2. \( p_{lb} = 5 \) \( / \frac{\text{g}}{\text{lb}} \)

\((1, 9, 0, 1, 6, 2, 12) \in \mathbb{R}

\text{Set up: } \text{Given } k \in \mathbb{R}

\text{Base: } \text{IE: that satisfies}

\text{Note Title: } 22/12/013
2) If \( d \to a \to 0 \), then \( d \) is 0.

1) If \( a \to b \to 0 \), then \( b \) is 0.

Example: For any 0 \( a \in \mathcal{O}(13) \),

\[
\begin{align*}
\{g, 6, 1, g^2, e, p, u, H, 1, H^1, H^2, \ldots\}
\end{align*}
\]

\( 3 \) Choose \( H \) such that \( H \to \mathcal{O}(13) \to 6 \).
\[
\left\langle I_0^0, I_2^0, \mathcal{G} \right\rangle \quad \forall C \subseteq \mathcal{G}
\]

\[
\forall \mathcal{G}, \exists \mathcal{G}' \implies I_0 \in \mathcal{G}' \quad \forall \mathcal{G}, \exists \mathcal{G}' \implies I_0 \in \mathcal{G}'
\]

\[
2. \quad \mathcal{G} \implies I_0 \implies I_0 \implies I_0
\]

\[
\mathcal{G} \implies I_0 \implies I_0 \implies I_0
\]

**Example:** A param set \( \mathcal{G} \), \( \mathcal{G} \), \( \mathcal{G} \), \( \mathcal{G} \), \( \mathcal{G} \)
\[ C = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \]

Let \( C = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \)

The determinant of \( C \) is:

\[ \det(C) = ad - bc \]

In this case, \( \det(C) = 2*2 - 1*1 = 3 \)

The inverse of \( C \) is:

\[ C^{-1} = \frac{1}{\det(C)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \]

\[ C^{-1} = \frac{1}{3} \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix} \]

The original matrix is:

\[ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \]

Decryption process:

\[ M = C^{-1} \cdot \begin{pmatrix} e \\ f \end{pmatrix} \]

// Insert the decryption formula here. //
than E A(\alpha \cup B \text{ attacking } E(c))

More precisely it \in A(\alpha \cup B)

\text{The above system is secure}

\text{If } 1 \leq i \leq r, \text{ then } H_2 (\text{I}_i, \text{I}_0) = \mu \left( H_2 (\text{I}_i, \text{I}_0) \right)

\text{I}_0 = \vee (H_2 (\text{I}_i, \text{I}_0))
$\beta \cdot 0.1 \ \text{with at least prob.}$
is IND-CCA secure in Gandon

then \( \forall_{\text{msg}} \sim \mathcal{D}(\|	ext{msg}\|, \mathcal{H}, (\|m\|, \mathcal{H})) \) if

Assume \( \exists_{\text{E}, \text{E}'}(\mathcal{M}, \mathcal{R}) \) IND-CCA secure pair

P using \( \mathcal{E}, \mathcal{E}' \) insecure - Okamoto scheme for R are both

\( \mathcal{E}, \mathcal{E}' \) indistinguishable - Okamoto scheme secure

\( \mathcal{E}, \mathcal{E}' \) indistinguishable - Basic Ident + cIBE

We can use P using Okamoto scheme
(0 \rightarrow H_i)

\text{E} = 0.13 \\
\text{Extract: no change}

H_2 = 20.13 \text{ m}

\text{Add: 0.13} \times 20.13 = 2.6

Setup: the same as basic data

Full infant

Description: oracle model.
3) \( m \Rightarrow n \)

2) \( \mathbb{I} \oplus \mathbb{I} \rightarrow \mathbb{I} \) \( \begin{array}{l}
\forall x, y \in (\mathbb{R} \oplus \mathbb{I}), \text{return } x + y \\ \\
\forall x, y \in (\mathbb{R} \oplus \mathbb{I}), \text{return } x \cdot y \\ \\
\forall x \in \mathbb{I}, \text{return } 2^x \end{array} \)

echorp for: given \( C = (\mathbb{I} \oplus \mathbb{I}) \implies \)

\((\mathbb{I} \oplus \mathbb{I}) \oplus (\mathbb{I} \oplus \mathbb{I}) \rightarrow \)

\((\mathbb{I} \oplus \mathbb{I}) \oplus (\mathbb{I} \oplus \mathbb{I}) \rightarrow \)

\((\mathbb{I} \oplus \mathbb{I}) \oplus (\mathbb{I} \oplus \mathbb{I}) \rightarrow \)

\((\mathbb{I} \oplus \mathbb{I}) \oplus (\mathbb{I} \oplus \mathbb{I}) \rightarrow \)

\((\mathbb{I} \oplus \mathbb{I}) \oplus (\mathbb{I} \oplus \mathbb{I}) \rightarrow \)

\((\mathbb{I} \oplus \mathbb{I}) \oplus (\mathbb{I} \oplus \mathbb{I}) \rightarrow \)
we want Alice to generate a random w

F_{E_{\mathcal{P}e}S_{\mathcal{A}pub}, w}(msg) = F_{E_{\mathcal{P}e}S_{\mathcal{A}pub}, w'}(msg)

Alice:

Goal: Bob wants to send messages to

else output 0

if \parallel \not= R then reject

(\eta, R \leftarrow +_3(0, w))
A pub, an

Passage 5 and

Key len(5) = Toke 5 a security

Discussing anything else.

Message with word in without

a server can read all the

for any word in such that
Given Alice's PE searchable NC:

\[ S \leq \text{PELS}(A_{pub}, \mu) \]

\[ \text{Test} \leq \text{PELS}(A_{pub}, S, \mu) \]

(1) \[ \text{Fill} \rightarrow \text{Tapedoor}(A_{pub}, \mu) \]

(2) \[ S = \text{PELS}(A_{pub}, \mu) \]

Searchable non-PE function

4 Rapid production
1) Challenger runs the experiment

2) Attacker makes queries any \( w \) of

\[ w = \text{random (4 to 16)} \]
If \( \theta = 6 \), attach the wings of

\( S \) attachers preceding \( G \)

not related to \( T \) or \( T' \)

A attachers ask more quarters

changing 7 or send \( T' \) for random

9-16

such that \( T' \) or \( T' \) never

A attachers sends 3\( \omega_1 \)
A dU (5) is negligible

A if we have that

I t for any $P \in \mathcal{A}$ attackers

chosen keyround attack

secure against an defender

We say that $P$ is semantically

$$A dU (5) = | P \mathcal{L} \mathcal{B} = b^\frac{1}{2}$$
IR 10-10 version IBE

Key word attacks imply

Sec. against adaptive chosen

A non-interactive PEKS that is

F((c,s) \rightarrow \frac{1}{g(c,s)} for all polynomials)

and large enough.

function \text{not } A \rightarrow \text{polys}
For IRE

master key

set A as teh


to get A again. Again.

run the keygen for dyes

construct the system as follows:

Test

Green a red as keygen. Red, Test, Green
$$c \in \mathbb{Z}^4 \subseteq \mathbb{R}^4$$

Let $a_0 \in \mathbb{Z}$ as 

enough for $I_0 \times a$ get 

$$\left( \text{Trapped door ( April, x(11))} \right)$$

$$\alpha = \int \text{Trapped door ( April, x(11))}$$

with $0 \times \mathbb{Z}^{0.13}$

The $I(\mathbb{Z})$ private key association

3. Extract: 
else if

Output (A + Test (4.56, C, T, M, I, "Y")

Output C + Test (C, [A, b], C, T, O)

Use dx = (0, 0, 1)

G lobal C T

Set 0 = 1
It is believed that opposite direction IS secure.

The scheme is INQ-ID-CCA.
\((G \times G) \cong G \times G\)

1) The map is bijective.

2) The map is computable.

and a bilinear map: \(G \times G \to G\) (groups)

are my favorite.

In this paper, both \(G_1\) and \(G_2\) use two groups:

Construction:
Prop 2.2
\[ \psi(p) = \frac{q}{c} \Rightarrow A \Rightarrow \] Security

Let \( \text{gen} = \text{given} \), compute \( p \), \( q \), \( g \), \( g_2 \)

1. \( g_2 \Rightarrow g_2 \Rightarrow 2 \cdot 13 \Rightarrow p \) (p)
2. \[ g \Rightarrow h \Rightarrow 2 \cdot 13 \Rightarrow g \]
3. \( e \Rightarrow e \Rightarrow e \Rightarrow e \Rightarrow e \Rightarrow e 

If \( \text{then} \), \( \text{else} \), \( \text{a generator of} \)

3. None - degenerate: If \( g \) is a generator
If $H_2 \in (T, (\mu, A)) = 0$ then

Let $s = (\Lambda, \psi) \in Tese (\Lambda, (\mu, s, T))$.

Therefor $L (\Lambda, \psi, w) = (\Lambda, \psi, w) \in L_1 (\psi, w) \cap L_2 (\psi, w)$

Output $\Psi (\Lambda, \psi, w)$ for random $\rho$
\[ f(15, e(H, m)) = (f_2(\sigma(15), e(H, m)) \times _e 1, y) \]

\[ (\sigma(4), (e(H, m), y)) = \frac{H^2(e(H, m), g)}{e(H, m), y} \]

\[ (\sigma(4), e(H, m)) \]

\[ g = H^2(e(H, m), y) = H^2(e(H, m), y) \]

\[ g(a, b) = \]
is such that given ciphertext
Also we assume that the
the searchable keywords are limited,
any fraud dealer function assuming that
A construction that can use
Random oracle model
is secure under \text{BFT in the
It can be proven that a bare scheme
From any \((6, E, 0)\)

It is easy to construct searchable encryption

when the length of the family \(Z\) is poly-size

\(\text{Anonymous as source - indistinguishable}\)

\(\text{this physically text is associated with}\)

it is hard to say what \(E\)
Return \( \text{random } w \in \mathbb{R}^n \)
\[
\text{Test:\ } A \cap \{1, 5, 7\} = \emptyset
\]
\[
\text{There\ door:\ } A \cap \{b, w\} = \emptyset
\]
\[
\text{Else output}\ w
\]
And between 8 & 9, the user name is 1506 (the date is)

... of certain logs such as you may want to delegate the auditing security. Assume audit logs are outsourced to cloud.

Consider audit logs outsourced to cloud.

Encryption: Attribute-Based Encryption
Cloud

From Open, data is accessed.
An empty subset of \( P \) is a monotone collection. Let \( A \subseteq \mathbb{P} \) be a set of partitions. A collection \( A \subseteq \mathbb{P} \) is monotone if \( \forall a, b \in A \), \( a \subseteq b \Rightarrow b \subseteq a \). Definition (Access Structure)

An monotone access structure \( A \subseteq \mathbb{P} \) is monotone if \( \forall a, b \in A \), \( a \subseteq b \Rightarrow b \subseteq a \).
A class structure over attributes

In our context, we will define sets

not in A are called unattainable

unattainable sets and the sol

The sets in A are called the
Key Generation (A, AL, PK) $\rightarrow$ D

Attribute set of

Encrypt: (m, x, y, PK) $\rightarrow$ E (ciphertext)

Setup: A, PK, AL $\rightarrow$ A (key-policy

Consists of four algorithms

Attribute Based Encryption
If \( \vec{y} \in A \)

otherwise

Access Structure

Cipher text for message

Decryption (\( E^{-1} y, d \) \( \rightarrow \) \( m \))
where $A \leq \forall y A \mathcal{F} \forall x A \mathcal{F}$

many access structures $A \mathcal{F}$

Phase 1: Add issuing authorities for

to $A \mathcal{F}$

Set up: Can analyse and judge the $x$ parameters

we unleash to be challenging

Intuit: Adversary (add) decloaks $\mathcal{F}$

selective set model for $A \mathcal{F}$
The vulnerability of Anu is defined as

\[ 0 \leq b \leq \text{Guess} \]

Phase 2: Please I is repeated

L is given to Anu,

\( l ) \) is randomly chosen from 6

\[ \text{encry}(E_{\text{key}}(b)) \] with key

Challenge to Anu subjects to Anu challenge.
$$\text{Sitie }P$$

Cyclic groups of

where both $G_1, G_2$ are multiplicative.

A bilinear map defined over $G_1, G_2$

$A B E$ scheme discussed uses

For secure $ABE$, advantage at

$$|P(1) = b - \frac{1}{2}|$$
The ASZ scheme is also based on D-BDH assumption implying
for q, b, c, z ∈ \mathbb{G}_2 chosen randomly, 
the following two tuples are indistinguishable,
\[(g, \hat{g}, \hat{g}^z, c, \hat{g}^c, \hat{g}^{bc}, \hat{g}^{bzc})\]
\[(g, \hat{g}, \hat{g}^z, c, \hat{g}^c, \hat{g}^{bc}, \hat{g}^{bzc})\]
An access structure

Access Tree T is a tree representation

Access Construction for Access Tree

A8F

\[ A = \{ a, b \}, B = \{ c, d \}, G = \{ x, y \} \]

DH over A, B, C, D
In this paper, we are 1, 1, 1, and

\[ y = \begin{cases} \frac{1}{x} & \text{if } x \neq 0, x \neq \frac{1}{2} \sqrt{y} \leq \frac{1}{2} \sqrt{w_f} \times x_f \\
\end{cases} \]

are threshold gate.

Each non-leaf node \( X \) is a
If $x > 0$ then $x = \text{num}_x$ becomes a gap.

$x < 0$ then $x = \text{num}_x$ becomes a gap.

If $x = 0$ then $x = \text{num}_x$ becomes a gap.

$L_x$ is the threshold value where $L_x | x | > 0$.
of a node

index(x) returns the index

parent(x) is the parent of node x

associated with each node is an attribute

\( \text{attr}(x) \)

... and a threshold value of 1

is described by an algorithm

each leaf node x at the tree
\[ f \in \mathcal{T}(\mathcal{R}) \text{ return } 1 \text{ if } \forall x \in \mathcal{R} \left[ f(x) \leq 1 \right] \]

If \( x \) is a root node then return 1 else return 0.

\[ \exists \text{ parent} \left( x \right) \]

\[ \mathcal{L}(\mathcal{R}) = \left\{ x \in \mathcal{R} \mid \not\exists \text{ parent} \left( x \right) \right\} \]

We say \( R \) satisfies \( \mathcal{T} \) with root \( x \).
\[ l_1 (8) = \frac{7}{8} (8) + \frac{3}{8} (8) \]
\[ y = ax^2 + c \]

\[ y = ax^2 + c \]

\[ 1 = (8)^{\frac{1}{2}} \]

\[ 0 = (8)^{\frac{3}{2}} \]

\[ 1 = \frac{1}{2} \times \frac{1}{2} = \frac{1}{4} \]

\[ 2 \leq (8)^\frac{1}{2} + (8)^\frac{1}{2} = (8)^1 \]
\[ y \geq z \]

\[ \forall p \in E \]

\[ \prod \]

\[ \sum \]

\[ \Pi = 3 \]

Set up: defining the units of attribution.

\[ \text{coefficient} \]

\[ \frac{1 - 5}{5} \leq x \leq 5 \]

\[ 1 \leq T(x) = \frac{x}{5} \]

\[ \forall t \in \mathbb{R} \text{ and set } S \text{ define} \]
Choose $p \rightarrow 2^p$

Every $p \in \mathbb{P}$, $q, r \in \mathbb{P}$

$2p + q, r \in \mathbb{P}$

$\forall p \in \mathbb{P}$

It is $\tau \subset \mathbb{P}$

Plural forms are
\[ \mathbf{z} = \mathbf{v} \]
For any other node $x$, for complete tree $T$ connect $x$ to $\mathcal{L}$.

Define $c + \mathcal{L}$ at other points of $\mathcal{L}$, and let $\mathcal{H}(\mathcal{L}) = y$. And let each node be associated with node $x$.

Is the degree of polynomial $x$ set $\mathcal{L} = \pm 1$ where $x$ for each node $x$? in the tree.
I. will output \( \frac{x}{y} \) for \( T \)

(8, 5, 3; 0, 5, 8)

 девяти моделей (E, 0, T)

\[ x = a + \frac{1}{t} \] where \( t \approx a(t) \)

the secret value to use

give secret value to use
dead end for each leaf node

And choose dx points to define
\[
F_{it} = \text{Decay+Node}(\mathbb{E}, 0, t, i, f)
\]

For each child of node \(a\):

\[
x_i \in \text{non-root node}
\]

\[
\text{if } x \notin \mathbb{E} \text{ non-root node}
\]

\[
\text{return } T
\]

\[
\forall \bar{x} \in \mathbb{E}, x^t \in \text{Decay+Node}(\mathbb{E}, 0, t, i, f) \Rightarrow x = \hat{e}(\bar{x}, t, f)
\]

\[
\begin{cases}
\hat{e}(\bar{x}, t, f) = e(\hat{e}(\bar{x}, t, h), t, f) & \text{if } x \notin \text{ root where } f = \text{ aff}(x)
\end{cases}
\]
\[ x \in \{ 2, 5 \} \]

\[ \text{L} = 7 \]

\[ \forall x \in \mathbb{Z} \]

\[ 5^x = 1 \mod (2) \]

\[ \exists x \in \text{index}(z) \]

\[ x \in \mathbb{Z} \]

\[ \text{L} = 7 \]

\[ \text{else} \]

\[ \text{if no such } x \]

\[ \text{return } 1 \]

\[ \text{set } a \text{ of } 2 \]

\[ \text{let } S \text{ be an arbitrary } x \]
let $x \in \mathbb{F}_5$,

$\left( \mathbb{F}_9 \right)_{\mathbb{F}_5} \times \mathbb{F}_5 \cong \mathbb{F}_5 \times \mathbb{F}_5 \times \mathbb{F}_5 \cong \mathbb{F}_5 \times \mathbb{F}_5$
The size of \( O(n^2) \) many \( O(n) \) many \( O(1) \) many \( O(1) \) many

Efficiency of Encryption

- \( M \)
- \( \mathcal{E}(x) \)
- \( \mathcal{T}(\mathcal{E}(x)) \)

and compute \( \mathcal{E}(\mathcal{E}(x)) \) to get

\[
\mathcal{E}(\mathcal{E}(x)) = 1
\]

Call decrypt node \( \mathcal{E}(\mathcal{E}(x)) \) for \( \mathcal{E}_{1/2} \) operations.
or disclosed.

Possibly. As we discussed, attributes can

be universal for attributes are

uniquely explained. If only

"you can reduce it to"

model is 

"the worst case for basic
decryption"
corresponding to predicates and
by a secret key $\pi$

$\pi$ can be decrypted

and attribute $\pi$ on a clip

and

some class $\pi$ and

secret keys correspond to predicates

goal: to somehow more

PLEASE ENTER
known private key.

except what is rejected by

writes all into about

If it re-arrives that a cryptotext

Goal: Attieude matching

(C (E) ) = 1
else \[ x = \frac{5}{y} \quad \text{if} \quad \frac{y}{x} > \frac{2}{3} = c \]

\[ f(z) = 3 \]

\[ x \div z \leq 30.13 \]

Given a vector \( \mathbf{x} \in \mathbb{R}^n \),

Important applications of any procedure

For details, please see the paper.
IBF - Private Key (ID)

Get PIL, S1, S2

Don't setup - Predecessor (M)

IBF - Setup C[n]

Easy

Anonymously IBF could be generated
run GomoryCut(I, k)

\[ \text{set } \mathbf{I} = \mathbf{I} \setminus (0, 1) \]

where \( \mathbf{I} \) is \((1, 0)\)
\[ a = \langle (0,1), (1,0) \rangle \quad \Rightarrow \quad 1 = (1,0) \uparrow \downarrow \]

\[ w : \exists \text{ PE}_c \in \mathcal{C} \]

So, \( \text{run} \text{ PE}_c \in \mathcal{C} \)
Every predicate consists of a set of attributes. Over the set of attributes, every scheme for the predicates
In the security parameter \( n \), the adversary is

\[
\exp \left( -\sqrt{\frac{2}{\pi n}} \right)
\]

negligible (success).

For all PPT adversaries \( \mathcal{A} \), the following hold:

At least \( 2 \) attributes

\[ f \text{ and } z \text{ are } \mathcal{A} \text{-indistinguishable.} \]

\[ f \text{ and } z \text{ are } \mathcal{A} \text{-indistinguishable.} \]

A predicate over attributes \( f \):
1) $A^{(n)}$ outputs $I_0, I_1 \in \Sigma$

2) Challenger runs setup to get $PK, SK$. Adversary is given $PK$.

3) $A$ can get any key $s_{f_i}$ s.t. $\forall i \in \{1, \ldots, l\}$, $f_i(I_0) = f_i(I_1)$
success at 6/6

(1) A outputs a bit, b, and
the step 3 can be repeated

(2) A is Arjen Van (⇒ 6/6)

(3) If is required \( m \)

the \( \frac{1}{2} + \frac{1}{2} + \frac{1}{2} \) the
The advantage of $A$ should be negligible.
\[
\phi \left( x_1, \ldots, x_n \right) = \begin{cases} 0 & \text{otherwise} \\
\sum_{1 \leq i < j \leq n} \text{sgn}(x_i - x_j) & \text{if } x_1 = \ldots = x_n = 0 \end{cases}
\]

where

\[
\phi
\]

for the class of predicate schemes.

HUE is a predicate on \( C(\text{HUE}) \) the Hue vector.
Create vectors \( \mathbf{A} = (A_1, A_2, \ldots, A_n) \)

- For predicate \( \phi \) have
- Set up \( \mathcal{E} \) the same

\[ \mathcal{E} = \ldots \]

We can use the set product \( \times \) for

\[ \text{predicate and scheme to implement} \]
To encrypt a message for

Run Bevery key

\[ \text{get the private key} \]

\[ q_1^{n-1} \equiv 1 \pmod{2^k} \]
Choose random \( f \). Let 

\[ X_1 = \begin{bmatrix} \frac{1}{2} \\ \frac{1}{2} \end{bmatrix}, \quad X_2 = \begin{bmatrix} \frac{1}{2} \\ \frac{1}{2} \end{bmatrix} \]

Note that 

\[ L = \begin{bmatrix} 2 \end{bmatrix}, \quad X = \begin{bmatrix} \frac{1}{2} \\ \frac{1}{2} \end{bmatrix} \]

where 

\[ x_{2i-1}^2 = x_i x_{i+1}, \quad 1 \leq i \leq 7 \]

\[ x_1 = x_8 = 1, \quad a_i \sim N(0, 1) \]

\[ y_i = \frac{1}{2}, \quad i = 1, \ldots, 7 \]
What is \( A \times B = \emptyset \Rightarrow 0 \in A \times B \Rightarrow (1, 1) \)?

Let \( A \) and \( X \) be sets.

\( A \neq \emptyset \), \( X \neq \emptyset \)

\( A \times X = \{(a, x) \mid a \in A, x \in X\} \)

Assume \( x_1, x_2 \in X \) and \( x_1 \neq x_2 \)

\( A \times \{x_1, x_2\} \Rightarrow \exists a \in A \) such that \( (a, x_1) \in A \times \{x_1, x_2\} \) and \( (a, x_2) \in A \times \{x_1, x_2\} \).
If \( \langle x, x \rangle = 0 \) then \( \forall x \in X \), \( \exists y \in Y \) such that\( \langle x, y \rangle = 1 \). For all \( \eta \in \Omega \), we have

\[
\eta = (2\eta_2) \quad \text{for} \quad \eta_2 \in \mathbb{C} \times (1, x_2) = 0.
\]

Thus, \( \eta \) is real.

For \( \eta = 0 \), we have

\[
0 = (\mathbb{C} \times (1, x_2)) \quad \text{for} \quad x_2 \in \mathbb{C}.
\]

For \( \eta = 1 \), we have

\[
1 = \frac{\eta}{\mathbb{C}} = \mathbb{C} \times (1, 1) = 1.
\]

For \( \eta = 2 \), we have

\[
2 = \frac{\eta}{\mathbb{C}} = \mathbb{C} \times (1, 2) = 2.
\]

For \( \eta = 3 \), we have

\[
3 = \frac{\eta}{\mathbb{C}} = \mathbb{C} \times (1, 3) = 3.
\]

For \( \eta = 4 \), we have

\[
4 = \frac{\eta}{\mathbb{C}} = \mathbb{C} \times (1, 4) = 4.
\]
$a = (\phi(x' - x, \ldots, x' - y))_n + 1$