情報理論的に安全な検索可能暗号の構成法について

吉澤 貴博[1]　渡邉 洋平[2]　四方 順司[1,3]

概要：検索可能暗号は情報を秘匿したまま検索が可能な方式であり, クラウドコンピューティングやゲノム解析での利用が期待されている. 中でもゲノム情報等の長期的安全性が必要な情報は情報理論的安全性が不可欠である. そこで CSS2015, SCIS2016 で我々は情報理論的に安全な共通鍵検索可能暗号を提案した. 本稿では, CSS2015 の構成法に加えて新たに構成法を提案し, それらの安全性解析を行う. 具体的には完全秘匿性より弱い安全性定義を考え, 本稿で提案する構成法や CSS2015 の構成法がどのレベルの安全性を達成するのか解析を行う. 更に, 効率性の立場から各構成法の鍵長, タグ長, 暗号文長の評価も行う.

キーワード：情報理論的安全性，検索可能暗号

Constructions of Unconditionally Secure Searchable Encryption Schemes

Takahiro Yoshizawa[1]　Yohei Watanabe[2]　Junji Shikata[1,3]

Abstract: Searchable symmetric encryption (SSE) enables us to search encrypted data with an arbitrarily chosen keyword without leaking information on the data and keyword. SSE is expected to use for, for example, cloud computing and genome analyses. In particular, privacy of genome data must be guaranteed for long periods, and therefore unconditionally secure cryptographic protocols, rather than computationally secure ones, should be used for protecting genome data. For this reason, we proposed unconditionally secure SSE schemes in CSS 2015 and SCIS 2016. In this paper, we propose new constructions of unconditionally secure SSE schemes. Specifically, we introduce weaker security notions than perfect secrecy, and rigorously analyze security of each scheme of our constructions including one proposed in CSS 2015. Furthermore, we evaluate sizes of secret keys, tags, and ciphertexts in terms of efficiency.

Keywords: Unconditional Security, Searchable Encryption

1. はじめに

1.1 背景

検索可能暗号はドキュメントを暗号化したまま検索可能な方式であり，2000 年代から研究が進められ [10], [16], クラウドコンピューティング等での利用が期待されている．検索可能暗号には大きく分けて公開鍵型（Public key Encryption with Keyword Search: PEKS）[1], [4] と共通鍵型（Symmetric Searchable Encryption: SSE）[10], [16] の 2 種類が存在し，本稿では後者を取り扱う．SSE は，ドキュメントの暗号化と検索用のタグ生成に共通の鍵が使われる方式であり，ユーザはキーワードに対応するタグを鍵を用いて生成し，サーバ側はそのタグを用いて対応したドキュメントを検索可能である．一方で，サーバに対して，検索されたキーワードの情報，また保存してある（暗号化された）ドキュメントの情報を漏らさないという安全性を持つ.

[1] 横浜国立大学 大学院環境情報学府/研究院
Graduate School of Environment and Information Sciences, Yokohama National University.
[2] 電気通信大学 大学院情報理工学研究科
Graduate School of Informatics and Engineering, The University of Electro-Communications. 日本学術振興会特別研究員 PD.
[3] 横浜国立大学 先端科学高等研究院
Institute of Advanced Sciences, Yokohama National University.

公開鍵暗号等の計算量的安全性を有する暗号技術は利便性が高い一方で，長期的（数十年以上）な安全性を保証することはできない．実際，NIST の発表 [5] によると，2,048 ビットの RSA 暗号であっても，2030 年までしか安全性を保証できないことがわかっている．

近年，クラウドコンピューティング環境で利用される，または利用が期待されている情報の中には長期的な安全性が必要な情報が存在する．例えば，ゲノム解析等の技術もクラウドコンピューティング環境での利用が期待されており [2], [17]，ゲノムデータは長期的な安全性が必要な情報の代表例である．

PEKS，SSE 両方を含む既存の検索可能暗号は全て計算量的安全性の枠組みで研究されており，長期的な安全性を保証することは難しい．

そこで既存研究として我々は CSS2015 にて，情報理論的に安全な完全秘匿性を持ち, 検索誤りと復号誤りが起こらない場合の検索可能暗号を提案した．具体的には，サーバに n 個のドキュメントが保存され, その後，高々 τ 個のキーワードを検索できる SSE を (n,τ)-SSE とし，復号誤り及び検索誤りが無く，完全秘匿であるような (n,τ)-SSE を定式化した．また, 我々は SCIS2016 で完全秘匿でない場合や復号誤り及び検索誤りがある場合のモデルを解析した．具体的には，攻撃者のアドバンテージを ϵ とし，また復号や検索が確率 δ で誤るとした場合の SSE を解析した．

本稿では CSS2015 にて提案した (n,τ)-SSE の安全性を 2 段階に分け, CSS2015 で提案した既存の構成法と新たに提案する構成法がそれぞれどちらの安全性を満たすかを解析する．また, 効率性の立場からそれぞれの構成法の鍵長, タグ長, 暗号文長を計算することで, 効率性と安全性のトレードオフを示す.

1.2 関連研究

SSE は，[10], [16] 等の初期研究段階を経て，[9] によって現在の標準的なモデル，安全性の定式化がなされた．また，既存研究で効率性の改善 [3], [7], [13] や付加的な機能 [6], [8] を持つ方式等が提案されている．

[14] は，計算量的に安全な既存方式を情報理論的安全性の観点から解析している．具体的には，ある統一的なモデルを定義し, そのモデルに [4], [12], [16] をそれぞれ当てはめ，既存の方式で利用しているハッシュ関数を情報理論的に安全なものに置き換える等の仮定を加えながら，情報理論的安全性の観点からどれだけ安全かを解析している．これはあくまで既存方式の解析であり，情報理論的に安全な検索可能暗号を提案するものではない.

2. 情報理論的に安全な検索可能暗号

2.1 モデル

本節では情報理論的に安全な検索可能暗号のモデル [18], [19] について述べる．まず簡単に本方式の流れを説明する．通信路は全て盗聴のみ可能なもの (Authenticated Channel) とする．

登録フェーズ．ドキュメントを保存するユーザは，共通鍵を用い，n 個のドキュメントを暗号化し，サーバに保存する．各ドキュメントにはキーワードが 1 つ以上紐付いているものとする．

検索フェーズ．検索を行うユーザは，共通鍵を用いて検索したいキーワードのタグを生成し，サーバに送る．サーバはそのタグを用いて検索を行い，対応するキーワードと紐付いたドキュメントの暗号文（厳密には，そのインデックス）を出力する．検索は高々 τ 回まで行え，ユーザは検索結果に応じて適宜暗号文を取り出し，共通鍵を用いて暗号文を復号できる．

ドキュメントを保存するユーザと検索するユーザは同一でも異なっていても良く，異なる場合は秘密鍵をあらかじめ（ドキュメントが暗号化される前に）共有しているものとする．この時，サーバは必ず正しくアルゴリズムを実行し，またサーバ内に保存されている暗号化されたドキュメントを改ざんすることは無いことを仮定する．ただし，暗号化されているドキュメントや検索に用いられたタグから元のドキュメントやキーワードが何であるかを推測しようとするものとする．このようなモデルはしばしば honest-but-curious モデルと呼ばれる[*1]．

より形式的に定義するため，本稿で用いる記法を定義する．特に断りがない限り，集合は筆記体のアルファベットで書き (例えば $\mathcal{X},\mathcal{Y}$)，確率変数は集合のローマ字体で書く (例えば $\mathcal{X}$ に対して X)．集合 $\mathcal{X}$ に対して，$|\mathcal{X}|$ は $\mathcal{X}$ の要素数を表し，$2^{\mathcal{X}}$ は $\mathcal{X}$ のべき集合を表す．$p\in\mathbb{N}$ に対して，$[p]:=\{1,2,\ldots,p\}$ とする．

$\mathcal{M}$，$\mathcal{W}=\{w_1,\ldots,w_d\}$，$\mathcal{K}$，$\mathcal{C}$，$\mathcal{T}$ をそれぞれドキュメント集合，キーワード集合，共通鍵集合，暗号文集合，タグ集合とし，各 w_i $(1\le i\le d)$ は辞書式順序に従うものとする．任意の部分集合 $\mathcal{D}=\{m_1,\ldots,m_n\}\subset\mathcal{M}$ に対して，$\mathcal{I}=\{id(m_1),\ldots,id(m_n)\}$ を識別子の集合とし，各 $id(m_i)$ $(1\le i\le n)$ は m_i の識別子を表す．

また，ドキュメントとキーワードの紐づきを表すために，$f:\mathcal{M}\to 2^{\mathcal{W}}\setminus\{\emptyset\}$ である写像 $f\in\mathcal{F}$ を考える．ここで，$\mathcal{F}$ は考え得る全ての f の集合（関数族）である．任意の $m\in\mathcal{M}$ に対し，$\mathcal{W}(m):=f(m)$ を m に紐づくキーワードの集合とする．また，任意の $\mathcal{D}\subset\mathcal{M}$ に対し，$\mathcal{W}(\mathcal{D}):=\bigcup_{m\in\mathcal{D}}f(m)$ とする．同様に，任意の $\mathcal{D}\subset\mathcal{M}$，任意の $w\in\mathcal{W}$ に対して，$\mathcal{D}(w):=\{id(m)\in\mathcal{I}\mid m\in\mathcal{D},w\in f(m)\}$ とする．す

[*1] サーバが，サーバ内に保存してあるドキュメントを改ざんすることは無いが，検索結果を改ざんする攻撃，すなわち検索されたキーワードに紐付いていないドキュメントを検索結果に含めたりする攻撃を仮定するモデルを，semi-honest-but-curious モデル [8] という．

なわち，D の中でキーワード w と紐付いているドキュメントの（インデックスの）集合を表している．

本方式では暗号化される n 個のドキュメントは確率分布 $P_{M_1,M_2,\ldots,M_n}$ から選ばれ，任意の異なる $i,j \in [n]$ に対して $M_i \neq M_j$ である．同様に，検索される τ 個のキーワードは確率分布 $P_{W_1,W_2,\ldots,W_\tau}$ から選ばれ，任意の異なる $i,j \in [\tau]$ に対して $W_i \neq W_j$ である．本稿では簡単化のため，これらの確率分布は一様であるとする．すなわち，任意の（異なる）$m_1, m_2, \ldots, m_i \in \mathcal{M}$ に対して，$P_{M_i=m_i|M_1=m_1,M_2=m_2,\ldots,M_{i-1}=m_{i-1}} = 1/(|\mathcal{M}| - i + 1)$ であり，任意の（異なる）$w_1, w_2, \ldots, w_i \in \mathcal{W}$ に対して，$P_{W_i=w_i|W_1=w_1,W_2=w_2,\ldots,W_{i-1}=w_{i-1}} = 1/(d-i+1)$ である．

(n,τ)-SSE Π を以下のように定義する．

定義 1 ((n,τ)-SSE)．*(n,τ)-SSE* Π は以下の 5 つのアルゴリズム *(Gen, Enc, Tag, Search, Dec)* と 6 つの有限集合 $\mathcal{M}, \mathcal{K}, \mathcal{W}, \mathcal{C}, \mathcal{T}, \mathcal{I}$ からなる．*Gen* は確率的アルゴリズム，*Enc*, *Tag*, *Search*, *Dec* は確定的アルゴリズムである．

1. $k \leftarrow Gen(n,\tau)$*:* 暗号化できるドキュメントの数 n 及び検索可能回数 τ を入力として秘密鍵 $k \in \mathcal{K}$ を出力する．
2. $(\mathcal{I}, \mathcal{ED}) \leftarrow Enc(k, \mathcal{D})$*:* 秘密鍵 k とドキュメント $\mathcal{D} = \{m_1, m_2, \ldots, m_n\} \subset \mathcal{M}$ を入力としてインデックス $\mathcal{I} = \{id(m_1), id(m_2), \ldots, id(m_n)\}$ と暗号文 $\mathcal{ED} = \{c_1, c_2, \ldots, c_n\} \subset \mathcal{C}$ を出力する．ただし，c_i を m_i の暗号文とし，k のもとで m_i から c_i が生成される．
3. $t \leftarrow Tag(k,w)$*:* 秘密鍵 k とキーワード $w \in \mathcal{W}$ を入力として，タグ $t \in \mathcal{T}$ を出力する．
4. $\mathcal{X} \leftarrow Search(\mathcal{I}, t)$*:* 識別子 $\mathcal{I}$ とタグ t を入力として，集合 $\mathcal{X} \subset \mathcal{I}$ を出力する．
5. m_i *or* $\perp \leftarrow Dec(k, c_i)$*:* k と c_i を入力として，m_i または $\perp$ を出力する．

(n,τ)-SSE Π は以下の search correctness と decryption correctness を満たすものとする．

– Search correctness: 全ての $k \leftarrow Gen(n,\tau)$，全ての $D \subset \mathcal{M}$ と $(\mathcal{I}, \mathcal{ED}) \leftarrow Enc(k, \mathcal{D})$，全ての $w \in \mathcal{W}$ に対して，以下が成り立つ．

$$\Pr\left[\mathcal{D}(w) = \mathcal{X} : \mathcal{X} \leftarrow Search(\mathcal{I}, Tag(k,w))\right] = 1.$$

これはすなわち，任意のキーワードに対して必ず正しい検索結果が出力されることを意味する．

– Decryption correctness: 全ての $k \leftarrow Gen(n,\tau)$ と全ての $\mathcal{D} = \{m_1, \ldots, m_n\} \subset \mathcal{M}$，全ての $(\mathcal{I}, \mathcal{ED} = \{c_1, \ldots, c_n\}) \leftarrow Enc(k, \mathcal{D})$，全ての $i \in \{1, \ldots, n\}$ に対して，以下が成り立つ．

$$\Pr\left[m_i \leftarrow Dec(k, c_i)\right] = 1.$$

これはすなわち，正しく暗号化された任意の暗号文に対して，必ず正しいドキュメントを復号出来ることを意味する．

2.2 安全性定義

安全性として，サーバに対する完全秘匿性を考える．すなわち，識別子 $\mathcal{I}$，暗号文 $\mathcal{ED}$，タグ $t_1, t_2, \ldots, t_\tau$ からドキュメント $\mathcal{D}$ 及び検索に用いられたキーワード $w_1, w_2, \ldots, w_\tau$ の情報が全く漏れないという安全性を考える．本稿では [18] 同様，Shannon エントロピーを用いて定式化するが，より $\mathcal{F}$ を意識した定義を考える．これは，$f \in \mathcal{F}$ によって構成法が安全性を満たす場合と満たさない場合に分かれることが有り得るからである．

定義 2 (安全性)．ある $\mathcal{F}_0 \subset \mathcal{F}$ が存在して，全ての $f \in \mathcal{F}_0$ に対して以下の条件を満たすとき，*(n,τ)-SSE* Π は *$\mathcal{F}_0$-(n,τ)-secure* であるという．

$$H(M_1, \ldots, M_n, W_1, \ldots, W_d \mid I_1, \ldots, I_n, C_1, \ldots, C_n, T_1, \ldots, T_d) = H(M_1, \ldots, M_n, W_1, \ldots, W_d).$$

特に，$\mathcal{F}_0 = \mathcal{F}$ であるとき，単に *(n,τ)-secure* であるという．

2.3 鍵長の下界の再考

[18] で導出された (n,τ)-secure SSE Π の鍵長の下界を基に，本稿で考えるモデルの下で改めて鍵長の下界を導出する．ただし，以下の下界は最も強い安全性（すなわち $\mathcal{F}$-(n,τ)-security）に対して導出されたものであることに留意されたい．従って，より弱いクラスの安全性（すなわち $\mathcal{F}_0$-(n,τ)-security）を達成する方式では，以下の下界よりも効率的な鍵長を実現できる可能性がある．

[18] ではドキュメントとキーワードの確率変数は独立に同一の確率分布に従うとしていたが，本稿では 2.1 節で述べたような $P_{M_1,M_2,\ldots,M_n}$ 及び $P_{W_1,W_2,\ldots,W_\tau}$ を考えるため，そこを考慮した上で鍵長の下界を導出する．証明は [18] と同様に行えるため省略する．

定理 1. 任意の *(n,τ)-secure SSE* Π に対して，以下が成り立つ．

$$H(K) \geq H(M_1, \ldots, M_n) + H(W_1, \ldots, W_\tau) = \sum_{i=1}^{n} H(M_i \mid M_1, \ldots, M_{i-1}) + \sum_{i=1}^{\tau} H(W_i \mid W_1, \ldots, W_{i-1}).$$

ここで，次のような $\mathcal{F}_0$-(n,τ)-SSE の構成法の最適性を定義する．

定義 3. *$\mathcal{F}_0$-(n,τ)-secure SSE* Π の構成法が定理 *1* の下界の等号を満たす時，その構成法は最適であるという．

3. 構成法

本節では，2 種類の構成法を提案する．まず，[18] で提案した構成法の安全性解析を厳密に行う．結果として，全

ての $f \in \mathcal{F}$ に対しては安全性を満たすわけではなく，ある $\mathcal{F}_0 \subset \mathcal{F}$ に対して $\mathcal{F}_0$-(n,τ)-secure であることを示す．具体的なクラス $\mathcal{F}_0$ に関しては後ほど詳述する．次に，既存の計算量的に安全な SSE の構成法 [9] を基にした構成法を示す．

3.1 構成法 [18]

$\mathbb{F}_{2^\lambda}$ を要素数 $2^\lambda(> n)$ 個の有限体とし，$\mathbb{Z}_\tau := \{0,1,\ldots,\tau-1\}$ とする．一般性を失わずに，$\mathcal{W} = \{w_1,\ldots,w_\tau\}$ の各元はそれぞれ $\mathbb{Z}_\tau$ の各元に $w_i \mapsto i-1$ の対応で符号化されているとする．従って，$\mathcal{W} = \mathbb{Z}_\tau$ であり，また $\mathcal{M} = \mathcal{C} = \mathbb{F}_{2^\lambda}$，$\mathcal{T} = \mathbb{Z}_\tau$ とする．また，$\mathcal{I} = \prod_{i=1}^{n} \left(\{0,1\}^{\lfloor \log n \rfloor + 1} \times \mathcal{Y}_i\right)$ であり，$\mathcal{Y}_i$ は以下で定義する．また，$\Sigma = \{\sigma\}$ を $\mathbb{Z}_\tau$ 上の置換からなる集合とする．すなわち，

$$\sigma = \begin{pmatrix} 0 & 1 & \cdots & \tau-1 \\ \sigma(0) & \sigma(1) & \cdots & \sigma(\tau-1) \end{pmatrix}.$$

また，この構成法では，以下のクラス $\mathcal{F}_0 \subset \mathcal{F}$ を考える: 全ての $f \in \mathcal{F}_0$ に対して，以下の条件を満たす．

(i) ある $k \in [d]$ が存在して，全ての $m \in \mathcal{M}$ に対して，$|f(m)| = k$.

(ii) ある $\ell \in [n]$ が存在して，$|\{m \in M \mid w \in f(m)\}| = \ell$.

すなわち，ドキュメントにひもづくキーワードの数は全て等しく，また各キーワードが紐づくドキュメント数も全て等しいような f の族が $\mathcal{F}_0$ である．

[18] における構成法は以下の通り．

- $k \leftarrow Gen(1^\lambda, \tau, n)$: 集合 Σ よりランダムに置換 σ を選ぶ．全ての $i \in \{1,\ldots,\tau\}$ に対して，$a_i = \sigma(w_i)$ とし，$(b_1,\ldots,b_n) \in \mathbb{F}_{2^\lambda}^n$ を一様ランダムに選ぶ．$k = (a_1,\ldots,a_\tau,b_1,\ldots,b_n)$ を出力する．
- $(\mathcal{I}, \mathcal{ED}) \leftarrow Enc(k, \mathcal{D} = \{m_1, m_2, \ldots, m_n\})$: 各 $j \in [n]$ に対して，以下を行う．
  (a) $CT_j = m_j + b_j$ を計算する．
  (b) $\mathcal{Y}_j = \{a_i \mid w_i \in f(m_j)\}$ を計算する[*2].
  (c) $c_j = (j, ct_j)$，また $id(m_j) = (j, \mathcal{Y}_j)$ とする．ここで $j \in \{0,1\}^{\lfloor \log n \rfloor + 1}$ である．
  $\mathcal{I} = \{id(m_1), id(m_2), \ldots, id(m_n)\}$ と $\mathcal{ED} = \{c_1, c_2, \ldots, c_n\}$ を出力する．
- $t \leftarrow Tag(k, w)$: w の $\mathcal{W}$ における順序を i 番目とし，$t = a_i$ を出力する．
- $\mathcal{X} \leftarrow Search(\mathcal{I}, t)$: $\mathcal{X} = \{i \mid (i, \mathcal{Y}_i) \in \mathcal{I}, t \in \mathcal{Y}_i\}$ を出力する．
- $m_i \leftarrow Dec(k, c_i)$: $c_i = (i, ct_i)$ とする．$m_i = ct_i - b_i$ を出力する．

定理 2. 上記の Π の構成法は上記の $\mathcal{F}_0$ に対して $\mathcal{F}_0$-(n,τ)-*secure* である．

証明. 以下では，簡単のため，$f(m_1), f(m_2), \ldots, f(m_n)$ のそれぞれに高々合計 ℓ 回しか同じキーワードが重複しない $\mathcal{D}$ が暗号化された場合について考える．すなわち，全ての $w \in \mathcal{W}$ に対し，$|\mathcal{L}(w)| := |\{i \mid m_i \in \mathcal{D}, w \in f(m_i)\}| \le \ell$ である．また更に解析を簡単にするため，全ての $w \in f(m_n)$ に対して，$|\{i \mid m_i \in \mathcal{D}, w \in f(m_i)\}| < \ell$ とする．すなわち，m_n に紐づくキーワードは高々 $\ell - 1$ 回までしか重複しないとする．すると，$|\{\mathcal{L}(w) = \ell \mid w \in \mathcal{W}\}| = j$ である時，$P_{M_1,M_2,\ldots,M_n}$ が一様であることから，上記の条件を満たす $\mathcal{D}$ に対して以下が成り立つ．

$$Pr[I_1 = id(m_1), I_2 = id(m_2), \ldots, I_n = id(m_n)] = \frac{1}{\binom{\tau}{k}\binom{\tau}{k}\cdots\binom{\tau-j}{k}}.$$

ここで，簡単のため上記の場合を考えるが，そうでない場合でも同様の議論が成り立つことに留意されたい．

上記構成法では，各暗号文 ct_j はワンタイムパッドとなっているため，明らかに $H(M_1,\ldots,M_n|C_1,\ldots,C_n) = H(M_1,\ldots,M_n)$ である．従って，全ての $id(m_1),\ldots,id(m_n),ct_1,\ldots,ct_n$ に対して以下も成り立つ．

$$\Pr[id(m_1),\ldots,id(m_n),ct_1,\ldots,ct_n] = \Pr[id(m_1),\ldots,id(m_n)] + \Pr[ct_1,\ldots,ct_n]. \quad (1)$$

ここで，全ての $ct_1,\ldots,ct_n$ に対して $\Pr[ct_1,\ldots,ct_n] = 1/(2^\lambda)^n$ である．また，任意の $j \in [\tau]$，全ての $id(m_1),\ldots,id(m_n),t_1,\ldots,t_\tau,w_1,\ldots,w_j$ に対して，

$$\Pr[t_1,\ldots,t_\tau,w_1,\ldots,w_j \mid id(m_1),\ldots,id(m_n)] = \Pr[t_1,\ldots,t_\tau,w_1,\ldots,w_j] \quad (2)$$
$$= \Pr[t_1,\ldots,t_\tau] + \Pr[w_1,\ldots,w_j]. \quad (3)$$

が成り立つ．ここで，(5) は f が満たす条件 (i) 及び (ii) から成り立ち，また (6) は置換 σ がランダムに選ばれていることから成り立つ．全ての $t_1,\ldots,t_\tau$ に対して $\Pr[t_1,\ldots,t_\tau] = 1/\tau!$ であり，全ての $w_1,\ldots,w_j$ に対して $\Pr[w_1,\ldots,w_j] = 1/\tau(\tau-1)\cdots(\tau-j+1)$ である．従って，全ての $id(m_1),\ldots,id(m_n),ct_1,\ldots,ct_n,t_1,\ldots,t_\tau,w_1,\ldots,w_j$ に対して，以下が成り立つ．

$$\Pr[id(m_1),\ldots,id(m_n),ct_1,\ldots,ct_n,t_1,\ldots,t_\tau,w_1,\ldots,w_j] = \frac{1}{\binom{\tau}{k}\binom{\tau}{k}\cdots\binom{\tau-j}{k}} \cdot \frac{1}{(2^\lambda)^n} \cdot \frac{1}{\tau!} \cdot \frac{1}{\tau(\tau-1)\cdots(\tau-j+1)}.$$

$Z := (I_1,\ldots,I_n,C_1,\ldots,C_n,T_1,\ldots,T_\tau)$ とする．
定義 2 における式の左辺を以下のように書き直す．

$$H(M_1,\ldots,M_n,W_1,\ldots,W_d \mid Z) = \sum_{i=1}^{\tau} H(W_i \mid Z,W_1,\ldots,W_{i-1}) + \sum_{i=1}^{n} H(M_i \mid Z,W_1,\ldots,W_\tau,M_1,\ldots,M_{i-1}).$$

まず，任意の $i \in [\tau]$ に対して，$H(W_i \mid Z,W_1,\ldots,W_{i-1}) = H(W_i \mid W_1,\ldots,W_{i-1})$ であるこ

[*2] 鍵を持つユーザならば，$(a_1,\ldots,a_\tau)$ の並びから，各 a_i がどのキーワードに対応しているか知ることができることに留意する．

とを示す．$H(W_i|Z,W_1,\ldots W_{i-1})$ に関して，次が成り立つ．

$$
\begin{aligned}
&H(W_i|Z,W_1,\ldots W_{i-1})\\
&=-\sum_{w_1\in\mathcal{W}}\cdots\sum_{w_i\in\mathcal{W}\setminus\{w_j\}_{j=1}^{i-1}}\sum_{z\in\mathcal{Z}}\\
&\quad\Pr[W_1=w_1,\ldots,W_{i-1}=w_{i-1},Z=z]\\
&\quad\quad\Pr[W_i=w_i\mid W_1=w_1,\ldots,W_{i-1}=w_{i-1},Z=z]\\
&\quad\quad\quad\log\Pr[W_i=w_i\mid W_1=w_1,\ldots,W_{i-1}=w_{i-1},Z=z]\\
&=-\sum_{w_1\in\mathcal{W}}\cdots\sum_{w_i\in\mathcal{W}\setminus\{w_j\}_{j=1}^{i-1}}\sum_{z\in\mathcal{Z}}\\
&\quad\frac{1}{\binom{\tau}{k}\binom{\tau}{k}\cdots\binom{\tau-j}{k}}\cdot\frac{1}{(2^\lambda)^n}\cdot\frac{1}{\tau!}\\
&\quad\quad\cdot\frac{1}{\tau(\tau-1)\cdots(\tau-i+2)}\cdot\frac{1}{\tau-i+1}\cdot\log\frac{1}{\tau-i+1}\\
&=\log(\tau-i+1).
\end{aligned}
$$

また，

$$
\begin{aligned}
&H(W_i\mid W_1,\ldots,W_{i-1})\\
&=-\sum_{w_1\in\mathcal{W}}\cdots\sum_{w_i\in\mathcal{W}\setminus\{w_j\}_{j=1}^{i-1}}\\
&\quad\Pr[W_1=w_1,\ldots,W_{i-1}=w_{i-1}]\\
&\quad\quad\Pr[W_i=w_i\mid W_1=w_1,\ldots,W_{i-1}=w_{i-1}]\\
&\quad\quad\quad\log\Pr[W_i=w_i\mid W_1=w_1,\ldots,W_{i-1}=w_{i-1}]\\
&=-\sum_{w_1\in\mathcal{W}}\cdots\sum_{w_i\in\mathcal{W}\setminus\{w_j\}_{j=1}^{i-1}}\\
&\quad\frac{1}{\tau\cdots(\tau-i+2)}\cdot\frac{1}{\tau-i+1}\cdot\log\frac{1}{\tau-i+1}\\
&=\log(\tau-i+1).
\end{aligned}
$$

従って，任意の $i\in[\tau]$ に対して，$H(W_i\mid Z,W_1,\ldots,W_{i-1})=H(W_i\mid W_1,\ldots,W_{i-1})$.

次に，任意の $i\in[n]$ に対して，$H(M_i\mid Z,W_1,\ldots,W_\tau,M_1,\ldots,M_{i-1})=H(W_i\mid W_1,\ldots,W_\tau,M_1,\ldots,M_{i-1})$ であることを示す．まず，先の議論と同様に，全ての $id(m_1),\ldots,id(m_n),ct_1,\ldots,ct_n,t_1,\ldots,t_\tau,w_1,\ldots,w_\tau,m_1,\ldots,m_j$ に対して，以下が成り立つ．

$$
\begin{aligned}
&\Pr[id(m_1),\ldots,id(m_n),ct_1,\ldots,ct_n,\\
&\qquad\qquad t_1,\ldots,t_\tau,w_1,\ldots,w_\tau,m_1,\ldots,m_j]\\
&=\frac{1}{\binom{\tau}{k}\binom{\tau}{k}\cdots\binom{\tau-j}{k}}\cdot\frac{1}{(2^\lambda)^n}\cdot\frac{1}{\tau!}\cdot\frac{1}{\tau!}\cdot\frac{1}{(2^\lambda)^n\cdots((2^\lambda)^n-j+1)}.
\end{aligned}
$$

従って，先の議論と同様に $H(M_i\mid Z,W_1,\ldots,W_d,M_1,\ldots,M_{i-1})=\log(2^\lambda-i+1)$ であることを示すことができる．一方で，$H(M_i\mid W_1,\ldots,W_\tau,M_1,\ldots,M_{i-1})=\log(2^\lambda-i+1)$ である．従って，任意の $i\in[n]$ に対して，$H(M_i\mid Z,W_1,\ldots,W_\tau,M_1,\ldots,M_{i-1})=H(W_i\mid W_1,\ldots,W_\tau,M_1,\ldots,M_{i-1})$.

以上より，$H(M_1,\ldots,M_n,W_1,\ldots,W_\tau\mid I_1,\ldots,I_n,C_1,\ldots,C_n,T_1,\ldots,T_\tau)=H(M_1,\ldots,M_n,W_1,\ldots,W_\tau)$ となるため，$\mathcal{F}_0$-(n,τ)-secure である． □

3.2 [9] を基にした構成法

[9] を基にした構成法では，$\mathbb{F}_{2^\lambda}$ を要素数 $2^\lambda(>n)$ 個の有限体とし，また d を素数とし，$\mathcal{M}=\mathcal{C}=\mathbb{F}_{2^\lambda}$，$\mathcal{W}=\{0,1\}^{\log d}$ ビットのビット列とし，$\mathcal{T}=\{0,1\}^{\log(dn^2)}$ とする．$\mathcal{I}=\prod_{i=1}^n\left(\{0,1\}^{\lfloor\log n\rfloor+1}\times\mathcal{Y}_i\right)$ であり，$\mathcal{Y}_i$ は以下で定義する．また，$s=\max|\mathcal{W}(m_i)|\cdot n$ $(1\le i\le n)$ とする．また，$\Sigma=\{\sigma\}$ を $\{0,1\}^{\log(dn^2)}$ 上の置換からなる集合とする．

[9] を基にした構成法は以下の通り．

- $k\leftarrow Gen(\tau,n)$: 集合 Σ よりランダムに置換 σ を選ぶ．任意の $i\in\{1,\ldots,d\}$ に対して，$a_{i,j}=\sigma(w_i||0^n||j)$ とし，$(b_1,\ldots,b_n)\in\mathbb{F}_{2^\lambda}^n$ を一様ランダムに選ぶ．
  $k=(a_{1,1},\ldots,a_{i,j},\ldots,a_{d,n},b_1\ldots,b_n)$ $(1\le i\le d,1\le j\le n)$ を出力する．
- $(\mathcal{I},\mathcal{ED})\leftarrow Enc(k,m_1,\ldots,m_n)$: 次に，各 $k\in\{1,\ldots,n\}$ に対して，以下を行う．
  (a) m_k の暗号文 $CT_k=m_k+b_k$ を計算する．
  (b) $\mathcal{Y}_j=\{\sigma(w_i||0^n||j)\mid w_i\in\mathcal{W}(m_j)\}$ を計算する．
  (c) $c_j=(j,CT_j)$，また $id(m_j)=(j,\mathcal{Y}_j)$ とする．ここで $j\in\{0,1\}^{\lfloor\log n\rfloor+1}$ とする．
  (d) $s'=\sum_{w\in W(\mathcal{D})}|D(w)|$ とし，$s'<s$ ならば全ての $id(m_i)$ に対して以下を行う．
    (i) e を $id(m_i)$ にひもづいているタグの数とする．$\sigma(0^{\lfloor\log d\rfloor+1}||i||\ell)$ $(1\le\ell\le max-c)$ を $\mathcal{Y}_i$ に追加する．
  $\mathcal{I}=\{id(m_1),\ldots,id(m_n)\}$ と $\mathcal{ED}=\{c_1,\ldots,c_n\}$ を出力する．
- $t\leftarrow Tag(k,w)$: w の $\mathcal{W}$ における順序を i 番目とし，$t=\{\sigma(w_i||0^n||1),\ldots,\sigma(w_i||0^n||n)\}$ を出力する．t の要素をそれぞれ $t=\{t_1,\ldots,t_n\}$ とする．
- $\mathcal{X}\leftarrow Search(\mathcal{I},t)$: $\mathcal{X}=\{id(m_\ell)\in\mathcal{I}\ (1\le\ell\le n)\mid t_i\in\mathcal{Y}_\ell\}$ $(1\le i\le n)$ を出力する．
- $m_i\leftarrow Dec(k,c_i)$: $c_i=ct_i$ とする．$m_i=ct_i-b_i$ を出力する．

定理 3. 上記の Π の構成法は (n,τ)-*secure* である．

証明. 上記の構成法ではドキュメントにひもづくキーワードが同じか異なるかに関わらずタグの値は全て異なり，全てのドキュメントがひもづくタグの数は等しくなっている．1 つのドキュメントにひもづくタグの数は $\max|\mathcal{W}(m_i)|$ である．$p=\max|\mathcal{W}(m_i)|$ とする．このとき，以下の式が成り立つ．

$$
\begin{aligned}
&Pr[I_1=id(m_1),I_2=id(m_2),\ldots,I_n=id(m_n)]\\
&=\frac{1}{(dn^2)\cdot(dn^2-1)\cdots(dn^2-np+1)}.
\end{aligned}
$$

上記構成法では，各暗号文 ct_j はワンタイムパッドとなっているため，明らかに $H(M_1,\ldots,M_n|C_1,\ldots,C_n)=H(M_1,\ldots,M_n)$ である．従って，全ての $id(m_1),\ldots,id(m_n),ct_1,\ldots,ct_n$ に対して以下も成り立つ．

$$\Pr[id(m_1),\ldots,id(m_n),ct_1,\ldots,ct_n]$$

$$= \Pr[id(m_1), \ldots, id(m_n)] + \Pr[ct_1, \ldots, ct_n]. \quad (4)$$

ここで，全ての $ct_1, \ldots, ct_n$ に対して $\Pr[ct_1, \ldots, ct_n] = 1/(2^\lambda)^n$ である．また，任意の $j \in [\tau]$，全ての $id(m_1), \ldots, id(m_n), t_1, \ldots, t_\tau, w_1, \ldots, w_j$ に対して，

$$\begin{aligned}\Pr[t_1, \ldots, t_\tau, w_1, \ldots, w_j \mid id(m_1), \ldots, id(m_n)] \\ = \Pr[t_1, \ldots, t_\tau, w_1, \ldots, w_j] \quad (5) \\ = \Pr[t_1, \ldots, t_\tau] + \Pr[w_1, \ldots, w_j]. \quad (6)\end{aligned}$$

が成り立つ．ここで，(5) はタグの値が全て異なることと，ドキュメントにひもづくタグの数が全て同じであることから成り立ち，また (6) は置換 σ がランダムに選ばれていることから成り立つ．全ての $t_1, \ldots, t_d$ に対して $\Pr[t_1, \ldots, t_d] = 1/dn^2 \cdots (dn^2 - d + 1)$ であり，全ての $w_1, \ldots, w_j$ に対して $\Pr[w_1, \ldots, w_j] = 1/d(d-1)\cdots(d-j+1)$ である．従って，全ての $id(m_1), \ldots, id(m_n), ct_1, \ldots, ct_n, t_1, \ldots, t_d, w_1, \ldots, w_j$ に対して，以下が成り立つ．

$$\begin{aligned}&\Pr[id(m_1), \ldots, id(m_n), ct_1, \ldots, ct_n, t_1, \ldots, t_d, w_1, \ldots, w_j] \\ &= \frac{1}{(dn^2) \cdot (dn^2 - 1) \cdots (dn^2 - np + 1)} \cdot \frac{1}{(2^\lambda)^n} \\ &\quad \cdot \frac{1}{d!} \cdot \frac{1}{d(d-1)\cdots(d-j+1)}.\end{aligned}$$

$Z := (I_1, \ldots, I_n, C_1, \ldots, C_n, T_1, \ldots, T_d)$ とする．定義 2 における式の左辺を以下のように書き直す．

$$\begin{aligned}&H(M_1, \ldots, M_n, W_1, \ldots, W_d \mid Z) \\ &= \sum_{i=1}^{\tau} H(W_i \mid Z, W_1, \ldots, W_{i-1}) \\ &\quad + \sum_{i=1}^{n} H(M_i \mid Z, W_1, \ldots, W_d, M_1, \ldots, M_{i-1}).\end{aligned}$$

まず，任意の $i \in [d]$ に対して，$H(W_i \mid Z, W_1, \ldots, W_{i-1}) = H(W_i \mid W_1, \ldots, W_{i-1})$ であることを示す．

$$\begin{aligned}&H(W_i|Z, W_1, \ldots W_{i-1}) \\ &= -\sum_{w_1 \in \mathcal{W}} \cdots \sum_{w_i \in \mathcal{W} \setminus \{w_j\}_{j=1}^{i-1}} \sum_{z \in \mathcal{Z}} \\ &\quad \Pr[W_1 = w_1, \ldots, W_{i-1} = w_{i-1}, Z = z] \\ &\quad \Pr[W_i = w_i \mid W_1 = w_1, \ldots, W_{i-1} = w_{i-1}, Z = z] \\ &\quad \log \Pr[W_i = w_i \mid W_1 = w_1, \ldots, W_{i-1} = w_{i-1}, Z = z] \\ &= -\sum_{w_1 \in \mathcal{W}} \cdots \sum_{w_i \in \mathcal{W} \setminus \{w_j\}_{j=1}^{i-1}} \sum_{z \in \mathcal{Z}} \\ &\quad \frac{1}{(dn^2) \cdots (dn^2 - np + 1)} \\ &\quad \cdot \frac{1}{(dn^2) \cdots (dn^2 - d + 1) \cdot (2^\lambda)^n \cdot d \cdots (d - i + 2)} \\ &\quad \cdot \frac{1}{(d - i + 1)} \log \frac{1}{d - i + 1} \\ &= \log(d - i + 1).\end{aligned}$$

また，定理 3.2 の証明と同様に任意の $i \in [d]$ に対して，

$$\begin{aligned}&H(W_i \mid W_1, \ldots, W_{i-1}) \\ &= \log(d - i + 1).\end{aligned}$$

従って，任意の $i \in [n]$ に対して

$H(W_i \mid Z, W_1, \ldots, W_{i-1}) = H(W_i \mid W_1, \ldots, W_{i-1})$ である．

まず，先の議論と同様に，全ての $id(m_1), \ldots, id(m_n), ct_1, \ldots, ct_n, t_1, \ldots, t_\tau, w_1, \ldots, w_\tau, m_1, \ldots, m_j$ に対して，以下が成り立つ．

$$\begin{aligned}&\Pr[id(m_1), \ldots, id(m_n), ct_1, \ldots, ct_n, \\ &\qquad t_1, \ldots, t_\tau, w_1, \ldots, w_\tau, m_1, \ldots, m_j] \\ &= \frac{1}{\binom{\tau}{k}\binom{\tau}{k}\cdots\binom{\tau-j}{k}} \cdot \frac{1}{(2^\lambda)^n} \cdot \frac{1}{\tau!} \cdot \frac{1}{\tau!} \cdot \frac{1}{2^\lambda \cdots (2^\lambda - j + 1)}.\end{aligned}$$

従って，先の議論と同様に $H(M_i \mid Z, W_1, \ldots, W_d, M_1, \ldots, M_{i-1}) = \log(2^\lambda - i + 1)$ であることを示すことができる．

次に，任意の $i \in [n]$ に対して，

$H(M_i \mid Z, W_1, \ldots, W_d, M_1, \ldots, M_{i-1}) = H(W_i \mid W_1, \ldots, W_d, M_1, \ldots, M_{i-1})$ であることを示す．

$$\begin{aligned}&H(M_i \mid Z, W_1, \ldots, W_d, M_1, \ldots, M_{i-1}) \\ &= -\sum_{w_1 \in \mathcal{W}} \cdots \sum_{w_d \in \mathcal{W} \setminus \{w_j\}_{j=1}^{d-1}} \sum_{z \in \mathcal{Z}} \sum_{m_1 \in \mathcal{M}} \cdots \sum_{m_i \in \mathcal{M} \setminus \{m_j\}_{j=1}^{i-1}} \\ &\quad \Pr[W_1 = w_1, \ldots, W_d = w_d, M_1 = m_1, \ldots, M_{i-1} = m_{i-1}, Z = z] \\ &\quad \Pr[W_i = w_i \mid W_1 = w_1, \ldots, W_d = w_d, \\ &\qquad M_1 = m_1, \ldots, M_{i-1} = m_{i-1}, Z = z] \\ &\quad \log \Pr[M_i = w_i \mid W_1 = w_1, \ldots, W_d = w_d, \\ &\qquad M_1 = m_1, \ldots, M_{i-1} = m_{i-1}, Z = z] \\ &= -\sum_{w_1 \in \mathcal{W}} \cdots \sum_{w_d \in \mathcal{W} \setminus \{w_j\}_{j=1}^{d-1}} \sum_{z \in \mathcal{Z}} \sum_{m_1 \in \mathcal{M}} \cdots \sum_{m_i \in \mathcal{M} \setminus \{m_j\}_{j=1}^{i-1}} \\ &\quad \frac{1}{(dn^2) \cdots (dn^2 - np + 1)} \\ &\quad \cdot \frac{1}{(dn^2) \cdots (dn^2 - d + 1) \cdot (2^\lambda)^n \cdot d! \cdot 2^\lambda \cdots (2^\lambda - i + 2)} \\ &\quad \cdot \frac{1}{(2^\lambda - i + 1)} \log \frac{1}{2^\lambda - i + 1} \\ &= \log(2^\lambda - i + 1).\end{aligned}$$

また，定理の証明と同様に任意の $i \in [d]$ に対して，

$$\begin{aligned}&H(M_i \mid W_1, \ldots, W_d, M_1, \ldots, M_{i-1}) \\ &= \log(2^\lambda - i + 1).\end{aligned}$$

従って，任意の $i \in [n]$ に対して

$H(M_i \mid Z, W_1, \ldots, W_d, M_1, \ldots, M_{i-1}) = H(W_i \mid W_1, \ldots, W_d, M_1, \ldots, M_{i-1})$ である．

以上より，$H(M_1, \ldots, M_n, W_1, \ldots, W_d \mid I_1, \ldots, I_n, C_1, \ldots, C_n, T_1, \ldots, T_d) = H(M_1, \ldots, M_n, W_1, \ldots, W_d)$ となるため，(n, τ)-secure である． □

4. 構成法の評価

4.1 構成法 [18]

まず一つ目の構成法の鍵長，タグ長，暗号文長の評価を行う．鍵長は $(n\lambda + \tau \log \tau)$ bit，タグ長は $\log \tau$ bit，暗号文長は λ bit である．

続いて，秘密鍵のエントロピーの評価する．一つ目の構

成法における秘密鍵 $a_1,\ldots,a_\tau,b_1,\ldots,b_n$ の確率変数をそれぞれ $A_1,\ldots,A_\tau,B_1,\ldots,B_n$ とする．また，これらはそれぞれ $\mathbb{F}_\tau$，$\mathbb{F}_{2^\lambda}$ から独立かつ一様に選ばれることに留意すると，

$$
\begin{aligned}
&H(K)=H(A_1,\ldots,A_\tau,B_1,\ldots,B_n)\\
&=-\sum_{a_1\in\mathbb{F}_\tau}\cdots\sum_{a_\tau\in\mathbb{F}_\tau\setminus\{a_j\}_{j=1}^{\tau-1}}\sum_{b_1\in\mathbb{F}_{2^\lambda}}\cdots\sum_{b_n\in\mathbb{F}_{2^\lambda}}\\
&\quad\Pr[A_1=a_1,\ldots,A_\tau=a_\tau,B_1=b_1,\ldots,B_n=b_n]\\
&\qquad\log\Pr[A_1=a_1,\ldots,A_\tau=a_\tau,B_1=b_1,\ldots,B_n=b_n]\\
&=-\sum_{a_1\in\mathbb{F}_\tau}\cdots\sum_{a_\tau\in\mathbb{F}_\tau\setminus\{a_j\}_{j=1}^{\tau-1}}\sum_{b_1\in\mathbb{F}_{2^\lambda}}\cdots\sum_{b_n\in\mathbb{F}_{2^\lambda}}\frac{1}{\tau!\cdot(2^\lambda)^n}\log\frac{1}{\tau!\cdot(2^\lambda)^n}\\
&=\log(\tau!\cdot(2^\lambda)^n).
\end{aligned}
$$

一方, 次が成り立つ.

$$
\begin{aligned}
&H(M_1,\ldots M_n)+H(W_1,\ldots,W_\tau)\\
&=-\sum_{m_1\in\mathbb{F}_{2^\lambda}}\cdots\sum_{m_n\in\mathbb{F}_{2^\lambda}\setminus\{m_j\}_{j=1}^{n-1}}\\
&\quad\Pr[M_1=m_1,\ldots,M_n=m_n]\log\Pr[M_1=m_1,\ldots,M_n=m_n]\\
&\quad-\sum_{w_1\in\mathbb{F}_\tau}\cdots\sum_{w_\tau\in\mathbb{F}_\tau\setminus\{w_j\}_{j=1}^{\tau-1}}\\
&\qquad\Pr[W_1=w_1,\ldots,W_\tau=w_\tau]\log\Pr[W_1=w_1,\ldots,W_\tau=w_\tau]\\
&=-\sum_{m_1\in\mathbb{F}_{2^\lambda}}\cdots\sum_{m_n\in\mathbb{F}_{2^\lambda}\setminus\{m_j\}_{j=1}^{n-1}}\\
&\qquad\frac{1}{(2^\lambda)\cdots((2^\lambda)-n+1)}\log\frac{1}{(2^\lambda)\cdots((2^\lambda)-n+1)}\\
&\qquad-\sum_{w_1\in\mathbb{F}_\tau}\cdots\sum_{w_\tau\in\mathbb{F}_\tau\setminus\{w_j\}_{j=1}^{\tau-1}}\frac{1}{\tau!}\log\frac{1}{\tau!}\\
&=\log(2^\lambda)\cdots((2^\lambda)-n+1)+\log\tau!\\
&=\log(\tau!\cdot(2^\lambda)\cdots((2^\lambda)-n+1)).
\end{aligned}
$$

以上より，そこまで大きな差ではないものの $H(K)>H(M_1,\ldots M_n)+H(W_1,\ldots,W_\tau)$ であるため, 定義 3 を満たしておらず，最適ではない.

4.2 [9] を基にした構成法

まず二つ目の構成法の鍵長, タグ長, 暗号文長の評価を行う．鍵長は $(n\lambda+dn\log(dn^2))$ bit, タグ長は $\log(dn^2)$ bit, 暗号文長は λ bit である.

続いて，秘密鍵のエントロピーの評価する．二つ目の構成法における秘密鍵 $a_1,\ldots,a_\tau,b_1,\ldots,b_n$ の確率変数をそれぞれ $A_1,\ldots,A_\tau,B_1,\ldots,B_n$ とする.

$$
\begin{aligned}
&H(K)=H(A_1,\ldots,A_\tau,B_1,\ldots,B_n)\\
&=-\sum_{a_1\in\{0,1\}^{\log(dn^2)}}\cdots\sum_{a_\tau\in\{0,1\}^{\log(dn^2)}\setminus\{a_j\}_{j=1}^{d-1}}\sum_{b_1\in\mathbb{F}_{2^\lambda}}\cdots\sum_{b_n\in\mathbb{F}_{2^\lambda}}\\
&\quad\Pr[A_1=a_1,\ldots,A_\tau=a_\tau,B_1=b_1,\ldots,B_n=b_n]\\
&\qquad\log\Pr[A_1=a_1,\ldots,A_d=a_d,B_1=b_1,\ldots,B_n=b_n]\\
&=-\sum_{a_1\in\{0,1\}^{\log(dn^2)}}\cdots\sum_{a_d\in\{0,1\}^{\log(dn^2)}\setminus\{a_j\}_{j=1}^{d-1}}\sum_{b_1\in\mathbb{F}_{2^\lambda}}\cdots\sum_{b_n\in\mathbb{F}_{2^\lambda}}\\
&\qquad\frac{1}{dn^2\cdots(dn^2-d+1)\cdot(2^\lambda)^n}\log\frac{1}{dn^2\cdots(dn^2-d+1)\cdot(2^\lambda)^n}\\
&=\log(dn^2\cdots(dn^2-d+1)\cdot(2^\lambda)^n).
\end{aligned}
$$

一方,

$$
\begin{aligned}
&H(M_1,\ldots M_n)+H(W_1,\ldots,W_\tau)\\
&=-\sum_{m_1\in\mathbb{F}_{2^\lambda}}\cdots\sum_{m_n\in\mathbb{F}_{2^\lambda}}\\
&\quad\Pr[M_1=m_1,\ldots,M_n=m_n]\log\Pr[M_1=m_1,\ldots,M_n=m_n]\\
&\qquad+\sum_{w_1\in\{0,1\}^{\log d}}\cdots\sum_{w_\tau\in\{0,1\}^{\log d}\setminus\{w_j\}_{j=1}^{\tau-1}}\\
&\qquad\Pr[W_1=w_1,\ldots,W_\tau=w_\tau]\log\Pr[W_1=w_1,\ldots,W_\tau=w_\tau]\\
&=-\sum_{m_1\in\mathbb{F}_{2^\lambda}}\cdots\sum_{m_n\in\mathbb{F}_{2^\lambda}}\frac{1}{(2^\lambda)^n}\log\frac{1}{(2^\lambda)^n}\\
&\qquad+\sum_{w_1\in\{0,1\}^{\log d}}\cdots\sum_{w_\tau\in\{0,1\}^{\log d}\setminus\{w_j\}_{j=1}^{\tau-1}}\\
&\qquad\frac{1}{d\cdots(d-\tau+1)}\log\frac{1}{d\cdots(d-\tau+1)}\\
&=\log(2^\lambda)^n+\log d\cdots(d-\tau+1)\\
&=\log(d\cdots(d-\tau+1)\cdot(2^\lambda)^n).
\end{aligned}
$$

以上より $H(K)>H(M_1,\ldots M_n)+H(W_1,\ldots,W_\tau)$ であるため, 鍵長の下界の等号を満たしていない.

5. まとめと今後の課題

本稿では，情報理論的に安全な検索可能暗号について再考し，構成法の厳密な解析を行った．具体的には，ドキュメントとキーワードの紐づき具合を考慮した安全性を定義し，鍵長の下界を導出し，またそれぞれの安全性を満たす構成法を提案した．今後の課題としては，鍵長の下界の等号を満たす，最適な構成法を提案することである．今回提案した構成法は，ドキュメントとキーワードの紐づき具合に制限を加えた一つ目の構成法ですら，鍵長の下界を達成できていない.

謝辞 本研究は JSPS 科研費 16J10532 及び 15H02710 の助成によるものです.

参考文献

[1] M. Abdalla, M. Bellare, D. Catalano, E Kiltz, T. Kohno, T. Lange, J. Malone-lee, G. Neven, P. Paillier and H. Shi: Searchable encryption revisited: Consistency properties, reration to anonymous IBE, and extensions. In: J.Cryptology, vol. 21, no. 3, pp.350–391, Springer (2008)

[2] E. Ayday, E. De Cristofaro, J. Hubaux, and G. Tsudik: The chills and thrills of whole genome sequencing. In: Computer, 99, p.1, IEEE (2013) The full version is available at `http://arxiv.org/abs/1306.1264`.

[3] G. Asharov, M. Naor, G. Segev, and I. Shahaf: Searchable symmetric encryption: optimal locality in linear space via two-dimensional balanced allocations. In: STOC'16,pp.1101–1114, ACM(2016)

[4] D. Boneh, G.D. Crescenzo, R. Ostrovsky, and G. Persiano: Public key encryption with keyword search. In:

EUROCRYPT 2004, LNCS 3027 pp.506–522, Springer (2004)

[5] E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid: Recommendation for key management — part 1: General (revision 3). In: NIST Special Publication 800-57. (2012) Available at `http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf`.

[6] D. Cash, S. Jarecki and C. Jutla: Highly-scalable searchable symmetric encry ption with support for boolean queries. In: CRYPTO 2013, Lecture Notes in Computer Science Volume 8042, pp 353–373, Springer (2013)

[7] D. Cash and S Tessaro: The locality of searchable symmetric encryption. In: EUROCRYPT 2014, Lecture Notes in Computer Science Volume 8441, pp.351–368, Springer (2014)

[8] Q. Chai and G. Gong: Verifiable symmetric searchable encryption for semi-honest-but-curious cloud servers. In: IEEE International Conference on Communications (ICC), pp.917–922, IEEE (2012)

[9] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky: Searchable symmetric encryption: improved definitions and efficient constructions. In: ACM CCS'06, pp.79–88, ACM (2006)

[10] Y. Chang and M. Mitzenmacher: Privacy preserving keyword searches on remote encrypted data. In: Applied Cryptography and Network Security(ACNS'05), volume 3531 of Lecture Notes in Computer Science, pp.442–455, Springer (2005)

[11] Y. Dodis: Shannon Impossibility, Revisited, In: Information Theoretic Security - 6th International Conference, Lecture Notes in Computer Science Volume 7412, pp.100–110, Springer (2012)

[12] Eu-jin Goh: Secure Indexes. In: Cryptology ePrint Archive, Report 2003/216 (2003)

[13] S. Kamara and C. Papamanthou: Parallel and dynamic searchable symmetric encryption. In: Financial Cryptography and Data Security, Lecture Notes in Computer Science Volume 7859, pp.258–274, Springer (2013)

[14] S. Sedghi, J. Doumen, P. Hartel and W. Jonker: Toward an Information Theoretic Analysis of Searchable Encryption (Extended Version), In: Information and Communications Security, 10th International Conference,Lecture Notes in Computer Science Volume 5308 pp.345–460, Springer (2008)

[15] J. Shikata: Formalization of Information-Theoretic Security for Encryption and Key Agreement, Revisited, In:Cryptology ePrint Archive, Report 2012/383 (2012)

[16] D. Song, D. Wagner and A. Perrig: Practical techniques for searching on encrypted data. In: IEEE Symposium on Research in Security and Privacy, pp.44–55, IEEE (2000)

[17] The Presdental Commission for the Study of Bioethical Issues: Privacy and progress in whole genome sequencing. In: President's Bioethics Commission Releases Report on Genomics and Privacy. (2012) Available at `http://bioethics.gov/sites/default/files/PrivacyProgress508.pdf`.

[18] 吉澤, 渡邉, 四方: 情報理論的に安全な検索可能暗号, In: コンピューターセキュリティシンポジウム 2015 (CSS 2015) 予稿集, 3C4-4, pp.1321–1326, (2015)

[19] 吉澤, 渡邉, 四方: 情報理論的安全性を持つ検索可能暗号の一般的モデルとその構成法, In: 暗号と情報セキュリティシンポジウム 2016 (SCIS 2015) 予稿集, 2A1-3, (2016)