(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 201448551 A
(43)公開日： 中華民國 103 (2014) 年 12 月 16 日

(21)申請案號：103107292 (22)申請日： 中華民國 103 (2014) 年 03 月 04 日
(51)Int. Cl.： *H04L9/00 (2006.01)*
(30)優先權：2013/03/04 美國 61/772,404
(71)申請人：湯普生證照公司 (法國) THOMSON LICENSING (FR)
法國
(72)發明人：尼卡蘭可 維利瑞亞 NIKOLAENKO, VALERIA (US)；溫斯伯格 艾胡德 WEINSBERG, EHUD (IL)；伊歐納迪斯 伊弗斯崔提歐 IOANNIDIS, EFSTRATIOS (GR)；喬伊 馬克 JOYE, MARC (BE)；塔夫特 尼納 安 TAFT, NINA ANNE (US)
(74)代理人：陳長文
申請實體審查：無 申請專利範圍項數：15 項 圖式數：7 共 34 頁

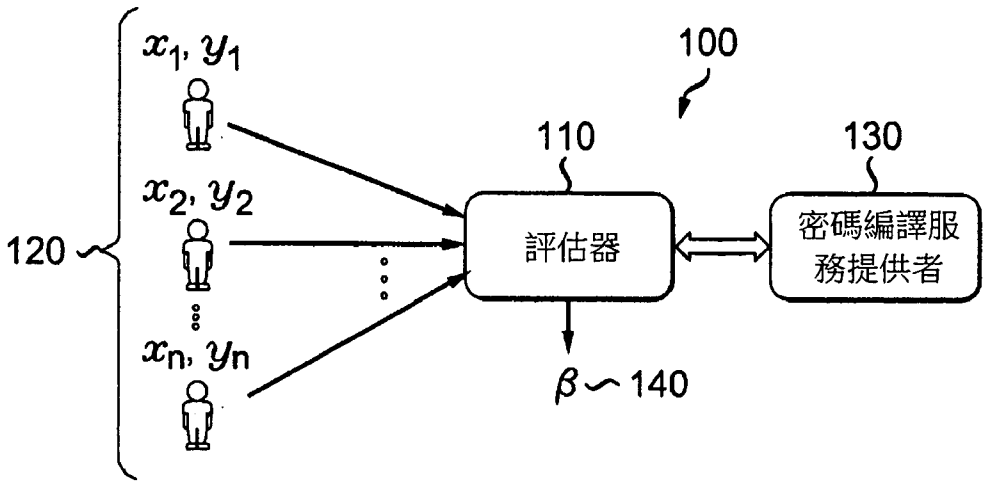
(54)名稱

使用部份同態之加密及遮罩之隱私保護脊狀回歸

PRIVACY-PRESERVING RIDGE REGRESSION USING PARTIALLY HOMOMORPHIC ENCRYPTION AND MASKS

(57)摘要

本發明提供一種用於使用部分同態加密及遮罩之隱私保護脊狀回歸之方法及系統。該方法包含以下各項步驟：向一密碼編譯服務提供者請求一混淆電路；自多個使用者收集已使用部分同態加密格式化並加密之資料；匯合已使用部分同態加密格式化並加密之該資料；將一所準備之遮罩應用於該所匯合資料；使用模糊傳送自該密碼編譯服務提供者接收對應於所準備之遮罩之混淆輸入；及使用該等混淆輸入及經遮罩資料來評估來自該密碼編譯服務提供者之該混淆電路。



100：系統
110：評估器
120：使用者
130：密碼編譯服務提供者
140：純文字預測模型β/學習模型β/模型β

圖 1

(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 201448551 A
(43)公開日： 中華民國 103 (2014) 年 12 月 16 日

(21)申請案號：103107292 (22)申請日： 中華民國 103 (2014) 年 03 月 04 日
(51)Int. Cl.： *H04L9/00 (2006.01)*
(30)優先權：2013/03/04 美國 61/772,404
(71)申請人：湯普生證照公司 (法國) THOMSON LICENSING (FR)
法國
(72)發明人：尼卡蘭可 維利瑞亞 NIKOLAENKO, VALERIA (US)；溫斯伯格 艾胡德 WEINSBERG, EHUD (IL)；伊歐納迪斯 伊弗斯崔提歐 IOANNIDIS, EFSTRATIOS (GR)；喬伊 馬克 JOYE, MARC (BE)；塔夫特 尼納 安 TAFT, NINA ANNE (US)
(74)代理人：陳長文
申請實體審查：無 申請專利範圍項數：15 項 圖式數：7 共 34 頁

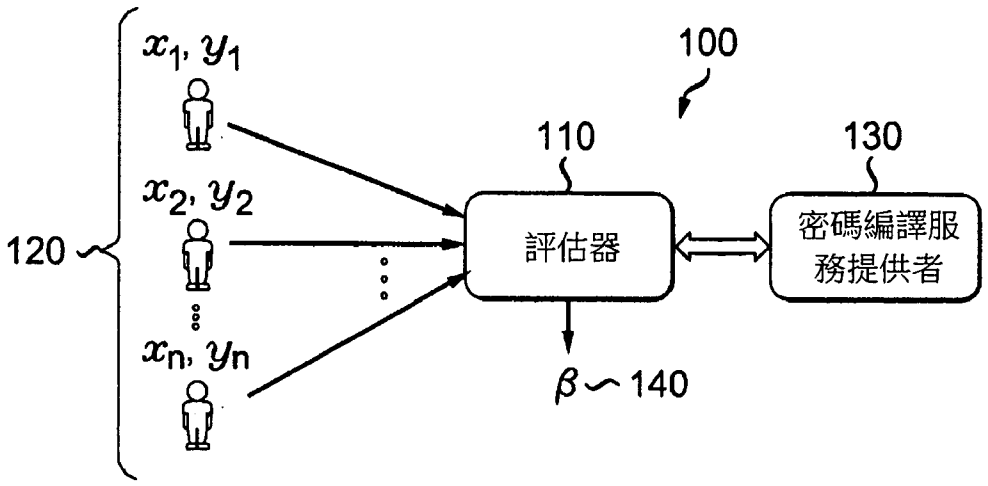
(54)名稱

使用部份同態之加密及遮罩之隱私保護脊狀回歸

PRIVACY-PRESERVING RIDGE REGRESSION USING PARTIALLY HOMOMORPHIC ENCRYPTION AND MASKS

(57)摘要

本發明提供一種用於使用部分同態加密及遮罩之隱私保護脊狀回歸之方法及系統。該方法包含以下各項步驟：向一密碼編譯服務提供者請求一混淆電路；自多個使用者收集已使用部分同態加密格式化並加密之資料；匯合已使用部分同態加密格式化並加密之該資料；將一所準備之遮罩應用於該所匯合資料；使用模糊傳送自該密碼編譯服務提供者接收對應於所準備之遮罩之混淆輸入；及使用該等混淆輸入及經遮罩資料來評估來自該密碼編譯服務提供者之該混淆電路。



100：系統
110：評估器
120：使用者
130：密碼編譯服務提供者
140：純文字預測模型β/學習模型β/模型β

圖 1

201448551

發明摘要

※ 申請案號：103107292

※ 申請日：103.3.4　　※IPC 分類：H04L 9/00 (2006.01)

【發明名稱】

使用部份同態之加密及遮罩之隱私保護脊狀回歸

PRIVACY-PRESERVING RIDGE REGRESSION USING PARTIALLY HOMOMORPHIC ENCRYPTION AND MASKS

【中文】

本發明提供一種用於使用部分同態加密及遮罩之隱私保護脊狀回歸之方法及系統。該方法包含以下各項步驟：向一密碼編譯服務提供者請求一混淆電路；自多個使用者收集已使用部分同態加密格式化並加密之資料；匯合已使用部分同態加密格式化並加密之該資料；將一所準備之遮罩應用於該所匯合資料；使用模糊傳送自該密碼編譯服務提供者接收對應於所準備之遮罩之混淆輸入；及使用該等混淆輸入及經遮罩資料來評估來自該密碼編譯服務提供者之該混淆電路。

【英文】

A method and system for privacy-preserving ridge regression using partially homomorphic encryption and masks is provided. The method includes the steps of requesting a garbled circuit from a crypto service provider, collecting data from multiple users that has been formatted and encrypted using partially homomorphic encryption, summing the data that has been formatted and encrypted using partially homomorphic encryption, applying a prepared masks to the summed data, receiving garbled inputs corresponding to prepared mask from the crypto service provider using oblivious transfer, and evaluating the garbled circuit from the crypto service provider using the garbled inputs and masked data.

【代表圖】

【本案指定代表圖】：第（1）圖。

【本代表圖之符號簡單說明】：

100　系統

110　評估器

120　使用者

130　密碼編譯服務提供者

140　純文字預測模型β/學習模型β/模型β

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：

無

發明專利說明書

（本說明書格式、順序，請勿任意更動）

【發明名稱】

使用部份同態之加密及遮罩之隱私保護脊狀回歸

PRIVACY-PRESERVING RIDGE REGRESSION USING PARTIALLY HOMOMORPHIC ENCRYPTION AND MASKS

相關申請案參考

本申請案主張於2013年3月4日提出申請之美國臨時申請案第61/772,404號之權益，該美國臨時申請案以全文引用之方式併入本文中。

本申請案亦與標題為「PRIVACY-PRESERVING RIDGE REGRESSION」及「PRIVACY-PRESERVING RIDGE REGRESSION USING MASKS」之申請案相關，該等申請案已同時提出申請且以全文引用之方式併入本文中。

【技術領域】

本發明大體而言係關於資料探勘且更特定而言係關於使用脊狀回歸來在資料探勘期間維護隱私。

【先前技術】

推薦系統藉由收集諸多使用者對不同項目之偏好及評級且對資料運行一學習演算法來操作。該學習演算法產生可用於預測一新使用者將如何評級特定項目之一模型。特定而言，已知一使用者對特定項目提供之評級，模型可預測彼使用者將如何評級其他項目。存在用於產生此預測模組之一龐大演算法陣列，且諸多演算法在如同Amazon及Netflix之大型網站處主動使用。學習演算法亦用於大型醫療資料庫、金融資料及諸多其他領域。

在目前實施方案中，學習演算法必須查看所有未加密之使用者資料以便建立預測模型。在本發明中，判定學習演算法是否可在無未加密之資料之情況下進行運算，藉此允許使用者保持對其資料之控制。針對醫療資料，此允許在不影響使用者隱私之情況下建立一模型。針對書籍及電源偏好，讓使用者保持對其資料之控制減少在服務提供者處之一資料缺口之情形中之未來不期望阻礙之風險。大致而言，存在用以資料探勘私用使用者資料之三種現有方法。第一種方法讓使用者使用秘密共用將其資料分割在多個伺服器當中。此等伺服器然後使用一分散式協定運行學習演算法且只要伺服器之大部分不串通即確保隱私。第二種方法係基於完全同態加密，其中對經加密資料執行學習演算法且一受信任第三方經委託以僅解密最終經加密模型。在一第三方法中，Yao之混淆電路構造可用於對經加密資料進行計算且在不學習關於使用者資料之任何其他資料之情況下獲得一最終模型。然而，基於Yao之一方法之前從未應用於回歸級演算法。

【發明內容】

本發明呈現一種使用同態加密及Yao混淆電路兩者之用以隱私保護之脊狀回歸之混合方法。系統中之使用者提交其依據諸如Paillier或Regev之一線性同態加密系統加密之資料。評估器使用線性同態來實施僅需要線性運算之演算法之第一階段。此階段產生經加密資料。在此第一階段中，要求系統處理大量記錄(與系統中之使用者之數目n成比例)此第一階段中之處理準備資料以使得演算法之第二階段與n無關。在一第二階段中，評估器評估一Yao混淆電路，該Yao混淆電路首先實施同態解密且然後進行回歸演算法之剩餘部分(如所示，一最佳化實現可避免混淆電路中之解密)。回歸演算法之此步驟需要一快速線性系統求解器且係高度非線性。針對此步驟，一Yao混淆電路方法比目前完全同態加密方案快得多。因此，藉由使用線性同態來處置

一大資料集且將混淆電路用於計算之大量非線性部分來獲得兩個領域之最佳。由於計算經分割成兩個階段之方式，因此第二階段亦與n無關。

在一項實施例中，提供用於隱私保護之脊狀回歸之方法。該方法包含以下各項步驟：向一密碼編譯服務提供者請求一混淆電路；自多個使用者收集已使用部分同態加密格式化並加密之資料；匯合已使用部分同態加密格式化並加密之該資料；將一所準備之遮罩應用於該所匯合資料；使用模糊傳送自該密碼編譯服務提供者接收對應於所準備之遮罩之混淆輸入；及使用該等混淆輸入及經遮罩資料來評估來自該密碼編譯服務提供者之該混淆電路。

在另一實施例中，提供用於隱私保護之脊狀回歸之計算裝置。該計算裝置包含儲存器件、記憶體及一處理器。該儲存器件用於儲存使用者資料。該記憶體用於儲存用於處理之資料。該處理器經組態以：向一密碼編譯服務提供者請求一混淆電路；自多個使用者收集已使用同態加密格式化並加密之資料；匯合已使用同態加密格式化並加密之該資料；將一所準備之遮罩應用於該所匯合資料；使用模糊傳送自該密碼編譯服務提供者接收對應於所準備之遮罩之混淆輸入；及使用該等混淆輸入及經遮罩資料來評估來自該密碼編譯服務提供者之該混淆電路。

目的及優點將藉助於申請專利範圍中特定指出之元件及耦合件實現及獲得。重要地，注意所揭示之實施例僅係本文中之創新教示內容之諸多有利用途之實例。應理解，前述一般說明及以下詳細說明兩者皆為實例性及解釋性的且並不限制如所主張之本發明。此外，某些陳述可適用於某些發明性特徵而不適用於其他特徵。一般而言，除非另有指示，否則在不失一般性之情形下，單數個元素可呈複數形式且反之亦然。在圖式中，在所有數個視圖中相似編號係指相似部件。

【圖式簡單說明】

圖1繪示根據一實施例之一隱私保護之脊狀回歸系統之一區塊示意圖。

圖2繪示根據一實施例之一計算裝置之一區塊示意圖。

圖3繪示根據一實施例之一例示性混淆電路。

圖4繪示根據實施例之用於提供一隱私保護之脊狀回歸之一方法之一高階流程圖。

圖5繪示根據實施例之用於提供隱私保護之脊狀回歸之一第一協定之操作。

圖6繪示根據實施例之用於提供隱私保護之脊狀回歸之一第一協定之操作。

圖7繪示根據實施例之用於喬裏斯基(Cholesky)分解之一演算法之一例示性實施例。

【實施方式】

本發明之重點係關於諸多學習演算法中所使用之一基本機制，即，脊狀回歸。已知處於高維度中之大量點，回歸演算法透過此等點產生一最佳擬合曲線。目標係在不曝露使用者資料或關於使用者資料之任何其他資訊之情況下執行計算。此係藉由使用如圖1中所示之一系統達成：

在圖1中，提供用於實施隱私保護之脊狀回歸之一系統100之一實施例之一方塊圖。系統包含彼此通信之一評估器110，一或多個使用者120及密碼編譯服務提供者(CSP) 130。評估器110實施於諸如一伺服器或個人電腦(PC)之一計算裝置上。CSP 130係類似地實施於諸如一伺服器或個人電腦之計算裝置上且經由網路(諸如乙太網路或Wi-Fi網路)與評估器110通信。一或多個使用者120經由諸如個人電腦、平板電腦、智慧型電話或諸如此類之計算裝置與評估器110及CSP 130

通信。

使用者120將經加密資料(舉例而言，來自一PC)發送至運行學習演算法之評估器110 (舉例而言，在一伺服器上)。在特定時刻，評估器可與被信任不與評估器110串通之一密碼編譯服務提供者130 (在另一伺服器上)互動。最終結果係純文字預測模型β 140。

圖2繪示可用於實施用於隱私維護之脊狀回歸之各種方法及系統元件之諸如一伺服器、PC、平板電腦或智慧型電話之一例示性計算裝置200。計算裝置200包含一或多個處理器210、記憶體220、儲存器件230及一網路介面240。下文將更詳細論述此等元件中之每一者。

處理器210控制電子伺服器200之操作。處理器200運行操作伺服器以及提供冷啟動推薦之功能性之軟體。處理器210連接至記憶體220、儲存器件230及網路介面240，且處置此等元件之間的資訊之傳送及處理。處理器210可係一般處理器或專用於一特定功能性之一處理器。在某些實施例中，可存在多個處理器。

記憶體220其中儲存由處理器執行之指令及資料。記憶體210可包含揮發性記憶體(RAM)、非揮發性記憶體(EEPROM)或其他適合媒體。

儲存器件230其中儲存處理器在執行本發明之冷儲存推薦方法中所使用及產生之資料。儲存器件可係磁性媒體(硬碟機)、光學媒體(CD/DVD-Rom)或基於快閃之儲存器件。

網路介面240處置伺服器200與其他裝置經由一網路之通信。一適合網路之一實例係一乙太網路。已知本發明之益處，熟習此項技術者將明瞭其他類型之適合家用網路。

應理解，圖2中所闡明之元件係說明性。伺服器200可包含任何數目個元件且某些元件可提供其他元件之功能之部分或全部。已知本發明之益處，熟習此項技術者將明瞭其他可能實施方案。

設定及威脅模型

A. 架構及實體

返回參考圖1，系統100經設計用於諸多使用者120以將資料貢獻至稱為評估器110之一中央伺服器。評估器110對所貢獻資料執行回歸且產生一模型β 140，該模型稍後可用於預測或推薦任務。更具體而言，每一使用者$i = 1;:::;n$具有包括兩個變數$x_i \in \mathbb{R}^d$及$y_i \in \mathbb{R}$之一私用記錄，且評估器希望計算$\beta \in \mathbb{R}^d$—模型—以使得$y_i \simeq \beta^T x_i$。目標係確保評估器不學習除由β 140揭示之資料(回歸演算法之最終結果)外之關於使用者之記錄之任何資料。為初始化系統，需要離線進行其工作之大部分之一第三方(其在本文中稱為一「密碼編譯服務提供者」)。

更精確而言，系統中之該等各方係如下，如圖1中所示。

●使用者120：每一使用者i使其發送之私用資料x_i, y_i經加密至評估器110。

●評估器110：對經加密資料運行一回歸演算法且獲得未加密之學習模型β 140。

●密碼編譯服務提供者(CSP) 130：藉由賦予設定參數至使用者120及評估器110來初始化系統100。

CSP 130遠在使用者120將其資料貢獻至評估器110之前離線進行其工作之大部分。在最高效設計中，在評估器110計算模型β 140時一短單回合線上步驟亦需要CSP 130

B. 威脅模型

目標係確保評估器110及CSP 130無法學習除由學習演算法之最終結果揭示之資料外之關於由使用者120貢獻之資料之任何資料。在評估器110與使用者120中之某些使用者串通之情形中，使用者120不應學習除由學習演算法之結果揭示之資料外之關於由其他使用者120

貢獻之資料之任何資料。

在此實例中，假定產生一正確模型β 140係評估器110之最佳利益。因此，此實施例並不與試圖損毀計算以希望產生一不正確結果之一惡意評估器110相關。然而，評估器110經誘導而行為不端且學習關於由使用者120貢獻之私用資料之資訊，此乃因此資料可能被出售給其他方(例如，廣告客戶)。因此，甚至一惡意評估器110應不能夠學習除由學習演算法之結果揭示之資料以外之關於使用者資料之任何資料。本文中闡明僅沒有一誠實但好奇評估器之危險之基本協定。

無威脅：系統經設計以防禦以下攻擊：

●假定評估器110及CSP 130不串通。每一者可如上文所論述試圖破壞系統，但其獨立如此進行。更精確而言，在辯論安全性時，假定此兩個方中至多一者係惡意的(此係一固有要求，在無該固有要求之情況下無法達成安全性)。

●假定設定工作正確，亦即，所有使用者120自CSP 130獲得正確公用密鑰。此可實際上在適當使用憑證機構之情況下強制執行。

先前技術

A.*學習一線性模型*

簡要回顧脊狀回歸，評估器110在系統110中進行以學習β 140之演算法。下文所論述之所有結果係典型的，且可在大部分統計及機器學習教科書中找到。

線性回歸：已知一組n個輸入變數$x_i \in \mathbb{R}^d$，及一組輸出變數$y_i \in \mathbb{R}$，學習一函數$f: \mathbb{R}^d \to \mathbb{R}$以使得$y_i \simeq f(x_i)$之一問題稱為*回歸*。舉例而言，輸入變數可係一人類之年齡、體重、身體質量指數等，而輸出可係其感染一疾病之可能性。

自實際資料學習此一函數具有使回歸在資料探勘、統計及機器學習中遍存之諸多興趣應用。一方面，函數自身可用於預測，亦即，

預測一新輸入$x \in \mathbb{R}^d$之輸出值y。此外，f之結構可有助於識別輸入影響輸出之困難程度—確立例如體重而非年齡與一疾病更強烈相關。

*線性回歸*係基於*f*係由一線性映射充分近似化之前提，亦即，

$$y_i \approx \beta^T x_i, \qquad i \in [n] \equiv \{1, \ldots, n\}$$

針對某些$\beta \in \mathbb{R}^d$。線性回歸係用於科學中之推斷及統計分析之最廣泛使用之方法中之一者。另外，其係統計分析及機器學習中數個較高階方法(諸如核心方法)之一基本建立區塊。舉例而言，學習係一2次多項式之一函數減化成針對$1 \le k, k' \le d$對$x_{ik}x_{ik'}$之線性回歸；相同原理可一般化以學習由一有限組基本函數生成之任何函數。

如上文所提及，除其明顯用於預測外，向量$\beta = (\beta_k)_{k=1,\ldots,d}$在其解釋y依賴於輸入變數之程度時令人感興趣。特定而言，一係數β_k之正負號指示與輸出之正相關或負相關，而量值決定相對重要性。為確保此等係數係可比較，而且實現數值穩定性，係數x_i經重新調節至相同有效值域(例如，[-1; 1])。

計算係數：為計算向量$\beta \in \mathbb{R}^d$，該向量藉由使以下關於$\mathbb{R}^d$之二次函數最小化而擬合於資料：

$$F(\beta) = \sum_{i=1}^{n} (y_i - \beta^T x_i)^2 + \lambda \|\beta\|_2^2 \ . \qquad (1)$$

使(1)最小化之程序稱為脊狀回歸；目標函數F(β)併入有懲罰項$\lambda \| \beta \|_2^2$，該懲罰項有助於簡約解。直觀地，針對$\lambda = 0$，使(1)最小化對應於求解一簡單最小平方問題。針對正$\lambda > 0$，項$\lambda \| \beta \|_2^2$用高范數懲罰解：在同樣擬合資料之兩個解之間，具有較不大係數之解係較佳的。回想，β之係數係輸入影響輸出之程度之指標，此充當「奧坎簡化論」之一形式：具有較不大係數之較簡單解係較佳的。實際上，一λ>0比所基於之最小平方解對新輸入賦予實際上較佳預測。假設

$y \in \mathbb{R}^n$係輸出之向量且$x \in \mathbb{R}^{n \times d}$係包括輸入向量(每一列中之向量)之一矩陣，亦即，

$$y = (y_i)_{i=1,\ldots,n} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}$$

且

$$X = (x_i^T)_{i=1,\ldots,n} = \begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1d} \\ x_{21} & x_{22} & \cdots & x_{2d} \\ \vdots & \vdots & & \vdots \\ x_{n1} & x_{n2} & \cdots & x_{nd} \end{pmatrix} .$$

可藉由求解線性系統計算(1)之最小值：

$$A\beta = b \qquad (2)$$

其中$A = X^TX + \lambda I$且$b = X^Ty$。針對$\lambda > 0$，矩陣A係對稱正定的，且可如下文所概述使用喬裏斯基分解找到一高效解。

B. Yao之混淆電路

在其基本版本中，Yao之協定(亦稱為混淆電路)允許在存在半誠實敵人之情況下對一函數$f(x_1; x_2)$之雙方評估。協定在輸入擁有者之間運行(a_i表示使用者i之私用輸入)。在協定結束時，獲得$f(a_1; a_2)$之值但無任何一方學習比自此輸出值所揭示之資料多之資料。

協定如下進行。第一方(稱為混淆器)建立計算f之一電路之一「混淆」版本。混淆器然後賦予第二方(稱為評估器)混淆電路以及對應於a_1之混淆電路輸入值(且僅彼等者)。記號GI(a_1)用於表示此等輸入值。混淆器亦提供混淆電路輸出值與實際位元值之間的映射。在接

收電路時，評估器以一2選1模糊傳送協定與混淆器接合，起到選擇器之作用，以便模糊獲得對應於其私用輸入a_2之混淆電路輸入值GI(a_2)。自GI(a_1)及GI(a_2)，評估器可因此計算f(a_1; a_2)。

更詳細而言，協定評估透過如圖3中所見之一布林電路(Boolean circuit) 300評估函數f。混淆器使分別對應於位元值b_i = 0及b_i = 1之兩個隨機密碼編譯密鑰$K_{w_i}^0$及$K_{w_i}^1$與電路之每一線w_i *310*、*320*相關聯。接下來，針對具有輸入線(w_i,w_j)310、320及輸出線w_k 330之每一二進制閘g (例如，一「或」閘)，混淆器計算四個密文

$$\mathrm{Enc}_{(K_{w_i}^{b_i},K_{w_j}^{b_j})}(K_{w_k}^{g(b_i,b_j)}) \text{ 針對 } b_i,b_j \in \{0,1\} .$$

此等四個隨機排序密文之集定義混淆閘。

需要藉由一對密鑰予以密鑰控制之對稱加密演算法Enc在所選擇明文攻擊下具有難以辨別之加密。亦要求，已知密鑰對($K_{w_i}^{b_i}$, $K_{w_j}^{b_j}$)，對應解密程序自構成混淆閘之四個密文明確地復原$K_{w_k}^{g(b_i,b_j)}$之值。對($K_{w_i}^{b_i}$, $K_{w_j}^{b_j}$)之知曉僅產生$K_{w_k}^{g(b_i,b_j)}$之值，且針對此閘無法復原任何其他輸出值。因此評估器可逐閘評估整個混淆電路以使得不洩漏關於中間計算之任何額外資訊。

混合方法

回想，在此設定中，每一輸入及輸出變數x_i、y_i ($i \in [n]$)係私用的，且由一不同使用者保留。評估器110希望學習判定輸入變數與輸出變數之間的線性關係之β (如在一已知$\lambda > 0$之情況下透過脊狀回歸獲得)。

如上文中所闡述，為獲得β，需要矩陣$A \in \mathbb{R}^{d \times d}$及向量$b \in \mathbb{R}^d$，如方程式(2)中所定義。一旦獲得此等值，評估器110可求解方程式(2)之線性系統且提取β。存在以一隱私保護方式解決此問題之數種方式。舉例而言，一個方式可依賴於秘密共用或完全同態加密。目前，此等

技術似乎不適合於本設定，此乃因其導致顯著(線上)通信或計算附加項。因此，如上文中所概述，探究了Yao之方法。

使用Yao之方法之一個簡單方式係設計針對$i \in [n]$且$\lambda > 0$具有輸入x_i、y_i之一單個電路，該單個電路計算矩陣A及b且隨後求解系統$A\beta = b$。此一方法過去已用於對來自多個使用者(諸如一拍賣之得標者)之輸入之簡單函數之計算。撇開執行問題(諸如如何設計求解一線性系統之一電路)，此一解決方案之一主要缺點係所得混淆電路取決於使用者之數目n以及β與輸入變數之維度d兩者。在實際應用中，較常見地，n係較大的，且可係大約數百萬使用者。相比而言，d係相對較小，大約10s。因此較佳減少或甚至消除混淆電路對n之相依性，一般獲得一可擴縮解決方案。為此，問題如下文所論述重新格式化。

A.重新格式化問題

注意，矩陣A及向量b可如下以一迭代方式計算。假定每一x_i及對應y_i由不同使用者保留，且使用者i可本端計算矩陣$A_i = x_i x_i^T$及向量$b_i = y_i x_i$。然後容易驗證，對部分貢獻求和產生：

$$A = \sum_{i=1}^{n} A_i + \lambda I \quad \text{且} \quad b = \sum_{i=1}^{n} b_i \ . \qquad (3)$$

方程式(3)重要展示A及b係一系列加法之結果。評估器之回歸任務可因此分成兩個子任務：(a)收集A_i及b_i以構造矩陣A及向量b，及(b)使用此等來透過線性系統(2)之解來獲得β。

當然，使用者無法發送其本端共用$(A_i;\ b_i)$至未加密之評估器。然而，若評估器使用一公用密鑰加性同態加密方案來加密，則評估器110可自對$(A_i;\ b_i)$之加密重新構造對A及b之加密。剩餘挑戰係藉助於CSP 130求解方程式(2)，而不揭示(至評估器110或CSP 130)除β外之任何額外資訊；下文闡述透過使用Yao之混淆電路如此操作之兩個不同

方式。

更明確地，假設

$$\mathfrak{E}_{\mathsf{pk}} : (A_i; b_i) \in \mathcal{M} \mapsto \mathfrak{c}_i = \mathfrak{E}_{\mathsf{pk}}(A_i; b_i)$$

係藉由一公用密鑰*pk*索引之一語義安全加密方案，該方案在訊息空間$\mathcal{M}$中接受輸入(一對$(A_i;\ b_i)$)且在*pk*, $\mathfrak{c}_i$下返回對$(A_i;\ b_i)$之加密。然後，其必須適用於任何pk及任何兩個對 $(A_i;\ b_i)$、$(A_j;\ b_j)$。以使得

$$\mathfrak{E}_{\mathsf{pk}}(A_i; b_i) \otimes \mathfrak{E}_{\mathsf{pk}}(A_j; b_j) = \mathfrak{E}_{\mathsf{pk}}(A_i + A_j; b_i + b_j)$$

針對某些公用二進制運算子。此一加密方案可藉由按分量加密A_i及b_i之項目來由任何語義安全加性同態加密方案構造。實例包含Regev方案及Paillier方案。

現在準備呈現協定。圖4中提供一高階流程圖400。流程圖400包含一準備階段410、一第一階段(階段1) 420及一第二階段(階段2) 430。彙總使用者共用之階段稱為*階段1* 420，且注意其涉及之加法線性依賴於*n*。隨後階段(其相當於依據*A*及*b*之經加密值計算方程式(2)之解)稱為*階段2* 430。應注意，*階段2* 430與*n*不相關。下文將結合特定協定論述此等階段。注意，假定下文存在可求解系統$A\beta = b$之一電路；本文中論述可如何高效實施此一電路。

B. 第一協定

第一協定之操作之一高階繪示500可在圖5中看到。第一協定如下操作。如上文所闡明，第一協定包括三個階段：一準備階段510、階段1 520及階段2 530。如將瞭解，僅階段2 530實際需要一線上處理。

準備階段(510)。評估器110提供規格至CSP 130，諸如輸入變數之維度(亦即，參數*d*)及其值範圍。CSP 130準備用於階段2 530中所闡述之電路之一Yao混淆電路且使混淆電路可用於評估器110。CSP 130

亦產生用於同態加密方案$\mathfrak{E}$之一公用密鑰pk_{csp}及一私用密鑰sk_{csp}，而評估器110產生用於加密方案ε (其不需要係同態)之一公用密鑰pk_{ev}及一私用密鑰sk_{ev}。

階段1 (520)。每一使用者i本端計算器部分矩陣A_i及向量b_i。然後可在CSP 130之公用加密密鑰pk_{csp}下使用加性同態加密方案$\mathfrak{E}$來加密此等值；亦即，

$$\mathfrak{c}_i = \mathfrak{E}_{\mathrm{pk}_{\mathrm{csp}}}(A_i; b_i)$$

為防止CSP 130存取此值，使用者i在評估器110之公開加密密鑰pk_{ev}下超級加密$\mathfrak{c}_i$之值；亦即，

$$C_i = \mathcal{E}_{\mathrm{pk}_{\mathrm{ev}}}(\mathfrak{c}_i)$$

且將C_i發送至評估器110。

評估器110計算$\mathfrak{c}_\lambda = \mathfrak{E}_{pk_{csp}}(\lambda I; 0)$。該評估器隨後收集所有所接收$C_i$且使用其私用解密密鑰$sk_{ev}$來將其解密以復原$\mathfrak{c}_i$；亦即，

$$\mathfrak{c}_i = \mathcal{D}_{\mathrm{sk}_{\mathrm{ev}}}(C_i), \qquad \text{針對 } 1 \le i \le n$$

然後該評估器彙總所獲得值且得到：

$$\mathfrak{c} = \left(\bigotimes_{i=1}^{n} \mathfrak{c}_i\right) \otimes \mathfrak{c}_\lambda = \mathfrak{E}_{\mathrm{pk}_{\mathrm{csp}}}\left(\sum_{i=1}^{n} A_i + \lambda I; \sum_{i=1}^{n} b_i\right)$$
$$= \mathfrak{E}_{\mathrm{pk}_{\mathrm{csp}}}(A; b) \ . \qquad (4)$$

階段2 (530)。在準備階段510中由CSP 130提供之混淆電路係取作輸入**GI(c)**且進行以下兩個步驟之一電路之一混淆：

1)用sk_{csp}解密$\mathfrak{c}$以復原A及b (此處sk_{csp}嵌入於混淆電路中)；及

2)求解方程式(2)且返回β。

在此階段2 530中，評估器110僅需要獲得對應於$\mathfrak{c}$之混淆電路輸入值；亦即，**GI(c)**。此等值係評估器110與CSP 130之間使用一標準模糊傳送(OT)獲得。

上述混合計算在混淆電路內對經加密輸入執行一解密。在上述情形可需要時，建議使用(舉例而言) Regev同態加密方案作為用於$\mathfrak{E}$之建立區塊，此乃因Regev方案具有一極其簡單解密電路。

C.第二協定

第二協定之操作之一高階繪示600可在圖6中看到。第二協定呈現使用隨機遮罩來避免在混淆電路中解密$(A;\ b)$之一修改方案。階段1 610大體上保持相同。因此將強調提示階段2 (及對應準備階段)。概念係利用同態性質來用一加性遮罩模糊輸入。注意，若$(\mu_A;\ \mu_b)$表示$\mathcal{M}$(即，同態加密$\mathfrak{E}$之訊息空間)中之一元素，則其依據方程式(4)得出：

$$\mathfrak{c} \otimes \mathfrak{E}_{\mathrm{pk_{csp}}}(\mu_A;\mu_b) = \mathfrak{E}_{\mathrm{pk_{csp}}}(A+\mu_A;b+\mu_b)$$

因此，假定評估器110在$\mathcal{M}$中選擇一隨機遮罩$(\mu_A;\ \mu_b)$，如上文所述模糊$\mathfrak{c}$，且將所得值發送至CSP 130。然後，CSP 130可應用其解密密鑰且復原經遮罩值

$$\hat{A}= A + \mu_A \text{且} \hat{b}= b + \mu_b$$

因此，可在將解密替換為移除遮罩之情況下應用先前章節之協定。更詳細而言，其涉及：

準備階段(610)。如之前，評估器110設立評估。評估器110提供規格至CSP 130以建立支援其評估之一混淆電路。CSP 130準備電路且使其可用於評估器110，且兩者皆產生公用及私用密鑰。評估器110選擇一隨機遮罩$(\mu_A;\ \mu_b)\in\mathcal{M}$且以一模糊傳送(OT)協定與CSP 130接合以獲得對應於$(\mu_A;\ \mu_b)$之混淆電路輸入值；亦即，GI ($\mu_A;\ \mu_b$)。

階段1 (620)。此類似於第一協定。另外，評估器110遮罩$\mathfrak{c}$作為

$$\hat{\mathfrak{c}} = \mathfrak{c} \otimes \mathfrak{E}_{\mathrm{pk_{csp}}}(\mu_A;\mu_b)$$

階段2 (630)。評估器110將$\hat{\mathfrak{c}}$發送至CSP 130，該CSP 130將其解密以獲得未加密之$(\hat{A};\hat{b})$。CSP 130然後將混淆輸入值$\mathrm{GI}(\hat{A};\hat{b})$往回發送至

評估器110。在準備階段由CSP 130提供之混淆電路係取作輸入$GI(\hat{A};\hat{b})$及$GI(\mu_A;\mu_b)$且進行以下兩個步驟之一電路之一混淆：

1)自$(\hat{A};\hat{b})$減去遮罩$(\mu_A;\mu_b)$以復原A及b；

2)求解方程式(2)且返回β。

混淆電路以及對應於$(\mu_A;\mu_b)$之混淆電路輸入值$GI(\mu_A;\mu_b)$係在準備階段610期間獲得。在此階段中，評估器110僅需要自CSP 130接收對應於$(\hat{A};\hat{b})$之混洗電路輸入值$GI(\hat{A};\hat{b})$。注意，在此階段不存在模糊傳送(OT)。

針對此第二實現方案，解密不作為電路之一部分執行。因此，實現方案並不限於選定可有效實施為一電路之一同態加密方案。替代Regev方案，建議使用Paillier方案或由Damgård及Jurik之其一般化作為用於$\mathfrak{E}$之建立區塊。此等方案具有比Regev短之一密文擴充且需要較小密鑰。

D.第三協定

針對某些應用，一相關概念在同態加密方案僅具有一部分同態性質時適用。此概念在接下來定義中變的明確。

定義1：*一部分同態加密方案*係一加密方案以使得且可能加上(若部分同態係加性)或乘以(若部分同態係乘性)一常數至一經加密明文而不需要私用加密密鑰。

此處係某些實例。

●假設$\mathbb{F}_p$表示一質體數且假設$G = \langle g \rangle$係由g產生之乘性群組$\mathbb{F}_p^*$之一循環子群組。假設q 表示G之階。針對純ElGamal加密，訊息空間係$\mathcal{M} = G$。共用加密密鑰係$y = g^x$而私用密鑰係x。$\mathcal{M}$中之一訊息m之加密係針對某些隨機$r \in \mathbb{Z}/q\mathbb{Z}$在$R = g^r$且$c = my^r$之情況下藉由$(R; c)$表示。然後在$m = c/R^x$時使用秘密密鑰$x$復原明文$m$。

–上述系統係相對於$\mathbb{F}_p^*$中之乘法部分同態：針對任何常數$K \in \mathcal{M}$，

$C' = (R; Kc)$係對訊息$m' = Km$之加密。

●所謂雜湊ElGamal密碼編譯系統另外需要一雜湊函數H，針對某些參數k，將群組元素自G映射至$\mathbb{F}_2^k$。訊息空間係$\mathcal{M}= \mathbb{F}_2^k$。密鑰產生係關於純ElGamal。對一訊息$m$之加密係針對某些隨機$r \in \mathbb{Z}/q\mathbb{Z}$在$R = g^r$且$c = m + H(y^r)$之情況下由$(R; c)$表示。然後在$m = c+H(R^x)$時使用秘密密鑰$x$來復原明文$m$。注意，「+」對應於$\mathbb{F}_2^k$中之加法(亦即，其可等效視為$k$位元串上之一XOR)。

-上述系統係關於XOR部分同態：針對任何常數$K \in \mathcal{M}$，$C' = (R;K + c)$係對訊息$m' = K + m$之加密。

為非限制性實例起見，現在假定$\mathfrak{c}$係依據一部分同態加密方案(即，$\mathfrak{E}$)對$(A; b)$之加密，然後若$(\mu_A; \mu_b)$表示$\mathcal{M}$ (亦即，部分同態加密$\mathfrak{E}$之訊息空間)中之一元素，則其依據方程式(4)得出

$$\mathfrak{c} \oplus \mathfrak{E}_{\mathrm{pk_{csp}}}(\mu_A; \mu_b) = \mathfrak{E}_{\mathrm{pk_{csp}}}(A + \mu_A; b + \mu_b)$$

針對某些運算子$\oplus$。(在上文闡述中，同態性經註明為加性；其確實適用於一乘性寫入同態。)

因此，假定評估器110在$\mathcal{M}$中選擇一隨機遮罩$(\mu_A; \mu_b)$，如上文模糊$\mathfrak{c}$，且將所得值發送至CSP 130。然後，CSP 130可應用其解密密鑰且復原經遮罩之值。

$\hat{A}= A + \mu_A$且$\hat{b}= b + \mu_b$

因此，可在將解密替換為移除遮罩之情況下應用先前章節之協定。

最終，注意，按照第二或第三協定使用一遮罩之手法並不限於脊狀回歸之情形。其可用於以一混合方式組合同態加密(分別部分同態加密)與混淆電路之任何應用中。

E.論述

所提出協定具有使其在真實情景中高效且實際之數個強項。首先，不存要使用者在程序期間保持在線上。由於階段1 420係增量，因此每一使用者可提交其經加密輸入，且離開系統。

此外，系統100可容易應用於執行脊狀回歸多次。假定評估器110希望執行ℓ估計，其可在準備階段410自CSP 130提取ℓ混淆電路。多重估計可用於適應新使用者120之到達。特定而言，由於共用密鑰係長效的，因此該等共用密鑰不需要過於經常再新，意味著當新使用者提交較多對$(A_i;\ b_i)$至評估器110時，評估器可用先前值對該等對求和且計算一經更新β。儘管此程序要求利用一新混淆電路，但已提交其輸入之使用者並不需要重新提交該等輸入。

最終，所需通信之量顯著限於一秘密共用方案中之通信之量，且僅評估器110及CSP 130使用模糊傳送(OT)通信。亦注意，在階段1 420中並不使用公用密鑰加密方案，使用者可使用任何手段來段建立與評估器110之一安全通信，諸如例如，SSL。

F.進一步最佳化

回想，矩陣A係在$\mathbb{R}^{d\times d}$中且向量b係在$\mathbb{R}^d$中。因此，假定k表示用於編碼實數之位元大小，矩陣A及向量b分別需要d^2k個位元及dk個位元用於其表示。第二協定在$\mathcal{M}$中需要一隨機遮罩$(\mu_A;\ \mu_b)$。假定，同態加密方案$\mathfrak{E}$係建立在其中A及b之每一項目經個別Paillier加密之Paillier方案之上。在此情形中，$\mathfrak{E}$之訊息空間$\mathcal{M}$係由針對RSA模組N之$\mathbb{Z}/N\mathbb{Z}$中之$(d^2 + d)$個元素構成。但由於彼等元素係k位元值，因此不需要在整個範圍$\mathbb{Z}/N\mathbb{Z}$中獲得對應遮罩值。將算出針對某些(相對短)安全長度l之任何$(k+l)$位元值，只要其在統計上隱藏對應項目。實務上，此在準備階段中導致較少模糊傳送且導致一較小混淆電路。

改良效率之另一方式係經由一標準分批次技術，亦即，將A及b之多個明文項目包裝至一單個Paillier密文中。舉例而言，將20個明文

值包裝至一單個Paillier密文(由足夠多0分離)中將使階段1之運行時間減少到1/20。

實施方案

為評估隱私保護系統之實用性，系統經實施且對合成資料集及真實資料集進行測試。實施上文所提出之第二協定，此乃因其在混淆電路內不需要解密，且允許使用對階段1 (僅涉及求和)高效之同態加密。

A.階段1實施方案

如上文所論述，針對同態加密，Paillier方案與一1024個位元長模組一起使用，此對應於80位元安全位準。為加速階段1，亦如上文中所概述實施分批次。已知n個使用者貢獻其輸入，可分批成1024個位元之一個Paillier密文之元素之數目係$1024=(b + \log_2 n)$，其中b係用於表示數目之位元之總數目。如下文所論述，b係依據所期望準確度判定，因此在此實驗中，在15與30個元素之間分批次。

B.電路混淆框架

系統係建立在FastGC (使得開發者能夠使用基本XOR、OR及AND閘定義任意電路之一基於Java之開放原始碼框架)之上。一旦電路經構造，框架處置混淆電路之混淆、模糊傳送及完整評估。FastGC包含數個最佳化。首先，使用「免費XOR」技術顯著減少電路中之XOR閘之通信及計算成本。第二，使用混淆列減少技術，FastGC使k扇入非XOR閘之通信成本減少$1=2^k$，此產生一25%通信節省，此乃因框架中僅定義2扇入閘。第三，FastGC實施OT延伸，該OT延伸可以k個OT且每額外OT數個對稱密鑰操作為代價執行實際上無限數目個傳送。最終，最後最佳化係簡潔「加入3個位元」電路，此定義具有四個XOR閘(所有XOR閘在通信及計算方面係「免費」)及僅一個AND閘之一電路。FastGC使得混淆及評估同時發生。更具體而言，CSP 130

在混淆表以由電路結構定義之次序產生時將該等混淆表傳輸至評估器110。評估器110然後判定哪一閘將接下來基於可用輸出值及表而評估。一旦一閘經評估，其對應表立即被摒棄。此總計與離線預計算所有混淆電路相同之計算及通訊成本，但使記憶體消費達至一常數。

C. 在一電路中求解一線性系統

本發明方法之主要挑戰中之一者係設計求解如方程式(2)中定義之線性系統$A\beta = b$之一電路。當將一函數實施為一混淆電路時，較佳使用係資料不可知(亦即，其執行路徑不依賴於輸入)之操作。舉例而言，由於輸入經混淆，因此評估器110需要執行一若-則-否則敍述之所有可能路徑，此在存在巢套條件敍述之情況下導致電路大小及執行時間兩者至一指數增長。此使得用於求解需要樞軸消元之線性系統之傳統演算法中之任何者(諸如例如高斯消去)不實用。

為簡潔起見，此系統實施下文所呈現之標準喬裏斯基演算法。然而，注意其複雜性可進一步減小至與使用類似技術之區塊式反演相同之複雜性。

存在用於求解線性系統之數個可能分解方法。喬裏斯基分解係僅當矩陣A係對稱正定性時可用之用於求解一線性系統之一資料不可知方法。喬裏斯基之主要優點係其係數值穩健而不需要樞軸消元。特定而言，其極其適於定點數表示。

由於針對$\lambda > 0$，$A = \lambda I + \Sigma_i^n x_i x_i^T$實際上係一正定矩陣，因此喬裏斯基經選擇作為在此實施方案中求解$A\beta = b$之方法。

下文簡要概述喬裏斯基分解之主要步驟。該演算法構造一下三角矩陣L以使得$A = L^T L$：求解系統$A\beta = b$，然後簡化成求解以下兩個系統：

$$L^T y = b \quad ；且$$

$$L\beta = y$$

由於矩陣L及LT係三角形，因此此等系統可使用後置法來容易求解。此外，由於矩陣A係正定的，因此矩陣L需要在對角線上具有非零值，因此不需要任何樞軸消元。

圖7中所示之演算法1中闡述分解$A = L^TL$。其設計$\Theta(d^3)$加法、$\Theta(d^3)$乘法、$\Theta(d^2)$除法及$\Theta(d)$平方根運算。此外，上文透過向後消去之兩個系統之解涉及$\Theta(d^2)$加法、$\Theta(d^2)$乘法及$\Theta(d)$除法。下文論述作為電路之此等運算之實施方案。

D. 表示實數

為求解線性系統(2)，需要以一二進制形式準確地表示實數。用於表示實數之兩個可能方法認為係：浮點及定點、一實數a之浮點表示係由公式表達：

$$[a] = [m; p] \quad ; \text{其中} a \approx 1.m \cdot 2^p$$

浮點表示具有適應實際任意量值之數之優點。然而，對浮點表示之基本運算(諸如加法)難以以一資料不可知方式實施。更重要地，使用喬裏斯基成為使用定點表示之依據，定點表示明顯較易於實施。已知一實數a，其定點表示由下式表達：

$[a] = \lfloor a \cdot 2^p \rfloor$，其中指數$p$係固定的。

如本文中所論述，需要執行之運算中之諸多者可經由定點數以一資料不可知方式實施。如此，經產生用於定點表示之電路更小。此外，回想，脊狀回歸xi之輸入變數通常經調節至相同值域(介於-1與1之間)以確保β之係數係可比較的，且實現數值穩定性。在此一設定中，已知，可用定點數對A執行喬裏斯基分解，而不導致溢出。此外，已知y_i之界限及矩陣A之條件數，可在以該方法求解上兩個三角系統時計算需要防止溢出之位元。因此，使用定點表示實施系統。分式部分之位元之數目p可經選定作為一系統參數，且在系統之準確度

與所產生電路之大小之間形成一折衷。然而，可基於所要準確度以一原則方式進行選定p。負數係使用標準2的補數表示來表示。

本文中所揭示之各種實施例可實施為硬體、韌體、軟體或其任何組合。此外，較佳地將該軟體實施為有形地體現於一程式儲存單元或電腦可讀取媒體上之一應用程式。該應用程式可上傳至包括任一適合架構之一機器且由該機器執行。較佳地，將該機器實施於具有諸如一或多個中央處理單元（「CPU」）、一記憶體及輸入/輸出介面等硬體之一電腦平臺上。該電腦平臺亦可包含一作業系統及微指令碼。本文中所闡述之各種處理程序及功能可係可由一CPU執行之微指令碼之部分或應用程式之部分或者其任一組合，無論是否明確展示此電腦或處理器。另外，各種其他周邊單元（諸如一額外資料儲存單元及一列印單元）可連接至電腦平臺。

本文中所陳述之所有實例及條件語言出於指導性目的意欲幫助讀者理解實施例之原理及由發明者貢獻以推廣此項技術之概念且應視為不限於此等具體陳述之實例及條件。此外，本文中陳述本發明之原理、態樣及實施例以及其特定實例之所有敘述意欲囊括其結構等效物及功能等效物兩者。另外，此等等效物意欲包含目前已知之等效物以及未來將要開發之等效物(例如，不管結構如何而執行相同功能之所開發之任何元件)兩者。

【符號說明】

100	系統
110	評估器
120	使用者
130	密碼編譯服務提供者
140	純文字預測模型β/學習模型β/模型β
200	計算裝置/電子伺服器/處理器/伺服器

210	處理器
220	記憶體
230	儲存器件
240	網路介面
300	布林電路
310	線w_i/輸入線
320	線w_i/輸入線
330	輸出線
g	二進制閘

申請專利範圍

1. 一種用於提供隱私保護之脊狀回歸之方法，該方法包括：

向一密碼編譯服務提供者請求一混淆電路；

自多個使用者收集已使用部分同態加密格式化並加密之資料；

匯合已使用部分同態加密格式化並加密之該資料，其中該匯合不需要一加密密鑰；

將一所準備之遮罩應用於該所匯合資料；

使用模糊傳送自該密碼編譯服務提供者接收對應於所準備之遮罩之混淆輸入；及

使用該等混淆輸入及經遮罩資料來評估來自該密碼編譯服務提供者之該混淆電路。

2. 如請求項1之方法，其中向一密碼編譯服務提供者請求一混淆電路之該步驟包括：

提供用於該混淆電路之輸入變數之一維度；及

提供該等輸入變數之值範圍。

3. 如請求項1之方法，其中實施於一計算裝置上之一評估器執行該方法。

4. 如請求項3之方法，其中該密碼編譯服務提供者實施於遠離該評估器於其上實施之該計算裝置之一計算裝置上。

5. 如請求項1之方法，其進一步包括：提供用於加密來自多個使用者之該資料之一加密密鑰之步驟。

6. 如請求項5之方法，其中用由該密碼編譯服務提供者提供之一加密密鑰來進一步加密來自多個使用者之該資料。

7. 如請求項1之方法，其中評估該混淆電路之該步驟進一步包括：

將該所準備之遮罩自該所匯合資料移除；及

求解由該混淆電路體現之該脊狀回歸方程式。

8. 如請求項1之方法，其中自多個使用者收集資料之該步驟包括：經由一計算裝置接收自該多個使用者中之每一者發送之資料。

9. 一種用於提供隱私保護之脊狀回歸之計算裝置，該計算裝置包括：

一儲存器件，其用於儲存使用者資料；

一記憶體，其用於儲存用於處理之資料；及

一處理器，其經組態以向一密碼編譯服務提供者請求一混淆電路；自多個使用者收集已使用部分同態加密格式化並加密之資料；匯合已使用部分同態加密格式化並加密之該資料，其中該匯合不需要一加密密鑰；將一所準備之遮罩應用於該所匯合資料；使用模糊傳送自該密碼編譯服務提供者接收對應於經遮罩資料之混淆輸入；及使用該等混淆輸入及經遮罩資料來評估來自該密碼編譯服務提供者之該混淆電路。

10. 如請求項9之計算裝置，其進一步包括用於連接至一網路之一網路連接。

11. 如請求項9之計算裝置，其中該密碼編譯服務提供者係實施於一單獨計算裝置上。

12. 如請求項9之計算裝置，其中向一密碼編譯服務提供者請求一混淆電路之該步驟包括：

提供用於該混淆電路之輸入變數之一維度；及

提供該等輸入變數之值範圍。

13. 如請求項9之計算裝置，其中評估該混淆電路之該步驟進一步包括：

將該所準備之遮罩自該所匯合資料移除；及

求解由該混淆電路體現之該脊狀回歸方程式。

14. 如請求項9之計算裝置，其中來自多個使用者之該資料係用由該密碼編譯服務提供者提供之一加密密鑰加密且藉由該計算裝置用一加密密鑰加密。

15. 一種含有當被執行時執行包括以下各項之步驟之指令之機器可讀媒體：

向一密碼編譯服務提供者請求一混淆電路；

自多個使用者收集已使用部分同態加密格式化並加密之資料；

匯合已使用部分同態加密格式化並加密之該資料，其中該匯合不需要一加密密鑰；

將一所準備之遮罩應用於該所匯合資料；

使用模糊傳送自該密碼編譯服務提供者接收對應於所準備之遮罩之混淆輸入；及

使用該等混淆輸入及經遮罩資料來評估來自該密碼編譯服務提供者之該混淆電路。

圖式

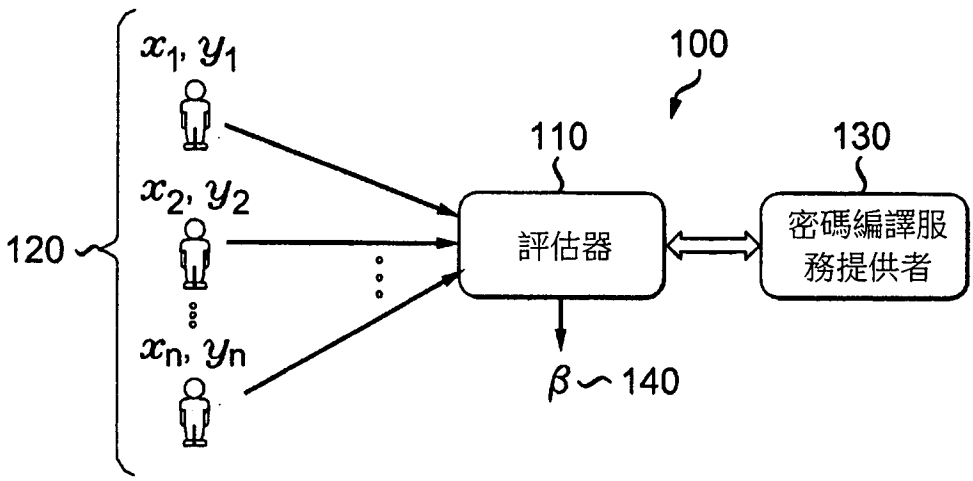

x_1, y_1
x_2, y_2
x_n, y_n
120
100
110
130
評估器
密碼編譯服務提供者
β
140

圖 1

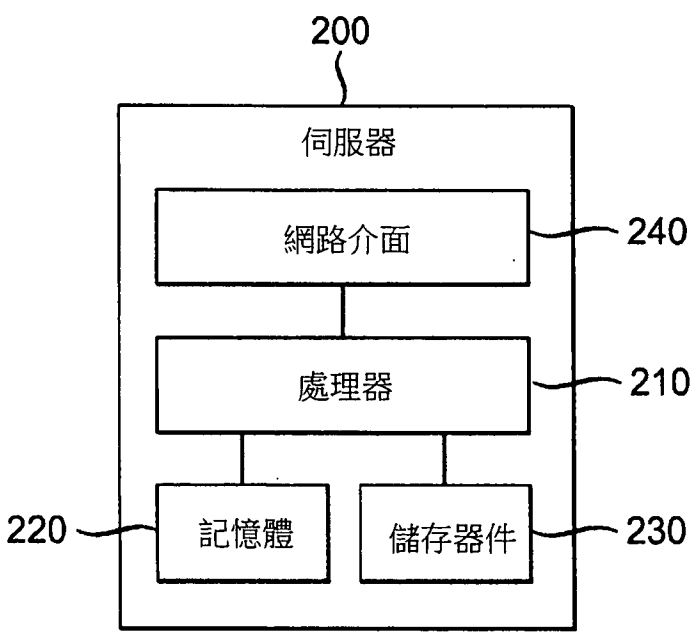

200
伺服器
網路介面
240
處理器
210
220
記憶體
儲存器件
230

圖 2

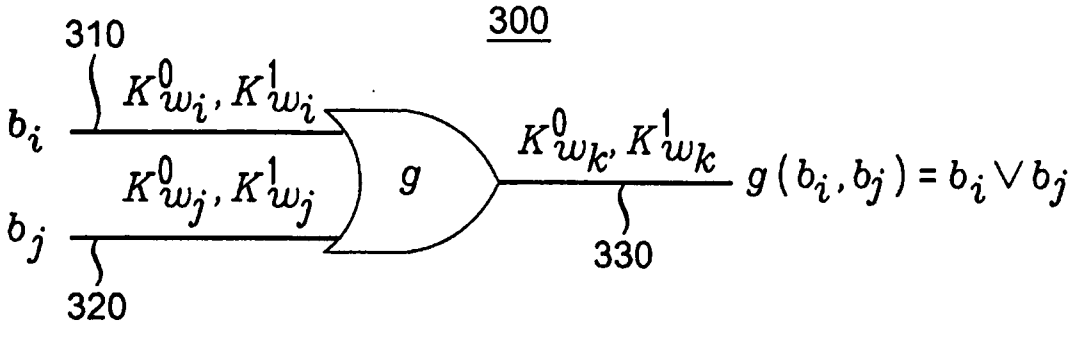

300
310
$K^0_{w_i}, K^1_{w_i}$
b_i
$K^0_{w_j}, K^1_{w_j}$
b_j
320
g
$K^0_{w_k}, K^1_{w_k}$
330
$g(b_i, b_j) = b_i \vee b_j$

圖 3

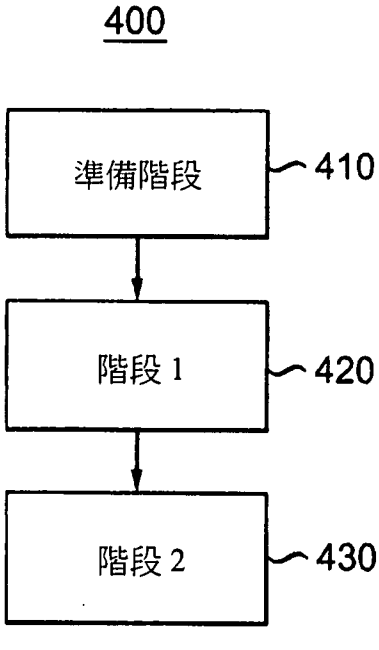

400
準備階段
410
階段 1
420
階段 2
430

圖 4

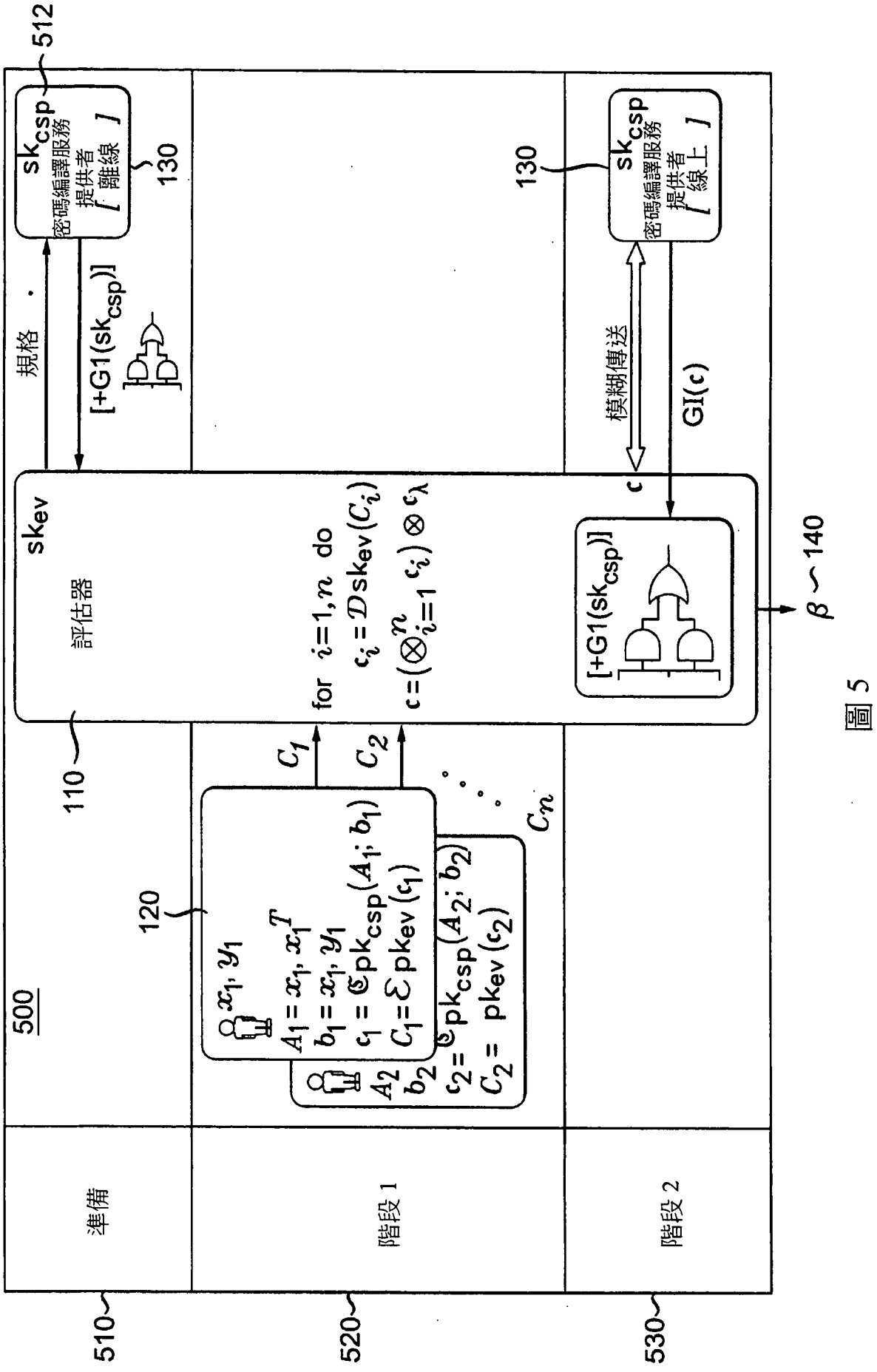

512
sk_{csp}
密碼編譯服務
提供者
離線
130
規格
$[+G1(sk_{csp})]$
130
sk_{csp}
密碼編譯服務
提供者
線上
模糊傳送
GI(c)
c
sk_{ev}
評估器
110
for $i=1,n$ do
$c_i = \mathcal{D}sk_{ev}(C_i)$
$c=(\otimes_{i=1}^{n} c_i) \otimes c_\lambda$
$[+G1(sk_{csp})]$
β
140
120
x_1, y_1
$A_1 = x_1, x_1^T$
$b_1 = x_1, y_1$
$c_1 = \mathcal{E}pk_{csp}(A_1; b_1)$
$C_1 = \mathcal{E}pk_{ev}(c_1)$
A_2
b_2
$c_2 = \mathcal{E}pk_{csp}(A_2; b_2)$
$C_2 = pk_{ev}(c_2)$
C_1
C_2
C_n
500
準備
階段 1
階段 2
510
520
530

圖 5

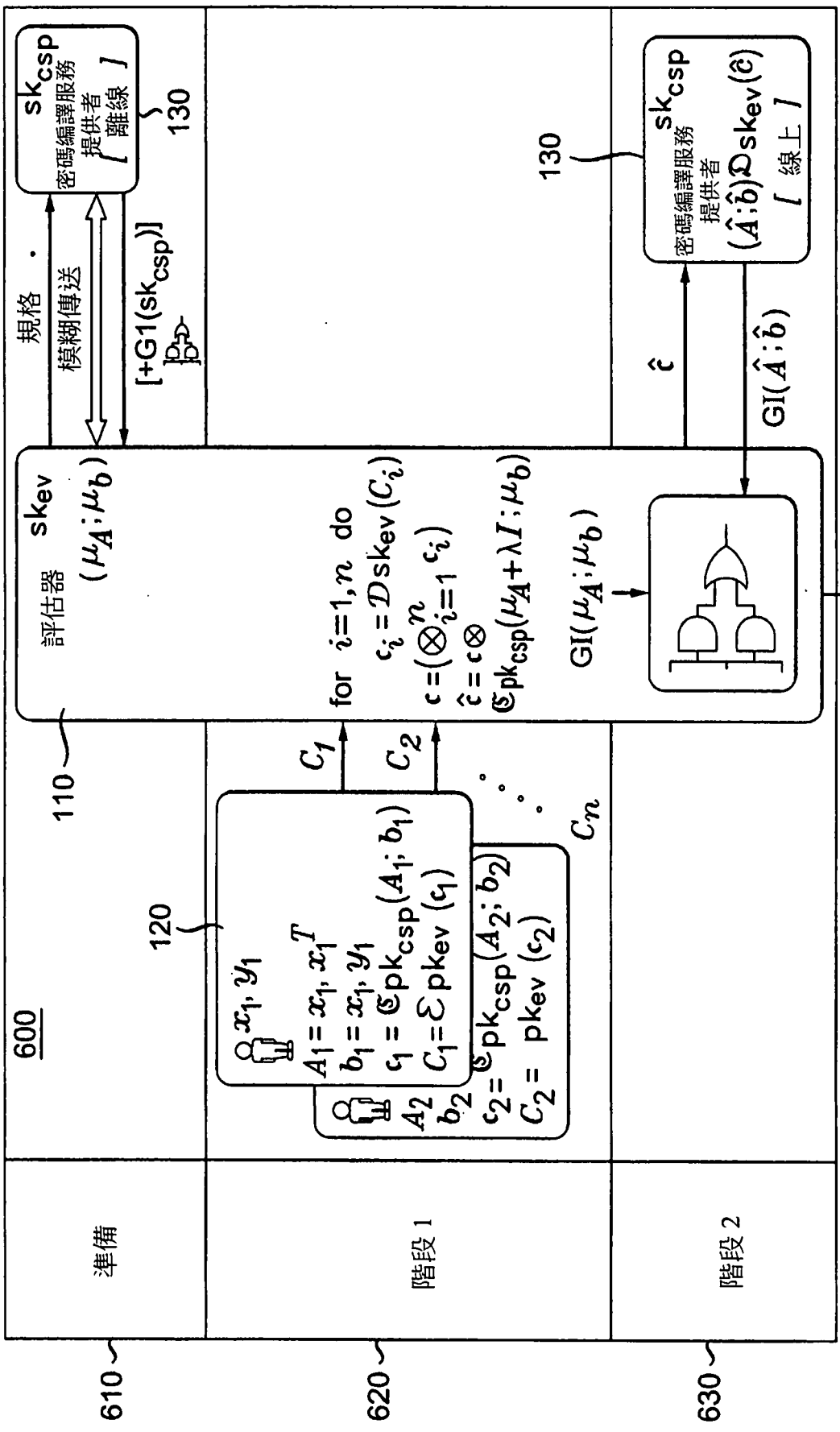

600
準備
階段 1
階段 2
610
620
630
110
120
130
130
評估器 sk_{ev} $(\mu_A;\mu_b)$
規格
模糊傳送
$[+G1(sk_{csp})]$
sk_{csp} 密碼編譯服務 提供者 [離線]
sk_{csp} 密碼編譯服務 提供者 $(\hat{A};\hat{b})\mathcal{D}sk_{ev}(\hat{c})$ [線上]
$\hat{c}$
$GI(\hat{A};\hat{b})$
$GI(\mu_A;\mu_b)$
x_1, y_1
$A_1 = x_1, x_1^T$
$b_1 = x_1, y_1$
$c_1 = \mathcal{E}pk_{csp}(A_1; b_1)$
$C_1 = \mathcal{E}pk_{ev}(c_1)$
A_2
b_2
$c_2 = \mathcal{E}pk_{csp}(A_2; b_2)$
$C_2 = pk_{ev}(c_2)$
C_1
C_2
C_n
for $i=1,n$ do
$c_i = \mathcal{D}sk_{ev}(C_i)$
$c = (\otimes_{i=1}^{n} c_i)$
$\hat{c} = c \otimes \mathcal{E}pk_{csp}(\mu_A + \lambda I; \mu_b)$
β
140

圖 6

演算法 1 A ∈ $R^{d\times d}$ 之喬裏斯基分解

Input: $A = (a_{ij})i,j\in\{1,...,d\}$

Output: L, s.t., $A = L^T L$

1: **for** j = 1, d **do**

2: **for** k = 1, $j-1$ **do**

3: **for** $i = j$, d **do**

4: $a_{ij} -= a_{ik}a_{jk}$

5: $a_{jj} = \sqrt{a_{jj}}$

6: **for** $k = j + 1$, d **do**

7: $akj \ /= \ ajj$

8: **return** $L := A$

圖 7