简单证明一个承诺值在特定区间内

伍前红, 张键红, 王育民
(西安电子科技大学 ISN 国家重点实验室, 陕西西安 710071)

摘 要: 顾客想向销售商证明其银行帐户上的钱足以购买某种商品, 但不愿意泄露她帐户上的钱, 因此需要一个工具证明一个承诺数在特定的区间内. 目前多数这样的协议要么不能实现完整的证明, 要么效率较低. 本文给出了一个新的协议, 协议简单、易于理解. 它能够实现完整的证明, 其效率比已知的协议更高. 该协议可以用于电子现金、群签名、可证实加密等安全协议设计.

关键词: 零知识证明; 离散对数; 陷门承诺
中图分类号: TN911.22 文献标识码: A 文章编号: 0372-2112 (2004) 07-1071-03

Simple Proof That a Committed Number Is in a Specific Interval

WU Qian-hong, ZHANG Jian-hong, WANG Yu-min
(National Key Lab on ISN, Xidian University, Xi. an, Shaanxi 710071, China)

Abstract: A buyer wishes to show she has enough money in her account without revealing her money to buy some commodities. Therefore, a tool is needed for proving that a committed number is in a specific interval. Up to now, most of such tools were either inefficient or inexact. In this paper, we present a new simple protocol, which is exact and more efficient than the previous ones. The protocol is suited to be used in electronic cash, group signatures, publicly verifiable secret encryption, etc.

Key words: zero-knowledge proof; discrete logarithm; trap-door commitment

1 引言

证明一个承诺数在一个给定的区间内是一个有用的密码协议, 这类协议可以被用于群签名、电子现金系统、公开可证实秘密分享方案以及其它零知识证明协议.

文[1]给出了协议证明一个承诺数在$[0, 2^k - 1]$内, 该协议效率很低, 完成这一证明需要发送大约 196.9kB 数据. 文[2]和[3]给出的协议效率更高, 所需发送的数据分别为 27.5kB 和 01241kB, 但只能证明被承诺数在比给定区间大得多的区间内. 文[4]给出的协议可以证明一个承诺数在特定的区间内, 效率则在上述协议之间, 所需发送大约 11.975kB 数据. 故对完全实现证明一个被承诺数在任何特定区间而言, Fabrice Boudot 协议是最有效的, 但是该协议形式上较为复杂. 本文将给出一个新的协议, 它能够证明一个被承诺数在任何特定区间内. 在相同安全条件下, 计算效率比 Fabrice Boudot 协议更高, 协议更简便.

2 主要思想

假设 Alice 向 Bob 承诺了一个整数 x: $g^x h^r \bmod n$, 她要向 Bob 证明 $x \in [a, b]$. 设 l, t, s 是安全参数, 我们的方案通过下述方式实现: Alice 选取随机整数 A>0, 发送 $u = A^2(x - a + 1) + X$ 给 Bob, Alice 向 Bob 证明: (1) u 确实是上述形式; (2) $|X| < 2^{t+l+s+T}$, Bob 验证(3) $u > 2^{t+l+s+T}$. 这使 Bob 确信 $x \geq a$. 否则, $x - a + 1 \leq 0$, $u = A^2(x - a + 1) + X < X < 2^{t+l+s+T}$, 这与(3)矛盾. 同样工作可证明 $x \leq b$, 从而完成证明 $x \in [a, b]$. Fabrice Boudot 协议通过下述方式证明: Alice 计算 x_1 是满足 $x - a = x_1^2 + Q, Q \geq 0$ 的最大整数, Alice 向 Bob 承诺 Q: $g^Q h^{r_2} \bmod n$, x_1: $g^{x_1^2} h^{r_1} \bmod n$, Alice 向 Bob 证明第一个承诺数 $|Q| < 2^{t+l+1}\sqrt{b-a}$, 第二个承诺数 x_1^2 是一个平方数; Alice 对 $b - x$ 做同样的工作, 这将使 Bob 确信 $x \in [a - 2^{t+l+1}, b + 2^{t+l+1}\sqrt{b-a}]$, 为了最终证明 $x \in [a, b]$, Alice 计算 $x_c = 2^T x$, 通过上述证明, Bob 确信 $x_c \in [2^T a - 2^{t+l+1+T/2}\sqrt{b-a}, 2^T b + 2^{t+l+1+T/2}\sqrt{b-a}]$, 选择 T 足够大使 $2^T > 2^{t+l+1+T/2}\sqrt{b-a}$, 则 $x_c \in [2^T a - 2^T + 1, 2^T b + 2^T - 1]$, 故 $x \in [a - \varepsilon, b + \varepsilon]$ 其中 $0 \leq \varepsilon < 1$. 由于 x 为整数, 故只可能是 $x \in [a, b]$. 我们的证明不需要人为放大 x, 证明也要简单一些.

3 符号与子协议

n 是一个 RSA 模数, 其分解未知, Z_n 表示模 n 的剩余类环, Z_n^* 表示 Z_n 中对乘法可逆的元素构成的乘法群, $|\cdot|$ 表示整数的二进制长度, $a \| b$ 表示两个二进制数的级联, $\log_g a$ 表

收稿日期: 2002-09-10; 修回日期: 2003-03-19
基金项目: 973 国家重大项目(No. G1999035804)

示在模 n 乘法群 Z_n^* 中以 g 为底 a 的离散对数, g 是 Z_n^* 中的元素, l, t, s 是安全参数, E(x, r)= $g^x h^r$, h 是由 g 生成的循环群中的元素, H( ) 是输出为 2t 比特的无碰撞杂凑函数, PK{x: R(x)}表示零知识证明知道 x 使 R(x) 为真, x∈R[a, b]表示 x 是[a, b]中的随机整数.

3.1.1 强 RSA 假设[5]

存在一个多项式时间算法, 输入|n|则输出一个 RSA 模数 n 和一个元素 z∈Z_n^*, 使得不可能找到整数 e|{-1, 1}和 u 满足 z= u^e mod n.

3.1.2 Fujisaki-Okamoto 承诺[5]

设 n 是一个 RSA 模数, Alice 和 Bob 不知道它的分解. h 是由 g 生成的循环群中的元素, g, h 的阶是大于 160 比特的素数使得在它们生成的循环群中计算离散对数是不可行的. Alice 不知道 $\log_g h$. Alice 选择随机整数 r∈R{-2^sn+1, , , 2^sn-1}, 计算 E(x, r)= $g^x h^r$ mod n, Alice 发送 E(x, r)给 Bob 作为对 x 的承诺. Alice 不可能找到 $x_1 \neq x_2$ 使得 E(x_1, r_1)= E(x_2, r_2), 除非他能分解 n 或者知道 $\log_g h$; Bob 也不可能从承诺中获得关于 x 的任何信息, 该协议是统计安全的, 详细的安全分析见文[5]. 下面称这一承诺方案为 FO 承诺.

3.1.3 PK{x, r: E= $g^x h^r$∧x∈[-2^{t+l}b, 2^{t+l}b]}

Alice 用 FO 承诺方案承诺了一个秘密随机数 x∈[0, b], 下述零知识协议将证明 x∈[-2^{t+l}b, 2^{t+l}b]. (1) Alice 选取 X∈R[0, 2^{t+l}b-1]和 G∈R[-2^{l+t+s}n+1, 2^{l+t+s}n-1], 计算 W= $g^X h^G$ mod n, C= H(W), c= C mod 2^t, D_1= cx+X, D_2= cr+G. 如果 D_1∈[cb, 2^{l+t}b-1], Alice 发送(c, D_1, D_2)给 Bob, 否则重复上述工作. (2) Bob 计算 c= C= H($g^{D_1} h^{D_2} E^{-c}$ mod n) mod 2^t 且验证 D_1∈[cb, 2^{l+t}b-1]. 协议失败的概率小于 2^{-l}, Alice 欺骗 Bob 成功的概率小于 2^{-t+1}, 在随机预言模式下是统计安全的, Bob 不可能从证明中获得关于 x 的任何信息, 详细的分析参阅文[4]. 下面称这一证明为 CFT 证明.

3.1.4 PK{x, r_1, r_2: E_1= $g_1^x h_1^{r_1}$∧E_2= $g_2^x h_2^{r_2}$}

Alice 有一个秘密数 x∈[0, b], 设 E= E_1(x, r_1)= $g_1^x h_1^{r_1}$, F= E_1(x, r_2)= $g_2^x h_2^{r_2}$为两个 FO 承诺, 其中 r_1∈R{-2^{s_1}n+1, , , 2^{s_1}n-1}, r_2∈R{-2^{s_2}n+1, , , 2^{s_2}n-1}, s_1, s_2 是安全参数. Alice 将向 Bob 证明 E 和 F 都是对 x 的承诺. (1) Alice 选取 X∈R[1, 2^{l+t}b-1], G_1∈R[1, 2^{l+t+s_1}b-1], G_2∈R[1, 2^{l+t+s_2}b-1], 计算 W_1= $g_1^X h_1^{G_1}$ mod n, W_2= $g_2^X h_2^{G_2}$ mod n, c= H(W_1+W_2), D= cx+X, D_1= cr+G_1, D_2= cr+G_2, 发送(c, D, D_1, D_2)给 Bob. (2) Bob 验证 c= H($g_1^D h_1^{D_1} E^{-c}$ mod n + $g_2^D h_2^{D_2} F^{-c}$ mod n).

记上述协议为 PK{x, r_1, r_2: E_1= $g_1^x h_1^{r_1}$∧E_2= $g_2^x h_2^{r_2}$}, 见文献[6]. 诚实的证明者总能成功地执行协议, 欺骗者成功的概率小于 2^{-t+1}, 协议在随机预言模式下是统计安全的.

4 协议

4.1 协议构造

Alice 使用 FO 承诺向 Bob 承诺了一个秘密随机数 x∈R[a, b], 1∉|a|, |b|, |b-a|∉T, 下面的零知识证明协议可以使 Bob 确信 x∈[a, b], Bob 或攻击者不可能从证明中获得关于 x 的进一步信息, Alice 成功欺骗的概率是可以忽略的.

Step 0 Alice 向 Bob 承诺 E(x, r)= $g^x h^r$ mod n 并执行 PK{x, r: E(x, r)= $g^x h^r$ mod n}, 其中 x∈R[a, b], r∈R[-2^sn+1, 2^sn-1]. Alice 计算 E= $g^{x-a+1} h^r$= $g^y h^r$ mod n, 其中记 y= x-a+1.

Step 1 Alice 选取随机整数 A∉{0, 1}, 0< X< $2^{l+t+s+T}$, 使 u= A^2y+X> $2^{l+t+s+T}$, Alice 选取随机整数 r_1, r_2, r_3∈R[-2^sn+1, 2^sn-1], 使 r_3-Ar_1-r_2∈[-2^sn+1, 2^sn-1], 计算 E_1= $E^A h^{r_1}$ mod n, E_2= $E_1^A h^{r_2}$ mod n, F= $g^X h^{r_3}$ mod n, U= g^u/E_2= $g^X h^{r_3-rA^2-r_1A-r_2}$ mod n.

Step 2 Alice 向 Bob 发送(u, E_1, E_2, F), 并执行:

PK{A, r_1, r_2: E_1= $E^A h^{r_1}$ mod n∧E_2= $E_1^A h^r$ mod n} (1)

PK{X, r_3, r_3-rA^2-r_1A-r_2: F= $g^X h^{r_3}$∧U= $g^X h^{r_3-rA^2-r_1A-r_2}$ mod n} (2)

PK{X, r_3: F= $g^X h^{r_3}$∧X-$2^{t+l+s+T}$∉X∉$2^{t+l+s+T}$} (3)

Step 3 Bob 可以计算 E= $g^{x-a+1} h^r$= E(x, r)g^{-a+1}= $g^y h^r$ mod n 和 U= g^u/E_2= $g^X h^{r_3-rA^2-r_1A-r_2}$ mod n.

Bob 验证零知识证明式(1)、(2)、(3)和 u= A^2y+X> $2^{l+t+s+T}$, 确信 x∈a.

Step 4 Alice 和 Bob 都能够计算 D= $g^{b-x+1} h^{-r}$= E(x, r)$^{-1} g^{b+1}$= $g^z h^{-r}$ mod n, 其中记 z= b-x+1 重复 Step 1、2、3 即可证明 x∉b.

上述协议及子协议都是非交互的, Alice 生成的所有数据可以只发送一次以减少通信的次数.

4.2 协议分析

下面基于强 RSA 假设对协议进行分析.

4.2.1.1 正确性 Alice 和 Bob 执行上述协议后可以确信 x∈[a, b].

由于 Alice 向 Bob 出示了式(1), Bob 确信 E= $g^y h^r$ mod n, E_1= $E^A h^{r_1}$ mod n, E_2= $E_1^A h^{r_2}$= $g^{A^2 y} h^{rA^2+r_1A+r_2}$ mod n; Alice 还向 Bob 出示了式(2), Bob 确信 F= $g^X h^{r_3}$ mod n. U= g^u/E_2= $g^X h^{r_3-rA^2-r_1A-r_2}$ mod n, 故 g^u= UE_2= $g^X h^{r_3-rA^2-r_1A-r_2}$ $g^{A^2 y}$ $h^{rA^2+r_1A+r_2}$= $g^{A^2 y+X}$ mod n. 则 u= A^2y+X mod U(n), 其中 U(n)是欧拉 Totient 函数. 由于 Alice 不知 n 的分解, 不可能求出 U(n), 由强 RSA 假设, 这只能是 u= A^2y+X. Alice 还向 Bob 出示了式(3), Bob 确信-$2^{t+l+s+T}$∉X∉$2^{t+l+s+T}$, Bob 还验证了 u> $2^{l+t+s+T}$, 则 Bob 确信 y>0, 否则 y∉0, u= A^2y+X∉X-$2^{l+t+s+T}$, 这与式(3)矛盾. 则 x-a+1>0, 即 x-a>-1, x-a∈0, x∈a. 同理可得 x∉b.

事实上, 上述协议中的 Step 0 和式(1)与(2)给出了一个独立的零知识证明协议: PK{x, A, X: u= A^2x+X}, 其中 x, A, X 已经进行 FO 承诺. 它易于推广为: PK{x_1, x_2, , , x_n: c= f(x_1, x_2, , , x_n)}, 其中 f(x_1, x_2, , , x_n:)为关于 x_1, x_2, , , x_n 的多元多项式, 限于篇幅, 本文不给出具体协议.

4.2.1.2 完备性 协议失败(诚实的证明者执行协议后未能通过验证)的概率小于 2^{-l}.

根据正确性分析, 协议失败的概率为零知识证明式(1)、

(2)或(3)失败的概率, 由于证明两个 FO 承诺相等的协议是完备的, 诚实的证明者执行式(1)、(2)一定能通过验证, 故协议失败的概率为 CFT 协议失败的概率, 小于 2^{-l}.

4.1.2.3　不可欺骗性　证明者成功欺骗验证者的概率小于 $3@2^{-t+1}$.

如果 Alice 向 Bob 承诺的 $E(x, r)=g^x h^r \bmod n$ 中的 $x \in [a, b]$, 证明者只有在下述两种情况下可以欺骗验证者: 一是寻求一个 x_c, r_c 使得 $x_c \in [a, b]$ 且 $g^x h^r \bmod n = g^{x_c} h^{r_c} \bmod n$, 然后用 x_c 代替 x 执行零知识证明式(1)、(2)和(3), 但这需要解离散对数, 在计算上是不可能的. 二是求解一个 x_c 使得 $x_c \in [a, b]$ 且 $g^x \bmod n = g^{x_c} \bmod n$, 但是在不知道 n 的分解的情况下, 这也是不可能的, 否则与强 RSA 假设矛盾. 在假设上述两种情况不可能欺骗的情况下, 证明者要成功欺骗, 则需要攻破零知识证明式(1)、(2)或(3), 其成功的概率都小于 2^{-t+1}, 故协议结束后证明者成功欺骗验证者的概率小于 $3@2^{-t+1}$.

4.1.2.4　零知识性　协议在随机预言模式下是统计零知识证明.

注意到零知识证明式(1)、(2)或(3)都是统计零知识证明, 攻击者具有无限的计算能力也不能求解出相应的离散对数. 攻击者另外获得的公开数据为 u, E_1, E_2, F 和 $E(x, r)=g^x h^r \bmod n$, 其中 $E_1=E^A h^{r_1} \bmod n$, $E_2=E_1^A h^{r_2} \bmod n$, $F=g^X h^{r_3} \bmod n$, $u=A^2(x-a+1)+X$, 这里有 7 个未知数(为随机整数): $x, r, A, r_1, r_2, r_3, X$, 但只有 5 个方程, 具有无限计算能力的攻击者可以任意猜测一个 x, 从而决定出其它随机数, 它们都是合法解. 因此验证者不可能从证明中获得关于 x 的进一步的信息.

4.1.2.5　协议优化与效率　Alice 在证明 $x \in [b]$ 时可以不必完全重复协议的 1、2、3 步, 她只需选择 $BX0$, 使 $v=B^2 z+X>2^{l+t+s+T}$ 其中 $z=b-x+1$, 向 Bob 证明 $v=B^2 z+X$, Bob 可以验证 $v>2^{l+t+s+T}$. 这样 Bob 也可以确信 $x \in [b]$, 因为前面已经证明 $-2^{t+l+s+T} < F < X < 2^{t+l+s+T}$. Bob 从 $u=A^2(x-a+1)+X$ 和 $v=B^2(b-x+1)+X$ 中不会得到 x 的任何信息, 协议仍然是统计安全的. 设 $|n|=1024, T=512, l=40, t=80, s=40, s_1=40, s_2=552$, 优化后完成证明需要发送数据 15432 比特, 只需 19 次离散对数计算. 在同样安全条件下, 目前效率最高的 Fabrice Boudot 协议需要 21 次离散对数计算. 我们的协议在效率上比 Fabrice Boudot 协议更高, 更简单一些.

5　结论

本文给出了一个统计零知识证明协议, 它能够实现证明一个 FO 承诺值在任何特定的区间内, 其效率比已知的协议更高, 也更简便. 该协议可以用于电子现金、群签名、可证实加密等安全协议. 作为独立兴趣, 本文很容易导出零知识证明一个公开数是一个秘密多项式的函数值, 它可作为一些可公开验证安全协议的子协议.

参考文献:

[1] Mao W. Guaranteed correct sharing of integer factorization with off2line share2holders[A]. Proceedings of Public Key Cryptography 98[C]. Berlin: Springer2Verlag, 1998. 27- 42.

[2] Brickell E Chanum, et al. Gradual and verifiable release of a secret [A]. Proceedings of CRYPTO. 87[C]. Berlin: Springer2Verlag, 1988. 156- 166.

[3] Chan A, Frankel Y, Tsiounis Y. Easy come2easy go divisible cash[A]. Proceedings of EUROCRYPT. 98[C]. Berlin: Springer2Verlag, 1998. 561- 575.

[4] Fabrice Boudot. Efficient proofs that a committed number lies in an in2 terval[A]. Proceedings of EUROCRYPT. 2000[C]. Berlin: Springer2 Verlag, 2000. 431- 444.

[5] Fujisaki E, Okamoto T. Statistical zero knowledge protocols to prove modular polynomial relations[A]. Proceedings of CRYPTO. 97[C]. Berlin: Springer2Verlag, 1997. 16- 30.

[6] Chaum D, Evertse J H, Van de Graaf J. An improved protocol for demonstrating possession of discrete logarithm and some generalizations [A]. Proceedings of EUROCRYPT. 98[C]. Berlin: Springer2Verlag, 1998. 127- 141.

作者简介:

伍前红　男, 1975 年生于四川内江市, 2001 年获四川大学运筹与控制专业理学硕士学位, 现为西安电子科技大在读博士, 主要研究方向为密码学、网络与信息安全、电子商务安全.

张键红　男, 1975 年生于河北石家庄市, 2001 年获贵州大学计算机科学专业工学硕士学位, 现为西安电子科技大在读博士, 主要研究方向为密码学、网络与信息安全、电子商务安全.

王育民　男, 1936 年 2 月 18 日出生, 1959 年 7 月毕业于西安电子科技大学五年制电信工程专业, 现任西安电子科技大学教授、博士导师, 中国电子学会和中国通信学会会士、中国密码学会理事、中国电子学会信息论学会委员、中国自然基金研究会会员、IEEE 高级会员, 长期从事通信、信息论、编码、密码的理论与应用的教学和科研工作, 在国内外学术刊物和会议上发表论文二百余篇. 享受政府特殊津贴.