非交互式零知识公钥密码体制

复旦大学计算机科学系　　赵一鸣

摘　要：零知识公钥密码体制是近年来计算机科学界和密码学界研究的一个重要课题。本文综合了在这方面的研究工作并着重介绍了一个新的零知识证明系统——非交互式零知识证明系统，以及在此基础上建立的第一个抗选择密文攻击的公钥体制。

§1 交互式零知识公钥体制

自七十年代初期 *Diffie* 和 *Hellman* 提出公钥密码体制以后，基于计算复杂性理论的密码体制受到人们的广泛重视。公钥体制的基本思想就是寻找陷门函数 f，使得对于明文 m，很容易得到密文 $f(m)$，但是除非掌握陷门信息，否则很难由 $f(m)$ 得到 m。概率加密体制通过用不可逼近陷门谓词 (UTP)[1] 的概念代替了陷门函数的概念，推动了公钥体制的研究。以概率加密的一种协议为基础：*1985* 年 *Goldwasser*、*Micali* 和 *Rockobb* 三人提出了交互式零知识证明方法[2]，为零知识公钥密码体制的研究奠定了基础。

交互式证明实质上是一个双方的协议。某种语言 L 的交互式证明系统是由证明者 A 和验证者 B 组成的。对于 A、B 共同知道的某一输入 X，A 向 B 提供说明 $X\in L$ 或 $X\notin L$ 的证明。对于一个交互式证明系统，我们假定 A 具有无限的计算能力，B 只限于多项式资源，并要求：若 $X\in L$，而且 A 按预先确定的程序运行，则 B 确定 $X\in L$ 的概率$>1-|X|^{-c}$（对任何常数 $C>0$）；若 $X\notin L$，则无论运行什么程序，B 确定 $X\notin L$ 的概率$>1-|X|^{-c}$（对任何常数 $C>0$）。

在讨论一个证明系统时，我们所说的知识是一个与特殊计算模型相关联的概念。这种模型具有特殊计算资源，人们可以通过学习获得有关的知识。因此，一个报文如果泄露了一个难解计算的结果，就是泄露了知识。如果一个交互式证明系统对于验证者 B 来说，除了确定 X 是否属于 L 之外，不能得到（即无法通过学习获得）任何附加知识，就称该证明系统为零知识证明系统。如果一个交互式证明系统对于窃听者来说不泄漏任何知识（意思是虽然可窃得所有报文，但确定 X 是否属于 L 的概率等同于随机猜测），则称该交互式证明系统是结果不可区分的。

设 $C_k^2=\{n|n=p.q$，且 n 的字长为 k，$p.q$ 为互异素数$\}$，

$Z_N^*=\{X|1<X<N-1$，X 与 N 互质$\}$

对于给定的 N 和 Z_N^* 中某个元素 Z，如果雅可比记号 $(\frac{Z}{N})=-1$，则 Z 一定是一个二次非剩余 $(mod\ N)$ 若 $(\frac{Z}{N})=+1$，则 Z 或者是一个二次剩余 $(mod\ N)$，或者是一个二次非剩余 $(mod\ N)$。令 $Z_N^{+1}=\{X|X\in Z_N^*,\ (\frac{X}{N})=+1\}$。由于 $(\frac{Z}{N})=+1$ 包含了两种情况，因此可把 Z_N^{+1} 分成两个等价类，一个是 Z_N^{+1} 中的二次剩余 $(mod\ N)$ 全体，另一个则为二次非剩余 $(mod\ N)$ 全体。现定义下述语言：

$$I=\{(N,Z)\mid N\in C^2,\ Z\in Z_N^*,\ (\frac{Z}{N})=+1\}$$

$L=\{(N,Z)\mid (N,Z)\in I$，并且Z是一个二次剩余$(mod\ N)\}$

对于语言L的交互式证明系统来说，I就是该证明系统的输入集。整个证明系统的协议分成两部分，一个是A向B证明某个输入$(N,Z)\in I$，另一个则是以(N,Z)为输入，A向B证明$(N,Z)\in L$或$(N,Z)\notin L$。这两个部分在设计时都必须是零知识的，并且第二部分应该是结果不可区分的。文〔3〕给出了系统的整个协议，在假设二次剩余问题是难解的情况下，该协议是零知识的，并且第二部分还是结果不可区分的。

事实上，对于任一语言L，若可容纳于交互式证明系统，则必可容纳于交互式零知识证明系统〔4〕。这就为我们提供了一系列可构造交互式零知识证明系统的语言。

基于交互式零知识证明系统的协议，我们就可建立一个公钥密码体制。设N为A的公钥（A知道N的质因子分解），在与B执行协议的过程中，对于任何$Z\in Z_N^{+1}$，一旦A向B证明了$Q_N(Z)^+$的值以后，Z就可以作为比特$Q_N(Z)$的密码，根据需要，Z可由A选取或由A、B共同选取。因此一元组$(Z_1、Z_2、\cdots\cdots Z_l)$可作为二进制序列$Q_N(Z_1)$、$Q_N(Z_2)\cdots\cdots Q_N(Z_l)$的密码在$A$、$B$之间传送。这种方案对于用户$B$以及窃听者都具有零知识性，具有强大的安全性来对抗被动的窃听者。

§2 非交互式零知识证明系统

对于任何一个交互式零知识证明系统，我们可通过共享一个随机串来代替交互过程。事实上如果P和V是可交互的，则可用电话掷硬币〔5〕方法来构造一个公共随机串，但反之则不一定。因此与交互式相比较，共享一个公共随机串是一弱要求。

非交互式零知识证明系统是出于这样一个想法，对于证明者A和验证者B，A和B拥有一个初始的公共定理，A以此为基础，发现了一些新定理，并且用零知识方法证明给B，使B确信定理的正确性。注意这一过程是非交互式的，确切地说是单向交互式的，只有从A到B的信息。因此所谓非交互式证明就是只有证明者A到验证者B的信息，而没有B到A的信息，整个过程不能互相交谈。

下面我们以证明4—可着色图为例说明非交互式证明系统协议的构造。

设$C_k^3=\{n\mid n=p_1\cdot p_2\cdot p_3$，$p_1$、$p_2$、$p_3$互异者$\}$，$B$：长为$k$，并且$p_1$、$p_2$、$p_3$是互异的素数$\}$由于此时$(\frac{Z}{n})=+1\ (Z\in$　　因此Z_N^{+1}分成4个等价类，Gen是一个密码强伪随机比特发生器$($　$=\begin{cases}1 & \text{若}Z\text{是一个二次剩余}\\ 0 & \text{若}Z\text{是一个二次非剩}\end{cases}$　　输入外，另外分成两步，首先是A非交互式地证明给B：$n\in C_k^3$，　　及4个等价类，然后以此为基础，非交互式地证明给B、G是4—可

公共输入$\{$　　B：一个随机串σop，一个安全参数k和一组4—可着色图G_1、$G_2\cdots$　　大否$\}$

注：$+Q_N($　　$\begin{cases}\text{余}\ (\text{mod } N)\\ \text{剩余}\ (\text{mod } N)\end{cases}$

第一步：A 随机选择 $n\in C_k^3$，并且非交互式零知识证明给 B，使 B 确信 $n\in C_k^3$。这个工作可化归为验证辅助图 H 是 3—可着色的[7]，A 用公共随机串 σ 证明 H 是 3—可着色的。事实上证明 3—可着色是证明 $n\in C_k^3$ 的一种特例。

第二步：对每个输入图 $G\in 4-COL_k$（这里 $4-COL_k=\{X$ 为 4—可着色图$||X|<k\}$），A、B 的程序构造如下：

证明者 A 的程序：

1° 对 Z_n^{+1} 的等价类依次以 1 到 4 给予标号。

2° 求 G 的一个 4—着色

3° 对 G 中任一顶点 V，如果 V 着色 i（$i=1$，2，3，4），则在第 i 类中随机选择一个元素 e_v，并且把 e_v 标在 V 上。令这样标好的图为 G'。

4° $A\rightarrow B$：G'

5° 对 G 中每一条边 (u, v)，随机选择 $y_{uv}\in Z_n^{+1}$，因此 $e_u\cdot e_v\cdot e_{uv}$ $(modn)$ 为某个数的平方，求该同余方程的解随机选取它的平方根 X_{uv}。

$A\rightarrow B$：y_{uv}，X_{uv}

6° 对每个 y_{uv} 做下述工作：

对输入串 ρ，输出 Gen 的后面 k^h 个比特（这里 h 是一个常量）。

令每 k 个比特为一个块，这样 k^h 个比特就构成了一组顺序块。

对所有的块分别检查是否代表了 Z_n^{+1} 中元素。

对每个代表一个平方 $(mod\ n)$ 的块，随机选择它的一个平方根送给 B。

对每个和 y_{uv} 在同一等价类的块，把它的平方根与 y_{uv} 的乘积送给 B。

验证者 B 和程序：

1° 检查 G 中所有标号是否为 Z_n^* 中满足雅可比记号为+1 的元素。

2° 对所有边 (u, v)，检查 Xuv 是否为 $e_u\cdot e_v\cdot y_{uv}$ $(mod\ n)$ 的一个根。

3° 对每个 y_{uv}，检查所接收到的平方根个数是否大于 $\frac{K^h}{5}$，以及 y_{uv} 与平方根乘积个数是否大于 $\frac{K^h}{5}$。

4° 如果所有的检查都是满足的，则 G 是 4—可着色。

对于上述协议，我们可以看出，通讯是单向的，即只有 A 到 B 的信息，并且 V 的所有计算可在概率多项式时间内完成。可以证明整个协议在平方剩余假设下，它是零知识的。事实上，我们可证明在平方剩余假设下，上述证明系统是一个非交互式零知识证明系统[7]。

§3 抗选择密文攻击的公钥体制

非交互式零知识证明系统一个重要的应用就是可以此协议为基础，构造一个公钥体制，这种基于非交互式零知识证明的密码体制具有抗选择密文攻击的特点，事实上，它是第一个抗选择密文攻击的公钥体制。

根据 *Diffie* 和 *Hellman* 提出的公钥体制思想，每个用户 U 公开一串 P_u，而与此有关

的另一串 S_u 保密。另一个用户若要将报文 m 送给 U，则可先计算 $y=E(p_u, m)$，把 y 送给 U，U 在收到 y 后，可利用自己保密的 S_u 通过计算 $D(Su, y)$ 得到 m。而对于其它截获到 y 的人，在多项式时间内由 y 求得 m 是困难的。在这种情况下，该公钥体制似乎是不可破解的。但是，这仅仅是认为攻击者只用截获手段通过计算去破一个密码体制，而实际上攻击者已采用选择密文攻击的手段来破一个体制了。

所谓选择密文攻击就是攻击者把自己选择的信息作为密文发给 U，并获取由此解得的密码的译文。在这种方法下，攻破一个密码体制就可能成功。例如：对于一个在采用编码设备的大银行工作的雇员，就可运用选择密文攻击的手段去攻击银行的密码体制。基于这种情况，人们就试图设计一种抗选择密文攻击的公钥体制，但都没有成功。非交互式零知识公钥体制则解决了这个问题。

在非交互式零知识公钥体制中，原来传送给 U 的报文 m 的密文 y，现在由两串 y 和 σ 所代替，这里 σ 是发送者已知 y 编码的情况下非交互式零知识证明的。编码函数器检查确证 σ，若正确则输出 y 的编码 m，否则就不输出任何东西。事实上，在应用时，我们只可输入已知可证明的编码的密文，编码函数器输出的也就是这些编码。换句话说，编码函数器只输出已知的东西。因此采用选择密文攻击手段是无法攻破这样的公钥体制的。

§4 结　语

本文介绍了非交互式零知识证明系统，并以这样一类语言构造的协议为基础，建立了一个非交互式零知识公钥密码体制，这种体制具有最强的安全性来对抗被动的窃听者，是第一个抗选择密文攻击的公钥密码体制。但是由于这种体制是以按位方式加密的，每一比特被加密成平均长度为 k 的符号串，因此如何克服它的低效率是一个值得研究的问题。以交互式零知识证明系统为基础设计的 *Fiat—Shamir* 方案在计算上有着易并行处理的特点，据估计比用 *RSA* 体制设计的同类系统快 *25—100* 倍。因此对于非交互式零知识证明系统的设计方案也可从易并行处理这一角度考虑，力求提高效率，以促进零知识公钥体制的发展。

参考文献

〔1〕S・Goldwasser and S・Micali, Probabilistic. Encryption, Jcss, Vol. 28, No 2, 1984 PP270—299

〔2〕S. Goldwasser, S. Micali and C. Rackoff, Knowledge Complexity of Interactive Proofs, Proc. 17th STOC, 1985, PP291—304

〔3〕Z. Galil, S. Haber and M. Yung, A Private Interactive Test of a Booleam Predicate and Mnowledge Pablic—key Cryptosystems, Proc. 26th Focs, 1985, PP360—371

〔4〕Everything Provable is Provable in Zero—Knowledgc, CRYPTO 88, August, 1988.

〔5〕M・Blum, Coin Flipping by Telephone, IEEE COMPCON 1982, PP133—137

〔6〕M・Blum and S・Micali, How to Generate Sequences of Cryptographically Strong Pseudo—Random Bits, SIAM J. on Compuling, vol. 13, Now 1984, PP850—

864

(7) M • Blum P • Feldman and S • Micali, Non—Interactive Zero—Knowledge and its Applications Proc 20th STOC, 1988, PP103—112