# 行政院國家科學委員會專題研究計畫 成果報告

## 安全多方計算協定的研究與應用
## 研究成果報告(精簡版)

計 畫 類 別 ：個別型
計 畫 編 號 ：NSC 100-2221-E-029-017-
執 行 期 間 ：100 年 08 月 01 日至 101 年 07 月 31 日
執 行 單 位 ：東海大學電機工程學系（所）

計 畫 主 持 人：鐘玉芳
共 同 主 持 人：陳澤雄
計畫參與人員：碩士班研究生-兼任助理人員：王柏鈞
碩士班研究生-兼任助理人員：鍾政宏
大專生-兼任助理人員：蔡孟洋
博士班研究生-兼任助理人員：李正哲

報 告 附 件 ：出席國際會議研究心得報告及發表論文

公 開 資 訊 ：本計畫涉及專利或其他智慧財產權，2 年後可公開查詢

中 華 民 國 101 年 08 月 23 日

中 文 摘 要 ： 本研究旨在探討安全多方計算之基本運算與協定、設計高效能的安全多方計算協定、評估安全多方計算之複雜度，並且以模運算及秘密分享協定為基礎，建構一般化的安全多方計算應用模式。因此，本研究針對公開模運算之減化 (Public Module Reduction) 與秘密模次方運算 (Private Module Exponentiation)進行分析，藉以獲得知識，將基礎協定中的位元分解 (Bit Decomposition) 擴展為數位分解協定及數位位元分解協定，使現行協定的複雜度從 O(nlog n) 降為線性時間，開發高效能的秘密位元運算協定，同時也使安全多方計算協定的應用更趨於多元。本研究方法採用具有可驗證性的秘密分享 VSS(Verifier Secret Sharing)協定，提出複雜度較低的可驗證秘密分享協定。此外，本研究更針對 UC (Universally Compostable) 模型下多方函數安全計算之充分必要條件進行探討。攻擊模式的選擇對於安全理論的建立相當重要，因此本研究以來自內部惡意參與者的 Cut-and-Choose 攻擊模式為安全設計之主要考量，提出安全的雙方計算協定設計。為了檢測惡意參與者輸入參數的一致性，協定使用簡單映射，以提高協定效率。

中文關鍵詞： 安全多方計算、位元分解、秘密分享、UC 模型

英 文 摘 要 ： This study aims to discuss the basic computation and protocol of Secure Multiparty Computation, design the high-performance protocol, evaluate the complexity, and construct the generalized application model based on module computation and secret sharing protocol. Aiming at Public Module Reduction and Private Module Exponentiation, analyses are proceeded for knowledge acquisition and expanding Bit Decomposition in the protocol to Digital Decomposition Protocol and Digital Bit Decomposition Protocol so that the complexity of present protocol reduces from O(nlog n) to linear time. The high-performance Secret Bit Computation Protocol is developed, and the application of Secure Multiparty Computation becomes multiple. With Verifier Secret Sharing (VSS) protocol, low complexity VSS protocol is proposed. Furthermore, the necessity and sufficiency of Secure Multiparty Computation in Universally Compostable Model is discussed. The selection of attacking mode is critical for the establishment of security theory. In this case, having the Cut-and-Choose attacking

mode of internal malicious participants be the primary consideration for the secure design, the secure computation protocol for both parties is designed. To test the consistency of the parameters input by malicious participants, simple mapping protocol is utilized for enhancing the efficiency.

英文關鍵詞： Secure Multiparty Computation, Bit Decomposition, Secret Sharing, Universally Compostable Model.

# 安全多方計算協定的研究與應用

The Study and Application of Secure Multiparty Computation Protocol

計畫編號：NSC 100-2221-E-029-017

執行期限：九十九年八月一日至一百年七月三十一日

主持人： 鐘玉芳 副教授 東海大學電機工程學系

共同主持人： 陳澤雄 教授 東海大學資訊管理學系

計畫參與人員： 李正哲 台灣大學電機工程研究所博士班

王柏鈞 東海大學電機工程研究所

鍾政宏 東海大學資訊管理研究所

蔡孟洋 東海大學電機工程學系

## 摘要

本研究旨在探討安全多方計算之基本運算與協定、設計高效能的安全多方計算協定、評估安全多方計算之複雜度，並且以模運算及秘密分享協定為基礎，建構一般化的安全多方計算應用模式。因此，本研究針對公開模運算之減化 (Public Module Reduction) 與秘密模次方運算 (Private Module Exponentiation)進行分析，藉以獲得知識，將基礎協定中的位元分解 (Bit Decomposition) 擴展為數位分解協定及數位位元分解協定，使現行協定的複雜度從 $O(n\log n)$ 降為線性時間，開發高效能的秘密位元運算協定，同時也使安全多方計算協定的應用更趨於多元。本研究方法採用具有可驗證性的秘密分享 VSS(Verifier Secret Sharing)協定，提出複雜度較低的可驗證秘密分享協定。此外，本研究更針對 UC (Universally Compostable) 模型下多方函數安全計算之充分必要條件進行探討。攻擊模式的選擇對於安全理論的建立相當重要，因此本研究以來自內部惡意參與者的 Cut-and-Choose 攻擊模式為安全設計之主要考量，提出安全的雙方計算協定設計。為了檢測惡意參與者輸入參數的一致性，協定使用簡單映射，以提高協定效率。

**關鍵字：**安全多方計算、位元分解、秘密分享、UC 模型。

# Abstract

This study aims to discuss the basic computation and protocol of Secure Multiparty Computation, design the high-performance protocol, evaluate the complexity, and construct the generalized application model based on module computation and secret sharing protocol. Aiming at Public Module Reduction and Private Module Exponentiation, analyses are proceeded for knowledge acquisition and expanding Bit Decomposition in the protocol to Digital Decomposition Protocol and Digital Bit Decomposition Protocol so that the complexity of present protocol reduces from $O(n\log n)$ to linear time. The high-performance Secret Bit Computation Protocol is developed, and the application of Secure Multiparty Computation becomes multiple. With Verifier Secret Sharing (VSS) protocol, low complexity VSS protocol is proposed. Furthermore, the necessity and sufficiency of Secure Multiparty Computation in Universally Compostable Model is discussed. The selection of attacking mode is critical for the establishment of security theory. In this case, having the Cut-and-Choose attacking mode of internal malicious participants be the primary consideration for the secure design, the secure computation protocol for both parties is designed. To test the consistency of the parameters input by malicious participants, simple mapping protocol is utilized for enhancing the efficiency.



**Keywords:** Secure Multiparty Computation, Bit Decomposition, Secret Sharing, Universally Compostable Model.

# 壹、 研究背景

本研究的研究範圍涵蓋安全多方計算的基本運算及協定和一般化安全多方計算協定，其中基本運算主要包含模減法、模次方等模算術，基本協定主要包含秘密分享、位元分解等協定方法，而一般化安全多方計算主要包括密碼學複雜度的研究及一般化安全多方計算協定的建立。在 1980 年代，Chandra 等人[1, 2]的背景下探討，求得連乘、求逆等基本運算，並沿用其提供的協定方法至今。在 2002 年的美國密碼安全協會，Algesheimer 等人在模數必須保密的情況下研究其它的基本運算，如模減法、求模次方等計算方法，此類計算方法在之後被用作為位元分解（Bit-Decomposition）的基本工具[3]。在 2006 年，位元分解在 TCC **(**Tiny C Compiler)經由 Damgard、Kiltz 等人提出，並設計出效率較高的方法[4]。同年，在歐洲密碼學會議上，Schoenmakers 等人，把位元分解的概念擴展到 Paillier 安全多方計算背景的密碼學模型上[5]。由於位元分解的複雜度較高，為了改進效率的缺點，2007 年 Nishide 等人在 PKC (Public Key Cryptography)提出去除位元分解進行大小比較及相等測試等運算方法，建構線性協定[6]。根據文獻[4, 6]的內容，在 2010 年的亞洲密碼學會議，非使用位元分解且具有線性複雜度的公開模運算協定被提出[7]；近年研究，不僅提出公開模運算協定也研究線性複雜度的秘密求模次方協定[8]。本研究在亞洲密碼學會議上，將位元分解擴展到數位分解方法上。藉由計畫中的數位分解協定，可以解決諸如 Summary of Product Characteristics 背景下的進制轉換、獲取秘密值使用 10 進制等問題。可驗證秘密分享是安全多方計算的另一項協定，在資訊理論模型中秘密通道模型將安全多方計算構建在可驗證的秘密分享協定的基礎上。秘密共享最早是在 1979 年由 Shamir[9]和 Blakley[10]分別提出，並藉由 Lagrange 插值多項式和映影幾何理論設計(t, n)門檻方法。此外，Chor 等人對秘密分享進行延伸性的研究，提出可抵抗主動攻擊者的可驗證秘密分享(Secret Sharing )的概念[11]。由於 Chor 協定的通信複雜度屬於指數運算，為了提高可驗證的秘密分享協定的效率，需設計秘密分

享協定的研究。Fitzi 等人[12]在雙變數多項式中，能有效設計安全的秘密分享協定。另外，Patra 等人[13]修改文獻[12]中的多項式分享協定，將分享協定增加重建的步驟，改良成可以分享重建的方法，更有效率的設計可驗證秘密分享協定。然而，在此基礎上，仍需要更進一步降低可驗證秘密分享在文獻中待改善的問題。

安全多方計算的目地是保證多個參與者在分散式的環境中，能安全地計算某個函數。因此，在特定的安全模型下，對各種功能函數的複雜度進行比較和分類；例如計算複雜性：不同功能函數的密碼複雜性，亦可通過兩者之間的歸納來做比較。在密碼學的研究中，最自然的歸納是 Oracle-TM。例如，若存在一個可行的協定，能夠通過 Oracle-TM 使用功能函數 G，安全設計功能函數 F，那麼稱安全設計函數 F 可以歸納到安全設計函數 G。表示在該模型下，安全設計 F 的複雜度小於安全設計函數 G 的複雜度。歸納的方式因安全模型而異，並不是所有的研究目的都能被安全設計。透過研究函數之間的密碼複雜度關係，分出複雜度的層次，有助於直接地比較和分類。此外，若能透過歸納找出複雜的問題，則有助於瞭解此類函數的本質。目前，關於安全多方計算複雜度的研究，大多集中在雙方對稱函數的計算問題，而對其他複雜的雙方或多方的功能函數之研究則相對較少。探究其原因可能是對某類問題的研究方法及結論與此類問題自身的結構特性以及相應的安全模式的類型相關，因此難以擴展到其他更為複雜的模型。因此，需要在已有研究成果的基礎上，建構出更具一般性的研究系統，使其可以應對更為複雜的安全多方計算問題。

# 貳、 研究方法與成果

## 一、安全多方計算的運算及協定之研究

### (一)對公開模運算的線性演算法之研究

對於公開模運算問題的探討，是否可以避免將位元分解運用到設計線性複雜度上。為了解決此問題，必須擴展位元分解的概念，將其擴展到m進制數位分解和數位位元分解方法；然而，將數位分解簡化，計算一個避免使用位元分解及具有線性複雜度的公開模運算簡化協定。雖然此協定的目的是為了要解決公開模運算簡化的問題，但對於位元分解之擴展，如：數位分解和數位位元分解也是相當的重要；不但可改良處理實際應用問題的能力，也增進位分解的擴展，尤其是對數位位元分解；但其設計的難度要比公開模運算簡化協定高出許多，所以是很具挑戰性的工作。

1. 對位元分解的擴展

位元分解的擴展，即m進制數位分解（Base-m Digit-Decomposition）和m進制數位位元分解（Base-m Digit-Bit Decomposition）；利用一個分享的秘密$[x]_p$和一個公開的m作為輸入參數，數位分解能夠輸出對x的所有m進制的分享，而數位位元分解則能夠輸出對x的所有m進制的分享。由上述可知，數位分解是對數位位元分解的簡化。數位位元分解協定的過程如圖1，此協定的架構與文獻[9]中的位元分解協定類似。

Digit-Bit-Decomposition(·, m)：m 進制數位位元分解協定演算法

一. 輸入參數：$[x]_p$ $(x \in Z_p)$ 和 $m \in \{2, 3, ..., p-1\}$

二. 輸出參數：$[x]^m_{D,B}$

三. 演算法：

1. $[r]^m_{D,B} \leftarrow$ Random-Solved-Digits-Bits(m)
2. $c \leftarrow \text{Reveal}([x]_p + [r]^m_{D,B})$
3. $c' \leftarrow c + p$
4. $[t]_p \leftarrow$ Digit-Bit-wise-LessThan($[c]^m_{D,B}$, $[r]^m_{D,B}$)
5. $[\tilde{c}]^m_{D,B} = [t]_p \,?\, [c']^m_{D,B} : [c]^m_{D,B}$
6. $[x]^m_{D,B} \leftarrow$ Digit-Bit-wise-Subtraction*($[\tilde{c}]^m_{D,B}$, $[r]^m_{D,B}$)
7. Return $[x]^m_{D,B}$

圖1: m進制數位位元分解的協定

2. 避免使用位元分解的公開模運算簡化協定

避免使用位元分解的公開模運算簡化協定（表示為Pub-MR(·)）的原因是由於此協定是一個常數輪次的線性協定，因此協定的複雜度是O(1)輪次。相反的，公開模運算簡化協定是一種存取最低m進制的位元協定，亦是文獻[6]中所提出的存取最低位元協定（即LSB協定）的一個應用。因此，根據前面的定義可知，對任意的整數x，其最低m進制的分享被表示為$[x_0]^m_p$，而其最低m進制的位元分享被表示為$[x_0]^m_B$，協定的詳細描述如圖2。

Pub-MR(·)：位元分解的公開模運算簡化協定演算法

一. 輸入參數：$[x]_p$ 和 $m \in \{2, 3, ..., p-1\}$

二. 輸出參數：$[x \bmod m]_p$

三. 演算法：

1. $[r]_{D,B}^m \leftarrow$ Random-Solved-Digits-Bits(m)
2. $c \leftarrow \text{Reveal}([x]_p + [r]_{D,B}^m)$
3. $[x_1]_p^m \leftarrow [c_0]_p^m - [r_0]_B^m$
4. $[x_2]_p^m \leftarrow [c_0]_p^m - [r_0]_B^m + m$
5. $[s]_p \leftarrow$ Bit-Wise-LessThan($[c_0]_B^m$, $[r_0]_B^m$)
6. $[x]_p^m \leftarrow [s]_p ? [x_2]_p^m : [x_1]_p^m$
7. $c' \leftarrow c + p$
8. $[x'_1]_p^m \leftarrow [c'_0]_p^m - [r_0]_B^m$
9. $[x'_2]_p^m \leftarrow [c'_0]_p^m - [r_0]_B^m + m$
10. $[s']_p \leftarrow$ Bit-Wise-LessThan($[c'_0]_B^m$, $[r_0]_B^m$)
11. $[x']_p^m \leftarrow [s']_p ? [x'_2]_p^m : [x'_1]_p^m$
12. $[t]_p \leftarrow$ Digits-Bit-Wise-LessThan($[c]_{D,B}^m$, $[r]_{D,B}^m$)
13. $[x \bmod m]_p = [x_0]_p^m \leftarrow [t]_p ? [x']_p^m : [x]_p^m$
14. Return $[x \bmod m]_p$

圖2：位元分解的公開模運算簡化協定

原始的公開模運算簡化並無要求提出(x mod m)位元分享(即$[x \bmod m]_B$)，所以在上述的協定中，本研究只計算了$[x \bmod m]_p$而沒有計算$[x \bmod m]_B$。但是如果其他方法有需要，則可以對上述Pub-MR(·)的協定進行改進，直接計算出$[x \bmod m]_B$，而後將此改良的公開模運算簡化協定表示為Enh-Pub-MR(·)。但實際上，此協定是數位位元分解的簡化。雖然$[x \bmod m]_B$可以透過$[x \bmod m]_p$運用位元分解而得到，但改良後的公開模運算簡化協定的效率比上述做法還要高。而改良版本的協定，即是Enh-Pub-MR(·)，如圖3為其步驟的過程。

Enh-Pub-MR(·)：改良的公開模運算簡化協定演算法

一. 輸入參數：$[x]_p$ 和 $m \in \{2, 3, ..., p-1\}$

二. 輸出參數：$[x \bmod m]_B$

三. 演算法：

1. $[r]_{D,B}^m \leftarrow$ Random-Solved-Digits-Bits(m)
2. $c \leftarrow \text{Re veal}([x]_p + [r]_{D,B}^m)$
3. $[\overline{M}_1]_B^m \leftarrow [c_0]_B^m$ , $[\bar{s}_1]_B^m \leftarrow [r_0]_B^m$
4. $[\overline{M}_2]_B^m \leftarrow [c_0 + m]_B^m$ , $[\bar{s}_2]_B^m \leftarrow [r_0]_B^m$
5. $[s]_p \leftarrow$ Bitwise-LessThan($[c_0]_B^m$, $[r_0]_B^m$)
6. $[\overline{M}]_B^m \leftarrow [s]_p ? [\overline{M}_2]_B^m : [\overline{M}_1]_B^m$
7. $[\bar{s}]_B^m \leftarrow [s]_p ? [\bar{s}_2]_B^m : [\bar{s}_1]_B^m$
8. $c' \leftarrow c + p$
9. $[\overline{M}'_1]_B^m \leftarrow [c'_0]_B^m$ $[\bar{s}'_1]_B^m \leftarrow [r_0]_B^m$
10. $[\overline{M}'_2]_B^m \leftarrow [c'_0 + m]_B^m$ $[\bar{s}'_2]_B^m \leftarrow [r_0]_B^m$
11. $[s']_p \leftarrow$ Bit-Wise-LessThan($[c'_0]_B^m$, $[r_0]_B^m$)
12. $[\overline{M}']_B^m \leftarrow [s']_p ? [\overline{M}'_2]_B^m : [\overline{M}'_1]_B^m$
13. $[\bar{s}']_B^m \leftarrow [s']_p ? [\bar{s}'_2]_B^m : [\bar{s}'_1]_B^m$
14. $[t]_p \leftarrow$ Digits-Bit-Wise-LessThan(c, $[r]_{D,B}^m$)
15. $[M]_B^m \leftarrow [t]_p ? [\overline{M}']_B^m : [\overline{M}]_B^m$
16. $[s]_B^m \leftarrow [t]_p ? [\bar{s}']_B^m : [\bar{s}]_B^m$
17. $[x \bmod m]_B = [x_0]_B^m \leftarrow$ Bitwise-Subtraction$^*$($[M]_B^m$, $[s]_B^m$)
18. Return $[x \bmod m]_B$

圖3：改良的公開模運算簡化協定

3. 各子協定的詳細設計

下面將說明前面所提出所有新的子協定。大致來講，這裏大部分的協定都是將文獻[4]中的協定從2進制轉換為m進制。

(1) 計算借位協定

首先，求借位協定BORROWS(·)是接收兩個位元的分享，利用輸入參數 $[x]_B = \{[x_{l-1}]_p, \ldots, [x_1]_p, [x_0]_p\}$ ； $[y]_B = \{[y_{l-1}]_p, \ldots, [y_1]_p, [y_0]_p\}$; 輸出 $\{[b_{l-1}]_p, \ldots, [b_1]_p, [b_0]_p\}$，其中，$b_i$ $(i \in \{0, 1, \ldots, l-1\})$是計算$x - y$時第i個位元位上產生的借位。

實際上，本研究的BORROWS(·)協定和CARRIES(·)協定非常相似，因此，簡述二者的區別如下。所使用的運算符號$\circ : \Sigma \times \Sigma \rightarrow \Sigma$，其中$\Sigma = \{S; P; K\}$。此運算符號的定義為對所有的$x \in \Sigma$，有$S \circ x = S$ ; $K \circ x = K$; $P \circ x = x$。據上述，$\circ$ 所描寫的是借位規則，因此將其命名為借位傳遞運算符號。因此，輸入參數$[x]_B = \{[x_{l-1}]_p, \ldots, [x_1]_p, [x_0]_p\}$和$[y]_B = \{[y_{l-1}]_p, \ldots, [y_1]_p, [y_0]_p\}$後，對每個位元 $i \in \{0, 1, \ldots, l-1\}$。

當$e_i = S$且僅當第i位元會產生借位（即$x_i < y_i$）；

當$e_i = P$且僅當第i位元會傳遞借位（即$x_i = y_i$）；

當$e_i = K$且僅當第i位元不會產生借位（即$x_i > y_i$）；

經由驗證得知 $b_i = 1$（表示第i位元產生了借位） 等價於 $e_i \circ e_{i-1} \circ \cdots \circ e_0 = S$。所以，當$\circ$被用做借位傳遞運算符號或進位傳遞運算符號時，其所對應的運算規則（即對所有的$x \in \Sigma$，有$S \circ x = S$ ; $K \circ x = K$; $P \circ x = x$）是完全相同的。因此，一旦得到了所有的 $e_i$，那麼求借位協定的後續部分就會和求進位協定完全相同。所以，求借位協定和求進位協定的區別只存在於求所有$e_i$的過程中。下述為此過程的簡述：過程與文獻[4]相同，將S; P; K分別表示為位元的三元組:

$\{(1, 0, 0), (0, 1, 0), (0, 0, 1)\} \in \{0, 1\}^3$，然後，對每個位元$i \in \{0, 1, \ldots, l-$

1}，其中$[e_i]_B = \{[s_i]_p, [p_i]_p, [k_i]_p\}$可以表示如下：$[s_i]_p = [y_i]_p - [x_i]_p[y_i]_p$；$[p_i]_p = 1 - [x_i]_p - [y_i]_p + 2[x_i]_p[y_i]_p$；$[k_i]_p = [x_i]_p - [x_i]_p[y_i]_p$。然而，上述的過程中只需要使用1次乘法運算，即$[x_i]_p[y_i]_p$。

(2) 位元減法協定

位元減法協定即是Bitwise-Subtraction(·)。位元減法問題被歸納到首碼比較問題的分類。在本研究中需重新考慮位元減法的問題，並運用和位元加法（Bitwise-Addition）類似的協定之方法來解決此問題。因此，只需要一個表示為Bitwise-Subtraction*的位元減法協定，此協定條件為其所輸入參數的被減數必須要大於減數，其詳細說明如圖4。

Bitwise-Subtraction*(·)：位元減法協定演算法

一. 輸入參數：$[x]_B = ([x_{l-1}]_p, \ldots, [x_1]_p, [x_0]_p)$和

$[y]_B = ([y_{l-1}]_p, \ldots, [y_1]_p, [y_0]_p)$, 滿足$x \geq y$

二. 輸出參數：$[x - y]_B = [d]_B = ([d_{l-1}]_p, \ldots, [d_1]_p, [d_0]_p)$

三. 演算法：

1. $([d_{l-1}]_p, \ldots, [d_1]_p, [d_0]_p) \leftarrow \text{BORROWS}([x]_B, [y]_B)$
2. $[d_0]_p \leftarrow [x_0]_p - [y_0]_p + 2[d_0]_p$
3. For $i = 1, 2, \ldots, l-1$ in parallel: $[d_i]_p \leftarrow [x_i]_p - [y_i]_p + 2[b_i]_p - [b_{i-1}]_p$
4. $[x - y]_B = [d]_B \leftarrow ([d_{l-1}]_p, \ldots, [d_1]_p, [d_0]_p)$
5. Return $[x - y]_B$

圖4：位元減法協定

值得注意的是此協定的輸出，即$[x - y]_B$，其位元長度是$l$，而不是$l + 1$；這是因為$x \geq y$成立，所以不需要符號位元。

(3) 隨機數位位元協定

隨機數位位元之協定，即是Random-Digit-Bit(·)。此協定能夠產生一個位元分享的隨機m進制數位 d。d 實際上是一個滿足$0 \le d \le m-1$的整數。此協定的輸出不是對 d 的分享，而是對d的位元之分享；所以，得知 d 的位元分享對於建構其他協定時可以提供許多幫助，如圖5所示。

| Random-Digit-Bit(·)：隨機數位位元協定演算法 |
|---|
| 一. 輸入參數： m，滿足$2 \le m \le p-1$<br>二. 輸出參數：$[d]_B^m = \left(\left[d^{L(m)-1}\right]_p, ..., \left[d^1\right]_p, \left[d^0\right]_p\right)$，滿足$0 \le d \le m-1$<br>三. 演算法：<br>1. For $i = 0, 1..., L(m)-1$ in parallel:$\left[d^i\right]_p \leftarrow$ Random-Bit().<br>2. $[d]_B^m \leftarrow \left(\left[d^{L(m)-1}\right]_p, ..., \left[d^1\right]_p, \left[d^0\right]_p\right)$<br>3. If $m = 2^{L(m)}$, then Return$[d]_B^m$，若條件不符合,則執行後續的指令。<br>4. $[r]_p \leftarrow$ Bitwise-LessThan$\left([d]_B^m, m\right)$<br>5. $r \leftarrow$ Reveal$([r]_p)$<br>6. 若$r = 0$ ，則結束此程式;否則Return$[d]_B^m$。 |

圖5：隨機數位位元協定

(4) 數位位元小於協定

此處的數位位元小於協定是對位元小於協定的一個改良，協定的詳細架構如圖 6 所示。

| 數位位元小於協定演算法 |
|---|
| 一. 輸入參數：<br>$[x]_{D.B}^m = \left(\left[x_{l(m)-1}\right]_B^m, ..., \left[x_1\right]_B^m, \left[x_0\right]_B^m\right)$和$[y]_{D.B}^m = \left(\left[y_{l(m)-1}\right]_B^m, ..., \left[y_1\right]_B^m, ..., \left[y_1\right]_B^m, \left[y_0\right]_B^m\right)$<br>二. 輸出參數： |

$\left[\left(x \overset{?}{<} y\right)\right]_p$，其中$\left(x \overset{?}{<} y\right)=1$且當 x < y 成立時

三. 演算法：

1. $[x]_B \leftarrow \left(\left[x_{l^{(m)}-1}^{L(m)-1}\right]_p, \ldots, \left[x_{l^{(m)}-1}^{1}\right]_p, \left[x_{l^{(m)}-1}^{0}\right]_p,\right.$
$\ldots$
$\left[x_1^{L(m)-1}\right]_p, \ldots, \left[x_1^1\right]_p, \left[x_1^0\right]_p$
$\left.\left[x_0^{L(m)-1}\right]_p, \ldots, \left[x_0^1\right]_p, \left[x_0^0\right]_p\right)$

2. $[Y]_B \leftarrow \left(\left[y_{l^{(m)}-1}^{L(m)-1}\right]_p, \ldots, \left[y_{l^{(m)}-1}^{1}\right]_p, \left[y_{l^{(m)}-1}^{0}\right]_p,\right.$
$\ldots$
$\left[y_1^{L(m)-1}\right]_p, \ldots, \left[y_1^1\right]_p, \left[y_1^0\right]_p$
$\left.\left[y_0^{L(m)-1}\right]_p, \ldots, \left[y_0^1\right]_p, \left[y_0^0\right]_p\right)$

3. $\left[\left(x \overset{?}{<} y\right)\right]_p = \left[\left(X \overset{?}{<} Y\right)\right]_p \leftarrow \text{Bitwise-LessThan}\left([x]_B, [Y]_B\right)$

4. $\text{Return}\left[\left(x \overset{?}{<} y\right)\right]_p$

圖6：數位位元小於協定

(5) 產生數位位元分享的秘密亂數協定

產生數位位元分享的秘密亂數協定Random-Solved-Digits-Bits(·)是一個很重要的子協定；此協定是對於Random-Solved-Bits(·)的一個改良。其詳細過程如圖7所示。

| Random-Digit-Bits(·)：隨機數位協定演算法 |
|---|
| 一. 輸入參數：m，期望的進制 |
| 二. 輸出:$[r]_{D.B}^m$，r 是一個均勻分布的隨機整數，且滿足 $r<p$ |
| 三. 演算法: |
| 1. For $i = 0, 1, \ldots, l^{(m)}-1$ in parallel: $[r_i]_B^m \leftarrow$ Random-Digit-Bit(m) |

2. $[r]_{D.B}^{m} \leftarrow \left([r_{l(m)-1}]_{B}^{m}, \ldots, [r_1]_{B}^{m}, [r_0]_{B}^{m}\right)$

3. $[c]_p \leftarrow \text{Digit-Bit-Wise-LessThen}\left([r]_{D.B}^{m}, [p]_{D.B}^{m}\right)$

4. $c \leftarrow \text{Reveal}\left([c]_p\right)$

如果 c = 0，則結束此程式；否則 $\text{Return}[r]_{D.B}^{m}$ 。

圖7：產生數位位元分享的秘密亂數的協定

(6) 數位位元減法協定

本研究運用數位位元減法協定Digit-Bit-Wise-Subtraction*(·)；要求輸入參數的被減數必須不小於減數，此協定在數位位元分解協定Digit-Bit-Decomposition(·)中不僅是最重要也是最複雜的一個子協定。與前述的Digit-Bit-Wise-LessThan(·)協定類似，將在此協定的分析中介紹使用與操作的過程。協定的過程如圖8所示。

Digit-Bit-Wise-Subtraction*(·)：數位位元減法協定演算法

一. 輸入參數：

$[x]_{D.B}^{m} = \left([x_{l^{(m)}-1}]_{B}^{m}, \ldots, [x_1]_{B}^{m}, [x_0]_{B}^{m}\right)$ 和 $[y]_{D.B}^{m} = \left([y_{l^{(m)}-1}]_{B}^{m}, \ldots, [y_1]_{B}^{m}, [y_0]_{B}^{m}\right)$ 滿足 $x \geq y$

二. 輸出參數： $[x-y]_{D.B}^{m} = [d]_{D.B}^{m} = \left([d_{l^{(m)}-1}]_{B}^{m}, [d_0]_{B}^{m}\right)$

三. 演算法：

1. $[x]_B \leftarrow \left([x_{l^{(m)}-1}^{L(m)-1}]_p, \ldots, [x_{l(m)-1}^{1}]_p, [x_{l(m)-1}^{0}]_p,\right.$
$\ldots$
$[x_1^{L(m)-1}]_p, \ldots, [x_1^{1}]_p, [x_1^{0}]_p,$
$\left.[x_0^{L(m)-1}]_p, \ldots, [x_0^{1}]_p, [x_0^{0}]_p\right)$

2. $[Y]_B \leftarrow \left(\left[y_{l^{(m)}-1}^{L(m)-1}\right]_p, \ldots, \left[y_{l^{(m)}-1}^{1}\right]_p, \left[y_{l^{(m)}-1}^{o}\right]_p,\right.$
$\cdots$
$\left[y_1^{L(m)-1}\right]_p, \ldots, \left[y_1^1\right]_p, \left[y_1^o\right]_p,$
$\left.\left[y_o^{L(m)-1}\right]_p, \ldots, \left[y_o^1\right]_p, \left[y_o^o\right]_p\right)$

3. $\left(\left[b_{l^{(m)}-1}^{L(m)-1}\right]_p, \ldots, \left[b_{l^{(m)}-1}^{1}\right]_p, \left[b_{l^{(m)}-1}^{0}\right]_p, \ldots, \left[b_1^{L(m)-1}\right]_p, \ldots, \left[b_1^1\right]_p, \left[b_1^0\right]_p,\right.$
$\left.\left[b_0^{L(m)-1}\right]_p, \ldots, \left[b_0^1\right]_p, \left[b_0^0\right]_p \leftarrow \mathrm{BORROWS}\left([X]_B, [Y]_B\right)\right)$

4. $\left[t_0^0\right]_p = \left[x_0^0\right]_p - \left[y_0^0\right] + 2\left[b_0^0\right]_p$

5. For $j = 1, \ldots, L(m)-1$, in parallel: $\left[t_0^j\right]_p = \left[x_0^j\right]_p - \left[y_0^j\right]_p + 2\left[b_0^j\right]_p - \left[b_0^{j-1}\right]_p$

6. For $i = 1, \ldots, l(m)-1$ do $\left[t_i^0\right]_p = \left[x_i^0\right]_p - \left[y_i^0\right]_p + 2\left[b_i^0\right]_p - \left[b_{i-1}^{L(m)-1}\right]_p$

7. For $j = 1, \ldots, L(m)-1$, in parallel: $\left[t_i^j\right]_p = \left[x_i^j\right]_p - \left[y_i^j\right]_p + 2\left[b_i^j\right]_p - \left[b_i^{j-1}\right]_p$

8. End for

9. $C \leftarrow 2^{L(m)} - m$

10. For $i = 0, 1, \ldots, l^{(m)} - 1$ do

11. $\left[t_i\right]_B^m \leftarrow \left(\left[t_i^{L(m)-1}\right]_p, \ldots, \left[t_i^1\right]_p, \left[t_i^0\right]_p\right)$

12. If $m < 2^{L(m)}$ then $\left[d_i\right]_B^m \leftarrow \text{Bitwise-Subtraction}^*\left(\left[t_i\right]_B^m, \left(\left[b_i^{L(m)-1}\right]_p ? C : 0\right)\right)$

13. Else $\left[d_i\right]_B^m \leftarrow \left[t_i\right]_B^m$

14. End if

15. End for

16. $\left[x\text{-}y\right]_{D.B}^m = \left[d\right]_{D.B}^m \leftarrow \left(\left[d_{i^{(m)}-1}\right]_B^m, \ldots, \left[d_1\right]_B^m, \left[d_0\right]_B^m\right)$

17. Return $\left[x\text{-}y\right]_{D.B}^m$

圖8：數位位元減法協定

## (二) 對秘密求模次方運算線性演算法之研究

本研究的問題是秘密求模次方運算之問題，如已知$[x]_p$、$[a]_p$，求$[x \bmod p]_p$避免使用位元分解來解決，進而使用在線性複雜度上。將這分別以兩部分說明最終的秘密求模次方運算協定，首先是在求解秘密求模次方運算的問題時應如何避

免使用位元分解，進而得到一個具有線性複雜度的協定；其次，將對此線性協定做進一步的改進，將其複雜度降低。

1. 避免使用位元分解的秘密求模次方運算協定

如圖9所示為避免使用位元分解來設計的秘密求模次方運算協定，此協定將被表示為Pri-Expo(·)。

Pri-Expo(·)：位元分解的秘密求模次方運算協定演算法

1. $[b]_P \leftarrow \text{Equ-Zero}([x]_P)$
2. $[\tilde{x}]_P = [x]_P + [b]_P$
3. $[r]_B \leftarrow \text{Solved-Bits}()$
4. $[c]_P = [a]_P + [r]_P$
5. $c \leftarrow \text{Reveal}([c]_P)$
6. $[c]_P \leftarrow \text{Pub-Expo}([\tilde{x}]_P, c)$
7. $[c']_P \leftarrow \text{Sec-Mult}([c]_P, [\tilde{x}]_P)$
8. $[f]_P \leftarrow \text{Bitwise-LessThan}(c, [r]_B)$
9. $[\tilde{c}]_P \leftarrow [f]_P ? [c']_P : [c]_P$
10. $[R]_P \leftarrow \text{Bit-Expo}([\tilde{x}]_P, [r]_B)$
11. $[R^{-1}]_P \leftarrow \text{Sec-Inver}([R]_P)$
12. $[\tilde{x}^a]_P \leftarrow \text{Sec-Mult}([\tilde{c}]_P, [R^{-1}]_P)$
13. $\text{Return}\ [x^a]_P = [\tilde{x}^a]_P - [b]_P$

圖9：位元分解的秘密求模次方運算協定

2. Pri-Expo(·)協定的改良

對前述所提出的Pri-Expo(·)協定做進一步的改良，具體的做法是改善此協定中在複雜度中占主要部分的子協定Bit-Expo(·)，而改良後的Pri-Expo(·)和Bit-Expo(·)協定將分別被表示為 Pri-Expo+(·)和Bit-Expo+(·)。總體而言，在Pri-Expo(·)協定中，將對Bit-Expo(·)的使用替換為對Bit-Expo+(·)的應用，得到此最新改良的秘密求模次方運算協定Pri-Expo+(·)，詳細的過程如圖10所示。

| Pri-Expo+(·)：改進的位元求模次方運算協定演算法 |
|---|
| 1. Protocol $\left[x^{a}\right]_{p} \leftarrow \text{Bit-Expo}^{+}\left(\left[x\right]_{p}, \left[a\right]_{B}\right)$, x = 0.<br>2. For j = 0, 1,..., t – 1 in parallel: $\left[A_{j}\right]_{p} \leftarrow \text{Pub-Expo}\left(\left[x\right]_{p}, 2^{j}\right)$<br>3. For i = 0, 1,..., s – 1 in parallel do<br>4. For j = 0, 1,..., t – 1 in parallel: $\left[B_{i,j}\right]_{p} \leftarrow \left[a_{i,j}^{s\times t}\right]_{p} ? \left[A_{j}\right]_{p} : 1$<br>5. $\left[B_{i}\right]_{p} \leftarrow \text{Sec-Prod}^{*}\left(\left[B_{i,0}\right]_{p}, \left[B_{i,1}\right]_{p}, ..., \left[B_{i,t}\right]_{p}\right)$<br>6. $\left[C_{i}\right]_{p} \leftarrow \text{Pub-Expo}\left(\left[B_{i}\right]_{p}, \left(2^{t}\right)^{i}\right)$<br>7. End for<br>8. Return $\left[x^{a}\right]_{p} \leftarrow \text{Sec-Prod}^{*}\left(\left[c_{0}\right]_{p}, \left[c_{1}\right]_{p}, ..., \left[c_{s-1}\right]_{p}\right)$ |

圖 10：改進的位元求模次方協定

在本研究主要探討安全多方計算的秘密求模次方運算之問題。此研究探討不但可以避免使用位元分解來解決問題，亦可以簡化為線性複雜度。因此，所得到的秘密求模次方運算協定（即Pri-Expo+(·)），其效率比已有的Pri-Expo-BD(·)協定要高出許多。

# 參、 VSS協定的複雜度之研究

基於雙變數多項式和信任圖分析方法，在 WSS 的分享階段，基於參與者之間互相發送的隨機因數，在第二輪中進行秘密配額的驗證；在 WSS 協定的基礎上，使用類似的方式構建 VSS 協定，設計了具有保密性、正確性和承諾性的 VSS 協定。

## 一、WSS協定的建構

### (一) 分享階段

本端計算：在有限域 $K$ 上選擇一個雙變數多項式 $F \in K[x, y]$，且兩變數的次數均不超過 $t$，並滿足 $F[0,0] = s$。定義 $f_i(x) = F[x, i], g_i(y) = F[i, y]$，其

中$1 \le i \le n$。

第 1 輪迴：運用點對點發送訊息

1. 向參與者發送兩個多項式 $f_i(x)$ 和 $g_i(y)$。
2. 每個參與者在有限域 $K$ 上隨機選擇 $r_{ij}$，並將 $r_{ij}$ 發送給參與者和本端，其中 $1 \le j \le n, j \ne i$。

第 2 輪迴：廣播訊息

1. 參與者廣播以下訊息：$a_{ij} = f_i(j) + r_{ij}, b_{ij} = g_i(j) + r_{ji}$，其中 $1 \le j \le n$。
2. 本端廣播 $c_{ij} = F_j(i) + r_{ij}$，其中 $1 \le j \le n, 1 \le i \le n$。

本端計算：在所有的參與者進行計算

1. 將集合 SH 初始化為空集合，對 $1 \le i \le n$，如果 $a_{ij} = c_{ij}$ 並且 $b_{ij} = c_{ji}$，則將參與者加入集合。
2. 如果 $|SH| < n - t$，則認為本端不誠實，即終止協定。

## (二) 重建階段

廣播：每個 $SH$ 集合中的參與者廣播其擁有的多項式 $f_i(x)$ 和 $g_i(y)$。

本端計算：在所有的參與者進行計算

1. 將 $SH$ 中的參與者作為節點建立圖 $G$，當參與者 $P_i$ 和 $P_j$ 間有 $f_i(j) = g_j(i)$ 且 $g_i(j) = f_j(i)$ 的關係時，在 $P_i$ 和 $P_j$ 節點間有一個邊。
2. 對圖 $G$ 進行以下的步驟：計算圖 $G$ 中節點的分支度，將分支度小於 $n-t$ 的節點都刪除，重複以上的步驟，直到沒有節點被刪除為止。如果剩餘的圖 $G$ 中節點數小於 $n-t$，則輸出 NULL。否則，使用剩餘節點中的任意 $t+1$ 個參與者對應的多項式進行 Lagrange 插值，重建多項式 $F^*(x, y)$，並得到對應的秘密 $s^* = F^*(0, 0)$。

## 二、 VSS協定的建構

### (一)分享階段

本端計算：

1. 在有限域 $K$ 上選擇一個隨機雙變數多項式 $F \in K[x, y]$，且兩變數的次方均不超過 $t$，並滿足 $f(0,0) = s$。定義 $f_i(x) = F[x, i], g_i(y) = F[i, y]$，其中 $1 \le i \le n$。

2. 參與者 $P_i$ 選擇亂數 $r_i$，其中 $1 \le i \le n$。

第 1 輪迴：運用點對點發送訊息

(1) 由本端向參與者 $P_i$ 發送兩個多項式 $f_i(x)$ 和 $g_i(y)$。

(2) 參與者 $P_i$ 使用一個 WSS，稱為 $\text{WSS}_i$，用於分享 $r_i$。其中使用的雙變數多項式為 $F_i^W(x, y)(F_i^W(0,0) = r_i)$，其中 $1 \le i \le n$。執行第 1 輪的 $\text{WSS}_i$。

(3) 參與者 $P_i$ 將 $F_i^W(x, y)$ 發送給本端。

第 2 輪迴：廣播訊息

(1) 參與者 $P_i$ 廣播以下訊息：$a_{ij} = f_i(j) + F_i^W(0, j), b_{ij} = g_i(j) + F_j^W(0, i)$，其中 $1 \le j \le n$。

(2) 本端廣播 $c_{ij} = F_j(i) + F_i^W(0, j)$，其中 $1 \le i \le n, 1 \le j \le n$。

(3) 同時執行 $\text{WSS}_i$，$1 \le i \le n$ 的第 2 輪迴。

本端計算：在所有的參與者進行計算

3. 將集合 $SH$ 初始化為空集合。對 $1 \le i \le n$，如果 $a_{ij} = c_{ij}$ 並且 $b_{ij} = c_{ji}$，則將參與者 $P_i$ 加入集合 $SH$。

4. 如果在 $\mathrm{WSS}_i$ 協定中 $P_i$ 被認為作假，則將 $P_i$ 從 $SH$ 中刪除。如果 $|SH| < n-t$ 則認為本端作假，即中止協定。

5. 令 $SH_i^W$ 表示 $\mathrm{WSS}_i$ 中分享階段中無作假的集合。對於每個 $P_i \in SH$ ，檢查是否最少有 $n-t$ 個參與者同樣在 $SH_i^W$ 集合中，如果條件不滿足，則將 $P_i$ 從集合 $SH$ 中刪除。如果最終的 $SH$ 集合中的元素數 $|SH| < n-t$ ，則認為本端作假並中止協定。

## (二)重建階段

廣播：在每個 $SH$ 集合中的參與者 $P_i$ 需同時執行 $\mathrm{WSS}_i$ 的重建階段。

本端計算：在所有的參與者進行計算

1. 建立 $REC$ 集合，令 $REC = SH$，對於每個 $P_i \in REC$ ， 如果 $\mathrm{WSS}_i$ 輸出為 NULL，那麼將 $P_i$ 從 $REC$ 中刪除。

2. 對於每個 $P_i \in REC$ ，使用其在分享階段第 2 輪迴廣播的 $a_{ij}$ 來計算 $f_i(j) = a_{ij} - F_i^W(0, j), 1 \le j \le n$

3. 使用這些 $f_i(j)$ 進行插值得到多項式 $f_i(x)$ ，檢查其次方是否最多為 $t$ ，如果不成立，則將 $P_i$ 從 $REC$ 中刪除。因此，從 $REC$ 中取 $t+1$ 個參與者，使用其多項式 $f_i(x)$ 進行插值得到 $F^*(x, y)$ ，並計算 $s^* = F^*(0,0)$ 。

# 三、 一般化安全多方計算協定之研究

本研究主要研究一般化安全多方計算的協定，一方面研究安全多方函數計算協定以設計兩個必要條件的充分性，並提出充要條件；另一方面在惡意模型下設計效率較高的一般化雙方安全計算協定。

## (一)多方函數計算協定可設計性的研究

根據 Prabhakaran 和 Rosulek[14]的分析，發現所提出的關於多方函數計算之必要條件，利用反證法來說明所提出的必要條件並不是充分的，因此進行探討多方函數計算運用 UC，以設計充分且必要條件的研究。回顧多方計算函數 UC 所設計的兩個必要條件，首先必須要證明其中一個必要條件不是充分的，其次為另一個必要條件在機率多項式時間計算環境下也不是充分的。

1. 必要條件

若想研究*m*-SFE函數的方法就是分割（Partitioning Argument）；透過分割，將*m*個參與者分割成兩個集合，進而瞭解2-SFE函數的特性。如果原始的*m*-SFE函數是可設計的，則分割出的2-SFE亦可設計的。利用分割的方法，Prabhakaran 和 Rosulek提出了多方函數計算有其可設計性之必要條件。

如果$\mathcal{F}$是一個 *m*-SFE 函數，透過完全保密的通道安全設計，那麼在由關係$\xrightarrow{\mathcal{F}}$推導出的有向圖中，或者所有邊有一個共用的原點，或者所有邊有一個共用的終點。

2. 相關定理

定理1: 令$\mathcal{F}(x_1, x_2, x_3, x_4)=(f_1, \ldots, f_m)$ 為一個*m*-SFE函數，如果在由關係$\xrightarrow{\mathcal{F}}$得到的有向圖中，通過參與者$P_i$ 的集合，如此，就不能得出結論，F可以用完全保密的通道$\mathcal{G}$安全設計。

反例1: $\mathcal{F}(x_1, x_2, x_3, x_4) = (f_1, \ldots, f_4) = (r, r, r, x_1+ x_2+ x_3+ x_4)$， $r \in \{0, 1\}$。

首先，參與者$P_i$ ($i$=1, 2, 3)的輸出獨立於其他參與者的輸入參數，所以沒有參與者影響$P_i$ ($i$=1, 2, 3)。另外，對於參與者$P_i$ ($i$=1, 2, 3)的兩個不同的輸入參數 $x_i$ 和 $x_i$'，將使得$P_4$的輸出也不同，所以參與者$P_i$ ($i$=1, 2, 3)會影響$P_4$，F通過$P_4$集合，如圖11所示由關係$\xrightarrow{\mathcal{F}}$推導出有向圖。

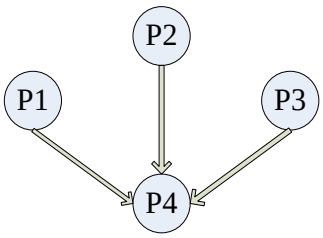


圖 11：有向圖的集合

下面，將證明F不能利用完全保密的通道$\mathcal{G}$安全設計。考慮具有下面幾種特性：

(1) 敵手為一個偽裝的敵手，不是參與者；

(2) 參數為 $x_i$ ($i$=1, …, 4)，提供輸入參數 $x_i$ 給參與者 $P_i$；

(3) 對偽裝敵手而言，不知道 $x_i$ 的選擇，這些指令使得 F 的延遲輸出，但最終都被傳送到參與者；

(4) 等待所有參與者返回輸出，如果 $P_1$、$P_2$ 和 $P_3$ 的輸出相同，且 $P_4$ 的輸出為 $x_1+x_2+x_3+x_4$，則輸出 1。

對於功能函數 F，證明 F 與完全保密的通道$\mathcal{G}$是不可分離的。由於 F 在$\mathcal{G}$混合模型中不能安全地被設計，4 方函數的可分離性必須要證明兩種交互的不可區分性。第一種是交互包含一個 F 的實例和另外一個傳輸器$\mathcal{T}$，其中$\mathcal{T}$視為一個敵手，第二種是交互包含 F 的 4 個獨立實例與 4 個傳輸器$\mathcal{T}_1$、$\mathcal{T}_2$、$\mathcal{T}_3$與$\mathcal{T}_4$的合成。

在第一種交互中輸出1的機率為1，假設分離的機會不是很大，則所有延遲的輸出都會被傳送。然而，在第二種交互中，不管其他的ITM的行為如何，F的四個實例是相互獨立的，參與者$P_1$、$P_2$與$P_3$將會以3/4的機率接收不同的輸出。因此，可以假設F通過$P_4$集合，但是F並不能通過完全保密的通道$\mathcal{G}$安全設計，從而判定定理1成立。

定理2：令$F(x_1, x_2, x_3, x_4)=(f_1, \ldots, f_m)$ 為一個$m$-SFE的函數。如果在由關係 $\xrightarrow{\mathcal{F}}$ 得到的有向圖中，而後通過參與者$P_i$ 的傳送，因此關係得不到在機率

多項式計算環境下，F可以使用完全保密的通道$\mathcal{G}$安全設計。

反例2：F $(x_1, x_2, x_3, x_4)= (f_1, \ldots, f_4)=(g_1(x_4), g_2(x_4), g_3(x_4), x_4+r)$，其中$g_i(\cdot)$，$i$=1, 2, 3是機率多項式計算環境下的單向抵抗碰撞函數。

首先，對於參與者$P_i$ ($i$=1, 2, 3)，輸入參數給$x_4$ 和$x_4$'，使得參與者$P_i$ ($i$=1, 2, 3)的輸出不同，即參與者$P_4$影響參與者$P_i$ ($i$=1, 2, 3)。另外，參與者$P_i$的輸出為獨立，除了參與者$P_4$外，無其他參與者能影響$P_i$。因此，F通過參與者$P_4$集合，如圖12所示。

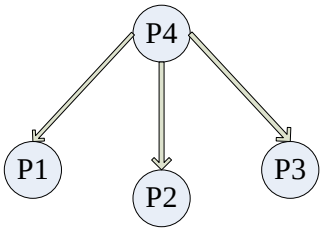


圖 12：有向圖的傳送

下述證明函數F與完全保密的通道$\mathcal{G}$是不可分離的，進而得出F在$\mathcal{G}$的混合模型中是不能安全設計。考慮具有下面的特性：

(1) 敵手為一個偽裝的敵手，不是參與者；

(2) 參數為 $x_i$ ($i$=1, …, 4)，輸入參數 $x_i$ 給參與者 $P_i$；

(3) 對偽裝敵手而言，不知道 $x_i$ 的選擇，這些指令使得 F 的延遲輸出，但最終都被傳送到任何的參與者；

(4) 等待所有參與者返回，如果 $P_1$、$P_2$ 與 $P_3$ 分別輸出 $g_1(x_4)$、$g_2(x_4)$與 $g_3(x_4)$，則輸出 1。

上述類型的機制都可以清楚的將分離性定義中的兩種交互區作區隔，下述證明對於 F 可能的分離。

因為假設分離的機會不是很大，因此在第一種交互中輸出1的機率為1，則所有延遲的輸出都將會被傳送。然而，在第二種交互中，因為$g_i(\cdot)$是單向函數，

機率多項式時間的ITM $\mathcal{T}_1$ 、$\mathcal{T}_2$ 、$\mathcal{T}_3$ 與 $\mathcal{T}_4$ 無法計算$x_4$的值，因此參與者$P_1$、$P_2$與$P_3$將會以絕大多數收到與真實輸出值不同偽裝的隨機值。

因此，F雖然通過參與者的傳送，但是在PPT計算環境下並不能通過完全保密的通道 $\mathcal{G}$ ，然而判定定理2成立。

文中必須注意在 UC 的定義中，有一個關鍵的因素是實際世界和理想模型中的敵手，為 A、S 與 Z 三者中的交互作用。UC 安全的可設計性意味著存在一個理想過程中的模擬器 $\mathcal{S}$ ，即可完成真實世界中敵手對一個真實參與者所做的一切。例如：理想中的模擬器必須能夠存取真實敵手所使用的輸入參數。因此在 UC 框架下可以安全設計的功能函數，是必須公開參與者的輸入參數；亦即，只有完全公開或者完全可逆的函數可以安全的設計。

3. 充要條件

下述將文獻[14-15]中雙方函數完全公開和完全可逆的定義擴展到多方計算的情形：

定義1(完全公開)：令F是$m$方安全計算功能函數，F必須通過參與者$P_i$的傳送。

如果存在可行的$R_1$ 和$R_2$，使得對於所有的輸入參數$x_1, x_2, \ldots, x_m$，滿足

$$x_1^*,\ldots, x_{i-1}^*, \quad x_{i+1}^*,\ldots., x_m^*, s \leftarrow R_1,$$

$$y_j^* \leftarrow f_j(x_1^*,\ldots, x_{i-1}^*, x_i, x_{i+1}^*,\ldots., x_m^*), j=1,2,\ldots,m, j\neq i.$$

$$x_i^* \leftarrow R_2(s, y_1^*, y_2^*, \ldots, y_m^*),$$

$$f_j(x_1,\ldots, x_{i-1}, x_i^*,. x_{i+1},\ldots., x_m) \approx f_j(x_1,\ldots, x_i,\ldots, x_m), \quad j=1,2,\ldots,m, j\neq i.$$

由此，可稱F是完全公開。

定義2(完全可逆)：令F是$m$方安全計算功能函數，F必須通過參與者$P_i$集合。對於所有$j=1, 2, \ldots, m, j\neq i$，如果存在可行的ITM $R_1^{(j)}$ 和 $R_2^{(j)}$ ，使得對於所有的輸入參數$x_1, x_2, \ldots, x_m$，滿足

$x_1^*, ..., x_{j-1}^*, x_{j+1}^*, \ldots, x_m^*, s \leftarrow R_1^{(j)}$,

$y_k^* \leftarrow f_k(x_1^*, ..., x_{j-1}^*, x_j, x_{j+1}^*, \ldots, x_m^*), k=1,2,\ldots,m, k \neq j$

$x_j^* \leftarrow R_2^{(j)}(s, y_1^*, ..., y_{j-1}^*, y_{j+1}^*, ..., y_m^*)$,

$f_i(x_1, ..., x_{j-1}, x_j^*, x_{j+1}, \ldots, x_m) \approx f_i(x_1, ..., x_j, \ldots, x_m)$

則稱F對於參與者$P_j$ ( $j$=1, 2,…, $m$，$j \neq i$)是完全可逆。下面提出$m$方SFE，UC安全設計的充要條件。

定理3：令$F(x_1, x_2, x_3, x_4)=(f_1, \ldots, f_m)$是$m$方安全計算功能函數。則F即可通過完全保密通道$\mathcal{G}$並在安全中設計有向圖的關係，在 $\xrightarrow{\mathcal{F}}$ 所構成的有向圖中，透過與參與者$P_i$的傳送且對參與者$P_j$，$j$=1, 2,…, $m$, $j \neq i$，屬於完全公開，或者F透過參與者$P_i$集合，且F對於參與者$P_j$，$j$=1, 2,…, $m$, $j \neq i$，屬於完全可逆。

## 四、惡意模型下效率較高的雙方安全計算協定

近年，一般化雙方安全計算的研究大都集中在如何提高效率的議題，文獻[16]中使用 Cut-and-Choose 的方法提出了一個在惡意模型下效率較高的解決方案。簡單而言，Cut-and-Choose 即是提出並要求計算電路的 N 個備份，然後讓對方隨機選取其中一部分並得到這部分隨機選取電路正確性的證明，所以此證明方法是透過隨機選取部分電路而使得對方相信剩餘電路的正確性。為了進一步提高效率，如文獻[17]運用 Equality-Checker 方法改進文獻[16]中的 Cut-and-Choose 方法。而後文獻[18]使用一個 d-正規圖形代替全連接圖形的方法，提高了文獻[17]的效率。而本文中所使用的協定是 Cut-and-Choose 的方法，因為在惡意參與者的情況下，此方法可以設計安全的雙方計算。然而，為了能夠檢測惡意參與者輸入參數的一致性，協定使用簡單的輪替映射，達到了提高協定的效率。

### (一)協定的架構

協定 1 的步驟如下：

1. 把參與者 B 的每一個輸入參數 $x_i$ 作為電路的 m 個輸入參數。
2. 將參與者 A 建構與原電路 $C_0$ ，計算出相同函數的 $n$ 個電路備份 $C_1, C_2 ... C_n$ 。而參與者 A 建構參與者 B 的輸入參數密鑰的對應承諾，保證參與者 A 輸入參數一致性的 Equality-Checker。
3. 對參與者 B 所輸入參數的 A 和 B 都須執行一個 $OT_2^1$ 協定，參與者 A 會把 B 的輸入參數對應的密鑰和解承諾傳送給參與者 B。
4. 參與者 A 把上面建構的電路如:混亂加密表、輸出對照表和承諾，將參與者 B 輸入參數密鑰對應的承諾和 A 輸入參數密鑰對應的 Equality-Checker 傳送給 B。
5. 而後 A 和 B 公平執行拋硬幣的協定，共同決定是否要打開 $n/2$ 個電路。
6. 參與者 A 將選定要打開電路之相關密鑰和解承諾皆傳給參與 B，而參與者 B 則檢驗電路建構是否正確。
7. 參與者 A 則把剩餘的 $n/2$ 個電路，對應於其輸入參數的密鑰和 Equality-Checker 傳送給參與者 B。
8. 參與者 B 可以根據 Equality-Checker 檢查剩餘 $n/2$ 個電路，檢查是否與參與者 A 輸入參數有一致性，並根據自己輸入參數的密鑰計算電路值。
9. 若有超過 $n/4$ 的電路計算得到相同的值，參與者 B 就可把計算得到的電路值 輸出。以下對協定做簡單的說明，首先添加第 1 步驟的原因是，通常 $OT_2^1$ 協定在惡意參與者 A 的參與下是不安全的，有可能洩漏參與者 B 的輸入參數 $y$ 之相關資訊[5]；再來，從協定可以看出為了防止參與者 A 建構假電路，協定使用 Cut-and-Choose 的方法建構了原電路的 $n$ 個備份，也就是使用隨機打開 $n/2$ 個電路的方法，此方法確保了剩餘 $n/2$ 個電路的正確性[7]。接著，為了保證參與者 A 的輸入參數 $x$ 在多個電路中的一致性，協定的第 2、6、7 步驟使用了 Equality-Checker 的方法[4]。

然而，Equality-Checker 是對兩個不同電路輸入參數對應的隨機密鑰 $k_{i,j}^{t_0}$，$k_{i,j'}^{t_0}$ 對應到同一個值做出的承諾，如為了保證 $C_j$，$C_{j'}$ 兩個電路的第 $i$ 個輸入參數的兩個隨機密鑰 $k_{i,j}^{t_0}$，$k_{i,j'}^{t_0}$ 對應著同一個值，那麼參與者 A 就構建一個關於兩個密鑰對應著同一個值的承諾 $C_{i,j,j'}^{t_0}(i,j,j',k_{i,j}^{t_0},k_{i,j'}^{t_0})$，承諾 $k_{i,j}^{t_0}$，$k_{i,j'}^{t_0}$ 對應著同一個值，比如對應到 1，就把這種承諾稱為 Equality-Checker。

## (二)雙方安全的協定

協定 2 的步驟如下：

輸入參數：B（Bob）輸入參數 $y = y_0 y_1 ... y_m \in (0,1)^m$，A（Alice）輸入參數 $x = x_0 x_1 ... x_m \in (0,1)^m$

輔助輸入參數：計算函數 $f$ 的電路 $C_0$

1. 首先是擴展輸入參數，必須把 B 的每一個輸入參數 $y_i \in (0,m)$ 使用於電路擴展　成 s 個輸入參數 $y_{i,1}, y_{i,2}..y_{i,s}$，這樣 B 的 m 個輸入參數就逐漸擴展成 m*s 個輸入參數 $y_{1,1}, y_{1,s} ... y_{m,1}, y_{m,s}$，則即可防止惡意參與者 A 通過 $OT_2^1$ 協定而得到 B 的輸入參數資訊。
2. 其次是建構電路，A 構建 $n$ 個與原電路計算相同函數 $f$ 的電路，分別編號為 $C_1, C_2 ... C_n$。然後把這 $n$ 個電路隨機分成相等的兩組，每組為 $n/2$ 個電路。
3. 再者是構建承諾，說明如下:

   在上述的每一個分組中，對 A 的第 $j' \in (1,2...n/2)$ 個電路的第 $i \in (1,2...m)$ 個輸入參數兩兩建構 Equality-Checker 承諾 $C_{i,j,j'}^{t_0}$，其中必須要 $j < j'$，如對第 $j$ 和 $j'$ 兩個電路的第 $i$ 個輸入參數對應的密鑰 $k_{i,j}^{t_0}$，$k_{i,j'}^{t_0}$ 建構的 Equality-Checker $C_{i,j,j'}^{t_0} = (i,j,j',k_{i,j}^{t_0},k_{i,j'}^{t_0})$，如此不同電路的同一輸入參數分別在每一組中有 $(n/2*(n-1)/2)*2 = n(n-1)$ 個 Equality-Checker，兩組共有 $(n^2-1)/4$ 個

Equality-Checker。

4. 然而，在兩個分組間隨機的做電路的映射 $f:C_i^k \to C_{i'}^{k'}(i,i' \in (1..n/2),k,k' \in (1..2))$，而後在這個一一映射的基礎上再做一個輪替映射。同樣地，在兩組有對應關係的電路之間建構 Equality-Checker，如此，不同的電路進行同一輸入參數，在兩組間共建構 $2n$ 個 Equality-Checker，與上一步一共建構了 $(n^2-1)/4+2n$ 個 Equality-Checker。
5. 此外，關於擴展的 B 之 m*s 個輸入參數，對每一個輸入參數建構一組承諾資訊 $(C_{i,1}^0, C_{i,2}^0 ... C_{i,n}^0)$，$(C_{i,1}^1, C_{i,2}^1 ... C_{i,n}^1)$，其中 $C_{i,j}^{t_0}$ 對應第 $j$ 個電路的第 $i$ 個輸入參數密鑰 $k_{i,j}^{t_0}$ 的承諾。

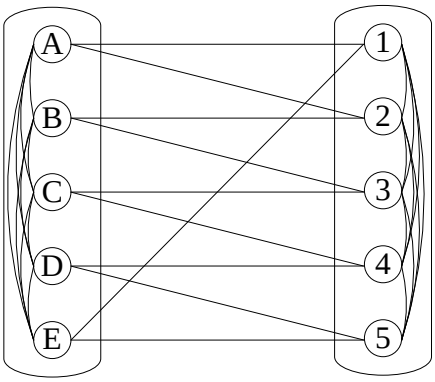


圖 13：電路分組和 Equality-Checker 的建構

6. B 的輸入參數密鑰，對 B 的每個輸入參數 A 和 B 執行一個 $OT_2^1$ 協定步驟，傳送下面兩組中的其中一個，$(k_{i,1}^0, DC_{i,1}^0, k_{i,2}^0, DC_{i,2}^0 ... k_{i,n}^0, DC_{i,n}^0)$

$(k_{i,1}^1, DC_{i,1}^1, k_{i,2}^1, DC_{i,2}^1 ... k_{i,n}^1, DC_{i,n}^1)$，其中特別是 $DC_{i,j}^{t_0}$ 為 $C_{i,j}^{t_0}$ 的解承諾參數，進而 A 將 B 的 m*s 個輸入參數所對應的密鑰和解承諾皆傳送給 B。
7. A 把上面建構的電路如:混亂加密表、輸出對照表和承諾參數，B 輸入參數密鑰對應的承諾和 A 輸入參數密鑰對應的 Equality-Checker 皆傳送給 B。
8. A 和 B 利用公平拋硬幣協定，將共同決定從 $n$ 個電路中隨機選出 $n/2$ 個電路，這 $n/2$ 個電路隨機分佈在上面所述的兩個分組中（如圖 13）。
9. 檢查所選的電路正確性。

10. A 把隨機選擇的電路與 A 的輸入參數密鑰相關 Equality-Checker 的解承諾 $DC^{t_0}_{i,j,j'}(i,j,j',k^{t_0}_{i,j},k^{t_0}_{i,j'})$ 以及輸入參數密鑰 $k^{t_0}_{i,j}$ 傳送給 B。

11. 把隨機選擇的電路與 B 的輸入參數密鑰相關的解承諾資訊 $DC^{t_0}_{i,j}$ 和密鑰 $k^{0}_{i,j}$ 傳送給 B。

12. A 把電路的混亂加密表與相應的輸出對應表傳送給 B。如此，B 就可以完全解密電路，並根據 Equality-Checker 不僅檢驗 A 輸入參數的一致性、B 的輸入參數，以及加密的混亂電路的正確性。

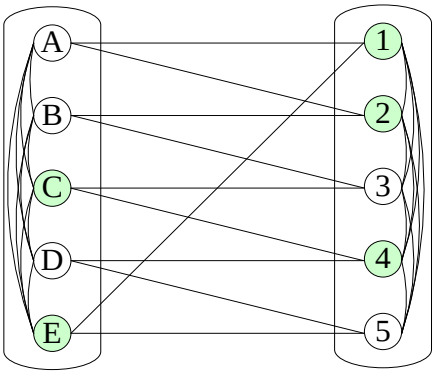


圖 14：電路的選擇和連通性方式

13. 傳送 A 的輸入參數密鑰並把剩餘的 $n/2$ 個電路對應於 A 的輸入參數密鑰與對應於這些密鑰一致性檢驗的 Equality-Checker 的解承諾傳給 B。

14. 檢驗 A 的輸入參數的一致性，因為所選電路的 Equality-Checker 在組內是一個全連接，而組間也是連通的，因而 B 可以根據 A 傳送 Equality-Checker 檢驗 A 關於 $n/2$ 個電路的輸入參數的一致性。

15. 最後是計算電路值，由上一步驟 B 就得到關於 A 輸入參數的密鑰，可以使用這些密鑰計算相關電路的值。而後，B 計算這些電路值，若相同值的電路數超過 $n/4$，則該值作為計算電路的值並輸出。

## 肆、 結論

本研究以研究安全多方計算協定為主要目的，其中對安全多方計算的基本運算和基礎協定、模運算、位元分解和秘密分享進行深入的研究，並在這些基本運算和基礎協定上加以應用。本研究還擴及一般化安全多方計算協定的研究，包括安全多方計算的密碼學與複雜度的研究，以及一般化雙方安全計算協定的建構。未來我們希望能夠進一步加強對安全多方計算的理論模型和基礎協定的了解，並更加具體化的將安全多方計算協定進行提取，讓研究能夠更加適合運用在實際網路環境中的安全模型。

## 參考文獻


[1] A. K. Chandra, S Fortune and R. J. Lipton, "Lower Bounds for Constant Depth Circuits for Prefix Problems," *Lecture Notes in Computer Science*, Vol. 154, pp. 109-117, 1983.

[2] A. K. Chandra, S. Fortune and R. J. Lipton, "Unbounded Fan-In Circuits and Associative Functions," *Journal of Computer and System Sciences*, Vol. 30, No. 2, pp. 222-234, 1983.

[3] J. Algesheimer, J. Camenisch and V. Shoup, "Efficient Computation Modulo A Shared Secret with Application to the Generation of Shared," *Lecture Notes in Computer Science*, Vol. 2442, pp. 417-432, 2002.

[4] I. Damgård, M. Fitzi, E. Kiltz, J. B. Nielsen and T. Toft, "Unconditionally Secure Constant-Rounds Multi-Party Computation for Equality Comparison, Bits and Exponentiation," *Lecture Notes in Computer Science*, Vol. 3876, pp. 285-304, 2006.

[5] B. Schoenmakers and P. Tuyls, "Efficient Binary Conversion for Paillier

Encrypted Values," *Lecture Notes in Computer Science*, Vol. 4004, pp. 522-537, 2006.

[6] T. Nishide and K. Ohta, "Multiparty Computation for Interval, Equality, and Comparison without Bit-Decomposition Protocol," *Lecture Notes in Computer Science*, Vol. 4450, pp. 343-360, 2007.

[7] C. Ning and Q. Xu, "Multiparty Computation for Modulo Reduction without Bit-Decomposition and A Generalization to Bit-Decomposition," *Lecture Notes in Computer Science*, Vol. 6477, pp. 483-500, 2010.

[8] C. Ning and Q. Xu, "Constant-Rounds, Linear Multi-party Computation for Exponentiation and Modulo Reduction," *Lecture Notes in Computer Science*, Vol. 7073, pp. 572-589, 2011.

[9] A. Shamir, "How to Share a Secret," *Communications of the ACM*, Vol. 22, No. 11, pp. 612-613, 1979.

[10] G. R. Blakley, "Safeguarding Cryptographic Keys," *National Computer Conference IEEE Computer Society*, Vol. 48, pp. 313-317, 1979.

[11] B. Chor, S. Goldwasser, S. Micali and B. Awerbuch, "Verifiable Secret Sharing and Achieving Simultaneity in the Presence of Faults," *Foundations of Computer Science*, pp. 383-395, 1985.

[12] M. Fitzi, J. Garay, S. Gollakota, C. P. Rangan and K. Srinathan, "Round-Optimal and Efficient Verifiable Secret Sharing," *Lecture Notes in Computer Science*, Vol. 3876, pp. 329-342, 2006.

[13] A. Patra, A. Choudhary, T. Rabin and C. P. Rangan,"The Round Complexity of Verifiable Secret Sharing Revisited," *Lecture Notes in Computer Science*, Vol. 5677, pp. 487-504, 2009.

[14] M. Prabhakaran and M. Rosulek, "Cryptographic Complexity of Multi-party

Computation Problems: Classifications and Separations," *Lecture Notes in Computer Science*, Vol. 5157. pp. 262-279, 2008.

[15] R. Canetti, E. Kushilevitz and Y. Lindell, "On the Limitations of Universally Composable Two-party Computation Without Set-up Assumptions," *Journal of Cryptology*, Vol. 19, No. 2, pp. 135-167, 2006.

[16] D. Malkhi, N. Nisan, B. Pinkas and Y. Sella, "Fairplay – A Secure Two-Party Computation System," *USENIX Security Symposium*, Vol. 13, pp. 287-302, 2004.

[17] P. Mohassel and M. K. Franklin, " Efficiency Tradeoffs for Malicious Two-Party Computation," *Lecture Notes in Computer Science*, Vol. 3958, pp. 458-473, 2006.

[18] D.P. Woodruff, "Revisiting the Efficiency of Malicious Two-Party Computation," *Lecture Notes in Computer Science*, Vol. 4515, pp. 79-96, 2007.

# 近三年已發表之相關期刊及研討會論文

## (A) 期刊論文

1. **Y. F. Chung**, and Z. Y. Wu, Casting Ballots over Internet Connection Against Bribery and Coercion, accepted by *The Computer Journal*, Dec. 2011. (SCI, EI, IF：1.327)
2. T. C. Hsiao, **Y. F. Chung**, T. S. Chen and G. B. Horng, Hierarchical Information-Protected System with Multiple Predecessors, *International Journal of Innovative Computing, Information and Control*, Vol. 8, No. 7, July, 2012. (SCI, EI, IF:1.664)
3. T. C. Hsiao, Z. Y. Wu, **Y. F. Chung**, T. S. Chen and G. B. Horng, A Secure Integrated Medical Information System, *accepted by Journal of Medical Systems*. (SCI, IF: 1.064)
4. J. Y. Huang, I. E. Liao, **Y. F. Chung** and K. T. Chen, Shielding Wireless Sensor Network using Markovian Intrusion Detection System with Attack Pattern Mining, *Information Sciences*, Available online 29 March 2011. (SCI, EI, IF: 2.836)
5. T. L. Chen, **Y. F. Chung** and F. Y. S. Lin, Secure Deployment of Mobile Agent for Medical Information System, *Journal of Medical Systems*, Vol. 36, No. 4, pp. 2493-2503, August, 2012. (SCI, IF: 1.064)
6. **Y. F. Chung**, T. L. Chen, T. S. Chen, and C. S Chen, A Study on Efficient Group-Oriented Signature Schemes for Realistic Application Environment, *International Journal of Innovative Computing, Information and Control*, Vol. 8, No. 4, pp. 2713-2728, April 2012. (SCI, EI, IF:1.664)
7. **Y. F. Chung**, T. L. Chen, C. S. Chen, and T. S. Chen, The Study on General Secure Multi-Party Computation, *International Journal of Innovative Computing, Information and Control*, Vol. 8, No. 1, pp. 1-10, Jan. 2012. (SCI, EI, IF: 1.664)
8. T. L. Chen, **Y. F. Chung** and F. Y. S. Lin, A Study on Agent-Based Secure Scheme for Electronic Medical Record System, *Journal of Medical Systems*, Vol. 35, No. 3, pp. 1345-1357, June, 2012. (SCI, IF: 1.064)

9. Z. Y. Wu, Y. J. Tseng, **Y. F. Chung**, Y. C. Chen, and F. Lai, A Reliable User Authentication and Key Agreement Scheme for Web-based Hospital-acquired Infection Surveillance Information System, *Journal of Medical Systems*, Vol. 36, No. 4, pp. 2547-2555, August, 2012April, 2011. (SCI, IF: 1.064)
10. C. H. Liu, **Y. F. Chung**, T. W. Chiang, T. S. Chen, and S. D. Wang, A Mobile Agent Approach for Secure Integrated Medical Information Systems, accepted by the *Journal of Medical Systems*, 2011. (SCI, IF：1.064)
11. T. L Chen, Y. L. Yu, **Y. F. Chung**, and T.S. Chen, Grey-Hierarchy Selection System for Businesses Introducing Electronic Commerce, *African Journal of Business Management*, Vol. 6, No. 22, pp. 6339-6346, May, 2012. (SSCI, IF:1.105)
12. T. L. Chen, **Y. F. Chung** and F. Y. S. Lin, A Secure Conference Key Protocol over ECC-based Grey Systems, *International Journal of Innovative Computing, Information and Control*, Vol. 7, No. 10, pp. 5717-5730, October 2011. (SCI, EI, IF: 1.664)
13. C. H. Liu, Y. F. Chung, T. S. Chen, and S. D. Wang, The Design of ID-Based Access Control System with Time-Sensitive Key for Mobile Agent's Migration, *International Journal of Innovative Computing, Information and Control*, Vol. 7, No. 12, pp. 7077-7090, Dec 2011. (SCI, EI, IF：1.664)
14. T. L. Chen, **Y. F. Chung** and F. Y. S. Lin, A Novel Grey Data Generating Technique on Elliptic Curve Cryptosystem, *International Journal of Innovative Computing, Information and Control*, Vol. 7, No. 1, pp. 379-394, January 2011. (SCI, EI, IF: 1.664)
15. Z. Y. Wu, **Y. F. Chung**, F. Lai, T. S. Chen, and H. C. Lee, An Enhanced Password-based User Authentication Scheme for Grid Computing, *International Journal of Innovative Computing, Information and Control*, Vol. 7, No. 7, pp. 3751-3760, July 2011. (SCI, EI, IF: 1.664)
16. **Y. F. Chung**, Y. T. Chen, T. L. Chen, and T. S. Chen, An Agent-Based English Auction Protocol Using Elliptic Curve Cryptosystem for Mobile Commerce, *Expert Systems with Applications*, Vol. 38, pp. 9900-9907, August, 2011. (SCI, EI, IF: 1.924)
17. C. H. Liu, **Y. F. Chung**, T. S. Chen, and S. D. Wang, An ID-Based Access Control in a Hierarchical Key Management for Mobile Agent, *International*

*Journal of Innovative Computing, Information and Control*, Vol. 7, No. 3, pp. 1443-1456, March 2011. (SCI, EI, IF: 1.664)

18. C. H. Liu, **Y. F. Chung**, T. S. Chen, and S. D. Wang, Mobile Agent Application and Integration in Electronic Anamnesis System, *Journal of Medical Systems*, Vol. 36, No. 3, pp. 1009-1020, 2011. (SCI, IF: 1.064)
19. Z. Y. Wu, **Y. F. Chung**, F. Lai, and T. S. Chen, A Password-Based User Authentication Scheme for the Integrated EPR Information System, *Journal of Medical Systems*, Vol. 36, No. 2, pp. 631-638, April, 2012. (SCI, IF: 1.064)
20. Victor R. L. Shen, Y. F. Chung, T. S. Chen, and Y. A. Lin, A Blind Signature Based on Discrete Logarithm Problem, *International Journal of Innovative Computing, Information and Control*, Vol. 7, No. 9, pp. 5403-5416, Sep 2011. (SCI, EI, IF: 1.664)
21. C. H. Liu, **Y. F. Chung**, T. S. Chen, and S. D. Wang, The Enhancement of Security in Healthcare Information Systems, *Journal of Medical Systems*, Vol. 36, No. 3, pp. 1673-1688, June, 2012. (SCI, IF：1.064)
22. Z. Y. Wu, C. W. Hsueh, C. Y. Tsai, F. Lai, H. C. Lee, and **Y. F. Chung**, Redactable Signatures for Signed CDA Documents, *Journal of Medical Systems*, Vol. 36, No. 3, pp. 1975-1808, June, 2012. (SCI, IF: 1.064)
23. Z. Y. Wu, Y. C. Lee, F. Lai, H. C. Lee, and **Y. F. Chung**, A Secure Authentication Scheme for Telecare Medicine Information Systems, *Journal of Medical Systems*, Vol. 35, No. 3, pp. 1529-1539, June, 2012. (SCI, IF: 1.064)

**(B) 研討會論文**

1. Z. Y. Wu, D. L. Chiang, T. C. Lin, **Y. F. Chung** and T. S. Chen, A Reliable Dynamic User-Remote Password Authentication Scheme over Insecure Network, *26th International Conference on Advanced Information Networking and Applications* (*AINA 2012*), pp. 25-28, Fukuoka, Japan, March, 2012.

2. Ching-Wei Hsu, Xiao-Ou Ping, Ja-Der Liang, Yi-Ju Tseng, Ya-Lin Wu, Pei-Ming Yang, Guan-Tarn Huang, **Y.F. Chung**, and Feipei Lai, "A CBR-based method for retrieving similar patients from case base," AMA IEEE Medical Technology Conference 2011, Boston, U.S.A., Oct. 16-18, 2011. (EI)

3. **Y. F. Chung**, M. H. Kao, T. L. Chen, and T. S. Chen, Efficient date-constraint access control and key management scheme for mobile agents, *IMECS 2010*, pp. 252-257 , Hong Kong, China, March 17-19, 2010. (EI)

4. C. H. Liu, **Y. F. Chung**, J. D. Jhuo, T. S. Chen, and S. D. Wang, A Novel Time-bound Hierarchical Key Assignment Scheme for Mobile Agent, *IMECS 2010*, pp. 258-263 , HongKong, China, March 17-19, 2010. (EI)

# 出席國際會議報告

2012 年 03 月 26~29 日

| 報告人姓名 | 鐘玉芳 | 職稱 | 電機系副教授 |
|---|---|---|---|
| 會議期間 | 2012.03.26 至 2012.03.29 | | |
| 會議地點 | 日本九州福岡工業大學 | | |
| 會議名稱 | 2012 26th International Conference on Advanced Information Networking and Applications Workshops (WAINA 2012) | | |
| 發表論文題目 | A Reliable Dynamic User-Remote Password Authentication Scheme over Insecure Network | | |

與會心得

26th International Conference on Advanced Information Networking and Applications Workshops (WAINA 2012)，在今年2012年3月26-29日於日本九州福岡工業大學舉行，吸引了超過一百位多位的專家學者參加，亦是來自 20多個國家- 如台灣、日本、韓國、香港、澳洲、印度、美國、新加坡...等國家，共計100多篇論文，分為Internet Computing and Web Applications、Wireless Mesh Networks、Dependable and Fault Tolerant Systems、Architectures and Middleware、Cryptography, Authentication and Security、Context Aware Middleware、Clustering and Classfication 、Efficient Resource Management and Allocation、Mobile and Ad Hoc Networks、Energy-Efficient Wireless Networks、Intelligent Systems and Applications、Wireless and Mobile Network Applications、Privacy and Information Poisoning、Sensor and Ad-Hoc Applications 、Information Retrieval 、Efficient Data Management and Allocation 、Distributed Database and Data Mining、Video Streaming and Life Streaming、Intrusion Detection and Blind Signature…進行發表。

議程中安排我發表論文的場次是W-FINA-S2，發表主題是關於Cryptography, Authentication and Security，時段為當地時間2012年03月26日上午11點00分至12點30分，報告時間約20分鐘，論文發表完畢後，會中主持人及與會學者也都熱烈討論、提出自己的見解與問題，大家都有著高度的學習熱誠，尤其國外學者們的研究成果及表達的邏輯思考能力，更是令人欽佩，讓我對於學習態度的收穫更大於對專業技能之收益。而在這幾天參與過程中，與來自世界各國的精英學者們接觸之後，我更深深感受到積極參與國際研討會的必要性，藉由研討會中有不同研究發表的新穎性，在國際研討會上我們可得到各國最新研究的資訊，也可交流我們的研究成果。總而言之，本次國際綜合型研討會不僅開拓個人視野外，更對國際上相關技術與發展有更進一步的認識。

# A Reliable Dynamic User-Remote Password Authentication Scheme over Insecure Network

[1]Zhen-Yu Wu, [2]Dai-Lun Chiang, [2]Tzu-Ching Lin, [3]Yu-Fang Chung, [2]Tzer-Shyong Chen
[1]Department of Information Management, National Penghu University of Science and Technology, Taiwan
[2]Department of Information Management, Tunghai University, Taiwan
[3]Department of Electrical Engineering, Tunghai University, Taiwan
E-mail: yfchung@thu.edu.tw

***Abstract*—Protocols of user authentication are able to ensure the security of data transmission and users' communication over insecure networks. Among various authenticated mechanisms run currently, the password-based user authentication, because of its efficiency, is the most widely employed in different areas, such as computer networks, wireless networks, remote login, operation systems, and database management systems. Even as password is endowed with the property of simple and human memorable, for which causes such an attack of brute force; for example, the previous works often suffer off-line password guessing attack. Therefore, an ameliorative password-based authentication scheme is proposed in this paper, achieving to resist off-line password guessing attacks, replay attacks, on-line password guessing attacks, and ID-theft attacks. In light of security, the proposed scheme is provided with good practicability, even over insecure network.**

***Keywords-Authentication; Password; Off-line password guessing attack; ID-theft attack;***

## I. INTRODUCTION

Under more intricate network environments than before, the question of how to ensure the security of data transmission and users' communication in such insecure channels has become much more important. To solve this kind of problem, some relevant user authentication schemes and some secret-key distribution protocols are proposed and have become the most significant security services in communication networks nowadays. Note that the protocols of user authentication and secret-key distribution are both the primary safeguards in network electronic applications. Among these protocols, Password-based mechanism is the most widely employed method because of its efficiency. Under such mechanism, each user is allowed to select a password and keep in mind himself without any additional assistant device for user authentication. The first remote user authentication scheme based on the concept of the password-based technology was proposed by Lamport in 1981 [4]. Yet, some security flaws were pointed out in [2], and these flaws would cause the whole authentication system to be insecure; therefore, many improved schemes were proposed in terms of security considerations or authentication practicability [3, 5-8, 10].

Also based on the password-based technology, Das et al. proposed a dynamic ID-based remote user authentication scheme in 2004 [1]. In their scheme, each user can choose or change his password anytime and anywhere and there is no business with the server, which means that the server does not have to keep maintaining any password verifier tables. Though Das et al.'s scheme showed its security against ID-theft attacks, replay attacks, and other malicious attacks, Wang et al. indicated recently that their scheme was completely insecure because of its independence of the password [9]. Besides, Wang et al. also pointed out some weaknesses in their scheme would make their scheme vulnerable. Thus, Wang et al. proposed an improved solution. An overview of Wang et al.' s scheme is done in the next section. Unfortunately, Wang et al.'s scheme is shown not able to withstand the off-line password guessing attack, and furthermore, the real IDs are transmitted in insecure channels in their scheme, which makes the property of dynamic identity ineffective.

The rest of this paper is organized as follows. In Section 2, we first review Wang et al.'s authentication scheme. Their security weaknesses are discussed in Section 3. In Section 4, we will present our enhanced remote password-based authentication scheme. Following, Security analyses are done in Section 5, and conclusions are drawn in Section 6.

## II. REVIEW OF WANG ET AL.'S SCHEME

Wang et al.'s scheme is basically composed of four phases; they are the registration phase, the login phase, the verification phase, and the password-change phase. The notation defined and used in their scheme is shown in Table I.

TABLE I. NOTATION DEFINED AND USED IN WANG ET AL.'S SCHEME

| | |
|---|---|
| $U$ | the user |
| $pw$ | the password of user U |
| $ID$ | the identity of user U |
| $S$ | the remote server |
| $h(.)$ | a public one-way hash function |
| $\oplus$ | a bit-wise XOR operation |

### A. *Registration phase*

Suppose user $U_i$ wants to register to a remote server $S$. Then he proposes a registration request so as to get his password and his smart card from the server as follows.

Step 1: $U_i$ sends his own identification $ID_i$ to $S$.

Step 2: $S$ computes $N_i = h(pw_i) \oplus h(x) \oplus ID_i$, where $x$ is the secret of the remote server, $pw_i$ is the password of $U_i$ chosen by $S$.

Step 3: $S$ personalizes the $U_i$'s smart card included with the parameters $[h(\cdot), N_i, y]$, where $y$ is a secret number chosen by the remote server and unknown to any other users.

Step 4: $S$ returns $pw_i$ and the smart card to $U_i$ through a secure channel.

### B. *Login phase*

When user $U_i$ wants to log into the remote server $S$, he firstly inserts his smart card into a terminal and then keys in his identification $ID_i$ along with his password $pw_i$. The smart card will execute the following steps automatically:

Step 1: Compute a dynamic ID for user $U_i$ at time $T$.

$CID_i = h(pw_i) \oplus h(N_i \oplus y \oplus T) \oplus ID_i$, where $T$ is the time stamp according to $U_i$'s computer.

Step 2: Send $ID_i$, $CID_i$, $N_i$, and $T$ to server $S$ through the common channel.

### C. *Verification phase*

When server $S$ receives a login request ($ID_i$, $CID_i$, $N_i$, $T$) at time $T'$, server $S$ does the verification as follows:

Step 1: Check the validity of the time interval. If $T^* - T \leq \Delta T$ holds, $S$ will accept the login request; otherwise, the login request is rejected.

Step 2: Compute $h'(pw_i) = CID_i \oplus h(N_i \oplus y \oplus T) \oplus ID_i$.

Step 3: Compute $ID'_i = N_i \oplus h(x) \oplus h'(pw_i)$.

Step 4: Verify whether $ID'_i$ is equivalent to $ID_i$. If it is, the login request is accepted; otherwise, the login request is rejected. Then $S$ computes

$a' = h(h'(pw_i) \oplus y \oplus T')$.

Step 5: Send ($a'$, $T'$) to user $U_i$ for a mutual authentication processing.

When user $U_i$ receives the reply message ($a'$, $T'$) at time $T''$, he does the verification as follows:

Step 1: Check whether $T^* - T' \leq \Delta T$ holds. If it does, user $U_i$ will accept the reply message and go on the next step; otherwise, he refuses the reply message.

Step 2: Compute $a = h(h'(pw_i) \oplus y \oplus T')$.

Step 3: Verify whether $a$ is equivalent to $a'$. If they are equivalent, user $U_i$ confirms that server $S$ is valid.

### D. *Password-change phase*

When user $U_i$ wants to change his password, he inserts his smart card into a terminal device. He firstly keys in his old password $pw_i$ and then follows his new password $pw_{new}$. The smart card will execute the following steps:

Step 1: Compute $N_i^* = N_i \oplus h(pw_i) \oplus h(pw_{new})$.

Step 2: Replace the original $N_i$ with this new one, $N_i^*$, and then the password is changed.

## III. WEAKNESSES IN WANG ET AL.'S SCHEME

In this section, we would like to point out the weaknesses in Wang et al.'s scheme. As we mentioned above, Wang et al.'s scheme is vulnerable to the off-line password guessing attack. Suppose an adversary A is one of the legitimate users in their proposal. He can make use of the parameters in hand to compare them with those intercepted information to guess the password of a certain user. The guessing procedure can be done in four steps iteratively shown in the following.

Step 1: Adversary $A$ guesses a possible password $pw'_i$ of user $U_i$, and calculates its corresponding hashing value $h(pw'_i)$ through the hash function $h(\cdot)$.

Step 2: Adversary $A$ uses the grabbed parameters $N_i$ and $ID_i$, which have been intercepted from user $U_i$, to compute $h(x') = N_i \oplus ID_i \oplus h(pw'_i)$.

Step 3: Adversary $A$ takes his own password $pw_a$ and identification $ID_a$ to XOR the hashing value $h(x')$; that is, he does the computation of $h(pw_a) \oplus ID_a \oplus h(x')$, and then compares the calculated value with the parameter $N_a$ of $A$ to see whether they are equivalent.

Step 4: If they are equivalent, then the guessed $pw'_i$ will be the valid password of user $U_i$.

If the value of $h(pw_a) \oplus ID_a \oplus h(x')$ is not equivalent to the parameter $N_a$ of $A$, Adversary $A$ will do the procedure from Step 1 to Step 4 again till the valid password of the eavesdropped user is gotten. Besides, their scheme employs user's real ID to convey in the login phase, which makes the property of dynamic identity meaningless, and also exposes the user to the risks of ID-theft attacks.

## IV. THE IMPROVED REMOTE AUTHENTICATION SCHEME

In this section, we would like to propose an improved remote authentication scheme to Wang et al.'s. We will modify some system parameters and procedural steps in Wang et al.'s scheme so as to withstand the off-line password guessing attacks, and to resist other attacks such as on-line password guessing attacks, and replay attacks. At the same time, our method reaches the characteristics of dynamic identity which lacked in Wang et al.'s. Our scheme is also composed of four phases. They are the registration phase, the login phase, the verification phase, and the password-change phase. Below is the detailed description of our proposal.

### A. Registration phase

Suppose user $U_i$ wants to register to a remote server $S$. Then he proposes a registration request so as to get his password and his smart card from the server as follows.

Step 1: $U_i$ sends his own identification $ID_i$ to $S$.

Step 2: $S$ computes $N_i = h(pw_i) \oplus h(x \| h(y \| ID_i)) \oplus ID_i$, where $\|$ is a bit concatenation operator, $x$ is the secret of the remote server, $pw_i$ is the password of $U_i$ chosen by $S$, and $y$ is a secret number selected by the remote server and stored into each registered user's smart card. The number $y$ is well protected by the device of smart card, and no user, even the smartcard holder, can catch the value of $y$.

Step 3: $S$ personalizes $U_i$'s smart card included with the parameters $[h(\cdot), N_i, y]$.

Step 4: $S$ returns $pw_i$ and the smart card to $U_i$ through a secure channel.

### B. Login phase

When user $U_i$ wants to log into the remote server $S$, he firstly inserts his smart card into a terminal and then keys in his identification $ID_i$ along with his password $pw_i$. The smart card will execute the following steps automatically:

Step 1: Compute a dynamic ID for user $U_i$ at time $T$.

$$CID_i = h(pw_i) \oplus h(N_i \oplus y \oplus T) \oplus h(y \| ID_i),$$

where $T$ is the time stamp according to $U_i$'s computer.

Step 2: Send $h(y \| ID_i)$, $CID_i$, $N_i$, and $T$ to server $S$ through the common channel.

### C. Verification phase

When server $S$ receives the login request $(h(y \| ID_i), CID_i, N_i, T)$ at time $T'$, server $S$ does the verification as follows:

Step 1: Check the validity of the time interval. If $T^* - T \leq \Delta T$ holds, $S$ accepts the login request of $U_i$; otherwise, the login request is rejected.

Step 2: Compute $h'(pw_i) = CID_i \oplus h(N_i \oplus y \oplus T) \oplus h(y \| ID_i)$.

Step 3: Compute $ID'_i = N_i \oplus h(x \| h(y \| ID_i)) \oplus h'(pw_i)$, and then hash the value with $y$ to form $h(y \| ID'_i)$.

Step 4: Verify whether $h(y \| ID'_i)$ is equivalent to $h(y \| ID_i)$. If it is, $S$ accepts the login request of $U_i$; otherwise, the login request is rejected. Then $S$ computes $a' = h(h'(pw_i) \oplus y \oplus T')$.

Step 5: Send $(a', T')$ to $U_i$ for a mutual authentication processing.

When user $U_i$ receives the reply message $(a', T')$ from server $S$ at time $T''$, $U_i$ does the verification as follows:

Step 1: Check whether $T^* - T' \leq \Delta T$ holds. If it does, user $U_i$ will accept the reply message and go on the next step; otherwise, he refuses the reply message.

Step 2: Compute $a = h(h'(pw_i) \oplus y \oplus T')$.

Step 3: Verify whether $a$ is equivalent to $a'$. If they are equivalent, user $U_i$ confirms that server $S$ is valid.

### D. Password change phase

When user $U_i$ wants to change his password, he inserts his smart card into a terminal device. He firstly keys in his old password $pw_i$ and then follows his new password $pw_{new}$. The smart card will execute the following steps:

Step 1: Compute $N_i^* = N_i \oplus h(pw_i) \oplus h(pw_{new})$.

Step 2: Replace the original $N_i$ with this new one, $N_i^*$, and then the password is changed.

## V. SECURITY ANALYSES

In this section, we would like to examine the security of our proposed scheme in terms of the following possible attacks: Replay attacks, On-line password guessing attacks, Off-line password guessing attacks, and ID-theft attacks.

### A. Replay attacks

A replay attack is a kind of network attack in which a valid data transmission is repeated maliciously. This kind of attack is generally done by some machinated adversary, who intercepts the data and transmits it repeatedly. In our scheme, we employ the concept of a time stamp to avoid such attacks. When server $S$ or user $U_i$ receives a message, he firstly calculates the difference between the current time $T^*$ and transmitted time $T$. And then he will check whether the difference is smaller than $\Delta T$. If it is, then the message is valid; otherwise, the message may be re-sent. Therefore, the replay attack is fruitless.

### B. On-line password guessing attacks

An on-line password guessing attack means that an attacker continuously guesses a possible password and tries to log into a remote server until he is successful. In our scheme, such attacks can be detectable. If an adversary attempts to identify the password of $U_i$, he is supposed to use every guessed password to obtain the corresponding $CID_i$ in the login phase. However, the probability of guessing the correct password is only $2^{-k}$, where $k$ is the length of the selected password. Generally, if a guess is wrong, server $S$ can detect easily that there is an adversary trying to acquire services illegally. Therefore, on-line password guessing attacks cannot succeed.

### C. Off-line password guessing attacks

An off-line password guessing attack means that an attacker can employ some intercepted information to guess the password of a specific user by brute force attacks. Take a glance on our scheme. The secret parameters such as $x$ and $y$ are protected by the cryptographic hash function and are not revealed to anyone; thus, this kind of attack will not work. Now, assume that an adversary has obtained the following parameters ($h(y \| ID_i)$, $CID_i$, $N_i$, $T$) in the login phase. However, without $y$, he cannot compute $h'(pw_i) = CID_i \oplus h(N_i \oplus y \oplus T) \oplus h(y \| ID_i)$. Similarly, it is also unable for him to calculate $h'(pw_i) = N_i \oplus h(x \| h(y \| ID_i)) \oplus ID'_i$ without $x$ and $ID_i$. Therefore, off-line password guessing attacks can be withstood.

### D. ID-theft attacks

An ID-theft attack means that a user's real identification is stolen and misappropriated for illegal crimes. In our proposal, user's real ID is concatenated with the secret number $y$ under the protection of a cryptographic hash function in all common exchanged messages. Therefore, it is a very difficult task for an adversary to identify or thieve a user's ID. Moreover, the property of dynamic identity issued by Das et al. can be kept in our scheme.

## VI. CONCLUSIONS

In this paper, we analyze the security weaknesses in the dynamic ID-based remote user authentication scheme proposed by Wang et al., and consequently propose an improved scheme. Compared to their scheme, our scheme makes their advantages kept and improves much more on resisting the replay attacks, on-line password guessing attacks, off-line password guessing attacks, and ID-theft attacks. This shows that our scheme is more secure and efficient to be implemented.


## ACKNOWLEDGMENT

This work was supported partially by National Science Council of Republic of China under Grants NSC 100-2221-E-029-017.


## REFERENCES


[1] Das, M. L., Saxena, A., Gulati, V. P., "A dynamic ID-based remote user authentication scheme," *IEEE Transactions on Consumer Electronics, 50 (2)*, pp. 629-631, 2004.

[2] Hwang, M.S., & Li, L.H., "A new remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics, 46 (1)*, pp. 28-30, 2000.

[3] Ku, W.C., & Chen, S.M., "Weaknesses and improvements of an efficient password base remote user authentication scheme using smartcards," *IEEE Transactions on Consumer Electronics, 50 (1)*, pp. 204-206, 2004.

[4] Lamport, L. "Password authentication with insecure communication," *Communications of the ACM, 24*, 1981.

[5] Lee, C.C., Li, L.H., & Hwang, M.S., "A remote user authentication scheme using hash functions," *ACM Operating Systems Review, 36 (4)*, pp. 23-29, 2002.

[6] Liao, I.E., Lee, C.C., & Hwang M.S., "A password authentication scheme over insecure networks," *Journal of Computer and System Sciences, 72*, pp. 727-740, 2006.

[7] Sun, H.M., & Yen, H.T., "Password-Based Authentication and Key Distribution Protocols with Perfect Forward Secrecy," *Journal of Computer System Science, 72*, pp. 1002-1011, 2006.

[8] Wu, S., & Chieu, B., "A user friendly remote authentication scheme with smart cards," *Computers and Security, 22 (6)*, pp. 547-550, 2003.

[9] Wang, Y.Y., Liu, J.Y., Xiao, F.X., & Dan, J., "A more efficient and secure dynamic ID-based remote user authentication scheme," *Computer Communications, 32*, pp. 583-585, 2009.

[10] Yoon, E., & Yoo, K., "An efficient password authentication schemes without using the server public key for grid computing," *GCC 2005, LNCS 3795*, pp. 149-154, 2005.

# 國科會補助計畫衍生研發成果推廣資料表

日期:2012/08/21

| 國科會補助計畫 | 計畫名稱: 安全多方計算協定的研究與應用 |
|---|---|
| | 計畫主持人: 鐘玉芳 |
| | 計畫編號: 100-2221-E-029-017- 學門領域: 資訊安全 |

無研發成果推廣資料

# 100 年度專題研究計畫研究成果彙整表

| 計畫主持人：鐘玉芳 | 計畫編號：100-2221-E-029-017- |
|---|---|
| 計畫名稱：安全多方計算協定的研究與應用 | |

| 成果項目 | | | 量化 | | | 單位 | 備註（質化說明：如數個計畫共同成果、成果列為該期刊之封面故事...等） |
|---|---|---|---|---|---|---|---|
| | | | 實際已達成數（被接受或已發表） | 預期總達成數(含實際已達成數) | 本計畫實際貢獻百分比 | | |
| 國內 | 論文著作 | 期刊論文 | 0 | 0 | 100% | 篇 | |
| | | 研究報告/技術報告 | 0 | 0 | 100% | | |
| | | 研討會論文 | 0 | 0 | 100% | | |
| | | 專書 | 0 | 0 | 100% | | |
| | 專利 | 申請中件數 | 0 | 0 | 100% | 件 | |
| | | 已獲得件數 | 0 | 0 | 100% | | |
| | 技術移轉 | 件數 | 0 | 0 | 100% | 件 | |
| | | 權利金 | 0 | 0 | 100% | 千元 | |
| | 參與計畫人力（本國籍） | 碩士生 | 2 | 2 | 100% | 人次 | |
| | | 博士生 | 1 | 1 | 100% | | |
| | | 博士後研究員 | 0 | 0 | 100% | | |
| | | 專任助理 | 0 | 0 | 100% | | |
| 國外 | 論文著作 | 期刊論文 | 2 | 2 | 100% | 篇 | |
| | | 研究報告/技術報告 | 0 | 0 | 100% | | |
| | | 研討會論文 | 1 | 1 | 100% | | |
| | | 專書 | 0 | 0 | 100% | 章/本 | |
| | 專利 | 申請中件數 | 0 | 0 | 100% | 件 | |
| | | 已獲得件數 | 0 | 0 | 100% | | |
| | 技術移轉 | 件數 | 0 | 0 | 100% | 件 | |
| | | 權利金 | 0 | 0 | 100% | 千元 | |
| | 參與計畫人力（外國籍） | 碩士生 | 0 | 0 | 100% | 人次 | |
| | | 博士生 | 0 | 0 | 100% | | |
| | | 博士後研究員 | 0 | 0 | 100% | | |
| | | 專任助理 | 0 | 0 | 100% | | |

| | |
|---|---|
| 其他成果<br>(無法以量化表達之成果如辦理學術活動、獲得獎項、重要國際合作、研究成果國際影響力及其他協助產業技術發展之具體效益事項等，請以文字敘述填列。) | 1. 參加日本九州福岡工業大學舉行的國際研討會，26th International Conference on Advanced Information Networking and Applications Workshops (WAINA 2012)<br>2. 2011 年瑞士日內瓦國際發明展得金牌：指導電機系蔡孟洋同學參加瑞士日內瓦國際發明展。其設計的「床邊照護視訊系統」獲得此次金牌獎。此項作品是利用創意改造而成為醫院床邊實用視訊系統，使資訊傳達、監視記錄、醫療服務等功能更完善、貼心，可滿足使用者全面性需求，並兼顧使用簡易與隱私安全，而獲得評審青睞。<br>3. 2011 年瑞士日內瓦國際發明展得金牌及特別獎：指導東大附中捷安特巨大董事長劉金標的雙胞胎孫女劉韋彤、劉韋均參加 2011 年瑞士日內瓦國際發明展得金牌及特別獎，其設計的「發音練習矯正系統」獲得此次金牌獎及特別獎。利用光學干涉原理，將攝影鏡頭藏於鏡子後面，運用錄影幫助弱勢小朋友練習及矯正英文發音。 |

| | 成果項目 | 量化 | 名稱或內容性質簡述 |
|---|---|---|---|
| 科教處計畫加填項目 | 測驗工具(含質性與量性) | 0 | |
| | 課程/模組 | 0 | |
| | 電腦及網路系統或工具 | 0 | |
| | 教材 | 0 | |
| | 舉辦之活動/競賽 | 0 | |
| | 研討會/工作坊 | 0 | |
| | 電子報、網站 | 0 | |
| | 計畫成果推廣之參與（閱聽）人數 | 0 | |

# 國科會補助專題研究計畫成果報告自評表

請就研究內容與原計畫相符程度、達成預期目標情況、研究成果之學術或應用價值（簡要敘述成果所代表之意義、價值、影響或進一步發展之可能性）、是否適合在學術期刊發表或申請專利、主要發現或其他有關價值等，作一綜合評估。

1. 請就研究內容與原計畫相符程度、達成預期目標情況作一綜合評估

■達成目標

□未達成目標（請說明，以 100 字為限）

□實驗失敗

□因故實驗中斷

□其他原因

說明：

2. 研究成果在學術期刊發表或申請專利等情形：

論文：■已發表 □未發表之文稿 □撰寫中 □無

專利：□已獲得 □申請中 ■無

技轉：□已技轉 □洽談中 ■無

其他：(以 100 字為限)

3. 請依學術成就、技術創新、社會影響等方面，評估研究成果之學術或應用價值（簡要敘述成果所代表之意義、價值、影響或進一步發展之可能性）(以 500 字為限)

本研究旨在探討安全多方計算之基本運算與協定、設計高效能的安全多方計算協定、評估安全多方計算之複雜度，並且以模運算及秘密分享協定為基礎，建構一般化的安全多方計算應用模式。因此，本研究針對公開模運算之減化 (Public Module Reduction) 與秘密模次方運算 (Private Module Exponentiation)，進行分析，藉以獲得知識，將基礎協定中的位元分解 (Bit Decomposition) 擴展為數位分解協定及數位位元分解協定，使現行協定的複雜度從 O(nlogn) 降為線性時間，開發高效能的秘密位元運算協定，同時也使安全多方計算協定的應用更趨於多元。本研究方法採用具有可驗證的秘密分享 VSS(Verifier Secret Sharing)協定，提出複雜度較低的可驗證秘密分享協定。此外，本研究更針對 UC (Universally Compostable) 模型下多方函數安全計算之充分必要條件進行探討。攻擊模式的選擇對於安全理論的建立，相當重要，因此本研究以來自內部惡意參與者的 Cut-and-Choose 攻擊模式為安全設計之主要考量，提出安全的雙方計算協定設計。為了檢測惡意參與者輸入參數的一致性，協定使用簡單映射，以提高協定效率。