基于随机背包的公钥密码

王保仓[①②] 韦永壮[③] 胡予濮[①]

[①](西安电子科技大学计算机网络与信息安全教育部重点实验室 西安 710071)

[②](信息安全国家重点实验室中国科学院软件研究所 北京 100049)

[③](桂林电子科技大学信息与通信学院 桂林 541004)

摘 要：该文构造了一个背包型公钥密码算法。该背包公钥密码具有如下优点：加解密只需要加法和模减法运算，因此加解密速度快；该算法是基于随机背包问题而不是易解背包问题而构造的；证明了在攻击者不掌握私钥信息情况下该密码算法能抵抗直接求解背包问题的攻击，包括低密度攻击和联立丢番图逼近攻击等；证明了攻击者能够恢复私钥信息与攻击者能够分解一个大整数是等价的。分析表明，该算法是一个安全高效的公钥加密算法。

关键词：公钥密码；随机背包；密钥恢复攻击；安全性

中图分类号：TN918.1 **文献标识码**： A **文章编号**：1009-5896(2010)07-1580-05

DOI: 10.3724/SP.J.1146.2009.01113

Public Key Cryptosystem Using Random Knapsacks

Wang Bao-cang[①②] Wei Yong-zhuang[③] Hu Yu-pu[①]

[①](*Key Lab of Computer Networks & Information Security*, *Ministry of Education*, *Xidian University*, *Xi'an* 710071, *China*)

[②](*State Key Lab of Information Security*, *Institute of Software*, *Chinese Academy of Sciences*, *Beijing* 100049, *China*)

[③](*School of Information and Communication*, *Guilin University of Electronic Technology*, *Guilin* 541004, *China*)

Abstract: A knapsack-type public key cryptosystem is proposed. The proposed knapsack cryptosystem has the following advantages. The encryption and decryption only need addition and modular minus operations, so the encryption and decryption speed is high; The cryptosystem is constructed based on random knapsacks but not easy-to-solve knapsack problems; It is proven that if the secret key is not possessed by the attacker, the proposed cryptosystem can withstand the attacks launched by directly solving the underlying knapsack problem, including low-density attack and simultaneous Diophantine approximation attack; It is proven that the attacker can recover the secret keys if and only if he can factor a large integer. Analysis shows that the proposal is an efficient and secure public key encryption algorithm.

Key words: Public key cryptography; Random knapsack; Key-recovery attack; Security

1 引言

公钥密码是确保信息安全和网络安全的重要技术之一。当前常用的公钥密码算法的安全性大都基于整数分解[1]及离散对数包括椭圆曲线上的离散对数问题[2]。陷门背包是密码学历史上最早被设计出来的几个公钥密码算法之一[3]。由于背包密码的快速加解密优势和背包问题的 NP 完全性，很长一段时间内背包算法都被认为是最吸引人的和最有前途的密码算法。背包公钥密码自上世纪 70 年代末 90 年代初一直是公钥密码中的一个研究热点。然而，截至目前，大多数背包公钥密码都被攻破了，这也使大多数密码学家相信背包公钥密码已经死亡。幸运的是，目前仍有一些背包公钥密码算法[4−8]。

背包公钥密码不安全的最重要的原因就在于，这些公钥密码算法在构造的时候都是首先构造易解背包问题，然后把易解背包问题伪装成一个看似困难的背包问题。这样一来就存在两种问题：(1)伪装后的背包问题仍可能属于易解背包问题。倘若如此，则攻击者直接求解从密文和公开背包向量出发构造的背包问题即获得明文。这一类的攻击包括低密度攻击[9]和联立丢番图逼近攻击[10]。(2)如果对易解背包问题伪装不充分，则攻击者能够从公钥求解出对应的私钥。即，此类背包公钥密码易遭受密钥恢复攻击，包括正交格攻击[11]、最大公因数攻击[12]及各

2009-08-21 收到，2010-02-22 改回

国家自然科学基金(60803149，60903200)，国家 973 计划项目(2007CB311201)，111 计划(B08038)，浙江省自然科学基金(Y1091085)和河南省基础与前沿技术研究项目(092300410159)资助课题

通信作者：王保仓 bcwang79@yahoo.com.cn

类格规约攻击[13,14]。因此，我们认为设计安全的背包密码算法的关键就在于使用随机选取背包问题，而不是人为地构造易解背包问题。

基于随机背包问题，本文构造了一个背包公钥加密算法。该算法加密只使用了简单的加法运算，而解密也只使用了模减法运算。因此具有快速的加解密功能。可以证明，给定密文和公钥，攻击者在不掌握私钥信息的情况下若能在多项式时间内通过直接求解底层的背包问题来获取密文，则攻击者同样可以在多项式时间内求解任意的背包问题。因此，给定密文，攻击者只能通过重构私钥才能获取对应的明文信息。分析指出，攻击者必须重构两个背包向量才能获取私钥信息，而公钥只为一个背包向量，攻击者无法重构两个相关的背包向量。因此，攻击者无法发起密钥恢复攻击。

2　背包公钥密码描述

整数 m 的二进制表示记为 $(m)_2$。该公钥密码算法描述如下。

密钥生成　该算法的公私钥生成算法如下。随机选取 n 维背包向量 $\boldsymbol{U}=(u_1,\cdots,u_n)$，其中 u_i 均为正整数，计算向量 $\boldsymbol{V}=(v_1,\cdots,v_n)$，其中 $v_i=u_i-2^{n-i}$，$i=1,\cdots,n$。随机选取两个不同的素数 p 和 q 使得

$$p>\sum_{i=1}^{n}u_i,\quad q>2\max\left\{\sum_{v_i>0}v_i,-\sum_{v_i>0}v_i\right\}\tag{1}$$

使用中国剩余定理计算向量 $\boldsymbol{A}=(a_1,\cdots,a_n)$，$0\le a_i\le pq-1$，即

$$a_i\equiv u_i(\bmod p),\quad a_i\equiv v_i(\bmod q),\quad i=1,\cdots,n\tag{2}$$

这里 a_i 是取模 $N=pq$ 的非负最小剩余。输出背包向量 $\boldsymbol{A}$ 为公钥，用户保存 p 和 q 为私钥。

加密　n 比特长的二进制明文 $(m)_2=m_1\cdots m_n$，其中 $m_i=0$ 或 1，被加密为 $c=a_1m_1+\cdots+a_nm_n$。

解密　接收到密文 c 后，作如下计算即可恢复明文。首先计算 $c_p=c(\bmod p)$，$c_q=c(\bmod q)$，这里 c_p 取模 p 的非负最小剩余，即 $0\le c_p\le p-1$，c_q 取模 q 的绝对最小剩余，即 $-q/2<c_q\le q/2$。则明文 $(m)_2=(c_p-c_q)_2$。即 c_p-c_q 的二进制表示就是 $m_1\cdots m_n$，其中 m_1 是 c_p-c_q 二进制表示的最高位，m_2 是 c_p-c_q 二进制表示的次高位，依次类推，m_n 是 $(c_p-c_q)_2$ 的最低位。

2.1 解密正确性

注意到 $c_p\equiv c\equiv u_1m_1+\cdots+u_nm_n(\bmod p)$，而由式(1)可知，$0\le u_1m_1+\cdots+u_nm_n\le u_1+\cdots+u_n<p$。因此，若取 c_p 为模 p 的非负最小剩余，则必有，$c_p=u_1m_1+\cdots+u_nm_n$。再者，$c_q\equiv c\equiv v_1m_1+\cdots+v_nm_n(\bmod q)$。同样根据式(1)，就有

$$-\frac{q}{2}<-\max\left\{\sum_{v_i>0}v_i,-\sum_{v_i<0}v_i\right\}\le\sum_{v_i<0}v_i\le\sum_{i=1}^{n}v_im_i\le\sum_{v_i>0}v_i\le\max\left\{\sum_{v_i>0}v_i,-\sum_{v_i<0}v_i\right\}<\frac{q}{2}$$

因此，若取 c_q 为模 q 的绝对最小剩余，则必有，$c_q=v_1m_1+\cdots+v_nm_n$。因此

$$\left(c_p-c_q\right)_2=\left(\sum_{i=1}^{n}m_i\left(u_i-v_i\right)\right)_2=\left(\sum_{i=1}^{n}m_i2^{n-i}\right)_2=m_1\cdots m_n=(m)_2$$

于是，n 比特长明文就是 c_p-c_q 的二进制表示。

2.2 举例

下面用一个具体的小例子说明该密码算法的密钥生成与加解密原理。

随机选取 $\boldsymbol{U}=(65,39,21,17,19,45,10,9)$ 并计算向量 $\boldsymbol{V}=(-63,-25,-11,1,11,41,8,8)$。选取满足式(1)的素数 $p=191$，$q=199$。据此可计算公开背包向量 $\boldsymbol{A}=(3121,1567,785,399,210,19108,9560,4784)$。私钥为 $p=191$，$q=199$。

设明文为 $(m)_2=m_1\cdots m_8=10110010$，则密文为 $c=a_1m_1+\cdots+a_nm_8=13865$。

解密时计算 $c_p=c=113(\bmod 191)$，$c_q=c=-65(\bmod 199)$，则 $(m)_2=(c_p-c_q)_2=10110010$。

2.3 性能分析

本文提出的公钥密码算法加密只需要计算 $c=a_1m_1+\cdots+a_nm_n$。因此，只需要进行 $O(n)$ 个加法运算。而在解密过程中，只需要两次取模运算 $c_p=c(\bmod p)$ 和 $c_q=c(\bmod q)$，取模运算实质上就是带余数除法运算，还需要一次普通的减法运算 c_p-c_q。算法在实现过程中均采用二进制表示，则此时的 c_p-c_q 就是对应的明文。据以上分析可以看出，本文的算法运算速度很快。

3　安全性分析

对于一个公钥密码算法有两种基本的攻击[15]：明文恢复攻击和私钥恢复攻击。前者是指从密文和加密函数出发来求解明文，后者是指重构密钥的构造过程，现讨论这两种攻击。

3.1 求解背包问题的攻击

下面证明，给定一个密文，攻击者必须通过密钥恢复攻击才能恢复相应的明文。为证明这一结论，假设攻击者未能获得相应的私钥信息。在这一假定

之下，我们证明，攻击者若存在一个多项式时间算法 P 以不可忽略概率能恢复出相应的明文，则给定任一背包问题，攻击者都可以以算法 P 为预言机获得该背包问题的解。

证明的基本思想如下。注意到，假设攻击者没能获取私钥信息，因此攻击者构造的多项式时间算法 P 是对私钥构造过程不敏感的。换言之，因为攻击者未掌握私钥信息，也就无从知道背包向量 $\boldsymbol{U}$ 和 $\boldsymbol{V}$ 的关系，即，$v_i = u_i - 2^{n-i}$，$i = 1,\cdots,n$，因此，多项式时间算法 P 也必定未使用密钥构造过程中的这一信息。对这一私钥信息进行类似替换，按照密钥构造过程式(1)和式(2)进行构造，同样可以重新构造一个背包问题。使用多项式时间算法 P 来求解该问题，即获得了原背包问题的解。具体证明过程如下。

任意给定一个背包问题 $s = b_1x_1 + \cdots + b_nx_n$，令背包向量 $\boldsymbol{U}^* = (u_1^*,\cdots,u_n^*) = (b_1,\cdots,b_n)$。任取整数 $e \approx (u_1^* + \cdots + u_n^*)/n$，计算向量 $\boldsymbol{V}^* = (v_1^*,\cdots,v_n^*)$，其中 $v_i^* = u_i^* - e$，$i = 1,\cdots,n$。根据式(1)和式(2)计算背包向量 $\boldsymbol{A}^* = (a_1^*,\cdots,a_n^*)$，即，随机选取两个不同的素数 p 和 q 使得

$$p > \sum_{i=1}^{n} u_i^*,\quad q > 2\max\left\{\sum_{v_i^*>0} v_i^*, -\sum_{v_i^*>0} v_i^*\right\} \tag{3}$$

而后，使用中国剩余定理计算向量 $\boldsymbol{A}^* = (a_1^*,\cdots,a_n^*)$，即

$$a_i^* \equiv u_i^* (\mathrm{mod}\, p),\quad a_i^* \equiv v_i^* (\mathrm{mod}\, q),\quad i = 1,\cdots,n \tag{4}$$

注意到多项式时间算法 P 对信息 $v_i = u_i - 2^{n-i}$，$i = 1,\cdots,n$ 和 $v_i^* = u_i^* - e$，$i = 1,\cdots,n$ 是不敏感的，因此，若多项式时间算法能以不可忽略概率求解背包问题 $s = a_1x_1 + \cdots + a_nx_n$，则 P 同样可以以不可忽略概率求解背包问题 $s^* = a_1^*x_1 + \cdots + a_n^*x_n$。

下面证明，攻击者若能用算法 P 以不可忽略概率求解背包问题 $s^* = a_1^*x_1 + \cdots + a_n^*x_n$，我们可以以 P 为一个预言机以不可忽略率概率获得原始背包问题 $s = b_1x_1 + \cdots + b_nx_n$ 的解。

注意到背包问题 $s = b_1x_1 + \cdots + b_nx_n$ 的解 $\boldsymbol{X} = (x_1,\cdots,x_n)$ 的汉明重量为 $0 \le \mathrm{Hw}(\boldsymbol{X}) \le n$，因此，可以在 $O(n)$ 的时间内穷举搜索 $\boldsymbol{X} = (x_1,\cdots,x_n)$ 的汉明重量 $\mathrm{Hw}(\boldsymbol{X})$。构造整数 $t = s - e\mathrm{Hw}(\boldsymbol{X})$，则背包问题 $s = b_1x_1 + \cdots + b_nx_n$ 与背包问题 $t = v_1^*x_1 + \cdots + v_n^*x_n$ 有公共解 $\boldsymbol{X} = (x_1,\cdots,x_n)$，这是因为

$$\begin{aligned} t &= s - e\mathrm{Hw}(\boldsymbol{X}) = \sum_{i=1}^{n} v_i^*x_i = \sum_{i=1}^{n} (u_i^* - e)x_i \\ &= \sum_{i=1}^{n} u_i^*x_i - e\mathrm{Hw}(\boldsymbol{X}) = \sum_{i=1}^{n} b_ix_i - e\mathrm{Hw}(\boldsymbol{X}) \end{aligned} \tag{5}$$

再根据中国剩余定理计算整数 s^*，$s^* \equiv s(\mathrm{mod}\, p)$，$s^* \equiv t(\mathrm{mod}\, q)$。注意到背包问题 $s^* = a_1^*x_1 + \cdots + a_n^*x_n$ 有解 $\boldsymbol{X} = (x_1,\cdots,x_n)$ 当且仅当 $s^* = a_1^*x_1 + \cdots + a_n^*x_n$ 模 p 和 q 均有解 $\boldsymbol{X} = (x_1,\cdots,x_n)$。由式(4)可知，$s = b_1x_1 + \cdots + b_nx_n = u_1^*x_1 + \cdots + u_n^*x_n (\mathrm{mod}\, p)$ 有解 $\boldsymbol{X} = (x_1,\cdots,x_n)$，这里模 p 取模 p 的非负最小剩余，$t = s - e\mathrm{Hw}(\boldsymbol{X}) = v_1^*x_1 + \cdots + v_n^*x_n (\mathrm{mod}\, q)$ 有解 $\boldsymbol{X} = (x_1,\cdots,x_n)$，此处模 q 取模 q 的绝对最小剩余。而由式(3)可知，$0 \le u_1^*x_1 + \cdots + u_n^*x_n \le u_1^* + \cdots + u_n^* < p$，于是，$s = b_1x_1 + \cdots + b_nx_n = u_1^*x_1 + \cdots + u_n^*x_n$；再者，注意到

$$\begin{aligned} -\frac{q}{2} &< -\max\left\{\sum_{v_i^*>0} v_i^*, -\sum_{v_i^*<0} v_i^*\right\} \le \sum_{i=1}^{n} v_i^*x_i \\ &\le \max\left\{\sum_{v_i^*>0} v_i^*, -\sum_{v_i^*<0} v_i^*\right\} < \frac{q}{2} \end{aligned}$$

我们就有 $t = s - e\mathrm{Hw}(\boldsymbol{X}) = v_1^*x_1 + \cdots + v_n^*x_n$。根据式(5)可知，$s = b_1x_1 + \cdots + b_nx_n = u_1^*x_1 + \cdots + u_n^*x_n$ 与 $t = s - e\mathrm{Hw}(\boldsymbol{X}) = v_1^*x_1 + \cdots + v_n^*x_n$ 同解。因此，$\boldsymbol{X} = (x_1,\cdots,x_n)$ 是 $s^* = a_1^*x_1 + \cdots + a_n^*x_n$ 的解的充要条件是 $\boldsymbol{X} = (x_1,\cdots,x_n)$ 也是 $s = b_1x_1 + \cdots + b_nx_n$ 的解。因此，如果存在多项式时间算法能够求解背包问题 $s^* = a_1^*x_1 + \cdots + a_n^*x_n$，则可以在多项式时间算法内获得原始背包问题 $s = b_1x_1 + \cdots + b_nx_n$ 的解。

以上证明了这样一个事实，若存在多项式时间算法 P 使得 P 对私钥信息 $v_i = u_i - 2^{n-i}$，$i = 1,\cdots,n$，不敏感，且 P 能够以不可忽略概率攻破该公钥密码的单向性，则给定任一背包问题 $s = b_1x_1 + \cdots + b_nx_n$，我们均可模拟密钥生成过程构造一个新的背包问题 $s^* = a_1^*x_1 + \cdots + a_n^*x_n$，以多项式时间算法 P 为预言机，穷举搜索背包问题 $s = b_1x_1 + \cdots + b_nx_n$ 解的汉名重量，访问 $O(n)$ 次该预言机就可以获得原始背包问题 $s = b_1x_1 + \cdots + b_nx_n$ 的解。考虑到背包问题的 NP 完全性，求解任意背包问题是不可能存在多项式时间算法的，因此，可以断定，给定密文，攻击者不掌握私钥信息 $v_i = u_i - 2^{n-i}$ 是无法通过直接求解背包问题来获得相应的明文的。因此，该密码算法可以抵抗所有通过直接求解背包问题而发起的攻击的，这些攻击包括低密度攻击[9]以及联立丢番图逼近攻击[10]等。

3.2 密钥恢复攻击

3.1 节的讨论说明给定密文 $c = a_1m_1 + \cdots + a_nm_n$，攻击者通过直接求解背包问题 $c = a_1m_1 + \cdots + a_nm_n$ 来获得明文 $(m)_2 = m_1\cdots m_n$ 是计算上不可行的。对攻击者来说，唯一的方法就是获得私钥信息 $\boldsymbol{U} = (u_1,\cdots,u_n)$ 和 $\boldsymbol{V} = (v_1,\cdots,v_n)$，其中 $v_i = u_i - 2^{n-i}$，$i = 1,\cdots,n$。此时，攻击者仅掌握公钥 $\boldsymbol{A} = (a_1,\cdots,a_n)$。

下面证明攻击者若能够获得私钥信息 $\boldsymbol{U}=(u_1,\cdots,u_n)$ 和 $\boldsymbol{V}=(v_1,\cdots,v_n)$ 当且仅当他能够获得模 $N=pq$ 和 N 的素因子 p 和 q 的值。

先证明充分性。攻击者若能够找到整数 N 并且把 N 分解成 $N=pq$ 的形式，则根据密钥的构造过程，即式(2)，就有，$u_i\equiv a_i(\bmod p)$，$v_i\equiv a_i(\bmod q)$，$i=1,\cdots,n$。因此攻击者就能够获得私钥信息 $\boldsymbol{U}=(u_1,\cdots,u_n)$ 和 $\boldsymbol{V}=(v_1,\cdots,v_n)$。

再看必要性，攻击者若能够获得私钥信息 $\boldsymbol{U}=(u_1,\cdots,u_n)$ 和 $\boldsymbol{V}=(v_1,\cdots,v_n)$，攻击者已经知道公钥信息 $\boldsymbol{A}=(a_1,\cdots,a_n)$。根据密钥构造过程的式(2)，就有，$p$ 能整除所有的 a_i-u_i，$i=1,\cdots,n$。因此，p 是所有 a_i-u_i 的最大公因数。可以使用欧几里德算法求解出所有 a_i-u_i，$i=1,\cdots,n$ 的最大公因数，即 p；同理，使用欧几里德算法可以求解出 a_i-v_i，$i=1,\cdots,n$ 的最大公因数 q。攻击者计算 $N=pq$ 则获得了模 N 的值。至此，攻击者获得了 $N=pq$ 和 N 的素因子 p 和 q 的值。

如上讨论说明了这样一个事实，攻击者若发起一个密钥恢复攻击，则攻击者必须仅依靠公开信息，即 $\boldsymbol{A}=(a_1,\cdots,a_n)$，找到模 N 的值，并且能够分解整数 $N=pq$。这是不可能的，首先，模数 N 的值是不公开的，公钥 $\boldsymbol{A}=(a_1,\cdots,a_n)$ 只能透露模 N 的数的二进制长度大小，并不足以透露 N 的值；其次，整数分解本身就是一个困难问题，则分解 N 也是计算上不可行的。

3.3 改进算法

我们可以对该密码进行改进，对密钥信息进一步进行隐藏。在密钥生成阶段，随机选取 $\boldsymbol{U}=(u_1,\cdots,u_n)$ 和 $\boldsymbol{V}=(v_1,\cdots,v_n)$，其中 $v_i=u_i-2^{n-i}$，$i=1,\cdots,n$ 之后，随机生成一个 2 阶的元素均为整数的可逆矩阵 $\boldsymbol{W}$，并记其逆为 $\boldsymbol{W}^{-1}$。然后计算 $(\boldsymbol{G},\boldsymbol{H})^{\mathrm{T}}=\boldsymbol{W}(\boldsymbol{U},\boldsymbol{V})^{\mathrm{T}}$ 获得向量 $\boldsymbol{G}=(g_1,\cdots,g_n)$ 和 $\boldsymbol{H}=(h_1,\cdots,h_n)$。随机选取素数 p 和 q 满足，$p>2\max\left\{\sum_{g_i>0}g_i,-\sum_{g_i<0}g_i\right\}$，$q>2\max\left\{\sum_{h_i>0}h_i,-\sum_{h_i<0}h_i\right\}$。使用中国剩余定理计算向量 $\boldsymbol{A}=(a_1,\cdots,a_n)$，$0\le a_i\le pq-1$，即，$a_i\equiv g_i(\bmod p)$，$a_i\equiv h_i(\bmod q)$，$i=1,\cdots,n$。公开 $\boldsymbol{A}$ 为公钥，保存 p 和 q 以及 $\boldsymbol{W}^{-1}$ 为私钥。

n 比特长的二进制明文 $(m)_2=m_1\cdots m_n$，其中 $m_i=0$ 或 1，被加密为 $c=a_1m_1+\cdots+a_nm_n$。

解密过程为，首先计算 $c_p=c(\bmod p)$，$c_q=c(\bmod q)$，这里 c_p 和 c_q 取模 p 和的绝对最小剩余。计算 $(s_p,s_q)^{\mathrm{T}}=\boldsymbol{W}^{-1}(c_p,c_q)^{\mathrm{T}}$，则明文 $(m)_2=(s_p-s_q)_2$。

解密正确性我们不再证明。这里指出的是，对原始算法进行了 $(\boldsymbol{G},\boldsymbol{H})^{\mathrm{T}}=\boldsymbol{W}(\boldsymbol{U},\boldsymbol{V})^{\mathrm{T}}$ 变换之后，对私钥向量 $\boldsymbol{U}=(u_1,\cdots,u_n)$ 和 $\boldsymbol{V}=(v_1,\cdots,v_n)$ 的关系 $v_i=u_i-2^{n-i}$，$i=1,\cdots,n$ 进行了更深一层的掩盖，因此，改进的算法会具有更高的抗密钥恢复攻击的安全强度。

3.4 安全性评述

需要指出的是，虽然我们证明了攻击者在不掌握私钥信息的情况下直接求解密文是计算上不可行的，而且攻击者能够恢复私钥信息 $\boldsymbol{U}=(u_1,\cdots,u_n)$ 和 $\boldsymbol{V}=(v_1,\cdots,v_n)$ 的充要条件是攻击者能够获得模数 N 的素因子 p 和 q，本文的背包公钥密码并不满足可证明安全性目标。事实上，目前已知的可证明安全的公钥密码大都是基于整数分解问题或离散对数问题。目前国际上对新型快速公钥密码算法的安全性的讨论仍然是讨论该密码是否抵抗已有的攻击和潜在的攻击。对这一类非传统的不基于整数分解和离散对数的公钥密码的安全性讨论仍然集中于底层的数学问题的困难性和私钥恢复的困难性上。

4　结束语

针对原有背包密码使用易解背包问题而带来的缺陷，构造了一个基于随机背包问题的公钥密码。针对明文恢复攻击和私钥恢复攻击攻击模式，均证明了攻击者均是计算上不可行的。给出了一个改进方案，改进方案对密钥的构造过程进一步伪装。对该密码算法效率方面的分析显示，该公钥密码算法的加解密速度快，只需要模加法和减法运算即可完成加解密功能。

参 考 文 献

[1] 姜正涛，张京良，王育民. 一种新的等价于大整数分解的公钥密码体制研究[J]. 电子与信息学报，2008, 30(6): 1450-1452.
Jiang Zheng-tao, Zhang Jing-liang, and Wang Yu-min. Research on a new public key cryptosystem as secure as integer factorization[J]. *Journal of Electronics & Information Technology*, 2008, 30(6): 1450-1452.

[2] 杨军，周贤伟. 基于离散对数问题的两层分散式组密钥管理方案[J]. 电子与信息学报, 2008, 30(6): 1457-1461.
Yang Jun and Zhou Xian-wei. A two-level decentralized group key management scheme based on the discrete logarithm problem[J]. *Journal of Electronics & Information Technology*, 2008, 30(6): 1457-1461.

[3] Merkle R C and Hellman M E. Hiding information and signatures in trapdoor knapsacks[J]. *IEEE Transactions on Information Theory*, 1978, 24(5): 525-530.

[4] 杨健，杜增吉，乔军. 基于 Rabin 算法的超递增背包公钥密码体制的研究与改进[J]. 数学的实践与认识，2009, 39(2):

109–114.

Yang Jian, Du Zeng-ji, and Qiao Jun. The study in knapsack of public-key system based on Merkle-Hellman knapsack system and Rabin algorithm[J]. *Mathematics in Practice and Theory*, 2009, 39(2): 109–114.

[5] 张卫东，王保仓，胡予濮. 一种新的背包型公钥密码[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[J]. *Journal of Xidian University*, 2009, 36(3): 506–511.

[6] Murakami Y and Nasako T. A new trapdoor in knapsack public-key cryptosystem with two sequences as the public key[C]. The Third International Conference on Convergence and Hybrid Information Technology-ICCIT 2008, Busan, Korea 2008: 357–362.

[7] Su P and Tsai C. New cryptosystems design based on hybrid-mode problems[J]. *Computers and Electrical Engineering*, 2009, 35(3): 478–484.

[8] Hwang M, Lee C, and Tzeng S. A new knapsack public-key cryptosystem based on permutation combination algorithm[J]. *International Journal of Applied Mathematics and Computer Sciences*, 2009, 5(1): 33–38.

[9] 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.

[10] Lagarias J C. Knapsack public key cryptosystems and Diophantine approximation[C]. Advances in Cryptology-CRYPTO 1983, New York: Plenum, 1984: 3–23.

[11] Nguyen P and Stern J. Merkle-Hellman revisited: a cryptanalysis of the Qu-Vanstone cryptosystem based on group factorizations[C]. Advances in Cryptology-Crypto 1997, Berlin: Springer-Verlag, 1997, LNCS 1294: 198–212.

[12] Brickell E F and Odlyzko A M. Cryptanalysis: A survey of recent results[C]. Contemporary Cryptology, The Science of Information Integrity, New York, IEEE Press, 1992: 501–540.

[13] Nasako T, Murakami Y, and Kasahara M. Security of a class of knapsack public-key cryptosystems against low-density attack[J]. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 2008, E91-A(10): 2889–2892.

[14] Youssef A M. Cryptanalysis of a knapsack-based probabilistic encryption scheme[J]. *Information Sciences*, 2009, 179(18): 3116–3121.

[15] Koblitz N. Algebraic Aspects of Cryptography[M]. Berlin: Springer-Verlag, 1998: 44–45.

王保仓： 男，1979 年生，副教授，博士，研究方向为公钥密码学.

韦永壮： 男，1977年生，副教授，博士，研究方向为密码函数与分组密码.

胡予濮： 男，1956年生，教授，博士生导师，研究方向为密码学与信息安全.