社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2006－CSEC－34 (36)
2006／7／21

プライバシを保護した内積比較プロトコルの提案

佐久間 淳† 小林 重信†

† 東京工業大学総合理工学研究科 〒226-8502 神奈川県横浜市緑区長津田町 4259
E-mail: †jun@fe. dis. titech. ac. jp, ††kobayasi@dis. titech. ac. jp

あらまし 本稿ではベクトル x_1, x_2 と y が二つのサイトに分散している場合に，互いに持つデータを開示せずに $x_1 \cdot y$, $x_2 \cdot y$ の大小関係の比較結果のみを計算する，秘匿内積比較プロトコルを提案する．提案プロトコルのセキュリティはシミュレーションパラダイムに基づいて証明される．また提案プロトコルの応用として，秘匿線形識別問題および秘匿ユークリッド距離比較問題への適用例を示す．

キーワード 準同型性暗号，マルチパーティープロトコル，シミュレーションパラダイム，プライバシー，内積比較，データマイニング

Privacy-Preserving Scalar Product Comparison Protocol

Jun SAKUMA† and Shigenobu KOBAYASHI†

† Department of Computational Ingelligence and Systems Science, Nagatsuta-cho, 4259, Midori-ku, Kanagawa, 226-8503, Japan
E-mail: †jun@fe. dis. titech. ac. jp, ††kobayasi@dis. titech. ac. jp

Abstract In this paper, a private scalar product comparison protocol is sudied. When private vectors x_1, x_2 and a private vector y is distributed among two parties, the private scalar product protocl compares the magnitude of $x_1 \cdot y$ and $x_2 \cdot y$ privately without revealing any information regarding privte vectors. The security of proposed protocol is shown following the simulation paradigm. As applications of private scalar comparison, we show the protocl to solve private linear discriminant problem and private Euclid distance comparison problem.

Key words Homomorphic encryption, multi-party protocol, simulation paradigm, privacy, scalar product comparison, data mining

1. はじめに

近年，複数のパーティーに分散されたデータを対象として，それぞれのデータを直接明かさずに，データのプライバシーを保護したまま様々な計算を実行するためのプロトコルが盛んに研究されていりう．特にデータマイニングの分野では，様々なマイニングアルゴリズムをデータを共有せずにプライベートに実行するためのプロトコルが多数提案されている．Pinkas らは分散して蓄積されたデータについて，それらを互いに開示せずに $ID3$ アルゴリズムにより決定木を生成するアルゴリズムを提案した [1]．またプライバシーを保護した Association rule の構築 [2] や，k-mean クラスタリング [3]，ベイジアンネットワークの構造決定 [4] などの例が知られる．

このような上位レベルのアルゴリズムは，基本的な計算を実行する様々な下位レベルのプロトコルをビルディングブロックとして実現されている．たとえば Pinkas らの決定木構築アルゴリズムでは，プライベートな $\log x$, $x \log x$ の計算プロトコルが下位レベルのプロトコルとして用いている．その他の下位レベルのプロトコルの例として，セキュアな和計算，内積計算 [12] [13]，統計計算 [15]，データベーステーブルの join 演算，intersection 演算 [8] などが知られる．

本稿では，様々な用途に利用可能な，新しい下位レベルのプロトコルとして秘匿内積比較プロトコルを提案する．秘匿内積比較とは，ベクトル x_1, x_2 と y が二つのパーティーにに分散しているときに，互いにデータを開示することなく $x_1 \cdot y$, $x_2 \cdot y$ の大小関係を比較する計算である．このプロトコルでは，両者は内積の大小関係のみを共有し，自分が有さないデータについては，比較結果から推測される情報以外何も情報を得ないという意味でセキュアである．

同種のプロトコルとして，ベクトル x と y が二つのパーティーに分散しているときに，内積 $x \cdot y$ をプライベートに計算し，その結果を共有する秘匿内積プロトコルが知られる．秘匿内積プロトコルは内積のプライベートな計算を実現するが，ベクトルの定義域が限定的である場合，プロトコルの実行結果から相手

の保持するプライベートなベクトルの候補が類推される危険性がある．例えば，Alice が x,Bob が y を保持しており，両者が計算結果 $x \cdot y$ を得たときに，ベクターの定義域が $\{0,1\}^d$ など限定されている場合，Alice は x と $x \cdot y$ を用いて，y の候補を多項式時間で列挙することが可能である．

従って上位アルゴリズムの実行に，内積の比較結果のみが必要とされる場合には，内積の計算結果を共有するプロトコルよりも，内積の比較のみを計算するプロトコルのほうが，漏洩する情報量が少ないという点でより安全である．

内積比較のみを利用して構成される上位アルゴリズムの例を以下に紹介する．

秘匿線形識別問題: Alice はデータ x_0 について，$\mathrm{sign}(\beta \cdot x_0)$ によってデータが属するクラスを識別する線形識別器 $f(x) = \beta \cdot x$ を保持している．Bob はクラスが不明なデータ x を保持している．二人の間のプロトコルの結果，Bob はデータ x の識別結果を得るが，それ以外は何も得ない．Alice は何も得ない．

この問題は，例えばサーバがクラスラベル付データセットによって学習した識別器を保持し，クライアントからのリクエストに応じてクライアントが保持するデータの識別結果を返すサービスに応用される．識別器 (この場合 β) がサーバにとって秘密でない場合は β をクライアントに送信することで，識別はクライアントサイドで実行可能である．一方，クライアントが保持するデータが秘密でない場合は，データ x をサーバに送ることで，識別はサーバサイドで実行可能である．しかし，識別器およびデータがそれぞれ秘密である場合には，$\beta \cdot x$ の符号をプライベートに計算するプロトコルが必要となる．

秘匿ユークリッド距離比較問題: Alice は地点 p_0 を保持している．Bob は地点 p_1, p_2 を保持している．二人の間のプロトコルの結果，Bob は地点間のユークリッド距離，$(p_0 - p_1) \cdot (p_0 - p_1)$ および $(p_0 - p_2) \cdot (p_0 - p_2)$ の大小比較の結果を得るが，それ以外は何も得ない．Alice は何も得ない．

この問題は，例えば分散しているモバイルエージェントが，互いの居場所を明かさずに，最適な移動経路や通信経路を決定する際に，利用可能である．

秘匿組み合わせ最適化問題: Alice はコスト関数 $f(x) = \beta \cdot x$ を保持している．Bob は解候補集合 $X = \{x_0, \ldots, x_N\}$ を保持している．二人の間のプロトコルの結果，Bob は $\{x_1, \ldots, x_N\}$ から $\beta \cdot x_i$ を最小にする解 x^* を得るがそれ以外は何も得ない．Alice は何も得ない．

この問題は，内積形式でコスト関数が表現される組み合わせ最適化問題について，サーバがコスト関数を保持し，クライアントからのリクエストに応じて，クライアントが保持する解候補集合から最適なコストを持つ解を探索するサービスに応用される．内積形式でコスト関数が表現される問題の例として，巡回セールスマン問題 (TSP) や配車計画問題 (VRP)，二次割当問題 (QAP) などが知られている．局所探索，タブサーチ，遺伝的アルゴリズムなど，コスト関数に関する知識を利用せずに動作可能なメタヒューリスティックと組み合わせることで，このようなサービスを実現することができる．このような問題の詳細とその解法については [16] を参照されたい．

本稿では，上記のような上位アルゴリズムのビルディングブロックとなる内積比較をプライベートに実行するためのプロトコルの提案およびそのセキュリティに関する証明を行う．以下は論文の構成である．

2 章では提案プロトコルに用いる暗号学的な要素技術と定義を紹介する．また秘匿内積比較問題を定式化し，既存の技術の組み合わせでは，内積比較がプライベートには実行できないことを指摘する．3 章では，秘匿内積比較プロトコルを提案し，その正しさとセキュリティを証明する．またその計算量について議論する．4 章では秘匿内積比較プロトコルの，秘匿線形識別問題および秘匿ユークリッド距離比較問題への応用例を示す．5 章は提案プロトコルをまとめ，今後の展望と課題を示す．

2. 既存研究

本章では提案プロトコルに関連する暗号学的な要素技術について説明する．またこれらの要素技術の単純な組み合わせによって構築される内積比較プロトコルが持つ問題点を指摘する．

2.1 準同型性暗号

公開鍵暗号系は，それぞれ鍵生成，暗号化，復号化のための確率的多項式時間アルゴリズムの組 (Gen, Enc, Dec) からなる．鍵生成アルゴリズムは有効な秘密鍵と公開鍵の組 (s_k, p_k) を生成する．暗号系が加法的準同型性 (additive homomorphic) であるならば，公開鍵と平文 $m_1, m_2 \in Z_m$ について，以下が成立する．

$$Dec_{s_k}(Enc_{p_k}(m_1)) \cdot Enc_{p_k}(m_2)) = m_1 + m_2,$$
$$Dec_{s_k}(Enc_{p_k}(m_1)^{m_2}) = m_1 m_2.$$

公開化鍵暗号系は確率的多項式時間の敵が，彼自身によって選択された二つの平文の暗号文について，どちらの暗号文がどちらの平文に対応するかを見分けることができない場合，強秘匿と呼ばれる．Paillier 暗号系 [9] は準同型性を有し，強秘匿である暗号系の一つである．Paillier 暗号系の詳細については付録を参照されたい．

2.2 2-パーティープロトコルのプライバシ

本稿では各パーティーは *semi-honest* に振舞うことを前提とする．semi-honest とは，各パーティーは，プロトコル実行中に得る情報を全て記録保持することを除き，プロトコルの全てのステップを正しく実行する振る舞いのことである．また semi-honest パーティーは記録された情報を用いてプロトコルの出力以外の情報を得ようとする．semi-honest パーティー間のプロトコルのセキュリティは [6] において，以下の様に定義されている．

$f = (f_1, f_2)$ を確率的多項式時間で動作する汎関数とする．パーティー 1 の入力を x，パーティー 2 の入力を y とする．また Π を f を計算する 2-パーティープロトコルとする．プロトコル Π 実行中のパーティー 1 の view は，$view_1^{\Pi}(x,y) = (x, r^1, m_1^1, \ldots, m_t^1)$，パーティー 2 の view は $view_2^{\Pi}(x,y) = (y, r^2, m_2^1, \ldots$

$, m_i^2$) と記述される．ここで，r^1, r^2 は各パーティ内部で発生させた乱数であり，m_i は受信した i 番目のメッセージをあらわす．このとき 2-パーティプロトコルのプライバシーは以下の様に定義される．

Definition 1. (2-パーティプロトコルのプライバシ) 決定的汎関数 f において，以下の式を満たす多項式時間アルゴリズム S_1 および S_2 が存在するならば，Π は f をプライベートに計算する．

$$\{S_1(x, f_1(x,y))\}_{x,y\in\{0,1\}^*} \equiv^c \{view_1^{\Pi}(x,y)\}_{x,y\in\{0,1\}^*}, \quad (1)$$

$$\{S_2(y, f_2(x,y))\}_{x,y\in\{0,1\}^*} \equiv^c \{view_2^{\Pi}(x,y)\}_{x,y\in\{0,1\}^*}. \quad (2)$$

ここで，$\equiv^c$ は，計算量的識別不可能 (computationally indistinguishable) であることを示す．式 1 と 式 2 は，各パーティーの view が，そのパーティーの入力・出力のみにアクセス可能な確率的多項式時間アルゴリズム S_1, S_2 によってシミュレートされるならば，各パーティーはプロトコルの実行によって出力以外の情報を得ないことを意味している．詳細については [6] を参照されたい．

2.3 秘匿内積プロトコル

秘匿内積プロトコルの問題定義を以下に示す．

Problem Statement 1. (秘匿内積計算問題) *Alice* がベクター $x_1, x_2 \in Z_\mu^d$，*Bob* がベクター $y \in Z_\mu^d$ を保持している．二人の間のプロトコルの実行の結果，二人は内積の計算結果 $x \cdot y$ を共有するが，それ以外は何も得ない．

秘匿内積計算のためのプロトコルは複数提案されている．Vaidiya らの方法では，複数パーティーで正則なランダム行列を共有し，秘密のベクターをランダム行列によってマスクすることによってプライベートなベクターを保護するとともに，それらの線形代数的演算によって内積計算が実行される [3]．Atallah らは 1-out-of-N oblivious transfer に基づく秘匿内積プロトコルを提案した [12]．Goethals らは，これらのプロトコルはある条件下においてはベクターのある要素が高い確率で漏洩することを示し，より安全性の高い準同型性暗号に基づく秘匿内積プロトコルを提案した．以下に Goethals らによる秘匿内積プロトコルを示す．

Z_m はある大きな m における平文空間とする．また $\mu = \lfloor\sqrt{m/d}\rfloor$ とする．また全ての計算はある m について Z_m 上で行われ，各パーティーは semi-honest に振舞うものとする．このとき，プロトコルは以下の様に記述される．

[Private scalar product protocol]

- **Private Input of Alice :** $x \in Z_\mu^d$
- **Private Input of Bob :** $y \in Z_\mu^d$
- **Private Output of Alice :** $x \cdot y - s_A \mod m$

（1） Alice: Generate a private and public key pair(p_k, s_k)

（2） Alice → Bob: Send p_k to Bob

（3） Alice → Bob: Send $c_i = \mathrm{Enc}_{p_k}(x_i)$ $(i = 1, \ldots, d)$

（4） Bob: Compute $w \leftarrow \prod_{i=1}^d c_i^{y_i}$

（5） Bob → Alice: Send $w' = w \cdot \mathrm{Enc}_{p_k}(-s_A)$, where $s_A \in_r Z_m$

（6） Alice: Compute $Dec(w') = x \cdot y - s_A$

ただし $\in_r$ は集合の中からランダムに一つ要素を選択する操作を表す．また y_i, x_i は y, x の i 番目の要素を表す．このプロトコルにおいて，Alice のプライバシーは,Bob の計算能力が確率的多項式時間ならば安全であり，また Bob のプライバシーは情報理論的に安全であることが示されている．

2.4 内積プロトコルを用いた内積比較の問題点

本節では，内積プロトコルの単純な組み合わせによって実現される内積比較プロトコルは，ある状況下においてプライバシーが保障されないことを示す．ベクター x_1, x_2, y について，不等式 I_- を $x_2 \cdot y - x_1 \cdot y \leqq 0$，$I_+$ を $x_2 \cdot y - x_1 \cdot y > 0$ と定義すると，内積比較問題は以下の様に記述される．

Problem Statement 2. (秘匿内積比較問題) *Alice* がベクター $x_1, x_2 \in \{1, \ldots, K\}^d$，*Bob* がベクター $y \in \{1, \ldots, K\}^d$ を保持している．二人の間のプロトコルの実行の結果，二人は内積の大小比較の結果を表す不等式 $I \in \{I_+, I_-\}$ を共有するが，それ以外は何も得ない．

2.3 に示した秘匿内積プロトコルを利用することによって，内積比較は即座に実行可能である．秘匿内積プロトコルに基づく秘匿内積比較プロトコルを以下に示す．

[Protocol-1]

- **Private Input of Alice :** $x_1, x_2 \in Z_\mu^d$
- **Private Input of Bob :** $y \in Z_\mu^d$
- **Output of Alice and Bob:** $I \in \{I_+, I_-\}$

（1） Bob : Send $c_i = \mathrm{Enc}_{p_k}(y_i)$ to Alice $(i = 1, \ldots, d)$

（2） Alice : Compute $w_1 \leftarrow \prod_{i=1}^d c_i^{x_{1,i}} \mathrm{Enc}_{p_k}(-s_A)$ where $s_A \in_r Z_m$ and send w to Bob

（3） Alice : Compute $w_2 \leftarrow \prod_{i=1}^d c_i^{x_{2,i}} \mathrm{Enc}_{p_k}(-s_A)$ and send w_2 to Bob

（4） Bob : Compute $Dec(w_1) = x_1 \cdot y - s_A$ and $Dec(w_2) = x_2 \cdot y - s_A$. If $Dec(w_2) \leqq Dec(w_1)$, return I_- to Alice. Else, return I_+ to Alice.

（5） Alice: Receive an inequality I and output I.

ただし $x_{1,i}, x_{2,i}$ はそれぞれ x_1, x_2 の i 番目の要素を表す．Protocol-1 は，正しい比較結果を与えるが，Alice のベクターに関する情報が Bob に漏洩する可能性がある．step 2 および 3 について，Bob は $Dec(w_1) = x_1 \cdot y - s_A$ と $Dec(w_2) = x_2 \cdot y - s_A$ を得る．後者から前者を引くことで，Bob は

$$Dec(w_2) - Dec(w_1) \quad = \quad (x_2 - x_1) \cdot y. \qquad (3)$$

を得る．つまり Bob は内積の比較結果だけでなく，内積の差分値を知ることができる．

$x_1, x_2 \in \{0,1\}^d$ のように定義域が狭く限定されている場合，$(x_1 - x_2) \cdot y$ から x_1, x_2 の候補を列挙することは多項式時間で可能である．よって Protocol-1 は秘匿内積比較の問題定義によ

ればセキュアではない.

このプロトコルは, $x_1 \cdot y$ と $x_2 \cdot y$ の比較を Bob の代わりに Alice が行うように修正することができる. 同じ入力, 出力において, Protocol-2 は以下の様に記述される.

[Protocol-2]

(1) Bob : Send $c_i = \mathrm{Enc}_{p_k}(y_i)$ to Alice

(2) Alice : Compute $w_1 \leftarrow \prod_{i=1}^{d} c_i^{x_{1,i}} \mathrm{Enc}_{p_k}(-s_{A1})$ where $s_{A1} \in_r Z_m$ and send w_1 to Bob

(3) Alice : Compute $w_2 \leftarrow \prod_{i=1}^{d} c_i^{x_{2,i}} \mathrm{Enc}_{p_k}(-s_{A2})$ where $s_{A2} \in_r Z_m$ and send w_2 to Bob

(4) Bob : Compute $Dec(w_1) = x_1 \cdot y - s_{A1}$ and $Dec(w_2) = x_2 \cdot y - s_{A2}$. Send $Dec(w_1)$ and $Dec(w_2)$ to Alice

(5) Alice : Compare $Dec(w_1) + s_{A1} = x_1 \cdot y$ and $Dec(w_2) + s_{A2} = x_2 \cdot y$. If $x_2 \cdot y - x_1 \cdot y \leqq 0$ output I_-. Else output I_+

Protocol-2 では, Alice の秘密のベクター x_1, x_2 は保護されるが, Alice は $x_1 \cdot y$ および $x_2 \cdot y$ を得るため, Protocl-2 も問題定義においてセキュアではない.

3. 秘匿内積比較プロトコルの提案

3.1 秘匿内積比較プロトコル

前章までに示したように, 秘匿内積比較は秘匿内積プロトコルの組み合わせではセキュアに実行することができない. 本章では秘匿内積比較のための新しいプロトコルを提案する. ベクターの次元数を $d \geqq 1$ とする. 簡単のためにここではベクターの定義域を $D = \{1, \ldots, K\}^d$, $K \geqq 2$ とする. ただし後に, 0 や負数を含むベクターの内積比較への拡張を示す. 秘匿内積比較問題を解くためのプロトコルは以下のように記述される.

[Private scalar product comparison]

- **Input of Alice:** Private vectors $x_1, x_2 \in D$
- **Input of Bob:** Private vector $y \in D$
- **Output of Alice and Bob:** inequality $I \in \{I_+, I_-\}$

(1) Bob: Generate a private and public key pair (s_k, p_k) for homomorphic encryption and send p_k to Alice

(2) Bob: Encrypt Bob's vector $c_i = Enc_{p_k}(y_i)$ and send it to Alice$(i = 1, \ldots, d)$

(3) Alice: Generate numbers $r, r', r'' \in Z_m$ randomly, such that $d^8 K^{16} < r$, $r < r' < (1 + \frac{1}{dK^2})r$, $0 < r'' < dK^2$

(4) Alice: $x_m \leftarrow rx_2 - r'x_1$

(5) Alice: Compute $w_m = \left(\prod_{i=1}^{d} c_i^{x_{m,i}}\right) \cdot Enc_{p_k}(r'')$ and send w_m to Bob

(6) Bob: Compute $S = Dec(w_m)$

(7) Bob: If $S < dK^2$, send I_- to Alice. Else, send I_+ to Alice.

(8) Alice: Receive an inequality I and output I

Alice は自由に x_1 と x_2 を交換できることに注意されたい. つまり, 比較結果は両者が共有するが, 比較するベクターの順序は Alice が自由に決定できるため, 結果として比較結果は Alice にしか知られない.

3.2 秘匿内積比較プロトコルのセキュリティ

本節では提案した秘匿内積比較プロトコルの正しさとセキュリティを証明する. まず, プロトコルの正しさを証明するための補助定理を示す.

Lemma 1. $L > dK^2$, $LdK^2 < r$, $r < r' < (1 + \frac{1}{dK^2})r$, $0 \leqq r'' < dK^2$ とする. また

$$S = (x_2 \cdot y)r - (x_1 \cdot y)r' + r'' \tag{4}$$

とする. このとき, 全ての $x_1, x_2, y \in D$ について,

$$x_2 \cdot y - x_1 \cdot y > 0 \iff S > L \tag{5}$$

$$x_2 \cdot y - x_1 \cdot y = 0 \iff -LdK^2 \leqq S < dK^2 \tag{6}$$

$$x_2 \cdot y - x_1 \cdot y < 0 \iff S < -LdK^2 \tag{7}$$

である.

Proof: (5) の十分条件をまず示す.

$$\begin{aligned} S - r'' &= (x_2 \cdot y)r - (x_1 \cdot y)r' \\ &> (x_2 \cdot y)r - (x_1 \cdot y)(1 + \frac{1}{dK^2})r \\ &= (x_2 \cdot y - x_1 \cdot y)r - \frac{r}{dK^2}(x_1 \cdot y). \end{aligned}$$

$x_2 \cdot y > x_1 \cdot y$ より, r の値にかかわらず $x_2 \cdot y = dK^2$, $x_1 \cdot y = dK^2 - 1$ のとき $S - r''$ は最小ゆえ, $S - r'' > \frac{r}{dK^2} > L$. よって, $x_2 \cdot y - x_1 \cdot y > 0 \Longrightarrow S > L$ である. 必要条件は $L > dK^2$ より自明である. よって (5) が示された.

続いて (6) を示す. $\frac{r' - r}{r} < \frac{1}{dK^2}$ ゆえ, $0 < r' - r < \frac{r}{dK^2} < L$ である. よって $x_1 \cdot y = x_2 \cdot y$, $x_1 \cdot y \neq 0$ より,

$$\begin{aligned} & S - r'' = x_1 \cdot y(r - r') \\ \iff & x_1 \cdot y(r - r') \leqq S < x_1 \cdot y(r - r') + dK^2 \\ \iff & -LdK^2 \leqq S < dK^2 \end{aligned}$$

よって (6) が示された.

最後に (7) を示す. まず十分条件を示す. S は $x_1 \cdot y$, $x_2 \cdot y$ の値にかかわらず $r' = r + 1$ の時に最大である. よって $x_2 \cdot y - x_1 \cdot y < 0$ のとき,

$$\begin{aligned} S - r'' &= (x_2 \cdot y)r - (x_1 \cdot y)r' \\ &< (x_2 \cdot y)r - (x_1 \cdot y)(r + 1) \\ &= -(x_1 \cdot y - x_2 \cdot y)r - x_1 \cdot y \\ &< -r - 1 < -LdK^2 \end{aligned} \tag{8}$$

続いて必要条件を示す.

$$S - r'' < (x_2 \cdot y - x_1 \cdot y)r - x_1 \cdot y < -LdK^2$$

において, $x_1 \cdot y < LdK^2$ より, $S < -LdK^2 \Longrightarrow x_2 \cdot y - x_1 \cdot y < 0$ である. よって (7) が示された. □

Lemma 1 を用いて，プロトコルの正しさを証明する．

Theorem 1. *Alice* と *Bob* は *semi-honest* に振舞うとする．このとき，*Alice* は秘匿内積比較プロトコルの実行後，正しい不等式 I^* を得る．

Proof: S が式 (4) で計算されたとき，step 5 において Alice に計算される w_m は

$$\begin{aligned} w_m &= \Big(\prod_{i=1}^{d} c_i^{x_{m,i}}\Big)\cdot Enc_{p_k}(r'') \\ &= \Big(\prod_{i=1}^{d} Enc_{p_k}\big(y_i x_{2,i} r - y_i x_{1,i} r'\big)\Big)\cdot Enc_{p_k}(r'') \\ &= Enc_{p_k}\Big(\sum_{i=1}^{d}\big(y_i x_{2,i} r - y_i x_{1,i} r'\big)\Big)\cdot Enc_{p_k}(r'') \\ &= Enc_{p_k}\big(r(y\cdot x_2) - r'(y\cdot x_1) + r''\big). \end{aligned} \tag{9}$$

である．ゆえに，Bob は

$$Dec(w_m) = r(x_2\cdot y) - r(x_1\cdot y) + r''$$

を step 6 て得る．Lemma 1 より，$S < dK^2$ ならば $x_2\cdot y - x_1\cdot y \leqq 0$，そうでなければ $x_2\cdot y - x_1\cdot y > 0$ が成立するため，Alice は正しい不等式を得る． □

続いて，scalar product comparison protocol のセキュリティを証明するために三つの補助定理を示す．

Lemma 2. $S > L$ とする．$L > d^4K^8$ のとき，$z_2 > z_1$ なる任意の $z_1, z_2 \in D$ について，$S = z_2 r - z_1 r' + r''$ を満たす (r, r', r'') が，$LdK^2 < r < r'$, $\frac{r'-r}{r} < \frac{1}{dK^2}$, $0 \geqq r'' < dK^2$ において少なくとも一組存在する．

Proof: $S > L$ のとき，Lemma 1 より，$z_2 > z_1$ である．z_1, z_2 が与えられたとき，$r, r' r''$ についての不定方程式

$$S = z_2 r - z_1 r' + r'' \tag{10}$$

は，$S - r''$ が $gcd(z_2, z_1)$ で割り切れるならば，解が存在する．$0 < z_1 < z_2 \leqq dK^2$ ゆえ，$0 \leqq r'' < dK^2$ の範囲で適切に $r'' = \bar{r}''$ とすることで $S - \bar{r}'' = \beta S'$ と書ける．また $z_2 = \beta X_2$, $z_1 = \beta X_1$ と書けるため，式 10 は $r'' = \bar{r}''$ において，

$$S' = X_2 r - X_1 r' \tag{11}$$

と等価である．ここで，$1 \leqq X_1 < X_2 < dK^2$, $S' > L/dK^2$ である．

不定方程式 $1 = X_2 r - X_1 r'$ の解の一つを $r = r_0, r' = r_0'$ とすると，式 11 の一般解は

$$\begin{cases} r = S' r_0 + X_1 t & (t = 0, \pm 1, \pm 2 \ldots) \\ r' = S' r_0' + X_2 t \end{cases}$$

であり $\frac{r'-r}{r}$ は t の関数として，

$$f(t) = \frac{r'-r}{r} = \frac{S'(r_0'-r_0) + (X_2 - X_1)t}{S' r_0 + X_1 t} \tag{12}$$

$$f'(t) = \frac{df(t)}{dt} = \frac{S'\{(X_2-X_1)r_0 - (r_0'-r_0)X_1\}}{(S' r_0 + X_1 t)^2} \tag{13}$$

と書ける．また $t_0 = \frac{-(X_2-X_1)}{S'(r_0'-r_0)}$ について $f(t_0) = 0$ である．このとき，$\frac{r'-r}{r} < \frac{1}{dK^2}$ を満たす整数 t が存在するための条件を考える．

分数関数の性質より，$(X_2-X_1)r_0 - (r_0'-r_0)X_1 > 0$ および $(X_2-X_1)r_0 - (r_0'-r_0)X_1 < 0$ の二つの場合が考えられる．

初めに，$(X_2-X_1)r_0 - (r_0'-r_0)X_1 > 0$ の場合を考える．この場合 $t = t_0$ 付近で $f(t)$ は上に凸の単調増加関数である．よって，$f'(t_0) < \frac{1}{dK^2}$ ならば，$[t_0, t_0+1)$ の範囲で $f(t) < \frac{1}{dK^2}$ を満足する整数 t が少なくとも一つ存在する．$t_0 = \frac{-(X_2-X_1)}{S'(r_0'-r_0)}$ を式 (13) に代入し，整理すると，

$$\begin{aligned} f'(t_0) &= \frac{(X_2-X_1)^2}{S'\{(X_2-X_1)r_0 - (r_0'-r_0)X_1\}} \\ &< \frac{d^2K^4}{L/dK^2} = \frac{d^3K^6}{L} \end{aligned}$$

を得る．よって，$L > d^4K^8$ ならば $\frac{r'-r}{r} < \frac{1}{dK^2}$ なる整数 t が存在することが示された．

次に，$(X_2-X_1)r_0 - (r_0'-r_0)X_1 < 0$ の場合を考える．このとき，$t = t_0$ 付近で $f(t)$ は上に凸の単調減少関数である．よって，$f'(t_0) > -\frac{1}{dK^2}$ ならば，$(t_0-1, t_0]$ の範囲で $f(t) < -\frac{1}{dK^2}$ を満足する整数 t が少なくとも一つ存在する．

上記と同様に，$t_0 = \frac{-(X_2-X_1)}{S'(r_0'-r_0)}$ を式 (13) に代入し，整理すると，

$$\begin{aligned} f'(t_0) &= \frac{(X_2-X_1)^2}{S'\{(X_2-X_1)r_0 - (r_0'-r_0)X_1\}} \\ &> -\frac{d^2K^4}{L/dK^2} = -\frac{d^3K^6}{L} \end{aligned}$$

を得る．よって，この場合でも $L > d^4K^8$ ならば $\frac{r'-r}{r} < \frac{1}{dK^2}$ なる整数 t が少なくとも一つ存在することが示された．

以上より，$L > d^4K^8$ のとき，$z_2 > z_1$ なる任意の $z_1, z_2 \in D$ について，$S = z_2 r - z_1 r' + r''$ を満たす (r, r', r'') が，$LdK^2 < r < r'$, $\frac{r'-r}{r} < \frac{1}{dK^2}$, $0 \leqq r'' < dK^2$ において少なくとも一組存在することが示された． □

Lemma 3. $S < -LdK^2$ とする．$L > d^7K^{14}$ のとき，$z_2 < z_1$ なる任意の $z_1, z_2 \in D$ について，$S = z_2 r - z_1 r' + r''$ を満たす (r, r', r'') が，$LdK^2 < r < r'$, $\frac{r'-r}{r} < \frac{1}{dK^2}$, $0 \leqq r'' < dK^2$ において少なくとも一組存在する．

Proof: Lemma 2 と同様に，r, r' における一般解に関して $f(t) = \frac{r'-r}{r}$ は式 12 で，$f'(t)$ は式 13 であらわされる．このとき，$f(t) < \frac{1}{dK^2}$ を満たす整数 t が存在する条件を考える．

分数関数の性質より，$S'(X_2-X_1)r_0 - S'(r_0'-r_0)X_1 > 0$ および $S'(X_2-X_1)r_0 - S'(r_0'-r_0)X_1 < 0$ の二つの場合が考えられる．

初めに，$S'(X_2-X_1)r_0 - S'(r_0'-r_0)X_1 > 0$ の場合を考える．$f(t)$ は $t_0 = \frac{1/dK^2 - S'(r_0'-r_0)}{X_1-X_1}$ において，$f(t_0) = \frac{1}{dK^2}$ であ

る．$S'<0$であることに注意すると，$t=t_0$付近で$f(t)$は下に凸の単調減少関数である．よって，$f'(t_0)>-\frac{1}{dK^2}$ならば，$(t_0-1,t_0]$の範囲で$f(t)<\frac{1}{dK^2}$を満足する整数tが存在する．t_0を式(13)に代入し，整理すると，

$$f'(t_0)=\frac{(X_2-X_1)^2\{(X_2-X_1)r_0-(r_0'-r_0)X_1\}^2}{S'\{\frac{X_1}{dK^2S'}+r_0(X_2-X_1)+X_1(r_0'-r_0)\}}>\frac{d^2K^4\cdot d^4K^8}{-L}.$$

を得る．よって，$L>d^7K^{14}$のとき，$f'(t_0)>-\frac{1}{dK^2}$であり，このとき$\frac{r'-r}{r}<\frac{1}{dK^2}$なる整数$t$が少なくとも一つ存在することが示された．

続いて，$S'(X_2-X_1)r_0-S'(r_0'-r_0)X_1<0$の場合を考える．$f(t)$は$t_0=\frac{1/dK^2-S'(r_0'-r_0)}{X_1-X_1}$において，$f(t_0)=\frac{1}{dK^2}$を取り，$t=t_0$付近で$f(t)$は下に凸の単調増加関数である．よって，$f'(t_0)<\frac{1}{dK^2}$ならば，$(t_0-1,t_0]$の範囲で$f(t)<\frac{1}{dK^2}$を満足する整数$t$が存在する．$t_0$を式(13)に代入し，整理すると，

$$f'(t_0)<\frac{d^2K^4\cdot d^4K^8}{L}.$$

を得る．よって，同様に$L>d^7K^{14}$のとき，$f'(t_0)<\frac{1}{dK^2}$であり，このとき$\frac{r'-r}{r}<\frac{1}{dK^2}$なる整数$t$が存在することが示された．

以上より，$L>d^7K^{14}$のとき，$z_2<z_1$なる任意の$z_1,z_2\in D$について，$S=z_2r-z_1r'+r''$を満たす(r,r',r'')が，$LdK^2<r<r',\frac{r'-r}{r}<\frac{1}{dK^2},0\leq r''<dK^2$において少なくとも一組存在することが示された．□

Lemma 4. $z_2=z_1$なる任意の$z_1\in D$について，$S=z_2r-z_1r'+r''$を満たす(r,r',r'')は，Sの値にかかわらず$r<r',\frac{r'-r}{r}<\frac{1}{dK^2},0\leq r''<dK^2$において少なくとも一組存在する．

$z_1=z_2$ゆえ，$S-r''=z_1(r-r')$なるr,r',r''について考える．$0<z_1\leq dK^2$ゆえ，$S-r''=\beta z_1$なるr''は$0\leq r''<dK^2$に少なくとも一つ存在する．このr''について，$\beta=r-r'$と書けるが，$LdK^2<r<r',\frac{r'-r}{r}<\frac{1}{dK^2},0\leq r''<dK^2$において，$\beta=r-r'$を満足する$r,r'$は無数に存在する．□

これらのLemmaを用いて，プロトコルのセキュリティを示す．2-パーティープロトコルのプライバシの定義に基づけば，パーティーのreal viewと，入力および出力のみから生成されたsimulation viewがcomputationally indistinguishableであるとき，そのパーティーはプロトコルの実行自体からは何も情報を得ないことが示される．

Theorem 2. *Alice* と *Bob* は *semi-honest* に振舞うならば，*scalar product comparison protocol* はセキュアであり，プロトコルの実行後，*Alice* と *Bob* は正しい不等式以外の情報を得ない．

Proof: Aliceのプロトコル実行における real view$\mathcal{D}^A$とsimulation view$\mathcal{D}^A_{sim}$は以下のように記述される．

$$\mathcal{D}^A\equiv\left\{x_1,x_2,c_1,\ldots,c_d\right\}_{x_1,x_2,y\in\{1,\ldots,K\}^d},$$
$$\mathcal{D}^A_{sim}\equiv\left\{x_1,x_2,\tilde{c}_1,\ldots,\tilde{c}_d\right\}_{x_1,x_2,y\in\{1,\ldots,K\}^d}.$$

またsimulation viewをAliceの入力x_1,x_2と出力Iに基づいて以下のように生成することにしよう．

（1） 公開鍵$\tilde{p}_k$をランダムに生成

（2） $\tilde{c}_i=Enc_{\tilde{p}_k}(\tilde{y}_i)$を計算．ここで$y_i\in_r Z_K$とする

このとき，暗号系は強秘匿性を持つため，$\mathcal{D}^A$と$\mathcal{D}^A_{sim}$はたとえyが与えられてもcomputationally indistinguishableである．

続いてBobのviewに移る．Bobのreal view　$\mathcal{D}^B$とsimulation view$\mathcal{D}^B_{sim}$は以下のように記述される．

$$\mathcal{D}^B\equiv\left\{y,w_m,S\right\}_{x_1,x_2,y\in\{1,\ldots,K\}^d}$$
$$\mathcal{D}^B_{sim}\equiv\left\{y,\tilde{w}_m,\tilde{S}\right\}_{x_1,x_2,y\in\{1,\ldots,K\}^d}.$$

Bobのsimulation viewをBobの入力yと出力Iのみを用いて以下の様に生成することにしよう．

（1） もし$I=I_-$ならば，$\tilde{x}_1$と$\tilde{x}_2$を，$\tilde{x}_2\cdot y-\tilde{x}_1\cdot y\leqq 0$を満たすように，ランダムに生成する．そうでなければ，$\tilde{x}_1$と$\tilde{x}_2$を，$\tilde{x}_2\cdot y-\tilde{x}_1\cdot y>0$を満たすように，ランダムに生成する．

（2） $\tilde{r},\tilde{r}',\tilde{r}''$を$d^8K^{16}<\tilde{r},\tilde{r}<\tilde{r}'<(1+\frac{1}{dK^2})\tilde{r},0\leq\tilde{r}''<dK^2$を満たすようにランダムに生成する．

（3） $\tilde{S}=(\tilde{x}_2\cdot y)\tilde{r}-(\tilde{x}_1\cdot y)\tilde{r}+\tilde{r}''$を計算する

（4） 公開鍵$\tilde{p}_k$をランダムに生成する

（5） $\tilde{w}_m=Enc_{\tilde{p}_k}(\tilde{S})$を計算する

このsumulation viewについてcomputational indistinguishabilityを示す．まずはじめに，$\{y,S\}$と$\{y,\tilde{S}\}$のindistinguishablilityを示す．distinguisherは

$$\tilde{S}=(x_2\cdot y)\tilde{r}-(x_1\cdot y)\tilde{r}++\tilde{r}''\qquad(14)$$

を満たす(r,r',r'')が存在するかどうかを真のx_1およびx_2よりチェックすることができる．もしそのような(r,r',r'')がが存在しなければdigtinguisherはSと$\tilde{S}$を識別できることになる．しかしながら，lemma 3,4および5は$L>d^7K^{14}$，$LdK^2<\tilde{r},\tilde{r}<\tilde{r}'<(1+\frac{1}{dK^2})\tilde{r},0\leq\tilde{r}''<dK^2$ならば，任意の$x_1,x_2$について式14を満足する$(r,r',r'')$が少なくとも一組存在することを保証している．ゆえに，distinguisherはこの方法では$\{y,S\}$と$\{y,\tilde{S}\}$を見分けることができない．計算論的には$\{y,S\}$と$\{y,\tilde{S}\}$は乱数r,r',r''の一様性のために indistinguishable である..

また，$\{w_m,S\}$，$\{\tilde{w}_m,\tilde{S}\}$は暗号系が強秘匿性ゆえcomputationally indistinguishableである．$\{y,w_m\}$，$\{y,\tilde{w}_m\}$もまた同様である．yとS，$\tilde{S}$は独立ゆえ，これらの結合分布である$\mathcal{D}^B$ and $\mathcal{D}^B_{sim}$はcomputationally indistinguishableである．

2-party computationのプライバシーの定義により，theoremが証明された．□

以上，Theorem 1および2より，秘匿内積比較プロトコルの正しさとセキュリティが示された．

3.3 秘匿内積比較の一般化

これまでに示した定理は，内積値が $(0, dK^2]$ に収まることを前提としているため，ベクターの定義域を $D = \{1, \cdots, K\}^d$, $K \geq 2$ としていた．本節ではこれを負数や 0 を含むベクトルに一般化する．

ベクターに 0 や負数が含まれる場合は，その下限値 $l(\leq 0)$ をあらかじめ見積もり，$x' = (x, 1)$, $y' = (y, -l+1)$ のように変換する．このとき $x' \cdot y' = x \cdot y - l + 1 > 0$ より，任意のベクターの内積の下限値を 0 より大きくすることができ，内積比較プロトコルを利用することができる．

下限値 l は必ずしも厳密に求める必要はなく，内積値が常に負にならいような大きな値を設定すれば十分である．

3.4 秘匿内積比較プロトコルの計算量

本節では秘匿内積プロトコルにおける計算量を議論する．

プロトコルにおいて最も時間計算量の大きいステップは Bob の step 2 における y の要素の暗号化と，step 5 における x_m の各要素についての累乗計算であり，それぞれ次元数 d に対して $O(d)$ である．ただし Bob の計算はプロトコル開始前に offline であらかじめ実行しておくことが可能である．

また最も通信計算量の大きいステップはステップ (2) における c_i の Bob から Alice への送信であり，同様に $O(d)$ である．

ただし，秘匿内積比較を複数回行い，かつ Bob のベクトルが不変で,Alice のベクトルのみが毎回変更される場合は，二回目以降は step(3) から開始することができるため，秘匿内積比較一回あたりの計算量は，通信計算量に $O(1)$ 抑えることができる．

後に示す秘匿線形識別問題や秘匿組み合わせ最適化問題など，複数回の秘匿内積プロトコルを適用する問題は，Bob 側のベクターが不変であることを前提としてよいケースが多く，このような場合には比較的小さい通信計算量でプロトコルを実行することができる．

また，複数回の秘匿内積プロトコルの適用において，Alice のベクターが逐次的に変化し，その変化量が小さい場合，step 5 の累乗計算は差分のみを計算することによって時間計算量は変更された要素数に比例した時間に抑えることができる．

[16] における秘匿組み合わせ最適化問題では，この性質を利用して，時間計算量，通信計算量ともに，比較一回あたり $O(1)$ に抑えている．

4. 秘匿内積比較プロトコルの応用

本章では秘匿内積比較プロトコルをビルディングブロックとして構築可能な問題への適用例を示す．

4.1 秘匿線形識別器

線形識別器とは統計的学習においてもっとも基本的な学習器として知られている．以下に問題定義を示す．

Problem Statement 3. *(秘匿線形識別器によるクラス判定問題) Alice* がベクター $x \in \{1, \ldots, K\}^d$, *Bob* が線形識別器 $y = \beta \cdot x, \beta \in \{1, \ldots, K\}^d$ を保持している．二人の間のプロトコルの実行の結果，*Alice* はベクター識別結果 $\{true, false\}$ を得るが，それ以外は何も得ない．*Bob* は何も得ない．

Bob が持つ識別器 $f(x) = \beta \cdot x$ はその出力の符号が識別結果に対応している．Alice は二つのベクター $(x + \eta, \eta)$ を用意し，Bob が保持する β に対して秘匿内積プロトコルを実行するとしよう．ただし η は Alice が定める任意のベクターである．このとき，両者の間のプロトコルの結果，$\beta \cdot (x + \eta), \beta \cdot \eta$ の比較結果を与える．これは $\beta \cdot x$, 0 の比較結果に等しいため，Alice は秘匿内積比較プロトコルによって x に関する識別結果をプライベートに得ることが可能である．

線形識別器は非常に単純な識別器であるが，カーネル法との組み合わせによって構築されるサポートベクターマシーンは非常に高い性能を示すことがしられ，これらとの組み合わせでは高性能かつセキュアな識別器が構成可能である．

4.2 ユークリッド距離の大小判定問題

ユークリッド距離の大小判定の問題定義を以下に示す．

Problem Statement 4. (秘匿距離比較問題) *Alice* がベクター $p_1, p_2 \in \{1, \ldots, K\}^d$, *Bob* がベクター $p_0 \in \{1, \ldots, K\}^d$ を保持している．二人の間のプロトコルの実行の結果，*Alice* はベクター間のユークリッド距離 $(p_0 - p_1) \cdot (p_0 - p_1)$, $(p_0 - p_2) \cdot (p_0 - p_2)$ の大小比較の結果を表す不等式 $I \in \{I_+, I_-\}$ を得るが，それ以外は何も得ない．*Bob* は何も得ない．

この問題において，

$$x_1 = p_1 + p_2$$
$$x_2 = -2p_0$$
$$y = p_1 - p_2$$

とすると，Alice が持つ 2 地点と Bob が持つ 1 地点の間のユークリッド距離の差は，

$$\begin{aligned} & (p_0 - p_1) \cdot (p_0 - p_1) - (p_0 - p_2) \cdot (p_0 - p_2) \\ = & (p_1 - p_2) \cdot (p_1 + p_2) + (p_2 - p_1) \cdot (2p_0) \\ = & y \cdot x_1 - y \cdot x_2 \end{aligned}$$

と表現され，内積比較プロトコルが適用可能である．この場合 Bob が x_2 を，Alice が y, x_1 を保持しているが，以下の様にプロトコルを変更することで正しい比較結果を得ることができる．

（1） Bob: $c_i = Enc(x_{2,i})$ とし，Alice に送信

（2） Alice: $w_m = \prod c_i^{r y_i} Enc(-r'(x_1 \cdot y) + r'')$ を計算し，Bob に送信

（3） Bob $Dec(w_m) = r x_2 \cdot y - r' x_1 \cdot y + r''$ を計算し，その符号を Alice に送信

この方法によれば，任意の 2 点間の距離の大小をプライベートに比較することが可能である．任意の二点間の距離の大小関係のみを利用して実行されるアルゴリズムは k-mean 法などのクラスタリングアルゴリズムをはじめとして，機械学習の分野では多く存在しており，秘匿内積プロトコルはこのようなアルゴリズムへの応用が可能である．

また位置情報を通信可能なカーナビゲーションシステムやモ

バイル機器において，位置を明かさずに経路探索を行うアルゴリズムなどへの応用も考えられる．

5. 終わりに

本稿では，複数のサイトに分散したベクターの内積の大小関係を比較する秘匿内積問題を定義し，それを解く新しいプロトコルを提案した．秘匿内積比較プロトコルは，従来の秘匿内積プロトコルに比べ共有される情報が少ないため，必ずしも内積の計算結果を必要としない問題に用いた場合，より高いレベルのセキュリティを保障することが可能である．

また秘匿内積比較を利用する問題として，秘匿線形識別問題および秘匿ユークリッド距離比較問題への適用例を示した．具体的な応用例としては，車両間通信を利用した走行経路計画があげられる．これらのシステムは車両の位置情報や走行履歴を外部に送信する必要があり，プライバシーの観点から問題がある．提案したプロトコルを利用することにより，より安全なシステムを設計することが可能になると考えられる．

また，提案プロトコルは匿名オークションに組み込むことも可能であると考えられる．提案プロトコルを利用したネットワーク経由の新しいサービスの開発することが今後の課題である．

文　献

[1] Y. Lindell and B. Pinkas, Privacy Preserving Data Mining, Advances in Cryptology – Crypto '00 Proceedings. LNCS 1880, Springer-Verlag, pp. 20-24, (2000).

[2] A. Evfimievski, R. Srikant, R. Agrawal and J. Gehrke, "Privacy Preserving Mining of Association Rules", Proc. of 8th ACM SIGKDD Intl. Conf. on Knowledge Discovery and Data Mining (KDD) pp. 217-228 (2002).

[3] Jaideep Vaidya, Chris Clifton, Privacy-preserving k-means clustering over vertically partitioned data, Proceedings of the ninth ACM SIGKDD international conference on Knowledge discovery and data mining, pp. 206 - 215 (2003).

[4] R. N. Wright and Z. Yang, Privacy-preserving Bayesian network structure computation on distributed heterogeneous data. In Proc. of the Tenth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pages 713–718. ACM Press, (2004).

[5] Koutarou Suzuki and Makoto Yokoo, Secure Generalized Vickrey Auction using Homomorphic Encryption, Seventh International Financial Cryptography Conference (FC-03) (2003).

[6] O. Goldreich. Secure multi-party computation, working draft, (2001).

[7] Moni Naor and Kobbi Nissim, Communication preserving protocols for secure function evaluation, Proceedings of the thirty-third annual ACM symposium on Theory of computing, pp. 590-599, (2001).

[8] Rakesh Agrawal, Alexandre Evfimievski and Ramakrishnan Srikant, Information sharing across private databases, Proceedings of the 2003 ACM SIGMOD, pp. 86-97, (2003).

[9] Pascal Paillier, Public-Key Cryptosystems Based on Composite Degree Residuosity Classes, EUROCRYPT 1999, pp223-238 (1999).

[10] M. -C. Silaghi and D. Mitra. Distributed constraint satisfaction and optimization with privacy enforcement. Intelligent Agent Technology, pp. 531-535, (2004).

[11] Michael J. Freedman, Kobbi Nissim, and Benny Pinkas. Efficient Private Matching and Set Intersection. In Christian Cachin and Jan Camenisch, editors, Advances in Cryptology , EUROCRYPT (2004).

[12] Wenliang Du and Mikhail J. Atallah. Privacy-preserving statistical analysis. In Proceeding of the Seventeenth Annual Computer Security Applications Conference, (2001).

[13] Bart Goethals, Sven Laur, Helger Lipmaa and Taneli Mielikа"inen. On Private Scalar Product Computation for Privacy-Preserving Data Mining. The 7th Annual International Conference in Information Security and Cryptology (ICISC 2004), volume 3506 of Lecture Notes in Computer Science, pages 104–120 (2004).

[14] Pascal Paillier, Public-Key Cryptosystems Based on Composite Degree Residuosity Classes, EUROCRYPT 1999, pp223-238 (1999).

[15] Hiranmayee Subramaniam, Rebecca N. Wright, Zhiqiang Yang, ",Experimental Analysis of Privacy-Preserving Statistics Computation," In Proceedings of the Workshop on Secure Data Management, held in conjunction with VLDB '04, August 30, (2004).

[16] 佐久間，小林，内積比較プロトコルに基づく分散巡回セールスマン問題のセキュアな最適化，電子情報通信学会 コンピュータセキュリティ研究会 (IPSJ-CSEC) (2006).

付　録

1. Paillier cryptosystem

Paillier cryptosystem is known as one of semantically secure cyrptosystems with homomorphic property [9].

The public key of Paillier is the RSA modulus $n = pq$, where $p, q \in P$, and element $g \in Z_{n^2}^*$ whose order is divisible by n. The secret key is $\lambda = \mathrm{lcm}(p-1, q-1)$.

In Paillier cryptosystem, a message m is encrypted by

$$c = E(m; r) = g^m r^n \mod n^2, \qquad \text{(A·1)}$$

for a random integer $r \in Z_n^*$. As shown in A·1, Paillier cryptosystem holds additive homomorphic property.

The ciphertext c is decrypted by

$$c = \mathrm{Enc}(m; r) = L(c^\lambda \mod n^2) L(g^\lambda \mod n^2)^{-1}, \qquad \text{(A·2)}$$

where $L(a \mod n^2) = (a-1)/n$ for an integer a such that $a = 1 \mod n$.

It is known that that semantic security of the Paillier cryptosystem is as intractable as breaking the decisional composite residuousity problem.