Confidential Truth Finding with Multi-Party Computation

Angelo Saadeh[1,6], **Pierre Senellart**[1,2,4,5,7], Stéphane Bressan[1,3,7]

[1]CNRS@CREATE LTD, Singapore

[2]DI ENS, ENS, PSL University, CNRS, Paris, France

[3]National University of Singapore, Singapore

[4]Inria, Paris, France

[5]Institut Universitaire de France, Paris, France

[6]LTCI, Télécom Paris, IP Paris, Palaiseau, France

[7]IPAL, CNRS, Singapore, Singapore

BDA 2023, Montpellier, 26 October 2023

Illustration Example

What are the capital cities of European countries?

	France	Italy	Poland	Romania	Hungary
Alice	Paris	Rome	Warsaw	Bucharest	Budapest
Bob	?	Rome	Warsaw	Bucharest	Budapest
Charlie	Paris	Rome	Katowice	Bucharest	Budapest
David	Paris	Rome	Bratislava	Budapest	Sofia
Eve	Paris	Florence	Warsaw	Budapest	Sofia
Fred	Rome	?	?	Budapest	Sofia
George	Rome	?	?	?	Sofia

Voting

Information: redundance

	France	Italy	Poland	Romania	Hungary
Alice	Paris	Rome	Warsaw	Bucharest	Budapest
Bob	?	Rome	Warsaw	Bucharest	Budapest
Charlie	Paris	Rome	Katowice	Bucharest	Budapest
David	Paris	Rome	Bratislava	Budapest	Sofia
Eve	Paris	Florence	Warsaw	Budapest	Sofia
Fred	Rome	?	?	Budapest	Sofia
George	Rome	?	?	?	Sofia
Frequence	**P.** 0.67 R. 0.33	**R.** 0.80 F. 0.20	**W.** 0.60 K. 0.20 B. 0.20	Buch. 0.50 Bud. 0.50	Bud. 0.43 **S.** 0.57

Evaluating Trustworthiness of Sources

Information: redundance, trustworthiness of sources (= average frequence of predicted correctness)

	France	Italy	Poland	Romania	Hungary	Trust
Alice	Paris	Rome	Warsaw	Bucharest	Budapest	0.60
Bob	?	Rome	Warsaw	Bucharest	Budapest	0.58
Charlie	Paris	Rome	Katowice	Bucharest	Budapest	0.52
David	Paris	Rome	Bratislava	Budapest	Sofia	0.55
Eve	Paris	Florence	Warsaw	Budapest	Sofia	0.51
Fred	Rome	?	?	Budapest	Sofia	0.47
George	Rome	?	?	?	Sofia	0.45
Frequence weighted by trust	**P.** 0.70 R. 0.30	**R.** 0.82 F. 0.18	**W.** 0.61 K. 0.19 B 0.20	**Buch.** 0.53 Bud. 0.47	Bud. 0.46 **S.** 0.54	

Iterative Fixpoint Computation

Information: redundance, trustworthiness of sources with iterative fixpoint computation

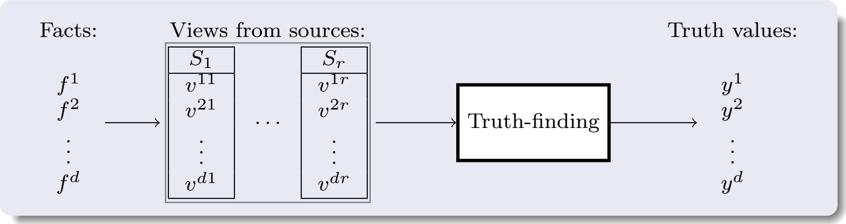
	France	Italy	Poland	Romania	Hungary	Trust
Alice	Paris	Rome	Warsaw	Bucharest	Budapest	0.65
Bob	?	Rome	Warsaw	Bucharest	Budapest	0.63
Charlie	Paris	Rome	Katowice	Bucharest	Budapest	0.57
David	Paris	Rome	Bratislava	Budapest	Sofia	0.54
Eve	Paris	Florence	Warsaw	Budapest	Sofia	0.49
Fred	Rome	?	?	Budapest	Sofia	0.39
George	Rome	?	?	?	Sofia	0.37
Frequence weighted by trust	**P.** 0.75 R. 0.25	**R.** 0.83 F. 0.17	**W.** 0.62 K. 0.20 B 0.19	**Buch.** 0.57 Bud. 0.43	**Bud.** 0.51 S. 0.49	

Formal Model

Let $f^1, \dots, f^d$ be facts/queries.

Each of the r sources inputs their view $(v^{ij})_{i=1\dots d, j=1\dots r} \in \{-1,0,1\}^{d\times r}$ of each fact.

Truth values $(y^i)_{i\in\{1,\dots,d\}} \in [-1,1]^d$

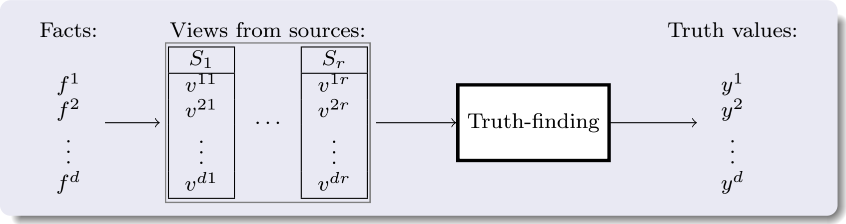


Formal Model

Let $f^1, \dots, f^d$ be facts/queries.

Each of the r sources inputs their view $(v^{ij})_{i=1\dots d, j=1\dots r} \in \{-1,0,1\}^{d \times r}$ of each fact.

Truth values $(y^i)_{i \in \{1,\dots,d\}} \in [-1,1]^d$

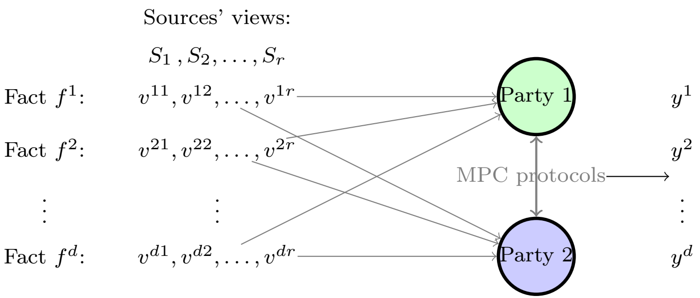


What if we want to keep the sources' views private?

Truth-finding on Confidential Views

Using **MPC** (secure multi-party computation) in truth-finding algorithms protects the views of the sources.

Asking each of the r sources for their view on d facts.

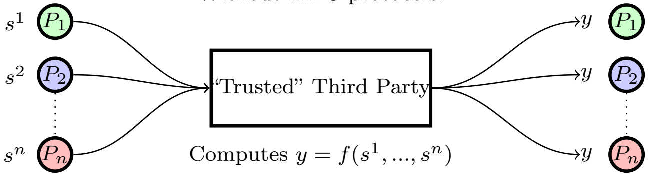


We compute $(y^i)_i \in [-1, 1]^d$ using **MPC** to protect $(v^{ij})_{i,j} \in \{-1, 0, 1\}^{d \times r}$.

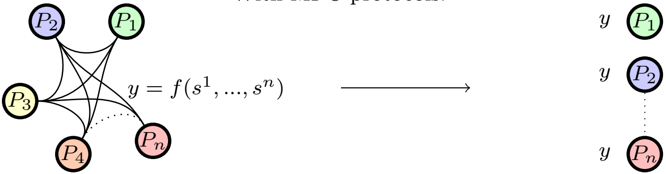
Secure Multi-party Computation (MPC)

Let f be a public function.

Without MPC protocols:



With MPC protocols:



Two-party Additive Secret-sharing

Let $l \in \mathbb{N}^*$, $\mathbb{Z}/2^l\mathbb{Z}$ a finite ring.

Two-party additive secret-sharing Π_{share} [MGW87]

Input: P_1 holds s^1

1. P_1 generates $s_2^1 \xleftarrow{\$} \mathbb{Z}/2^l\mathbb{Z}$
2. $s_1^1 \leftarrow s^1 - s_2^1 \mod 2^l$
3. P_1 sends s_2^1 to P_2

Notation: $\left[s^1\right]$ correspond to the shares s_1^1 and s_2^1 of s^1.

Computing mod 2^l is crucial to keep the shares uniformly distributed in the ring.

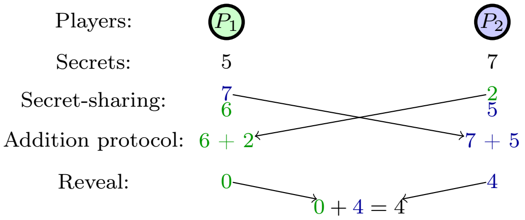
Addition protocol

Two-party addition protocol Π_{add}

Input: P_i holds x_i,y_i for i in $\{1, 2\}$
Output: P_i holds z_i for i in $\{1, 2\}$ such that $z_1 + z_2 = x + y$

1. P_i computes $z_i \leftarrow x_i + y_i$ for i in $\{1, 2\}$

Example of the sum of two secrets modulo 8:

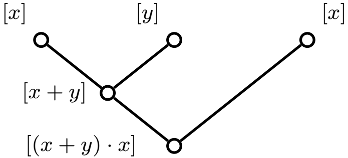


Arithmetic Circuit Evaluation in MPC

With $(x_1, x_2) \leftarrow [x]$ and $(y_1, y_2) \leftarrow [y]$ we can have:

- $(z_1, z_2) \leftarrow [x + y]$ with an addition protocol
- $(t_1, t_2) \leftarrow [xy]$ with a multiplication protocol [Bea91]

We can privately evaluate the arithmetic circuit of a function $f : (x, y) \rightarrow (x + y) \cdot x$:



From Real Elements to Finite Ring Elements [MZ17]

Real elements	Decimals	Finite Ring elements
$I = [-2^{l-p-1}, 2^{l-p-1})$	$D_{p,l} = \{k \cdot 2^{-p}, k \in \mathbb{Z}\}$	$\mathbb{Z}_{2^l} = [0, 2^l) \cap \mathbb{Z}$

$$x \longrightarrow \tilde{x} \longrightarrow \overline{x}$$

$$\text{round}(x) = k_x 2^{-p} \qquad k_x \mod 2^l$$

Example for $l = 2, p = 1$:

$I = [-1, 1)$	$D_{1,2} = \{-1, -0.5, 0, 0.5\}$	$\mathbb{Z}/2^2\mathbb{Z} = \{0, 1, 2, 3\}$
-1	$\widetilde{-1} = -1 = -2 \cdot 2^{-1}$	$\overline{-1} = -2 \mod 2^2 = 2$
-0.5	$\widetilde{-0.5} = -0.5 = -1 \cdot 2^{-1}$	$\overline{-0.5} = -1 \mod 2^2 = 3$
0.6	$\widetilde{0.6} = 0.5 = 1 \cdot 2^{-1}$	$\overline{0.6} = 1 \mod 2^2 = 1$

For simplicity, we omit the bar.

Computing Real Functions in the Finite Ring

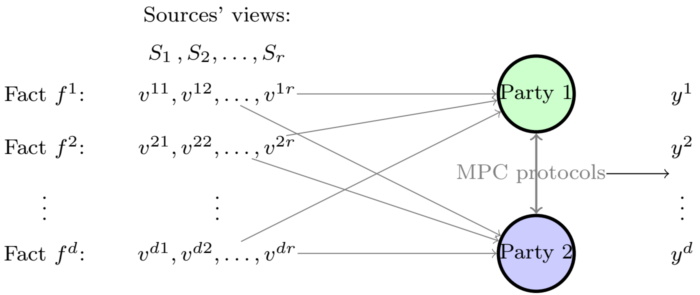
We compute the arithmetic circuits of real functions using Π_{add} and Π_{mult}.

Example: For a positive secret $[x]$ compute $\left[\frac{1}{x}\right]$ in MPC [Kno+21].

1. Define the function $g(y) = x - \frac{1}{y}$
2. Use Newton-Rapshon iterations to find the root x of g because $g(\frac{1}{x}) = 0$
3. The sequence is defined as follows: $y_{n+1} = -y_n^2 x + 2y_n$

Truth-Finding Security Model

- There are d binary facts $f^1, \ldots, f^d$
- For $i \in \{1, ..., d\}, j \in \{1, ..., d\}$, source j answers $v^{ij} \in \{-1, 0, 1\}$ to f^i
- A truth-finding algorithm returns a truth value $y^i \in [-1, 1]$ for each fact f^i



A Truth-finding Algorithm: Cosine

Simplified version of Cosine [Gal+10]

Input: The answers $(v^{ij})_{i,j}$
Output: The truth values $(y^i)_i$

1. Initialize truth values $(y^i) \leftarrow 1$
2. For a number of iterations do:
   1. For every source j:

$$\theta^j \leftarrow \frac{\sum_{i,v^{ij}=1} y^i - \sum_{i,v^{ij}=-1} y^i}{\sqrt{\left(\sum_{i,v^{ij}\neq 0} v^{ij}\right)\left(\sum_{i,v^{ij}\neq 0} (y^i)^2\right)}}$$

   2. For every fact f^j:

$$y^i \leftarrow \frac{\sum_{j,v^{ij}=1} (\theta^j)^3 - \sum_{j,v^{ij}=-1} (\theta^j)^3}{\sum_{j,v^{ij}\neq 0} (\theta^j)^3}$$

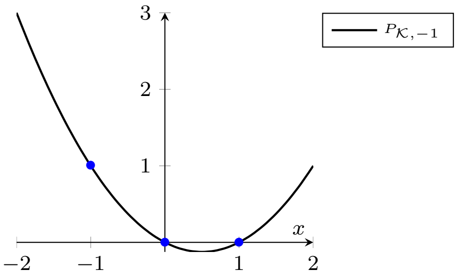
Pseudo-Equality Test with Polynomial Evaluation

For a secret $[x]$ and a public element k we need:

$$[y] = \Pi_{\text{equal}}([x], k) \text{ with } y = \begin{cases} 1 & \text{if } x = k \\ 0 & \text{otherwise.} \end{cases}$$

For truth-finding algorithms, $k \in \mathcal{K} = \{-1, 0, 1\}$.
A classic equality test could be replaced by a degree-two polynomial $P_{\mathcal{K},k}$.

Examples for $k = -1, P_{\mathcal{K},-1}(x) = \frac{1}{2}(x^2 - x)$**:**



Alternative for the Secure Inverse Algorithm for Negative Values

Secure inverse algorithm [Kno+21]:

For a secret $[x]$
If $x > 0$, the inverse is computed as:

$$[y] = \Pi_{\text{inv}}([x]) \text{ with } y = \frac{1}{x}$$

If $x < 0$, the inverse is computed as:

$$[y] = \Pi_{\text{sign}}([x]) \cdot \Pi_{\text{inv}}(\Pi_{\text{abs}}([x])) \text{ with } y = \frac{\text{sign}(x)}{|x|} = \frac{1}{x}$$

If $x < 0$, we replace the sign computation with two multiplications:

$$[y] = [x] \cdot \Pi_{\text{inv}}([x] \cdot [x]) \text{ with } y = \frac{x}{x^2} = \frac{1}{x}$$

Results on Confidential Truth-Finding

Cosine on MNIST
120 **facts and** 15 **sources**

	Non-confidential	MPC with classic inverse	MPC with optimized inverse
Wall time	10^{-4} s	0.47 s	0.44 s
Accuracy	90%	90%	90%

Results on Confidential Truth-Finding

Cosine on MNIST
120 **facts and** 15 **sources**

	Non-confidential	MPC with classic inverse	MPC with optimized inverse
Wall time	10^{-4} s	0.47 s	0.44 s
Accuracy	90%	90%	90%

3-Estimates on HubDub

	Non-confidential	MPC with classic normalization	MPC with optimized normalization
Wall time	0.02 s	52.85 s	0.58 s
Accuracy	67.59%	67.59%	67.95%

Conclusion:

Take home message:

Confidential truth-finding can be achieved with secret-sharing-based MPC

Contributions of the paper:

- MPC primitives for functions used in truth-finding
- Arithmetic MPC protocols for the equality tests on finite sets

Future research:

- Truth-finding with differential privacy
- Truth-finding algorithm that protects the facts

Machine Learning and Data

Data → **Machine Learning Algorithm** → Model

Examples of federated learning:

Data from banks → Fraud detection

Data from social media and eCommerce platforms → Marketing segmentation

Data from cars → Vehicle automation

Federated Learning with Confidential Data

Constraints:

- Data is too confidential to be shared.
- Rules and regulations prevent sharing sensitive data.

Secure Multi-party Computation (MPC) allows computing the model output without revealing any participant's secret data input.

Example of MPC to fight human trafficking by Roseman Labs:

	Sensitive data:	
NGO	Real Victims List	Stop human-traficking
Law enforcement	Potential Victims List	

Truth Finding

- Truth-finding algorithms aim to know if a statement is correct or not
- They involve collecting sources answers to queries, and analyzing the answers
- These algorithms could be used to complete missing data

Given the answers to d queries from r sources: $(v^{ij})_{i=1\dots r, j=1\dots d}$

The algorithm outputs $y^1, \dots, y^d$ the truth value of each of the d queries.

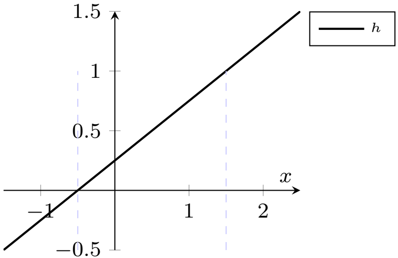
MPC-Friendly Normalization Alternative

For a vector of secrets $([x^1], \ldots, [x^n])$ we need:

$$([y^1], \ldots, [y^n]) = \Pi_{\text{norm}}([x^1], \ldots, [x^n]) \text{ with } y^i = \frac{x^i - \min_i x^i}{\max_i x^i - \min_i x^i}.$$

The goal is to scale the elements of the secret vector to $[0, 1]$ with less communication.

We apply a linear transformation $h(x) = 0.5x + 0.25$ instead of Π_{norm}:



Related work

Reference	**Algorithms**
[Chi+16; NBK15]	Majority Voting
[Mia+15; Zhe+20; ZDW18]	Conflict Resolution on Heterogeneous Data (CRH) [Li+16]
[SSB23]	Cosine and 3-Estimates [Gal+10]

Bibliography I

[Bea91] Donald Beaver. "Efficient Multiparty Protocols Using Circuit Randomization". In: *Advances in Cryptology - CRYPTO '91, 11th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1991, Proceedings.* Ed. by Joan Feigenbaum. Vol. 576. Lecture Notes in Computer Science. Springer, 1991, pp. 420–432. DOI: `10.1007/3-540-46766-1\_34` (cit. on p. 12).

[Chi+16] Ilaria Chillotti et al. "A Homomorphic LWE Based E-voting Scheme". In: *Post-Quantum Cryptography - 7th International Workshop, PQCrypto 2016, Fukuoka, Japan, February 24-26, 2016, Proceedings.* Ed. by Tsuyoshi Takagi. Vol. 9606. Lecture Notes in Computer Science. Springer, 2016, pp. 245–265. DOI: `10.1007/978-3-319-29360-8\_16` (cit. on p. 26).

[Gal+10] Alban Galland et al. "Corroborating information from disagreeing views". In: *Proceedings of the Third International Conference on Web Search and Web Data Mining, WSDM 2010, New York, NY, USA, February 4-6, 2010.* Ed. by Brian D. Davison et al. ACM, 2010, pp. 131–140. DOI: `10.1145/1718487.1718504` (cit. on pp. 16, 26).

Bibliography II

[Kno+21] Brian Knott et al. "CrypTen: Secure Multi-Party Computation Meets Machine Learning". In: *Advances in Neural Information Processing Systems 34: Annual Conference on Neural Information Processing Systems 2021, NeurIPS 2021, December 6-14, 2021, virtual.* Ed. by Marc'Aurelio Ranzato et al. 2021, pp. 4961–4973 (cit. on pp. 14, 18).

[Li+16] Yaliang Li et al. "Conflicts to Harmony: A Framework for Resolving Conflicts in Heterogeneous Data by Truth Discovery". In: *IEEE Trans. Knowl. Data Eng.* 28.8 (2016), pp. 1986–1999. DOI: 10.1109/TKDE.2016.2559481 (cit. on p. 26).

[Mia+15] Chenglin Miao et al. "Cloud-Enabled Privacy-Preserving Truth Discovery in Crowd Sensing Systems". In: *Proceedings of the 13th ACM Conference on Embedded Networked Sensor Systems, SenSys 2015, Seoul, South Korea, November 1-4, 2015.* Ed. by Junehwa Song et al. ACM, 2015, pp. 183–196. DOI: 10.1145/2809695.2809719 (cit. on p. 26).

[MGW87] Silvio Micali et al. "How to play any mental game". In: *Proceedings of the Nineteenth ACM Symp. on Theory of Computing, STOC.* ACM. 1987 (cit. on p. 10).

Bibliography III

[MZ17] Payman Mohassel et al. "SecureML: A System for Scalable Privacy-Preserving Machine Learning". In: *2017 IEEE Symposium on Security and Privacy, SP 2017, San Jose, CA, USA, May 22-26, 2017*. IEEE Computer Society, 2017, pp. 19–38. DOI: 10.1109/SP.2017.12 (cit. on p. 13).

[NBK15] Divya G. Nair et al. "An Improved E-voting scheme using Secret Sharing based Secure Multi-party Computation". 2015. arXiv: 1502.07469 (cit. on p. 26).

[SSB23] Angelo Saadeh et al. *Confidential Truth Finding with Multi-Party Computation (Extended Version)*. 2023. arXiv: 2305.14727 [cs.CR] (cit. on p. 26).

[ZDW18] Yifeng Zheng et al. "Learning the Truth Privately and Confidently: Encrypted Confidence-Aware Truth Discovery in Mobile Crowdsensing". In: *IEEE Trans. Inf. Forensics Secur.* 13.10 (2018), pp. 2475–2489. DOI: 10.1109/TIFS.2018.2819134 (cit. on p. 26).

[Zhe+20] Yifeng Zheng et al. "Privacy-Aware and Efficient Mobile Crowdsensing with Truth Discovery". In: *IEEE Trans. Dependable Secur. Comput.* 17.1 (2020), pp. 121–133. DOI: 10.1109/TDSC.2017.2753245 (cit. on p. 26).