ISSN 1000-9825 Journal of Software 软件学报 2000,11(10):1283~1285

Remarks on a Minimal Leak Proof Protocol*

JIANG Shao-quan FENG Deng-guo QING Si-han

(State Key Lab. of Info. Security Institute of Software Chinese Academy of Sciences Beijing 100080)
(Eng. Research Center of Info. Security Technology Chinese Academy of Sciences Beijing 100080)
E-mail: jiangshq@sina.com
http://cist.iscas.ac.cn; http://www.ercist.ac.cn

Abstract The error of a Minimal Leak Proof Protocol is analyzed and a corrected proof protocol is proposed. Also the security of the protocol is considered.

Key words Security, protocol, zero knowledge.

Arto Salomaa gived a Minimal Leak Proof of Identification in Ref.[1]. However, we find that the proof is not secure. We find that although the protocol can prove the identification of the prover, it is possible that the verifier can get the important information of the prover's secret key. Thus the system is compromised.

The following sections are arranged as follows. Section 1 introduces and analyzes the protocol of Arto Salomaa. Section 2 gives an improved protocol that is secure and feasible.

1 Analysis of the Protocol of Arto Salomaa

Now assume n is an RSA number. Set $n=pq$, where p and q are primes. And the prover wants to prove to the verifier that he is the owner of the number n. Arto Salomaa's protocol is as follows:

V: Verifier, P: Prover

(1) V selects a random x, and sends $c=x^4$ to P;

(2) P replies with $d=x^2$ to V;

(3) V checks that $d=x^2 \bmod n$.

The protocol is not always secure. Here is the analysis.

On receiving $c=x^4 \bmod n$, to obtain d, by computing the square root of c without knowing x, the prover can derive d satisfying one of the following four equations:

$$\begin{cases} d=x^2 \bmod p \\ d=x^2 \bmod q \end{cases}, \tag{1}$$

$$\begin{cases} d=-x^2 \bmod p \\ d=x^2 \bmod q \end{cases}, \tag{2}$$

* This research is supported by the National Natural Science Foundation of China (国家自然科学基金, No. 19931010) and the National Foundation Research Programme of China (国家基础研究发展规划项目, No. G1999035802). **JIANG Shao-quan** was born in 1972. His research interest is cryptography. **FENG Deng-guo** was born in 1965. He is a professor and doctoral supervisor of the Institute of Software, The Chinese Academy of Sciences. His main research areas are cryptography and information security. **QING Si-han** was born in 1939. He is a professor and doctoral supervisor of the Institute of Software, The Chinese Academy of Sciences. His main research areas are technology of information security etc.

Manuscript received 2000-05-31, accepted 2000-06-30.

$$\begin{cases} d=-x^2 \bmod p \\ d=-x^2 \bmod q \end{cases} \tag{3}$$

$$\begin{cases} d=x^2 \bmod p \\ d=-x^2 \bmod q \end{cases} \tag{4}$$

Let's consider which solutions can be used as the candidate of d by the prover.

(1) If $p=1 \bmod 4$ or $q=1 \bmod 4$ (without loss of generality, assume $p=1 \bmod 4$), then $(-1/p)=1$. Let r be the square root of -1 in F_p. It's easy to see that the solution of the equation $\begin{cases} t=rx \bmod p \\ t=x \bmod q \end{cases}$ satisfies $t^4=x^4 \bmod n$. So it's possible that P replies with t'. But $t' \neq x^2 \bmod n$, because $t^2 = x^2 \bmod p$. Thus V can factor n by computing (t^2+x^2,n) and (t^2-x^2,n). So it's not the minimal leak protocol and in fact V gets all the information of n. If it's the prover's public key, V can know all the secret keys easily.

If $q=1 \bmod 4$, then two solutions out of four can be made use of to factor n. If $q=3 \bmod 4$, then one solution out of two can be made use of to factor n. And these valid solutions can be replied by P randomly. So in fact, through the protocol, the probability that V can factor n is 50%.

(2) If $p=q=3 \bmod 4$, then $(-1/p)=(-1/q)=-1$. In this case, of solutions of the four equations above, only the first solution satisfies $(d/p)=(d/q)=1$. Thus P will only reply with this solution, i.e. $x^2 \bmod n$ if he is the owner of n. Seeing that V knows $x^2 \bmod n$ himself, the protocol, in fact, is a zero protocol. That is, in this case the protocol is safe.

2 Corrected Identification Proof Protocol

In this section we will give an corrected protocol based on that of Arto Salomaa. And also we will give the analysis of its security. First we give a useful theorem.

Theorem. Let $p=2^R t+1$, $q=2^s u+1$. Without loss of generality, assume $R \geqslant s$. For any $r \geqslant R$, x^{2^r} that satisfies $x^{2^{r+1}}=C \bmod n$ is sole if the solution exists.

Proof. We only need to prove if $x^{2r+1}=y^{2r+1} \bmod n$ then $x^{2^r}=y^{2^r} \bmod n$. Furthermore, we only need to prove the following.

If $x^{2^{r+1}}=1 \bmod p$, $x^{2r+1}=1 \bmod p$; if $x^{2^{r+1}}=1 \bmod q$, $x^{2r+1}=1 \bmod q$.

We only need to prove the first statement. Let g be a primitive element of F_p, then all the solutions of the equation $Y^{2^r}=1 \bmod p$ are 1, $-1=g^{t2^{r-1}}$. Let $x=g^l$ be one solution of the equation $x^{2^{r+1}}=1 \bmod p$, then $l2^r=0$ or $t2^{R-1} \bmod 2^R t$, which gives $t \mid l$ and $l2^r=t2^{R-1} \bmod 2^R t$ is impossible. That is, $x^{2^r}=1 \bmod p$. Thus the proof is completed.

The theorem is saying, in fact, the r-residue solution of the equation $Y^2=C \bmod n$ is sole if it exists. But the problem is how to derive the solution. Now let's introduce our method. In fact, if we have found the solutions of $Y^2=C \bmod p$ and $Y^2=C \bmod q$, we can easily get the solution of $Y^2=C \bmod n$ by using Chinese Remainder Theorem. The efficient method to find square roots can be found in Ref. [2].

Because $-1=g^{t2^{R-1}}$, -1 is not R-residue. Therefore it's not r-residue. And the method to check whether a is v-residue is as follows. For $v \geqslant R$, a is v-residue if and only if $a^t=1 \bmod p$. For $v<R$, a is v-residue if and only if $a^{t2^{R-v}}=1 \bmod p$. The proof is simple and we omit it.

Now let's propose a new Identification Proof protocol. Parameters are the same as those in the theorem above. Now P wants to prove to V that he is the owner of n. Assume r is agreed on before the protocol and also satisfies the condition of the theorem.

(1) V selects a random x and computes $c=x^{2^{r+1}} \bmod n$ and $Ha=H(x^{2^r})$, where $H()$ is a one-way hash function, then V sends c and Ha to P.

(2) P computes the r-residue square root Y of c, checks whether $Ha=H(Y)$ and sends back to V. If such a square root is not found or the check is not successful, he refuses to reply by claiming c is a number in a wrong form or asks c to be sent again.

(3) On receiving Y, V checks whether $Y=x^{2^r} \bmod n$. If yes, he accepts P is the owner of n. If not, he refuses to accept such a fact.

2.1 Security analysis

From the analysis above, we know that if V is honest then Y derived by P must be x^{2^r}. So the protocol can be carried out safely. On the other hand, if he sends the number c in an invalid form, assume c is expressed as $x^{2^m} \bmod n$ and the form maybe is known to V. If $m<R$, c will be found invalid when P computes Y and checks whether it is r-residue. If $m \geqslant R+1$, c is, in fact, valid. If $m=R$, it's easy to prove the r-residue square root Y of c also exists. But to achieve $Ha=H(Y)$ and also because of the security of hash function $H()$, V must know Y. Because n is secure, to get Y, V must first choose Y and then compute $Y^2=C \bmod n$. That is, $Y=x^{2^{m-1}} \bmod n$. However, Y is not r-residue. So P can find out c is in a wrong form. Thus the security of the protocol is proved.

If $R=s$, then in fact hash function $H()$ can be moved away. Because in this case, c in the form of $x^{2^R} \bmod nP$ must reply with $-x^{2^{R-1}} \bmod n$ which is useless in factoring n. Thus in this case the protocol is really an improvement of Arto Salomaa's. We would like to repeat the protocol as follows.

(1) V selects a random x and computes $c=x^{2^{r-1}} \bmod n$, then sends c and Ha to P.

(2) P computes the r-residue square root Y of c and sends back to V. If such a square root is not found, he refuses to reply by claiming c is a number in a wrong form or asks c to be sent again.

(3) On receiving Y, V checks whether $Y=x^{2^r} \bmod n$. If yes, he accepts P is the owner of n. If not, he refuses to accept such a fact.

3 Conclusion

This paper points out an error in Arto Salomaa's Minimal Leak Proof of Identification protocol. Then a corrected protocol is proposed, and the security is proved.

References

1 Salomaa A. Public-Key Cryptography. Berlin, Heidelberg: Springer-Verlag, 1990

2 Koblitz N. A Course in Number Theory and Cryptography. New York: Springer-Verlag, 1987. 46~49

关于极小泄露证明协议的注记

蒋绍权 冯登国 卿斯汉

(中国科学院软件研究所信息安全国家重点实验室 北京 100080)

(中国科学院信息安全技术工程研究中心 北京 100080)

摘要 分析了一个极小泄露证明协议的错误,给出一个更正的协议,并证明了其安全性.

关键词 安全,协议,零知识.

中图法分类号 TP393