SCIS 2002 The 2002 Symposium on Cryptography and Information Security
Shirahama,Japan, Jan.29-Feb.1,2002
The Institute of Electronics, Information and Communication Engineers

データ交換可能な多対多マッチングプロトコル

Matching oblivious tranfer: How to exchange valuable data

松尾真一郎* 尾形わかは*
Shin'ichiro Matsuo Wakaha Ogata

あらまし Internet 上の商取引の普及により，電子マネーと有料のデジタルコンテンツなど価値ある情報を直接交換するようなサービスが登場することが想定される．このようなサービスにおいては，利用者のプライバシを保護し，交換において不正がないことを保証する必要がある．本論文では，価値のある情報と電子マネーを，利用者の交換希望価格を秘匿しながらマッチングを行い，さらに価値のある情報と電子マネー自体をセキュアに交換する Matching Oblivious Transfer プロトコルを提案する．このプロトコルは，利用者が交換の注文を完了すると，その後のマッチングを行うセンタとの相互通信が必要ないという点で効率的である．

キーワード 紛失通信, マルチパーティープロトコル, 電子取引市場, マッチング

1 はじめに

背景 Internet の普及により, インターネットバンキングや, オンラインオークション, オンライン株取引などの電子商取引がインターネット上で実現されつつある．とりわけ, オンライン株取引の規模が急速に拡大している．これらのサービスでは, システムは 2 者間の契約を結ぶ部分のみをサポートしていて, 商品の流通や決済は別の手段によって実現している．しかし, 将来的に電子マネーや電子株券のような電子化された価値のある情報が普及すれば, 契約を行うだけでなく, 電子化された価値のある情報そのものの交換までをインターネット上で行うようになると考えられる．本論文では, これらの電子化された価値のある情報を安全に, かつ効率的に交換するための方式を提案する．このような取引システム（以下市場と記述）では, 複数の売り手と買い手が同時に存在する．売り手は電子データと引き換えに電子マネーを得たいと考え, 買い手は電子マネーの代わりに電子データを得たいと考える．このような市場では, 電子マネーと電子株券, 別の通貨の電子マネー, 電子チケット, 電子会員権, そして音楽や映画などのデジタルコンテンツと交換することが想定される．

このような電子市場を構築する場合, いくつかのセキュリティ機能を考慮する必要がある．市場は売り手や買い手の売買希望価格のプライバシを守る必要がある．また買い手はマッチした電子情報のみを受け取り, 売り手はマッチした電子マネーのみを受け取るようにしなければならない．

関連研究 受信者のプライバシを守ったまま，ある特定のデータだけを受信者に送信する場合, 紛失通信（Oblivious Transfer,OT）プロトコルが重要なツールとなる．$(1, N)$-OT プロトコルでは, 送信者は N 個のデータを送信し, 受信者はそのうちの任意の 1 つだけを得ることができる．ただしそのデータ以外の情報については何も得ることができない．また送信者は, 受信者がどのデータを受け取ったかを知ることができない [4]．OT のバリエーションとして, データ購入者がどのデータを購入したかというプライバシを守りながら安全にデジタルデータを販売するプロトコルが提案されている [7]．このプロトコルでは, 購入者は購入したデータ以外のデータを得ることができない．しかし，このプロトコルでは売り手は 1 人である．また, 価格に応じたマッチングの機能を持たない．

一方,1 人の売り手と複数の買い手におけるプライバシを守ったマッチングシステムは Sealed-bid Auction Protocol として知られている [13]．しかし, このプロトコルは複数の売り手を扱うことができない．プライバシを守りながら複数の売り手と買い手のマッチングを行う最初のプロトコルは, 松尾と森田によって提案されている [1]．しかし, このプロトコルはマッチングと価格決定は行うが, データの交換は行わない．また, 通信回数が多いため大規模な市場に使えないという欠点が存在する．

電子的な株式システムについては McKenzie らによって電子株券を実現する方式が提案されている [2]．この方式では, 電子株券による株主の権利を保証する方式が

* 東京工業大学, 〒 152-0033 東京都目黒区大岡山 2-12-1, Tokyo Institute of Technology, 2-12-1, O-okayama, Meguro-ku, Tokyo, 152-0033, Japan, { matsuo, wakaha } @crypt.ss.titech.ac.jp

提案されている．また,Crescenzo は, 買いと売りの数量を秘匿する売買プロトコルを提案している [3]．しかし, この方式には売買希望価格に応じたマッチングの機能はない．

このように, 安全に複数の売り手と買い手のマッチングを行い，かつ電子データの交換まで行うプロトコルはこれまでに提案されていない．

本論文の結果　本論文では，OT の新たなバリエーションとして，Matching Oblivious Transfer という概念を提案する．この OT は，複数の売り手と買い手が存在する中で，売り手と買い手のプライバシとおよび電子データの秘匿性を守りつつ注文のマッチングとデータの交換を行うプロトコルである．本論文では，いくつかの暗号技術を用いた Matching Oblivious Transfer の実現例も挙げる．提案プロトコルは公平性，電子データの秘匿性と完全性，プライバシ，そして匿名性を持っている．また，一度売り手，買い手が市場に注文を行ったら，市場との間の相互通信が必要ない．よって，提案プロトコルは実用的であると言える．

2　Matching Oblivious Transfer

本章では，市場におけるマッチングとデータの交換を行うシステムとして Matching Oblivious Transfer という概念を提案する．市場で交換される価値のデジタル情報としては電子株券，電子チケット，電子会員権，音楽や動画などのデジタルコンテンツなどが考えられるが，以降では簡単のため，電子株券の売買の取引に限定する．また 1 つの市場は 1 種類の電子株券を扱うとする．

2.1　Matching Oblivious Transfer の機能

提案システムには，ある同じ会社の電子株券を，それぞれの売買希望価格で売りたい複数の売り手が存在する．一方，それぞれの売買希望価格で電子株券を購入したい複数の買い手が存在する．売り手と買い手をあわせて注文者と呼ぶ．また注文のマッチングを行うセンタである市場が存在する．売り手は売却したい電子株券と希望価格を含む売り注文を作成し，市場に送信する．同様に，買い手は代金の電子マネーと希望価格を含む買い注文を作成し，市場に送信する．市場は売り手，買い手から注文を受け取り，あるルールに基づいてマッチングを行う．

本論文では，一般的な市場で用いられている以下のマッチングルールを想定する．

1. 同じ希望価格の売り注文と買い注文をマッチングする．
2. 2 つ以上の同じ希望価格の売り注文，あるいは同じ希望価格の買い注文が存在する場合，先に市場に届いた注文を優先する，

これらのマッチングに必要な性質を以下に挙げる．

データ交換の正当性: 売り手 U_S の売り注文 O_S と，買い手 U_B の買い注文 O_B がマッチした場合，U_S は O_B に含まれる電子マネーを受け取り，U_B は O_S に含まれる電子株券を受け取る．

データの秘匿性: 市場は全ての電子マネーと電子株券を受け取ることができない．また全ての売り手は，マッチした電子マネー以外の電子マネー，電子株券を得ることが出来ない．全ての買い手は，マッチしたもの以外の電子株券，電子マネーを得ることができない．

希望価格の秘匿性: 全ての注文者，市場ともに，全ての注文の希望価格と，希望価格毎の注文数を知ることができない．

匿名性: 全ての注文者，市場ともに，マッチした電子マネー，電子株券を誰が受け取ったかを知ることができない．

交換データの完全性: 市場は，各注文の中の電子マネー，電子株券の正当性を検証することができる．また，市場は無効な注文を送った不正な注文者を追跡することができる．

市場と注文者によって行われるプロトコルが上記の性質を満たすとき，このプロトコルを Matching Oblivious Transfer プロトコルと呼ぶ．交換データの完全性は交換データの秘匿性と相反する性質であるが，市場の能力を複数のサーバに分散することにより，両方の性質を満たすことが可能である．

さらに以下の性質を持つことが望ましい．

注文者における処理の実用性: 注文者が市場への注文送信が完了した後は，注文者は市場と相互通信を必要としない．加えて，注文者が実行するプロトコルは計算量的に軽い．

2.2　通信モデル

本稿では, 匿名性の確保と注文後の相互通信の排除のため，以下のような通信モデルを使用する．

セットアップ 市場 M がシステムパラメータを設定し，公開する．

売り注文サブプロトコル 売り手 U_S が注文情報 O_S を作成し，市場に送信する．O_S が正当である場合，M は O_S をデータベース DB に格納し，情報 K_B を U_S に送信する．

買い注文サブプロトコル 買い手 U_B が注文情報 O_B を作成し，市場に送信する．O_B が正当である場合，

M は O_B をデータベース DB に格納し，情報 K_S を U_B に送信する．

ブロードキャストサブプロトコル M は DB に格納された情報をブロードキャストする．各注文者はブロードキャストされた情報を受信し，K_B あるいは K_S を使用して，マッチした電子マネーあるいは電子株券を受け取る．

3 基本的なツール

ここでは提案プロトコルで利用する基本的な暗号ツールについて説明する．

3.1 紛失通信

紛失通信（Oblivious Transfer:OT）は，送信者 Alice が受信者 Bob に複数のメッセージに送り，Bob は Alice が送信したメッセージのうちの 1 つのみを受信し，Alice は Bob がどのメッセージを受信したかを知ることができないという，2 パーティープロトコルである．$(1, N)$-OT[4] では，Alice が N 個のメッセージ $\{m_1, \ldots, m_N\}$ を Bob に送信し，Bob は受信するメッセージのインデックス $i \in \{1, \ldots, N\}$ を選ぶ．$(1, N)$-OT を実行した結果，Bob は m_i のみを受け取り，その他のメッセージについては何も得ない．また，Alice は i については何も得ない．効率的な $(1, N)$-OT プロトコルは Naor と Pinkas によって提案されている [5, 6]．

3.2 検証可能な秘密分散

秘密分散（Secret Sharing: SS）では，ディーラーが秘密 s を持ち，その秘密に対する n 個のシェアを作成する．そして，ディーラーは各シェアを n 人のプレーヤーに配布する．各プレーヤーは，自分に配られたシェアからは秘密 s を知ることができないが，ある定められたプレーヤーの集合が協力することによって s を復元することができる．(k, n) しきい値 SS は，$k-1$ 人のプレーヤーの協力では s は復元できないが，k 人以上のプレーヤーの協力により s を復元することができるしきい値 SS であり，Shamir によって提案された方式 [8] がある．

検証可能な秘密分散（Verifiable Secret Sharing: VSS）は，各プレーヤーが，自分に配付されたシェアが s から正しく計算されていることを検証できる SS である．VSS としては Ben-or らが提案した方式 [9] が有名である．

多くの SS は準同型性を持っている．すなわち，$\{S_{1,1}, S_{1,2}, \ldots, S_{1,n}\}$ を秘密 s_1 のシェア，$\{S_{2,1}, S_{2,2}, \ldots, S_{2,n}\}$ を秘密 s_2 のシェアとすると，s_1+s_2 は，$\{S_{1,1}+S_{2,1}, S_{1,2}+S_{2,2}, \ldots, S_{1,n}+S_{2,n}\}$ から復元することができる．準同型性を利用すると，分散されたシェアが 0 または 1 のシェアであることを証明する効率の良いプロトコルを作ることができる [12]．

3.3 マルチパーティープロトコル

マルチパーティープロトコルは，複数のパーティーがそれぞれ秘密に保持している値を秘匿しながら，それらの値を使って関数の値を計算する暗号プロトコルである．

任意の関数について，t 人に不正なパーティーがいたとしても安全に計算を行うことができるマルチパーティープロトコルがいくつか提案されている．これらには，OT と組み合わせ回路に基づくもの [10]，VSS とゼロ知識証明によるもの，SS と組み合わせ回路によるもの [11]，そして VSS と組み合わせ回路によるものなどがある．

3.4 暗号文の正当性証明

ある 1 つの平文 p を持っている prover と，複数の暗号文 $c_1, \ldots, c_n$ を持っている verifier がいると仮定する．この状況で，p が $c_1, \ldots, c_n$ のいずれかの平文であることを，該当する暗号文のインデックスを秘匿したまま証明することを考える．この証明は，ゼロ知識証明を用いることにより実現可能である．

4 提案プロトコル

4.1 システムモデル

市場 M のモデルとして以下を考える．電子株券の価格 i は $1 \leq i \leq l$ の範囲内にあるとする．M は以下のカウンタ，データベースを保持する．

C_i^S, C_i^B: 価格 i についての売り手用，買い手用のカウンタ．同じ i についてはそれぞれの初期値は同じである．

DB_S, DB_B: 売却用の電子株券，購入用の電子マネーを収めるデータベース．

DB_S に収められる電子株券は，それぞれの売買希望価格 i について C_i^S の値 c から一意に計算される共通鍵 $K_{i,c}^S$ で暗号化される．同様に，DB_B に収められる電子マネーは $K_{i,c}^B$ で暗号化される．これらの鍵は c によって一意に計算され，ある鍵から別の鍵が類推できてはいけない．このような鍵は RSA 暗号の暗号化関数 Enc，M の公開鍵 PkM を用いて以下のように生成できる．ここで，$a||b$ はデータ a と b の結合である．

$$
\begin{aligned}
K_{i,c}^S &= Enc < PkM > \{i||c||0\} \\
K_{i,c}^B &= Enc < PkM > \{i||c||1\}
\end{aligned}
$$

売り手が価格 P_S の売り注文を出したときは，売り注文サブプロトコルの結果，共通鍵 $K_{P_S,c}^B$ を受け取る．後のブロードキャストサブプロトコルで $K_{P_S,c}^B$ を使うことでマッチした電子マネーを受け取ることができる．同様に，買い手は買い注文サブプロトコルで共通鍵 $K_{P_B,c}^S$ を受け取り，ブロードキャストサブプロトコルでマッチした電子株券を受け取る．

4.2 基本プロトコル

ここでは，M が信頼できる機関であると仮定したプロトコルを考える．つまり，M は全てのプライベートな情報を公開しないと仮定する．

セットアップ M は全てのカウンタを初期化する．すなわち，M は乱数 r_i を生成し，以下のようにカウンタをセットする．

$$C_i^B = C_i^S = r_i \quad (i = 1, \ldots, l)$$

売り注文サブプロトコル 売り手 U_S が電子株券の売り注文を希望価格 P_S で M に送信するとする．ここで d_S を発行者による電子署名がついた電子株券とする．

Step1. U_S は価格情報 $O = \{o_1, o_2, \ldots, o_l\}$:

$$o_i = \begin{cases} 1 & i = P_S \text{ の場合} \\ 0 & \text{その他} \end{cases} \qquad (i = 1, 2, \ldots, l)$$

を作成する．U_S は O と d_S に電子署名を付与したものを注文情報 O_S として M に送信する．

Step2. M は O_S の正当性を検証する．最初に d_S に付与された発行者の電子署名を検証する．続いて M は $o_i (1 \leq i \leq l)$ のうちの 1 つだけが 1 で，その他が 0 であることを検証する．

Step3. M は d_S を暗号化するための鍵 $K^S_{P_S,c}$ と，マッチする電子マネー m_B を復号するための鍵 $K^B_{P_S,c}$ を作成する．ここで，c はカウンタ $C^S_{P_S}$ の現在値とする．

Step4. M は，d_S を $K^S_{P_S,c}$ で暗号化する．

$$EC = E_{K^S_{P_S,c}}(d_S)$$

ここで，$E_{K^S_{P_S,c}}(d_S)$ は，d_S を鍵 $K^S_{P_S,c}$ を用いて暗号化した結果を表す．

Step5. M は $K^B_{P_S,c}$ を U_S に送信し，EC を DB_S に格納する．

Step6. M はカウンタ $C^S_{P_S}$ の値を変更する．

$$C_i^S := C_i^S + o_i \quad (i = 1, \ldots, l)$$

買い注文サブプロトコル 買い手 U_B が電子株券の買い注文を希望価格 P_B で M に送信するとする．ここで m_B を発行者による電子署名がついた電子マネーとする．

Step1. U_B は価格情報 $O = \{o_1, o_2, \ldots, o_l\}$:

$$o_i = \begin{cases} 1 & i = P_B \text{ の場合} \\ 0 & \text{その他} \end{cases} \qquad (i = 1, 2, \ldots, l).$$

を作成する．U_B は O と m_B に電子署名を付与したものを注文情報 O_B として M に送信する．

Step2. M は，O_B の正当性を検証する．M は m_B の電子署名を検証するとともに，m_B の額面と O との整合性を検証する．また，O の正当性を売り注文サブプロトコルと同様に検証する．

Step3. M は鍵 $K^B_{P_B,c}$，$K^S_{P_B,c}$ を生成する．ただし c は現在の $C^B_{P_B}$ の値．

Step4. M は m_B を鍵 $K^B_{P_B,c}$ で暗号化する．

$$EP = E_{K^B_{P_B,c}}(m_B)$$

Step5. M は $K^S_{P_B,c}$ を U_B に送信し，EP を DB_B に格納する．

Step6. M はカウンタ C^B_i の値を変更する．

$$C_i^B := C_i^B + o_i \quad (i = 1, \ldots, l)$$

ブロードキャストサブプロトコル ブロードキャストサブプロトコルは定期的に実行される．

Step1. M は DB_S，DB_B の全てのコンテンツを全注文者にブロードキャストする．

Step2-S. U_S は DB_B 内の全ての暗号化された電子マネーを $K^B_{i,c}$ を用いて復号化し，得られた電子マネーの正当性を検証する．もし，マッチした電子マネーがあれば，U_S はその電子マネー m_B を受け取る．

Step2-B. 同様に U_B は DB_S 内の全ての暗号化された電子株券を $K^S_{i,c}$ を用いて復号しその正当性を検証する．

ここで，鍵はすべて異なるので，DB_S 内の全ての暗号化された電子株券 EC について以下が成り立つ．

$$D_{K^S_{i,c}}(EC) = \begin{cases} d_S & \text{EC がマッチする場合} \\ random & \text{その他} \end{cases}$$

すなわち，$K^S_{i,c}$ を持つ U_B はマッチした d_S のみを受け取り，同様に $K^B_{i,c}$ を持つ U_S はマッチした m_B のみを受け取る．

もし U_B の注文にマッチする電子株券が注文の時点で M に存在しないとしても，将来マッチする電子株券が DB_S に格納された場合，将来のブロードキャストでマッチした電子株券を得ることができる．同様に，U_S の注文にマッチする電子マネーが注文の時点で M に存在しないとしても，将来のブロードキャストでマッチした電子マネーを受け取ることができる．

4.3 市場サーバを分散させたプロトコル

M に対する秘匿性は，M の機能を n 台のサーバ $M_1, \ldots, M_n$ に分散させることによって実現できる．ここでは，n 台中の $k-1$ 台のサーバの不正に耐えるプロトコルについて基本プロトコルからの変更点を示す．

カウンタの加算　カウンタ値を準同型性を持った (k,n) しきい値 VSS を用いて n サーバに分割する．カウンタのシェアを $C^S_{i,j}, C^B_{i,j}(j=1,\ldots,n)$ とする．また，注文者は O を n 台のサーバに同じ VSS を用いて分散する．o_i のシェアを $o_{i,j}(j=1,\ldots,n)$ とする．カウンタの加算は VSS の準同型性を用いて実行する．

$$C^S_{i,j} := C^S_{i,j} + o_{i,j}(1 \le i \le l, 1 \le j \le n)$$

カウンタ値が秘密分散されているため，M 内の $k-1$ 台以下のサーバの結託では，カウンタの現在値やどのカウンタが更新されたかを知ることができない．

注文情報の正当性の検証　分散された価格情報 O の正当性，つまり o_i のうちの 1 つだけが 1 で残りが 0 であることを検証するためには以下を行えばよい．まず各サーバは配付されたシェア $o_{i,j}$ の総和 $\sum_{i=1}^{l} o_{i,j}$ を計算する．続いてそれらの総和から，元の秘密の総和 $\sum_{i=1}^{l} o_i$ を復元し，復元した結果が 1 であるかを検証する．その後，サーバと注文者の間で，全ての i についてシェア $o_{i,j}(1 \le j \le n)$ が 0 か 1 のシェアであることをゼロ知識証明を用いて証明する．

電子株券・電子マネーの正当性の検証　d_S, m_B とその署名は市場の複数のサーバに分散されているため，電子株券・電子マネーの正当性を検証するには，分散された署名の検証を行うマルチパーティープロトコルを市場のサーバの間のみで実行する．さらに電子マネーの場合には，注文情報に含まれる注文希望価格と，電子マネーの額面が一致していることを検証する必要がある．仮に，電子マネーの額面を表すデータ構造が価格情報 O と同一であるとすれば，VSS の準同型性を用いて，分散された額面のシェア $s^{m_B}_{i,k}$ と O のシェア $o_{i,j}$ の引き算を行う．

$$D_{i,j} = o_{i,j} - s^{m_B}_{i,k}(1 \le i \le l, 1 \le j \le n)$$

その結果を復元し，復元された結果が全て 0 であることを確認できれば，注文希望価格と電子マネーの額面が一致していることが確認できる．

鍵の生成とデータの暗号化　個々のサーバは注文者の希望価格を知ってはいけないので，データベースに格納すべき暗号化された電子データ，つまり正しい価格の正しいカウンタで暗号化された情報は，注文者と協力して作成しなければならない．そこで，全ての価格に対してカウンタの現在値から計算できる鍵を使って暗号文を作成し，$(1,l)$-OT を用いて注文価格に相当する暗号文を注文者に選んでもらうことにより，電子データの暗号化を行う．具体的には以下の通りに実行する（ここでは売り注文について説明する）．

サーバ群 $(M_1,\ldots,M_n)$ は以下のマルチパーティープロトコルを実行する．全ての価格に対してカウンタの現在値，注文の種類から鍵 $K^S_{i,c}$ を生成し，次に電子株券 d_S を $K^S_{i,c}$ を用いて共通鍵暗号で暗号化する．最後にこの結果を U_S の公開鍵 PkU_S で暗号化する．この結果，M は全ての価格 i について以下を得る．

$$EE_i = Enc < PkU_S > \{E_{K^S_{i,c}}(d_S)\}$$

ここで，各サーバは $K^S_{i,c}$ と $E_{K^S_{i,c}}(d_S)$ については何も得ないようなマルチパーティープロトコルを構成する．また，U_S に送付する $K^B_{i,c}$ についても，同様に全ての価格について計算する．

鍵の送付と暗号化情報のデータベースへの格納　鍵 $K^B_{P_S,c}$ の送付は $(1,l)$-OT を用い行う．$(1,l)$-OT では，注文者は配付される鍵のうちの任意の 1 つを得られるために，不正な注文者は注文情報 O_S と異なる価格の鍵を手にしてしまうことができる．またデータベースに格納する暗号文も O_S に合った鍵で暗号化されている必要がある．そこで，鍵，暗号文，O_B の整合性を取るために，M は以下を行うマルチパーティプロトコルを実行する．

全ての価格 i について，価格情報 O と同じデータ構造を持つ価格を表す情報 $O^{i,*} = \{O^{i,*}_1,\ldots,O^{i,*}_l\}$ を生成し，その情報を n 個のシェア $O^{i,*}_k$ に分散し，それぞれを PkU_S で暗号化する．また全ての価格 i に対して

$$K^B_{i,c} = k^{B,(1)}_{i,c} + k^{B,(2)}_{i,c}$$

となるようにランダムに鍵を分割し，$k^{B,(1)}_{i,c}$，$k^{B,(2)}_{i,c}$ を PkU_S で暗号化する．EE_i と合わせて DK_i を作成する．

$$\begin{aligned} DK_i \quad := \quad & \{EE_i, Enc < PkU_S > \{o^{i,*}_{1,1}\},\ldots, \\ & Enc < PkU_S > \{o^{i,*}_{l,n}\}, k^{B,(1)}_{i,c}\} \end{aligned}$$

次に，M は $(1,l)$-OT を使い DK_{P_S} を注文者に送信する．注文者は受け取った $O^{P_S,*}_k(1 \le k \le l, 1 \le j \le n)$ と $E_{K^S_{P_S,c}}(d_S)$ を M に送り返す．M は $O^{P_S,*}_k$ と，価格情報 O との整合性を VSS の準同型性と引き算を用いて検証する．まず，各サーバが

$$D_{k,j} := o_{k,j} - o^{P_S,*}_{k,j}$$

を計算し，$D_{k,j}$ から秘密 d_k を復元し，全ての d_K が 0 であることことを確認する．その後，暗号化された電子データが，EE_i のどれかの平文であることを 3.4 の方法を用い，証明する．以上の検証により，利用者が正しい $(1,l)$-OT を実行したことが検証でき，不正な注文者が注文価格でない鍵で電子データを暗号化することを防止する．

EE_i の検証が正しく終了した場合のみ，M は $k^{B,(2)}_{i,c}$ を再び $(1,l)$-OT を用いて配付する．最後に注文者は，$k^{B,(1)}_{i,c}$,$k^{B,(2)}_{i,c}$ から最終的な復号鍵 $k^B_{i,c}$ を得る．最初の鍵の受領で正しく振る舞い，もう片方の鍵の受領で注文価格でない鍵を取得しようとしても，本来の復号鍵を得ることはできない．

5 考察

データ交換の正当性: 本プロトコルでの電子データ暗号化・復号用の鍵は M がユニークに作成する．一方復号化用の鍵は注文価格，カウンタに応じた鍵が配付される．鍵の生成，配付が正しく行われていることは，$(1,l)$-OT，VSS，ゼロ知識証明によって検証可能である．

データの秘匿性: データベース内の電子マネーや電子株券はサーバによって暗号化されている．暗号化の鍵は $(1,l)$-OT を使って配付され，サーバは注文者が注文価格と同じ価格の鍵を受け取ったことを検証できる．また，個々の鍵は衝突困難な一方向性関数を使って生成されている．よって，各注文者は受け取った鍵から，別の鍵を知ることは困難であり，マッチした電子マネーや電子株券以外の情報を得ることができない．

希望価格の秘匿性: 注文価格は VSS を用いて複数のサーバに分散されている．また全ての価格についてカウンタも分散されている．よって，サーバはどのカウンタが加算されたかを知ることができない．サーバは鍵の配付に $(1,l)$-OT を使っているために，どの鍵を受け取ったかを知ることができない．そのため，サーバは各注文の注文価格を知ることができない．もちろん，各注文者はブロードキャストされたデータの注文価格を知ることはできない．

匿名性: 注文者が注文を市場に送信するとき，注文者を特定する情報は送信データに含まれない．ブロードキャストされるデータにも注文者を特定する情報が含まれないため，各電子マネーや電子株券を誰と誰が交換したかを知ることができない．

交換データの完全性: 本論文における電子マネーや電子株券は発行者によって電子署名を付与されていて，M がこれらを検証するため，不正な電子マネー，電子株券を用いた注文を検知することができる．また，全ての市場との通信データには注文者の電子署名が付与されるため，システムは不正利用者を特定することができる．

注文者における処理の実用性: 提案プロトコルでは，注文者は売り注文サブプロトコル，買い注文サブプロトコルを完了した後は，ブロードキャストされる情報を受信するだけでよく，相互通信が不要である．

提案プロトコルでは，一般的な関数に対するマルチパーティープロトコルを使っている．これらのプロトコルは一般的に効率的ではない．しかし，提案プロトコルにおけるマルチパーティープロトコルは市場のサーバだけで実行されている．そのため注文者のプロトコルは効率的である．一般的にサーバの処理能力は，クライアントの処理能力よりもはるかに優れていると仮定できるため，提案プロトコルは全体として効率的に実行することが可能である．

参考文献

[1] S. Matsuo and H. Morita, *Secure protocol to construct electronic trading*, IEICE Transactions on Fundamentals of Electronics, Communication and Computer Sciences, VOL.E84-A, No.1, pp.281-288, January 2001.

[2] P. McKenzie and J. Sorensen, *Anonymous Investing*, In Proceedings of Financial Cryptography '99, Lecture Notes in Computer Science, Vol.1648, pp.212-229, Anguilla, BWI, February, 1999.

[3] G. D. Crescenzo, *Privacy for the Stock Market*, In Pre-Proceedings of Financial Cryptography '01, Grand Cayman, BWI, February, 2001.

[4] G. Brassard, C. Crépeau and J.-M. Robert, *All-or-Nothing Disclosure of Secrets*, Advances in Cryptology - Crypto '86, Lecture Notes in Computer Science, Vol.263, pp.234-238, 1987.

[5] M. Naor, B. Pinkas, *Oblivious Transfer and Polynomial Evaluation*, Proc. of 31st ACM Symposium of Theory on Computing, pp.245-254, 1999.

[6] M. Naor and B. Pinkas, *Efficient Oblivious Transfer Protocols*, In proceedings of SODA 2001.

[7] B. Aiello, Y. Ishai and O. Reingold, *Priced Oblivious Transfer; How to sell Digital Goods*, Advances in Cryptology - EUROCRYPT 2001, Lecture Notes in Computer Science, Vol.2045, pp. 119-135, 2001.

[8] A. Shamir, *How to Share a Secret*, Communications of the ACM, Vol.22, No.11, pp.612-613, 1979.

[9] M. Ben-or, S. Goldwasser, and A. Widgerson, *Completeness theorems for non-cryptographic fault-tolerant distributed computation*, STOC '88, pp.1-10, 1988.

[10] O. Goldreich, S. Micali and A. Wigderson, *How to Play Any Mental Game, or a Completeness Theorem for Protocols with Honest Majority*, Proc. of 19th STOC, pp218-229, 1987.

[11] J. Benaloh and J. Leichter, *Generalized Secret Sharing and Monotone Functions*, Advances in Cryptology - Crypto '88, Lecture Notes in Computer Science, Vol. 403, pp.27-35, 1990.

[12] R. Cramer, I. Damgård, and B. Schoenmakers, *Proofs of partial knowledge and simplified design of witness hiding protocols*, Advances in Cryptology - CRYPTO'94, Lecture Notes in Computer Science, Vol.839, pp.174-187, 1995.

[13] M. Harkavy, J. D. Tyger and H. Kikuchi, *Electronic auction with private bids.*, in Third USENIX Workshop on Electronic Commerce Proceedings, pp.61-74, 1998.