プライバシーを保護した公平なリストマッチング

渡邊裕治[†] 沼尾雅之[†]

多項式の根としてリストを表現することにより，リストの項目を秘匿したままリストの共通部分を交換する手法を提案する．本方式は，オフラインの第三者機関をトラブルを解決する仲裁者として利用することにより，公平なリストの比較を実現する．

Fair Private List Matching Schemes

Yuji Watanabe[†] and Masayuki Numao[†]

A method for computing common elements between private lists is presented in this paper, where the lists are represented as polynomials whose roots are the element values. Our approach uses an off-line trusted arbiter in order to achieve the fairness of exchanging the knowledge of the common elements.

1. はじめに

複数のサーバからなるネットワークにおいて，各サーバがそれぞれ異なるデータの組合せから構成されるリストを秘密に保持しているものとする．この状況で各サーバ間でリストの共通部分が何であるかを計算する問題（共通部分計算，List Matching）を考える．たとえば，金融機関が支払延滞者のリストを持つとする．支払延滞者のリストは各金融機関の重要な企業秘密である．その一方で，各金融機関は，複数の金融機関で支払を滞らせているメンバを要注意貸出先として登録したいと考えている．このような場合，各金融機関は延滞者のリストを公開することなく，複数の金融機関で共通に延滞者として登録されている借り手を調査する必要がある．

このような問題を解決するために，暗号学的手段を用いた従来手法が知られている．Naorらは紛失多項式計算（Oblivious Polynomial Evaluation，OPE）を用いた手法を示している[1)]．OPEとは，2者間（Alice，Bobとする）のプロトコルであり，Aliceの秘密入力 x_A を入力として，Bobと通信した後，Bobが持つ秘密の n 次多項式 $f_B(x)$ の出力 $f_B(x_A)$ をAliceのみが得るという性質を持つプロトコルである．文献1)では，OPEをサブプロトコルとして共通部分の計算に利用する以下の手法を示している．

(1) S_A と S_B は，それぞれ n 次多項式 $f_A(x)$，$f_B(x)$ を秘密に用意する．
(2) S_A はOPEを用いて $\{f_B(\alpha_i)\}_{i=1}^n$ を，同様に S_B も $\{f_A(\beta_i)\}_{i=1}^n$ を計算する．
(3) S_A は $\{f_A(\alpha_i)+f_B(\alpha_i)\}_{i=1}^n$ を，S_B は $\{f_A(\beta_i)+f_B(\beta_i)\}_{i=1}^n$ を，それぞれ公開する．

このプロトコルでは，双方が単独では計算できない多項式 $f_A(x)+f_B(x)$ にデータの値を入力した結果を公開しているため，各サーバのリストにないデータ X が相手のリストに含まれているかを無制限に計算することはできない．

このプロトコルはAliceとBobがプロトコルに従う限り互いのリストの秘匿性を維持することが可能である．ところが，AliceとBobの一方が能動的に不正を行った場合，不正者が相手に対して有利な情報を取得することが可能である．たとえば，S_A がOPEの出力を偽り，S_B に対して $\{f'_A(\beta_i)\}_{i=1}^n$（ここで，$f'_A(x)\neq f_A(x)$）を送ることにより，$S_A$ は共通部分を知ることができるが，S_B は共通部分を知ることができない（もしくは共通でない値を共通部分として認識してしまう）．また，最後に一方だけが値を公開しない場合，一方だけが共通部分を知りうる状況が発生する．

一方，沼尾は，リストをその要素項目を根にする多項式（リスト表現多項式）で表現することにより，共通部分抽出を共通根導出に帰着させる手法を示している[2)]．

† 日本アイ・ビー・エム株式会社，東京基礎研究所
IBM Japan, Tokyo Research Laboratory

すなわち，A は $\mathcal{L}_A = \{\alpha_1, \ldots, \alpha_n\}$ を表現するために，$f_A(\alpha_i) = 0$ $(i = 1, \ldots, n)$ となるような n 次多項式 $f_A(x)$ を用意する．B の持つ多項式を $f_B(x)$ とすると，その加算結果の多項式 $F(x) = f_A(x) + f_B(x)$ は，両者の共通項目を根に持つ．だが，このプロトコルでは安全に多項式の和を求めるため，プロトコル中で信頼できる第三者機関（TTP）をオンラインで利用できる必要があるため，TTP に負荷が集中することが予想される．また，この方式は各サーバがプロトコルに従う場合には秘匿性を維持できるが，能動的な不正に対する安全性は考慮されていない．

このような能動的な不正は現実に起こりうる問題である．たとえば，先の金融機関の延滞者リストの照合では，自身のリストを偽ることで，他の金融機関が持つ延滞者リストに関する情報を入手することができる．このようなケースを考慮した場合，他の金融機関が正しいリストを照合しているか検証する手段がなければ，すべての参加者が安心してシステムを利用することができない．

文献 3) は OPE を拡張することにより，(1) Alice は $f_A(\tilde{x}) = 0$ を満たす $\tilde{x}$ について，$f_B(\tilde{x}) = 0$ かを判定できる，(2) Alice は $f_A(\tilde{x}) \neq 0$ を満たす $\tilde{x}$ について，$f_B(\tilde{x}) = 0$ か判定できない，(3) Bob は Alice の持つ秘密の多項式 $f_A(x)$ に関する情報を得ることができない，という性質を満たすプロトコルを提案している．このプロトコルを利用することにより，OPE に基づく文献 1) の手法と同様に，共通部分を計算するプロトコルを構成できる．この共通部分計算プロトコルは，文献 3) の持つ入力の検証可能性により，「Alice は自分のリストにない値が Bob のリストに含まれるかを判定することはできない」という性質を満たすことができる．だが，文献 3) は Bob が Alice の入力に対し，正しく多項式を計算することを前提にしている．したがって，このプロトコルだけでは，Alice が入力した値を Bob がリストに含む場合，Bob が「自分のリストにはない」と偽るといった Bob の不正を防ぐことはできない．

本論文は，従来手法[2),3)]を拡張し，(1) 互いの持つリストの共通部分以外の情報を相手にいっさい漏らさない（秘匿性，Privacy），(2) サーバの不正行為により一方が不利を被ることを防止する（公平性，Fairness），という性質をオフライン型の第 3 者信頼機関を用いて実現する手法を示す☆．

本手法は，各サーバの持つリストを多項式として表現し，多項式の係数に対するコミットメントを事前に公開する．このコミットメントを用いて，(1) サーバ間でプロトコル中で交換される情報が正確であること，(2) 不正発覚時にコミットメントから調停機関が共通部分を計算することができること，を検証可能にする．これにより，不正なサーバが利益を得ることを防止し，また不正検出時には，調停機関に依頼することにより，公正なやり方でプロトコルを終了できるようにする．

1.1 関連技術

オンライン型の TTP を用いる手法は文献 2)，5)，6) がある．一方，オンライン型の TTP を用いない手法は文献 1)，7)，8) がある．文献 1) は Oblivious Polynomial Evaluation（OPE）を用いてリストの共通部分を計算する手法を示している．また，文献 7) は ElGamal 暗号に基づく OPE を示している．文献 3) では，文献 7) で示される OPE の入力がコミットされた多項式の根となっていることを 2 者間で非対話的に証明することで，共通部分計算に対して応用する手法を示している．だが，この手法では，共通部分の計算結果は一方にのみ与えられるため，共通部分の計算結果を 2 者間で公平に交換することを考慮していない．

2. 準　　備

2.1 パラメータ

本論文で用いるパラメータを定義する．G_q を Decisional Diffie-Hellman（DDH）仮定が成立する位数 q（q は素数）の群とし，g，h を G_q のランダムな元とする．ここで，$\log_g h$ は未知とする．$H(\cdot)$ を理想的な一方向性ハッシュ関数，$\alpha \in Z_q$ に対するコミットメントを $\pi(\alpha, r) = g^{\alpha} h^{r}$ $(r \in_R Z_q)$ とする☆☆．また，G_q 上の ElGamal 暗号 $E_y(m, r)$ を $E_y(m, r) = (g^r, my^r)$（ただし，$r \in_R Z_q$，m は平文，y は公開鍵）とする．対応する秘密鍵による復号を D_y と表す（つまり，$D_y(E_y(m, r)) = m$）．m が G_q 上の元に限定される場合，この暗号化は DDH 仮定の元で強秘匿☆☆☆であることが知られている．また本論文では，ElGamal 暗号の次の性質を用いる．

$$(E_y(m, r))^k = E_y(m^k, kr)$$
$$E_y(m, r) \times E_y(m', r') = E_y(mm', r + r')$$

☆ 本論文は研究報告[4)]に基づく拡張である．

☆☆ $x \in_R G$ は「G からランダムに取り出した要素を x とする」の意．

☆☆☆ メッセージの対 (m_0, m_1) とそのいずれかの暗号文 $E_e(m_b)$ $(b \in \{0, 1\})$ を与えられて，1/2 よりも高い確率で b を判定することが計算量的に困難であるという性質．

以後，文脈に応じて $E_y(m,r)$ の公開鍵 y，および乱数 r を省略して $E(m)$ とする記述を適宜用いることにする．

2.2 モデル

サーバ A，B および調停機関 T を考える．各サーバはそれぞれ n，$\bar{n}$ 個のデータをリストに保持しており，すべてのデータには一意に区別できる番号（データ番号）が割り振られているものとし，データ番号全体の集合を $\mathcal{L}$ とする．また，A が持つ n 個のデータのデータ番号のリストを $\mathcal{L}_A = \{\alpha_1, \ldots, \alpha_n\}$ とする．同様に B のリストを $\mathcal{L}_B = \{\beta_1, \ldots, \beta_{\bar{n}}\}$ とする．T は，公開鍵暗号 $E_{y_T}()$ に対応する復号鍵を保持する．T は通常プロセスでは登場せず，例外発生時に正常にプロトコルを終了させるための機能を持つ．

本論文が対象とする「共通部分抽出」は任意の 2 組のサーバ A，B の間で，それぞれの持つ秘密のリスト $\mathcal{L}_A$ と $\mathcal{L}_B$ の共通部分 $\mathcal{L}_A \cap \mathcal{L}_B$ を互いに共有することである．この際，(1) 共通部分以外に関する情報を相手に漏らさないこと，(2) 一方だけが共通部分を知る不正を防ぐことが要求される．以下にプロトコルの流れを示す．

コミットメントフェーズ A は $\mathcal{L}_A$ に関するコミットメント com_A および生成パラメータ $open_A$ を生成し，com_A を公開する．$open_A$ は A が秘匿する．同様に B も com_B を公開し $open_B$ を秘匿する．

リストの比較 A と B の間の処理の流れを次に示す．

(1) **コミットメントの検証** A は，com_B が正しいことを検証する．ここで，例外時には com_B を用いて例外解決できることを確認する．不正な場合は以後の処理を行わず，中止を宣言する．B も com_A を検証する．

(2) **応答の生成** A は，com_B と $open_A$ を用いて応答 ans_A を計算し，B へ送信する．B も同様の処理を行い，応答 ans_B を A へ送信する．

(3) **結果出力** A は，com_B を用いて ans_B を検証する．検証を通過すれば結果 res_A を計算する（受信できなければ例外発生を宣言する）．ans_B が正しければ res_A は共通部分である．ans_B が不正であれば，res_A はエラーとなり例外発生を宣言する．逆に，B も ans_A に対して同様の処理を行う．

例外処理 例外が発生した場合には A は T と通信して com_B と $\mathcal{L}_A$ から共通部分を計算する（B も同様）．

各サーバは，リストに対するコミットメントを公開することにより，プロトコル中で他のサーバに対して自身のリストを偽ることはできない．また，コミットメントには，例外発生時に一方が不利を被らないよう，T が調停できるようにするための情報が含まれている．したがって，各サーバは「コミットメントが正確に構成されており，万一の場合には調停機関による問題解決が可能であること」をリスト比較の冒頭においてチェックすることができる．

2.3 基本プロトコル

本論文で用いるいくつかの構成要素を示す．

ElGamal 暗号を用いた OPE A は値 $\gamma\ (\in Z_q)$ を，B は多項式 $f_B(x) = \sum_{i=0}^{n} b_i x^i \pmod q$ を秘密に保持する．A の公開鍵を y とする．本プロトコルは，(1) A は B に γ を知られずに，$g^{f_B(\gamma)}$ を得ることができる，(2) A は $f_B(x)$ に関してそれ以外の情報を知ることはできない，という性質を持つ．以下にプロトコルを示す．

(1) $i = 1, \ldots, n$ について，A は乱数 $r_i\ (\in_R Z_q)$ を用いて g^{γ^i} を ElGamal 暗号化する（$c_i = E_y(g^{\gamma^i}, r_i)$）．$A$ は，$c_1, \ldots, c_n$ を B へ送信する．

(2) B は，乱数 $r_0 (\in_R Z_q)$ を選び，次の計算を行う．

$$\hat{c} = E_y(g^{b_0}, r_0) \times \prod_{i=1}^{n} {c_i}^{b_i} = E_y(g^{f_B(\gamma)}, \tau)$$

ここで，$\tau = r_0 + \sum_{i=1}^{n} b_i r_i \pmod q$ である．B は $\hat{c}$ を A へ送信する．

(3) A は，$\hat{c}$ を復号して $g^{f_B(\gamma)}$ を得る．

証明プロトコル 1 m_0，m_1 を G_q の元，$\hat{c} = (c_1, c_2) = E_y(m_1, \delta) = (g^\delta, m_1 y^\delta)$ を公開鍵 y を用いた m_1 の ElGamal 暗号文とする．このとき共通入力 $(g, y, m_0, \hat{c})$ に対し，暗号文 $\hat{c}$ に対応する平文 m_1 の m_0 に対する離散対数 γ を知っていることを証明する．すなわち，知識の非対話証明 $(e, s, t) = PK\{(\gamma, \delta) : (c_1 = g^\delta) \wedge (c_2 = m_1 y^\delta) \wedge (m_1 = {m_0}^\gamma)\}$ は次のように構成できる．

(1) r_1，$r_2 \in_R Z_q$ を選ぶ．

(2) 次式により (e, s, t) を計算する．

$$e = H(g \| y \| m_0 \| \hat{c} \| g^{r_1} \| y^{r_1} {m_0}^{r_2})$$
$$s = r_1 - e\delta, \quad t = r_2 - e\gamma \pmod q$$

検証者は，次式が成立するとき証明を受理する．

$$e = H(g \| y \| m_0 \| \hat{c} \| g^s {c_1}^e \| y^s {m_0}^t {c_2}^e)$$

証明プロトコル 2 m_1，m_2，m_1'，m_2' を G_q の元，$\hat{c}_1 = (c_{1,1}, c_{1,2}) = E_y(m_1', \delta_1) = (g^{\delta_1}, m_1' y^{\delta_1})$，$\hat{c}_2 = (c_{2,1}, c_{2,2}) = E_y(m_2', \delta_2) = (g^{\delta_2}, m_2' y^{\delta_2})$ を公開鍵 y を用いたそれぞれ m_1'，m_2' の ElGamal 暗号文とする．

このとき共通入力 $(g,\ y,\ m_1,\ m_2,\ \hat{c}_1,\ \hat{c}_2)$ に対し，暗号文 $\hat{c}_1$，$\hat{c}_2$ に対応する平文 m_1'，m_2' のそれぞれ m_1，m_2 に対する離散対数が等しいことを証明する．すなわち，知識の非対話証明 $(e,s,t,u) = PK\{(\gamma,\delta_1,\delta_2) : \{(c_{i,1} = g^{\delta_i}) \wedge (c_{i,2} = m_i' y^{\delta_i}) \wedge (m_i' = {m_i}^{\gamma})\}_{i=1,2}\}$ は次のように構成できる．

(1) 乱数 r_1，r_2，$r_3 \in_R Z_q$ を選ぶ．

(2) 次式により，(e,s,t,u) を計算する．

$$\begin{aligned} e = H(g\|y\|m_1\|m_2\|\hat{c}_1\|\hat{c}_2\|g^{r_1}\|g^{r_2} \\ \|{y^{r_1}m_1}^{r_3}\|{y^{r_2}m_2}^{r_3}) \\ s = r_1 - e\delta_1, \quad t = r_2 - e\delta_2 \\ u = r_3 - e\gamma \pmod q \end{aligned}$$

検証者は，次式が成立するとき証明を受理する．

$$\begin{aligned} e = H(g\|y\|m_1\|m_2\|\hat{c}_1\|\hat{c}_2\|g^s{c_{1,1}}^e\|g^t{c_{2,1}}^e \\ \|{y_1}^s{m_1}^u{c_{1,2}}^e\|{y_2}^t{m_2}^u{c_{2,2}}^e) \end{aligned}$$

同様に $PK\{(\gamma,\{\delta_i\}_{i=1}^n) : \{(c_{i,1} = g^{\delta_i}) \wedge (c_{i,2} = m_i' y^{\delta_i}) \wedge (m_i' = {m_i}^{\gamma})\}_{i=1}^n\}$ を構成することも可能である．

証明プロトコル 3 m_0 を G_q の元，$i = 1,\ldots,n$ のそれぞれ対して $\hat{c}_i = (c_{i,1}, c_{i,2}) = (g^{\delta_i}, m_i y^{\delta_i})$ を公開鍵 y を用いた m_i の ElGamal 暗号文とする．このとき，共通入力 $(g,y,m_0,\hat{c}_1,\ldots,\hat{c}_n)$ に対し，$(m_0, D_y(\hat{c}_1), D_y(\hat{c}_2),\ldots,D_y(\hat{c}_n)) = (m_0, {m_0}^{\gamma}, {m_0}^{\gamma^2},\ldots,{m_0}^{\gamma^n})$ という関係を満足する γ が存在することを γ を明かさずに証明する．すなわち，知識の非対話証明 $(e,\{s_i\}_{i=1}^n,t) = PK\{(\gamma,\{\delta_i\}_{i=1}^n) : \{(c_{i,1} = g^{\delta_i}) \wedge (c_{i,2} = m_i y^{\delta_i}) \wedge (m_i = {m_0}^{\gamma^i})\}_{i=1}^n\}$ は次のように構成できる．ここで，簡潔のため，$(c_{0,1},c_{0,2}) = E_y(m_0,0) = (1,m_0), \delta_0 = 0$ とする．

(1) r_1，$r_2 \in_R Z_q$ を選ぶ．

(2) 次式により $(e,s_1,\ldots,s_n,t)$ を計算する．

$$\begin{aligned} e = H(g\|y\|m_0\| \\ \{(\hat{c}_i, g^{r_i}{c_{i,1}}^w, y^{r_i}{c_{i,2}}^w)\}_{i=1}^n) \\ s_i = r_i + e(\delta_{i-1}\gamma - \delta_i) \pmod q \\ t = w - e\gamma \pmod q \end{aligned}$$

検証者は，次式が成立するとき証明を受理する．

$$\begin{aligned} e = H(g\|y\|m_0\|\{(\hat{c}_i, g^{s_i}{(c_{i-1,1})}^t{c_{i,1}}^e, \\ y^{s_i}{(c_{i-1,2})}^t{c_{i,2}}^e)\}_{i=1}^n) \end{aligned}$$

3. プロトコル

A，B をそれぞれ n，$\bar{n}$ 個の要素から構成されるリストを持つサーバとする．A，B は互いに相手のリストのサイズをプロトコル開始時に知っているものとする．最大のリストサイズを $N = \max(n,\bar{n})$ とする．A はリスト $\mathcal{L}_A = \{\alpha_1,\ldots,\alpha_n\}$ に対し，$f_A(x) = \prod_{\alpha_l \in \mathcal{L}_A}(\alpha_l - x)/\alpha_l \pmod q$ を計算する．このとき，$f_A(x) = 1 + \sum_{l=1}^n a_l x^l$ は定数項が 1 であり，$\mathcal{L}_A$ のすべての要素を根に持っている．同様に，B はリスト $\mathcal{L}_B = \{\beta_1,\ldots,\beta_{\bar{n}}\}$ に対し $f_B(x) = 1 + \sum_{i=1}^{\bar{n}} \bar{a}_l x^l$ を計算する．A は $\alpha_i \in \mathcal{L}_A$ を入力とする OPE を実行することにより，α_i が B の多項式 $f_B(x)$ の根になっているかを検査する．これにより，α_i が共通部分であるか知ることができる．

コミットメント生成 A は係数 $\{a_l\}_{l=1}^n$ に対して $\{c_l = g^{a_l}h^{b_l}\}_{l=1}^n$ を作成する（b_l は乱数）．$w_A(x) = \sum_{l=1}^n b_l x^l \pmod q$ とする．次に，以下の処理を $i = 1,\ldots,n$ について行う（y は A の公開鍵）．

(1) u_i，$v_i \in_R Z_q$ を選び，$g_i = g^{u_i}$，$h_i = h^{v_i}$ とする．次に，$\{\psi^{(i,j)} = E_y(g^{{\alpha_i}^j})\}_{j=1}^N$，$\{\psi_g^{(i,j)} = E_y({g_i}^{{\alpha_i}^j})\}_{j=1}^{\bar{n}}$，$\{\psi_h^{(i,j)} = E_y({h_i}^{{\alpha_i}^j})\}_{j=1}^{\bar{n}}$，$\{\psi_c^{(i,j)} = E_y({c_j}^{{\alpha_i}^j})\}_{j=1}^n$，および $\psi_t^{(i)} = E_{y_T}(g^{\alpha_i})$ を計算する（y_T は調停機関 T の公開鍵）．また，その計算が正確に行われていること示す証明 $pk_{i,1}$ を構成する．$\psi_t^{(\cdot)}$ から調停機関は g^{α_i} を復号できることから，「調停機関が問題発生時に問題解決できる」ということが検証可能である．

$$\begin{aligned} pk_{i,1} = PK\{(\gamma) : \\ \cap_{j=1}^N \{D_y(\psi^{(i,j)}) = g^{\gamma^j}\} \\ \wedge\ \cap_{j=1}^{\bar{n}} \{D_y(\psi_g^{(i,j)}) = {g_i}^{\gamma^j}\} \\ \wedge\ \cap_{j=1}^{\bar{n}} \{D_y(\psi_h^{(i,j)}) = {h_i}^{\gamma^j}\} \\ \wedge\ \cap_{j=1}^{n} \{D_y(\psi_c^{(i,j)}) = {c_j}^{\gamma^j}\} \\ \wedge\ D_{y_T}(\psi_t^{(i)}) = g^{\gamma}\} \end{aligned}$$

この証明は以下の $N+2$ 個の証明を組み合わせることにより構成できる．ここで，$sub\_pk_{i,1}^{(1)},\ldots,sub\_pk_{i,1}^{(N)}$ および $sub\_pk_{i,1}^{T}$ は前章で述べた「証明プロトコル 2」の手法を，$sub\_pk_{i,1}^{poly}$ は「証明プロトコル 3」の手法をそれぞれ用いることにより構成する．

$$\begin{aligned} sub\_pk_{i,1}^{(j)} = \\ PK\{\ (\gamma) : D_y(\psi^{(i,j)}) = g^{\gamma} \\ \wedge\ D_y(\psi_g^{(i,j)}) = {g_i}^{\gamma} \wedge D_y(\psi_h^{(i,j)}) = {h_i}^{\gamma} \\ \wedge\ D_y(\psi_c^{(i,j)}) = {c_j}^{\gamma}\} \\ sub\_pk_{i,1}^{T} = PK\{\ (\gamma)\ : \\ \{D_{y_T}(\psi_t^{(i)}) = g^{\gamma} \wedge D_y(\psi^{(i,1)}) = g^{\gamma}\} \\ sub\_pk_{i,1}^{poly} = PK\{\ (\gamma)\ : \\ \{D_y(\psi^{(i,j)}) = g^{\gamma^j}\}_{j=1}^N\} \end{aligned}$$

(2) $f_A(\alpha_i) = 0$ を満たすことを示す証明 $pk_{i,2}$ を前章の「証明プロトコル 1」の手法により構成

する．$f(\alpha_i)=0$ のとき，$g\times\prod_{j=1}^{n}\psi_c^{(i,j)}=E(g^{f_A(\alpha_i)}h^{w_A(\alpha_i)})=E(h^{w_A(\alpha_i)})$ が成立する事実より，この値の h に対する離散対数の知識を証明することは，$f_A(\alpha_i)=0$ を証明することと等価である（逆に，$f_A(\alpha_i)\neq 0$ であれば，証明を構成することは不可能である）．

$$pk_{i,2}=PK\left\{(\delta):D_y\left(g\times\prod_{j=1}^{n}\psi_c^{(i,j)}\right)=h^{\delta}\right\}$$

(3) コミットメント com_A は次のように構成される．

$$com_A=\{c_i,\ g_i,\ h_i,\ pk_{i,1},\ pk_{i,2},\ \psi_t^{(i)},\ \{\psi^{(i,j)}\}_{j=1}^{N},\ \{\psi_g^{(i,j)}\}_{j=1}^{\bar{n}},\ \{\psi_h^{(i,j)}\}_{j=1}^{\bar{n}},\ \{\psi_c^{(i,j)}\}_{j=1}^{n}\}_{i=1}^{n}$$

一方，生成パラメータ $open_A$ は，

$$open_A=\{a_i,\ b_i,\ u_i,\ v_i\}_{i=1}^{n}$$

となる．

同様に B も $open_B=\{\bar{a}_i,\bar{b}_i,\bar{u}_i,\bar{v}_i\}_{i=1}^{\bar{n}}$ を用い，

$$com_B=\{\bar{c}_i,\ \bar{g}_i,\ \bar{h}_i,\ \bar{pk}_{i,1},\ \bar{pk}_{i,2},\ \bar{\psi}_t^{(i)},\ \{\bar{\psi}^{(i,j)}\}_{j=1}^{N},\ \{\bar{\psi}_g^{(i,j)}\}_{j=1}^{n},\ \{\bar{\psi}_h^{(i,j)}\}_{j=1}^{n},\ \{\bar{\psi}_c^{(i,j)}\}_{j=1}^{\bar{n}}\}_{i=1}^{\bar{n}}$$

を生成し，公開する．

応答の生成 com_A を受け取った B は以下の処理を $i=1,\ldots,n$ に対して行う．

(1) $pk_{i,1}$ および $pk_{i,2}$ を検証する．

(2) ElGamal 暗号を用いた OPE と同様の手順により $\varphi_g^{(i)}$，$\varphi_h^{(i)}$ を計算する．$\varphi_g^{(i)}$ は A が B から返すことを期待している値 $f_B(\alpha_i)$ の暗号化である．

$$\varphi_g^{(i)}=E_y(g_i)\times\prod_{j=1}^{n}(\psi_g^{(i,j)})^{\bar{a}_j}=E_y({g_i}^{f_B(\alpha_i)})$$

$$\varphi_h^{(i)}=\prod_{j=1}^{n}(\psi_h^{(i,j)})^{\bar{b}_j}=E_y({h_i}^{w_B(\alpha_i)})$$

(3) $f_B(\alpha_i)$ が零か非零か以外の情報を隠蔽するため，$\varphi_g^{(i)}$ を $\xi_1^{(i)}$ 乗することにより $\mu_g^{(i)}$ を計算する．また，$w_v(\alpha_i)$ に関する情報を隠蔽するため，$\varphi_h^{(i)}$ に $\nu^{(i)}=(h_i)^{\xi_2^{(i)}}$ をかけ，ξ_3 乗することにより $\mu_h^{(i)}$ を計算する．

$$\mu_g^{(i)}=(\varphi_g^{(i)})^{\xi_1^{(i)}}\quad(\xi_1^{(i)}\in_R Z_q)$$
$$\nu^{(i)}=(h_i)^{\xi_2^{(i)}}\quad(\xi_2^{(i)}\in_R Z_q)$$
$$\mu_h^{(i)}=(\nu^{(i)}\times\varphi_h^{(i)})^{\xi_1^{(i)}}$$

(4) (2)，(3)が正確に計算されていることを A の側で検証可能にするための証明 $\{pk_{i,3}\}_{i=1}^{n}=\{\lambda_g^{(i)},\ \lambda_h^{(i)},\ s^{(i)}\}_{i=1}^{n}$ を構成する．これにより応答は $ans_B=\{\mu_g^{(i)},\nu^{(i)},\ \mu_h^{(i)},\ pk_{i,3}\}_{i=1}^{n}$ となる．

$$pk_{i,3}=PK\{\gamma_i:g_i=g^{u_i}\wedge h_i=h^{v_i}\wedge Y=g\prod_{j=1}^{\bar{n}}\bar{c_j}^{\alpha_j{}^{j}}=g^{f_B(\alpha_i)}h^{w_B(\alpha_i)}\wedge D_y((\mu_g^{(i)})^{1/u_i}(\mu_h^{(i)})^{1/v_i})=((\nu^{(i)})^{1/v_i}Y)^{\gamma_i}\}$$

ただし，$\lambda_g^{(i)}$，$\lambda_h^{(i)}$，$e^{(i)}$，$s^{(i)}$ は次式により計算される．

$$\lambda_g^{(i)}=(\varphi_g^{(i)})^{\xi_3^{(i)}}\quad(\xi_3^{(i)}\in_R Z_q)$$
$$\lambda_h^{(i)}=(\nu^{(i)}\times\varphi_h^{(i)})^{\xi_3^{(i)}}$$
$$e^{(i)}=H(com_A\|\ com_B\|\ \nu^{(i)}\ \|\ \mu_g^{(i)}\ \|\mu_h^{(i)}\ \|\lambda_g^{(i)}\ \|\ \lambda_h^{(i)})$$
$$s^{(i)}=\xi_3^{(i)}-e^{(i)}\times\xi_1^{(i)}$$

である．

ここで $pk_{i,3}$ が成立するならば，(2)，(3)が正確に計算されていること，すなわち $\mu_g^{(i)}=E_y(g^{\chi_i f_B(\alpha_i)})$ を満たす χ_i が存在することを以下に示す（χ_i が存在すれば，明らかに A は $\mu_g^{(i)}$ から $f_B(\alpha_i)=0$ かどうかを判定できる）．初めに，$\mu_g^{(i)}=E_y({g_i}^{l_{11}}g^{l_{12}}{h_i}^{l_{13}}h^{l_{14}})$，$\mu_h^{(i)}=E_y({g_i}^{l_{21}}g^{l_{22}}{h_i}^{l_{23}}h^{l_{24}})$，$\nu^{(i)}={g_i}^{l_{31}}g^{l_{32}}{h_i}^{l_{33}}h^{l_{34}}$ とする（ただし，$l_{ij}\in Z_q$）．このとき，$pk_{i,3}$ が成立するならば，次式が成立する．

$$(u_il_{11}+l_{12})/u_i+(u_il_{21}+l_{22})/v_i=\gamma_i(u_il_{31}+l_{32})/v_i+\gamma_i f_B(\alpha_i)$$
$$(v_il_{13}+l_{14})/u_i+(v_il_{23}+l_{24})/v_i=\gamma_i(v_il_{33}+l_{34})/v_i+\gamma_i w_B(\alpha_i)$$

このとき，証明者 B は $u_i=\log_g g_i$，$v_i=\log_h h_i$ の知識を持たないため，次式の成立が必要である．

$$(l_{11},l_{12},l_{13},l_{14})=(\gamma_i f_B(\alpha_i),\ 0,\ 0,\ 0)$$
$$(l_{21},l_{22},l_{23},l_{24})=(\gamma_i l_{31},\gamma_i l_{32},\gamma_i(l_{33}+w_B(\alpha_i)),\gamma_i l_{34})$$

したがって $pk_{i,3}$ が成立すれば，$\mu_g^{(i)}=E_y({g_i}^{\gamma_i f_B(\alpha_i)})=E_y(g^{u_i\gamma_i f_B(\alpha_i)})$ が成立する．

結果の生成 A は応答 ans_B を受け取ると $i=1,\ldots,n$ に対して以下の処理を行う．

(1) ans_B に含まれる $pk_{i,3}$ を検証する．

$$\tilde{e}^{(i)}=H(com_A\|\ com_B\|$$

$$\nu^{(i)} \parallel \mu_g^{(i)} \parallel \mu_h^{(i)} \parallel \lambda_g^{(i)} \parallel \lambda_h^{(i)})$$

$$\sigma_g^{(i)} = D_y((\mu_g^{(i)})^{1/u_i}) \quad [= g^{\xi_1^{(i)} \times f_B(\alpha_i)}]$$

$$\sigma_h^{(i)} = D_y((\mu_h^{(i)})^{1/v_i}) \quad [= h^{\xi_1^{(i)} \times (w_B(\alpha_i) + \xi_2^{(i)})}] \quad [= g^{\xi_3^{(i)} \times f_B(\alpha_i)}]$$

$$\tau_h^{(i)} = D_y((\lambda_h^{(i)})^{1/v_i}) \quad [= h^{\xi_3^{(i)} \times (w_B(\alpha_i) + \xi_2^{(i)})}]$$

$$\eta^{(i)} = (\nu^{(i)})^{1/v_i} \times g \prod_{j=1}^{\bar{n}} \bar{c}_j^{\alpha_j{}^j} \quad [= g^{f_B(\alpha_i)} h^{(w_B(\alpha_i) + \xi_2^{(i)})}]$$

を計算し，次式が成立するか検証する．

$$\tau_g^{(i)} \tau_h^{(i)} = (\eta^{(i)})^{s^{(i)}} (\sigma_g^{(i)} \sigma_h^{(i)})^{\tilde{e}^{(i)}}$$

(2) 検証が通過しなければ例外処理を行う．$\sigma_g^{(i)} = 1$ ならば，$f_B(\alpha_i) = 0$ であることから，$\alpha_i \in \mathcal{L}_B$ が分かる．逆に，$\sigma_g^{(i)} \neq 1$ ならば，$\alpha_i \notin \mathcal{L}_B$ である．

例外処理 例外発生時には，A は com_A および com_B を T へ送信する．T は com_A に含まれる $\bar{\psi}_t^{(i)} = E_{y_T}(g^{\alpha_i})$，および com_B に含まれる $\bar{\psi}_t^{(i)} = E_{y_T}(g^{\beta_i})$ を復号し，g^{α_i}，g^{β_i} を求める．$i = 1, \ldots, n$，$j = 1, \ldots, \bar{n}$ について，T は $\rho^{(i,j)} = (g^{\alpha_i}/g^{\beta_j})^{z^{(i,j)}}$（ただし，$z^{(i,j)} \in_R Z_q$）を計算し，$A$ および B へ送信する．A は $\rho^{(i,j)} = 1$ ならば $\alpha_i = \beta_j$ であると判定できる．

4. 安 全 性

本章では提案プロトコルの安全性について議論する．

4.1 秘 匿 性

本プロトコル中，A が B から得る情報はコミットメント com_B と応答メッセージ ans_B の 2 つである．これら 2 つの情報から，A が共通部分以外の有意な情報を得ることができないとき，「B のリストの共通部分以外の要素が秘匿される」と呼ぶ．以下，コミットメントと応答メッセージの秘匿性について議論する．

要件 1（コミットメントの秘匿性） A は B のコミットメント com_B から L_B，$f_B(x)$ に関する情報を得ることはできない．

【証明】 証明プロトコル 1，2，3 の零知識性，および ElGamal 暗号の強秘匿性より明らか．

要件 2（応答メッセージの秘匿性） A は $\{\alpha_1, \ldots, \alpha_n\} \in L_A$ を入力とした B の応答 ans_B から $f_B(\alpha_i) = 0$ かどうか以外の情報を得ることはできない．

【証明】 コミットメントの検証により，B は A の入力が正しいことを検証する．したがって，A が得ることができる結果は $g^{\xi_1^{(i)} \times f_B(\alpha_i)}$，$h^{\xi_1^{(i)} \times (w_B(\alpha_i) + \xi_2^{(i)})}$，$g^{\xi_3^{(i)} \times f_B(\alpha_i)}$，$h^{\xi_3^{(i)} \times (w_B(\alpha_i) + \xi_2^{(i)})}$，$g^{f_B(\alpha_i)} h^{(w_B(\alpha_i) + \xi_2^{(i)})}$ である．ここで，$\xi_1^{(i)}$，$\xi_2^{(i)}$，$\xi_3^{(i)}$ は B の選択する乱数であるため．$f_B(\alpha_i) \neq 0$ であれば，DDH 問題の困難性より，A はこれらの値をランダムな値と区別することはできない．

4.2 能動的不正に対する安全性

能動的不正とは A，B のいずれかのメンバが行う以下の 2 種類の不正である．

コミットメントに対する能動的不正 公開するコミットメントを不正に計算し，自分の多項式の根でない値（すなわち自身のリストにない値）を相手の多項式に入力することにより，共通部分以外の情報を入手しようとする．以下は，A が不正をする例である．

(1) A はリスト L_A に対応する多項式 $f_A(x)$，$w_A(x)$ を構成し，$\{c_i\}_{i=1}^n$ を計算する．

(2) A は異なるリスト $\tilde{L_A} (\neq L_A)$ の要素に対して，コミットメントの $\{c_i\}_{i=1}^n$ 以外の要素を計算する．これに $\{c_i\}_{i=1}^n$ をあわせて $\widetilde{com}_A$ として公開する．

(3) A は B から応答を受け取り，$\tilde{L_A} \cap L_B$ $(\neq L_A \cap L_B)$ を計算する．

応答メッセージに対する能動的不正 相手の正しい入力に対し，自身の多項式とは異なる多項式の出力を計算することにより応答メッセージを構成する，あるいは応答メッセージを送信しない，などの手段により，正しい共通部分の情報を相手に与えないようにする．以下は，B が不正をする例である．

(1) A はリスト L_A に対応するコミットメント com_A を計算する．

(2) B はリスト L_B に対応するコミットメント com_B を計算する．

(3) B は異なるリスト $\tilde{L_B}$ に対応する多項式 $\tilde{f_B}(x)$ を用いて，A への応答メッセージを計算する．

(4) A は B から応答を受け取り，$L_A \cap \tilde{L_B}$ $(\neq L_A \cap L_B)$ を計算する．

一方，上述の能動的不正に対する耐性とは，(1) 上記の不正を検出できる，(2) 不正検出時に例外処理に問題解決できることを事前に検証できる，を保証することである．これを満たすために以下の 2 つの性質が必要である．

要件 3（コミットメントの検証可能性） B は A の入力がコミットしていた値に対応する入力であること，かつ例外解決が可能であることを検証できる．

【証明】 com_A を見た B は，$pk_{i,1}$ から，ある (α_i, g_i, h_i) に対して $\{\psi^{(i,j)}\}_{j=1}^{N}$，$\{\psi_g^{(i,j)}\}_{j=1}^{\bar{n}}$，$\{\psi_h^{(i,j)}\}_{j=1}^{\bar{n}}$ および $\{\psi_c^{(i,j)}\}_{j=1}^{n}$ が正確に計算されていることが検証できる．また $pk_{i,2}$ から，その α_i，および $\{c_i\}_{i=1}^{n}$ に係数がコミットされている多項式 $f_A(x)$ について $f_A(\alpha_i) = 0$ が成立することが検証できる．このことから，B は com_A があるリスト L_A に対して正確に計算されていることを確認することができる．

また，$pk_{i,1}$ の中で，$\psi_t^{(i)} = E(g^{\alpha_i})$ を検証することにより，例外発生時に，T が $\psi_t^{(i)}$ から g^{α_i} を計算できる，すなわち T がこの値を使って例外解決を行うことができることを確認できる．

要件 4（応答メッセージの検証可能性） A は B からの応答メッセージ ans_B から計算される結果が B がコミットメント com_B を計算する際に用いた多項式 $f_B(x)$ を用いて計算される結果と同じであることを検証できる．

【証明】 前章の「応答の生成 (4)」で議論したように，A は ans_B に含まれる $pk_{i,3}$ から，ある $\chi \in Z_q$ および事前にコミットされた多項式 $f_B(x)$ に関して，$\mu_g^{(i)} = E_y(g^{\chi f_B(\alpha_i)})$ が成立することを検証できる．したがって，$D_y(\mu_g^{(i)})$ を観察することで，$f_B(\alpha_i) = 0$ かどうかを知ることができる．

4.3 公平性

例外処理において，調停機関 T は，例外が本当に生じているかを確認しなければならない．送受信されるメッセージに不正がある場合には，T はその事実を検証することで，例外の発生を確認できる．一方，たとえば A と B の間のリストの共通部分計算において，A が B に対して応答を送信したにもかかわらず，B が A に対して応答を送らないことによる例外発生も考えられる．この場合には，メッセージからエラーが検出できなくても例外の解決が必要になる．ところが，より困難なのは，T は以下の 2 つのケースを区別しなければならないことである．

- B が本当に応答メッセージを A に対して送っていない．
- A が，実際は B とのやりとりを行っていないにもかかわらず，例外発生を主張し，不正に B の持つリストとの共通部分を知ろうとしている．

したがって，公平な共通部分計算を実現するため，T は一定のルールに基づいて例外解決する必要がある．ここで，提案プロトコルが対象とする公平性を次に定義する．

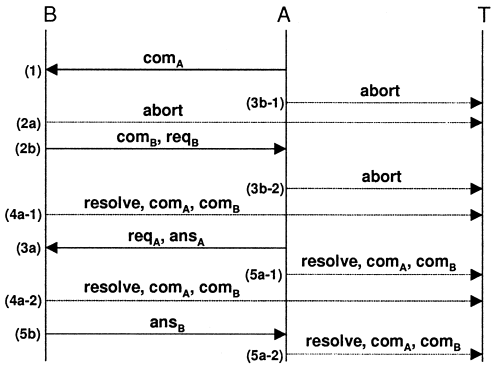

図 1 例外発生の検証方法
Fig. 1 Dispute resolution protocol.

要件 5（公平性） B を能動的な不正を行ったとしても，A が正しくプロトコルを行う限り，プロトコルの実行結果が以下のいずれかになるとき,「共通部分計算が公平性を満たす」とする．

- A と B がともに $L_A \cap L_B$ を得る（このケースを「$Success$」とする）．
- A と B がともに $L_A \cap L_B$ を得ることができない（このケースを「$Failure$」とする）．

公平性を満たす共通部分計算は，前節で述べた能動的不正に対する検証可能性に加え，公平な署名交換[9]で用いられている中止宣言（Abort）を利用した問題解決手法を利用することにより解決できる．ここでは，非同期（Asynchronous）型のメッセージ交換の例を示す（**図 1**）．この場合，T が例外解決を行うルールは「A（リスト交換の開始者）から中止宣言（Abort）が出されていないこと」である（ここで B は中止宣言を出せないことに注意）．T は例外解決を行った場合には，共通部分を A と B の両者に対して配布するものとする．またコミットメントはプロトコルの最初で交換するものとする．メッセージ交換プロトコルを示す（以下は A が最初に B に対してコミットメントを開示する例である）．

(1) A は B にコミットメント com_A を開示する．
(2) B は com_A が正しいかチェックする．
  (a) B は com_A が不正であればリスト比較を止める．
  (b) B は com_A が正しければ，A に対してコミットメント com_B を開示する．
(3) A は com_B の到着を待つ．
  (a) com_B が到着し，それが正しければ，B に対して応答 ans_A を送信する．

(b) com_B が到着しないか (3a-1), あるいは不正な場合 (3a-2) は，中止宣言を行う．

(4) B は ans_A の到着を待つ．

(a) ans_A が到着しないか (4a-1), あるいは ans_A が不正な場合 (4a-2) は例外解決を行う．

(b) 正しければ，A に対して応答 ans_B を送信する（B は結果を得る）．

(5) A は ans_B の到着を待つ．

(a) ans_B が到着しないか (5a-1), あるいは ans_B が不正な場合 (5a-2) は例外解決を行う．

(b) 正しければ，A は結果を得る．

ここで，上記のプロトコルが公平性を満たすことを以下に示す．まず，A は (3a) のタイミングまで中止宣言を出すことができる．このタイミング以降，A も B も相手の検証済みのコミットメントを保持しているため，いつでも例外解決により公平な結果を導くことが可能である．上記のメッセージ交換の流れを以下のとおり時間軸上で分類することにより，いずれのケースでも Success か Failure になるということを示す．

- (1) から (2b) の間：B だけが A のコミットメントを持っている．
  - A の中止宣言→ $Failure$
  - B の例外解決要求→ $Success$☆
- (2b) から (3a) の間：A と B が互いのコミットメントを持っている．
  - A の中止宣言→ $Failure$
  - A の例外解決要求→ $Success$
  - B の例外解決要求→ $Success$
- (3a) から (5b) の間：B だけが応答を得ている．
  - A の例外解決要求→ $Success$
  - B の例外解決要求→ $Success$
- (5b) 以降：A は応答を，B は正しい結果を得ている．
  - A の例外解決要求→ $Success$

5. 効　　率

本手法は，(1) サーバの能動的な攻撃を検出できる，(2) 例外発生時に，調停機関の調停によりプロトコルを安全に終了できる，(3) 調停機関は例外発生時にのみ関与する，という性質を満たす．

☆ このとき，B のみが com_A を持ち例外解決が可能となるが，例外解決を行う際に，B は T に com_A だけでなく，com_B も提示する必要がある．そのため，T は例外解決後，A にも共通部分の情報を送ることができる．

従来手法[2]は，本論文を比較すると，(1) コミットメントを公開しなくてもよい，(2) 各サーバの計算量が少ない，という 2 点が優れているが，能動的な攻撃に対して考慮されていない．また TTP をオンラインで用いる点も本方式とは異なる．各サーバが不正操作を行わず，秘匿性だけを達成したいという場合には従来手法[2]を，各サーバが不正操作により利益を得ることを防ぎたい場合には本論文を用いるという利用形態になる．

6. ま と め

本論文では，複数のサーバが秘密に保持するリストの共通部分が何であるかを計算する List Matching に対し，(1) 互いの持つリストの共通部分以外の情報を相手にいっさい漏らさない（秘匿性，Privacy），(2) サーバの不正行為により一方が不利を被ることを防止する（公平性，Fairness），という性質をオフライン型の第 3 者信頼機関を用いて実現する手法を示した．提案方式は，金融機関の持つ支払延滞者のリストなど，企業秘密の名寄せを行う場合に，各企業が自身のリストを偽ることで，他の他企業のリストに関する情報を不当に入手することを防止することが可能である．

さらなる拡張として，より一般的なリストの共通部分抽出を考えた場合，本論文で対象としている値の全一致にとどまらず，部分一致や大小比較なども望まれる．リストのプライバシーを維持したまま，より複雑な比較演算を公平に実現する方法は今後の課題である．

参 考 文 献

1) Naor, M. and Pinkas, B.: Oblivious transfer and polynomial evaluation, *Proc. STOC'99* (1999).
2) 沼尾雅之：A method for symmetric private list matching, *CSS2001* 予稿集 (2001).
3) 渡邊裕治，沼尾雅之：共通根検査プロトコル，*SCIS2002* 予稿集 (2002).
4) 渡邊裕治，沼尾雅之：プライバシーを保護したリストマッチングの拡張，*CSS2002* 予稿集 (2002).
5) 小林邦生：1 対多人数間マッチングプロトコル，信学技報，ISEC2001-73 (2001).
6) Matsuo, S. and Ogata, W.: Matching oblivious transfer: How to exchange valuable data, *IEICE Trans. Fundamentals*, E86-A (1), pp.189–193 (2003).
7) Lindell, Y. and Pinkas, B.: Privacy preserving data mining, *Proc. CRYPTO2000* (2000).
8) 國廣　昇，Maywah, A.: 多人数による oblivious value comparison プロトコル，*SCIS2001* 予稿集 (2001).

9) Asokan, N., Shoup, V. and Waidner, M.: Optimistic fair exchange of digital signatures, *Proc. EUROCRYPT'98* (1998).

(平成 14 年 11 月 29 日受付)
(平成 15 年 6 月 3 日採録)

渡邊 裕治

昭和 48 年生．平成 13 年東京大学大学院工学系研究科電子情報工学専攻博士課程修了．同年日本アイ・ビー・エム株式会社入社．東京基礎研究所副主任研究員．ネットワークセキュリティ，プライバシー保護方式に関する研究開発に従事．工学博士．

沼尾 雅之（正会員）

昭和 33 年生．昭和 58 年東京大学大学院工学系研究科電子情報工学専攻修士課程修了．同年日本アイ・ビー・エム株式会社入社．現在，同社東京基礎研究所にて ID&プライバシーグループ担当，専任研究員．ネットワークセキュリティ，プライバシー保護方式に関する研究開発に従事．人工知能学会理事．