有效率的可搜尋多關鍵字之對稱加密機制

張儷子
中興大學資訊科學與工程學系
s9856042@cs.nchu.edu.tw

陳昱圻
中興大學資訊科學與工程學系
phd8909@cs.nchu.edu.tw

洪國寶
中興大學資訊科學與工程學系
gbhorng@cs.nchu.edu.tw

摘要

由於雲端計算越來越普及，個人的私密訊息可以隨時隨地的公開存放於網路伺服器當中。而如何保護個人的私密資訊以及通訊的隱密性成為重要的議題。我們希望存放伺服器的資料是安全的，亦或是攻擊者無法取得重要的訊息。針對上述的議題，Ballard 等人提出了一種有效的對稱式可搜尋關鍵字加密的機制。在本文中，我們提出一個更有效的基於關鍵字對稱式可搜尋加密機制。所提出的機制是可安全抵擋動態選擇關鍵字攻擊。

關鍵詞：對稱式加密、可搜尋加密、多關鍵字搜尋、暗門(Trapdoor)

Abstract

To realize cloud computing, the protection of personal private information becomes very important in communications. The private information in the open network server can be accessed at any time. At the same time, the server or attacker is unable to obtain any significant information from these data. In 2005, Ballard et al. proposed an efficient symmetric keyword-searchable encryption scheme. In this paper, we propose an efficient symmetric keyword-searchable encryption scheme. The proposed scheme is secure against adaptive chosen keyword attacks, and it also provides multi-keywords search.

Key words: symmetric encryption, searchable encryption, multi-keyword search, trapdoor

1 前言

目前有各種不同的方法用來保護存放在不懷好意伺服器之中訊息的私密性。例如，在開放式的伺服器當中存入加密的資料，讓使用者透過網路取得這些加密過的資料。然而，當使用者只需要存取一小部份的資訊時，也必須取得所有加密過後的資料然後將資料解密，進而選擇所想要的資訊。儘管，這方法可以有效預防攻擊，但由於搜尋大量加密過後的文件會導致通訊成本的提高，無法提供給使用者更方便地獲取一部分或者是全部的資訊。而這種方式也不適用於運算能力較弱的設備像是移動式設備、PDA 以及手機。因此我們需要一種方法可以用來尋找加密資料並只回傳我們所想要的部分，省去不必要的資料轉換。也因此基於關鍵字搜尋的加密方法，是一個非常有幫助的方法。

在本文，我們提出一個有效率基於多關鍵字對稱搜尋加密方法。在方法中所提到的伺服器都必須為誠實地回應，即使伺服器是不可信任或者是好奇的。本篇論文的章節安排如下，相關背景知識在第 2 章節，相關研究則在第 3 節介紹。而我們所提出的方法、安全分析在第 4 節有詳細的敘述。第 5 節則是比較[3][11]計算量。最後在第 6 節則是我們的結論。

2 背景知識

在此章節，我們首先介紹對稱式加密搜尋機制(Symmetric Searchable Encryption，簡稱SSE)系統架構及 SSE 的安全 model。接著介紹 bilinear pairing 性質，最後介紹困難的問題。

2.1 對稱式加密搜尋

假設有一使用者要儲存一個有關鍵字 $W_1, W_2, \ldots W_m$ 的加密文件。透過 $[E_K[M]\text{SSE}(K,W_1),\text{SSE}(K,W_2),\ldots,\text{SSE}(K,W_m)]$ 式子來儲存訊息，K 是一個鑰匙，M 是明文的訊息，E 是一個安全的對稱式加密機制，m 是關鍵字欄位的數量，而 SSE 為我們提出的關鍵字加密演算法。SSE 演算法不會洩漏訊息有關的任何資訊，而且可以用來搜尋特定的關鍵字。

我們使用 Golle 等人[8]提出的假設:

1. 同一份文件的欄位上不會重複出現相同的關鍵字。
2. 每個訊息定義每個關鍵字欄位。

舉例來說，如果文件是電子郵件，我們定義了四個欄位：From、To、Date、Subject，傳送文件格式如{From:Bob}、{To:Amy}、{Date:2010.12.31}、{Subject:Hi }，其 From 欄位的關鍵字就是 Bob。當欄位沒有關鍵字時，則填入 *NULL*，表示為空值。我們用一個向量 $D_i=(W_{i,1},W_{i,2},\ldots,W_{i,m})$ 表示為第 i 個文件擁有 m 個關鍵字。

定義 1. 一個基於關鍵字對稱式加密搜尋機制由多項式時間隨機亂數演算法組成。

1. **KeyGen**(1^k):輸入安全參數 1^k，此演算法會產生一個金鑰 K 及安全參數。
2. **SSE**(K, D):輸入金鑰 K 及關鍵字的文件集合 $D=\{W_1,W_2,\ldots,W_m\}$，此演算法會產生一個可搜尋 D 的加密的密文 S。
3. **Trapdoor**(K,Q):輸入金鑰 K 和欲搜尋的關鍵字，得到一個暗門(trapdoor) T_Q。
4. **Test**(S,T_Q):伺服器端驗證可收尋的加密 S 及暗門 T_Q，如果 $W_{I_j}=W_j^{'}$，則輸出"yes"，表示有搜尋到符合的關鍵字，否則輸出"no"。

上述 SSE 機制可抵擋動態選擇關鍵字攻擊(adaptive chosen keyword attacks)。攻擊者無法得知那些關鍵字是否有在加密訊息中時。我們利用了 ICC、ICR、ICLR 三種安全遊戲模型來解決動態選擇關鍵字攻擊(adaptive chosen keyword attacks)。其 ICC、ICR、ICLR 三種詳細介紹請參考[8]。函數 *Rand(D,T)* 表示在關鍵字集合 D 中會分別隨機選擇 T 中的關鍵字，而 T 是所有關鍵字的集合。SSE 機制的安全遊戲可藉由上述三種安全遊戲模擬攻擊者 A 和挑戰者 B 的互動，方法如下:

架設在 ICC(Indistinguishability of Ciphertext from Ciphertext)安全遊戲方法：

1. 攻擊者 A 適當的詢問可搜尋關鍵字的密文和暗門的詢問。
2. 攻擊者 A 選擇兩個文件集合 D_0 和 D_1，傳送給挑戰者 B。
3. 挑戰者 B 回傳可搜尋的密文 $E(D_B)$給攻擊者 A。
4. A 仍然繼續詢問可搜尋關鍵字的密文和暗門的詢問，除了步驟 2 的 D_0 和 D_1 的暗門不能再詢問。
5. 最後 A 輸出一個值 $b^{'}\in\{0,1\}$，成功破解 ICC 的條件為 $\beta^{'}=\beta$。我們定義攻擊者 A 擁有 ϵ 的優勢，其中 A 的優勢為 $\text{Adv}_A(1^k)=\left|\Pr[\beta_A=\beta]-1/2\right|>\epsilon$ 。

架設在 ICR(Indistinguishability of Ciphertext from Random)安全遊戲方法：

1. 攻擊者 A 適當的詢問可搜尋關鍵字的密文和暗門的詢問。
2. 攻擊者 A 選擇文件集合 D_0，傳送給挑戰者 B。
3. 挑戰者 B 產生一個 $D_1=Rand(D_0,T)$，且計算可搜尋的密文 $E(D_B)$回傳給攻擊者 A。

4. A 仍然繼續詢問可搜尋關鍵字的密文和暗門的詢問，除了步驟 2 的 D_0 的暗門不能再詢問。
5. 最後 A 輸出一個值 $b' \in \{0,1\}$，成功破解 ICR 的條件為 $\beta' = \beta$。我們定義攻擊者 A 擁有 ϵ 的優勢，其中 A 的優勢為 $\mathrm{Adv}_A(1^k) = |\Pr[\beta_A = \beta] - 1/2| > \epsilon$。

架設在 ICLR(Indistinguishability of Ciphertext from Limited random)安全遊戲方法：

1. 攻擊者 A 適當的詢問可搜尋關鍵字的密文和暗門的詢問。
2. 攻擊者 A 選擇文件 D，傳送給挑戰者 B。
3. 挑戰者 B 產生 $D_0 = Rand(D,T)$ 和 $D_1 = Rand(D_0, T-\{t\})$，其中 $T \subseteq \{1,2,...,m\}$，$t \in T$，且計算可搜尋的密文 $E(D_B)$ 回傳給攻擊者 A。
4. A 仍然繼續詢問可搜尋關鍵字的密文和暗門的詢問，除了步驟 2 的 D 的暗門不能再詢問。
5. 最後 A 輸出一個值 $b' \in \{0,1\}$，成功破解 ICLR 的條件為 $\beta' = \beta$。我們定義攻擊者 A 擁有 ϵ 的優勢，其中 A 的優勢為 $\mathrm{Adv}_A(1^k) = |\Pr[\beta_A = \beta] - 1/2| > \epsilon$。

定理 1. *如果攻擊者 A 贏得 ICC 的優勢為 ϵ，則攻擊者 A 贏得 ICLR 的優勢為 $\epsilon/2m^2$。*

證明. Golle 等人[8]以證明此定理。

2.2 雙線性配對(Bilinear pairing)

大多數的可搜尋加密機制都是基於雙線性配對[2]，本文也不例外。簡單的說，雙線性配對是子群上的一個函數，可以將橢圓曲線上的一對特殊的點投射成特定有限體內的數字。接著，我們簡單介紹這個函數。

在橢圓曲線之上，G_1 和 G_2 為循環加法群，其 order 為 q，而 G_t 為有限體之中的一個循環乘法群，其 order 也為 q。存在一個雙線性配對函數 $\hat{e}: G_1 \times G_1 \to G_t$，其特性如下：

1. 可計算的(computable)：給 $h_1 \in G_1$ 和 $h_2 \in G_2$，存在有多項式時間演算法可以將 $\hat{e}(h_1,h_2) \in G_t$ 計算出來。
2. 雙線性(bilinear)：對任何整數 $x, y \in Z_q^*$，$\hat{e}(xP,yQ) = \hat{e}(P,Q)^{xy}$，其 $P \in G_1$，$Q \in G_2$。
3. 非退化的(non-degenerate)：如果 P_1 是 G_1 的生成點（generator），P_2 是 G_2 的生成點，則 $\hat{e}(P_1,P_2) \neq 1$。

如果 $G_1 = G_2$，則雙線性配對函數可表示為 $\hat{e}: G \times G \to G_t$。其雙線性配對計算的成本相當高[2]。在許多已發表中都使用了 paring 改善計算量[14][15]。

2.3 困難問題的假設

這些困難的問題被用來證明安全性。

定義 2. Decision Diffie-Hellman problem **(簡稱為** DDH)

在循環群 G 中，有一 order q，其生成點為 P。DDHP 能夠區別 (aP,bP,cP) 和 (aP,bP,abP)，其 $a,b,c \in Z_q^*$ 為隨機選擇。如果 $|\Pr[A(aP,bP,cP)] - \Pr[A(aP,bP,abP)]| > \epsilon$，則一個多項式時間攻擊者 A 擁有優勢 ϵ 可以解決 DDHP。更多詳細內容請參考[4][8]。

定義 3. varied co-external Diffie-Hellman problem (簡稱為 vcoXDH)

vcoXDH 問題是 coXDH 問題和 1-BDHI 問題的變化[3][10]。在擁有相同 order q 的 G_1 和 G_2，其 P_1 為 G_1 的生成點，P_2 為 G_2 的生成點。則雙線性配對函數 $\hat{e}: G_1 \times G_2 \to G_t$。vcoXDH 問題能夠區分 $(P_1, P_2, \frac{1}{a}P_1, aP_2, bP_1, cP_1)$ 和 $(P_1, P_2, \frac{1}{2}P_1, aP_2, bP_1, \frac{b}{a}P_1)$，其 $a,b,c \in Z_q^*$ 為隨機選擇。如果 $|\Pr[A(P_1, P_2, \frac{1}{a}P_1, aP_2, bP_1, cP_1)] - \Pr[A(P_1, P_2, \frac{1}{2}P_1, aP_2, bP_1, \frac{b}{a}P_1)]| > \epsilon$，則一個多項

式時間攻擊者 A 擁有優勢ϵ可以解決 vcoXDH 問題。

3 相關研究

近幾年許多研究探討可搜尋加密的安全和效率。早期是由 Song 等人[12]所提出的對稱式金鑰技術，它只允許使用者對加密的資料設置暗門的詢問。Goh[7]提出了利用索引(index)的方法來建構索引 Z- index 改善關鍵字搜尋的效率。另外也有很多在探討多關鍵字搜尋的研究[1][3][5][6][8][10][11]，這些機制都是利用公開金鑰技術(簡稱 PEKS)應用於電子郵件系統，傳送者利用接收者的公鑰加密訊息，接收者用密鑰產生關鍵字的暗門，伺服器利用暗門和可搜尋的密文做測試。Jeong 等人[9]提出了一個在 PEKS 機制上的公開問題，其為如果傳送者和接收者擁有相同的關鍵字，PEKS 機制無法抵抗離線關鍵字猜測攻擊(off-line keyword guessing attacks)。Tang[13]提出了一種交互式 PEKS 機制成功的抵擋了離線關鍵字猜測攻擊(off-line keyword guessing attacks)。在此節，我們回顧 Ballard 等人[3]所提出的一個有效率的對稱是可搜尋加密機制，簡稱為 BKM。

BKM 機制對於一個單一關鍵字需要一個擬亂函式$f:\{0,1\}^l\times\{0,1\}^*\rightarrow Z_q^*$和雙線性配對函數$\hat{e}:G_1\times G_2\rightarrow G_t$，其多項式時間隨機演算法如下：

- **KeyGen**(1^l)：給一個安全參數 1^l，且定義循環群 G_1，G_2，G_t 有相同的 order q 和循環群 G_1 和 G_2 的生成點分別為 P_1 和 P_2。此演算法會隨機產生密鑰$K\in\{0,1\}^l$，並且保持 P_2 的隱密性。
- **SSE**(K,D)：輸入密鑰 K 和關鍵字的文件集合 D，此演算法會隨機產生一個亂數$r\in Z_q^*$，輸出可搜尋的密文 $S=[rf_K(W_1)P_1,rf_K(W_2)P_1,\ldots,rf_K(W_m)P_1,rP_1]$。
- **Trapdoor**(K,Q)：輸入金鑰 K 和欲搜尋的關鍵字$Q=[W_{I_1}^{'},\ldots,W_{I_t}^{'},I_1,\ldots,I_t]$，演算法會選擇一個亂數$u\in Z_q^*$，和產生一個暗門$T_Q=[T_1,T_2,I_1,..,I_t]$，其中 $I_1,..,I_t$ 為 Q 的關鍵字欄位 (fields) 位置，$T_1=\sum_{n=1}^{t}f_K(W_{I_n}^{'})P_2$，$T_2=uP_2$。
- **Tesst**(S,T_Q)：伺服器端利用 $S=[A_1,..,A_m,B,C]$ 和 T_Q 做測試。測試$\hat{e}(A_{I_1}+\ldots+A_{I_t},T_2)=\hat{e}(T_1,B)$，如果相等則輸出"yes"，否則輸出"no"。

4 提出的方法

在此節，分別介紹協定架構和安全性分析。首先在 4.1 介紹我們所提出一個新的對稱式可搜尋加密機制(a new Symmetric Searchable Encryption scheme，簡稱為 SSE)，能更有效率的應用在移動設備上。在 4.2 探討機制的安全性分析。

4.1 協定架構

我們所提出的機制使用兩個雜湊函數$H_1:\{0,1\}^*\rightarrow Z_q^*$，$H_2:G_t\rightarrow G_t$。我們提出機制的詳細步驟如下：

- **KeyGen**(1^l)：給一個安全參數 1^l，且定義 G_1，G_2，G_t 在 DDH group 有相同的 order q。此演算法會隨機挑選$s_1,s_2\in\{0,1\}^l$，而 G_1 和 G_2 的生成點分別為 P_1 和 P_2。接著輸出 $K=[s_1,s_2]$和保持 P_2 的隱密性，並公開參數 $<P_1,G_1,G_2,G_t,\hat{e}>$。
- **SSE**(K,D)：輸入密鑰K和關鍵字的集合D，此演算法會隨機產生一個亂數$r\in Z_q^*$，並且計算$A_i=\frac{1}{rs_l}H_1(W_i)P_1$，$B=rs_2P_2$，$C=rP_2$。最後輸出可搜尋密文 $S=[A_1,\ldots A_m,B,C]$。
- **Trapdoor**(K,Q)：輸入金鑰 K 和欲搜尋的關

鍵字$Q=[W_{I_1}',\ldots,W_{I_t}',I_1,\ldots,I_t]$，演算法會選擇一個亂數$u\in Z_q^*$，和產生$v=\frac{s_2+u}{s_1}\sum_{i=1}^{t}H_1(W_{I_1}')$，$X=\hat{e}(P_1,P_2)$是可以預先計算的。最後輸出一個暗門 $T_Q=[T_1,T_2,I_1,..,I_t]$，其中 $I_1,..,I_t$ 為 Q 的關鍵字欄位(fields)，$T_1=H_2(X^v)$，$T_2=u$。

- **Tesst**(S,T_Q)：伺服器端利用 $S=[A_1,..,A_m,B,C]$ 和 T_Q 做測試。伺服器驗證 $H_2(\hat{e}(\sum_{i=1}^{t}A_{I_1},B+T_2C))?=T_1$，如果式子相等則輸出"yes"，否則輸出"no"。

當 $W_{I_1}=W_I'(1\le i\le t)$ 時，我們可以得到

$$H_2\left(\hat{e}\left(A_{I_1}+A_{I_2}+\ldots+A_{I_t},B+T_2C\right)\right)$$

$$=H_2(\hat{e}\,(\frac{1}{rs_1}H_1(W_{I_1})P_1+\ldots+\frac{1}{rs_1}H_1(W_{I_t})P_1,\ rs_2P_2+urP_2\,))$$

$$=H_2\left(\hat{e}\left(\sum_{i=1}^{t}H_1(W_{I_i})P_1,\frac{s_2+u}{s_1}P_2\right)\right)$$

$$=H_2\left(\hat{e}\left(\frac{s_2+u}{s_1}\sum_{i=1}^{t}H_1(W_{I_i})P_1,P_2\right)\right)$$

$$=H_2(\hat{e}(vP_1,P_2))$$

$$=H_2(X^v)=T_1$$

4.2 安全性分析

我們所提出的機制架構於 random oracle(RO)模型上，能夠在 vcoXDH 問題下抵擋動態選擇關鍵字攻擊(adaptive chosen keyword attack)具有語意上的安全。

定理 2 *如果vcoXDH問題是難以解決的問題，上述 SSE 機制架設在 ICRL 遊戲的 random oracle(RO)模型是安全的，且能抵擋選擇關鍵字攻擊(chosen keyword attack)。*

證明 我們假設有一攻擊者有不可忽略的機率贏得 ICLR 遊戲。在此分析中，我們考慮了可搜尋加密中的關鍵字和位置兩個部分。攻擊者 A 擁有ϵ的優勢可以贏得 ICLR。假設 A 最多可詢問 q_T 次暗門。我們建立一個挑戰者 B 有不可忽略的優勢ϵ'可以解決 vcoXDH 問題。使 P_2，aP_2，bP_1 和 cP_1 根據定義 3 做 vcoXDH 挑戰給 B。B 挑選一個 z 是隨機的。

KeyGen. B 給兩個值，$X=\hat{e}(P_1,P_2)$和$s\in Z_q$為一個密鑰。

SSE-queries. B 擁有四個欄位<W, x, Y, d>的 SSE-list，模擬 SSE 演算法如下。B 從 A 得知每一個關鍵字 W_i。如果關鍵字 W_i 不存在於 SSE-list 時，B 產生一個隨機位元值$d_i\in\{0,1\}$，$\Pr[d_i=0]=1/q_T$。且挑選隨機亂數$x_i\in Z_q$執行以下判斷：

- 如果 $d_i=0$，B 就回傳$Y_i=x_i(bP_1)\in G_1$。
- 如果 $d_i=1$，B 就回傳$Y_i=x_iP_1\in G_1$，並且增加<W_i, x_i, Y_i, d_i>到 SSE-list 中。

當我們要求計算 SSE(K,D_j)，其 d_z，W_z 同樣為 0 時，則 B 挑選隨機亂數 r_j，輸出

$$\mathrm{SSE}(K,D_j)=[\ \frac{1}{r_j}x_1P_1,\ \frac{1}{r_j}x_2P_1,\ \ldots,\frac{1}{r_j}x_z(bP_1),\ldots,\frac{1}{r_j}x_mP_1,\ r_jP_2,\ sP_2]。$$

Trapdoor-queries. 當要求計算 ***Trapdoor***(K,Q)時，A 不可以詢問位址為 z 的關鍵字 W_z，其 $Q=[W_{I_1}',\ldots,W_{I_t}',I_1,\ldots,I_t]$。如果 A 詢問了，就回報錯誤並且終止，B 選擇一個亂數$u\in Z_q$且計算$\tilde{x}=x_{I_1}+\ldots+x_{I_j}$，最後回傳$T_1=X^{(s+u)\tilde{x}}$和$T_2=u$給 A，其$x_{I_1},\ldots,x_{I_j}$是 SSE-list 中的關鍵字。

Challenge. A 給$D=\{W_1,W_2,\ldots,W_m\}$，索引的集合 $T\subseteq\{1,\ldots,m\}$，且決定$t\in T$。

- 如果$z\neq t$，B 就回應對於 vcoXDH 的一個隨機猜測。
- 如果$z=t$，B 就會執行以下工作：得到 $E_t=x_t(\frac{1}{a}P_1)$和當$j\in T$時，E_j 為一亂數，且 $j\neq t$；當$j\notin T$時，$E_j=x_j(aP_1)$。

接著 B 會傳送可搜尋的密文$(E_1,\ldots,E_m,aP_2,saP_2)$給 A。如果 B 得到 $z=t$ 且關鍵字為 W_z，則 B 是一個無效的挑戰。我們可以知道密文在$j\notin T$

的位置上，如同 D 的 SSE 一樣。如果$c=\frac{b}{a}$，則密文如同 D 的 SSE 在相同的位置 t 上；否則不相同。

More queries. 在 **Challenge** 之後，A 可以繼續詢問 SSE 和 Trapdoor。惟一的限制是 A 不可以詢問先前的 D。這個限制可以確保 B 已經成功地回應所有的詢問

Output. 最後，攻擊者 A 會輸出所猜測的 $\alpha \in \{0,1\}$，決定挑戰的密文是從 B 回應的 D_0 或 D_1。

- 如果$\alpha=0$，則 B 猜測此挑戰不是 vcoXDH 中的四個值。
- 如果$\alpha=1$，則 B 猜測此挑戰是 vcoXDH 中的四個值。

在加密時，位置 t 是隨機的若且為若挑戰的不是 vcoXDH 中的四個值。

經過上述，我們定義了兩個事件：

- ε_1：B 成功計算 ***Trapdoor***(K,Q)。在詢問有關位置 t 的關鍵字後，機率至少為 $1/e$[7]。A 的暗門詢問並不會尋找 $d=0$ 的關鍵字。我們假設最多 m 個關鍵字會被搜尋到，則機率為$(1/e)^m$，所以$\Pr[\varepsilon_1] \geq 1/e^m$。
- ε_2：在挑戰過程中 B 不會失敗。因為 B 猜測的位置 z 剛好和位置 t 相同，A 將決定 ICLR 遊戲中的第 2 步驟。所以$\Pr[\varepsilon_2] \geq 1/q_T m$。

最後，B 不會失敗。根據ε_1和ε_2，得$\Pr[\varepsilon_1 \cap \varepsilon_2] \geq 1/e^m q_T m$。對手 B 解決 vcoXDH 的優勢為$\epsilon' \geq \epsilon / e^m q_T m$。

對於上述的分析，讓我們給定一個詢問的範例。A 必須詢問許多關鍵字，其中一個關鍵字是"DH"，這個關鍵字被決定在 SSE 清單中 $d=0$，$Y=x(bP_1)$以及位置 z。當 A 產生暗門詢問，並不會問關鍵字"DH"，這能夠確保遊戲並不會失敗。最後 A 傳送一個挑戰文件給 B 用來執行 $Rand(D,T)$，$Rand(D,T\text{-}\{t\})$。如果挑戰的關鍵字位置為 $t=z$ 而且是"DH"，A 可以猜測成功，等同於 B 可以針對 A 的結果來解決 vcoXDH 問題。

5 比較

此節將我們所提出的機制和 Ballard 等人[3]、Ryu 等人[11]的機制做一計算成本的比較，如表 1。使用符號的定義如下：

符號定義	
S	：橢圓曲線的純量乘法
exp	：有限領域的指數
pr	：雙線性配對的計算量
m	：關鍵字欄位的數量
Encryption	：Encryption 的計算成本
Trapdoor	：Trapdoor 的計算成本
Test	：Test 的計算成本

圖 1 符號定義圖

雙線性配對的計算成本遠大於橢圓曲線上點的純量積[2][16]。在相同的 order q 之下，有限領域的指數的執行效率比橢圓曲線純量乘法好。我們所提出的機制在 **Trapdoor** 和 **Test** 的效率比 RT[11]及 BKM[3]來的好。我們所提出的機制基於 vcoXDH 問題上能夠適當的抵擋選擇關鍵字攻擊(adaptive chosen keyword attack)具有語意上的安全。

表 1 效率比較表

Factor	RT[18]	BKM[4]	Proposed
Encryption	$(m+1)S+1pr$	$(m+1)S$	$(m+1)S$
Trapdoor	$2S$	$2S$	$1exp$
Test	$2pr$	$2pr$	$1pr$

6 結論

我們提出一個改進的基於關鍵字對稱式

可搜尋加密的機制。攻擊者無法從可搜尋的密文或暗門獲得重要的訊息。我們所提出的機制更有效率且可適用於移動設備上。在 random oracle(RO) 模型下可抵擋動態選擇關鍵字攻擊具有語意上的安全。

致謝

本研究由國科會補助完成，計畫編號：NSC99-2221-E-005-078。

參考文獻

[1] J. Baek, R. Safavi-Naini, andW. Susilo, "Public key encryption with keyword search revisited," in: ***Computational Science and Its Applications 2008***, LNCS 5072, 2008, pp. 1249-1259.

[2] J. Baek, R. Safavi-Naini, and W. Susilo. "Certificateless public key encryption without pairing," in: ***ISC 05***, LNCS 3650, 2005, pp. 134-148.

[3] L. Ballard, S. Kamara, and F. Monrose, "Achieving Efficient Conjunctive Keyword Searches over Encrypted Data," in: ***ICICS 2005***, LNCS 3783, 2005, pp. 414-426.

[4] D. Boneh. "The Decision Diffie-Hellman Problem," in: ***ANTS-III***, LNCS1423, 1998, pp. 48-63.

[5] D. Boneh, G.D. Crescenzo, R. Ostrovsky, G. "Persiano, Public key encryption with keyword search," in: ***Eurocrypt 2004***, LNCS 3089, 2004, pp. 31-45.

[6] J. Byun, D. Lee, and J. Lim, "Efficient Conjunctive Keyword Search on Encrypted Data Storage System," in: ***EuroPKI 2006***, LNCS 4043, 2006, pp. 184-196.

[7] E.J. Goh, "Secure index," ryptology ePrint Archive: Report 2003/216, 2003.

[8] P. Golle, J. Staddon, B. Waters, "Secure conjunctive keyword search over encrypted data," in: ***ACNS 2004***, LNCS 3089, 2004, pp. 31-45.

[9] I. Jeong , J. Kwon, D. Hong, and D. Lee, "Constructing PEKS schemes against keyword guessing attacks is possible? ," ***Computer Communications 32 (2009)***, pp. 394-396.

[10] D.J. Park, K. Kim, P.J. Lee, "Public key encryption with conjunctivefield keyword search," in: ***WISA 2004***, LNCS 3325, 2004, pp. 73-86.

[11] E. K. Ryu and T. Takagi, "Efficient Conjunctive Keyword-Searchable Encryption," in: ***Advanced Information Networking and ApplicationsWorkshops***, 2007, pp. 409-414.

[12] D. Song, D.Wagner, A. Perrige, "Practical techniques for searches on encrypted data," in: ***Proceedings of the IEEE Security and Privacy Symposium***, 2000, pp. 44-55.

[13] Q. Tang. "Revisit the Concept of PEKS: Problems and a Possible Solution," Technical Report TR-CTIT-08-54, Centre for Telematics and Information Technology, University of Twente, Enschede, 2008.

[14] V. Miller, "Short programs for functions on curve," unpublished manuscript, 1986.

[15] C. Liu, G. Horng, and T. Chen, "Further refinement of pairing computation based on Miller's algorithm," ***Applied Mathematics and Computation 189 (2007)***, pp.395-409.

[16] A. Saxena, "The BLS Scheme to Identity Based Signatures," http://sites.google.com/site/saxenaamitabh/saxena05ibs.pdf, 2006.