グループ鍵生成プロトコルに関する一考察*

1H－05

陳　志松†　山本雅基†　矢尻えみ子††　石田　亨†††　神保雅一††
†(株)デンソークリエイト　††慶応義塾大学理工学部数理科学科　†††情報科学芸術大学院大学

1. はじめに

グループ鍵生成プロトコルは、グループに属する複数のピアが情報を秘密に交換するための共通鍵を、安全ではない通信回路を使って安全に生成するために使われる。

グループ鍵を生成するには、鍵共有(Key Contribution あるいは Key Agreement) と鍵配送(Key Distribution)の二通りの方法がある。鍵共有とは、ピア全員が自分の秘密鍵をもとに加工したデータを公開し、これらの公開データを使って各々のピアが共通鍵を生成する方法。一方、鍵配送とは、グループ内特定のピアが共通鍵を作り、その鍵を安全に各々のピアに配る方法。鍵共有は、さらにIKA(Initial Key Agreement)とAKA(Auxiliary Key Agreement)の二つに分けることができる。IKAとは、グループを最初に形成するときに使われるプロトコルである。これに対して、AKAとは、すでに存在しているグループに、ピアの追加や削除、または鍵の更新といった操作を行うときに使われるプロトコルである。

本発表では、従来の鍵共有IKAプロトコルを考察し、より効率よくするために改良と修正を加えたプロトコルを提案する。

2. 従来の鍵共有IKAプロトコル

2ピア間の鍵共有方法として、Diffie-Hellman鍵共有プロトコルがある。近年、Diffie-Hellman鍵共有プロトコルに基いたいろんな形で複数ピア間に拡張するプロトコルが数多く提案されている。

本章ではこれらの拡張から二つの代表的なプロトコル[1][2]を紹介する。私たちがこの二つのプロトコルを考察し、改良と修正を試みた。

本発表で使う記法を以下でまとめて示す：

N	：	グループに属するピアの数
i,j,m	：	ピアの順番を示す添え字
P	：	ピア、Piはi番目のピア
q	：	素数
α	：	GF(q)の原始元
N	：	秘密鍵、Niはi番目のピアの秘密鍵
Z,X,Y	：	公開データ
K	：	共通鍵

2.1 IKA.1 プロトコル

IKA.1[2]は、Steinerらによって考案された鍵共有IKAプロトコルである、Diffie-Hellmanプロトコルの"自然"拡張という。IKA.1の手順を以下に示す:

(1)　1～n-1番目のピアにおいて、P_iがN_iを選び、P_{i+1}に以下の公開データをユニキャストする[1]：

$$Z_i:\ \{\alpha^{N_1\Lambda N_i/N_j} \mid j\in[1,i]\},\alpha^{N_1\Lambda N_i}$$

(2)　n番目のピアP_nがN_nを選び、ピア全員に以下の公開データをブロードキャストする：

$$\{Y_i\}:\ \{\alpha^{N_1\Lambda N_n/N_i} \mid i\in[1,n]\}$$

(3)　i番目のピアP_iが共通鍵$Y_i^{N_i}$を生成する。

生成される共通鍵は：$K=\alpha^{N_1N_2\Lambda N_n}$である。

2.2 Burmester - Desmedt プロトコル

Burmester - Desmedtプロトコル[1](以下、B-Dプロトコルと呼ぶ)は、Diffie-Hellmanプロトコルを拡張し、$K=\alpha^{N_1N_2+\Lambda+N_{n-1}N_n+N_nN_1}$のような共通鍵を効率よく生成する方法として知られている。B-Dプロトコルの手順を以下に示す：

(1) ピア全員がそれぞれNiを選び、$Z_i=\alpha^{N_i}$を全員にブロードキャストする[2]。

---

* Study about Group Key Generation Protocol.
†Zhisong Chen, †Masaki Yamamoto, ††Emiko Yajiri, †††Akira Ishida, ††Masakazu Jimbo
†Denso Create Inc., ††Faculty of Science and Technology, Keio University, †††Institute of Advanced Media Arts and Sciences

[1] 公開データは法qでモジュロを取る、以下同様。
[2] 添え字は法nでモジュロを取る、以下同様。

(2) ピア全員がそれぞれ $X_i = \left(\frac{Z_{i+1}}{Z_{i-1}}\right)^{N_i}$ を全員にブロードキャストする。

(3) i番目のピア P_i が共通鍵を生成する：

$$K = (Z_{i-1}^{N_i})^n X_i^{n-1} X_{i+1}^{n-2} \Lambda\ X_{i-2}$$

以上のように、B-D プロトコルは2回のブロードキャストで、鍵共有ができる。

3. 従来プロトコルの改良と修正

IKA.1 と B-D プロトコルは、Diffie-Hellman 法を拡張し、鍵共有の有効な方法を提供した。しかし、以下の点において、不満が残る：

(a) IKA.1 は鍵共有でのピアごとの計算量が均等ではない、大きい順番ほど負担が大きい。

(b) B-D プロトコルは IKA として優れているが、鍵の形により AKA に適していない[2]。

本発表では上記の不満を解消する改良 IKA.1 プロトコルと修正 B-D プロトコルを提案する。

3.1 改良 IKA.1 プロトコル

説明を簡潔にするため、ピアの数 n が 2^k と仮定する[3]。グループを均等に2つのサブグループに分け、サブグループにおいて同じ過程を繰り返し、最終のサブグループのピア数が 1 となるまで繰り返す。図1のように、サブグループからピアのツリーを構成し、矢印方向に、ピア P_i が上位のピア P_{i-1} から公開データ Z_{i-1} を受け取り、下位のピアに $Z_i=(Z_{i-1})^{N_i}$ をユニキャストする。

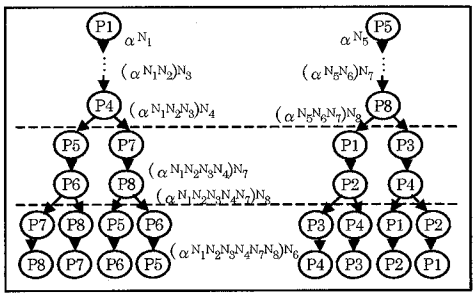

図1　改良 IKA.1 プロトコル（k=3 の場合）

改良 IKA.1 プロトコルは、IKA.1 と比べ、ピアごとの計算量均等でない問題を解消し、全体のべき乗計算量も $O(n^2)$ から $O(n\log n)$ に減少した。

3.2 修正 B-D プロトコル

q'=2q+1 が素数で、α を GF(q')の原始根とする。以下に修正 B-D プロトコルを示す：

(1) ピア全員がそれぞれ q と互いに素である奇数の Ni を選び、$Z_i = \alpha^{N_i}$ を全員にブロードキャストする。

(2) ピア全員がそれぞれ $X_i = \left(\frac{Z_{i+1}}{Z_{i-1}}\right)^{N_i}$ を全員にブロードキャストする。

(3) ピア全員がそれぞれ以下を全員にブロードキャストする：

$$Y_i = (Z_{i-1})^n (X_i^{n-1} X_{i+1}^{n-2} \Lambda\ X_{i-2})^{N_i^{-1}}$$

(4) i 番目のピア P_i が共通鍵 $K = Y_i^{N_i}$ を生成する。

ここで、Y_i は以下の形をしていることに注意して欲しい：

$$Y_i = \left(\alpha^{N_1 N_2 + \Lambda + N_n N_1}\right)^{N_i^{-1}}$$

これにより、Y_i の形は IKA.1 と異なるが、Steiner らの提案した AKA プロトコル[2]に容易に適用できる。

4. 今後の課題

今回は鍵共有 IKA プロトコルに絞って、検討を行った。これをスタートとして、今後は AKA プロトコルに検討対象を広げ、より効率的な方法を考えていきたい。さらに、認証付きのグループ鍵の生成プロトコルにも検討を行い、実用レベルまで完成し、これらのプロトコルを適用したアプリケーションを開発したい。

参考文献

[1] M. Burmester and Y. Desmedt, A secure and effcient conference key distribution system, in Advances in Cryptology EUROCRYPT '94, 1994.

[2] M. Steiner, G. Tsudik, and M. Waidner, Key agreement in dynamic peer groups, IEEE Transactions on Parallel and Distributed Systems, 11(08), August 2000.

3 ピアの数 n が 2^k でないとき、$2^{k-1}<n<=2^k$ なる k を用いる、存在しない人の秘密鍵 Nm(m=n+1,…,2^k)を 1 とすればよい。