Controllabe Privacy Preserving Search Based on Symmetric Predicate Encryption in Cloud Storage

Authors: Chun-I Fan and Shi-Yuan Huang

Department of Computer Science and Engineering
National Sun Yat-sen University, Taiwan (R.O.C.)

The final publication is available at http://www.sciencedirect.com

CyberC 2011: International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, Beijing, China, Oct. 10-12, 2011
Controllable Privacy Preserving Search Based on Symmetric Predicate Encryption in Cloud Storage

Outline

- Introduction
- Mathematical Background & Definition of Security
- Proposed Scheme
- Security Proofs & Properties Comparisons
- Implementation
- Conclusion
Controllable Privacy Preserving Search Based on Symmetric Predicate Encryption in Cloud Storage

Introduction

System Overview

Secret Key Owner (Manager)

Secret Key Generation

Token Generation

Cloud Storage Server

Encryption

M, SK, Vector x

Ciphertext CT

Delegated Person (Staff)

Query (Generate Query by Using Search Token)

Matched Ciphertexts

Test

{M}

Search Token

Secret Key Owner

SK

SK, Vector y

Search Token

Encryption

Decryption

Search Token
Propose a variant of symmetric predicate encryption, which provides controllable privacy preserving search functionalities

- **Revocable delegated search**
  - The owner of a cloud storage can easily control the lifetimes of search token

- **Un-decryptable delegated search**
  - A delegated person cannot decrypt the returned matched ciphertexts even though he has the delegated privilege of search
Controllable Privacy Preserving Search Based on Symmetric Predicate Encryption in Cloud Storage

Mathematical Background

- Bilinear Pairing

- Asymmetric prime order bilinear groups
- Cyclic multiplicative groups \( G_1, G_2 \) and \( G_T \) of order \( p \)
- Pairing function \( e : G_1 \times G_2 \rightarrow G_T \)
- \( e(x^a, y^b) = e(x, y)^{ab} \) for all \( x \in G_1, y \in G_2, x \neq 1, y \neq 1, a, b \in \mathbb{Z}_p \)
- \( g_1, g_2 \) and \( e(g_1, g_2) \) are generators of \( G_1, G_2 \) and \( G_T \) respectively
The Decisional BDH Problem. The Decisional BDH problem in \((G_1, G_2)\) is defined as follows: given a 8-tuple \([g_1, g_1^{z_1}, g_1^{z_2}, g_1^{z_3}, g_2, g_2^{z_1}, g_2^{z_2}, Z] \in G_1^4 \times G_2^3 \times G_T\) for random \([z_1, z_2, z_3] \in \mathbb{Z}_p^3\) as input, output 1 if \(Z = e(g_1, g_2)^{z_1 z_2 z_3}\) or 0 otherwise.

The Decisional Linear Problem. The Decisional Linear problem in \((G_1, G_2)\) is defined as follows: given a 9-tuple \([g_1, g_1^{z_1}, g_1^{z_2}, g_1^{z_1 z_3}, g_1^s, g_2, g_2^{z_1}, g_2^{z_2}, Z] \in G_1^5 \times G_2^3 \times G_1\) for random \([z_1, z_2, z_3, s] \in \mathbb{Z}_p^4\) as input, output 1 if \(Z = g_1^{z_2(s - z_3)}\) or 0 otherwise.
Controllable Privacy Preserving Search Based on Symmetric Predicate Encryption in Cloud Storage

Definition of Security

Experiment of Semantic Security
Controllable Privacy Preserving Search Based on Symmetric Predicate Encryption in Cloud Storage

- Definition of Security
- Experiment of Attribute Hiding

**Adversary**

- $(x_0, x_1)$ with $x_0 \neq x_1$

**Simulator**

- Generate $SK$

Request $K_y$

- $K_y$ with $P_{x_0}(y) = P_{x_1}(y)$

Choose $\mu, \bar{\mu} \in \{0,1\}$

- $CT \leftarrow Encryption(SK, x_\mu, M_{\bar{\mu}})$

Request $K_y$

- $K_y$ with $P_{x_0}(y) = P_{x_1}(y)$

Output $\mu', \bar{\mu'} \in \{0,1\}$

- $\mu'$

- $Pr[\mu' = \mu]$ significant?
Controllable Privacy Preserving Search Based on Symmetric Predicate Encryption in Cloud Storage

- Proposed Scheme
- Secret Key Generation

Secret Key Generation

Token Generation

Secret Key Owner

Encryption

Cloud Storage Server

Test

Delegated Person

Decryption

{M}

M, SK, Vector x

Ciphertext CT

PToken, TRToken

Query (Generate Query by Using PToken, TRToken)

Matched Ciphertexts

PToken, TRToken

SK

SK, Vector y

PToken, TRToken
[Secret Key Generation] Initially, the secret key owner publishes public parameters
\[ I = [p, G_1, G_2, G_T, g_1, g_2, e, H : G_T \rightarrow G_T, H_2 : \{0, 1\}^* \rightarrow G_2^*, H_3 : G_2 \rightarrow G_2^*] \]

- Randomly choose \( f \) and \( \bar{f} \in \mathbb{Z}_p \) and set \( F = e(g_1, g_2)^f \) and \( \bar{F} = e(g_1, g_2)^{\bar{f}} \).

- For \( 1 \leq i \leq n \), randomly choose \( a_{i,0}, a_{i,1}, b_{i,0}, b_{i,1} \in \mathbb{Z}_p \) and set \( A_{i,0} = g_1^{a_{i,0}} \), \( A_{i,1} = g_1^{a_{i,1}} \), \( B_{i,0} = g_1^{b_{i,0}} \), \( B_{i,1} = g_1^{b_{i,1}} \), \( \hat{A}_{i,0} = g_2^{a_{i,0}^{-1}} \), \( \hat{A}_{i,1} = g_2^{a_{i,1}^{-1}} \), \( \hat{B}_{i,0} = g_2^{b_{i,0}^{-1}} \), \( \hat{B}_{i,1} = g_2^{b_{i,1}^{-1}} \).

- Set the secret key \( SK = (I, F, \bar{F}, f, \bar{f}, \{SK_i\}_{i=1}^n) \), where \( SK_i = (A_{i,0}, A_{i,1}, B_{i,0}, B_{i,1}, \hat{A}_{i,0}, \hat{A}_{i,1}, \hat{B}_{i,0}, \hat{B}_{i,1}) \).
Controllable Privacy Preserving Search Based on Symmetric Predicate Encryption in Cloud Storage

Proposed Scheme

Encryption

---

Secret Key Generation

Token Generation

Delegated Person

Secret Key Owner

Cloud Storage Server

Encryption

Ciphertext $CT$

$M, SK, \text{Vector } x$

$SK, \text{Vector } y$

PToken, TRToken

Query (Generate Query by Using PToken, TRToken)

Matched Ciphertexts

Test

Decryption

PToken

$\{ M \}$
[Encryption] Before storing messages in the cloud storage, the secret key owner does the following encryption procedure.

- Input: a message $M \in \mathbb{G}_T$, an attribute vector $\mathbf{x} = (x_1, x_2, ..., x_n) \in \{0,1\}^n$ and $SK$.
- Randomly choose $s \in \mathbb{Z}_p$, and select $s_i \in \mathbb{Z}_p$ at random for $1 \leq i \leq n$.
- Randomly choose a one-time session key $K \in \mathbb{G}_T$.
- Compute a ciphertext: $CT = Enc(SK, K, \mathbf{x}, M) = [\Omega_1, \Omega_2, \theta, \{X_i, V_i\}_{i=1}^n]$, where $\Omega_1 = \bar{F}^{-s}$, $\Omega_2 = K \cdot F^{-s}$, $\theta = M \oplus H(K)$, $X_i = A_{i,s_i}^{s-s_i}$, $V_i = B_{i,s_i}^{s_i}$.
- Return $CT$. 
Controllable Privacy Preserving Search Based on Symmetric Predicate Encryption in Cloud Storage

Proposed Scheme

Token Generation

Secret Key Owner

Secret Key Generation

SK

M, SK, Vector x

Encryption

Cloud Storage Server

Test

PToken, TRToken

Query (Generate Query by Using PToken, TRToken)

Matched Ciphertexts

Decryption

{M}

Delegated Person

PToken, TRToken

SK, Vector y

PToken, TRToken

Encryption

PToken
[Token Generation] Produce a predicate token $PToken$ and a time restrictive token $TRToken$. $PToken$ can provide un-decryptable delegated search while $TRToken$ is used for revocable delegated search.

- **Input**: a vector $y = (y_1, y_2, \ldots, y_n) \in \{0, 1, *\}^n$ and $SK$.
- Let $S_y$ be the set of indices for $y_i \neq *$ and $|S_y| = n'$.
- For each $i \in S_y$, randomly choose $t_{i,1}, t_{i,2} \in \mathbb{Z}_p$ such that $\Sigma_{i \in S_y} t_{i,1} \equiv \bar{f}(\text{mod } p)$, $\Sigma_{i \in S_y} t_{i,2} \equiv f(\text{mod } p)$ and set the predicate token $PToken$, $K_y = (i, Y_{i,1}, W_{i,1}, Y_{i,2}, W_{i,2})_{i \in S_y}$, where $Y_{i,1} = \hat{A}_{i,y_i}^{t_{i,1}}$, $W_{i,1} = \hat{B}_{i,y_i}^{t_{i,1}}$, $Y_{i,2} = \hat{A}_{i,y_i}^{t_{i,2}}$ and $W_{i,2} = \hat{B}_{i,y_i}^{t_{i,2}}$.
- If the secret key owner does not permit the delegated person to decrypt the returned matched ciphertexts received from the server, then output the $PToken$, $K_y = (i, Y_{i,1}, W_{i,1}, \bot, \bot)_{i \in S_y}$.
- In order to control the lifetime period of delegated search privilege, the secret key owner randomly chooses a time restrictive token $TRToken$, $K_t \in \mathbb{Z}_p$ for the predicate token, and sends a public value $g_3^{K_t}$ to the server, where $g_3 = H_3(\Sigma_{i \in S_y} (Y_{i,1} + W_{i,1}))$.
- Return $(K_y, K_t)$. 
Controllable Privacy Preserving Search Based on Symmetric Predicate Encryption in Cloud Storage

**Proposed Scheme**

**Test**

---

**Secret Key Owner**

- **Secret Key Generation**
  - SK

- **Token Generation**
  - SK, Vector y
  - PToken, TRToken

**Encryption**

- M, SK, Vector x
- Ciphertext CT

**Cloud Storage Server**

**Delegated Person**

- PToken, TRToken

**Query (Generate Query by Using PToken, TRToken)**

**Decryption**

- Matched Ciphertexts

- PToken

- \{M\}

---

{15 / 41}
[Test] The cloud storage server performs the test procedure to search all matched ciphertexts.

- The delegated person makes a query \( \{(i, Y_{i,1}, W_{i,1})_{i \in S_y}, T_{send}, H_2(T_{send})^{K_t}, K_r \} \) to the server.

- The cloud storage server verifies if
  \[
  e(H_3(\Sigma_{i \in S_y} (Y_{i,1} + W_{i,1})), H_2(T_{send})^{K_t}) = e(g_3^{K_t}, H_2(T_{send})).
  \]

- For \( \Omega_1 \) of every ciphertext in the cloud storage, check if \( 1 = \Omega_1 \cdot \prod_{i \in S_y} e(X_i, Y_{i,1}) e(V_i, W_{i,1}) \). If true, keep this matched ciphertext; else discard it.

- Encrypt all matched ciphertexts \( CT \)'s and then send \( \{CT \}'s \) to the delegated person.
Verification of $H_2(T_{\text{send}})^{K_t}$:
\[
e(H_3(\Sigma_{i\in S_y} (Y_{i,1} + W_{i,1})), H_2(T_{\text{send}})^{K_t})
= e(g_3, H_2(T_{\text{send}})^{K_t})
= e(g_3^{K_t}, H_2(T_{\text{send}}))
\]

Correctness of Test:
\[
\Omega_1 \cdot \prod_{i\in S_y} e(X_i, Y_{i,1}) \cdot e(V_i, W_{i,1})
= \Omega_1 \cdot \prod_{i\in S_y} e(A_{i,x_i}^{s-s_i}, \hat{A}_{i,y_i}^{t_i,1}) \cdot e(B_i^{s_i}, \hat{B}_{i,y_i}^{t_i,1})
= \Omega_1 \cdot \prod_{i\in S_y} e(A_{i,x_i}^{s-s_i}, \hat{A}_{i,x_i}^{t_i,1}) \cdot e(B_i^{s_i}, \hat{B}_{i,x_i}^{t_i,1})
= \Omega_1 \cdot \prod_{i\in S_y} e(g_1^{a_i,x_i(s-s_i)}, g_2^{a_i^{-1} \cdot t_i,1}) \cdot e(g_1^{b_i,x_i \cdot s_i}, g_2^{b_i^{-1} \cdot t_i,1})
= \Omega_1 \cdot \prod_{i\in S_y} e(g_1^{(s-s_i)_{t_i,1}}, g_2) \cdot e(g_1^{s_i \cdot t_i,1}, g_2)
= \Omega_1 \cdot \prod_{i\in S_y} e(g_1, g_2)^{s \cdot t_i,1}
= \Omega_1 \cdot e(g_1, g_2)^{s \cdot \Sigma_{i\in S_y} t_i,1} = \Omega_1 \cdot e(g_1, g_2)^{s \cdot \bar{f}}
= \bar{F}^{-s} \cdot e(g_1, g_2)^{s \cdot \bar{f}} = e(g_1, g_2)^{-s \cdot \bar{f}} \cdot e(g_1, g_2)^{s \cdot \bar{f}}
= 1
Controllable Privacy Preserving Search Based on Symmetric Predicate Encryption in Cloud Storage

Proposed Scheme

Decryption and Revocation of Search Privilege

Secret Key Owner

Secret Key Generation

$SK$

$SK$, Vector $y$

Encryption

Cloud Storage Server

Ciphertext $CT$

Test

Matched Ciphertexts

Delegated Person

Token Generation

PToken, TRToken

Query (Generate Query by Using PToken, TRToken)

Decryption

PToken

{$M$}
[Decryption] The delegated person performs the decryption procedure for each returned ciphertext to get the corresponding plaintext.

- Input: a returned CT and \((i, Y_{i,2}, W_{i,2})_{i \in S_y}\).
- Compute \(K = \Omega_2 \cdot \prod_{i \in S_y} e(X_i, Y_{i,2})e(V_i, W_{i,2})\).
- Compute \(M = \theta \oplus H(K)\).

[Revocation of Search Privilege]

- If the secret key owner wants to revoke the delegated person’s predicate token, he can easily perform the revocation procedure by deleting \(g_3^{K_t}\) in the cloud storage server.
- The revoked predicate token cannot pass the test procedure hereafter.
Correctness of Decryption:
\[ \Omega_2 \cdot \prod_{i \in S_y} e(X_i, Y_{i,2}) e(V_i, W_{i,2}) = \Omega_2 \cdot \prod_{i \in S_y} e(A_i^{s-s_i}, \hat{A}_{i,x_i}^{t_i,2}) e(B_{i,x_i}, \hat{B}_{i,y_i}^{t_i,2}) = \Omega_2 \cdot \prod_{i \in S_y} e(A_i^{s-s_i}, \hat{A}_{i,x_i}^{t_i,2}) e(B_{i,x_i}, \hat{B}_{i,x_i}^{t_i,2}) = \Omega_2 \cdot \prod_{i \in S_y} e(g_1 a_{i,x_i}^{s-s_i}, g_2^{-1} b_{i,x_i}^{-1} t_i^{t_i,2}) e(g_1, g_2)^{a_{i,x_i}^{-t_i,2} b_{i,x_i} s_i} = \Omega_2 \cdot \prod_{i \in S_y} e(g_1, g_2)^{s \cdot t_i,2} = \Omega_2 \cdot e(g_1, g_2)^{s \cdot \Sigma_{i \in S_y} t_i,2} = \Omega_2 \cdot e(g_1, g_2)^{s \cdot f} = K \cdot F^{-s} \cdot e(g_1, g_2)^{s \cdot f} = K \cdot e(g_1, g_2)^{-s \cdot f} \cdot e(g_1, g_2)^{s \cdot f} = K \]
Proof. Suppose that there exists a PPT adversary $A$ who successfully wins the game of semantic security with probability non-negligibly larger than $1/2$.

An adversary $B$ can be constructed for the game of Decision BDH that uses $A$ as subroutine. Suppose a Decision-BDH problem instance is given to the simulator $B$ a 8-tuple $[g_1, Z_1 = g_1^{z_1}, Z_2 = g_1^{z_2}, Z_3 = g_1^{z_3}, g_2, \hat{Z}_1 = g_2^{z_1}, \hat{Z}_2 = g_2^{z_2}, Z] \in G_1^4 \times G_2^3 \times G_T$ for random $[z_1, z_2, z_3] \in (\mathbb{Z}_p)^3$, decide whether $Z = e(g_1, g_2)^{z_1z_2z_3}$ or a random element of $G_T$.
**Initiation.** $B$ runs $A$ who announce an attribute vector $x = (x_1, x_2, \ldots, x_n)$ that $A$ wishes to attack.

**Setup.** Let $F = e(Z_1, \hat{Z}_2)$, it implies $f = z_1 z_2$. Randomly choose $(\vec{a}_i, 0, \vec{a}_i, 1, \vec{b}_i, 0, \vec{b}_i, 1) \in \mathbb{Z}_p$ for $i = 1$ to $n$. Then we let $A_{i,x_i} = g_1^{\vec{a}_i x_i}$, $B_{i,x_i} = g_1^{\vec{b}_i x_i}$, $A_{i,1-x_i} = Z_2^{\vec{a}_i,1-x_i}$ and $B_{i,1-x_i} = Z_2^{\vec{b}_i,1-x_i}$. Finally, set $SK = [I, F, f, (A_{i,0}, A_{i,1}, B_{i,0}, B_{i,1})_{i=1}^n]$. 

**Security Proofs**

**Semantic Security**
Query 1.

- we must select an index $j$ such that $x_j \neq y_j$ and $y_j \neq \ast$. We set a initial value of a variable $\hat{f} = 0$.

- For each index $i$, $i \neq j$ and $y_i \neq \ast$, we randomly choose $\bar{\epsilon}_i \in \mathbb{Z}_p$ and set $\hat{f} \leftarrow \sum \bar{\epsilon}_i$.

Then let $Y_j = \hat{Z}_1^{\frac{1}{a_j}, \bar{\epsilon}_j} g_2^{\frac{1}{a_j}, y_j}$ and $W_j = \hat{Z}_1^{\frac{1}{b_j}, \bar{\epsilon}_j} g_2^{\frac{1}{b_j}, y_j}$.

- Next, for each index $i(i \neq j)$: (1) If $y_i = x_i$, then set $Y_i = \hat{Z}_2^{\frac{\bar{\epsilon}_i}{a_i y_i}}$ and $W_i = \hat{Z}_2^{\frac{\bar{\epsilon}_i}{b_i y_i}}$.

(2) If $y_i \neq x_i$, then set $Y_i = g_2^{\frac{\bar{\epsilon}_i}{a_i y_i}}$ and $W_i = g_2^{\frac{\bar{\epsilon}_i}{b_i y_i}}$. Finally, $B$ returns a token $K_y = (Y_i, W_i)_{i \in S_y}$ to $A$. 
Challenge. Adversary \( \mathcal{A} \) gives two messages \( M_0 \) and \( M_1 \) to the simulator \( \mathcal{B} \). A random bit \( \mu \in \{0, 1\} \) is chosen by \( \mathcal{B} \). Then \( \mathcal{B} \) computes \( \Omega_1 = Z^{-1}, \Omega_2 = K \cdot Z^{-1}, \theta = M_\mu \oplus H(K), X_i = Z_3^{\bar{a}_i} A_i^{-s_i}, V_i = B_i^{s_i} \). Finally, \( \mathcal{B} \) returns a ciphertext \( CT = \{\Omega_1, \Omega_2, \theta, (X_i, V_i)_{i=1}^n\} \) to \( \mathcal{A} \).

We observe that if \( Z = e(g_1, g_2)^{z_1 z_2 z_3} \), then \( CT \) is \( \{\Omega_1 = F_{z_3}^{-1}, \Omega_2 = K \cdot F_{z_3}^{-1}, \theta = M_\mu \oplus H(K), X_i = Z_3^{\bar{a}_i} A_i^{-s_i}, V_i = B_i^{s_i}\} \) with \( s = z_3 \). If \( Z \) is a random element of \( G_T \), then \( CT \) is independent from \( \mu \).
Query II. It is identical to Query I.

**Output.** $A$ outputs a bit $\mu' \in \{0, 1\}$. $B$ return 1 iff $\mu' = \mu$. 
**Security Proofs**

**Attribute Hiding**

**Proof.** Suppose that there exists a probabilistic polynomial time adversary $A$ who successfully wins the game of Attribute Hiding with probability non-negligibly larger than $1/2$. An adversary $B$ can be constructed for the Decisional Linear game that uses $A$ as a subroutine. Suppose that the simulator $B$ is given to a Decisional Linear problem instance, i.e., a 9-tuple $[g_1, Z_1 = g_1^{z_1}, Z_2 = g_1^{z_2}, Z_{13} = g_1^{z_1z_3}, S = g_1^s, g_2, \hat{Z}_1 = g_2^{z_1}, \hat{Z}_2 = g_2^{z_2}, Z] \in \mathbb{G}_1^6 \times \mathbb{G}_2^3$ for random $[z_1, z_2, z_3] \in (\mathbb{Z}_p)^3$. $B$ wants to decide whether $Z = g_1^{z_2(s-z_3)}$ or not.

The detailed description of proof for attribute hiding is written in the paper.

<table>
<thead>
<tr>
<th>Adversary</th>
<th>Simulator</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\langle x_0, x_i \rangle$ with $x_0 \neq x_i$</td>
<td>$\langle x_0, x_i \rangle$ with $x_0 \neq x_i$</td>
</tr>
<tr>
<td>Request $K_r$</td>
<td>Generate $SK$</td>
</tr>
<tr>
<td>$K_r$ with $P_{\ast}(y) = P_{\ast}(y)$</td>
<td>$M_0, M_1$</td>
</tr>
<tr>
<td>$CT \leftarrow Encryption(SK, x_i, M_x)$</td>
<td>Choose $\mu, \overline{\mu} \in_r {0,1}$</td>
</tr>
<tr>
<td>Request $K_r$</td>
<td></td>
</tr>
<tr>
<td>$K_r$ with $P_{\ast}(y) = P_{\ast}(y)$</td>
<td></td>
</tr>
<tr>
<td>Output $\mu', \overline{\mu'} \in {0,1}$</td>
<td>$\mu'$</td>
</tr>
<tr>
<td>$Pr[\mu' = \mu]$ significant?</td>
<td></td>
</tr>
</tbody>
</table>
**Properties Comparisons**

<table>
<thead>
<tr>
<th></th>
<th>Blundo et al.</th>
<th>Shen et al.</th>
<th>Ours</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revocable Delegated Search</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td>Un-decryptable Delegated Search</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td>Prime Order*</td>
<td>YES</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td>Supporting Inner Product**</td>
<td>NO</td>
<td>YES</td>
<td>NO</td>
</tr>
</tbody>
</table>

*: It is more efficient than the schemes based on composed-order groups.

**: Inner product based schemes can support more complex queries.
Controllable Privacy Preserving Search Based on Symmetric Predicate Encryption in Cloud Storage

Implementation (Web-Based System)

Secret Key Owner

Private Cloud

Secret Key Generation

Token Generation

Public Cloud

Encryption

Cloud Storage Server

Test

User

Query (Generate Query by Using PToken, TRToken)

Matched Ciphertexts

Decryption

{M}
Java

Libraries:
- The Pairing-Based Cryptography Library (http://crypto.stanford.edu/pbc/)
- The GNU Multiple Precision Arithmetic Library (http://gmplib.org)

The default language of graphical interface is Traditional Chinese (In version 1)
- The implemented system can process English or Chinese data
探雲取物 神秘空手 設計

這是一個即將走向雲端化的時代
人們不再單獨依賴個人電腦進行運算，而將所有的資料放置雲端
但是讓雲端看見我們的資料，真的讓人放心嗎？

本作品為「探雲取物 密文搜尋系統」
僅讓雲端儲存密文而無法瞭解資料內容，同時我們亦能對密文做歸檔與搜尋等管理

系統可分為公有雲與私有雲
在公有雲進行密文搜尋，而在私有雲進行檔案加密與金鑰權限管理
藉此保護使用者資料之隱私

公有雲 密文搜尋系統
私有雲 金鑰權限管理系統

神密空手 諸葛萬有
本網站建議使用 Google Chrome 檢覽器觀看，並設定 1280*1024 解析度，以獲得最佳瀏覽效果
Controllable Privacy Preserving Search Based on Symmetric Predicate Encryption in Cloud Storage

Implementation (Web-Based System)

Public Cloud – Login
Controllable Privacy Preserving Search Based on Symmetric Predicate Encryption in Cloud Storage

Implementation (Web-Based System)

Public Cloud – Search or Test
Controllable Privacy Preserving Search Based on Symmetric Predicate Encryption in Cloud Storage

Implementation (Web-Based System)

Public Cloud – Download Decryption Program
Controllable PrivacyPreserving Search Based on Symmetric Predicate Encryption in Cloud Storage

Implementation (Web-Based System)

Public Cloud – Decryption Program
Controllable Privacy Preserving Search Based on Symmetric Predicate Encryption in Cloud Storage

Implementation (Web-Based System)

Private Cloud – Login
Controllable Privacy Preserving Search Based on Symmetric Predicate Encryption in Cloud Storage

Implementation (Web-Based System)

Private Cloud – Token Generation
Controllable Privacy Preserving Search Based on Symmetric Predicate Encryption in Cloud Storage

Implementation (Web-Based System)

Private Cloud – Revocation of Search Token
Controllable Privacy Preserving Search Based on Symmetric Predicate Encryption in Cloud Storage

Implementation (Web-Based System)

Private Cloud – Encryption
Controllable Privacy Preserving Search Based on Symmetric Predicate Encryption in Cloud Storage

Implementation (Web-Based System)

Private Cloud – Management
Our scheme makes it possible for a cloud storage owner to easily manage the lifetimes and search privileges of his cloud data.

- We have implemented a web-based system according to our proposed scheme.
- Our further research will focus on the construction that can support complex access control and search privileges.
Thank you!

http://ac.cse.nsysu.edu.tw/