東海大學資訊管理研究所

碩士學位論文

基於橢圓曲線密碼技術下一個新型 *n* 選 *t* 類型的模糊傳輸協定

A Novel *t*-out-of-*n* Oblivious Transfer Protocol Based on Elliptic Curve Cryptography

指導教授：余心淳 博士

研 究 生：沈怡庭 撰

中華民國 105 年 06 月

東海大學資訊管理學系碩士學位

考試委員審定書

資訊管理學系研究所 沈怡庭 君所提之論文

基於橢圓曲線密碼技術下一個新型 n 選 t 類型的模糊傳輸協定

經本考試委員會審查，符合碩士資格標準。

學位考試委員會 召集人：[illegible] （簽章）

委 員：張顧耀

[illegible]

[illegible]

余心淳

中 華 民 國 105 年 6 月 30 日

致謝

即將要畢業離開學校了，從大學起就是就讀東海大學資訊管理系，因為時間與環境的關係，選擇申請系上的五年一貫，並在大三時順利錄取，因此在大四時跟著指導教授余心淳老師開始閱讀論文。而兩年的研究所生涯也即將告一個段落，回想起那時的我，其實對於做研究懵懵懂懂，很徬徨與不知所措，不確定自己是否有能力完成論文並取得碩士學位，感謝余心淳老師在我最無助時出現，一開始時，研究的領域一直不得要領，但經過老師不斷的指點與教導，在這個領域愈來愈有心得，也跟著培養出信心。在這段時間裡，老師教導我的不僅僅是學術方面，待人處事方面更是老師重視的一環，老師也常常分享與我們自身的經歷，並且傳授正確的邏輯思考與做研究應有的精神。

論文能夠完成，非常感謝余心淳老師的提攜與幫助，在我遇到瓶頸時給我許多意見與指導，讓我了解如何用不同的角度去思考同一件事情，還要感謝口試委員邱紹豐教授、張顧耀教授與黃正炎博士給予許多寶貴的指導和建議，使我的論文能更加完善，另外也要特別感謝國鴻、家柔、照芸學姊與其他研究所的同學們，不管是在課業上的幫助還是在提供論文上的一些想法，總是可以讓我的論文與課業順利的進行，以及一路支持我的家人與朋友，給予我關懷與鼓勵，並做我堅強的後盾，讓我能夠把所有的心思都放在研究上，可以說如果沒有你們我可能就無法這麼順利的完成我的論文與學業課程。

沈怡庭 謹誌於

東海大學資訊管理研究所

中華民國 105 年 6 月

論文名稱：基於橢圓曲線密碼技術下一個新型 n 選 t 類型的模糊傳輸協定

校所名稱：東海大學資訊管理學系研究所

畢業時間：2016/06

研究生：沈怡庭　　指導教授：余心淳 博士

論文摘要：

由於網路是一個公開且透明的環境，透過網路進行通訊時，可能潛藏許多危機與攻擊，因此必須藉由密碼系統來保護通訊雙方的隱私安全，而模糊傳輸協定被視為密碼學中重要的基礎通訊技術，主要是因為模糊傳輸的機制可以被應用在許多方面，例如：電子商務、秘密資料交換、電子契約等等。在 n 選 t 的模糊傳輸協定中，傳送方擁有 n 個訊息，接收方可以選擇其中 t 個訊息，但傳送方無法得知接收方選擇的是哪 t 個訊息，接收方也無法得知其餘未選擇的$n-t$個訊息內容為何。將橢圓曲線密碼系統應用到模糊傳輸協定上，以點運算取代指數運算，相較於其它的密碼系統，不僅可以減少計算量，同時也可強化協定的安全性。

現今基於橢圓曲線密碼系統的模糊傳輸協定可區分為「先加密訊息後計算金鑰」與「先計算金鑰後加密訊息」二個運作模式。「先加密訊息後計算金鑰」是現今最普遍的模糊傳輸機制，無論是在 2 選 1 模糊傳輸協定、n 選 1 模糊傳輸協定與 n 選 t 模糊傳輸協定的問題上已經有許多演算法與傳輸協定的導出與討論，但是在「先計算金鑰後加密訊息」的模式下，目前大部分相關的文獻中只有針對 2 選 1 模糊傳輸協定與 n 選 1 模糊傳輸協定的問題上有所討論，對於更為實用與複雜的 n 選 t 模糊傳輸協定的問題上缺乏完整的研究討論與設計實現。因此本論文特別針對此一問題，提出一個可基於橢圓曲線密碼系統技術下「先計算金鑰後加密訊息」模式下的 n 選 t 模糊傳輸協定。

本論文提出的 n 選 t 模糊傳輸協定除了利用橢圓曲線密碼系統的特性大幅降低了計算量之外，亦使用數學上 Cantor 配對函數來設計金鑰，以有效地區分出 t 個要選取與解密的訊息，但本協定的整體訊息傳輸量仍高於一般「先加密訊息後

計算金鑰」模式下的 n 選 t 模糊傳輸協定，因此在本論文中進一步延伸討論如何將 Cantor 配對函數應用至模糊傳輸的協定上，以降低訊息的總傳輸量，使 n 選 t 模糊傳輸能更能符合實際應用上高安全性、高效率與低頻寬的需求。

關鍵字：資訊安全、模糊傳輸、橢圓曲線密碼系統、Cantor 配對函數

Title of Thesis：A Novel *t*-out-of-*n* Oblivious Transfer Protocol Based on Elliptic Curve Cryptography

Name of Institute：Tunghai University, Graduate Institute of Information Management

Graduation Time：2016/06

Student Name：Yi-Ting Sheng Advisor Name：Sc.D. Hsin-Chun Yu

Abstract：

The Internet is an open, public and transparent environment in which various security threats and malicious attack are hidden during communications. Cryptosystems are therefore utilized for protecting the privacy of communication parties. An oblivious transfer protocol has been regarded as an important secure communication technique in cryptology, mainly because the oblivious transfer mechanism could be applied to e-commerce, confidential information exchange, e-contract, and so on. In the *t*-out-of-*n* oblivious transfer protocol, the sender possesses *n* pieces of information, from which the receiver could choose *t* pieces of information. However, the sender could not know which information is selected by the receiver and the receiver does not know the contents of the rest $n-t$ pieces of information. Comparing to other cryptosystems, applying elliptic curve cryptosystems to the oblivious transfer protocol and replacing exponent operations with point operations not only could reduce the computational cost of oblivious transfer but also reinforce the protocol security.

Current elliptic curve cryptosystem based oblivious transfer systems could be divided into the operation models of “first encrypting message and then calculating the key” and “first calculating the key and then encrypting message”. The former is the commonest oblivious transfer mechanism currently, with which 1-out-of-2, 1-out-of-*n*, and *t*-out-of-*n* oblivious transfer protocols have been derived from various algorithms and transfer protocols and discussed. Nevertheless, most research, under the model of

"first calculating the key and then encrypting message", focuses on 1-out-of-2 and 1-out-of-*n* oblivious transfer protocols. More practical and complicated *t*-out-of-*n* problems are lack of complete research discussion and design implementation. Aiming at such a problem, the *t*-out-of-*n* oblivious transfer protocol based on the model of "first calculating the key and then encrypting information" under the elliptic curve cryptosystem technology is proposed in this study.

In addition to largely reducing the calculation amount with the characteristics of elliptic curve cryptosystems, the proposed *t*-out-of-*n* oblivious transfer protocol also designs the key with Cantor pairing function to effectively distinguish *t* pieces of selected and decrypted information. Nonetheless, the overall information transfer amount through this protocol is higher than general *t*-out-of-*n* oblivious transfer protocols under the model of "first encrypting message and then calculating the key". The application of Cantor pairing function to oblivious transfer protocols is therefore extended in this study to reduce the total information transfer amount and allow *t*-out-of-*n* oblivious transfer better conforming to the practical requirements of high security, high efficiency, and low bandwidth.

Key words: information security, oblivious transfer, elliptic curve cryptosystem, Cantor pairing function

目錄

圖目錄

表目錄

第一章　緒論

由於網路使用者愈來愈重視資訊安全，而模糊傳輸協定可以確保網路通訊者的隱私安全與資料傳輸的正確性，因此本研究利用模糊傳輸協定的概念，並結合橢圓曲線密碼系統，提出一個新型的 n 選 t 模糊傳輸協定。

第一節　研究背景

隨著網際網路、通訊科技的蓬勃發展以及電腦技術的日益發達，網路已融入大多數人的生活中，成為不可或缺的存在，而人們利用網路從事交易也變得更加方便與頻繁，但同時也帶來許多數位經濟行為的衝擊與變革，影響了職場以及商業行為。再加上電腦與網路的普及，使得越來越多的交易與資料傳輸發生在公眾網路間，然而網際網路是一個高度透明且開放的公開環境，暴露了網路上資料傳輸的危險性，若要傳遞重要的訊息，則有可能潛藏許多的危機，包括被竊取、偽造、竄改資料與攻擊等等，甚至是產生電腦犯罪，因此人們對公眾網路上資訊安全的要求越來越高，所以如何確保資料的安全傳輸以及設計一個安全，且有效能的密碼系統是相當重要的課題。

為了確保數位化資訊在網路環境安全地進行交易，必須建立一個可信賴的網路環境，而密碼系統的設計是其中一個安全且有效率的方法。密碼系統可對訊息進行加密，故安全、實用的密碼系統可以有效確保人們在公眾網路上傳輸資訊的安全，藉由密碼學的技術來保護通訊雙方所傳遞的訊息，使通訊雙方保有個人隱私及交換訊息的完整性和機密性，密碼學相關研究便成為資訊安全的重要的議題。設計安全的密碼系統，需要一個安全的密碼協定，近年來模糊傳輸(Oblivious Transfer, OT)技術已被視為密碼學中一項重要且關鍵的基礎通訊技術，模糊傳輸的機制可以被應用在許多方面，以提供商業交易與傳輸機密性資料一個安全可信賴的網路環境。

模糊傳輸的機制可以被應用在解決網路通訊者傳遞訊息安全問題之環境，當傳送方擁有一些秘密訊息，接收方可以從中選擇自己想要的訊息，透過模糊傳輸的機制傳送方無法得知接收方選擇哪些訊息，也無法得知是否取得訊息，而接收方也只能取得選擇的訊息，藉以確保傳送方和接收方的隱私安全，現今模糊傳輸協定可應用許多方面，例如：私密資訊擷取機制(Private Information Retrieval, PIR)、數位資料交易、電子病歷、零知識證明、網路拍賣系統，以及資料庫管理系統等。

模糊傳輸協定是屬於兩方通訊的傳輸協定，且是現今密碼技術中相當重要資訊傳輸的安全機制，其主要概念為傳送方擁有一個或多個訊息，接收方可以從中選擇想要的訊息，但傳送方無法得知接收方選擇的是哪個訊息，接收方也無法得知未選擇的訊息內容為何。在 1918 年 Rabin[30]最先提出模糊傳輸協定的機制，模糊傳輸協定是屬於兩方通訊的傳輸協定，通訊雙方分別稱為傳送方與接收方，他提出的非有即無的概念，可想像為解決利用電話完成丟銅板的遊戲，傳送方擁有一個祕密訊息，並將這個秘密訊息傳送給接收方，但接收方只有二分之一的機率能得到該訊息，而有二分之一的機率什麼也得不到。而在遊戲結束後，傳送方亦無法得知接收方是否接收到該訊息。

在 1985 年 Even 等人[13]延伸 Rabin[30]的想法提出 2 選 1 模糊傳輸協定，傳送方傳送兩個秘密訊息m_1和m_2給接收方，接收方能夠從兩個訊息中選擇一個想要的訊息，在傳輸結束後，傳送方無法得知接收方選擇的是哪一個訊息，接收方也無法得知另一個未選擇的訊息內容為何。

接著在 1997 年 Brassard 與 Crepeau[4]延伸 2 選 1 模糊傳輸協定提出 n 選 1 的模糊傳輸協定，而 Naor 與 Pinkas[26]、Stern[32]、Tzeng[34]也先後提出 n 選 1 的模糊傳輸協定，協定中傳送方擁有 n 個訊息$m_1, m_2, \ldots, m_n$，接收方可以從 n 個訊息中選擇其中一個訊息，在傳輸完成後，傳送方無法得知接收方選擇的訊息為何，接收方也僅能得知所選的該筆訊息的內容，其餘皆無法得知。

此後，模糊傳輸被廣泛地討論及研究，Mu 等人[23]、Wakaha 與 Ryota[35]、

Huang 與 Chang[16]，以及 Zeng 等人[37]分別進一步提出 n 選 t 的模糊傳輸機制，傳送方擁有 n 個訊息，接收方可同時選擇其中的 t 個訊息，協定完成後，傳送方無法得知接收方選擇的是哪 t 個訊息，接收方也無法得知其餘未選擇的$n-t$個訊息內容為何。

由上述的介紹得知模糊傳輸協定按照傳送方擁有的訊息量以及接收方可選擇的訊息量分為下列幾類：

1. 非有即無的模糊傳輸協定：傳送方傳送 1 個訊息給接收方，而接收方獲得與未獲得該訊息的機率各為二分之一，傳輸結束後，傳送方無法得知接收方是否獲得。

2. 2 選 1 的模糊傳輸協定：傳送方傳送 2 個訊息給接收方，而接收方只能從中選擇 1 個想要的訊息，傳輸結束後，傳送方無法得知接收方選擇何者，接收方也無法得知另一個訊息內容為何。

3. n 選 1 的模糊傳輸協定：傳送方傳送 n 個訊息給接收方，而接收方只能從中選擇 1 個想要的訊息，傳輸結束後，傳送方無法得知接收方選擇何者，接收方也無法得知其餘$n-1$ 個的訊息內容為何。

4. n 選 t 的模糊傳輸協定：傳送方傳送 n 個訊息給接收方，而接收方可以從中選擇 t 個想要的訊息，傳輸結束後，傳送方無法得知接收方選擇哪些訊息，接收方也無法得知其餘$n-t$個的訊息內容為何。

除此之外，模糊傳輸協定也可以按照傳送方和接收方訊息傳遞的方式區分為交談式(Interactive)與非交談式(Non-Interactive)兩類。兩者的主要差異是在於交談式的模糊傳輸協定需要傳送方與接收方以互動的方式來交換訊息，非交談式的模糊傳輸協定則不需要傳送方和接收方透過互動來交換訊息。在 1981 年 Blum[3]首先提出交談式的模糊傳輸協定，並利用此協定實現電話丟銅板(Coin flipping by

telephone)、如何交換秘密(How to exchange secret)，以及如何傳送被確認的郵件(How to send certified electronic mail)這三種應用。而 Even 與 Lempel[13]進一步提出交談式的 2 選 1 模糊傳輸協定，但交談式的模糊傳輸協定通訊雙方必須來回傳遞訊息，在實際應用上效率是比較差的。因此 1989 年 Bellare 與 Micali[2]首先提出非交談式的 2 選 1 模糊傳輸協定，在此協定中不需要透過雙方互動傳遞訊息，而是接收方先公開一些資訊，傳送方利用公開資訊進行計算，並單向傳送訊息給接收方，接收方即可正確地獲得其中一個訊息，且傳送方無法得知接收方選擇的訊息是哪一個。Harn 與 Lin[15]也在同年提出非交談式的 2 選 1 模糊傳輸協定，此協定也是相同的概念，但進一步提升協定的效能，並降低了資料的傳輸量。

由上述的介紹得知模糊傳輸協定的發展可以分為非有即無的模糊傳輸協定、2 選 1 的模糊傳輸協定、n 選 1 的模糊傳輸協定以及 n 選 t 的模糊傳輸協定，然而無論何種類型的模糊傳輸協定皆必須符合下列三項安全要求 [25][34]：

1. 正確性：如果傳送方和接收方皆遵循傳輸協定之協議，接收方則可以正確地獲得所選擇的訊息。
2. 傳送方的隱私安全：在傳輸協定結束後，接收方只能獲得所選擇的訊息，而無法獲得其餘未選擇的訊息。
3. 接收方的隱私安全：在傳輸協定結束後，傳送方無法得知接收方選擇的訊息為何。

第二節　研究動機

由於網路的快速發展，愈來愈多人透過網路進行交易或者傳遞資料，也愈來愈重視網路上的資訊安全，因此保護通訊雙方的隱私安全是個相當重要的議題，而密碼系統的技術是增進網路通訊安全的重要工具，近年來模糊傳輸協定更是密碼系統中一個重要且關鍵的技術。

模糊傳輸協定是兩方的通訊協定，可以分為非有即無的模糊傳輸協定、2 選

1 的模糊傳輸協定、*n* 選 1 的模糊傳輸協定，以及 *n* 選 *t* 的模糊傳輸協定。根據研究顯示，大部分的 *n* 選 *t* 模糊傳輸協定可以滿足 2 選 1 的模糊傳輸協定和 *n* 選 1 的模糊傳輸協定，而模糊傳輸協定又可以分為「先加密訊息後計算金鑰」與「先計算金鑰後加密訊息」[2][7][9][16]兩種模式，至今「先加密訊息後計算金鑰」的模糊傳輸協定已有學者提出 2 選 1 模糊傳輸協定、*n* 選 1 模糊傳輸息定與 *n* 選 *t* 模糊傳輸協定。在學術界已知發表的文章中「先計算金鑰後加密訊息」的模糊傳輸協定只有 2 選 1 模糊傳輸協定[29]與 *n* 選 1 模糊傳輸協定機制有相關的研究成果發表[16][29]。

2006 年 Parakh[28]首先將橢圓曲線密碼系統應用到模糊傳輸協定上，因橢圓曲線密碼系統加密的金鑰長度較 RSA[18]短，執行效率較佳，且擁有較高的安全性，因此提出非有即無的模糊傳輸協定，以及以非有即無的模糊傳輸協定為基礎延伸出 2 選 1 的模糊傳輸協定，協定中利用點的運算取代以往的指數運算來降低計算量，並提高整體的效能。基於橢圓曲線密碼系統的 *n* 選 1 模糊傳輸協定與 *n* 選 *t* 模糊傳輸協定也陸續有學者提出，但至今學者只有提出「先加密訊息後計算金鑰」的 *n* 選 *t* 模糊傳輸協定，因此本研究希望提出先計算金鑰的 *n* 選 *t* 模糊傳輸協定，使模糊傳輸協定能有更多的應用領域。

第三節　研究目的

「先加密訊息後計算金鑰」的模糊傳輸協定優點在於訊息傳輸量較低，但在訊息傳輸的過程中，傳送方將加密完的訊息全部傳給接收方，而加密的金鑰是傳送方自己設計的，若攻擊者破解傳送方的編碼方式，加密的訊息就容易被破解。而「先計算金鑰後加密訊息」的模糊傳輸協定則為傳送方和接收方會先相互協議金鑰的機制，相當於金鑰有雙層的保護機制，較不容易被攻擊者破解，因此協定整體的安全性較高，適合傳輸機密性資料，但缺點是訊息傳輸量會比「先加密訊息後計算金鑰」模式來的高。如前所述，在已知發表的文獻中，大部分的學者皆

集中討論「先加密訊息後計算金鑰」模式下的 2 選 1、*n* 選 1 與 *n* 選 *t* 相關的模糊傳輸協定；但「先計算金鑰後加密訊息」模式下的模糊傳輸協定只有 2 選 1 與 *n* 選 1 的模糊傳輸協定有相關的討論與研究成果，尚無 *n* 選 *t* 模糊傳輸協定的研究成果發表。因此本論文的研究目的是在以 Parakh[29]提出的 *n* 選 1 模糊傳輸協定為基礎，進一步提出基於橢圓曲線密碼學技術下「先計算金鑰後加密訊息」模式中的 *n* 選 *t* 模糊傳輸協定，冀望利用橢圓曲線密碼系統的低計算量與高安全等優點，以及整合 Cantor 配對函數 1 對 1 的映射特性來設計金鑰，增加協定計算的複雜度與提升協定的安全性，以及有效區分出 *t* 個要選取與解密的訊息，並進一步討論如何將 Cantor 廣義 *n* 元配對函數應用至模糊傳輸協定中，期望降低協定的訊息傳輸量，使模糊傳輸協定能實際應用在低頻寬的環境，同時也能保障通訊者的隱私安全。

第四節　章節概要

本論文的章節架構共分為五章，第一章為緒論，主要說明本研究的研究背景、動機與目的。第二章為文獻探討，分別介紹密碼系統、雙鎖密碼系統(Two-Lock Cryptosystem)、橢圓曲線密碼系統(Elliptic Curve Cryptosystem)，與模糊傳輸協定的訊息傳輸步驟，以及基於橢圓曲線的模糊傳輸協定之概念。在第三章會詳細說明本研究提出基於橢圓曲線密碼學技術下「先計算金鑰後加密訊息」模式中的 *n* 選 *t* 模糊傳輸協定，並進行安全性分析和效能分析。第四章延伸討論 Cantor 配對函數(Cantor Pairing Function)應用到模糊傳輸協定的結果。最後第五章為結論與未來展望。

第二章　文獻探討

以往在密碼系統中 RSA 是最常被採用的，但為了提高安全性，RSA 金鑰的長度也隨之增加，在相同的安全性下，橢圓曲線密碼系統所需的金鑰長度比 RSA 短。而模糊傳輸協定在密碼學中是一個重要的基礎協定，可同時保護通訊雙方的隱私安全。因此在以下章節分別介紹密碼系統、雙鎖密碼系統、橢圓曲線密碼系統、模糊傳輸協定，以及結合橢圓曲線密碼系統和模糊傳輸的傳輸協定。

第一節　密碼系統

密碼系統是由明文(Plaintext)、密文(Ciphertext)、加密演算法(Encryption Algorithm)，與解密演算法(Decryption Algorithm)組合而成[20][26][30]。以下為這四個名詞的解釋：

一、 明文(Plaintext)：加密前的原始資料。

二、 密文(Ciphertext)：加密後的資料。

三、 加密演算法(Encryption Algorithm)：利用加密金鑰對明文進行加密動作的演算法。

四、 解密演算法(Decryption Algorithm)：利用解密金鑰對密文進行解密動作的演算法。

密碼系統可以確保資訊傳輸的私密性，以及提供雙方驗證識別，與資料傳輸來源、接收目的地或交易證明，防止中間人惡意竊聽或攻擊，並可以偵測資料是否被不當地篡改。安全性主要取決於加密技術的強度，而加密技術的強度是指密碼被破解所需要花費的時間與資源，其中演算法、金鑰保護機制與金鑰長度是影響加密技術強度的主要因素。按照金鑰使用個數的差異可以將密碼系統分為對稱式密碼系統與非對稱式密碼系統二種。

對稱式密碼系統(Symmetric Cryptosystems)又稱為單一密碼系統、私密金鑰

密碼系統或傳統加密系統，在此系統中加密與解密使用的是同一把金鑰，合法使用者必須產生一把自己的金鑰，並用這把金鑰與資料進行運算以產生密文。當通訊雙方擁有同一把金鑰並進行秘密通訊時，傳送方利用金鑰將訊息加密後傳給接收方，接收方再利用同一把金鑰將訊息解密。

非對稱式密碼系統(Asymmetric Cryptosystems)又稱為公開金鑰密碼系統，系統中加密與解密使用不同的金鑰，分別為公開金鑰(Public Key)以及私密金鑰(Private Key)，這兩把金鑰是對應的，但無法輕易互相計算得出，其中公開金鑰是公開的，而私密金鑰只有自己知道。當通訊雙方進行秘密通訊時，接收方必須先將自己的公開金鑰傳給傳送方，傳送方利用接收方的公開金鑰加密訊息後回傳給接收方，接收方再利用自己的私密金鑰解密出訊息。

第二節　雙鎖密碼系統

雙鎖密碼系統(Two-Lock Cryptosystem)[36]是一種三回通訊的加密方式，但不屬於公開密碼系統，因為其兩把金鑰皆為私密金鑰，所以概念上就如同真實世界中的 Padlock(中文稱為掛鎖)，這個 Padlock 可以被輕易地關上，但是當沒有私密金鑰它很難被打開。Alice 可以透過郵件寄送一個公開 Padlock 給 Bob(等同於公開金鑰)，Bob 接著將訊息放進 Padlock 盒子裡並且利用 Padlock 上鎖，最後 Bob 將此 Padlock 盒子寄送回給 Alice，而 Alice 利用她的私密金鑰將訊息取出。

假設 Alice 想要傳送一個祕密訊息m給 Bob，Alice 和 Bob 的加密演算法為 A 和 B，Alice 和 Bob 分別隨機選擇自己的密鑰k和s，如果對任意k和s都會滿足$B_s\big(A_k(m)\big) = A_k(B_s(m))$，則進行加密通訊如以下步驟：

Step 1.　Alice 傳送給 Bob：$Y = A_k(m)$

Step 2.　Bob 傳送給 Alice：$Z = B_s(Y)$

Step 3.　Alice 傳送給 Bob：$C = A_k^{-1}(Z)$

Step 4.　Bob 解密：$m = B_s^{-1}(C)$

在這裡$A_k^{-1}(\bullet)$ 表示為$A_k(\bullet)$的解密，Bob 可以解密密文C且得到訊息$m = B_s^{-1}(C)$，我們稱此密碼原型為雙鎖密碼系統，當$A = B$時，它也被稱為可交換式加密。一個雙鎖密碼系統應該使得攻擊者無法找到k滿足 $C = A_k^{-1}(Z)$或是得到s滿足$Z = B_s(Y)$，由於雙鎖密碼系統無法抵禦中間人攻擊，因此需要一個 Bob 及 Alice 皆經過身分驗證的專屬通道,驗證通道技術在此不屬本文重點則省略敘述。

第三節　橢圓曲線密碼系統

Miller[22]及 Koblitz[17]首先提出橢圓曲線結合密碼系統(Elliptic Curve Cryptosystems, ECC)，橢圓曲線密碼系統其安全性是建立在解橢圓曲線離散對數問題(Elliptic Curve Discrete Logarithm Problem, ECDLP)上，意即橢圓曲線上取任意兩點 P 和 Q，假設$Q = kP$，在已知 k 和 P 的情況下，Q 可以透過計算得出，但如果已知 P 和 Q，要反推計算出k則是很困難的。橢圓曲線密碼系統最大的優點在於相同金鑰長度之下，擁有比其他密碼系統如 RSA 更高的安全性，反之在相同安全性之下橢圓曲線密碼系統所需金鑰長度比其他密碼系統如 RSA 更短，例如橢圓曲線密碼系統金鑰長度 160 位元之安全性等同於 RSA 金鑰長度 1024 位元。

橢圓曲線使用在密碼學的通式如下[16]：

$$y^2 = x^3 + ax + b$$

其中 a、b 為小於 p 之正整數，設定 p 是一個大於 3 的質數，並將橢圓曲線取質數 p 的同餘$(mod\ p)$，表示如下：

$$E_p(a,b)：y^2 = x^3 + ax + b \ mod\ p$$

質數 p 會固定住橢圓曲線$E_p(a,b)$的上限，因此橢圓曲線$E_p(a,b)$為一個有限體，且橢圓曲線的判別式必須不等於 0，上述方程式$E_p(a,b)$的判別式表示如下：

$$\Delta = 4a^3 + 27b^2 \ mod\ p \neq 0$$

在橢圓曲線的定義中存在無窮遠點O，假設$P=(x_1,y_1)$及$Q=(x_2,y_2)$為橢圓曲線$E_p(a,b)$上的兩點，如果$x_1=x_2\ mod\ p$，則$P+Q=O$，如果$y_1=0\ mod\ p$，則$P=-P$，且$2P=O$，其餘非上述的情況下，$P+Q$的總合是透過計算而得，若$P+Q=(x_3,y_3)$，$x_3=\lambda^2-a-x_1-x_2$，$y_3=\lambda(x_1-x_3)-y_1\ mod\ p$，若$P\neq Q$，則$\lambda=\frac{x_1-x_2}{y_1-y_2}\ mod\ p$，若$P=Q$，則$\lambda=\frac{3{x_1}^2+2ax_1+b}{2y_1}\ mod\ p$，對於橢圓曲線上的 P 及 Q 兩點，加法運算規則定義如下：

1. $O+P=P$且$P+O=P$。
2. 如果$Q=-P$，則$P+Q=O$。
3. $-O=O$。
4. 如果$P=(x,y)\neq O$，則$-P=(x,-y)$，且P和$-P$是橢圓曲線$\mathrm{E_p}$上具有相同 x 坐標的唯一點。
5. 對任意正整數k和橢圓曲線上的任一點P，其純量乘法$kP=P+P+\cdots+P$，會等於P累加k次。
6. 橢圓曲線上正整數點的個數稱為級數，假設橢圓曲線$E_p(a,b)$的級數為 N，對於橢圓曲線$E_p(a,b)$上所有的點皆滿足$NP=O\ mod\ p$。

第四節　模糊傳輸協定

模糊傳輸協定是屬於兩方通訊的傳輸協定，且是現今密碼技術中相當重要資訊傳輸的安全機制，其主要概念為傳送方擁有一個或多個訊息，接收方可以從中選擇想要的訊息，但傳送方無法得知接收方選擇的是哪個訊息，接收方也無法得知未選擇的訊息內容為何。以下介紹兩種 *n* 選 *t* 模糊傳輸協定：

一、Chang 與 Lee 提出的 *n* 選 *t* 模糊傳輸協定

Chang 與 Lee[7]提出的 *n* 選 *t* 模糊傳輸協定證明 2003 年 Mu 等人[24]提出的

模糊傳輸協定無法確保傳送方的隱私，接收方可以取得選擇的 t 個訊息以外的訊息內容，因此 Chang 與 Lee[7]提出此協定，利用盲簽章(Blind Signature)與中國餘數定理(Chinese Remainder Theorem)的概念，加強確保傳送方的隱私，並降低頻寬的消耗與減少傳送方和接收方的計算量，但由於協定的安全性是建立在 RSA 上，因此計算量還是太大。Chang 與 Lee 所提出的演算法[7]如圖 2-1 所示，以下為協定的傳輸步驟：

Step 1. 在收到 Bob 所傳送所有訊息的要求$a_1, a_2, \dots, a_n$後，Alice 選擇相應的 n 個質數$d_1, d_2, \dots, d_n$，以及計算$D = d_1 * d_2 * \dots * d_n$，再建立一致性系統 $C \equiv a_1 \bmod d_1$，$C \equiv a_2 \bmod d_2$，…，$C \equiv a_n \bmod d_n$，接著再計算 $C = \left(\frac{D}{d_1}\right) y_1 a_1 + \left(\frac{D}{d_2}\right) y_2 a_2 + \dots + \left(\frac{D}{d_n}\right) y_n a_n \bmod D$，此外，Alice 會再計算下列數值：$T_1 = d_1^e \bmod N$，$T_2 = d_2^e \bmod N, \dots, T_n = d_n^e \bmod N$，其中 e 為公鑰。最後 Alice 將 C 以及$(ID_i, T_i, i = 1,2, \dots, n)$公開。

Step 2. 如果 Bob 想要知道 Alice 擁有的資訊，那麼 Bob 首先必須選擇 t 個 $(ID_j', T_j', j = 1,2, \dots, t) \in (ID_i, T_i, i = 1,2, \dots, n)$，並產生 t 個相對應的隨機數r_1，r_2，…，r_t，接著再分別計算$\alpha_1 = r_1^e * T_1' \bmod N$，$\alpha_2 = r_2^e * T_2' \bmod N$，…，$\alpha_t = r_t^e * T_t' \bmod N$，其中 e 為 Alice 的公鑰，最後將$\{\alpha_1, \alpha_2, \dots, \alpha_t\}$傳回給 Alice。

Step 3. 接收到 Bob 傳送的$\{\alpha_1, \alpha_2, \dots, \alpha_t\}$後，Alice 利用自己的私鑰 d 來計算$\beta_1 = \alpha_1^d \bmod N$，$\beta_2 = \alpha_2^d \bmod N$，…，$\beta_t = \alpha_t^d \bmod N$，之後再將計算完的$\{\beta_1, \beta_2, \dots, \beta_t\}$傳送給 Bob。

Step 4. 收到從 Alice 傳回的訊息後，Bob 接著計算$d_1' = r_1^{-1} * \beta_1 \bmod N$，$d_2' = r_2^{-1} * \beta_2 \bmod N$，…，$d_t' = r_t^{-1} * \beta_t \bmod N$，最後再計算 $b_1 = C \bmod d_1'$，$b_2 = C \bmod d_2'$，…，$b_t = C \bmod d_t'$即可以成功得到想要的訊息。

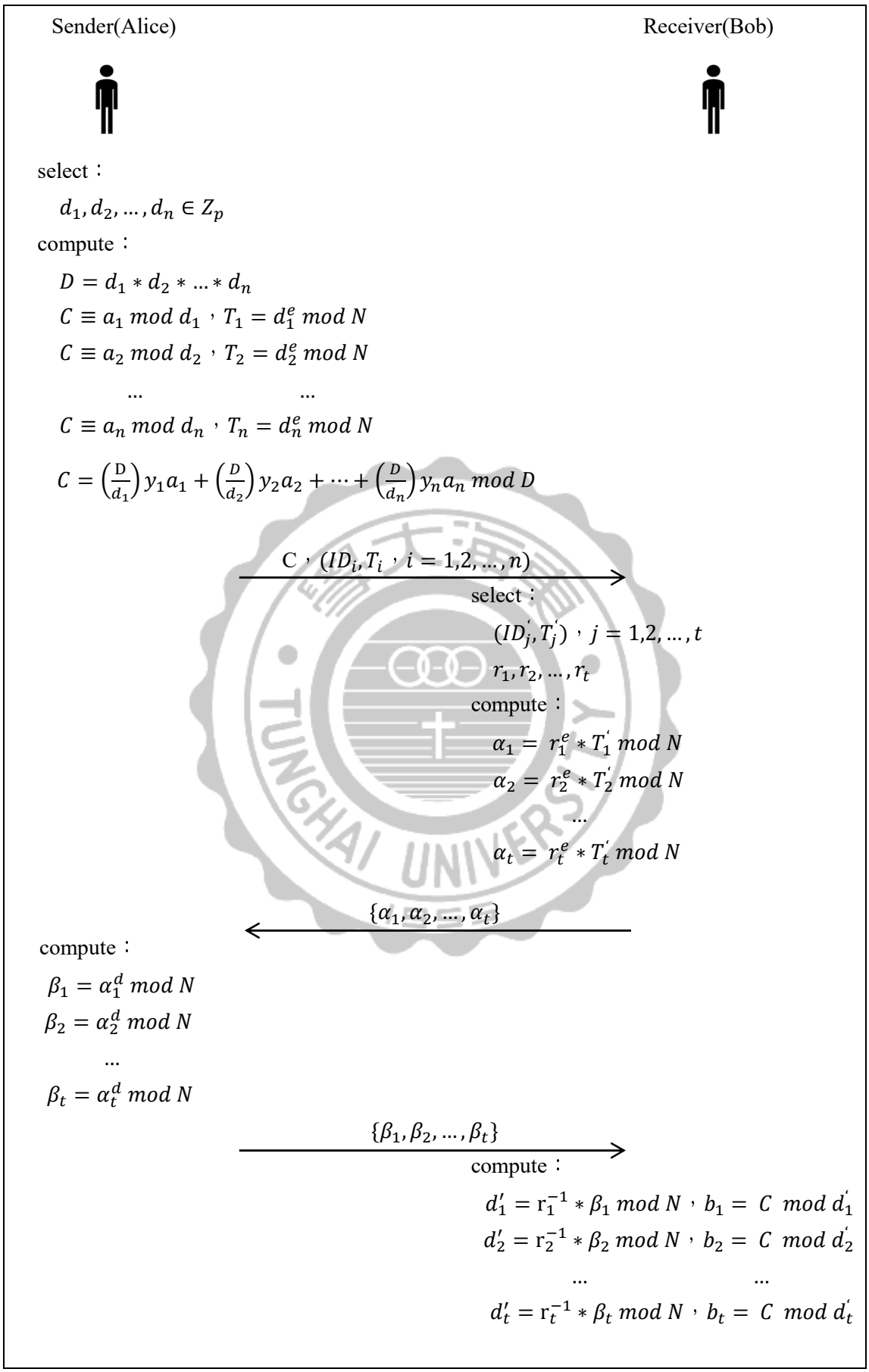

圖 2-1　Chang 與 Lee[7]提出的 n 選 t 模糊傳輸協定

二、 Chen 等人提出的 n 選 k 模糊傳輸協定

Chen 等人[9]提出的 n 選 k 模糊傳輸協定利用雙線性映射(Bilinear Pairing)的概念，建構一個安全且低消耗頻寬的 n 選 k 模糊傳輸協定，但與基於橢圓曲線密碼系統的模糊傳輸協定相比計算量還是稍嫌太大。

協定一開始先設定公開系統參數集合$\{G_1, G_2, q, P, e, H\}$，其中G_1是一個從級數為 q 的 P 產生的加法循環群，G_2是一個相同級數為 q 的乘法循環群，e 是一個雙線性配對函數 $e: G_1 * G_2 \rightarrow G_2$，$H$ 是一個單向的雜湊函數 $H\{0, 1\}$，Bob 是接收方，而 Alice 是傳送方。Chen 等人所提出的演算法[9]如圖 2-2 所示，訊息傳輸步驟如下：

Step 1. Bob 隨機選擇正整數 t、w 及s_i，$i = 1,2, \ldots, n$，接著計算$A_i = ws_i\mathrm{P}$，$i = 1,2, \ldots, n$，與$B_j = ts_{\sigma j}P$，$j = 1,2, \ldots, k$，以及$V = tP$，其中σ_j表示為 Bob 所選擇的 n 個隨機正整數s_i中的第 k 個指標，之後 Bob 再傳送A_1，$A_2, \ldots, A_n$，與B_1，$B_2, \ldots, B_n$，以及 V 給 Alice。

Step 2. Alice 收到 Bob 傳送的訊息後，隨即選擇正整數 r，並計算$C_i = m_i \oplus H(e(A_i, V)^r)$，$i = 1,2, \ldots, n$，與$D_j = rB_j$，$j = 1,2, \ldots, k$，接著再傳送$C_1$，$C_2$，…，$C_n$，以及$D_1$，$D_2$，…，$D_k$給 Bob。

Step 3. Bob 接收到C_1，C_2，…，C_n，與D_1，D_2，…，D_k後，計算$m_{\sigma j} = c_{\sigma j} \oplus H(e(D_j, P)^w$，Bob 即可取得選擇的到$m_{\sigma i}$。

接收方收到C_1，C_2，…，C_n，與D_1，D_2，…，D_k後，利用 k 個D_j解密出 n 個C_i，接收方就可以正確地取得 k 個訊息$m_{\sigma 1}, m_{\sigma 2}, \ldots, m_{\sigma k}$，計算如下：

$m_{\sigma j} = c_{\sigma j} \oplus H(e\big(D_j, P\big)^w = c_{\sigma j} \oplus H(e(rB_j, P)^w = c_{\sigma i} \oplus H(e(rts_{\sigma j}P, P)^w = c_{\sigma i} \oplus H(e(ws_{\sigma j}P, tP)^r = c_{\sigma i} \oplus H(e(A_{\sigma j}, V)^r$ 。

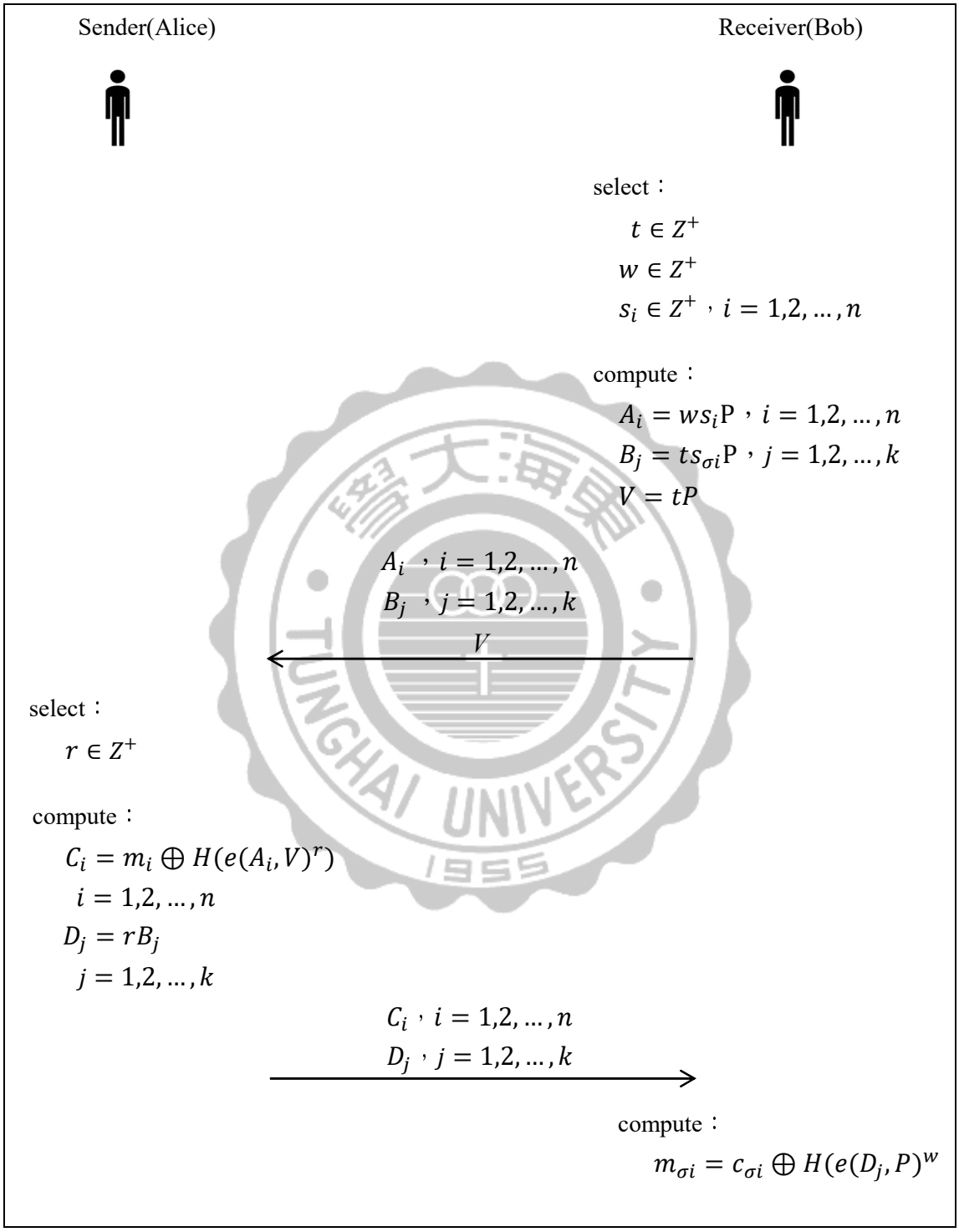

圖 2-2　Chen 等人[9]提出的 n 選 k 模糊傳輸協定

第五節　模糊傳輸協定之應用

模糊傳輸協定可以保護通訊者個人的隱私，以及確保訊息的完整性和機密性，因此被應用在提高網路雙方傳遞訊息時的安全通訊之環境，以下介紹五種在模糊傳輸協定上的應用。

一、私密資訊擷取

使用者可以透過資料庫來查詢最新的資訊，但會有洩漏個人隱私的風險，因為其他人可以按照使用者查詢的內容，來推斷使用者的個人資訊，為了確保使用者從資料庫中查詢一些資料區塊後，資料庫管理員無法知道他想查詢的是哪些資料區塊，以此保護使用者的隱私安全。換言之，私密資訊擷取(Private Information Retrieval, PIR)[10][12][13]是指資料庫儲存 n 筆資料，使用者想抓取其中 t 筆，而資料庫管理員無法得知使用者感興趣的資料是哪些。

PIR 分為 computational Private Information Retrieval(cPIR)與 secure hardware PIR[10]，cPIR 與 secure hardware PIR 的差異在於 cPIR 中資料庫的所有資料被儲存在同一台伺服器，當使用者使用資料庫時，cPIR 會讓伺服器無法得知使用者存取的資料為何，而 secure hardware PIR 是指伺服器中置入一個防竄改的中央處理器，當中央處理器接收到使用者存取資料的要求後，將資料轉為加密型式並回傳給使用者。

二、網路拍賣

網路拍賣(Online Auction)[1]是指消費者在網路上進行商品的交易，但由於網路是一個公開的環境，導致消費者可能會有隱私安全的問題，因此希望賣方在買方購買商品後，無法得知買方的任何訊息。假設網路賣家擁有 n 件商品，買家希望購入其中 t 件，而賣家無法得知買家購買的是哪些商品。假設買方先付給賣方預付款，接著買方為了取得總價值不超過預付款的數位商品和賣方進行互動。當

預付款花完，在買方重新支付預付款前，無法取得任何額外的商品，而賣方無法得知買賣當中金額的變動量與預付款總額，也無法得知買方的餘額和花費的金額。

三、個人健康紀錄

病歷的記載由傳統的紙本方式，轉變為電子病歷，但是此方式主要是將生理資訊提供給具醫療背景的醫護人員觀看。因此有個人健康紀錄(Personal Health Record, PHR)[8]的出現，期望病患自己管理自己的資訊。個人健康紀錄的合法使用者(例如：醫生、照護人員或使用者本身)選擇自己所想的資訊，而個人健康紀錄的雲端管理者能安全將個人健康紀錄的資訊回傳，然而管理者不會知道接收方的選擇，另一方面，使用者則除了所選擇的訊息之外，無法得知其他資訊。也就是說假設儲存在雲端的個人健康紀錄有 n 筆資訊，使用者希望從中讀取 t 筆資訊，而雲端管理者無法得知使用者讀取的資料為何，使用者也無法讀取其餘未選擇的資訊內容。

四、秘密整數的安全比較

秘密整數的安全比較(Secure Comparison of Secret Integers)[36]是假設 Alice 有一個祕密整數 a，Bob 有一個祕密整數 b，他們希望互相比較，但不希望透露出自己的秘密整數，也就是說 Alice 即使有無限的計算能力，也無法得知 Bob 的秘密整數 b，而 Bob 也無法得知 Alice 得秘密整數 a 為何。

第六節　基於橢圓曲線密碼系統之模糊傳輸協定

影響模糊傳輸協定效能的主要因素是運算成本，因此在 2006 年 Parakh[28]提出將橢圓曲線密碼系統應用到模糊傳輸協定，將以往模糊傳輸協定的指數運算轉換為點的加法、減法和乘法的運算，降低計算的複雜度與總訊息傳輸量，來達到提升整體的效能。此後，利用橢圓曲線的模糊傳輸協定被廣泛的討論，陸續有學者經研究後提出相關的傳輸協定[11][16][29][36]。以下對 Parakh[29]所提出的

2 選 1 模糊傳輸協定，與 Li[19]提出的 n 選 1 和 n 選 t 模糊傳輸協定做介紹：

一、 Parakh 提出的 2 選 1 模糊傳輸協定

Parakh[28]提出 2 選 1 的模糊傳輸協定，在橢圓曲線$E_p(a,b)$下，選出兩個相同 x 座標的點P_1、P_2，且$P_1 = -P_2$，再來 Alice 選擇兩個不相同的私密值s_0、s_1，並利用兩個私密值s_0、s_1分別產生出n_{A0}、n_{A1}，接著 Bob 從P_1、P_2中選擇一個點P_B，而可能發生的情況為$P_B = P_1$ 或 $P_B = P_2$。Parakh 所提出的演算法[28]如圖 2-3 所示，Alice 選擇私鑰n_{A0}、n_{A1}，以下為訊息傳輸步驟：

Step 1. Alice 將$(n_{A0}P_1 \ , \ n_{A1}P_2)$傳給 Bob。

Step 2. Bob 將訊息$\{n_BP_B \ , \ n_B(n_{A0}P_1) + R \ , \ n_B(n_{A1}P_2) + R \ , \ n_BR\}$傳給 Alice，其中$n_B$為Bob 的私鑰，$R$ 是 Bob 在橢圓曲線$E_p(a,b)$中隨機選擇的點。

Step 3. Alice 分別計算訊息$H_1 = n_{A0}[n_B(n_{A0}P_1) + R - n_{A0}(n_BP_B)]$ 與
$H_2 = n_{A1}[n_B(n_{A1}P_2) + R - n_{A1}(n_BP_B)]$。

Step 4. Alice 將$\{n_{A0}(n_BP_B) + H_1 \ , \ n_{A0}(n_BR) + P_{nA0} \ , \ n_{A1}(n_BP_B) + H_2 \ , \ n_{A1}(n_BR) + P_{nA1}\}$傳給 Bob。

其中P_{nA0}、P_{nA1}為 Alice 欲傳送給 Bob 的訊息，且各自對應n_{A0}與n_{A1}。必須於 Step2 時決定$P_B = P_1$ 或 $P_B = P_2$，在 Step4 後，Bob 在 Alice 傳送的兩組訊息中選取一組由 Bob 在 Step2 就已經決定所欲得到的訊息做運算。假設 Bob 所選擇的$P_B = P_1$，則 Bob 使用$\{n_{A0}(n_BP_B) + H_1 \ , \ n_{A0}(n_BR) + P_{nA0}\}$計算。

Step 5. Bob 計算$K = n_{A0}(n_BP_B) + H_1 - n_B(n_{A0}P_1) = H_1 = n_{A0}R$ 與
$P_{nA0} = n_{A0}(n_BR) + P_{nA0} - n_BK$。

若 Bob 選擇為$P_B = P_1$，因此$P_{nA0} = n_{A0}(n_BR) + P_{nA0} - n_BK = n_{A0}(n_BR) + P_{nA0} - n_B(n_{A0}R)$，表示 Bob 最後得到 Alice 的訊息$P_{nA0}$。

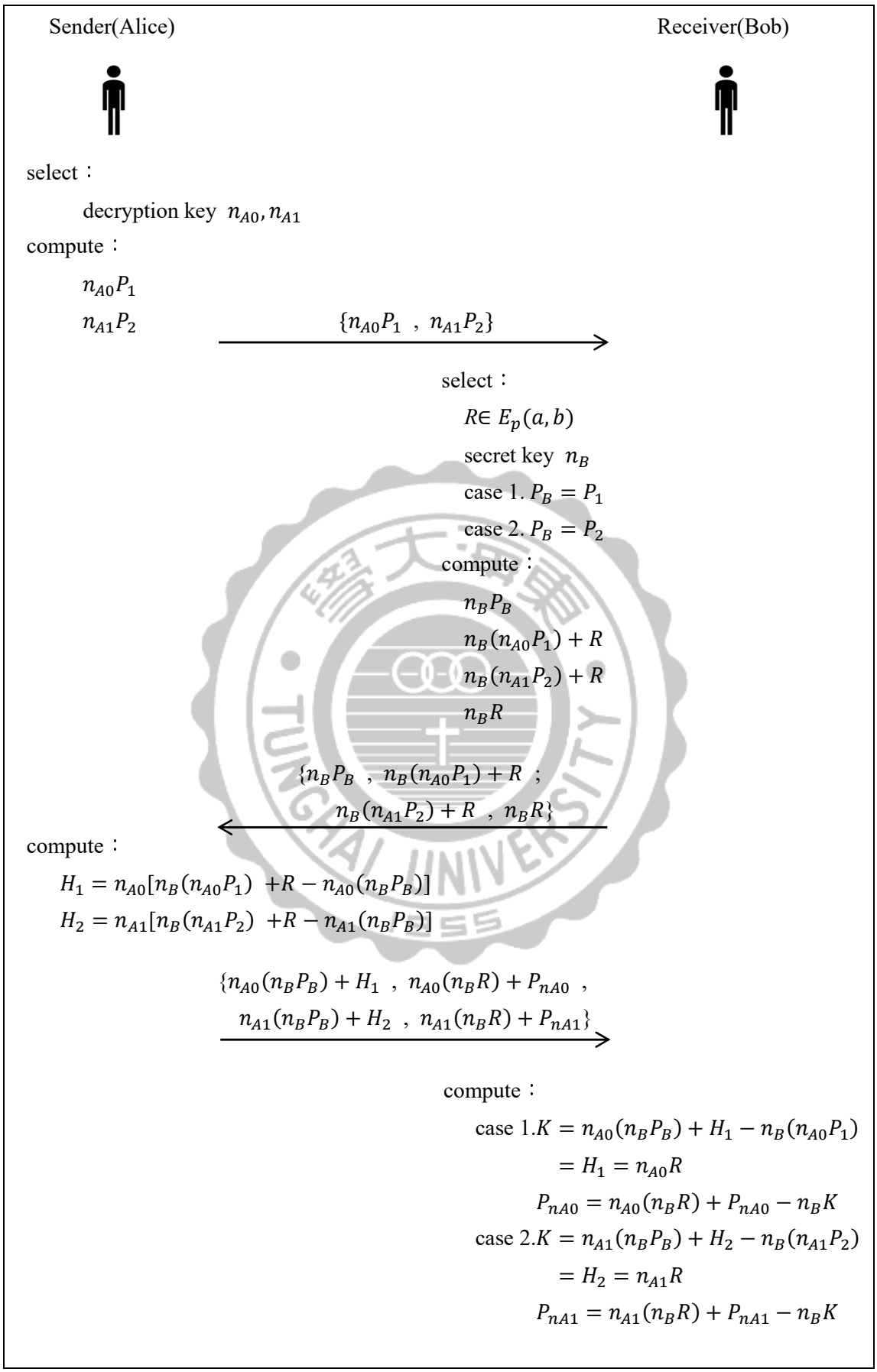

圖 2-3 Parakh[28]所提出的 2 選 1 模糊傳輸協定

二、 Li 提出的 n 選 1 模糊傳輸協定

Li[19]提出的 n 選 1 模糊傳輸協定首先設定 R 是一個大質數，橢圓曲線 $E_R(a,b)$其係數$a,b \in Z_R$，與變數$x,y \in Z_R$，P 為橢圓曲線上的點，q 表示為橢圓曲線的級數，且 q 是一個很大的值。

Alice 先在橢圓曲線上選擇 n 個點$P_{ai} \in E_R(a,b)$，$i = 1,2,\dots,n$，並將這 n 個點公開。Li 所提出的演算法[19]如圖 2-4 所示，以下為訊息傳輸步驟：

Step 1. Alice 隨機選擇 n 個私密值$s_i \in Z_q$，$i = 1,2,\dots,n$，並且計算s_iP_{ai}，$i = 1,2,\dots,n$。

Step 2. Alice 將s_iP_{ai}，$i = 1,2,\dots,n$，傳送給 Bob。

Step 3. Bob 隨機選擇 1 個私密值$r \in Z_q$，以及一個對照點$P_{ab} \in P_{ai}$，$i = 1,2,\dots,n$，$s_bP_{ab} \in s_iP_{ai}$，$b \in i$，$i = 1,2,\dots,n$，並從橢圓曲線上隨機選擇一個點$K \in E_R(\mathrm{a},\mathrm{b})$，接著計算$\mathrm{r}P_{ab}$ 及 $r(s_bP_{ab}) + rK$。

Step 4. Bob 傳送rP_{ab}以及$r(s_bP_{ab}) + rK$給 Alice。

Step 5. Alice 分別計算出$H_i = s_i[r(s_bP_{ab}) + rK - s_i(rP_{ab})]$，$i = 1,2,\dots,n$，以及$s_i(rP_{ab}) + H_i$和$H_i + P_{mi}$，$i = 1,2,\dots,n$。

Step 6. Alice 傳送$s_i(rP_{ab}) + H_i$，$H_i + P_{mi}$，$i = 1,2,\dots,n$等 2 個訊息給 Bob。

Step 7. 接收方計算$H_b = s_b(rP_{ab}) + H_b - r(s_bP_{ab})$與$P_{mb} = H_b + P_{mb} - H_b$。

上述協定的計算效能會優於基於離散對數問題 DLP(Discrete Logarithm Problem, DLP)和 Diffie-Hellman 判決問題 (Decisional Diffie-Hellman Problem, DDHP)的模糊傳輸協定，但訊息的總傳輸量會比較多，因此適用在計算能力弱且接收訊息總傳輸量較大的環境下，像是區域網路或是企業內部的網路。

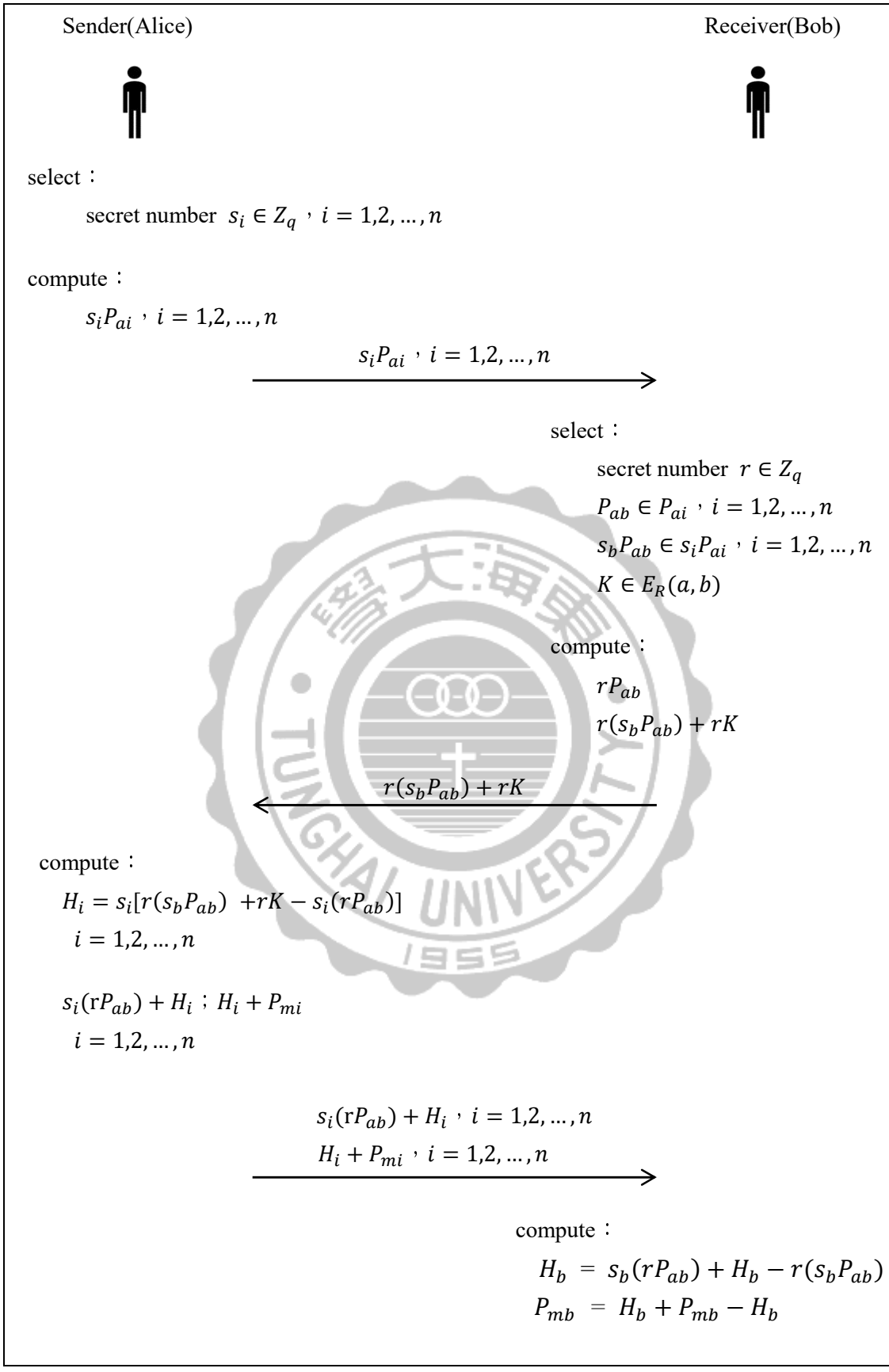

圖 2-4　Li[19]提出的 n 選 1 模糊傳輸協定

三、 Li 提出的 n 選 t 模糊傳輸協定

Li[19]提出的 n 選 t 模糊傳輸協定首先設定 R 是一個大質數，橢圓曲線 $E_R(a,b)$其係數$a,b \in Z_R$，與變數$x,y \in Z_R$，P 為橢圓曲線上的點，q 表示為橢圓曲線的級數，q 是一個極大的值。

Alice 先在橢圓曲線上選擇 n 個點$P_{ai} \in E_R(a,b)$，$i = 1,2,\dots,n$，並將這 n 個點公開。Li 所提出的演算法[19]如圖 2-5 所示，以下為訊息傳輸步驟：

Step 1. Alice 隨機選擇私密值$s \in Z_q$，在橢圓曲線上選擇一個點$P_{ac} \in E_R(a,b)$和 n 個點$P_{ai} \in E_R(a,b)$，$i = 1,2,\dots,n$，並計算$P_{cai} = P_{ai} + P_{ac}$，$i = 1,2,\dots,n$，以及$X_i = sP_{ai} + P_{mi}$，$i = 1,2,\dots,n$。

Step 2. Alice 將複合數對(P_{cai}, X_i)，$i = 1,2,\dots,n$，傳送給 Bob。

Step 3. Bob 隨機選擇 1 個私密值$r \in Z_q$，以及在橢圓曲線上選擇 2 組各 t 個點 $P_{bj} \in E_R(a,b)$，$j = 1,2,\dots,t$，$K_{bj} \in E_R(\mathrm{a,b})$，$j = 1,2,\dots,t$，$(P_{caj}, X_j) \in (P_{cai}, X_i)$，$i = 1,2,\dots,n$，$j = 1,2,\dots,t$，接著計算$W_j = P_{caj} + \mathrm{r}K_{bj}$，$j = 1,2,\dots,t$，與$Y_j = X_j + P_{bj}$，$j = 1,2,\dots,t$。

Step 4. Bob 傳送(K_{bj}, W_j, Y_j)，$j = 1,2,\dots,t$給 Alice。

Step 5. Alice 計算sK_{bj}，$j = 1,2,\dots,t$，與$Z_j = Y_j - s(W_j - P_{ac})$，$j = 1,2,\dots,t$。

Step 6. Alice 傳送(sK_{bj}, Z_j)，$j = 1,2,\dots,t$，給 Bob。

Step 7. Bob 計算$r(sK_{bj})$，$j = 1,2,\dots,t$，最後透過計算$P_{mj} = Z_j + r(\mathrm{s}K_{bj}) - P_{bj}$，$j = 1,2,\dots,t$，以獲得選擇的訊息$P_{mj}$。

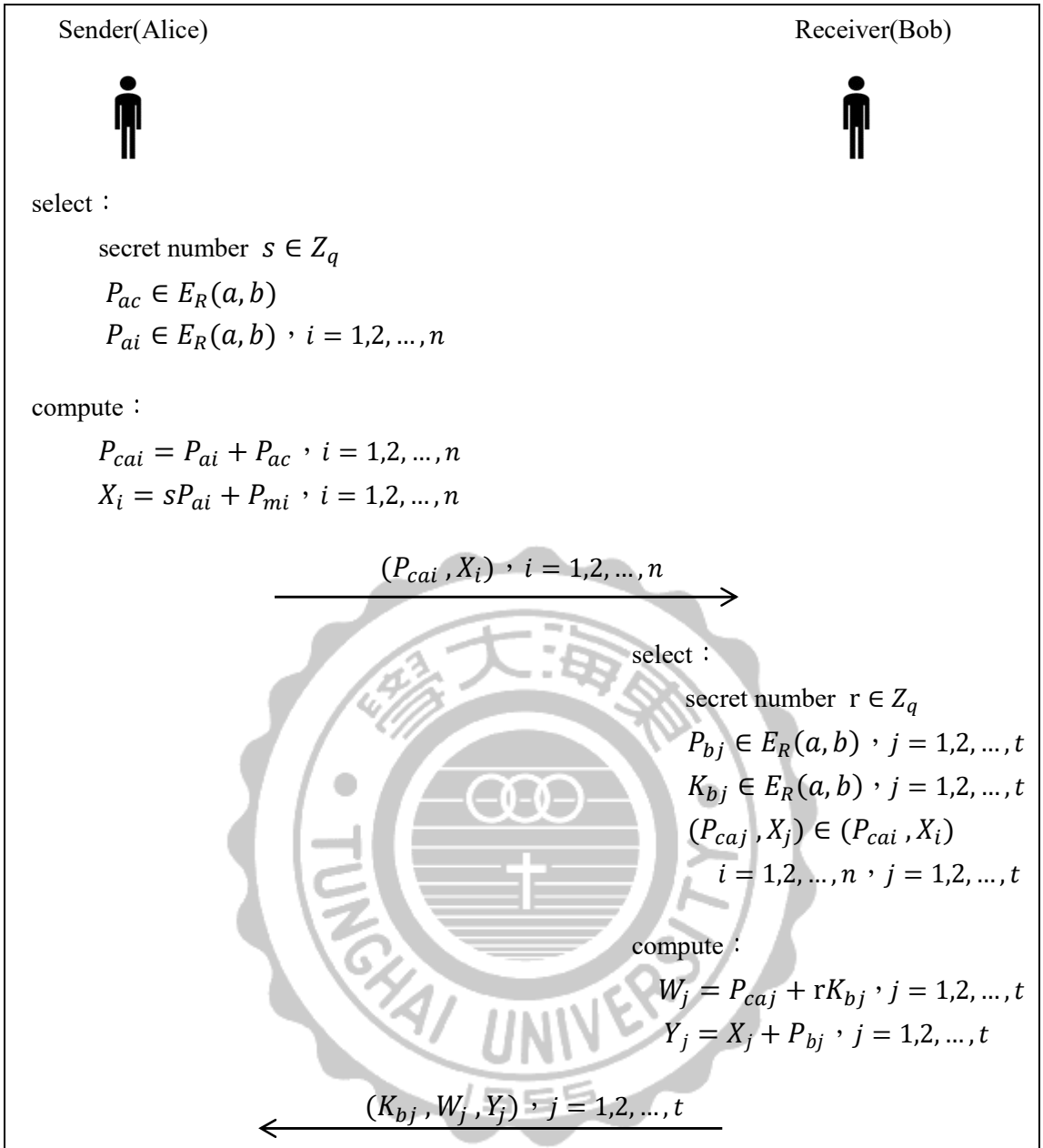

圖 2-5　Li[19]提出的 *n* 選 *t* 模糊傳輸協定

第三章　「先計算金鑰後加密訊息」的 n 選 t 模糊傳輸協定

非有即無模糊傳輸協定、2 選 1 模糊傳輸協定、n 選 1 模糊傳輸協定和 n 選 t 模糊傳輸協定的分類方式是按照傳送方擁有的訊息數以及接收方能夠選擇的訊息數來做分類，是目前最常見的分類方式。除了以訊息數做為分類依據，本研究按照加密訊息的先後，將模糊傳輸協定分為「先加密訊息後計算金鑰」與「先計算金鑰後加密訊息」兩種模式。

第一節　先加密訊息後計算金鑰

在「先加密訊息後計算金鑰」模式的傳輸協定中，傳送方將加密的訊息傳給接收方，接收方再將私鑰乘上欲解密的訊息，並回傳給傳送方，接著傳送方解密自己加密的訊息後，再傳給接收方，最後接收方解密自己加密的訊息，即可讀取選擇的訊息。此種模式是大多數模糊傳輸協定所用的模式，以 2007 年 Huang 與 Chang[16]提出的模糊傳輸協定為例，此協定利用雙鎖密碼系統的概念，提出一個低消耗頻寬的 n 選 t 模糊傳輸協定，而此協定僅需要 3 回的傳輸，且 Alice 只傳送$n+t$個訊息給接收方，而 Bob 只傳送 t 個訊息給傳送方，Huang 與 Chang 所提出的演算法[16]如圖 3-1 所示。

Alice 選擇一個大質數$q(q \cong 2^{160})$，橢圓曲線表示為E_q：$y^2 = x^3 + ax^2 + bx + c \ mod\, q$，而此方程式的判別式則表示為$\Delta = 27c^2 + 4a^3c + 4b^3 - a^2b^2 + 8abc \neq 0 \ mod\, q$，Alice 擁有的訊息 M_1, M_2, …, $M_n \in E_q$，假設E_q上的元素個數為N_q，P 表示為橢圓曲線E_q上的點，會使得$N_qP = O$，其中橢圓曲線E_q：$y^2 = x^3 + ax^2 + bx + c \ mod\, q$與$N_q$是公開的。以下為訊息傳輸步驟：

Step 1.　Alice 選擇私密值 a，使得$gcd(a,\ N_q) = 1$，並計算 $C_i = a\, M_i \ mod\, q$，$i = 1,2,\ldots,n$，再將 C_1, C_2, …, C_n 傳給 Bob。

Step 2. Bob 選擇私密值 b，使得$gcd(b,\ N_q)=1$，並選擇 $C_{i_1},\ C_{i_2},\ldots,\ C_{i_t}\in\{C_1,\ C_2,\ldots,\ C_n\}$，與計算 $P_{i_1}=\mathrm{b}C_{i_1}\ mod\ q$，$P_{i_2}=\mathrm{b}C_{i_2}\ mod\ q,\ldots,\ P_{i_t}=\mathrm{b}C_{i_t}\ mod\ q$，接著將 $P_{i_1},\ P_{i_2},\ldots,\ P_{i_t}$ 傳給 Alice，此處的 $P_{i_j}=bC_{i_j}=b\left(a\ M_{i_j}\right)\ mod\ q,\ j=1,2,\ldots,t$。

Step 3. Alice 取得$a^{-1}\ mod\ N_q$，計算 $Y_{i_j}=a^{-1}P_{i_j}\ mod\ q,\ j=1,2,\ldots,t$，將 Y_{i_j}，$j=1,2,\ldots,t$傳給 Bob。

Step 4. Bob 取得$b^{-1}\ mod\ N_q$，計算 t 個訊息$b^{-1}Y_{i_j}\ mod\ q,\ j=1,2,\ldots,t$，$b^{-1}Y_{i_j}$即為訊息$M_{i_j}\in\{M_1,\ M_2,\ \ldots,\ M_n\}$。

協定中 $C_i=a\ M_i\ mod\ q$，$gcd(a,\ N_q)=1$，訊息$M_{i_j}\in\{M_1,\ M_2,\ \ldots,\ M_n\}$，而 $P_{i_j}=\mathrm{b}C_{i_j}=b\left(a\ M_{i_j}\right)\ mod\ q=abM_{i_j}\ mod\ q$，$gcd(b,\ N_q)=1$，其中$a$、$b$分別為 Alice 和 Bob 所選擇的，並未公開，因此 Alice 透過計算$a^{-1}\ mod\ N_q$，以及 $Y_{i_j}=a^{-1}P_{i_j}\ mod\ q=a^{-1}\left(ab\ M_{i_j}\right)=bM_{i_j}\ mod\ q$，接著 Bob 計算$b^{-1}\ mod\ N_q$，與計算$b^{-1}Y_{i_j}\ mod\ q=b^{-1}\left(b\ M_{i_j}\right)=M_{i_j}$，$M_{i_j}\in\{M_1,\ M_2,\ \ldots,\ M_n\}$，Bob 即可取得所選擇的訊息。

Alice 無法得知 Bob 隨機選擇的整數b為何，也就無法得知 Bob 選擇哪些訊息，因此 Bob 接收到 Y_{i_j}後，可透過計算$b^{-1}Y_{i_j}\ =M_{i_j}\ mod\ q$來取得 t 個秘密訊息。此協定的安全性建立在解困難的橢圓曲線離散對數問題上，Bob 無法從$C_{i_j}=a\ M_{i_j}\ mod\ q$中得知$a$，也就無法利用計算$a^{-1}C_i$反推出其他訊息 M_i。

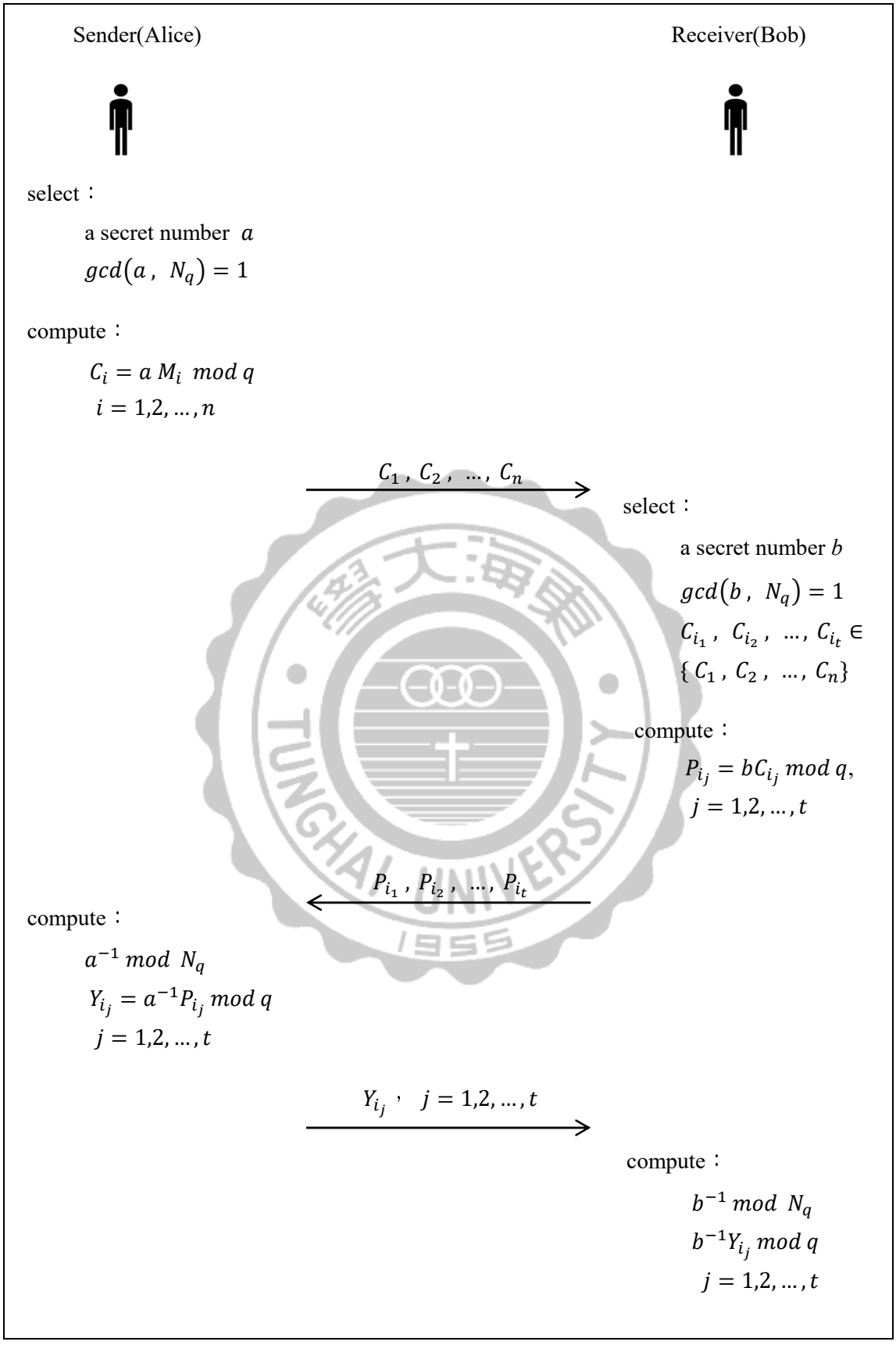

圖 3-1　Huang 與 Chang[16]所提出的 *n* 選 *t* 模糊傳輸協定

第二節　先計算金鑰後加密訊息

在「先計算金鑰後加密訊息」模式的傳輸協定中，接收方先依傳送方傳送的訊息計算出解密金鑰，而後進行訊息傳遞，傳送方再利用這些訊息計算出加密金鑰，並利用加密金鑰加密所擁有的訊息，最後由接收方再利用解密金鑰解出所選擇的訊息。在此模式下 Li[19]和 Parakh[29]分別提出 n 選 1 的模糊傳輸協定，在此以 2012 年 Parakh[29]所提出的 n 選 1 模糊傳輸協定為例來說明，其概念如下：

橢圓曲線表示為$E_R(a,b)$：$y^2 \bmod p = (x^3 + ax + b) \bmod p$，其中橢圓曲線$E_R(a,b)$的係數$a$和$b$、變數$x$和$y$為介於$0 \sim p-1$中的正整數，假設橢圓曲線上的點$T = (x_1, y_1)$ 和級數 r，會滿足$rT = O$，且級數 r 是一個很大的值，橢圓曲線上的基點表示為 G。傳送方擁有 n 個秘密字串s_0, s_1,…, s_{n-1}，接收方的選擇表示為$\sigma \in \{0,1,\ldots,n-1\}$，Parakh 所提出的演算法[29]如圖 3-2 所示，以下為傳輸步驟：

Step 1.　Alice 在橢圓曲線上選擇點 $C = P$。

Step 2.　Alice 隨機選擇一個私密值 r，且計算rG 。

Step 3.　Alice 傳送C和rG給 Bob。

Step 4.　Bob 隨機選擇一個私密值 k，且設定$PK_\sigma = kG$ 。

Step 5.　Bob 計算解密金鑰 $krG = \sigma C - PK_\sigma$。

Step 6.　如果$\sigma \neq 0$，Bob 計算$PK_0 = \sigma C - PK_\sigma$ 。

Step 7.　Bob 傳送PK_0給 Alice。

Step 8.　Alice 計算rPK_0，且計算$rPK_i = riC - rPK_0$，$1 \leq i \leq n-1$。

Step 9.　Alice 利用金鑰rPK_i加密字串s_i，並表示為$E(s_i)$，並傳送給 Bob。

Step 10.　Bob 選擇$E(s_\sigma)$，並利用解密金鑰rPK_σ解密出s_σ。

當$\sigma = i$，$rPK_i = riC - rPK_0 = r\sigma C - r\sigma C - rPK_\sigma = rPK_\sigma$

當$\sigma \neq i$，Bob 無法得到任何訊息

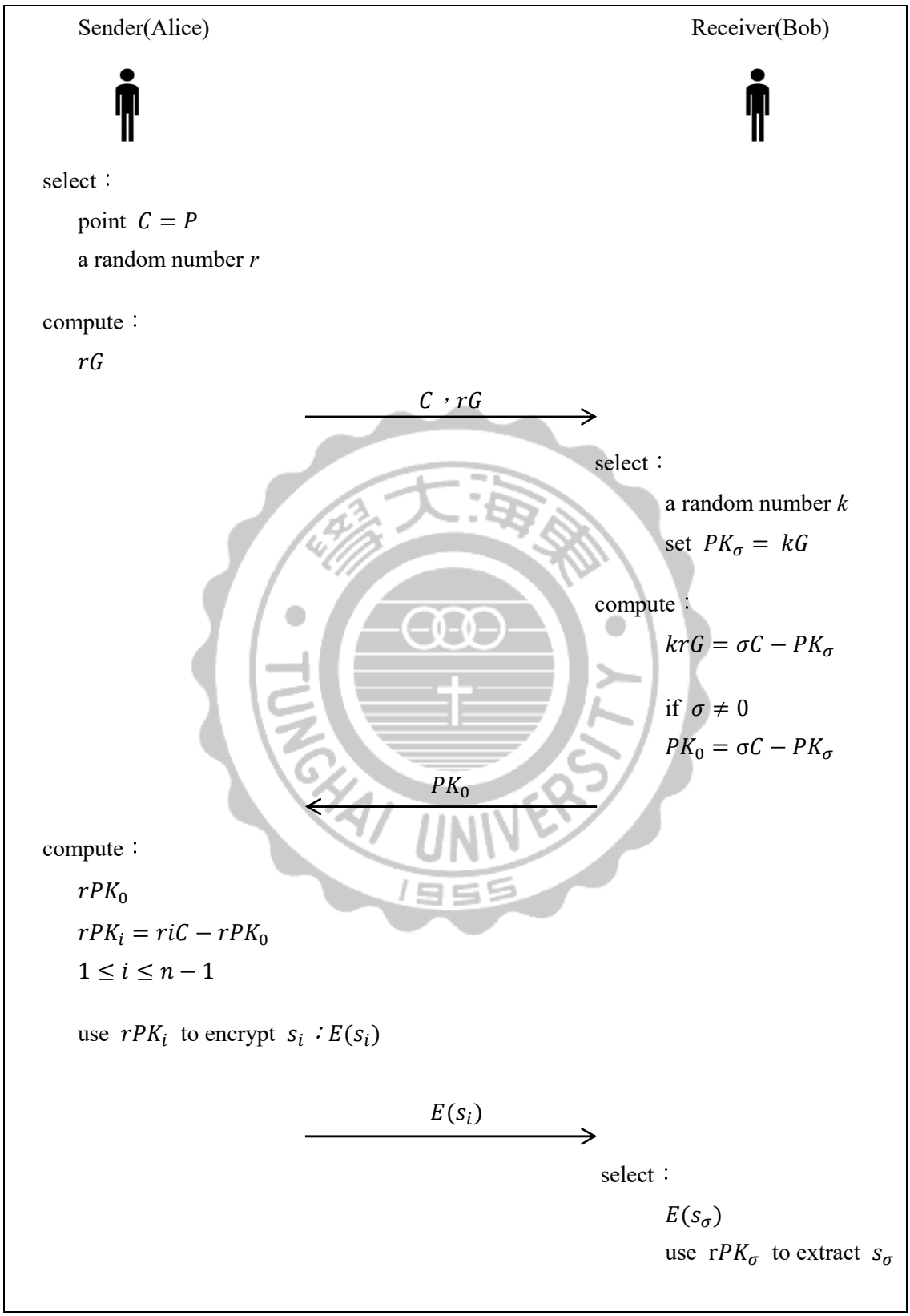

圖 3-2　Parakh[29]所提出的 n 選 1 模糊傳輸協定

第三節　Cantor 配對函數

在數學中配對函數(Pairing Function)是將兩個自然數映射到唯一的自然數的方式，表示為$\boldsymbol{P:N\times N\rightarrow N}$，可以在集合理論被用來證明整數和有理數具有相同的基數，且為自然數。Cantor 配對函數(Cantor Pairing Function)[6]是一種配對函數，兩個非負整數映射到唯一的非負整數，定義如下：

$$P(x,y)=\frac{(x+y)^2+3x+y}{2}$$

在實際應用上，為了將數據壓縮或者協議不允許分別傳送多個不同的值，可能就有必要對兩個值進行編碼成一個，而最簡單的方式就是利用 Cantor 配對函數將兩個整數轉為單一值。例如：當 $x=3$，$y=5$ 時，$P(3,5)=\frac{(3+5)^2+3\times3+5}{2}=39$，在表 3-1 列出 Cantor 配對函數起始階段的值：

表 3-1　Cantor 配對函數起始階段的值

$P(x,y)$	0	1	2	3	4	5	6	7	8	…
0	0	1	3	6	10	15	21	28	36	…
1	2	4	7	11	16	22	29	37	46	…
2	5	8	12	17	23	30	38	47	57	…
3	9	13	18	24	31	39	48	58	69	…
4	14	19	25	32	40	49	59	70	82	…
5	20	26	33	41	50	60	71	83	96	…
6	27	34	42	51	61	72	84	97	111	…
7	35	43	52	62	73	85	98	112	127	
8	44	53	63	74	86	99	113	128	144	
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮			⋮

為了清楚說明 Cantor 配對函數的演算機制，在此特別呈現 *C#*的程式碼，由於 Cantor 配對函數是一個可逆的函數，因此程式碼包含兩個自然數映射到唯一的自然數，以及將單一值反向映射回原來兩個自然數的過程。Cantor 配對函數的

計算複雜度是 $O(1)$，若在 64 位元作業系統與 2GHz 處理器的桌上型上執行 Cantor 配對函數程式只需花 0.00022355 秒，程式碼表示如下：

```
static int CantorPairFuntion(short x, short y)
 {
     return ((x + y) * (x + y ) + 3x + y) / 2;
 }
 static short[] Reverse(int n)
 {
     short[] pairnumber = new short[2];
     int t = (int)Math.Floor((-1D + Math.Sqrt(1D + 8 * n))/2D);
     int x = t * (t + 3) / 2 - n;
     int y = n - t * (t + 1) / 2;
     pair[0] = (short)x;
     pair[1] = (short)y;
     return pairnumber;
 }
```

由於輸入的兩個值有可能是很大的整數，程式在將這兩個很大的整數映射成單一值的時候會有溢位的問題，因此將程式碼進行修改，使其可以適用於任何非負整數，並表示如下：

```
static    ulong CantorPair( uint x, uint y)
            {
                if (x >= y)
                {
                    return ( ulong )x * x + x + y;
                }
                else
                {
                    return ( ulong )y * y + x;
                }
            }
```

```
static    uint [] CantorReverse（ULONG Z）
{
      UINT [] pair = new uint [ 2 ];
      double preciseN = Math.Sqrt(n);
      ulong floor = ( ulong )Math.Floor(preciseN);
      if (floor * floor > n)
      {
            floor -- ;
      }
      ulong t = n - ( ulong )(floor * floor);
      if (t < floor)
      {
            pair[ 0 ] = ( uint )t;
            pair[ 1 ] = ( uint )floor;
      }
      else
      {
            pair[ 0 ] = ( uint )floor;
            pair[ 1 ] = ( uint )t - ( uint )floor;
      }
      return pair;
}
```

第四節　基於橢圓曲線密碼系統之「先計算金鑰後加密訊息」的 *n* 選 *t* 模糊傳輸協定

模糊傳輸協定發展至今，「先加密訊息後計算金鑰」之模式已有學者將 *n* 選 1 的模糊傳輸協定延伸為 *n* 選 *t* 的模糊傳輸協定，例如 Huang 與 Chang[16]，但「先計算金鑰後加密訊息」之模式至今仍只有 *n* 選 1 的模糊傳輸協定，尚未有學者提出 *n* 選 *t* 的模糊傳輸協定，因此本研究以 2012 年 Parakh[29]所提出的 *n* 選 1 模糊傳送協定為基礎，推導出 *n* 選 *t* 的版本，下表為本文提出的演算機制會使用到的符號定義：

表 3-2　本文所使用的符號定義

符號	說明
$E_p(a,b)$	代表一個有限體的橢圓曲線，係數 a、b 與變數 x、y 為介於0~$p-1$的整數
$P(\bullet)$	Cantor 配對函數
C	代表橢圓曲線$E_p(a,b)$上的點
G	代表橢圓曲線$E_p(a,b)$上的基點
r	Alice 的私密值
m	Alice 的私密值
rPK_i	Alice 的加密金鑰
s_i	Alice 擁有的 n 個訊息，$i=1,\dots,n$
$E(s_i)$	Alice 加密後的 n 個訊息，$i=1,\dots,n$
k_{d_j}	Bob t 個欲選擇項目的私密值，$j=1,2,\dots,t$
rPK_{d_j}	Bob 的解密金鑰
$E(s_j)$	Bob 選擇的 t 個加密訊息，$j=1,\dots,t$
s_j	Bob 解密出的 t 個訊息

一、 訊息傳輸步驟

設定 p 是一個大質數，橢圓曲線表示為$E_p(a,b)$：$y^2=x^3+ax+b \ mod\ p$，其中 a, b, x, y 為0~$p-1$間的整數值，G 是橢圓曲線$E_p(a,b)$的基點(Base Point)，而橢圓曲線$\mathrm{E_p}(a,b)$和基點 G 為 Alice 和 Bob 所知的。本研究的演算法如圖 3-3 所示，以下為訊息傳輸步驟：

Step 1. Alice 從橢圓曲線$E_p(a,b)$上任意選擇一個點$C = P$。

Step 2. Alice 選擇私密值m與r，m與$r \in Z_p$，並計算mG、rG。

Step 3. Alice 將C、mG和rG傳送給 Bob。

Step 4. Bob 選擇私密值k_d，$d = 1,2,\dots,n$，$k_d \in Z_p$，並設定$PK_d = k_d G$。其中 t 個欲選擇項目的k_d表示為k_{d_j}，$j = 1,2,\dots,t$，以及其相對應的PK_d表示為$PK_{d_j} = k_{d_j} G$。

Step 5. Bob 利用 Cantor 配對函數 $P{:}Z \times Z \to Z$來計算$\mathrm{P}(PK_d) = V_d \in Z$，$d = 1,2,\dots,n$，其中 t 個欲選擇項目的V_d分別表示為$V_{d_j} = V_{d_1}, V_{d_2}, \dots, V_{d_t} \in \{V_1, V_2, \dots, V_n\}$。

Step 6. Bob 計算$rPK_{d_j} = k_{d_j} rG$，$j = 1,2,\dots,t$，rPK_{d_j}即為解密金鑰。

Step 7. Bob 計算$W_d = dC - PK_d + \prod_{j=1}^{j=t} \left(P(PK_d) - V_{d_j}\right) \cdot mG$，

$d = 1,2,\dots,n$，$j = 1,2,\dots,t$。

Step 8. Bob 將所有的W_d，$d = 1,2,\dots,n$傳送給 Alice。

Step 9. Alice 計算加密金鑰 $rPK_i = riC - rW_i$，$i = 1,2,\dots,n$。

Step 10. Alice 以rPK_i作為加密金鑰來加密訊息s_i，並表示為$E(s_i)$，$i = 1,2,\dots,n$，並將加密後的訊息傳送給 Bob。

Step 11. Bob 選擇$E(s_j)$，且以rPK_{d_j}解密出想要的訊息s_j，此時只有被選取的 t 個訊息的內容可以分別被解密並讀取。

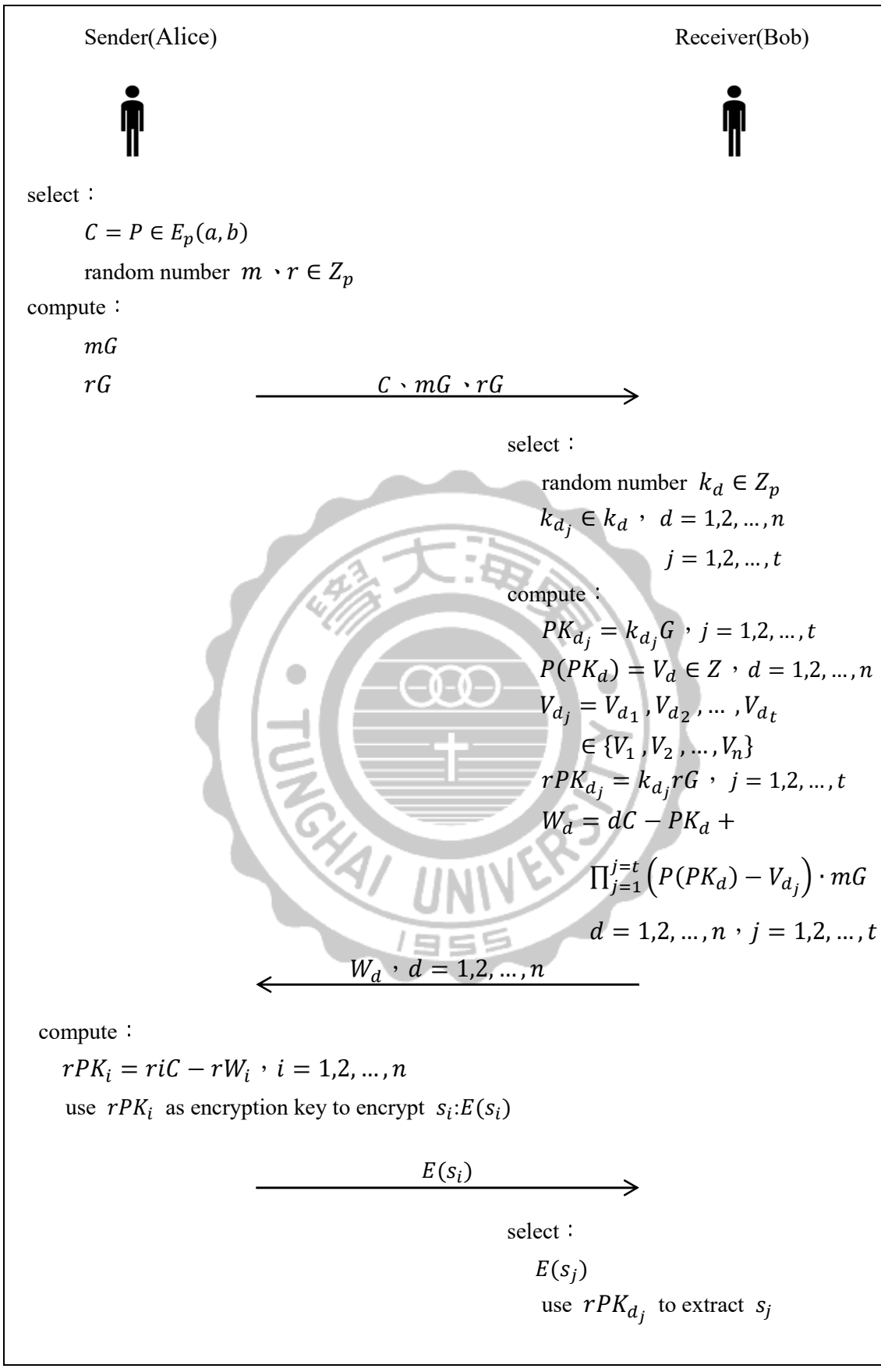

圖 3-3　本研究提出的 n 選 t 模糊傳輸協定

二、 安全性分析

模糊傳輸協定須符合正確性、傳送方及接收方隱私安全，分別解釋如下：

(一)、 正確性(Correctness)：

若 Alice 和 Bob 都遵循協議，協定完成後 Bob 可以利用解密金鑰解出選擇的 t 個訊息。以下假設$n=3$，$t=2$，以 3 取 2 的模糊傳輸協定來做正確性的驗證：

Step 1. Alice 從橢圓曲線$E_p(a,b)$上任意選擇一個點$C=P$。

Step 2. Alice 選擇私密值m與r，m與$r \in Z_p$，並計算mG、rG。

Step 3. Alice 將C、mG和rG傳送給 Bob。

Step 4. Bob 選擇私密值k_1、k_2、k_3，並設定$PK_1=k_1G$、$PK_2=k_2G$、$PK_3=k_3G$。其中 2 個欲選擇項目的$k_{d_1}=k_1$、$k_{d_2}=k_3$，其相對應$PK_1=PK_{d_1}=k_{d_1}G$、$PK_3=PK_{d_2}=k_{d_2}G$。

Step 5. Bob 計算$\mathrm{P}(PK_1)=V_1 \in Z$、$\mathrm{P}(PK_2)=V_2 \in Z$、$\mathrm{P}(PK_3)=V_3 \in Z$，其中 2 個欲選擇項目的$V_{d_1}=V_1$、$V_{d_2}=V_3$。

Step 6. Bob 計算解密金鑰$k_{d_1}rG=rPK_{d_1}$、$k_{d_2}rG=rPK_{d_2}$。

Step 7. Bob 計算$W_1=1\cdot C-PK_1+\left(P(PK_1)-V_{d_1}\right)\cdot mG$

$$=C-PK_1+(V_1-V_1)\cdot mG=C-PK_{d_1}-O=C-PK_{d_1}$$

$$W_2=2\cdot C-PK_2+\left(P(PK_2)\right)\cdot mG$$

$$=2\mathrm{C}-PK_2+mGV_2$$

$$W_3=3\cdot C-PK_3+\left(P(PK_3)-V_{d_2}\right)\cdot mG$$

$$=3C-PK_3+(V_3-V_3)\cdot mG=3C-PK_{d_2}-O=3C-PK_{d_2}。$$

Step 8. Bob 將W_1、W_2、W_3傳送給 Alice。

Step 9. Alice 計算加密金鑰 $rPK_1 = r1C - rW_1$

$$rPK_2 = r2C - rW_2$$

$$rPK_3 = r3C - rW_3 \quad 。$$

Step 10. Alice 以加密金鑰來加密訊息，並將加密後的訊息$E(s_1)$、$E(s_2)$、$E(s_3)$傳送給 Bob。

Step 11. Bob 以rPK_{d_1}、rPK_{d_2}解密出想要的訊息s_1、s_3，此時只有被選取的 2 個訊息的內容可以分別被解密並讀取。

由上述協定 $rPK_1 = r1C - rW_1 = rC - r\left(C - PK_{d_1}\right) = rPK_{d_1}$

$$rPK_2 = r2C - rW_2 = 2rC - r(2\mathrm{C} - PK_2 + \ mGV_2) = rPK_2 + rmGV_2$$

$$rPK_3 = r3C - rW_3 = 3rC - r\left(3C - PK_{d_2}\right) = rPK_{d_2}$$

可知 $rPK_1 = rPK_{d_1}$、$rPK_3 = rPK_{d_2}$，因此 Bob 可以解出所選擇的 2 個訊息。

(二)、 傳送方的隱私安全(Sending Privacy)：

此協定中接收方(Bob)若想取得其餘未選擇的$n - t$個訊息，必須由 $rPK_i = riC - rW_i$，$i = 1,2, \dots, n$中求得 rPK_i，接收方雖然知道C、mG和rG，但基於橢圓曲線離散對數問題，無法反推出 r、m 為何，因此確保了傳送方(Alice)的隱私。

(三)、 接收方的隱私安全(Receiving Ambiguity)：

此協定中，接收方(Bob)只傳送了W_d給傳送方(Alice)，若傳送方想要得知接收方選擇哪些訊息，必須分解出W_d中的V_{d_j}，但傳送方沒有足夠的條件去分解出V_{d_j}，而且在W_d中還有利用 Cantor 配對函數的概念，增加計算的複雜度，因此傳送方無法得知接收方選擇哪 t 個訊息，確保了接收方的隱私安全。

三、 效能分析

由於本論文提出的協定導入橢圓曲線密碼系統，藉由點的運算取代以往的指數運算達到大幅降低協定的計算量，因此僅針對訊息傳輸量進行分析。表 3-3 為本研究提出 n 選 t 模糊傳輸協定，假設 $t = 1$ 時，與其他 n 選 1 模糊傳輸協定訊息傳輸量的比較表。本研究提出的協定在傳送方訊息的傳輸量遠比其他協定還要來的少，但接收方的訊息傳輸量卻較多，總傳輸量與其他協定差不多，但本協定的訊息傳輸量會少於同樣基於橢圓曲線密碼系統 Li[19]的模糊傳輸協定。

表 3-3 訊息傳輸量比較表

	傳送方 訊息傳輸量	接收方 訊息傳輸量	總傳輸量
Naor[26]	$2n$	1	$2n+1$
Tzeng[35]	$2n$	1	$2n+1$
Li[19]	$3n$	2	$3n+2$
本協定	$n+3$	n	$2n+3$

表 3-4 為本研究提出的 n 選 t 模糊協定與其他學者提出的 n 選 t 模糊傳輸協定之訊息傳輸量比較表，由表 3-4 可發現本論文提出的協定與同為利用橢圓曲線密碼系統 Huang 與 Chang[16]提出的協定相比，傳送方擁有的訊息數 n 與接收方選擇的訊息數 t 為正整數，且 t 介於 0 到 n 之間，在$\boldsymbol{t > \frac{n+3}{2}}$的情況下，本協定的總訊息傳輸量會較少。

表 3-4 訊息傳輸量比較表

	傳送方 訊息傳輸量	接收方 訊息傳輸量	總傳輸量
Huang 與 Chang[16]	$n+t$	t	$n+2t$
Wu 與 Zhang[36]	$n+t$	t	$n+2t$
Li[19]	$2n+2t$	$3t$	$2n+5t$
本協定	$n+3$	n	$2n+3$

第四章　Cantor 配對函數應用於模糊傳輸協定之延伸討論

由訊息傳輸量比較表可發現本研究提出的「先計算金鑰後加密訊息」模式的 *n* 選 *t* 模糊傳輸協定的總訊息傳輸量仍比一般「先加密訊息後計算金鑰」模式的 *n* 選 *t* 模糊傳輸協定還要來的多，因此進一步討論將 Cantor 配對函數分別應用至兩種模式的模糊傳輸協定上，以降低整體的訊息傳輸量，並對兩者進行比較。

第一節　Cantor 廣義 *n* 元雙映射配對函數

Cantor 廣義 *n* 元雙映射配對函數(Generalized Cantor *n*-tupling Bijection)[32]是由 Cantor 配對函數推廣而來，從兩個自然數映射到一個自然數，增加為 n 個自然數映射到一個自然數，不變的是映射出來的數值都具有唯一性，以及可逆推的特性，定義為：$K_n : N^n \to N$。更精確的說，在N^2的整數坐標軸上之反對角線配對函數$x_1 + x_2 = C$的數列可以被映射到整數坐標軸上的超平面$x_1 + x_2 + \cdots + x_k = C$的點上，與 2007 年 Lisi[19]所推導證明出的公式稍微不一樣但是會得到相同的結果，則雙映射函數K_n公式定義如下：

$$K_n(x_1, \ldots, x_n) = \sum_{k=1}^{n} \binom{k - 1 + x_1 + \cdots + x_k}{k}$$

由上式$K_n(x_1, \ldots, x_n)$定義的 Cantor 廣義 n 元雙映射配對函數是一組 n 次多項式的參數，根據 1999 年 Cegielski 和 Richard[5]和 1923 年 Fueter 和 Polya[14]的推測認為這一組 n 次多項式是 1 到 n 的排列。其中$\binom{n}{k}$也被稱為二項式係數，表示在 n 個元素的集合中，擁有任意 k 個元素的子集組合以及x^k在二項式$(x + y)^n$的擴展係數。

第二節　基於 Cantor 配對函數之模糊傳輸協定

為了降低模糊傳輸協定的整體訊息傳輸量，本文將 Cantor 廣義 n 元雙映射配對函數的概念應用至「先加密訊息後計算金鑰」與「先計算金鑰後加密訊息」兩種模式之模糊傳輸協定上，前者以 Huang 與 Chang[16]為例，後者以本研究提出的 n 選 t 模糊傳輸協定為例，並討論兩者的總訊息傳輸量。

一、「先加密訊息後計算金鑰」之模糊傳輸協定

將 Cantor 廣義 n 元雙映射配對函數應用至 Huang 與 Chang[16]提出的 n 選 t 模糊傳輸協定後的演算法如圖 4-1 所示，其概念如下：

橢圓曲線表示為$E_q: y^2 \equiv x^3 + ax^2 + bx + c \ mod\, q$，Alice 擁有的訊息表示為 $M_1, M_2, \ldots, M_n \in E_q$，假設$E_q$上的元素個素為$N_q$，$P$ 表示為橢圓曲線E_q上的點，會使得$N_q P = O$，其中橢圓曲線$E_q: y^2 \equiv x^3 + ax^2 + bx + c \ mod\, q$與$N_q$是公開的。

Step 1. Alice 選擇私密值 a，使得$gcd(a, N_q) = 1$，並計算 $C_i = a\, M_i \ mod\, q$，$i = 1,2, \ldots, n$，再將 $C_1, C_2, \ldots, C_n$ 傳給 Bob。

Step 2. Bob 選擇私密值 b，使得$gcd(b, N_q) = 1$，並選擇 $C_{i_1}, C_{i_2}, \ldots, C_{i_t} \in \{C_1, C_2, \ldots, C_n\}$，計算 $P_{i_1} = bC_{i_1} \ mod\, q$，$P_{i_2} = bC_{i_2} \ mod\, q, \ldots, P_{i_t} = bC_{i_t} \ mod\, q$，以及利用 Cantor 廣義 n 元雙映射配對函數$P_n: Z_1 \times Z_2 \times \ldots \times Z_n \to Z$來計算$P_n\left(P_{i_j}\right)$，$j = 1,2, \ldots, t$。

Step 3. 接收方利用傳送方的公鑰K_{pA}對$P_n\left(P_{i_j}\right)$加密，表示為$E_A\left(P_n\left(P_{i_j}\right)\right)$，並將$\left\{\mathrm{t}, E_A\left(P_n\left(P_{i_j}\right)\right)\right\}$傳給傳送方。

Step 4. Alice 利用自己的私鑰K_{sA}解密$E_A\left(P_n\left(P_{i_j}\right)\right)$得出$P_n\left(P_{i_j}\right)$，並透過計算$P_n\left(P_{i_j}\right)$還原出 P_{i_j}，$j = 1,2,\ldots,t$。

Step 5. Alice 取得$a^{-1}\ mod\ N_q$，計算 $Y_{i_j} = a^{-1}P_{i_j}\ mod\ q$， $j = 1,2,\ldots,t$，以及計算$P_n\left(Y_{i_j}\right)$，並利用 Bob 的公鑰K_{pB}加密$P_n\left(Y_{i_j}\right)$：$E_B\left(P_n\left(Y_{i_j}\right)\right)$，再將$\left\{t\ , E_B\left(P_n\left(Y_{i_j}\right)\right)\right\}$傳給 Bob。

Step 6. Bob 利用自己的私鑰K_{sB}解密$E_B\left(P_n\left(Y_{i_j}\right)\right)$得出$P_n\left(Y_{i_j}\right)$，並透過計算$P_n\left(Y_{i_j}\right)$反推出 Y_{i_j}，$j = 1,2,\ldots,t$。

Step 7. Bob 取得$b^{-1}\ mod\ N_q$，計算 t 個訊息$b^{-1}Y_{i_j}\ mod\ q$， $j = 1,2,\ldots,t$，而$b^{-1}Y_{i_j}$即為訊息$M_{i_j} \in \{M_1, M_2, \ldots, M_n\}$。

二、 「先計算金鑰後加密訊息」之模糊傳輸協定

將 Cantor 廣義 n 元雙映射配對函數應用至本研究提出的 n 選 t 模糊傳輸協定後的演算法如圖 4-2 所示，其概念如下：

設定 p 是一個大質數，橢圓曲線表示為$E_p(a,b)$：$y^2 = x^3 + ax + b\ \ mod\ p$，其中係數 a、b 與變數 x、y 為$0 \sim p-1$間的整數值，G 是橢圓曲線$E_p(a,b)$的基點，而橢圓曲線$\mathrm{E_p}(a,b)$和基點 G 為 Alice 和 Bob 所知的。

Step 1. Alice 從橢圓曲線$E_p(a,b)$上任意選擇一個點$C = P$。

Step 2. Alice 選擇私密值m與r，m與$r \in Z_p$，並計算mG、rG。

Step 3. Alice 將C、mG和rG傳送給 Bob。

Step 4. Bob 選擇私密值k_d，$d = 1,2,\ldots,n$，$k_d \in Z_p$，並設定$PK_d = k_dG$。其中

t 個欲選擇項目的$k_d = k_{d_j}$，$j = 1,2,\dots,t$，以及其相對應的PK_d表示為$PK_{d_j} = k_{d_j}G$。

Step 5. Bob 利用配對函數 $P{:}Z \times Z \to Z$來計算$\mathrm{P}(PK_d) = V_d \in Z$，$d = 1,2,\dots,n$，其中 t 個欲選擇項目的V_d分別表示為$V_{d_j} = V_{d_1}, V_{d_2}, \dots, V_{d_t} \in \{V_1, V_2, \dots, V_n\}$。

Step 6. Bob 計算解密金鑰$k_{d_j}rG = rPK_{d_j}$，$j = 1,2,\dots,t$。

Step 7. Bob 計算$W_d = dC - PK_d + \prod_{j=1}^{j=t}\left(P(PK_d) - V_{d_j}\right) \cdot mG$，

$d = 1,2,\dots,n$，$j = 1,2,\dots,t$。

Step 8. Bob 利用 Cantor 廣義 n 元雙映射配對函數$P_n : Z_1 \times Z_2 \times \dots \times Z_n \to Z$來計算$P_n(W_d)$，$d = 1,2,\dots,n$，並利用傳送方的公鑰$K_{pA}$加密$P_n(W_d)$：$E_A\left(P_n(W_d)\right)$，再將$\{n, E_A\left(P_n(W_d)\right)\}$傳送給 Alice。

Step 9. Alice 利用自己的私鑰K_{sA}解密$E_A\left(P_n(W_d)\right)$得出$P_n(W_d)$，並透過計算$P_n(W_d)$反推出W_d，$d = 1,2,\dots,n$。

Step 10. Alice 計算加密金鑰$rPK_i = riC - rW_i$，$i = 1,2,\dots,n$。

Step 11. Alice 以rPK_i作為加密金鑰來加密訊息$s_i{:}E(s_i)$，$i = 1,2,\dots,n$，並將加密後的訊息傳送給 Bob。

Step 12. Bob 選擇$E(s_j)$，且以rPK_{d_j}解密出想要的訊息s_j，此時只有被選取的 t 個訊息的內容可以分別被解密並讀取。

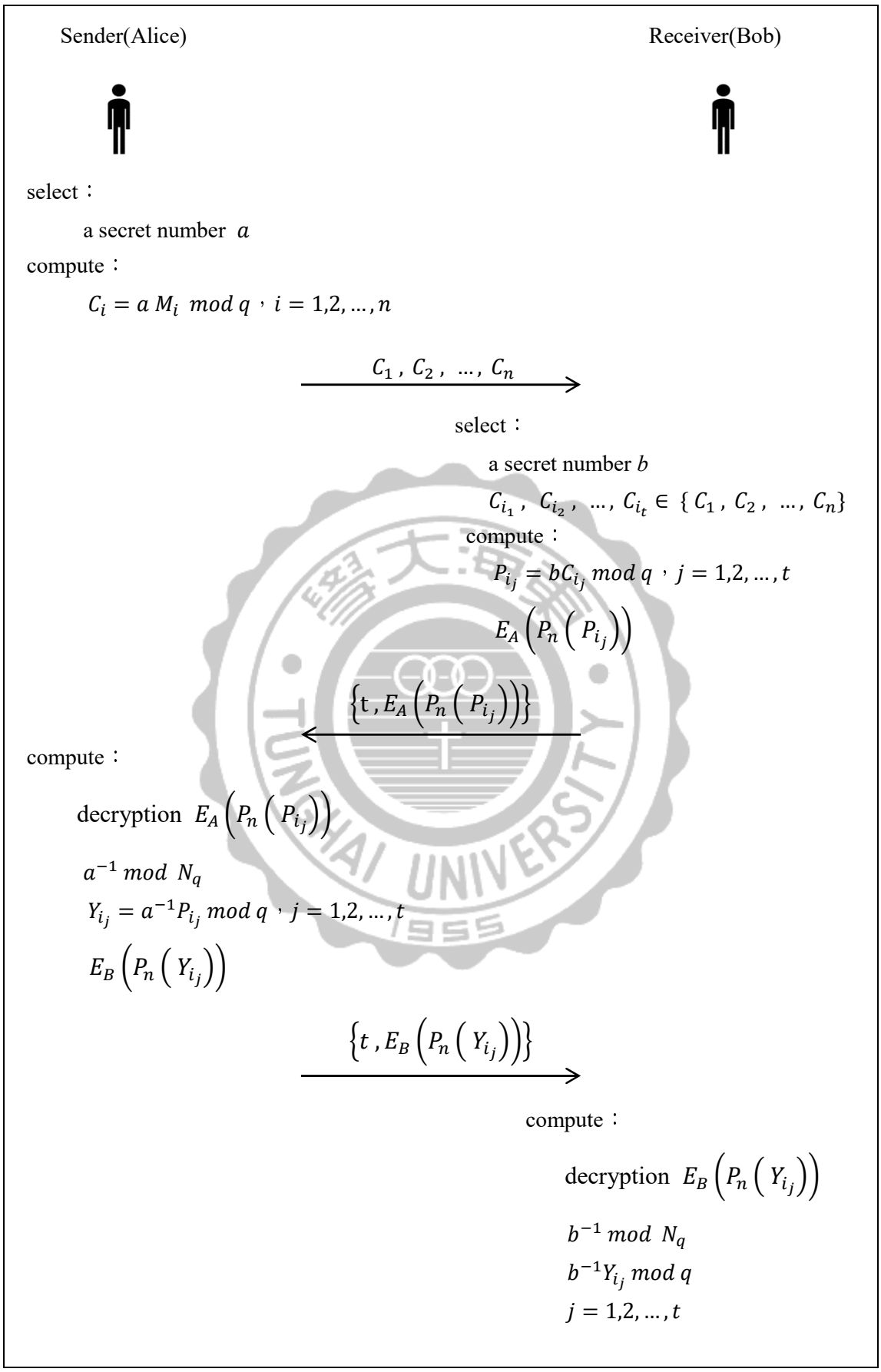

圖 4-1　Huang 與 Chang[16]所提出的 n 選 t 模糊傳輸協定

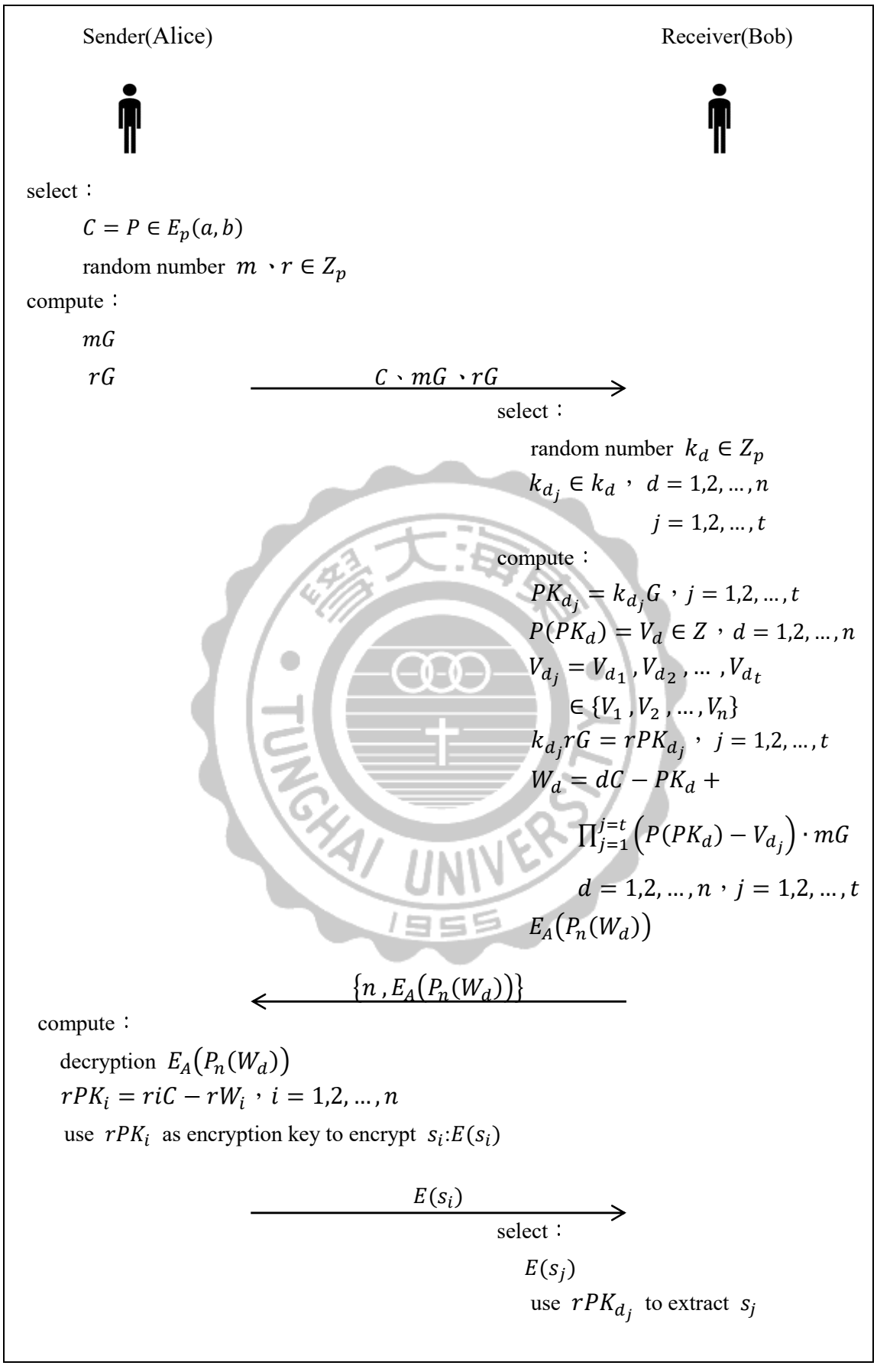

圖 4-2　本研究提出的 *n* 選 *t* 模糊傳輸協定

三、 效能分析

由表 4-1 可發現，Huang 與 Chang[16]提出 *n* 選 *t* 模糊傳輸協定的傳送方訊息傳輸量變為 *n*+1，而接收方的訊息傳輸量變為 1，總訊息傳輸量皆變為 *n*+2，而本研究提出 *n* 選 *t* 模糊傳輸協定的傳送方訊息傳輸量變為 *n*+3，接收方的訊息傳輸量變為 1，總訊息傳輸量皆變為 *n*+4，因此加入 Cantor 廣義 *n* 元雙映射配對函數後，總訊息傳輸量大幅降低，且兩種模式下的模糊傳輸協定的總訊息傳輸量差不多。

表 4-1 訊息傳輸量比較表

	傳送方 訊息傳輸量	接收方 訊息傳輸量	總傳輸量
Huang 與 Chang[16]	*n*+1	1	*n*+2
本協定	*n*+3	1	*n*+4

本章最主要的目的是將 Cantor 廣義 *n* 元雙映射配對函數分別導入至「先加密訊息後計算金鑰」模式與「先計算金鑰後加密訊息」模式的模糊傳輸協定中，而兩者的總訊息傳輸量會趨於一致，且均大幅降低訊息的傳輸量，類似有壓縮的功能，更符合低頻寬的要求，適合應用在傳輸品質差的環境，像是無線通訊的環境，能減少訊息傳輸時受到干擾或破壞的機率。

第五章　結論與未來展望

第一節　研究回顧與結論

模糊傳輸協定是密碼學中一項重要且基礎的機制，而本研究提出的協定結合了橢圓曲線加密與模糊傳輸的概念提高安全性，更可以應用在需要確保雙方隱私的環境，例如私密資訊擷取機制，當使用者希望從資料庫中取得一些資料，但不希望資料庫管理者知道他取得的資料為何，就可以將模糊傳輸協定的概念應用到其中，確保使用者的隱私安全，其餘還有許多應用。

物聯網的時代來臨，無線射頻辨識(Radio Frequency Identification, RFID)已有許多行業開始使用該技術，而 RFID 包含標籤(Tag)、讀取器(Reader)與應用系統(Application)三大元件，可以對貨品、資產、人員等進行追蹤與管理，但應用 RFID 技術可能涉及侵犯個人隱私的問題，因此可以將模糊傳輸協定應用到 RFID 上，解決隱私權的問題。假設讀取器讀取 n 個商品的標籤，廠商希望取得其中 t 個商品的資料，但不希望讀取器得知自己選擇的是哪 t 個資料，以此來確保自身的隱私安全。模糊傳輸機制也可以應用在雲端資料的分享上，確保使用者透過雲端存取資料時能正確的取得資料，並不被雲端的資料管理端知道存取哪些資料，以保障使用者的隱私。

本研究依據加密訊息的先後順序，將基於橢圓曲線密碼系統的模糊傳輸協定分為「先加密訊息後計算金鑰」與「先計算金鑰後加密訊息」兩種模式，而「先加密訊息後計算金鑰」是現今模糊傳輸協定最常使用的方式，目前已有學者提出「先加密訊息後計算金鑰」的 2 選 1 模糊傳輸協定、n 選 1 模糊傳輸協定，以及 n 選 t 模糊傳輸協定，但「先計算金鑰後傳遞訊息」模式的模糊傳輸協定在相關的文獻中只有討論 2 選 1 模糊傳輸協定與 n 選 1 模糊傳輸協定，根據研究顯示大部分的 n 選 t 模糊傳輸協定可以滿足 2 選 1 和 n 選 1 的模糊傳輸協定的，因此

本研究利用橢圓曲線密碼系統與模糊傳輸協定的概念，並以基於橢圓曲線密碼系統的「先計算金鑰後加密訊息」的 n 選 1 模糊傳輸協定為基礎，進一步提出基於橢圓曲線密碼系統下「先計算金鑰後加密訊息」模式的 n 選 t 模糊傳輸協定，解決基於橢圓曲線的「先計算金鑰後加密訊息」的 n 選 1 模糊傳輸協定中接收方只能選擇一個訊息的限制。

本研究所提出的 n 選 t 模糊傳輸協定利用橢圓曲線密碼系統的特性，將以往常用的指數運算轉為點的運算，大幅降低協定的計算量。此外，協定中亦使用 Cantor 配對函數來設計金鑰，以有效區分出接收方欲選取與解密的訊息，以及增加計算的複雜度，使其更不容易被攻擊或破解，藉此提升協定的安全性。但本協定整體訊息的傳輸量仍高於「先加密訊息後計算金鑰」模式下大多數的 n 選 t 模糊傳輸協定，因此在本文中延伸討論如何將 Cantor 廣義 n 元雙映射配對函數應用至模糊傳輸協定上，以降低訊息的總傳輸量，且「先加密訊息後計算金鑰」與「先計算金鑰後加密訊息」兩種模式的總訊息傳輸量會趨於一致，適合用來解決無線網路通訊有雜訊和訊息容易被破壞的問題，使 n 選 t 模糊傳輸協定更能符合實際應用，且具有高安全性、高隱私性、高效率與低頻寬的特性。

第二節　未來展望

模糊傳輸協定已經被討論多年，必須進一步提升協定的安全性與效能，使模糊傳輸協定能更適合應用在實際環境中，然而基於橢圓曲線密碼系統的「先計算金鑰後加密訊息」模式的 n 選 t 模糊傳輸協定在訊息傳輸量的部分仍然稍嫌太多，未來若該模式不使用 Cantor 配對函數，則需導入新的特性或機制來降低協定的訊息傳輸量，或者更詳盡的討論 Cantor 配對函數，使其更廣泛的應用在基於橢圓曲線密碼系統的模糊傳輸協定上，達到壓縮資料，並兼顧協定的安全性與低頻寬的要求。

參考文獻

[1] Aiello, B., Ishai, Y. & Reingold, O. (2001). Priced oblivious transfer: How to sell digital goods, *Lecture Notes in Computer Science*, *2045*, 119-135. doi:10.1007/3-540-44987-6_8.

[2] Bellare, M. & Micali, S. (1989). Non-Interactive Oblivious Transfer and Applications. *Advances in Cryptology — CRYPTO'89 Proceedings*, *435*, 547-557. doi:10.1007/0-387-34805-0_48.

[3] Blum, M. (1981). Three applications of the oblivious transfer: Part I: Coin flipping by telephone; Part II: How to exchange secrets; Part III: How to send certified electronic mail. *University of California, Berkeley*, *CA*.

[4] Brassard, G. & Crépeau, C. (1997, May). Oblivious transfers and privacy amplification. *In Proceedings of the 16th annual international conference on Theory and application of cryptographic techniques*, *16*(4), 219-237.

[5] Cegielski, P. & Richard, D. (1999). On arithmetical first-order theories allowing encoding and decoding of lists. *Theoretical Computer Science*, *222*(1), 55-75.

[6] Cégielski, P. & Richard, D. (2001). Decidability of the theory of the natural integers with the cantor pairing function and the successor. *Theoretical Computer Science*, *257*(1), 51-77.

[7] Chang, C. C. & Lee, J. S. (2009). Robust t-out-of-n oblivious transfer mechanism based on CRT. *Journal of network and computer applications*, *32*(1), 226-235.

[8] Chen, S. W., Chiang, D. L., Liu, C. H., Chen, T. S., Lai, F., Wang, H. & Wei, W. (2016). Confidentiality Protection of Digital Health Records in Cloud Computing. *Journal of medical systems*, *40*(5), 1-12.

[9] Chen, Y., Chou, J. S. & Hou, X. W. (2010). A novel k-out-of-n Oblivious Transfer Protocols Based on Bilinear Pairings. *IACR Cryptology ePrint Archive*, *2010*, 27.

[10] Chor, B., Kushilevitz, E., Goldreich, O. & Sudan, M. (1998). Private information retrieval. *Journal of the ACM (JACM)*, *45*(6), 965-981.

[11] Chou, T. & Orlandi, C. (2015). The Simplest Protocol for Oblivious Transfer. *Progress in Cryptology--LATINCRYPT 2015*, 40-58. doi:10.1007/978-3-319-22174-8_3.

[12] Di Crescenzo, G., Malkin, T. & Ostrovsky, R. (2000). Single database private information retrieval implies oblivious transfer. *International Conference on the*

Theory and Applications of Cryptographic Techniques, 122-138. doi:10.1007/3-540-45539-6_10.

[13] Even, S., Goldreich, O. & Lempel, A. (1985). A randomized protocol for signing contracts. *Communications of the ACM*, *28*(6), 637-647.

[14] Fueter, R. & Pólya, G. (1923). Rationale abzählung der gitterpunkte. *Vierteljschr. Naturforsch. Ges. Zürich*, *58*, 380-386.

[15] Harn, L. & Lin, H. Y. (1990). Noninteractive oblivious transfer. *Electronics Letters*, *26*(10), 635-636.

[16] Huang, H. F. & Chang, C. C. (2007). A new t-out-n oblivious transfer with low bandwidth. *Applied Mathematical Sciences*, *1*(7), 311-320.

[17] Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of computation*, *48*(177), 203-209.

[18] Kocher, P. C. (1996, August). Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In *Annual International Cryptology Conference,* 104-113. doi:10.1007/3-540-68697-5_9.

[19] Li, J. Y.(2008). Oblivious Transfer Protocols Based on Elliptic Curve Cryptography, Department of Information Management, Southern Taiwan University of Science and Technology, unpublished.

[20] Lisi, M. (2007). Some remarks on the Cantor pairing function. *Le Matematiche*, *62*(1), 55-65.

[21] Merkle, R. C. (1980, April). Protocols for Public Key Cryptosystems. *IEEE Symposium on Security and privacy,* 122. doi:10.1109/SP.1980.10006.

[22] Miller, V. S. (1985). Use of elliptic curves in cryptography. *Advances in Cryptology—CRYPTO'85 Proceedings,* 417-426. doi:10.1007/3-540-39799-X_31.

[23] Mu, Y., Zhang, J. & Varadharajan, V. (2002). m out of n Oblivious Transfer. *Proc. of the 7th Australasian Conference on Information Security and Privacy (ACISP'02), LNCS 2384*, 395-405. doi:10.1007/3-540-45450-0_30.

[24] Mu, Y., Zhang, J., Varadharajan, V. & Lin, Y. X. (2003). Robust non-interactive oblivious transfer. *The Institute of Electrical and Electronics Engineers*, *7(4),* 153-155.

[25] Naor, M. & Pinkas, B. (1999). Oblivious transfer and polynomial

evaluation. *Proceedings of the thirty-first annual ACM symposium on Theory of computing,* 245-254. doi:10.1145/301250.301312.

[26] Naor, M. & Pinkas, B. (2001). Efficient oblivious transfer protocols. *Proceedings of the twelfth annual ACM-SIAM symposium on Discrete algorithms*, 448-457.

[27] Paillier, P. (1999). Public-key cryptosystems based on composite degree residuosity classes. *International Conference on the Theory and Applications of Cryptographic Techniques*, 223-238. doi:10.1007/3-540-48910-X_16.

[28] Parakh, A. (2006). Oblivious Transfer Using Elliptic Curves. IEEE *CIC'06. 15th International Conference on Computing*, 323-328. doi:10.1109/CIC.2006.49.

[29] Parakh, A. (2012). Communication Efficient Oblivious Transfer Using Elliptic Curves. *IEEE 14th International Symposium on High-Assurance Systems Engineering (HASE)*, 173-174. doi:10.1109/HASE.2012.14.

[30] Rabin, M. O. (1981). How to Exchange Secrets with Oblivious Transfer. *IACR Eprint archive.*

[31] Rivest, R. L. Shamir, A. & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, *21*(2), 120-126.

[32] Stern, J. P. (1998). A new and efficient all-or-nothing disclosure of secrets protocol. *International Conference on the Theory and Application of Cryptology and Information Security*, 357-371. doi:10.1007/3-540-49649-1_28.

[33] Tarau, P. (2012). Deriving a fast inverse of the generalized cantor N-tupling bijection. *LIPIcs-Leibniz International Proceedings in Informatics*, *17*, 312-322.

[34] Tzeng, W. G. (2004). Efficient 1-out-of-n oblivious transfer schemes with universally usable parameters. *IEEE Transactions on Computers*, *53*(2), 232-240.

[35] Wakaha, O., & Ryota, S. (2004). k out of n Oblivious Transfer without Random Oracle. *IEICE Transactions on Fundamentals of Electronics, Communication and Computer Sciences*, *87*(1), 147-15.

[36] Wu, Q. H., Zhang, J. H. & Wang, Y. M. (2003). Practical t-out-n oblivious transfer and its applications. *International Conference on Information and Communications Security*, 226-237. doi:10.1007/978-3-540-39927-8_21.

[37] Zeng, B., Tang, X., Xu, P. & Jing, J. (2011). Practical Frameworks For h-Out-Of-n Oblivious Transfer With Security Against Covert and Malicious

Adversaries. *IEEE Transactions on Information Forensics and Security*, *7*(2), 465-479.