Estimating Incidental Collection in Foreign Intelligence Surveillance

Large-Scale Multiparty Private Set Intersection with Union and Sum

Anunay Kulshrestha Jonathan Mayer

Center for Information Technology Policy
Princeton University

Background and Motivation

Section 702 of the Foreign Intelligence Surveillance Act (FISA)

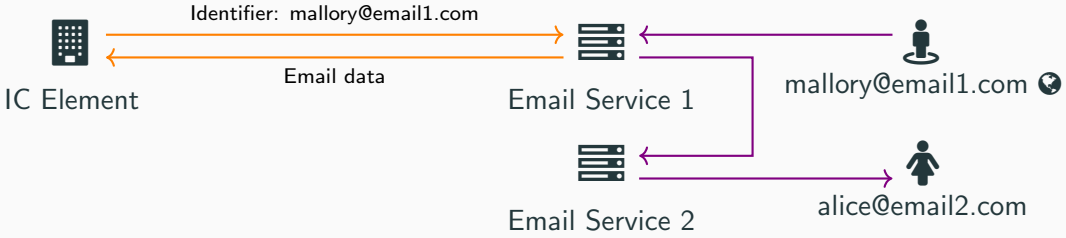
- Authorizes the U.S. Intelligence Community (IC) to collect communications **inside the U.S.** when targeting **foreigners abroad**[1]
- **Does not require** applying to a court for a warrant demonstrating probable cause for an individual target (IC obtains an annual program approval)
- Structure and details of Section 702 have prompted **significant** controversy

Incidental Collection

- Targets of surveillance under Section 702 must be **foreign** nationals located **outside the U.S.**
- Targets communicate with non-targets who are **U.S. persons**
- Communications of non-targets are **incidentally** collected

[1] 50 U.S.C. § 1881a; Donohue (2015); Office of the Director of National Intelligence (2017)

Background and Motivation



	mallory@email1.com		alice@email2.com	
Knowledge State	Location	Collection	Location	Collection
IC Element	🌐	🔒	?	🔒
Email Service 1	🌐	🔒	?	🔒
Email Service 2	?	?		?

→ Communication between users

→ Collection under Section 702

Background and Motivation

- Members of both houses of the U.S. Congress[2] and many civil society groups[3] have repeatedly asked for an estimate of the scale of incidental collection of Americans' communication data under Section 702
- Senior officials of the IC had promised an estimate multiple times[4] in the past
- But the IC does not (and should not) know that Alice is in the U.S.

[2] Wyden and Udall (2011); Director of National Intelligence (2011); Wyden and Udall (2012a,b); House Judiciary Committee (2016a,b); Chair of the House Judiciary Committee (2017)

[3] Brennan Center for Justice et al. (2015); Electronic Frontier Foundation (2016); Brennan Center for Justice et al. (2016); ACLU et al. (2017)

[4] Inspector General of the Intelligence Community (2012); Office of the Director of National Intelligence (2015); Director of National Intelligence (2012); Coats (2017); Director of National Intelligence (2017a,b)

Assumptions

- U.S person $\approx$ located in the U.S.
- Service providers know the location of users associated with identifiers used by their services
- In particular, service providers can construct sets of identifiers they believe to be associated with users inside the U.S.
- IC elements hold sets of non-target identifiers whose communications they have incidentally collected

Model

$X_0 \subset \{0,1\}^*$ $X_1 \subset \{0,1\}^*$ $X_2 \subset \{0,1\}^*$ $X_{n-1} \subset \{0,1\}^*$

$V \subset \mathbb{Z}^+$

X_0 is the **set of identifiers** whose communications were incidentally **collected**

V is a **set of associated values**: e.g. number of communications **collected**

X_i for $i > 0$ is the **set of identifiers** associated with users believed, by service provider i, to be **in the U.S**.

Aim: Privately compute $\sum_{x \in \mathcal{I}} V[x]$ for $\mathcal{I} = X_0 \bigcap (\bigcup_{i=1}^{n-1} X_i)$ with large sets: $|X_0| \approx 2^{23}$, $|X_i| \approx 2^{30}$ for $i > 0$

Ideal Functionalities

MPSI

There are n parties $\mathcal{P}_0, \mathcal{P}_1, \ldots, \mathcal{P}_{n-1}$ with delegate $\mathcal{P}_0$.
Inputs: $X_i \subseteq \{0,1\}^*$ held by party $\mathcal{P}_i$.
Outputs: $\mathcal{P}_0$ receives $\bigcap_{i=0}^{n-1} X_i$. Others receive nothing.

MPSIU-Sum

There are n parties $\mathcal{P}_0, \mathcal{P}_1, \ldots, \mathcal{P}_{n-1}$ with delegate $\mathcal{P}_0$.
Inputs: $X_i \subseteq \{0,1\}^*$ held by party $\mathcal{P}_i$ and associated values $V \subseteq \mathbb{F}_q$ held by the delegate.
Outputs: $\mathcal{P}_0$ receives $\sum_{x \in \mathcal{I}} V[x]$ and $|\mathcal{I}|$ for $\mathcal{I} = X_0 \bigcap (\bigcup_{i=1}^{n-1} X_i)$. Other parties receive nothing.

Threat Model

No party learns any new information about the location of the user of an identifier

No service provider learns any information about identifiers whose communications were incidentally collected

- Secure against private information extraction by a **malicious IC element**
- Secure against private information extraction by any **coalition of malicious service providers**
- **Do not prevent** intentional false positives, false negatives, inaccurate set cardinality, or inaccurate sum computation, as MPC participants can generally cheat with input
- **Do not prevent** participants from intentionally l ca, as is generally true of MPC
- The aggregate cardinality and sum **output** from MPSIU-Sum **itself** may reveal information about $X_1, \ldots, X_{n-1}$ to $\mathcal{P}_0 \rightarrow$ add noise to mitigate risk

Limitations

- Generate an **estimate** of incidental collection, not a definitive count
- Assume that aggregation of transparency statistics on incidental collection will **not** reveal intelligence sources or methods
- Estimates are for incidental collection on users located in the U.S. and **do not** include citizens and permanent residents abroad
- Count communications **identifiers** rather than **individuals**
- Limited risk of **false negatives** $\implies$ the results are a **lower bound** on the true scale of incidental collection

Primitives

Hash Maps. In a hash map of size 2^l, the index of string x is the l-bit prefix of a l'-bit cryptographic hash of x with $l' \geq l$.

Hashing to Elliptic Curves. We implement the latest draft of the evolving IETF Hash-to-Curve standard. $H_E : \{0,1\}^* \to E$ can be modeled as a **random oracle**.

Diffie-Hellman Random Self-Reduction. In a group of order q with generator G where the DDH problem is hard, define DH.Reduce for random scalars $\beta, \gamma \xleftarrow{\$} \mathbb{F}_q$.

$$(L, T, P) \text{ is a DDH tuple} \iff L = \alpha \cdot G \text{ and } P = \alpha \cdot T \text{ for some } \alpha \in \mathbb{F}_q.$$
$$\text{DH.Reduce}(L, T, P) = (\beta \cdot T + \gamma \cdot G, \beta \cdot P + \gamma \cdot L)$$

DH.Reduce reduces DDH tuples to DDH tuples[5] and non-DDH tuples to independent random values in $E(\mathbb{F}_q)$

If (L, T_1, P_1) and (L, T_2, P_2) are DDH tuples, so is $(L, T_1 + T_2, P_1 + P_2)$.

[2] Naor and Reingold (1997); Bhowmick et al. (2021)

Primitives

Distributed ElGamal Cryptosystem (EG.Enc, EG.Dec, EG.Add)

- Data encrypted under aggregate key can only be **decrypted jointly** by all parties
- ElGamal in the exponent: message $m \in \mathbb{F}_q$ is represented by $m \cdot G$
- Preserves **additive homomorphism** but decryption involves computing **discrete logarithms**, which is infeasible for large m
- Solution: encrypt m modulo c fixed moduli, use **Chinese Remainder Theorem** and **Baby Step Giant Step** to efficiently decrypt
- MPSI-Sum and MPSIU-Sum require the decryption of **one** ElGamal ciphertext each, MPSI and MPSIU require **none**.

Protocol Design: Overview

- If (L, T, P) is a DDH tuple, then $L = \alpha \cdot G$ and $P = \alpha \cdot T$ for some $\alpha \in \mathbb{F}_q$
- Without knowledge of α, DDH tuples cannot be distinguished efficiently
- Delegate $\mathcal{P}_0$ constructs encrypted hashmap M
- Using M, $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_{n-1}$ jointly construct hashmap R such that slots of R corresponding to the intersection-with-union yield DDH tuples
- $\mathcal{P}_0$ holds α, so other parties do not learn information about the intersection-with-union as R is constructed
- The last provider $\mathcal{P}_{n-1}$ constructs encrypted array B using R such that $\mathcal{P}_0$ can only decrypt (using α) elements corresponding to DDH tuples
- $\mathcal{P}_0$ receives B and computes the protocol result

MPSIU-Sum

Public Parameters: EC group $E(\mathbb{F}_q)$ with generator G, hash function $H_E : \{0,1\}^* \to E$, map size $m = 2^l$.
Parties: Delegate $\mathcal{P}_0$.
Inputs: $\mathcal{P}_0$ holds set $X_0 \subset \{0,1\}^*$, associated values $V \subset \{0,1\}^*$, encryption key ek, encryption function Enc.
Outputs: Blinding key α, EC point L, and hashmap M.

1. Generates $\alpha \xleftarrow{\$} \mathbb{F}_q$ and sets $L = \alpha \cdot G$.
2. For every $w_j \in X_0, v_j \in V$, sets $M_{\mathsf{index}(w_j)} \leftarrow \{\alpha \cdot H_E(w_j), \mathsf{Enc}(\mathsf{ek}, v_j)\}$.
3. For every unmodified index $0 \leq j < m$ in M, sets $M_j \leftarrow \{r \cdot G, \mathsf{Enc}(\mathsf{ek}, 0)\}$ for $r \xleftarrow{\$} \mathbb{F}_q$.

Protocol: Delegate-Start

Public Parameters: EC group $E(\mathbb{F}_q)$, size $m = 2^l$.
Parties: Last party $\mathcal{P}_{n-1}$.
Inputs: Hashmaps R and M, ElGamal public key apk (optional).
Outputs: Array B.

1. Initializes array B of size m. For $0 \leq j < m$, sets

$$\mathsf{ct}_j \leftarrow \begin{cases} \mathsf{EG.AddZero}(\mathsf{apk}, M_{j,1}) & \text{if apk was provided} \\ M_{j,1} & \text{otherwise} \end{cases}$$

$$B_j \leftarrow \{R_{j,0}, \mathsf{AEAD.Enc}(\mathsf{KDF}(R_{j,1}), \mathsf{ct}_j)\}$$

2. Samples permutation π over $\{0, \ldots, m-1\}$ and shuffles $B \leftarrow \pi(B)$.

Protocol: Blind-Encrypt

Public Parameters: EC group $E(\mathbb{F}_q)$, array size $m = 2^l$.
Parties: Delegate $\mathcal{P}_0$.
Inputs: Blinding key α and array B.
Outputs: Set of AEAD plaintexts D.

1. For $0 \leq j < m$, computes $K_j \leftarrow \mathsf{KDF}(\alpha \cdot B_{j,0})$ and $d_j \leftarrow \mathsf{AEAD.Dec}(K_j, B_{j,1})$.

$$D \leftarrow \{d_j : d_j \neq \perp, 0 \leq j < m\}$$

Protocol: Delegate-Finish

MPSIU-Sum

Public Parameters: EC group $E(\mathbb{F}_q)$ with generator G, hash function $H_E : \{0,1\}^* \to E$, map size $m = 2^l$
Parties: $\mathcal{P}_0, \mathcal{P}_1, \ldots, \mathcal{P}_{n-1}$ with delegate $\mathcal{P}_0$.
Inputs: $\mathcal{P}_i$ holds set $X_i \subset \{0,1\}^*$ for $0 \leq i < n$ and P_0 holds associated values V_0.
Outputs: Delegate $\mathcal{P}_0$ receives the result of the protocol, other parties receive nothing.

1. (All parties) Choose $\mathsf{sk}_i \xleftarrow{\$} \mathbb{F}_q$ and run $\mathsf{apk} \leftarrow \text{Key-Aggregation}(\mathsf{sk}_0, \ldots, \mathsf{sk}_{n-1})$.
2. (Delegate $\mathcal{P}_0$) Runs $(\alpha, L, M) \leftarrow \text{Delegate-Start}(X_0, V_0, \mathsf{apk}, \mathsf{EG.Enc})$ and publishes M, L.
3. (Party $\mathcal{P}_1$) Initializes map R of size m.
4. (Party $\mathcal{P}_i$ for $1 \leq i \leq n-1$) For every $w \in X_i$, computes $j \leftarrow \text{index}(w)$ and sets $R_j \leftarrow \text{DH.Reduce}(L, H_E(w), M_{j,0})$.
5. (Party $\mathcal{P}_1$) For $0 \leq j < m$, if R_j was not modified in step 4, sets $R_j \leftarrow \{Q', S'\}$ for $Q', S' \xleftarrow{\$} E$.
6. (Party $\mathcal{P}_i$ for $1 < i \leq n-1$) For $0 \leq j < m$, if R_j was not modified in step 4, sets $R_j \leftarrow \text{DH.Reduce}(L, R_{j,0}, R_{j,1})$.
7. (Party $\mathcal{P}_i$ for $1 \leq i < n-1$) Sends R to $\mathcal{P}_{i+1}$.
8. (Last party $\mathcal{P}_{n-1}$) Runs $B \leftarrow \text{Blind-Encrypt}(R, M, \mathsf{apk})$ and sends B to delegate $\mathcal{P}_0$.
9. (Delegate $\mathcal{P}_0$) Runs $C_{\mathsf{sum}} \leftarrow \mathsf{EG.Add}(\text{Delegate-Finish}(\alpha, B))$ and broadcasts C_{sum} to all other parties.
10. (All parties) Run $\text{Joint-Decryption}(C_{\mathsf{sum}}, (\mathsf{sk}_0, \ldots, \mathsf{sk}_{n-1}))$ and delegate $\mathcal{P}_0$ learns the plaintext result.

Asymptotic Computation Cost

Elliptic curve (EC) point multiplications in MPSI and MPSIU-Sum

Operation	MPSI		MPSIU-Sum			
	$\mathcal{P}_0$	$\mathcal{P}_i$ for $0 < i \leq n-1$	$\mathcal{P}_0$	$\mathcal{P}_1$	$\mathcal{P}_2, \ldots, \mathcal{P}_{n-2}$	$\mathcal{P}_{n-1}$
Key-Aggregation	–	–	1	1	1	1
Delegate-Start	$m+1$	–	$m(2c+1)+1$	–	–	–
Computation on R	–	$2(m+\lvert X_i\rvert)$	–	$2(m+\lvert X_1\rvert)$	$4m$	$4m$
Blind-Encrypt	–	–	–	–	–	$2mc$
Delegate-Finish	m	–	m	–	–	–
Joint-Decryption	–	–	c	c	c	c
Total	$2m+1$	$2(m+\lvert X_i\rvert)$	$(2m+1)(c+1)+1$	$2(m+\lvert X_1\rvert)+c+1$	$4m+c+1$	$(2m+1)(c+2)-1$

$m = |M| = |R| = |B|$ and c is the number of CRT moduli

Benchmarks

Runtime (in seconds) and false negative rate (FNR) for MPSI and MPSIU-Sum using 2 CRT moduli (at least 16-bits each) and 4 parties

$\lvert X_0\rvert = \lvert V_0\rvert$	$\lvert X_i\rvert$, $i > 0$	$\lvert M\rvert$	MPSI					MPSIU-Sum				
			$\mathcal{P}_0$	$\mathcal{P}_1$	$\mathcal{P}_2$	$\mathcal{P}_3$	*FNR*	$\mathcal{P}_0$	$\mathcal{P}_1$	$\mathcal{P}_2$	$\mathcal{P}_3$	*FNR*
2^{20}	2^{20}	2^{24}	80	41	49	79	$\sim 10\%$	81	52	74	145	$\sim 8\%$
2^{20}	2^{20}	2^{25}	152	72	79	144	$\sim 5\%$	191	76	111	270	$\sim 4\%$
2^{21}	2^{21}	2^{25}	156	89	89	153	$\sim 10\%$	183	103	151	303	$\sim 8\%$
2^{21}	2^{21}	2^{26}	268	158	181	307	$\sim 5\%$	299	154	236	534	$\sim 4\%$
2^{22}	2^{22}	2^{26}	299	201	214	339	$\sim 10\%$	364	193	265	602	$\sim 8\%$

Using a 64-core AMD EPYC 7742 @ 2.76 GHz with 1024GB RAM and parties running locally in serial order

`https://github.com/citp/mps-operations`

Related Work

MPSI. Constructed from many primitives.[6] Maliciously secure constructions are also known.[7] However, most protocols have only been evaluated on set sizes $\leq 2^{20}$.

Kolesnikov et al. (2017) provide benchmarks for larger sets but of protocols insecure against collusion. Bay et al. (2021) is more efficient if set sizes are much smaller (≤ 256) and number of participants higher (≤ 50).

Unbalanced MPSI-CA. Faster than past work, but increased communication.[8]

[5] Miyaji and Nishida (2015); Hazay and Venkitasubramaniam (2017); Kolesnikov et al. (2017); Inbar et al. (2018); Wang et al. (2021); Debnath et al. (2021); Badrinarayanan et al. (2021); Bay et al. (2021); Branco et al. (2021)

[6] Hazay and Venkitasubramaniam (2017); Zhang et al. (2019); Ghosh and Nilges (2019); Nevo et al. (2021); Efraim et al. (2021)

[7] Lv et al. (2020)

Related Work

PSI Sum. Only studied in the two-party case and for small X_0 ($\leq 2^{12}$).[9]

Multiparty Private Set Union. Efficient protocols known for two or three parties.[10] Multiparty protocols have not been benchmarked or implemented.[11]

Multiparty Private Set Intersection-with-Union (MPSIU) has not been formalized before.

[8] Ion et al. (2017); Chen et al. (2018); Cong et al. (2021)
[9] Kolesnikov et al. (2019); Garimella et al. (2021); Davidson and Cid (2017); Mohassel et al. (2020)
[10] Seo et al. (2012); Shishido and Miyaji (2018); Wang et al. (2020)

Extensions

Collusion. Security against any coalition of malicious participants is obtained by distributing blinding factor α such that no single party can distinguish DDH tuples

Differential Privacy.[12] Calibrated noise can be easily added during the computation of any general function (including sum) of the intersection: prevents privacy loss between re-runs

Arbitrary Functions of the Intersection. General functions of the intersection-with-union can be computed by modifying MPSIU-Sum to use FHE

External Delegation. MPSIU-Sum can be modified to allow an external party (one without an input set) to compute the protocol result

[11] Dwork (2006); Xue et al. (2017)

Thank you!

Please send questions to anunay@cs.princeton.edu

References

50 U.S.C. § 1881a.

ACLU et al. Letter from Civil Society Organizations to the Director of National Intelligence. `https://www.aclu.org/letter/coalition-letter-director-national-intelligence-dan-coats-decision-aband` June 2017.

S. Badrinarayanan, P. Miao, S. Raghuraman, and P. Rindal. Multi-party Threshold Private Set Intersection with Sublinear Communication. In *IACR International Conference on Public-Key Cryptography*, pages 349–379. Springer, 2021.

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*, 17:1–15, 2021.

References

A. Bhowmick, D. Boneh, S. Myers, K. Talwar, and K. Tarbe. The Apple PSI System. Technical report, Apple, Inc., 2021. `https://www.apple.com/child-safety/pdf/Apple_PSI_System_Security_Protocol_and_Analysis.pdf`.

P. Branco, N. Döttling, and S. Pu. Multiparty Cardinality Testing for Threshold Private Intersection. In *IACR International Conference on Public-Key Cryptography*, pages 32–60. Springer, 2021.

Brennan Center for Justice et al. Letter from Civil Society Organizations to the Director of National Intelligence. `https://www.brennancenter.org/sites/default/files/analysis/Coalition_Letter_DNI_Clapper_102915.pdf`, October 2015.

References

Brennan Center for Justice et al. Letter from Civil Society Organizations to the Director of National Intelligence. `https://www.brennancenter.org/our-work/research-reports/letter-director-national-intelligence`, January 2016.

Chair of the House Judiciary Committee. Letter from the Chair and Ranking Member of the House Judiciary Committee to the Director of National Intelligence. `https://republicans-judiciary.house.gov/wp-content/uploads/2017/04/040717_Letter-to-DNI-Coats.pdf`, April 2017.

H. Chen, Z. Huang, K. Laine, and P. Rindal. Labeled PSI from Fully Homomorphic Encryption with Malicious Security. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pages 1223–1237, 2018.

References

D. Coats. Senate Intelligence Committee: Daniel Coats Nomination Hearing. `https://www.intelligence.senate.gov/hearings/open-hearing-nomination-daniel-coats-be-director-national-intelligence`, 2017.

K. Cong, R. C. Moreno, M. B. da Gama, W. Dai, I. Iliashenko, K. Laine, and M. Rosenberg. Labeled PSI from Homomorphic Encryption with Reduced Computation and Communication. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, pages 1135–1150, 2021.

A. Davidson and C. Cid. An Efficient Toolkit for Computing Private Set Operations. In *Australasian Conference on Information Security and Privacy*, pages 261–278. Springer, 2017.

References

S. K. Debnath, T. Choudhury, N. Kundu, and K. Dey. Post-Quantum Secure Multi-Party Private Set-Intersection in Star Network Topology. *Journal of Information Security and Applications*, 58:102731, 2021.

Director of National Intelligence. Letter from the Director of National Intelligence to Senators Wyden and Udall. `https://www.wyden.senate.gov/imo/media/doc/2011-07-28%20DNI%20Letter.pdf`, July 2011.

References

Director of National Intelligence. Letter from the Director of National Intelligence to Senators Wyden et al. https://www.wyden.senate.gov/imo/media/doc/08-24-2012%20Letter%20from%20Clapper%20regarding%20FISA%20Reauthorization.pdf, August 2012.

Director of National Intelligence. Senate Intelligence Committee: Open Hearing on FISA Legislation. https://www.intelligence.senate.gov/hearings/open-hearing-fisa-legislation-0, 2017a.

References

Director of National Intelligence. Letter from the Director of National Intelligence to the Chair and Ranking Member of the House Judiciary Committee. https://www.intelligence.senate.gov/sites/default/files/documents/FISA%20QFRs%202017-06-07.pdf, July 2017b.

L. K. Donohue. Section 702 and the Collection of International Telephone and Internet Content. *Harvard Journal of Law and Public Policy*, 38, 2015.

C. Dwork. Differential Privacy. In *International Colloquium on Automata, Languages, and Programming*, pages 1–12. Springer, 2006.

A. B. Efraim, O. Nissenbaum, E. Omri, and A. Paskin-Cherniavsky. Psimple: Practical Multiparty Maliciously-Secure Private Set Intersection. *Cryptology ePrint Archive, Report 2021/122.*, 2021. https://ia.cr/2021/122.

References

Electronic Frontier Foundation. House Judiciary Committee: Letter regarding Section 702, May 2016. URL `https://www.eff.org/document/114th-congress-april-22-2016-house-judiciary-letter-702-number-american-`

G. Garimella, P. Mohassel, M. Rosulek, S. Sadeghian, and J. Singh. Private Set Operations from Oblivious Switching. In *IACR International Conference on Public-Key Cryptography*, pages 591–617. Springer, 2021.

S. Ghosh and T. Nilges. An Algebraic Approach to Maliciously Secure Private Set Intersection. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 154–185. Springer, 2019.

References

C. Hazay and M. Venkitasubramaniam. Scalable Multi-Party Private Set-Intersection. In *IACR International Workshop on Public Key Cryptography*, pages 175–203. Springer, 2017.

House Judiciary Committee. Letter from House Judiciary Committee Members to the Director of National Intelligence. `https://irp.fas.org/congress/2016_cr/hjc-702.pdf`, April 2016a.

House Judiciary Committee. Letter from House Judiciary Committee Members to the Director of National Intelligence. `https://judiciary.house.gov/sites/democrats.judiciary.house.gov/files/documents/letter%20to%20director%20clapper%20(12.16.16).pdf`, December 2016b.

References

R. Inbar, E. Omri, and B. Pinkas. Efficient Scalable Multiparty Private Set-Intersection via Garbled Bloom Filters. In *International Conference on Security and Cryptography for Networks*, pages 235–252. Springer, 2018.

Inspector General of the Intelligence Community. Letter from the Inspector General of the Intelligence Community to Senators Wyden and Udall. `https://www.wired.com/images_blogs/dangerroom/2012/06/IC-IG-Letter.pdf`, June 2012.

M. Ion, B. Kreuter, E. Nergiz, S. Patel, S. Saxena, K. Seth, D. Shanahan, and M. Yung. Private Intersection-Sum Protocol with Applications to Attributing Aggregate Ad Conversions. *Cryptology ePrint Archive, Report 2017/738*, 2017. `https://ia.cr/2017/738`.

References

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*, pages 1257–1272, 2017.

V. Kolesnikov, M. Rosulek, N. Trieu, and X. Wang. Scalable Private Set Union from Symmetric-key Techniques. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 636–666. Springer, 2019.

S. Lv, J. Ye, S. Yin, X. Cheng, C. Feng, X. Liu, R. Li, Z. Li, Z. Liu, and L. Zhou. Unbalanced Private Set Intersection Cardinality Protocol with Low Communication Cost. *Future Generation Computer Systems*, 102:1054–1061, 2020.

References

A. Miyaji and S. Nishida. A Scalable Multiparty Private Set Intersection. In *International Conference on Network and System Security*, pages 376–385. Springer, 2015.

P. Mohassel, P. Rindal, and M. Rosulek. Fast database joins and PSI for secret shared data. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, pages 1271–1287, 2020.

M. Naor and O. Reingold. Number-Theoretic Constructions of Efficient Pseudo-Random Functions. In *Proceedings 38th Annual Symposium on Foundations of Computer Science*, pages 458–467. IEEE, 1997.

References

O. Nevo, N. Trieu, and A. Yanai. Simple, Fast Malicious Multiparty Private Set Intersection. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, pages 1151–1165, 2021.

Office of the Director of National Intelligence. Letter from the Office of the Director of National Intelligence to Civil Society Organizations. `https://www.brennancenter.org/our-work/research-reports/letter-office-director-national-intelligence`, December 2015.

Office of the Director of National Intelligence. *The FISA Amendments Act: Q&A*. 2017. `https://www.dni.gov/files/icotr/FISA%20Amendments%20Act%20QA%20for%20Publication.pdf`.

References

J. H. Seo, J. H. Cheon, and J. Katz. Constant-Round Multi-Party Private Set Union using Reversed Laurent Series. In *International Workshop on Public Key Cryptography*, pages 398–412. Springer, 2012.

K. Shishido and A. Miyaji. Efficient and Quasi-Accurate Multiparty Private Set Union. In *2018 IEEE International Conference on Smart Computing (SMARTCOMP)*, pages 309–314. IEEE, 2018.

W. Wang, S. Li, J. Dou, and R. Du. Privacy-Preserving Mixed Set Operations. *Information Sciences*, 525:67–81, 2020.

Z. Wang, K. Banawan, and S. Ulukus. Multi-Party Private Set Intersection: An Information-Theoretic Approach. *IEEE Journal on Selected Areas in Information Theory*, 2(1):366–379, 2021.

References

R. Wyden and M. Udall. Letter from Senators Wyden and Udall to the Director of National Intelligence. https://www.wyden.senate.gov/imo/media/doc/2011-07-14%20Clapper%20FISA%20Letter.pdf, July 2011.

R. Wyden and M. Udall. Letter from Senators Wyden and Udall to the Inspector General of the Intelligence Community and the Inspector General of the National Security Agency. https://www.wyden.senate.gov/imo/media/doc/2012-05-04%20WydenUdall%20Letter%20to%20NSA%20on%20Estimating%20Number%20of%20Americans%20Communications%20Monitored.pdf, May 2012a.

References

R. Wyden and M. Udall. Letter from Senators Wyden et al. to the Director of National Intelligence. `https://www.wyden.senate.gov/imo/media/doc/Letter%20to%20Clapper.pdf`, July 2012b.

Q. Xue, Y. Zhu, J. Wang, and X. Li. Distributed Set Intersection and Union with Local Differential Privacy. In *2017 IEEE 23rd International Conference on Parallel and Distributed Systems (ICPADS)*, pages 198–205. IEEE, 2017.

E. Zhang, F.-H. Liu, Q. Lai, G. Jin, and Y. Li. Efficient Multi-party Private Set Intersection against Malicious Adversaries. In *Proceedings of the 2019 ACM SIGSAC Conference on Cloud Computing Security Workshop*, pages 93–104, 2019.