

P2P マルチキャストのための動的グループ鍵構成法

沼尾 雅之[†] 渡邊 裕治[†]

任意のホスト間の直接通信が容易だという P2P の環境下では、ホストどうしの結託も容易であるため、従来のクライアント・サーバ型のモデルを前提にした、受信者の結託閾値に基づいたグループ鍵暗号法では問題が生じる場合がある。本論文では、インターネットに常時接続されている計算機のように、全体集合や受信グループがあらかじめ指定できない条件下で、任意のホスト間でのマルチキャスト通信を目的にしたグループ鍵構成法を提案する。ここでは、任意のホストが情報発信者になることができ、また、任意の複数ホストを受信グループとして指定することができ、そのグループに属するホストだけが復号できるような、グループ鍵で暗号化されたメッセージを発信できる。この構成法では、受信グループ以外のユーザの結託にたいして耐性がある代わりに、復号処理のためにグループ内のホストどうしの通信が必要になる。本論文では、これを利用した新しいアプリケーションについても説明する。

Dynamic Group Key Construction for P2P Multicast

MASAYUKI NUMAO[†] and YUJI WATANABE[†]

Most existing group key encryption methods are based on client/server model, where clients are assumed to be disconnected unless they are intermediated by a server. Many group key encryption schema introduced a collusion threshold as a security parameter, by which, the system is secure unless the number of colluded peers is less than the parameter. However, under the P2P environment where any peer can directly communicate to other peer, collusion between peers is also very easy, and thus, it is not suitable to set it as a security parameter. In this paper, we propose a new group key construction for P2P multicast. It assumes Internet peers, any of which can join or leave to the network dynamically. Any peer can become a sender, and it can specify any subset of peers as a recipient group, and send a single message which could be decrypted by only the members of group. In this construction, system is secure against the collusion by any number of peers, on the other hand, the collaboration by the member of peers is necessary. We will also explain new applications by using this feature.

1. はじめに

インターネットにおけるブロードバンド接続や、有線および無線 TV 放送などをはじめとするブロードキャストチャンネルにおいて、加入者である特定グループのユーザのホストに対してだけコンテンツを配信するための技術が、多くのビジネスやアプリケーションにとって必要とされている。これらはマルチキャストのセキュリティとして研究されており¹³⁾、多数の受信者に対して、効率的かつ安全に鍵の配送、更新、削除ができることが求められている。暗号的にはグループ鍵配送問題として、Fiat らによる Broadcast Encryption⁵⁾などで定式化されているが、問題としては、ユーザグループの任意のサブセットを受信グループと

して、そのメンバだけが復号できるような暗号鍵の構成法を、個々のユーザにあらかじめ配っておく鍵のサイズと、送信者が送るメッセージの長さ、および鍵更新時に送るメッセージの長さなどとの関係で与えるものである。前提条件はさまざまであるが、不正ユーザの結託閾値をパラメータとしているものが多い。

ところで、現実のインターネットに接続された計算機(ホスト)の利用状態を見てみると、個々の計算機は、従来のクライアント・サーバモデルのように、すべての情報をサーバを介して通信しているわけではなく、自ら他のホストに直接接続して情報を交換する P2P モデルで構成されていると考えられる。これは、Napster や Gnutella といったファイル共有プログラムが、直接ホストどうしの接続によってファイルを交換していることから明らかである。また、最近のゲーム機やデジタル TV などのホームゲートウェイ端末も、インターネット接続機能を持っており、コンテン

[†] 日本アイ・ビー・エム東京基礎研究所
IBM Research, Tokyo Research Laboratory

ツ所有者や情報発信者が、当初前提にしていたクライアント・サーバ型のビジネスモデルが、成り立たなくなっている。このような環境下で、マルチキャストのセキュリティを考えるとときには、ホストどうしの結託を不正とするような、従来の仮定は成り立たなくなっており、P2P に適合した新しい仮定が必要となる。本論文では、この P2P 環境を前提にして、グループ鍵配送問題を再構成する。

本論文では、まず本モデル構築の動機となった、P2P 環境でのグループ鍵配信における仮定と要件について説明し、従来のモデルとの違いを明確にする。次に、準備として動的グループ鍵配送問題を定義し、ディールを必要とする場合と、必要としない場合の 2 つについて、プロトコルの構成法を示す。前者は秘密鍵暗号を、後者は公開鍵暗号を利用している。さらに、復号時に受信者間の協調が必要だという特徴を利用した、新しいアプリケーションについても説明する。また、本論文で使っている暗号手法は、グループ鍵暗号⁸⁾などの閾値暗号とも関連が深い⁹⁾が、これらとの比較についても説明する。

2. P2P 環境下でのグループ鍵配信システムへの要件

P2P 型システムが、従来のクライアント・サーバ型システムと異なる点としては、大きく以下があげられている³⁾。

- 対称性：クライアント・サーバ型では、サーバが情報発信、クライアントが情報受信というように、役割が非対称であったのに対して、P2P のホストは、クライアントとサーバの両方の機能をあわせ持っている。
- 接続性：クライアント・サーバ型では、クライアントがサーバの IP アドレスを指定することによって、サーバに接続していたが、P2P 型では、アプリケーション層に新たなアドレス空間を定義することによって、IP にとらわれないホストどうしの接続を確保しようとしている。また、モバイル環境も考慮しているため、動的なホストの加入や離脱にも対応している。
- 状態依存性：HTTP など IP 上のプロトコルが状態を持たないものであったのに対し、Peer 間の通信では、トランザクションの状態を保持したプロトコルを定義しているものが多い。

これらの特長によって、分散計算や協調計算システム、ファイル共有システムなどの P2P アプリケーションが実現されている。これを、グループ鍵配信の観点

から見ると、以下のような P2P 環境への対応が必要とされる。

- ホストどうしの協調動作への対応：ホスト機能の対称性およびホストどうしの接続性から、ホスト間の協調動作が普通に行われることが前提となる。これは、従来のグループ鍵配信モデルでは、受信者の結託攻撃と見なされていたものであるが、これを防ぐことはもちろんであるが、さらに、協調動作を積極的に利用した方法が望まれる。
- 動的な受信者集合への対応：ホスト間の接続性から、受信者集合は動的に変化する。全体集合も、受信グループ集合も変化するので、あらかじめこれらの集合を固定した方法では対応できない。送信者が、受信グループや閾値を動的に決められることが望ましい。
- スケーラビリティへの対応：実際のインターネットに接続されたホストを扱うためには、全体集合、受信グループとも非常に大きいものになる。したがって、プロトコルは、これらのサイズには依存しないことが望まれる。

ここから、P2P 環境下でのグループ鍵配信システムへの要件を以下のように定義する。

動的グループ鍵生成 送信者は、メッセージ送信時に受信グループを任意に決められる。

動的復号閾値生成 送信者は、指定した受信グループのうち、何人が集まれば復号できるかの閾値を、メッセージ送信時に決められる。次に定義する協調復号を前提にしているので、この閾値は、受信グループで指定されていたメンバが、復号前に離脱してしまうような場合に備えるものである。

協調復号 受信グループは、復号閾値で指定された人数が集まってはじめて、メッセージを協調復号することができる。このとき、ネットワークのエッジ部分にある受信者同士は、LAN などの低コストかつ高帯域の回線で接続されていることを仮定する。

結託耐性 受信グループ以外の者が何人共謀しても、送信されたメッセージの復号や、他のメンバの秘密鍵を知ることはできない。

全体集合非依存性 グループ鍵は全体集合には依存しない。

グループサイズ非依存性 メッセージ長は、受信グループの人数には依存しない。

3. 動的グループ鍵配送問題

3.1 定義

問題を定義するために、まず、参加者として次の 3

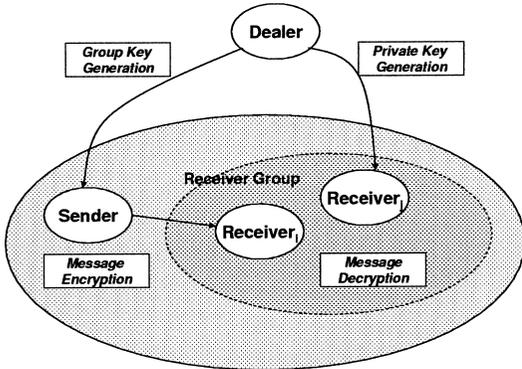


図1 動的グループ鍵暗号システム
Fig. 1 Dynamic group key cryptosystem.

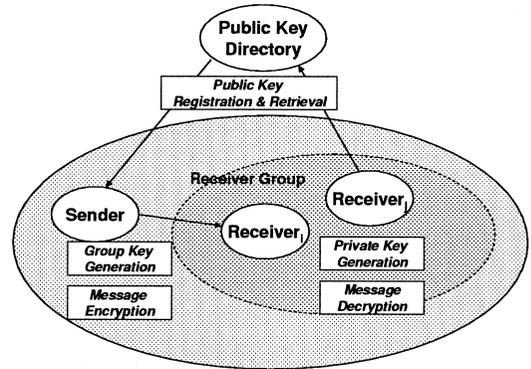


図2 公開鍵型動的グループ鍵暗号システム
Fig. 2 Public-key dynamic group key cryptosystem.

者を定義する (図 1 参照).
 ディーラ (D) ユーザのための秘密鍵を生成し, それを配布するもの. ユーザの秘密鍵を知っているので, 信頼された第三者機関が運営するのが普通である. グループ鍵の生成にもかかわることがある. 受信者 (R) 暗号化された情報を受信し, 秘密鍵を用いることによって復号する.
 発信者 (S) グループを選択し, そのグループ鍵を生成して情報を暗号化して発信する. グループ鍵の生成にディーラの助けを必要とする場合もある. さらに記号として以下のものを定義する.
 ユーザの全体集合 $U = \{R_1, R_2, \dots, R_N\}$, $|U| = N$ とする.

受信グループの集合 $G_R = \{R_{g_1}, R_{g_2}, \dots, R_{g_n}\} \subseteq U$, $|G_R| = n$ とする.
 受信グループの ID 集合 $G_{ID} = \{g_1, g_2, \dots, g_n\}$ とする.
 復号メンバの集合 $M \subseteq G_R$, $|M| = m$ とする.
 復号メンバの ID 集合 $G'_{ID} = \{g'_1, g'_2, \dots, g'_m\}$ とする.

3.2 パラメータ

本論文で用いるパラメータを定義する. p, q を $q|p-1$ を満たす大きな素数, g を有限体 Z_p 上の位数 q の元とする. このとき, g を生成元として構成される群 G_q 上で Decisional Diffie-Hellman (DDH) 仮定が成立するものとする. また, G_q 上の ElGamal 暗号を $ElG_y(M, r) = (g^r, My^r)$ とする. ただし, $r \in Z_q$ は確率暗号にするための乱数, $M \in Z_p$ は平文, y は公開鍵とする. 特に断らない限り, 計算は $\text{mod } p$ 上で行われるとする.

3.3 プロトコルの概要

プロトコルの概要は以下ようになる. 本論文の主目的はディーラを不要にすることであるが, ディーラ

が必要な場合と不必要な場合についての, 両方のプロトコルを説明する. また, ここで使われる要素アルゴリズム Ψ, Γ については後述する.

3.3.1 ディーラが必要な場合

- (1) 個人鍵の生成と配布: すべてのユーザは受信グループの対象になりうる. ディーラは, ユーザ (受信者) R_i に対して, その秘密鍵を s_i を生成して配布する.
- (2) グループ鍵の生成: ディーラは, 送信者が指定した受信グループ集合 G と復号閾値 m から, メッセージ暗号化のためのグループ鍵 s_G と補足情報 ϕ を生成アルゴリズム Ψ_s を使って生成し, 送信者に送付する.
- (3) メッセージの暗号化: 発信者はまず, セッション鍵 K を生成し, それをグループ鍵 s_G で暗号化し, 補足情報 ϕ とともにメッセージヘッダに加える. そしてメッセージ M をセッション鍵で暗号化する. マルチキャストする送信メッセージ c は, これらをつなげたものであり, $c = E_{s_G}(K) || \phi || E_K(M)$ となる. ここで $E_K(M)$ は, 秘密鍵 K によるメッセージ M の秘密鍵方式による暗号化とする.
- (4) メッセージの復号: 受信者は, メッセージ復号アルゴリズム Γ_s を用いて, 同一受信グループの他のメンバと協調することによってメッセージを復元する.

3.3.2 ディーラが不要な場合

ディーラを不要にするために公開鍵暗号系を用いる. ディーラの代わりに, 公開鍵を公開するためのディレクトリサーバが必要になる (図 2 参照).

- (1) 個人鍵の生成と配布: ユーザ (受信者) R_i は自分で秘密鍵 s_i を生成し, 公開鍵 $y_i = g^{s_i}$ をディレクトリサーバなどに公開する.
- (2) グループ鍵の生成: 送信者は, 送信したい受信

グループ集合 G_R に対応する公開鍵を、ディレクトリサーバなどから取得し、これと復号閾値 m を生成アルゴリズム Ψ_p に入力することによって、グループ公開鍵 y_G と補足情報 $\phi(x)$ を生成する。ここで、補足情報は、後のメッセージ暗号化のときの ElGamal 暗号の乱数 r に依存させる必要があるので、関数としている。

- (3) メッセージの暗号化：送信者はまず、乱数 r とセッション鍵 K を生成し、これを ElGamal 暗号 $ElG_{y_G}(K, r)$ によってグループ公開鍵で暗号化し、これと補足情報 $\phi(r)$ をメッセージヘッダとし、次にメッセージ M をセッション鍵で暗号化する。マルチキャストする送信メッセージ c は、これらをつなげたもので、 $c = ElG_{y_G}(K, r) || \phi(r) || E_K(M)$ となる。
- (4) メッセージの復号：受信者は、メッセージ復号アルゴリズム Γ_p を用いて、同一受信グループの他のメンバと協調することによってメッセージを復元する。

3.4 セキュリティ要件

上記モデルにおいて、秘密鍵型グループ鍵生成プロトコル Ψ_s 、秘密鍵型復号プロトコル Γ_s 、公開鍵型グループ鍵生成プロトコル Ψ_p 、公開鍵型復号プロトコル Γ_p は、以下のような要件を満たす必要がある。なお、秘密鍵型、公開鍵型に共通の特性については、 Ψ 、 Γ を用いる。

グループ鍵生成 (S1) Ψ で得られたグループ鍵は、指定された受信グループ G_R のすべての秘密鍵 (n 個) または、そのうちの m 個を補完する補足情報を用いなければ復元できない。

グループ鍵復号 (S2) Γ は、補足情報 ϕ を用いることによって、受信グループのメンバのうち m 人の秘密鍵を用いればグループ鍵を復元できる。

公開鍵型グループ鍵生成 (S3) Ψ_p は、受信グループのユーザの公開情報のみから構成できる。

公開鍵型グループ鍵復号 (S4) Γ_p では、受信グループのメンバはお互いに秘密鍵を交換しなくても、 Ψ_p で暗号化されたメッセージを復号できる。

4. 秘密鍵による動的グループ鍵構成法

4.1 プロトコル

4.1.1 グループ鍵生成アルゴリズム $\Psi_s(S_G, m)$

受信者グループ G_R に属する受信者の秘密鍵の集合 $S_G = \{s_{g_1}, \dots, s_{g_n}\}$ と復号閾値 m から、グループ秘密鍵 s_G と補足情報 ϕ を生成するアルゴリズム。

- (1) グループ鍵 s_G の生成法

ディーラは、まず次数 $n-1$ の多項式 $f(x)$ を、Lagrange の補間法を用いて以下のように構成する。

$$f(x) = \sum_{i \in G_{ID}} \lambda_i(x) s_i$$

$$\lambda_i(x) = \prod_{j \in G_{ID}, j \neq i} (x-j)(i-j)^{-1}$$

グループ鍵を次のように定める $s_G = f(0)$ 。

- (2) 補足情報 ϕ の生成法

ディーラは $n-m$ 個の点集合 $\Delta = \{\delta_1, \dots, \delta_{n-m}\}$ を、ユーザ ID と重ならないように選び、その点上での多項式の値 $s_{\delta_j} = f(\delta_j)$ を計算する。補足情報は以下のように、この仮想点と値のリストととなる。 $\phi = \{(\delta_1, s_{\delta_1}), \dots, (\delta_{n-m}, s_{\delta_{n-m}})\}$ 。

4.1.2 メッセージ復号アルゴリズム $\Gamma_s(c)$

グループ秘密鍵 s_G によって暗号化されたメッセージ $c = E_{s_G}(K) || \phi || E_K(M)$ から、平文 M を得るアルゴリズム。受信者グループ間のプロトコルによって行う。

- (1) グループ鍵の復元

受信グループのうち m 人の復号メンバが集まれば、その ID 集合 G'_{ID} と、その秘密鍵の集合 $S_M = \{s_{g'_1}, \dots, s_{g'_m}\}$ と、補足情報 ϕ から、Lagrange の補間法を用いて以下のようにして、 $n-1$ 次多項式 $f'(x)$ を一意に求めることができる。

$$f'(x) = \sum_{i \in G'_{ID} \cup \Delta} \lambda_i(x) s_i$$

$$\lambda_i(x) = \prod_{j \in G'_{ID} \cup \Delta, j \neq i} (x-j)(i-j)^{-1}$$

グループ鍵は $s_G = f'(0)$ によって復元される。

- (2) メッセージの復号

グループ鍵 s_G を用いて、セッション鍵 K が復号され、それによって、メッセージ M も復号される。

4.2 セキュリティの考察

上記のプロトコルでは以下を前提にしている。

- ディーラ-ユーザ間の秘密チャンネル：秘密鍵配布時のディーラとユーザ間の通信、およびグループ鍵配布時のディーラと発信者の間の通信は、秘密チャンネルを通して行われる。
- ユーザ-ユーザ間の秘密チャンネル：復号処理時のユーザ同士の通信は秘密チャンネルを通して行われる。

セキュリティの要件 S1, S2 については, $n - 1$ 次多項式が, n 個の点が与えられない限り不定であることから, 明らかである. ただし, この秘密鍵型では, 公開鍵型の要件 S3, S4 については成り立たない. なぜなら, グループ鍵はディールによって生成されるし, 復号時には, 受信者同士で秘密鍵の交換が必要なので, 秘密鍵は 1 回限りの使い捨てにする必要があるからである.

5. 公開鍵による動的動的グループ鍵構成法

5.1 プロトコル

5.1.1 グループ鍵生成アルゴリズム $\Psi_p(Y_G, m)$

受信者グループ G_R に属する受信者の公開鍵の集合 $Y_G = \{y_{g_1}, \dots, y_{g_n}\}$ と復号閾値 m から, グループ公開鍵 y_G と補足情報 $\phi(x)$ を生成するアルゴリズム.

(1) グループ公開鍵 y_G の生成法

送信者は, 以下のようにグループメンバの公開鍵を使ってグループ公開鍵 y_G を計算する.

$$y_G = \prod_{i \in G_{ID}} y_i^{\lambda_i(0)} \pmod{p}$$

$$\lambda_i(0) = \prod_{j \in G_{ID}, j \neq i} (-j)(i - j)^{-1} \pmod{q}$$

(2) 補足情報 $\phi(x)$ の生成法

次に $n - m$ 個の仮想点の集合 $\Delta = \{\delta_1, \dots, \delta_{n-m}\}$ を, ユーザ ID と重ならないように選び, その点上での公開鍵 y_{δ_k} ($k = 1, \dots, n - m$) を以下のように計算する.

$$y_{\delta_k} = \prod_{i \in G_{ID}} y_i^{\lambda_i(\delta_k)} \pmod{p}$$

$$\lambda_i(\delta_k) = \prod_{j \in G_{ID}, j \neq i} (\delta_k - j)(i - j)^{-1} \pmod{q}$$

補足情報は, 以下のように, この仮想点と, その仮想点上での公開鍵を, 変数 x でべき乗計算できるように関数化したもののリストとなる.

$$\phi(x) = \{(\delta_1, y_{\delta_1}^x), \dots, (\delta_{n-m}, y_{\delta_{n-m}}^x)\}.$$

5.1.2 メッセージ復号アルゴリズム $\Gamma_p(c)$

グループ公開鍵 y_G によって暗号化されたメッセージ $c = ElG_{y_G}(K, r) || \phi(r) || E_K(M)$ から, 平文 M を得るアルゴリズム. 受信者グループ間のプロトコルによって行う.

(1) セッション鍵の直接復元

グループ公開鍵 y_G に対応する秘密鍵 s_G は以下のように構成される.

$$s_G = \sum_{i \in G_{ID}} s_i^{\lambda_i(0)} \pmod{p}$$

$$\lambda_i(0) = \prod_{j \in G_{ID}, j \neq i} (-j)(i - j)^{-1} \pmod{q}$$

これを求めるには, 受信グループのメンバが, 秘密鍵を互いに交換する必要があり, そうすると秘密鍵の再利用ができなくなってしまう. しかし, 閾値暗号⁴⁾で提案された部分情報を用いることによって, 秘密鍵を直接交換しなくても, グループ公開鍵で Elgamal 暗号化されたセッション鍵 $ElG_{y_G}(K) = (g^r, Ky_G^r)$ を復号できる. ここで, 以下のように ElGamal 暗号の前半部を A , 後半部を B とする.

$$(A, B) = (g^r, Ky_G^r)$$

受信者グループのうち, m 人の復号メンバが A^{s_i} を計算して, メンバ間で共有することによって, 各自が補足情報 $\phi(r)$ を用いて, 次のように s_G を知ることなく, (A^{s_G}) を直接計算することができる. ここで, m 人の復号メンバの ID の集合を G'_{ID} とする. $|G'_{ID} \cup \Delta| = n$ である.

$$A^{s_G} = \prod_{i \in \Delta} y_i^{r\lambda_i(0)} \prod_{i \in G'_{ID}} A^{s_i\lambda_i(0)} \pmod{p}$$

$$\lambda_i(0) = \prod_{j \in G'_{ID} \cup \Delta, j \neq i} (-j)(i - j)^{-1} \pmod{q}$$

ここで, $y_G = g^{s_G}$ になっているので,

$$\frac{B}{A^{s_G}} = \frac{Ky_G^r}{(g^r)^{s_G}} = K \pmod{p}$$

となり, セッション鍵 K が復号できる.

(2) メッセージの復号

復元されたセッション鍵 K を用いて, メッセージ M も復号される.

5.2 セキュリティの考察

上記プロトコルでは以下を前提にしている.

- ユーザ-ユーザ間の秘密チャネル: 復号処理時のユーザ同士の通信は秘密チャネルを通して行われる.

本プロトコルでは, グループ公開鍵 y_G が, 受信グループのメンバの公開鍵 n 個から決定される $n - 1$ 次多項式 $Y(x)$ における定数項 $Y(0)$ を用いていて, これが, 受信グループのメンバの秘密鍵 n 個から決定される, $n - 1$ 次多項式 $f(x)$ によって決められるグループ秘密鍵 $s_G = f(0)$ との間で, 離散対数問題を構成していることを利用している.

ここから, セキュリティ要件のグループ鍵と補足情

報 S1, S2 については, $n-1$ 次多項式の補間には, n 個の点が与えられなければ不定であることから, また, 公開鍵グループ鍵と公開鍵復号 S3, S4 については, $y = g^x \pmod{p}$ の離散対数問題から, それぞれ満たされることが示される.

6. 応用例

6.1 コンテンツ配信システム

本システムを利用することによって, コンテンツ供給者, コンテンツ利用者ともに以下のような利点のあるコンテンツ配信が可能になる.

- コンテンツ供給者 (発信者): 発信者が, 任意のサブセットを受信グループとして定義でき, そのグループのメンバだけが, 復号化できるようなグループ暗号鍵が構成できる. 暗号鍵は, 受信者の公開鍵のみから構成できるので, TTP のような信頼機関は必要ない.
- コンテンツ利用者 (受信者): 受信者は, 自分で自分の秘密鍵を生成でき, その公開鍵を公開するだけで, 本コンテンツ配信システムの受信者となりうる. すなわち, ネットワークに接続さえすれば受信者になりうる.

このシステムを使った典型的なシナリオは以下のようになる.

- (1) コンテンツ供給者は, 自らの Web サイトを立ち上げ, 利用者を募る.
- (2) コンテンツ利用者は, コンテンツ供給者のサイトに登録する. このとき, 自分で秘密鍵を生成し, それに対応する公開鍵を, メンバリストに登録する. 料金の支払いなどもこのとき行う.
- (3) コンテンツ供給者は, メンバリストに登録された公開鍵に基づいて, グループ暗号鍵を生成し, コンテンツを暗号化して, マルチキャストする.
- (4) コンテンツ利用者は, メンバリストを参照しながら, 他のグループメンバと協力して, コンテンツを復号し利用する.

6.2 合議事項伝達システム

本システムでは, 受信グループのサイズを n としたとき, $1 \leq m \leq n$ で指定された閾値 m のメンバが集まらないと復号ができない. これを積極的に利用すると次のようなアプリケーションが考えられる. たとえば閾値を議決に必要な過半数 $m = n/2$ に設定して, 議題を送信すると, これを受信するために, $n/2$ 人以上が (ネットワーク上で) 集まらなければならない. このシステムを使った典型的なシナリオは以下のようになる.

- (1) 議決の要求者はまず, 会議のメンバあてのグループ鍵を作って, さらに閾値 m を議決定数に設定し, メッセージをグループ鍵で閾値暗号化して, マルチキャストする.
- (2) 会議のメンバが, このメッセージを復号するためには, 閾値 m 以上のメンバが集まる必要がある.
- (3) メッセージに対する返答が, 議決要求者に返送される. 議題が読めたということは, 議決定数の人間が集まったということであるから, その返事である議決も, 有効なものと見なすことができる.

6.3 サーバ訪問メータリングシステム

暗号メッセージを, 受信グループのメンバに送るのが通常の使い方であるが, 受信グループ以外の, ユーザに送ることを考える. すると, そのユーザは, グループ鍵を復号できる, 受信グループのメンバを訪問し, 閾値 m 個分の部分復号情報を集めることによって, メッセージが解読できるという応用が考えられる. これは, いくつのサーバを回ったかという, メータリングに使うことができる. 以下にこれを使ったビジネスモデルを示す.

- (1) 宣伝者は, ユーザに訪問してほしいサイトを受信グループにしてグループ鍵を構成し, チケット (または電子マネー) をその鍵で暗号化して送付する.
- (2) ユーザは, 受信グループに属するサイトを訪問するたびに, 部分復号情報をもろう. これが, 当初決められた閾値に達すると, チケットが解読でき, バリユーを得ることができる.

6.4 任意のグループに対する秘密分散システム

あるグループのグループ鍵で暗号化した秘密をグループのメンバに送信したということは, そのメンバが秘密を分散保管しているということになる.

- (1) 秘密保持者は, 秘密分散対象者の公開鍵からグループ鍵を作り, メッセージを暗号化して送付する. このとき, 閾値 m を, 秘密復元に必要な最低人数として設定する.
- (2) もし, 秘密の復元が必要になったときには, m 人の分散値保持者が集まることによって, 復元ができる.

7. 類似システムとの比較

グループ鍵配送問題としては, 本論文の公開鍵による構成や, Broadcast Encryption⁵⁾などが対象としているように, 任意のサブセットに対して, そのグループ暗号鍵を生成することを問題にしたものと, 目的は異なるが, 閾値型 ElGamal 暗号が用いられていて, 構成法が本論文のものと類似しているものがある. そこ

表 1 グループ鍵暗号システムの比較
Table 1 Comparison of group key cryptosystems.

	[NW03]	[FN94]	[Ped91]	[GPS96]	[KD98]	[AMM99]
秘密鍵生成	ユーザ	TTP	ユーザ	ユーザ	TTP	TTP
グループ指定	送信者	TTP	固定	送信者	送信者	送信者
協調復号	(m,n) 閾値 m, n 可変	-	(m,n) 閾値 m, n 固定	(m,n) 閾値 m, n 可変	-	-
結託閾値	-	k	-	-	k	k
秘密鍵量	1	$k \log k \log n$	1	1	1	1
送信メッセージ量	$1 + k'$ $k' = n - m$	$k^2 \log^2 k \log n$	1	n	k	k
復号メッセージ量	m^2	-	m^2	m^2	-	-

で、それらのシステムとの比較をする。

まず、受信グループが協力することによって復号を可能にしたグループ鍵暗号システムを Pedersen が提案している⁸⁾、これは本論文の公開鍵型システムと同様に、ディールを使わずに鍵生成ができ、また、復号閾値をいれることもできる。本システムとの違いは、受信グループと閾値が固定されていることである。これは、ユーザが自分の秘密鍵に対するシェアを、固定された閾値によって計算しておき、これを、あらかじめ他のユーザに分配しておくことが必要なため、本システムが目的とするような、任意の情報発信者が、それぞれ受信グループと閾値を決められるというモデルには適していない。

次に、Ghodosi らは、RSA をベースにした動的閾値暗号系⁶⁾を提案しており、これは、送信者が動的に受信グループや復号閾値を指定できることを要件としていて、本論文のモデルに非常に近い。しかし、送信メッセージのサイズが、受信グループの人数に比例して大きくなるので、受信グループサイズが大きな P2P 鍵配信には向かない。この方式の特徴は、Information Dispersal⁹⁾のように、受信グループの人数に応じて暗号化できるメッセージ自身のサイズも大きくできるので、暗号化したいメッセージが長い場合には有効であるが、本論文のように、セッション鍵を配信するような場合には、メッセージ長が受信グループのサイズには依存しない方が望ましい。

また、目的は異なるが、 k 人の不正者の結託に対して耐性のある鍵配送システムとして Kurosawa らが提案している不正者追跡 (traitor tracing) システム⁷⁾ や、Anzai らが提案している k 人までのメンバを排除できる鍵更新システム¹⁾がある。これらは、いずれも第三者信頼期間 (TTP) があらかじめ個人鍵を発行しておいたうえで、鍵更新者が、セッション鍵をメッセージとしてマルチキャストするというモデルなので、本論文のように、自由に入出力できるユーザ全体集合

に対して複数の情報発信者が任意のサブセットを受信グループに選んでマルチキャストできるというモデルとは用途が異なっている。

表 1 に各システムとの比較を示す。表中で、[NW03] は本論文の公開鍵による構成、[FN94] は Fiat らによる Broadcast Encryption⁵⁾、[Ped91] は Pedersen によるグループ暗号⁸⁾、[GPS96] は Ghodosi らによる動的閾値暗号系⁶⁾、[KD98] は Kurosawa らの不正者追跡システム⁷⁾、[AMM99] は Anzai らの鍵更新システム¹⁾を、それぞれ示す。評価項目としては、2章で定義された P2P 環境下での要件から、(1) 秘密鍵生成をユーザが TTP を使わずにできるか、(2) グループ指定を送信者が動的にできるか、(3) 協調復号ができるか、(4) 結託閾値が存在するかについての 4 項目と、定量的な評価として、(5) ユーザが管理しなければいけない秘密鍵の量、(6) 送信メッセージサイズ、および、(7) 復号処理のときにユーザ間で交換しなければならないメッセージ総量の 3 項目について比較してある。表から、送信者が動的に受信グループと閾値を選べ、送信メッセージサイズが受信グループに依存しないのは、本論文が提案する方法だけであることが分かる。ここで、 $k' = n - m$ は、受信グループのメンバであるにもかかわらず復号処理をしない欠席者の人数であり、送信メッセージサイズは、この欠席者の人数だけに依存する。

ここから、欠席者が受信グループのサイズに対して小さいときに有効な方法であることが分かる。

8. おわりに

本論文では、インターネットに常時接続された計算機のように、多数のホストの接続が動的に変化し、ユーザの全体集合や受信グループを、あらかじめ指定できないような条件下での、P2P マルチキャスト通信を目的にしたグループ鍵構成法を提案した。任意のホスト間の直接通信が容易だという P2P の環境下では、ホ

ストどうしの結託も容易であるため、従来のクライアント・サーバ型のモデルを前提にした、受信者の結託閾値に基づいたグループ鍵暗号法では、問題が生じることが考えられる。本論文で示した構成法では、任意の送信者が、公開情報のみを使って、動的に受信グループや閾値を設定でき、その鍵サイズは、受信グループのサイズには依存しない。また、受信グループ以外のユーザの結託に対して耐性がある代わりに、復号処理のためにグループ内の受信者同士の通信が必要になる。これを逆に利用した、新しいアプリケーションについてもビジネスモデルとともに提案した。

参 考 文 献

- 1) Anzai, J., Matsuzaki, N. and Matsumoto, T.: A Quick Group Key Distribution Scheme with Entity Revocation, *ASIACRYPT'99*, LNCS (1999).
- 2) Berjivutsm, S.: How to Broadcast a Secret, *EUROCRYPT'91*, LNCS (1991).
- 3) Crowcroft, J. and Pratt, I.: Peer to Peer: Peering into the Future, *Advanced Lectures on Networking, NETWORKING 2002*, LNCS (2002).
- 4) Desmedt, Y. and Frankel, Y.: Threshold Cryptosystems, *CRYPTO'89*, LNCS (1990).
- 5) Fiat, A. and Naor, M.: Broadcast Encryption, *CRYPTO'93*, LNCS (1994).
- 6) Ghodosi, H., Pieprzyk, J. and Safavi-Naini, R.: Dynamic Threshold Cryptosystems: A New Scheme in Group Oriented Cryptography, *PRAGOCRYPTO '96* (1996).
- 7) Kurosawa, K. and Desmedt, Y.: Optimum Traitor Tracing and Asymmetric Scheme, *EUROCRYPT'98*, LNCS (1998).
- 8) Pedersen, T.: A Threshold Cryptosystem without a Trusted Party, *EUROCRYPT'91*, LNCS (1991).
- 9) Rabin, M.: Efficient dispersal of information for security, load balancing, and fault tolerance, *J. ACM*, Vol.36, No.2, ACM (1989).
- 10) Host Extensions for IP Multicasting. <ftp://ftp.isi.edu/in-notes/rfc1112.txt>
- 11) Internet Group Management Protocol, Ver. 2. <ftp://ftp.isi.edu/in-notes/rfc2236.txt>
- 12) 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).
- 13) 山内長承, 石川憲洋, 高橋 修: IP マルチキャストの配送制御とそのセキュリティへの応用, *情報処理学会論文誌*, Vol.41, No.1 (2001).

(平成 15 年 5 月 12 日受付)

(平成 15 年 12 月 2 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・ピー・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。



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修士課程修了。同年日本アイ・ピー・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。