植基於簡易金鑰交換暨密碼認證協定之研究

摘要

拜資訊科技之賜，促使網路加速普及，各企業資訊交流型態亦隨之改變。繼公開金鑰概念提出後，可於雙方互不認識基礎下，執行認證程序，以確保安全通訊，防止傳輸資料外洩情事。

本研究基於金鑰同意及密碼認證協定精神，建構一套改良式多人金鑰交換暨密碼認證協定系統，適時遏止僞冒者利用密碼僞造法及映射法達成達成攻擊目的，在使用者未公開其密碼原則下，仍能驗明正身，以期達到零知識之要求。

關鍵字：金鑰交換暨密碼認證、二元一次同餘方程、離散對數、映射攻擊法、零知識

一、前言

網際網路之無遠弗屆功能，縮短彼此間之距離，大量數據透過網路通道互相交換資訊，此等便利雖帶來無限商機，然而卻無法避免有心人士從中窺探，彰顯整體網路環境極不安全。過去 Kwon 及 Song 等人提出廣義金鑰同意與密碼認證協定之研究（A Study on the Generalized Key Agreement and password Authenticated protocol）[2]，其主要目的在保障通訊者雙方透過安全通道傳遞訊息，即使僞冒者從中竊取相關數據，仍然無法達成目的，除非攻擊者可以解決離散對數問題，亦即能解決 Diffie-Hellman 問題[1]。爾後相繼有不少學者針對[2]提出不同版本之攻擊法[3,4]。本研究以[2]爲其核心精神，改良原通訊架構，除有效防止現有攻擊外，亦提昇原始版本侷限雙方通訊之窘境。第二節回顧 Kwon-Song 協定系統，第三節爲葉氏等人攻擊法之探討，第四節探討顧氏等人映射攻擊法，第五節爲本文提出之群體金鑰交換暨密碼認證協定，結論及未來研究方向將於最後著墨。

二、**Kwon-Song Protocol** 回顧

2000 年韓國學者 Kwon 及 Song 提出一個廣義金鑰同意與密碼認證協定概念，主要特點不同於傳統方法係在對於金鑰環境下，以認證公開金鑰機制，使其密鑰與整體系統達到安全性。諸如[5,6,7]爲 two party 認證，[8]爲 three party 認證，這些都屬於傳統公開金鑰基礎建設之傳統協定，Kwon-Song 的版本適合於任一有限循環群之運作，其原理如下：

符號說明：

A ：代表 User A，在此即 Alice

B ：代表 User B，在此即 Bob

E ：代表 User E，在此即僞冒者 Emma

$\parallel$ ：代表 Concatenation，即連結

$A \to B$ ：代表 User A 傳送給 User B

Alice 與 Bob 預先約定共同使用一隨機資料庫（Random Oracle），並分享一個薄弱的密碼 S 於安全通道上（weak secret on secure channel），雙方同意基於同一個產生器 G（Generator G）及一個乘法群 Z_p^* 下進行通訊協定。Alice 任選二隨機整數變數 α 與 x，其值區間落於 2≦ α 且 $x \leq P-2$ 範圍內，並計算式子（1）及（2）之結果。

$$g^{\alpha} \qquad (1)$$

$$g^{\alpha+h_1(s,g^{\alpha})} \qquad (2)$$

將結果傳送給 Bob，$h()$ 乃爲單向雜湊函數（One way hash function），且 $g^{\alpha+h_1(s,g^{\alpha})} = g^x \cdot g^{h_1(s,g^{\alpha})}$，等待 Bob 回應前，Alice 可以善用閒置時段（idle time）先行計算 $-xs \mod P-1$ 之值。

$$1.\ A \to B: A \parallel g^{\alpha} \parallel g^{x+h_1(s,g^{\alpha})} \qquad (3)$$

Bob 自遠端安全儲存器（secure local storage）中提取 Alice 傳過來的密碼 s，亦同時選取二個隨機整數變數 l 及 y，其值範圍限於 2≦ l 且 y ≦P－2 區間內，計算式子（4）

$$(g)^{y}(g^{\alpha})^{ls} \qquad (4)$$

Bob 設定 $b_0 = g$ ，$b_1 = g^{\alpha}$ ，$e_0 = y$ ，$e_1 = ls$ 爲有效之架構，將密文（cipher text）再傳回至 Alice，且等待回應時，計算式子（5）

$$(g^{x+h_1(s,g^{\alpha})})^{y}(g)^{-yh_1(s,g^{\alpha})} \qquad (5)$$

Bob 設定 $b_0 = g^{x+h_1(s,g^{\alpha})}$ ，$b_1 = g$ ，$e_0 = y$ ，$e_1 = -yh_1(s,g^{\alpha})$ ，透過 $(g^{x+h_1(s,g^{\alpha})})^{y}(g)^{-yh_1(s,g^{\alpha})} = g^{xy}$ ，則能夠得到共同協定之密鑰值 $K = h_4(g^{xy})$ 。

$$2.\ A \leftarrow B : l \,\|\, g^{y} \,\|\, (g^{\alpha})^{ls} \qquad (6)$$

Alice 根據 Bob 所傳過來之訊息（如式子 6），利用自己的私鑰值（ x 及預先計算求得之 $-xs$ 值），予以解析，即式子（7）

$$(g^{y+\alpha ls})^{x}(g^{x})^{-xls} \qquad (7)$$

Alice 設定 $b_0 = g^{y+\alpha ls}$ ，$b_1 = g^{\alpha}$ ，$e_1 = x$ ，$e_1 = -xls$ ，則 $(g^{y+\alpha ls})^{x}(g^{x})^{-xls} = g^{xy}$ ，她亦能求的共同協定之密鑰值 $K = h_4(g^{xy})$ ，再將計算 $h_2(g^{\alpha}, K)$ 所得之值傳給 Bob。

$$3.\ A \rightarrow B : h_2(g^{\alpha}, K) \qquad (8)$$

Bob 接收來自 Alice 傳遞之值 h_2 ，與自己產生之 h_2' 相互比較，如果 $h_2 = h_2'$ 時，對 Alice 施予認證（Authenticated），並且回覆 $h_3(l, K+1)$ 予以 Alice。

$$4.\ A \leftarrow B : h_3(l, K+1) \qquad (9)$$

此時 Alice 亦收到 Bob 傳遞之訊息 h_3 （如式子 9），她同樣將自己產生之 h_3' 與 h_3 做比較，假使 $h_3 = h_3'$ ，則對 Bob 給予認證，自此，雙方則同意協定之金鑰值爲 K ，爲爾後彼此通信建立信任機制。

綜理完整通訊協定概述如下：

$$\left.\begin{aligned} &1.A \rightarrow B : A \,\|\, g^{\alpha} \,\|\, g^{x+h_1(s,g^{\alpha})} \\ &2.A \leftarrow B : l \,\|\, g^{y} \,\|\, (g^{\alpha})^{ls} \\ &3.A \rightarrow B : h_2(g^{\alpha}, K) \\ &4.A \leftarrow B : h_3(l, K+1) \end{aligned}\right\} \qquad (10)$$

然而 Kwon-Song 認爲原始版本（original version，指式子 10）仍然可以由四個步驟精簡成三個步驟，並且將原本雙方共同協定基礎下之 G 產生器（Generator G），額外新增一個 η 產生器（Generator η ），並且迫使通信之另一方（例如以 Bob 爲例）選擇 η ，使其與 G 產生器具有相同循環群（cyclic group），則 $g^{\alpha} \equiv \eta (\mathrm{mod}\, P)$ 對 Z_p^* 乘法群，有著 $G.C.D(a, P-1) = 1$ 效果，或對於 q 爲子群之秩（subgroup of g order），$G.C.D(a, q) = 1$ 。植基於此，精簡之通訊協定整理爲三個階段後，描述如下：

$$\left.\begin{aligned} &1.A \rightarrow B : \eta^{\alpha} \,\|\, g^{x+h_1(s,g^{\alpha})} \\ &2.A \leftarrow B : l \,\|\, g^{y} \eta^{\alpha ls} \,\|\, h_2(\eta^{\alpha}, K) \\ &3.A \rightarrow B : h_3(l, K+1) \end{aligned}\right\} \qquad (11)$$

爲利於區分，式子 10 稱爲原始版本，而式子 11 則稱爲進階版（enhanced version）。

三、葉氏等人攻擊法版本研析

2001 年，葉氏等人提出 Kwon-Song 版本之安全性分析[3]，渠等認爲，若以離線密碼猜測攻擊法（Off-line password guessing attacks）而言，進階版相對存在安全之虞（insecure）。葉氏等人更進一步指出，攻擊者可以將公開之資訊（或已知之相關參數及認證資料），預存於近端媒體中（stores locally），因此藉由離線的狀態，試圖尋找滿足驗證程式之密碼 S（weak secret password）。由於離線特性，致使伺服器（server）無法預測出離線猜測攻擊。僞冒者 Emma 首先選取已猜測密碼 s' 及兩個隨機整數 α 與 x ，使計算

$\eta^{\alpha} \| g^{x+h_1(s',g^{\alpha})}$，再將運算結果傳給 Bob，此時 Emma 可以佯裝成 Alice 來達到欺騙 Bob 的目的。
佯騙步驟如下：

$$Eve \rightarrow B : \eta^{\alpha} \| g^{x+h_1(s',g^{\alpha})} \quad (12)$$

Bob 收到 Emma 的訊息後，按正常程序，由本端安全儲存器中，提取 s，亦同時隨機挑選兩個整數 l 及 y 計算 $K = h_4((g^{x+h_1(s',g^{\alpha})})^y g^{-yh_1(s,g^{\alpha})})$，然後求出 $g^y \eta^{\alpha ls}$ 後，將其訊息（式子 13）回傳至 Emma。

$$Eve \leftarrow B : l \| g^y \eta^{\alpha ls} \| h_2(\eta^{\alpha}, K) \quad (13)$$

此時 Emma 收到來自 Bob 傳送之結果，則將訊息（式子 13）予以本端儲存（stores message locally），接著按離線密碼攻擊法，Emma 再另選一密碼 s'' 使計算 $R = g^y \eta^{\alpha ls} \eta^{-\alpha ls''}$，因 α 是由 Emma 選取的，且 l 則爲一明文資料(Plaintext data)，然後 Emma 求得 $K' = h_4((R)^{x+h_1(s',g^{\alpha})-h_1(s'',g^{\alpha})})$，此較 $h_2(\eta^{\alpha}, K)$ 與 $h_2(\eta^{\alpha}, K')$ 是否相同，如果相同則 Emma 就猜得正確密碼，反之再另選一密碼直到命中爲止。

四、顧氏等人攻擊版本分析

2004 年顧氏等人提出 Kwon-Song 原始版本之安全性分析[4]，其中不同於葉氏等人之處在於採用映射攻擊法，而且該法亦爲一種回覆式攻擊（Replay Attack），於截收訊息（intercepted message）後，仍能將截收之訊息再送回至發送者。
其運作原理描述如下：
Alice 起始於 S1 與 Bob 通聯，而僞冒者 Emma 開始於 S2 與 Alice 通訊。

$$\left.\begin{array}{ll}
\text{S1/Step 1.} & A \rightarrow B(E) : A \| g^{\alpha} \| g^{x+h_1(s,g^{\alpha})} \\
\text{S2/Step 1.} & B(E) \rightarrow A : B \| g^{\alpha} \| g^{x+h_1(s,g^{\alpha})} \\
\text{S2/Step 2.} & B(E) \leftarrow A : l \| g^y g^{\alpha ls} \\
\text{S1/Step 2.} & A \leftarrow B(E) : l \| g^y g^{\alpha ls} \\
\text{S1/Step 3.} & A \rightarrow B(E) : h_2(g^{\alpha}, K) \\
\text{S2/Step 3.} & B(E) \rightarrow A : h_2(g^{\alpha}, K) \\
\text{S2/Step 4.} & B(E) \leftarrow A : h_3(l, K+1) \\
\text{S1/Step 4.} & A \leftarrow B(E) : h_3(l, K+1)
\end{array}\right\} \quad (14)$$

‘$A \rightarrow B(E) : message$’ 表示 Emma 截收 Alice 對 Bob 傳送之訊息，且防止 Bob 收到。
‘$B(E) \rightarrow A : message$’ 則表示 Emma 僞裝成 Bob 送出訊息至 Alice。在 S2/Step 3 階段後，Alice 相信她自己與 Bob 通聯，事實上 Emma 已佯裝 Bob 對她執行第一次的認證程序；而在 S1/Step 4 階段，Emma 再次僞冒 Bob 對她實施第二次認證。
由此明白揭示 Kwon-Song 原始版本的協定中，其協定金鑰雖然未被僞冒者 Emma 知悉，然而狡滑的攻擊者可藉由系統洩漏出潛在的弱點著手攻擊。顧氏等人認爲，原始版本通訊協定的設計在某些強制的環境中，並未使用協定金鑰 K 值來保護 Alice 與 Bob 協定交換同意時附隨於後的訊息。
例如原始協定中使用一個識別機制的架構，自僅隨於後的訊息尚未藉由認證碼（Message Authentication Code, MAC）或透過協定金鑰 K 值加以保護。因此，Emma 容易佯裝 Bob 去欺騙 Alice，顧氏等人建議對 Step3 部分由直接依賴性（direction-independent）修正爲間接依賴性(indirection-independent)，即可避免映射攻擊（Reflection Attack）。描述步驟如下：

$$\text{Step3}' \quad A \rightarrow B : h_2(g^{\alpha}, K, B) \quad (15)$$

Emma 於 S1/step 3 及 S2/Step 3 處截收與轉送訊息，由於 $h_2(g^{\alpha}, K, B)$ 並非爲 $h_2(g^{\alpha}, K, A)$，因此，Alice 可斷然否絕該訊息，則 S2 程序將立即終止。植基於此，Emma 無法佯裝 Bob 回覆給 Alice 於 S1/Step 4 階段，整體通聯將導致無法通過認證而宣告失敗。

五、群體金鑰交換暨密碼認證協定

5.1 一次同餘方程

本節以二元一次同餘方程（congruence）爲其架備，強化系統承受攻擊者藉由字典攻擊（Dictionary

Attack）或密碼猜測攻擊（Guessing Attack）來達成目的。並迫使通聯過程之當事者雙方必須誠實動用密碼，而在雙方產生共同協定金鑰值 K 時，仍能予以認證，免除居中攻擊（Middle in Man Attack）之威脅，於訊息交換過程階段，對驗證不誠實或非法偽冒之一方可立即終止通聯程序。其描述如下：

密鑰值： a,b,c,d

私鑰值： u,v

原根： g

$$ax+b\equiv u \pmod{P} \quad (16)$$

$$cx+d\equiv v \pmod{P} \quad (17)$$

$$\Delta\equiv(ad-bc)\pmod{P} \quad (18)$$

$$\Delta\cdot\Delta^{-1}\equiv 1\pmod{P} \quad (19)$$

$$x\equiv\Delta^{-1}(bv-du)\pmod{P} \quad (20)$$

$$(\Delta,P)=1 \quad (21)$$

首先 Alice 預與 Bob 取得共同協定，Alice 隨機選取兩正整體數 a 與 b ，其值選定限於 $2<a\le P-2$ 且 $2<b\le P-2$ 區間，及系統隨機產生一整數 x（ $2<x\le P-2$ ），計算 $ax+b\equiv u \pmod{P}$ ，並將運算結果(式子 22、23)傳送給 Bob。

$$g^{u+x} \quad (22)$$

$$g^{x} \quad (23)$$

Bob 亦隨機選出兩整數 c 與 d ，其值選定限於 $2<c\le P-2$ 且 $2<d\le P-2$ ，，計算出 $cx+d\equiv v \pmod{P}$

$$A\rightarrow B: A,g^{u},g^{u+x} \quad (24)$$

Bob 接收來自 Alice 之訊息（式子 24），並設定 $b_0=g^{u+x}$ ，$b_1=g^{v}$ ，$e_0=v$ ，$e_1=-x$ ，計算 $(g^{u+x})^{v}\cdot(g^{v})^{-x}=g^{uv}$ ，Bob 將求得共同協定金鑰 $K=g^{uv}$ 。

$$A\leftarrow B: B,g^{v},g^{v+x} \quad (25)$$

Alice 根據 Bob 所傳送之訊息(式子 25)，啓動祕鑰 u 並設定 $b_0=g^{v+x}$ ，$b_1=g^{u}$ ，$e=u$ ，$e_0=-x$ ，亦可求得共同協定金鑰 $K=(g^{v+x})^{u}\cdot(g^{x})^{-u}=g^{uv}$ 。

$$A\rightarrow B: A,g^{a},g^{b},(A,K) \quad (26)$$

Alice 再將 g^a 及 g^b 傳送至 Bob，並先行計算 $(g^{v})^{-b}$ 。

Bob 收到 Alice 之 g^a 及 g^b ，藉由私鑰 c 及 d 可求出 $\Delta=(g^{a})^{d}\cdot(g^{b})^{-c}\equiv g^{(ad-bc)}$ ，再利用 Δ 值計算其乘反元素 $\Delta^{-1}\cdot\Delta\equiv 1 \pmod{P}$。先計算 $(g^{b})^{-v}$ 之值，並驗証 $\Delta x=\Delta^{-1}(g^{u})^{d}(g^{b})^{-v}\equiv x\pmod{P}$，若相等則對 Alice 認證核可，並回傳 g^a 及 g^c 給 Alice。

$$A\leftarrow B: B,g^{d},g^{c},(B,K) \quad (27)$$

Alice 收到 Bob 傳遞來之 g^d 及 g^c，亦可透過私鑰 a 與 b 計算得知 $\Delta=(g^{d})^{a}(g^{c})^{-b}\equiv g^{(da-cb)}$，再以 Δ 求得其反元素，並驗証 $\Delta x=\Delta^{-1}(g^{d})^{u}(g^{v})^{-b}\equiv x\pmod{P}$，若相等則對 Bob 認證核可。爾後 Alice 與 Bob 即擁有一組共同協定金鑰 K 。

5.2 編碼暨安全行分析

5.2.1 編碼

$$A\equiv g^{u}\pmod{P} \quad (28)$$

$$B\equiv g^{v}\pmod{P} \quad (29)$$

Alice 欲將 (A,z) 傳送至 Bob，則她可以令 $z\equiv B^{u}\cdot m\pmod{P}$ 。Bob 收到 (A,z) 時，設 $t=P-1-v$ 並計算 $m\equiv A^{t}z\pmod{P}\equiv K^{-1}z\pmod{P}$ ，即可還原明文 m 。

證明：

$$\left.\begin{aligned} & m \equiv A^t z (\text{mod}\ \ P) \\ & A^t z \equiv (g^u)^{P-1-v} (g^v)^u m (\text{mod}\ \ P) \\ & \equiv g^{uP} g^{-u} g^{-uv} g^{uv} m (\text{mod}\ \ P) \\ & \equiv (g^{P-1})^u m (\text{mod}\ \ P) \\ & \equiv 1 g m (\text{mod}\ \ P) \qquad \text{Q 費馬小定理 } g^{P-1} \equiv 1 (\text{mod}\ \ P) \end{aligned}\right\} \quad (30)$$

證畢。

5.2.2 安全性分析

假使偽冒者 Emma 隨機選取兩整數 a_e 與 b_1 並計算 $a_e x + b_e \equiv u_e (\text{mod}\ \ P)$，則可求出

$\Delta_e \equiv (a_e d - b_e c) (\text{mod}\ \ P)$，並透過 $\Delta_e g \Delta_e^{-1} \equiv 1 (\text{mod}\ \ P)$。

$$A_e \equiv g^{u_e} (\text{mod}\ \ P) \quad (31)$$

$$K_e \equiv (g^{u_e + x})^v (g^v)^{-x} \equiv g^{u_e v} (\text{mod}\ \ P) \quad (32)$$

$$a_e x + b_e \equiv u_e (\text{mod}\ \ P) \quad (33)$$

$$\Delta_e \equiv (a_e d - b_e c) (\text{mod}\ \ P) \quad (34)$$

$$\Delta_e g \Delta_e^{-1} \equiv 1 (\text{mod}\ \ P) \quad (35)$$

$$\Delta x_e \equiv \Delta_e^{-1} (d u_e - b_e v) (\text{mod}\ \ P) \quad (36)$$

對二元一次同餘方程組有唯一解，即 $\Delta \equiv (ad - bc) (\text{mod}\ \ P)$ 與 $x \equiv \Delta^{-1} (bv - du) (\text{mod}\ \ P)$，若式子（35）成立，對式子（36）亦成立，且式子（35）恆等於式子（19），及式子（36）恆等於式子（30）。

由上述得知，二元一次同餘方程組有二組以上解，顯然與結果不符。因此 $\Delta \neq \Delta_e$ 且 $\Delta^{-1} \neq \Delta_e^{-1}$，式子（34）不等於式子（18），由式子（34）產生之（35）至（36）必矛盾。除非擁有正確之密鑰 a 與 b，以計算對映之 u 值，再透過交叉運算（式子 26 至 27）求得 Δ，再依據 Δ 推導其乘法反元素 Δ^{-1}，若如法得知 Δ，則無法正確計算出 Δ^{-1}。

建構三人以上通聯系統修正如下：

$$\begin{cases} a_1 x + b_1 \equiv c_1 (\text{mod}\ \ P) \\ a_2 x + b_2 \equiv c_2 (\text{mod}\ \ P) \\ a_3 x + b_3 \equiv c_3 (\text{mod}\ \ P) \end{cases} \quad (37)$$

證明：略。

六、結論

金鑰交換概念運用在業界已相當普及，諸如 SSL 及 PKCS 等均源自此精神，此等演算法乃基於解離散對數之困難度。若雙方在不安全的通道下通聯仍有可能洩漏資訊，本文以一次同餘方程結合解離散對數之複雜性進行彼此參數交換，確保通訊雙方於不公開參數原則下，仍能完成認證程序，期使任何可能洩漏之資訊降至最低，並達成零知識之要求。

七、參考文獻

1. W. Diffie and M. E. Hellman, New direction in cryptography, IEEE transaction on Information Theory, Vol. IT-11, pp. 644-654, Nov. 1976.
2. T. Kwon and J. Song, A study on the generalized key agreement and password authentication protocol, IEICE transaction on Communication, Vol. E83-B, No.9, pp.2044-2050, Sep. 2000.
3. Her-Tyan Yeh, hung-Min Sun and Tzonelih Hwang, Security Analysis of the Generalized Key Agreement and Password Authentication Protocol, IEEE Communication Letter, Vol. 5, No.11, pp.462-463, Nov. 2001.
4. Wei-chi Ku, Hui-Lung Lee and Chien-Ming Chen, Reflection Attack on a Generalized Key Agreement and Password Authentication Protocol, IEICE transaction on Communication, Vol. E87-B, No.5, pp.1386-1388, May. 2004.
5. Alain Mayer and Moti Yung, Secure protocol transformation via “expansion”: from two-party to groups, Proceedings of the 6th ACM conference on Computer and communications security, Nov. 1999.

6. Philip MacKenzie, Alina Oprea and Michael K. Reiter, Cryptographic protocols/ network security: Automatic generation of two-party computations, Proceedings of the 10th ACM conference on Computer and communication security, October 2003.
7. Yehuda Lindell, Bounded-concurrent secure two-party computation without setup assumptions, Proceedings of the thirty-fifth annual ACM symposium on Theory of computing, June 2003.
8. Chun-Li Lin, Hung-Min Sun and Tzonelih Hwang, Three-party encrypted key exchange: attacks and a solution, ACM SIGOPS Operating Systems Review, Vo. 34, Issue 4, Oct. 2000.