



Private Set Membership

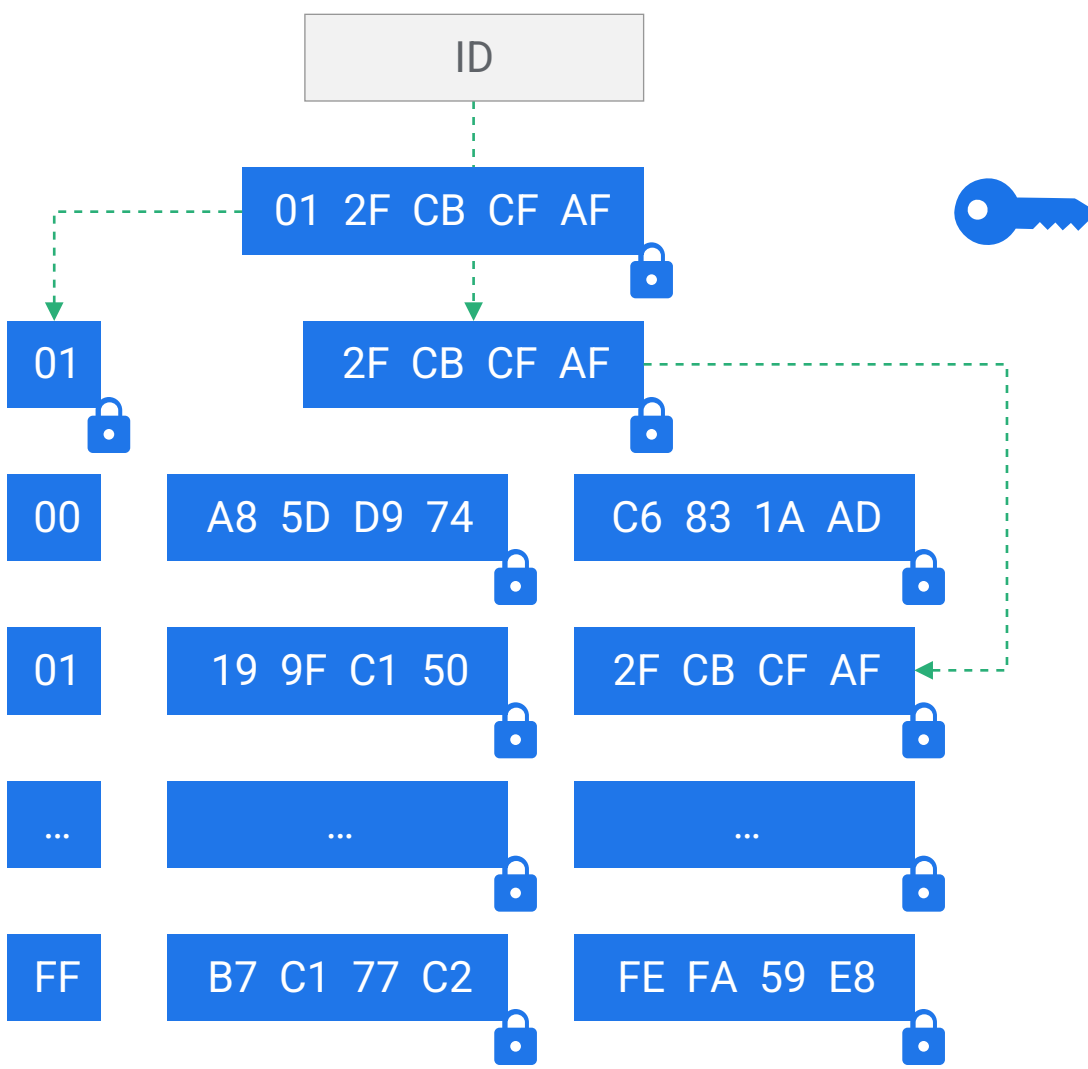
Summary

Private Set Membership considers the setting in which Google holds a set of items and user devices need to contact Google to check whether a specific item is a member of the set. Often, the set’s contents and the queried items are sensitive. Private Set Membership is designed to perform this task while preserving the privacy of both the user’s queried items and Google’s set.



1

Google hashes each item in the set with a private key only known to Google. All hashed items are bucketized using a prefix of the hash and the remainder of the hash is stored in the bucket.



2

The device starts the oblivious hashing protocol by blinding the query using a private key only known to the device.



ID

87 F9 E4 E3 35

87 F9 E4 E3 35

3

Google re-blinds and the device un-blinds the query using their private keys to complete oblivious hashing.



0E BC BF 06 71

01 2F CB CF AF

0E BC BF 06 71



4

The device encrypts the bucket identifier using homomorphic encryption.



01

01

00

01

...

FF

A8 5D D9 74

19 9F C1 50

...

B7 C1 77 C2

C6 83 1A AD

2F CB CF AF

...

FE FA 59 E8

5

Google computes an encryption of the desired bucket’s contents. The device decrypts the bucket contents and performs matching entirely on-device.



2F CB CF AF

19 9F C1 50

19 9F C1 50

2F CB CF AF

2F CB CF AF

19 9F C1 50

19 9F C1 50

2F CB CF AF

2F CB CF AF