論文 / 著書情報
Article / Book Information

題目(和文)	秘密分散とその変換プロトコルに関する研究
Title(English)	A Study on Secret Sharing with Share Conversion
著者(和文)	菊池亮
Author(English)	Ryo Kikuchi
出典(和文)	学位:博士（工学）, 学位授与機関:東京工業大学, 報告番号:甲第9976号, 授与年月日:2015年9月25日, 学位の種別:課程博士, 審査員:尾形　わかは,植松　友彦,山田　功,松本　隆太郎,田中　圭介
Citation(English)	Degree:, Conferring organization: Tokyo Institute of Technology, Report number:甲第9976号, Conferred date:2015/9/25, Degree Type:Course doctor, Examiner:,,,,
学位種別(和文)	博士論文
Category(English)	Doctoral Thesis
種別(和文)	論文要旨
Type(English)	Summary

（博士課程）
Doctoral Program

論 文 要 旨

THESIS SUMMARY

専攻： Department of	集積システム　専攻	申請学位（専攻分野）： Academic Degree Requested	博士　（　工学　） Doctor of
学生氏名： Student's Name	菊池 亮	指導教員（主）： Academic Advisor(main)	尾形 わかは 教授
		指導教員（副）： Academic Advisor(sub)	

要旨（和文 2000 字程度）
Thesis Summary（approx.2000 Japanese Characters ）

本論文は，「A Study on Secret Sharing with Share Conversion（秘密分散とその変換プロトコルに関する研究)」と題し，英文６章より構成されている．
第１章「Introduction（はじめに)」では，まず，データを複数のシェアに分割して分散管理することにより安全にデータを保管することのできる技術である秘密分散と，その応用として，個々のデータは秘密にしたまま分析結果のみを得ることができる秘密計算を紹介し，近年のデータ活用においてはこれらが重要な役割を果たすことが期待されていることを述べている．また，秘密計算を実社会で用いる場合，秘密分散には，シェアが小さいことを示す「コンパクト性」と，より効率的な秘密計算が可能であることを示す「秘密計算への拡張性」の２つの性質が要求されるが，これらを兼ね備える秘密分散方式の構築が困難であるという課題を説明している．その上で，本論文では，コンパクト性を持つ秘密分散方式と秘密計算への拡張性を持つ秘密分散方式とを相互に変換するプロトコルを構築し，２つの秘密分散方式を必要に応じて変換して併用するアプローチを提案することにより，課題を解決することを述べている．
第２章「Preliminaries（準備)」では，必要な記号の定義や，以降で提案する秘密分散方式の構成要素として用いられる疑似乱数生成器や Information dispersal algorithm（情報分割アルゴリズム）の定義を与えている．
第３章「Secret Sharing（秘密分散)」では，秘密分散の安全性として，攻撃者の計算能力を限定しない情報理論的安全と，攻撃者の計算能力を高々問題の長さの多項式に制限した計算量的安全の２つの定義を与えている．また，複数の秘密分散方式を包含する種々のクラスについて説明し，秘密計算への拡張性またはコンパクト性を持つ既存の秘密分散方式を紹介している．
第４章「New Computationally-Secure Secret Sharing Schemes（新しい計算量的安全な秘密分散方式)」では，コンパクト性を持ち計算量的安全な秘密分散方式を２つ提案している．これらは，コンパクト性を持ち計算量的安全な Krawczyk の手法を，効率的で安全な変換プロトコルが構成できるように変更したものである．１つ目の提案方式は，結託しきい値をｔとした場合，シェア生成時にｔ＋１個の疑似乱数を用いて秘密データをマスクしている．２つ目の提案方式では，秘密データはより多くの疑似乱数によりマスクされ，１つ目の方式に比べシェアは大きくなるが，より安全性の高い変換プロトコルが構築可能となる．
第５章「Share-Conversion Protocol（変換プロトコル)」では，まず，ある秘密分散方式から他の秘密分散方式への変換を可能とする変換プロトコルを定義し，変換プロトコルの安全性として，攻撃者が盗聴のみを行うと仮定する受動的攻撃に対する安全性と，攻撃者は改ざん等の任意の攻撃を行う能動的攻撃に対する安全性の，２つの定義を与えている．それぞれの安全性は，攻撃者の計算能力の制限の有無により計算量的安全および情報理論的安全に二分されるため，安全性の設定は合計４つとなる．次に，４つの安全性の設定それぞれにおいて，コンパクト性を持つ秘密分散から秘密計算への拡張性を持つ秘密分散への変換プロトコルおよび逆方向の変換を行うプロトコルを提案している．さらに，情報理論的安全かつ能動的攻撃者に対して安全な変換プロトコルの構成において，シェアから秘密データを復元する手順の効率化を行っている．秘密データの復元は秘密計算などにおいても頻繁に行われる処理であり，この効率化は他の用途においても応用可能であると考えられる．
第６章「Concluding Remarks（結論)」では，本論文の成果を要約している．
以上を要約すると，本論文は，秘密計算を実用に供するために秘密分散に求められる２つの性質を指摘し，これらを同時に達成することが困難である現状において，一方の性質を持つ秘密分散から他方の性質を持つ秘密分散へ変換することで，２つの性質を両立させることが可能であることを示したものである．

備考：論文要旨は、和文 2000 字と英文 300 語を 1 部ずつ提出するか、もしくは英文 800 語を 1 部提出してください。
Note：Thesis Summary should be submitted in either a copy of 2000 Japanese Characters and 300 Words (English) or 1copy of 800 Words (English).

（博士課程）
Doctoral Program

論 文 要 旨

THESIS SUMMARY

専攻： Department of	集積システム　専攻	申請学位（専攻分野）： Academic Degree Requested	博士　（　工学　） Doctor of
学生氏名： Student's Name	菊池 亮	指導教員（主）： Academic Advisor(main)	尾形 わかは 教授
		指導教員（副）： Academic Advisor(sub)	

要旨（英文 300 語程度）
Thesis Summary（approx.300 English Words ）

Secret sharing scheme (SS) has been extensively studied since SS is important not only as a method for storing data securely but also as a fundamental building block for multiparty computation (MPC). In recent years, MPC has been improved greatly in speed, and there are some demonstrations of practical use. Our observation is that an application of MPC requires SS of two properties, compact and MPC-friendly: The share-size of SS should be small and there must be MPCs that efficiently compute a high-level operation on the SS. However, these two properties are incompatible. Known compact SSs are not MPC-friendly and MPC-friendly SSs are not compact.

We employ an approach in which one can convert the shares of compact/MPC-friendly SS to those of MPC-friendly/compact SS to satisfy the two properties simultaneously. Therefore, we propose several SSs that are convenient to be converted and conversion protocols that are bidirectional conversion between compact and MPC-friendly SS.

There are two criteria of evaluating security of SS and conversion protocols. The first criterion is the computational power of adversaries, computational and information-theoretical security. The second criterion is adversary's behavior, passive and active security. It depends on scenes which setting we should choose. Therefore, we consider all scenes.

First, we propose two SSs with computational security that can be converted efficiently. We then propose conversion protocols in each setting. We have four settings, computational and passive, computational and active, information-theoretic and passive, and information-theoretic and active, and two directions, from compact SS to MPC-friendly SS, from MPC-friendly SS to compact SS. Therefore, we propose eight conversion protocols in total.

Our results enables one to store data compactly and perform MPC efficiently when needed. We believe that our new SSs and the conversion protocols accelerates the practical use of MPC.

備考 ： 論文要旨は、和文 2000 字と英文 300 語を 1 部ずつ提出するか、もしくは英文 800 語を 1 部提出してください。
Note : Thesis Summary should be submitted in either a copy of 2000 Japanese Characters and 300 Words (English) or 1copy of 800 Words (English).

注意：論文要旨は、東工大リサーチリポジトリ(T2R2)にてインターネット公表されますので、公表可能な範囲の内容で作成してください。
Attention: Thesis Summary will be published on Tokyo Tech Research Repository Website (T2R2).