SECDISPATCH
@IETF 123

Private set intersection (PSI) based on ECDH

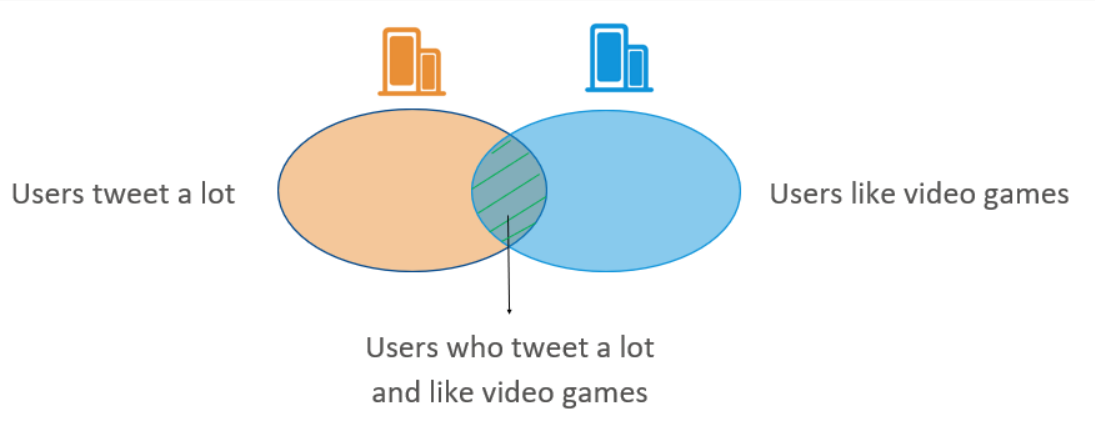
draft-wang-ppm-ecdh-psi

Wenting Chang, Alipay

IETF

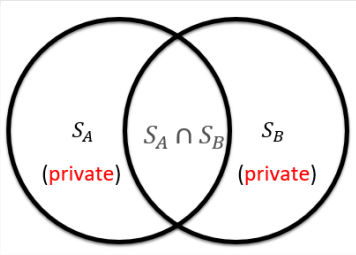
Motivation

- Company A and Company B wants to find their mutual customers
  - To establish a joint marketing campaign
- Reveal the (property of) mutual customers but **not any additional information**
  - The Private Set Intersection (PSI) problem



A standard protocol to enables between two or more parties is needed to **identify overlapping data elements** while **preserving the confidentiality** of each party's complete dataset!

Background: PSI technologies and applications



- Sending Hashed user ID is not enough
  - User ID does not have enough entropy; Require specific cryptographic protocols
- Many related researches on PSI
  - Based on Diffie-Hellman / Oblivious Transfer / VOLE ..

	Years since publication	Computation	Communication volume	Communication round
Diffie-Hellman based	**~30**	**Low**	**Low**	**Low**
Oblivious Transfer based	~10	Low	High	Moderate
VOLE-based	~3	Lowest	Low	Moderate

- ECDH-PSI have been widely deployed by Alibaba, Alipay, Bytedance, Bank of China …
  - Fraud detection \ card activation \ issue coupons …
- An example use case
  - "Chinese X" and "Chinese Youtube", each holding ~1B PIDs, made an ECDH-PSI in ~half a day.
  - Important business decisions were made according to the PSI output.

IETF

Background: ECDH-PSI protocol

- ECDH-PSI
  - Stem from private matching protocol [Meadows86]
  - Diffie-Hellmen style PSI with Elliptic Curve parameters
  - Records are converted to points on curve, and masked by the secret keys of both parties with scalar multiplications
  - If $r_A = r_B$,they will be masked to the same point after the joint masking process
  - If $r_A \neq r_B$,the will be masked to different points, but a participant cannot recover r_A or r_B since it does not know sk_A or sk_B ,which makes the matching private

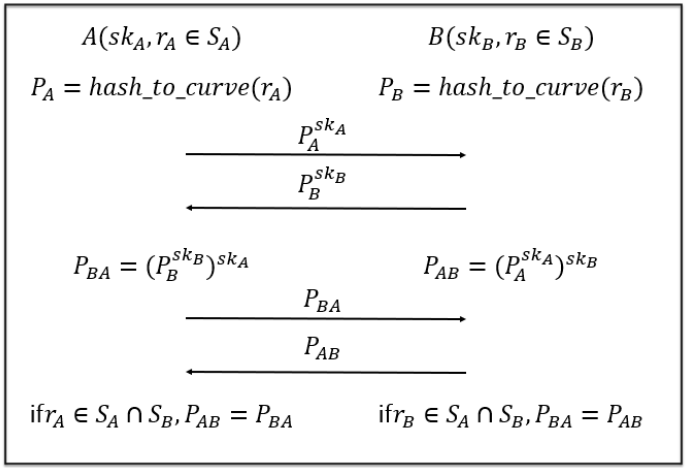


Figure 1. The one-record example of private matching

Status of our proposal: ECDH-PSI

- Draft of Private set intersection (PSI) based on Elliptic Curve Diffie-Hellman (ECDH) has been submitted to PPM WG since IETF-121.
  - Initial proposal https://datatracker.ietf.org/doc/draft-ecdh-psi/
  - Code: https://github.com/secretflow/interconnection

- We received very detailed and valuable comments and suggestions from Thomas Pronin and Christopher Patton
  - Release a new 01 version https://datatracker.ietf.org/doc/draft-wang-ppm-ecdh-psi/

- The proposal has been discussed in the Privacy-Preserving Measurement (PPM) WG interim working group. PPM Chair Benjamin M. Schwartz believes this is a highly promising and worthwhile technology, yet it falls outside the charter of PPM☹.

IETF

Hoped dispatch outcome

Dispatch the proposal to a WG for private set intersection discussion

Release a new 01 version https://datatracker.ietf.org/doc/draft-wang-ppm-ecdh-psi/

IETF

THE END!

THANK YOU!

tianwu.wyc@antgroup.com
bainuan.cwt@antgroup.com

IETF