第33卷 第19期 计 算 机 工 程 2007年10月
Vol.33 No.19 Computer Engineering October 2007
·安全技术· 文章编号：1000—3428(2007)19—0128—02 文献标识码：A 中图分类号：TP393

# 基于RSA的同态密钥协商

向广利[1]，朱 平[2]，张俊红[2]，马 捷[2]
(1. 武汉理工大学计算机学院，武汉 430070；2. 武汉大学计算机学院，武汉 430072)

**摘 要：**回顾了密钥管理的基本内容，介绍了RSA公钥密码体制和整数环上的同态加密机制，提出了基于RSA的同态密钥协商。该协议主要利用RSA的公钥和同态加密机制建立一个会话密钥。与Diffie-Hellman以及基于口令的密钥协商协议相比，它分别有更快的运算速度和较好的安全性。利用BAN逻辑证明了该协议的安全性。

**关键词：**同态加密；密钥协商；BAN逻辑

# Homomorphism Key Agreement Based on RSA

XIANG Guang-li[1], ZHU Ping[2], ZHANG Jun-hong[2], MA Jie[2]
(1. School of Computer, Wuhan University of Technology, Wuhan 430070; 2. School of Computer, Wuhan University, Wuhan 430072)

**【Abstract】** This paper reviews the basic content of key management. It introduces RSA public key cryptosystems and homomorphic encryption scheme in the integer ring. The homomorphism key agreement based on RSA and homomorphic encryption scheme is presented. The protocol can use the public key of RSA to create the contributory, forward secrecy the session key. Compared with Diffie-Hellman protocol and key agreement protocol based on password, it has separately quicker operation speed and better security. The security of the protocol is proved by BAN logic.

**【Key words】** homomorphic encryption; key agreement; BAN logic

密钥管理(key management)是在一种安全策略指导下进行密钥的产生、存储、分配、删除、归档及应用等活动的总称。涉及密钥自产生到最终销毁的整个过程中的有关问题。不同的密码体制(对称密码体制和公钥密码体制)下密钥管理方法也不同[1～3]。在密钥管理的整个过程中，密钥分配(key distribution)与密钥协商(key agreement)有着极其特殊的意义。传统的密钥交换协议有：Diffie-Hellman密钥交换协议，端-端协议(STS)，MTI协议等。这些协议要么不能抵抗中间人攻击，要么需要数字证书或数字签名以抵抗中间人攻击。本文利用RSA和同态加密机制建立一个会话密钥，最终得到的会话密钥是等献的、前向保密的。

## 1 背景知识

在介绍提出的新的同态密钥协商之前，首先来回顾与本文方法相关的基础知识RSA和HES。

### 1.1 RSA

1978年，文献[4]提出了RSA算法，它是第1个既能用于数据加密也能用于数字签名的算法。RSA基础是数论中的欧拉定理，其安全性依赖于大数的因式分解的困难性。

在建立RSA公钥密码系统时，用户首先选取两个大的不同的安全素数p和q。计算：$n = p * q$，然后选取正整数d，使d满足等式：$\gcd(d,\Phi(n))=1$。此处$\Phi(n)$是欧拉函数，并且$\Phi(n)=(p-1)(q-1)$。最后，利用公式：$e * d \equiv 1 \pmod{\Phi(n)}$，计算出e，将(n，e)公布作为加密密钥，(n，d)作为解密密钥。

RSA是一种分组密码系统，加密时首先将明文m数字化，并取长…度小于$\log_2^n$位的数字作为明文块，即$m=m_1 + m_2+\cdots+m_i$。对应的密文是：$c_i = E(m_i)= (m_i)^e \pmod n$。如果已知解密密钥(n，d)时，作计算：$m_i = D(c_i)= (c_i)^d \pmod n$即可解密。

RSA的安全性依赖于大数分解，若$n=p*q$被因式分解，则RSA便被攻破。RSA的加密算法和解密算法互为逆运算，故也经常用于数字签名，其重要性不亚于作为公钥加密体制。

### 1.2 同态加密机制

Sander和Tschudin提出了整数环上的加法、乘法同态加密机制(homomorphic encryption scheme，HES)，加法、乘法同态确保两个变量加密后的计算结果与加密前的计算结果相同[5～8]。

由于整数环上普通的加法和乘法都同态，因此整数环上的同态加密就显得非常简单。设R和S为整数环，用R表示明文空间，S表示密文空间。a，b∈R，E是R→S上的加密函数。如果存在算法PLUS和MULT，使其满足：

$E(a+b)=PLUS(E(a)，E(b))$

$E(a*b)=MULT(E(a)，E(b))$

就可以利用E(a)和E(b)的值计算出E(a+b)和E(a*b)，而不需要知道a，b的值。本文称其分别满足加法同态和乘法同态。

利用整数环上的加法、乘法同态可以采用以下算法进行加密计算：

令$E(x)=(x+r*q) \bmod n$，这里p，q是两个大的素数，r是一个随机整数，$n= q*p$，PLUS是普通的加法，MULT是普通的乘法。

解密算法为：$x=E^{-1}(y)=y \bmod q$，$y=E(x)$。

分为3类的HES(加法同态、乘法同态、混合乘法同态)仅有2种操作：加法和乘法。需要指出的是：(1)明文x和密文E(x)之间是一个一对多的关系(即对明文x，虽然

**作者简介：**向广利(1973－)，男，博士、副教授，主研方向：移动计算，信息安全；朱 平，讲师、博士研究生；张俊红，高级工程师、博士研究生；马 捷，博士研究生

**收稿日期：**2006-10-13 **E-mail：**xianggl@e21.edu.cn

E1(x)≠E2(x)，但 D(E1(x))=D(E2(x)))；(2)仅有一些元素满足混合乘法同态，否则混合乘法同态和乘法同态产生异常。这样，对于整数集，仅有一个整数(x=1)可以满足混合乘法同态，E(xy)=E(x)y。

## 2 同态密钥协商

基于RSA的同态密钥协商需要用到RSA以及HES，在这里，即将进行通信的A、B两个用户拥有自己的基于RSA公钥/私钥对($E_A$, $D_A$)和($E_B$, $D_B$)。A、B两个用户都知道对方的公钥$E_A$和$E_B$，也知道对方的身份标识$ID_A$和$ID_B$。基于RSA的同态密钥协商具体描叙如下：

### 2.1 两方协议

步骤(1)A → B：$ID_A$, $E_B$ ($Y_A$,n,q)

用户A首先选取两个大的安全素数p和q，计算$Y_A=(X_A+R_A*q) \bmod n$，其中，$X_A$ 和$R_A$为随机整数；n= q*p。用户A用B的公钥$E_B$加密$Y_A$,n和q，并且将加密之后的值$E_B$($Y_A$,n,q)和用户A的身份标识$ID_A$一起发送给用户B。

步骤(2)B → A：$K_{AB}(C_B)$, $E_A$ ($Y_B$)

用户B用自己的私钥$D_B$解密$E_B(Y_A,n,q)$，即作运算$D_B(E_B(Y_A,n,q))$，获得$Y_A$,n和q。然后用户B选取两个随机整数$X_B$ 和$R_B$，计算出$Y_B=(X_B+R_B*q) \bmod n$，则可以进一步计算出会话密钥$K_{AB}=(Y_A + Y_B) \bmod q$。用户B接着随机选择一个整数$C_B$并且用会话密钥$K_{AB}$进行加密，同时用A的公钥$E_A$加密$Y_B$ ，将加密后的数据$K_{AB}(C_B)$和$E_A$ ($Y_B$)发送给用户A。

步骤(3)A → B：$K_{AB}(C_A, C_B)$

用户A接收到用户B传来的$E_A(Y_B)$，用自己的私钥$D_A$解密后得$Y_B$。此时用户A也能够计算出会话密钥$K_{AB}=(Y_A + Y_B) \bmod q$。用户B对$K_{AB}(C_B)$进行解密得$C_B$。用户A随机选择一个整数$C_A$，用会话密钥$K_{AB}$加密$C_A$和$C_B$，并将加密后的数据$K_{AB}(C_A, C_B)$发送给用户B。

步骤(4)B → A : $K_{AB}(C_A)$

消息(3)使用户B确信用户A能够正确地解密消息(2)，用户B用会话密钥$K_{AB}$加密$C_A$，并将加密后的结果$K_{AB}(C_A)$发送给用户A。用户A收到$K_{AB}(C_A)$后进行解密得$C_A$，这使用户A确信用户B也正确地计算出了会话密钥$K_{AB}$。

### 2.2 多方协议

假设在一个组里有k个用户$M_1, M_2, \cdots, M_k$，他们有自己的基于RSA公钥/私钥对($E_i$, $D_i$), (1≤i≤k)。每个用户都知道其他用户的公钥$E_i$。组的领导者选取两个大的安全素数p和q，并且计算出n= q*p，用每个用户的公钥$E_i$将n和q发给其他的用户。每个用户$M_i$都生成两个随机数$X_i$和$R_i$，并计算$Y_i=(X_i+R_i*q) \bmod n$，该组用户最终的会话密钥$K = (Y_1 + Y_2 +\cdots+ Y_k) \bmod q$，每个用户对密钥的生成都有自己的贡献。

具体协议如下：

(1) $M_i \rightarrow M_{i+1} : Y_1 + Y_2 +\cdots+ Y_i$，(1≤i≤k-2)

每个用户$M_i$依此向下一个用户$M_{i+1}$发送$Y_1 + Y_2 +\cdots+ Y_i$，i从 1 到k-2。这一步由k-2 子步组成，第一子步用户$M_1$ 计算$Y_1$ 并发送给用户 $M_2$，以此类推，在第k-2 子步$M_{k-1}$收到$Y_1 + Y_2 +\cdots+ Y_{k-2}$，然后结合自己的$Y_{k-1}$生成中间密钥$PI = Y_1 + Y_2 +\cdots+ Y_{k-1}$。

(2) $M_{k-1} \rightarrow ALL : PI = Y_1 + Y_2 +\cdots+ Y_{k-1}$

用户$M_{k-1}$计算出$PI = Y_1 + Y_2 +\cdots+ Y_{k-1}$，并将PI广播给组内所有的用户。

(3) $M_i \rightarrow M_k : D_i (C_i)$, (1≤i≤k-1)

每个用户$M_i$(1≤i≤k-1)从PI中删除自己的$Y_i$并插入一个随机的盲因子$Y'_i$，即$C_i = PI - Y_i + Y_i'$，并用自己的私钥$D_i$对$C_i$进行加密，将加密后的值$D_i$ ($C_i$)都发送给第k个用户$M_k$。

(4) $M_k \rightarrow M_i : (C_i) + Y_k$，(1≤i≤k-1)

第k个用户$M_k$ 用每个用户的公钥$E_i$解密$D_i$ ($C_i$)分别获得相应的 $C_i$，向前面k-1 个用户发送$(C_i) + Y_k$。每个用户收到$(C_i) + Y_k$后，去掉盲因子$Y'_i$，重新插入原来的$Y_i$就可以计算出会话密钥$K = (Y_1 + Y_2 +\cdots+ Y_k) \bmod q$。

(5) $M_i \rightarrow ALL : M_i$, $K(M_i, h(M_1, M_2,\cdots, M_k)$

每个用户$M_i$分别向其他用户发送$M_i$, $K(M_i, h(M_1, M_2,\cdots, M_k)$，以便进行密钥确认，这里h()是普通的hash函数。

该协议需要盲因子$Y'_i$的原因是：(1)没有盲因子，在协议(3)中用户$M_{k-1}$用私钥加密的数和第 1 步中接收到的数相同。(2)攻击者在协议(2)可以发送$Y_1 + Y_2 +\cdots+ Y_i$ 给$M_i$ 以替代PI。如果$M_i$在协议(3)中用这个数生成新的消息，这将和$M_i$在协议(1)中收到的消息相同。为了阻止字典攻击，盲因子是必需的，该协议还实现了前向保密。

## 3 安全性证明

BAN 逻辑是由Burrows，Abadi和Needham提出的一种基于信仰的逻辑，其主要推理规则有消息意义规则、随机数验证规则、裁判规则、新鲜规则以及看见规则等[9]。下面用BAN逻辑对本文所提出的协议进行分析。

本文所提出的协议的主要目的是在通信双方A、B之间建立会话密钥$K_{AB}$。该协议的初始假设有：

(1) $B \mid\equiv \overset{E_A}{\mapsto} A$，即B相信A的公钥是$E_A$

(2) $A \mid\equiv \overset{E_B}{\mapsto} B$，即A相信B的公钥是$E_B$

两方协议的步骤(1)A → B : $ID_A$, $E_B$ ($Y_A$,n,q)，可形式化为：

(3) $B \lhd ID_A$

(4) $B \lhd \{Y_A, n, q\}_{E_B}$

两方协议的步骤(2)B → A : $K_{AB}(C_B)$, $E_A$ ($Y_B$)，可形式化为：

(5) $A \lhd \{Y_B\}_{E_A}$

(6) $A \lhd \{\#(C_B)\}_{K_{AB}}$

两方协议的步骤(3)A → B : $K_{AB}(C_A, C_B)$，可形式化为：

(7) $B \lhd \{\#(C_A, C_B)\}_{K_{AB}}$

两方协议的步骤(4)B → A : $K_{AB}(C_A)$，可形式化为：

(8) $A \lhd \{\#(C_A)\}_{K_{AB}}$

由看见规则和(4)，可以得出：$B \lhd Y_A, n, q$，则B可以构造$Y_B$，进而计算出$K_{AB}=(Y_A + Y_B) \bmod q$，即有：

(9) $B \mid\equiv A \overset{K_{AB}}{\longleftrightarrow} B$，B相信A、B之间的会话密钥是$K_{AB}$

由看见规则和(5)，可以得出：$A \lhd Y_B$，则A可以计算出$K_{AB}=(Y_A + Y_B) \bmod q$，即有：

(10) $A \mid\equiv A \overset{K_{AB}}{\longleftrightarrow} B$，A相信A、B之间的会话密钥是$K_{AB}$

由新鲜规则、看见规则和(6)、(7)，可以得出：

(11) $A \mid\equiv B \mid\equiv A \overset{K_{AB}}{\longleftrightarrow} B$，即A相信“B相信A、B之间的会话密钥是$K_{AB}$”

由新鲜规则、看见规则和(8)，可以得出：

(12) $B \mid\equiv A \mid\equiv A \overset{K_{AB}}{\longleftrightarrow} B$，即B相信“A相信A、B之间的会话密钥是$K_{AB}$”

由(9)～(12)可以看出，本文提出的协议是安全的。

## 4 小结

利用 Sander 和 Tschudin 提出的在整数环上的同态加密机制和 RSA 公钥密码体制，本文提出了一种新的密钥协商——

（下转第 139 页）