属性指定型動的コミュニティ生成のための セキュリティとプライバシー

沼尾雅之† 渡邊裕治†

本論文では，個人情報を共通属性に使った動的コミュニティ生成のためのセキュリティとプライバシーについて論じ，これらを満たす構成例として，オフライン型の属性鍵配信システムを使ったシステムを示す．共通の趣味や好みといった，個人属性に基づいたコミュニティにおいては，メンバだけが知りうる情報も共有されることから，プライバシーの保護が重要になる．属性鍵配信システムにおいては，送信者は，指定した属性を満たしたユーザにだけ，メッセージを配信することができ，一方，ユーザは，自分の属性を送信者を含めた誰にも知られることなく，自分宛のメッセージを解読することができる．技術的には，1対1のプロトコルであるOblivious Transfer（OT）を，多対多のマルチキャストメッセージ配信に対応させるために，オフライン属性鍵管理サーバを導入し，主催者，ユーザ，鍵管理サーバという3者のプロトコルを構成した．従来のマッチメーキングや，パーソナライズドページ，プッシュ型情報配信サービスなどは，ほとんどがサーバを全面的に信頼することを前提にしていたが，本技術を用いることによって，完全にプライバシーが守られる形で，こうしたサービスが実現できる．

Security and Privacy for Attribute-based Dynamic Community Creation

Masayuki Numao† and Yuji Watanabe†

In this paper, we first defined the security and privacy model which is necessary for the creation of attribute-base dynamic community on Internet. For a small and private community whose members share the common interests or preferences, privacy protection is very important because the members want to exchange very private information. We then propose an attribute-based message multicast system as a realization of the secure and privacy-protected dynamic community model. Our idea is to distribute the Oblivious Transfer (OT) protocol by introducing an attribute key server which generates the key pair for each attribute, and delivers the public and private keys to the senders and receivers, respectively, before actual attribute-based messaging is taken place. There are many applications of this technology, such as privacy-protected personalized message multicast, match-making, dynamic community creation, and auction, etc.

1. はじめに

近年の少子化，高齢化といった社会構造の変化にともなって，インターネットの利用も，従来のECやB2Bなどの企業，大組織主体のものから，インスタント・メッセージやコミュニティ形成など，地域や個人を重視したものへと変化している[13]．コミュニティとしては，会社，学校，市区町村など，その個人が属する組織や地域から決められるものから，スポーツクラブや同好会など，その個人の趣味や好みで決まるようなものまで考えられる．前者の，組織が主体となったコミュニティは，入会の条件が組織によって決められ，半永続的なものであるのに対し，後者のコミュニティは，たとえば，同じ趣味の人が2人以上集まったときに半自然的に生じ，また，趣味が変化したら解散するなど，非常に動的なものになる．こうしたコミュニティは，共通の属性を持った人たちが集まって形成されるものであり，趣味や好みといった，より個人的な属性が共通属性となることから，プライバシーの保護が重要になる．

インターネット上のコミュニティの中には，チャットルームのように出入り自由のものや，フォーラムのように議長が入会の審査をする場合もあるが，本論文では，主催者が，共通となる属性を指定することによって，コミュニティが生成され，その共通属性を有する人だけがメンバになれるような枠組みを提案する．また，このときに使われる属性は，会員証や免許証と

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

いった，第三者が証明しなければならない属性ではなく，趣味や嗜好といった個人的な属性や，病歴といったプライバシーを守らなければならない情報とする．

コミュニティの主催者にとっては，コミュニティ生成のときに，属性を満たすユーザを，メンバに指定しなければならないが，このときに，ユーザの属性を知ることは，そのユーザのプライバシーを侵害することになる．したがって，ユーザの属性を知ることなく，属性を満たすユーザに，グループ共通鍵を配るような，相反する目的を満足させるシステムが必要となる．

本論文では，オフラインの属性鍵管理サーバの導入と，ユーザとサーバとの間での Oblivious Transfer プロトコル（OT）に基づく事前属性鍵登録によって，ユーザのプライバシーや，それ以外のセキュリティを損なうことなく，属性指定型動的コミュニティ生成ができることを示す．OT は 1 対 1 のプロトコルであるので，マルチキャストには向かないが，鍵管理サーバと受信者との間の OT で，あらかじめ属性鍵を配布しておくことによって，主催者は，指定された属性を満たすユーザグループに対して，グループ共通鍵を配信することが可能になる．グループ鍵による配信システムは数多く提案されている[3),15)]が，受信者 ID からグループ鍵を構成するものがほとんどであり，属性鍵の組合せをグループ鍵とするものは知られていない．

本論文の構成は以下のとおりである．まず，2 章で，個人的コミュニティの指定に必要な任意属性について定義し，そのセキュリティ・プライバシー要件を示す．3 章では，この任意属性に基づく動的コミュニティ生成システムの構成法を示す．4 章では，ユーザが属性鍵を事前登録するための k-out-of-N OT のプロトコルを説明し，属性選択に関わるプライバシーが守られることを示す．5 章では，主催者がコミュニティを募集する際の，属性鍵配信システムのための条件鍵の構成法を示す．特に，複数の属性が AND や OR で結ばれた複合条件や，数値の大小比較をともなう数値属性の構成法について説明する．さらに，このモデルを応用したビジネスアプリケーションの例を，6 章で紹介する．

2. 任意属性におけるセキュリティとプライバシー

2.1 認定属性と任意属性

個人の持つ属性には，名前，住所，性別，年齢，職業，年収，趣味，好みなどさまざまであるが，これらを第三者に認定してもらう認定属性（Authorized 属性）と，個人の裁量で決められる任意属性（Discretionary 属性）に分けることができる．たとえば，前記の名前，住所，性別，年齢については，地方自治体の発行する住民票や，都道府県公安委員会の発行する運転免許証によって認定されるし，職業や年収については，会社の発行する就業証明書などによって認定されるが，趣味，好みについては，そのような認定証は存在しない．趣味，好み，宗教，支持政党などは，個人の信念や嗜好に基づく非常に個人的な属性であるので，ここでは任意属性と定義する．

ところで，こうした属性を IT 的に扱うものとして，属性証明書（AC: Attribute Certificate）がある．これは，通常の公開鍵証明書が本人性を証明するのに対して，その人物がユーザ権限として，どんな属性を持っているかを証明するもので，IETF の定める X.509 で仕様が定められている[10)]．また，発行も公開鍵証明書を発行する公開鍵認証局（CA）ではなく，属性認証機関（AA: Attribute Authority）によって行われる．このように，本人性と属性の認証を分ける動きは，OASIS の標準である SAML[11)]でも取り入れられており，複数の独立機関によるドメインをまたがった柔軟な認証・認可を可能にし，Federated ID という新しい認証サービスの提案にもつながっている[12)]．ところが，属性証明書で扱われる属性は，公的な第三者に認定してもらう認定属性だけで，趣味のような個人的な属性には，プライバシーの保護の観点から，第三者機関を認証機関とするのは適さない．筆者らは文献 16), 17) において，プライバシーを守りながら個人属性を指定したメッセージ配信や，個人属性で投票者の制限をできる電子投票をする仕組みを提案した．本論文でも，個人的なコミュニティ生成のために必要な属性は，趣味や好みといった任意属性が主になることから，この任意属性についてのセキュリティ，プライバシーを考察する．

2.2 任意属性のセキュリティ要件

たとえば，趣味を同じくする人たちのコミュニティを作ることを考える．コミュニティのメンバ同士は，お互いに趣味が同じだということを知っているのは問題ないが，コミュニティ以外のメンバには，その趣味のことは教えたくない．また，コミュニティ募集の話をメンバの友人などから聞いた人が，自分の趣味ではないのに，そのコミュニティに入りたいだけの理由で，一時的に自分の趣味を変えて入ってくるのも望ましくない．また，最初からすべてのコミュニティに入れるように，自分の趣味以外のすべての趣味を，あらかじめ登録しておくことも防がなければならない．以上をまとめると，セキュリティ要件は以下のように定めら

れる．

個人のプライバシー（P1） 個人が選択した属性は，本人以外は知りえない．もちろん，コミュニティのメンバは，お互いに共通した属性を持っていることは知っているが，共通属性以外の属性については知りえない．

コミュニティのプライバシー（P2） コミュニティ内で交わされる通信内容は，コミュニティメンバ以外のものには知りえない．

属性選択のコミット メント（S1） 個人がいったん選択した属性を，偽ることはできない．もちろん，属性選択時に，自分の属性を偽って決めることを防ぐことはできない．その場合には，その人は，自分の本当の属性を共通属性とするコミュニティには参加できなくなる．

属性値条件の遵守（S2） 属性ごとに決められたN者k択条件（k-out-of-N）を満たさなければならない．たとえば，趣味の選択肢が10個あって，そのうち3つまでが選択可能という制限が設けられる．

3. 属性指定型動的コミュニティ生成システムの構成

3.1 属性鍵の事前登録によるコミュニティ生成モデル

任意属性に基づく属性指定型動的コミュニティ生成システムを**図1**に示すように，ユーザ，主催者，オフライン属性鍵管理サーバから構成し，これら3者の間に，以下のような3つのプロトコルを定義する．

(1) 属性の事前登録プロトコル
(2) コミュニティ募集プロトコル
(3) コミュニティ内通信プロトコル

このように，属性の登録とコミュニティ募集のタイミングを別々にすることによって，2章で示した要件**S1**を満たすことができる．つまり，ユーザにあらかじめ属性を選択させておくことによって，コミュニティ募集時には，いったん選択した属性を変更することはできなくなる．

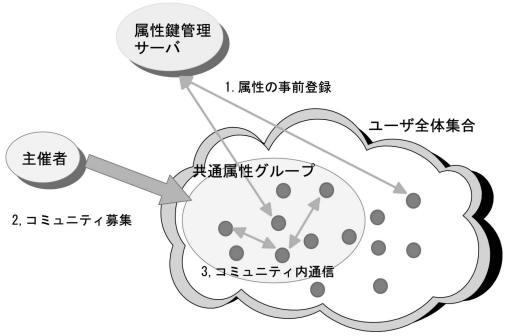

図1 属性指定型動的コミュニティ生成システム
Fig. 1 Attribute-based dynamic community creation system.

また，属性の登録とコミュニティ共通属性の指定のために，公開鍵系に基づく属性鍵を導入する．まず，属性鍵管理サーバは，個々の属性に対して，秘密鍵と公開鍵の鍵ペアを生成する．次に，属性の事前登録において，ユーザは自分の属性に対する属性秘密鍵を取得する．コミュニティ募集において，主催者は，生成したいコミュニティの属性を属性公開鍵によって指定する．これによって，主催者は，属性秘密鍵を知らずに，コミュニティの指定をすることができる．

通常，公開鍵系暗号は，送信者が公開鍵で暗号化したメッセージを送信し，これを受信者が，秘密鍵で復号して読むというモデルである．これに対応させると，主催者が送信者，共通属性を持つユーザグループが受信者で，さらに，特定のユーザを指定するのではなく，属性をアドレスとした属性通信のモデルと考えることができる．このような，属性通信のセキュリティ，プライバシーは以下のようになる．

- 通信の秘密：送信者が指定した属性を持たない受信者は，メッセージを読めない．
- 受信者のプライバシー保護：受信者の属性が，送信者および第三者に漏洩しない．

これは，それぞれ，2章で示したコミュニティのプライバシー **P2** と個人のプライバシー **P1** に対応する．**P2** が公開鍵暗号系自体の特性であるのに対し，**P1** は，普通に，属性鍵管理サーバから秘密鍵を取得するようにすると，属性鍵管理サーバが，どの鍵を取得したかを知ることになり，プライバシーが守られなくなってしまう．本論文では，属性鍵配布にOblivious Transferのプロトコルを応用することによって，個人のプライバシー **P1** と，属性値条件の遵守 **S2** を守る枠組みを提案する．

3.1.1 属性の事前登録

まず，コミュニティ募集では，第三者機関である，オフラインサーバを利用することによって，ユーザは，自分の属性（複数）を事前登録する．具体的には，ユーザは，サーバの用意した属性秘密鍵の中から，自分の属性に一致するものだけを，属性値条件の遵守（**S2**）の制限内で，サーバには，どれを選択したかを知らせずに（**P2**）取得する．このとき，ユーザ認証を行うことによって，1人のユーザが2回以上属性の事前登録をすることを防ぐことができる．

通常，このようなプライバシーを保持した通信のた

めの技術として，Oblivious Transfer（OT）[2),6)]が用いられることが多い．これは情報提供者と選択者の 2 人の間のプロトコルであり，提供者が持つ複数個の情報のうち，いくつかを選択者が選んで得るというものである．典型的な OT である 1-out-of-2 OT では以下の 2 つの要件が満たされる．

- 選択者のプライバシー：提供者は選択者がどの情報を選んだかを知ることができない．
- 提供者のプライバシー：選択者は選んだ情報以外を知ることはできない．

これらは，それぞれ，要件 **P2**，**S2** に対応する．

3.1.2 コミュニティ募集

主催者は，コミュニティ共通属性を指定し，その共通属性を持つユーザだけが，復号できるような属性条件鍵を構成し，それによってグループ共通鍵（セッション鍵）を暗号化したものを募集メッセージとする．そして，これを IP Multicast [8),9)]などのプロトコルを用いてマルチキャストする．マルチキャストされたメッセージは，ユーザ集合全体が受信することができるが，条件鍵の条件に適合するユーザだけが，メッセージを復号し，グループ共通鍵を取り出すことができる．

3.1.3 コミュニティ内通信

グループ共通鍵を復号できたユーザは，これをセッション鍵とすることによって，チャットルームに参加したり，メンバ間のメッセージ通信を行ったりする．チャットルームは ISP などが運営するが，メッセージは，すべて，グループ共通鍵によって暗号化されているので，その属性を持たない会員は，読むことができない．つまり，属性に適合する受信者だけがチャットルームに参加できる．属性条件として，位置情報なども入れられれば，場所や嗜好に特化した動的なコミュニティが構成できる．

3.2 定　　義

まず，以下の 3 者を定義する．

- 属性鍵管理サーバ（1 つ）：属性のとりうる属性値ごとに秘密鍵・公開鍵ペアを生成し，公開鍵を公開する．また，ユーザとの間で，属性値の受け渡しプロトコルを実行する．属性鍵サーバは，複数存在してもかまわない．たとえば，異なる属性に対して，異なる属性鍵サーバを用意してもよいが，ここでは，簡単のために 1 つとする．
- ユーザ（複数）：ユーザは，まず，属性の事前登録として，属性ごとに自分の選択した属性値に対する秘密鍵を，サーバとの間の属性値受け渡しプロトコルによって取得する．次に，主催者によるコミュニティ募集のときには，属性鍵によって暗号化された募集メッセージを，属性秘密鍵によって復号し，メッセージ内のグループ共通鍵を解読する．最後に，このグループ共通鍵によって，コミュニティ内通信を行う．
- 主催者（1 つ）：主催者は，コミュニティのメンバが持つべき共通属性を決め，それに対応した属性公開鍵をサーバから取得して，これらを組み合わせて属性条件鍵を構成し，この属性条件鍵によって，グループ共通鍵などのメッセージを暗号化したうえで，マルチキャストによって，コミュニティ募集をする．主催者は，1 つのコミュニティ生成にたいして，1 人必要である．特に主催者に対して特別な制限はなく，普通のユーザが主催者になることも可能である．

また，属性および，属性値を以下のように定義する．ここで，属性および，その属性のとりうる属性値は，あらかじめ決められているものとする．

- 属性集合：$S_A = \{A_i | i = 1, .., N_A\}$
- 属性値集合：属性 A_i に対する属性値集合 $V_i = \{v_{i,1}, v_{i,2}, ..v_{i,n_i}\}$
- 属性値条件：属性 A_i に対して，ユーザが選択できる属性値個数 $k_i, (1 \leq k_i \leq n_i)$ たとえば A_S が性別だとすると $V_S =$ { 男，女 } で，$n_S = 2$，$k_S = 1$ となる．

さらに，属性秘密鍵，属性公開鍵，属性条件，属性条件鍵，セッション鍵，グループ鍵，メッセージを以下のように定義する．

- 属性秘密鍵：属性 A_i に対する属性値集合 $V_i = \{v_{i,1}, v_{i,2}, ..v_{i,n_i}\}$ に対して，属性秘密鍵集合を $S_i = \{s_{i,1}, s_{i,2}, ..s_{i,n_i}\}$ とする．
- 属性公開鍵：属性 A_i に対する属性値集合 $V_i = \{v_{i,1}, v_{i,2}, ..v_{i,n_i}\}$ に対して，属性公開鍵集合を $Y_i = \{y_{i,1}, y_{i,2}, ..y_{i,n_i}\}$ とする．
- 属性条件（A_{Cond}）：複数の属性値を，&(AND)，|(OR) で組み合わせたもの．たとえば，{ 性別=男，年齢=30 代，職業=会社員，趣味=旅行またはパソコン } に対応する属性条件は，性別 (男)&年齢 (30 代)&職業 (会社員)&(趣味 (旅行)| 趣味 (パソコン)) と記述される．
- 属性条件鍵（$E_{Cond}(A_{Cond}, K)$）：属性条件 A_{Cond} を満たすユーザだけが，その属性秘密鍵を使って，セッション鍵 K を復号できるようにした暗号化．属性公開鍵で，セッション鍵を暗号化したものを組み合わせて，構成することができる．
- グループ共通鍵（K_G）：A_{Cond} の属性条件を満たすユーザだけが，復号し，共有できるセッション鍵．

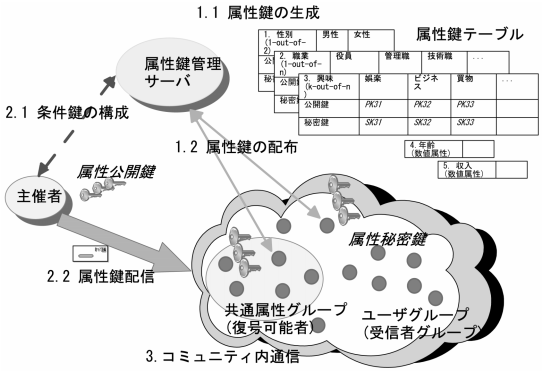

図 2 属性鍵配信プロトコル
Fig. 2 Attribute key distribution system.

- メッセージ（M）：主催者が，ユーザ集合に対してコミュニティ募集をするときのメッセージ．メッセージは，受信グループ指定のための属性条件 A_{Cond}，グループ共通鍵 K_G を属性条件鍵で暗号化したもの $E_{Cond}(A_{Cond}, K_G)$ と，グループ共通鍵で暗号化されたメッセージ本体から構成される．グループ共通鍵の配布だけが目的の場合には，メッセージ本体は空になる．

3.3 プロトコル

プロトコルは，動的属性指定型コミュニティ生成モデルに対応して，以下のようになる（**図 2** 参照）．ここで，G_q を Decisional Deffie-Helman（DDH）仮定が成立する位数 q の群とし，Z_q を素数 q の下での乗法群とする．そして，p は，$p = nq+1$（n は整数）を満たす大きな素数．g は G_q 上のランダムな元とする．

（1） 属性の事前登録

- 1.1 属性鍵の生成：鍵管理サーバは，登録された属性 A_i に対する属性値の集合 $\{v_{i,1}, v_{i,2}, .., v_{i,n}\}$ の各々の値に対して，属性秘密鍵 $s_{i,j} \in Z_q$ をランダムに選び，さらに属性公開鍵 $y_{i,j} = g^{s_{i,j}} \pmod p$ を公開する．
- 1.2 属性鍵の配布：ユーザは，属性鍵管理サーバとの間で，個々の属性 A_i ごとに，4 章に記述する k-out-of-n-OT を行うことによって，自分の属性に対する属性秘密鍵 s_{i,U_j}，$(j = 1, ..k_i)$ を，属性鍵管理サーバに知られることなく取得する．

（2） コミュニティ募集

- 2.1 条件鍵の構成：主催者は，複数の属性 A_{O_i} から，それぞれ複数の属性値 $v_{O_i,O_{i,j}}$，$(j = 1, .., n_{O_i})$ を選び（主催者は属性値個数条件を守る必要はない），これを AND や OR で結び付けることによって，複合属性条件 A_{Cond} を指定する．ここから，5 章に記述する属性条件鍵 $E_{Cond}(A_{Cond}, K_G)$ によって，グループ共通鍵 K_G を暗号化する．
- 2.2 属性鍵配信：主催者は，募集内容 m をグループ共通鍵 K_G を暗号化したもの $E(K_G, m)$ をメッセージ本体とし，全体のメッセージ M を以下のように構成する．
  $M = A_{Cond}||E_{Cond}(A_{Cond}, K_G)||E(K_G, m)$
  これをユーザグループ全体に対し，マルチキャストする．

（3） コミュニティ内通信：主催者の指定した属性条件を持つユーザだけが，属性条件鍵を復号することができ，グループ共通鍵 K_G と，募集メッセージ m を読むことができる．コミュニティ内通信では，このグループ共通鍵 K_G で，メッセージ m_G を，$E(K_G, m_G)$ のように，共通鍵方式で暗号化することによって，主催者と共通属性グループのメンバだけが読めるメッセージを構成できる．

4. k-Out-Of-N Oblivious Transfer による属性鍵配布

属性の中には性別のような二者択一のもの，年齢のように複数の中から 1 つを選ぶもの，さらに趣味のように，複数の中からいくつかを選ぶものがある．このような選択形態は，k-out-of-N Oblivious Transfer（OT）として一般化される．k-out-of-N OT を実現する方法としては，1-out-of-2 OT を要素技術として 1-out-of-N OT [6]を構成し，これを独立に k 回繰り返すことによって実現する方法と，k-1 次の多項式を用いて直接実現する方法がある[7),16)]．本論文では，選択可能数 N が，比較的小さいときに有効な後者の方法を，属性秘密鍵配布プロトコルとして用いる．

4.1 プロトコル k-out-of-N OT($s_0, .., s_n$)

サーバが持つ秘密情報を $s_1, .., s_n$ として，このうちの k 個をユーザに選ばせるプロトコル．ここで，G_q 上の ElGamal 暗号 $E_y(m)$ を $E_y(m) = (g^r, my^r)$ とする．ただし，$r \in Zq$, 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 $D_y(E_y(m, r)) = m$ となる．

（1） サーバはあらかじめランダムに秘密の値 $t_0 \in Z_q$ を決め，これに対応した公開値 $Q_0 = g^{t_0} \pmod p$ を計算し公開しておく．

（2） ユーザは，k 個の秘密鍵 $\{t_1, t_2, .., t_k\}$ をランダムに Z_q から選び，その公開鍵 $Q_i = g^{t_i} \pmod p$ を計算する．次に，$h(i), i = 1, .., k$ を選択した要素のインデックスとする（つまり，ユ

ーザはサーバの秘密情報 $s_{h(i)}$，$i = 1,..,k$ を秘密裏に取得したいとする）．まず，$k+1$ 点 $(0,Q_0),(h(1),Q_1),..,(h(k),Q_k)$ を通るような k 次多項式 $Y(x)$ はラグランジュの補間法を使えば一意に決められる．この多項式を使って n 点 $Y_i = Y(i)$，$i = 0,..,n-1$ を計算し，$\{Y_1, Y_2, .., Y_n\}$ をサーバに送る．

(3) サーバはユーザの公開している n 点が k 次多項式上の点であることを 4.2 節の方法で検証した後，正しければ，Y_i をそれぞれ ElGamal 暗号の公開鍵として，秘密情報 s_i を暗号化したもの $E_y(s_i, Y_i)$，$i = 1,..,n$ をユーザに送る．

(4) ユーザは $h(j)$，$j = 1,..,k$ によって指定された k 個の点については，それに対応する秘密鍵 t_j を持っているので，サーバから送り返された ElGamal 暗号文を復号できる．したがって，k 個の秘密情報を得ることができる．

4.2 n 点が k 次多項式上の点であることの検証

本来は，$n+1$ 個の点集合 $\{0,1,..,n\}$ から $k+1$ 個の点をランダムに選んだ 2 つの集合 S_1 と S_2 を作り，それぞれのセットから k 次多項式 $Y_1(x)$，$Y_2(x)$ を構成し，それらが等しいことを検証することが必要である．しかし，これを簡単に行うには，ランダムに $\delta(\in Z_q)$ を選び，$Y_1(\delta) = Y_2(\delta)$ を比較したとしても，誤って異なる 2 つの k 次多項式が点 δ で一致する確率は，$1-(k/q)$ であるので十分な検証ができる．これは以下のようにできる．

$$Y_1(\delta) \stackrel{?}{=} Y_2(\delta) \pmod p$$

$$\prod_{i\in S_1} Y_i^{\lambda_i} \stackrel{?}{=} \prod_{j\in S_2} Y_j^{\lambda_j} \pmod p$$

ただし，

$$\lambda_i = \sum_{k\in S_1} (\delta - k)(i-k)^{-1} \pmod q$$

かつ，

$$\lambda_j = \sum_{k\in S_2} (\delta - k)(j-k)^{-1} \pmod q$$

4.3 安全性の考察

サーバとユーザ双方のプライバシーが守られるかについて，以下のように考察される．

- **サーバ（提供者）のプライバシー**

ユーザの選択は公開鍵リスト $Y_0,..,Y_{n-1}$ で与えられるが，4.2 節によりこの点が k 次多項式上にあることを仮定すると，ユーザが選んだ点以外の Y_x は以下のように表現される．

$$Y_x = Q_0^{\lambda_0(x)} g^{(\sum_{i=1}^{k}(t_i \lambda_{h(i)}(x)))} \pmod p$$

ただし，

$$\lambda_i(x) = \sum_{j\in\{0,h(1),..,h(k)\}, j\neq i} (x-j)(i-j)^{-1}, \pmod q$$

これは，サーバの指定した Q_0 の離散対数が知られない限り，Y_x の離散対数も求められないことを意味するので，ユーザは k 個以上の秘密情報は知りえない．

- **ユーザ（選択者）のプライバシー**

ユーザの選択は公開鍵リスト $Y_1,..,Y_n$ で与えられるが，これらはサーバから見ると，サーバの指定した点 Y_0 を通る任意の k 次多項式上の点群と区別がつかない．したがって，この公開鍵リストのうち，どの k 個の離散対数をユーザが持っているかについての知識はなにも与えられない．

5. 属性鍵配信によるコミュニティ属性条件指定

主催者は，鍵管理サーバが公開している属性公開鍵を組み合わせることによって，属性条件 A_{Cond} に対応する条件鍵 $E_{Cond}(A_{Cond}, K)$ を構成する．ここで，$E_{P_K}(K)$ は，公開鍵 P_K でセッション鍵 K を暗号化することを，また，$E(K,M)$ は，秘密鍵 K でメッセージ M を，共通鍵暗号方式で暗号化することを示す．

5.1 複合属性条件鍵の構成

(1) AND 鍵の構成：属性条件 $Ai(v_{i,j})\&A_k(v_{k,l})$ に対しては，それぞれ属性公開鍵 $y_{i,j}$，$y_{k,l}$ が対応している．2 つのセッション鍵 K_1，K_2 をランダムに選び，これを公開鍵でそれぞれ暗号化すると条件鍵は $\{E_{y_{i,j}}(K_1), E_{y_{k,l}}(K_2)\}$ となり，対応するセッション鍵は $K = K_1 \oplus K_2$ になる．ただし，$\oplus$ はビットごとの排他的論理和とする．また，これ以外の方法としては，2 つのセッション鍵を使わずに，セッション鍵 K をランダムに選び，$E_{y_{i,j}}(E_{y_{k,l}}(K))$ で条件鍵とする方法もある．

(2) OR 鍵の構成：属性条件 $A_i(v_{i,j})|A_k(v_{k,l})$ に対しては，それぞれ属性公開鍵 $y_{i,j}$，$y_{k,l}$ が対応している．セッション鍵 K を 1 つランダムに選び，これを 2 つの公開鍵で暗号化する．条件鍵は $\{E_{y_{i,j}}(K), E_{y_{k,l}}(K)\}$ となる．

(3) AND/OR の複合条件：上記を最下位レベルのオペレータから繰り返して，条件鍵を結合し，セッション鍵を計算していけば，任意の AND，OR の

組合せに対する条件鍵およびセッション鍵が作れる．この最後のセッション鍵を，グループ共通鍵 K_G とする．

5.2 数値属性条件鍵の構成

年収や年齢などの数値属性に対しては，1,000 万円台とか，30 歳代などのように分割することによって，前述の 1-out-of-N OT で扱える属性値とすることもできるが，数値のままの属性値で受信者を指定したい場合もある．ここでは，ある数値属性 S に対して，受信者が属性値 P を登録し，発信者が属性値 Q を指定し，$P \geq Q$ のときに限り，受信者がメッセージを読めるような，条件鍵を生成することを考える．n ビットの正整数 P，Q のビット列表現を $P = (p_{n-1}, .., p_0)$，$Q = (q_{n-1}, .., q_0)$ とする．

(1) 属性鍵管理サーバは，数値属性 S に対して，n 個の秘密鍵ペア $(s_i^{(0)}, s_i^{(1)})$，$i = 0, .., n-1$ と，それに対する公開鍵ペア $(y_i^{(0)}, y_i^{(1)})$，$i = 0, .., n-1$ を生成する．

(2) 受信者は，鍵管理サーバとの間で，1-out-of-2 OT を n 回繰り返すことによって，属性値 P に対する属性秘密鍵 $s_i^{(p_i)}$，$i = 0, .., n-1$ を取得する．

(3) 送信者は，まず乱数 $k_{n-1}, .., k_0$ を生成し，K を数値属性条件（$X \geq Y$）に対するセッション鍵とする．次に，補助変数 $C = (c_{n-1}, .., c_0)$ を以下のように計算する．

$$c_j = E_{y_j^{(1)}}(k_j) \quad if \quad q_j = 1$$

$$c_j = E_{y_j^{(0)}}(k_j) || E_{y_j^{(1)}}(K) \quad if \quad q_j = 0$$

条件鍵は以下のようになる．

$(c_{n-1}, E(k_{n-1}, c_{n-2}), .., E(k_1, c_0))$ ここで，$k_0 = K$ となるように，k_0 を選ぶと，等号が成り立つとき（$P = Q$）でもセッション鍵が復号できる．

このように，条件鍵を構成することによって，最大 L の数値データに対して，長さ $log_2 L$ の条件鍵によって，大小関係の比較を記述することができる．

6. アプリケーション

本章では，オフライン型の属性管理サーバを用いた属性の事前登録と，属性条件を指定した，グループ共通鍵配信の枠組みを応用した，ビジネス的に将来性のあるアプリケーションについて紹介する．

6.1 マッチメーキングサービス

これはお見合いサービスである．サービスプロバイダは属性鍵管理サーバを運営し，ユーザが会員になる．主催者もユーザである．相手を見つけたいユーザは，交際希望相手の条件を属性鍵の組合せによって表現し，そのユーザとの交際条件やアドレスを記述したメッセージを配信する．

受信者は，自分で気に入れば返事をすることによって，交際を始めることができるが，そうでない場合には受信者のプライバシーは完全に守られる．また，主催者にとっても，交際希望相手としての条件を満たすユーザだけに自分の返信アドレスを記したメッセージを送ることができるので，属性を満たさない他人に対しては秘密にできる．同様のアプリケーションは，リストマッチングプロトコル[14]を用いても実現することができるが，1 対 1 のプロトコルを組み合わせているので，スケーラビリティに劣る．

6.2 パーソナライズド メールサービス

サービスプロバイダが属性鍵管理サーバを運営し，メールを配信する主催者に対して課金するようなモデルが考えられる．属性に関するプライバシーは完全に守られるので，ユーザは，安心して自分の属性に対する秘密鍵を取得し，パーソナライズされた情報を受け取ることができる．これは従来のデータベースマーケティングが，送信者側の類推によって，受信者を選別していたモデルと異なり，受信者が，自分のほしい情報を能動的に取ることができるため，よりヒット率の高い配信が可能になる．

一方，受信者側に課金をするような，プッシュ型情報配信サービスも考えられる．この場合は，情報プロバイダが属性鍵管理サーバを運営し，受信者は，属性秘密鍵を購入する形になる．たとえば，医療情報の配信サービスなどでは，質の高い情報を，必要とする患者に配信することが求められているが，このとき，患者の病歴などのプライバシを守ることが必要となり，本論文のような枠組みが有効になる．

ただ，こうしたメール配信システムでは，送信者が，メールの受信者数などの受信者に対しての統計的な情報を得たい場合があり，プライバシーを保持した枠内で，送信者への情報提供ができるようなシステムの開発は今後の課題となる[1]．

6.3 分散検索サービス

検索エンジンの運営者が属性管理サーバを運営し，属性としては，専門分野などをキーワードとして登録しておく．ユーザは自分の専門分野の属性秘密鍵を取得しておく．質問者が主催者で，質問をキーワードの組合せの形で配信する．ユーザは，質問が自分の専門に適合するときだけ，それを読むことができる．ビジネスモデルとしては，質問を読んだユーザが，返答するときに契約が結ばれ，その料金の一部が検索エンジ

ン運営者に支払われるようなモデルが考えられる．

7. おわりに

本論文では，個人情報を属性に使った，動的コミュニティ生成のためのセキュリティとプライバシーについて論じ，その実現例として，属性鍵配信システムを使った構成例を示した．技術的には，1対1のプロトコルであるOTを，多対多のマルチキャストメッセージ配信に対応させるために，オフライン属性鍵管理サーバを導入し，主催者，ユーザ，鍵管理サーバという3者のプロトコルを提案した．この構成法は，以下のように実用性の高い特徴を持つ．

- 効率性および鍵取得のオフライン性：ユーザは，サーバから属性秘密鍵を受け取るが，これは1ラウンドのプロトコルで実現される．事前に一度，鍵取得をしておけば，その後のマルチキャストに何回でも利用可能である．
- 主催者の登録不要：主催者は，サーバの属性公開鍵を利用するが，このとき，サーバとの対話は必要ないし，属性公開鍵は再利用可能なので，だれでもが主催者になりうる．
- サーバのオフライン性：サーバは，ユーザの鍵取得時だけに関わり，実際の通信には関わらない．したがって，実際の通信は，IPマルチキャストなどの一般的なマルチキャスト，あるいはブロードキャストプロトコルを使うことができる．
- 受信グループのオープン性：メッセージマルチキャストによって，主催者は，受信者グループおよび受信可能な全体集合を知ることなく送信ができる．いい換えると，ユーザは，サーバから属性秘密鍵を受け取るだけで，コミュニティに参加する資格を得ることができる．

本論文では，任意属性に限定したシステムを構成したが，公的属性認証機関に認定してもらった認定属性を，主催者がコミュニティ募集の際に属性条件の1つとして組み合わせることも可能である．これをさらに発展させると，複数の公的属性認証機関や，任意属性鍵管理機関の鍵を自由に組み合わせて，コミュニティを指定することが考えられる．このときの要件としては，属性条件を構成するときに，どこの機関で作られた鍵かを記述できなければならないが，それらを含めたプロトコルの標準化が今後の課題といえる．

参考文献

1) Aiello, B., Ishai, Y. and Reingold, O.: Priced Oblivious Transfer: How to Sell Digital Goods, Advances in Cryptology (*Eurocrypt 2001*), pp.119–135 (2001).
2) Bellare, M. and Micali, S.: Non-interactive oblivious transfer and applications, *Advances in Cryptology* (*Crypto '89*), pp.547–557 (1990).
3) Fiat, A. and Naor, M.: Broadcast Encryption, *Crypto93*, LNCS (1993).
4) Hubermann, B.A., Franklin, M., and Hogg, T.: Enhancing Privacy and Trust in Electronic Communities, *1st Conference on Electronic Commerce* (*EC*), New York, pp.78–86, ACM (1999).
5) Kormann, D.P. and Rubin, A.D.: Risks of the Passport Single Signon Protocol, *Computer Networks*, Vol.33, pp.51–58, Elsevier Science Press (2000).
6) Naor, M. and Pinkas, B.: Oblivious Transfer and Polynomial Evaluation, *Proc. STOC* (1999).
7) Mu, Y., Zhang, J. and Varadharajan, V.: m out of n Oblivious Transfer, *Information Security and Privacy* (*ACISP 2002*), pp.395–405 (2002).
8) Host Extensions for IP Multicasting. ftp://ftp.isi.edu/in-notes/rfc1112.txt
9) Internet Group Management Protocol, Ver 2. ftp://ftp.isi.edu/in-notes/rfc2236.txt
10) RFC 3281 on An Internet Attribute Certificate. http://www1.ietf.org/mail-archive/ietf-announce/Current/msg18344.html
11) OASIS Security Service TC, Security Assertion Markup Language (SAML). www.oasis-open.org/committees/security/
12) Liberty Alliance. http://www.projectliberty.org/
13) Eジャパン協議会：eコミュニティ構築支援活動. http://www.ejf.gr.jp/katsudou/index.html
14) 沼尾雅之：プライバシーを保持したリストマッチングプロトコル，CSS2001, IPSJ (2001).
15) 沼尾雅之，渡邊裕治：P2Pマルチキャストのための動的グループ鍵生成法，SCIS2002, IEICE (2002).
16) 沼尾雅之，渡邊裕治：プライバシーを保持した属性鍵配信システム，コンピュータセキュリティシンポジウム (CSS2002), IPSJ (2002).
17) 沼尾雅之，渡邊裕治：属性を考慮した匿名投票システムの提案，暗号と情報セキュリティシンポジウム（SCIS2003），IEICE (2003).

(平成15年 5 月16日受付)
(平成15年11月 4 日採録)

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・プライバシー技術担当，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．

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．