様式 C-19

科学研究費補助金研究成果報告書

平成２２年５月７日現在

研究種目：若手研究（B）
研究期間：2007～2009
課題番号：19700060
研究課題名（和文） 高信頼広域分散ストレージにおけるデータ配送のための分散アルゴリズム
研究課題名（英文）Distributed Algorithm for Share Transfer in a Secure Distributed Storage System
研究代表者
宮本　俊幸（MIYAMOTO　TOSHIYUKI）
大阪大学・工学研究科・准教授
研究者番号：00294041

研究成果の概要（和文）：
秘密分散共有法とは秘密情報をグループで分散共有することによって，秘密性・安全性を高める方法である。本研究では，秘密分散共有法を用いた分散ストレージシステムにおけるデータ配置問題（シェア配送問題）が NP 困難であることを示した。また，発見的手法を用いて解くためにスタイナー木問題に帰着させる方法を提案した。さらに，秘密分散共有法を用いた分散データベース実現のためのいくつかの問題について手法を提案した。

研究成果の概要（英文）：
The secret sharing scheme enhances security and safety of secure data by sharing cryptogram among a group. In this research, I showed NP-hardness of the problem transferring cryptograms, called Share Transfer Problem, in secure distributed storage systems, and proposed a method to reduce the Share Transfer Problem into the Steiner Tree Problem. Moreover, I proposed several methods to realize distributed database systems by using the secret sharing scheme.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２００７年度	９００，０００	０	９００，０００
２００８年度	１，１００，０００	３３０，０００	１，４３０，０００
２００９年度	１，０００，０００	３００，０００	１，３００，０００
年度			
年度			
総　計	３，０００，０００	６３０，０００	３，６３０，０００

研究分野：総合領域
科研費の分科・細目：情報学・計算機システム・ネットワーク
キーワード：ネットワーク，アルゴリズム，インターネット高度化，大規模ファイルシステム

１．研究開始当初の背景

ネットワーク上で情報を最小コストで配信する問題は以前から多くの研究がなされており，今後のネットワーク社会の発展に伴いさらに重要な問題となってくると考えられる。これらの問題としてデータ転送問題，ファイル配置問題などが知られている。これらの問題ではネットワークのコストは考慮されてい

るが途中の計算コストは考慮されていない。本申請課題ではネットワーク上でデータを目的地まで配送する場合に，途中でデータに対してある種の処理を施す必要がある場合を対象とする。例えば映像データをレート変換しながらマルチキャストする場合などが対象システムの例として挙げられる。このような問題を配送問題と呼ぶことにする。

申請者らは秘密分散共有法の一種である(k, n) しきい値法を利用した秘密分散ストレージシステム（以下SSSS: Secret Sharing Storage System と呼ぶ）を提案している。SSSS では秘密データから(k, n) しきい値法を用いてn 個のシェアと呼ばれる符合データを生成し，シェアを分散配置する。データの復号にはk 個のシェアを集めればよい。SSSS は(k, n)しきい値法を利用しているため，従来のネットワークストレージシステムに対して，よりネットワークやハードウェアの障害に強く，より秘密データの盗聴に強いなどの利点を有している。しかし，秘密分散共有法における符号化・復号化処理は多くの時間がかかり，その高速化が重要な課題の一つであった。また，ネットワークのトポロジーに対して最適なシェア配送や，SSSSを用いた分散データベースの実現など様々な課題があった。

２．研究の目的

(1) 配送問題に対する検討

過去の研究において開発したシステムでは一つのサーバですべてのシェアを作成し，他のサーバへ送信している。しかし，シェアの計算には一つの秘密情報あたり kn 回の掛け算が必要である。また，格納するデータ全部を一回の演算で暗号化することは出来ず，いくつかのブロックに分割して暗号化を行う必要があり，暗号化における計算負荷が問題点の一つであった。

SSSS における符号化処理は分散処理が可能であるため，符号化とデータ転送を同時にすることを考えれば，SSSS におけるデータ格納問題は配送問題に帰着される。

本研究では配送問題の複雑さを数理的な枠組みの中で明らかにし，効率化のための方策について検討する。

(2) SSSS を用いた分散データベース実現のための基本設計

近年，個人情報の漏えい事故が多発しており，データベースセキュリティに対する注目が高まっている。分散データベースは集中データベースよりも拡張性が高く，負荷分散が可能という利点がある。しかし，分散データベースではデータが複数箇所に配置されるためデータの機密性や完全性の保護が難しい。機密性，完全性の高いデータ分散符号化の方法として秘密分散共有法が挙げられる。 そこで分散データベースを構築するサーバ同士が，秘密分散共有法を用いてデータを分散共有することによって上記の問題を解決できると考えられる。 本研究では，ユーザのなりすましなどの脅威に対するシステム全体としての機能及び各機能におけるサーバの動作を設計する。

(3) 分散クエリの最適化

秘密分散共有法を用いた分散データベースでは，(k, n) しきい値法によりデータをn 個のシェアに暗号化し，ネットワークで介されたデータベースでシェアを分散共有している。ユーザからの要求に返答するためには元のデータを復号化する必要があり，I/O コストが通常の分散データベースシステムより高くなってしまう。また，シェアを集めることでどのデータベース上でもフラグメントを復号化できるという特殊性を持つ。本研究は，秘密分散共有法を用いた分散データベースのこの特殊性を考慮してユーザからの要求を文字列で表現したクエリの最適化に関する新しい手法の提案を行う。

３．研究の方法

(1) 配送問題に対する検討

2007 年度においては，SSSS におけるデータ格納作業の効率化のために，配送問題の複雑さ，および近似解法についての検討を行った。

(2) SSSS を用いた分散データベース実現のための基本設計

2008 年度においては，SSSS を用いた分散データベース実現のために，その基本設計を行った。脅威モデルを構成し，分散認証局などの概念を用いて安全な分散データベース実現に向けて検討を行った。

(3) 分散クエリの最適化

2009 年度においては，SSSS を用いた分散データベースにおいて重要な問題である，分散クエリの最適化について検討を行った。分散クエリ最適化のための定式化を行い，最良優先探索に基づくアルゴリズム設計を行った。

４．研究成果

(1) 配送問題に対する検討

秘密分散共有法における符号化・復号化処理問題をシェア配送問題として定式化した。シェア配送問題は組み合わせ最適化問題であり，その解法を検討するに当たり計算複雑度の検討が必要不可欠である。検討の結果シ

表１　シェア配送問題に対するヒューリスティックアルゴリズム評価実験結果の一例。上段の数値は最適解に対する評価値の比。下段の数値は求解に失敗した例題数。Pruned-MST は Shortest-Paths や WWW に対して評価値がかなり悪いことが分かる。

	Pruned-MST	Shortest-Paths	WWW
Best	1	1	1
Mean	1.40	1.01	1.01
Worst	2.33	1.17	1.17
Fail	0	0	0

ェア配送問題が NP 困難であるという知見を得た。

また，シェア配送問題をスタイナー木問題に帰着させる方法を提案し，シェア配送問題をヒューリスティック手法により解くことを可能とした。また，Pruned-MST 等の 4 種類のスタイナー木問題に対する既存のヒューリスティックアルゴリズムについて，計算機上で比較実験を行い（表１），最短路木を用いる方法が有効であることの知見を得た。

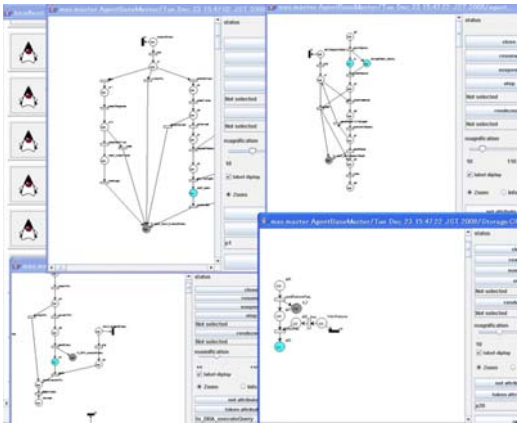

図１　MAN 実行モデルの実行状況。分散データベースを構成する各種機能毎の動作モデルをペトリネットを用いて作成し，実行している状況。

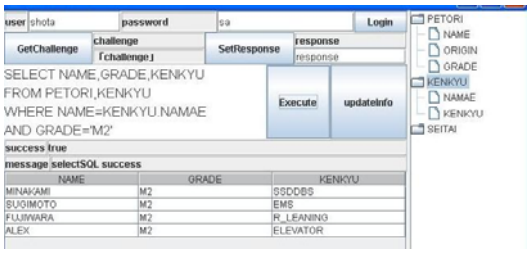

図２　データベースインターフェース。

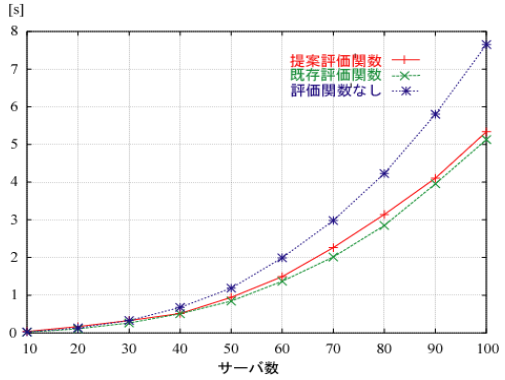

図３　分散クエリ最適化アルゴリズムの計算時間の比較。

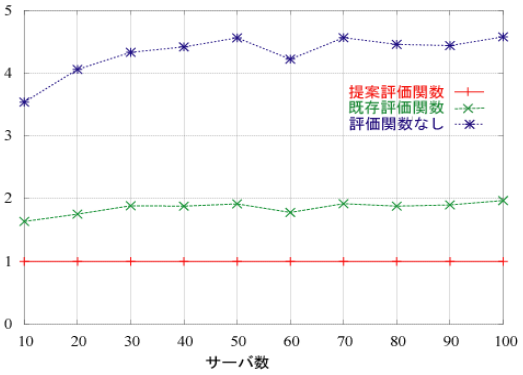

図４　分散クエリ最適化アルゴリズムの解の質の比較。提案手法は既存手法と同程度の計算時間で良質の解を導出することに成功している。

(2) SSSS を用いた分散データベース実現のための基本設計

SSSS を用いた分散データベースの実現に向けて，脅威モデルに基づいてデータベースの基本的な動作要求に対する動作を設計し，秘密分散共有法を用いた分散認証局や耐故障性のある分散アルゴリズムを用いることにより，より秘匿性の高い分散データベースを実現することが出来た。また，ペトリネットを拡張したマルチエージェントネット（MAN）を用いて実装した（図１，図２）。MAN の実行環境を用いて設計したモデルの動作検証を行い，データ配送を含めた最適化が重要であることの知見を得た。

(3) 分散クエリの最適化

秘密分散共有法を用いた分散データベースにおける分散クエリ最適化について検討を行った。クエリ処理効率化のための最適化問題を定式化し，発見的手法を提案した。また，計算機実験によって提案手法の有効性を示し，その結果を論文報告した（図３，図４）。

秘密分散共有法を用いた分散データベースは他に類を見ないものであり，重要情報を安全に保管する上で今後ますます必要とされる技術である。上記(1)，(2)，(3)で得られた知見は SSSS を用いた分散データベースの実現において重要な結果である。

５．主な発表論文等
（研究代表者，研究分担者及び連携研究者には下線）

〔雑誌論文〕（計５件）
(1) T. Miyamoto and T. Ikemura, ``Subquery Allocation Problem and Heuristics for Secret Sharing Distributed Database System'', Journal of Computer Systems, Networks, and Communications, 査読有, Vol.2010, Article ID 984059, 2010, 6 pages.

(2) 水上翔太，宮本俊幸，``秘密分散共有法を用いた分散データベースシステムの設計及び実装''，電子情報通信学会技術研究報告，査読無，Vol.108，no.415，2009，pp.51-56.

(3) T. Miyamoto and S. Kumagai, ``An Optimal Share Transfer Problem on Secret Sharing Storage Systems'', IEICE Trans. Fundamentals, 査読有, Vol.E90-A, no.11, 2007, pp.2458-2464.

(4) 水上翔太，宮本俊幸，熊谷貞俊，``秘密分散共有法を用いた分散データベースシステムのマルチエージェントネットによる実現について''，電子情報通信学会技術研究報告，査読無，Vol.108，no.362，2007，pp.1-6.

(5) T. Miyamoto and S. Kumagai, ``An Optimal Share Transfer Problem on Secret Sharing Storage Systems'', Lecture Notes in Computer Science, 査読有, Vol.4742, 2007, pp.371-382.

〔学会発表〕（計３件）
(1) 水上翔太，``秘密分散共有法を用いた分散データベースシステムの設計及び実装''，電子情報通信学会 コンカレント工学研究会，2009 年 1 月 29 日，神奈川県産業振興センター，横浜市.

(2) 水上翔太，``秘密分散共有法を用いた分散データベースシステムのマルチエージェントネットによる実現について''，電子情報通信学会 コンカレント工学研究会，2007 年 11 月 30 日，新潟大学，新潟市.

(3) T. Miyamoto, ``An Optimal Share Transfer Problem on Secret Sharing Storage Systems'', 5th International Symposium on Parallel and Distributed Processing and Applications, 2007 年 8 月 30 日，ナイアガラフォールズ，カナダ.

６．研究組織

(1)研究代表者
宮本　俊幸（MIYAMOTO　TOSHIYUKI）
大阪大学・工学研究科・准教授
研究者番号：00294041

(2)研究分担者
（　　）

研究者番号：

(3)連携研究者
（　　）

研究者番号：