# 隱私強化技術應用指引

數位發展部

中華民國 113 年 01 月

目錄

# 圖目錄

# 表目錄

# 壹、 簡介

## 一、 指引目的

隨著資通訊科技的進步，資料的數量及複雜度迅速增長，政府公部門或民間企業在兼顧隱私保護及資料合理利用之前提下，不可避免地須導入隱私保護措施或隱私強化技術，以增進資料當事人之信任，降低資料利用之風險，如 Google 分別將差分隱私技術及聯合學習等技術應用在 Chrome 及智慧型手機的文字輸入法[1][2]，另 Apple 也應用差分隱私技術於 macOS 及 iOS 系統之使用者回饋資訊[3]；Microsoft 則提供具差分隱私之資料庫查詢服務[4]，以進一步保障查詢分析結果之隱私。

隨著人工智慧、巨量資料探勘等技術之高速發展，傳統隱私強化技術，如直接刪除辨識碼方法或 k-匿名化等方式，正面臨隱私保護有效性的挑戰。如 2006 年 Netflix 宣稱不含使用者資訊之資料集遭有心人士與其他外部資料進行比對及連結，導致其使用者隱私外洩[5]；2018 年美國人口普查局（U.S. Census Bureau）研究小組，運用新興資料庫重建技術，將已經過隱私強化處理之 2010 年美國人口普查結果連結其他公開資料，進行再識別還原測試，結果顯示有高達 46%的內容可部分還原[6]。

---

[1] “Learning statistics with privacy, aided by the flip of a coin”, Google Online Security Blog. Available: https://security.googleblog.com/2014/10/learning-statistics-with-privacy-aided.html. Accessed: Aug 31, 2023.

[2] Brendan McMahan & Daniel Ramage, “Federated Learning: Collaborative Machine Learning without Centralized Training Data”, Apr. 2017. Available: https://blog.research.google/2017/04/federated-learning-collaborative.html. Accessed: Aug 31, 2023.

[3] “Learning with Privacy at Scale”, Apple Machine Learning Research. Available: https://machinelearning.apple.com/research/learning-with-privacy-at-scale. Accessed: Aug 31, 2023.

[4] “Private SQL: A Differentially Private SQL Query Engine”, Microsoft Research, Apr. 2019. Available:https://www.microsoft.com/en-us/research/video/private-sql-a-differentially-private-sql-query-engine/. Accessed: Aug 31, 2023.

[5] E. L. T.- Ravens, “Data Privacy — The Netflix Prize competition”, Medium, Jul. 2022. Available: https://medium.com/@EmiLabsTech/data-privacy-the-netflix-prize-competition-84330d01cc34. Accessed: Aug 31, 2023.

[6] 陳艷秋，「美國人口普查避免個別資料揭露方法之變革」，主計月刊, no. 802, pp. 74–79, 2022.

有鑑於傳統隱私強化技術存在安全性及有效性之疑慮，國際上陸續推動新興隱私強化技術之政策與法規制定，如聯合國於 2020 年成立聯合國隱私強化技術實驗室（UN PET Lab），並與美國人口普查局、荷蘭中央統計局（Statistics Netherlands）、義大利國家統計局（Italian National Institute of Statistics）以及英國國家統計局（UK’s Office for National Statistics）共同合作，展開測試計畫，藉由隱私強化技術的導入，促進資料共享並同時兼顧資料之安全性與合規性[7]。此外，為了推廣隱私強化技術，UN PET Labs 亦舉辦黑客松（Hackathon）比賽，參賽者須藉由差分隱私、合成資料、可信執行環境完成為時 3 天的競賽[8]。美國於 2021 年之民主高峰會中，亦將隱私強化技術視為支持民主國家之基本人權與共享價值的新興技術，並宣布美國與英國為推動隱私強化技術發展將舉辦創新技術獎項[9]；英國資訊委員辦公室（Information Commissioner’s Office，ICO）則於 2023 年 6 月發布《隱私強化技術指引》[10]，將常見的 8 種新興隱私強化技術，包含：同態加密、安全多方運算、私有集合交集、聯合學習、可信執行環境、零知識證明、差分隱私、合成資料等納入指引，詳細介紹各技術之優缺點、與「個人資料保護相關法規」遵循之關聯、應用時之注意事項、相關風險等內容，提供組織依其目的，評估並選擇適當之隱私強化技術。

綜整上述說明，隱私強化技術已然成為確保資料使用安全性的重要工具。然而，隱私強化技術如何運用於不同應用情境，以增進個人或隱私資料之保護，同時維持資料之可用性，亦成為各組織進行資料應用及治理時亟待克服的課題。有鑑於此，本指引參考國際相關文獻，提出具指標性隱私強化技術之運作概念、應用情境、施用風險與限制，並提供應用案例，希冀透過本指引之制定，使大眾對於隱私強化技術有更深入的了解。此外，也期待本指引能有效鼓勵政府公部門或民間企業藉由導入隱私強化技術，降低資料利用之風險、增進資料當事

7 “UN launches first of its kind ‘privacy lab’ to unlock benefits of international data sharing,” The UN Committee of Experts on Big Data and Data Science, Dubai, UAE; London, UK., Jan. 25, 2022. [Online]. Available: https://unstats.un.org/bigdata/events/2022/unsc-un-pet-lab/UN PET Lab - Press Release - 25 Jan 2022.pdf Accessed: Jan. 15, 2024.

8 “UN PET Lab’s Hackathon”. Available: https://petlab.officialstatistics.org/. Accessed: Aug. 31, 2023.

9 “National Strategy To Advance Privacy-Preserving Data Sharing And Analytics The United Nations Guide On Privacy-Enhancing Technologies For Official Statistics”., United States Government, Available: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Strategy-to-Advance-Privacy-Preserving-Data-Sharing-and-Analytics.pdf Accessed: Aug 31, 2023.

10 “ICO call for views: Privacy-enhancing technologies guidance”, Jun. 2023. Available: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies/. Accessed: Jan. 13, 2024.

人信任及強化隱私保護。

二、 名詞解釋

1. 假名化（Pseudonymization）：以編碼或別名替換個人識別資訊之過程，亦稱為擬匿名化。
2. 匿名化（Anonymization）：個資不可逆地變更之過程，以此方式，使得無法直接或間接識別個資當事人。
3. 去識別化（De-Identification）：移除識別資料與個資當事人連結的過程。
4. 資料最小化（Data Minimisation）：將資料之處理限制於與處理目的具有適當性、關聯性及必要性。
5. k-匿名性（k-Anonymity）：一種隱私保護力指標，表示資料集中的任何一筆資料，其可用於識別出個體的背景資訊皆至少與 k-1 筆資料相同。
6. t-相似性（t-Closeness）：一種隱私保護力指標，表示攻擊者利用特定個人的資訊，查詢到的敏感資訊機率分佈與整體資料表之差異，是否不超過 t。一旦攻擊者查詢到的機率分佈與整體資料表差異過大，可藉由資料表推敲出特定個人的敏感資訊。
7. ℓ-多樣性（ℓ-Diversity）：一種隱私保護力指標，表示攻擊者利用特定個人的資訊，查詢到的敏感資訊數值是否至少有 ℓ 種。一旦攻擊者查詢到的數值種類過少，可藉由資料表推敲出特定個人的敏感資訊。
8. 再識別風險（Re-Identification Risk）：攻擊者從已去識別化處理之資料表識別出特定個人的風險。
9. 鏈接攻擊（Linkage Attack）：一種針對表格資料的隱私攻擊方式，攻擊者透過對照其他資料表，識別出已去識別化之資料表裡的特定個人。
10. 可擴展性（Scalability）：指系統能夠因應資料或處理的任務增加的擴充能力。
11. 過度擬合（Overfitting）：指機器學習模型在訓練過程中過度適應訓練資料，導致對新資料的預測能力下降，出現預測誤差增加的情況。
12. 隱私預算（Privacy Budget）：一種量化指標，衡量在保護資料隱私的前提

下，進行資料查詢或資料分析的最大程度。當預算用完，進一步的查詢或分析皆可能增加隱私洩漏風險。

**13.** 私密資訊擷取（Private Information Retrieval）：一種隱私強化技術，可在不揭露檔案辨識資訊的情況下，從伺服器下載檔案。

**14.** 私有集合交集（Private Set Intersection）：一種隱私強化技術，可使兩個參與方在不透露原始資料集的情況下，求取兩方資料集之交集。

**15.** 可搜尋式加密（Searchable Encryption）：一種隱私強化技術，可使資料在加密的情況下，能夠支援搜尋功能。

**16.** 可信執行環境（Trusted Execution Environments）：一種隱私強化技術，創造一個與主系統並行的安全、隔離執行環境來處理敏感資料。

**17.** 零知識證明（Zero-Knowledge Proofs）：一種隱私強化技術，可使一個參與方在不透露原始資料的情況下，向另一方證明其擁有某秘密資訊。

**18.** 拉普拉斯雜訊機制（Laplace Mechanism）：一種差分隱私的實現機制，其在資料中加入呈拉普拉斯分佈的雜訊，使攻擊者難以辨識出個人。

**19.** 高斯雜訊機制（Gaussian Mechanism）：一種差分隱私的實現機制，其在資料中加入呈高斯分佈的雜訊，使攻擊者難以辨識出個人。

**20.** 指數雜訊機制（Exponential Mechanism）：一種差分隱私的實現機制，其在資料中加入呈指數分佈的雜訊，使攻擊者難以辨識出個人。

**21.** 隨機回應機制（Randomized Response）：一種差分隱私的實現機制，透過提供具隨機性的回答來達成隱私保護。

**22.** 資料保真度（Fidelity）：經合成資料處理之資料在統計上與原始資料相符的程度。

**23.** 對抗式生成網路（Generative Adversarial Network）：一種基於兩個類神經網路相互對抗的機器學習方式。

**24.** 蒙地卡羅模擬法（Monte Carlo Method）：一種基於亂數產生以及隨機抽樣的合成資料方法。

**25.** 貝氏網路（Bayesian Network）：可應用於合成資料方法中的一種機率模型，是基於隨機變數之間利用聯合機率分佈以局部表示的拓撲變化。

**26.** 模型偏差（Bias）：模型的預測值與真實數值之間的系統性誤差或錯誤。

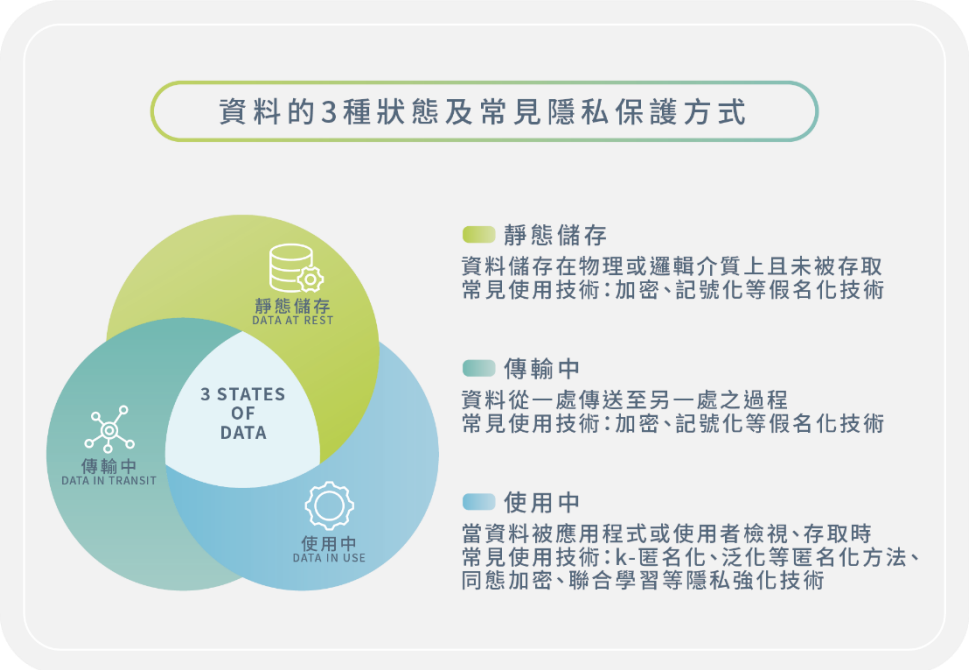
**27.** 列聯表（Contingency Table）：一種統計學工具，用於呈現兩個或多個變數之間的關係，通常用於探討不同變數的交互作用或相關性。

# 貳、　什麼是隱私強化技術

## 一、　隱私強化技術概述

廣義上隱私強化技術（Privacy Enhancing Technologies, PETs）可泛指所有用於保護資料隱私或資料機敏性之技術方法。包含加密確保資料於傳輸（in transit）及靜態儲存（at rest）時的機密性及各種已發展成熟的傳統去識別化技術，如記號化（tokenization）等假名化技術，以及 k-匿名化（k-anonymization）、泛化等匿名化方法。

於全球發展資料驅動治理及創新的趨勢下，各種新興的隱私強化技術也引領隱私保護方法的革新，這類技術更強化保障資料在使用階段（in use）的隱私安全，也更著重於為時下資料應用場景所面臨之隱私挑戰，衡平隱私保護與資料運用需求，透過技術方法降低直接利用原始資料所衍生之風險，同時保有資料可用性。




▲圖一、資料的 3 種狀態及常見隱私保護方式

上圖參考自[11]並經指引編輯團隊重新繪製。

[11] Sealpath.com, Inc, “The Three States of Data Guide - Description and How to Secure them,” Protecting the three states of data, Jun. 23, 2020. https://www.sealpath.com/blog/protecting-the-three-states-of-data/ Accessed: Sep. 07, 2023.

舉例來說：

1. 針對提供資料供機器學習或資料分析應用，可採生成對抗網路（Generative Adversarial Network, GAN）產生以假亂真的合成資料，進而提供該合成資料進行後續應用，避免提供原始資料所衍生的風險，亦兼顧資料的可用性。
2. 隨雲端運算盛行，可採用同態加密技術，讓資料維持在加密狀態進行運算，運算過程中皆無需解密，在零信任的時代提供最根本的機敏性保障。
3. 進行具敏感性資料蒐集或調查時，可採用安全多方運算保障參與調查者的隱私，即便是主辦調查單位，亦僅可獲得總體計算的結果，而無從得知任何個別參與調查者之原始資料，進而增進參與者的意願。

（一） 常見的傳統去識別化技術有哪些？

**1.** 抑制/編修（Suppression/Redaction）：將資料集內的識別資料移除或以標籤置換之，如：僅保留身分證字號後 6 碼或將身分證字號欄位刪除。

**2.** 遮罩（Masking）：對資料局部置換為特殊符號，如：○或※。

**3.** 記號化（Tokenization）：將原始資料變化為另一組隨機產生，但與真實資料樣態相同之值，如：將身分證字號置換為另一組符合身分證字號編碼原則的字號，但不是真實資料。

**4.** 雜湊化（Hashing）：將敏感資訊套用函數產生出固定長度的雜湊值，並取代原始資料，如 SHA-256。

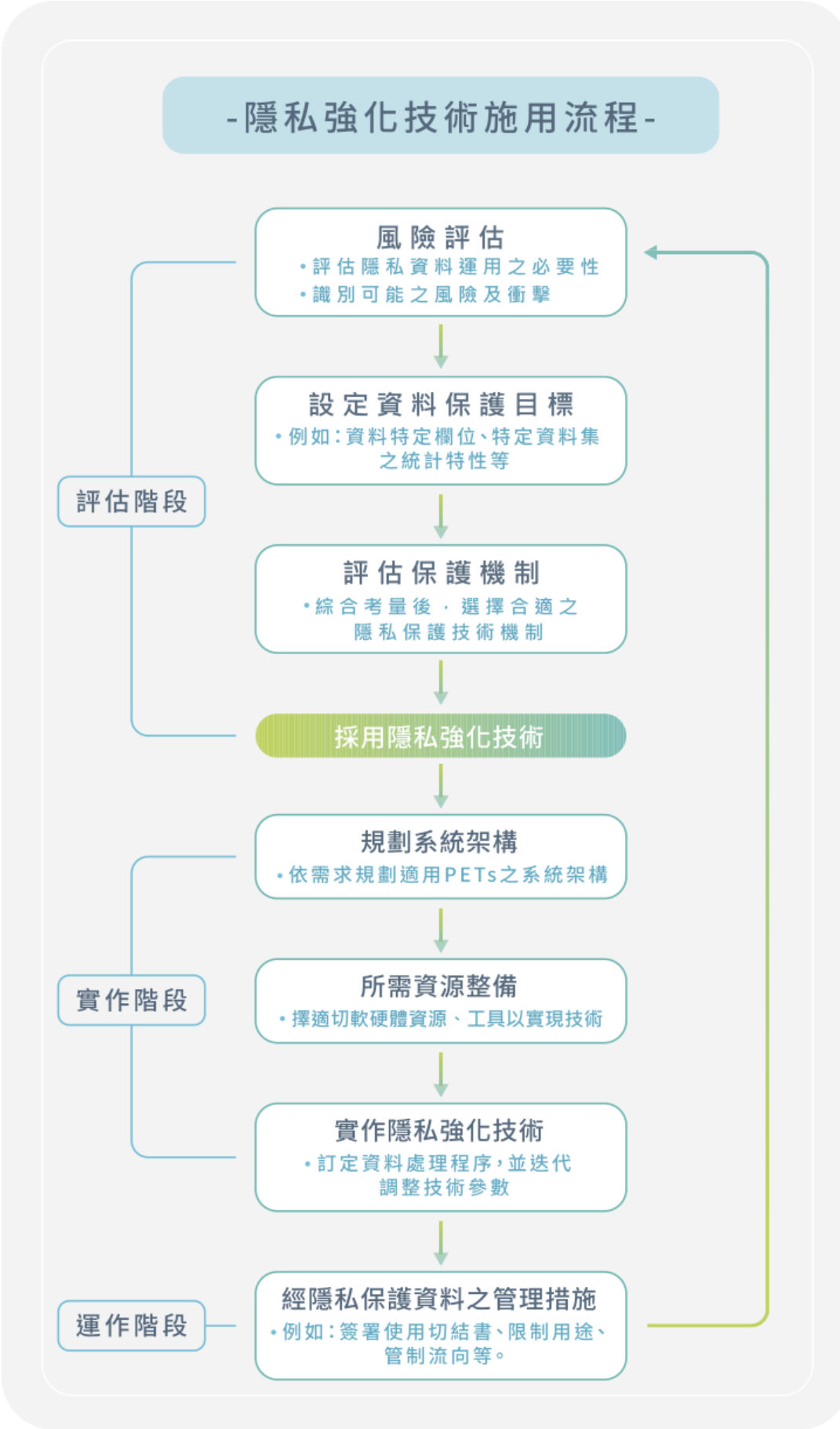
**5.** 泛化（Generalization）：依預先定義之層次結構，降低識別資料之精確度，如：將年齡 25 歲，泛化為年齡 20~29 歲。

**6.** k-匿名化（k-anonymization）：結合各種去識別化技術，並確保經處理之資料集的任何一筆資料，其可用於識別出個體的背景資訊皆至少與 k-1 筆資料相同。

## 二、　隱私強化技術施用流程

隱私強化技術種類繁多，個別技術具有不同之資源需求及投入成本，當組織進行資料之蒐集、處理及利用時，應評估採取具有適當比例原則之安全措施。

下列之施用流程即以風險評估之結果作為是否使用隱私強化技術之評估參考，並由組織設定隱私保護之目標情境(如保護隱私資料於蒐集階段之機密性)，評估適宜之隱私保護技術機制，並於實作階段規劃系統架構、整備所需資源、進行技術實作，於運作階段應將經隱私強化處理之資料納入風險評估，並定期執行，以因應如法規、技術環境變遷等內外部因素。




▲圖二、隱私強化技術施用流程

（二） 流程說明

1. 評估階段

(1) 風險評估：針對資料之蒐集、處理及利用過程進行評估，識別隱私保護要求事項、可能之風險及衝擊等級，以利進行後續風險處理。

(2) 設定資料保護目標：根據評估之結果，為應用場景之各關係人設定資料保護目標，進行風險處理，以降低隱私風險之可能性或其衝擊。資料保護目標可能視資料的用途、資料類型或資料流而有所不同，如可設定保護資料於儲存、傳輸或運算之機密性、可用性或完整性。

(3) 評估保護機制：依據所設定之資料保護目標，考量實作及維護所需之資源、人員知能等因素，以選擇適合之隱私保護技術機制，如假名化、匿名化、去識別化及差分隱私等隱私強化技術。

2. 實作階段

(1) 規劃系統架構：定義資料流、規劃隱私強化技術與參數選用、設計如何與現有環境、異質系統整合協同運作。

(2) 所需資源整備：隱私強化技術種類繁多，且單一技術可能有多種開源工具可供運用，原則上應採用穩定版或最新版之開源工具。

(3) 實作隱私強化技術：依資料之用途及所採用隱私保護技術之特性，以資料最小化為原則訂定如資料前置處理、隱私保護技術之特定參數（如差分隱私之雜訊參數）、取樣程序等，其中，部分前置處理或參數設定會經歷測試、迭代調整的過程。

3. 運作階段

(1) 經隱私保護資料之管理措施：經隱私強化技術處理後之資料如授權（或委任）予特定對象使用，建議採行適當之管理措施，如簽署使用切結書、限制用途、管制流向等。

(2) 定期辦理風險評估：採用隱私強化技術後，定期評估經隱私強化技術處理後資料之剩餘風險、隱私保護要求事項、對組織或當事人權益之可能衝擊、技術環境改變等內外部因素，進行風險評估。

## 三、 隱私強化技術之分類與應用

隱私強化技術的採用展現組織在資料保護和資料最小化的實際作為。適當技術使用也可在資料使用合規前提下，解決原本無法實現之資料分享與應用。本章節將介紹技術原理和適用情境之分類，及技術選用時需要考量的因素。

在資料傳輸和儲存（in transit, at rest）狀態加密是普遍的資料保護機制，而在資料使用（in use）階段，組織可利用代換識別碼達成假名化或利用傳統常見的去識別化做法，例如直接移除機敏欄位、遮罩（masking）、泛化（generalization）等，以及綜合利用上述方法達成 k-匿名化。

新興的隱私強化技術包含多種技術方法，更著重於為資料使用（data in use）階段提供隱私保障，並平衡隱私保護與資料運用需求。

### （三） 技術原理分類

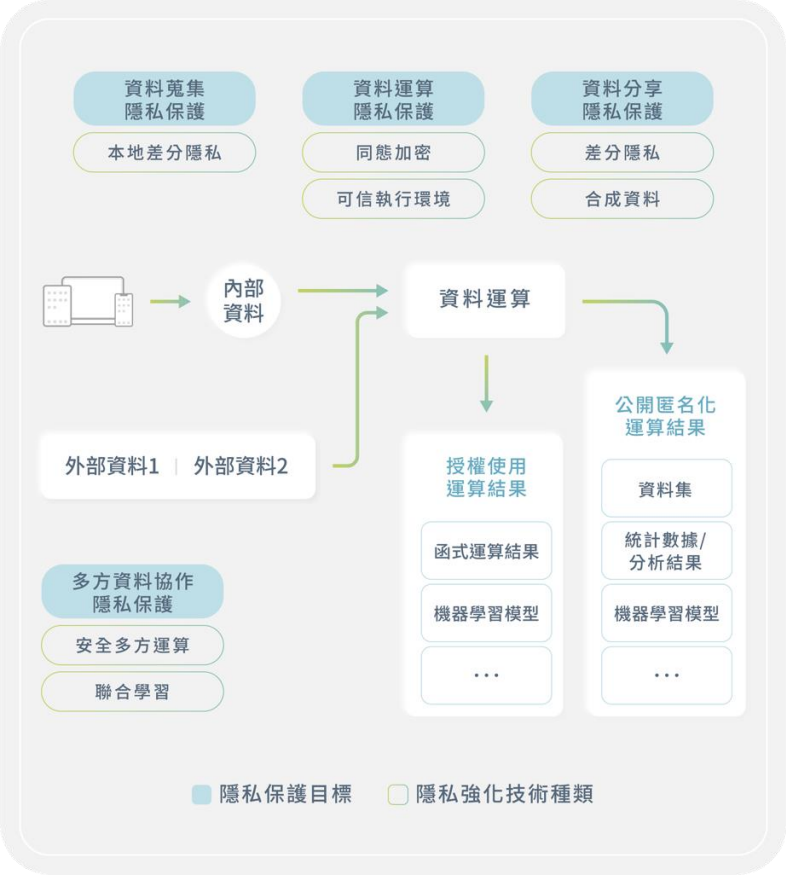
根據技術之運作原理，主要可以區分為：

1. 改變原始資料以減少或移除個人識別資訊：此類技術之目的為減弱或破壞有關個人及衍生資料間的關聯，同時保留原始資料的特性以增進衍生資料的可用性。與原始資料相比，此類方法產生之資料準確性可能較低，亦或其應用結果將與原資料衍生結果有差距，所以較不適合需精確結果之應用。此類技術如差分隱私、合成資料，以及傳統的去識別化方法。
2. 對原始資料進行保密性處理後進行操作：此類技術之目的為保護個人隱私，同時不影響資料的可用性和準確性。資料能在加密狀態下進行運算或在不揭露原始資料下達到應用之目的。此類方法常伴隨額外的運算和傳輸時間。此類技術包括同態加密、安全多方運算（包含私有集合交集）、零知識證明、可搜尋式加密、私密資訊擷取。

**3.** 設計系統運算機制達到資料保護效果：此類技術之目的為最大限度地減少隱私資料的共享，同時確保資料機密性、完整性，並兼顧資料的可用性及準確性。此類方法透過系統和資料運算架構設計，定義資料存取、運算方法和子系統間溝通與認證機制。如聯合學習、可信執行環境。

（四） 應用場景分類

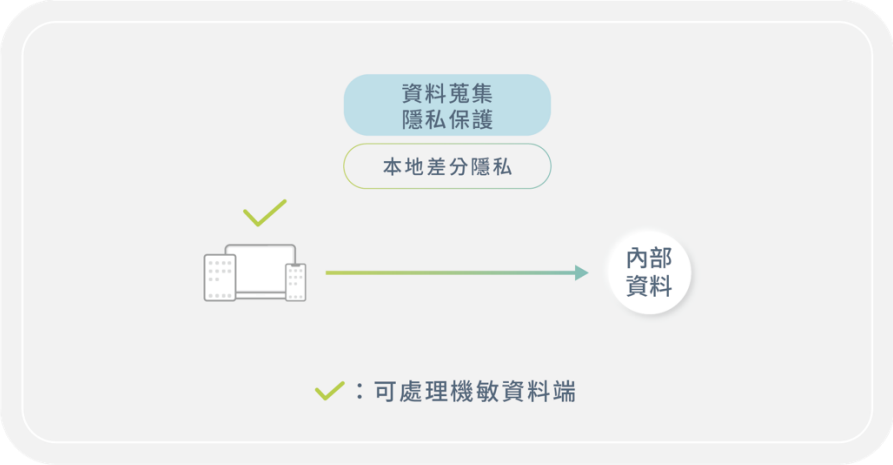
不同隱私強化技術依據資料提供者、協作者、資料量、運算目的、運算結果分享對象等因素，適用在不同使用情境。一般而言，資料經隱私強化技術運算的結果樣態可包括匿名化資料集、統計分析結果、機器學習模型、協議之共同運算函式結果等；其中運算的結果分享對象又可分成對外公開或授權使用。在整個資料處理流程中，依情境在不同階段中有不同隱私保護的挑戰，圖三描繪出不同隱私強化技術所對應的場景與隱私保護目標：




▲圖三、隱私保護目標及適用之隱私強化技術[12]

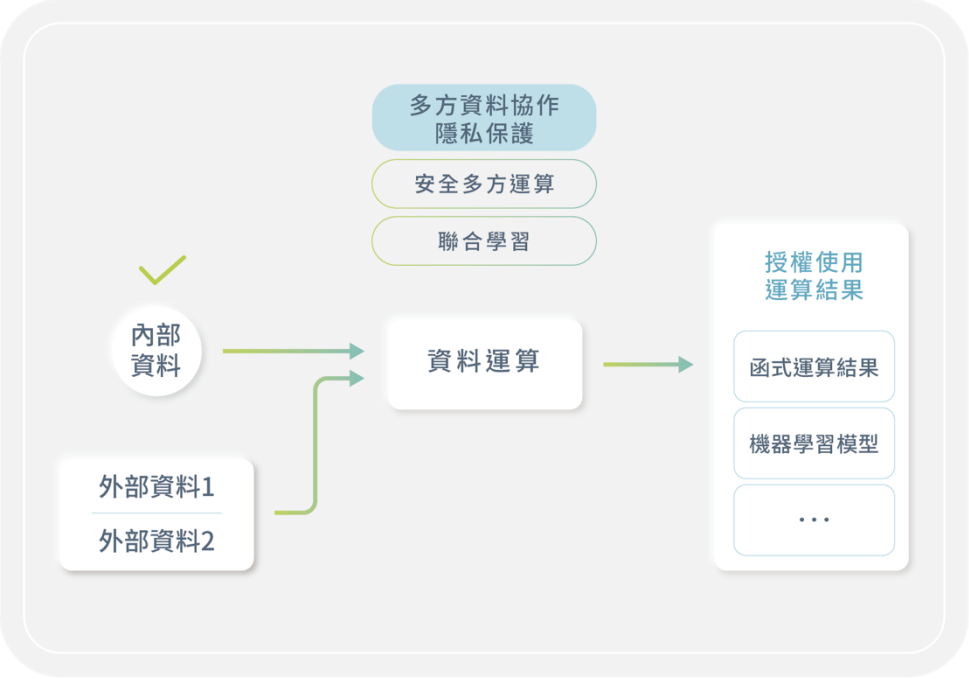
12 TUMULT Labs https://www.tmlt.io/

1. 資料蒐集：資料從終端蒐集階段在傳送至資料庫前便進行隱私保護，終端裝置或使用者的資料可經由本地端差分隱私或是初步資料統計技術，以達到原始資料無法從資料庫被辨識，如圖四所示。



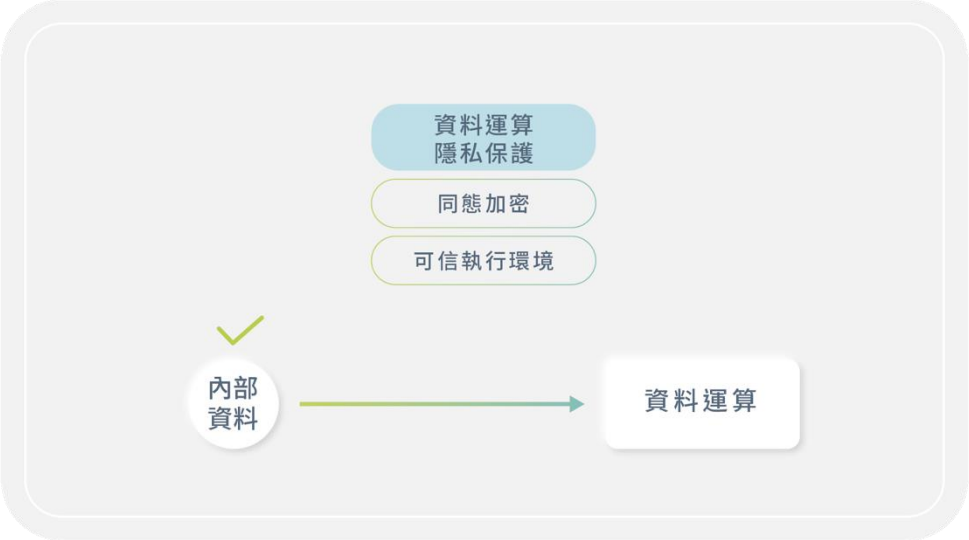

▲圖四、隱私強化技術對應資料蒐集示意圖

2. 多方資料協作：圖五表示運算資料來源來自多方，且須在多方資料協作下兼顧隱私保護，安全多方運算可用於多方共同協議的運算函式，使授權之其中數方或所有參與運算的協作者獲得結果。另外，聯合學習可用於協作目標為共同訓練機器學習模型的情境，透過各方本地端使用其資料訓練本地端模型，最後整合成精確度更高的模型供參與協作者使用。



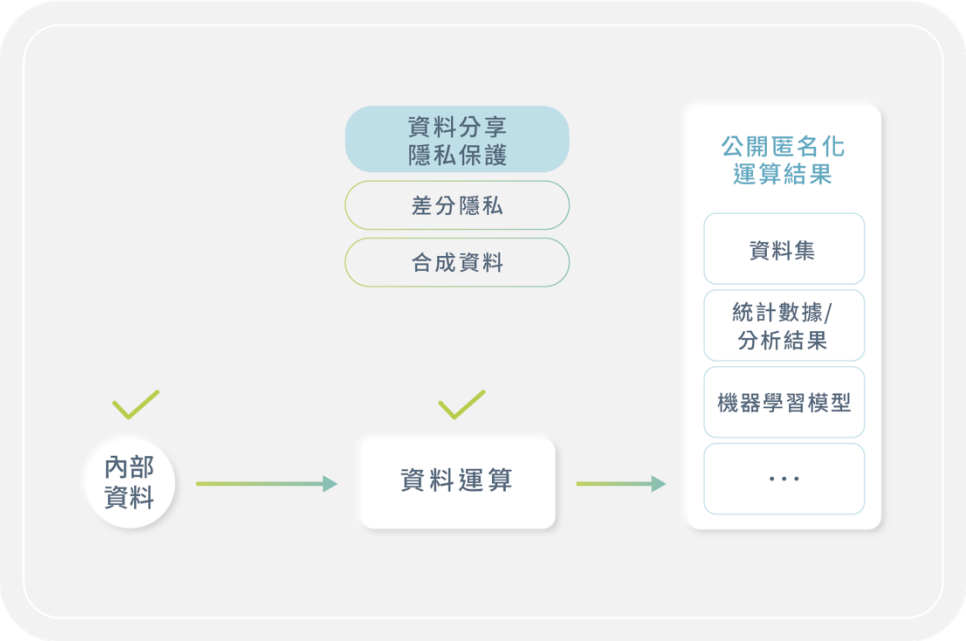

▲圖五、隱私強化技術對應多方資料協作情境示意圖

3. 資料運算：同態加密可在資料加密的狀況下進行運算，並獲得正確的運算結果。可信執行環境利用硬體的方法使得在特定的運算處理器和記憶體區塊可存取機敏資料，確保只有受認證的程式碼可以使用機敏資料作運算。基於運算階段的隱私保護，若多方協調好互操作性機制，此類技術也能達到多方資料協作的效果。




▲圖六、隱私強化技術對應資料運算情境示意圖

4. 資料分享：圖七表示資料處理的目的為分享資料集以供外界再利用並確保資料集之隱私保護，傳統 k-匿名化、差分隱私、合成資料可作為資料集準備的方法。其中 k-匿名化是過去較為普遍的做法，其使資料集中無法從至少有 k 筆資料中辨別個別紀錄，但 k-匿名化資料集曾發生透過外部公開資訊比對而被再識別的個案。差分隱私透過加雜訊在資料集中，使其無從判斷單一原始紀錄是否存在資料集中，其背後具有隱私保護強度的數學證明。合成資料多利用數學建模或機器學習等方式產生資料集。此類應用的技術選擇多在隱私保護強度和資料可用性間進行權衡。若資料集釋出目的是分享統計分析結果，並希望避免資料集遭鏈結外部資訊而被再識別，在資料集釋出過程中運用差分隱私可解決此問題。類似的概念，在訓練模型過程中，對訓練資料或於模型參數更新過程套用差分隱私亦可保障公開模型之隱私。




▲圖七、隱私強化技術對應資料分享情境示意圖

真實世界的應用案例多樣且複雜，將多種技術合併使用是常見的做法。下表[13]彙整各隱私強化技術的概述與比較。詳細技術細節將在「具指標性之隱私強化技術」章節中介紹。

[13] The National Science and Technology Council, "National Strategy to Advance Privacy-Preserving Data Sharing and Analytics," Washington, DC, USA, Mar. 2023. [Online] Available: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Strategy-to-Advance-Privacy-Preserving-Data-Sharing-and-Analytics.pdf

▼表一、各隱私強化技術的概述與比較表

| 技術 | 說明 | 價值 | 限制 |
|---|---|---|---|
| k-匿名化 | 結合各種去識別化技術，並確保經處理之資料集的任何一筆資料，其可用於識別出個體的背景資訊皆至少與 k-1 筆資料相同。 | 減少重新辨識的風險。 | 該技術僅可處理表格類資料，無法處理影像或聲音等資料。由於該技術之原理為將資料集分成若干相等群組，若資料分布過於分散或資料量過少，會有過度匿名化的情況發生，以至於降低資料集之資料可用性。經處理之資料集，若與額外的公開訊息相互對照，則容易受到再識別攻擊，可透過 ℓ-多樣性（ℓ-diversity）及 t-相似性（t-closeness）等進階技術增強隱私保護。 |
| 差分隱私 | 對原始資料添加雜訊，使攻擊者無法判斷個人的資料是否有包含在原始資料集之中。 | 降低資料重建或鏈接攻擊的可能性，並提供具數學證明的隱私保證。 | 該技術僅適用於表格資料，無法處理影像或聲音等資料。資料集的屬性欄位個數若過多，或資料分佈過於分散，容易大幅降低處理後資料之可用性。應用該技術時須在隱私保護及資料可用性之間進行取捨，以達成平衡。在設定的隱私保證之下，欲保護的資料集之資料筆數越多越好，才可讓雜訊較成功地互相抵銷，獲得較佳的資料可用性。 |
| 合成資料 | 以人工合成的資料做為真實資料的替代品。 | 保留原始資料集整體的屬性或特性。 | 原始資料需具備一定資料量，以供該技術學習其資料分佈特徵。且因其技術特性，不宜對合成資料中之個別紀錄進行再處理及利用。合成之資料易受原始資料之既有誤差影響，使用時應考慮原始資料之誤差。合成之資料仍有可能洩漏原始資料集中的隱私敏感訊息，可透過差分隱私等技術增強隱私保護。 |

| 技術 | 說明 | 價值 | 限制 |
| --- | --- | --- | --- |
| 安全多方運算 | 允許多方執行共同協議之運算函式，使授權之數方或所有參與運算的協作者取得運算結果。 | 在不洩露原始資料的情況下，取得分散式資料的運算結果。 | 計算和通訊成本/負擔較高。依據選用協議與參與方數量之不同，可能需多輪通訊方能完成計算，較不適合於有頻寬限制或網路狀態不佳之環境使用。處理浮點數時效率較低，易有溢位風險。 |
| 同態加密 | 可在資料加密的狀況下進行運算，並獲得正確的運算結果。 | 只有授權使用者可以檢視明文之原始與/或計算資料。 | 使用全同態加密進行加密後所得的密文大小，可能擴張達數十萬或數百萬倍，因此應審慎評估，只對必要的資料進行加密。此外同態加密所需運算資源龐大，且存在運算延遲，較不適合注重即時性的應用。可視應用情境，讓具有運算能力的一方或採雲端計算服務匯集加密資料進行運算，最後再回傳結果。 |
| 零知識證明 | 可使一個參與方在不透露原始資料的情況下，向另一方證明其擁有某秘密資訊。 | 在不洩露敏感訊息的情況下提高驗證訊息的能力。 | 在使用零知識證明時，必須確保資料的可靠性，因為任何不正確的資料都可能導致錯誤的證明。使用零知識證明時，必須將欲陳述之內容轉換為特殊格式，但轉換可能依陳述內容之複雜程度，使所需空間急遽擴大，進而增加計算負擔。 |
| 可信執行環境 | 創造一個與主系統並行的安全、隔離執行環境來處理敏感資料。 | 與加密技術相比，允許對資料進行更快的安全分析。 | 可信執行環境可能有限制處理的資料量大小，且該技術需透過硬體實現，因此需要支援該技術之相關硬體。若該技術執行之程式存在漏洞，或運行於虛擬機器上，則有可能使該技術的保護能力失效。 |
| 聯合學習 | 允許多個實體在不共享原始資料的情況下，共同分散式地協作機器學習模型訓練。 | 在訓練共同模型時最小化共享的資料。 | 各種資料重建或推理攻擊仍有可能發生。不同資料提供者之間的資料量和特徵可能存在差異，需要進行資料轉換和對齊，並需留意模型參數傳輸時的風險，通常需搭配其他隱私強化技術如差分隱私、同態加密一同使用。 |

## 四、 隱私強化技術應用之挑戰

隱私強化技術並非隱私保護之萬靈丹。適當使用可降低資料隱私風險和提升資料可用性。所有資料處理仍須符合法律規範、公平及透明原則。在技術採用和實際案例整合需考量以下潛在挑戰：

### （一） 部份技術成熟度不足

隱私強化技術種類多樣，但並非所有技術皆發展成熟，因此使用隱私強化技術時，需仔細評估其成熟度和使用風險。舉例來說，可能有些新興技術缺乏可擴展性（Scalability），導致無法處理大量資料，也可能是技術缺乏標準或規範，導致實作時無所依循，或者是技術過於理論，導致難以實作，甚至是技術尚無法有效抵禦攻擊，可能洩漏隱私資訊[14]。

### （二） 實作不佳與設定錯誤

若實作或使用隱私強化技術工具時，缺乏專業知識、理解錯誤，可能造成技術實作與理論之間存在落差，或是輸出資料無法達到保護力與可用性的適當平衡[15]，最終導致輸出資料錯誤、難以實際應用或洩漏隱私資訊。

### （三） 驗測機制未臻明確

部分隱私強化技術屬於新興科技，尚未發展統一之技術標準、國際規範或得以驗證其隱私保護效力之機制，若驗測實作機制仍不夠明確完整，可能導致個人資料被洩漏的風險[16]。

---

[14] Information Commissioner's Office, "Privacy-enhancing technologies (PETs)." Jun. 2023. [Online]. Available: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies/

[15] *Id.*

[16] The European Union Agency for Cybersecurity (ENISA), "PETs controls matrix - A systematic approach for assessing online and mobile privacy tools," Sep. 2016.

## （四） 合規性挑戰

依我國個人資料保護法第 2 條第 1 款，個人資料係指各種得以直接或間接方式識別個人之資料，為避免個資當事人人格權受侵害，其蒐集、處理及利用過程皆受個人資料保護法規範。因此，如將個人資料進行去識別化等技術處理，使資料無法用於直接或間接識別當事人，即非受個人資料保護法所保護之客體（111 年憲判字第 13 號判決參照）。

本指引將現行具指標性之隱私強化技術歸納為以下 3 類：第 1 類為「改變原始資料以減少或移除個人識別資訊」，如差分隱私、合成資料；第 2 類為「對原始資料進行保密性處理後進行操作」，如同態加密、安全多方運算（包含私有集合交集）、零知識證明；第 3 類為「透過設計系統運算機制達到資料保護效果」，如聯合學習、可信執行環境。這些新興的技術採用有別於傳統去識別化技術之技術原理，為資料應用提供具隱私保護的解決方案。惟需注意的是，經隱私強化技術處理後之個人資料，未必能與去識別化之資料劃上等號，例如：經差分隱私處理後之個人資料，若設定之「隱私預算」較高，所含可識別個人之資訊亦可能較高，因而再識別之風險較高。

觀測先進國家如歐盟及英國，於隱私強化技術使用與合規性間亦面臨相同之課題，惟因歐盟 GDPR（General Data Protection Regulation）個人資料處理之安全性（第 25 條、第 32 條）及英國 Data Protection Act 2018 皆規範有關個人資料處理之權利及自由之保護，須採取適當之技術性或組織性措施，亦即，控管者應採取符合「設計（by design）與預設（by default）資料保護」之規則與措施。而隱私強化技術之採用即可作為組織遵從 GDPR 及 Data Protection Act 2018 之佐證。我國個人資料保護法及其施行細則第 12 條第 2 項亦有相似規範，即依該條第 1 項所採取之措施與欲達成之個人資料保護目的間，具有適當比例為原則之安全措施。雖然運用隱私強化技術處理後的特定資料是否已脫離個人資料保護法適用範圍，尚需個人資料保護法之主管機關個案判斷，但隱私強化技術能於合規前提下為個人資料之蒐集、處理及利用提供實質的隱私保護，並可作為採行符合比例原則安全措施之法規遵循性證明。

# 參、 具指標性之隱私強化技術

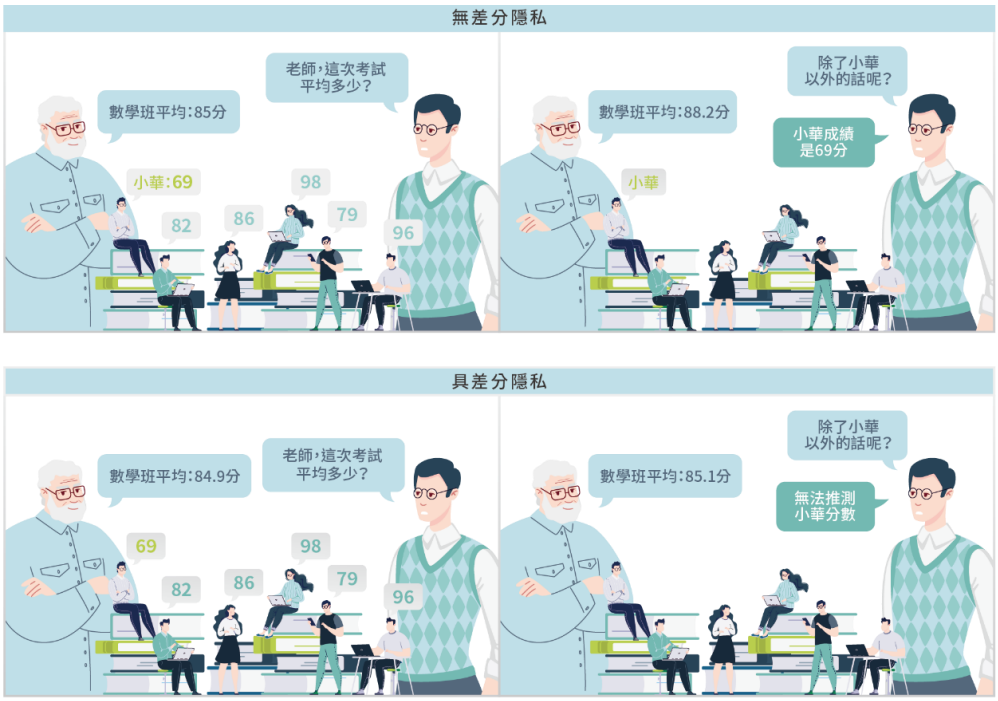
## 一、 差分隱私（Differential Privacy）

### （一） 技術說明

**1.** 技術概述：

差分隱私（Differential Privacy, DP）是一種保護個人資料隱私的方法，通過在資料中加入一定的雜訊，使得資料釋出後不會揭露個人資訊。差分隱私廣泛應用於資料共享、資料挖掘、機器學習等領域，可有效保護敏感資訊的隱私，同時保持資料的可用性和可分析性。

差分隱私的原理可理解成，若對僅有一筆紀錄不同的兩個資料庫比對分析，無論兩者差異是加入、刪除或修改該筆紀錄，其透過隨機演算法的分析結果將不會有重大差異，即分析結果的差異是可控的。這也意味著一個具有差分隱私保護的系統或演算法在分析過程中能有效地隱藏個人的參與資訊。換言之，差分隱私透過設定隱私損失（ε，或稱隱私預算）提供了可量化的隱私保護框架，可以應用於各種資料分析與資料共享的服務，並確保個人隱私得到適當的保障。




▲圖八、差分隱私運用情境示意圖

**2.** 欲解問題：資料共享在當今數位時代中扮演著重要的角色，它帶來了許多優點和益處，包含促進各種加值應用、決策支援、促進服務最佳化等，使資料發揮一加一大於二的協同效應。以醫療資料共享為例，醫院或醫療機構之間共享病人的醫療紀錄與健康資訊，有助於疾病研究和醫療改進。然而，潛在的隱私風險包括醫療檔案中所記錄的個人敏感資訊（例如疾病診斷、處方藥物等）可能被洩漏，導致侵犯個人隱私等問題。為了應對這些潛在的隱私風險，差分隱私技術適用於資料共享情境中。在資料蒐集階段，透過在資料中添加適當的雜訊，差分隱私技術可以確保即使在具有詳細訊息的資料集中，也無法準確識別特定個體的敏感資訊。這樣的技術機制有助於保障資料當事人的隱私，可促進資料當事人參與資料蒐集的意願。同時，在資料釋出階段，由於差分隱私技術確保資料釋出不會揭露個人的敏感資訊，並且添加的雜訊符合統計分布的限制，資料的可用性相較於傳統匿名化技術更有利於各種科學用途。

**3.** 發展沿革：差分隱私的起源可以追溯到 2006 年，當時 Cynthia Dwork 等人[17]提出了差分隱私的定義。起初，差分隱私的主要技術是基於拉普拉斯雜訊機制（laplace mechanism）或指數雜訊機制（exponential mechanism），以保護釋出的資料。這些機制能夠量化和控制資料分享時的隱私洩漏風險。在 2008 年，美國普查局首次應用差分隱私來發布通勤模式的統計資料[18]。除了政府部門，Google 在 2014 年提出了 RAPPOR 方法，以基於差分隱私的統計方法收集 Chrome 瀏覽器的使用者資料[19]。隨著機器學習在資料分析中的重要性不斷增加，2016 年，Martín Abadi

[17] C. Dwork, F. McSherry, K. Nissim, and A. Smith, “Calibrating noise to sensitivity in private data analysis,” in Theory of cryptography: Third theory of cryptography conference, new york, NY, USA: Springer, Mar. 2006, pp. 265–284. [Online] Available: https://people.csail.mit.edu/asmith/PS/sensitivity-tcc-final.pdf

[18] A. Machanavajjhala, D. Kifer, J. Abowd, J. Gehrke, and L. Vilhuber, “Privacy: Theory meets practice on the map,” in 2008 IEEE 24th international conference on data engineering, IEEE, 2008, pp. 277–286. [Online] Available: https://ieeexplore.ieee.org/abstract/document/4497436

[19] Ú. Erlingsson, V. Pihur, and A. Korolova, “Rappor: Randomized aggregatable privacy-preserving ordinal response,” in Proceedings of the 2014 ACM SIGSAC conference on computer and communications security, 2014, pp. 1054–1067. [Online] Available: https://dl.acm.org/doi/abs/10.1145/2660267.2660348

等人提出 Advanced Composition 方法，解決了過去差分隱私在神經網路訓練中效果不彰的問題[20]。同年，歐盟通過了《一般資料保護規則》（GDPR），其中將差分隱私作為一種可行的資料保護方法之一[21]。自此以後，差分隱私技術被廣泛應用於各個產業或學術研究中[22][23][24][25][26][27][28]。差分隱私在保護個人隱私的同時，為資料共享和分析提供了一種有效的解決方案，成為當今數據時代中不可或缺的技術之一。

[20] Abadi, Martin, et al. “Deep learning with differential privacy.” Proceedings of the 2016 ACM SIGSAC conference on computer and communications security, 2016.
[21] The Working Party on the Protection of Individuals with regard to the Processing of Personal Data, “Opinion 05/2014 on Anonymisation Techniques.” Apr. 10, 2014. [Online] Available: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf
[22] Apple Inc., “Apple previews iOS 10, the biggest iOS release ever.” Accessed: Aug. 31, 2023. [Online] Available: https://www.apple.com/newsroom/2016/06/apple-previews-ios-10-biggest-ios-release-ever/
[23] B. Ding, J. (Jana) Kulkarni, and S. Yekhanin, “Collecting Telemetry Data Privately,” presented at the Advances in Neural Information Processing Systems 30, Long Beach, CA, USA, Dec. 2017. Available: https://www.microsoft.com/en-us/research/publication/collecting-telemetry-data-privately/
[24] Privitar Ltd, “Enterprise Data Privacy Management Software & Tools,” Privitar. https://www.privitar.com/products/data-privacy-software/ (accessed Aug. 31, 2023).
[25] The OpenDP Team, “OpenDP Library.” Sep. 01, 2023. Accessed: Sep. 03, 2023. [Online] Available: https://github.com/opendp/opendp
[26] R. Rogers et al., “LinkedIn’s Audience Engagements API: A privacy preserving data analytics system at scale,” 2020, [Online] Available: https://arxiv.org/abs/2002.05839
[27] U. C. Bureau, “Understanding Differential Privacy”, 2020. Available: https://www.census.gov/programs-surveys/decennial-census/decade/2020/planning-management/process/disclosure-avoidance/differential-privacy.html. Accessed: Aug 31, 2023.
[28] “Past Prize Challenges”, NIST, May 24, 2019. Available: https://www.nist.gov/ctl/pscr/open-innovation-prize-challenges/past-prize-challenges. Accessed: Aug 31, 2023.

**4.** 技術現況：在差分隱私領域，目前存在多種技術變形和應用，並且這些技術的發展日益成熟。若資料擁有者欲就其所蒐集之資料於釋出或是共享前強化隱私保護，則可考慮採用全域差分隱私，一般來說簡稱為差分隱私。而在全域的設定中，有兩種差分隱私設定，分別為純粹差分隱私與近似差分隱私。前者最普遍的機制為拉普拉斯機制，即通過向結果加入具有拉普拉斯分佈的雜訊來保護資料的隱私，並由於該機制沒有 $\delta$（錯誤機率）的概念而被視為嚴格的差分隱私機制；後者利用高斯機制，其可以保證近似差分隱私。該機制所加入的雜訊為高斯分佈產生，這將使分布更加連續和平滑，可獲得較高的資料可用性，但有微小機率（$\delta$）會產出隱私保護程度不足（隱私損失風險超過 $\varepsilon$）之資料集。本地端差分隱私（local differential privacy）的情境設定與全域差分隱私不同；具體來說，在本地端差分隱私時，蒐集資料的伺服器被認為是不可信任的，所以每個握有部分資料集的使用者將不再直接送出原始資料給伺服器。取而代之地是每個使用者將會先對手上的原始資料進行隱私處理之後才送出給伺服器。要達到本地端差分隱私的機制包含了上述的拉普拉斯機制與高斯機制外，隨機回應機制（randomized response）也更常被運用在本地端差分隱私。

差分隱私的數學定義如下：
令隱私預算 $\varepsilon$ 為一正實數，而 $A$ 為一隨機演算法，以一資料庫為該演算法的輸入。令 $S$ 為演算法 $A$ 所映射的空間。若對所有僅有一筆紀錄（例如某個人的資料）不同的兩個資料庫 $D_1$ 和 $D_2$，以及 $S$ 的所有子集 $s$，符合下列不等式，則稱該演算法 $A$ 可以提供 $\varepsilon$-差分隱私。其中，機率的隨機性來自於演算法 $A$。

$$P_r[A(D_1) \in s] \leq exp\,(\varepsilon) \cdot P_r[A(D_2) \in s]$$

## （二） 適用情境

差分隱私技術適用於許多應用場景，特別適合於組織已擁有一份原始資料欲透過技術方式產製兼顧資料隱私保障及資料可用性之開放資料或共享資料的情境。隨人工智慧、探勘技術等技術發展，相較過去常被運用在相似情境的傳統去識別化技術，差分隱私提供了具有數學證明的隱私強度保證，有助於確保隱私保護的有效性。以美國人口普查為例[29]，其研究小組運用新興資料庫重建技術，將已經過隱私處理之 2010 年美國人口普查結果，進行再識別還原測試，即發現有大量的個人資料能夠被還原[30]。為強化隱私保護的有效性，美國人口普查局於 2020 年所釋出的人口普查資料即改以基於差分隱私的保護框架，實現對參與普查使用者的資訊防護。此外，隨著各界對於個人資料及隱私保護意識提升，相應的規範也趨於嚴謹，許多企業仍有蒐集用戶資訊進行產品開發及優化的需求，其為了保障用戶資訊並避免觸犯法規而付出天價罰款[31][32]，差分隱私技術扮演了重要的技術解方，如 Google 發展 RAPPOR[33]演算法，在即時蒐集使用者資訊時運用差分隱私技術，確保回傳資料的隱私保障。

如欲採用差分隱私作為產製合成資料之核心技術時，建議考量下列面向之適用性：

1. 資料面：資料集在日後不會有增刪資料的情況，並且資料集的屬性欄位個數不宜過多，以避免資料分布呈稀疏狀態，進而造成差分隱私合成資料的可用性降低。另為符合差分隱私定義，資料利用時必須將每筆紀錄視為單一個體，各筆紀錄之間並無關聯性。
2. 架構面：演算法設計要能支援多執行續以縮短資料處理的時間成本，並

[29] U. C. Bureau, supra note 27, at 24.
[30] U. C. Bureau, “The Census Bureau’s Simulated Reconstruction-Abetted Re-identification Attack on the 2010 Census”. Available: https://www.census.gov/data/academy/webinars/2021/disclosure-avoidance-series/simulated-reconstruction-abetted-re-identification-attack-on-the-2010-census.html. Accessed: Aug 31, 2023.
[31] C. Page, “EU hits Amazon with record-breaking $887M GDPR fine over data misuse”, Jul 30, 2021. Available: https://techcrunch.com/2021/07/30/eu-hits-amazon-with-record-breaking-887m-gdpr-fine-over-data-misuse/. Accessed: Aug 31, 2023.
[32] European Data Protection Board, “1.2 billion euro fine for Facebook as a result of EDPB binding decision | European Data Protection Board”, May 22, 2023. Available: https://edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en. Accessed: Aug 31, 2023.
[33] Ú. Erlingsson, V. Pihur, and A. Korolova, supra note 19, at 23.

且也要考慮記憶體消耗而採用切分批次檔案讀寫的設計，因為資料屬性的資料定義域空間（domain space）通常會非常龐大。

3. 可用性：由於差分隱私的技術原理是將雜訊加入資料或是演算法以保障資料隱私，如期望最後運算結果（如單行平均、神經網路預測等）可獲得較好的資料可用性，循經驗法則應盡可能的提升原始資料集的資料筆數，以利加入的雜訊能成功地互相抵銷。反之，如原始資料分布過於發散，則差分隱私合成資料的可用性亦將受到局限。

（三） 技術施用風險

如欲採用差分隱私作為產製合成資料之核心技術時，建議將下列運算資源及硬體成本納入評估：

1. 基於差分隱私技術的合成資料通常需要進行資料預處理，將資料集各屬性的值進行數值化（string to integer）或離散化，並建立字典檔以使得最後產生的合成資料可以對應回原始資料集的域（domain），此處理需考慮記憶體和效能上的權衡。
2. 依差分隱私合成資料生成演算法的類型可分為以下 2 類，參數化方式多為基於神經網路的做法，故可應用 GPU 提升運算效能，而非參數化之做法則受限於技術實作限制，大多無法應用 GPU 加速運算。

▼表二、差分隱私合成資料生成演算法比較表

| 演算法類型 | 參數化（parametric） | 非參數化（non parametric） |
|---|---|---|
| 運作概念 | 利用如神經網路的機器學習模型學習資料樣態並產生資料 | 以統計列聯表（contingency table）依機率採樣產生資料 |
| GPU 適用性 | 透過大量的樣本學習可提升資料準確性，GPU 記憶體為影響時間成本的關鍵要素 | 資料屬性的資料定義域空間會直接受到 CPU 記憶體限制，使得演算法設計上需進行動態追蹤，大多無法應用 GPU 加速運算 |

（四） 開源工具與社群

參考工具之維護狀況、社群活躍度、Github star 數/fork 數、可支援模型和隱私方法、說明文件和教學檔案，經綜合評估列舉差分隱私之開源工具如下。

▼表三、差分隱私開源工具分析表

| 工具名稱 | 開發語言 | 基本文字介紹 | 優缺點/擅長解決之問題 |
|---|---|---|---|
| google/ differential-privacy | C++/ Go/ Java/ Python | 該套件庫包含用於計算 $\varepsilon$ 或（$\varepsilon, \delta$）差分隱私統計資訊的常見函數，例如實現拉普拉斯機制和高斯機制所需加入雜訊，以及隱私花費的計算。 | • 拉普拉斯機制和高斯機制之累計隱私花費計算。<br>• 多種常見統計函數之全域敏感度計算及對應雜訊生成。 |
| Opacus | Python | 該套件庫支援 PyTorch 在具有差分隱私的情況下進行訓練，並且對於整體運算效能影響較小。同時，套件庫也允許即時累計隱私花費的計算（常搭配 DP-SGD 使用）。此外，服務對象主要為機器學習的使用者。 | • 要轉化為差分隱私版本，僅需修改部分程式碼。<br>• 支援累計隱私花費的計算。 |
| Diffprivlib | Python | 該套件庫支援多種差分隱私模型的訓練，包含分群法、分類器、回歸預測等，並且操作上和 Scikit-learn 套件庫模式一樣而好上手。 | • 訓練差分隱私模型。<br>• 操作方式與 Scikit-learn 相同。<br>• 不支援自訂雜訊加入方式或作用位置。 |
| ARX | Java | 該套件庫為針對個人隱私資訊進行匿名化的綜合開源軟體，如 k-匿名化、差分隱私語意模型等。同時，該套件庫還提供了匿名化資料的可用性驗證與隱私驗證的方法。 | • 支援多種經典資料去識別化方法。<br>• 支援差分隱私語意模型的訓練。<br>• 匿名化資料的資料可用性分析。<br>• 匿名化資料的再識別風險分析。 |
| OpenDP | Rust | 該套件庫支援多種基於不同差分隱私模型的統計 | • 支援多種統計分析模型。 |

| 工具名稱 | 開發語言 | 基本文字介紹 | 優缺點/擅長解決之問題 |
| --- | --- | --- | --- |
| | | 分析，並提供周邊工具，供使用者建構完整差分隱私系統。 | • 支援評估參數設定與資料失真程度的關係。<br>• 提供建構報告、儀表板之工具以協助評估處理效果。 |

## （五） 標準

▼表四、差分隱私之標準統整表

| 標準名稱 | 標準編號 | 發布組織 | 類型 | 發布日期 | 標準說明 |
|---|---|---|---|---|---|
| 隱私增強資料去識別化術語與技術分類（Privacy enhancing data de-identification terminology and classification of techniques） | ISO/IEC 20889:2018 | ISO/IEC | 標準 | 2018-11 | 本標準描述了隱私增強資料去識別化技術，並根據 ISO/IEC 29100 準則設計資料去識別化措施，其中明確定義各種技術之分類，並闡述了降低再識別風險的適應性。<br>此標準適用於各類型、規模之組織，包括公有和民營企業、政府部門以及非營利團體等，並且作為個人可識別資訊（PII）的管控者或代表把關者身分行事之 PII 管理者，得實施資料去識別化流程以達隱私增強保護目的。 |
| 資訊技術－安全技術－個人資訊去識別化過程管理系統－要求事項（Information technology − Security techniques − Requirements for a personal information de-identification process management system） | CNS 29100-2:2019 | 經濟部標檢局 | 標準 | 2019-09 | 本標準為國內自訂之國家標準，主要遵循我國個人資料保護法及其施行細則，並參考 ISO 29100 系列、ISO 27018（資訊技術－安全技術－公用雲 PII 處理者保護個人可識別資訊（PII）之作業規範）等國際標準所訂定。 |

## （六） 示範性案例

**1.** 擬真情境案例：以差分隱私實現具隱私保護之科研資料共享-以糖尿病預測資料為例

**2.** 實際案例

▼表五、差分隱私之實際案例列表

| 參與者 | 描述 | 使用技術 | 開發成熟階段 |
|---|---|---|---|
| 美國普查局<br>大眾 | 美國普查局公開普查資料讓大眾使用時，透過差分隱私技術加入雜訊，兼顧隱私保護力與資料可用性。資料集包括美國不同種族人口與居住地相關敏感資料。資料處理流程是先依據地理單位由大至小計算統計資料，再依隱私洩漏風險與隱私預算 $\varepsilon$ 值加入雜訊。 | 差分隱私之 TopDown 演算法[34] | 正式上線 |
| BankCo<br>金融服務業者<br>金融機構 | BankCo 金融服務業者透過安全多方運算技術，在不透漏原始資料的情況下，協助金融機構評估客戶信用風險。其資料來源多樣，包含來自債務催收機構、信用卡發行機構、公開紀錄等的個人財務資訊。金融服務業者從各來源蒐集原始資料後，對原始資料加入差分隱私雜訊，執行並產出分析結果供金融機構應用。 | 差分隱私 | 正式上線 |
| 韓國政府、私人企業 | 韓國統計局結合同態加密、安全多方運算與差分隱私等技術，在不暴露敏感資訊的狀況下，讓政府各部門的資料可以安全的連結與使用。此應用試辦之資料為韓國統計局登記之各企業詳細資訊，如機構名稱、公司登記號碼與行政區碼。過程中資料會在加密的狀態下進行連結與分析。 | 同態加密、安全多方運算、差分隱私 | 應用試辦 |

[34] J. Abowd, D. Kifer, S. Garfinkel and A. Machanavajjhala, “Census TopDown: Differentially Private Data, Incremental Schemas, and Consistency with Public Knowledge”, 2019. Available: https://www.semanticscholar.org/paper/Census-TopDown%3A-Differentially-Private-Data%2C-and-Abowd-Kifer/cd020070f56f155a45e13ee404109edf3f452ebc. Accessed: Aug 31, 2023.

| 參與者 | 描述 | 使用技術 | 開發成熟階段 |
| --- | --- | --- | --- |
| 帝濶智慧科技<br>聯新國際醫療<br>資料服務公司 | 為確保資料（資料服務公司會員行為分析、醫療科學研究資料及數位化轉型資料共享）於雲端儲存、釋出使用及資料分析階段之隱私保障。資料服務公司、新國際醫療與帝濶智慧科技，合作試辦結合差分隱私、同態加密技術等技術，以生成合成資料、分析去識別化資料及安全加密檔案管理系統。該系統提供資料擁有者多種隱私強化方案，於資料上傳至雲端前進行去識別化或加密處理，經處理之資料保存於雲端平台，供後續查詢、釋出及結合其他保存於雲端平台之跨機構資料進行跨域分析。 | 合成資料、<br>差分隱私、<br>可搜尋加密、<br>同態加密 | 應用試辦 |

## 二、 合成資料（Synthetic Data）

### （一） 技術說明

**1.** 技術概述：合成資料是一種生成資料的技術，藉由數學模型或演算法，產生與真實資料相近的人造資料，其具有真實資料的統計特徵與結構，可以在不透漏真實資料的情況下，替代真實資料進行統計分析、機器學習訓練等應用。此技術被廣泛應用於軟體測試、消除機器學習模型偏差、標註深度學習資料標籤與保護隱私資料等不同用途。合成資料的應用廣泛，本指引主要針對有助於隱私保護的應用進行說明及闡述。

**2.** 欲解問題：在當今數位化時代，資料需求的不斷增長以及對資料隱私與安全問題的日益關注，部分資料涉及隱私，需要受到嚴格保護的情況下，如何兼顧資料使用效益與隱私安全，便是一個重要的課題。如機器學習等資料應用中，當訓練的資料量及品質提升越有機會獲得可用性高之輸出結果。不過這樣的資料可能洩漏敏感資訊，特別是涉及高度敏感的個人資訊（如健康資料）的資料分析及應用時，一旦洩漏可能會侵害資料當事人權利並造成嚴重負面影響，因此通常使用這些資料集時必須依循法規[35]，如我國個人資料保護法等。而為了滿足法律規範之資料保護程度，使用傳統匿名化技術可能使資料缺損，降低資料可用性，以致於無法得到良好應用成果。合成資料技術則為可解決上述痛點的解決方式之一，其產生近於真實資料的人造資料，具有相同統計特徵與結構，可以替代真實資料進行應用，具備高度資料可用性，且同時保障真實資料之隱私。

[35] J. Jordon et al., “Synthetic Data – what, why and how?”, 2022, Doi: 10.48550/ARXIV.2205.03257. Available: https://arxiv.org/abs/2205.03257. Accessed: Aug 31, 2023.

**3.** 發展沿革：合成資料技術最早始於 1940 年代，由 Stanislaw Ulam 與 John von Neumann 開創性地使用蒙地卡羅模擬法生成資料[36]，不過當時並未考慮隱私保護應用。直到 1990 年代，Donald Rubin 與 Roderick Little 提出方法[37][38][39]，可以讓合成資料替代真實資料進行運用而不侵犯隱私，並產生了一個基於美國人口普查、可公開散播的資料集，開啟了應用於隱私保護的合成資料技術根基。而近年來隨著機器學習的發展，也出現了許多基於機器學習的生成資料方式，例如 Ian Goodfellow 提出的對抗式生成網路 (Generative Adversarial Networks, GAN)，為現今廣泛使用的合成資料技術。

[36] N. Metropolis and S. Ulam, “The Monte Carlo Method”, Journal of the American Statistical Association,vol.44, no.247, pp. 335–341, Sep. 1949, Doi: 10.1080/01621459.1949.10483310. Available: http://www.tandfonline.com/doi/abs/10.1080/01621459.1949.10483310. Accessed: Aug 31, 2023.

[37] D. B. Rubin, “Multiple Imputation for Nonresponse in Surveys”, in "Wiley Series in Probability and Statistics”. Wiley, 1987, Doi: 10.1002/9780470316696. Available: https://onlinelibrary.wiley.com/doi/book/10.1002/9780470316696. Accessed: Aug 31, 2023.

[38] D. B. Rubin, “Discussion: Statistical Disclosure Limitation”, Journal of Official Statistics, vol.9, no.2, pp. 461–468, 1993. Accessed: Aug 31, 2023.

[39] R. J. A. Little, “Statistical analysis of masked data”, Journal of Official Statistics, vol.9, no.2, pp. 407–426, 1993. Accessed: Aug 31, 2023.

4. 技術現況：基於合成資料產生的方式，可歸納為機器學習、數學建模、隨機生成三種方式：

(1) 機器學習方式，透過真實資料訓練機器學習模型，產生新的人造資料，常見的模型如對抗式生成網路 GAN，基於兩個類神經網路相互對抗，其優點是能夠平行化生成資料[40]。

(2) 數學建模方式，透過數學模型模擬真實資料分佈，產生新的人造資料，常見的模型如貝氏網路，基於隨機變數之間的條件依賴關係，其優點是可以處理不同種類之大型資料集[41]。

(3) 隨機生成方式，透過隨機事件產生新的人造資料，常見的演算法有蒙地卡羅模擬法，基於亂數產生以及隨機抽樣，其優點是運算效率快[42]。

隱私保護程度取決於透露真實資料之資訊量多寡，透露之資訊量越少，安全性越高[43]。機器學習與數學建模兩種合成資料方式，目前皆有結合差分隱私之相關研究，以評估與保護隱私安全[44][45]。

## （二） 適用情境

合成資料技術適用於需要共享資料集給第三方使用，卻因資料保護問題或資料缺損，無法直接提供真實資料的情境，如提供資料集供其他組織進行科學研究、產品測試開發、機器學習訓練等應用。實際應用案例包含：英國臨床研

40 I. Goodfellow, " 2016 Tutorial: Generative Adversarial Networks", 2017, Doi: 10.48550/ARXIV.1701.00160. Available: https://arxiv.org/abs/1701.00160. Accessed: Aug 31, 2023. 76..

41 G. Gogoshin, S. Branciamore and A. S. Rodin, "Synthetic data generation with probabilistic Bayesian Networks", Mathematical Biosciences and Engineering, vol.18, no.6, pp. 8603–8621, 2021, Doi: 10.3934/mbe.2021426. Accessed: Aug 31, 2023.

42 D. P. Kroese, T. Brereton, T. Taimre and Z. I. Botev, "Why the Monte Carlo method is so important today, WIREs Comp Stat", vol.6, no.6, pp. 386–392, Nov. 2014, doi: 10.1002/wics.1314. Available: https://onlinelibrary.wiley.com/doi/10.1002/wics.1314. Accessed: Aug 31, 2023.

43 J. Jordon et al., supra note 35, at 33.

44 E. Bao, X. Xiao, J. Zhao, D. Zhang and B. Ding, "Synthetic Data Generation with Differential Privacy via Bayesian Networks", JPC, vol.11, no.3, Dec. 2021, Doi: 10.29012/jpc.776. Available: https://journalprivacyconfidentiality.org/index.php/jpc/article/view/776. Accessed: Aug 31, 2023.

45 L. Rosenblatt, X. Liu, S. Pouyanfar, E. de Leon, A. Desai and J. Allen, "Differentially Private Synthetic Data: Applied Evaluations and Enhancements". arXiv, Nov. 2020. Available: http://arxiv.org/abs/2011.05537. Accessed: Aug 31, 2023.

究資料庫（Clinical Practice Research Datalink, CPRD），其儲存英國藥品和醫療產品監督管理局自 2018 年開始蒐集之診所病患就醫資料，該原始資料具有高度敏感性。該研究中心即透過合成資料技術，提供接近真實資料的心血管疾病與 COVID-19 資料集，讓研究人員能夠透過各種分析或機器學習手段，進行對社會有益之研究，而不侵犯病患隱私[46]。加拿大統計局提供黑客松競賽資料集，其原始資料包含人口普查資料、健康變數和死亡指標等敏感資訊，透過合成資料技術，可在不侵犯個人隱私的情況下，提供高可用性且貼近真實的資料讓參賽者進行分析[47]。更有組織將此技術應用於生成貼近真實資料之副本資料集，以便真實資料超過法定資料保留期限刪除後，仍保有可供使用之資料。

如欲採用合成技術作為資料隱私保護之主要方式時，建議考量下列面向之適用性：

**1.** 資料面：以對抗式生成網路為例，可用於生成結構及非結構化資料[48]，以達成保護真實資料隱私之目的，但由於合成資料之產生係本於原始資料之特徵以產製出貼近原始資料之合成資料，因此建議採用此技術之原始資料須具有一定之資料量[49]，並考量原始資料特徵樣本之全面性，以免產生具有偏差[50]之合成資料集。

---

46 The Royal Society, “From privacy to partnership,” Jan. 2023. [Online] Available: https://royalsociety.org/topics-policy/projects/privacy-enhancing-technologies/

47 United Nations Committee of Experts on Big Data and Data Science for Official Statistics, “United Nations Guide on Privacy-Enhancing Technologies for Official Statistics.” 2023. [Online] Available: https://unstats.un.org/bigdata/task-teams/privacy/guide/2023_UN%20PET%20Guide.pdf

48 M. Jovanovic and M. Campbell, “Generative Artificial Intelligence: Trends and Prospects, Computer”, vol.55, no.10, pp. 107–112, Oct. 2022, Doi: 10.1109/MC.2022.3192720. Available: https://ieeexplore.ieee.org/document/9903869/. Accessed: Aug 31, 2023.

49 J. Jordon et al., supra note 35, at 33.

50 N. Mehrabi, F. Morstatter, N. Saxena, K. Lerman and A. Galstyan, “A Survey on Bias and Fairness in Machine Learning”, ACM ACM Computing Surveys, vol.54, no.6, pp. 1–35, Jul.2022, Doi: 10.1145/3457607. Available: https://dl.acm.org/doi/10.1145/3457607. Accessed: Aug 31, 2023.

2. 架構面：雖目前亦有學術研究探討分散式架構之合成資料機制，如結合聯合學習之技術變形等[51]，惟一般而言，合成資料技術常見之運作架構仍以該技術施用者集中擁有原始資料，於產製合成資料集後，提供其他單位使用為主。

3. 可用性：可用性的評估面向主要取決於應用需求，該技術產製之合成資料僅是與原始資料具有相同特徵之擬真資料，因此須確保資料之應用目的可接受採用非真實之資料，且可接受產製過程中之資料誤差，如對整份合成資料進行資料分析適用該技術，但若須對單一資料進行處理之應用則不適合。此外，合成資料之生成過程須給定原始資料集，並產製僅包含該原始資料集特徵之合成資料，因此無法包含未來之樣本特徵，並較適合用於非即時之運作情境。

（三） 技術施用風險

由於合成資料是基於原始資料生成，若真實資料中存在偏差，亦可能導致經合成資料處理後的資料存在偏差[52]。其次，為了保證隱私安全性，現行亦有將合成資料技術結合差分隱私之技術應用，如 DPGAN（Differentially Private Generative Adversarial Network）等，該機制可進一步為產製之合成資料隱私性提供數學理論的證明，惟其亦可能導致真實資料中關鍵統計特徵與結構消失，使可用性降低或讓應用的結果無法代表真實資料之風險。因此，施用合成資料應納入偵測並糾正偏差之程序。尤其經合成資料處理後的資料，將對個人產生具法律效力或健康方面的影響時，更必須為之。

另須注意，經合成資料處理後的資料屬匿名資料與否，仍須根據處理後資料能否識別出個人隱私而定。因此，施用合成資料後，亦建議評估處理後資料之再識別風險。

在本章介紹的 3 種合成資料方式中，採機器學習方式需投入較高之硬體資源，如準備可支援機器學習之顯示卡，同時也需要機器學習相關軟體套件與函

[51] M. R. Behera, S. Upadhyay, S. Shetty, S. Priyadarshini, P. Patel and K. F. Lee, “FedSyn: Synthetic Data Generation using Federated Learning”. arXiv, Apr. 2022. Available: http://arxiv.org/abs/2203.05931. Accessed: Aug 31, 2023.
[52] J. Jordon et al., supra note 35, at 33.

式庫，如 PyTorch 或 Keras 等。而數學建模與隨機生成方式則需要相關軟體或函式庫，如 MATLAB、Mathematica 或 PyMC3 等。

合成資料仍可能隱含隱私資訊，可進一步結合差分隱私等技術以增強隱私保護。此外，針對機器學習方式產製合成資料可能面臨之資安威脅主要為「破壞模型」及「竊取隱私資訊」之攻擊，破壞模型的攻擊方式是透過惡意的輸入使模型訓練出不滿意或錯誤的結果，例如迴避攻擊（Evasion Attack）與數據投毒攻擊（Data Poisoning Attack）；而竊取隱私資訊的攻擊方式則是透過輸出推斷出原始輸入資料或合成資料模型之參數、函數等，或是透過背景資訊推斷出敏感屬性，例如模型萃取攻擊（Model Extraction Attack）、成員推理攻擊（Membership Inference Attack）以及屬性推理攻擊（Attribute Inference Attack）[53]。這些攻擊方式皆有可能降低合成資料的可用性或造成資料隱私外洩。

機器學習方式產製合成資料面臨之資安威脅如下：

1. 迴避攻擊：設計惡意訓練資料集，使模型學習得到效果不佳的訓練結果。
2. 數據投毒攻擊：注入惡意樣本至訓練資料集中，使模型學習得到錯誤的訓練結果。
3. 模型萃取攻擊：以輸入與輸出推斷模型之參數與函數，可還原出整個模型。
4. 成員推理攻擊：以輸出推斷某個特定的樣本是否存在於訓練資料集，可還原出訓練資料集。
5. 屬性推理攻擊：依背景資訊連接輸出與其他資料集，推斷出機敏資訊。

[53] H. Sun, T. Zhu, Z. Zhang, D. Jin, P. Xiong and W. Zhou, “Adversarial Attacks Against Deep Generative Models on Data: A Survey”, in IEEE Transactions on Knowledge and Data Engineering, vol.35, no.4, pp. 3367–3388, Apr. 2023, Doi: 10.1109/TKDE.2021.3130903. Available: https://ieeexplore.ieee.org/document/9627776/. Accessed: Aug 31, 2023.

（四） 開源工具與社群

下表彙整合成資料相關 Github star 數前 10 名且一年內程式碼有更新之開源工具。

▼表六、合成資料開源工具分析表

| 工具名稱 | 開發語言 | 基本文字介紹 | 優缺點/擅長解決之問題 |
|---|---|---|---|
| Mimesis | Python | 用於生成表格資料的 Python 套件，由 Likid Geimfari 與眾多貢獻者維護。 | • 可生成表格資料，如姓名、電話、Email、時間等屬性資料<br>• 可產生 JSON/XML 或 Pandas Dataframe |
| SDV | Python | 用於生成表格資料的 Python 套件，最初起源於 2016 年於麻省理工學院 Data To AI 實驗室，開發者於 2020 年成立 DataCebo 公司持續發展此工具。 | • 可生成單個、具有排序關係或是多個互相連結的表格<br>• 以 GAN 生成資料<br>• 視覺化分析生成資料 |
| YData Synthetic | Python | 用於生成表格或時間序列資料的 Python 套件，由 YData 公司推出。 | • 可生成表格或時間序列資料<br>• 實作多種合成資料模型，如：GAN、高斯混合模型等<br>• 具有圖像介面方便操作 |
| Gretel Synthetics | Python | 用於生成表格或時間序列資料的 Python 套件，由 Gretel 公司推出。 | • 可以生成表格或時間序列資料<br>• 結合差分隱私技術 |

| 工具名稱 | 開發語言 | 基本文字介紹 | 優缺點/擅長解決之問題 |
| --- | --- | --- | --- |
| SmartNoise SDK | Python | 用於生成表格資料的 Python 套件，由 OpenDP 社群維護。 | • 可以生成表格或關聯式資料<br>• 結合差分隱私技術，且實作多種合成資料模型 |
| synthcity | Python | 用於生成表格資料、時間序列資料或圖片的 Python 套件，由劍橋大學 van der Schaar 實驗室維護。 | • 可生成表格資料、時間序列資料或圖片等多樣資料<br>• 實作多種合成資料模型，如：GAN 等<br>• 實作評估資料正確性與隱私保護力的指標 |

## （五） 標準

▼表七、合成資料之標準統整表

| 標準名稱 | 標準編號 | 發布組織 | 類型 | 發布日期 | 標準說明 |
|---|---|---|---|---|---|
| Synthetic Data-Industry Connections | IC21-013-01 | IEEE | 尚未發展成標準/指南之專案 | - | 此標準仍在發展中，預計完成後將規範合成資料 API 標準、命名方案、本體結構等，以接收垂直傳輸之資訊並增強資訊與 AI 系統的互操作性。 |

（六） 示範性案例

**1.** 擬真情境案例：以差分隱私實現具隱私保護之科研資料共享-以糖尿病預測資料為例

**2.** 實際案例：

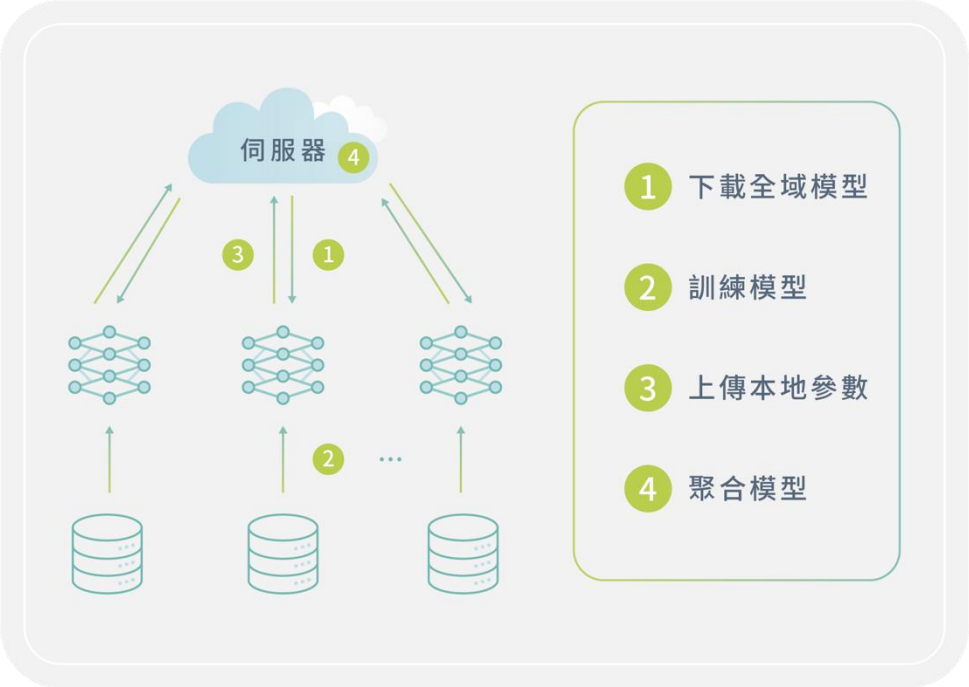
▼表八、合成資料之實際案例列表

| 參與者 | 描述 | 使用技術 | 開發成熟階段 |
|---|---|---|---|
| 加拿大統計局、黑客松競賽參賽者 | 加拿大統計局透過合成資料技術之機器學習方式，可在不侵犯個人隱私的情況下，產製高可用性且貼近真實的資料讓黑客松競賽參賽者進行分析。資料集包含人口普查、健康和死亡資料等敏感資訊。 | 基於合成資料之機器學習 | 應用試辦 |
| 帝濶智慧科技、聯新國際醫療、資料服務公司 | 為確保資料（資料服務公司會員行為分析、醫療科學研究資料及數位化轉型資料共享）於雲端儲存、釋出使用及資料分析階段之隱私保障。資料服務公司、新國際醫療與帝濶智慧科技合作試辦結合差分隱私、同態加密技術等技術，以生成合成資料、分析去識別化資料及安全加密檔案管理系統。該系統提供資料擁有者多種隱私強化方案，於資料上傳至雲端前進行去識別化或加密處理，經處理之資料保存於雲端平台，供後續查詢、釋出及結合其他保存於雲端平台之跨機構資料進行跨域分析。 | 合成資料、差分隱私、可搜尋加密、同態加密 | 應用試辦 |

## 三、 聯合學習（Federated Learning）

### （一） 技術說明

**1.** 技術概述：聯合學習是一種具隱私保護機制的分散式機器學習方式，其主要架構是由多個擁有訓練資料的分散式端點及一個伺服器所構成。透過聯合學習各分散式端點可利用其資料集訓練本地模型，並僅傳輸該本地模型之參數至伺服器進行全域模型更新，從而實現毋須傳輸本地端真實資料但仍可參與機器學習訓練的目的。




▲圖九、聯合學習運作流程[54]

聯合學習的運作流程如下：

(1) 下載全域模型：伺服器會初始化模型及參數，並讓所有本地端的參與者下載進行訓練。

(2) 訓練模型：本地端使用本地資料進行模型訓練並調整參數，最終產生本地模型。

(3) 上傳本地參數：本地端不須上傳原始資料，只需上傳更新的參數至

[54] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated Machine Learning: Concept and Applications," ACM Trans. Intell. Syst. Technol., vol. 10, no. 2, p. 12:1-12:19, Jan. 2019, Doi: 10.1145/3298981.

伺服器。

(4) 聚合模型：伺服器將所有本地端上傳的更新參數進行聚合，成為新一輪的全域模型。

**2.** 欲解問題：如何取得足夠且精準的資料一直是發展資料分析及機器學習等技術需面臨的課題，然而部分的資料可能具機敏性或內容涉及隱私，因而無法如一般資料直接進行傳輸並有效利用，聯合學習可解決該類資料參與機器學習訓練之難點，藉由實現安全且具隱私保護之資料利用機制，以增進各分散式端點參與機器學習訓練的意願，進而擴充所蒐集的資料量及資料多樣性，以充分發揮資料價值。除上述效益外，聯合學習僅對外傳輸經本地端處理而產生之模型參數，提供中央伺服器進行聚合，相較於集中式的機器學習需對外傳輸全部的原始資料，才可參與訓練，所需傳輸的資料量較少，亦可達成降低傳輸成本的效益。

**3.** 發展沿革：聯合學習技術為 Google 研究團隊於 2016 年時提出。當時，Google 在一篇名為《Federated Learning: Strategies for Improving Communication Efficiency》的論文中提出了聯合學習的概念和原理，主要介紹了如何在多個移動設備之間進行模型訓練，以實現個性化的語音識別和鍵盤預測等應用。

聚合是聯合學習中的重要技術，傳統的聚合方法主要採用簡單的模型平均，後來的研究提出了更複雜的聚合演算法，如 FedAvg（Federated Averaging）和 FedProx（Federated Proximal）等，以改善聚合過程中的效果和性能，而著名的應用有：

(1) Apple 公司採用聯合學習來訓練人工智慧助手 Siri 語音識別功能，本地模型在個人的 iPhone 上進行訓練，中央伺服器通過聚合本地模型的參數來構建全域模型。[55]

[55] Karen Hao, “How Apple personalizes Siri without hoovering up your data”, MIT Technology Review. Available: https://www.technologyreview.com/2019/12/11/131629/apple-ai-personalizes-siri-federated-learning/. Accessed: Aug 31, 2023.

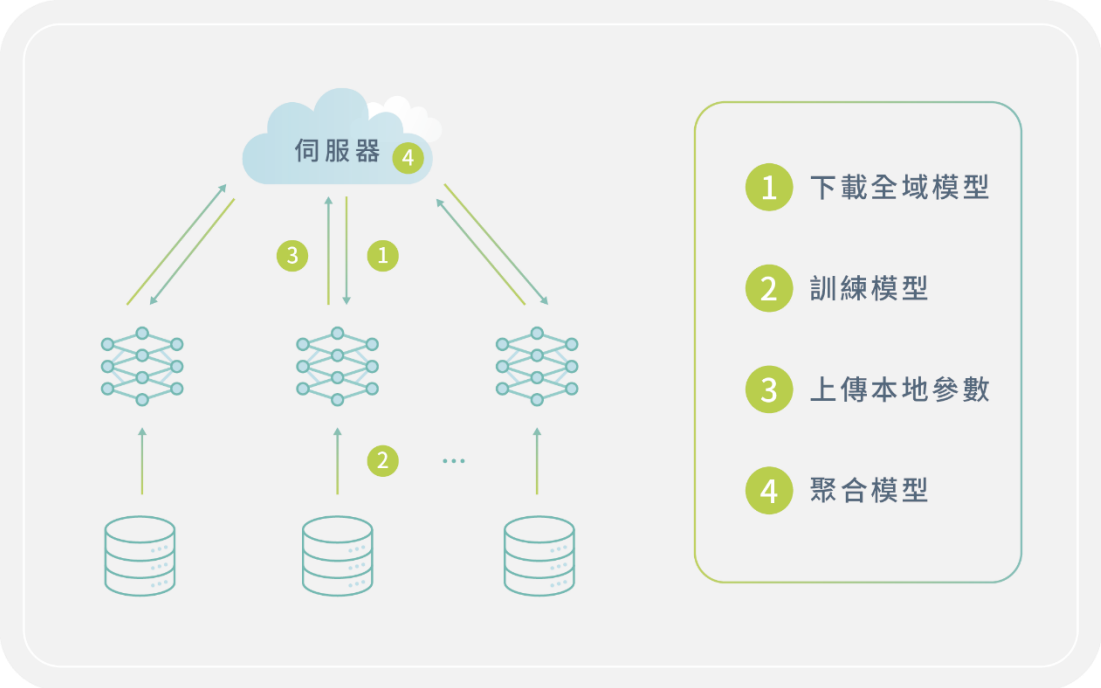
(2) 科技部全幅健康照護中心、健保署與台灣醫院及大學院校獲邀參與NVIDIA與麻省布萊根綜合醫院合作執行的EXAM聯合學習計畫，該計畫與全球 20 個機構合作，旨在建立一個名為 EMR CXR AI Model（EXAM）的模型，在不侵害患者隱私的情況下，使用生命體徵、實驗室資料和胸部X射線，預測新冠肺炎患者的未來氧氣需求，以便最有效率的安置病患。[56][57]

**4.** 技術現況：根據資料的儲存分佈和使用者的重疊程度，可將聯合學習區分成橫向、縱向、遷移學習三種。橫向通常用於各個本地端所擁有相同的資料特徵，但資料分屬於不同的資料當事人，例如在醫療領域中，每個醫療機構擁有不同的患者病歷資料，此方法能更準確的預測癌症以及基因疾病等病症。若訓練的資料集之間特徵重疊少但資料當事人重疊多，適合使用縱向來進行訓練，例如使用客戶的貸款歷史、收入和支出等資料，與來自擁有不同資料面向的機構來訓練信用評估風險模型。通過結合這些資料，模型可以更全面地評估風險，從而提高準確性。而遷移學習的每個設備都有自己的資料集和特徵空間，資料集之間可能存在差異，於是使用遷移學習的方式，使模型在不同的設備上訓練來幫助模型適應新的資料集，常見之應用有語音識別、自然語言處理等。

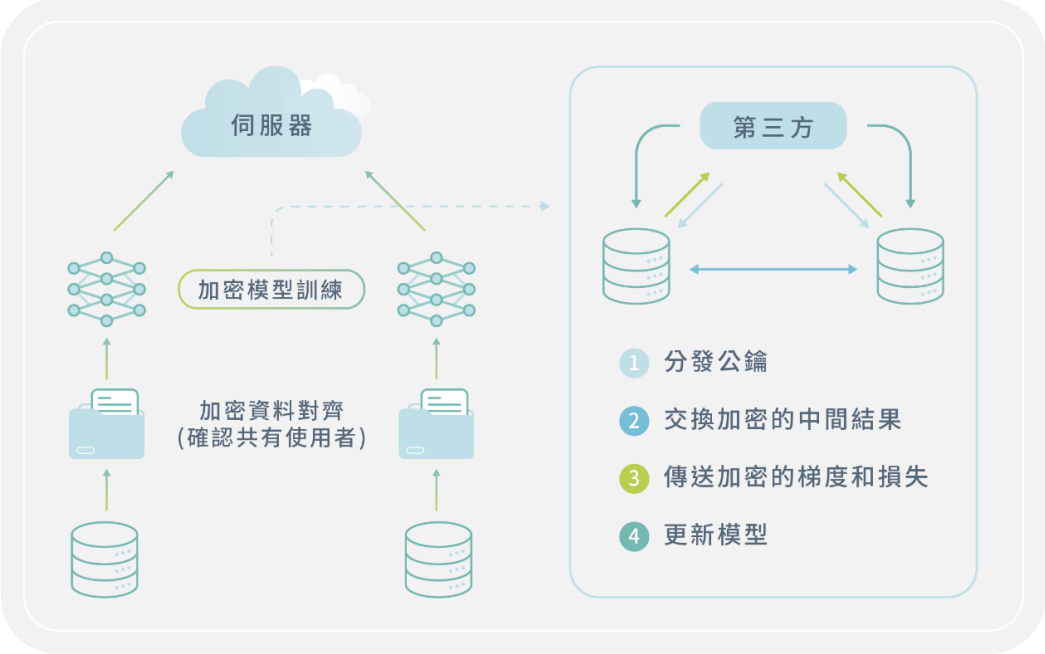
[56] I. Dayan et al., “Federated learning for predicting clinical outcomes in patients with COVID-19,” Nature Medicine, Vol. 27, pp. 1735-1743. , 2021. Available: https://www.nature.com/articles/s41591-021-01506-3. Accessed: Aug 31, 2023.

[57] 「MeDA Lab - 全球大規模聯邦學習」. https://www.medalab.ai/research/fl（引見於 2023 年 9 月 3 日）

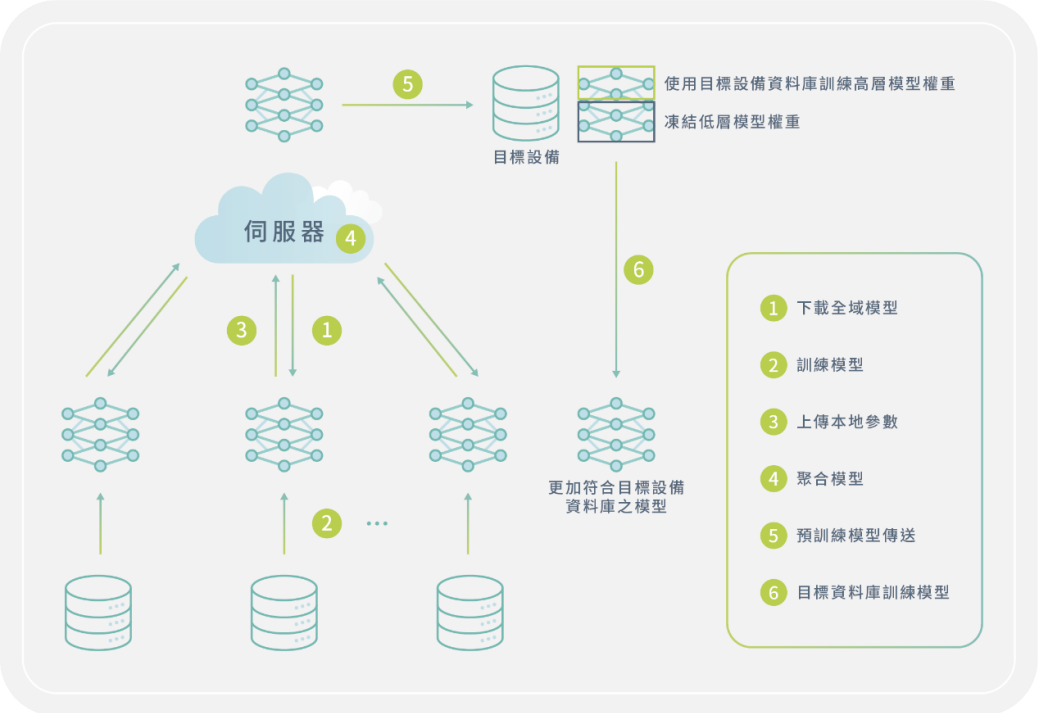
然而聯合學習仍存在安全與隱私問題，例如訓練中可能遭遇攻擊，常見的攻擊有下毒攻擊和推理攻擊，因此同態加密、差分隱私、安全多方計算等隱私強化技術經常被整合至系統中，現今研究指出，只加入一種隱私強化技術已不足以保護敏感資訊的安全及隱私性，因此多種隱私強化技術的搭配，整合入系統中已是常見手法，例如同態加密結合安全多方計算、差分隱私結合安全多方計算等等。




▲圖十、橫向聯合學習




▲圖十一、縱向聯合學習




▲圖十二、聯合遷移學習[58]

## （二） 適用情境

此技術的實用效益包含分散式資料分享、資料安全以及有效資源利用。在分散式資料的情況下，聯合機器學習能夠解決資料分散在不同地方的問題，以允許資料在個別設備上進行模型訓練，避免了集中存儲資料的需求，提供了更大的靈活性和效率，而在訓練模型時，資料可能包含個人隱私或敏感資訊，可通過本地加密資料和安全傳輸方式，避免資料傳輸過程中出現的資料洩露和攻擊的問題，確保了資料的安全性和隱私性。此外，透過聯合機器學習，能夠擴增機器學習所需之訓練資料量及增展資料多樣性，結合分散式資料之巨量資料分析的同時，也兼顧資料安全特性，提升模型的準確性和擴大可預測資料的範圍。同時能夠充分利用分散的計算資源，減輕集中式模型訓練中的計算負擔，實現了資源的有效利用。

醫療領域中的疾病檢測及金融領域中的信用評估為常見應用案例，無論是醫療或是金融相關的資料，皆有分散在不同組織之特性，並且具高度的機敏性。同時，醫療與金融皆有巨量資料分析的需求，因此資料的安全性保護，造成了

[58] Q. Yang, Y. Liu, T. Chen, and Y. Tong, supra note 54, at 43.

資料分享上很大的阻礙。聯合學習的分散式資料處理與安全性保護的特性，提供了這些應用場景相當優異的功能性與安全性，也因此提高了這些場域的資料利用機會，並產出分類效能更為優異的人工智慧模型。

聯合學習的適用性因素及限制可在資料面、模型面和架構面，三方面進行探討：

1. 資料面：聯合學習可以適用於結構化和非結構化資料的處理，無論是表格資料還是圖像、文字、時間等，也適用於資料量豐富的場景，因為參與者可以共享不同的資料樣本，從而提高整體訓練效果。
2. 模型面：聯合學習的訓練模型與資料型態密切相關，不同的資料型態需要不同的模型來處理和分析，適合的模型可以使整體訓練更有效率和準確，例如數值型資料較適合使用線性迴歸、邏輯迴歸、深度學習網路進行訓練，而圖片型資料較適合使用卷積神經網路來訓練。
3. 架構面:聯合學習通過在分散環境中進行訓練,達到隱私資料的保密性。即敏感資料不需要集中存儲在單一伺服器上，從而保護了隱私。此外，在聯合學習中第三方可以是一個中立的實體或平台，負責協調參與者之間的通訊和協作，但並不參與資料的傳輸或訓練過程，第三方必須確保資料隱私和安全性。

## （三） 技術施用風險

採用聯合學習時，需留意有關資料及傳輸方面的風險。首先，因聯合學習過程中，模型參數交換與聚合過程，因參數洩漏而使得原始訓練資料被還原是一個主要的隱私性攻擊威脅，因此聯合學習仍然需要搭配其他隱私性保護方法來進行設計，方能達到保護資料的隱私的最終目標。此外，資料機率分布的不一致和訓練資料特徵種類的差異性也是挑戰，因為不同資料提供者之間的資料取樣來源與方式可能存在差異，因此仍需要進行資料轉換和對齊。

在傳輸方面，傳輸延遲與頻寬限制，可能會影響訓練的效率，以及無法滿足大量資料的傳輸需求。穩定性是另一個考慮因素，通道在傳輸過程中可能出現連接中斷或資料遺失，進而影響訓練的結果。

在軟體方面，可以選擇可信賴的聯合機器學習專案，如 TensorFlow Federated、OpenFL 和 Pysyft 等，這些專案提供了不同的隱私強化技術和使用方式。同時，在硬體方面，若是結合同態加密等技術來增強資料的隱私保護，需要較高的運算資源，可利用硬體設備來提高演算法的效率和性能。

（四） 開源工具與社群

參考工具之維護狀況、社群活躍度、Github star 數/fork 數、可支援模型和隱私方法、說明文件和教學檔案，經綜合評估列舉聯合學習之開源工具如下。

▼表九、聯合學習開源工具分析表

| 工具名稱 | 開發語言 | 基本文字介紹 | 優點/擅長解決之問題 |
|---|---|---|---|
| NVFlare | Python | Nvidia 推出的聯合學習框架，於 2021 年開放原始碼，可連接伺服器、客戶端和不同角色的使用者。 | • 為商業應用而設計<br>• 支援多種訓練模型<br>• 可使用 NVIDIA 的 GPU 硬體加速<br>• 多種隱私安全保護功能 |
| Flower | Python | 起源於牛津大學的研究項目，現由德國公司 adap GmbH 管理，提供不同機器學習框架的執行文件和範例。 | • 提供的工具和介面使開發者能輕鬆構建和訓練聯合學習模型<br>• 自訂、擴充套件、修改或替換現有的組件相對簡單<br>• 可將任何機器學習框架設置成聯合學習 |
| PySyft | Python | OpenMined 團隊推出的安全深度學習函式庫，有活躍的開源社群，提供聯合學習實作工具。 | • 常用於深度學習模型<br>• 多種隱私安全保護功能 |
| TensorFlow Federated（TFF） | Python | Google 建立在 TensorFlow 機器學習框架之上的聯合學習框架，應用於行動裝置鍵盤輸入預測。 | • 使用者能夠自訂模型框架以及聚合方法<br>• 部分隱私安全保護功能<br>• 適合熟悉 Tensorflow 之使用者 |

（五） 標準

▼表十、聯合學習之標準統整表

| 標準名稱 | 標準編號 | 發布組織 | 類型 | 發布日期 | 標準說明 |
|---|---|---|---|---|---|
| 隱私強化技術（Privacy-enhancing technologies,PETs） | 無 | 英國資訊委員辦公室（ICO） | 指南 | 2023-06-21 | 本指南包含：技術定義和用途、集中式和分散式設計、保護資料方式、實作考量、隱私安全風險、可能遭受的攻擊 |
| 對抗性機器學習：攻擊和緩解的分類和術語（Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations） | NIST AI 100-2 E2023 | 美國國家標準暨技術研究院（National Institute of Standards and Technology, NIST） | 尚未發展成標準/指南之技術文件 | 2023-03-08 | 本文件內容包含：技術定義和用途、可能遭受的攻擊 |
| 隱私強化技術指南（THE PET GUIDE） | 無 | 聯合國（United Nations） | 指南 | 2023-02-09 | 本文件內容包含：技術定義和用途、應用範例、開放程式碼、隱私相關風險、技術成本 |
| AI 系統基礎安全性分析（Security of AI-Systems: Fundamentals） | 無 | 聯邦資訊安全辦公室（Bundesamt für Sicherheit in der Informationstechnik） | 尚未發展成標準/指南之官方技術分析報告 | 2022-08 | 本文件內容包含：聯合學習的基本架構和流程、聯合學習的優點、聯合學習的隱私保護問題、聯合學習的應用場景 |
| 保護機器學習演算法的安全性 | 無 | 歐盟網路安全 | 指南 | 2021-12 | 本指南包含：機器學習演算法分類、機器 |

| 標準名稱 | 標準編號 | 發布組織 | 類型 | 發布日期 | 標準說明 |
| --- | --- | --- | --- | --- | --- |
| （ SECURING MACHINE LEARNING ALGORITHMS） | | 局（The European Union Agency for Cybersecurity） | | | 學習威脅和漏洞、安全控制 |
| IEEE 聯合學習架構框架和應用指南（ IEEE Guide for Architectural Framework and Application of Federated Machine Learning） | IEEE 3652.1-2020 | 電機電子工程師學會（Institute of Electrical and Electronics Engineers） | 標準 | 2021-03-19 | 本標準包含：技術定義和用途、技術架構、實作考量、隱私安全、效率、經濟可行性、效能評估 |
| 數位安全展望（Developing our capability in cyber security） | 無 | 美國國家反情報和安全中心（National Counterintelligence and Security Center） | 尚未發展成標準/指南之技術分析報告 | 2020-07 | 本文件內容包含：<br>多所歐洲知名大學對於資訊安全的專欄<br>其中 Imperial College London 有提到對聯合學習的應用 |

（六） 示範性案例

**1.** 擬真情境案例：以聯合學習實現金融詐欺事件偵測

**2.** 實際案例

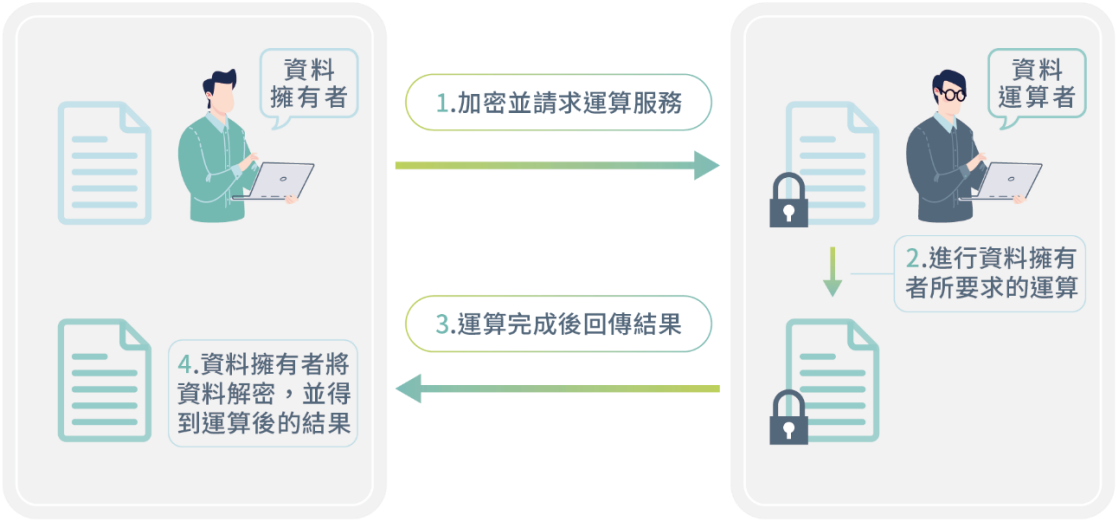
▼表十一、聯合學習之實際案例列表

| 參與者 | 描述 | 使用技術 | 開發成熟階段 |
|---|---|---|---|
| 歐盟統計局、參與研究之受試者 | 歐盟統計局結合聯合學習、安全多方運算與同態加密等技術，透過與受試者智慧裝置持續低強度的互動，在不洩漏隱私的情況下進行調查研究。資料集包含受試者回覆問題的答案，以及智慧裝置內傳感器的資料，如加速度計、陀螺儀資料等。 | 聯合學習、安全多方運算、同態加密 | 概念性驗證 |

## 四、 同態加密（Homomorphic Encryption）

### （一） 技術說明

**1.** 技術概述：同態加密是一種密碼學技術，採用有同態性的加密演算法可以直接對已加密的資料進行運算，且可產生與運算未加密資料一致的結果。這項技術可用以確保資料在傳輸、運算及輸出運算結果的過程中，全程將資料維持在加密狀態，對須將機敏或隱私資料傳輸委由他人執行運算的情境下，保障了資料的機敏性。




▲圖十三、同態加密實際使用示意圖

**2.** 欲解問題：隨雲端運算興起，資料儲存及運算也朝雲端化發展，這些儲存在雲端的資料可能會因為未加密或必須解密後才能執行運算，使雲端服務提供者有可能得知資料內容，而具有資訊外洩的風險[59]，進而限制了敏感或隱私資料雲端化的發展。當資料於不受信任的環境中保存或運算時，如何確保整體過程之機密性已成為雲端運算發展之重要課題。透過全同態加密的輔助，可使資料處理者、雲端服務提供者或他人皆無從得知未加密之原始資料與運算結果，這為資料提供者降低了隱私洩露的

[59] M. Naehrig, K. Lauter, V. Vaikuntanathan, “Can homomorphic encryption be practical? ”, Proceedings of the 3rd ACM workshop on Cloud computing security workshop, Chicago Illinois USA: ACM, 2021, pp. 113–124. Doi: 10.1145/2046660.2046682.

風險，也進一步促進了這些資料雲端化並得以安全的方式被應用，妥善發揮資料的價值。此外，面對需匯集多方資料合作執行運算的資料應用需求，全同態加密也可在原有合作運算的基礎上增強其隱私保護力，或結合其他隱私強化技術，如私有集合交集（Private-Set Intersection）[60]或聯合學習（Federated Learning）。[61]

**3.** 發展沿革：早在 1978 年密碼學家 Ronald L. Rivest 等人即於《On data banks and privacy homomorphisms》[62]中以借貸公司將客戶貸款資料委外儲存及運算的情境下，如何使借貸業務順利運作同時達成隱私保護為研究背景，提出隱私同態（Privacy Homomorphisms）的概念，並可視為同態加密研究的開端。其後則發展出半同態加密（Partially HE, PHE）、近似同態加密（Somewhat HE, SWHE）等，僅支援部分運算或有限制運算次數之同態加密技術，直到 2009 年才由 Gentry[63]提出可支援加法及乘法運算，且無運算次數限制的全同態（Fully HE, FHE）技術，並被認為是第一代的全同態加密，並為全同態加密的發展開創了新局。

以下就密碼系統對於運算種類的支援性進行歸納：

▼表十二、各類型同態加密之特性列表

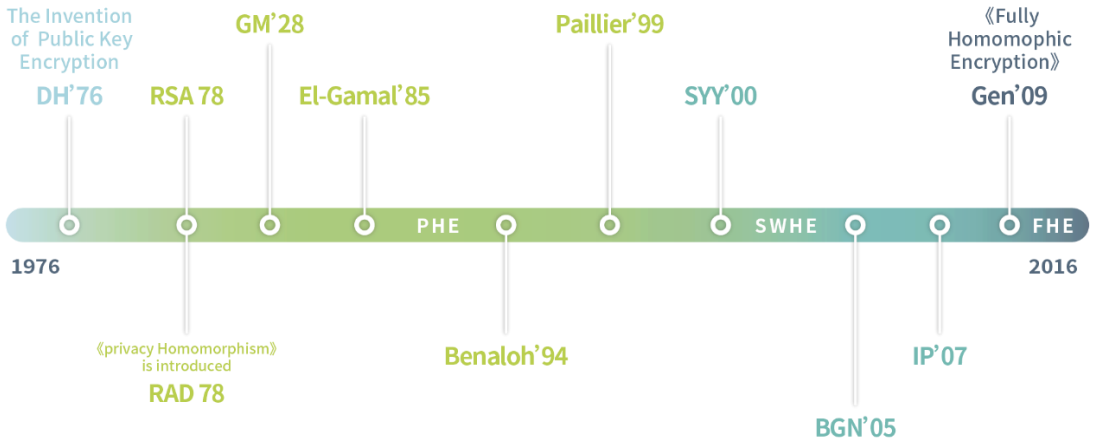
| 類型 | 半同態加密 | 近似同態加密 | 全同態加密 |
|---|---|---|---|
| 特性 | 僅支援加法或乘法運算。 | 在有限的運算次數條件下，可支援加法及乘法運算。 | 支援加法及乘法運算，且無運算次數限制。 |

60 F. Kerschbaum, “Outsourced private set intersection using homomorphic encryption”, Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security, Seoul Korea: ACM, 2012, pp. 85–86. Doi: 10.1145/2414456.2414506.

61 Hardy, Stephen, et al. “Private federated learning on vertically partitioned data via entity resolution and additively homomorphic encryption.” arXiv preprint arXiv:1711.10677, 2017.

62 R. Rivest, L. Adleman, and M. Dertouzos, “On data banks and privacy homomorphisms,” in Foundations of Secure Computation, Academic Press, Cambridge, Massachusetts, USA, 1978, pp. 169–177.

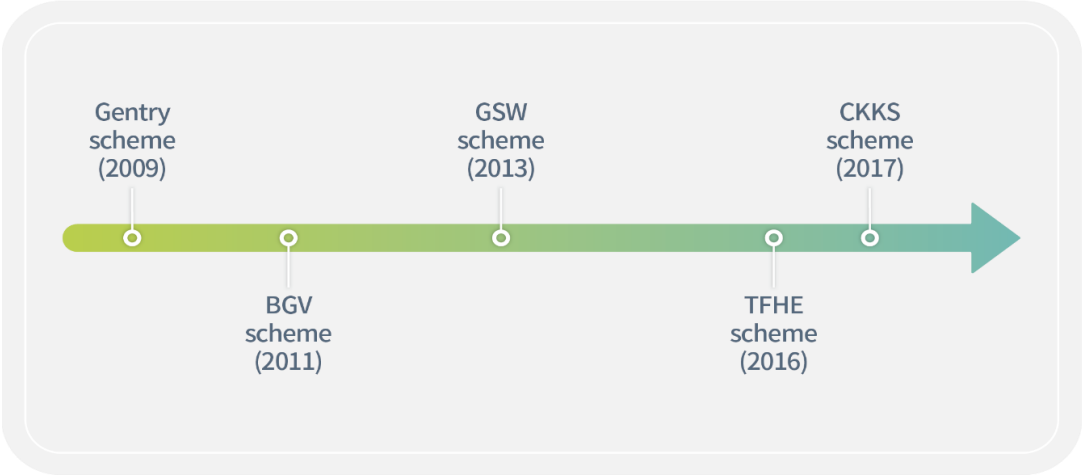
63 Gentry, Craig. “Fully homomorphic encryption using ideal lattices.” Proceedings of the forty-first annual ACM symposium on Theory of computing. 2009, pp.169-178. Doi: 10.1145/1536414.1536440.




▲圖十四、同態加密發展歷程[64]

（於 Gentry 提出第一代全同態加密技術前）

**4.** 技術現況：自第一代全同態加密發表後，相關領域的研究也逐漸朝提升運算效能及擴充支援的資料型態推進，並發展出不同方案（Scheme）之同態加密技術：




▲圖十五、同態加密技術重點發展歷程[65]

其中，有幾個較有代表性的方案，例如 BGV 方案支援整數運算，並第一個實現 leveled FHE 的同態加密技術，使得使用者可以在沒有 bootstrapping 的情況下進行一定量的運算[66]；GSW 方案雖然同樣是支援整數運算，但相較於以前

64 Acar, Abbas, et al. "A survey on homomorphic encryption schemes: Theory and implementation." ACM Computing Surveys (Csur) , vol.51, no.4, 2018, pp. 1-35. doi: 10.1145/3214303.
65 *Id.*
66 Z. Brakerski, C. Gentry, V. Vaikuntanathan, "Fully homomorphic encryption without bootstrapping", Proceedings

的方案，GSW 方案使用的運算資源較少[67]；而 TFHE 方案可以支援二進制（binary）運算，使得部分運算方法可以更加方便實現與使用[68]；還有 CKKS 方案，是第一個支援浮點數運算的方案[69]。

現階段全同態加密仍受限於運算時間及成本因素，尚未普遍運用於商業環境，但已有學研單位及新創公司積極發展各種領域的應用，如：由美國 3 所大學所共同舉辦的 iDASH Privacy & Security Workshop，自 2014 年起即以舉辦競賽的方式積極發展同態加密在健康醫療領域的應用，如以同態加密結合機器學習分析 COVID-19 病毒株、建構安全的表現型預測委外協定等競賽主題[70]，而新創公司則以全同態加密為技術主軸，發展資料庫及機器學習分析產品，並提供應用於金融、醫療研究、個人化行銷及客戶隱私保護等不同領域之技術解決方案，並持續發展及維護如 OpenFHE 及 TFHE 等開源專案。

（二） 適用情境

全同態加密可保護資料在傳輸、儲存及運算過程中的隱私，且因是採密碼學技術保護資料隱私，故毋需對資料進行調整（相較於其他非密碼學之隱私強化技術），可產出正確之運算結果，適用於下列情境中提供隱私保護：

1. 跨組織合作產出運算結果或共同訓練機器學習模型，如新創公司[71]應用於實現合規之金融犯罪調查及健康醫療研究。
2. 提供具隱私保護之個人化服務，如法國新創公司[72]應用於保障人臉辨識及語音助理服務所涉個人資料之機密性；並將同態加密技術與區塊鏈技

of the 3rd Innovations in Theoretical Computer Science Conference, Cambridge Massachusetts: ACM, 2012, pp. 309–325. Doi:10.1145/2090236.2090262.

67 Craig Gentry, Amit Sahai, and Brent Waters, “Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based.” in: Gerhard Goos, Juris Hartmanis(Eds.), “Lecture Notes in Computer Science”, Berlin, Heidelberg: Springer, 2013, pp. 75-92. doi: 10.1007/978-3-642-40041-4_5.

68 Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène, “Faster Fully Homomorphic Encryption: Bootstrapping in less than 0.1 Seconds”, in: Gerhard Goos, Juris Hartmanis(Eds.), “Lecture Notes in Computer Science”, Berlin, Heidelberg: Springer, 2016, pp. 3-33. Doi: 10.1007/978-3-662-53887-6_1.

69 Cheon, Jung Hee; Kim, Andrey; Kim, Miran; Song, Yongsoo. “Homomorphic encryption for arithmetic of approximate numbers”. Takagi T., Peyrin T. (eds) Advances in Cryptology – ASIACRYPT 2017, “Lecture Notes in Computer Science.” Berlin, Heidelberg: Springer, 2017, pp. 409–437. doi:10.1007/978-3-319-70694-8_15.

70 “iDASH Privacy & Security Workshop”, IDASH PRIVACY & SECURITY WORKSHOP 2023 - secure genome analysis competition. http://www.humangenomeprivacy.org/2023/. (Accessed: Aug. 31, 2023).

71 “Duality Technologies - Secure Data Collaboration Products”, Duality Technologies. https://dualitytech.com/ (Accessed: Aug. 31, 2023).

72 zama https://github.com/zama-ai

術結合，提供具隱私保護的智能合約。

在決定是否採用全同態加密時，建議考量下列面向：

1. 資料面：視資料與選擇加密方式的不同，使用全同態加密進行加密後所得的密文大小，可能從理想情況完全不擴張，到擴張達數十萬或數百萬倍皆有可能。因此，應審慎評估納入同態加密計算的資料，並只對必要的資料進行加密。
2. 架構面：考量同態加密所需運算資源龐大，因此需視應用情境，擇具有運算能力的一方或採用雲端計算服務，匯集加密資料進行運算並回復運算結果。
3. 可用性：全同態加密的運算會消耗大量的運算資源與時間，目前已有研究採硬體加速的方式如 ASIC 晶片、GPU 等，已可大幅提高運算效能[73][74]，惟現階段全同態加密運算與明文運算相比，回應時間仍具有明顯的延遲，而無法適用於即時性要求高之系統。

（三） 技術施用風險

於實作同態加密時，因有多種演算法、軟體（如函式庫、framework、開源專案）及不同等級之安全參數選擇，應視所運用的情境不同選擇最適合之解決方案，方能安全且有效率的達成運算目標，因而具有較高之技術門檻。如各種演算法對資料類型之支援性不同或對特定類型運算有較高之處理效能、運用函式庫開發時可能需要處理較底層之運算操作、選擇開源專案進行開發時則，建議評估專案之可信賴度及更新頻率等，而安全參數選擇方面以 OpenFHE 為例，提供了 TOY、MEDIUM、STD128、STD192、STD256 等 5 個等級，其後三者的數字就代表了「安全強度」，並根據 NIST 建議[75]，應高於 112 方能提供足夠的安全保證。

---

[73] Wang, Zhiwei, et al. “HE-Booster: An Efficient Polynomial Arithmetic Acceleration on GPUs for Fully Homomorphic Encryption.” IEEE Transactions on Parallel and Distributed Systems. vol.34, no.4,pp 1067–1081, Apr. 2023, Doi: 10.1109/TPDS.2022.3228628.

[74] J. Kim et al., “ARK: Fully homomorphic encryption accelerator with runtime data generation and inter-operation key reuse,” 2022 55th IEEE/ACM International Symposium on Microarchitecture (MICRO), Chicago, IL, USA: IEEE, Oct, 2022. p p. 1237-1254. Doi: 10.1109/MICRO56248.2022.00086

[75] “Cryptographic Key Length Recommendation”, BlueKrypt. https://www.keylength.com/en/4 (Accessed: Aug 31, 2023)

同態加密亦有遭受差分攻擊（Differencing Attack）之風險。差分攻擊是指藉比較多個資料集統計結果，推導出資料集中個人的資訊特徵。以受同態加密保護的交易紀錄資料庫為例，假設資料庫可提供當月系統總交易金流統計，以及當月系統信用卡總交易金流統計，若恰好當月僅有一筆非信用卡交易紀錄，查詢者可藉比較兩統計資料推算出該非信用卡交易紀錄的實際金額，此即差分攻擊。同理，若比較更多統計結果，也有反向推導整份資料集的風險。

此外，其他對稱式加密系統所面臨的資訊安全風險，全同態加密亦有，因此，必須使用適當的技術和安全措施來確保密鑰安全。如密鑰之管理程序、生成新密鑰機制、採行安全的傳輸協定等，另隨解密技術的不斷發展，應持續留意所採用密碼演算法之攻擊威脅，並採取相應風險之處理措施，如調整系統安全強度或更新密碼演算法等。

（四） 開源工具與社群

參考工具之維護狀況、社群活躍度、Github star 數/fork 數、可支援模型和隱私方法、說明文件和教學檔案，經綜合評估列舉同態加密之開源工具如下。

▼表十三、同態加密開源工具分析表

| 工具名稱 | 開發語言 | 基本文字介紹 | 優缺點/擅長解決之問題 |
|---|---|---|---|
| lattigo | go | lattigo 是一個以 go 開發的專案。支援 BFV、CKKS 等演算法的加法、減法、乘法、內積等運算。<br>預設的參數皆支援 128-bits 以上的安全強度，也可以微調以符合需求。 | • 乘法次數有限<br>• 速度快<br>• 有為安全多方運算設計的函式庫 |
| OpenFHE | C++ | OpenFHE 是一個以 C++開發的專案，支援 BFV、BGV、CKKS、TFHE 和 FHEW。預設的參數皆支援 128-bits 以上的安全強度，也可以微調以符合需求。 | • CKKS、TFHE 和 FHEW 支援 bootstrapping<br>• 有為安全多方運算、threshold FHE 和 proxy re-encryption 設計函式庫<br>• 支援最多方案 |
| HElib | C++ | HElib 是一個以 C++開發的專案，支援 BGV、CKKS 的加法、乘法等運算。可依專案說明文件之建議調整安全參數。 | • CKKS、BGV 支援 bootstrapping<br>• 製作團隊持續更新功能 |
| SEAL | C#/C++ | SEAL 是一個同態加密庫，以 C#及 C++開發，允許對加密整數或實數執行加法和乘法。BFV 和 BGV 方案允許對加密整數執行模算術。CKKS 方案允許對加密實數或複數進行加法和乘法。預設的參數皆支援 128-bits 以上的安全強度，也可以微調以符合需求。 | • 用 C++和 C#開發<br>• 支援乘法平行化 |

（五） 標準

▼表十四、同態加密之標準統整表

| 標準名稱 | 標準編號 | 發布組織 | 類型 | 發布日期 | 標準說明 |
|---|---|---|---|---|---|
| 資訊安全技術–加密演算法–第 6 部分：同態加密（IT Security techniques – Encryption algorithms – Part 6: Homomorphic encryption） | ISO/IEC 18033-6:2019 | ISO/IEC | 標準 | 2019-05 | 規範了適用於同態加密的演算法：<br>• Exponential ElGamal 加密<br>• Paillier 加密<br>對於每一種演算法規定了以下流程：<br>• 生成參數與實體密鑰<br>• 加密資料<br>• 解密資料<br>• 操作加密資料 |
| 同態加密標準（Homomorphic Encryption Standard） | 無 | Homomorphicryption.org 社群 | 標準 | 2019-08-18 | 本文件紀錄了關於 BGV、BFV、GSW 等加密演算法之相關知識，並推薦同態加密於不同安全級別之參數。另提供已知攻擊及其預計運行時間，以利設定安全參數時參考。 |

（六） 示範性案例

1. 擬真情境案例：以全同態加密實現犯罪資料雲端運算

2. 實際案例

▼表十五、同態加密之實際案例列表

| 參與者 | 描述 | 使用技術 | 開發成熟階段 |
|---|---|---|---|
| Duality 科技公司、跨國金融機構、執法機構、第三方資料處理平臺 | Duality 科技公司與多個跨國金融機構及執法機構共組聯盟，透過同態加密技術，在不直接共享金融客戶資料下，共同識別與防治金融相關犯罪。其資料來源為各個聯盟成員之客戶資料。客戶資料經資料持有方使用同態加密保護後，以密文形式交由資料處理平臺進行分析處理，並由資料處理平臺分享處理結果供其他聯盟成員解密應用。除處理結果外，聯盟成員無法反向追溯原始資料，並以此保障客戶資料隱私。 | 同態加密 | 正式上線 |
| 韓國政府、私人企業 | 韓國統計局結合同態加密、安全多方運算與差分隱私等技術，在不暴露敏感資訊的狀況下，讓政府各部門的資料可以安全的連結與使用。此應用試辦之資料為韓國統計局登記之各企業詳細資訊，如機構名稱、公司登記號碼與行政區碼。過程中資料會在加密的狀態下進行連結與分析。 | 同態加密、安全多方運算、差分隱私 | 應用試辦 |

| 參與者 | 描述 | 使用<br>技術 | 開發成熟<br>階段 |
| --- | --- | --- | --- |
| 帝濶智慧科技、<br>聯新國際醫療、<br>資料服務公司 | 為確保資料（資料服務公司會員行為分析、醫療科學研究資料及數位化轉型資料共享）於雲端儲存、釋出使用及資料分析階段之隱私保障。資料服務公司、新國際醫療與帝濶智慧科技合作試辦結合差分隱私、同態加密技術等技術，以生成合成資料、分析去識別化資料及安全加密檔案管理系統。該系統提供資料擁有者多種隱私強化方案，於資料上傳至雲端前進行去識別化或加密處理，經處理之資料保存於雲端平台，供後續查詢、釋出及結合其他保存於雲端平台之跨機構資料進行跨域分析。 | 合成資料、<br>差分隱私、<br>可搜尋加密、<br>同態加密 | 應用<br>試辦 |
| 歐盟統計局、<br>參與研究之受試者 | 歐盟統計局結合聯合學習、安全多方運算與同態加密等技術，透過與受試者智慧裝置持續低強度的互動，在不洩漏隱私的情況下進行調查研究。其資料包含受試者回復問題的答案，以及智慧裝置內傳感器的資料，如加速度計、陀螺儀資料等。 | 聯合學習、<br>安全多方運算、<br>同態加密 | 概念性驗證 |
| 加拿大統計局、<br>零售商、<br>雲端運算平台 | 加拿大統計局研究透過同態加密技術，在不透露原始資料的情況下，於不信任之雲端平台進行機器學習。其資料為各零售商提供之產品資料。其流程會先由零售商以同態加密技術加密資料，再將其上傳至不信任的雲端運算平台訓練機器學習模型，然後將運算結果回傳至加拿大統計局，最後以密鑰解密得到模型權重。 | 同態加密 | 概念性驗證 |
| 國立中山大學資訊工程學系、國立中山大學醫學科技研究所、高雄榮民總醫院、病患（資料當事人）、病患授權之資料存取者 | 為克服資料上雲後的隱私保護挑戰，國立中山大學團隊與高雄榮民總醫院合作，開發「具隱私保護暨安全資料探勘之醫療資料倉儲系統」。於概念性驗證過程中，團隊將病患醫療測試資料加密上傳雲端，加密後之資料在密文狀態下仍可搜尋及統計分析，並可由資料當事人自主設定資料存取權限，提供資料參與聯合學習或其他資料應用。此概念驗證為儲存於雲端的病歷提供資料生命周期全程隱私保障，並賦予病患自主運用資料的權力。 | 同態加密、<br>可搜尋式加密、<br>屬性加密 | 概念性驗證 |

## 五、 安全多方運算（Secure Multiparty Computation）

### （一） 技術說明

**1.** 技術概述：安全多方運算（Secure Multiparty Computation, SMPC）允許多個參與者在不洩漏自身秘密輸入（值）的情況下，實現聯合計算。

**2.** 欲解問題：安全多方運算是一種兼具資料隱私保護及促進多方資料協作的技術，並且無須彙集資料於指定的第三方。多方資料協作，可讓多個參與者運用其所擁有的資料共同解決面臨的難題或是發展進步創新。而當這些共享的資料涉及機敏性、隱私或營業秘密時，往往會造成參與意願降低，進而導致資料協作運作困難，甚或失敗。以財務分析[76]為例，如多家公司間期望進行財務統計測量，但每間公司皆不願透露其商業機密。一般來說較常見的作法是由參與者共同指定一個可信任的第三方，以利彙集所有共享的資料並進行資料利用以達成資料協作的目的。惟考量可信任的第三方在實務運作上難以指定，且該第三方需彙集各方的機敏資料，無論是參與者或是第三方所承受的資料管理風險皆會因此上升。安全多方運算的發展旨在解決上述難點，並促進多方參與資料協作。

**3.** 發展沿革：安全多方運算的概念最早是來自 1982 年姚期智所提出的百萬富翁問題[77]：兩個百萬富豪想要知道誰比較有錢，但是不想向對方透露自身財富。當時其提出以模糊傳輸為基礎的解法，但是兩個百萬富翁問題只針對安全「兩」方運算提出方案（比較雙方大小），所以 1987 年姚期智再提出了姚氏混淆電路來完整實現安全「兩」方運算[78]。隨著姚氏混淆電路出現，陸續有人提出各種協議來進一步擴張參

---

76 Easily Discover Tax and VAT Fraud with Sharemind Technologies | Sharemind, Apr. 2016. Available: https://sharemind.cyber.ee/tax-vat-fraud/. Accessed: Aug 31, 2023.

77 A. C. Yao, “Protocols for secure computations,” in 23rd Annual Symposium on Foundations of Computer Science (sfcs 1982), Nov. 1982, pp. 160–164. Doi: 10.1109/SFCS.1982.38.

78 S. Micali, O. Goldreich, and A. Wigderson, “How to play any mental game,” in Proceedings of the nineteenth ACM symp. on theory of computing, STOC, ACM New York, NY, USA, 1987, pp. 218–229.

與方數量以實現安全多方運算。

除了混淆電路外，另一種常見用以實現安全多方運算的技術為「秘密分享」：1979 年 Adi Shamir 與 G. Blakley 分別提出構造方案，前者提出藉由多項式函數求解以及 Lagrange 插值來構造秘密分享（Secret Sharing）[79]；Blakley 則是利用線性幾何的投影法來構造[80]。

2000 年到 2008 年間開始出現將理論與實際問題結合的研究，並逐步針對安全多方運算協議之計算、通訊成本進行改善及最佳化，進而實際運作。其中較為著名的是 2004 年由 Malkhi 設計的安全多方運算平台 Fairplay[81]，及 2008 年丹麥甜菜拍賣應用[82][83]，在農民及甜菜加工工廠雙方皆不想讓對方事先知道自己的要求，以避免被抬價或壓價的情況下。透過安全多方運算以解決此供需媒合問題，包含計算出該向哪些農民收購多少甜菜量，以及該用何種價格進行收購等。

**4.** 技術現況：當前安全多方運算的實作技術主要能分成以下兩種[84]：

(1) 混淆電路：先把計算函數轉換成邏輯電路，再藉由標籤替換、加密與模糊傳輸來使得電路計算運行時，各參與方無法辨認出彼此的秘密輸入，進而達到安全多方運算的目的。混淆電路是最先提出來實現安全多方運算的技術，因此有許多種不同的協議，與秘密分享相比，混淆電路通常有較好的計算效率，但是為了混淆各個秘密輸入，

[79] A. Shamir, “How to share a secret”, Commun. ACM, vol. 22, no.11, pp. 612–613, Nov. 1979, Doi: 10.1145/359168.359176. Available: https://dl.acm.org/doi/10.1145/359168.359176. Accessed: Aug 31, 2023.
[80] G. R. Blakley, “Safeguarding cryptographic keys”, 1979 International Workshop on Managing Requirements Knowledge (MARK), pp. 313–318, Jun. 1979, Doi: 10.1109/MARK.1979.8817296. Available: https://ieeexplore.ieee.org/document/8817296/. Accessed: Aug 31, 2023.
[81] “Fairplay”. Available: https://www.cs.huji.ac.il/project/Fairplay/Fairplay.html. Accessed: Aug 31, 2023.
[82] P. Bogetoft et al., “Secure Multiparty Computation Goes Live”, in Financial Cryptography and Data Security, R. Dingledine P. Golle, Editor, in Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2009, pp. 325–343, Doi: 10.1007/978-3-642-03549-4_20. Available: https://link.springer.com/chapter/10.1007/978-3-642-03549-4_20 Accessed: Aug 31, 2023.
[83] “Danish Sugar Beet Auction”. Accessed: Aug 31, 2023. Available: https://csrc.nist.gov/csrc/media/events/meeting-on-privacy-enhancing-cryptography/documents/toft.pdf
[84] D. Evans, V. Kolesnikov, and M. Rosulek, “A pragmatic introduction to secure multi-party computation,” Foundations and Trends® in Privacy and Security, vol. 2, no. 2–3, pp. 70–246, Dec. 2018, Doi: 10.1561/3300000019.

因此通訊效率較差。

(2) 秘密分享：一種資料分拆與重組、保護機密資料的技術。將秘密（Secret）分成多份「份額」（Share）給參與者，只有當一定數量的參與者同意提供其所持有的份額時，才能夠正確還原出秘密（若是只有未達數量的「份額」，將無法獲得任何有用的資訊）。參與者藉由分享彼此的「份額」，並且加以運算來實現安全多方運算。

另外，同態加密和零知識證明也是常見會運用至安全多方運算的技術，前者可擴及多個參與者基於密碼學原理進行安全多方運算，而後者則是用以輔助或驗證安全多方運算之各方輸入合法性。

（二） 適用情境

安全多方運算允許多個參與者在沒有可信任第三方，且不洩漏彼此的秘密輸入的情況下，實現聯合計算。而依據使用不同的技術、協議，安全多方運算適用情境不盡相同，概略地說混淆電路適合安全「兩」方運算，而秘密分享則適用安全「多」方運算，然而也存在可以擴充至安全多方運算的混淆電路協議，因此以下僅舉例安全多方運算技術的適用場景，不深入探究底層所用之技術、協議等。

**1.** 電子投票[85]：選民在不揭露自身選擇（秘密輸入）的情況下，計算出各個候選者的票數，惟安全多方運算無法滿足抗強迫性（Coercion Resistance），也就是說投票者無法證明選民是否有投票，因此實際應用需要建構其他安全設置。

**2.** 封閉式拍賣（Sealed-bid Auction）：競標者在不向彼此揭露出價金額（秘密輸入）的情況下，計算誰的出價較高。

**3.** 防止衛星碰撞[86]：衛星公司不希望透露其所有衛星軌道的確切位置，但

[85] D. G. Nair, V. P. Binu and G. S. Kumar, “An Improved E-voting scheme using Secret Sharing based Secure Multi-party Computation”. arXiv, Feb. 2015, Doi: 10.48550/arXiv.1502.07469. Available: http://arxiv.org/abs/1502.07469. Accessed: Aug 31, 2023.

[86] B. H. Welser Bill, “Cryptographers Could Prevent Satellite Collisions”, Scientific American. Doi: 10.1038/s

也不希望與其他衛星發生碰撞。公司之間透過安全多方運算協議，以估算碰撞的機率，且無須揭露衛星軌道之資訊。

4. 私有集合交集（Private Set Intersection）：屬於安全多方運算的子問題，參與方各擁有一個集合（秘密輸入），想要聯合計算這些集合的交集，但是都不想透露交集以外的資訊。舉例來說，Google 在 2019 年時提出一種 Chrome 擴充功能–Password Checkup[87]，其中就有使用到私有集合交集的技術，檢測使用者存在 Chrome 的密碼與 Google 雲端的不安全密碼庫是否有交集，如此不但能達到檢測弱密碼的目的，也不會洩漏任何使用者密碼給 Google。
5. 閾值簽名方案（Threshold Signature Schemes）[88]：藉由秘密分享技術將私鑰分解成數份「份額」分散保存，當有需簽署數位簽章時，再利用安全多方運算將各個「份額」計算成數位簽章。該做法效益包含：將私鑰以「份額」的方式分散保存，能避免單一節點被突破而丟失私鑰；藉由閾值秘密分享（Threshold Secret Sharing）能實現更細緻的私鑰管理，需要一定數量「份額」持有者甚至是特定「份額」持有者同意方能簽章[89]。

由於安全多方運算需要額外的加密資訊傳輸與計算，在評估效率的時候需考量傳輸趟數、傳輸資料量以及計算複雜度與所需時間。以下分別以幾個方面來討論安全多方運算的適性與限制：

1. 計算效率：聯合計算函數越複雜則需要更高的計算資源，在機器學習上實現安全多方運算，混淆電路的計算電路會更複雜、更多電路閘，而秘密分享也需要進行更多次加、乘法的計算。

---

cientificamerican0215-28b. Available: https://www.scientificamerican.com/article/cryptographers-could-prevent-satellite-collisions/. Accessed: Aug 31, 2023.

87 “Protect your accounts from data breaches with Password Checkup”, Google Online Security Blog. Available: https://security.googleblog.com/2019/02/protect-your-accounts-from-data.html. Accessed: Aug 31, 2023.

88 J.-P. Aumasson, A. Hamelink and O. Shlomovits, “A Survey of ECDSA Threshold Signing”. 2020. Available: https://eprint.iacr.org/2020/1390. Accessed: Aug 31, 2023.

89 T. Tassa, “Hierarchical Threshold Secret Sharing, J Cryptology”, vol.20, no.2, pp. 237–264, Apr. 2007, Doi: 10.1007/s00145-006-0334-8. Available: https://doi.org/10.1007/s00145-006-0334-8. Accessed: Aug 31, 2023.

2. 通訊效率：通訊效率會隨著參與方變多、協議執行輪次增加而下降，以混淆電路為例，由於需要用到模糊傳輸，加上依據不同計算電路與選用協議，可能需要多輪通訊方能完成安全多方運算，故不適合於頻寬受限，或是網路環境不穩定的環境下使用（不過近年隨著技術與協議的最佳化，已逐步改善此問題）。
3. 資料面：基本上預設輸入為數值化資料，若不是則需要預先做轉化處理，此外，目前僅部分開源工具能夠支援浮點數運算，惟浮點數計算效率通常較低，且容易因底層技術牽涉到加解密無法傳遞大量資料，而易有溢位問題。

（三） 技術施用風險

安全多方運算的信任環境、安全性通常由真實-理想模型 (Real-Ideal Paradigm) 來定義：藉由證明攻擊者 (Adversary) 在實際構造 (Real Model) 下造成的危害不會比在理論模型 (Ideal Model) 下更多，以此來驗證該理論模型能抵抗威脅模型。

一般來說，依據攻擊者的能力可以大致分為以下兩種安全模型（Security Model）[90]：

1. 半誠實（Semi-Honest）：攻擊者會正確地執行協議，但是會企圖從得到的資訊中破解其他人的秘密，也就是誠實但富有好奇心的攻擊方，是最低限度的攻擊者假設，大多數協議只要有如實執行皆可防範。
2. 惡意（Malicious）：攻擊者可能不會正確地執行協議，甚至會試圖破壞協議執行。是更貼近現實執行的安全模型，但也因為更強的安全性保證，通常需要更加昂貴的建構成本。設置上有以下兩種形式：
   (1) 主動安全中止（Active Security with Abort）：一旦攻擊者沒有正確地執行協議，其他參與者會有極高機率終止協議，甚至是發現不遵守

90 D. Evans, V. Kolesnikov, and M. Rosulek, supra note 84, at 66.

協議的攻擊者。

(2) 強韌安全（Robust Security）：即使攻擊者不遵守協議，只要誠實參與者多過攻擊方的數量，協議仍可正常執行。

實際在挑選適用協議與模型時，應評估使用情境中可能面臨的攻擊的樣態，並在安全性與協議執行效率間進行平衡。

▼表十六、安全多方運算安全模型比較表

| 安全模型 | 半誠實 | 惡意 |
|---|---|---|
| 優點 | 建構成本較低且簡易 | 具有更好的安全性 |
| 缺點 | 只能適用在苛刻假設的條件下 | 需要導入額外的技術（例如：零知識證明等），亦要額外的儲存空間與通訊成本 |

安全多方運算特性為保障輸入資料與計算期間之機密性，但不保護輸出結果。因此，若輸出結果亦為需保密之資料，部署時應對靜態和傳輸中的資料施予適當之加密措施，以降低機敏資料洩露的風險。

（四） 開源工具與社群

參考工具之維護狀況、社群活躍度、GitHub star 數/fork 數、可支援模型和隱私方法、說明文件和教學檔案，經綜合評估列舉安全多方運算之開源工具如下：

▼表十七、安全多方運算開源工具分析表

| 工具名稱 | 開發語言 | 基本文字介紹 | 優缺點/擅長解決之問題 |
|---|---|---|---|
| MP-SPDZ | C++, Python | 將 SPDZ-2（實現能抵抗惡意攻擊的 BGW 協議之變體——SPDZ 協議）擴充至 30 多個 SMPC 協議變體，使其能夠在各種安全模型中對各式安全多方運算協議進行測試。 | • 多種協議選擇：一般 SMPC 開源工具只提供單一協議框架，而 MP-SPDZ 提供誠實和不誠實的多數、半誠實和惡意腐敗等各式協議模型可調試，因此能針對同樣計算做不同模型選擇的運算、通訊成本比較<br>• 機器學習：完整支援 TensorFlow 框架。<br>• 介紹文件完整<br>• 記憶體消耗大：基於格的密文相對較大（兆位元組量級），使用的零知識證明需要存儲數百個密文。因此預期每個執行續至少使用 1MB 的空間<br>• 與實際部署的距離：實際部署上關鍵程式碼仍應進行安全審查 |
| CrypTen | Python | 基於 PyTorch 構建的隱私保護機器學習框架，目標是實現機器學習的安全多方運算。 | • 機器學習：能支援 PyTorch 中的張量計算、自動微分等。<br>• Library-based：更容易進行 DeBug 與測試機器學習模型<br>• 數值問題：浮點數溢位問題將比僅使用 PyTorch 時嚴重<br>• 與實際部署的距離：僅實現任意參與方的半誠實安全多方運算模型，無法抵禦惡意攻擊，且易受溢位攻擊 |
| ABY | C++ | 由 Demmler 等人在 2015 年提出提供了支援算術、布林秘密分享和姚氏混淆電路等三種秘密分享方案，使用者 | • 三種底層技術轉換：有效地結合了基於算術、布林秘密分享和姚氏混淆電路，藉由將秘密在這三種形式間進行轉換，以實現對不同計算的更高效率。 |

| 工具名稱 | 開發語言 | 基本文字介紹 | 優缺點/擅長解決之問題 |
| --- | --- | --- | --- |
| | | 可以在運算過程中手動切換類型。 | • 可擴充至多方：該框架僅支援兩方，但可以藉由將從多方秘密分享到兩個計算方，然後重建輸入並實現功能。<br>• 模糊傳輸擴充：提供了擴充套件以實現基於預先計算的模糊傳輸。 |
| Obliv-C | OCaml, C | Obliv-C 由美國維吉尼亞大學（University of Virginia）安全研究小組研發，該框架是以 C 語言為基礎，並進行擴充以實現並執行混淆電路。 | • 不須深入電路層面即可使用：提供開發人員程式語言的抽象層，只要在程式語言中描述要保護的秘密資料，即可借助函式庫實現安全運算。<br>• 僅支援兩方混淆電路。 |

由於安全多方運算有許多不同的威脅模型及協議，相關資料亦可進一步參考 MPC-Sok Frameworks Research[91][92]，其提供了十七種開源框架的簡介及比較。

[91] M. Hastings, B. Hemenway, D. Noble, and S. Zdancewic, “SoK: General-purpose compilers for secure multi-party computation,” in 2019 IEEE symposium on security and privacy (SP), 2019.

[92] M. Hastings, “A Layperson’s Guide,” MPC-SoK/frameworks Wiki, Nov. 14, 2018. Available: https://github.com/MPC-SoK/frameworks/wiki/A-Layperson’s-Guide

## （五） 標準

▼表十八、安全多方運算之標準統整表

| 標準名稱 | 標準編號 | 發布組織 | 類型 | 發布日期 | 標準說明 |
|---|---|---|---|---|---|
| 資訊技術–安全技術–秘密分享–第 1 部分：概述（Information technology- Security techniques- Secret sharing） | ISO/IEC 19592-1:2016 | ISO/IEC | 指引 | 2016-11 | 重點討論秘密分享的基礎模型和相關術語，並介紹了秘密分享方案可能具有的屬性。 |
| 資訊技術–安全技術–秘密分享–第 2 部分：基礎機制（Information technology- Security techniques- Secret sharing） | ISO/IEC 19592-2:2017 | ISO/IEC | 標準 | 2017-10 | 涵蓋五種秘密分享算法，滿足訊息機密性和可恢復性之要求 |
| 資訊安全–安全多方運算–第 1 部分：概述（Information security- Secure multiparty computation- Part 1: General） | ISO/IEC 4922-1:2023 | ISO/IEC | 標準 | 2023-07 | 本文件規定了安全多方運算和相關技術的定義、術語和流程，以建立分類法並實現互操作性。 |
| 資訊安全–安全多方運算–第 2 部分：秘密分享機制（Information security- Secure multiparty computation- Part 2: Mechanisms based on secret sharing） | ISO/IEC FDIS 4922-2 | ISO/IEC | 標準 | 尚未發展成標準 | 關於基於秘密分享的 SMPC 即將推出的標準。 |
| IEEE 安全多方計算推薦實踐（IEEE Recommended Practice for Secure Multi-Party Computation） | IEEE 2842-2021 | IEEE | 標準 | 2021-11 | SMPC 的技術框架，並包括安全級別和應用。 |
| 隱私強化技術（Privacy-enhancing technologies, PETs） | 無 | 英國資訊委員辦公室（ICO） | 指南 | 2023-06-21 | 本指南包含：定義和用途、保護資料的方式、實作考量、隱私安全風險。 |

（六） 示範性案例

1. 擬真情境案例：以安全多方運算實現平均薪資之隱私保護案例
2. 實際案例

▼表十九、安全多方運算之實際案例列表

| 參與者 | 描述 | 使用技術 | 開發成熟階段 |
|---|---|---|---|
| 波士頓女性勞動力委員會、波士頓大學、非營利組織 | 波士頓女性勞動力委員會透過安全多方運算技術，在不透露原始資料的情況下，統計波士頓地區之性別和種族薪資差距。其資料是由多個非營利組織提供之試算表。其流程會先由非營利組織將原始資料加上隨機遮罩，再加密遮罩，一併上傳至波士頓大學開發之系統進行統計，完成後會將結果傳至波士頓女性勞動力委員會，最後解密遮罩並將其從統計結果移除，得到真實薪資差距之資料。 | 安全多方運算 | 正式上線 |
| 韓國政府、私人企業 | 韓國統計局結合同態加密、安全多方運算與差分隱私等技術，在不暴露敏感資訊的狀況下，讓政府各部門的資料可以安全的連結與使用。此應用試辦之資料為韓國統計局登記之各企業詳細資訊，如機構名稱、公司登記號碼與行政區碼。過程中資料會在加密的狀態下進行連結與分析。 | 同態加密、安全多方運算、差分隱私 | 應用試辦 |
| 歐盟統計局、參與研究之受試者 | 歐盟統計局結合聯合學習、安全多方運算與同態加密等技術，透過與受試者智慧裝置持續低強度的互動，在不洩漏隱私的情況下進行調查研究。其資料包含受試者回覆問題的答案，以及智慧裝置內傳感器的資料，如加速度計、陀螺儀資料等。 | 聯合學習、安全多方運算、同態加密 | 概念性驗證 |

# 肆、 隱私強化技術應用案例

## 一、 應用案例整理與說明

隱私強化技術尚屬新興技術，各種潛在應用亦尚在發展中。此指引欲透過案例分享使組織更了解隱私強化技術能解決的問題和帶來的效益。下表案例收集自：彙整公開的國際實際案例[93]、探訪國內案例並與學術團隊合作開發模擬案例等，依本指引中《隱私強化技術之分類與應用》章節說明之四種應用場景類別分類。

93 “UN Guide on Privacy-Enhancing Technologies for Official Statistics // Task Team on Privacy Enhancing Techniques — UN-CEBD”. Available: https://unstats.un.org/bigdata/task-teams/privacy/guide/index.cshtml. Accessed: Aug 31, 2023.

## （一） 與資料蒐集相關之案例

▼表二十、與資料蒐集相關應用案例整理與說明表

| 參與者 | 描述 | 使用技術 | 開發成熟階段 |
|---|---|---|---|
| BanCo 金融服務業者、金融機構 | BankCo 金融服務業者透過安全多方運算技術，在不透漏原始資料的情況下，協助金融機構評估客戶信用風險。其資料來源多樣，包含來自債務催收機構、信用卡發行機構、公開紀錄等的個人財務資訊。金融服務業者從各來源蒐集原始資料後，對原始資料加入差分隱私雜訊，執行並產出分析結果供金融機構應用。 | 差分隱私 | 正式上線 |
| 韓國政府、私人企業 | 韓國統計局結合同態加密、安全多方運算與差分隱私等技術，在不暴露敏感資訊的狀況下，讓政府各部門的資料可以安全的連結與使用。此應用試辦之資料為韓國統計局登記之各企業詳細資訊，如機構名稱、公司登記號碼與行政區碼。過程中資料會在加密的狀態下進行連結與分析。 | 同態加密、安全多方運算、差分隱私 | 應用試辦 |
| 澳洲蒙納許大學、醫生、應用程式使用者 | 澳洲蒙納許大學團隊透過零知識證明技術開發應用程式，能在不透露隱私資訊的狀況下，追蹤與確診者接觸的人員並通知其進行隔離[94]。資料集為應用程式使用者之行動裝置與接觸人員資料。資料處理流程是先由使用者安裝之應用程式紀錄接觸史，一旦醫生判定使用者確診 COVID-19，使用者可以在不透露隱私的情況下證明其接觸者之真實性，最後醫生透過系統發出訊息，通知接觸者進行自我隔離。 | 零知識證明之 Σ-協定 | 概念性驗證 |

94 J. K. Liu et al., “Privacy-Preserving COVID-19 Contact Tracing App: A Zero-Knowledge Proof Approach”. May. 2020. Available: https://eprint.iacr.org/2020/528. Accessed: Aug 31, 2023.

## （二） 與多方資料協作相關之案例

▼表二十一、與多方資料協作相關應用案例整理與說明表

| 參與者 | 描述 | 使用技術 | 開發成熟階段 |
|---|---|---|---|
| 波士頓女性勞動力委員會、波士頓大學、非營利組織 | 波士頓女性勞動力委員會透過安全多方運算技術，在不透露原始資料的情況下，統計波士頓地區之性別和種族薪資差距。資料集是由 100 多個非營利組織提供之試算表。資料處理流程是先由非營利組織將原始資料加上隨機遮罩，再加密遮罩，一併上傳至波士頓大學開發之系統進行統計，完成後會將結果傳至波士頓女性勞動力委員會，最後解密遮罩並將其從統計結果移除，得到真實薪資差距之資料。 | 安全多方運算 | 正式上線 |
| 義大利國家統計研究所、義大利銀行、連結服務平台 | 義大利國家統計研究所與義大利銀行透過私有集合交集技術，在不共享原始資料集的情況下，連結雙方資料集以求更佳的實用性。資料集為社會人口統計與金融資料集，兩資料集具有共同欄位「稅號」。資料處理流程分成四個步驟，首先雙方先同步協定參數，再來以私有集合交集技術求取雙方具相同「稅號」的資料列，然後加密上傳至連結服務平台，最後雙方便可向平台查詢連結之資料列。 | 私有集合交集之 PSI-A 框架 | 應用試辦 |
| 韓國政府、私人企業 | 韓國統計局結合同態加密、安全多方運算與差分隱私等技術，在不暴露敏感資訊的狀況下，讓政府各部門的資料可以安全的連結與使用。此應用試辦之資料為韓國統計局登記之各企業詳細資訊，如機構名稱、公司登記號碼與行政區碼。過程中資料會在加密的狀態下進行連結與分析。 | 同態加密、安全多方運算、差分隱私 | 應用試辦 |
| 歐盟統計局、參與研究之受試者 | 歐盟統計局結合聯合學習、安全多方運算與同態加密等技術，透過與受試者智慧裝置持續低強度的互動，在不洩漏隱私的情況下進行調查研究。資料集包含受試者回覆問題的答案，以及智慧裝置內傳感器的資料，如加速度計、陀螺儀資料等。 | 聯合學習、安全多方運算、同態加密 | 概念性驗證 |

| 參與者 | 描述 | 使用技術 | 開發成熟階段 |
| --- | --- | --- | --- |
| 加拿大統計局、零售商、雲端運算平台 | 加拿大統計局研究透過同態加密技術，在不透露原始資料的情況下，於不信任之雲端平台進行機器學習。資料集為各零售商提供之產品資料。資料處理流程是先由零售商以同態加密技術加密資料，再將其上傳至不信任的雲端運算平台訓練機器學習模型，然後將運算結果回傳至加拿大統計局，最後以密鑰解密得到模型權重。 | 同態加密 | 概念性驗證 |

## （三） 與資料運算相關之案例

▼表二十二、與資料運算相關應用案例整理與說明表

| 參與者 | 描述 | 使用技術 | 開發成熟階段 |
|---|---|---|---|
| Duality 科技公司、跨國金融機構、執法機構、第三方資料處理平臺 | Duality 科技公司與多個跨國金融機構及執法機構共組聯盟，透過同態加密技術，在不直接共享金融客戶資料下，共同識別與防治金融相關犯罪。其資料來源為各個聯盟成員之客戶資料。客戶資料經資料持有方使用同態加密保護後，以密文形式交由資料處理平臺進行分析處理，並由資料處理平臺分享處理結果供其他聯盟成員解密應用。除處理結果外，聯盟成員無法反向追溯原始資料，並以此保障客戶資料隱私。 | 同態加密 | 正式上線 |
| 印尼旅遊部、行動網路業者 | 印尼旅遊部透過可信執行環境技術，在不直接共享原始資料的情況下，合併多個行動網路業者之使用者漫遊資料，統計跨境旅遊資料。資料集為多個行動網路業者提供之境內同時段 IMSI（International Mobile Subscriber Identity）清單。資料處理流程是先由行動網路業者將 IMSI 清單之數值部份位元雜湊處理後，由加密管道傳至硬體隔離平台計算統計資料，最後再將結果由加密管道傳至印尼旅遊部。 | 可信執行環境 | 正式上線 |
| 韓國政府、私人企業 | 韓國統計局結合同態加密、安全多方運算與差分隱私等技術，在不暴露敏感資訊的狀況下，讓政府各部門的資料可以安全的連結與使用。此應用試辦之資料為韓國統計局登記之各企業詳細資訊，如機構名稱、公司登記號碼與行政區碼。過程中資料會在加密的狀態下進行連結與分析。 | 同態加密、安全多方運算、差分隱私 | 應用試辦 |
| 帝濶智慧科技、聯新國際醫療、資料服務公司 | 為確保資料(資料服務公司會員行為分析、醫療科學研究資料及數位化轉型資料共享)於雲端儲存、釋出使用及資料分析階段之隱私保障。資料服務公司、新國際醫療與帝濶智慧科技，合作試辦結合差分隱私、同態加密技術等技術，以生成合成資料、分析去識別化資料及安全加密檔案管理系統。該系統提供資料擁有者多種隱私強化方案，於資料上傳至雲端前進行去識別化或加密處理，經處理之資料保存於雲端平台，供後續查詢、釋出及結合其他保存於雲端平台之跨機構資料進行跨域分析。 | 合成資料、差分隱私、可搜尋加密、同態加密 | 應用試辦 |

| 參與者 | 描述 | 使用技術 | 開發成熟階段 |
| --- | --- | --- | --- |
| 歐盟統計局、參與研究之受試者 | 歐盟統計局結合聯合學習、安全多方運算與同態加密等技術，透過與受試者智慧裝置持續低強度的互動，在不洩漏隱私的情況下進行調查研究。資料集包含受試者回覆問題的答案，以及智慧裝置內傳感器的資料，如加速度計、陀螺儀資料等。 | 聯合學習、安全多方運算、同態加密 | 概念性驗證 |
| 加拿大統計局、零售商、雲端運算平台 | 加拿大統計局研究透過同態加密技術，在不透露原始資料的情況下，於不信任之雲端平台進行機器學習。資料集為各零售商提供之產品資料。資料處理流程是先由零售商以同態加密技術加密資料，再將其上傳至不信任的雲端運算平台訓練機器學習模型，然後將運算結果回傳至加拿大統計局，最後以密鑰解密得到模型權重。 | 同態加密 | 概念性驗證 |
| 國立中山大學資訊工程學系、國立中山大學醫學科技研究所、高雄榮民總醫院、病患（資料當事人）、病患授權之資料存取者 | 為克服資料上雲後的隱私保護挑戰，國立中山大學團隊與高雄榮民總醫院合作，開發「具隱私保護暨安全資料探勘之醫療資料倉儲系統」[95]。於概念性驗證過程中，團隊將病患醫療測試資料加密上傳雲端，加密後之資料在密文狀態下仍可搜尋及統計分析，並可由資料當事人自主設定資料存取權限，提供資料參與聯合學習或其他資料應用。此概念驗證為儲存於雲端的病歷，提供資料生命周期全程隱私保障，並賦予病患自主運用資料的權力。 | 同態加密、可搜尋式加密、屬性加密 | 概念性驗證 |

[95] 盧奕昕，「保護病歷不被偷看和竄改！專訪國立中山大學資訊工程學系范俊逸特聘教授談如何『加密』善用醫療資訊」，科技大觀園。載於：https://scitechvista.nat.gov.tw/Article/C000003/detail?ID=e3b61ad5-8c66-46a2-b6c7-b9e6d20e3bf5.

## （四） 與資料分享相關之案例

▼表二十三、與資料分享相關應用案例整理與說明表

| 參與者 | 描述 | 使用技術 | 開發成熟階段 |
|---|---|---|---|
| 美國普查局<br>大眾 | 美國普查局公開普查資料讓大眾使用時，透過差分隱私技術加入雜訊，兼顧隱私保護力與資料可用性。資料集包括美國不同種族人口與居住地相關敏感資料。資料處理流程是先依據地理單位由大至小計算統計資料，再依隱私洩漏風險與隱私預算 ε 值加入雜訊。 | 差分隱私之 TopDown 演算法[96] | 正式上線 |
| 加拿大統計局、黑客松競賽參賽者 | 加拿大統計局透過合成資料技術之機器學習方式，可在不侵犯個人隱私的情況下，產製高可用性且貼近真實的資料讓黑客松競賽參賽者進行分析。資料集包含人口普查、健康和死亡資料等敏感資訊。 | 合成資料之機器學習方式 | 應用試辦 |
| 帝濶智慧科技、聯新國際醫療、資料服務公司 | 為確保資料（資料服務公司會員行為分析、醫療科學研究資料及數位化轉型資料共享）於雲端儲存、釋出使用及資料分析階段之隱私保障。資料服務公司、新國際醫療與帝濶智慧科技，合作試辦結合差分隱私、同態加密技術等技術，以生成合成資料、分析去識別化資料及安全加密檔案管理系統。該系統提供資料擁有者多種隱私強化方案，於資料上傳至雲端前進行去識別化或加密處理，經處理之資料保存於雲端平台，供後續查詢、釋出及結合其他保存於雲端平台之跨機構資料進行跨域分析。 | 合成資料、差分隱私、可搜尋加密、同態加密 | 應用試辦 |

[96] J. Abowd, D. Kifer, S. Garfinkel and A. Machanavajjhala, “Census TopDown: Differentially Private Data, Incremental Schemas, and Consistency with Public Knowledge”, 2019. Available: https://www.semanticscholar.org/paper/Census-TopDown%3A-Differentially-Private-Data%2C-and-Abowd-Kifer/cd020070f56f155a45e13ee404109edf3f452ebc. Accessed: Aug 31, 2023.

## 二、 模擬案例一：共享糖尿病預測科研數據

### （一） 情境說明

為進行糖尿病預測相關科學研究，醫院提供糖尿病患資料予研究中心，並於資料釋出前使用差分隱私、合成資料或 k-匿名化技術，以保障病患隱私。

### （二） 情境使用資料說明

本案例使用 NHANES 預測糖尿病之資料集[97]，欄位說明如下：

1. 性別：Male、Female。
2. 年齡：[20, 80]。
3. 人種：Black、Hispanic、Mexican、White、Other。
4. 教育水平：9th、11th、HighSchool、College、Graduate。
5. 婚姻狀況：Married、Widowed、Divorced、Separated、Never、Partner。
6. 是否憂鬱症：是（1）、否（0）。
7. 是否貧困：是（1）、否（0）。
8. 活動量：每週進行的特定活動的天數（以天/週為單位）乘以每天特定活動的持續時間(以分鐘/天為單位)得出 Metabolic Equivalent Scores(METs)（以分鐘/週為單位）。
9. 活動量四分位数：Q1、Q2、Q3、Q4。
10. 是否糖尿病：是（1）、否（0）。

[97] kikn88, “PWSCup 2021 (NHANES diabets).” Apr. 21, 2023. Accessed: Oct. 31, 2023. [Online]. Available: https://github.com/kikn88/pwscup2021

▼表二十四、模擬案例一使用之資料集部分節錄

| | A | B | C | D | E | F | G | H | I | J | K | L |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 01 | Female | 66 | Black | 11th | Divorced | 31.7 | 0 | 1 | 6.2 | 480 | Q2 | 0 |
| 02 | Female | 66 | Other | 9th | Married | 23.7 | 0 | 0 | 6.2 | 600 | Q2 | 0 |
| 03 | Female | 75 | Black | College | Widowed | 38.9 | 0 | 1 | 6.3 | 1440 | Q3 | 0 |
| 04 | Male | 56 | Other | Graduate | Married | 21.3 | 0 | 0 | 5.7 | 3360 | Q3 | 0 |
| 05 | Male | 67 | White | HighSchool | Divorced | 23.5 | 1 | 0 | 5.6 | 1080 | Q2 | 0 |
| 06 | Female | 54 | Black | College | Married | 39.9 | 0 | 0 | 12.7 | 0 | Q1 | 1 |
| 07 | Male | 71 | Other | HighSchool | Married | 22.5 | 0 | 1 | 6.2 | 41440 | Q4 | 0 |
| 08 | Male | 61 | Other | Graduate | Married | 30.7 | 0 | 0 | 5.6 | 3840 | Q3 | 0 |
| 09 | Male | 22 | White | HighSchool | Never | 24.5 | 1 | 1 | 5.1 | 840 | Q2 | 0 |
| 10 | Male | 45 | Black | HighSchool | Never | 22 | 0 | 0 | 5.7 | 1200 | Q2 | 0 |
| 11 | Female | 60 | Mexican | 9th | Married | 35.9 | 0 | 0 | 5.2 | 0 | Q1 | 0 |
| 12 | Female | 60 | White | College | Divorced | 23.8 | 0 | 0 | 5.8 | 0 | Q1 | 0 |
| 13 | Male | 70 | Other | Graduate | Married | 23.9 | 0 | 0 | 5.8 | 2640 | Q3 | 0 |
| 14 | Male | 42 | Black | 11th | Never | 27.6 | 0 | 1 | 5.3 | 0 | Q1 | 0 |
| 15 | Male | 57 | Hispanic | 11th | Widowed | 28.6 | 0 | 0 | 13.3 | 1600 | Q3 | 1 |
| 16 | Male | 52 | Hispanic | 9th | Married | 35.1 | 0 | 1 | 5 | 1920 | Q3 | 0 |
| 17 | Male | 26 | Hispanic | College | Never | 33.7 | 0 | 0 | 5.6 | 29520 | Q4 | 0 |

（三） 使用之隱私強化技術

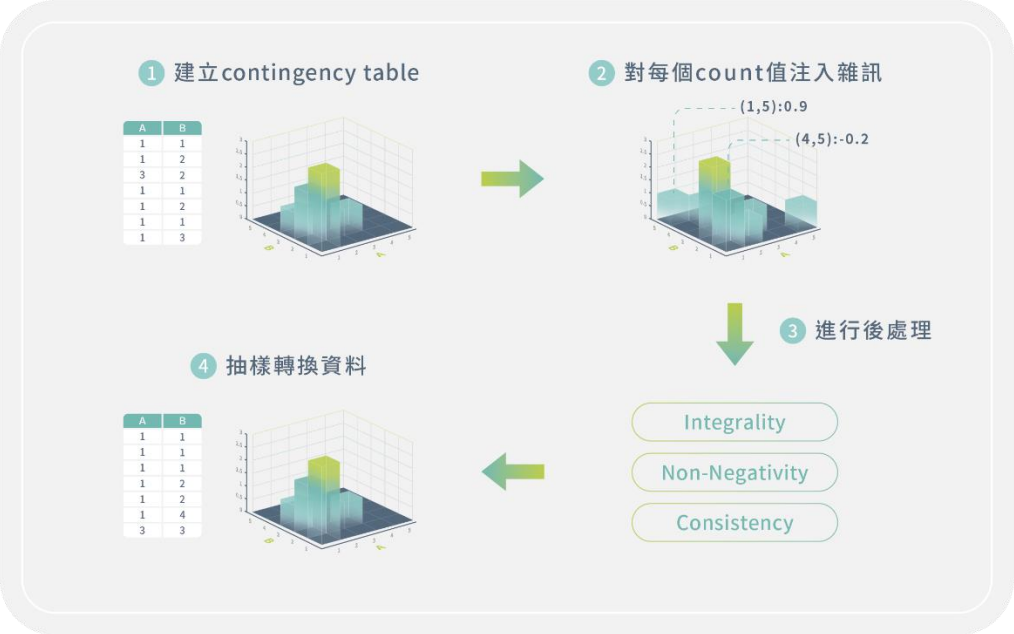
差分隱私、合成資料或 k-匿名化。

（四） 隱私強化技術使用目的

保護參與 NHANES 資料蒐集的受試者資訊，以避免這些受試者遭受推論攻擊，而被推測特定人是否在此名單之中。此外，該資料亦須具備相當程度的可用性，以供後續資料分析及研究。

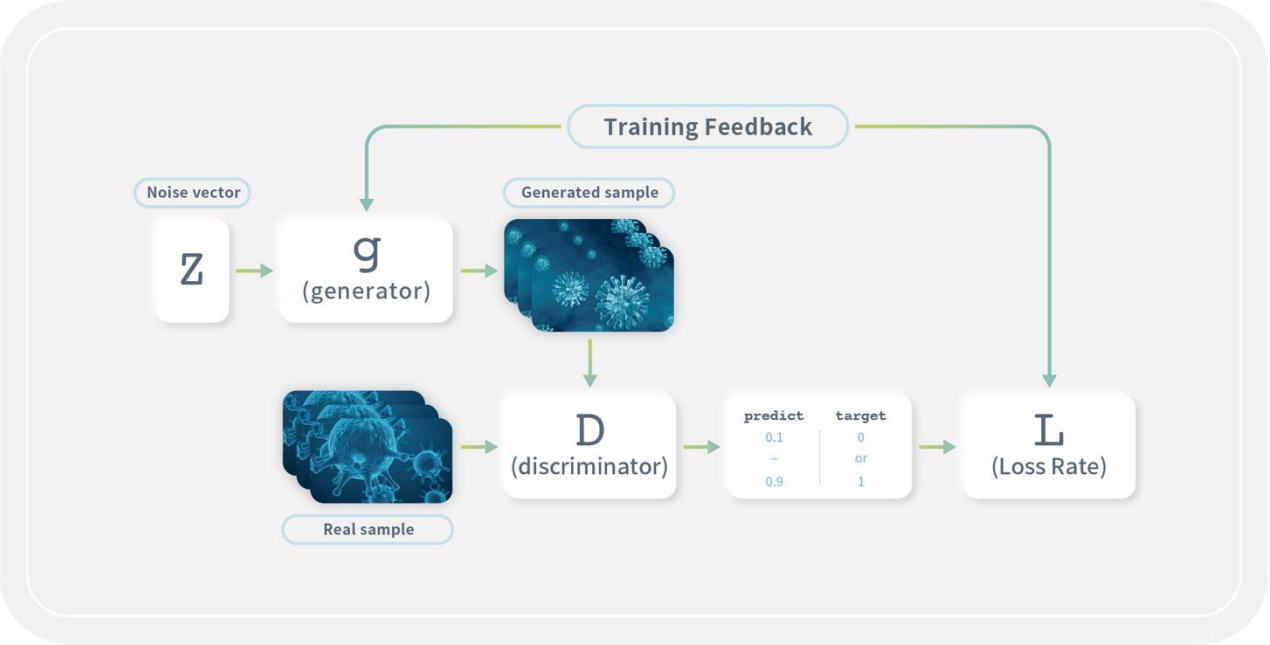
（五） 隱私強化技術運作方式/機制說明

1. 差分隱私：欲使 NHANES 資料集釋出滿足差分隱私，則必須先找到某種資料生成的方式並在其中涉及統計計算的函式輸出注入雜訊。其作法係將資料分布轉換成列聯表(Contingency Table)的形式，然後對每一個 count 值注入雜訊後，再根據新的統計分布透過抽樣轉換回資料型態。下圖簡略敘述了具差分隱私的資料生成方法，但要注意的是在注入雜訊後接續進行了後處理的程序(Post-Processing)，此步驟目的在於讓充滿雜訊的分布能更合理，且貼近實際分布狀況，例如應避免 count 值負值等。




▲圖十六、以差分隱私生成資料之運作流程

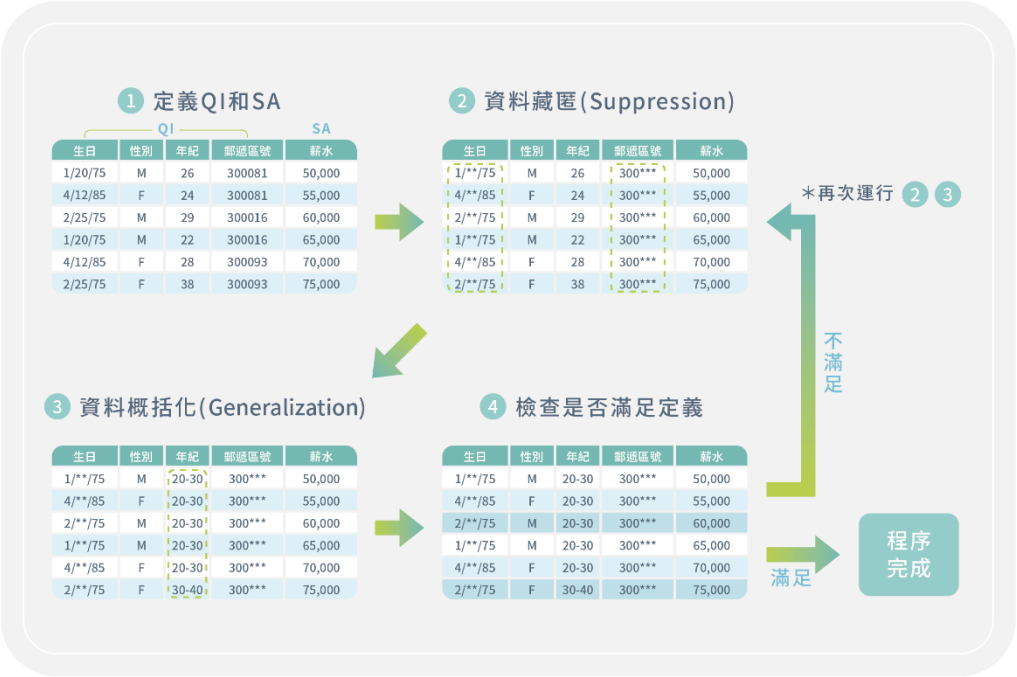
**2.** 合成資料：要從 NHANES 資料集釋出一個可供發佈之資料集，首先需選定一種產生合成資料之方式，如機器學習模型或數學建模等，來捕捉 NHANES 資料集的統計特徵。以生成對抗網路（Generative Adversarial Network）為例，該模型將以 NHANES 資料集為輸入，藉由模型的生成器（Generator）和判別器（Discriminator）機制，學習資料集的統計特徵，如下圖所示。待模型訓練完畢，再以此模型的生成器產出合成資料。產出之合成資料即可在其數值與原始資料不完全相同的情況下，表現出與原始資料相似之統計特徵。




▲圖十七、以合成資料生成資料集之運作流程[98]

**3.** k-匿名化：為使 NHANES 資料集釋出滿足 k-匿名性，必須先決定資料集中哪個欄位作為敏感屬性（Sensitive Attribute, SA）且其餘屬性當作準識別符（Quasi-identifier, QI）。接續針對類別行屬性運行抑制（Suppression）與泛化（Generalization）。其目的為確保資料中的任一筆紀錄有較大可能與資料集中至少 k-1 筆紀錄具有相同的資料。然而，僅憑單次的程序通常很難滿足上述要求，因為資料進行去識別化的同時應該要盡可能保有原始資料的可利用性。故去識別化程序通常會採用漸進式運行，逐漸增加資料抑制與泛化的強度（如郵遞區號從遮住尾二碼增至三碼），直至符合 k-匿名性定義才輸出 k-匿名化資料集。

[98] S.-W. Park, J.-S. Ko, J.-H. Huh, and J.-C. Kim, “Review on generative adversarial networks: Focusing on computer vision and its applications,” Electronics, vol. 10, no. 10, Art. no. 1216, 2021, Doi: 10.3390/electronics10101216.




▲圖十八、以 k-匿名化生成資料集之運作流程

## （六） 適用此隱私強化技術之其他領域

本案例使用之隱私保護技術均適用於資料共享、釋出統計資料之情境，並常見應用於醫療衛生、科學研究、金融等領域。

## 三、 模擬案例二：金融欺詐事件偵測

### （一） 情境說明

信用卡詐欺對企業、銀行和個人造成的巨大經濟損失，使其在全球備受關注。隨著電子支付的普及，詐欺者可利用更多安全漏洞竊取敏感資訊。這不僅會造成金錢損失，金融機構的聲譽損害，還會影響消費者對電子支付的信任。因此，有效的詐欺檢測系統（Fraud Detection System, FDS）非常重要。FDS 通常利用機器學習和資料分析技術進行檢測，使用已知的詐欺和非詐欺交易資料，例如交易方式、地點、商品、金額等等行為特徵來建立模型。若是想獲得性能良好的模型，需要資料量足夠多的資料集。

一個典型的作法是將這些資料集中到一個中央資料庫，但這種方法會帶來一些隱私方面的挑戰，例如：信用卡交易資料為極具隱私性之資料，因此資料的擁有者可能不希望共享這些資訊，資料傳輸過程中也可能遭到外洩。考量到信用卡交易資料可能推論出個資相關的隱私資訊，集中式 FDS 並不是最合適的方法。

而使用聯合學習訓練 FDS，使多個金融機構在伺服器的協調下進行協作，能夠將每個銀行的資料保存在自己的本地系統中。此舉降低了暴露敏感資料的風險，並且與每家銀行單獨訓練模型相比，能更好地檢測詐欺行為。然而，攻擊者依然可以由傳輸的模型參數中還原原始訓練資料。因此，仍需採用差分隱私來為參數引入雜訊，使得原始模型參數難以被準確識別。若有人試圖通過分析共享模型中的參數來推斷原始訓練資料，也會因模型參數加入雜訊，而難以得到準確原始訓練資料，進一步導致模型準確性下降。經過差分隱私保護的本地端模型參數，在經過伺服器進行聚合後，仍然具有預期的預測準確度。然而在限定模型存取權限的情況下，希望限制伺服器對訓練完成並經過聚合的全域模型參數的存取。因此，通過安全多方計算，系統可以進一步限制伺服器對於本地端模型參數的存取，同時間仍然可完成模型參數的聚合工作。同時加入上述的兩種隱私強化技術，使系統可以在不洩漏敏感客戶資料以及模型參數的情況下進行協作學習，可以為信貸信用分析或詐欺檢測等重要任務生成更準確的模型。

（二） 情境使用資料說明

Credit Card Fraud Detection 資料集包含 2013 年 9 月歐洲持卡人使用信用卡進行的交易紀錄。由於保密問題，公開資料集無法提供資料的原始特徵和更多背景資訊，部分欄位資料為主成分分析（Principal Components Analysis, PCA）轉換後的數值（欄位 V1、V2 至 V28）。主成分分析本質上是一種維度縮減技術，能夠在減少維度的同時保留重要特徵。因此，這 28 個欄位之數值可以被視為是由更多不同資料（如客戶詳情、交易金額、交易地點等）組合而成的綜合數值。

資料集各欄位說明如下：

1. Time：每筆交易與資料集中第一筆交易之間經過的秒數
2. V1, V2, …, V28：通過 PCA 轉換的結果（可能包含隱私資料）
3. Amount：交易金額
4. class：詐欺的情況為 1，否則為 0（預測的目標變量）

▼表二十五、模擬案例二使用之資料集部分節錄

| Time | V1 | V2 | V3 |
|---|---|---|---|
| 0 | -1.3598071336738 | -0.0727811733098497 | 2.53634673796914 |
| Time | V4 | V5 | V6 |
| 0 | 1.37815522427443 | -0.338320769942518 | 0.462387777762292 |
| Time | V7 | V8 | V9 |
| 0 | 0.239598554061257 | 0.0986979012610507 | 0.363786969611213 |
| Time | V10 | V11 | V12 |
| 0 | 0.0907941719789316 | -0.551599533260813 | -0.617800855762348 |
| Time | V13 | V14 | V15 |
| 0 | -0.991389847235408 | -0.311169353699879 | 1.46817697209427 |
| Time | V16 | V17 | V18 |
| 0 | -0.470400525259478 | 0.207971241929242 | 0.0257905801985591 |
| Time | V19 | V20 | V21 |
| 0 | 0.403992960255733 | 0.251412098239705 | -0.018306777944153 |
| Time | V22 | V23 | V24 |
| 0 | 0.277837575558899 | -0.110473910188767 | 0.0669280749146731 |
| Time | V25 | V26 | V27 |
| 0 | 0.128539358273528 | -0.189114843888824 | 0.133558376740387 |
| Time | V28 | Amount | class |
| 0 | -0.0210530534538215 | 149.62 | 0 |

（三） 使用之隱私強化技術

聯合學習除了滿足個別訓練資料擁有者的資料保護需求外，也會需要因應各種潛在的攻擊者來採用不同的隱私強化技術，來抵禦對應的攻擊，例如安全多方運算、差分隱私等技術。聯合學習的隱私性保護因此能夠隨著使用者需要進行調整，滿足不同環境下的資料安全性需求。在此以詐欺檢測系統聯合學習進行舉例說明。

1. 使用聯合學習：透過聯合學習，散落在不同金融機構的客戶信用卡交易資料可進行共同的詐欺檢測模型訓練，每個金融機構在本地使用自己的資料訓練本地模型，再上傳本地參數至伺服器進行全域聚合模型和更新，由於資料不需要傳輸到伺服器或第三方集中，因此能夠保護到不同金融機構之交易資料隱私。

   然而，在此情況下，伺服器能夠直接地獲得每個金融機構的模型參數更新，而外部攻擊者可能在傳輸通道上進行竊聽，以獲取相關資訊並進行推理攻擊，這可能對資料隱私造成威脅。因此，在實施聯合學習時，必須考慮加強資料隱私性保護措施。
2. 加入差分隱私（隱私強化保護之聯合學習）：為了避免伺服器或是外部攻擊者得到金融機構的模型參數更新，將差分隱私加入聯合機器學習中。差分隱私能夠使用多種統計學機制對模型參數加入雜訊防止原始資料之暴露，提高隱私保護程度，然而，增加雜訊可以提高隱私保護程度，但同時會影響模型的準確性。因此，需要在合理的雜訊範圍內找到平衡，確保隱私得到適當保護的同時，維持模型的合理性能。

（四） 隱私強化技術使用目的

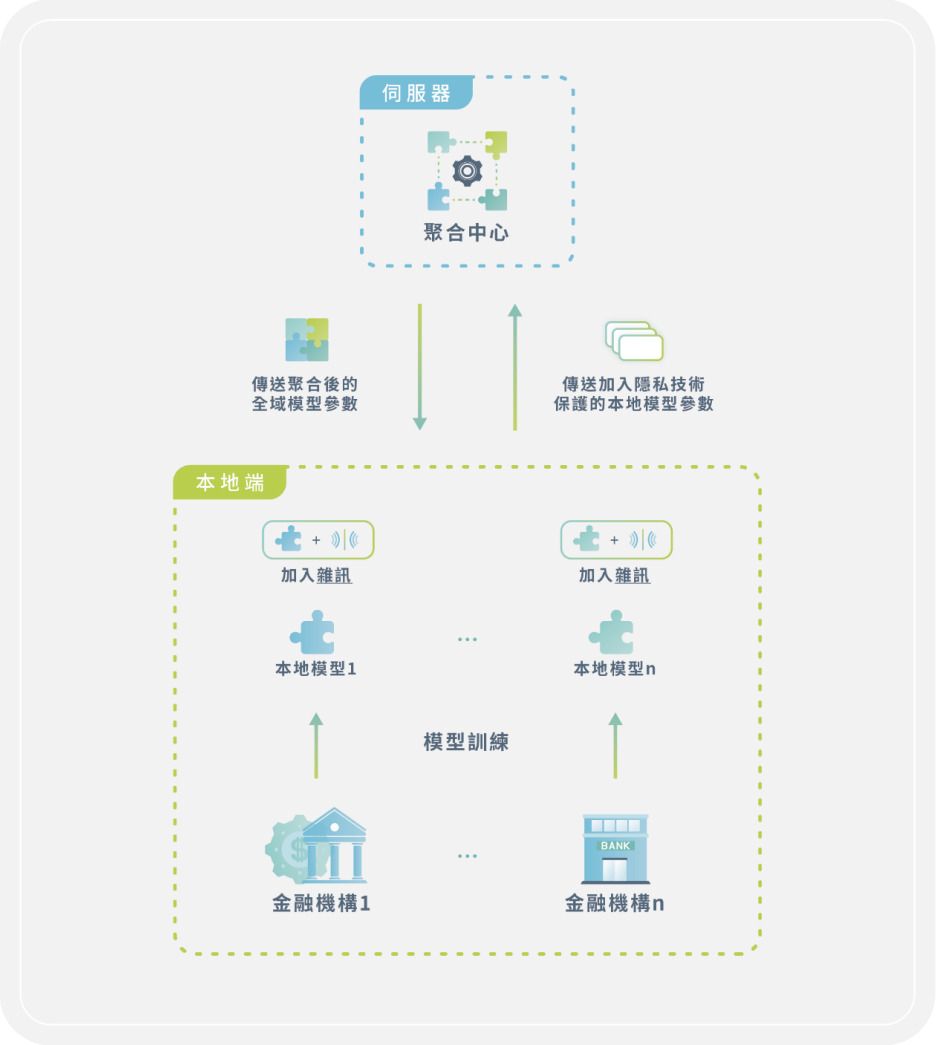
使用聯合學習將資料保存在各自的本地系統中，降低了暴露敏感資料的風險，並且每個本地端皆可從共享模型中獲益，能比個別訓練所得出的模型效能更好。

使用差分隱私防止伺服器與資料提供者合作，藉由彼此所擁有的資訊來推理隱私資料，並防止攻擊者竊聽傳輸通道獲取資料來推理隱私資料。

（五） 隱私強化技術運作方式/機制說明

在隱私強化保護之聯合學習的架構中，指定一個可信任的第三方作為金鑰發放中心，並將每個參與訓練的金融機構視為獨立的本地端。本案例使用公有雲端服務平台（如 AWS、Azure 或 Google Cloud）上的伺服器作為聚合伺服器。為了增強隱私保護，還採用了其他隱私強化技術，因此訓練過程如下：

1. 本地端使用本地資料對模型進行訓練，將獲得的本地模型參數加入差分隱私的隨機雜訊，保護本地模型參數不受伺服器之直接窺探。
2. 將受保護之參數本地模型上傳至聚合伺服器。
3. 當伺服器收到本地端上傳的資料後，將這些資料進行聚合，完成後即可更新全域模型，更新後的全域模型會被傳送回所有本地端，以進行新一輪的訓練。




▲圖十九、聯合學習擬真情境運作架構

## （六） 適用此隱私強化技術之其他領域

需要隱私性保護之分散式機器學習訓練之場景，如智慧醫療、智慧工業控制、車聯網路、智慧電網、物聯網路等。

## 四、 模擬案例三：犯罪資料雲端運算

### （一） 情境說明

近年來，行政院於全台許多組織單位，推動「資訊資源向上集中」，使得許多單位的主機等資通設備，不再各自管理，而是交由上級單位或資訊管理單位統一集中維運。雖然向上集中的作法，可以使得資通系統方便管理，然而，此方法卻也意味著資訊管理單位，易於取得其所管理主機的資料，產生了隱私外洩的可能性。

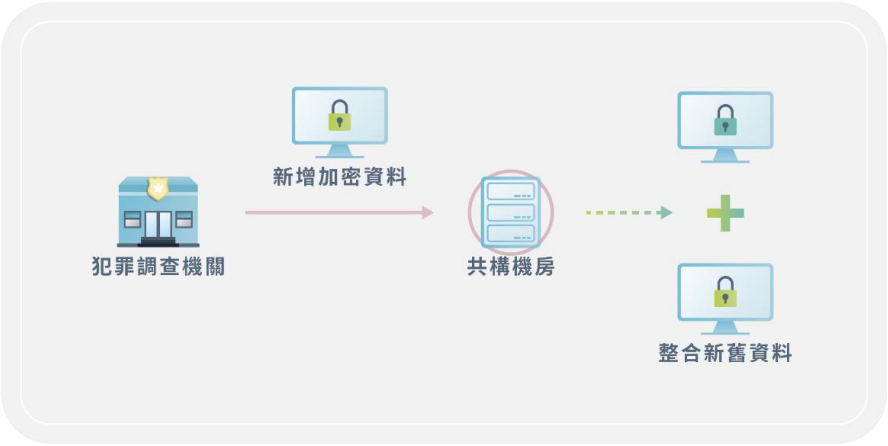
如上所述，假設行政院的各部機關，希望推動向上集中的計畫時，同樣需要面臨此議題。因此，藉由模擬犯罪調查權責機關實行向上集中計畫，將犯罪相關之資料集中於他方機構（例如：共構機房）進行管理，並在此模擬情境中，將全同態加密（fully homomorphic encryption）技術應用於隱私保護，將欲向上集中之資料透過加密，使共構機房無法得到資料的明文內容，並利用全同態加密之特性，讓共構機房在不知道明文內容的條件下，一樣得以進行各種運算操作。這樣，便可以解決上述之難題，讓向上集中計畫與隱私保護得以同時並行。

在擬真情境中，利用全同態加密的機制，先將犯罪調查機關（以下稱為 client 端）所有的明文犯罪資料進行加密，然後傳送至共構機房（以下稱為 server 端），由共構機房進行保管與運算。


▲圖二十、同態加密擬真情境運作架構

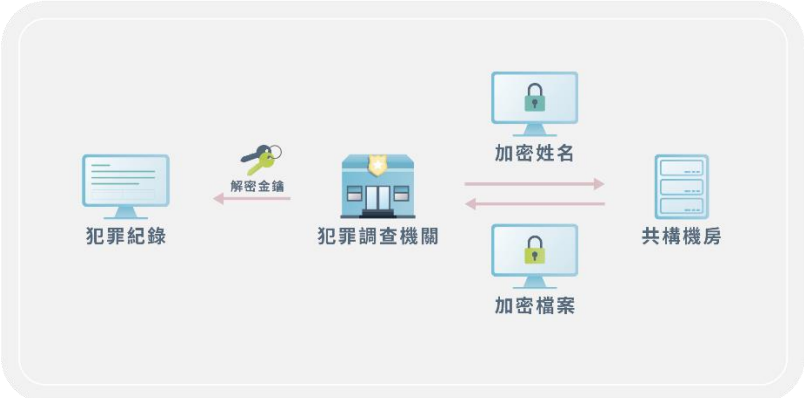
而 server 端可以提供如下三種服務：

1. 新增案件：client 端可以利用全同態加密，以密文的形式，上傳多筆新增的案件資料，由 server 端將新的資料與舊的案件資料合併。



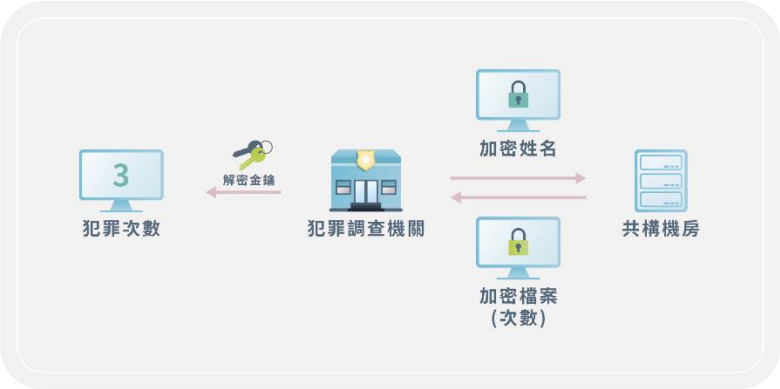

▲圖二十一、同態加密擬真情境運作架構：新增案件

2. 犯罪案件查詢：client 端可以利用全同態加密，上傳一個加密過後的姓名資料，由 server 端對所有資料以密文形式進行比對，最後，再將對應姓名的犯罪資料，傳送回 client 端，由 client 端自行解密，得到此犯罪者的所有犯罪資料。




▲圖二十二、同態加密擬真情境運作架構：犯罪案件查詢

3. 犯案次數查詢：client 端可以上傳一個加密過後的姓名資料，由 server 端對所有資料以密文形式進行比對，並計算此人的犯罪次數，最後，再將密文的犯罪次數回傳至 client 端，由 client 端自行解密，得到此犯罪者的犯罪次數。




▲圖二十三、同態加密擬真情境運作架構：犯案次數查詢

## （二） 情境使用資料說明

本案例參考政府資料開放平台[99]其中的犯罪資料，來生成模擬犯罪調查機關的犯罪資料集。

資料集各欄位說明如下：

1. 姓名：實際記錄犯罪者的姓名，此處說明以*表示。
2. 案類：記錄每一次犯罪的案件類別。
3. 發生日期：記錄每一次犯罪的發生日期。
4. 發生地點：記錄每一次犯罪的發生地點。

▼表二十六、模擬案例三使用之資料集部分節錄

| 姓名 | 案類 | 發生日期 | 發生地點 |
|---|---|---|---|
| * | 住宅竊盜 | 1100701 | 苗栗縣後龍鎮 |
| * | 住宅竊盜 | 1100701 | 花蓮縣吉安鄉 |
| * | 住宅竊盜 | 1100701 | 新北市深坑區 |
| * | 住宅竊盜 | 1100701 | 新竹縣竹北市 |
| * | 住宅竊盜 | 1100701 | 南投縣埔里鎮 |
| * | 住宅竊盜 | 1100702 | 桃園市八德區 |
| * | 住宅竊盜 | 1100702 | 新北市新莊區 |

[99] 政府資料開放平台，〈犯罪資料〉，網址： https://data.gov.tw/dataset/14200/ （檢索日期：2023 年 8 月 31 日）。

| 姓名 | 案類 | 發生日期 | 發生地點 |
| --- | --- | --- | --- |
| * | 住宅竊盜 | 1100703 | 新北市三重區 |
| * | 住宅竊盜 | 1100703 | 臺北市大同區 |

（三） 使用之隱私強化技術

全同態加密（fully homomorphic encryption）

（四） 隱私強化技術使用目的

透過全同態加密技術，使共構機房在無法得到明文資料的條件下，仍然得以進行各種運算操作。

（五） 隱私強化技術運作方式/機制說明

在大部分的加密系統中，加密過後的資料，是很難在不解密的條件下，對其做有效運算的。然而，資料的解密，常常伴隨著隱私外洩的風險。而全同態加密（homomorphic encryption）技術，是解決此問題的最佳方法之一。

全同態加密技術的運作方式如下圖所示。假設資料的擁有者，需要將資料交給他方進行運算，其運作機制為：

1. 資料的擁有者先將欲傳送的資料，利用全同態加密技術的金鑰，進行加密，再將密文資料傳送給資料運算者。
2. 資料運算者得到密文後，可以根據資料擁有者的需求，對資料在密文的條件下，進行對應的運算。
3. 資料運算者計算完成後，再把經過運算的密文資料，傳送回資料的擁有者。
4. 資料的擁有者可以利用解密金鑰，將經過運算的密文進行解密，得到需要的計算結果。


▲圖二十四、同態加密實際使用情境示意圖

全同態加密技術的優勢在於，除了資料的擁有者外，其他人都無法得到資料的明文內容，包括資料的運算者。其原因在於，資料的擁有者給予他方的資料，都是經過加密的密文資料，而共構機房的所有運算，也都是以密文條件下進行的，因此，不會有因為需要計算，導致資料需要先解密，造成的隱私洩漏。這樣的機制，可以極大程度的保護資料擁有者的隱私安全。

（六） 適用此隱私強化技術之其他領域

1. 醫療：在醫療領域中，一直非常重視關於病患的個人資料保護，但是在保存醫療資料時，仍舊會需要將這些隱私資料儲存在資料庫中。而全同態加密技術，正好可以應用在這些隱私資料的儲存上。近年來，已經有許多相關研究[100]，在探討全同態加密技術，應用於醫療資料倉儲的可能性。
2. 資料分析：近年由於人工智慧領域快速的發展，使得資料分析技術備受重視。然而，有些個人或企業的資料，往往有資料量不夠龐大，難以使用神經網路預測的問題。這時，合併多方的資料一起進行預測，即是一個好的解決方案。當然，多方合併資料，必定會產生如何保護個人隱私的疑問，而全同態加密，就是解決此問題的最佳手段之一。如，Microsoft 團隊即曾利用全同態加密技術，開發了可以實現隱私資料保護的神經網路模型：CryptoNets[101]。

[100] 謝承翰、范俊逸，〈具隱私保護暨安全資料探勘之醫療資料倉儲系統〉，T&D 飛訊，第 294 期，國家文官學院，2022 年 9 月 1 日。

[101] R. Gilad-Bachrach, N. Dowlin, K. Laine, K. Lauter, M. Naehrig, and J. Wernsing, “Cryptonets: Applying neural networks to encrypted data with high throughput and accuracy,” in International conference on machine learning,

## 五、 模擬案例四：具隱私保護之平均薪資計算

### （一） 情境說明

本案例是參考波士頓女性勞動力委員會（Boston Women’s Workforce Council）於 2015 年、2016 年、2017 年、2019 年及 2021 年實際運用安全多方運算（SMPC）[102]，調查波士頓約六分之一受薪員工的薪資資訊，以評估性別薪資差距，據以討論和使用基於證據的方法來縮小其差距，並隨著時間的推移衡量所取得的進展。

性別薪資差異是指在相同職位或相似工作中，因性別而導致的薪資差異。這種現象在許多國家和不同行業中普遍存在，但具體的差異程度會因地區、行業、教育水平、職位等因素而有所不同。

考量以下因素，薪資調查之機制應導入隱私強化技術，以保障員工及雇主之權益，並增進參與調查的意願：

1. 隱私保護:薪資屬個人隱私，洩漏薪資恐侵犯員工的隱私，甚至導致部分員工遭受外界的不必要干涉和評判。
2. 社會比較和尷尬：個人薪資洩漏可能會引起同事之間的比較和不必要的競爭或摩擦。
3. 複雜度和多樣性：組織內部的薪資結構往往非常複雜，涉及到不同職位、工作經驗、技能水平等因素，因此僅部分員工之薪資往往無法正確反映該組織實際的薪資策略。
4. 職業保密性：部分職位可能需要保守秘密，洩漏這些職位的薪資恐對企業的運作造成不利影響。

因此本案例規劃運用安全多方運算的技術，以實現性別平均薪資之調查，同時兼顧參與者之隱私保障。

[102] D. Buckley, “1. Boston Women’s Workforce Council,” UN Statistics Wiki, Aug. 2023. https://unstats.un.org/wiki/pages/viewpage.action?pageId=150012020 (accessed Sep. 03, 2023).

（二） 情境使用資料說明

本案例採隨機生成模擬薪資資料，資料欄位說明如下：

**1.** 性別：記錄員工之性別，有男、女、其他三種。

**2.** 薪資（新臺幣/月）：該員工每月之薪資，以新臺幣（元）為單位。

▼表二十七、模擬案例四使用之資料集部分節錄

| 編號 | 性別 | 薪資（新臺幣/月） |
|---|---|---|
| 1 | 男 | 1123701 |
| 2 | 女 | 31090 |
| 3 | 其他 | 70221 |

（三） 使用之隱私強化技術

安全多方運算：秘密分享

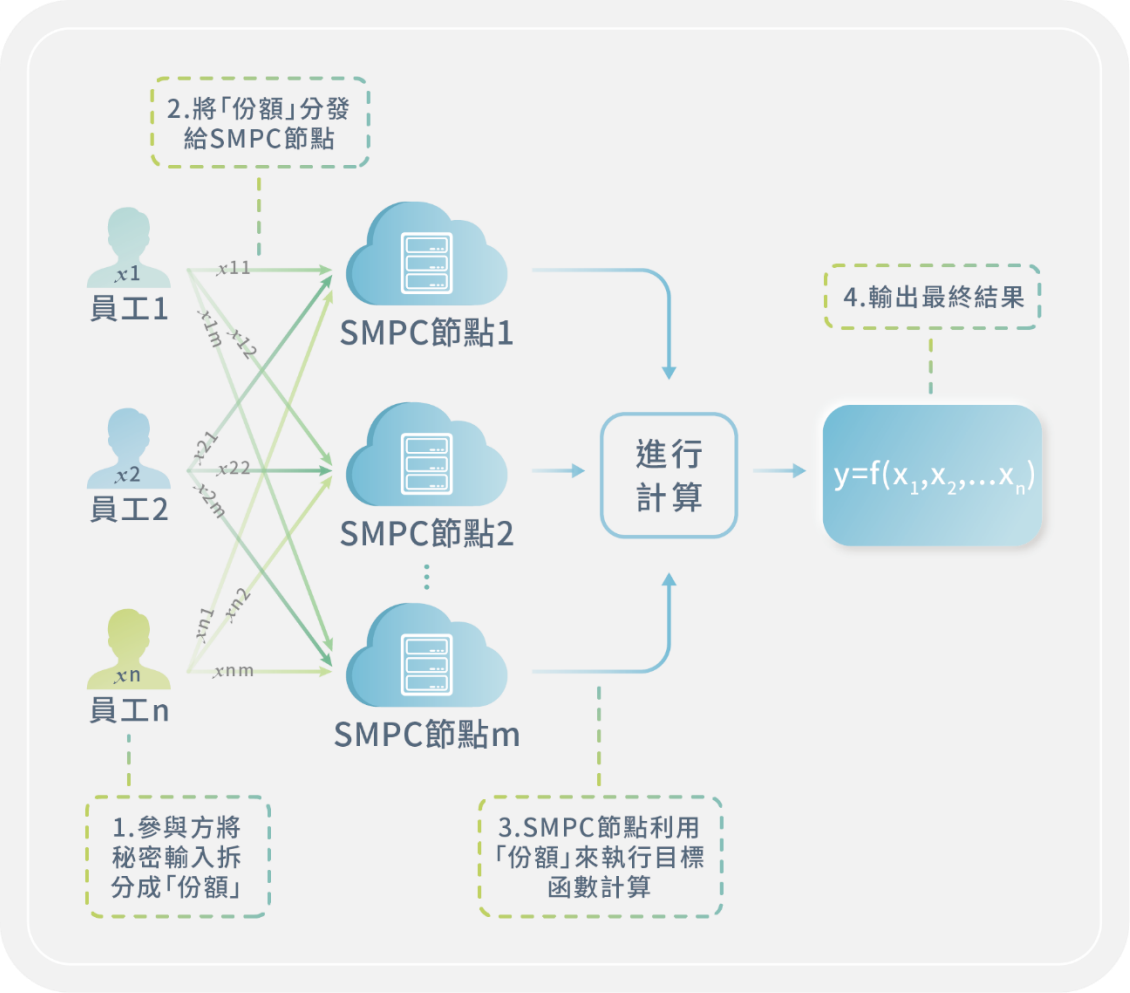
（四） 隱私強化技術使用目的

藉由安全多方運算來實現於保障參與薪資調查之員工薪資待遇隱私前提下，能夠同時計算出員工的平均薪資。

（五） 隱私強化技術運作方式/機制說明

安全多方運算的基礎運作方式是各個參與薪資調查的員工（參與方）先將自身實際薪資（秘密輸入）處理成無法被破解的形式，藉此保護實際的薪資輸入。而後交由部署好的 SMPC 節點進行運算再彼此交互計算出共同運算的目標。詳細流程如下圖[103]所示：

[103] G. Tsaloli, G. Banegas,and A. Mitrokotsa, “Practical and Provably Secure Distributed Aggregation: Verifiable Additive Homomorphic Secret Sharing”, Cryptography, vol.4, no.3, pp. 25, Sep. 2020, doi: 10.3390/cryptography4030025.




▲圖二十五、安全多方運算擬真情境運作架構

在此案例中，藉由秘密分享的技術來讓員工把自身薪資轉化成數份「份額」，這將使得各個 SMPC 節點無法獨力破解出特定員工的薪資；等收集完所有員工的薪資「份額」後，各個 SMPC 節點就可以開始進行安全多方運算，最終計算出各性別的平均薪資。

（六） 適用此隱私強化技術之其他領域

安全多方運算能夠適用於許多領域，凡是欲保持輸入資料的隱私，以求得問題輸出之情境，皆適用安全多方運算，常見如：電子投票[104][105]、數位簽章的閾值簽名方案（Threshold Signature Schemes）[106]、封閉式拍賣等

104 M. Rivinius, “Accountable secure multi-party computation for tally-hiding e-voting”, University of Stuttgart, 2020.
105 D. G. Nair, V. P. Binu, G. S. Kumar, “An Improved E-voting scheme using Secret Sharing based Secure Multi-party Computation”, Eighth International Conference on Computer communication networks. Feb 26, 2015.
106 Jean-Philippe Aumasson, Adrian Hamelink, and Omer Shlomovits, “A Survey of ECDSA Threshold Signing”, Cryptology ePrint Archive, Nov. 2020. Available: https://eprint.iacr.org/2020/1390.pdf Accessed: Aug 31, 2023.

# 伍、 相關文獻


1. A. Bellos, “Can a new form of cryptography s olve the internet’s privacy problem?” The Obse rver, Oct. 29, 2022. Accessed: Sep. 03, 2023. [Online]. Available: https://www.theguardian.com /technology/2022/oct/29/privacy-problem-tech-enh ancing-data-political-legal
2. O. A. Fdal, “What Are Privacy-Enhancing Tec hnologies (PETs) And How You Can Choose t he Right One(s) - CPO Magazine,” CPO Maga zine, Jul. 01, 2022. Accessed: Sep. 03, 2023. [Online]. Available: https://www.cpomagazine.co m/data-privacy/what-are-privacy-enhancing-techno logies-pets-and-how-you-can-choose-the-right-one s/
3. L. Qin et al., “From usability to secure compu ting and back again,” in Fifteenth symposium on usable privacy and security (SOUPS 2019), Santa Clara, CA, Aug. 2019, pp. 191–210. [On line] Available: https://www.usenix.org/conferenc e/soups2019/presentation/qin
4. A. Bestavros, M. Varia, and R. Canetti, “Acces sible and Scalable Secure Multi-Party Computat ion.” https://multiparty.org/ (accessed Sep. 03, 2 023).
5. Apple Inc., “Apple previews iOS 10, the bigge st iOS release ever.” Accessed: Aug. 31, 2023. [Online] Available: https://www.apple.com/news room/2016/06/apple-previews-ios-10-biggest-ios-r elease-ever/
6. E. Barker and A. Roginsky, “Transitioning the use of cryptographic algorithms and key length s,” National Institute of Standards and Technol ogy, NIST SP 800-131Ar2, Mar. 2019. Doi: htt ps://doi.org/10.6028/NIST.SP.800-131Ar2.
7. J. Benaloh, “Dense probabilistic encryption,” in Proceedings of the workshop on selected area s of cryptography, 1994, pp. 120–128. [Online] Available: https://sacworkshop.org/proc/SAC_94 _006.pdf
8. D. Boneh, E.-J. Goh, and K. Nissim, “Evaluati ng 2-DNF formulas on ciphertexts,” in Theory of cryptography: Second theory of cryptography conference, cambridge, MA, USA, february 10 -12, 2005, pp. 325–341. [Online] Available: htt ps://crypto.stanford.edu/~dabo/papers/2dnf.pdf
9. D. Buckley, “1. Boston Women’s Workforce C ouncil,” UN Statistics Wiki, Aug. 2023. https:// unstats.un.org/wiki/pages/viewpage.action?pageId =150012020 (accessed Sep. 03, 2023).
10. Information Technology Laboratory Computer S ecurity Division, “Cryptographic Algorithm Vali dation Program (CAVP),” Mar. 2023. https://csr c.nist.gov/projects/cryptographic-algorithm-validat ion-program
11. Information Technology Laboratory Computer S ecurity Division, “Cryptographic Module Valida tion Program (CMVP),” Aug. 2023. https://csrc. nist.gov/projects/cryptographic-module-validation- program
12. J. Fan and F. Vercauteren, “Somewhat practical fully homomorphic encryption.” 2012. [Online] Available: https://eprint.iacr.org/2012/144
13. B. Ding, J. (Jana) Kulkarni, and S. Yekhanin, “Collecting Telemetry Data Privately,” presented at the Advances in Neural Information Proces sing Systems 30, Long Beach, CA, USA, Dec. 2017. Available: https://www.microsoft.com/en-u s/research/publication/collecting-telemetry-data-pri vately/
14. C. Dwork, F. McSherry, K. Nissim, and A. S mith, “Calibrating noise to sensitivity in private data analysis,” in Theory of cryptography: Thi rd theory of cryptography conference, new yor k, NY, USA: Springer, Mar. 2006, pp. 265–28 4. [Online] Available: https://people.csail.mit.edu /asmith/PS/sensitivity-tcc-final.pdf
15. T. ElGamal, “A public key cryptosystem and a signature scheme based on discrete logarithms,” IEEE transactions on information theory, vol. 31, no. 4, pp. 469–472, 1985.
16. 個人資料保護法. 2013.
17. Google LLC, “Device administration overview,” Android Developers. https://developer.android.c om/guide/topics/admin/device-admin (accessed S ep. 01, 2023).
18. C. Holguera, S. Schleier, B. Mueller, and J. W illemsen, “OWASP Mobile Application Security Testing Guide.” Sep. 2022. Accessed: Sep. 01, 2023. [Online] Available: https://github.com/O WASP/owasp-mastg/
19. hung, “Threshold Signature Scheme (ECDSA) 介紹,” Taipei Ethereum Meetup, Jan. 07, 20 23. https://medium.com/taipei-ethereum-meetup/t hreshold-signature-scheme-ecdsa-介紹-e17923e64 d0 (accessed Aug. 31, 2023).
20. 教育部, 「公立高級中等以下學校資通安全防護計畫」. [線上]. 載於： https://cloudschool.ch c.edu.tw/open-message/074606/get-file/600779a72 1bcff7d38543439
21. 經濟部標準檢驗局, 「資訊技術－安全技術－個人資訊去識別化過程管理系統－要求事項」. 2019 年 9 月 24 日.
22. 經濟部工業局, 「行動應用 App 基本資安規範」. 2015 年 4 月 20 日.
23. A. Machanavajjhala, D. Kifer, J. Abowd, J. Ge hrke, and L. Vilhuber, “Privacy: Theory meets practice on the map,” in 2008 IEEE 24th inter national conference on data engineering, IEEE, 2008, pp. 277–286. [Online] Available: https://i eeexplore.ieee.org/abstract/document/4497436
24. S. Meier, “Advancing automated security protoc ol verification,” Ph.D, ETH Zurich, 2013.
25. mpc-alliance, “Multiparty computation (MPC) wiki,” Aug. 20, 2023. https://wiki.mpcalliance.o rg/ (accessed Aug. 31, 2023).
26. M. Hastings, B. Hemenway, D. Noble, and S. Zdancewic, “SoK: General-purpose compilers fo r secure multi-party computation,” in 2019 IEE E symposium on security and privacy (SP), 20 19.
27. National Institute of Standards and Technology,

"Security requirements for cryptographic modules," National Institute of Standards and Technology, Gaithersburg, MD, NIST FIPS 140-2, May 2001. Doi: 10.6028/NIST.FIPS.140-2.
28. M. Ogata, J. Franklin, J. Voas, V. Sritapan, and S. Quirolgico, "Vetting the security of mobile applications," National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-163r1, Apr. 2019. Accessed: Sep. 01, 2023. [Online] Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-163r1.pdf
29. P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in International conference on the theory and applications of cryptographic techniques, Springer, 1999, pp. 223–238. [Online] Available: https://link.springer.com/content/pdf/10.1007/3-540-48910-X_16.pdf
30. The Centre for Data Ethics and Innovation's (CDEI), "Privacy Enhancing Technologies Adoption Guide," PETs Adoption Guide. https://cdeiuk.github.io/pets-adoption-guide/ (accessed Sep. 01, 2023).
31. Information Commissioner's Office, "Privacy-enhancing technologies (PETs)." Jun. 2023. [Online] Available: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies/
32. The Royal Society, "From privacy to partnership," Jan. 2023. [Online] Available: https://royalsociety.org/topics-policy/projects/privacy-enhancing-technologies/
33. 達文西個資暨高科技法律事務所, 「『強化數位隱私保障所涉個人資料保護法 相關議題研析』委託研究計畫結案報告」, 國家發展委員會, 10月 2021. [線上]. 載於： https://ws.ndc.gov.tw/Download.ashx?u=LzAwMS9hZG1pbmlzdHJhdG9yLzEwL3JlbGZpbGUvNTc0NC8zNTQ5Ny9hYzEwMjg5MC0yYzc1LTRiZDItYjBkNC1lMzM1NzliMDE4MzgucGRm&n=5ZyL5a6255m85bGV5aeU5ZOh5pyDXzExMOW5tOW6pl%2FjgIzlvLfljJbmlbjkvY3pmrHnp4Hkv53pmpzmiYDmtonlgIvkuros4fmlpnkv53orbfms5Xnm7jpl5zorbDpoYznoJTmnpDjgI3lp5ToqJfnoJTnqbboqIjnlatf57WQ5qGI5aCx5ZGKLnBkZg%3D%3D&icon=.pdf
34. R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, vol. 21, no. 2, Art. no. 2, 1978.
35. R. Rogers et al., "LinkedIn's Audience Engagements API: A privacy preserving data analytics system at scale," 2020, [Online] Available: https://arxiv.org/abs/2002.05839
36. K. A. Scarfone, M. P. Souppaya, A. Cody, and A. D. Orebaugh, "Technical guide to information security testing and assessment.," National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-115, 2008. Doi: 10.6028/NIST.SP.800-115.
37. P. Thaine, "Privacy Enhancing Technologies Decision Tree." PRIVATE AI, Oct. 18, 2020. [Online] Available: https://www.private-ai.com/wp-content/uploads/2021/10/PETs-Decision-Tree.pdf
38. The MITRE Corporation, "Common Vulnerabilities and Exposures (CVE)," Aug. 14, 2023. https://cve.mitre.org/ (accessed Sep. 01, 2023).
39. The MITRE Corporation, "Common Weakness Enumeration (CWE)," Aug. 22, 2023. https://cwe.mitre.org/ (accessed Sep. 01, 2023).
40. The OpenDP Team, "OpenDP Library." Sep. 01, 2023. Accessed: Sep. 03, 2023. [Online] Available: https://github.com/opendp/opendp
41. The Working Party on the Protection of Individuals with regard to the Processing of Personal Data, "Opinion 05/2014 on Anonymisation Techniques." Apr. 10, 2014. [Online] Available: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf
42. Tumult Labs, "Tumult Labs | Privacy Protection Redefined." https://www.tmlt.io/
43. United Nations Committee of Experts on Big Data and Data Science for Official Statistics, "United Nations Guide on Privacy-Enhancing Technologies for Official Statistics." 2023. [Online] Available: https://unstats.un.org/bigdata/task-teams/privacy/guide/2023_UN PET Guide.pdf
44. Privitar Ltd, "Enterprise Data Privacy Management Software & Tools," Privitar. https://www.privitar.com/products/data-privacy-software/ (accessed Aug. 31, 2023).
45. A. Yanai, "Private Set Intersection," Mar. 29, 2020. https://decentralizedthoughts.github.io/2020-03-29-private-set-intersection-a-soft-introduction/ (accessed Aug. 31, 2023).
46. Trans. Intell. Syst. Technol., vol. 10, no. 2, p. 12:1-12:19, Jan. 2019, Doi: 10.1145/3298981.
47. I. Damgård, K. Damgård, K. Nielsen, P. S. Nordholt, and T. Toft, "Confidential benchmarking based on multiparty computation." 2015. [Online]. Available: https://eprint.iacr.org/2015/1006
48. A. C. Yao, "Protocols for secure computations," in 23rd Annual Symposium on Foundations of Computer Science (sfcs 1982), Nov. 1982, pp. 160–164. Doi: 10.1109/SFCS.1982.38.
49. T. Chou and C. Orlandi, "The simplest protocol for oblivious transfer." 2015. [Online]. Available: https://eprint.iacr.org/2015/267