两种背包型的公钥密码算法的安全性分析

韩立东[①] 刘明洁[②] 毕经国[①]
[①](山东大学密码技术与信息安全教育部重点实验室 济南 250100)
[②](清华大学高等研究院 北京 100084)

摘 要：背包型公钥密码体制是几个最早的公钥密码体制之一，分析其安全性十分重要。该文对两种抵抗 Shamir 攻击和低密度攻击的背包型公钥密码体制进行了安全性分析，提出一种新的攻击方法，指出可以利用多项式时间算法以很大的概率找到私钥，从而破解了它们。

关键词：公钥密码体制；陷门背包；密码分析
中图分类号：TP309 **文献标识码**： A **文章编号**：1009-5896(2010)06-1485-04
DOI: 10.3724/SP.J.1146.2009.01396

Security Analysis of Two Knapsack-Type Public Key Cryptosystems

Han Li-dong[①] Liu Ming-jie[②] Bi Jing-guo[①]
[①](*Key Laboratory of Cryptographic Technology and Information Security, Ministry of Education, Shandong University, Jinan* 250100, *China*)
[②](*Institute for Advanced Study, Tsinghua University, Beijing* 100084, *China*)

Abstract: Knapsack-type public-key cryptosystem is one of several earliest public key cryptosystems, and it is very important to analyze their security. This article argues the security of two new knapsack cryptosystems which are secure against Shamir's attack and low density attack. A new attack method is proposed, and it is showed that can be used a polynomial time algorithm to find the secret keys with high probability, and hence break the new knapsack cryptosystems.

Key words: Public-key cryptosystem; Trapdoor knapsack; Cryptanalysis

1 引言

1978 年，Merkle 和 Hellman[1]提出了第一个基于背包问题的公钥密码体制。随后，许多基于背包问题的密码体制相继被提出。作为一类重要的公钥密码算法，对其进行安全性分析是十分必要的。1982 年，Shamir[2]提出了对基本的 Merkle-Hellman 密码体制的多项式时间攻击算法。Coster 等人[3]提出一般的子集和问题的求解方法，其攻击成功的条件是低密度(d<0.9408)和存在求最短向量的预言机，这些方法所利用的工具是 LLL 算法。大部分背包型密码算法都不抵抗这种攻击。

设计与分析抵抗 Shamir 攻击和低密度攻击的背包型密码体制成为密码学家研究背包密码体制的的主要目的。近年来，出现了许多抵抗 Shamir 攻击和低密度攻击新的背包体制的设计与分析的文章[4−8]。本文主要对两种新的背包型密码体制[7,8]进行安全性分析。本文分析方法不是基于 Shamir 攻击方法，因此不需要进行格构造和 LLL 算法。本文第 2 节是对张等人[7]的背包型公钥密码体制的安全性分析，给出多项式时间的攻击方法。第 3 节是对王等人[8]高密度背包型密码算法的安全性分析。通过分析得出，在设计基于背包型公钥密码体制时，不仅要考虑抵抗 Shamir 攻击和低密度攻击，同时还要考虑防止其它的有效攻击方法。

2 新的背包型公钥密码体制及攻击分析

2.1 新的背包型公钥密码体制

密钥生成 随机选取 n 个奇数 $c_1,\cdots,c_n$，其中 $c_n=1$，c_i 为 $n-i$ bit，$i=1,\cdots,n-1$，计算向量 $\boldsymbol{A}=(a_1,\cdots,a_n)$，其中 $a_i=2^{i-1}c_i$。随机选取两个数 M 和 w，满足条件 $M>a_1+\cdots+a_n$，$w<M$ 和 $\gcd(M,w)=1$，计算 $b_i=a_i w \bmod M$ 及 w 模 M 的逆元 w^{-1}。该背包型密码体制的公钥为 $B=(b_1,\cdots,b_n)$。私钥是 w^{-1} 和 M。

加密 二进制明文 $m=(m_1,\cdots,m_n)$，密文 $c=$

2009-10-19 收到，2010-03-03 改回
国家重点基础研究发展计划(2007CB807903)和国家自然科学基金(60525201)资助课题
通信作者：韩立东 hanlidong@mail.sdu.edu.cn

$E(m)=b_1m_1+\cdots+b_nm_n$。

解 密 计 算 $s\equiv cw^{-1}\equiv\sum_{i=1}^{n}b_im_iw^{-1}\equiv\sum_{i=1}^{n}a_im_i(\mathrm{mod}\,M)$， 由于 $M>a_1+\cdots+a_n$，所以 $s=a_1m_1+\cdots+a_nm_n$，此方程可以用有效的方法求解，参见文献[7]。因此可以恢复明文 m。

2.2 攻击方法

本文给出的攻击方法很简单，不同于 Shamir 的方法，但是十分有效。

分析密钥生成过程： $c_n=1$， c_i 为 $n-i$ bit，$i=1,\cdots,n-1$。 因此可以知道 c_{n-1} 是 1 bit，而 1 bit 的奇数只能是1，我们得到 $b_n\equiv a_nw\equiv 2^{n-1}w\,\mathrm{mod}\,M$，$b_{n-1}\equiv a_{n-1}w\equiv 2^{n-2}w\,\mathrm{mod}\,M$，则 $M\mid(2b_{n-1}-b_n)$。当 $2b_{n-1}\neq b_n$ 时，可以通过分解 $2b_{n-1}-b_n$ 求出 M。否则，当 $2b_{n-1}=b_n$ 时， 考虑 c_{n-2}， c_{n-2} 为 2 bit 的奇数 3，所以 $b_{n-2}\equiv a_{n-2}w\equiv 3\cdot 2^{n-3}w\,\mathrm{mod}\,M$，得到 $M\mid(4b_{n-2}-3b_n)$ 和 $M\mid(2b_{n-2}-3b_{n-1})$。当 $4b_{n-2}\neq 3b_n$ 分解 $4b_{n-2}-3b_n$ 即可得到 M， 或者 $2b_{n-2}\neq 3b_{n-1}$ 时分解 $2b_{n-2}-3b_{n-1}$。若 $2b_{n-1}\neq b_n$， $4b_{n-2}\neq 3b_n$ 同时成立，存在另一种求 M 的快速算法，计算 $d=\gcd(2b_{n-1}-b_n,4b_{n-2}-3b_n)$，分解 d 得到 M。依此类推，还可以分析 $c_{n-3},c_{n-4},\ldots$ 的取值。实验数据表明只需分析几个就可以求出并验证正确的 M。知道 M 后，计算 $w=b_n2^{1-n}\,\mathrm{mod}\,M$ 得到 w。从而破解了整个密码算法。

设计者提出为了提高安全性，先对公钥 B 进行随机置换后公开。设 $b_i'=\pi(b_i)$ 是置换后的公钥，攻击者只需对公钥集合 $\{b_i'\}$ 搜索 $O(n^2)$ 次就可以找到对应的 b_n 和 b_{n-1}，然后按照前面所述方法进行分析。

时间复杂度和攻击成功概率：由上面的分析知，该攻击算法的主要运算是模逆运算，这里假设分解大整数的复杂度很小，因为所分解的数是 M 的常数倍。因此对无随机置换的公钥攻击的时间复杂度是 $O(\log^3 M)$，对随机置换后公钥攻击的时间复杂度是 $O(n^2\log^3 M)$。对于攻击成功的概率，首先分析 $2b_{n-1}\neq b_n$ 的概率，记此概率为 p。由 b_i 的生成算法和随机理论知， $p=1/2$。如果 $2b_{n-1}=b_n$，需进一步考虑 $4b_{n-2}\neq 3b_n$ 或 $2b_{n-2}\neq 3b_{n-1}$ 成立的概率，因此攻击成功的概率大于 $1/2$。

3 高密度背包型密码体制及安全性分析

为叙述方便，本文介绍文献[8]中的 3 个定理，其证明见文献[8]。

3.1 几个引理

引理 1 设 $A=(a_1,\cdots,a_n)$ 为背包向量，记 $d_1=a_1$， $d_i=\gcd(a_i,d_{i-1})$， $d_n=\gcd(a_n,d_{n-1})=1$， $D=(d_1,\cdots,d_n=1)$。如果 $k\le d_{i-1}/d_i$， $i=2,\cdots,n$， 则广义背包问题：

$$\sum_{i=1}^{n}a_ix_i=s,\quad 0\le x_i\le k-1 \tag{1}$$

是易解的且至多有一个解。

引理 2 设 $U=\{14,17,19,22,23,26,28,29,30,31,34,37,38,39,40,41,42,43,44,46,47\}$， $V=\{s\mid s\in Z,s>50\}$， $R=U\cup V$， 任取 R 中元素 r， 对任意不同的 $i,j\in\{0,1,\cdots,7\}$， 则 $i^2\neq j^2(\mathrm{mod}\,r)$。

注：原文 U 中包含 48，但是 48 不满足引理 2 的条件，例 $1^2\equiv 7^2\,\mathrm{mod}\,48$。

引理 3 设 $A=(a_1,\cdots,a_n)$ 为背包向量，记 $d_1=a_1$， $d_i=\gcd(a_i,d_{i-1})$， $d_n=\gcd(a_n,d_{n-1})=1$， $D=(d_1,\cdots,d_n=1)$。如果 $d_{i-1}/d_i\in W$， $i=2,\cdots,n$， 则广义背包问题：

$$\sum_{i=1}^{n}a_ix_i^2=s,\quad 0\le x_i\le 7 \tag{2}$$

是易解的且至多有一个解。

3.2 高密度背包型密码体制

密钥生成 随机选背包向量 $\boldsymbol{A}=(a_1,\cdots,a_n)$，记 $d_1=a_1$， $d_i=\gcd(a_i,d_{i-1})$， $d_n=\gcd(a_n,d_{n-1})=1$，$D=(d_1,\cdots,d_n=1)$，而且满足 $d_i/d_{i-1}\in W$。随机选取模数 $M>49\sum_{i=1}^{n}a_i$ 以及与 M 互素的 w 满足：$0<w<M$，计算 $b_i=a_iw(\mathrm{mod}\,M)$ 以及 w 模 M 的逆元 w^{-1}。公钥为 $\boldsymbol{B}=(b_1,\cdots,b_n)$。私钥为 D，w^{-1} 和 M。

加密 明文 $X=(x_1,\cdots,x_n)$， $0\le x_i\le 7$，密文为 $c=\sum_{i=1}^{n}b_ix_i^2$。

解 密 计 算 $s\equiv cw^{-1}\equiv\sum_{i=1}^{n}b_ix_i^2w^{-1}\equiv\sum_{i=1}^{n}ax_i^2(\mathrm{mod}\,M)$， 由 于 $M>49\sum_{i=1}^{n}a_i$， $s=\sum_{i=1}^{n}ax_i^2$，根据引理 3 求解该方程从而恢复出明文 $X=(x_1,\cdots,x_n)$。

参数说明

(1)为了提高安全性，对向量 $\boldsymbol{B}$ 进行随机置换，把置换后的向量作为公钥。

(2)选 $n=120$。

(3)背包向量 $\boldsymbol{A}=(a_1,\cdots,a_n)$ 的选取。随机 $U=\{14,17,19,22,23,26,28,29,30,31,34,37,38,39,40,41,42,43,44,46,47\}$ 中选出(可以重复) $n-1$ 个数 $g_1,g_2,\cdots,g_{n-1}$。令 $d_i=\prod_{k=i}^{n-1}g_k$， $1\le i\le n-1$， $d_n=1$，然后随机选取与 $g_1,g_2,\cdots,g_n$ 都互素的 $n-1$ 个数 $h_2,\cdots,h_n$，记 $a_1=d_1$， $a_i=h_id_i$， $i=2,\ldots,n$，而 $h_2,\cdots,h_n$ 的选取要使得 $a_1,\cdots,a_n$ 具有相同的比特长度。

3.3 攻击思路及方法

首先考虑公钥 $\boldsymbol{B}=(b_1,\cdots,b_n)$ 是没有经过随机置换的。从参数说明中可以得到

$$\left.\begin{aligned}b_1&\equiv a_1w\equiv d_1w(\mathrm{mod}\,M),\\ b_2&\equiv a_2w\equiv h_2d_2w\equiv(h_2d_1w)/g_1(\mathrm{mod}\,M)\end{aligned}\right\} \tag{3}$$

可以得到U中所有元素的素因子包含所有小于 50 的素数，所以 $h_2,\cdots,h_n$必须是所有素因子都大于 50 的数，才能满足与$g_1,g_2,\cdots,g_n$都互素。同时还要满足$a_1,a_2,\cdots,a_n$具有相同的比特长度。因为$a_1=d_1=g_1d_2, a_2=h_2d_2$， h_2与g_1的比特最多相差 1 bit，又g_1小于 48，所以h_2一定大于 50 小于 96，且是素数，因此h_2一定在集合$H=\{53,59,61,67,71,73,79,83,89\}$之中。由式(3)得到另一组方程：

$$\left.\begin{aligned} &h_2b_1\equiv h_2a_1w\equiv h_2d_1w(\bmod M),\\ &g_1b_2\equiv g_1a_2w\equiv g_1h_2d_2w\equiv h_2d_1w(\bmod M)\end{aligned}\right\} \tag{4}$$

得到$M\mid(h_2b_1-g_1b_2)$。只要分解$h_2b_1-g_1b_2$，就可得到M的所有可能值。

对U所有的元素及H中所有元素，一定存在$g_1\in U$和$h_2\in H$，满足式(4)。也就是说，穷搜所有$g_1\in U$和$h_2\in H$，对每一对(g_1,h_2)分解$h_2b_1-g_1b_2$，一定有一个是M的倍数。因g_1，h_2小于 100 且b_1,b_2小于M，所以倍数很小。

下面介绍如何找到正确的g_i，h_i。分两种情况讨论

(1) $\gcd(M,b_i)=1$，$1\le i\le n$。由密钥生成得下面式子

$$\left.\begin{aligned} b_1&\equiv a_1w\equiv d_1w\equiv g_1g_2g_3\cdots g_nw(\bmod M)\\ b_2&\equiv a_2w\equiv h_2d_2w\equiv h_2g_2g_3\cdots g_nw(\bmod M)\\ &\vdots\\ b_i&\equiv a_iw\equiv h_id_iw\equiv h_ig_i\cdots g_nw(\bmod M)\end{aligned}\right\} \tag{5}$$

得到等价关系

$$\left.\begin{aligned} &b_2b_1^{-1}\equiv h_2g_1^{-1}(\bmod M)\\ &b_3b_2^{-1}\equiv h_3g_2^{-1}h_2^{-1}(\bmod M)\\ &b_4b_3^{-1}\equiv h_4g_3^{-1}h_3^{-1}(\bmod M)\\ &\quad\vdots\\ &b_{i+1}b_i^{-1}\equiv h_{i+1}g_i^{-1}h_i^{-1}(\bmod M)\end{aligned}\right\} \tag{6}$$

由前面分析，g_1，h_2已知，通过式(6)的第二个，穷搜U所有的元素，对每一个元素，记为g_2，计算$g_2h_2b_3b_2^{-1}\equiv h_3(\bmod M)$，因为$h_3<M$，所以可以得到$h_3$的值，验证$h_3$与$g_2\cdot h_2$的比特是否相同且$h_3$与$U$所有的元素互素，若条件满足则找到$g_2$，$h_3$。依此类推，下一次搜索$g_3$，验证$h_4$的条件，得到$g_3$，$h_4$，最后计算出所有$g_1,g_2,\cdots,g_n$，$h_2,\cdots,h_n$，然后可以通过$b_1\equiv a_1w\equiv d_1w\equiv g_1g_2g_3\cdots g_nw(\bmod M)$计算出$w$，从而破解整个密码体制。

当M是大素数或是几个大素数的乘积时，$\gcd(M,b_i)=1$，$1\le i\le n$是很大概率成立的，此概率也是攻击成功的概率。该攻击方法的时间复杂度很低，对于第i次搜索，就可得到g_i，h_{i+1}，一共需要n次搜索，所以最多需要$22\cdot n$次运算。

(2)至少有一对$\gcd(M,b_i)\ne1$。第一对不互素的记为(M,b_i)，此时$g_1,g_2,\cdots,g_{i-1}$，$h_2,\cdots,h_i$已知。若(M,b_{i+1})互素，利用$b_ib_{i+1}^{-1}\equiv g_ih_ih_{i+1}^{-1}(\bmod M)$进行类似第一种情况的的分析，可以得到$h_{i+1}^{-1}$。因为$(M,b_{i+1})$互素，所以$h_{i+1}^{-1}\bmod M$存在，然后求出$h_{i+1}$。

若(M,b_{i+1})不互素，不妨设$d=\gcd(M,b_i)$，$d'=\gcd(M,b_{i+1})$。由于$\gcd(M,w)=1$和h_i，h_{i+1}的选取，实际上，

$$d=\gcd(M,h_ig_i\cdots g_n)=\gcd(M,g_i\cdots g_n)\gcd(M,h_i)$$

$$d'=\gcd(M,h_{i+1}g_{i+1}\cdots g_n)=\gcd(M,g_{i+1}\cdots g_n)\gcd(M,h_{i+1})$$

记$\overline{d}'=\gcd(M,g_{i+1}\cdots g_n)$，$H'=\gcd(h_{i+1},M)$，$\Delta=d'/\gcd(d,d')$，则$d'\mid(\Delta\cdot d)$。由$b_i\equiv h_ig_i\cdots g_nw(\bmod M)$及同余性质得$\Delta b_i\equiv\Delta h_ig_i\cdots g_nw(\bmod M)$成立，考虑下面的两个式子：$\dfrac{\Delta\cdot b_i}{d'}=\dfrac{\Delta wg_ih_i}{H'}\dfrac{g_{i+1}\cdots g_n}{\overline{d}'}\left(\bmod\dfrac{M}{d'}\right)$，$\dfrac{b_{i+1}}{d'}=\dfrac{wh_{i+1}}{H'}\dfrac{g_{i+1}\cdots g_n}{\overline{d}'}\cdot\left(\bmod\dfrac{M}{d'}\right)$，因为$\dfrac{b_{i+1}}{d'}$与$\dfrac{M}{d'}$互素，得到

$$\left(\frac{\Delta\cdot b_i}{d'}\right)\left(\frac{b_{i+1}}{d'}\right)^{-1}=\left(\frac{\Delta g_ih_i}{H'}\right)\left(\frac{h_{i+1}}{H'}\right)^{-1}\left(\bmod\frac{M}{d'}\right) \tag{7}$$

因为Δ,d',H'可以计算出，且h_i已知，就可以利用第一种情况的讨论，搜索U所有的元素记为g_i，通过求解同余方程计算出$\left(h_{i+1}/H'\right)^{-1}\bmod(M/d')$，然后求出$h_{i+1}$，验证$h_{i+1}$与$g_i\cdot h_i$的比特是否相同且$h_{i+1}$与$U$所有的元素互素，找出满足条件的$g_i$，$h_{i+1}$。

对于公钥是随机置换后公开的情况，攻击者只需对公钥$\{b_i\}$搜索$O(n^2)$次就可以找到对应的b_1和b_2，然后按照前面所述方法进行分析。

4　结束语

针对两种新的抵抗 Shamir 的攻击和低密度攻击的背包型公钥密码算法，给出不同于以往的新的有效攻击方法，在多项式时间内以很大概率找到私钥，从而破解这两种密码体制。

参 考 文 献

[1] Merkle R C and Hellman M E. Hiding information and signature in trapdoor knapsack[J]. *IEEE Transactions on Information Theory*, 1978, 24(5): 525–530.

[2] Shamir A. A polynomial–time algorithm for breaking the basic Merkle-Hellman cryptosystem[J]. *IEEE Transactions on Information Theory*, 1984, 30(5): 699–704.

[3] Coster M J, Joux A, and LaMacchia B A, *et al*.. Improved

low-density subset sum algorithms[J]. *Computational Complexity*, 1992, 2(2): 111–128.

[4] Wang B, Wu Q H, and Hu Y P. A knapsack-based encryption scheme. *Information Sciences*, 2007, 177(19): 3981–3994.

[5] Wang B C and Hu Y P. Quadratic compact knapsack public-key cryptosystem[J]. *Computers and Mathematics with Applications*, 2009. doi:10.1016/j.camwa. 2009.08.031.

[6] Youssef A M. Cryptanalysis of a knapsack-based probabilistic encryption scheme. *Information Sciences*, 2009, 179: 3116–3121.

[7] 张卫东，王保仓，胡予濮. 一种新的背包型公钥密码算法[J]. 西安电子科技大学学报, 2009, 36(3): 506–511.
Zhang Wei-dong, Wang Bao-cang, and Hu Yu-pu. New knapsack-type public-key cryptographic algorithm. *Journal of Xidian University*, 2009, 36(3): 506–511.

[8] 王保仓，胡予濮. 高密度背包型公钥密码体制的设计[J]. 电子与信息学报，2006, 28(12): 2390–2393.
Wang Bao-cang and Hu Yu-pu. Knapsack-type public-key cryptosystem with high density[J]. *Journal of Electronics & Information Technology*, 2006, 28(12): 2390–2393.

韩立东： 男，1982 年生，博士生，研究方向为计算数论与密码学.

刘明洁： 女，1985 年生，博士生，研究方向为数论代数安全计算.

毕经国： 男，1985 年生，博士生，研究方向为公钥密码学的分析与设计.