PGPを用いた情報セキュリティに関する研究*

1S－4

○森　隆之　松山　実　横井　利彰
武蔵工業大学

1　はじめに

ネットワーク社会が到来しつつあるが，現在オンライン上のデータは保護されているとはいえない．特にインターネットでは見ず知らずの人が管理者を務める中継ネットワークをデータが通過するので，いつどこで改竄されるか分からない．電子メールなどの個人のプライバシーの保護も大切である．しかし，現在は組織的にデータを保護するのが難しく，従って個人でプライバシーを守る必要がある．個人でプライバシーを守る方法としてPGP (Pretty Good Privacy:プライバシー機能実現メール)が注目されている．

本報告では，PGPを用いる上で問題となる鍵の配送を，ゼロ知識対話証明を適用してメールのやり取りのみで行う方法について述べる．

2　PGP

PGPとは共通鍵と公開鍵を併用した暗号システムで，ファイル及び電子メールの暗号化，ファイルなどへの電子署名が個人レベルで可能である．

2.1　暗号化

PGPの暗号化には共通鍵暗号法(IDEA)と公開鍵暗号法(RSA)が用いられている．本文の暗号化にはIDEAを用いる．その際，鍵はランダムに生成するものとし，鍵の暗号化にはRSAを用いる．これにより暗号化の時間短縮を図る．電子署名は，本文のMD5(一方向ハッシュ関数)をとり，それをRSAで暗号化し本文に添付する[1].

2.2　鍵の配送

PGPでは公開鍵の配送をメールで行うか，直接手渡すのが基本である．しかし，メールで配送する場合，途中で改竄される可能性があるので，鍵の指紋(fingerprint)を電話等でいちいち確認しなければならないのが面倒である．この鍵の指紋は，公開鍵から一意的に定まるが，他の鍵の指紋と重複する可能性はある．

3　ゼロ知識対話証明

ゼロ知識対話証明は，自分の持っている秘密情報を漏らさずに，その秘密情報を持っていることを相手に納得させる方法である．

ここでは，上記の鍵の指紋の信憑性を，ゼロ知識対話証明を用いて検証する．

4　適用

ここでは，ゼロ知識対話証明の一実現方法としてFiat-Shamir法を用いる．この方法は，RSA暗号よりも約100倍高速である[2].

公開鍵を公開する人を証明者とし，受け取る人を検証者と呼ぶことにする．証明者は2つの素数$p, q(p > q)$を生成して，$N(= p \times q)$を公開する．秘密情報s（これに，鍵の指紋を割り当てる）に対して$I = s^2 \bmod N$を満たすIを計算し公開する．Nは素因数分解できれば，任意のIに対し$\bmod N$での平方剰余性が簡単に判定できてしまうので，10進200桁(664ビット)以上の数を用いるべきだとされている[1,2]. 証明者は，この$I = s^2 \bmod N$を満たすs（鍵の指紋）を持っていること，すなわ

*Information security with PGP
Takayuki Mori,Minoru Matsuyama,Toshiaki Yokoi
Musashi Institute of Technology

ち検証者の持っているものと同一であることをゼロ知識対話証明で検証者に証明する.

ステップは以下のようになる.

Step 1 証明者は乱数rを選び, $X = r^2 \bmod N$なるXを計算して, 検証者に送信する.

Step 2 検証者は2進数$e \in \{0,1\}$をランダムに生成して, 証明者に送信する.

Step 3 証明者はeを受信し, $Y = r \cdot s^e \bmod N$を計算して, 検証者に送信する.

Step 4 検証者は$Y^2 \equiv X \cdot I^e \pmod N$が成り立つことを検証する. これで検証者は, 証明者が確かに鍵を保持していることが検証できる.

Step 5 証明者は乱数rを検証者に送信し, 検証者側で追試する. これで検証者は, 証明者と同一の鍵を持っていることが検証できる.

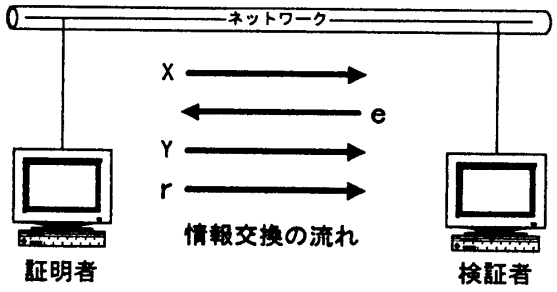

図 1: 処理の流れ

公開鍵が改竄されていても発見できない確率 (なりすませる確率) は1回の検査で2^{-1}なので, 以上の手順をl回繰り返すとその確率は2^{-l}になる. また, 1回しか繰り返さなくても, 秘密情報をk個にすれば, 同様になりすませる確率は2^{-k}になる. 鍵の指紋は以下のような16byteのビット列である.

AB 2C 72 30 E7 1F 84 6E C0 D9 36 73 5F 12 6A 49

ここで最初の1byteを1番目の秘密情報とすれば, なりすませる確率は2^{-16}となる. 秘密情報が1byteで小さい場合は, 数byteで1つの秘密情報とすることも考えられる. また, 以上の方法では1回の検査のために4回の情報交換が必要なので, 計64回の対話が必要になる. しかし, 16回分の検査を同時実行してまとめて送信すれば, 計4回の対話で証明が完了する[3].

なお現在, 以下の仮定を設けている.

- 通信路は常に盗聴が可能である.
- 改竄は乱数rの送信の時のみ不可能とする.

公開鍵の配布であるから, その情報が盗聴されてもかまわない. しかし, Step 5 の鍵の検証に用いる乱数rが改竄されるとそれに気付かない場合がある. 従って, Step 1〜4 で情報が改変された場合でも, 乱数rは改竄されないものとしなければならない. 実際に用いるには, この乱数をメールアドレスや両者が持っている (同一であろう) 公開鍵から求めるなどの工夫を加える必要がある. 検証者側の負荷は大きくなるが, 確率的に鍵の指紋を用いて数通りの乱数を生成し, 検証者側でも同様に生成, 改竄者の計算量を増やすという方法も考えられる.

5 おわりに

PGPという一般的になりつつある暗号化システムの公開鍵の配送について, ゼロ知識対話証明を適用した. 現在は, 証明者が用いた乱数rは, 一切改竄されずに相手まで届くと仮定している. しかし, この仮定には無理がある. 今後は, 鍵を直接配送する場合と, 後に必要になる乱数を配送する場合とでは, 後者の方が安全性を確保しやすいということを, 通信路と送受信者の計算能力の違い[4]を基に示す. 更に, 改竄された場合や, なりすましの人物が間にいた場合の問題点を明らかにする.

参考文献

[1] Bruce Schneier,(力武健次, 道下宣博 訳):「E-mail セキュリティ」, オーム社(1995)

[2] 岡本龍明, 太田和夫(共編):「暗号・ゼロ知識証明・数論」, 共立出版(1995)

[3] 小林信博, 岡本隆司, 桜井幸一:「零知識証明のコンピュータ間認証への適用」, 情報処理学会第44回全国大会,4,pp.265-266(1992)

[4] 坂本直志:「情報を意図的に改変する可能性のある通信路における安全な通信について」, 信学論(D-I),J79-D-I,pp.621-630(1993)