部分復元可能な秘密分散システムの分割方法による復元速度の評価

1180347　竹中　壮磨　【 ネットワーク信号処理研究室 】

1　はじめに

災害時，バックアップした医療データを外部の医療従事者に瞬時に提供できれば，被災地での医療行為を円滑に行うことができる．よって, バックアップした医療データから医療行為に必要な情報のみを提供できる仕組みがあればよい. 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]．提案されたシステムは，意味のある項目ごとにデータを分割し，分割したデータを分散している．しかし，提案されたシステムは演算量が大きく，復元速度が遅いため，緊急的に医療情報を必要とする災害時には適していない．本研究では，災害時に適した速度で，部分復元できるように，データを一定のサイズごとに分割する方法を提案し，部分復元可能な秘密分散システムの分割サイズによる復元速度の評価を行う．

2　部分復元可能な秘密分散システム

提案された部分復元可能な秘密分散システムの部分復元アルゴリズムと復元にかかる演算量について述べる．

2.1　部分復元アルゴリズム

秘密分散するデータ S を意味のある項目ごとに分割したものを，$S_i(i=1,2,3)$，S_i のデータサイズを l_i とする．S_2 を秘匿したまま復元するための紐付け情報を

$$U_2 = \left(\begin{array}{cc} \prod_{m=2}^{3} 2^{lm}, & 1 \end{array} \right)^{\mathrm{T}} \tag{1}$$

とする．分散時には，S_1, S_2, S_3 それぞれを (k,n) しきい値秘密分散法を用いて n 個の分散情報 (以降シェアと呼ぶ) に分散する．復元時には S_i のシェア集合 W_1, W_3 それぞれからシェアを k 個集め，U_2 を用いて部分復元用シェアを作成し，復元すると，$S_1 \prod_{m=2}^{3} 2^{lm} + S_3 = S'$ となり，S_2 部分が秘匿された S' を得ることができる．

2.2　復元にかかる演算量

提案されたシステムでは，S 以上のデータが表現できる拡大体 $GF(2^m)$ で復元演算を行い，一回の乗算に m^2 の演算量がかかる．そのため，データサイズが大きい場合，復元まで何時間もかかってしまうと予想できる．

3　提案システムと分割サイズによる復元速度の評価

提案するサイズによる分割を行った部分復元可能な秘密分散システムの部分復元アルゴリズムと復元にかかる演算量について述べる．そして，分割サイズによる復元速度の評価を述べる．

3.1　サイズによる分割を行った部分復元アルゴリズム

分散するデータ S を一定のサイズ F で 2 個に分割したデータを $S_t(t=1,2)$，S_t を秘匿部分を選択できるように分割したものを $S_{t,i}(i=1,2)$，$S_{t,i}$ のデータサイズを $l_{t,i}$ とする．$S_{1,2}$ を秘匿するための紐付け情報を

$$u_{1,2} = \left(\begin{array}{ccc} 2^{l_{1,2}}, & 2^{l_{2,2}}, & 1 \end{array} \right)^{\mathrm{T}} \tag{2}$$

とする．部分復元した S'_t を紐付ける，最終紐付け情報を

$$b = \left(\begin{array}{cc} 2^{F}, & 1 \end{array} \right)^{\mathrm{T}} \tag{3}$$

とする．分散時には，$S_{1,1}, S_{1,2}, S_{2,1}, S_{2,2}$ それぞれを (k,n) しきい値秘密分散法を用いて n 個のシェアに分散する．復元時には $S_{t,i}$ のシェア集合 $W_{1,1}, W_{2,1}, W_{2,2}$ それぞれからシェアを k 個集め，$u_{1,2}$ を用いて部分復元用シェアを作成する．そして，部分復元用シェアを復元すると，S'_t が得られ，最終紐付け情報 b で紐付けると，$S_{1,1} \cdot F \cdot 2^{l_{1,2}} + S_{2,1} \cdot 2^{l_{2,2}} + S_{2,2} = S'$ となり，$S_{1,2}$ 部分が秘匿された S' を得ることができる．

3.2　復元にかかる演算量

提案したシステムでは，$GF(2^F)$ 上で復元演算を行い，一回の乗算に F^2 の演算量がかかる．そのため，分割サイズ F を小さくするに従って復元にかかる演算量を小さくできる．

3.3　分割サイズによる復元速度の評価

表 1 に実装した提案システムで，2048Byte のデータの復元にかかった時間を示す．表 1 より分割サイズを小さくすれば，並列処理の実装や CPU の性能によって，復元したいデータサイズが大きい場合でも十分高速に復元できると推定できる．

表 1　2048Byte のデータの復元にかかった時間 (s)

分割サイズ	復元時間
16bit	0.0749998
32bit	0.0835935

4　まとめ

本研究では，部分復元可能な秘密分散システム [1] の復元時間を速くすることを目的として，サイズによる分割を行った秘密分散システムを提案した．分割サイズによる復元速度の評価を行った結果，復元したいデータサイズが大きい場合でも，分割サイズを小さくすれば，実装環境によって，十分高速に復元できると推定できた．

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.