Advanced International Journal for Research (AIJFR)
E-ISSN: 3048-7641 ● Website: www.aijfr.com ● Email: editor@aijfr.com

Efficient and Secure Cryptographic Protocol for Comparing Data

Solomon SARPONG

Department of Physical and Mathematical Sciences,
University of Environment and Sustainable Development, Somanya, Ghana
Email- ssarpong@uesd.edu.gh

Abstract

Comparison of information among individuals, companies or government agencies in some instances is unavoidable. In scenarios of the comparison of information, the individual data owners have to willingly or compelled to find the intersection of their private set of information. Cryptographic private set intersection helps in the computation of the intersections securely without the disclosure of any other information not in the intersection. The protocol in this paper helps users securely and efficiently compute their private set intersection without disclosing any other information. The protocol has communication and computation complexities of $O(m)$. The sizes of the communication and computation complexities make the protocol ideal to be used on any device.

Keywords: Binary attributes, cryptographic, malicious, privacy.

1. Introduction

Since the inception and development of the Internet, privacy has been more and more difficult to achieve and maintain. In order to maintain the privacy and the anonymity of the data whether at rest or in transit, it is usually encrypted. In some jurisdictions, storing or transmitting unencrypted data legal consequences. [1] opined that, there are national privacy protection laws that forbid the processing of non-anonymized records between institutions and even within the same institution. Even though non-anonymized or encrypting data secures it from unauthorised usage, it makes it almost impossible for statistical studies. As a result of data being encrypted, comparison of data from different organizations is difficult or impossible in some cases. In order to find the items that are common in two or more list, brings to the fore private set intersection (PSI). PSI is a class of cryptographic protocols that allows the computation of the intersection between private set of attributes of two or more parties without revealing any other information apart from the intersection set.

Hence, PSI has the capability of helping two or more parties compute the intersection of their attributes while ensuring that, nothing beyond the intersection is revealed. PSI can be applied in scenarios such as:

- A government agency wants to know the students exposed to a condition but the school is not willing to give out its list of students;

- In order to check if persons on a travel ban are on the flight manifest of an airline, the law enforcement agency is not willing to disclose its list of persons on the travel ban and the airline also does not want to give out its flight manifest;
- A bank investigating if a loan defaulter has savings in other banks but each bank unwilling to disclose the identities of its customers.

Since PSI was proposed by [2], there have been many variants. Some of the variants of PSI in literature include those based on; homomorphic encryption [3], [4], [5], [6], [7], [8], [9], [10], [11], [12]; Oblivious Polynomial Evaluation and transfer [13], [2], [14], [15], [16], [17], [18], [19], [12]; garbled circuit [20], and [21]. In most real-world applications of PSI, the protocol is unbalanced. In unbalanced PSI protocols, one party, usually the client, has a smaller set of attributes and less computational power as compared to the other party, the Server [22], [23], [24], [25], [26], [27], [28]. This is a common assumption in many applications of PSI. The laconic PSI is a variant of the unbalanced PSI in which only the Server learns the output of the intersection protocol [22], [23]. Labelled PSI is an unbalanced intersection protocol where each of the attributes in the private set of the server has an identity attached to it, [29].

Circuit PSI is an intersection protocol where the output of the intersection is computed as a function instead of either the number or type of attributes in the intersection set. Another variant of intersection protocol is the PSI-Cardinality. In this intersection protocol, the output is the size of the number of attributes. In scenarios where the sum of the values of the elements in the protocol is of interest, the PSI-Sum [30] is used.

This research paper seeks to propose efficient and privacy-preserving protocol for the computation of the intersection between parties. The protocol is secure against semi malicious and malicious attacks. In order to make it usable on handheld devices, the proposed protocol is light-weight as it does not use algorithms with high computational complexities.

In this paper, private set intersection is discussed in Section 2; related research works is in Section 3; the proposed protocol – the algorithm for the matchmaking and the security of our algorithms are presented in Section 4 with the conclusion in Section 5

2. Literature Review

[31] proposed three private-set intersection sums with cardinality protocols which relies on Diffie-Hellman techniques and use Random Oblivious Transfer and encrypted Bloom filters. [32], [33] proposed algorithms based on homomorphic encryption scheme for the secure and efficient computation of the intersection of several data sets. In order to avoid expensive computation using homomorphic encryption or zero-knowledge proof, [34] proposed a game-theoretic model for the computation of intersection of sets which satisfies computational Nash equilibrium.

Oblivious Bloom intersection protocol with linear complexity and relies mostly on efficient symmetric key operations was proposed by [35] for the computation of intersection. [31] in their paper proposed four PSI protocols – based on bilinear maps, secret sharing, modular inverse and symmetric encryption

for the optimal computation of intersection of private sets. [36] proposed an efficient multi-client functional encryption (MCFE) scheme that is capable of computing the intersection of ciphertexts from two parties. To mitigate the problem of securely and efficiently computing the intersection of private sets of two parties, multi-party protocols based on Bloom filters and homomorphic PKEs was proposed by [33].

[37] proposed an intersection protocol to model scenarios where all vehicles at an intersection can safely go through it without collisions. They were of the view that, their protocol can replace traffic lights as the vehicles will execute the proposed protocols among themselves to determine who has the right of way. [38] proposed an efficient MP-PSI protocol that is resistant against collision, malicious attacks and enables large number of participants with small number of attributes without performance dropping. [32] proposed two multi-party (MPSI and T-MPSI) protocols based on Bloom filters and threshold homomorphic PKEs with linear computation and communication costs. These protocols are secure in the semi-honest model.

In order to enable client and servers compute the intersection of their attribute sets efficiently and securely, [29] proposed PEPSI. [39] proposed a TPSI protocol based on garbled Bloom filter (GBF) and threshold secret sharing. Reed-Solomon decoding algorithm was combined with the proposed protocol to help reduce the computation cost and enhance efficiency.

The practical applications of two-party PSI include measuring the effectiveness of online advertising [40], contact discovery [28]. On the other hand, multiparty PSI finds application in contract tracing during the COVID-19 [27].
The real-world application of PSI is based on protocols utilizing trusted third-party, or the distributed approach or a hybrid of the two. Protocols that are based on the trusted third party include [41], [42], [43], [44]; the protocols that are based on the distributed approach include (Yang et al., 2010), [46], [47], [48]; also, some of the protocols based on the hybrid system include [49], [50], [51], [52], [53], [54], [55], [56], [57], [58], [59], [60].

3. Proposed Protocol

The algorithm 1 in this research paper is based on modified protocol in [61]. Each of the parties who want to undertake the private set intersection have a set of attributes chosen from a larger set U. Using the attributes in the larger set $\vec{U}$, each of the parties A and B form a binary set of their attributes. For simplicity of the protocol, let us assume there are only two persons A and B in the protocol. Let $\vec{a} = (a_1, a_2, \dots, a_m)$ and $\vec{b} = (b_1, b_2, \dots, b_m)$ be the binary set of private set of attributes of A and B respectively. It must be noted that, $\vec{U} \gg \vec{a}$, $\vec{U} \gg \vec{b}$ and $\vec{U} \gg \vec{a} + \vec{b}$. In order to ensure the privacy and security of the individual binary attributes, each binary private set of attributes are randomised to prevent attribute mapping attack. Assume A wants to compute the number of attributes that's common to B A chooses two large primes α, β and n positive random numbers $(c_1, c_2, \dots, c_n)$ such that $\sum_{i=1}^{n} c_i < (\alpha - n)$. A executes steps (i – v) of Algorithm 1 keeps (β, K) secret and sends $(\vec{a},\ \alpha, c_1, c_2, \dots, c_n)\ to\ B$. Also, B computes steps vi and vii of Algorithm 1 and sends $D = \sum_{i=1}^{m} D_i$ to A. When A receives D, computation of $E - E \mathrm{mod} \alpha^2 / \alpha^2$ is made, where $E = D + K mod \beta$. This

computation represents the scalar product of $\vec{a} * \vec{b} = \sum_{i=1}^{m} a_i * b_i$. The output of the computation of the scalar product indicates the number of attributes common to both sets. When Algorithm 1 is completed, the number of elements they have in common will be known. If the number of attributes they have in common is greater than ε (a threshold set by A) and they want to know the actual elements common to both, they proceed to Algorithm 2.

Algorithm 1 Privacy-preserving Scalar Product Computation

Requirements: A binary vector $\vec{a} = (a_1, a_2, \dots, a_m)$ and B binary vector $\vec{b} = (b_1, b_2, \dots, b_m)$

A does the following operations;

i : chooses two large primes α, β

ii : set $K = 0$ and choose n positive random numbers $(c_1, c_2, \dots, c_n)$ such that $\sum_{i=1}^{n} c_i < (\alpha - n)$

iii : for each element $a_i \in \vec{a}$, U_i chooses a random number r_i and compute $r_i\beta$.

iv : A further computes $k_i = r_i\beta - c_i$.

$$\begin{cases} C_i = \alpha + c_i + r_i\beta, & a_i = 1 \\ C_i = c_i + r_i\beta & a_i = 0 \end{cases} \text{ for } K = K + k_i$$

v : A keeps (β, K) secret and send $(\vec{a}, \alpha, C_1, C_2, \dots, C_n)$ *to* U_j

vi : B does the following; for each $b_i \in \vec{b}$,

if $b_j = 1$

$$\text{then } D_i = \alpha C_i = \begin{cases} \alpha^2 + \alpha c_i + \alpha\beta r_i, & if\ a_i = 1 \\ \alpha c_i + \alpha\beta r_i, & if\ a_i = 0 \end{cases}$$

if $b_j = 0$

$$\text{then } D_i = C_i = \begin{cases} \alpha + c_i + \beta r_i, & if\ a_i = 1 \\ c_i + \beta r_i, & if\ a_i = 0 \end{cases}$$

If $a_i = 1$ and $b_j = 1$, then

vii : B computes and sends $D = \sum_{i=1}^{m} D_i$ to U_i

viii : Both A and B compute $E - E \bmod \alpha^2 / \alpha^2$ which is the scalar product of $\vec{a} * \vec{b} = \sum_{i=1}^{m} a_i * b_i$

where $E = D + K \bmod \beta$

A and B choose large primes k_A and k_B as their secret keys respectively. Each of them exponentiates the attributes with the secret key, computes the hash and exchange with each other. A sends $h_p(a_i)^{k_A}\ \forall\ a_i \in A$ to Bob; while Bob also sends $h_p(b_j)^{k_B}\ \forall\ b_j \in B$ to Alice. Bob exponentiates $h_p(a_i)^{k_A}$ with his secret key and returns $\left\{(h_p(a_i)^{k_A}),\ (h_p(a_i)^{k_A})^{k_B}\right\}\ \forall\ (h_p(a_i)^{k_A})$ to Alice. Alice also exponentiates $h_p(b_j)^{k_B}$ with her secret key and returns $\left\{\left(h_p(b_j)^{k_B}\right),\ \left(h_p(b_j)^{k_B}\right)^{k_A}\right\}\ \forall\ \left(h_p(b_j)^{k_B}\right)$ to Alice. Each of them computes the intersection $\left\{(h_p(a_i)^{k_A})^{k_B} \cap \left(h_p(b_j)^{k_B}\right)^{k_A}\right\} = A \cap B$. The elements obtained in the computation of this intersection, is the set formed from the first element of the pairs in $T = \left\{a_i, \left(h_p(b_j)^{k_A}\right)^{k_B}\right\}$ whose second element is in the set $S = \left\{b_j, (h_p(a_i)^{k_A})^{k_B}\right\}$. At the end of Algorithm 2, the actual attributes they have in common will be known by each of them. In the

protocol in this paper, attributes are the same if they are semantically the same. The protocol has communication and computation complexities of $O(m)$.

Algorithm 2 Exchanging of Common Attributes

Require: A's interests are $(a_1, a_2, \dots, a_n)$ and secret key k_A
B's interests are $(b_1, b_2, \dots, b_m)$ and secret key k_B

1: Alice computes and sends to Bob $h_p(a_i)^{k_A} \forall\ a_i \in A$
Bob computes and sends to Alice $h_p(b_j)^{k_B} \forall\ b_j \in B$

2: Bob computes and sends to Alice, $T = \left\{(h_p(a_i)^{k_A}),\ (h_p(a_i)^{k_A})^{k_B}\right\} \forall (h_p(a_i)^{k_A})$
Alice computes and sends Bob, $S = \left\{\left(h_p(b_j)^{k_B}\right),\ \left(h_p(b_j)^{k_B}\right)^{k_A}\right\} \forall \left(h_p(b_j)^{k_B}\right)$

3: Alice creates a list $T = \left\{a_i, \left(h_p(b_j)^{k_A}\right)^{k_B}\right\} \forall\ a_i \in A$
Bob also creates a list $S = \left\{b_j, \left(h_p(a_i)^{k_A}\right)^{k_B}\right\} \forall\ b_j \in B$

4: Alice and Bob compute $T \cap S = \left\{a_i, \left(h_p(b_j)^{k_A}\right)^{k_B}\right\} \cap \left\{b_j, \left(h_p(a_i)^{k_A}\right)^{k_B}\right\}$
The computation of the intersection, $T \cap S$ is the set formed from the first element of the pairs in S whose second element is in the set T.

4. Security

Recently, privacy and security of private information have become very difficult to achieve and maintain with the advent of Internet. There are situations where untrusting parties need to compare the information they possess individually. The protocol in this paper helps users to compare the content of a document or a set of attributes without leaking any other information. The first part of the protocol enables them know only number of attributes they have in common. The parties will proceed to execute the second algorithm if the actual attributes need to be known.

4.1 Correctness of the Algorithm

Each party computes $D = \sum_{i=1}^{m} D_i$ where $D_i = \begin{cases} \alpha^2 + \alpha c_i + \alpha\beta r_i, & if\ a_i = 1 \\ \alpha c_i + \alpha\beta r_i, & if\ a_i = 0 \end{cases}$ when $b_j = 1$ and for $b_j = 0$, $D_i = C_i = \begin{cases} \alpha + c_i + \beta r_i, & if\ a_i = 1 \\ c_i + \beta r_i, & if\ a_i = 0 \end{cases}$. With the knowledge of D, each of them is able to compute $E - E \bmod \alpha^2 /_{\alpha^2}$ which is the scalar product of $\vec{a} * \vec{b} = \sum_{i=1}^{m} a_i * b_i$, where $E = D + K mod \beta$. Hence, at the end of this protocol, each party is able to know just the number of attributes that are common in both private attribute set. In algorithm 2, both compute $T \cap S = \left\{a_i, \left(h_p(b_j)^{k_A}\right)^{k_B}\right\} \cap \left\{b_j, \left(h_p(a_i)^{k_A}\right)^{k_B}\right\}$. Hence, both get to know the actual number of attributes they have in common simultaneously. Since, the computation of, $\vec{a} * \vec{b}$, the number of attributes common to both parties and $T \cap S$, gives the actual attributes they have in common by both, the protocol is correct.

4.2 Achievement of Privacy in the Algorithm

The protocols in this paper ensures the privacy of users' attributes. At the end of algorithm 1, only the number of attributes they have in common is known by both parties. Hence, nothing about the actual attributes of each party is disclosed. Also, at the end of algorithm 2, the actual attributes they have in common will be known by both. Only the attributes they have in common but nothing else.

4.3 Attacks on the Protocol and Countermeasures

In algorithm 1, $\vec{U}$ is very large set of attributes such that, $\vec{U} \gg \vec{a}$, $\vec{U} \gg \vec{b}$ and $\vec{U} \gg \vec{a} + \vec{b}$. Each user uses $\vec{U}$ to form a binary set of his / her attributes. Mapping a user's attributes to the $\vec{U}$, one (1) indicates the presence of the attribute in the user's set and zero (0) indicates the absence of the attribute in the user's set. The randomisation of each user's set of attributes is to prevent mapping attacks. Mapping attack occurs when an attacker is able to map the binary representations to the actual attributes of the other. Hence, this protocol is resistant against this form of attack. The protocols are executed individually hence, one party may not know the other parties in the protocol. However, if some parties want to know the attributes of *A*, there should be the collusion of $\left({}^{n}/_{\epsilon} - 1\right)$ individuals. Hence, this protocol is collusion resistant.

5. Discussion and Conclusion

The world is now inter-connected on all sphere of human activities. In as much as the inter-connectivity is good, unfortunately it has its issues. One of the issues is the privacy of personal information. Even in situations where personal information is not meant to be private, owners of the data there are concerns about who might be using it. In some scenarios, individuals, companies or agencies need to compare the information each has. The protocol in this paper facilitates the comparison of the content of their respective information. The protocol has communication and computation complexities of $O(m)$. The sizes of the communication and computation complexities make the protocol ideal to be used on any device.

References

1. G. Bruno *et al.*, "Are post-crisis statistical initiatives completed?" Basel," pp. 30–31, 2018.
2. M. J. Freedman, K. Nissim, and B. Pinkas, "Efficient private matching and set intersection," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 3027, pp. 1–19, 2004, doi: 10.1007/978-3-540-24676-3_1.
3. J. D. Ferrer, "A new privacy homomorphism and applications," *Inf Process Lett*, vol. 60, no. 5, pp. 277–282, Dec. 1996, doi: 10.1016/S0020-0190(96)00170-6.
4. N. Jain, "Implementation and Analysis of Homomorphic Encryption Schemes," *International Journal on Cryptography and Information Security*, vol. 2, no. 2, pp. 27–44, 2012, doi: 10.5121/ijcis.2012.2203.

5. J. M. Kukucka and M. Zuker, “An investigation of the theory and applications of homomorphic cryptography,” *Rensselaer Polytechnic Institute*, 2013.
6. M. Neill, E. O’sullivan, Y. Doröz, and B. Sunar, “Practical homomorphic encryption: A survey,” *IEEE*, p. 2792, 2014, doi: 10.1109/ISCAS.2014.6865753.
7. B. Pulido-Gaytan *et al.*, “Privacy-preserving neural networks with Homomorphic encryption: Challenges and opportunities,” *Peer Peer Netw Appl*, vol. 14, no. 3, pp. 1666–1691, May 2021, doi: 10.1007/S12083-021-01076-8.
8. F. Rezaeibagha, Y. Mu, S. Zhang, and X. Wang, “Provably secure (broadcast) homomorphic signcryption,” in *International Journal of Foundations of Computer Science*, World Scientific Publishing Co. Pte Ltd, Jun. 2019, pp. 511–529. doi: 10.1142/S0129054119400100.
9. A. M. Vengadapurvaja, G. Nisha, R. Aarthy, and N. Sasikaladevi, “An Efficient Homomorphic Medical Image Encryption Algorithm for Cloud Storage Security,” *Procedia Comput Sci*, vol. 115, pp. 643–650, 2017, doi: 10.1016/J.PROCS.2017.09.150.
10. G. L. Xiang, X. M. Chen, P. Zhu, and J. Ma, “A method of homomorphic encryption,” *Wuhan University Journal of Natural Sciences*, vol. 11, no. 1, pp. 181–184, 2006, doi: 10.1007/bf02831727.
11. Q. Xie *et al.*, “Efficiency Optimization Techniques in Privacy-Preserving Federated Learning With Homomorphic Encryption: A Brief Survey,” *IEEE Internet Things J*, vol. 11, no. 14, pp. 24569–24580, 2024, doi: 10.1109/JIOT.2024.3382875.
12. Y. Yang, Y. Yang, X. Chen, X. Dong, Z. Cao, and J. Shen, “DMPSI: Efficient Scalable Delegated Multiparty PSI and PSI-CA with Oblivious PRF,” *IEEE Trans Serv Comput*, vol. 17, no. 2, pp. 497–508, Mar. 2024, doi: 10.1109/TSC.2024.3356667.
13. M. Chase and P. Miao, “Private Set Intersection in the Internet Setting From Lightweight Oblivious PRF,” *Advances in Cryptology -- CRYPTO 2020*, pp. 34–63, 2020, doi: 10.1007/978-3-030-56877-1_2.
14. S. Jarecki and X. Liu, “Efficient Oblivious Pseudorandom Function with Applications to Adaptive OT and Secure Computation of Set Intersection,” in *Theory of Cryptography, 6th Theory of Cryptography Conference, TCC 2009, San Francisco, CA, USA, March 15-17, 2009. Proceedings*, in Lecture Notes in Computer Science, vol. 5444. Springer, 2009, pp. 577–594. doi: 10.1007/978-3-642-00457-5_34.
15. S. Jarecki and X. Liu, “Efficient oblivious pseudorandom function with applications to adaptive ot and secure computation of set intersection,” *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 5444 LNCS, pp. 577–594, 2009, doi: 10.1007/978-3-642-00457-5_34.
16. S. Jarecki and X. Liu, “Efficient oblivious pseudorandom function with applications to adaptive ot and secure computation of set intersection,” *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 5444 LNCS, pp. 577–594, 2009, doi: 10.1007/978-3-642-00457-5_34.
17. Z. Jiang, X. Guo, T. Yu, H. Zhou, J. Wen, and Z. Wu, “Private Set Intersection Based on Lightweight Oblivious Key-Value Storage Structure,” *Symmetry 2023, Vol. 15, Page 2083*, vol. 15, no. 11, p. 2083, Nov. 2023, doi: 10.3390/SYM15112083.

18. V. Kolesnikov, N. Matania, B. Pinkas, M. Rosulek, and N. Trieu, "Practical multi-party private set intersection from symmetric-key techniques," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 2017, pp. 1257–1272.
19. V. Kolesnikov, R. Kumaresan, M. Rosulek, and N. Trieu, "Efficient batched oblivious PRF with applications to private set intersection," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016, pp. 818–829.
20. Y. Huang, D. Evans, and J. Katz, "Private Set Intersection: Are Garbled Circuits Better than Custom Protocols?," pp. 5–8, 2012, Accessed: Dec. 09, 2025. [Online]. Available: http://MightBeEvil.org
21. D. Heath, "Garbled Circuits," pp. 1–6, 2025.
22. N. Alamati, P. Branco, N. Döttling, S. Garg, M. Hajiabadi, and S. Pu, "Laconic Private Set Intersection and Applications," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 13044 LNCS, pp. 94–125, 2021, doi: 10.1007/978-3-030-90456-2_4.
23. D. F. Aranha, C. Lin, C. Orlandi, and M. Simkin, "Laconic Private Set-Intersection From Pairings," *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, CCS*, pp. 111–124, 2022, Accessed: Dec. 05, 2025. [Online]. Available: https://signal.org/
24. H. Chen, Z. Huang, K. Laine, and P. Rindal, "Labeled PSI from Fully Homomorphic Encryption with Malicious Security," *24th ACM Conference on Com- puter and Communications Security (CCS)*, 2018, Accessed: Dec. 05, 2025. [Online]. Available: http://sealcrypto.org
25. H. Chen, K. Laine, and P. Rindal, "Fast Private Set Intersection from Homomorphic Encryption," *23rd ACM Conference on Computer and Communications Security (CCS)*, 2017.
26. K. Cong *et al.*, "Labeled PSI from Homomorphic Encryption with Reduced Computation and Communication," *27th ACM Conference on Computer and Communications Security (CCS)*, 2021.
27. T. Duong, D. Hieu Phan, and N. Trieu, "Catalic: Delegated PSI Cardinality with Applications to Contact Tracing," *Advances in Cryptology – ASIACRYPT 2020: 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea*, pp. 870–899, 2020.
28. D. Kales, C. Rechberger, T. Schneider, M. Senker, and C. Weinert, "Mobile Private Contact Discovery at Scale (Full Version) *," *In 28th USENIX Security Symposium (USENIX Security 19), USENIX*, pp. 1447–1464, 2019, Accessed: Dec. 05, 2025. [Online]. Available: https://www.backes-srt.com/en/solutions-2/whatsbox
29. R. A. Mahdavi *et al.*, "PEPSI: Practically Efficient Private Set Intersection in the Unbalanced Setting," *33rd USENIX Security Symposium (USENIX Security 24)*, p. 6453, 2024, Accessed: Nov. 04, 2025. [Online]. Available: https://www.usenix.org/conference/usenixsecurity24/presentation/mahdavi
30. B. Kacsmar *et al.*, "Differentially Private Two-Party Set Operations," *2020 IEEE European Symposium on Security and Privacy (EuroS&P).*, pp. 390–404, 2020.
31. I. Andreea, "Private Set Intersection: Past, Present and Future," *In Proceedings of the 18th International Conference on Security and Cryptography (SECRYPT 2021)*, pp. 680–685, 2021, doi: 10.5220/0010525806800685.

32. A. ; Bay, A. ; Erkin, Z. ; Alishahi, and M. Vos, “Multi-party private set intersection protocols for practical applications,” pp. 515–522, 2021, doi: 10.5220/0010547605150522.
33. A. ; Bay, Z. ; Erkin, J. H. Hoepman, S. ; Samardjiska, and J. Vos, “Practical Multi-party Private Set Intersection Protocols,” *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY*, vol. 17, p. 1, 2021, doi: 10.1109/TIFS.2021.3118879.
34. A. Miyaji and M. S. Rahman, “Private Two-Party Set Intersection Protocol in Rational Model,” *Journal of Internet Services and Information Security (JISIS)*, no. 2(12-6), 2012.
35. C. Dong, L. Chen, and Z. Wen, “When private set intersection meets big data: an efficient and scalable protocol,” in *Proceedings of the 2013 ACM SIGSAC conference on Computer \& communications security*, 2013, pp. 789–800.
36. S. Lee, J. Lee, and I. Lee, “A Study of Secure and Efficient Data Sharing Scheme for Cloud Storage Architecture,” pp. 452–457, 2021.
37. K. Alpturer, J. Y. Halpern, and R. Van Der Meyden, “A Knowledge-Based Analysis of Intersection Protocols,” *arXiv preprint arXiv:2408.09499*, 2024.
38. L. Wei, J. Liu, L. Zhang, Q. Wang, W. Zhang, and X. Qian, “Efficient multi-party private set intersection protocols for large participants and small sets,” *Comput Stand Interfaces*, vol. 87, Jan. 2024, doi: 10.1016/j.csi.2023.103764.
39. E. N. Zhang, J. Chang, and Y. U. Li, “Efficient Threshold Private Set Intersection,” vol. 9, 2021, doi: 10.1109/ACCESS.2020.3048743.
40. M. Ion *et al.*, “Private Intersection-Sum Protocol with Applications to Attributing Aggregate Ad Conversions,” 2017.
41. K. A. Li, T. Y. Sohn, S. Huang, and W. G. Griswold, “Peopletones: a system for the detection and notification of buddy proximity on mobile phones,” in *Proceedings of the 6th international conference on Mobile systems, applications, and services*, 2008, pp. 160–173.
42. J. Kjeldskov and J. Paay, “Just-for-us: a context-aware mobile information system facilitating sociality,” in *Proceedings of the 7th international conference on Human computer interaction with mobile devices \& services*, 2005, pp. 23–30.
43. N. Eagle and A. Pentland, “Social Serendipity: Mobilizing social software,” *IEEE Pervasive Computing, Special Issue: The Smartphone*, pp. 28–34, 2005.
44. A.-K. Pietiläinen, E. Oliver, J. LeBrun, G. Varghese, and C. Diot, “Mobiclique: middleware for mobile social networking,” in *Proceedings of the 2nd ACM workshop on Online social networks*, 2009, pp. 49–54.
45. Z. Yang, B. Zhang, A. C. Champion, D. Li, D. Xuan, and J. Dai, “E-SmallTalker: A Distributed Mobile System for Social Networking in Physical Proximity,” in *2010 IEEE 33th International Conference on Distributed Computing Systems*, Los Alamitos, CA, USA: IEEE Computer Society, Jun. 2010, pp. 468–477. doi: 10.1109/ICDCS.2010.56.
46. M. Li, N. Cao, S. Yu, and W. Lou, “FindU: Privacy-preserving personal profile matching in mobile social networks,” *Proceedings - IEEE INFOCOM*, no. 1, pp. 2435–2443, 2011, doi: 10.1109/INFCOM.2011.5935065.
47. R. Lu, X. Lin, X. Liang, and X. Shen, “A secure handshake scheme with symptoms-matching for mHealthcare social network,” *Mobile Networks and Applications*, vol. 16, no. 6, pp. 683–694, Dec. 2011, doi: 10.1007/S11036-010-0274-2.

48. R. Lu, X. Lin, and X. Shen, "SPOC: A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 3, pp. 614–624, 2013, doi: 10.1109/TPDS.2012.146.
49. S. Sarpong, "Privacy of Friendship on Social Media: Application of Honey Encryption," 2022. [Online]. Available: http://ijses.com/
50. S. Sarpong, "Privacy-Preserving Zero Knowledge Scheme for Attribute-based Matchmaking," *International Journal of Scientific Research & Engineering Trends*, vol. 7, no. 2, pp. 2395–566, 2021.
51. S. Sarpong, "Privacy-Preserving Zero Knowledge Scheme for Attribute-based Matchmaking," 2021.
52. S. Sarpong, "P RIVACY AND SECURITY OF PERSONAL HEALTH INFORMATION IN MOBILE HEALTH (M H EALTH) CARE," vol. 8, no. 6, pp. 984–988, 2020.
53. S. Sarpong, "Spam: Secure and Privacy-Preserving Attribute-based Matchmaking," 2024. [Online]. Available: www.ijisrt.com
54. S. Sarpong and C. Xu, "Privacy-preserving attribute matchmaking in proximity-based mobile social networks," *International Journal of Security and its Applications*, vol. 9, no. 5, pp. 217–230, 2015, doi: 10.14257/ijsia.2015.9.5.22.
55. S. Sarpong and C. Xu, "Privacy-preserving attribute matchmaking in proximity-based mobile social networks," *International Journal of Security and its Applications*, vol. 9, no. 5, pp. 217–230, 2015, doi: 10.14257/ijsia.2015.9.5.22.
56. S. Sarpong and C. Xu, "Privacy-preserving attribute matchmaking in proximity-based mobile social networks," *International Journal of Security and its Applications*, vol. 9, no. 5, pp. 217–230, 2015, doi: 10.14257/ijsia.2015.9.5.22.
57. S. Sarpong and C. Xu, "A secure and efficient privacy-preserving matchmaking for mobile social network," in *International Conference on Computer, Network Security and Communication Engineering (CNSCE)*, 2014, pp. 362–366.
58. Y. Wang, J. Hou, Y. W. Tan, and X. Nie, "A recommendation-based matchmaking scheme for multiple mobile social networks against private data leakage," in *Procedia Computer Science*, Elsevier B.V., Jan. 2013, pp. 781–788. doi: 10.1016/j.procs.2013.05.100.
59. Y. Wang, J. Hou, Y. Xia, and H. Z. Li, "Efficient privacy preserving matchmaking for mobile social networking," *Concurr Comput*, vol. 27, no. 12, pp. 2924–2937, Aug. 2015, doi: 10.1002/CPE.3284.
60. Y. Wang, T. T. Zhang, H. Z. Li, L. P. He, and J. Peng, "Efficient privacy preserving matchmaking for mobile social networking against malicious users," in *Proc. of the 11th IEEE Int. Conference on Trust, Security and Privacy in Computing and Communications, TrustCom-2012 - 11th IEEE Int. Conference on Ubiquitous Computing and Communications, IUCC-2012*, 2012, pp. 609–615. doi: 10.1109/TrustCom.2012.142.
61. R. Lu, X. Lin, and X. Shen, "SPOC: A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 3, pp. 614–624, 2013, doi: 10.1109/TPDS.2012.146.