結合NTRU公開金鑰密碼系統與行動條碼以強化交易安全機制

Transaction Security Enhancement Achieved by Integrating NTRU-based Public Key Cryptosystem with QR Code

張浩銘
崇右技術學院休閒事業經營系
義七路40號
基隆市201信義區
hchang0608@gmail.com

陳志誠
大同大學資訊經營學系
中山北路三段40號
台北市104中山區
chenps@ttu.edu.tw

簡銘成
大同大學資訊經營學系
中山北路三段40號
台北市104中山區
s0300882@hotmail.com

摘要

行動條碼(QR Code)具有系統架構開放、抗污損，建置成本低廉等優點，加上設備普及，在各個商務層面中被廣泛應用。但也由於條碼標籤規格開放，且易於產生與複製等之特點，在防偽的機制上並無健全的機制。有鑑於此，本研究提出行動條碼整合NTRU公開金鑰密碼系統之防偽機制，其特點除可滿足行動通訊裝置與行動條碼之需求外，亦可將研究延伸至各項資訊安全防護。與其它非對稱式密碼系統比較之下，NTRU具有金鑰短、產生速度快與加解密速度高的優點，也是在理論上可以有效抵擋未來"量子計算機"攻擊之密碼系統。在本研究中，我們將針對行動商務之付款流程，建立一個有效且安全的機制，透過本論文所提出的方法，能夠將二維條碼的應用範圍擴大，也避免傳統交易方式的風險，讓顧客與供應商可以更安全地完成每一筆交易，有助於未來行動商務的推廣，強化使用者對行動商務的信賴感。在實證上，我們將NTRU公開金鑰密碼系統與行動條碼作結合，發展出一個系統雛型，加解密速度很快。在應用面上，此一系統可以強化商家對條碼票證的真偽驗證，也可協助客戶正確使用該票證，使交易更安全可靠，有助於行動商務的健全發展。在電子化政府的應用上，利用條碼可使民眾正確登入政府網站，也可以讓民眾方便得申請戶籍、地籍等謄本，作好便民措施。

關鍵詞: 行動商務、資訊安全、公開金鑰密碼系統、NTRU、行動條碼。

Abstract

Barcode is operated on a well-established open system. The tags can be generated and copied easily and cheaply, so it is widely used in a variety of business sectors, also in mobile commerce. Since the tag specifications are open to the public and the tags can be read easily, security mechanism should be enhanced. Herein, we suggest the use of NTRU encryption in barcode system to enhance security in mobile applications. Compared to other asymmetric encryption systems, NTRU has the advantages of short key, high speed in computation and high security. It can even resist the attacks from future quantum computers. In this research, we illustrate its application in mobile transactions, aiming to establish an effective and safe process. Through the methods proposed in this paper, the two-dimensional QR code can further expand its scope of applications. It can also avoid the risks in trading, so that customers and suppliers can complete their transactions more quickly and safely. It will help promote future business operations, by enhancing the trust of users in e.g. mobile business. We have implemented a prototype based on the NTRU public key cryptosystem integrated with QR code and assessed the effectiveness of using such a mechanism in mobile commerce. System evaluation reveals that the system can encrypt and decrypt in acceptable time. It can help merchant distinguish from tampered QR Code and help customer control the use of the code. There are also various possible applications in eGovernment.

Keywords: Mobile Commerce, Information Security, NTRU Cryptosystem, Quick Response Code.

一、導論

1. 研究背景

行動條碼(Quick Response Code, QR Code)具有系統架構開放、條碼標籤易於產生與複製、抗污損等優點，因建置成本低廉且設備普及，在各個商務環節中廣泛被應用。近年來，伴隨行動通訊裝置技術發展快速，進而促使條碼逐步應用於行動商務之領域上。國內已有相關單位引進行動條碼之技術，並運用於產品資訊之檢驗(方碼，2015)。

非對稱性密碼系統因為能解決身分認證和不可否認性等問題，因此廣泛被用在電子商務和電子化政府之上。現今常見之RSA與Elliptic Curve等公開金鑰密碼系統，其系統安全性建 立於因數分解與離散對數問題難以破解之基礎上，雖廣泛應用於資訊安全防護之各項工作中，但有計算速度慢的缺點。有人曾提出行動條碼結合RSA公開金鑰密碼系統之學理研究(翁仍方，2007)，且可應用於行動條碼相關資訊傳遞之實務，但此防偽機制仍受限於行動通訊裝置計算能力薄弱與行動條碼資訊儲存量有限之困境，導致資訊安全之防護工作仍有待提升，以進一步滿足行動交易付款或其它機敏資料傳遞之需求。

NTRU密碼系統在國際上已經被IEEE所重視，並且成立IEEE 1363 Working Group制定標準，而NTRU也是美國國家標準及技術局(NIST)所認定，最能夠抵擋量子攻擊的密碼系統。

2. 研究問題

本研究將採用NTRU公開金鑰密碼系統以替補上述系統應用於實務時能力之不足；NTRU密碼系統具有金鑰長度短、金鑰便於產生、加解密速度快與所需記憶體少等特點，可滿足行動通訊裝置與行動條碼兩者之需求。而藉由本階段對於NTRU公開金鑰密碼系統之研究發展，更可確保行動條碼相關資訊防護得以完善，亦促使行動條碼進一步拓展行動商務應用之領域。

二、 文獻探討

1. 一維條碼與行動二維條碼

(1)行動條碼與分類

一維條碼乃最早之條碼應用。一維條碼以黑白條紋來表示，並以其粗細程度來定義資料內容。目前因為資訊的質與量發展迅速，一維條碼的儲存量已經不敷使用。Yang等人提及一維條碼不能直接表示資訊的內容，只能提供資料的索引值，因此若在缺乏網路與資料庫系統的環境中，一維條碼即失去資訊傳遞的功能。二維條碼的特性則突破一維條碼的限制，不僅在儲存量上面遠優於一維條碼，二維條碼本身即代表資訊的內容，不須再經由索引值查詢資料庫。可使用內建數位鏡頭的行動裝置掃描，經由軟體分析解讀，即可得到訊息內容(Yang et al. 2007；余忠憲，2013)。

現今行動條碼的主要代表者有日本Denso公司所提出之QR Code、美國Symbol Technologies公司所提出之PDF417、美國RVSI Acuity CiMatrix公司所提出之DataMatrix與美國UPS公司所提出之Maxi Code等種類。依編碼型態即可區分為堆疊式(Stacked)與矩陣式(Matrix) 兩種[1,2,3]。堆疊式行動條碼乃為一維條碼(Bar Code)之延伸，將其原有符號(Symbol)進行壓縮以增加訊息之容量，並藉此形成堆疊式行動條碼；而矩陣式行動條碼則運用二進位(Binary)之空白「0」與點「1」進行資訊內容顯示，並於條碼列印範圍內形成二維矩陣之幾何符號以利辨識。目前QR Code因其優勢，也為國內相關企業組織所廣泛採用[4,5,6] (黃信捷，1996)。

(2)行動條碼之安全性

依據行動上網聯盟(Open Mobile Internet Alliance, OMIA)於2005年5月所訂定之「行動條碼應用共通標準規範」[7]，可區分為自動化文字輸入、數位內容下載、網址快速連結與身份鑑別及商務交易等四大類。其中又以身份鑑別及商務交易之類別最為重要，國內系統設計者往往運用唯一性：單一序號(Sequential Number)、時效性：時戳(Timestamp)(Sun & Chen, 1999; Sun, 2000; Seino, 2004)與管制性：標章機制進行相關資訊

[1] Magicode <http://www.iconlab.com.tw/product_service.php> (Retrieved May 2011)
[2] QR code <http://www.denso-wave.com/qrcode/index-e.html> (Retrieved May 2011)
[3] Quickmark <http://diy.quickmark.com.tw/eten/?c=301> (Retrieved May 2011)
[4] 中華電信行動條碼 <http://qrcode.emome.net/qrcpromote/code01.html?vcrm=200804082143@8656616c8c27db0687cca4f0beb032a2> (Retrieved May 2011)
[5] 台灣農產品安全追溯資訊網 <http://taft.coa.gov.tw/welcome.asp?mp=8&role=C&mpap=A> (Retrieved May 2011)
[6] 網路小額付費機制 <http://www.micro-payment.net> (Retrieved May 2011)
[7] 行動上網聯盟 <http://www.meworks.net/meworksv2/meworks/page1.aspx?no=92> (Retrieved May 2011)

之防護(Gouda & Liu, 2004; Hasan & Raygan, 2007; Tan & Teo, 2007; Price, 2007)，以防有心人士從中獲取不當利益，但因條碼標籤規格開放且易於產生與複製等之特點，其防偽機制仍相當薄弱。

2. 公鑰密碼系統

資訊安全是一門綜合學科，所涉及內容涵蓋資訊理論、管理科學及密碼學等多方面知識，它的主要任務及內容是研究電腦系統和通信網路內資訊的保護及確保系統內資訊的可用、保密、真實和完整。資訊安全的核心之一是密碼技術。密碼是結合數學、電腦科學、電子與通信等諸多學科的技術。它不僅能夠保證機密性資訊的加密，而且能夠達到數位簽章、身份驗證、系統安全等功能。是現代化發展的重要科學之一。公鑰密碼系統、私鑰密碼系統及RSA 演算法為目前密碼學最廣泛流行及應用的顯學。在公鑰系統中，繼RSA 演算法之後，NTRU公鑰密碼演算法因其高效快速及運算簡單等特點，已逐漸獲得廣泛應用。

(1)公開金鑰系統簡介

目前的加密演算法按密鑰方式可分為單鑰密碼演算法和公鑰密碼演算法。單鑰密碼又稱對稱式密碼，是一種比較傳統的加密方式，其加密運算、解密運算使用的是同樣的密鑰，資訊的發送者和資訊的接收者在進行資訊的傳輸與處理時，必須共同持有該密碼（稱為對稱密碼）。因此，通信雙方都必須獲得這把鑰匙，並保持鑰匙的秘密。

公鑰密碼是美國史丹福大學的兩名學者Diffie與Hellman於1970年代提出的，在公鑰密碼系統中，加密和解密使用的是不同的密鑰，這兩個密鑰之間存在著相互依存關係：即用其中任一個密鑰加密的資訊只能用另一個密鑰進行解密。這使得通信雙方無需事先交換密鑰就可進行保密通信。其中加密密鑰和演算法是對外公開的，人人都可以通過這個密鑰加密檔然後發給收信者，這個加密密鑰又稱為公鑰；而收信者收到加密檔後,它可以使用他的解密密鑰解密，密鑰是由私人掌管不需要分發，因此又成稱為私鑰 (Shand & Vuillemin, 1993)。Hwang等人提及公鑰加密的另一用途是身份驗證：用私鑰加密的訊息，可以用公鑰拷貝對其解密，接收者由此可知這條信息確實來自於擁有私鑰的某人(Hwang, Su, Yeh, & Chen, 2005)。

(2)RSA密碼系統

RSA為目前最著名的公開金鑰密碼系統，是由三位MIT的學者Rivest、Shamir與Adleman於1978年提出(Rivest, Shamir & Adleman, 1978)。RSA密碼系統可作為加解密、數位簽章、金鑰交換等之用，其使用因數分解(factorization)的方式定義金鑰產生、加解密程序、簽署驗證程序。其安全性乃依賴該因數分解數學式的困難程度。

(3)Polynomial-Based NTRU密碼系統

具多項式基礎之公開金鑰密碼系統－NTRU，其特點為加解密速度快、金鑰長度小及安全性高等之屬性，並可適用於嵌入式裝置與安全性要求較高之環境，故極具實用之價值。NTRU因為有了商用產品問世，IEEE特別組織了一個Working Group IEEE P1363，制定標準，並撰寫相關技術文件[8]。 由於本研究立基於NTRU密碼系統，在此謹對其演算法簡介如下: NTRU是以一個代數結構環(Ring)為基礎。環結構的重要數學特性

[8] NTRU PKCS Tutorial <https://www.securityinnovation.com/uploads/Crypto/NTRU%20PKCS%20Tutorial.pdf> (Retrieved Dec 2015)

之一是乘法對加法的分配律。例如 $a*(b+c)=a*b+a*c$。 NTRU密碼系統中對乘法作一些稍微的修改，就是限制變數的次方: 利用截斷乘法(Truncated multiplication)以限制兩個多項式相乘之後，次方的增長。一個 $N-1$ 次方的截斷(Truncated Polynomials)多項式*a*所包含的係數如下：

$$a=[a_0+a_1x+a_2x^2+...+a_{N-1}x^{N-1}]\%(x^N-1)$$

其中%為求餘運算。NTRU密碼系統需要三個參數(*N*, *q*, *p*) ,其作用在於控制信息的長度、金鑰的長度，以及演算時變化多項式。這三個參數 (*N*, *q*, *p*)之作用分別為:

- *N*為在截斷多項式環中的多項式的次方。
- *q*大的模數(modulus): 通常該截斷多項式環的係數會以 *q*求餘數。
- *p*小的模數(modulus)作為解密的最後步驟，該訊息的係數將會以*p*求餘數。

加密程序使用多項式代數(Polynomial Algebra)與求餘運算以*p*和*q*降低模數之混合系統，而解密程序則依據機機率理論所進行。系統安全性來自多項式混合系統與降低模數*p*和*q* 獨立性之相互作用，且亦仰賴格(Lattice)難以尋找極短向量(Shortest Vector)之困難度。一般密碼系統由金鑰產生模組、加密模組和解密模組共同組成。

(A)金鑰產生模組

使用者B想要創造一對公私鑰以NTRU公鑰加密系統為基礎。我們首先隨機選擇兩個"小的"多項式*f*和*g*，*f*和*g*是由截斷多項式的集合 *R*中取出。

使用者B必須將多項式*f*和*g*之值保密，因為任何人知道這兩個多項式的任一個值，他們就能把訊息解密了。 算出 $f\%q$ 的反元素和 $f\%p$ 的反元素，亦即以下列算式算出多項式f_q *和* f_p

$$f*f_q=1\%q \quad 和 \quad f*f_p=1\%p$$

接著在算出以下之*h*值作為公鑰

$$h=(p*f_q*g)\%q$$

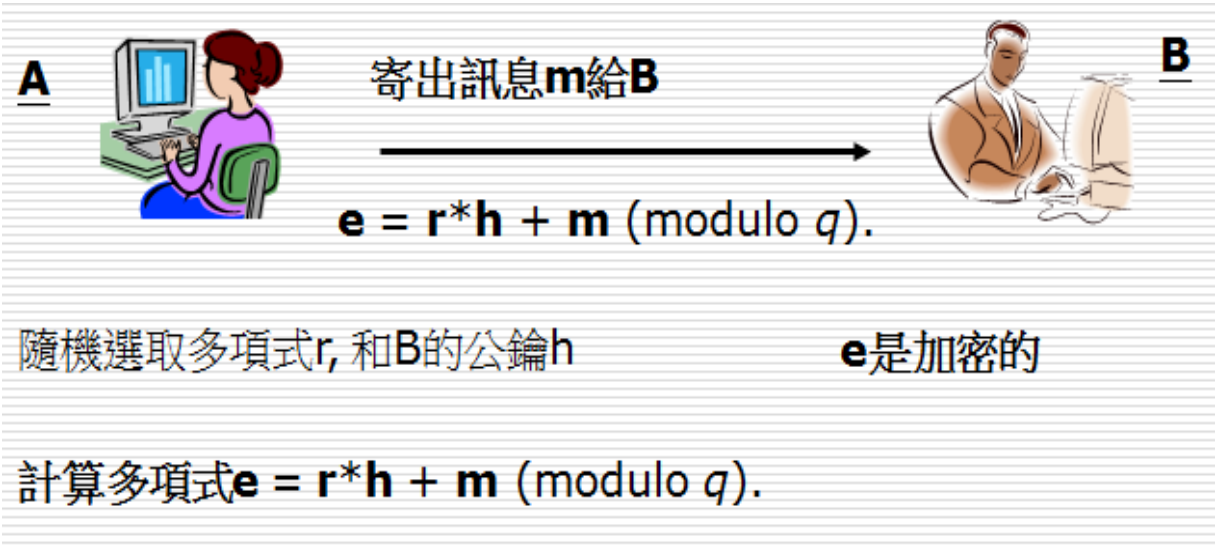
私鑰就是多項式*f* 和 f_p，公鑰是多項式*h*。

(B)加密模組

今有一位使用者A，欲寄信給使用者B(圖一)，他必須將信的明文*m*加密成為密文*e*，其公式如下：

$$e=(r*h+m)\%q$$

其中*r*是隨機選取的，*h*則是接收方A的公鑰。



圖一：A利用B的公鑰進行加密

(C)解密模組:

當B已收到A的加密訊息e，且他想要解密此訊息。B開始以他的私鑰多項式f，分三步驟計算，其結果以三個多項式a, b, c表示:

$$a = (f * e)\%q$$
$$b = a\%p$$

最後，B使用它的私鑰f_p算出c

$$c = (f_p * b)\%p = m;\ m \text{ 就是A的原始發送訊息。}$$

(D)正確性檢驗

$$a \equiv (f * e)\%q$$
$$\equiv (f * (r * h) + m)\%q \quad (\text{因為 } e = (r * h + m)\%q)$$
$$\equiv (f * (r * p * f_q * g + m))\%q \quad (\text{因為 } h = (p * f_q * g)\%q)$$
$$\equiv (f * (r * p * f_q * g + m))\%q \quad (\text{因為 } (f * f_q)\%q \equiv 1)$$
$$\because b \equiv (f * m)\%p$$
$$\therefore c \equiv (f_p * b)\%p = (f_p * f * m)\%p = m\%p = m \quad (\text{回復明文})$$

3. Polynomial Based NTRU密碼系統安全性分析

一般而言，對密碼系統的入侵方式有暴力攻擊(Brute force attack)、中介攻擊(Man-in-the-middle attack)(Howgrave-Graham, Silverman & Whyte, 2003)、多重傳輸攻擊(Multiple transmission attack)(Hoffstein & Silverman, 1998)、感應攻擊(Reaction attack)(Hoffstein & Silverman, 1999)、選擇密文攻擊(Chosen ciphertext attack) (Hoffstein & Silverman, 2000)與被Shamir提議的以格為基礎的攻擊(Lattice based attack)(Coppersmith &

Shamir, 1997)。在諸多研究中，都討論過NTRU密碼系統對不同方式的攻擊效果以及建議採取的回應，提高了NTRU系統的安全性。

在諸多密碼攻擊中，攻擊者可能建構有效密文去猜測相對應之明文，密碼學上稱為明文察覺(Plaintext aware)，而失敗之明文察覺將引起像是Bleichenbacher主動式選擇密文攻擊(Adaptive chosen ciphertext attack)。在以公開金鑰系統為基礎的通訊協定中，明文於開始加密前普遍上置入於數位信封(Digital envelope)，數位信封必須包含一些隨機填補(Padding)以避免相似於原有訊息與一些允許有效訊息驗證之特點。對於Bleichenbacher型態攻擊之對策，包含：

(1)頻繁變更金鑰。

(2)嚴格檢查解密後之訊息格式。

(3)於解密成功前，傳送者須證明資料之了解。

(4)如果訊息因任何理由遭致拒絕，則錯誤訊息之格式與時間應與傳送者相同。

(5)增加建構資料(包含資料雜湊)以降低訊息被接受之機率。

4. NTRU之優越性

由於NTRU的本質屬於公鑰密碼系統，可以使用JAVA實作NTRU系統，其計算速度優於RSA，因為多項式加法與乘法，皆可化為基本的算術運算，大幅提升計算效率。

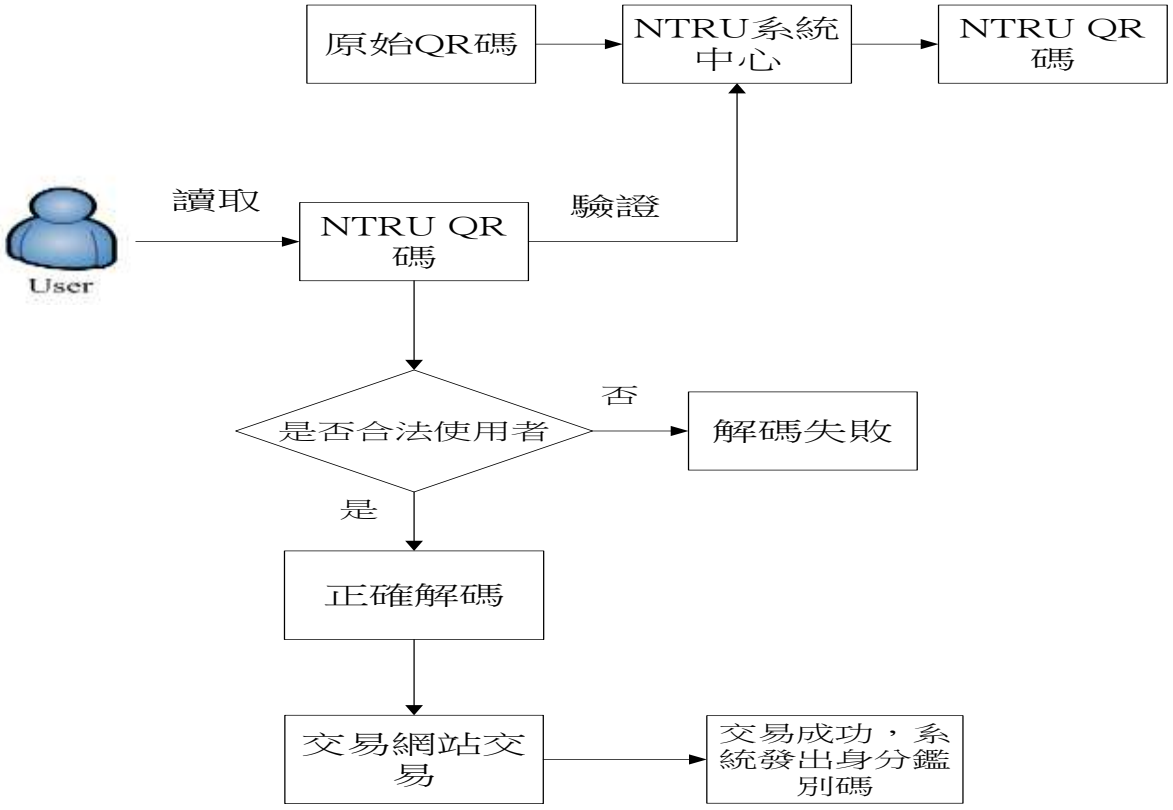
三、 系統分析與設計

1. 行動交易模式介紹

目前實務上QR CODE的交易應用，利用手機讀取鏡頭讀取條碼資訊，導引使用者連線至交易網站，引導客戶完成交易流程之後，系統自動發出QR 碼做為憑證，以便身分鑑別之用，大多應用於購買票卷。客戶必須妥善保管此驗證碼，以做為交易之證明。今以高鐵T Express為例，說明其購票流程如下 (高鐵T Express, 2015)：

- 乘客透過行動網路，到手機軟體程式市集，下載T Express，安裝於其至慧型手機；
- 透過購票系統介面，選擇車次、乘車日期時間、前往地點、座位等，取得訂位代號；
- 透過購票系統介面，進行付款；
- 付款完畢，乘客可以檢視購票資訊，並取得QR Code 車票。

圖二：利用QR Code的交易流程



圖三：導入NTRU之交易流程

以上的行動交易模式，雖然方便，不須透過電腦，用手機即可完成交易的流程(如圖二)所示。但若遭遇有心人的惡意攻擊，此種交易模式非常容易就有虞慮，例如：攻擊者惡意散佈假冒的QR CODE，引導消費者至釣魚網頁進行交易，不僅造成金錢上的損失，甚至客戶的帳戶密碼被盜，帳戶內存款可能被盜領，這也是使用者對於此類型交易無法完全信任原因之一。考慮行動裝置效率上的需求，我們建議導入NTRU密碼系統，進一步使得交易更迅速、安全。

(1)NTRU導入交易模式之交易流程

我們將上述的流程內容，加入了NTRU防護機制，目的在有效防堵有心人士故意偽造QR碼誘導使用者進入釣魚網頁。如果不合法的QR碼經過NTRU系統的驗證，就會發生驗證失敗，使用者即可避免掉入有心人士的陷阱中。系統在發出QR碼之前，將對QR碼經過演算法的流程進行加密，進而產生NTRU QR碼，由於NTRU演算法中即加入混淆值，即使同樣的交易網址，經過加密之後，也會是不同密文的NTRU QR碼，更能防禦一般的統計攻擊(如圖三)。完成交易後，系統經由演算法的加密，產生身分鑑別碼，也為使用者提供多一層的防護。

(2)系統開發環境

本研究使用Visual Basic 2005來進行開發，設計金鑰產生、加密、解密模組，QR CODE轉碼程式使用open source QR Code Library以C#設計，而Visual Basic 2005能透過

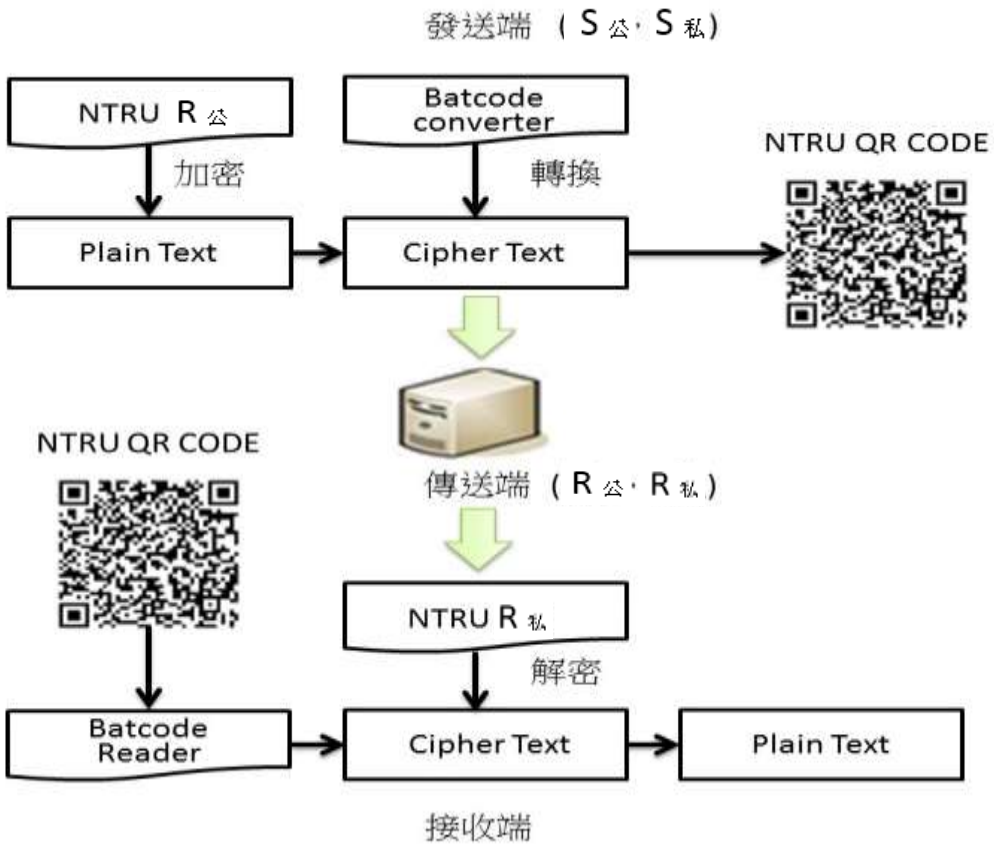
ADO.NET2.0或使用.NET Framework 2.0版新增的資料來源(Data Source)來存取資料庫的紀錄資料，來建立Visual Basic資料庫應用程式(陳會安，2006)。其硬體配備如下：

硬體： CPU：i3 540 3.07GHz
RAM：8G

軟體： 作業系統：Windows 7 64bit
Microsoft Visual Basic 2005
Microsoft Visual C #
Microsoft Office Access 2003

2. 系統流程與架構

本研究實作一個雛型介面，來實現NTRU加密演算法，並結合QR碼轉碼程。本系統架構圖 (如圖四)：



圖四：系統架構圖

系統介面說明

本系統分為四個部分，加密、解密、資料庫與一個QR碼產生模組。NTRU商用系統對安全性要求很嚴謹，參數數值很大(如表一)：

表一：商用NTRU系統參數

	N	*q*	*p*
普通安全	167	128	3
標準安全	251	128	3
高度安全	347	128	3
最高安全	505	256	3

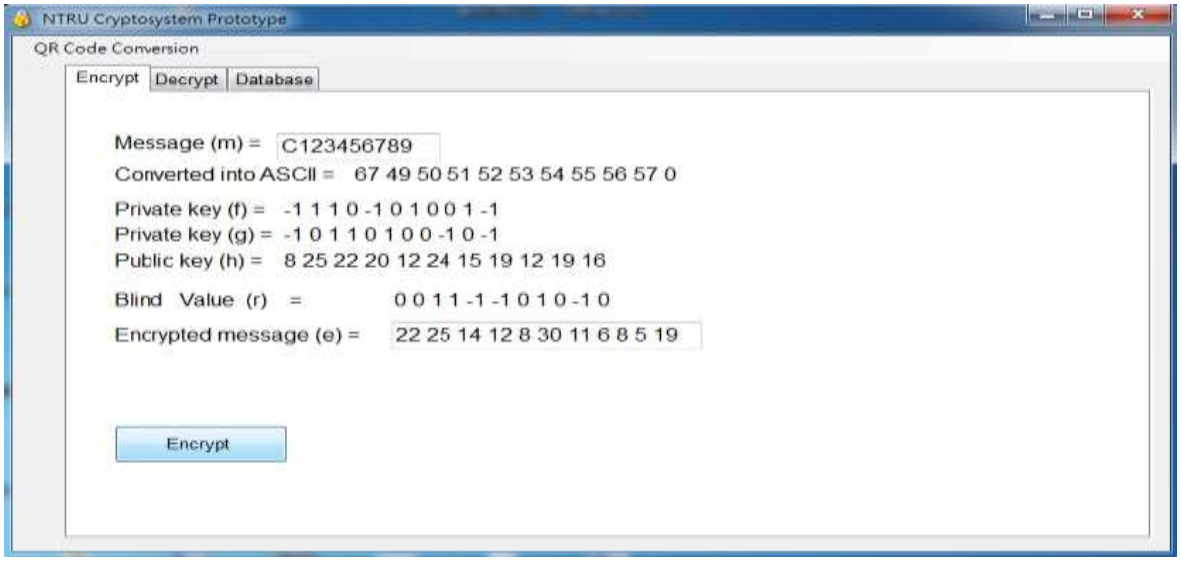
按照以上參數，計算所得數值極大，無法讓讀者一目了然。雖然我們所實作的雛型系統，亦採用普通安全標準參數(*N=167*、*q=128*、*p=3*)。為使易於說明起見，謹以NTRU tutorial (Hoffstein et al. 1998)上範例*N=11*、*q=32*、*p=3*為例作說明，以下我們以客戶的機密檔案代碼為例，對「客戶代碼」(C123456789)作加密；只有合法的商家者，才能夠對此代碼解密，並查詢其相關資料。

(1)加密端

系統建構資料欄位及操作介面如(表二及圖五)所示。例如客戶欲其客戶代碼傳給商家，以利商家由其資料庫找出客戶之基本資料，假設欲加密之資料為客戶代碼“ C123456789”。使用者將客戶代碼傳送給商家，於是Message *m*=“ C123456789”，系統將其轉為ASCII代碼。商家利用其私鑰 $R_{私}=(f, g)$，產生公鑰 $R_{公}=h$；而系統將利用此公鑰配合亂數Blind Value *r*對Message *m*進行加密，得出“22 25 14 12 8 30 11 6 8 5 19”的密文(如圖五)。表二則說明了加密端的資料格式。

表二：加密端資料欄位

功能項	資料型態	說明
Message (*m*)	nchar(11)	輸入欲加密資訊。
Converted into ASCII	varchar(11)	系統依據使用者輸入的資訊，轉換為ASCII碼。
Private Key (*f*)	varchar(11)	商家解密之金鑰 。
Private Key (*g*)	varchar(11)	系統自動產生之私鑰，加密運算所需之值。
Public Key (*h*)	varchar(11)	商家對外公開之公鑰
Blind Value (*r*)	varchar(11)	隨機產生之亂數值。
Encrypted Message (*e*)	varchar(11)	加密之後得到之密文。



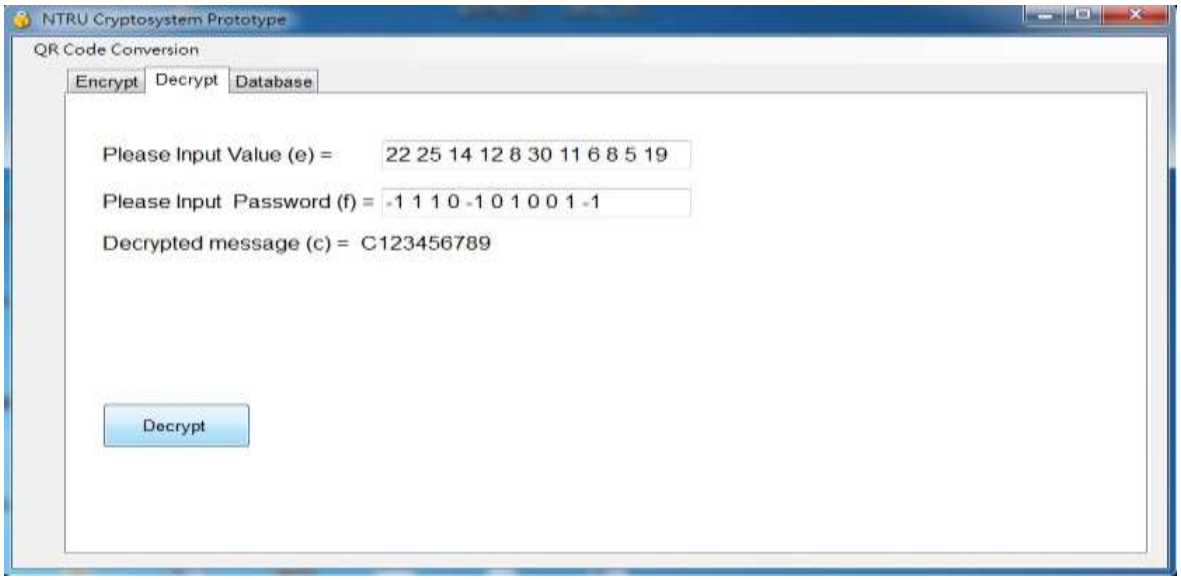
圖五：加密端系統介面

(2)解密端

系統建構資料欄位及操作介面如(表三及圖六)所示。商家於接獲密文*e*之後，輸入其私鑰*f*，即可解密得到原文訊息*m*。

表三：解密端資料欄位

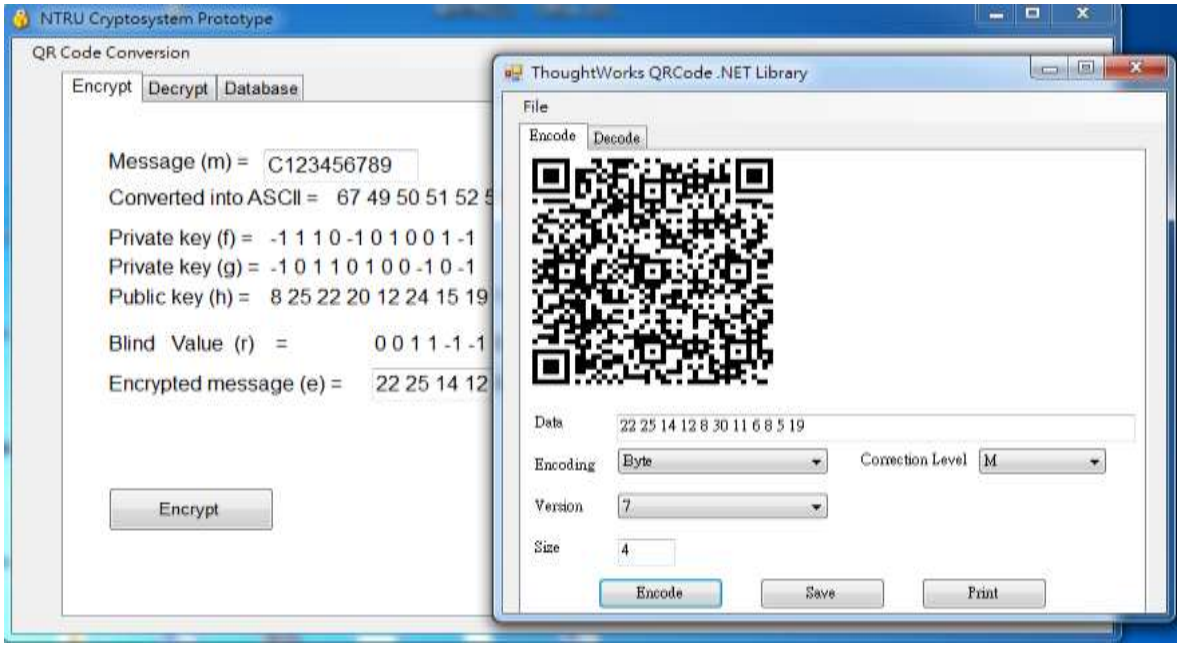
功能項	資料型態	說明
Input Value (e)	varchar(11)	輸入接收到的密文。
Input Password (f)	varchar(11)	商家所持有之私鑰。
Decrypted Message (c)	varchar(11)	解密得到的明文。



圖六：解密端系統介面

(3)QR碼產生模組

將加密完成的資訊，轉換至此模組中，並資訊轉換成QR CODE，此即為NTRU QR CODE 系統建構 (如圖七及圖八)所示。

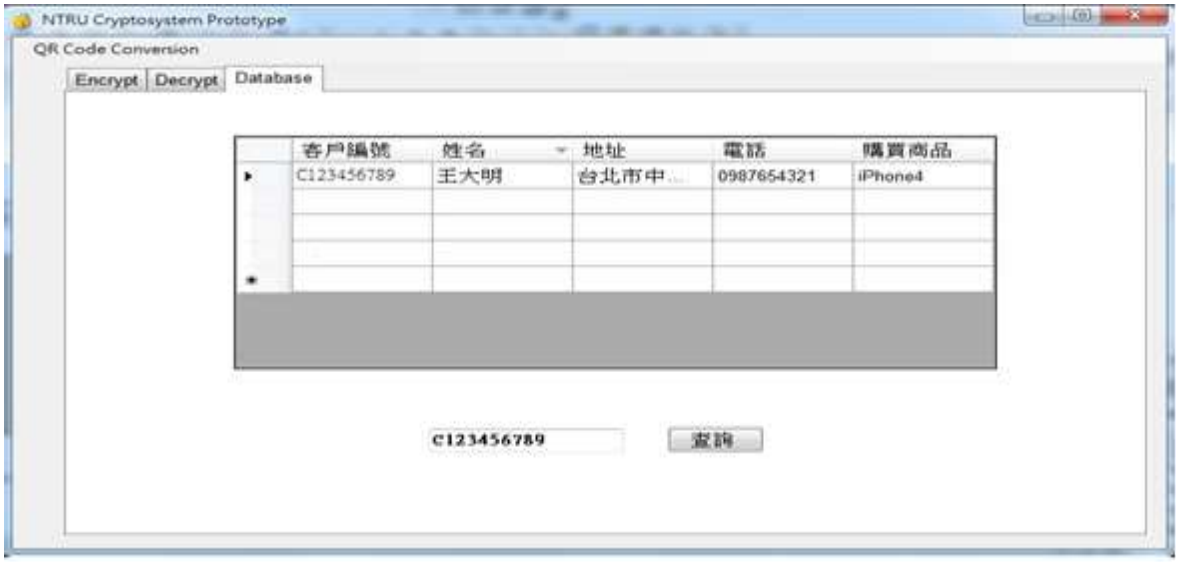


圖七：QR碼轉換模組(轉碼)

圖八：QR碼轉換模組(解碼)

(4)資料庫

最後輸入正確解密之客戶代碼(圖九)，顯示客戶相關詳細資料。



圖九：資料庫查詢

四、績效評估與問題討論

1. 系統績效

本研究測試係針對NTRU雛形系統進行正確性及實用性測試，測試結果顯示，NTRU系統其理論基礎實務上實屬可行，未來將進行執行速度及攻擊測試，以確保NTRU系統在實際應用中的可用性及安全性。由於NTRU 速度快安全性高，具有相當高的研究價值，可繼續探討NTRU本身演算法之性質，進一步改良，使得NTRU更加強韌，可結合更多的應用，若能推廣至實務面，可為目前使用的系統帶來更大的變革。

(1)對解碼錯誤之測試

本系統經由固定私鑰，對隨機亂數值r隨機訊息進行解碼之測試，共計86400次，結果並未發現錯誤之情形出現。

(2)計算速度測試

對於100000組資料(長度<= n)之加密，並且解密，所需之時間為3小時15分； 平均每次計算約需117微秒。計算簡單快速，實為其優點。

2. 實務面的應用探討

(1)商家

企業若採用此架構之系統，在發行票證時，可以改以數位化集中管理的方式來發行票證，除了響應環保的概念，節省紙張，對於票證使用權方面，伺服端也能及時查證票據使用是否合法。若非合法使用者或非經由使用者授權，則不能行使票證的權利，提升使用者對系統的信賴度，企業也可以減少多餘的作業流程，或是接洽使用者票證上問題的抱怨等等…在流程上可以著實省下不少時間，確實提升企業工作效率。

(2)客戶

使用者購買票證，本身應負妥善保管之責任；但是，萬一不慎遺失，本系統亦可協助排解此一問題: 他只須要上網驗證自己的票證使用狀態，即可行使該票證的權利，達到快速簡單的目的，對於客戶的使用意願必能大幅提升。

(3)電子化政府

在電子化政府的應用上，首先是提高QR Code的安全性，利用NTRU加密的行動條碼不易被仿冒，不會淪為不法者所偽裝的釣魚網站，可使民眾正確得利用政府服務。此外，行動條碼也可以讓民眾方便的申請戶籍、地籍等謄本，查詢各項案件辦理進度等，提升政府的e化水準，作好便民措施。

3. 未來發展

Nayak等人建議了Matrix-Based NTRU，以矩陣代替多項式作為群的物件集合，為NTRU的理論系統，開啟新的一頁(Nayak et al., 2008; Nayak et al., 2010)。我們以後的系統設計，也可以建立在以矩陣為基礎的NTRU之上，因為它沒有多項式NTRU必須選擇理想金鑰的要求，否則會再解密時發生錯誤。

五、結論

本文首先探討QR Code 的特性，它具有系統架構開放、抗污損，建置成本低廉等優點，加上設備普及，在各個商務層面中被廣泛應用。然而也因條碼標籤規格開放，易於產生與複製，在防偽的機制上有強化之必要。鑒於手持裝置計算能力較弱，我們建議以NTRU密碼配合QR Code來強化安全機制，因為NTRU系統只利用簡單算數運算，計算速度快，且安全性高，適於用在行動通信設備上。在本文中，我們實作了一個雛型系統，做了加解密速度的測量和正確性的驗證，結果顯示此一系統的確可以在行動交易上使用。利用本研究所建議的系統，商家可以驗證票證的真偽，客戶也可以知悉票證的使用狀況，君有助於行動商務之推展。同樣的，政府也可以利用安全的QR Code推行各項便民服務，提升行政效率，是電子化政府各種應用更加便捷、多元化。

參考文獻

[1] 中華電信行動條碼 <http://qrcode.emome.net/qrcpromote/code01.html?vcrm=200804082143@8656616c8c27db0687cca4f0beb032a2> (Retrieved Mar 2015)

[2] 方碼科技 <http://www.funcode-tech.com/QR_Encoder.aspx> (Retrieved Dec 2015)

[3] 行動上網聯盟 <http://www.meworks.net/meworksv2/meworks/page1.aspx?no=92> (Retrieved Jan 2015)

[4] 台灣農產品安全追溯資訊網 <http://taft.coa.gov.tw/welcome.asp?mp=8&role=C&mpap=A> (Retrieved Mar 2015)

[5] 余宗憲，運用行動條碼結合線上整合式售票系統之研究，碩士論文，資訊傳播研究所，南台科技大學，2013 。

[6] 黃信捷，電子資料交換EDI 在圖書出版與圖書館編目自動化之應用一以「二維條碼」之應用談起，圖書館管理學報, vol. 2, pp.73-88, 1996.

[7] 翁仍方，行動條碼行動條碼加密機制之研究，碩士論文，資訊工程系，大同大學，2007。

[8] 網路小額付費機制 <http://www.micro-payment.net> (Retrieved Feb 2014)

[9] 簡銘成，行動條碼整合NTRU公開金鑰密碼系統之防偽機制，碩士論文，資訊經營系，大

同大學，2011。
[10] 高鐵T Express <https://www.thsrc.com.tw/tw/Article/ArticleContent/58764cad-504a-486c-b1dc-f42aaa4f3552> (Retrieved Dec 2015)
[11] Coppersmith, D. and Shamir, A., Lattice attacks on NTRU. In Proceeding of Eurocrypt '97, LNCS, vol. 1233, Springer-Verlag, pp.52-61, 1997.
[12] Gouda, M.G. and Liu, A.X., "Formal Specification and Verification of a Micropayment Protocol," 13th International Conference on Computer Communications and Networks, pp. 489-494, 2004.
[13] Hasan, A. and Raygan, K., "A Mobile Telephone Based, Secure Micro-Payment Technology using the Existing ICT Infrastructure," International Conference in Communication and Networking, pp. 22-24, 2007.
[14] Hoffstein, J. and Silverman, J.H., "Optimization for NTRU", In Proceedings of Public-Key Cryptography and Computational Number Theory, de Gruyter, Warsaw, September, 2000.
[15] Hoffstein, J. and Silverman, J.H., Implementation Notes for NTRU PKCS Multiple Transmissions, NTRU Technical Report #006, May 1998, www.ntru.com
[16] Hoffstein, J. and Silverman, J.H., Protecting NTRU Against Chosen Ciphertext and Reaction Attacks, NTRU Technical Report #016, June 2000, www.ntru.com
[17] Hoffstein, J., Pipher, J. and Silverman, J.H., NTRU: A Ring-Base Public Key Cryptosystem. In J. P. Buhler, editor, Algorithmic Number Theory (ANTS III), Lecture Notes in Computer Science, volume 1423, pages 267–288, Berlin, 1998. Springer-Verlag.
[18] Howgrave-Graham N., Silverman, J.H. and Whyte, W., A meet-in-the-middle attack on an NTRU private key. NTRU Cryptosystems Technical Report #004, Version 2, June 2003.
[19] Hoffstein, J. and Silverman J.H., Reaction Attacks Against the NTRU Public Key Cryptosystem, NTRU Technical Report #015, August 1999, www.ntru.com
[20] Hwang R. J., Su F.-F., Yeh Y.-S. and Chen C.-Y., "An efficient decryption method for RSA cryptosystem," Proc. of the 19th AINA Int. Conf. on Advanced Information Networking and Applications, Taipei, Taiwan, vol. 1, pp.585-590, Mar. 2005.
[21] Magicode <http://www.iconlab.com.tw/product_service.php> (Retrieved Feb 2010)
[22] Price, S. M., "Protecting Privacy Credentials from Phishing and Spyware Attacks," Information Assurance and Security Workshop, pp. 167-174, 2007.
[23] QR code <http://www.denso-wave.com/qrcode/index-e.html> (Retrieved Jan 2010)
[24] Quickmark <http://diy.quickmark.com.tw/eten/?c=301> (Retrieved Jan 2010)
[25] Nayak, R., Sastry, C.V. and Pradhan, J., "A matrix formulation for NTRU cryptosystem", IEEE ICON 2008.
[26] Nayak, R., Sastry, C.V. and Pradhan, J., "Algorithmic Comparison between Polynomial Baseand Matrix Base NTRU Cryptosystem", IJCNS, 2010.
[27] Rivest, R., Shamir, A. and Adleman, L., 1978 "A method for obtaining digital signatures and public-key cryptosystem," Communications of the ACM, Vol.21, pp.120-126.
[28] Sun H. M. and Chen B. J., "Time-stamped proxy signatures with traceable receivers," Proceedings of the ninth national conference on Information security, pp. 247-253, 1999.
[29] Sun H. M., "Design of time-stamped proxy signature with traceable receivers, " In: IEE proc. Computers &Digital Techniques, Vol. l47, pp.462-466, Nov., IEE, 2000.
[30] Silverman, J. H., Plaintext awareness and the NTRU PKCS. Technical Report #007, NTRU Cryptosystems, July 1998, www.ntru.com.
[31] Silverman, J.H., Wraps, Gaps, and Lattice Constants, NTRU Technical Report #011, January 1999, available at www.ntru.com

[32] Seino, K., Kuwabara, S., Mikami, S., Takahashi, Y., Yoshikawa, M., Narumi, H., Koganezaki, K., Wakabayashi, T. and Nagano, A., “Development of the traceability system which secures the safety of fishery products using the QR Code and a digital signature,” Proc. of MTS/IEEE TECHNO-OCEAN, Kobe, Japan, vol. 1, pp.476-481, Nov. 2004.

[33] Shand, M. and Vuillemin, J., “Fast implementations of RSA cryptography,” Proc. of the 11th IEEE Symposium on Computer Arithmetic, Windsor, Ontario, Canada, pp.252-259, Jun.-Jul. 1993.

[34] Tan, J. S., “QR Code: the 2D code of 21st century and its applications,” Information Technology Standards Committee Synthesis Journal, pp.7-14, Oct. 2002.

[35] Tan, C. H. and Teo, J. C. M., “Protection Against Web-based Password Phishing,” Information Technology, pp. 754-759, 2007.

[36] Yang, C. N., Yen, C. E., Wang, C. H., Chen, C. M., Chen, T. S. and Lee, Y. F., "Campus Micropayment System by Mobile Barcode," TANET 2007, Oct, 2007.