部分復元可能な秘密分散法における秘密分散データを用いた検索

1190350　中村　巴　【 ネットワーク信号処理研究室 】

1　はじめに

災害時，外部から派遣された医療従事者に医療データを提供することができれば，被災地での医療行為を円滑に行うことができる．そこで，部分復元可能な秘密分散システムが提案された [1]．しかし，提案システムは，分散バックアップデータをシェアの状態で検索することはできない．そこで，部分復元可能な秘密分散バックアップした医療データ検索方法が提案された [2]．しかし，付与した検索用の情報を復元するため，検索に時間がかかる．本研究では，検索の高速化を目的とし，シェア同士の一致の判定を可能とする方法を提案する．

2　部分復元可能な秘密分散バックアップした医療データ検索方法 [2]

提案方法は，医療データに検索用の情報を付与し，検索時は検索用の情報を復元して該当するデータを見つける．検索用の情報のデータサイズを d とすると，検索用の情報の復元には多項式を解くための逆行列の作成に $\mathcal{O}(d^3)$ の計算量がかかる．そして，医療データの数を Y とすると，Y 回以上の復元が行われるため，検索に時間がかかる．提案方法の検索の流れを図 1 に示す．

3　秘密分散データを用いた復元不要な検索

本研究では，シェア同士の一致の判定を可能とする方法を提案する．検索用シェア $rw_{i,j}(i = 1, 2, 3)(j = 1, 2, \cdots, n)$ と検索キーシェア $kw_{i,j}$ の生成には定数の集合 X, R を用いることにより，検索用の情報を RI，検索キーワードを RK とすると

$$rw_{i,j} = RI + r_1 x_j + r_2 x_j^2 + \cdots + r_{k-1} x_1^{k-1} \pmod p$$
$$kw_{i,j} = RK + r_1 x_j + r_2 x_j^2 + \cdots + r_{k-1} x_j^{k-1} \pmod p$$

となり，$RI = RK$ であれば同じ値になることを利用し，シェア同士での一致判定を可能としている．その結果，検索用の情報の復元処理を省略することができ，検索に必要な計算量は，検索キーシェアの作成に行列とベクトルの乗算を行うため $\mathcal{O}(d^2)$ となる．秘密分散データを用いた検索の検索時の流れを図 2 に示す．

4　従来の検索方法 [2] と提案検索方法の比較

医療データ検索方法と秘密分散データを用いた検索の安全性と検索にかかる時間の比較を行う．

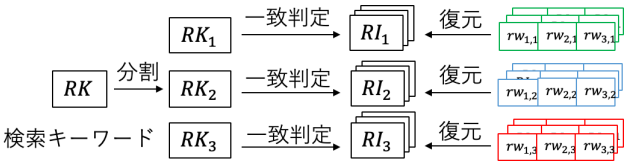

図 1　従来の検索方法の検索時の流れ

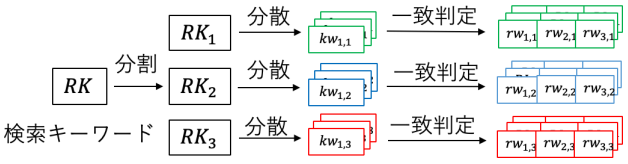

図 2　秘密分散データを用いた検索時の流れ

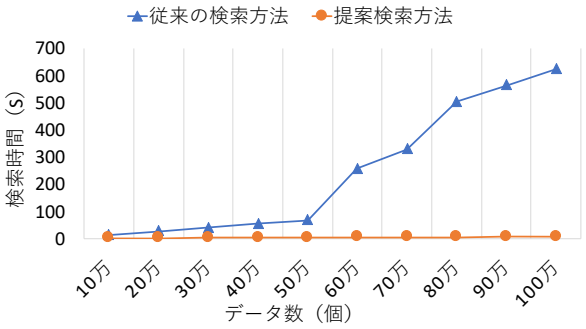

図 3　従来の検索方法と提案検索方法の検索にかかった時間

4.1　安全性の比較

従来の検索方法は，検索用の情報の分散に乱数を用いているため，1 組の乱数が漏洩してもすべての検索用の情報を知られることは無い．しかし，提案検索方法では定数が漏洩すると，すべての検索用の情報を知られる．また，検索用シェアを見ると，同じ検索用の情報が付与されているデータが分かるという問題がある．

4.2　検索にかかる時間の比較

従来の検索方法と，提案検索方法の検索にかかった時間を比較する．6bytes の検索用の情報を 2bytes ごとに 3 個に分割して，$(3, 5)$ しきい値秘密分散し，データのシェアに付与し，検索にかかった時間を chrono 関数を用いて計測した．結果を図 3 に示す．従来の検索方法より，提案検索方法の検索にかかる時間が短縮できていることが分かる．

5　まとめ

本研究では，部分復元可能な秘密分散バックアップした医療データ検索方法 [2] の高速化を目的として，秘密分散データを用いた検索を提案した．従来の検索方法より検索にかかる時間は短縮できたが，安全性が劣っていることが分かった．

参考文献

[1] 田中麻実，福冨英次，福本昌弘，“秘密分散バックアップした医療データの部分復元，”信学技報 IA2015-74，pp. 31–36，Dec. 2015.

[2] 沼尚樹，“部分復元可能な秘密分散バックアップした医療データ検索方法，”平成 29 年度高知工科大学学士学位論文，Mar. 2018.