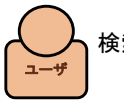
ISEC研究会@東海大学 高輪キャンパス
2017/3/10

検索可能暗号における最小漏洩情報に関する考察

中井 雄士†，○野島 拓也††，岩本 貢††，太田 和夫††
†電気通信大学 情報理工学研究科 総合情報学専攻
††電気通信大学 情報理工学研究科 情報学専攻

文書の検索

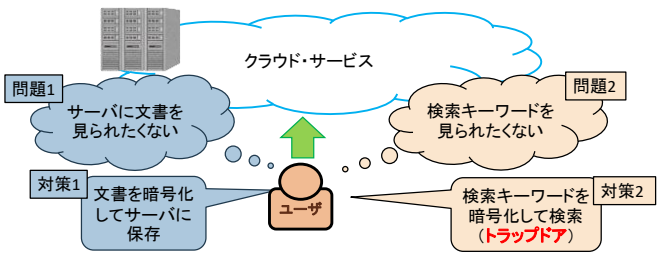
文書①: I have a pen.
文書②: I have an apple.
文書③: you want a pen.



検索キーワード: pen

文書①, 文書③

検索可能暗号とは



暗号文を復号せずトラップドアを使用して検索

検索可能暗号

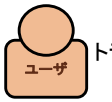
- 共通鍵暗号方式ベース (Searchable Symmetric Encryption, SSE) [2][5]
- 公開鍵暗号方式ベース (Publickey Encryption with Keyword Search, PEKS) [1]

[1] Dan Boneh, Giovanni Di Crescenzo, Rafail Ostrovsky, and Giuseppe Persiano. Public key encryption with keyword search. In Eurocrypt 2004, Vol.3027 in LNCS, pp.506-522,2004
[2] Reza Curtmola, Juan Garay, Seny Kamara, and Rafail Ostrovsky. Searchable symmetric encryption: Improved definitions and efficient constructions. In ACM CCS 2006, pp.79–88, 2006.
[5] Dawn Xiaodong Song, David Wagner, and Adrian Perrig. Practical techniques for searching on encrypted data. InIEEE Security and Privacy, pp. 44–55, 2000.

SSEの構成のアイディア

文書①: I have a pen.
文書②: I have an apple.
文書③: you want a pen.

暗号化



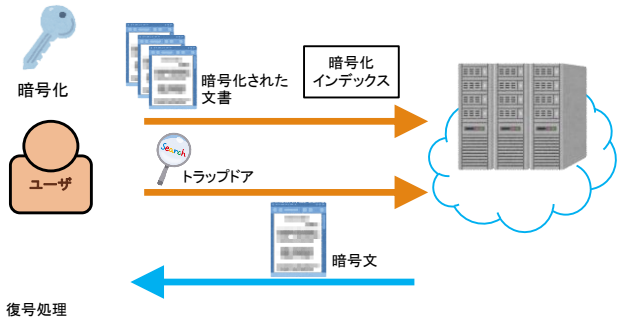
トラップドア: pen

①, ③の暗号文

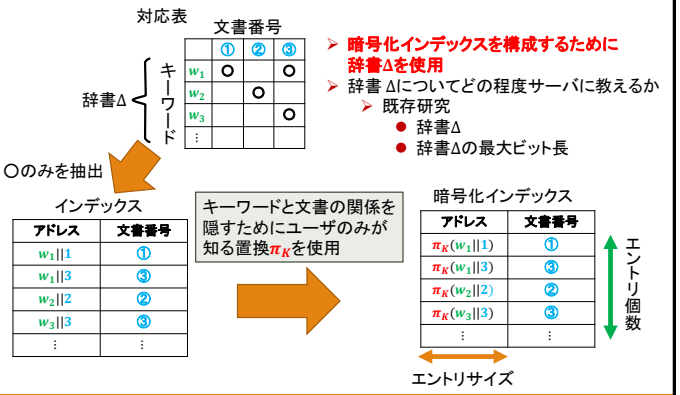
キーワードと文書の関係表: インデックス

キーワード	文書番号
w_1 = pen	①, ③
w_2 = apple	②
w_3 = want	③
⋮	⋮

SSEのプロトコルの流れ



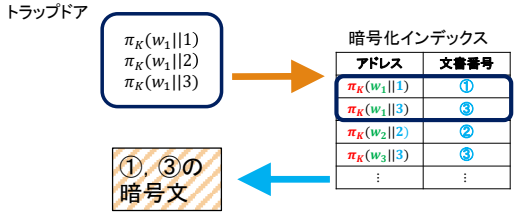
暗号化インデックスの作成例



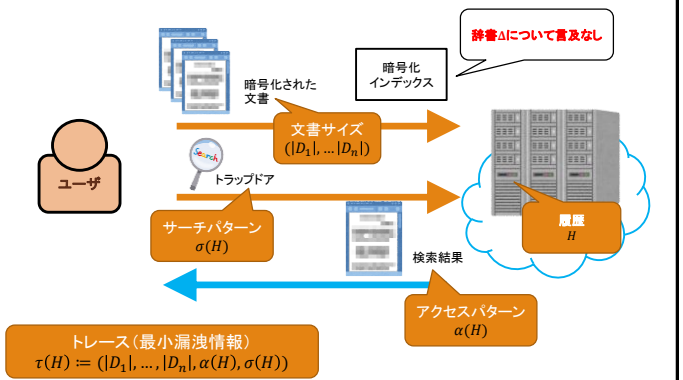
- **暗号化インデックスを構成するために辞書Δを使用**
- 辞書 Δについてどの程度サーバに教えるか
  - 既存研究
    - 辞書Δ
    - 辞書Δの最大ビット長

検索方法：キーワードw_1を検索する場合

- キーワードw_1を含む文書の番号候補は以下のアドレスに含まれる
  $\pi_K(w_1||1)$
  $\pi_K(w_1||2)$
  $\pi_K(w_1||3)$



最小漏洩情報[2]とは



[2] Reza Curtmola, Juan Garay, Seny Kamara, and Rafail Ostrovsky. Searchable symmetric encryption: Improved definitions and efficient constructions. In ACM CCS 2006, pp.79–88, 2006.

理想的なSSE

1. サーバに漏れる情報が少ない
2. 暗号化インデックスが小さい

[問題]
サーバはインデックスから**文書に含まれるキーワードの個数が分かる**.

暗号化インデックス

アドレス	文書番号
$\pi_K(w_1\|\|1)$	①
$\pi_K(w_1\|\|3)$	③
$\pi_K(w_2\|\|2)$	②
$\pi_K(w_3\|\|3)$	③

文書に含まれるキーワードの偏りが分かる

[対策の基本方針]
ダミーのエントリーを用意し文書に含まれるキーワードの個数を隠す

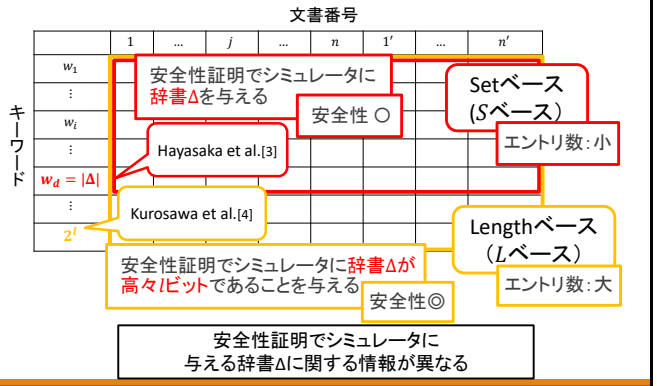
研究の成果(1)

- Curtmolaら[2]：サーバに仕方なく漏洩する情報を最小漏洩情報と定義
  - しかし，安全性証明に辞書Δの漏洩情報を使用
- 辞書Δの漏洩情報について扱いがSSEによって異なる
  - 辞書Δが高々lビットと辞書Δ全体のどちらが漏れていいか
  - 安全性証明でシミュレータに与える辞書Δの漏洩情報が異なる

辞書Δの漏洩情報を分類したい

[2]Reza Curtmola, Juan Garay, Seny Kamara, and Rafail Ostrovsky. Searchable symmetric encryption: Improved definitions and efficient constructions. In ACM CCS 2006, pp.79-88, 2006

暗号化インデックスの作成の違い



[3] Kenichiro Hayasaka, Yutaka Kawai, Yoshihiro Koseki,Takato Hirano, Kazuo Ohta, and Mitsugu Iwamoto. Probabilistic generation of trapdoors: Reducing information leakage of searchable symmetric encryption. In Cryptology and Network Security - 15th International Conference,CANS2016, Vol. 10052 in LNCS, pp. 350-364, 2016
[4] Kaoru Kurosawa and Yasuhiro Ohtaki. UC-secure searchable symmetric encryption. In Financial Cryptography, Vol.7397 in LNCS, pp. 285-298, 2012

辞書に関する漏洩情報の違い

構成方法の違い

	Sベース	Lベース
Δ	**公開**	**秘匿**
Δに含まれる最大キーワード長	公開	公開
エントリ数	小	大
安全性	○	◎
既存研究	Hayasaka et al.[3]	Kurosawa et al.[4]

[3] Kenichiro Hayasaka, Yutaka Kawai, Yoshihiro Koseki,Takato Hirano, Kazuo Ohta, and Mitsugu Iwamoto. Probabilistic generation of trapdoors: Reducing information leakage of searchable symmetric encryption. In Cryptology and Network Security - 15th International Conference,CANS2016, Vol. 10052 in LNCS, pp. 350-364, 2016
[4] Kaoru Kurosawa and Yasuhiro Ohtaki. UC-secure searchable symmetric encryption. In Financial Cryptography, Vol.7397 in LNCS, pp. 285-298, 2012

研究の成果(2)

- Curtmolaら[2],SSE-2：adaptively secure
  - ○ エントリの個数：小
  - × 動かない[4] [本研究]
- Kurosawaら[4]： UC-security
  - × エントリの個数：大
  - ○ 動く

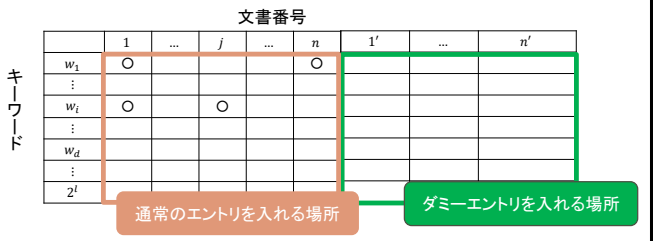
Curtmolaらのアイディアを基に正常に動き
エントリの個数が小さいプロトコルを構成した

[2]Reza Curtmola, Juan Garay, Seny Kamara, and Rafail Ostrovsky. Searchable symmetric encryption: Improved definitions and efficient constructions. In ACM CCS 2006, pp.79-88, 2006
[4] Kaoru Kurosawa and Yasuhiro Ohtaki. UC-secure searchable symmetric encryption. In Financial Cryptography, Vol.7397 in LNCS, pp. 285-298, 2012

Curtmolaらのプロトコル[2]

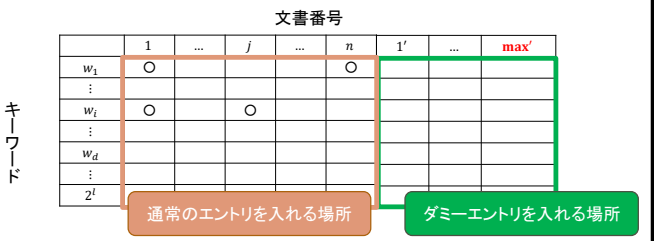
[2]Reza Curtmola, Juan Garay, Seny Kamara, and Rafail Ostrovsky. Searchable symmetric encryption: Improved definitions and efficient constructions. In ACM CCS 2006, pp.79-88, 2006

ダミーエントリ（素朴な方法）



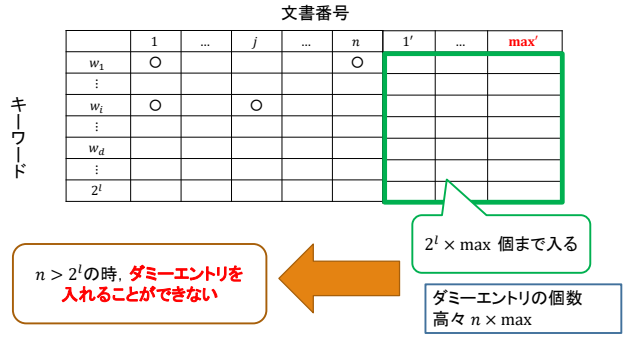
- 登録時は，ダミーエントリを使用し各文書番号の個数を2^lに統一
  - ダミーエントリは通常のエントリと同じ大きさ
  - ダミーエントリは高々$2^l \times n$
- 検索時は，通常のエントリだけを見る

Curtmolaらのアイディア



- エントリの個数を減らすために各文書番号の個数をmax 個に統一
  - max ：文書サイズが最大な文書に注目し，そこに含めることができるキーワードの種類の上限
  - ダミーエントリは高々$\mathbf{max} \times n < 2^l \times n$

SSE-2の誤りの指摘[本研究]
ダミーエントリの限界

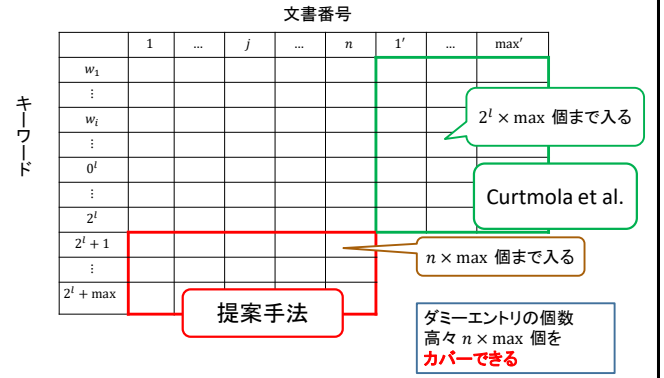


17

提案プロトコル

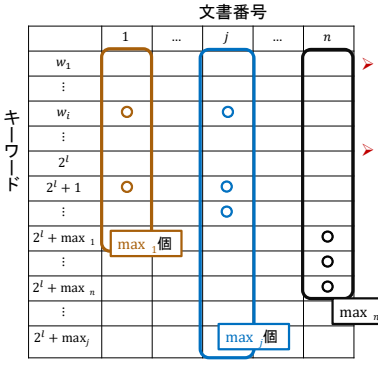
18

アイディア(1)
[必ずダミーエントリが入る構成]



19

アイディア(2)[エントリ数の削減]



- 文書D_jの番号の個数を$\max_j$にする
  - $\max_j$:各文書D_jに対して$\max$ を計算したもの
- Curtmolaらの手法よりも少ないエントリ数で構成.

$$\sum_{j=1}^{n} \max_j < \max \times n$$

$\max = \max_j$の最大値

20

エントリの比較

	Curtmola et al.[2]	Kurosawa et al.[4]	Hayasaka et al.[3]	提案手法
エントリの個数：s	$\max_i \times n$	$2^l \times n$	$\lvert\Delta\rvert \times n$	$\sum_{j=1}^{n} \max_j$ $< \max_i \times n$
エントリサイズ：e	$2^l \times (n + \max_i)$	$(2^l + 2^l) \times n$	$(2^l + 2^l) \times n$	$(2^l + \max_i) \times n$
Δに基づく安全性の分類	動作しない	Lベース	Sベース	Lベース

注：$\max_i \leq \max \leq 2^l$

暗号化インデックスのサイズ
提案手法 ＜ Kurosawa

Δに基づく安全性
提案手法 ＝ Kurosawa ＝ Lベース

[2]Reza Curtmola, Juan Garay, Seny Kamara, and Rafail Ostrovsky. Searchable symmetric encryption: Improved definitions and efficient constructions. In ACM CCS 2006, pp.79-88, 2006
[3] Kenichiro Hayasaka, Yutaka Kawai, Yoshihiro Koseki,Takato Hirano, Kazuo Ohta, and Mitsugu Iwamoto. Probabilistic generation of trapdoors: Reducing information leakage of searchable symmetric encryption. In Cryptology and Network Security - 15th International Conference,CANS2016, Vol. 10052 in LNCS, pp. 350-364, 2016
[4] Kaoru Kurosawa and Yasuhiro Ohtaki. UC-secure searchable symmetric encryption. In Financial Cryptography, Vol.7397 in LNCS, pp. 285-298, 2012

まとめ

- 辞書Δの漏洩情報がSSEによって異なる.
  - Sベース：キーワード集合Δを公開
  - Lベース：Δの最大のキーワードの長さを公開
  - 安全性の観点からはLベースが優れる.（しかし，暗号化インデックスは大きくなる問題がある.）
- Curtmolaらは，新たにmax を導入し文書番号の軸で使用することで暗号化インデックスを小さくしようとしたが，この方針では問題が解決できないことを示した.
- Curtmolaらのアイディア（max ）をキーワードの軸で使用することで暗号化インデックスを小さくした.
  - 文書毎にmax を個別に定義して利用すると，暗号化インデックスの大きさを更に小さくできることを示した.