ビットコミットメントを用いたユーザ認証方式の安全性に関する一考察

4H－10

羽田 知史　田中 俊昭
国際電信電話(株)

1. はじめに

Schnorr が提案したユーザ認証方式は離散対数問題に基づく最もシンプルなユーザ認証方式である[1]。しかし、Schnorr 法が非転用性 (non-transferability) を満たすことは知られていない。また、素因数分解に基づくユーザ認証方式としては、Guillou-Quisquater の認証方式が有名であるが、同様にその安全性は証明されていない。これらの認証方式では、検証者が、証明者の第１メッセージに基づいて、チャレンジビットを生成することが可能であり、それにより何らかの情報が検証者に漏洩するという考え方もある。これを回避するための一手法として、コインフリッププロトコルによりチャレンジビットを生成するプロトコルが考えられるが、これまで、その安全性は議論されていない。本稿では、そのプロトコルの安全性について考察する。

2. 準備

2.1 ユーザ認証方式とその安全性の定義

定義 (ユーザ認証方式)

初期化：各ユーザ (例えば、A) は確率的多項式時間アルゴリズムにより、鍵サイズを入力として、自分の公開鍵 PK_A と秘密鍵 SK_A を生成する。

プロトコル：証明者 A は検証者 B に、自分の公開鍵を共通入力とする何らかのプロトコルに従って、秘密鍵を所持することを証明する。プロトコルの結果として、検証者は「受理」あるいは「拒否」する。

定義 (非転用性)

プロトコルに従う証明者および検証者を、それぞれ $\tilde{A}, \tilde{B}$ で表す。また、プロトコルに従わない証明者および検証者を、それぞれ $\tilde{A}, \tilde{B}$ と表す。特に、$\tilde{A}$ は秘密鍵を所持しない。ユーザ認証法式 (A, B) は以下の条件を満たすならば、安全である (非転用性を満たす)。

(1)$(\tilde{A}, \tilde{B})$ は、確率１で成功し、V は受理する。

(2)$(\tilde{A}, \tilde{B})$ を多項式回、実行した後に、$\tilde{B}$ が得る通信履歴を $\tilde{A}$ に転送した時、$(\tilde{A}, \tilde{B})$ が無視できない確率で成功するような、ペア $(\tilde{A}, \tilde{B})$ は存在しない。

2.2 Schnorr のユーザ認証方式

初期化：まず、$q|p-1$ を満たす素数 p, q、位数 q の元 $g \in Z_p^*$ を生成する。秘密鍵 $s \in Z_q$ をランダムに選び、公開鍵 $v = g^{-s} \bmod p$ を計算する。

プロトコル：**(Step1)** A は乱数 $r \in Z_q$ を生成し、$x = g^r \bmod p$ を計算し、B に送信する。**(Step2)** B はチャレンジビット $e \in Z_q$ を生成し、A に送信する。**(Step3)** A は $y = r + es \bmod q$ を計算し、B に送信する。**(Step4)** B は $x = v^e g^y \bmod p$ が満たされていれば受理する。

2.3 ビットコミットメントプロトコル

本稿では、平方剰余性判定問題に基づく二つのビットコミットメントプロトコルを利用し、証明者がコミットする側になる。N を二つの素数 P, Q の積とする。ある乱数 $x \in Z_N^1$ が与えられた時、x が平方剰余であるか平方非剰余であるか判別することは困難であると考えられている。ただし、$Z_N^1 = \{x | x \in Z_N^* \text{ and } (x/N) = 1\}$ である。

トラップドアビットコミットメント BC_1

初期化：N と平方剰余 z を生成する。

プロトコル：A は、$b \in \{0,1\}$ にコミットしたい時、乱数 $r \in Z_N^*$ を選び、$c = BC_2(z,b,r) = z^b r^2 \bmod N$ を計算して、B に送信する。デコミット時には、b, r を B に送信し、B は $c = z^b r^2 \bmod N$ をチェックする。この場合では、P, Q (または z の平方根) がトラップドアであり、この情報を知っていれば、証明者は c を $\{0,1\}$ のどちらのコミットとしてでも、デコミットすることが可能である。

ノントラップドアビットコミットメント BC_2

初期化：N と平方非剰余 z を生成する。

プロトコル：上に同じ。この場合、トラップドアは存在しない。

これらのビットコミットメントは、パラレルに実行することにより１ビットだけでなく、複数ビットコミットすることが可能である。以下では、複数ビットのコミットメントを仮定する。

3. 安全性の考察

本稿では、Schnorr 法を例にとり、その修正プロトコルを考える。先に述べたようにオリジナルの Schnorr 法では、B はそのチャレンジビットを、A の第１メッセージに依存して生成することが可能である。これを回避するために、以下のようなプロトコルが考えられる。ここで、BC は BC_1 あるいは BC_2 である。

プロトコル：**(Step1)** A は乱数 $r, b, \in Z_q, r' \in Z_N^*$ を生成し、$x = g^r \bmod p, c = BC(z,b,r')$ を計算し、B に

"A Note on the Security of Identification Schemes using Bit Commitment" by Satoshi HADA and Toshiaki TANAKA
KDD R & D Laboratories.
2-1-15 Ohara, Kamifukuoka-shi, Saitama 356. Japan

送信する。**(Step2)**Bはチャレンジビット $e \in Z_q$を生成し、A に送信する。**(Step3)**A は $y = r+(e+b)s \bmod q$ を計算し、y, b, r'を Bに送信する。**(Step4)**Bは $x = v^{e+b}g^y \bmod p$ かつ $c = BC(z, b, r')$ が満たされていれば受理する。

この修正プロトコルでは、チャレンジビットの役割を果たすのは $e+b$ であり、この値は BCを利用したコインフリッププロトコルにより得られる。以下、平方剰余性判定問題が困難であるという仮定のもとで、上記修正プロトコルの安全性を考察する。

3.1 $BC = BC_1$の場合の安全性

この場合、秘密鍵 s を所持しなくても、トラップドアを所持していれば、$\tilde{A}$をシミュレート可能である。なぜなら、$e+b$ の値を自由に操作できるからである。

プロトコルの非転用性が満たされないと仮定すると、離散対数問題を多項式時間で計算できることを示す。仮定により、定義の条件 (2) における $(\tilde{A}, \tilde{B})$ ペアが存在する。v, q, p が与えられたとし、$(\tilde{A}, \tilde{B})$ ペアを利用して、vの離散対数を計算する多項式時間アルゴリズムを述べる。v, q, pを入力として、**(Step1)**$N = PQ$ と平方剰余 zを生成する。**(Step2)** トラップドア P, Q を用いて $(\tilde{A}, \tilde{B})$ をシミュレートする。ここで、vは$\tilde{A}$の公開鍵と考える。**(Step3)**Step2 で得られた通信履歴を使用して、$(\tilde{A}, \tilde{B})$ をシミュレートし、$(\tilde{A}, \tilde{B})$ が成功することを確認する。**(Step4)**$\tilde{A}$を利用して、離散対数 s を算出する。

Step3 において、$(\tilde{A}, \tilde{B})$ は無視できない確率で成功する。また、平方剰余性判定問題が困難であるので、$\tilde{A}$はトラップドアを所持できない。したがって、$x = v^{e_1+b}g^{y_1} = v^{e_2+b}g^{y_2} \bmod p$ $(e_1 \neq e_2)$ を満たす (x, e_1, y_1, e_2, y_2) が算出される。つまり、vの離散対数 s が算出される。

3.2 $BC = BC_2$の場合の安全性

平方剰余性判定問題が困難であるという仮定のもとでは、$\tilde{B}$は、プロトコルで使用している BCが BC_1であるのか BC_2であるのか判定することは困難である。

プロトコルの非転用性が満たされないと仮定した場合、平方剰余性判定問題を多項式時間で解けることを示す。N, zを入力として、**(Step1)** 初期化により v, s, q, p を生成する。**(Step2)**sを使用して、$(\tilde{A}, \tilde{B})$ をシミュレートする。**(Step3)**Step2 で得られた通信履歴を使用して、$(\tilde{A}, \tilde{B})$ をシミュレートし、$(\tilde{A}, \tilde{B})$ が成功すれば 0 を、失敗すれば 1 を出力する。

zが平方剰余の場合、$BC = BC_1$であるので、前節の非転用性の証明により Step3 で $(\tilde{A}, \tilde{B})$ が成功し、0 が出力される確率は無視できる。それに対し、zが平方非剰余の場合、$BC = BC_2$であるので、仮定より $(\tilde{A}, \tilde{B})$ が成功し、0 が出力される確率は無視できない。したがって、平方剰余性判定問題を多項式時間で解くことができる。

4. 考察

これまで、非転用性を満たす 3 ラウンドのユーザ認証方式がいくつか提案されている。それらの証明技法は 2 つある。(1) 1 つの公開鍵に対して、複数の秘密鍵が存在し、証拠識別不能性 (witness indistinguishability) の概念[2] を利用して安全性の証明がなされる。(2)$BC = BC_1$の場合のように秘密鍵以外に秘密情報が存在し、その秘密情報により$\tilde{A}$をシミュレートできることを利用して安全性の証明がなされる[3]。$BC = BC2$ の場合は、このどちらにもあてはまらない新しい証明技法である。特に、$BC = BC2$ の場合のプロトコルは、1 つの公開鍵に対してユニークな秘密鍵をもつ知識の証明 (proofs of knowledge) であり、さらに非転用性を満たす 3 ラウンドプロトコルである。そのようなプロトコルはこれまで知られていない (4 ラウンド以上ではそのようなプロトコルはゼロ知識証明として存在する)。

本稿では、離散対数問題に基づく Schnorr 法の修正プロトコルとして考察してきたが、任意の NP 問題のゼロ知識証明のパラレルバージョン (3 ラウンド) に対しても、全く等価な非転用性を満たす修正プロトコルが構成できる。また、本稿の安全性の考察は非転用性のみに着目したが、証拠隠蔽性 (witness hiding)[2]に関しても、3 章の考察に従って証明できるものと考えられる。したがって、平方剰余性判定問題が困難であるという仮定のもとで、任意の NP 問題に対して証拠隠蔽性を満たす知識の証明を構成できると考えられる。

5. まとめ

Schnorr 法において、検証者が証明者の第 1 メッセージに依存したチャレンジビットを生成することを回避するために、ビットコミットメントを用いた修正 Schnorr 法の安全性を考察し、平方剰余性判定問題が困難であるという仮定のもとで、非転用性が満たされることを証明した。本結果は、任意の NP 問題そして証拠隠蔽性の概念へも適用できるものと考えられ、別の機会で報告する予定である。

参考文献:(1)Schnorr, C. P., "Efficient Signature Generation by Smart Cards," Journal of Cryptology, 1991.(2)Feige, U. and Shamir, A., "Witness Indistinguishable and Witness Hiding Protocols," 22nd STOC, 1990. (3)Shoup, V., "On the Security of a Practical Identification Scheme," Eurocrypt'96.