一个数据膨胀率为1的概率公钥密码系统*)

王小非 崔国华 李 俊 汤学明
(华中科技大学计算机学院信息安全系 武汉 430074)

摘 要 在RSA公钥密码的基础上,采用时间戳和hash函数技术,并利用以Blum数为模的二次同余式中求平方根的不可计算性,设计了一个概率公钥密码系统,此密码系统的密码强度不低于RSA的密码强度和求以Blum数为模的二次同余式平方根的难度,加、解密的时间复杂度为$O(k^3)$,其中k为模数的长度,密码的数据膨胀率等于1,因此在数据膨胀率上,此概率公钥密码系统是最优的。

关键词 概率公钥密码系统,数据膨胀率,时间戳,二次同余

A Probabilistic Public Key Cryptosystem with a Message Expansion of 1

WANG Xiao-Fei CUI Guo-Hua LI Jun TANG Xue-Ming
(College of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074)

Abstract Based on the RSA public key cryptosystem, a probabilistic public key cryptosystem is proposed, using the techniques of time stamp and hash function. The new scheme makes use of the intractability of solving the square roots in quadratic congruence equation with a Blum integer modulus, whose cipher intensity is no lower than that of RSA scheme and of the difficulty of solving the square root in quadratic congruence equation. In our scheme encoding and decoding requires $O(k_3)$ operation, where k is the length of modulus. And the message expansion is 1, so the scheme is optimal in the message expansion.

Keywords Probabilistic public key cryptosystem, Message expansion, Time stamp, Quadratic congruence

1 引言

在信息安全领域中,公钥密码占有非常重要的地位,通常的公钥密码都是确定性的密码,即当加密密钥取定后,对于一个明文只能产生唯一一个密文。由于在对敏感信息实施机密性保护中,公钥密码通常都是公开加密密钥,因此,确定性公钥密码无法抵抗选择明文攻击。针对公钥密码的这一弱点,Goldwasser和Micali设计了一种非确定性密码,即概率密码[1],此密码可抵抗选择明文攻击,但由于数据膨胀率太大而无实用价值。Blum和Goldwasser随后设计了一种新的概率密码[2],将数据膨胀率减少到$1+k/t$。近年来,有一些关于概率公钥密码方面的研究成果[3~5],但此膨胀率仍然大于1。如何设计出数据膨胀率为1的概率密码,这一直是概率密码设计者向往的一个目标。

2 符号、定义及相关结论

设N是正整数集,$n\in N$,记$Z_n=\{0,1,2,\cdots,n-1\}$,$Z_n^*=\{x|x\in z_n$,且$(x,n)=1\}$。

定义1 若$n=p\cdot q$,其中p和q为两个互不相同的素数,并且满足$p\equiv q\equiv 3 \bmod 4$,则称$n$为Blum数。

定义2 若$a\in Z_n^*$,且存在x满足二次同余式$x^2\equiv a \bmod n$,则称a为模n的二次同余,称x为模n下a的平方根。模n的所有二次同余的集合记为Q_n,若$a\in Z_n^*$且$a\notin Q_n$,则称a为模n的非二次同余,模n的所有非二次同余的集合记为$\overline{Q}_n$。

引理1 若p为素数且$p\equiv 3 \bmod 4$,$a\in Q_P$,则$x^2\equiv a \bmod p$在模p下有且仅有二个平方根,分别为$x\equiv\pm a^{\frac{p+1}{4}} \bmod p$。

证明:先证仅有二个平方根。因为$a\in Q_p$,所以二次同余式有平方根,设x是一个平方根,可验证$-x$也是平方根。下证$x\neq -x \bmod p$。设$x\equiv -x \bmod p$,则$2x\equiv 0 \bmod p$,由此推出$a\equiv 0 \bmod p$,与$a\in Z_p^*$矛盾,因此$\pm x$是$x^2\equiv a \bmod p$的二个平方根。若还有一个根$\bar{x}$,则$x^2-\bar{x}^2\equiv 0 \bmod p$,由此推出或$\bar{x}\equiv x \bmod p$或$\bar{x}\equiv -x \bmod p$,与假设矛盾,因此$x^2\equiv a \bmod p$在模$p$下有且仅有二个根。

因为$p\equiv 3 \bmod 4$,所以$(p+1)/4$为整数。因为$a\in Q_p$,由欧拉定理得$a^{\frac{p-1}{2}}\equiv 1 \bmod p$,由于$a\in Z_p^*$,因此$a^{\frac{p-1}{2}+1}\equiv a \bmod p$,$a^{\frac{p+1}{2}}\equiv a \bmod p$,即$(a^{\frac{p+1}{4}})^2\equiv a \bmod p$,所以$x\equiv\pm a^{\frac{p+1}{4}} \bmod p$是$x^2\equiv a \bmod p$在模$p$下的二个根。证毕。

引理2 设p和q为两个互不相同的素数,$n=p\cdot q$,则对于任一整数a,有$a\in Q_n$等价于$a\in Q_p$且$a\in Q_q$。

证明:因为p和q为两个互不相同的素数,所以$a\in Z_n^*\Leftrightarrow a\in Z_p^*$且$a\in Z_q^*$,因此$x^2\equiv a \bmod n\Leftrightarrow\begin{cases}x^2\equiv a \bmod p\\ x^2\equiv a \bmod q\end{cases}$即$a\in Q_n\Leftrightarrow a\in Q_p$且$a\in Q_q$。证毕。

引理3 设$n=p\cdot q$为Blum数,$a\in Q_n$,则$a^{\frac{\lambda(n)}{4}}\equiv 1 \bmod n$。

证明:因为n为Blum数,所以$(p-1)/2$和$(q-1)/2$为奇数,由引理2$\Rightarrow a\in Q_p$且$a\in Q_q$,由欧拉定理得$a^{\frac{\lambda(n)}{2}}=$

*)本课题得到国家自然科学基金(60403027)、国家"八六三"高科技研究发展计划基金(301-1-3)资助。王小非 博士研究生,主要研究方向为密码理论与密码技术;崔国华 教授,博士生导师,主要研究方向为信息安全,计算机算法;李 俊 博士研究生,主要研究方向为密码理论与数字签名技术;汤学明 博士研究生,主要研究方向为密码理论与密码技术。

$a^{(p-1)\cdot\frac{q-1}{2}}\equiv 1 \bmod p$。同理可得 $a^{\frac{\phi(n)}{2}}\equiv 1 \bmod q$。

因为 p 与 q 互素，所以由 $\begin{cases}a^{\frac{\phi(n)}{2}}\equiv 1 \bmod p\\ a^{\frac{\phi(n)}{2}}\equiv 1 \bmod q\end{cases}\Rightarrow a^{\frac{\phi(n)}{2}}\equiv 1 \bmod n$。因为 $\frac{\phi(n)}{2}=(\frac{p-1}{2})\cdot(\frac{q-1}{2})\cdot 2$，所以 $a^{\frac{\phi(n)}{2}}-1=(a^{\frac{\phi(n)}{4}}+1)(a^{\frac{\phi(n)}{4}}-1)\equiv 0 \bmod n$，所以或 $a^{\frac{\phi(n)}{4}}\equiv 1 \bmod n$ 或 $a^{\frac{\phi(n)}{4}}\equiv -1 \bmod n$。下用反证法证明 $a^{\frac{\phi(n)}{4}}\equiv -1 \bmod n$ 不成立。

设 $a^{\frac{\phi(n)}{4}}\equiv -1 \bmod n$，

则 $\Rightarrow\begin{cases}a^{\frac{\phi(n)}{4}}\equiv -1 \bmod p\\ a^{\frac{\phi(n)}{4}}\equiv -1 \bmod q\end{cases}\Rightarrow\begin{cases}(\frac{-1}{p})=(\frac{a}{p})^{\frac{\phi(n)}{4}}\\ (\frac{-1}{q})=(\frac{a}{q})^{\frac{\phi(n)}{4}}\end{cases}$

因为 $a\in Q_p$，所以 $(\frac{a}{p})=1$，所以 $(\frac{-1}{p})=(\frac{a}{p})^{\frac{\phi(n)}{4}}=1$，又 $(\frac{-1}{p})=(-1)^{\frac{p-1}{2}}$，因为 $\frac{p-1}{2}$ 为奇数，所以 $(\frac{-1}{p})=-1$，这与 $(\frac{-1}{p})=1$ 矛盾，因此 $a^{\frac{\phi(n)}{4}}\neq -1 \bmod n$，即 $a^{\frac{\phi(n)}{4}}\equiv 1 \bmod n$。证毕。

定理 1 设 $n=p\cdot q$ 为 Blum 数，$a\in Q_n$，则对于二次同余式 $x^2\equiv a \bmod n$，有

①在模 n 下有四个平方根；

②这四个平方根中仅有一个 $\in Q_n$，其表达式为：$x\equiv a^{\frac{\phi(n)+4}{8}} \bmod n$。

证明：先证结论①。

因为 $x^2\equiv a \bmod n\Leftrightarrow\begin{cases}x^2\equiv a \bmod p & (1)\\ x^2\equiv a \bmod q & (2)\end{cases}$

根据引理 1，由式(1)得 $x_{1,1}\equiv a^{\frac{p+1}{4}} \bmod p$，$x_{1,2}\equiv -a^{\frac{p+1}{4}} \bmod p$。由式(2)得 $x_{2,1}\equiv a^{\frac{q+1}{4}} \bmod q$，$x_{2,2}\equiv -a^{\frac{q+1}{4}} \bmod q$，因此可由

$\begin{cases}x\equiv x_{1,1} \bmod p\\ x\equiv x_{2,1} \bmod q\end{cases}\begin{cases}x\equiv x_{1,1} \bmod p\\ x\equiv x_{2,2} \bmod q\end{cases}$，

$\begin{cases}x\equiv x_{1,2} \bmod p\\ x\equiv x_{2,1} \bmod q\end{cases}$ 和 $\begin{cases}x\equiv x_{1,2} \bmod p\\ x\equiv x_{2,2} \bmod q\end{cases}$

求得 $x^2\equiv a \bmod n$ 的所有四个平方根。

再证明结论②。因为 $p=3 \bmod 4$，所以 $\frac{p-1}{2}$ 为奇数，由欧拉定理得 $(\frac{-1}{p})=(-1)^{\frac{p-1}{2}}=-1$，所以 $(\frac{-a^{\frac{p+1}{4}}}{p})=(\frac{-1}{p})\cdot(\frac{a^{\frac{p+1}{4}}}{p})=-(\frac{a^{\frac{p+1}{4}}}{p})$，因此 $x_{1,1}$ 和 $x_{1,2}$ 中仅有一个 $\in Q_p$，记此值为 x_1，同理可证在 $x_{2,1}$ 和 $x_{2,2}$ 中仅有一个 $\in Q_q$，记为 x_2，由引理 2 得 $x\in Q_n\Leftrightarrow x\in Q_p$ 且 $x\in Q_q$，因此 $x^2\equiv a \bmod n$ 的四个平方根中仅有一个 $\in Q_n$，即由 $\begin{cases}x\equiv x_1 \bmod p\\ x\equiv x_2 \bmod q\end{cases}$ 产生。

下求此平方根。由引理 3 得：$a^{\frac{\phi(n)}{4}}\equiv 1 \bmod n$，所以 $a^{\frac{\phi(n)}{4}+1}\equiv a \bmod n$

因为 n 为 Blum 数，可验证 $\frac{\phi(n)}{4}+1$ 为偶数，所以 $a^{\frac{\phi(n)+4}{4}}=(a^{\frac{\phi(n)+4}{8}})^2\equiv a \bmod n$，即 $a^{\frac{\phi(n)+4}{8}}$ 为 $x^2\equiv a \bmod n$ 的一个平方根。因为 $a\in Q_p$，所以 $(\frac{a^{\frac{\phi(n)+4}{8}}}{p})=(\frac{a}{p})^{\frac{\phi(n)+4}{8}}=1$，所以 $a^{\frac{\phi(n)+4}{8}}\in Q_p$，同理可证 $a^{\frac{\phi(n)+4}{8}}\in Q_q$，由引理 2 得 $a^{\frac{\phi(n)+4}{8}}\in Q_n$，即结论②成立。证毕。

3 密码算法设计

3.1 算法的预处理阶段

对于用户 $i(i=1,2,\cdots)$需进行下述前期工作：

① 构造二个大素数 p_i 和 q_i，其中 $n_i=p_i\cdot q_i$ 为 Blum 数，公开 n_i，对 p_i 和 q_i 保密；

② 产生 RSA 密码的加、解密密钥 e_i 和 d_i，公开 e_i，对 d_i 保密；

③取一个整数 $u_0(i,j)\in Z_{n_j}^*$，其中 n_j 是用户 j 产生的 Blum 数，计算 $u_1(i,j)\equiv u_0^2(i,j) \bmod n_j$，$u_2(i,j)\equiv u_1^2(i,j)\equiv u_1^2(i,j) \bmod n_j$，公开 $u_2(i,j)$，对 $u_0(i,j)$ 和 $u_1(i,j)$ 保密。

3.2 具体算法

当用户 i 要将明文 m 传输给用户 j 时，用户 i 进行下述加密操作：

① 将 $u_1(i,j)$ 联接此次通信的时间戳[6] t，得 $s=u_1(i,j)\square t$；

② 以时间戳 t 为种子，通过 hash 函数 h 产生随机数 $h(s)$；

③ $C_1\leftarrow m\oplus h(s)$；

④ $C\leftarrow C_1^{e_j} \bmod n_j$，将密文 C 传输给用户 j。

当用户 j 收到密文 C 后进行下述解密操作：

① $C_1\leftarrow C^{d_j} \bmod n_j$；

② 根据定理 1 计算 $u_1(i,j)\equiv u_2(i,j)^{\frac{\phi(n_j)+4}{8}} \bmod n_j$；

③ $s\leftarrow u_1(i,j)\square t$；

④ $m\leftarrow C_1\oplus h(s)$。

4 密码算法分析与评价

(1)密码正确性证明

主要是验证用户 j(收方)能正确解密。因为用户 j 拥有解密密钥 d_j，所以可由 C 求出 C_1。因 $\phi(n_j)=(p_j-1)\cdot(q_j-1)$，因此用户 j 可算出 $\phi(n_j)$，并通过定理 1 和用户 i 公开的 $u_2(i,j)$。计算出 $u_1(i,j)$，由解密过程的第三步产生 s。因为 $C_1=m\oplus h(s)$，所以 $m=C_1\oplus h(s)$，由此产生明文 m。

(2)密码强度分析

此密码可分为两层加密，第一层 $m\oplus h(u_1(i,j)\square t)$ 由产生中间加密结果 C_1。第二层是对 C_1 采用 RSA 实施超加密，产生最终的密文 C。在第一层中，解密工作是由 C_1 求 m，因此必须知道 $u_1(i,j)$，由于 $u_1(i,j)\in Q_n$ 且是 $u_2(i,j)$ 的平方根，因此对于仅知 $u_2(i,j)$ 和 n_j 的用户，要计算模 n_j 下 $u_2(i,j)$ 的平方根，这在计算上是不可行的。对于第二层，其密码强度就是 RSA 的密码强度，因此整个算法的密码强度不低于 RSA 的密码强度和求以 Blum 数为模的二次同余式平方根的难度。

(3)密码的加、解密效率分析

密码加、解密的时间开销主要是计算 hash 函数值 $h(s)$ 和 RSA 的加、解密，由于计算 hash 函数值的速度比 RSA 的加、解密速度快得多(例如取 MD5 为 hash 函数)，因此，此密码加、解密的时间复杂度与 RSA 加、解密的时间复杂度相同，等于 $O(k^3)$，其中 k 为模数的长度[7,8]。

(4)密码算法的评价

①可防止选择明文攻击

由于时间戳可取为每次通信的时间或通信序列号，而加密过程中密文是通过以时间戳为种子的 hash 函数值与明文

进行一系列运算而产生，因此，对于同一明文产生的密文具有很好的随机性。同时，由于除了通信双方外，任何用户都不能在多项式时间内得到 $u_1(i,j)$，因此不能进行加密操作，也就无法进行选择明文攻击。

②密码的数据膨胀率为 1

由于此密码是以模数的长度为组长的分组公钥密码，因此与 RSA 一样，其数据膨胀率 $=\frac{\text{每组的密文长度}}{\text{每组的明文长度}}=1$，即完全消除了密文的膨胀，从这一点看，此密码是最优的概率密码。

参 考 文 献

1 Goldwasser S, Micali S. Probabilistic encryption. Journal of Computer and System Sciences, 1984,28(2): 270～229

2 Blum M, Goldwasser S. An efficient probabilistic public-key encryption scheme which hides all partial information. Advances in Cryptology Procedings of CRYPTO'84 (LNCS196), 1985. 289～299

3 Park S J, Lee Bo Young, Won D H. A Probabilistic Encryption using very high Residuosi ty and Its Applications. Global Telecommunications Conference. GLOBECOM'95., IEEE. 1995, 2: 1179～1182

4 Choi D H, Choi S, Won D. Improvement of Probbilistic Public Key Cryptosystems Using Discrete Logarithm. ICICS 2001, LNCS 2288, 2002. 72～80

5 Katz J, Yung M. Characterization of Security Notions for Probabilistic Private-Key Encryption[EB/OL]. J. Cryptology, Springer-Verlag, 2005, DOI: 10. 1007/s00145-005-0310-8

6 Stalings W. Cryptography and Network Security. Thiryd ediootn, Pearson Education, Inc., 2003

7 Montgomery P L. Modular multiplication without trial sivision. Math. Comp., 1985, 44(170): 519～521

8 杨宁，董威，戎蒙恬. 基于 RSA 系统的 Montgomery 算法的改进设计. 通信技术，2003(134): 87～88

(上接第 102 页)

列，序列中的项既可以是原子类型，也可以是节点类型。如果返回空序列或返回的序列中只包含一项值为假的布尔类型，则表示订购区域和发布区域不相交，不通过该接口进行转发；反之，则表示订购区域和发布区域相交，通过该接口进行转发。

这种使用 XML 文档片断进行发布、使用 XPath 查询进行订购的表示模型不仅克服了传统主动兴趣管理中数据包格式固定、难以扩展、无法构建实际通用主动路由器的缺点，使得构建实用的主动兴趣管理系统成为可能，而且同传统数据包的二维结构相比，使用 XML 发布数据对于 DVE 系统中使用 XML 格式的数据，如 X3D 等，有更加自然的支持。这种特性随着 XML 数据格式在 DVE 应用中越来越广泛的趋势，将更加突出。

3 系统实现

为了实现的方便，我们尽可能使用了同 AIMNET 一致的协议结构、软件体系架构、渲染引擎等，实现了和 AIMNET 相同的环境和功能。

由于硬件实现的 XML 路由器相当昂贵，也缺乏实际的大规模 XML 路由网络，我们仍然使用软件模拟 XML 路由器的运作情况。模拟的 XML 路由器使用了 JDOM 1.0 来处理 XPath 查询。由于遵循了 XML 路由器的一般规范，这样的软件模拟的 XML 路由器可以方便地替换为实际的 XML 路由器，以构建实际的 DVE 系统。但是，在带来灵活的结构和强大表示能力的同时，软件实现的 XML 路由器的效率显然要低于传统使用兴趣表达式的路由方式。因此，我们并没有对比它们的效率，而仅仅证明了基于 XML 路由网络的主动兴趣管理技术的可行性。随着优化 XPath 查询处理的研究的不断深入，以及 XML 路由器的不断发展与普及，使用实际 XML 路由器的基于 XML 路由网络的主动兴趣管理的性能将远远优于传统主动兴趣管理。

结论和进一步工作 采用 XPath 查询作为路由表，路由 XML 格式数据的 XML 路由技术，使得构建实际的 XML 路由器不仅在理论上，而且在实际上成为可能。因此，将 XML 路由技术引入主动兴趣管理便可以克服主动兴趣管理技术的相关缺陷，提高这一技术的实用性。

由于 XPath 查询的结果可以是节点集，如果在针对 XML 数据包进行转发的同时，还能够根据 XPath 查询的节点集过滤不需要进行转发的节点，还可以进一步提高主动兴趣管理的效率。此外，针对 XPath 查询处理的优化也是进一步工作的方向。

参 考 文 献

1 Macedonia MR. A Network Software Architecture for Large Scale Virtual Environments: [Ph D Thesis]. Monterey, California: Naval Postgraduate School, 1995

2 Frécon E, Stenius M. DIVE: A Scaleable Network Architecture for Distributed Virtual Environments. Distributed Systems Engineering Journal (special issue on Distributed Virtual Environments), 1998, 5(3): 91～100

3 Purbrick J, Greenhalgh C. Extending Locales: Awareness Management in MASSIVE-3. In: Proc. of the IEEE Virtual Reality 2000 Conference. Washington, DC: IEEE Computer Society, 2000. 287

4 Funkhouser TA. Network Topologies for Scalable Multi-User Virtual Environments. In: Proc. of the 1996 Virtual Reality Annual International Symposium. Washington, DC: IEEE Computer Society, 1996. 222～228

5 Macedonia MR, Zyda MJ. A Taxonomy for Networked Virtual Environments. IEEE Multimedia, 1997, 4(1): 48～56

6 Oliveria M, Crowcroft J, Diot C. Router Level Filtering for Receiver Interest Delivery. In: Proc. of NGC 2000 on Networked group communication. New York: ACM Press, 2000. 141～150

7 Zabele S, Dorsch M, Ge Z, et al. SANDS: Specialized Active Networking for Distributed Simulation. In: Proc. of the 2002 DARPA Active Networks Conference and Exposition. Washington, DC: IEEE Computer Society, 2002. 356～365

8 孙元浩，龚爱宇，李惠，等. 可扩展主动兴趣管理技术研究. 中国图形图像学报，2003, 8A (spec): 771～775

9 Abrams HA. Extensible Interest Management for Scalable Persistent Distributed Virtual Environments: [Ph D Thesis]. Monterey, California: Naval Postgraduate School, 1999

10 Oliveira JC, Georganas ND. VELVET: An Adaptive Hybrid Architecture for VEry Large Virtual Environments. Teleoperators and Virtual Environments, 2003, 12(6): 555～580

11 Balikhina T, Ball F, Duce D. Distributed Virtual Environments-An Active future? In: Proc. of the 20th Eurographics UK Conference. Washington, DC: IEEE Computer Society, 2002. 33～37

12 Bray T, Paoli J, Sperberg-McQueen CM, et al. Extensible Markup Language (XML)1.0 (Third Edition). Available at: http://www.w3.org/TR/2004/REC-xml-20040204/

13 Kuznetsov E. XML-Aware Networking. XML J2002, 3(8): 22～23

14 Berglund A, Boag S, Chamberlin D, et al. XML Path Language (XPath)2.0. Available at: http://www.w3.org/TR/2005/CR-xpath20-20051103/