検索可能暗号を用いた順序開示暗号の一般的な構成について

吉野 雅之[1,a)]　長沼 健[1,2]　國廣 昇[3]　佐藤 尚宜[1]

概要：企業や組織から，個人情報や機密情報等の不正な持出，流出の事件が社会問題化している．この課題を解決するため，データを暗号化したまま処理を可能とする様々な暗号方式が研究されている．本稿では，暗号化データの一致検索を実現する共通鍵型の検索可能暗号に着目し，この検索可能暗号を用いて範囲検索を実現するクエリ型の順序開示暗号 (Query-based Order Revealing Encryption) の一般的な構成法を示す．一般に，共通鍵型の検索可能暗号は実用的な高速性を特徴としており，提案する構成法に基づいた順序開示暗号も同様に高速性を有する．

キーワード：Order Revealing Encryption，順序開示暗号, 検索可能暗号，範囲検索

Generalization of Query-based Order Revealing Encryption using Symmetric Searchable Encryption

Masayuki Yoshino[1,a)]　Ken Naganuma[1,2]　Noboru Kunhiro[3]　Hisayoshi Sato[1]

Abstract: The leakage of personal information and confidential information from companies and organizations are recorgnized as serious issues. In order to solve this problem, various cryptosystems that enable processing with data encrypted have been researched. In this paper, we employ symmetric searchable encryption that realizes perfect search of encrypted data to construct query type order revealing encryption for encrypted range search. In general, symmetric searchable encryptions are equipped with high speed, thus the order revealing encryptions based on the proposed configuration achive high speed as well.

Keywords: Order Revealing Encryption，Searchable Encryption, Range Search, Order Preserving Encryption

1. はじめに

順序開示暗号とは，暗号化されたデータ同士で値の大小関係を判定する比較処理が可能な暗号化方式である．具体的な順序開示暗号方式としては, 参考文献 [1,9,10,15] などが知られている．これら順序開示暗号は，共通鍵暗号と公開鍵暗号に大別できる．処理速度を優先し，高速性に優れる共通鍵暗号が実用化の観点では先行している．本稿でも，共通鍵暗号の順序開示暗号を研究対象とする．以降，特に断りがない限り，順序開示暗号は共通鍵暗号を想定する．

平文の順序情報に関する比較を判定可能とする暗号化技

1 (株) 日立製作所, Hitach, Ltd.
2 東京大学, The University of Tokyo
3 筑波大学, University of Tsukuba
a) masayuki.yoshino.aa@hitachi.com

術の一つである順序開示暗号は，その利便性に優れる反面，平文の順序情報を用いた不正解析が攻撃の温床となりやすい．実際，この順序情報に着目し，順序開示暗号で暗号化したデータを解読する攻撃が報告されている [18]．攻撃者は，ストレージ内に保存された暗号文を盗み，暗号文が開示する順序関係と統計情報等の公開情報を組み合わせることにより，平文を推測する．例えば，年齢を暗号化したデータを攻撃者が入手した場合，平文空間は 100 程度と極端に小さいため，暗号化されたデータ同士の比較により，高い確率で元の平文を推測できる [18]．

暗号化されたデータの大小比較が可能な暗号化方式として，以下が知られる．

- Order Preserving Encryption（OPE）[1–3]
  データベース内の暗号化されたデータ同士の大小比較が平文と同じ手続で処理できる [1]．一方，暗号化されたデータの大小がそのまま元の平文の大小を表しているため，元の平文が推測されやすい，という脆弱性を抱える．これを解消するには，少なくとも準指数関数の暗号文空間を要することが証明されている．実用上は OPE だけでは安全性の確保が難しいため，古典的なアクセス対策と併用する必要がある．
- Order Revealing Encryption（ORE）[9,10,15]
  OPE と異なり、暗号化されたデータの比較用の関数を用いる方式である．この比較用の関数は，一般にはデータベースに組み込んで動作させる．原理的には OPE と同様のセキュリティである．
- Query-based Order Revealing Encryption（QORE）[10,15]
  QORE は，上記 2 種類の暗号化方式とは異なり，比較用に暗号化されたデータ（以下，暗号化クエリと呼ぶ）とデータベース内の暗号化されたデータ（以下、暗号文と呼ぶ）のみの比較が可能である．データベース内の暗号文同士の大小判定は暗号化クエリなしでは困難であるため，推論攻撃からも安全性を確保しやすい．

本稿では，推論攻撃からの安全性を重視し，QORE の構築法を提案する．

QORE に関しては，いくつかの先行研究がある．[10] では，暗号化クエリをトリガーとするソート可能暗号と，それを用いた QORE の構成法を提案している．しかし，暗号文と暗号化トークンの比較処理の結果として，大小関係に加え，暗号化データと暗号化トークンの距離も漏洩させてしまう，というセキュリティ上の課題がある．[15] では，比較処理の結果のみを開示するセキュアな QORE を実現する手法を提案しているが，一方で暗号文のサイズが指数的に増加してしまい，実用的ではない．また，暗号文のサイズを縮小する手法も提案してるが，それを用いた場合，[10] 同様，距離が漏えいする，という課題がある．

表 1 QORE モデルの各種方式の安全性とデータサイズ

	[10]	[15]-1	[15]-2	$\mathtt{QORE}_{\mathtt{SSE}}$
識別困難性	No	No	Yes	Yes
暗号文のサイズ	n	$\lceil n/x \rceil 2^x$	2^n	n
暗号化クエリのサイズ	n	$\lceil n/x \rceil$ $(x < n)$	1	n

2. 準備

n 未満の非負の整数の集合 $\{i | i \in [0, n-1] \wedge i \in \mathbb{Z}\}$ を $[n]$ で表す．平文空間を $\mathbb{P} = [2^n]$ と定義する．平文 $pt \in \mathbb{P}$ は $pt = \sum_{i=1}^{n-1} pt_i 2^i$ と 2 進数 pt_i で表せ，$pt = (pt_{n-1}, \ldots pt_0)$ とする．同様に，平文クエリ $pq \in \mathbb{P}$ も $pq = (pq_{n-1}, \ldots pq_0)$ とする．平文 pt と平文クエリ pq をそれぞれ暗号化したデータを暗号文 ct，暗号化クエリ cq と呼ぶ．また暗号文の長さを $|ct|$，暗号文クエリの長さを $|cq|$ とし，暗号文空間を $\mathbb{C}_T$，暗号化クエリ空間を $\mathbb{C}_Q$ とする．任意の $c \in \mathbb{N}$ に $f = o(1/\lambda^c)$ が成り立つとき，関数 $f(\lambda)$ を λ について無視可能関数と呼ぶ．λ を引数とする無視可能関数を $negl(\lambda)$，多項式を $poly(\lambda)$ と表す．ある事象の生起確率が $negl(\lambda)$ であるとき，その事象を λ について無視可能という．

2.1 検索可能暗号

共通鍵方式の検索可能暗号 (Symmetric Searchable Encryption：SSE) は，鍵生成アルゴリズム Gen，暗号化アルゴリズム Enc，暗号化クエリ生成アルゴリズム Query，比較アルゴリズム Cmp の 4 つの多項式時間アルゴリズムの組として定義される, 共通鍵暗号方式である．

$$\mathtt{SSE} = (\mathtt{Gen}, \mathtt{Enc}, \mathtt{Query}, \mathtt{Cmp})$$

- Gen: セキュリティパラメータ $\lambda \in \mathbb{N}$ を入力とし，公開パラメータと秘密鍵 sk を出力する確率的アルゴリズム．

$$\mathtt{SSE.Gen}(\lambda) \rightarrow sk$$

- Enc: 秘密鍵 sk と平文 $pt \in \mathbb{P}$ を入力とし，暗号文 ct を出力する確率的アルゴリズム．

$$\texttt{SSE.Enc}(sk, pt) \to ct$$

- Query: 秘密鍵 sk と平文クエリ $pq \in \mathbb{P}$ を入力とし，暗号化クエリ cq を出力する確定的アルゴリズム（もしくは，確率的アルゴリズム）．

$$\texttt{SSE.Query}(sk, pq) \to cq$$

- Cmp: 暗号文 ct と暗号化クエリ cq を入力とし，暗号文 ct が暗号化クエリ cq と等しいことを表す値 1, または異なることを表す値 0 のいずれかを出力する確定的アルゴリズム．

$$\texttt{SSE.Cmp}(ct, cq) \to 1 \text{ or } 0$$

定義 1. [SSE の完全性] 全ての $pt \in \mathbb{P}$, $pq \in \mathbb{P}$ に対し，$\texttt{SSE} = (\texttt{Gen}, \texttt{Enc}, \texttt{Query}, \texttt{Cmp})$ が次式を満足するとき，SSE は完全性を満たすという．

$$\texttt{SSE.Cmp}(ct, cq) = \begin{cases} 1 (pt \neq pq) \text{ (ただし，確率 } 1 - negl(\lambda)) \\ 0 (pt = pq) \text{ (ただし，確率 } 1) \end{cases}$$

ここで, λ はセキュリティパラメータとし, $sk \leftarrow \texttt{SSE.Gen}(\lambda)$, $ct \leftarrow \texttt{SSE.Enc}(sk, pt)$, $cq \leftarrow \texttt{SSE.Query}(sk, pq)$ とする．

次に SSE に対する安全性モデルを定義する．

定義 2. 任意の多項式時間アルゴリズム $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ に対し, SSE=(Gen, Enc, Query, Cmp) が次式を満足する時，SSE は識別困難であるといい，Secure SSE と呼ぶ．

$$Adv^{\lambda}_{\mathcal{C},\mathcal{A}} := \left| Pr[Exp^{ind-b}_{\texttt{SSE},\mathcal{A}} = b] - \frac{1}{2} \right| < negl(\lambda)$$

ここで，$Exp^{ind-b}_{\texttt{SSE},\mathcal{A}}$ は，$b \in \{0, 1\}$ に対し，次のように定義されるゲームとする．

$Exp^{ind-b}_{\texttt{SSE},\mathcal{A}}$:
$sk \leftarrow \texttt{SSE.Gen}(\lambda)$;
$(pt^0, pt^1, st) \leftarrow \mathcal{A}_1^{\mathcal{E},\mathcal{Q}}(n)$;
$b \xleftarrow{R} \{0, 1\}$; $ct^b \leftarrow \texttt{SSE.Enc}(sk, pt^b)$;
$b' \leftarrow \mathcal{A}_2^{\mathcal{E},\mathcal{Q}}(pt^0, pt^1, ct^b, n, st)$;
return b'

ここで，st は内部変数，$\mathcal{E}$ は任意の平文 pt に対し，$\texttt{SSE.Enc}(sk, pt)$ により暗号文 ct を返答する SSE 暗号化オラクルとする．また，$\mathcal{Q}$ は平文クエリ pq に対して，$\texttt{SSE.Query}(sk, pq)$ により暗号化クエリ cq を返答する SSE 暗号化クエリ生成オラクルとする．なお，自明な識別を回避すべく，(pq, pt^0, pt^1) の問い合わせは次式を満たす場合は禁止する．

$$pt^0 = pq, \ pt^1 = pq$$

3. クエリベースの順序開示暗号

順序開示暗号 (Order Revealing Encryption) は，サーバが暗号文同士の比較を主目的として設計されるが，セキュリティの観点からサーバが暗号文同士の比較を自由に行えることは望ましくない．本稿では，暗号文同士の比較は検討対象とせず，ユーザからの要求に応じ暗号文を比較するクエリベースの順序開示暗号 QORE(Query-based Order Revealing Encryption) について報告する．

3.1 QORE モデル

QORE は，鍵生成アルゴリズム Gen，暗号化アルゴリズム Enc，暗号化クエリ生成アルゴリズム Query，比較アルゴリズム Cmp の 4 つの多項式時間アルゴリズムの組として定義される, 共通鍵暗号方式である．

$$\texttt{QORE} = (\texttt{Gen}, \texttt{Enc}, \texttt{Query}, \texttt{Cmp})$$

- Gen: セキュリティパラメータ $\lambda \in \mathbb{N}$ と範囲パラメータ $n \in \mathbb{N}$ を入力とし，公開パラメータと秘密鍵 sk を出力する確率的アルゴリズム．

$$\texttt{QORE.Gen}(\lambda, n) \to sk$$

- Enc: 秘密鍵 sk と平文 $pt \in \mathbb{P}$ を入力とし，暗号文 ct を出力する確率的アルゴリズム．

$$\texttt{QORE.Enc}(sk, pt) \to ct$$

- Query: 秘密鍵 sk と平文クエリ $pq \in \mathbb{P}$ を入力とし，暗号化クエリ cq を出力する確定的アルゴリズム（もしくは，確率的アルゴリズム）．

$$\texttt{QORE.Query}(sk, pq) \to cq$$

- Cmp: 暗号文 ct と暗号化クエリ cq を入力とし，暗号文 ct が暗号化クエリ cq より大きいことを表す値 1, 等しいことを表す値 0, 小さいことを表す値 -1 のいずれか

を出力する確定的アルゴリズム.

$$\texttt{QORE.Cmp}(ct, cq) \rightarrow 1, 0 \text{ or } -1$$

定義 3. [QORE の完全性] 全ての $pt \in \mathbb{P}$, $pq \in \mathbb{P}$ に対し，$\texttt{QORE} = (\texttt{Gen}, \texttt{Enc}, \texttt{Query}, \texttt{Cmp})$ が次式を満足するとき，QORE は完全性を満たすという.

$$\texttt{QORE.Cmp}(ct, cq) = \begin{cases} 1(pt > pq) \text{ (ただし確率 } 1 - negl(\lambda)) \\ 0(pt = pq) \text{ (ただし確率 } 1) \\ -1(pt < pq) \text{ (ただし確率 } 1 - negl(\lambda)) \end{cases}$$

ここで，λ はセキュリティパラメータ，n は範囲パラメータとし，$sk \leftarrow \texttt{QORE.Gen}(\lambda, n)$, $ct \leftarrow \texttt{QORE.Enc}(sk, pt)$, $cq \leftarrow \texttt{QORE.Query}(sk, pq)$ とする.

QORE に復号アルゴリズムは無いが，AES 暗号等の標準的な共通鍵暗号による暗号化を QORE.Enc 内に追加することにより，容易に復号アルゴリズムを備えることができる．本稿では，単純化のため，復号アルゴリズムは省く.

確率的多項式時間アルゴリズムの組（ユーザ $\mathcal{U}$，サーバ $\mathcal{S}$）により，2 者間プロトコル $\Sigma_{\texttt{QORE}} = (\mathcal{U}, \mathcal{S})$ は定義される．$\Sigma_{\texttt{QORE}}$ は，最初に一度だけ実行する登録フェーズと，何度も実行する比較フェーズの組から成り，各フェーズにおいて QORE の各アルゴリズム (Gen, Enc, Query, Cmp) が $\mathcal{U}$ または $\mathcal{S}$ により適宜選択される.

登録フェーズ

(1) $\mathcal{U}$ は QORE.Gen により秘密鍵 sk と公開パラメータを生成する．また，公開パラメータは $\mathcal{S}$ に渡す.

(2) $\mathcal{U}$ は多項式個の平文の集合 $PT = \{\ldots, pt[i] \ldots\}$ を平文空間 $\mathbb{P}$ から抽出，QORE.Enc により暗号文の集合 $CT = \{\ldots, ct[i] \ldots\}$ を作成する.

(3) $\mathcal{U}$ は暗号文の集合 CT を $\mathcal{S}$ に渡す.

比較フェーズ

(1) $\mathcal{U}$ は平文クエリ pq を平文空間 $\mathbb{P}$ から抽出，QORE.Query により暗号化クエリ cq を作成，$\mathcal{S}$ に渡す.

(2) $\mathcal{S}$ は cq と CT における全ての暗号文との比較結果 $\{\ldots, \texttt{QORE.Cmp}(ct[i], cq) \ldots\}$ を作成する.

(3) $\mathcal{S}$ はインデックス i と比較結果の組の集合 $\{\ldots, (i, \texttt{QORE.Cmp}(ct[i], cq)) \ldots\}$ を $\mathcal{U}$ に渡す.

3.2 QORE モデルのセキュリティ

QORE モデルにおいて，開示される Cmp の出力は，攻撃者が暗号文を解析する際の重要なヒントになる．例えば，あるしきい値と暗号文の大小が判定可能であり，かつそのしきい値を攻撃者が自由に設定可能である場合，攻撃者は暗号文を容易に識別できる．そのため，Cmp が暗号解読に有利な出力を与えることが自明な場合を除いた，QORE モデルにおける暗号文の安全性を考察する.

暗号化クエリをトリガーとした比較可能な暗号文の識別困難性は Furukawa が定義している [10]．これを QORE モデルに拡張した暗号文の識別困難性を次のように定義する.

定義 4. 任意の多項式時間アルゴリズム $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ に対し，$\texttt{QORE}=(\texttt{Gen}, \texttt{Enc}, \texttt{Query}, \texttt{Cmp})$ が次式を満足するとき，QORE は識別困難であるといい，この QORE を Secure QORE と呼ぶ.

$$Adv^{\lambda}_{\mathcal{C},\mathcal{A}} := \left| Pr[Exp^{ind-b}_{\texttt{QORE},\mathcal{A}} = b] - \frac{1}{2} \right| < negl(\lambda)$$

ここで，$Exp^{ind-b}_{\texttt{QORE},\mathcal{A}}$ は，$b \in \{0, 1\}$ に対し，次のように定義されるゲームとする.

$Exp^{ind-b}_{\texttt{QORE},\mathcal{A}}$:
$sk \leftarrow \texttt{QORE.Gen}(\lambda, n)$;
$(pt^0, pt^1, st) \leftarrow \mathcal{A}_1^{\mathcal{E},\mathcal{Q}}(n)$;
$b \xleftarrow{R} \{0, 1\}$; $ct^b \leftarrow \texttt{QORE.Enc}(sk, pt^b)$;
$b' \leftarrow \mathcal{A}_2^{\mathcal{E},\mathcal{Q}}(pt^0, pt^1, ct^b, n, st)$;
return b'

ここで，st は内部変数，$\mathcal{E}$ は任意の平文 pt に対し，$\texttt{QORE.Enc}(sk, pt)$ により暗号文 ct を返答する QORE 暗号化オラクルとする．また，$\mathcal{Q}$ は平文クエリ pq に対して，

QORE.Query(sk, pq) により暗号化クエリ cq を返答する QORE 暗号化クエリ生成オラクルとする．なお，自明な識別を回避すべく，(pq, pt^0, pt^1) の問い合わせは次式を満たす場合は禁止する．

$$pt^0 \leq pq \leq pt^1 \tag{1}$$

4. 既存手法の問題

[10] と [15] では，ORE(Order Revealing Encryption) の具体的な構成法を提案するとともに，QORE の構成法も提案している．しかし，この時の Cmp は，ct と cq の大小が決定すると，処理を停止し，大小比較の結果を出力する．従って，暗号文 ct と暗号化クエリ cq の 1 回の比較を通し，Cmp を実行する $\mathcal{S}$ には大小比較の算出により，暗号文 ct と暗号化クエリ cq の上位ビットは等号であったこと，即ち $(0, \ldots, 0, x, *, \ldots, *)$ が $\mathcal{S}$ に開示される．ただし $x \in \{-1, 0, 1\}$，$*$ は不明な値である．従って，cp と cq の距離が漏洩されてしまっている．

5. SSE を用いた QORE の一般的構成法

本章では，SSE を用いた QORE の一般的な構成法を述べる．

5.1 提案手法: QORE_{SSE}

暗号文空間を抑制するには，平文を 1 ビットずつ分割した方が暗号文と暗号化クエリのサイズを抑えられる．一方，1 ビットへの分割は，暗号文と暗号化クエリの比較結果がビット単位で判定されるため，漏洩する情報量が大きくなりやすい．そこで，われわれの QORE 設計の基本戦略は以下の通りとした．

- 暗号文と暗号化クエリのサイズを抑制するため，平文と平文クエリを 1 ビットずつ暗号化する
- 余分な情報を漏洩しないよう，平文と平文クエリの全ビットを比較し，等号または不等号は 1 回のみ出力する

この基本戦略に基づき，設計した QORE_{SSE} を述べる．

既存手法では，比較結果に加え，平文と平文クエリのビット位置も開示されてしまい，暗号文の安全性が低下する，という課題がある．このビット位置を秘匿するため，QORE_{SSE} では，平文と平文クエリのビット位置を秘匿する手法を提案する．$\mathcal{U}$ は平文を 1 ビットずつ符号化し，その平文のビット位置をランダムにシャッフルした上で，暗号化する．平文クエリも同様にランダムなシャッフルをしてから暗号化する．$\mathcal{U}$ から暗号文と暗号化クエリを渡された $\mathcal{S}$ には，平文と平文クエリのビット位置が秘匿されている．

QORE_{SSE} を構成する (Gen, Enc, Query, Cmp) について述べる．

- Gen: セキュリティパラメータ λ を入力とする．

(1) $\text{SSE.Gen}(1^\lambda) \to sk$

(2) sk と公開パラメータを出力する

- Enc: 秘密鍵 sk と平文 pt を入力とする．

(1) 平文を $pt = (pt_{n-1}, \ldots, pt_0)$ ただし $pt_i \in \{0, 1\}$ とする

(2) ランダム置換 $\pi : [n] \to [n]$ を生成する

(3) 全ての $i \in [n]$ に対し，
$ct_{\pi(i)} = \text{SSE.Enc}(sk, pt_{n-1} \ldots, pt_i)$ を計算する

(4) 暗号文 $ct = (ct_{n-1}, \ldots ct_0)$ を出力する．

- Query: 秘密鍵 sk，平文クエリ pq を入力とする．

(1) ランダム置換 $\pi : [n] \to [n]$ を生成する

(2) 全ての $i \in [n]$ に対し，

(a) $cq_{\pi(i)+} = \text{SSE.Query}(sk, pq_{n-1} \ldots, pq_i + 1)$ を計算する．ただし $pq_i + 1 \in \{1, 2\}$

(b) $cq_{\pi(i)-} = \text{SSE.Query}(sk, pq_{n-1} \ldots, pq_i - 1)$ を計算する．ただし $pq_i - 1 \in \{-1, 0\}$

(3) 暗号化クエリ $cq = ((cq_{(n-1)+}, cq_{(n-1)-}), \ldots (cq_{0+}, cq_{0-}))$ を出力する．

- Cmp: 暗号文 ct，暗号化クエリ cq を入力とする．

(1) $i = n - 1$ とする．

(2) $j = n - 1$ とする．

(a) $\text{SSE.Cmp}(ct_i, cq_{j+}) = 1$ ならば，-1 $(pt < pq)$ を出力する

(b) $\text{SSE.Cmp}(ct_i, cq_{j-}) = 1$ ならば，1 $(pt > pq)$ を出力する

(c) $j > 0$ ならば，j を 1 減らし，Step.(2)(a) へ戻る．

(3) $i = 0$ ならば，0 $(pt = pq)$ を出力する

(4) i を 1 減らし，Step.(2) へ戻る．

[完全性] $pt_i = pq_i + 1$ のとき，無視可能な確率を除き，$\text{SSE.Cmp}(ct_i, cq_{j+}) = 1$ が成立する．従って，$\text{SSE.Cmp}(ct, cq_{i+}) = 1$ ならば $pt_i > pq_i$ と判断できる．このとき $pt > pq$ と判断できる（よって，QORE.Cmp は 1 を出力）．同様に，$\text{SSE.Cmp}(ct_i, cq_{j-}) = 1$ ならば無視可能な確率を除き $pt_i < pq_i$ が成立するので，$pt < pq$ と判断できる（よっ

て，QORE.Cmp は -1 を出力)．全ての $i \in [n]$，$j \in [n]$ に対して $\mathtt{SSE.Cmp}(ct_i, cq_{j+}) \neq 1$ かつ $\mathtt{SSE.Cmp}(ct_i, cq_{j-}) \neq 1$ であるならば，$pt = pq$ である（よって，QORE.Cmp は 0 を出力)．

$\mathtt{QORE}_{\mathtt{SSE}}$ の Cmp は，ランダム置換により平文 pt と平文クエリ pq のビット位置が暗号文 ct と暗号化クエリ cq から秘匿されている．従って，暗号文 ct と暗号化クエリ cq の 1 回の比較を通し，Cmp を実行する $\mathcal{S}$ には大小比較の結果のみが $\mathcal{S}$ に開示される．ただし，平文または平文クエリを $\mathcal{S}$ が選択できる場合，$(*, \ldots, *, y, *, \ldots, *)$ または $(0, \ldots, 0)$ がサーバ $\mathcal{S}$ に開示される．ただし $y \in \{-1, 1\}$，$*$ は不明な値である．従って，大小判定した y の位置が判明する，または全ビットが同じであったことが判明する．

6. まとめ

本稿では，暗号化データの一致検索を実現する共通鍵型の検索可能暗号に着目し，この検索可能暗号を用いて範囲検索を実現するクエリ型の順序開示暗号 (Order Revealing Encryption) を安全性モデルと共に定義した．次に，共通鍵暗号の検索可能暗号を用いたクエリ型の順序開示暗号の一般的な構成法を示した．一般に，共通鍵型の検索可能暗号は高速性を特徴としており，提案する構成法に基づいた順序開示暗号も高速性を有する．

参考文献

[1] Agrawal, R., Kiernan, J., Srikant, R., and Xu, Y. Order-preserving encryption for numeric data. In *Proceedings of the ACM SIGMOD International Conference on Management of Data* (2004), ACM, pp. 563–574.

[2] Boldyreva, A., Chenette, N., Lee, Y., and O'Neill, A. Order-preserving symmetric encryption. In *Advances in Cryptology - EUROCRYPT 2009, 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques* (2009), vol. 5479 of *Lecture Notes in Computer Science*, Springer, pp. 224–241.

[3] Boldyreva, A., Chenette, N., and O'Neill, A. Order-preserving encryption revisited: Improved security analysis and alternative solutions. In *Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference* (2011), vol. 6841 of *Lecture Notes in Computer Science*, Springer, pp. 578–595.

[4] Cao, Z., Mao, C., Liu, L., Kong, W., and Wang, J. Analysis of one dynamic multi-keyword ranked search scheme over encrypted cloud data. *I. J. Network Security 20*, 4 (2018), 683–688.

[5] Ceselli, A., Damiani, E., di Vimercati, S. D. C., Jajodia, S., Paraboschi, S., and Samarati, P. Modeling and assessing inference exposure in encrypted databases. *ACM Trans. Inf. Syst. Secur. 8*, 1 (2005), 119–152.

[6] Chatterjee, S., and Das, M. P. L. Property preserving symmetric encryption revisited. In *Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security* (2015), vol. 9453 of *Lecture Notes in Computer Science*, Springer, pp. 658–682.

[7] Curtmola, R., Garay, J., Kamara, S., and Ostrovsky, R. Searchable symmetric encryption: Improved definitions and efficient constructions. In *Proceedings of the 13th ACM Conference on Computer and Communications Security* (New York, NY, USA, 2006), CCS, ACM, pp. 79–88.

[8] Ding, Y., and Klein, K. Model-driven application-level encryption for the privacy of e-health data. In *ARES 2010, Fifth International Conference on Availability, Reliability and Security* (2010), IEEE Computer Society, pp. 341–346.

[9] Furukawa, J. Request-based comparable encryption. In *18th European Symposium on Research in Computer Security* (2013), vol. 8134 of *Lecture Notes in Computer Science*, Springer, pp. 129–146.

[10] Furukawa, J. Short comparable encryption. In *Cryptology and Network Security* (2014), Springer, pp. 337–352.

[11] Goh, E. Secure indexes. *IACR Cryptology ePrint Archive* (2003), 216.

[12] Hacigümüs, H., Iyer, B. R., Li, C., and Mehrotra, S. Executing SQL over encrypted data in the database-service-provider model. In *Proceedings of the 2002 ACM SIGMOD International Conference on Management of Data* (2002), ACM, pp. 216–227.

[13] Hacigümüs, H., Mehrotra, S., and Iyer, B. R. Providing database as a service. In *Proceedings of the 18th International Conference on Data Engineering* (2002), IEEE Computer Society, pp. 29–38.

[14] Kamara, S., and Papamanthou, C. Parallel and dynamic searchable symmetric encryption. In *Financial Cryptography and Data Security - 17th International Conference* (2013), vol. 7859 of *Lecture Notes in Computer Science*, Springer, pp. 258–274.

[15] Lewi, K., and Wu, D. J. Order-revealing encryption: New constructions, applications, and lower bounds. In *the 2016 ACM SIGSAC Conference on Computer and Communications Security* (2016), ACM, pp. 1167–1178.

[16] Liu, H., Wang, H., and Chen, Y. Ensuring data storage security against frequency-based attacks in wireless networks. In *Distributed Computing in Sensor Systems* (2010), vol. 6131 of *Lecture Notes in Computer Science*, Springer.

[17] Lu, W., Varna, A. L., and Wu, M. Security analy-

sis for privacy preserving search of multimedia. In *17th International Conference on Image Processing* (2010), IEEE, pp. 2093–2096.

[18] Naveed, M., Kamara, S., and Wright, C. V. Inference attacks on property-preserving encrypted databases. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, October 12-16, 2015* (2015), ACM, pp. 644–655.

[19] Pandey, O., and Rouselakis, Y. Property preserving symmetric encryption. In *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings* (2012), vol. 7237 of *Lecture Notes in Computer Science*, Springer, pp. 375–391.

[20] Popa, R. A., Redfield, C. M. S., Zeldovich, N., and Balakrishnan, H. Cryptdb: Processing queries on an encrypted database. *ACM Communications 55*, 9 (Sept. 2012), 103–111.

[21] Emily Shen, Elaine Shi, and Brent Waters. Predicate Privacy in Encryption Systems. In *TCC*, volume 5444 of *LNCS*, pages 457–473. Springer, 2009.

[22] Tang, Q. Privacy preserving mapping schemes supporting comparison. In *Proceedings of the 2nd ACM Cloud Computing Security Workshop* (2010), A. Perrig and R. Sion, Eds., ACM, pp. 53–58.