ゼロ知識個人認証を用いたメッセージ認証プロトコルの設計

2L−3

佐藤　信　　阿部　芳彦*
岩手大学工学部情報工学科

1　はじめに

相互接続型ネットワークは独立したネットワークを組み合わせることにより柔軟にネットワークを構成できる。しかし，各サイトの管理運営組織が異なる場合，通信をおこなう端点間の経路上のそれぞれのサイトのセキュリティ機能を使用して各ユーザが望むレベルのセキュリティを確保するためには複雑な管理が必要である。そのため通信をおこなう端点間のプロトコルのみで一定レベルのセキュリティを確保する機能が必要となる。本稿では，知識の所有のゼロ知識個人認証プロトコルである Fiat-Shamir 法 [1] を基本としたメッセージ認証プロトコルの設計について述べる。本プロトコルは以前設計した知識の所有のゼロ知識個人認証プロトコルを基にしたメッセージ認証プロトコル [2] を改良したものである。以前のプロトコルでは一つのステップで複数のメッセージを原始的に転送するために電子署名を使用する必要があった。任意のプロトコルデータに電子署名を使用するのは，セキュリティとプライバシの点で好ましくない。そこで一つのステップで一つのメッセージのみを転送することにより電子署名を使用しないようにプロトコルを改良した。

2　プロトコルの設計方針

Fiat-Shamir 法では知識の所有のゼロ知識個人認証をおこなうために，証明者と検証者が乱数データを送受信する。この乱数成分を使用して個人認証だけでなくデータを伝送するためのプロトコルが研究されている。Desmedet ら [3] は Fiat-Shamir 法の通信データをサブリミナルチャネルとして使用するためのプロトコルを提案している。Okamoto と Ohta[4] は Fiat-Shamir 法の通信データの乱数成分を使用して安全に鍵配布するためのプロトコルを提案している。
現在，インターネットでの認証方式としては認証局を使用した方式が研究されている。認証局を使用したセキュリィティシステムとして kerberos[5] がある。kerberos では鍵配布センターが配布するチケットを使用して認証をおこなう。この鍵配布のために Needham と Schoroeder のプロトコル [6] を使用している。Ellison[7] は認証局を使用しないで認証するためのプロトコルを提案している。このプロトコルは検証者が実際に証明者を知っているのだが，現在使用できるセキュリティシステムに証明者が登録されていない場合などに使用できる。このプロトコルを使用すると，証明者と検証者が通信をする前にあらかじめそれぞれの公開鍵を認証局に登録する必要がなくなる。そのためにセキュリティシステムの設計，開発そして管理を簡略化できる。公開鍵の安全性だけをもとに証明者と検証者の間にセキュリティチャネルを形成することができれば，認証局を使用しないで認証をおこなえる。そこで，筆者らはつぎのプロトコルを提案した。

（前処理） 証明者は剰余計算に使用する素数 p, q の合成数 $n = p*q$ を決定する。秘密鍵 s を作成してこれより公開鍵 $I = s*s(mod\, n)$ を作成する。証明者は n, I を検証者に知らせる。

（認証処理） 以下の手順を $O(|n|)$ 回繰り返す。

step1: 証明者は乱数を生成して，
$X = r*r(mod\, n)$ を計算する。
証明者は検証者に送信する
メッセージ t から，
$T = t*t(mod\, n)$ を計算する。
証明者は X, T を検証者に送信する。

step2: 検証者は乱数ビット $e \in \{0, 1\}$ を
生成して，これを証明者に送信する。

step3: 証明者は $e = 0$ のとき，
$Y = r\ (mod\, n)$
$e = 1$ のとき，
$Y = r*s*\mathrm{t}*(\mathrm{r}*\mathrm{s}+\mathrm{t})\ (mod\, n)$
を計算して検証者に送信する。

step4: 検証者は，$e = 0$ のとき，
$X \equiv Y*Y\ (mod\, n)$ を確認する。
$e = 1$ のとき，
Y, X, I と T から $P \equiv r*s*t\ (mod\, n)$ を
計算し，

*Design of Message Identification Protocol using Zero-Knowledge Interactive Proof, Makoto Satoh, Yoshihiko Abe,Iwate University, Department of Computer and Information Science 4-3-5 Ueda,Morioka,Iwate 020,Japan

$P*P \equiv (X*I*T)^2 (mod\ n)$ を確認する。
$t = Y*(X*I+P)^{-1} (mod\ n)$
を計算する。

すべての，検査に合格したら，証明者は公開鍵 I に対する秘密鍵 s を所有していることを確認できる。このとき，メッセージ t が全て同じならばメッセージ認証は知識の対話証明の健全性と同程度の健全性である。

上述のプロトコルでは，step 1で証明者は検証者に T, X を原始的に送信する必要がある。そのために T, X にディジタル署名を付加してメッセージを送信する。しかし，任意の通信データにディジタル署名を付加することはセキュリティとプライバシの点で問題がある。そこで，ディジタル署名を使用しないようにプロトコルを変更した。

3 プロトコルの設計

（前処理） 証明者は剰余計算に使用する素数 p, q の合成数 $n = p*q$ を決定する。秘密鍵 s を作成してこれより公開鍵 $I = s*s (mod\ n)$ を作成する。証明者は n, I を検証者に知らせる。

（認証処理） 以下の手順を $O(|n|)$ 回繰り返す。

step1: 証明者は乱数を生成して，
$X = r*r (mod\ n)$ を計算する。
証明者は X を検証者に送信する。

step2: 検証者は乱数ビット $e \in \{0, 1\}$ を
生成して，これを証明者に送信する。

step3: 証明者は $e = 0$ のとき，
$Y = r*t\ (mod\ n)$
$e = 1$ のとき，
$Y = r*s*(r*s+t)\ (mod\ n)$
を計算して検証者に送信する。
t はメッセージである。

step4: 検証者は $e = 0$ と $e = 1$ の
のレスポンスを受信したら，
$e = 0$ のときの X, Y から，
$T = Y*Y/X\ (mod\ n)$ を計算する。
$e = 1$ のときの X, Y，I と T から
$P \equiv r*s*t\ (mod\ n)$ を
計算し，
$P*P \equiv (X*I*T)^2 (mod\ n)$ を確認する。
$t = Y*(X*I+P)^{-1} (mod\ n)$
を計算する。

すべての，検査に合格したら，証明者は公開鍵 I に対する秘密鍵 s を所有していることを確認できる。このとき，メッセージ t が全て同じならばメッセージ認証も知識の所有の対話証明と同程度の健全性である。

4 検討

完全性，健全性そしてゼロ知識性に関してはFiat-Shamir法と同様に証明可能[8]である。

完全性 正しい証明者がその秘密鍵を使用して本プロトコルを実行すると，step4の検証者の検査に確立1で合格する。

健全性 同一の $X = r*r, t\ (mod\ n)$ に対して $Y = r*t$ と $Y = r*s*t(r*s+t)\ (mod\ n)$ を知ることができれば秘密鍵 s を計算可能であることを使用して健全性を証明可能である。

ゼロ知識性 $X = r*r\ (mod\ n)$ または $X = r*r/I (mod\ n)$ を使用すると秘密鍵を知らなくても1／2の確立で検査に合格することができることを使用してシュミレータを構成して証明可能である。

5 おわりに

本プロトコルにより，相互接続型ネットワークで柔軟，容易そして安全に知識の所有のゼロ知識証明を用いたメッセージ認証をおこなえる。任意の通信データにディジタル署名を付加しないので，このプロトコルを使用するアプリケーションを設計する場合などに任意の通信データにディジタル署名を付加することにより生じるセキュリティとプライバシの問題を解決できた。今後は，本プロトコルをグループ認証プロトコルに拡張する予定である。

参考文献

1）太田，藤岡：ゼロ知識証明の応用，
情報処理 Vol.32 N0.6, pp.654-662(1991)
2）佐藤，阿部：ゼロ知識個人認証を用いた
メッセージ転送プロトコルの設計，
コンピュータセキュリティシンポジウム'98，
pp131-134(1998)
3）Y.desmedt 他：Special Uses and Abuses of the Fiathamir Passport Protocol,
Cripto'87(1987)
4）T.Okamoto, K.Ohta：How to Utilize the Randomness of Zero-Knowledge Proofs,
Cripto'90(1990)
5）GEORGE COULOURIS 他：
分散システム，電気書院, pp.859-888
6）Menezes, van Oorschot, Vanstone：
HANDBOOK of APPLIED CRYPTOGRAPHY,
CRC press(1997)
7）Carl M. Ellison：Establishing Identity without Certification Authorities,
6th USENIX Security Symposium
8）岡本 栄司：暗号理論入門，共立出版，
pp.145-154