:10.14569/IJACSA.2017.081023. pages VI, 25

[3] Martin RC. The Clean Architecture; 2012. Available from: `https://blog.cleancoder.com/uncle-bob/2012/08/13/the-clean-architecture.html` [cited 2022/08/25]. pages VI, 53, 54

[4] Szymański M, Rathman K. As Internet user numbers swell due to pandemic, UN Forum discusses measures to improve safety of cyberspace - United Nations Sustainable Development. 2021 12. Available from: `https://www.un.org/sustainabledevelopment/blog/2021/12/as-internet-user-numbers-swell-due-to-pandemic-un-forum-discusses-measures-to-improve-safety-of-cyberspace/` [cited 2022/07/24]. pages 1

[5] Chen Q, Ilia P, Polychronakis M, Kapravelos A. Cookie swap party: Abusing first-party cookies for web tracking; 2021. DOI:10.1145/3442381.3449837. pages 1, 8

[6] Papadogiannakis E, Papadopoulos P, Kourtellis N, Markatos EP. User tracking in the post-cookie era: How websites bypass gdpr consent to track users; 2021. DOI:10.1145/3442381.3450056. pages 1, 8

[7] Castell-Uroz I, Sole-Pareta J, Barlet-Ros P. TrackSign: Guided web tracking discovery. vol. 2021-May; 2021. DOI:10.1109/INFOCOM42981.2021.9488842. pages 1, 6

[8] UNCTAD. Data Protection and Privacy Legislation Worldwide — UNCTAD. 2021 12. Available from: `https://unctad.org/page/data-protection-and-privacy-legislation-worldwide` [cited 2022/07/24]. pages 1

[9] Markit I. THE ECONOMIC VALUE OF BEHAVIOURAL TARGETING IN DIGITAL ADVERTISING 2 CONTENTS; 2019. Available from: `https://iabeurope.eu/knowledgehub/policy/the-economic-value-of-data-driven-advertising/`. pages 1

[10] Mayer JR, Mitchell JC. Third-party web tracking: Policy and technology; 2012. DOI:10.1109/SP.2012.47. pages 3, 10, 11

[11] Nikiforakis N, Kapravelos A, Joosen W, Kruegel C, Piessens F, Vigna G. Cookie-less monster: Exploring the ecosystem of web-based device fingerprinting; 2013. DOI:10.1109/SP.2013.43. pages 3

[12] Acar G, Eubank C, Englehardt S, Juarez M, Narayanan A, Diaz C. The web never forgets: Persistent tracking mechanisms in the wild; 2014. DOI:10.1145/2660267.2660347. pages 3

[13] Bujlow T, Carela-Espanol V, Lee BR, Barlet-Ros P. A Survey on Web Tracking: Mechanisms, Implications, and Defenses. Proceedings of the IEEE. 2017;105. DOI:10.1109/JPROC.2016.2637878. pages 3, 6, 10

[14] Takano Y, Ohta S, Takahashi T, Ando R, Inoue T. MindYourPrivacy: Design and implementation of a visualization system for third-party Web tracking; 2014. DOI:10.1109/PST.2014.6890923. pages 4

[15] Agarwal L, Shrivastava N, Jaiswal S, Panjwani S. Do not embarrass: Re-examining user concerns for online tracking and advertising; 2013. DOI:10.1145/2501604.2501612. pages 4

[16] Hamed A, Ayed HKB. Privacy scoring and users' awareness for Web tracking; 2015. DOI:10.1109/IACS.2015.7103210. pages 4

[17] Gill P, Erramilli V, Chaintreau A, Krishnamurthy B, Papagiannaki D, Rodriguez P. Follow the money understanding economics of online aggregation and advertising; 2013. DOI:10.1145/2504730.2504768. pages 4

[18] Castell-Uroz I, Sole-Pareta J, Barlet-Ros P. Network Measurements for Web Tracking Analysis and Detection: A Tutorial. IEEE Instrumentation and Measurement Magazine. 2020;23. DOI:10.1109/MIM.2020.9289071. pages 5

[19] Yu Z, Macbeth S, Modi K, Pujol JM. Tracking the trackers. 25th International World Wide Web Conference, WWW 2016. 2016:121-32. DOI:10.1145/2872427.2883028. pages 5

[20] Cozza F, Guarino A, Isernia F, Malandrino D, Rapuano A, Schiavone R, et al. Hybrid and lightweight detection of third party tracking: Design, implementation, and evaluation. Computer Networks. 2020;167. DOI:10.1016/j.comnet.2019.106993. pages 5

[21] Le H, Fallace F, Barlet-Ros P. Towards accurate detection of obfuscated web tracking; 2017. DOI:10.1109/IWMN.2017.8078365. pages 6

[22] Isaak J, Hanna MJ. User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. Computer. 2018;51. DOI:10.1109/MC.2018.3191268. pages 6

[23] Narayanan A, Huey J, Felten EW. A Precautionary Approach to Big Data Privacy; 2016. DOI:10.1007/978-94-017-7376-8_13. pages 6, 33

[24] Budak C, Goel S, Rao J, Zervas G. Understanding emerging threats to online advertising; 2016. DOI:10.1145/1234567.1234567. pages 6, 42

[25] Samarasinghe N, Mannan M. Towards a global perspective on web tracking. Computers and Security. 2019;87. DOI:10.1016/j.cose.2019.101569. pages 7

[26] Jakobi T, Stevens G, Seufert AM, Becker M, Grafenstein MV. Web Tracking under the New Data Protection Law: Design Potentials at the Intersection of Jurisprudence and HCI. i-com. 2020;19. DOI:10.1515/icom-2020-0004. pages 7

[27] Urban T, Tatang D, Degeling M, Holz T, Pohlmann N. Measuring the Impact of the GDPR on Data Sharing in Ad Networks; 2020. DOI:10.1145/3320269.3372194. pages 7

[28] Kretschmer M, Pennekamp J, Wehrle K. Cookie Banners and Privacy Policies: Measuring the Impact of the GDPR on the Web. ACM Transactions on the Web. 2021;15. DOI:10.1145/3466722. pages 7

[29] Amarasekara BR, Mathrani A, Scogings C. Online Tracking: When Does it Become Stalking? Vietnam Journal of Computer Science. 2021;8. DOI:10.1142/S2196888821500226. pages 7

[30] Deuser C, Passmann S, Strufe T. Browsing unicity: On the limits of anonymizing web tracking data. vol. 2020-May; 2020. DOI:10.1109/SP40000.2020.00018. pages 8, 22

[31] Cassel D, Lin SC, Buraggina A, Wang W, Zhang A, Bauer L, et al. OmniCrawl: Comprehensive Measurement of Web Tracking With Real Desktop and Mobile Browsers. Proceedings on Privacy Enhancing Technologies. 2022;2022. DOI:10.2478/popets-2022-0012. pages 8

[32] Yang Z, Yue C. A Comparative Measurement Study of Web Tracking on Mobile and Desktop Environments. Proceedings on Privacy Enhancing Technologies. 2020;2020. DOI:10.2478/popets-2020-0016. pages 8

[33] Krupp B, Hadden J, Matthews M. An Analysis of Web Tracking Domains in Mobile Applications; 2021. DOI:10.1145/3447535.3462507. pages 9

[34] Pestana G. THEMIS: A Decentralized Privacy-Preserving Ad Platform with Reporting Integrity; THEMIS: A Decentralized Privacy-Preserving Ad Platform with Reporting Integrity. 2021 6. Available from: `https://doi.org/10.48550/arXiv.2106.01940`. pages 9

[35] Servan-Schreiber S, Hogan K, Devadas S. AdVeil: A Private Targeted Advertising Ecosystem. Cryptology ePrint Archive. 2021. Available from: `https://eprint.iacr.org/2021/1032`. pages 9

[36] Competition & Markets Authority. Online platforms and digital advertising; 2020. Available from: `www.nationalarchives.gov.uk/doc/open-government-`. pages 9

[37] About Attribution - Analytics Help; 2022. Available from: `https://support.google.com/analytics/answer/9397590?hl=en#zippy=%5C%2Cin-this-article` [cited 2022/08/12]. pages 10, 35

[38] EUROPEAN DATA PROTECTION SUPERVISOR. DIRECTIVE 2009/136/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. Official Journal of the European Union. 2009 11. Available from: `https://edps.europa.eu/sites/default/files/publication/dir_2009_136_en.pdf`. pages 11

[39] EUROPEAN DATA PROTECTION SUPERVISOR. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. Official Journal of the European Union. 2016 4. Available from: `https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679`. pages 11

[40] O'Reilly L. Google Pushes Back Plan to Ditch Third-Party Cookies in Chrome to 2023; 2021. Available from: `https://www.businessinsider.com/google-pushes-back-phase-out-cookies-chrome1-year-2023-2021-6?r=US&IR=T` [cited 2022/08/18]. pages 11

[41] Wilander J. Full Third-Party Cookie Blocking and More — WebKit; 2020. Available from: `https://webkit.org/blog/10218/full-third-party-cookie-blocking-and-more/` [cited 2022/08/18]. pages 11

[42] Mozilla. Firefox Rolls Out Total Cookie Protection By Default To All Users; 2022. Available from: `https://blog.mozilla.org/en/products/firefox/firefox-rolls-out-total-cookie-protection-by-default-to-all-users-worldwide/` [cited 2022/08/18]. pages 11

[43] Danezis G, Domingo-Ferrer J, Hansen M, Hoepman JH. Privacy and Data Protection by Design-from policy to engineering Privacy and Data Protection by Design-from policy to engineering About ENISA. European Union Agency for Network and Information Security. 2014 12. DOI:10.2824/38623. Available from: `http://www.un.org/en/documents/udhr/`. pages 12

[44] Private Click Measurement Discussion Forum; 2022. Available from: `https://github.com/privacycg/private-click-measurement` [cited 2022/08/10]. pages 12, 14

[45] Attribution Reporting API Discussion Forum; 2022. Available from: `https://github.com/WICG/attribution-reporting-api` [cited 2022/08/10]. pages 12

[46] Interoperable Private Attribution Discussion; 2022. Available from: `https://github.com/patcg/private-measurement` [cited 2022/08/28]. pages 12, 17

[47] Salinas S, Meredith S. Full text of Apple CEO Tim Cook's keynote in Brussels. CNBC. 2018 10. Available from: `https://www.cnbc.com/2018/10/24/apples-tim-cook-warns-silicon-valley-it-would-be-destructive-to-block-strong-privacy-laws.html`. pages 13

[48] Statcounter. Browser Market Share Worldwide — Statcounter Global Stats; 2022. Available from: `https://gs.statcounter.com/browser-market-share`. pages 13

[49] Davenport C. Mozilla and Meta (Facebook) are now actually working together. XDA. 2022 2. Available from: `https://www.xda-developers.com/mozilla-meta-interoperable-private-attribution/`. pages 13

[50] Wilander J. Privacy Preserving Ad Click Attribution For the Web — WebKit; 2019. Available from: `https://webkit.org/blog/8943/privacy-preserving-ad-click-attribution-for-the-web/` [cited 2022/08/10]. pages 14

[51] Wilander J. Introducing Private Click Measurement, PCM — WebKit; 2021. Available from: `https://webkit.org/blog/11529/introducing-private-click-measurement-pcm/` [cited 2022/08/10]. pages 14

[52] Wilander J. Private Click Measurement, Draft Community Report; 2021. Available from: `https://privacycg.github.io/private-click-measurement/` [cited 2022/08/11]. pages 14

[53] Dutton S. What is the Privacy Sandbox? - Chrome Developers; 2021. Available from: `https://developer.chrome.com/docs/privacy-sandbox/overview/` [cited 2022/08/10]. pages 15

[54] Nalpas M, Dutton S, White A. Attribution Reporting - Chrome Developers; 2021. Available from: `https://developer.chrome.com/docs/privacy-sandbox/attribution-reporting/` [cited 2022/08/11]. pages 15

[55] Nalpas M, White A. Attribution Reporting proposal updates in January 2022 - Chrome Developers; 2022. Available from: `https://developer.chrome.com/blog/attribution-reporting-jan-2022-updates/` [cited 2022/08/11]. pages 15

[56] Harrison C, Delaney J, Paseltiner A. Attribution Reporting, Draft Community Report; 2022. Available from: `https://wicg.github.io/attribution-reporting-api/` [cited 2022/08/11]. pages 15

[57] Taubeneck E, Savage B, Thomson M. Interoperable Private Attribution (IPA); 2022. Available from: `https://docs.google.com/document/d/1KpdSKD8-RnObWPTu4UtK54ks0yv2j22pA5SrAD9av4s/edit#` [cited 2022/08/28]. pages 17, 42

[58] Li XB, Sarkar S. Privacy protection in data mining: A perturbation approach for categorical data. Information Systems Research. 2006;17. DOI:10.1287/isre.1060.0095. pages 22

[59] Kessler GC. An Overview of Cryptography (Updated Version, 3 March 2016). 2016 3. Available from: `https://commons.erau.edu/publication/127`. pages 25

[60] Ghouse M, Nene MJ, VembuSelvi C. Data Leakage Prevention for Data in Transit using Artificial Intelligence and Encryption Techniques; 2019. DOI:10.1109/ICAC347590.2019.9036839. pages 25

[61] The HTTPS-Only Standard;. Available from: `https://https.cio.gov/` [cited 2022/08/23]. pages 25

[62] Das ML, Samdaria N. On the security of SSL/TLS-enabled applications. Applied Computing and Informatics. 2014;10. DOI:10.1016/j.aci.2014.02.001. pages 25

[63] Felt AP, Barnes R, King A, Palmer C, Bentzel C, Tabriz P. Measuring HTTPS Adoption on the Web. In: Proceedings of the 26th USENIX Conference on Security Symposium. SEC'17. USA: USENIX Association; 2017. p. 1323–1338. pages 25

[64] Fontaine C, Galand F. A survey of homomorphic encryption for nonspecialists. Eurasip Journal on Information Security. 2007;2007. DOI:10.1155/2007/13801. pages 26, 27

[65] Lauter K, Naehrig M, Vaikuntanathan V. Can homomorphic encryption be practical?; 2011. DOI:10.1145/2046660.2046682. pages 26, 27

[66] Callegati F, Cerroni W, Ramilli M. Man-in-the-middle attack to the HTTPS protocol; 2009. DOI:10.1109/MSP.2009.12. pages 26

[67] Acar A, Aksu H, Uluagac AS, Conti M. A survey on homomorphic encryption schemes: Theory and implementation; 2018. DOI:10.1145/3214303. pages 27

[68] Chase M, Chen H, Ding J, Goldwasser S, Gorbunov S, Hoffstein J, et al. SECURITY OF HOMOMORPHIC ENCRYPTION. Microsoft. 2018 1. Available from: `https://www.microsoft.com/en-us/research/wp-content/uploads/2018/01/security_homomorphic_encryption_white_paper.pdf`. pages 27

[69] Sabt M, Achemlal M, Bouabdallah A. Trusted execution environment: What it is, and what it is not. vol. 1; 2015. DOI:10.1109/Trustcom.2015.357. pages 28

[70] Goldwasser S. Multi Party Computations: Past and Present. In: Proceedings of the Sixteenth Annual ACM Symposium on Principles of Distributed Computing. PODC '97. New York, NY, USA: Association for Computing Machinery; 1997. p. 1–6. Available from: `https://doi.org/10.1145/259380.259405`. pages 28

[71] Celi S. A note on Privacy-Preserving Measurements Techniques. 2022 7. Available from: `https://sofiaceli.com/thoughts/ppm-tech-01.pdf`. pages 30, 31, 33

[72] Wood A, Altman M, Bembenek A, Bun M, Gaboardi M, Honaker J, et al. Differential Privacy: A Primer for a Non-Technical Audience. SSRN Electronic Journal. 2019. DOI:10.2139/ssrn.3338027. pages 31, 32, 33

[73] Wright C, Rumsey K. The Strengths, Weaknesses and Promise of Differential Privacy as a Privacy-Protection Framework; 2018. Available from: `https://www.math.unm.edu/~knrumsey/pdfs/projects/DifferentialPrivacy.pdf`. pages 33

[74] Rescorla E. Overview of Interoperable Private Attribution; 2022. Available from: `https://educatedguesswork.org/posts/ipa-overview/` [cited 2022/08/26]. pages 44, 49