情報処理学会論文誌 Vol.60 No.1 240–249 (Jan. 2019)

推薦論文

秘匿検索の頻度分析対策としての複数DB活用について

伊藤 隆[1,a)] 平野 貴人[1] 森 拓海[1] 服部 充洋[1]

受付日 2018年4月3日, 採録日 2018年10月2日

概要：秘匿検索（検索可能暗号）は，ユーザがデータセンタに登録した暗号化データを，暗号化したままで検索するための技術である．秘匿検索では，暗号化キーワードの頻度からキーワードを推定する頻度分析攻撃に対抗するため，確率的暗号を用いるなどして頻度情報を隠ぺいする．しかし，秘匿検索システムが運用されて検索が行われると，キーワードの同一性や頻度情報が徐々に漏れるため，最終的には頻度分析攻撃が可能になるという問題があった．本論文では，暗号化データを複数データセンタのいずれかに振り分け，この際各データセンタにおける頻度分布が撹乱されるよう工夫することで，効率面でのオーバヘッドを生じることなく，頻度分析対策を実現する方式を提案する．また，提案方式による頻度分析耐性の向上を，攻撃者によるキーワード推定の的中率に基づいて評価した結果，データセンタ数は2個で十分であること，都道府県名を秘匿する例で的中率を78%から17%に低減できることなどが確認できた．

キーワード：暗号，検索可能暗号，頻度分析

Introducing Multiple Databases in Searchable Encryption as a Countermeasure to the Frequency Analysis

Takashi Ito[1,a)] Takato Hirano[1] Takumi Mori[1] Mitsuhiro Hattori[1]

Received: April 3, 2018, Accepted: October 2, 2018

Abstract: Searchable encryption allows users to conduct a keyword search over encrypted data without decryption. Typical searchable encryption schemes employ probabilistic encryption to combat the frequency analysis in which an attacker would guess the keywords hidden in encrypted data by analyzing the frequency of the encrypted data that is identical in binary form. In practice, however, conducting a keyword search will reveal at least a small portion of the frequency of the hidden keywords and eventually the frequency analysis may become a practical threat. We propose in this paper a searchable encryption scheme that counteracts this security threat. In our scheme, encrypted data is distributed to multiple databases and thereby the frequency of the hidden keywords in each database is distorted. Experimental results show that our scheme is highly resistant to the frequency analysis and only two databases should suffice to distort the frequency; for example, when prefectures are designated as sensitive keywords, our scheme can suppress the adversary's correct estimation ratio from 78% to 17% using only two databases.

Keywords: encryption, searchable encryption, frequency analysis

1. はじめに

秘匿検索（検索可能暗号）は，ユーザがデータセンタに登録した暗号化データを，暗号化したままで検索するための技術である．秘匿検索を用いると，データセンタへの機密情報のアウトソーシングや，データセンタ上での暗号化メールのフィルタリングなどが実現可能となるため，機能性・安全性・効率性などを考慮した，様々な秘匿検索方式が提案されている [1], [2], [3], [4], [5], [6], [7], [8].

検索用のキーワードを直接暗号化するタイプの秘匿検索の場合，同じキーワードが同じ暗号化キーワードになることで頻度分析攻撃されることを防ぐため，通常はキーワー

[1] 三菱電機株式会社情報技術総合研究所
Mitsubishi Electric Corporation Information Technology R&D Center, Kamakura, Kanagawa 247–8501, Japan
[a)] Ito.Takashi@aj.MitsubishiElectric.co.jp

本論文の内容は2017年6月のマルチメディア，分散，協調とモバイル（DICOMO2017）シンポジウムにて報告され，コンピュータセキュリティ研究会主査により情報処理学会論文誌ジャーナルへの掲載が推薦された論文である．

© 2019 Information Processing Society of Japan

ドを確率的暗号で暗号化する [1], [2]．一方で，確定的暗号をベースとしつつ，頻度分析攻撃への耐性を持たせた方式も提案されている [6], [7]．

しかし，確率的暗号・確定的暗号のいずれを用いる場合でも，実際に秘匿検索システムが運用されて検索が行われると，検索要求とマッチした複数の暗号化キーワードについてキーワードの同一性が判明し，その頻度情報もデータセンタに漏れてしまう．これが繰り返されることで，最終的にはデータセンタによる頻度分析攻撃が可能になるという問題があった．

この問題に対し，山岡らの論文 [8] では，全キーワードを，k（≥ 2）個以上のキーワードで構成されるグループのいずれかに分類し，検索時にはキーワードの代わりにグループ ID を用いる方式が提案されている．この方式の利点は，攻撃者がグループ ID や，グループを構成するキーワード群を特定できた場合でも，正しいキーワードが k 個のうちどれであるかを特定できないことである．しかしこの方式には，検索処理量，特にデータセンタからデータ検索者に送信される検索結果のサイズが約 k 倍に悪化するという，効率面での課題がある．

そこで本論文では，データセンタを 2 個以上の少数用意したうえで，暗号化データをいずれかのデータセンタに振り分けて登録することで，攻撃者による頻度分析攻撃を困難にする方式を提案する．ただし，登録先データセンタを複数用意しても，登録先を一様ランダムに選ぶ方式や，（分散ハッシュテーブルなどを用いて）キーワードから一意に登録先を決定する方式では頻度分析攻撃を防ぐことはできない．提案方式では，**キーワードごとに**設定された振り分け確率に従って登録先を選択することで，各データセンタにおけるキーワードの頻度分布を，元のキーワードの頻度分布から変化させ，頻度分析攻撃を困難にする．提案方式の本質は簡潔な処理であるため，既存の多くの秘匿検索方式への適用が期待できるとともに，データセンタのストレージや，各エンティティの計算量・通信量を増加させることなく，秘匿検索の頻度分析対策を実現することが可能である．

また，提案方式による頻度分析耐性の向上を，合理的な攻撃者によるキーワード推定の的中率を評価指標として定量的に評価した．評価の結果，データセンタ数は 2 個で十分であることが分かり，たとえば都道府県名を秘匿検索対象として 10 万人分の情報が登録される場合で，無対策の場合に 78%となる的中率を，提案方式の適用で 17%まで低減できるなどの結果が得られた．

2. 既存の秘匿検索方式と課題

本章では，秘匿検索について簡単に説明したのち，秘匿検索システムの分類および既存方式の紹介を行う．その後，秘匿検索システムに対する攻撃の 1 つである「頻度分析攻撃」について説明する．

2.1 秘匿検索システムのエンティティと要件

秘匿検索（検索可能暗号）技術とは，暗号化データを暗号化したままで検索する技術の総称である．本論文で扱う「秘匿検索システム」では，登場するエンティティは以下の 3 つとする．

- **データセンタ：**データ検索者が利用するデータを，データ検索者に代わって保持するエンティティ．データ検索者に対して検索機能を提供する．
- **データ登録者：**データセンタにデータを登録するエンティティ．通常，データ検索者がデータを検索できるよう，各データに対して適切なキーワードを付与する．なお，データ登録者と，次のデータ検索者は同一のエンティティが兼ねることもある．
- **データ検索者：**データセンタに登録されたデータを検索するエンティティ．データ検索や，検索後に取得したデータの復号に利用する秘密情報を持っている．

秘匿検索システムでは，データセンタに対して余計な情報を漏らさないまま，データセンタによる検索処理を可能とすることが求められる．具体的には，以下のような要件が設定される．

- **要件 1（機能性）：**データ検索者が，指定した検索キーワードに対応するデータを得られること．
- **要件 2（安全性）：**データセンタに対し，データ検索者が利用するデータの情報，およびデータに付与されたキーワード（登録キーワード）の情報が漏れないこと．
- **要件 3（効率性）：**ストレージ・計算量・通信量などの面で効率的であること．

2.2 秘匿検索システムの分類

本節では，秘匿検索システムをいくつかの観点から分類し，それぞれに対応する関連研究をあげる．

2.2.1 公開型と非公開型

秘匿検索システムは，データ登録の権限を一般に公開するか，もしくは決められたエンティティのみに限定するかで，以下の 2 つに大別することができる．

- **公開型：**データ登録の権限を一般に公開するもの．データや検索用のキーワードは公開鍵暗号で暗号化される．外部から来る暗号化メールを，暗号化したまま分類したい場合などに利用できる．代表例は文献 [2], [4] など．
- **非公開型：**データ登録者にも秘密情報を持たせることで，データ登録の権限を，決められたエンティティのみに限定するもの．データやキーワードの暗号化に共通鍵暗号を用いることが多いが，公開鍵暗号を利用しつつ，公開鍵を非公開にするといった使い方も可能である．企業内のデータをデータセンタに外部委託したい場合などに用いられる．代表例は文献 [1], [3], [5] など．

© 2019 Information Processing Society of Japan

2.2.2 タグ型とインデックス型

- **タグ型**：個々の検索用キーワードから**タグ**と呼ばれる暗号化キーワードを生成し，検索時には各タグと検索要求とのマッチを逐一確認するもの．次のインデックス型に比べ，データの追加・削除が容易であるという長所を持つ．代表例は文献 [1], [2], [4] など．
- **インデックス型**：あらかじめ，文書とそれに含まれるキーワードの対応表である**インデックス**を作成しておき，検索時にはインデックスに対して処理を行うことで検索用キーワードを含む文書を特定する．一般にタグ型よりも高速であるが，データの追加・削除に複雑な処理を必要とすることが多い．代表例は文献 [3], [5] など．

2.2.3 確定的暗号ベースと確率的暗号ベース

特にタグ型の秘匿検索システムについて，キーワードからタグを生成する際に利用する暗号方式によって，以下のような分類も行われる．両方式では，検索時にタグと検索要求とのマッチを確認する方法が異なる．

- **確定的暗号ベースの方式**：キーワードからタグを生成する際に確定的暗号を利用するもの．確定的暗号を用いて単純にタグを生成する場合，同一のキーワードからつねに同一のタグが生成されるため，検索時のマッチ確認ではタグと検索要求のバイナリ一致判定を行うだけでよく，レコード数 n に対して $\mathrm{O}(\log n)$ で検索できる利点がある．ただし，そのままでは頻度分析攻撃によってキーワードを推定されるリスクがあるため，通常は何らかの対策を行う．代表例は文献 [4], [6], [7] など．
- **確率的暗号ベースの方式**：キーワードからタグを生成する際に確率的暗号を利用するもの．同一のキーワードから毎回異なるタグが生成されるため，検索時のマッチ確認ではタグと検索要求の間で特殊な演算を行う必要があり，レコード数 n に対して $\mathrm{O}(n)$ の検索時間を必要とする．一方で，多数のタグを観測してもキーワードの頻度情報が漏れないため，確定的暗号ベースの方式よりは安全性が高いとされる．代表例は文献 [1], [2] など．

2.3 本論文で対象とする秘匿検索システム

本論文では，非公開型，かつタグ型の秘匿検索システムを対象とし，下記の手順に従って動作するシステムを想定する．以下ではデータセンタを $\mathcal{C}$，データ登録者を $\mathcal{R}$，データ検索者を $\mathcal{S}$ で表す．また，データ暗号化アルゴリズムを E_1，キーワード暗号化アルゴリズムを E_2 とし，E_2 に対応する検索要求生成アルゴリズムを Q とする．なお，E_2 が確定的・確率的のいずれであるかは問わない．E_2 が確定的である場合，Q は E_2 と同一アルゴリズムとなる．

準備

(1) $\mathcal{S}$ は，データ秘匿用の鍵，キーワード秘匿用の鍵を生成する．また，データ・キーワードの暗号化に用いる鍵を $\mathcal{R}$ に通知する．

登録

(2) $\mathcal{R}$ は，$\mathcal{C}$ に登録するデータ d に対し，登録キーワード w を設定する．

(3) $\mathcal{R}$ は，データ d およびキーワード w を暗号化し，得られた暗号化データ $E_1(d)$ およびタグ $E_2(w)$ を $\mathcal{C}$ に送信する．

(4) $\mathcal{C}$ は，$\mathcal{R}$ から受信した $E_1(d)$，$E_2(w)$ を対応付けたうえで，暗号化 DB に登録する．複数のデータを受信・登録した結果，暗号化 DB はたとえば**表 1** のようになる．

表 1 暗号化 DB
Table 1 An encrypted DB.

レコード ID	暗号化データ	タグ
1	$E_1(d_1)$	$E_2(w_1)$
2	$E_1(d_2)$	$E_2(w_2)$
3	$E_1(d_3)$	$E_2(w_3)$
4	$E_1(d_4)$	$E_2(w_4)$
5	$E_1(d_5)$	$E_2(w_5)$
⋮	⋮	⋮

検索

(5) $\mathcal{S}$ は，検索キーワード w' に対応する検索要求 $Q(w')$ を生成し，$\mathcal{C}$ に送信する．

(6) $\mathcal{C}$ は，暗号化 DB の各レコードについて，タグが検索要求とマッチするかを確認する．

(7) $\mathcal{C}$ は，マッチしたタグに対応する暗号化データを $\mathcal{S}$ に送信する．

(8) $\mathcal{S}$ は，受信した暗号化データを復号し，データを得る．

2.4 秘匿検索システムに対する頻度分析攻撃

2.4.1 確定的暗号に対する頻度分析攻撃

前述のように，確定的暗号を利用してタグを生成すると高速な検索が可能という利点があるが，確定的暗号を単純に用いただけでは，観測したタグの頻度分布からタグに対応するキーワードを推定する「頻度分析攻撃」に弱いという欠点がある．

例として，日本居住者に関する個人情報 d_i を暗号化して DB に登録する際，検索用のキーワードとして都道府県名を利用し，これを確定的暗号化することを考える．この場合，確定的暗号化アルゴリズムを E_{D} とすると，データセンタが保持する暗号化 DB はたとえば**表 2** のようになる．ここで，レコード ID 2, 5 におけるタグ E_{D}(東京) は同一の値となることから，データセンタは元のキーワードが同一であることが分かる．さらに，DB に含まれる全タグの出現数を数えることで，たとえば**表 3** のような頻度分布を得ることができる（この時点では各タグに対応するキーワードは判明していない）．なお，表 3 のような，特定 DB に

© 2019 Information Processing Society of Japan

表 2 暗号化 DB（確定的暗号でタグを生成する場合）
Table 2 An encrypted DB with deterministic encryption.

レコード ID	暗号化データ	タグ
1	$E_1(d_1)$	E_D(北海道)
2	$E_1(d_2)$	E_D(東京)
3	$E_1(d_3)$	E_D(三重)
4	$E_1(d_4)$	E_D(岩手)
5	$E_1(d_5)$	E_D(東京)
⋮	⋮	⋮

表 3 タグの頻度分布
Table 3 Frequency of tags.

タグ	出現数（比率）
E_D(東京)	10,528（0.105）
E_D(神奈川)	7,393（0.074）
E_D(大阪)	6,882（0.069）
E_D(愛知)	5,910（0.059）
E_D(埼玉)	5,684（0.057）
⋮	⋮
総数	100,000

表 4 キーワードの頻度分布
Table 4 Frequency of keywords.

都道府県	人口比率
東京	0.106
神奈川	0.072
大阪	0.070
愛知	0.059
埼玉	0.057
⋮	⋮

含まれるタグの頻度を以降では単に「**タグの頻度**」と記す．

一方，都道府県の人口比率は**表 4**（平成 27 年国勢調査の結果 [9] から算出）のとおりであることが知られているため，データセンタはこれらの頻度を比較することで，各タグに対応する都道府県名を推定することが可能となる．Lacharité らは，タグとキーワードを頻度の高い順から 1 つずつ対応付ける自然な推定が，最尤推定となることを示した [10]．この推定を行うと，例示したような 10 万件のレコードを観測したデータセンタは，78%のレコードについて正しい都道府県名を推定できる．なお，表 4 のような，各キーワードと対応付いたキーワードの母集団頻度を以降では単に「**キーワードの頻度**」と記す．

確定的暗号ベースの方式における頻度分析対策として，検索に使用しない単語に乱数をパディングすることでタグの種類を増加させる方式 [6] や，偏ったキーワードの頻度を分割することで頻度を均一化し，キーワードの特定を困難にする方式 [7] などが提案されている．

2.4.2 検索で判明する頻度を利用した頻度分析攻撃

確率的暗号ベースの方式や，前述の対策を行った確定的暗号ベースの方式では，DB 中のタグのみを観測した頻度分析攻撃は成立しない．しかし，いずれの場合でも，検索処理が行われ，データセンタが検索要求 $Q(w')$ を受け取ってマッチを確認する（2.3 節の手順 (6)）と，$Q(w')$ にマッチしたすべてのタグに関して，対応するキーワードが同一であることが分かり，その出現数も判明する．最も単純な例では，2 値データ（性別，合否，病気の有無など）を秘匿検索対象とした場合，1 回の検索が行われるだけでキーワードの同一性と出現数がすべて判明するため，頻度分析攻撃が可能となる．また，都道府県名のようにキーワードの種類が多い場合でも，システムで十分な検索が行われると，すべてのタグに関する出現数が判明すると考えられるため，最終的にはデータセンタによる頻度分析攻撃が可能になってしまう．なお，検索後に判明した同一性に基づくタグの頻度に関しても，以降では単に「タグの頻度」と記す．

単純な回避策として，実在するキーワードや架空のキーワードから生成したタグを含む，ダミーのレコードを追加することでタグの頻度を撹乱する方法が考えられるが，ダミー追加にともなうストレージ・計算量・通信量のオーバヘッドが避けられないうえ，頻度分析耐性が確実に向上するようなダミー追加の方法は自明でない．

一方，ダミーのレコードを使わない方法として，山岡らの論文 [8] では，全キーワードを，k（≥ 2）個以上のキーワードで構成されるグループのいずれかに分類し，検索時にはキーワードの代わりにグループ ID を用いる方式が提案されている．この方式の利点は，攻撃者がグループ ID や，グループを構成するキーワード群を特定できた場合でも，正しいキーワードが k 個のうちどれであるかを特定できないことである．しかしこの方式には，検索処理量，特にデータセンタからデータ検索者に送信される検索結果のサイズが約 k 倍に悪化するという，効率面での課題がある．

なお，検索後に行われる頻度分析攻撃として，検索要求の頻度から検索キーワードを推定する攻撃も考えられるが，本論文ではタグの頻度を利用した攻撃を対象とし，検索要求の頻度を利用した攻撃についてはスコープ外とする．

3. 提案方式

検索で判明する頻度の利用も含めた頻度分析攻撃に対し，既存の対策は，データセンタのストレージや計算量，通信量などに何らかのオーバヘッドを生じるものであった．本章では，これらのオーバヘッドを生じない頻度分析対策として，登録データを複数データセンタのいずれかに振り分け，この際各データセンタにおけるタグの頻度が撹乱されるよう工夫することで，頻度分析攻撃を困難にする方式を提案する．

なお，提案方式では複数データセンタを利用するが，各データセンタは結託しないことを前提とする．提案方式は

© 2019 Information Processing Society of Japan

表 5 振り分け確率
Table 5 Distribution probabilities.

キーワード	$\mathcal{C}_1$	$\mathcal{C}_2$
東京	0.362	0.638
神奈川	0.585	0.415
大阪	0.845	0.155
愛知	0.151	0.849
埼玉	0.645	0.355
⋮	⋮	⋮

データセンタどうしの通信が不要な方式であるため，各データセンタが結託すべき相手を特定することは容易でなく，この前提は現実的な妥当性を持つと考える．

3.1 特徴

提案方式では，データを複数データセンタ $\mathcal{C}_1, \mathcal{C}_2, \ldots$ に振り分けて登録するが，この際，あらかじめ秘密情報として設定した「**振り分け確率**」に従って振り分けを行う．振り分け確率はたとえば**表 5** のように設定され，それぞれの確率は「当該キーワードが設定されたデータの登録先として $\mathcal{C}_i$ を選択する確率」を表す．ここで，キーワードごとに異なる振り分け確率を設定することが本質であり，これによって各データセンタにおけるタグの頻度が撹乱される．

3.2 振り分け確率設定の具体例

振り分け確率は様々な方法で設定できるが，本節では，キーワード集合が既知・未知それぞれの場合について，振り分け確率設定の具体例を示す．なお，以降ではキーワード集合を $\{w_i\}$，キーワード w_i が設定されたデータを $\mathcal{C}_j$ に振り分ける確率を q_{ij} で表す．また，データセンタの数を m（≥ 2）とする．

3.2.1 キーワード集合が既知である場合

有限個のキーワードが事前に判明している場合（たとえば性別，都道府県名，国名など），各キーワード w_i に対して以下を行うことで，振り分け確率を設定することができる．

(1) $[0,1)$ の一様乱数を m 個生成し，$q'_{i1}, \ldots, q'_{im}$ とする．
(2) 上記を，合計が 1 となるよう正規化したものを振り分け確率とする．すなわち，$q_{ij} = q'_{ij} / \sum_{k=1}^{m} q'_{ik}$．

この場合，振り分け確率全体 $\{q_{ij}\}$ が秘密情報となる．

3.2.2 キーワード集合が未知である場合

事前にすべてのキーワードが判明しない場合（たとえば人名，フリーワードなど），表 5 のような確率テーブルを事前に得ることはできない．このような場合でも，「キーワード w_i から振り分け確率 q_{ij} を確定的に算出する方法」をたとえば以下のように定めておくことで，提案方式を同様に適用できる．

(1) 各 $j \in \{1, \ldots, m\}$ に対し，鍵付きハッシュ関数 H_K の出力を数値と見なして $h_{ij} = H_K(w_i|j)$ を計算する（$|$ は文字列としての連結）．
(2) 上記を，合計が 1 となるよう正規化したものを振り分け確率とする．すなわち，$q_{ij} = h_{ij} / \sum_{k=1}^{m} h_{ik}$．

この場合，H_K の秘密鍵 K のみが秘密情報となる．

3.3 アルゴリズム

前述の振り分け確率を取り入れた，提案方式の処理手順を以下に示す．

準備
(1) $\mathcal{S}$ は，データ秘匿用の鍵，キーワード秘匿用の鍵を生成する．また，データ・キーワードの暗号化に用いる鍵を $\mathcal{R}$ に通知する．
(2) $\mathcal{S}$ は，秘密情報として振り分け確率を設定し，$\mathcal{R}$ に通知する．

登録
(3) $\mathcal{R}$ は，登録するデータ d に対し，登録キーワード w を設定する．
(4) $\mathcal{R}$ は，登録キーワード w に関する振り分け確率に従い，登録先 $\mathcal{C}^*$ を決定する．
(5) $\mathcal{R}$ は，データ d およびキーワード w を暗号化し，得られた暗号化データ $E_1(d)$ およびタグ $E_2(w)$ を，(4) で決定した $\mathcal{C}^*$ に送信する．
(6) $\mathcal{C}^*$ は，$\mathcal{R}$ から受信した $E_1(d)$，$E_2(w)$ を対応付けたうえで，暗号化 DB に登録する．

検索
(7) $\mathcal{S}$ は，検索キーワード w' に対応する検索要求 $Q(w')$ を生成し，**すべての** $\mathcal{C}_j$ に送信する．
(8) 各 $\mathcal{C}_j$ は，暗号化 DB の各レコードについて，タグが検索要求とマッチするかを確認する．
(9) 各 $\mathcal{C}_j$ は，マッチしたタグに対応する暗号化データを $\mathcal{S}$ に送信する．
(10) $\mathcal{S}$ は，すべての $\mathcal{C}_j$ から受信した暗号化データを復号し，データを得る．

3.4 効果：タグの頻度撹乱による頻度分析耐性向上

提案方式を用いると，各データセンタで観測されるタグの頻度が撹乱されることを実例で示す．

日本全国から一様に選んだ 10 万人分のデータを，都道府県名をキーワードとして登録する際，表 5 の確率に従って 2 個のデータセンタに振り分ける場合を考える．このとき，キーワードを東京とするデータ（全体の 10.6%程度）は，確率 0.362 で $\mathcal{C}_1$ に，確率 0.638 で $\mathcal{C}_2$ に登録されるため，全体の 3.8%程度が $\mathcal{C}_1$ に，全体の 6.8%程度が $\mathcal{C}_2$ に登録されることになる．他の都道府県についても同様に考えると，各データセンタに登録されるタグの頻度はたとえば**表 6** のようになり，キーワードの頻度から大きく変化していることが分かる．したがって，振り分け確率を秘密情報

© 2019 Information Processing Society of Japan

表 6 タグの頻度分布，および各 DB における比率
Table 6 Frequency of tags, and the ratio in each DB.

タグ	$\mathcal{C}_1$	$\mathcal{C}_2$
E_{D}(東京)	3,825（0.071）	6,703（0.146）
E_{D}(神奈川)	4,355（0.080）	3,038（0.066）
E_{D}(大阪)	5,790（0.107）	1,092（0.024）
E_{D}(愛知)	845（0.016）	5,065（0.111）
E_{D}(埼玉)	3,698（0.068）	1,986（0.043）
⋮	⋮	⋮
総数	54,228	45,772

として扱う限り，各データセンタにおけるタグの頻度からキーワードを推定することが困難となる（4 章で定量的に評価する）．

なお，提案方式ではキーワードごとに異なる振り分け確率を設定することが本質である．キーワードを考慮せず無作為に振り分けを行った場合，各データセンタにおけるタグの頻度分布は，キーワードの頻度分布からほぼ変化しないことになり，頻度分析対策としての効果が得られない．

一方，分散ハッシュテーブルなどを用いて，キーワードごとに決められたデータセンタに登録（たとえば北海道・東北地方のデータを $\mathcal{C}_1$ へ，関東地方のデータを $\mathcal{C}_2$ へ，など分散）し，検索時は必要なデータセンタのみにアクセスすることでデータセンタの計算量を削減する方式も考えられる．この場合，各データセンタに登録されるタグの頻度分布が変化するため，一見すると頻度分析対策も兼ねるようにも思えるが，実際には各タグの頻度比がキーワードの頻度比から変化しないため，頻度分析対策としての効果は薄い（以上についても 4 章で評価する）．

3.5 効率

まず，データセンタ側から見た場合，提案方式を用いた場合の処理は，単一データセンタを利用する場合の処理とまったく変わらない．また，全データセンタが扱うデータの総量（ストレージ・計算量・通信量）も変わらないため，オーバヘッドを生じることなく秘匿検索を実現できる．

データ登録者，データ検索者から見た場合も，追加の処理は登録先の決定，検索結果の集約などごくわずかであり，追加の情報も振り分け確率（または鍵付きハッシュ関数の秘密鍵）だけであるため，効率面でのデメリットはほとんどないと考えてよい．

4. 安全性評価

本章では，既存方式と提案方式について，検索で判明する頻度を利用した頻度分析攻撃への耐性を定量的に評価した結果を記す．

4.1 評価対象

本論文では，データ量や通信量などのオーバヘッドを生じない方式を評価対象とし，下記の 4 方式について評価を行った．方式 1〜3 が既存方式に相当し，方式 4 が提案方式である．

なお，方式 1〜3 は，提案方式における振り分け確率 $\{q_{ij}\}$ を別の方法で設定した方式と見なすことができるため，各方式に相当する $\{q_{ij}\}$ の設定方法もあわせて記載する．

- 方式 1：単一 DB
  頻度分析攻撃への対策を何も行わない．すなわち，すべてのデータを単一 DB に登録する方式（$m = 1$, $q_{i1} = 1$）．
- 方式 2：均一振り分け
  登録データを複数 DB に振り分けるが，キーワードによらず，登録先 DB を一様ランダムに決定する方式（$q_{ij} = 1/m$）．
- 方式 3：確定的振り分け
  秘匿検索対象となる各キーワードに対し，単一の登録先 DB をあらかじめ決めておく方式（各 i について $k \in \{1, \ldots, m\}$ を一様ランダムに選択し，$q_{ik} = 1$, $q_{ij} = 0 (j \neq k)$）．
- 方式 4：確率的振り分け（提案方式）
  3 章で述べた提案方式．すなわち，秘匿検索対象となる各キーワードに対し，各 DB への振り分け確率をあらかじめ決めておく方式（$\{q_{ij}\}$ は 3.2.1 項のとおり設定）．

4.2 評価指標

本節では，本論文で安全性評価に用いた指標と，評価の中で攻撃者が行う最尤推定について説明する．

4.2.1 評価指標：攻撃者によるキーワード推定の的中率

本論文では，下記の条件下で行ったキーワード推定の的中率を評価指標として利用する．

キーワード

- キーワードは有限集合とし，要素数を l とする．
- 各キーワードの頻度が決まっており，登録データのキーワードは，前記頻度に従って発生する．

攻撃者

- 各データセンタを，キーワード推定を行う攻撃者とする．データセンタどうしは結託しない[*1]．
- 各データセンタは，秘匿検索システムのアルゴリズム，振り分け確率の設定方法を知っている．ただし，（方式 3，4 で）設定された振り分け確率は分からない．
- 各データセンタは，キーワードの頻度を知っている．ただし，保持する DB における各キーワードの出現数は分からない．
- 各データセンタは全キーワードに関する検索要求を受

[*1] 方式 1 に対する攻撃者は全データを観測できるが，方式 2〜4 に対する攻撃者は一部データしか観測できないという差が生じる．方式 1，2 における的中率の違いはこの差が要因である．

© 2019 Information Processing Society of Japan

表 7 攻撃者による推定の例
Table 7 An example of the adversary's estimation.

タグ	$\mathcal{C}_1$ 頻度	$\mathcal{C}_1$ 推定	$\mathcal{C}_1$ 的中	$\mathcal{C}_2$ 頻度	$\mathcal{C}_2$ 推定	$\mathcal{C}_2$ 的中
E_{D}(東京)	17	東京	○	17	東京	○
E_{D}(神奈川)	10	神奈川	○	7	愛知	×
E_{D}(大阪)	7	愛知	×	11	大阪	○
E_{D}(愛知)	9	大阪	×	12	神奈川	×
E_{D}(埼玉)	5	埼玉	○	5	埼玉	○
総数	48			52		

信しており，保持する DB における全タグの頻度（出現数）を観測できる．

推定方法

- 各データセンタは，l 種類のキーワードと，l 種類[*2]のタグの対応付けを，最尤推定によって推定する．

なお，的中率は「キーワード推定が的中したレコード数の，全データセンタにおける総和」を「全データセンタに登録したレコード数」で割ったもので定義する．たとえば，タグの頻度と攻撃者による推定が**表 7** のようになった場合，$\mathcal{C}_1$ で 32 レコード，$\mathcal{C}_2$ で 33 レコードが的中しているため，的中率は $(32+33)/(48+52)=0.65$ で 65%となる．

4.2.2 攻撃者による最尤推定

本項では，前項で述べた最尤推定について説明する．

方式 1 に対する最尤推定は Lacharité らが示したとおり，タグとキーワードを頻度の高い順から 1 つずつ対応付けるものである（たとえば表 7 における推定）．これは，l 種類のタグからなる集合を $\{t_i\}$ とし，タグ t_i の頻度（出現数）を u_i，キーワード w_i の頻度（確率）を p_i で表した際，各 w_i と t_i が対応すると推定した場合の尤度（推定が正しい場合に各 t_i が u_i 個観測される確率）

$$\frac{(\sum u_i)!}{\prod (u_i!)} \prod_{i=1}^{l} {p_i}^{u_i}$$

を最大とするのが，$\{p_i\}$ と $\{u_i\}$ がそれぞれ降順に並んだ場合であることを意味する．なお，方式 2，4 についても，「頻度の高いタグは頻度の高いキーワードから生成された可能性が高い」という性質は変わらないため，方式 1 と同様に最尤推定を行うことができる．

一方，方式 3 で単一のデータセンタが観測するタグは，全タグ集合に対する部分集合 $T \subset \{t_i\}$ となる．この場合，$W \subset \{w_i\}, |W| = |T|$ を満たすすべての部分集合 W について「W と T が集合として対応付く前提条件のもとで，各要素の対応付けを推定する最尤推定」を行って尤度を計算し，全体で最大尤度となったものを T に対する最尤推定とすればよい．

方式 3 に対する最尤推定の具体例として，**表 8** の頻度に対する $\mathcal{C}_1$ の推定を考える．$\mathcal{C}_1$ の観測では $|T| = 2$ であるため，$|W| = 2$ を満たす部分集合の 1 つとして $W = \{$東京, 神奈川$\}$ を考えると，東京が選択される条件付き確率が $0.106/(0.106+0.072) = 0.596$ であることから，尤度 $\frac{44!}{34!10!} \times 0.596^{34} \times 0.404^{10} = 0.006$ が得られる．この尤度をすべての W について計算すると，$W = \{$東京, 埼玉$\}$ とした場合の尤度 $\frac{44!}{34!10!} \times 0.650^{34} \times 0.350^{10} = 0.030$ が最大となるため，頻度 34 のタグを東京，頻度 10 のタグを埼玉と推定する最尤推定を得ることができる．

[*2] 出現数 0 で観測されなかったタグも仮想的に含める．

表 8 方式 3 におけるタグの頻度分布の例
Table 8 An example of frequency of tags in the scheme 3.

タグ	$\mathcal{C}_1$	$\mathcal{C}_2$
E_{D}(東京)	34	0
E_{D}(神奈川)	0	17
E_{D}(大阪)	0	18
E_{D}(愛知)	0	21
E_{D}(埼玉)	10	0
総数	44	56

なお，方式 3 に対する最尤推定は，直感的には観測されたタグの頻度比（上述の例では 34 : 10）に最も近くなるようなキーワードの組合せを選択することに相当する．また，推定の精度は $|T|$ の値に依存し，たとえば $|T|$ が小さいとタグの頻度が狭い範囲に密集する可能性があり，この場合推定の精度が悪くなってしまう．一方，$|T|$ がある程度大きい場合は，タグの頻度が適度にばらつく可能性が高いため，推定の精度が安定すると考えられる．

4.3 評価方法

的中率は，下記の手順で計算機シミュレーションを実施して評価した．なお，n は DB に登録する総レコード数を表す．

(1) 各キーワードの振り分け確率を 4.1 節のとおり設定．
(2) キーワードの頻度分布に従い，n 個のキーワードをランダムに決定．
(3) 各キーワードの振り分け確率に従い，n 個のキーワードの登録先をランダムに決定．
(4) DB ごとに，当該 DB におけるタグの頻度のみを観測した攻撃者による，キーワードの最尤推定を実施．
(5) DB ごとのキーワード的中数を合計し，n で割ったものを (3) の決定に対する的中率とする．
(6) (3) に戻ってランダム決定を 50 回繰り返し，的中率の平均値を (2) の決定に対する的中率とする．
(7) (2) に戻ってランダム決定を 50 回繰り返し，的中率の平均値を (1) の決定に対する的中率とする．
(8) (1) に戻ってランダム決定を 50 回繰り返し，的中率の平均値を評価対象方式に対する的中率とする．

なお，方式 3 に対する最尤推定は，原理的には 4.2.2 項の方法で可能だが，観測したタグの種類 $|T|$ が大きくなると，総当たりによる最尤推定が計算量的に困難となる．そこで

© 2019 Information Processing Society of Japan

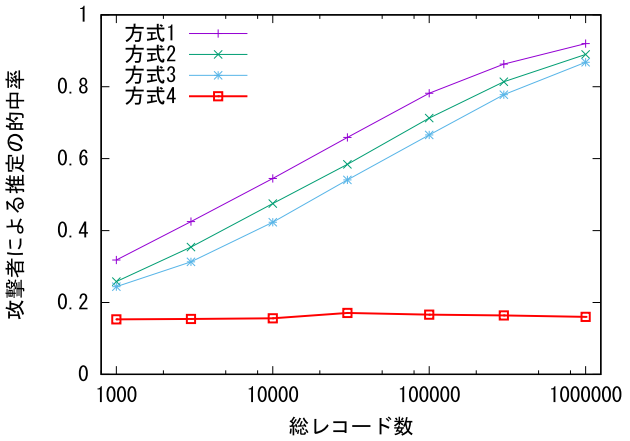


図 1 都道府県名を秘匿検索対象とした場合の安全性比較

Fig. 1 Security comparison when prefectures are designated as sensitive keywords.

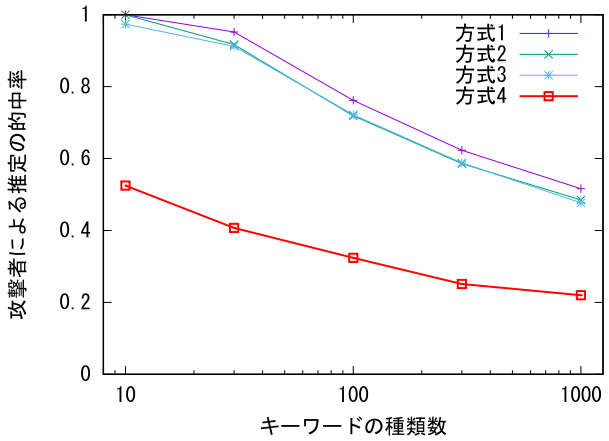


図 2 キーワード種類数を変化させた場合の的中率 (1)

Fig. 2 The ratio of correct estimation for various number of different keywords (1).

本論文では，貪欲アルゴリズムに基づく近似的な最尤推定によって的中率を評価した（詳しくは付録 A.1 に記載）．

4.4 評価結果

4.3 節までで述べた条件のもとで，DB に登録するレコード数，出現するキーワードの種類数，DB 数を変化させ，攻撃者による推定の的中率を評価した結果を記す．

4.4.1 頻度分布の実例に対する各方式の安全性比較

まずは現実に即した例として，DB の各レコードに日本居住者の情報が登録されており，このうち都道府県名を秘匿検索対象とする場合を想定し，各方式の安全性（攻撃者による都道府県推定の的中率）を比較した．なお，方式 2〜4 における DB 数は 2 個とし，都道府県の頻度分布は平成 27 年国勢調査の結果 [9] から算出した（表 4）．

評価結果は**図 1** のとおり．要点を以下に記す．

- 無対策（方式 1）の場合，たとえば 10 万レコードのうち 78%のキーワードが的中してしまう．頻度分析攻撃は現実的な脅威であるといえる．
- 単に複数 DB への分散を行うだけ（方式 2，3）では，頻度分析対策としての効果は限定的．
- 提案方式（方式 4）は，レコード数によらず，頻度分析対策として安定した効果を持つ（的中率 15〜17% [*3]）．

4.4.2 キーワードの種類数を変化させた場合

次に，頻度分布が異なる場合の的中率を見るために，下記の頻度分布それぞれについて，キーワードの種類数 l を変化させて評価を行った．なお，総レコード数は 10 万件，方式 2〜4 における DB 数は 2 個とした．

(1) 頻度が順位に反比例して減少する分布[*4]

例：$l = 5$ のとき 43.8%，21.9%，14.6%，10.9%，8.8%

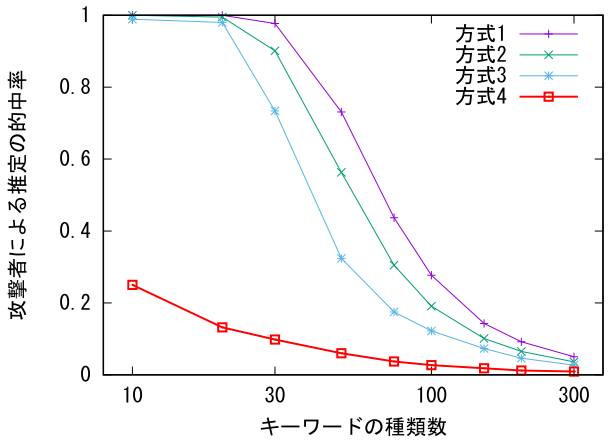


図 3 キーワード種類数を変化させた場合の的中率 (2)

Fig. 3 The ratio of correct estimation for various number of different keywords (2).

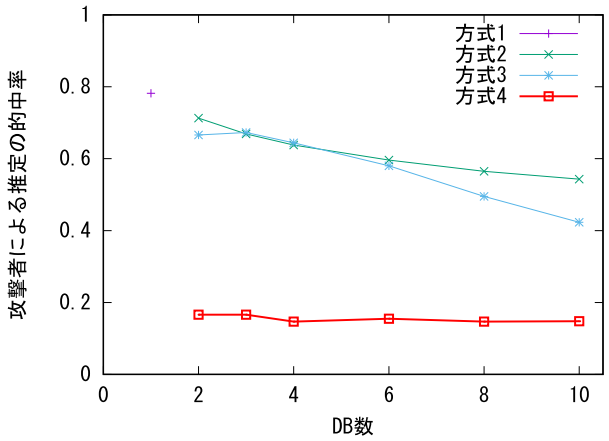


図 4 DB 数を変化させた場合の的中率

Fig. 4 The ratio of correct estimation for various number of DBs.

(2) 頻度が線形に減少する分布

例：$l = 5$ のとき 33.3%，26.7%，20.0%，13.3%，6.7%

評価結果はそれぞれ**図 2**，**図 3** のとおり．様々な頻度分

[*3] 東京の人口比率が 10.6%であるため，どんな対策をしても 10.6%の的中は可能である点に注意．

[*4] ロングテール型 DB の頻度分布としてよく見られる（Zipf 分布）．

© 2019 Information Processing Society of Japan

布において，提案方式が安定した効果を持つことが分かる．

4.4.3 DB 数を変化させた場合

提案方式における最適な DB 数を論じるために，総レコード数を 10 万件に固定したうえで，DB 数を変化させて評価を行った（方式 2，3 もあわせて評価）．なお，頻度分布については 4.4.1 項同様，都道府県のものを利用した．

評価結果は**図 4** のとおり．提案方式の効果は DB 数にほとんど依存せず，したがって 2 個の DB で十分な効果が得られることが分かる．

5. まとめ

本論文では，既存の秘匿検索システムが，検索で判明する頻度を利用した頻度分析攻撃に弱いという課題に対し，頻度撹乱の手段として複数 DB を活用し，キーワードごとに設定した振り分け確率に従って登録先 DB を選択することで，効率面でのオーバヘッドを生じることなく，頻度分析対策を実現する方式を提案した．また，頻度分析攻撃への耐性を定量評価するための指標を，最尤推定を行う攻撃者によるキーワード的中率として定義し，提案方式が頻度分析対策として安定した効果を持つことを述べた．提案方式の本質は登録先のランダム選択という簡潔な処理であるため，既存の多くの秘匿検索方式と組み合わせて使えるという利点を持つ．

今後の課題としては，本論文で定義した評価指標を，オーバヘッドを生じる他の方式にも適用して比較することや，システムを実際に構築して性能評価を行うことなどがあげられる．

参考文献

[1] Song, D.X., Wagner, D. and Perrig, A.: Practical Techniques for Searches on Encrypted Data, *Proc. IEEE Symposium on Security and Privacy*, pp.44–55, IEEE Computer Society (2000).

[2] Boneh, D., Di Crescenzo, G., Ostrovsky, R. and Persiano, G.: Public Key Encryption with Keyword Search, *Proc. Advances in Cryptology - EUROCRYPT 2004*, LNCS 3027, pp.506–522 (2004).

[3] Curtmola, R., Garay, J., Kamara, S. and Ostrovsky, R.: Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions, *Proc. 13th ACM Conference on Computer and Communications Security*, pp.79–88 (2006).

[4] Bellare, M., Boldyreva, A. and O'Neill, A.: Deterministic and Efficiently Searchable Encryption, *Proc. Advances in Cryptology - CRYPTO 2007*, LNCS 4622, pp.535–552 (2007).

[5] Kamara, S., Papamanthou, C. and Roeder, T.: Dynamic Searchable Symmetric Encryption, *Proc. 2012 ACM Conference on Computer and Communications Security*, pp.965–976 (2012).

[6] 清本晋作，田中俊昭，三宅 優，三田村好矩，乗越雅光：全文検索可能な暗号化 DB の実装・評価，コンピュータセキュリティシンポジウム 2003 論文集，Vol.2003, No.15, pp.301–306 (2003).

[7] 伊藤 隆，服部充洋，松田 規，坂井祐介，太田和夫：頻度分析耐性を持つ高速秘匿検索方式，電子情報通信学会技術研究報告，Vol.110, No.443, pp.1–6 (2011).

[8] 山岡裕司，牛田芽生恵，伊藤孝一：頻度分析を k-匿名性で緩和する検索可能共通鍵暗号，コンピュータセキュリティシンポジウム 2015 論文集，Vol.2015, No.3, pp.568–575 (2015).

[9] 総務省統計局：平成 27 年国勢調査 人口等基本集計結果 (2015)（オンライン），入手先 ⟨http://www.stat.go.jp/data/kokusei/2015/kekka.htm⟩.

[10] Lacharité, M.S. and Paterson, K.G.: A note on the optimality of frequency analysis vs. ℓ_p-optimization, Cryptology ePrint Archive, Report 2015/1158 (2015) (online), available from ⟨http://eprint.iacr.org/2015/1158⟩.

付 録

A.1 最尤推定の近似アルゴリズム

4 章で述べた，方式 3 に対する最尤推定について，本論文で利用した近似アルゴリズムを以下に記す．なお，キーワード集合を $\{w_i\}$，観測されたタグの集合を $T = \{t'_i\}$ で表し，キーワードおよびタグは頻度の降順で並んでいるものとする．

(1) タグ t'_1 がキーワード w_1 に対応付くとの仮定をおく．
(2) (1) の仮定のもとで，観測されたタグが $\{t'_1, t'_2\}$ の 2 種類だけとした場合の最尤推定を行い，尤度が最大となる $W \subset \{w_i\}$（$|W| = 2$）を決定する．
(3) 観測されたタグの種類を 1 つずつ増やしながら (2) を繰り返すことで W の要素を 1 つずつ確定させ，最終的に，観測されたタグが $\{t'_1, \ldots, t'_{|T|}\} = T$ である場合に尤度が最大となる W（$|W| = |T|$）を決定する．
(4) (1) に戻って (1)〜(3) を実行する．ただし，タグ t'_1 はキーワード w_2 に対応付くとの仮定に変更し，以降 w_1 は推定候補から外す．
(5) 同様に，タグ t'_1 の対応付けを $w_3, w_4, \ldots$ と変えながら (1)〜(3) を繰り返し，全体を通して尤度が最大となったものを最終的な最尤推定とする．

推薦文

本研究は，検索可能暗号に対する代表的な攻撃である「頻度分析攻撃」に対し，複数のデータベースを用いることで安全性を高める手法を提案している．技術的には単純な方法であるが，それにより，効率の低下を招かず，自然な形で様々な検索可能暗号方式へこの手法を適用することができる．提案手法の持つ優れた有用性・拡張性と，DICOMO2017 の発表論文の中で特に評価が高かった事実をあわせ，本論文を推薦する．

（コンピュータセキュリティ研究会主査 寺田雅之）

© 2019 Information Processing Society of Japan



伊藤 隆 （正会員）

1976 年生．2000 年東京大学工学部計数工学科卒業．2002 年同大学大学院修士課程修了．同年三菱電機株式会社入社．情報セキュリティの研究に従事．



平野 貴人 （正会員）

1982 年生．2004 年大阪教育大学教育学部教養学科数理科学専攻卒業．2006 年東京都立大学大学院理学研究科数学専攻修士課程修了．2010 年東京工業大学大学院情報理工学研究科数理・計算科学専攻博士課程修了．博士（理学）．2010 年三菱電機株式会社入社．情報セキュリティの研究に従事．電子情報通信学会会員．



森 拓海 （正会員）

1985 年生．2007 年公立はこだて未来大学システム情報科学部情報アーキテクチャ学科卒業．2009 年同大学大学院修士課程修了．同年三菱電機株式会社入社．情報セキュリティの研究に従事．



服部 充洋 （正会員）

1980 年生．2003 年京都大学工学部電気電子工学科卒業．2005 年同大学大学院修士課程修了．同年三菱電機株式会社入社．情報セキュリティの研究に従事．電子情報通信学会会員．

© 2019 Information Processing Society of Japan