秘密分散法を用いた
電子権利二次流通方式の研究

廣　田　啓　一

博士　(情報学)

総合研究大学院大学
複合科学研究科
情報学専攻

平成 20 年度
(2008)

2008 年 9 月

本論文は総合研究大学院大学複合科学研究科情報学専攻に
博士（情報学）授与の要件として提出した博士論文である.

審査委員：

主査	曽根原 登 教授	国立情報学研究所／総合研究大学院大学
	岡田 仁志 准教授	国立情報学研究所／総合研究大学院大学
	東倉 洋一 教授	国立情報学研究所／総合研究大学院大学
	山田 茂樹 教授	国立情報学研究所／総合研究大学院大学
	安田 浩 教授	東京電機大学／東京大学

（主査以外はアルファベット順）

A Study for Secure Rights Trading Method using Secret Sharing Scheme

Keiichi Hirota

DOCTOR OF
PHILOSOPHY

Department of Informatics
School of Multidisciplinary Sciences
The Graduate University for Advanced Studies (SOKENDAI)

September 2008

A dissertation submitted to
the Department of Informatics,
School of Multidisciplinary Sciences,
The Graduated University for Advanced Studies (SOKENDAI)
in partial fulfillment of the requirements for
the degree of Doctor of Philosophy

Advisory Committee:

Prof. Noboru Sonehara (Chair)	National Institute of Informatics/ The Graduated University for Advanced Studies
Assoc.Prof. Hitoshi Okada	National Institute of Informatics/ The Graduated University for Advanced Studies
Prof. Yohichi Tohkura	National Institute of Informatics/ The Graduated University for Advanced Studies
Prof. Shigeki Yamada	National Institute of Informatics/ The Graduated University for Advanced Studies
Prof. Hiroshi Yasuda	Tokyo Denki University/The University of Tokyo

(Alphabet order of last name except chair)

要旨

本研究は，近年著しく普及が進んでいる電子権利を対象として，利用者間で権利取引を行う二次流通を可能とする，安全かつ簡便な権利二次流通方式を実現することを目的とする．

従来の権利流通方式は，安全性を確保するために，公開鍵・秘密鍵の複雑な管理と電子署名や検証などの演算処理，端末間での複数回の通信処理を必要とし，直接的かつ同期的な権利流通に限られ，利便性に欠けていた．本研究では，利便性の問題を解決するために，有限体上の多項式を用いた比較的簡易な演算処理で情報量的安全性を実現する情報保管技術である秘密分散法の，権利流通方式への適用を検討し，秘密情報の一部分を一意に復元可能とする部分情報の復元制御が可能となる方式を考案した．また，これにより権利流通方式への適用を可能とし，権利取引に必要な情報を分散流通させることにより安全かつ簡便な権利取引を行う，新たな電子権利二次流通方式を実現した．

提案方式は口座管理型の電子権利を対象とするもので，譲渡元ユーザが生成した権利取引を宣言する取引情報を，秘密分散法を用いて分散符号化して流通させることで，秘密情報の解読や取引情報の改竄，偽造といった攻撃に対して安全な権利流通を可能とする．また，提案方式では，譲渡元ユーザと譲渡先ユーザ，権利管理機関の３者間において，最少となるただ２回の非同期なトランザクションで権利取引が完了するため，任意のコミュニケーション手段を使った取引情報の流通を行うことができ，また第三者への安全な権利取引の預託が可能となり，利便性の問題が解決される．

本研究の成果は，比較的簡易な演算処理で情報量的安全性を実現するセキュリティ技術である秘密分散法に着目し，秘密分散法を用いた新たな権利二次流通方式を実現したことにある．本研究で実現した権利交換プロトコルは，安全性だけでなく匿名性や健全性といった権利取引の要件を満たし，かつ取引情報の安全性が情報量的に保証されることを明らかにした．このため，従来の権利流通方式では困難であった，第三者への権利取引の預託が可能となった．

また，提案プロトコルに基づく C2B2C 型の権利二次流通システムを設計し，提案方式の安全性と利便性を理論的に示すだけでなく，その有用性を検証した．今後，技術とビジネス（市場）の関係にとどまらず，社会の規範（商習慣）や公共政策，法制度との関係を含めて提案方式を実用化する．

以下、本論文の構成とその概要について示す．

第１章では，本研究の背景を述べ，電子権利の流通市場と二次流通について示す．また，本研究が対象とする権利取引の要件と，既存の権利流通方式および権利流通システムの課題の簡単な整理を行い，本研究の目的を示した後に，本論文の構成を概観する．

第２章では，本研究が対象とする電子権利の定義とその実現方式，および権利流通のモデルについて整理した上で，従来研究の調査に基づいて既存方式の分類を行い，権利流通方式に求められる要求条件を整理する．また，権利流通方式の分類として，口座管理型の電子権利と価値保存型の電子権利のそれぞれについて概要を示し，既存の権利譲渡プロトコルおよび権利交換プロトコルの方式例を示す．さらに，本研究が

主眼とする電子権利流通の安全性と利便性の両立の観点から，既存方式に対する評価を行うとともに，既存方式の課題について示し，本研究で解くべき技術的課題について整理を行う．

第 3 章では，比較的簡易な演算処理により情報量的安全性を実現するセキュリティ技術である秘密分散法について概説し，権利流通方式への応用に向けた検討を行う．秘密分散法は，秘密情報を複数の分散情報に分散符号化することで秘匿化するもので，一定数未満の分散情報からは秘密情報を復元できず，情報量的に安全である．本研究では秘密分散法の従来手法における部分情報復元の原理を明らかにし，分散関数への適用を行うことで，特定の分散情報の組み合わせにより任意の部分情報一意な復元を可能とする，復元制御型の秘密分散法を考案した．考案方式について述べるとともに，低次の分散関数における構成例を示す．また，アクセス構造と情報量に関する既存手法との比較評価を行い，その安全性を示す．

第 4 章では，復元制御型の秘密分散法を用いた権利二次流通方式として，情報量的に安全な権利交換プロトコルについて示す．提案プロトコルは，口座管理型の電子権利を対象とするもので，電子権利の所有者が権利取引を宣言する情報を生成して複数の分散情報に分散符号化し，譲渡元ユーザと譲渡先ユーザおよび権利管理機関の３者間においてこの分散情報を流通させることで，権利取引を実行する．利便性の向上を目的にトランザクション数の削減を図って譲渡元ユーザから権利管理機関への分散情報の送付を不要とし，３者間において２回のトランザクションで権利取引が完了する，最少のトランザクション数による権利交換プロトコルを実現した．プロトコルの安全性および利便性についての評価を行い，その有効性を確認する．

第 5 章では，提案プロトコルを用いた権利二次流通システムの実現に向けて，まず C2B2C 型の権利取引を行う二次流通の市場モデルについて調査し，プロトコルの適用を検討する．市場モデルの比較の結果として，譲渡元ユーザによる権利取引の提案をブローカが仲介することにより取引機会の増加を図る，ブローカ仲介モデルによる C2B2C 型権利二次流通システムの設計を行った．電子チケットを対象とした権利二次流通システムの構成を示し，譲渡元ユーザおよび譲渡先ユーザの持つユーザクライアント，ブローカの持つ取引仲介サーバ，権利管理機関の持つ権利管理サーバのそれぞれにおける処理の概要と，各装置間のトランザクション，および権利取引の管理と制御について記述する．また，設計したシステムの安全性と利便性について議論し，その有用性を示す．

最後に第 6 章で本研究の成果をまとめるとともに，提案方式の実用化に向けた課題の整理を行って，本論文のまとめとする．

Abstract

This research aims to construct secure and usable rights trading method which enables trading electronic rights and its counter values among users in the area of secondary market for electronic rights which growing rapidly in recent years.

Conventional researches required complicated managements of public keys and private keys, heavy computations for the electronic signature and its verification and several transactions between clients, so the trading among users was limited to be direct and synchronous one and it lacked usability. In this paper, I investigated the application of the secret sharing scheme to rights trading method, which is a kind of secure information protection technology that enables unconditional secure storage of secret information by relatively light computation using polynomial function over finite field. I invented a novel scheme which enables partial reconstruction of the secret information that means a part of secret information is reconstructed specifically under the controlled conditions. Then I realized a novel rights trading method using proposed scheme, which enables secure and usable rights trading by dispersing and circulating the necessary information for trading rights and its counter values among users.

The proposal method handles the account-based electronic rights which are stored in users account held by rights manager and it circulates dispersed trading declaration information which declares the dealings of the electronic right that assignor holds using secret sharing scheme. So the protocol is secure against cryptoanalysis of dispersed trading declaration information and is also safe against interpolation and forgery of it. Furthermore, in addition to such strong safety, the proposal method completes trading within only two asynchronous transactions among the three players of assignor, assignee and rights manager, so users can trade their rights over any communication channel and can also entrust its trading declaration safely to other users so the proposal method improves the usability of rights trading.

The main contribution of this research is the realization of a novel rights trading method providing both strong security and high usability to users, by applying secret sharing schemes which is a kind of security techniques that promises unconditional security with relatively light computation. The rights trading protocol achieved in this research satisfies security requirements of rights trading such as anonymity and soundness as well as safety, and promises unconditional security of trading declaration information. Therefore it enables secure deposit of the rights trading declaration information to the third parties which is not allowed in conventional researches.

Moreover, I design C2B2C rights trading system based on the proposal method, show its strong security and high usability theoretically and proved its feasibility. In the future, I will put the proposal method to practical use considering not only relationship between the technology and the business (market) but

also relationships among social model (business manner), public policy and legal system.

This paper is organized as follows.

In Chapter 1, I describe the background and the purpose of this research and show the market of electronic rights trading and its secondary market. I also organize the security requirements of the rights trading which is the focus of this research, and outline the problems of conventional researches and systems, then I describe the main purpose of this research and show the overview of this paper.

In Chapter 2, I classify conventional rights trading methods based on survey of existing researches and organize the requirements of rights trading methods and clarify the point of discussion. As the classification of the rights trading methods, I first outline two types of electronic rights, account-based type and stored-value type, and then I show conventional protocol examples for both rights transfer and rights trading. Finally, I evaluate conventional approaches from viewpoint of both security and usability which is main subject of this thesis, and describe the problems of conventional rights trading methods and the technical problems which I try to solve in this research.

In Chapter 3, I focus on secret sharing schemes which is a kind of security techniques that promises unconditional security with relatively light computation, and make a study to apply it to rights trading method. Secret sharing schemes disperse and conceal the secret information into several dispersed informations (called shares). No one can reconstruct the secret information from such dispersed informations less than threshold, so schemes are said to be unconditionally secure. In this research, I elucidated the principle of partial reconstruction in conventional schemes and I invented reconstruction controlled secret sharing scheme which enables partial reconstruction of the secret under the controlled combinations of shares. I describe the proposed scheme and show some examples of construction of disperse function of low degree. I also discuss the security of the proposed scheme by evaluating access structure and information entropy compared to conventional schemes.

In Chapter 4, I propose unconditional secure rights trading protocol which is one of the achievements in this thesis and an application of reconstruction controlled secret sharing scheme described in Chapter 3. The proposal protocol handles the account-based electronic rights. It circulates dispersed trading information which is a declaration of dealings of the electronic right that assignor holds, and it enables to complete rights trading within 3 transactions among the 3 players of assignor, assignee and rights manager. Furthermore, I attempt to reduce the transactions for the purpose of improving usability, and introduce the idea of one time password to eliminate the transaction between assignor and rights manager. As a result, I established rights trading protocol of at least transactions which complete rights trading within only 2 transactions among 3 players. I discuss security and usability to confirm effectiveness of the proposed protocols.

In Chapter 5, I investigate the C2B2C rights trading market models and review the application of the proposed rights trading protocol to realize a practical rights trading system using proposed protocol. As a result of comparative estimation, I propose and design C2B2C rights trading system based on broker-mediated model which increases trading opportunity by depositing assignor's dispersed trading information to the broker. I show the construction of rights trading system for trading electronic tickets

among users, and describe the outline of processes, transactions and managements of rights trading on each components, user client which users use, broker server which brokers hold and rights management server which rights manager holds. I also discuss the design of the system guaranteeing both security and usability, and then I conclude its effectivity.

Finally, in Chapter 6, I organize the summary of the results in this paper and discuss additional challenges to realize the proposed rights trading method, and then I conclude the thesis.