1 Introduction

This document is a summary of work so far on defining security notion for searchable encryptions and finding good/bad constructions with respect to the notions. In particular, we have considered using idea of g-leakage to measure security of a given scheme with respect to a target (gain) function and shown it is equivalent to an experiment-based adversary. We have studied three schemes we proposed, and shown that even though all of the schemes are secure against keyword guessing attack, they are not equally secure against other types of attacks. This demonstrates that security against keyword guessing attack is not sufficient for an encryptions scheme to be secure. For instance, one of the scheme we proposed is secure against inference attack but it leaks all keywords in all documents information-theoretically.

2 Notation

Notation	**Explanation**
DB	Database that has not been encrypted
EDB	Encrypted database
d	A document in the database
f	A file associated to some document
K	A set of keywords associated to some file
k	A keyword in a keyword set
ed	An encrypted document
ef	An encrypted file
EK	A set of encrypted keywords
ek	An encrypted keyword

Structure of the database We write $DB = (d_1, d_2, \ldots, d_{n_0})$ where n_0 is the number of documents in the database. Each document d can be written as $d = (K, f)$ where f is some file and K is the set of keywords associated to f. Finally, K is a list of keywords so $K = \{k_1, \ldots, k_l\}$ for some l.

Structure of the encrypted database Similarly, on encrypted database, we have $EDB = (ed_1, ed_2, \ldots, ed_{n_1})$ where n_1 is the number of encrypted documents in the database. Each encrypted document ed can be written as $ed = (EK, ef)$ where ef is some encrypted file and EK is the set of encrypted keywords associated to ef. Finally, K is a list of encrypted keywords so $EK = \{ek_1, \ldots, ek_l\}$ for some l.

We omit definition of syntax of searchable encryption in this document.

3 g-leakage

G-leakage is first studied by Alvim et al. in [1]. To understand how it works, we first define (classic) vulnerability, leakage and capacity.

Definition 1 (Information Channel)**.** *A channel is a triple $(\mathcal{X}, \mathcal{Y}, \mathcal{C})$, where $\mathcal{X}$ and $\mathcal{Y}$ are finite sets and $\mathcal{C}$ is a channel matrix, an $|\mathcal{X}| \times |\mathcal{Y}|$ matrix whose entries are between 0 and 1 and whose rows each sum to 1.*

Definition 2 (Vulnerabilities)**.** *Given prior distribution π on $\mathcal{X}$ and channel C, the prior vulnerability is given by:*

$$V(\pi) = \max_{x \in \mathcal{X}} \pi[x], \tag{1}$$

and the posterior vulnerability is given by:

$$V(\pi, \mathcal{C}) = \sum_{y \in \mathcal{Y}} \max_{x in \mathcal{X}} \pi[x]\mathcal{C}[x, y]. \tag{2}$$

Definition 3 (Leakage and Capacity)**.** *We define min-entropy leakage $\mathcal{L}(\pi, \mathcal{C})$ and min-capacity $\mathcal{ML}(\mathcal{C})$ to be:*

$$\mathcal{L}(\pi, \mathcal{C}) = -\log V(\pi) + \log V(\pi, \mathcal{C}) = \log \frac{V(\pi, \mathcal{C})}{V(\pi)} \tag{3}$$

$$\mathcal{ML}(\mathcal{C}) = \sup_{\pi} \mathcal{L}(\pi, \mathcal{C}). \tag{4}$$

G-leakage is different from the classic definition by allowing the adversary to guess part of x from observation y, and his gain is measured by a gain function g. We define g-leakage with the following definitions.

Definition 4 (Gain function)**.** *Given a set $\mathcal{X}$ of possible secrets and a finite, non-empty set $\mathcal{W}$ of allowable guesses, a gain function is a function $g : \mathcal{W} \times \mathcal{X} \to [0, 1]$.*

There is no restriction on how the gain function behaves from this definition. In particular, it is possible to set the gain to be 0 even if the adversary makes a perfect guess from what he has observed. Therefore, in our work, we need to define a class of well-behaved gain functions in order to talk about semantic meaning of the leakage. (**Note: not done yet.**)

Definition 5 (Prior g-vulnerability)**.** *Given gain function g and prior π, the prior g-vulnerability is*

$$V_g(\pi) = \max_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} \pi[x] g(w, x). \tag{5}$$

Definition 6 (Posterior g-vulnerability)**.** *Given gain function g, prior π, and channel C, the posterior g-vulnerability is*

$$V_g(\pi, C) = \sum_{y \in \mathcal{Y}} \max_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} \pi[x] C[x, y] g(w, x). \tag{6}$$

Definition 7 (g-leakage and g-capacity)**.** *G-leakage $\mathcal{L}_g(\pi, \mathcal{C})$ and g-capacity $\mathcal{ML}_g(\mathcal{C})$ are defined as:*

$$\mathcal{L}_g(\pi, \mathcal{C}) = -\log V_g(\pi) + \log V_g(\pi, \mathcal{C}) = \log \frac{V_g(\pi, \mathcal{C})}{V_g(\pi)}$$

$$\mathcal{ML}_g(\mathcal{C}) = \sup_{\pi} \mathcal{L}_g(\pi, \mathcal{C}).$$

For application to searchable databases, $\mathcal{X}$ in the definition is the database and other secrets the adversary tries to guess, and $\mathcal{Y}$ is the encrypted database he observes. The adversary may not only be interested in recover some information about the unencrypted database but also some relation between the unencrypted database and its encryption. For instance, the adversary may want to know what is the encryption of each keyword, i.e. keyword guessing attack. Hence, we extend the gain function as:

Definition 8 (Extended gain function)**.** *Given a set $\mathcal{X}$ of possible secrets, a set $\mathcal{Y}$ derived from $\mathcal{X}$ and a finite, non-empty set $\mathcal{W}$ of allowable guesses, a gain function is a function $g : \mathcal{W} \times \mathcal{X} \times \mathcal{Y} \to [0, 1]$.*

In our application, the prior vulnerability has no operational meaning so we decide to look at posterior vulnerability only. The posterior vulnerability with the new gain function is defined as follows.

Definition 9 (Extended posterior g-vulnerability)**.** *Given gain function g, prior π, and channel C, the extended posterior g-vulnerability is*

$$EV_g(\pi, C) = \sum_{y \in \mathcal{Y}} \max_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} \pi[x] C[x, y] g(w, x, y). \tag{7}$$

4 Security Notions

In this section, we consider several experiment-based adversary on searchable encryption. We motivate with an experiment that is very similar to an IND-CPA experiment (for brevity, we do not give definition of standard IND-CPA here) specifically for keyword guessing attack. In the experiment, the adversary receives the encryption of the database he chooses, and his goal is to match keywords to their encryptions. To move a step further, we modify this experiment by only giving the adversary leakage of the encryption scheme associated to the database in the experiment. We then generalise the experiments to allow for arbitrary target functions of the adversary.

4.1 Security Notion for Keyword Guessing Attack

There is a multitude of ways to evaluate how well the adversary has recovered information through keyword guessing attack. We will present with one of the simplest here. Namely, the adversary wins if he recovers a correct pair of keyword and its encryption (with one guess).

For simplicity, we only consider snapshot attack here, so it suffices to assume that the searchable encryption scheme has some key generation function $\mathsf{KGen}(\cdot)$, some encryption function $\mathsf{Enc}(\cdot)$ that encrypts the database, and there is a decryption function $\mathsf{Dec}(\cdot)$ that decrypts encrypted documents one at a time. Because we are interested in security of the search index, we abuse $\mathsf{Dec}(\cdot)$ to be the function that decrypts an encrypted document or a set of encrypted keywords associated to an encrypted document, and outputs the set of real keywords.

Definition 10 (Security against Keyword Guessing Attack)**.** *We define an keyword guessing attack adversary to be $\mathcal{A} = (\mathcal{A}_0, \mathcal{A}_1)$, where $\mathcal{A}_0$ is a probabilistic polynomial time (PPT) adversary which takes in the security parameter and generates a database DB, and $\mathcal{A}_1$ is a PPT adversary which takes in the security parameter, generated database DB and encrypted database EDB, and returns a pair of keyword and encrypted keyword. The experiment can be described as follows:*

$\underline{Exp_{\mathcal{A}}^{Keyword\text{-}Guessing}(n)}$

$\mathsf{k} \leftarrow_{\$} \mathsf{KGen}(1^n)$

$DB \leftarrow \mathcal{A}_0(1^n)$

$EDB \leftarrow \mathsf{Enc}(1^n, \mathsf{k}, DB)$

$(m, c) \leftarrow \mathcal{A}_1(1^n, DB, EDB)$

if $(\mathsf{Dec}(c) = m)$**return** $1 - f(m, DB)$

else return $-f(m, DB)$

where $f(m, DB)$ is a function that returns the frequency of keyword m in database DB.

Advantage $Adv_{\mathcal{A}}^{Keyword\text{-}Guessing}(n)$ of an inference attack adversary $\mathcal{A}$ is defined to be

$$Adv_{\mathcal{A}}^{Keyword\text{-}Guessing}(n) = \mathbb{E}\left[Exp_{\mathcal{A}}^{Keyword\text{-}Guessing}(n)\right]. \tag{8}$$

We say that a scheme is secure against keyword guessing attack if $Adv_{\mathcal{A}}^{Keyword\text{-}Guessing}(n)$ is less than some negligible function in n.

Intuitively, a scheme is secure against keyword guessing attack if there is no way he can guess any plaintext-ciphertext pair with probability greater than the frequency of the plaintexts. There are other possible definitions, for instance, one can look at the probability the adversary guessing all pairs of plaintexts and ciphertexts correctly.

This security notion is hard to work with because the database the adversary can generate is literally anything and the encryption scheme can generate any ciphertext. But in our game, we really do not care if keywords are '1' and '2' or 'one' and 'two', nor do we care how the ciphertexts look like. To simplify the problem, we want to work with idealised databases and encryption schemes which allows us to ignore information that are not relevant to our security game. Due to necessity of efficient searchability, encryption schemes for searchable encryption cannot achieve IND-CPA security, and the 'insecure part' of encryption function (and query functions) are understood in terms of leakage functions. Informally speaking, leakage function associated to a scheme captures what is leaked about the unencrypted database by looking at its encryption. For example, number of documents is part of leakage for any scheme that does not pad fake documents because after enough queries, all documents will be returned at least once (unless part of the database is never going to be returned by any query, but that defeats the purpose of putting them there in the first place).

In the next experiment, the adversary is only given the leakage associated to the mechanism applied to the generated database. We argue that by choosing the leakage carefully, the advantage for the experiment will be the same as the previous one, up to an additive negligible term. We begin by defining leakage of searchable encryption.

Definition 11 (Leakage of Searchable Encryption)**.** *Let* Enc *be the encryption algorithm for some searchable encryption scheme. We say* $\mathcal{L}_{\mathcal{M}}$ *is a valid leakage function for the mechanism if there exists an adversary* $\mathcal{A}$ *and a simulator* $\mathcal{S}$ *such that for any PPT distinguishers* $\mathcal{D}$*, the following two games are indistinguishable.*

$\underline{Real_{\mathcal{A}}(n)}$

1 : $\mathsf{k} \leftarrow\!\!\$\ \mathsf{KGen}(1^n)$
2 : $DB \leftarrow \mathcal{A}(1^n)$
3 : $EDB \leftarrow \mathsf{Enc}(1^n, \mathsf{k}, DB)$
4 : **return** EDB

$\underline{Sim_{\mathcal{A},\mathcal{S}}(n)}$

1 : $\mathsf{k} \leftarrow\!\!\$\ \mathsf{KGen}(1^n)$
2 : $DB \leftarrow \mathcal{A}(1^n)$
3 : $\mathcal{L} \leftarrow \mathcal{L}_{\mathcal{M}}(1^n, \mathsf{k}, DB)$
4 : $EDB \leftarrow \mathcal{S}(1^n, \mathcal{L})$
5 : **return** EDB

This definition quantifies a class of valid leakages. But clearly not all of them are useful. For instance, the identity function is always a valid leakage in this definition. What we are interested in is really the minimal leakage which makes these two games indistinguishable. (**TO DO: 1. Define minimal leakage properly. 2.Discuss the implication when the leakage used in the experiment is not minimal.**)

Definition 12 (Minimal Leakage)**.**

Now we are ready to define security against idealised keyword guessing attack.

Definition 13 (Security against Idealised Keyword Guessing Attack)**.** *We define an idealised keyword guessing attack adversary to be* $\mathcal{A} = (\mathcal{A}_0, \mathcal{A}_1)$*, where* $\mathcal{A}_0$ *is a PPT adversary which takes in the security parameter and generates a database* DB*, and* $\mathcal{A}_1$ *is any adversary (not necessarily polynomial time bounded) which takes in the security parameter, generated database* DB *and leakage* $\mathcal{L}$ *generated by the minimal leakage function* $\mathcal{L}_{\mathcal{M}}$*, and returns a pair of keyword and encrypted keyword. The experiment can be described as follows:*

$\underline{Exp_{\mathcal{A}}^{Keyword\text{-}Guessing\text{-}Ideal}(n)}$

1 : $\mathsf{k} \leftarrow\!\!\$\ \mathsf{KGen}(1^n)$
2 : $DB \leftarrow \mathcal{A}_0(1^n)$
3 : $\mathcal{L} \leftarrow \mathcal{L}_{\mathcal{M}}(1^n, \mathsf{k}, DB)$
4 : $(m, c) \leftarrow \mathcal{A}_1(1^n, DB, \mathcal{L})$
5 : **if** $(\mathsf{Dec}(c) = m)$ **return** $1 - f(m, DB)$
6 : **else return** $-f(m, DB)$

where $f(m, DB)$ is a function that returns the frequency of keyword m in database DB.

Advantage $Adv_{\mathcal{A}}^{Keyword\text{-}Guessing\text{-}Ideal}(n)$ of an idealised inference attack adversary $\mathcal{A}$ is defined to be

$$Adv_{\mathcal{A}}^{Keyword\text{-}Guessing\text{-}Ideal}(n) = \mathbb{E}\left[Exp_{\mathcal{A}}^{Keyword\text{-}Guessing\text{-}Ideal}(n)\right]. \tag{9}$$

We say that a scheme is secure against idealised keyword guessing attack if $Adv_{\mathcal{A}}^{Keyword\text{-}Guessing\text{-}Ideal}(n)$ is less than some negligible function in n.

Notice that in the definition, $\mathcal{A}_1$ does not need to be PT bounded. This is because we are in the idealised world where the cryptographic part has already been dealt with in the leakage. Also, the decryption function $\mathsf{Dec}(\cdot)$ we have in the experiment is idealised. For example, if an IND-DCPA secure deterministic encryption is used to encrypt keywords, then the idealised encryption function and decryption function are just bijections. This is different from original encryption and decryption functions because they are not keyed so it the adversary cannot use brute force to recover the key and break security of the scheme.

It is clear that if $\mathcal{L}_{\mathcal{M}}$ is a well-defined minimal leakage, then all PPT distinguisher $\mathcal{D}$ can only distinguish the real experiment and the idealised experiment with probability no greater than a negligible function in n.

4.2 Moving from Fixed Target Function to Generic Gain Function

In the two games for keyword guessing attack we defined above, the content returned by the games are fixed so proving security with respect to the games only says the scheme is secure against this specific adversary who tries to recover this specific information. This is very inflexible as a security notion for application in searchable encryption. In addition, wrong guesses in these games are completely punished in this setting in the sense that they will never show up in the advantage term, even though wrong guesses can still reveal some information. Consider the case where the adversary always tries to guess decryption of some ciphertext c and he always fails because his guess is some m such that $\mathsf{Dec}(c) \neq m$. But ultimately, the goal of the adversary can be to recover some keywords in some documents. If m always appears together with $\mathsf{Dec}(c)$ in all documents, then in fact, the adversary recovers a significant amount of information about the underlying database, even though the guess itself is wrong. So we need to reward those guesses that are not completely correct but still reveals information about the database appropriately.

To do so, we use idea of gain function from g-leakage paper [1]. To put it in simple words, instead returning something from the experiment and analyse it in the advantage term, we compute the gain at the end of the experiment, and the advantage is defined to be the expectation of the result of the experiment for the best adversary. We now define the games with gain functions.

Definition 14 (Real Game with Gain Function)**.** *We define a real adversary with gain function g to be $\mathcal{A} = (\mathcal{A}_0, \mathcal{A}_1)$, where $\mathcal{A}$, is a PPT adversary which takes in the security parameter and generates a database DB, and $\mathcal{A}_1$ is a PPT adversary which takes in the security parameter, generated database DB and encrypted database EDB, and returns some guess w in the set of allowed guesses $\mathcal{W}$. The experiment can be described as follows:*

$\underline{Real_{\mathcal{A}}^{g}(n)}$

1 : $\mathsf{k} \leftarrow\!\!\$\, \mathsf{KGen}(1^n)$
2 : $DB \leftarrow \mathcal{A}_0(1^n)$
3 : $EDB \leftarrow \mathsf{Enc}(1^n, \mathsf{k}, DB)$
4 : $w \leftarrow \mathcal{A}_1(1^n, DB, EDB)$
5 : **return** $g(w, (DB, \mathsf{k}), EDB)$

Advantage $Adv^{Real}_{\mathcal{A},g}(n)$ *is defined to be:*

$$Adv^{Real}_{\mathcal{A},g}(n) = \mathbb{E}[Real^{g}_{\mathcal{A}}(n)]\,. \tag{10}$$

Definition 15 (Ideal Game with Gain Function)**.** *We define an ideal adversary with gain function* g *to be* $\mathcal{A} = (\mathcal{A}_0, \mathcal{A}_1)$*, where* $\mathcal{A}$*, is a PPT adversary which takes in the security parameter and generates a database* DB*, and* $\mathcal{A}_1$ *is a PPT adversary which takes in the security parameter, generated database* DB *and minimal leakage* $\mathcal{L}$*, and returns some guess* w *in the set of allowed guesses* $\mathcal{W}$*. The experiment can be described as follows:*

$\underline{Ideal^{\mathcal{L},g}_{\mathcal{A}}(n)}$

1 : $\mathsf{k} \leftarrow\!\!\$\ \mathsf{KGen}(1^n)$
2 : $DB \leftarrow \mathcal{A}_0(1^n)$
3 : $\mathcal{L} \leftarrow \mathcal{L}_{\mathcal{M}}(1^n, \mathsf{k}, DB)$
4 : $w \leftarrow \mathcal{A}_1(1^n, DB, \mathcal{L})$
5 : **return** $g(w, (DB, \mathsf{k}), \mathcal{L})$

Advantage $Adv^{Ideal}_{\mathcal{A},\mathcal{L},g}(n)$ *is defined to be:*

$$Adv^{Ideal}_{\mathcal{A},\mathcal{L},g}(n) = \mathbb{E}\left[Ideal^{\mathcal{L},g}_{\mathcal{A}}(n)\right]. \tag{11}$$

Note that we are not putting any condition to quantify when a scheme is secure under these notions, because the advantage really depends on the choice of g. But with well-defined g, the advantage will have an operational meaning and we can understand the level of security offered by our scheme from there.

4.3 Games with Gain Function are equivalent to some Extended Posterior g-vulnerability

In this subsection, we prove that in fact, we can look at the advantage from the games or some corresponding extended posterior g-vulnerability exchangeably. To do so, we need a slight tweak to the games above.

Let π be the prior on the joint distribution of databases and keys. Then the games above is equivalent to the following.

$\underline{\text{Real}^{\pi,g}_{\mathcal{A}}(n)}$

1 : $(DB, \mathsf{k}) \leftarrow\!\!\$\ \pi$
2 : $EDB \leftarrow \mathsf{Enc}(1^n, \mathsf{k}, DB)$
3 : $w \leftarrow \mathcal{A}_1(1^n, DB, EDB)$
4 : **return** $g(w, (DB, \mathsf{k}), EDB)$

$\underline{\text{Ideal}^{\pi,\mathcal{L},g}_{\mathcal{A}}(n)}$

1 : $(DB, \mathsf{k}) \leftarrow\!\!\$\ \pi$
2 : $\mathcal{L} \leftarrow \mathcal{L}_{\mathcal{M}}(1^n, \mathsf{k}, DB)$
3 : $w \leftarrow \mathcal{A}_1(1^n, DB, \mathcal{L})$
4 : **return** $g(w, (DB, \mathsf{k}), \mathcal{L})$

Theorem 16 (Real game is equivalent to an extended posterior g-vulnerability)**.** *Let* π *of the extended posterior g-vulnerability be that in the real experiment. Let* $\mathcal{X} = \{(DB, k)\}$*. Let* $\mathcal{Y} = \{\mathsf{Enc}(1^n, \mathsf{k}, DB)\}$*. Let* $\mathcal{C}_{\mathcal{L}}$ *be the channel matrix from* $\mathcal{X}$ *to* $\mathcal{Y}$*. Then*

$$\sup_{\pi \in Dist} \sup_{\mathcal{A}} Adv^{Real}_{\mathcal{A},\pi,g}(n) = EV_g(\pi, \mathcal{C}_{\mathcal{L}}). \tag{12}$$

where Dist is the set of valid prior for the database.

Theorem 17 (Ideal game is equivalent to an extended posterior g-vulnerability)**.** *Let* π *of the extended posterior g-vulnerability be that in the real experiment. Let* $\mathcal{X} = \{(DB, k)\}$*. Let* $\mathcal{Y} = \{\mathcal{L}_{\mathcal{M}}(1^n, \mathsf{k}, DB)\}$*. Let* $\mathcal{C}_{\mathcal{L}}$ *be the channel matrix from* $\mathcal{X}$ *to* $\mathcal{Y}$*. Then*

$$\sup_{\pi \in Dist} \inf_{\mathcal{L} \in Valid} \sup_{\mathcal{A}} Adv^{Real}_{\mathcal{A},\pi,\mathcal{L},g}(n) = EV_g(\pi, \mathcal{C}_{\mathcal{L}}). \tag{13}$$

where Dist is the set of valid prior for the database.

Note: Need to explain the leakage in the theorem after we define minimal leakage properly.

We prove the second theorem, and by taking the leakage function as the encryption function, and change g appropriately, we obtain the first theorem.

Proof. For simplicity, we assume *Dist* is a point distribution. Furthermore, $\inf_{\mathcal{L}\in\text{Valid}}$ is a technical condition to ensure the leakage we consider is really some minimal leakage, so it suffices to look at the expression $\sup_{\mathcal{A}} \text{Adv}^{\text{Real}}_{\mathcal{A},\pi,\mathcal{L},g}(n)$ with $\mathcal{L}$ being a valid minimal leakage. Suppose $\mathcal{L}$ is indeed a valid minimal leakage, then

$$\sup_{\mathcal{A}} \text{Adv}^{\text{Real}}_{\mathcal{A},\pi,\mathcal{L},g}(n) \tag{14}$$

$$= \sup_{\mathcal{A}} \mathbb{E}\left[\text{Ideal}_{\mathcal{A}}^{\mathcal{L},g}(n)\right] \tag{15}$$

$$= \mathbb{E}_{\mathcal{L}}\left[\max_{w\in\mathcal{W}} \mathbb{E}_{\pi}\left[g(w,(DB,\mathsf{k}),\mathcal{L}) \mid \mathcal{L}\right]\right] \tag{16}$$

$$= \mathbb{E}_{\mathcal{Y}}\left[\max_{w\in\mathcal{W}} \mathbb{E}_{\pi}\left[g(w,\mathcal{X},\mathcal{Y}) \mid \mathcal{Y}\right]\right] \tag{17}$$

$$= \sum_{y\in\mathcal{Y}} \Pr[\mathcal{Y}=y] \max_{w\in\mathcal{W}} \sum_{x\in\mathcal{X}} \Pr[\mathcal{X}=x \mid \mathcal{Y}=y]\, g(w,x,y) \tag{18}$$

$$= \sum_{y\in\mathcal{Y}} \max_{w\in\mathcal{W}} \sum_{x\in\mathcal{X}} \Pr[\mathcal{X}=x, \mathcal{Y}=y]\, g(w,x,y) \tag{19}$$

$$= \sum_{y\in\mathcal{Y}} \max_{w\in\mathcal{W}} \sum_{x\in\mathcal{X}} \pi[x]\mathcal{C}_{\mathcal{L}}[x,y] g(w,x,y) \tag{20}$$

$$= EV_g(\pi, \mathcal{C}_{\mathcal{L}}). \tag{21}$$

In the proof, equation 15 is just writing out the adversary explicitly. Equation 16 uses the fact that for any given leakage, there is a deterministic guess that maximises the conditional expectation and the best adversary overall does this for any leakage $\mathcal{L}$ he sees. The next few lines of the proof are just re-writing the expectation into algebraic form and re-arranging the terms. □

In the next section, we will present a few constructions of searchable encryptions. In the section after, we will show how to use the extended posterior g-vulnerability and the idealised game with gain function to analyse security of the schemes.

5 Constructions

In this section, we motivate and give several constructions of searchable encryption.

5.1 Additional Notations

Let $K(\cdot)$ denotes a function that takes in a file or document and returns the set of keywords associated to it. If it takes the whole database as input, it returns the set of keywords in all documents. Similarly, we let $f(d)$ to be a function that returns the file associated to a document d. We write $P_a^{K(DB)}$ to mean a permutation

on $K(DB)$. The permutation is a product of $\frac{|K(DB)|}{a}$ disjoint cycles of length a. When the keyword set is well-understood, we omit it from the notation. Let K be a set of keywords, we abuse the notation $P_a(K)$ to mean $P_a(K) = \{P_a^n(w) \mid w \in K\}$.

5.2 Motivation

From previous works, we know that the leakage of most searchable encryptions is repetition of keywords in files, meaning that if the same keyword appears in two different documents, the adversary is aware of that. There are constructions that hides this information from the adversary in the passive case but this is nonetheless leaked through queries. There are many known attacks that abuse this information to perform inference attack. Our goal is to construct a scheme that is secure against any inference attack.

To motivate, we start by describing the attacks. The basic attack is the well-known frequency analysis. Upon obtaining the information on the database, the adversary computes the frequency of each encrypted keyword. The information is then compared to his prior knowledge on the distribution. The encrypted keywords are matched to their most likely unencrypted counterparts. Naveed et al. [4] have shown that this attack is very efficient and accurate on attribute-based encrypted tables, and their attack can be extended to other forms of encrypted databases easily.

The more advanced attacks aim to improve accuracy of keyword recovery by making use of co-occurrences of keywords. In this case, instead of looking at frequency of keywords one by one, the adversary looks at pairs of keywords and find frequencies on them. The frequencies computed is usually put into a matrix, known as the co-occurrence matrix and some optimization algorithm is performed to find a permutation between keywords and their encryptions which fits the objective function the best. It has been shown that attacks of this form can recover a substantial amount of plaintext-ciphertext pairs even if frequency analysis fails so.

Attack of this genre does not stop here. We imagine there are adversaries who make use of higher order information such as frequency of every three keywords occur together and more. So ultimately, a necessary condition for a scheme to be secure is that it is secure against inference attack that abuses co-occurrence matrices at all levels.

All of our constructions rely on a permutation P_a. The idea is that we transform the original database into a form such that after permuting the keywords with P_a, the view of the encrypted database should stay the same. Thus, the adversary cannot distinguish if the original keywords are those without the permutation or the ones with it. Of course, since P_a is a permutation, we can apply P_a again and the view of the encrypted database is still unchanged. In fact, there are (at least) a different orientations of the transformed database such that the encrypted views are the same.

5.3 Co-occurrence Matrices and Permutability

In this subsection, we give definition of co-occurrence matrices and permutable co-occurrence matrices, and show how these can help us achieve security.

Definition 18 (Co-occurrence at level l with Documents)**.** *Co-occurrence at level l on database DB with documents is defined to be $DC_l^{DB} : K(DB)^l \to d^*$.*

$$DC_l^{DB}(k_1, \ldots, k_l) := \{d \mid (k_i \neq k_j \forall i, j) \wedge (d \in DB) \wedge (\{k_1, \ldots, k_l\} = K(d))\}. \tag{22}$$

Sometimes, only the counts in the co-occurrence matrix is of interest to us. So we define the corresponding co-occurrence matrix to be:

Definition 19 (Co-occurrence at level l with Counts)**.** *Co-occurrence at level l on database DB with counts is defined to be $CC_l^{DB} : K(DB)^l \to \mathbb{N}$.*

$$CC_l^{DB}(k_1, \ldots, k_l) := \left| DC_l^{DB}(k_1, \ldots, k_l) \right|. \tag{23}$$

When the database DB is well-understood, we omit it from the notation. With this definition, we can talk about co-occurrence of arbitrary number of keywords. For example, counts of keywords corresponds to CC_1, and co-occurrence is CC_2. Similar definition can be made with the encrypted database, we give them briefly here.

Definition 20 (Co-occurrence at level d with Encrypted Documents)**.** *Co-occurrence at level l on encrypted database EDB with encrypted documents is defined to be $EDC_l^{EDB} : EK(EDB)^l \to ed^*$.*

$$EDC_l^{EDB}(ek_1, \ldots, ek_l) := \{ed \mid (ek_i \neq ek_j \forall i, j) \wedge (ed \in EDB) \wedge (\{ek_1, \ldots, ek_l\} = \mathsf{Dec}(ed))\}. \tag{24}$$

Definition 21 (Co-occurrence at level l with Encrypted Counts)**.** *Co-occurrence at level d on database DB with encrypted counts is defined to be $ECC_l^{EDB} : EK(EDB)^l \to \mathbb{N}$.*

$$ECC_l^{EDB}(ek_1, \ldots, ek_l) := \left| EDC_l^{EDB}(ek_1, \ldots, ek_l) \right|. \tag{25}$$

Finally, we can define the collection of co-occurrences at all levels with the following definition.

Definition 22 (Co-occurrences at all levels)**.** *Co-occurrences at all levels with documents is $DC^{DB} = \left\{DC_1^{DB}, \ldots, DC_{K(DB)}^{DB}\right\}$. Co-occurrences at all levels with counts is $CC^{DB} = \left\{CC_1^{DB}, \ldots, CC_{K(DB)}^{DB}\right\}$.*

Co-occurrences at all levels with encrypted documents is $EDC^{EDB} = \left\{EDC_1^{EDB}, \ldots, EDC_{K(EDB)}^{EDB}\right\}$. Co-occurrences at all levels with encrypted counts is $ECC^{EDB} = \left\{ECC_1^{EDB}, \ldots, ECC_{EK(EDB)}^{EDB}\right\}$.

All of our constructions rely on transforming co-occurrences into a way such that the adversary can no longer recover the information he wants. The property we achieve with our transformation is what we called permutability.

Definition 23 (Permutability)**.** *Given co-occurrence C of any form above, and a permutation P on a co-ordinate of the input, we say C is P-permutable if*

$$C_l(w_1, \ldots, w_l) = C_l(P(w_1), \ldots, P(w_l)) \tag{26}$$

for all $w_1, \ldots, w_l$.

We say that co-occurrence at all levels are permutable by P if all co-occurrences are permutable by P.

In dimensions 1 and 2, this is easier to understand in terms of vectors and matrices. The following is an example of $(w_1\ w_2\ w_3)$-permutable co-occurrence count in matrix form:

$$\begin{bmatrix} 0 & 5 & 5 \\ 5 & 0 & 5 \\ 5 & 5 & 0 \end{bmatrix} \tag{27}$$

Note that co-occurrences are always symmetric due to the definition. Now imagine these are the only documents in our database. If we use a secure deterministic encryption scheme to encrypt these keywords, the adversary is going to see a permuted version of this co-occurrence. But he is not able to tell which ciphertext corresponds to which keyword because all pairs of keywords have the same count. Our encryption schemes essentially takes co-occurrences (at all levels) in any shape, and transform them into these permutable matrices. With a clever choice of permutation P, we can achieve desired security with respect to some gain functions. In the next subsection, we will show how to transform arbitrary co-occurrence into a permutable one.

5.4 Our Constructions

In this section, we describe our constructions. All of the constructions are secure against keyword guessing attack (it is going to be a security notion slightly different from the one defined above, see later) but they achieve different level of security against other attacks.

5.5 Permutation with Adding Fake Documents

One straightforward way to achieve the permutation property is to pad fake documents. Let $(\overline{\mathsf{KGen}}, \overline{\mathsf{Enc}}, \overline{\mathsf{Dec}})$ be a secure encryption scheme on searchable encryption (i.e. with leakage being repetition of keywords). Let $\mathsf{KGen}'(a, K(DB))$ be a key generation scheme that takes in a positive integer a which divides $|K(DB)|$ and set of keywords in DB, and returns a permutation on $K(DB)$ that is a product of disjoint cycles of length a. Let $\texttt{FGen}(1^n, K)$ be a function that generates a random fake file with the given set of keywords K. We can define scheme 1 to be $\texttt{scheme1} = (\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ in the following way.

$\mathsf{KGen}(n, a, K(DB))$

$\mathsf{k} \leftarrow \overline{\mathsf{KGen}}(1^n)$

$P_a \leftarrow \mathsf{KGen}'(a, K(DB))$

return (k, P_a)

$\mathsf{Enc}(1^n, (\mathsf{k}, P_a), DB)$

$DB' = ()$

for $d \in DB$:

  $DB' = DB' + (K(d), (True, f(d)))$

  for $i = 1, \ldots, a-1$:

    $DB' = DB' + ((P_a)^i(K(d)), (False, \texttt{FGen}(1^n, (P_a)^i(K(d)))))$

return $\overline{\mathsf{Enc}}(1^n, \mathsf{k}, DB')$

$\mathsf{Dec}(1^n, (\mathsf{k}, P_a), EDB)$

$DB = ()$

for $ed \in EDB$:

  $(K, (b, f)) \leftarrow \overline{\mathsf{Dec}}(1^n, (\mathsf{k}, P_a), ed)$

  if $b = True$:

    $DB = DB + ((K, f))$

return DB

Insertion and deletion are straightforward and other functions, namely trapdoor generation and search, are taken from the aforementioned encryption scheme directly so we will omit them here.

5.6 Scheme in IKK paper

In the paper written by Islam et al. [3], the authors introduced an encryption scheme that is secure against inference attack. Their security notion is different from the one we described in section 4. We recall their definition and results here.

Definition 24 ((α, t)-secure index)**.** *We say an $m \times n$ binary index matrix ID is (α, t)-secure for a given $\alpha \in [1, m]$ and $t \in \mathcal{N}$ if there exists a set of partitions $\{S_i\}$ s.t. the following holds.*

1. *The partition set is complete. That is $\cup_i S_i = [1, m]$.*
2. *The partitions in the set are non-overlapping. That is, $\forall i, j, S_i \cap S_j = \emptyset$.*
3. *Each partition has at least α rows. That is, $\forall j, |S_j| \geq \alpha$.*

4. *Finally, the hamming distance between any two rows of a given partition j is at most t. That is, $\forall i_1, i_2 \in S_j, d_H(ID_{i_1}, ID_{i_2}) \leq t$.*

Intuitively, (α, t)-secure index is a measure on how indistinguishable keywords are. If we want to achieve better security, we want to have large α and small t. Indeed, the authors' goal is to find a lossless (there is no deletion of documents or keywords) transformation from the given index to an $(\alpha, 0)$-secure index, for some α specified by the user as the security parameter. The authors have given a theorem on $(\alpha, 0)$-secure index as follows.

Theorem 25. *Let ID be an $m \times n$ $(\alpha, 0)$-secure index for some $0 < \alpha \leq m$. Given the response of a query $q_i = Trapdoor_w$ for some keyword w and the complete ID matrix, an attacker can successfully identify the keyword w with probability at most $\frac{1}{a}$ by just using background information related to ID matrix.*

It is important to note that the adversary described in the above theorem is different from the one we discussed in definition 10. In particular, we have here that the adversary cannot guess any keyword from its encryption with probability greater than $\frac{1}{a}$, which is independent from the keyword frequencies. In fact, all of our schemes have this property.

To transform an index to an $(\alpha, 0)$-secure one, the authors used a clustering algorithm to pad the original index with fake keywords.

5.7 Permutation with Adding Fake Keywords

In this section, we describe a scheme that is very similar to that in the IKK paper. The main difference is that our scheme is dynamic, i.e. it supports document insertions and deletions. The idea is similar: our goal is to pad fake keywords so that groups of a keywords are indistinguishable from each other. Again, we can use a permutation P_a to achieve this.

Let $(\overline{\mathsf{KGen}}, \overline{\mathsf{Enc}}, \overline{\mathsf{Dec}})$ be a secure encryption scheme on searchable encryption (i.e. with leakage being repetition of keywords). Let $\mathsf{KGen}'(a, K(DB))$ be a key generation scheme that takes in a positive integer a which divides $|K(DB)|$ and set of keywords in DB, and returns a permutation on $K(DB)$ that is a product of disjoint cycles of length a. We can define scheme 1 to be $\texttt{scheme2} = (\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ in the following way.

$\mathsf{KGen}(n, a, K(DB))$

1 : $\mathsf{k} \leftarrow \overline{\mathsf{KGen}}(1^n)$
2 : $P_a \leftarrow \mathsf{KGen}'(a, K(DB))$
3 : **return** (k, P_a)

$\mathsf{Enc}(1^n, (\mathsf{k}, P_a), DB)$

1 : $DB' = ()$
2 : **for** $d \in DB$:
3 : $K' = \cup_{i=0}^{a-1}(P_a)^i(K(d))$
4 : $DB' = DB' + (K', f(d))$
5 : **return** $\overline{\mathsf{Enc}}(1^n, \mathsf{k}, DB')$

$\mathsf{Dec}(1^n, (\mathsf{k}, P_a), EDB)$

1 : $DB = ()$
2 : **for** $ed \in EDB$:
3 : $DB = DB + \mathsf{Dec}(ed)$
4 : **return** DB

Insertion and deletion are straightforward and other functions, namely trapdoor generation and search, are taken from the aforementioned encryption scheme directly so we will omit them here.

5.8 Permutation with a Documents

Our last scheme takes a step further and apply the permutation to a set of files instead of one file each time. All functions except the encryption function for this scheme are the same as that of `scheme2` so we will not repeat it here. For simplicity, we assume that the number of documents in DB is a multiple of a. The encryption scheme for `scheme3` is the following.

$\underline{\mathsf{Enc}(1^n, (\mathsf{k}, P_a), DB)}$

$DB' = ()$
for $\{d_1, \cdots, d_a\} \leftarrow\!\!\$\ DB$:
  $K' = \cup_{i=1}^{a} (P_a)^{a-i+1}(K(d_i))$
  $db' = db' + ((K', f(d_1)))$
  for $j = 2, \cdots, a$:
    $K' = (P_a)(K')$
    $DB' = DB' + ((K', f(d_j)))$
  $DB = DB \backslash \{d_1, \cdots, d_a\}$
return $\overline{\mathsf{Enc}}(1^n, \mathsf{k}, DB')$

Insertion (of a documents each time) is straightforward and other functions, namely trapdoor generation and search, are taken from the aforementioned encryption scheme directly so we will omit them here. The drawback of this scheme is that deletion cannot be done straightaway in a way such that security is still preserved. One way to achieve deletion is to delete the target file and retrieve the other $a - 1$ files with keywords permuted from the target file, and insert them back with future insertions or documents that are already in local cache. It is also possible to store this information on the server side with an IND-CPA secure scheme without the the index structure.

6 Security Analysis

In this section, we analyse security of the schemes we described above. We begin by defining and proving the leakage of our schemes. The, we show that all of our schemes are secure against the inference attack (different from definition 10) we will define in this section. We show that security against inference attack is not sufficient. Namely, a scheme that is secure against inference attack can still leak a lot of information about the unencrypted database. We demonstrate this with a gain function and analysis of this gain function on the schemes we proposed.

6.1 Cryptographic Proofs

IND-DCPA is equivalent to Indistinguishability under Permutation. In this part, we prove equivalence between IND-DCPA and indistinguishability under permutation. The first notion is used to exam security of deterministic encryption schemes. We recall it here.

Definition 26 (IND-DCPA)**.** *Let* $(\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ *be a deterministic encryption scheme. Let* $\mathcal{A}$ *be an adversary that has access to a left-right encryption oracle and* $b \in \{0, 1\}$ *a random bit. Consider the following experiment:*

$\underline{Exp_{\mathcal{A}}^{IND\text{-}DCPA\text{-}b}(n)}$

$\mathsf{k} \leftarrow\!\!\$\ \mathsf{KGen}(1^n)$
$b' \leftarrow \mathcal{A}^{\mathsf{Enc}(\mathsf{k}, \mathcal{LR}(\cdot,\cdot,b))}$
return b'

It is required that the messages queried to the left oracle are all unique, so does the right oracle. The IND-DCPA advantage is defined to be

$$Adv_{\mathcal{A}}^{IND-DCPA}(n) = \left|\Pr\left[Exp_{\mathcal{A}}^{IND\text{-}DCPA\text{-}1}(n) = 1\right] - \Pr\left[Exp_{\mathcal{A}}^{IND\text{-}DCPA\text{-}0}(n) = 1\right]\right|. \tag{28}$$

A scheme is said to be secure in IND-DCPA if for any PPT adversary $\mathcal{A}$, the advantage above is negligible in n.

Intuitively, if a scheme is IND-DCPA secure, no adversary should be able to identify the right permutation between plaintexts and ciphertexts with probability better than random guessing. We formalise this idea as a security notion we call indistinguishability for deterministic encryption under permutation (IND-DP).

Definition 27 (IND-DP)**.** *Let* $(\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ *be a deterministic encryption scheme. Let* $\mathcal{A} = (\mathcal{A}_0, \mathcal{A}_1)$ *be an adversary where* $\mathcal{A}_0$ *is an adversary that given security parameter, generates a list of non-repeating messages and a permutation on messages;* $\mathcal{A}_1$ *is an adversary that given security parameter, a list of encrypted messages and a permutation on the plaintexts, determine if the encryption is an encryption of original messages or those in permuted order. Let* $b \in \{0, 1\}$ *be a random bit. The experiment for IND-DP can be described as follows.*

$\underline{Exp_{\mathcal{A}}^{IND\text{-}DP\text{-}b}(n)}$

1 : $\mathsf{k} \leftarrow\!\!\$\, \mathsf{KGen}(1^n)$
2 : $((m_0, \cdots, m_l), \sigma) \leftarrow \mathcal{A}_0(1^n)$
3 : $M_0 = (m_0, \cdots, m_l); M_1 = (\sigma(m_0), \cdots, \sigma(m_l))$
4 : $C \leftarrow \mathsf{Enc}(1^n, \mathsf{k}, M_b)$
5 : $b' \leftarrow \mathcal{A}_1(1^n, (m_0, \cdots, m_l), \sigma, C)$
6 : **return** b'

It is required that m_i are all unique. The IND-DP advantage is defined as:

$$Adv_{\mathcal{A}}^{IND-DP}(n) = \left|\Pr\left[Exp_{\mathcal{A}}^{IND\text{-}DP\text{-}1}(n) = 1\right] - \Pr\left[Exp_{\mathcal{A}}^{IND\text{-}DP\text{-}0}(n) = 1\right]\right|. \tag{29}$$

A scheme is said to be secure in IND-DP if for any PPT adversary $\mathcal{A}$, the advantage above is negligible in n.

Now we will show that a scheme is IND-DCPA secure if and only if it is IND-DP secure. We formalise it in the following theorem.

Theorem 28 (IND-DCPA and IND-DP are Equivalent)**.** *A scheme is IND-DCPA secure if and only if it is IND-DP secure.*

Proof. (IND-DCPA $\Rightarrow$ IND-DP) We show the contrapositive is true. Suppose a scheme is not secure under IND-DP, so there is some list of non-repeating messages M_0 and permutation σ such that the adversary for IND-DP can distinguish encryption of M_0 from M_1 (as those defined in the experiment above). We construct an IND-DCPA adversary $\mathcal{B}$ as follows:

- Let the message to the left oracle be M_0, and that to the right oracle be M_1.
- Query pairs of messages one by one until $C = \mathsf{Enc}(\mathsf{k}, M_b)$ is obtained.
- Run $\mathcal{A}_1(1^n, M_0, \sigma, C)$ for IND-DP, return what the adversary returns.

If $M = (m_0, \cdot, m_l)$, and σ a permutation on $\{m_0, m_1, \cdot, m_l\}$, we abuse the notation and write $\sigma(M)$ to mean

$(\sigma(m_0), \cdot, \sigma(m_l))$. Working out the advantages, we see that:

$$\begin{aligned}
&\mathrm{Adv}_{\mathcal{B}}^{IND-DCPA}(n) \\
=&\left|\Pr\left[\mathrm{Exp}_{\mathcal{B}}^{\text{IND-DCPA-1}}(n)=1\right]-\Pr\left[\mathrm{Exp}_{\mathcal{B}}^{\text{IND-DCPA-0}}(n)=1\right]\right| \\
=&\left|\Pr[\mathcal{A}_1(1^n, M_0, \sigma, \mathsf{Enc}(\sigma(M_0)))=1]-\Pr[\mathcal{A}_1(1^n, M_0, \sigma, \mathsf{Enc}(\sigma(M_0)))=0]\right| \\
=&\left|\Pr\left[\mathrm{Exp}_{\mathcal{A}}^{\text{IND-DP-1}}(n)=1\right]-\Pr\left[\mathrm{Exp}_{\mathcal{A}}^{\text{IND-DP-0}}(n)=1\right]\right| \\
=&\mathrm{Adv}_{\mathcal{A}}^{IND-DP}(n).
\end{aligned}$$

So the forward implication is verified.

(IND-DP ⇒ IND-DCPA) The reverse direction is straightforward. Suppose $\mathcal{A}$ is an adversary against IND-DCPA. We construct IND-DP adversary $\mathcal{B}$ as follows:

- Generate a list of non-repeating plaintexts M_0 and a permutation σ.
- Upon obtaining the list of ciphertexts C, run $\mathcal{A}^{\mathsf{Enc}(\mathsf{k},\mathcal{LR}(M_0,\sigma(M_0),b))}$. Return what the adversary returns.

By analysing the advantage of the corresponding IND-DP adversary, we see that:

$$\begin{aligned}
&\mathrm{Adv}_{\mathcal{B}}^{IND-DP}(n) \\
=&\left|\Pr\left[\mathrm{Exp}_{\mathcal{B}}^{\text{IND-DP-1}}(n)=1\right]-\Pr\left[\mathrm{Exp}_{\mathcal{B}}^{\text{IND-DP-0}}(n)=1\right]\right| \\
=&\left|\Pr\left[\mathcal{A}^{\mathsf{Enc}(\mathsf{k},\mathcal{LR}(M_0,\sigma(M_0),1))}=1\right]-\Pr\left[\mathcal{A}^{\mathsf{Enc}(\mathsf{k},\mathcal{LR}(M_0,\sigma(M_0),1))}=0\right]\right| \\
=&\left|\Pr\left[\mathrm{Exp}_{\mathcal{A}}^{\text{IND-DCPA-1}}(n)=1\right]-\Pr\left[\mathrm{Exp}_{\mathcal{A}}^{\text{IND-DCPA-0}}(n)=1\right]\right| \\
=&\mathrm{Adv}_{\mathcal{A}}^{IND-DCPA}(n).
\end{aligned}$$

So the reverse implication is verified. □

In fact IND-DP says a bit more than what is in the experiment. From the experiment, we see that $\mathsf{Enc}(M)$ and $\mathsf{Enc}(\sigma(M))$ are indistinguishable. But since $\mathsf{Enc}(\cdot)$ is a deterministic encryption, there is some permutation τ on the ciphertexts such that $\mathsf{Enc}(\sigma(M)) = \tau(\mathsf{Enc}(M))$. Therefore, the order of ciphertext looks completely random in the view of the adversary. Since deterministic encryption itself can be seen as a bijection between plaintexts and ciphertexts, we conclude that IND-DCPA secure deterministic encryption schemes acts like a random bijection.

Leakage as Co-occurrences. We have so far not specified any encryption scheme to build the index so the leakage is not fixed for the overall scheme. Now we consider those schemes whose leakage is repetition of keywords in files. Let $DB(K)$ be a function to return all documents containing keywords K, and $EDB(EK)$ be a function to return all encrypted documents containing encrypted keywords EK. We abuse the notation $\mathsf{Enc}(K)$ to mean encryption of the keywords in the search index. Then formally, we have that for all keyword sets K, $|DB(K)| = |EDB(\mathsf{Enc}(K))|$.

Since we are only interested in the security of the index (assuming the documents are securely encrypted and there is no leakage), the unencrypted database is reduced to co-occurrence at all levels with documents, and the encrypted index is reduced to co-occurrence at all levels with encrypted documents. Leakage described above is just the count version of the two.

6.2 All of our Constructions are Secure against Inference Attack

In this subsection, we show that all of our schemes are secure against inference attack. We will use extended posterior g-vulnerability to analyse the schemes. For simplicity, we assume that the database is a point

distribution, i.e. the adversary knows exactly how the database looks like. The gain function we consider here is the following:

- $\mathcal{W} = K(DB) \times EK(EDB)$,
- $\mathcal{X} = DC \times \mathcal{P}$,
- $\mathcal{Y} = \mathcal{L}(\mathcal{X}) = \{\mathsf{Enc}(DC, \sigma) \mid \sigma \in \mathcal{P}\}$,
- $g((m, c), (DC, \sigma), y) = \mathbb{1}(\sigma(m) = c)$.

Here $\mathcal{P}$ denotes the set of all possible bijections from $K(DB)$ to $EK(EDB)$, and $\mathsf{Enc}(DC, \sigma)$ is an idealised encryption function that encrypts with bijection σ and returns co-occurrences at all levels with encrypted documents. The gain function is 1 if the adversary can guess any pair of keyword and its encryption correctly in one try, and 0 otherwise. Here, the permutation P_a we used for the encryption is assumed to be known to the adversary. He can recover this piece of information by file injection attack or inspecting the algebraic structure of the leakage (since we are working with an information-theoretic adversary, this is permitted).

Furthermore, we assume in this section that the unencrypted database is singular, i.e. co-occurrences at all levels with counts is not permutable by any permutation except the identity permutation. This is an assumption that is opposite of that in [2]. We argue that their assumption is unrealistic because even for simple databases this assumption does not hold, e.g. $DB = (\{\{1\}, f_0), (\{1\}, f_1), (\{2\}, f_2))$ and one queries keyword 1 and 2 once each. In fact, it is evident from the known attacks that non-singularity is not a reasonable assumption. Furthermore, non-singularity is not a very strong classification on encrypted databases. For instance, one can achieve non-singularity by making only two keywords indistinguishable and reveal all other information.

In the next part of the subsection, we first show that any scheme that preserves singularity after encryption is not secure in our notion. We then prove that permutability can be used to achieve security. Finally, we prove that all of our constructions satisfies some form of permutability, thus they are secure under our notion.

Insecure Schemes are Insecure. We present the result as a theorem.

Theorem 29. *Let the distribution of database be a fixed distribution π, i.e. the adversary knows that the unencrypted database is DB. Let $\mathcal{X}$ be the secrets and $\mathcal{Y}$ be the leakage. given $y \in \mathcal{Y}$, and $\mathcal{L}$ the leakage function for the encryption scheme. We assume that there is a unique $x \in \mathcal{X}$ such that $\mathcal{L}(x) = y$. Then, for the gain function g defined above,*

$$EV_g(\pi, \mathcal{C}_\mathcal{L}) = 1 \tag{30}$$

Proof.

$$\begin{aligned}
&EV_g(\pi, \mathcal{C}_\mathcal{L}) \\
=&\sum_{y \in \mathcal{Y}} \Pr[\mathcal{Y} = y] \max_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} \Pr[\mathcal{X} = x \mid \mathcal{Y} = y]\, g(w, x, y) \\
=&\sum_{y \in \mathcal{Y}} \Pr[\mathcal{Y} = y] \max_{w \in \mathcal{W}} \Pr\left[\mathcal{X} = \mathcal{L}^{-1}(y) \mid \mathcal{Y} = y\right] g(w, \mathcal{L}^{-1}(y), y) \\
=&\sum_{y \in \mathcal{Y}} \Pr[\mathcal{Y} = y] \max_{w \in \mathcal{W}} 1 \cdot g(w, \mathcal{L}^{-1}(y), y) \\
=&\sum_{y \in \mathcal{Y}} \Pr[\mathcal{Y} = y] \cdot 1 \\
=&1.
\end{aligned}$$

The proof uses the property that $\Pr[\mathcal{X} = x \mid \mathcal{Y} = y]$ is 1 when $x = \mathcal{L}^{-1}(y)$ and 0 otherwise. Furthermore, since the adversary knows the pre-image completely, his maximal guess is 1 for every $g(\cdot)$. □

Permutability of Encryption implies Security. The encryption schemes we proposed do not have invertible leakage function. This is because the padding part of our schemes transforms the database into one that is P_a permutable, where P_a is part of the secret key in our schemes. We always assume that document identifiers are permuted randomly by the encryption scheme so there is no leakage by looking at the document identifiers only. Therefore, it suffices to look at the co-occurrences with counts. We formalise this as a theorem.

Theorem 30. *Let CC^{DB} be a P_a-permutable co-occurrences at all levels with counts. Let Q be a bijection from $K(DB)$ to $EK(EDB)$ that represents the idealised IND-DCPA secure encryption function on keywords. Then $Q \cdot (P_a)^i$ for $i = 1, \ldots, a-1$ generates the same leakage as Q. Furthermore, no PPT adversary can guess the correct idealised encryption function on keywords with probability greater than $\frac{1}{a}$.*

Proof. Since CC^{DB} is P_a-permutable, $(P_a)^i(CC^{DB}) = CC^{DB}$ for all $i = 0, \ldots, a-1$. By definition, this means for all $i = 0, \ldots, a-1$, for all $l = 1, \ldots, |EK(EDB)|$, for all $k_1, \ldots, k_l \in EK(EDB)^l$,

$$CC_l^{DB}((P_a)^i(k_1), \ldots, (P_a)^i(k_l)) = CC_l^{DB}(k_1, \ldots, k_l). \tag{31}$$

Recall from above that the encryption scheme for the index leaks repetition of keywords. So

$$CC_l^{DB}(k_1, \ldots, k_l) = ECC_l^{EDB}(Q(k_1), \ldots, Q(k_l)) \tag{32}$$

and

$$CC_l^{DB}((P_a)^i(k_1), \ldots, (P_a)^i(k_l)) = ECC_l^{EDB}(Q \cdot (P_a)^i(k_1), \ldots, Q \cdot (P_a)^i(k_l)). \tag{33}$$

Using equation 31, we obtain the desired result as

$$ECC_l^{EDB}(Q(k_1), \ldots, Q(k_l)) = ECC_l^{EDB}(Q \cdot (P_a)^i(k_1), \ldots, Q \cdot (P_a)^i(k_l)). \tag{34}$$

The second half of the theorem follows immediately from theorem 28. □

Because P_a is a permutation, for any $i \neq 0 \mod a$, $Q \cdot (P_a)^i(k) \neq Q(k)$ for all $k \in K(DB)$. That is, if the adversary's guess is based on the wrong permutation, he cannot guess any pair of keyword and its encryption correctly. With this observation, we can compute extended posterior vulnerability with gain function for inference attack with the following proposition.

Proposition 31. *Let the distribution of database be a fixed distribution π, i.e. the adversary knows that the unencrypted database is DB. Let CC^{DB} be a P_a-permutable co-occurrence at all levels with counts. Let Q be a bijection from $K(DB)$ to $EK(EDB)$ that represents the idealised IND-DCPA secure encryption on keywords. Let g be the gain function defined at the start of the subsection. Then*

$$EV_g(\pi, \mathcal{C}_\mathcal{L}) = \frac{1}{a}. \tag{35}$$

Proof. From theorem 30, we know that if Q is a bijection between keywords and their encryptions as an idealised encryption which can generate some given leakage, then so does $Q \cdot (P_a)^i$ for $i = 1, \ldots, a-1$. Due to indistinguishability of the encryption scheme, all these can be the actual encryption function with

probability $\frac{1}{a}$. Putting everything together, we get

$$\begin{aligned}
&EV_g(\pi, \mathcal{C}_{\mathcal{L}}) \\
=&\sum_{y \in \mathcal{Y}} \Pr[\mathcal{Y} = y] \max_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} \Pr[\mathcal{X} = x \mid \mathcal{Y} = y]\, g(w, x, y) \\
=&\sum_{y \in \mathcal{Y}} \Pr[\mathcal{Y} = y] \max_{w \in \mathcal{W}} \sum_{i=0}^{a-1} \Pr\left[\mathcal{X} = (DB, Q_y \cdot (P_a)^i) \mid \mathcal{Y} = y\right] g(w, (DB, Q_y \cdot (P_a)^i), y) \\
=&\sum_{y \in \mathcal{Y}} \Pr[\mathcal{Y} = y] \max_{w \in \mathcal{W}} \sum_{i=0}^{a-1} \frac{1}{a} \cdot g(w, (DB, Q_y \cdot (P_a)^i), y) \\
=&\sum_{y \in \mathcal{Y}} \frac{\Pr[\mathcal{Y} = y]}{a} \max_{w \in \mathcal{W}} \sum_{i=0}^{a-1} g(w, (DB, Q_y \cdot (P_a)^i), y) \\
=&\sum_{y \in \mathcal{Y}} \frac{\Pr[\mathcal{Y} = y]}{a} \cdot 1 \\
=&\frac{1}{a}.
\end{aligned}$$

The second line is obtained by re-writing the vulnerability. The third and fourth lines are obtained as a result of theorem 30. The fifth line is just re-arranging the equation. The sixth line is due to the fact that if the guess is correct for some i, then it cannot be correct for any other i. So the maximum over the expression is 1. Hence, the extended posterior vulnerability is $\frac{1}{a}$. □

Our Schemes are Secure against Inference Attack. We are now ready to show that our schemes are secure against inference attack. It suffices to show that the (unencrypted) padded database is P_a-permutable for all the schemes.

Theorem 32. *All of our schemes produces P_a-permutable padded databases.*

Proof. Since document identifiers are not relevant in this proof, we can simply look at the co-occurrences at all levels with counts.

(`scheme1`) Let CC be the co-occurrences at all levels with counts for the original database. We compute an expression for the padded co-occurrences CC' at all levels with counts and show that it is P_a-permutable. Pick an arbitrary level l, for some $k_1, \ldots, k_l \in K(DB)^l$, we see that

$$CC'_l(k_1, \ldots, k_l) = \sum_{i=0}^{a-1} CC((P_a)^i(k_1), \ldots, (P_a)^i(k_l)).$$

Therefore,

$$\begin{aligned}
&CC'_l((P_a)(k_1), \ldots, (P_a)(k_l)) \\
=&\sum_{i=0}^{a-1} CC((P_a)^{i+1}(k_1), \ldots, (P_a)^{i+1}(k_l)) \\
=&\sum_{i=0}^{a-1} CC((P_a)^i(k_1), \ldots, (P_a)^i(k_l)) \\
=&CC'_l(k_1, \ldots, k_l).
\end{aligned}$$

Since our choice of l and $k_1, \ldots, k_l$ are arbitrary, we conclude that CC' is P_a-permutable at all levels.

(scheme2) Let CC be the co-occurrences at all levels with counts for the padded database. We check that for any level l and for any $k_1, \ldots, k_l \in K(DB)^l$, $CC_l(k_1, \ldots, k_l) > 0$ implies $CC_l(k_1, \ldots, k_l) = CC_l((P_a)(k_1), \ldots, (P_a)(k_l))$. We show that for each document insertion, this holds, and by induction on the number of documents, this holds for the whole database. Suppose we insert some document with keyword $K = \{k'_1, \ldots, k'_m\} \subset K(DB)$. Then the set of keywords we have with padding is $K' = \cup_{i=0}^{a-1}(P_a)^i(K)$. Clearly, $(P_a)(K') = (K')$, so the statement is verified for the document. By induction on the number of documents, this holds for the whole database. Thus, CC is P_a-permutable.

(scheme3) We show that for groups of a documents inserted together, the permutation property holds. And then by induction on the number of documents, we have that the co-occurrences at all levels with counts for the padded database is P_a-permutable. Let $K_1, \ldots, K_a$ be the sets of keywords for the documents. Padded keyword sets for the document can be written as $K'_j =$

$$\begin{aligned} & K'_j \\ =& \cup_{i=1}^{a} (P_a)^{a-i+j}(K_i) \\ =& \cup_{i=1}^{a} (P_a)(P_a)^{a-i+j-1}(K_i) \\ =&(P_a)\left(\cup_{i=1}^{a}(P_a)^{a-i+j-1}(K_i)\right) \\ =&(P_a)(K'_{j-1}). \end{aligned}$$

Thus, the co-occurrences with counts generated by the padded keyword sets are indeed P_a-permutable. By induction on the number of documents, the co-occurrences at all levels with counts for the whole database is P_a-permutable. □

Note: do we have to write down the induction explicitly?

6.3 Security against Inference Attack is not Enough

In this subsection, we show that it is not sufficient to judge security of an encryption scheme by its security against inference attack. We show an attack on one of our schemes that can recover significant amount of information. We use extended posterior g-vulnerability to compare security of our schemes against that attack. The comparison cannot be done in the traditional setting of indistinguishability-based notions, thus demonstrating the advantages of our approach.

Exact Keyword Set Guessing Attack. The goal of adversary for exact keyword set guess attack is to recover the exact set of keywords for some document. Without loss of generality, we can assume that the goal of the adversary is to recover the keyword set for the first encrypted file.

From above, we know that the set of encryption functions indistinguishable by the adversary is $Q \cdot (P_a)^i$ for $i = 1, \ldots, a-1$ where Q is the true idealised encryption function. So in the leakage channel, we only have to look at these as secrets corresponding to encryption because all others result in $p(x \mid y) = 0$. To make it more interesting, we assume that the adversary does not have access to the exact unencrypted database (otherwise there are trivial attacks for some databases). Note that in this case, the encryption function mentioned above can still be recovered. This is because the adversary can work with aggregated information such as aggregated co-occurrences at level 1 and 2 with counts. Thus, we can model the secret as the set of keywords in the first encrypted document and the encryption function, and the leakage as the encrypted keywords in the first encrypted document. We define the leakage channel and gain function as follows.

- $\mathcal{W} = \mathcal{P}(K(DB))$,
- $\mathcal{X} = \mathcal{P}(K(DB)) \times \{Q \cdot (P_a)^i \mid i = 0, \ldots, a-1\}$,
- $\mathcal{Y} = \mathcal{P}(EK(EDB))$,

- $g(w, (K, Q \cdot (P_a)^i), EK) = \mathbb{1}(w = K)$.

Security of `Scheme1` against Exact Keyword Set Guessing Attack. Under the gain function above, we will show that extended posterior g-vulnerability of `scheme1` is $\frac{1}{a}$. We will then argue that by combining exact keyword set guess attack with semantics of keywords, one can break the security of the scheme.

Theorem 33. *Let the leakage channel and gain function be those described above. Furthermore, we assume that for all $y \in \mathcal{Y}, (P_a)(y) \neq y$. Then*

$$EV_g^{scheme1}(\pi, \mathcal{C}_{\mathcal{L}}) = \frac{1}{a}. \tag{36}$$

Proof. We observe that for any leakage $y = EK$, if we know the encryption function is $Q \cdot (P_a)^i$ for some i, then the set of keywords for the unencrypted document is exactly $(Q \cdot (P_a)^i)^{-1}(EK)$. Because $(P_a)(y) \neq y$ for all $y \in \mathcal{Y}$, $(Q \cdot (P_a)^i)^{-1}(EK)$ is the exact set of keywords only when $(Q \cdot (P_a)^i)^{-1}$ is the correct decryption function. This happens with probability $\frac{1}{a}$. In terms of extended posterior g-vulnerability, we have

$$\begin{aligned}
&EV_g^{\texttt{scheme1}}(\pi, \mathcal{C}_{\mathcal{L}}) \\
=&\sum_{y \in \mathcal{Y}} \Pr[\mathcal{Y} = y] \max_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} \Pr[\mathcal{X} = x \mid \mathcal{Y} = y]\, g(w, x, y) \\
=&\sum_{y \in \mathcal{Y}} \Pr[\mathcal{Y} = y] \max_{w \in \mathcal{W}} \sum_{i=0}^{a-1} \Pr\left[\mathcal{X} = ((Q \cdot (P_a)^i)^{-1}(y), Q \cdot (P_a)^i) \mid \mathcal{Y} = y\right] g(w, ((Q \cdot (P_a)^i)^{-1}(y), Q \cdot (P_a)^i)), y) \\
=&\sum_{y \in \mathcal{Y}} \Pr[\mathcal{Y} = y] \max_{w \in \mathcal{W}} \sum_{i=0}^{a-1} \frac{1}{a} \cdot g(w, ((Q \cdot (P_a)^i)^{-1}(y), Q \cdot (P_a)^i)), y) \\
=&\sum_{y \in \mathcal{Y}} \frac{\Pr[\mathcal{Y} = y]}{a} \max_{w \in \mathcal{W}} \sum_{i=0}^{a-1} g(w, ((Q \cdot (P_a)^i)^{-1}(y), Q \cdot (P_a)^i)), y) \\
=&\sum_{y \in \mathcal{Y}} \frac{\Pr[\mathcal{Y} = y]}{a} \cdot 1 \\
=&\frac{1}{a}.
\end{aligned}$$

□

There is in fact a more detrimental attack based on this. In the adversary above, the sets of keywords $(Q \cdot (P_a)^i)^{-1}(y)$ are equally likely because we do not care if the first encrypted document is a real or fake one. Suppose now our goal is to recover the exact keyword set for some real document (not necessarily the first one). By the algebraic structure of the encryption scheme, all of $(Q \cdot (P_a)^i)^{-1}(y)$ can be the keyword set for a real document. But in practice, they are not equally likely to happen. This is because keywords have semantic meaning so some set of keywords occur together more frequently than the others. By using this extra information, one can guess with success rate higher than $\frac{1}{a}$.

`Scheme2` and `scheme3` are more Secure. Now we show that `Scheme2` and `scheme3` achieves better security with respect to the gain function. We will do this by comparing the extended posterior g-vulnerability of the three schemes without explicitly computing them. Hence, demonstrating the advantage of using extended posterior g-vulnerability to evaluate security of encryption schemes.

Theorem 34. *Let the leakage channel and gain function be those described above. Furthermore, we assume that for all $y \in \mathcal{Y}, (P_a)(y) \neq y$. Then*

$$EV_g^{scheme1}(\pi, \mathcal{C}_{\mathcal{L}}) \geq EV_g^{scheme2}(\pi, \mathcal{C}_{\mathcal{L}}) \geq EV_g^{scheme3}(\pi, \mathcal{C}_{\mathcal{L}}). \tag{37}$$

Proof. We examine the sets of keywords which can possibly give leakage y in each scheme, and compare the conditional probability $\Pr[x \mid y]$ for the schemes. For `scheme1`, we see that $\{((Q \cdot (P_a)^i)^{-1}(y), Q \cdot (P_a)^i) \mid i = 0, \ldots, a-1\}$ is the set of x that can generate leakage y. Each occurs with probability $\frac{1}{a}$ and only one of them contains the correct keyword set. So $\max_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} \Pr[\mathcal{X} = x \mid \mathcal{Y} = y]\, g(w, x, y) = \frac{1}{a}$.

On the other hand, the feasible keyword sets is $\bar{\mathcal{X}} = \{(P_a)^i(x) \mid (x \subset y) \wedge (i = 0, \ldots, a-1) \wedge (\cup_{i=0}^{a-1} (P_a)^i(x) = y)\}$. Each keyword set can be paired with any encryption function $Q \cdot (P_a)^j$ for $j = 0, \ldots, a-1$. Therefore, we only need to look at the distribution of elements in $\bar{\mathcal{X}}$. But there are at least a elements (since y is not P_a-permutable), so the probability of guessing the correct keyword is less than or equal to $\frac{1}{a}$. This means $\max_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} \Pr_{\texttt{scheme2}}[\mathcal{X} = x \mid \mathcal{Y} = y] g(w, x, y) \leq \max_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} \Pr_{\texttt{scheme1}}[\mathcal{X} = x \mid \mathcal{Y} = y] g(w, x, y)$. Thus, $EV_g^{\texttt{scheme1}}(\pi, \mathcal{C}_{\mathcal{L}}) \geq EV_g^{\texttt{scheme2}}(\pi, \mathcal{C}_{\mathcal{L}})$.

For `scheme3`, we see that the set of feasible keyword sets contains all of $\bar{\mathcal{X}}$. At the same time, we have that each keyword set can be paired with any encryption function $Q \cdot (P_a)^j$ for $j = 0, \ldots, a-1$. So it must be the case that $\max_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} \Pr_{\texttt{scheme3}}[\mathcal{X} = x \mid \mathcal{Y} = y] g(w, x, y) \leq \max_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} \Pr_{\texttt{scheme2}}[\mathcal{X} = x \mid \mathcal{Y} = y] g(w, x, y)$. Therefore, $EV_g^{\texttt{scheme2}}(\pi, \mathcal{C}_{\mathcal{L}}) \geq EV_g^{\texttt{scheme3}}(\pi, \mathcal{C}_{\mathcal{L}})$. □

There is an easy way to see this inequality. We simplify the attack to only guessing the number of real keywords in the first document. Let n be the number of keywords in the first encrypted document. For `scheme1`, since there is no padding of keywords to documents, so the number of real keywords is n. For `scheme2`, due to collisions, we only know that the number of keywords can fall in the range $\lceil \frac{n}{a} \rceil$ to n. For `scheme3`, the number of keywords can be any integer from 1 to n.

References

[1] M. S. Alvim, K. Chatzikokolakis, C. Palamidessi, and G. Smith. Measuring information leakage using generalized gain functions. In *2012 IEEE 25th Computer Security Foundations Symposium*, pages 265–279, June 2012.

[2] Reza Curtmola, Juan A. Garay, Seny Kamara, and Rafail Ostrovsky. Searchable symmetric encryption: improved definitions and efficient constructions. In Ari Juels, Rebecca N. Wright, and Sabrina De Capitani di Vimercati, editors, *ACM CCS 06: 13th Conference on Computer and Communications Security*, pages 79–88, Alexandria, Virginia, USA, October 30 – November 3, 2006. ACM Press.

[3] Mohammad Saiful Islam, Mehmet Kuzu, and Murat Kantarcioglu. Access pattern disclosure on searchable encryption: Ramification, attack and mitigation. In *ISOC Network and Distributed System Security Symposium – NDSS 2012*, San Diego, CA, USA, February 5–8, 2012. The Internet Society.

[4] Muhammad Naveed, Seny Kamara, and Charles V. Wright. Inference attacks on property-preserving encrypted databases. In Indrajit Ray, Ninghui Li, and Christopher Kruegel:, editors, *ACM CCS 15: 22nd Conference on Computer and Communications Security*, pages 644–655, Denver, CO, USA, October 12–16, 2015. ACM Press.