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２１日現在

研究種目：若手研究(B)
研究期間：2008～2009
課題番号：20700073
研究課題名（和文）大容量データに適した秘密分散法に関する研究

研究課題名（英文） Secret Sharing Schemes for Large Data

研究代表者
栃窪　孝也（TOCHIKUBO KOUYA）
日本大学・生産工学部・講師
研究者番号：60440038

研究成果の概要（和文）：
これまで秘密分散法のネットワーク接続型ストレージへの適用の検討は行なわれていたが、従来の(k, n) しきい値法では秘密情報の分散・復元には複雑な計算が必要だったため有効なシステムは提案されていなかった。本研究では、高速に秘密情報の分散・復元ができる秘密分散法を用いた秘密分散システムを開発し、これまで実現することができなかった機密性と可用性とを両立する実用的なシステムを実現した。また、(k, n) しきい値法以外の柔軟なアクセス構造を実現可能な効率のよい秘密分散法を提案した。

研究成果の概要（英文）：
We have proposed an efficient storage network system using fast secret sharing schemes. The proposed system can compute shares from the secret and recover the secret efficiently only using XOR operations. Furthermore, we have proposed secret sharing schemes for general access structures. For any access structure the proposed schemes are more efficient than general secret sharing schemes which are based on minimal access structures.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２００８年度	700,000	210,000	910,000
２００９年度	500,000	150,000	650,000
年度			
年度			
年度			
総　計	1,200,000	360,000	1,560,000

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：ネットワークセキュリティ技術、データストレージ、セキュア・ネットワーク

１．研究開始当初の背景

秘密分散法とは、暗号で利用する鍵などの秘密情報の安全な保管で利用され、情報の盗難対策と紛失対策の両方に有効な情報化社会においてニーズの高い技術であるといえる。一般に、紛失の対策として情報のコピーを作成することは効果的であるが、この場合、その分だけ盗難のリスクが高くなる。秘密分

散法の基本原理であるしきい値秘密分散法((k, n) しきい値法) では、秘密情報をn 個の分散情報に分割し、得られた分散情報を n 人の管理者が管理する。秘密情報を復元する場合は、n 人の管理者の中から任意のk 人が集まり、管理している分散情報を用いて元の秘密情報を計算する。この手法は、任意の k 個の分散情報を集めれば元の秘密情報が復元できるが、k-1 個の分散情報からでは元の秘密情報に関する情報がまったく得られないということ(完全性) が情報理論的に証明されている。このため、分散情報の一部が漏えいしても元の秘密情報は安全であり、また、分散情報の一部を紛失しても元の秘密情報を復元することが可能な情報の管理を実現することができる。

また、国内で個人情報保護法が施行されてから、情報の保護に対する関心が高まり、一般にもセキュリティを確保するという考え方が浸透したといえる。しかし、個人情報取扱業者から経済産業省へ報告があった個人情報の漏えい事案では、PC やメモリの盗難や紛失が多く、PC のハードディスクや USB メモリ等の持ち運び可能な記録媒体での有効な情報の保護方法が必要となっている。このため、従来から利用されてきた暗号化技術に加え、秘密分散法が注目され、さまざまな製品の開発が盛んに行なわれている。また、情報の保護には技術的な問題以外に人的要因も関係するので、重要な情報は持ち出さないというポリシーのもので、データはサーバに保存し、外出先ではシンクライアントを利用する企業が増えてきている。このため、サーバ等に保存されている大容量データに秘密分散法を適用する試みがなされているが、大容量データに対する秘密分散は実用化されていないのが現状である。

２．研究の目的

前述したように、これまで秘密分散法のネットワーク接続型ストレージへの適用の検討は行なわれていたが、従来の(k, n) しきい値法では秘密情報の分散・復元には複雑な計算が必要だったため有効なシステムは提案されていなかった。本研究では高速に秘密情報の分散・復元ができる秘密分散法によるネットワーク接続型ストレージを開発することでこれまで実現することができなかった機密性と可用性とを両立する実用的なシステムを実現することが目的である。しかしながら、以下の２つの問題のため大容量データに対する秘密分散は実用化されていない。

1 つ目は秘密分散法には秘密の分散・復元処理の演算量に関する問題である。一般的な(k, n) しきい値法は、大きな素数 p により定まる有限体 Z_p における f(0) の値を秘密情報としたk-1 次曲線f(x) 上のn 点を分散情報とする。秘密情報を復元する際には、k 個の分散情報(f(x) 上のk 点) からf(x) を一意に求めることにより秘密情報(f(0)) を計算する。したがって、秘密情報の分散・復元の処理では k-1 次式の演算が必要となり、暗号化鍵等の少量のデータの場合は秘密情報の分散・復元の計算量は問題にならないが、その計算量から、大量のデータの場合には適用することが難しい。

2 つ目は、分散情報のサイズに関する問題である。秘密情報を復元する権限を持つ管理者のグループの集合(アクセス構造) という観点でみると、(k, n) しきい値法のアクセス構造は、n 人の分散情報の管理者のうち、任意のk 人以上のグループの集合となり、非常に限定的な場合を実現していることになる。そこで、アクセス構造を限定しない秘密分散法(一般アクセス構造を実現する秘密分散法) に関する研究が多数行なわれているが、どの手法も管理者に多数の分散情報を割当てることで実現しており、元の秘密情報と管理者が管理する分散情報の比(情報比) に着目すると、(k, n) しきい値法のように方式が最適な場合の情報比が 1 であるのに対し、これまで知られている手法の情報比は非常に小さくなり、効率的ではなかった。

上記の２つの問題を解決し、高速に秘密情報の分散・復元できる秘密分散法によるネットワーク接続型ストレージを実現することで、一のストレージデバイスが盗難にあっても元の秘密がまったく流出せず、かつ、一部のストレージデバイスが地震等の災害で利用不可能になっても元の秘密情報を復元可能なストレージシステムを構築可能となる。さらに、提案方式はネットワーク接続型のストレージに限らず、PC やサーバの HDD で利用される RAID、ユビキタス環境でのシンクライアントによる機密情報の持ち出しや USB メモリによるデータの運搬などさまざまな応用が考えられ、その波及効果は計り知れない。

３．研究の方法

大容量データに適した秘密分散法の研究については、高速に秘密情報の分散・復元が可能な秘密分散法の研究が最近になって活発に行なわれており、大容量データに対する秘密分散法の実用化の道筋ができたといえる。本研究では、これまで研究代表者らが提案した方式を基に大容量データを高速に分散・復元可能な秘密分散法を検討し、NFS(Network File System)、SAN(Storage Area Network)や NAS(Network Attached Storage) などのネットワーク接続型のストレージへの適用を検討する。さらに、本研究では、検

討した秘密分散法を実装し、その有効性を検証する。

次に、より柔軟な秘密管理の可能な高速な秘密分散法についての研究方法を述べる。複数のストレージデバイスで秘密情報を分散する場合、ストレージデバイスやその使用環境に応じてストレージデバイスのセキュリティレベルを定義することができる。セキュリティレベルの異なるストレージデバイスを用いる場合、セキュリティレベルの高いストレージデバイスならば2つの分散情報から元の秘密情報が復元でき、セキュリティレベルの低いストレージデバイスならば4つの分散情報から元の秘密情報が復元できるといった柔軟な管理方法を実現することで、セキュリティを低下させることなく保存するデータ量を全体として減らすことが可能となる。研究代表者はこれまで任意のアクセス構造を実現する秘密分散法をテーマとして研究を行なっており、従来の方式より非常に効率のよいものを提案している。そこで、より柔軟なアクセス構造を効率よく実現可能な秘密分散法の検討も行なう。

４．研究成果

(1) 大容量データに適した秘密分散法の研究

本研究では、UNIX で利用されている NFS(Network File System)に Null ファイルシステムを使用し、write/read オペレーションに分散/復元モジュールを組み込むことで、秘密分散法ファイルシステムを実現している。

NFS は、1985 年に開発されたファイルシステムであり、UNIX で標準的に使われている。NFS は、UFS などのローカルファイルシステムと同じく、ファイルシステムの一種として実装されている。このため、NFS を利用している場合、ユーザにとってはローカルなディスクを読み書きする場合も、離れた場所にあるマシンのディスクを読み書きする場合とでも大きな違いはない。このような透過的なネットワークを構成することができるのが NFS の特徴である。 NFS の利用によって、同じファイルを複数のマシンからアクセスすることが可能になるため、ディスクスペースの節約につながることや、データを一箇所に集中できるため、管理が簡単になるなどが挙げられる。 また、Null ファイルシステムとは、既存のファイルシステム上の任意の位置にマウントすることが可能であり、新しいファイルシステムを開発する際のテンプレートとして用いられている。このため、予めクライアント/サーバ間を NFS(Network File System)でマウントしておくと、Null ファイルシステムに NFS を組み込む必要がない。

本研究で開発した秘密分散システムでは、ユーザにファイル操作を意識させずに秘密分散処理を行うことが可能であるのが特徴である。また、提案システムでは、2005 年に藤井らによって提案された高速な(2,n)しきい値法を用いている。この秘密分散法は、排他的論理和のみで実現可能であり、従来の方法よりも非常に処理が高速である。以下では(2,3)しきい値法を用いて、元の情報 S を分散/復号する場合の手順について説明する。

分散アルゴリズム：

- 2d bit の元の情報 S を、d bit の S_1 と S_2 に分割する。
- d bit の乱数 K_1、K_2 を生成する。
- 3つの分散情報 W_1, W_2, W_3 を以下の図1のような計算を行い生成する。

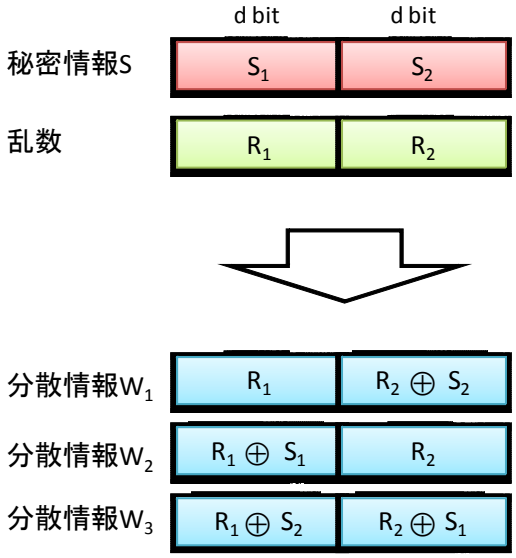

図１　秘密分散処理の概要

復元アルゴリズム：
k=2 なので、任意の分散情報を2つ取得する。
分散情報を用いて、以下のような計算を行い、元の情報 S を取得する。

分散情報 W_1, W_2 を取得した場合：

$$S_1 = R_1 \oplus (R_1 \oplus S_1)$$
$$S_2 = (R_2 \oplus S_2) \oplus R_2$$

分散情報 W_1, W_3 を取得した場合：

$$S_2 = R_1 \oplus (R_1 \oplus S_2)$$
$$S_1 = (R_2 \oplus S_2) \oplus (R_2 \oplus S_1) \oplus S_2$$

分散情報 W_2, W_3 を取得した場合：

$$S_1 = R_2 \oplus (R_2 \oplus S_1)$$
$$S_2 = (R_1 \oplus S_1) \oplus (R_1 \oplus S_2) \oplus S_1$$

次に、秘密分散法ファイルシステム用いた分散/復元時の処理手順について説明する(図 2)。

分散手順：
- ユーザプロセスより、write システムコールが発生する。
- write オペレーションは、分散を行う元の情報を読み出し、分散モジュールで元の情報から分散情報を 3 つ生成する。
- 分散モジュールで作成した 3 つの分散情報をサーバ A、サーバ B、サーバ C に書き込む。

復元手順：
- ユーザプロセスより、read システムコールが発生する。
- read オペレーションは、サーバ A、サーバ B、サーバ C の中に保存されている 3 つの分散情報のうち 2 つを読み込む。
- read オペレーションは、復元モジュールで元の情報を復元する。

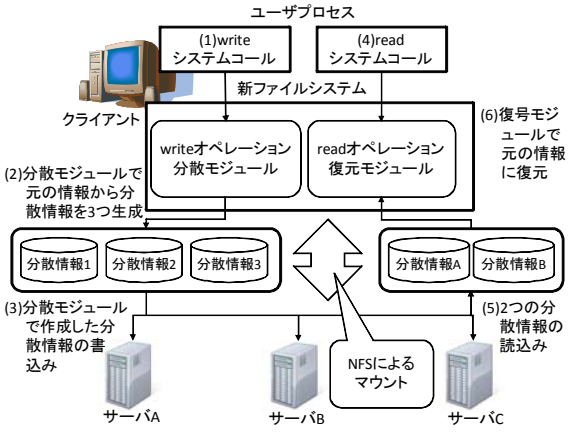

図 2　開発したシステムの構成

本研究では提案システムと従来のシステムを実装し、秘密分散処理の処理時間測定を行った。実験では、提案システムが非常に高速なことがわかった。

(2) 柔軟なアクセス構造を実現可能な効率のよい秘密分散法の検討

(k, n)しきい値法のようなある特別なアクセス構造を実現する秘密情報分散方法ではなく、ある管理者の集合に対して、任意のアクセス構造を実現する秘密分散情報として、1887 年に伊藤、斎藤、西関が分散情報の管理者に複数の分散情報割り当てる複数割り当て法を提案している。また、他の手法としては、1988 年に Benaloh と Leichter による単調回路の理論を応用した手法等が提案されている。伊藤、斎藤、西関の手法や Benaloh と Leichter の手法は、分散情報の割り当て方法が簡単ではあるが、アクセス構造によっては、各管理者が管理する分散情報の数が膨大な数になってしまう場合が生じる。研究代表者は、2008 年に伊藤、斎藤、西関の手法よりも任意のアクセス構造に対して分散情報の管理者に割り当てられる分散情報の数を削減可能な効率よい手法を提案しており、2005 年に Benaloh と Leichter の手法よりも効率のよい手法を提案している。

本研究では、2005 年に提案している Benaloh と Leichter の手法よりも常に効率のよい手法を改良し、さらに効率のよい手法を 2 つ提案した。提案手法は、(k, n)しきい値法と同様に秘密を復元する権利のない管理者の分散情報を集めても元の秘密情報の情報が全く分からない完全な手法であること証明している。また、提案手法は(k, n)しきい値法で実現されるアクセス構造に提案手法を適用する場合、(k, n)しきい値法と一致することも証明しており、さらに、従来の手法に比べどれくらい効率がよいかを明らかにしている。この手法を用いることで、(k, n)しきい値法では実現できないアクセス構造に対しても秘密分散を効率よく実現することができる。なお、本研究で得られた成果は学会誌に投稿中である。

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）

〔学会発表〕（計２件）

①川田　大，　高速な秘密分散法を用いたストレージネットワーク，電子情報通信学会 2010 年総合大会(2008.03.18)，東北大学

②K. Tochikubo, A construction method of secret sharing schemes based on authorized subsets, Proc. of 2008 International Symposium on Information Theory and its Application (ISITA2008) (2008.12.08), New Zealand

６．研究組織

(1)研究代表者

栃窪　孝也（TOCHIKUBO KOUYA）

日本大学・生産工学部・講師

研究者番号：60440038