グループにおける情報理論的に安全な相手認証方式

一 将吾　　渡邉 洋平　　四方 順司

横浜国立大学大学院環境情報学府/研究院
240-8501 神奈川県横浜市保土ケ谷区常盤台 79-7
{hajime-shogo-vm, watanabe-yohei-xs, shikata}@ynu.ac.jp

あらまし 本稿では、情報理論的安全性に基づき，通信相手の正当性を確認できる相手認証方式に関して対称鍵を用いて提案する．具体的には, 黒澤による 2 者間の相手認証を n 人のユーザグループ内の任意の 2 者間の相手認証に拡張する．この相手認証方式に対して, その数理モデル，安全性の定式化を与え，秘密鍵長及びレスポンス長のタイトな下界, 最適な構成法を示す.

Unconditionally Secure Entity Authentication in a Group

Shogo Hajime　　Yohei Watanabe　　Junji Shikata

Graduate School of Environment and Information Sciences,
Yokohama National University,
79-7,Tokiwadai,Hodogaya,Yokohama,Kanagawa 240-8501,Japan
{hajime-shogo-vm, watanabe-yohei-xs, shikata}@ynu.ac.jp[1ex]

Abstract In this paper, we study unconditionally secure entity authentication in a group by use of symmetric-keys. Specifically, we extend Kurosawa's result of unconditionally secure entity authentication protocols between two users to the one in which any two users in an n-user group can execute entity authentication. For the protocols, we formalize a model and a security definition. Also, we derive tight lower bounds on sizes of secret-keys and responses. Furthermore, we propose an optimal direct construction of the protocols.

1 はじめに

これまでに多くの暗号技術が提案されているが, それらの安全性は主に計算量的安全性あるいは情報理論的安全性に基づいて保証されている．計算量的安全性は素因数分解問題や離散対数問題などの計算量的な問題を解くことが難しいという仮定に基づいて安全性を保証し，情報理論的安全性は計算量的な仮定を用いずに確率論や情報理論に基づいてその安全性を保証する．情報理論的安全性に基づく暗号技術は計算量的安全性に基づく暗号技術に比べて一般的に必要な記憶容量が多く，また全てのエンティティが自身の鍵を秘密に保持する必要がある．しかし計算量的な仮定を用いないために攻撃者の計算能力に関わらず定量的なセキュリティを長期間保証できるという利点がある．計算機の計算能力の向上やアルゴリズムの進歩を考えると，情報理論的安全性に基づく暗号技術の有用性が増すことが期待され，これらについて議論する意義は大きい.

相手認証技術は通信相手の正当性を保証するための技術である．相手認証技術に関して，これまでに多くの論文が発表されているが，その殆どは計算量的安全性に基づくもの（例えば, [1, 2] 等）で，情報理論的安全性に基づく論文

はごく僅かである [3, 4].

本稿では，情報理論的安全性に基づいて, グループにおける安全な相手認証方式を提案する. 具体的には，数理モデル，安全性の定式化を与え，鍵サイズのタイトな下界, 最適な構成法を示す．また，本方式は [3] の論文にある 2 者間モデルを n 人のユーザグループに拡張したものとなっている.

2 モデル

本方式は，n 人の中の任意の二者間で相手認証を行うプロトコルである．相手認証方式では，ユーザの役割として，自身の正当性を証明する役割（その役割のユーザを証明者と呼ぶ），また相手の正当性を検証する役割（その役割のユーザを検証者と呼ぶ）の 2 つの役割があり，本方式では各ユーザがどちらの役割にもなることができる（これを役割任意という）．また，相手認証方式には，片側認証方式（二者間で一方のユーザがもう一方のユーザを認証する）と相互認証方式（二者間でお互いを認証する）があるが，本方式は片側認証方式となっている.

また，本方式では TA モデルを考える．TA モデルとは，信頼できる第三者機関の存在を仮定するモデルである．TA はプロトコルの開始時のみ起動し，各エンティティに鍵などの情報を配送し，その後は登場しないエンティティである．提案するモデルでは，TA と n 人の利用者 $U_1, U_2, \ldots, U_n$(以下，ID の集合を同一視する) が登場する.

まずモデルの概要を述べる．プロトコルの開始時に TA は各ユーザの秘密鍵を生成し，それを安全な通信路を用いて各ユーザに配送した後, 自身のメモリから削除する．これ以降 TA は登場しない．次に，検証者 U_j はチャレンジを生成し，証明者 U_i に送信する．U_i はチャレンジに対して自身の秘密鍵を用いてレスポンスを生成，U_j に送信する．最後に，U_j は自身の秘密鍵とチャレンジ，レスポンスから相手の正当性を検証する．形式的な定義は次の通りである.

定義 1. n 人のユーザグループによる役割任意の片側認証方式 Π は，以下に示す $n+1$ のエンティティ，4 つのアルゴリズムからなる.

記法

- 信頼機関 TA
- n 人のユーザ (ID 情報), $U_1, U_2, \ldots, U_n$
- ユーザ ID の集合 $U = \{U_1, \ldots, U_n\}$
- 各ユーザ U_i の鍵情報 K_i $(i = 1, \ldots, n)$
- 鍵生成アルゴリズム $Gen()$: 確率的アルゴリズムであり，セキュリティパラメータ 1^k を入力値としてとり，各ユーザの鍵 K_i $(1 \leq i \leq n)$ を出力する.
- チャレンジ生成アルゴリズム $Challenge$: 確率的アルゴリズムであり、各ユーザの ID を入力値としてとり，ランダムなチャレンジ値を出力する.
- レスポンス生成アルゴリズム $Response$: 確定的アルゴリズムであり，受信情報（相手からのチャレンジ値を含む）と自身の鍵 K_i を入力としてとり、レスポンス値を出力する.
- レスポンス検証アルゴリズム $Verify$: 確定的アルゴリズムであり，受信情報（相手からのレスポンス値を含む），送信情報（自身のチャレンジ値を含む）と自身の鍵 K_j を入力としてとり，2 値 (0 or 1) を出力する.

1. 鍵生成・配布
   TA はセキュリティパラメータと鍵生成アルゴリズム Gen を用いて鍵 K_i を生成し, 各ユーザ U_i に鍵 K_i を安全な通信路を用いて配送する．また各ユーザは ID 情報 U_i を公開する.
2. チャレンジ生成
   検証者 U_j はチャレンジ生成アルゴリズム $Challenge$ を用いてチャレンジ X を生成し, M_1= (U_j, U_i, X) を証明者 U_i へ送る.
3. レスポンス生成
   証明者 U_i は M_1 を受け取ると, M_1 と K_i をレスポンス生成アルゴリズム $Response$ に入力することでレスポンス Y を生成し, M_2= (U_i, U_j, X, Y) を検証者 U_j へ送る.
4. レスポンス検証
   検証者 U_j は M_2= (U_i, U_j, X', Y') を受信すると，M_1, M_2, K_j から、レスポンス検証

アルゴリズム *Verify* を用いて検証を行う．*Verify* は認証成功を意味する 1，または認証失敗を意味する 0 を出力する．

3 安全性定義

本節では，本方式の安全性について述べる．まず，システム全体で検証者が生成する M_1 の生成回数及び証明者が生成する M_2 の生成回数をそれぞれ t 回とする．次に，W を n 人のユーザグループ内の最大 ω 人 ($\leq n-2$) の結託者の集合とする．攻撃者 W は次の 2 つの行動をするものとし，攻撃者 W は $U_i(\notin W)$ になりすまして $U_j(\notin W)$ の認証に成功することを目的とする．ただし，攻撃者 W はユーザ間でやり取りされる情報をそのまま受け流す攻撃はしないものとする．また (U_i,U_j) 間で複数回の認証が行われる場合では相手に送信するチャレンジ X はすべて異なるとする．

以上を踏まえ，次のような攻撃モデルを考える．W は U_i になりすましたいので，U_i の持っている秘密情報を少しでも得ようとする攻撃を考える．具体的には，W が U_i に対して検証者としてチャレンジを投げ，それに対するレスポンスを得る攻撃である[1]．M_1, M_2 の生成回数がそれぞれ t 回のため，最大 $t-1$ 回までこの攻撃を行うものとする．その後，得られた情報を用いて，U_j に対して U_i としてなりすまそうとする攻撃を試みる．

定義 2. n 人のユーザグループによる役割任意の片側認証方式 Π は，条件 $P \leq \epsilon$ を満たすとき，(ϵ, t, ω, n)-*secure* であるという．P は以下のように定義される: まず，攻撃を以下のように定義する．

(1) $Session(t_1)$：攻撃者 W が $U_i \notin W$ に対して検証者として認証を行う．このとき任意のチャレンジに対するレスポンスを高々 t_1 個入手する事象.

(2) $Cheat$：攻撃者 W が $U_j(\notin W)$ に対して U_i になりすまして証明者として認証を行う．このときの認証が成功する事象.

ただし M_1,M_2 の生成回数がそれぞれ高々 t 回と制限されているので，$t_1 \leq t-1$ である．このとき攻撃者 W の攻撃成功確率 P を以下のように定義する．

$$P := \max \Pr(Cheat \mid Session(t_1)).$$

ここでの max は，可能なすべての $Session(t_1)$ を考え，$Cheat$ の成功確率が最大となるものをとる．

4 下界

本節では，n 人のユーザグループにおける役割任意の片側認証方式の攻撃成功確率，ユーザ U_i の秘密鍵の鍵長，レスポンス長のタイトな下界について示す．以降，Y_i^t は t 回目の認証において証明者であるユーザ U_i が自身の秘密鍵 K_i を用いてレスポンス生成アルゴリズムから生成したレスポンスの値をとる確率変数，X_j^t は t 回目の認証において検証者であるユーザ U_j が選んだチャレンジの値をとる確率変数とする．

定理 1. 任意の (ϵ, t, ω, n)-secure 片側認証方式 Π に対して，なりすまし攻撃の成功確率 P は以下の不等式をみたす．W $(0 \leq |W| \leq \omega)$ を任意の結託集合, 任意の $U_i, U_j \notin W$, 任意の非負整数 s $(0 \leq s \leq t)$ に対して,

$$P \geq 2^{-I(Y_i^s; K_j | K_W, Y_i^1, \ldots, Y_i^{s-1}, X_j^1, \ldots, X_j^s)}.$$

証明. これが成り立つことは [5] の定理 3.1 の証明と同様の流れで証明できる． □

次に各ユーザの秘密鍵の鍵長 $\log|K_j|$ [bits], レスポンス長 $\log|Y_i^t|$ [bits] の下界を示す.

定理 2. 任意の (ϵ, t, ω, n)-secure 片側認証方式 Πに対して，以下の不等式が成り立つ.

$$\begin{aligned} \log|K_j| &\geq t(\omega+1)\log\epsilon^{-1}, \\ \log|Y_i^t| &\geq \log\epsilon^{-1}. \end{aligned}$$

[1] W が U_i に対して証明者としてなりすますことは考えない．なぜなら，その結果得られる情報は U_i がランダムに選んだチャレンジのみだからである.

証明. まず、2つ目の不等式から示す．定理1より，$H(Y_i^t) \geq \log \epsilon^{-1}$．したがって，$\log |Y_i^t| \geq \log \epsilon^{-1}$.

次に1つ目の不等式を示す.

$$\begin{aligned} H(K_j) &\geq I(K_1...K_{\omega+1}; K_j | X_j^1...X_j^t) \\ &= H(K_1...K_{\omega+1}|X_j^1...X_j^t) \\ &\quad -H(K_1...K_{\omega+1}|K_jX_j^1...X_j^t) \quad (1) \end{aligned}$$

ここで，まず以下の不等式を得る．

$$\begin{aligned} &H(K_1...K_{\omega+1}|X_j^1...X_j^t) \\ &= \sum_{s=1}^{\omega+1} H(K_s|K_1...K_{s-1}X_j^1...X_j^t) \\ &= \sum_{s=1}^{\omega+1} \{I(Y_s^1...Y_s^t; K_s|K_1...K_{s-1}X_j^1...X_j^t) \\ &\quad +H(K_s|Y_s^1...Y_s^tK_1...K_{s-1}X_j^1...X_j^t)\} \\ &\geq \sum_{s=1}^{\omega+1} \{H(Y_s^1...Y_s^t|K_1...K_{s-1}X_j^1...X_j^t) \\ &\quad -H(Y_s^1...Y_s^t|K_sK_1...K_{s-1}X_j^1...X_j^t) \\ &\quad +H(K_s|Y_s^1...Y_s^tK_1...K_{s-1}K_jX_j^1...X_j^t)\} \\ &= \sum_{s=1}^{\omega+1} \{H(Y_s^1...Y_s^t|K_1...K_{s-1}X_j^1...X_j^t) \\ &\quad +H(K_s|Y_s^1...Y_s^tK_1...K_{s-1}K_jX_j^1...X_j^t)\} \\ &= \sum_{r=1}^{t}\sum_{s=1}^{\omega+1} H(Y_s^r|K_1...K_{s-1}X_j^1...X_j^tY_s^1...Y_s^{r-1}) \\ &\quad + \sum_{s=1}^{\omega+1} H(K_s|Y_s^1...Y_s^tK_1...K_{s-1}K_jX_j^1...X_j^t). \end{aligned}$$

一方，以下の等式を得る．

$$\begin{aligned} &H(K_1...K_{\omega+1}|K_jX_j^1...X_j^t) \\ &= \sum_{s=1}^{\omega+1} H(K_s|K_jK_1...K_{s-1}X_j^1...X_j^t) \\ &= \sum_{s=1}^{\omega+1} \{I(Y_s^1...Y_s^t; K_s|K_1...K_{s-1}K_jX_j^1...X_j^t) \\ &\quad +H(K_s|Y_s^1...Y_s^tK_1...K_{s-1}K_jX_j^1...X_j^t)\} \\ &= \sum_{s=1}^{\omega+1} \{H(Y_s^1...Y_s^t|K_1...K_{s-1}K_jX_j^1...X_j^t) \\ &\quad -H(Y_s^1...Y_s^t|K_sK_1...K_{s-1}K_jX_j^1...X_j^t) \\ &\quad +H(K_s|Y_s^1...Y_s^tK_1...K_{s-1}K_jX_j^1...X_j^t)\} \\ &= \sum_{s=1}^{\omega+1} \{H(Y_s^1...Y_s^t|K_1...K_{s-1}K_jX_j^1...X_j^t) \\ &\quad +H(K_s|Y_s^1...Y_s^tK_1...K_{s-1}K_jX_j^1...X_j^t)\} \\ &= \sum_{r=1}^{t}\sum_{s=1}^{\omega+1} H(Y_s^r|K_1...K_{s-1}K_jX_j^1...X_j^tY_s^1...Y_s^{r-1}) \\ &\quad + \sum_{s=1}^{\omega+1} H(K_s|Y_s^1...Y_s^tK_1...K_{s-1}K_jX_j^1...X_j^t). \end{aligned}$$

よって, (1) は

$$\begin{aligned} &\sum_{r=1}^{t}\sum_{s=1}^{\omega+1} H(Y_s^r|K_1...K_{s-1}X_j^1...X_j^tY_s^1...Y_s^{r-1}) \\ &+\sum_{s=1}^{\omega+1} H(K_s|Y_s^1...Y_s^tK_1...K_{s-1}K_jX_j^1...X_j^t) \\ &-\sum_{r=1}^{t}\sum_{s=1}^{\omega+1} H(Y_s^r|K_1...K_{s-1}K_jX_j^1...X_j^tY_s^1...Y_s^{r-1}) \\ &-\sum_{s=1}^{\omega+1} H(K_s|Y_s^1...Y_s^tK_1...K_{s-1}K_jX_j^1...X_j^t) \\ &= \sum_{r=1}^{t}\sum_{s=1}^{\omega+1} I(Y_s^r; K_j|K_1...K_{s-1}X_j^1...X_j^tY_s^1...Y_s^{r-1}) \\ &\geq t(\omega+1)\log \epsilon^{-1}. \end{aligned}$$

ここで, 最後の不等式は定理1より従う． □

実は，5節で示す片側認証方式の構成法は，定理2の等号成立の場合である．したがって導出した鍵の下界はタイトである．ここで，下界の等号が成り立つような構成法を以下のように特徴づける．

定義 3. (ϵ, t, ω, n)-*secure* 片側認証方式 Π の構成法が定理 2 の等号をすべて満たすとき，この構成法は最適であるという．

5 構成法

本節では 3 節の安全性を満たす片側認証方式の構成法を以下に示す．ただし，以下では F_q を q 個の要素からなる有限体とする．またこの構成法が最適であることも示す．

鍵生成・配布: TA は，以下のような F_q 上のランダムな 3 変数多項式を生成する．

$$f(x,y,z) = \sum_{h=0}^{\omega}\sum_{i=0}^{\omega}\sum_{j=0}^{t-1} a_{hij}x^h y^i z^j,$$
$$a_{hij} \in F_q \text{ かつ } a_{hij} = a_{ihj} \text{ for } \forall h,i,j.$$

また，各ユーザ ID に関して適切な符号化により $U_i \in F_q$ とする．各ユーザ U_i の秘密鍵 K_i は，$K_i := f(U_i, y, z)$ とし，各 K_i は安全な通信路を用いて U_i に配送される．

チャレンジ生成アルゴリズム $Challenge$: U_j から U_i へのチャレンジ生成では，ランダムな $X = m(\in F_q)$ が選ばれる．そして，$M_1 := (U_j, U_i, X)$ が検証者 U_j から証明者 U_i へ送られる．

レスポンス生成 $Response$: U_j から送られてきた $M_1 = (U_j, U_i, X)$ $(X = m)$，U_i の秘密鍵 $K_i = f(U_i, y, z)$ を入力として，U_i のレスポンス $Y = f(U_i, y, z)|_{y=U_j, z=m}$ を出力する．このとき，$M_2 := (U_i, U_j, X, Y)$ が U_i から U_j へ送られる．

レスポンス検証 $Verify$: 証明者 U_i から送られてきた情報 $M_2 = (U_i, U_j, X', Y')$，検証者 U_j の秘密鍵 $f(U_j, y, z)$，既に生成したチャレンジ $X(= m)$ を入力値としてとり，$X' = X$ かつ $Y' = f(U_j, y, z)|_{y=U_i, z=m}$ のときに限り 1 を出力し，そうでないときは 0 を出力する．

定理 3. 上記の構成による片側認証方式 Π は，(ϵ, t, ω, n)-secure であり，最適な構成法である．ただし，$\epsilon = \frac{1}{q}$.

証明. 攻撃者 W が証明者 $U_i(\notin W)$ になりすまして検証者 $U_j(\notin W)$ の認証に成功する確率を考える．攻撃者 W による攻撃が成功するというのは，t 回目の認証において検証者 U_j が生成した $M_1 = (U_j, U_i, X_j^t)$ に対応して，最終的に受理する $M_2 = (U_i, U_j, X_j^t, Y_i^t)$ を生成することである．

攻撃者 W が $Session(t-1)$ で集めた M_2 の集合 B を以下のように表す．

$$B = \{(U_i, U_j, X_j^k, Y_i^k)\}(1 \le k \le t-1).$$

$Session(t-1)$ によって M_2 を $t-1$ 個所持しているが，その中には X_j^t は存在しない．また多項式 $f(x,y,z)$ の変数 x, y, z に関する次数はそれぞれ ω，ω，$t-1$ であり U_i, U_j 以外の ω 人が結託し，ω 個の鍵を集め，M_2 を $t-1$ 個集めたとしても K_i, K_j に関する情報も Y_i^t に関する情報も得ることができない．よって攻撃者 W は Y_i^t の部分にランダムな値 $R \in F_q$ を入れて $M_2 = (U_i, U_j, X_j^t, R)$ を生成するよりも高い成功確率で生成することはできない．よって攻撃者 W が U_j による 1 回の認証に対して，認証成功となる確率は

$$Pr(\text{ 認証成功 } (R = Y_i^t)) = \tfrac{1}{q}.$$

以上より, $\epsilon := \frac{1}{q}$ として, 本構成法が (ϵ, t, ω, n)-secure であることが示せた．

次に本構成法における鍵長，レスポンス長は以下のようになる．

$$\log|K_j| = t(\omega+1)\log q \text{ [bits]}$$
$$\log|Y_i^t| = \log q \text{ [bits]}$$

したがって, 本稿で提案した構成法は定理 2 の鍵長，レスポンス長の下界の等号を満たすため，最適な構成法である． □

6 まとめ

本稿では，情報理論的に安全な片側認証方式を提案し，その数理モデル，安全性の定式化，鍵長及びレスポンス長のタイトな下界，最適な構成法について示した．

参考文献

[1] M. Bellare and P. Rogaway, "Entity authentication and key distribution, Advances in Cryptology - CRYPTO'93, LNCS 773, pp. 232-249, Springer, Heidelberg (1993).

[2] R. Bird, I. Gopal, A. Herzberg, P. Janson, S. Kutten, R. Molva and M. Yung, "Systematic design of two-party authentication protocols, Advances in Cryptology - CRYPT0 '91, LNCS 576, pp. 44-61, Springer, Heidelberg (1991).

[3] K. Kurosawa, "Unconditionally secure entity authentication, "Proceedings ofISIT'98, pp. 298, IEEE(1998).

[4] 二井 将太, 四方 順司, 松本 勉, "情報理論的安全性に基づく相手認証方式", 2009 暗号と情報セキュリティシンポジウム (SCIS2009) 予稿集, 電子情報通信学会 (2009).

[5] R. Safavi-naini, ,H. Wang, : Multireceiver Authentication Codes: Model, Bounds, Constructions and Extentions. Information and Computation, vol.151, pp. 148-172.(1999).

[6] C. Blundo, A. D. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-Secure Key Distribution for Dynamic Conferences", Information and Computation, vol.146, pp. 1-23, (1998).