



OVERVIEW, MECHANICS, IMPLICATIONS

GOOGLE PAIR

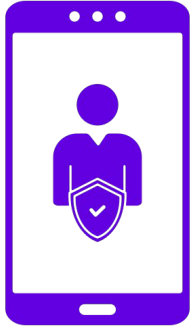
Google PAIR (Publisher Advertiser Identity Reconciliation) is a protocol that allows publishers and advertisers to match first party data for audience targeting on DV360 in a secure, privacy-compliant manner.

PAIR key points

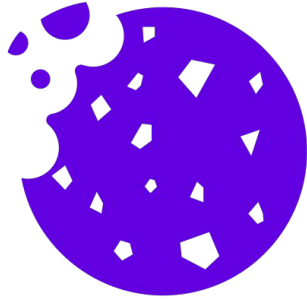
- [Introduced](#) by Google in October 2022.
- Allows advertisers using DV360 to better target known users on partner publisher properties.
- PAIR is a “protocol” connecting Data Clean Rooms to DV360 / SSPs.
 - PAIR is currently integrated with Infosum and LiveRamp/Habu clean rooms.
- Advertisers can only deploy PAIR via DV360 whereas publishers can enable PAIR using any SSP (that’s integrated with DV360).
- IAB Tech Lab [announced](#) industry unified standard version of PAIR¹ in May 2024.

¹ Google contributed PAIR protocol to IAB Tech Lab for further development as an open industry standard.

Why it's important



**Data privacy
regulation &
consumer
concern**



**Decline of
traditional 3P
identifiers**



**The rise of 1P
data collaboration**



**New paradigm for
1:1 audience
targeting**

How PAIR works

Before we begin

PAIR is a process where an input string (ie. an email) has **multiple encryption keys** applied to it. The output of the process is the same for a given input **regardless of the order the keys are applied**. To properly represent this, let's first cover some important terminology and notations.

DATASETS

Represented as emails as PAIR currently only supports email IDs

- **a_Emails** - Advertiser email list
- **p_Emails** - Publisher email list

ENCRYPTION KEYS

PAIR uses 3 encryption keys. They are represented as follows:

- **(A)** = Advertiser key
- **(P)** = Publisher key
- **(S)** = Secret key (generated by Publisher)

ENCRYPTION PROCESS

Each individual encryption step is represented by an asterisk (*).

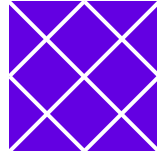
Ex: **a_Emails*(A)*(S)** = Advertiser dataset encrypted using (A) to output a single-encrypted dataset. This is then encrypted again using (S) to output a double-encrypted dataset.

ENCRYPTION STATES

The encryption state (ie. single/double/triple encryption) of the datasets within each data clean room instance is represented like so:



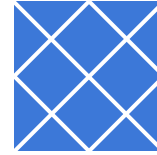
Advertiser
encrypted
(2x)



Advertiser
encrypted
(3x)



Publisher
encrypted
(2x)



Publisher
encrypted
(3x)

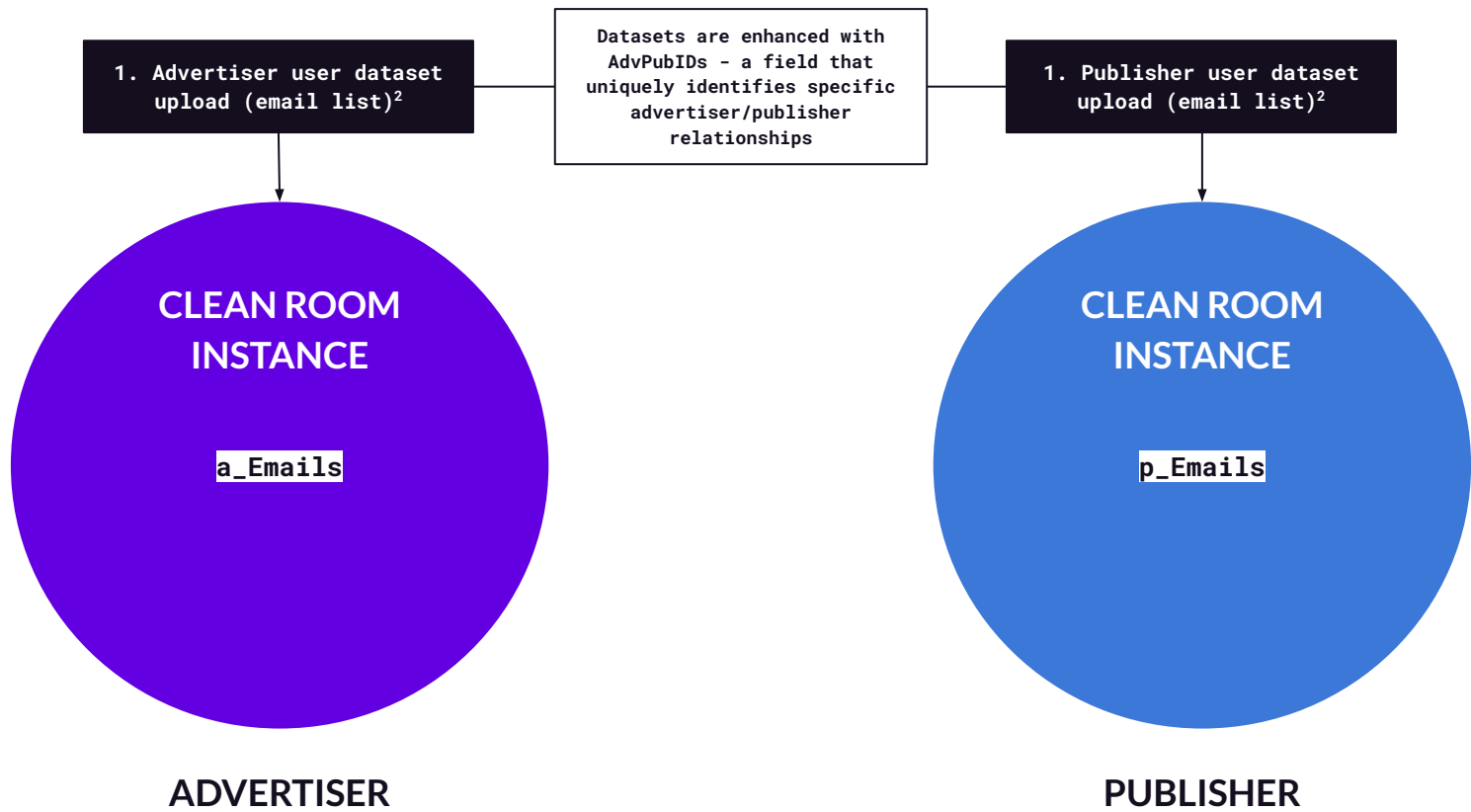
COMMUTATIVE CIPHERS

Commutative = A mathematics term meaning that the outcome of an operation is the same regardless of the order of its elements.

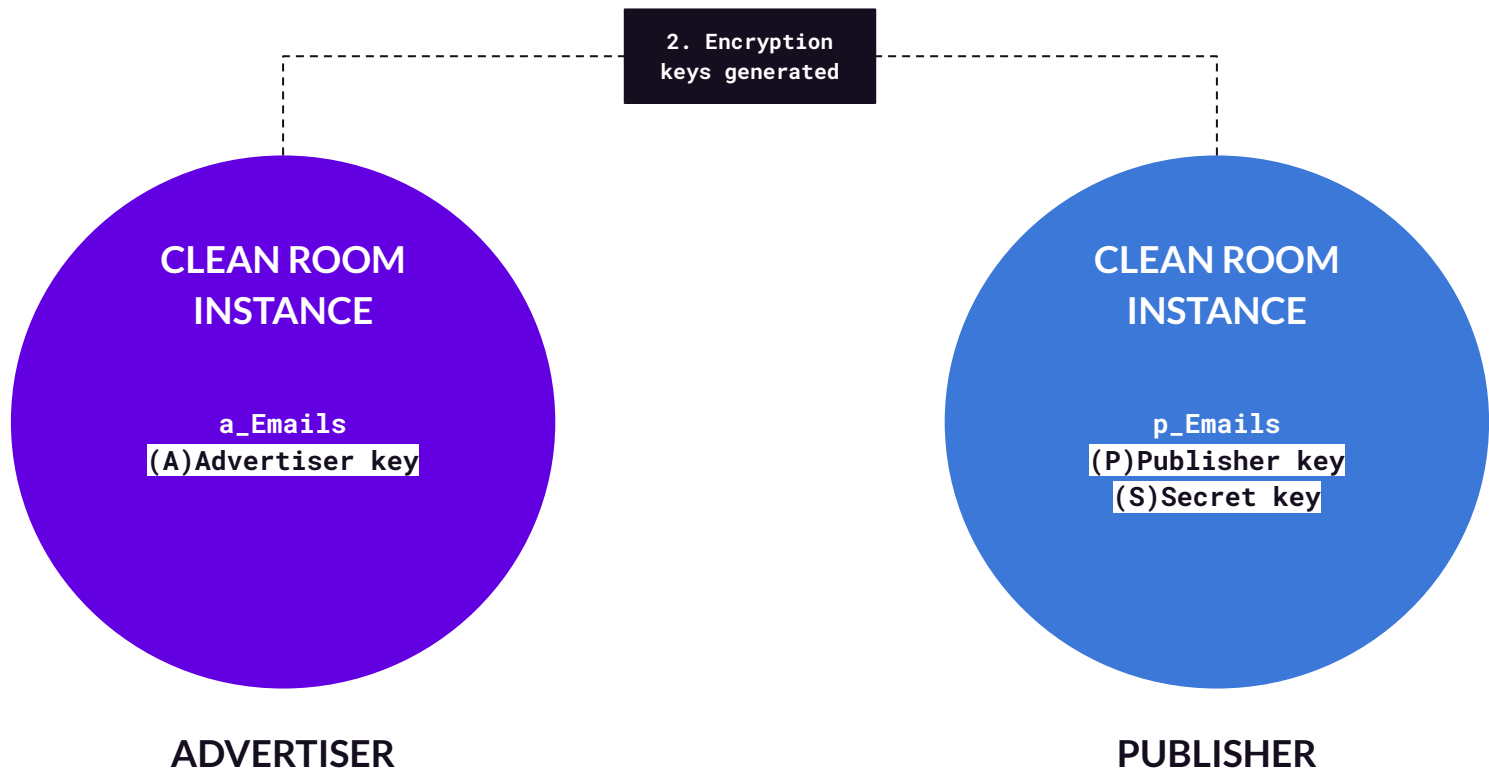
Cipher = A method used in cryptography (ie. an algorithm) for performing encryption or decryption

Taken together, **Commutative Ciphers** is an encryption method where the output is the same for a given input regardless of the order the keys are applied. *Ex: vince@mail.com*(A)*(P) = vince@mail.com*(P)*(A) = Same output*

Protocol walkthrough



² PAIR only supports email IDs at this time



2. Encryption keys generated

CLEAN ROOM INSTANCE

a_Emails

(A)Advertiser key

ADVERTISER

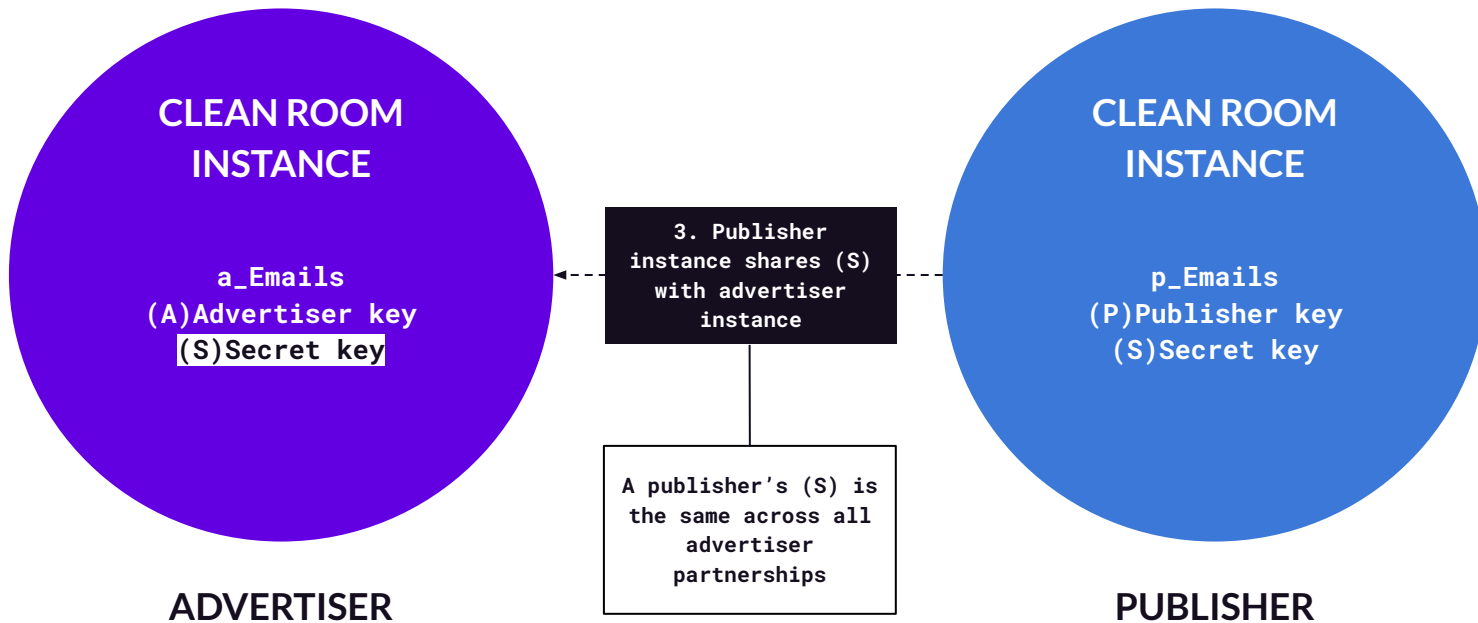
CLEAN ROOM INSTANCE

p_Emails

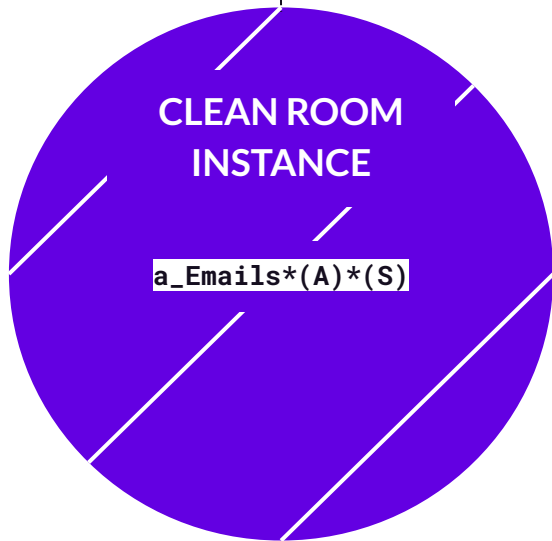
(P)Publisher key

(S)Secret key


PUBLISHER



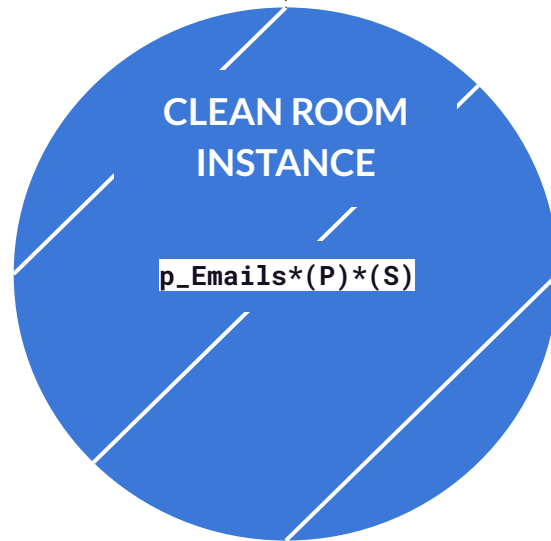
4. Advertiser dataset
encrypted twice with
(A) and (S) keys




ADVERTISER

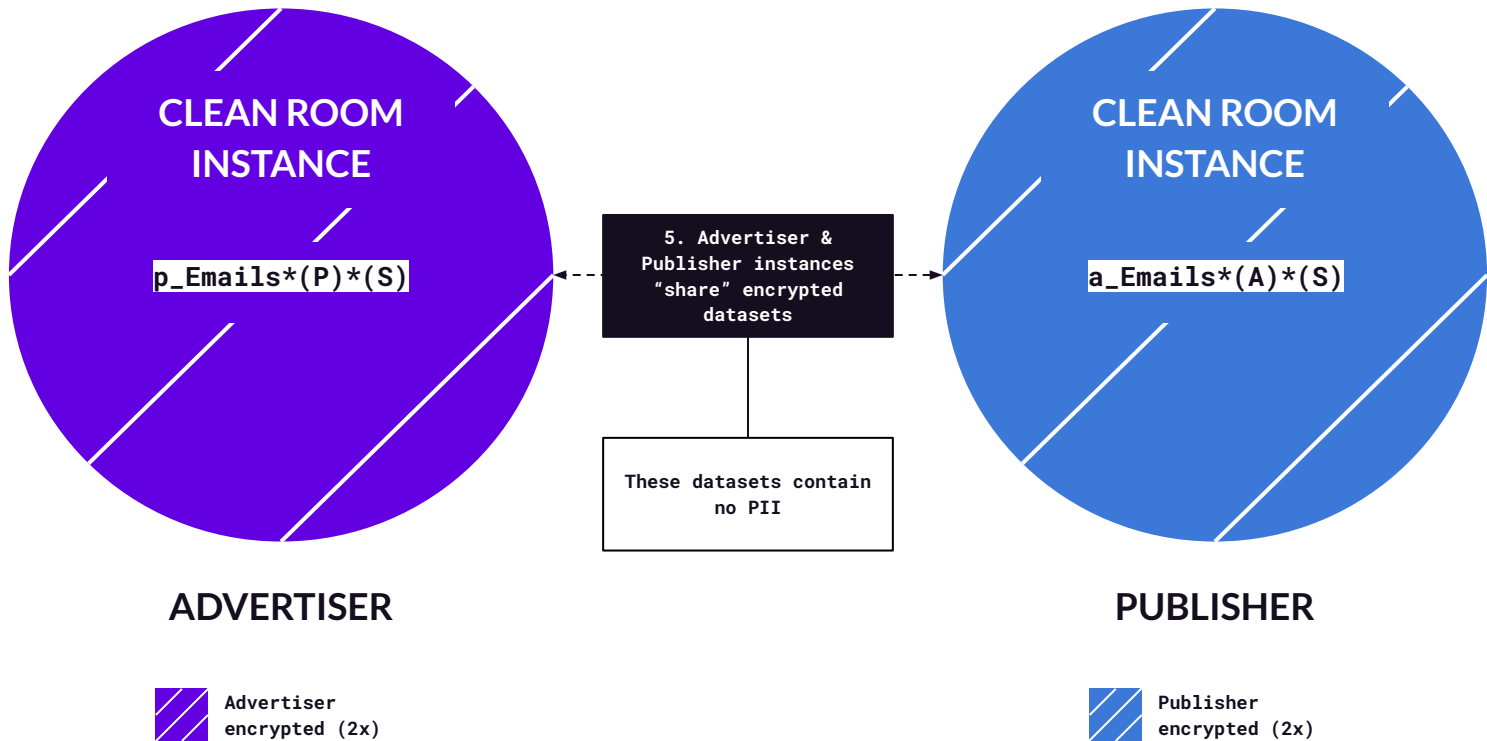
 Advertiser
encrypted (2x)

4. Publisher dataset
encrypted twice with
(P) and (S) keys

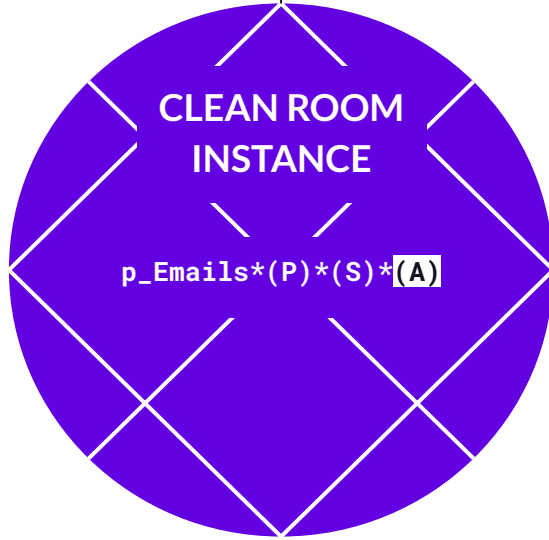


PUBLISHER


 Publisher
encrypted (2x)



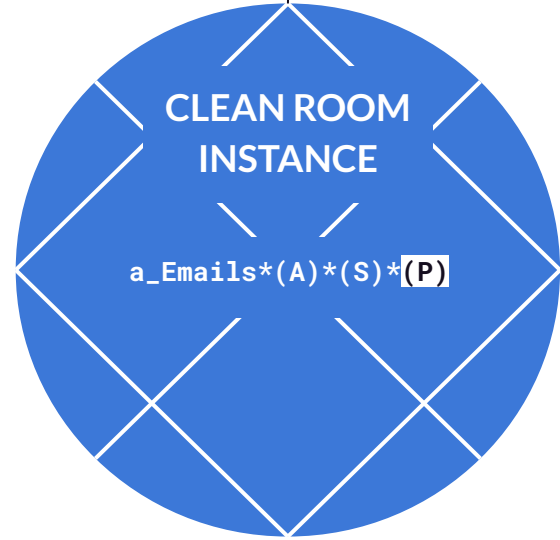
6. Advertiser reapplies (A)
key to shared Publisher
2x encrypted dataset




ADVERTISER

 Advertiser
encrypted (3x)

6. Publisher reapplies (P)
key to shared Advertiser
2x encrypted dataset



PUBLISHER

 Publisher
encrypted (3x)


6. Advertiser reapplies (A)
key to shared Publisher
2x encrypted dataset


6. Publisher reapplies (P)
key to shared Advertiser
2x encrypted dataset

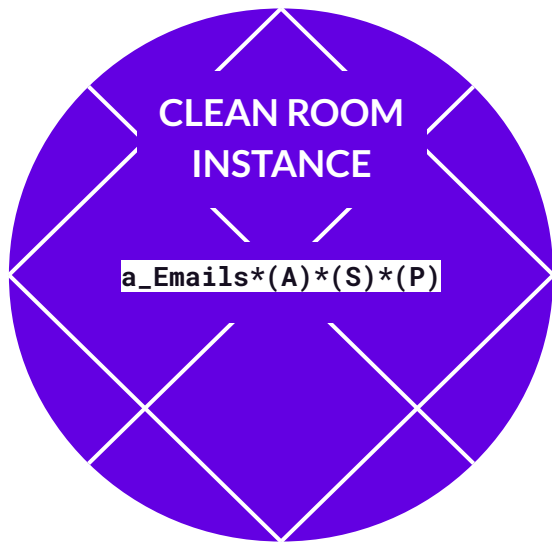
These triple
encrypted datasets
are the **PAIR IDs**.

ADVERTISER


PUBLISHER

 Advertiser
encrypted (3x)

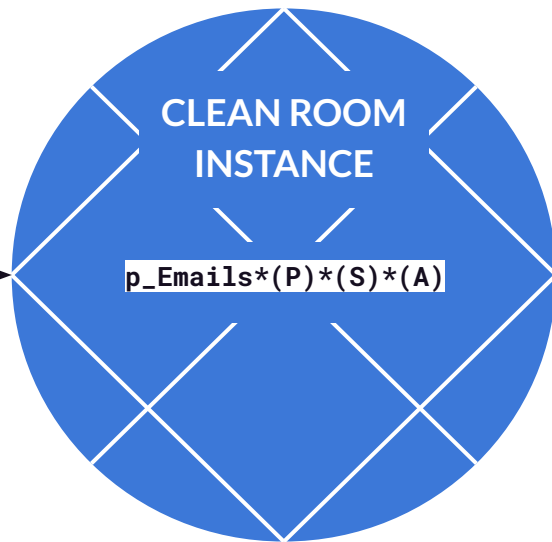
 Publisher
encrypted (3x)




ADVERTISER

 Advertiser
encrypted (3x)

7. Advertiser &
Publisher instances
"share back" PAIR ID
lists with each other



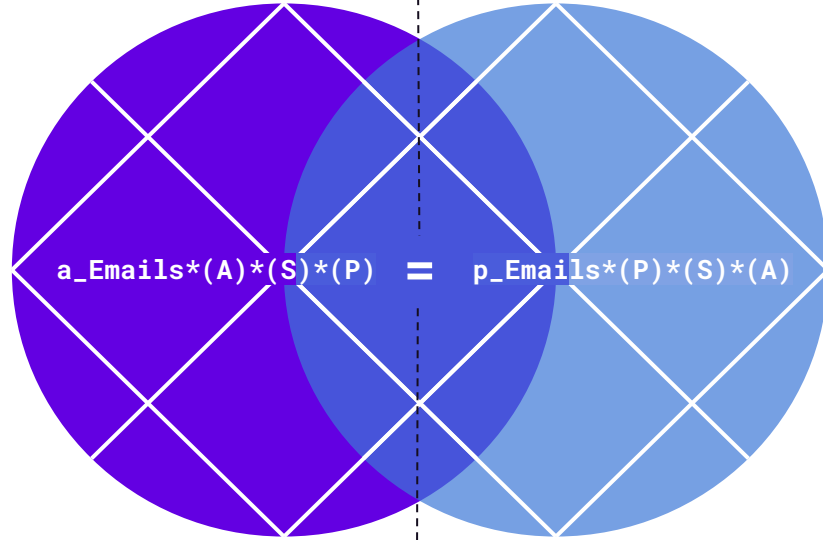
PUBLISHER

 Publisher
encrypted (3x)

Commutative ciphers allow for multiple key encryption to produce same encrypted values regardless of order

8a. PAIR ID matching between Advertiser and Publisher instances takes place

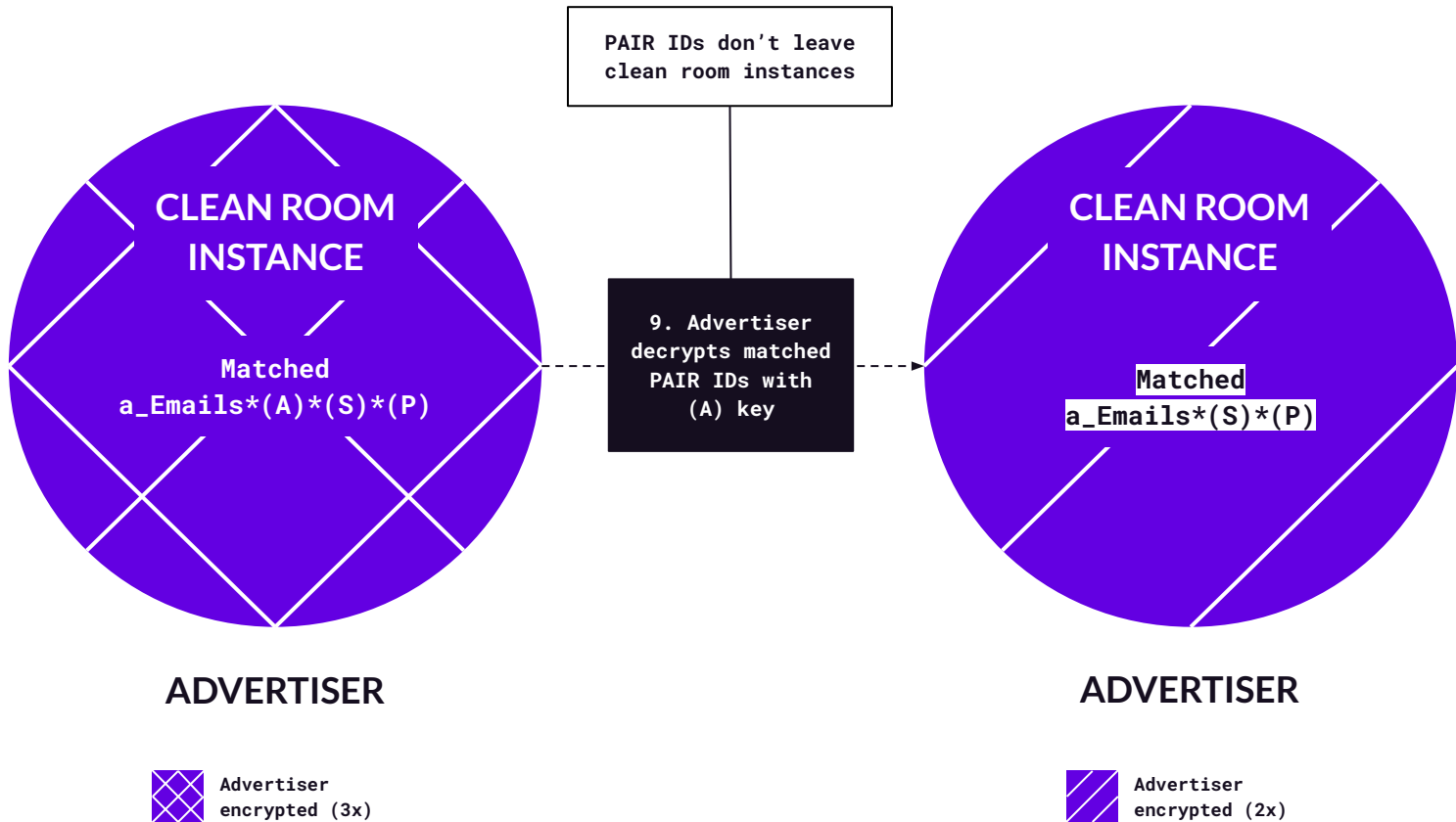
ADVERTISER
CLEAN ROOM
INSTANCE

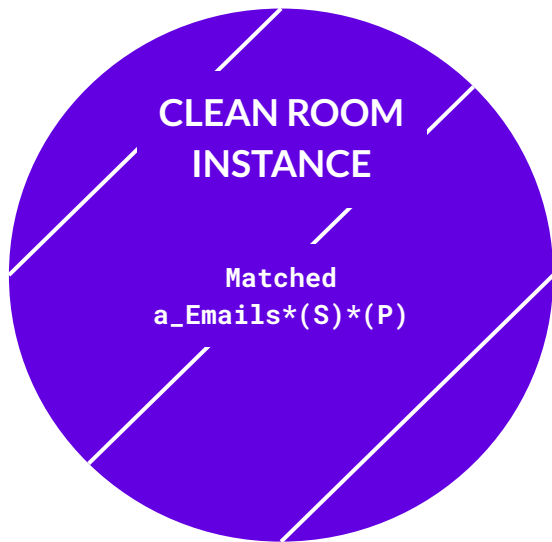


PUBLISHER
CLEAN ROOM
INSTANCE

8b. Matching process produces matched PAIR ID list ie. $a_Emails*(A)*(S)*(P)$

Aggregated match rates are shared with the advertiser and publisher





ADVERTISER

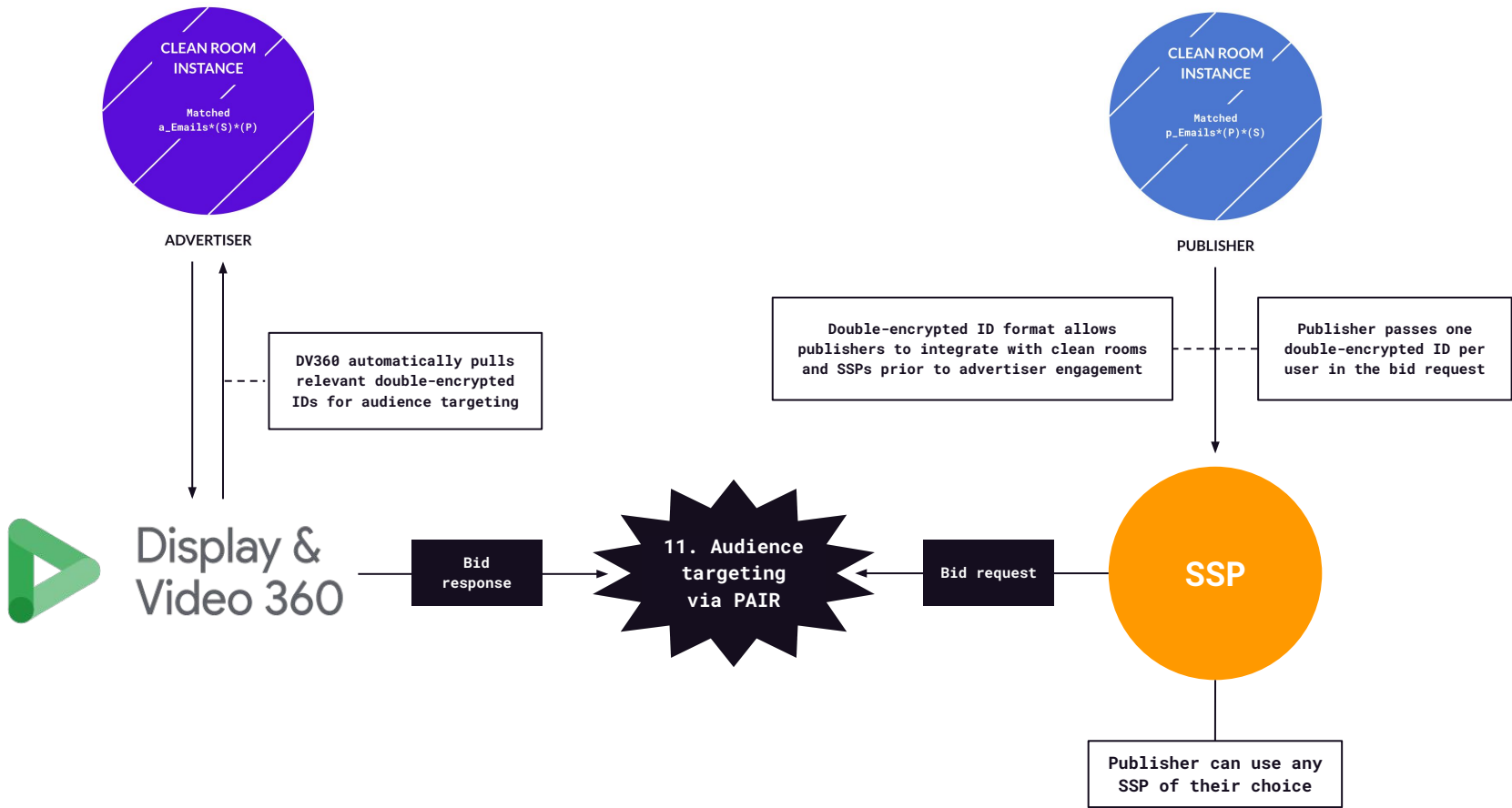
No encryption keys are
shared with DV360

10. Advertiser clean room
permissions DV360 to
access partially
decrypted PAIR IDs

No list or identifier is
downloadable from DV360



Display &
Video 360



PAIR vs other audience targeting solutions

Universal ID solutions

Ex: Unified ID 2.0, ID5, RampID, Panorama ID

Similarities

- Both PAIR and universal IDs can use encrypted emails to facilitate 1:1 audience targeting between advertiser and publishers across devices.
- Both PAIR and universal IDs were created as privacy-safe, post-cookie identity solutions.

Differences

- Universal IDs support not only emails, but also other ID types like phone number, name and address. Some also incorporate probabilistic techniques for enhance matching.
- PAIR is primarily an activation/targeting protocol whereas universal IDs is designed to be used for a wider variety of use cases (e.g. attribution, analytics).
- DV360 is PAIR's (Google-version) only buy-side endpoint whereas universal IDs are DSP agnostic (assuming integration).
- PAIR IDs only work in the context of a single advertiser/publisher relationship whereas universal IDs can be accessed for media targeting across exchanges/networks. This attribute makes PAIR superior at preventing bidstream data leakage.

Direct Hashed ID upload

Ex: Customer Match (Google), Customer List Custom Audience (Meta)

Similarities

- Both PAIR and direct hashed ID upload solutions use encryption techniques to facilitate 1:1 audience targeting without sharing the underlying user data.

Differences

- PAIR matches an advertiser's 1PD against a publisher's 1PD whereas hashed ID upload match an advertiser's 1PD against the platform's ID graph.
- PAIR can be used with any SSP whereas hashed ID upload only works with the platform's owned and operated supply source.³
- PAIR offers more privacy protection because there is no data "pooling" as advertisers and publishers maintain control over their own data. In contrast, hashed ID upload workflows require advertisers to upload their data to a centralized platform (ie. Google, Meta), which can lead to increased privacy risks.

³ As of Mar'24, Google has removed the ability to use Customer Match on non-Google O&O inventory in the EEA. PAIR is filling this use-case void.

Browser-based APIs for audience targeting

Ex: Protected Audience API (Google Chrome), Ad Selection API (Microsoft Edge)

Similarities

- Both PAIR and browser-based APIs are designed to enable audience targeting while protecting user privacy, albeit via very different pathways.

Differences

- PAIR facilitates 1:1 audience targeting whereas browser-based APIs focus on creating/targeting audience (interest) cohorts.
- PAIR (Google version) uses data clean rooms for data matching with DV360/SSPs as the delivery endpoints. Browser-based APIs run the majority (if not all) processes on users' web browser, but can be integrated to work with a variety of adtech platforms.
- PAIR protects against data leakage and pooling by having advertisers and publishers maintain control over their user data. Browser-based APIs protect user data by storing audience information locally on the device and uses on-device signals for ad selection and bidding.

Moving beyond Google

In May 2024, the IAB Tech Lab announced a **unified industry standard version of PAIR** built on the foundations of Google PAIR and existing Tech Lab Privacy Enhancing Technology Working Group initiatives.

IAB Tech Lab
@IABTechLab

#IABTechLab is excited to introduce IAB Tech Lab PAIR, a solution built upon the foundations of Google Publisher Advertiser Identity Reconciliation (PAIR) protocol and IAB TL Privacy Enhancing Technology Working Group initiatives! Read more in latest blog: bit.ly/4biguft

iab. 10
TECH LAB

10:27 PM · May 14, 2024 · 744 Views

ADVERTISING

Google to open source PAIR identity tool with IAB Tech Lab

By **Bevin Fletcher** · Apr 29, 2024 2:10pm

Google identity solutions NewFronts NBCUniversal

What will be different in the IAB Tech Lab version?

- **Open industry standard** - While Google PAIR can only be deployed via DV360 from the buy-side, Tech Lab (TL) PAIR will be an open standard, making it compatible with wider range of platforms and tech.
- **Integration with OPJA** - TL PAIR will integrate Google PAIR with [Open Private Join and Activation \(OPJA\)](#), a related initiative by the TL Addressability and PET⁴ Working group to become one, unified standard for activating a common audience between two parties.
- **Stewardship and development** - The Addressability and PETs Working group will oversee the standard with industry parties like clean room providers (e.g. Optable, Decentriq) and adtech companies (e.g. Magnite) contributing to its development.

⁴ PET = Privacy enhancing technologies

Why this matters

INDUSTRY LEVEL

- Google PAIR and OPJA both represent an evolution of how audience targeting will work in the new marketing data and tech paradigm.
- By integrating data clean rooms/PETs with adtech, these protocols represent the first wave of recalibrating traditional advertising workflows to work in data privacy-safe manner.
- The IAB Tech Lab taking over development of the standard will not only increase PAIR's industry adoption, but also represents how friction for 1PD-based collaboration use cases will continue to decrease.

Why this matters

ADVERTISERS AND PUBLISHERS

- A singled, unified, interoperable standard will allow advertisers to more easily reach their known users across more publisher properties.
- For publishers of requisite scale, this provides the means to more easily monetise their visitor data.

Thanks!

© 2024 Skeleton Key

contact@skeletonkey.digital