对陷门单向函数加密模型的新思考

陈 原,肖国镇,王育民
(西安电子科技大学 ISN 综合业务网国家重点实验室,陕西西安 710071)

摘 要: NTRU 公钥密码体制的陷门单向函数与以往的有所不同,其单向性依赖于会话密钥的随机性,且解密不需要知道有关随机会话密钥的任何信息. 有人把它称为概率陷门单向函数,但不能完全体现特殊性. 为此提出了具有辅助随机变量的陷门单向函数这一概念,用它可以统一概率公钥加密的陷门单向函数模型. 最后将该定义推广到了多元的情况,并讨论了可能的用途.

关键词: 陷门单向函数; 公钥加密; NTRU; 具有辅助随机变量的陷门单向函数
中图分类号: TN918.1 **文献标识码**: A **文章编号**: 0372-2112 (2005) 04-0752-03

A New Consideration on the Trapdoor One-Way Function Encryption Model

CHEN Yuan, XIAO Guo-zhen, WANG Yu-min
(*National Key Lab. of Integrated Service Network, Xidian University, Xi'an, Shaanxi* 710071, *China*)

Abstract: The trapdoor one-way function in NTRU is different from previous ones. Its one-wayness depends on the randomness of session keys, and decryption needs not any information about the session key. Someone called this kind of functions as "probabilistic" trapdoor one-way function. We believe this cannot show all the particularities. So we proposed a new notion, i.e. trapdoor one-way function with an auxiliary random variable, by which we can also unify the trapdoor one-way function model of probabilistic public key encryptions. The concept has been extended to the situation of higher dimension, and possible use has been discussed finally.

Key words: trapdoor one-way function; public-key encryption; NTRU; trapdoor one-way function with an auxiliary random variable

公钥加密体制自提出以来,得到了广泛的重视. 从开始的确定性加密到现在的概率加密[1],陷门单向函数加密模型是最基本的设计模式. 但是 NTRU 公钥密码体制的出现[2],使得我们开始重新考虑陷门单向函数加密模型,因为它的陷门单向函数与以往的有太多不同之处.

1 公钥加密的陷门单向函数模型

由于确定性加密安全性水平太低,实际中使用的公钥加密大都是概率型的[1]. 它的一般模型,即模型 I,由三个算法组成(本文中如不特殊说明算法均为多项式时间的):

(1) 概率密钥生成算法 G:输入安全参数 1^k,输出 (e, d), e 是公钥, d 是私钥.

(2) 概率加密算法 E:输入安全参数 1^k,对 $m \in M$, $e \in G(1^k)$,输出密文 c.

(3) 确定性解密算法 D:对 $c \in E(1^k, e, m)$, $d \in G(1^k)$,输出 m',满足 $Prob(m' \neq m)$ 可忽略.

注 1: 1^k 表示 k 的一元编码.

注 2:当算法输入 1^k 时,表明它的输出是随机的,也称其是概率算法.

注 3:函数 $\mu: N \to R$ 是可忽略的,如果对任意的正多项式 $p(\cdot)$,存在一个 N,使得对所有 $n > N$,有 $\mu(n) < 1/p(n)$.

注 4:有时解密算法 D 也可以是概率的,譬如可否认加密.

概率公钥加密一般也由陷门单向函数实现,大多数流行的方案都以此实现,譬如 RSA 等,它的模型,即模型 II 为:

(1) 生成算法 G:输入安全参数 1^k,输出一对 (f, t_f), f 是陷门单向函数, t_f 是与之相关的陷门信息.

(2) 概率加密算法 E:输入安全参数 1^k,对 $m \in M$, $E(1^k, f, m) = f(1^k, m)$.

(3) 确定性解密算法 D:给定 $c \in E(1^k, f, m)$ 和 t_f,

$$D(t_f, c) = f^{-1}(c) = f^{-1}(f(1^k, m)).$$

2 NTRU 及其特殊性

2.1 NTRU 公钥密码体制

NTRU 公钥密码体制[2]为我们提供了一个新视角,它的陷门单向函数与以往有所不同,下面将简要介绍 NTRU 公钥密码体制.

Z 为整数环、Z_q 为模 q 整数环,其中的元在 $(-\frac{q}{2}, \frac{q}{2}]$ 之

收稿日期:2003-04-23;修回日期:2005-01-31
基金项目:"十五"军事通信预研项目(No. 41001040102)

内、$R = Z_q[X]/(X^N - 1)$ 表示所有系数在 Z_q 内、次数不超过 N 的多项式之集.

设 $f \in R$, $f = \sum_{i=0}^{N-1} f_i X^i = (f_0, f_1, \cdots, f_{N-1})$, 定义 $(f * g)_k \triangleq \sum_{i+j \equiv k \bmod n} f_i g_j$.

密钥生成:随机选取 $f \in L_f$, $g \in L_g$, 要求 f 有模 p、模 q 逆, 分别记为 F_p, F_q, 则公钥为 $h \equiv F_q * g \pmod q$, 私钥为 f 和 F_p.

加密:随机选取 $\phi \in L_\phi$, 密文 $e \equiv p\phi * h + m \pmod q$.

解密:计算 $a \equiv f * e \pmod q \equiv f * m + p\phi * g \pmod q$, 正确选择参数空间使 $f * m + p\phi * g \pmod q = f * m + p\phi * g$, 再计算 $F_p * a \pmod p$ 即得 m.

NTRU 的参数选择由于篇幅所限本文不做介绍.

2.2　NTRU 陷门单向函数的特殊性

NTRU 显然满足概率公钥加密模型, 但是它却不满足概率公钥加密的陷门单向函数模型. 因为在模型 II 中生成算法无法输出一个确定的陷门单向函数, 在 ϕ 固定的情况下, NTRU 不是陷门单向函数, 只是一般非单向函数. $p\phi * h$ 此时是确定的, 如果 $e \equiv p\phi * h + m \pmod q$, 那么 $m \equiv ((e - p\phi * h) \pmod q) \pmod p$. 也就是说, NTRU 的单向性依赖于 ϕ 的随机性, 这显然与以往的陷门单向函数不同, 譬如 RSA 等, 在会话密钥确定的情况下虽然会影响安全性, 但它们仍然是单向的.

不仅如此, 我们看到 NTRU 中 ϕ 和 m 是处于不同的地位的, 在不知道 ϕ 的情况下, 陷门信息拥有者可以直接得到 m, 在得到 m 之前, 一定不能得到 ϕ. 这与以往的加密方案也有所不同, 它们都需要将会话密钥以某种形式传给解密者, 譬如 RSA-OAEP[3]、Cramer-Shoup[4] 等.

3　具有辅助随机变量的陷门单向函数及相应的加密模型

有人把 NTRU 的陷门单向函数称为概率陷门单向函数[5], 它不是一个函数, 而是一个函数族 $\{f_r\}_{r \in R}$, R 是随机会话密钥的取值范围. 公钥加密的概率陷门单向函数模型由于篇幅所限本文不再赘述, NTRU 满足该模型. 但是概率陷门单向函数只能体现出"概率单向性", 并不能表明当随机会话密钥确定时函数并非单向, 且解密不需要知道有关它的任何信息的含义.

因为在 NTRU 的陷门单向函数中 r 和 m 的地位不同, 所以我们将这种陷门单向函数记为 $f(r; m)$, "; "前表示随机变量, "; "后表示一般变量, 并称其为具有辅助随机变量的陷门单向函数, "; "前的变量称为辅助随机变量, "; "后的变量为一般变量. 它的具体定义可以如下给出:

定义 1　(具有随机变量的陷门单向函数):称一个函数 $f(r; m)$, $r \in R$, $m \in M$, 是一个具有辅助随机变量的陷门单向函数, 若它满足以下两条性质:

1° 辅助陷门单向性:当 r 是 R 上的随机变量时(即 r 对敌手不确定), f 是陷门单向函数, 其对应的陷门信息为 t_f; 而当 r 对敌手确定时, f 并非单向.

2° r 处于辅助地位:知道陷门信息 t_f 的任何敌手, 不需要知道有关 r 的任何信息, 就可由 $f(r; m)$ 求得 m. 求出 m 后可以求出 r, 但在得到 m 前得不到 r.

这种陷门单向函数完全不同于经典的 RSA 或基于离散对数问题构造的陷门单向函数, 用它可以大大地扩展构造概率公钥加密的方法, 这只需要将模型 II 中的一般陷门单向函数换作具有随机变量的陷门单向函数. 这与概率陷门单向函数加密模型不同, 密钥生成算法中不必生成一族函数, 这也是我们引入它的原因之一, 即统一了公钥加密的陷门单向函数模型.

4　具有辅助随机向量的多元陷门单向函数

事实上, 具有辅助随机变量的陷门单向函数这一概念的提出, 还有助于考虑多元的陷门单向函数. 因为我们也可以把具有辅助随机变量的陷门单向函数 $f(r; m)$ 看作是二元陷门单向函数, 只是对自变量做了一些限制. 人们大多认为二元或多元的陷门单向函数复杂性太高, 或者计算不方便, 比用一个一元陷门单向函数加密多次花销大, 但是如果把 NTRU 看作二元陷门单向函数, 就表明多元陷门单向函数也具有良好的应用前景.

把具有辅助随机变量的陷门单向函数推广到多维的情况, 得到具有辅助随机向量的多元陷门单向函数. 虽然尚不能找到这种函数, 但可以假设它们存在.

定义 2　(具有辅助随机向量的多元陷门单向函数):称一个函数 $f(\mathrm{r}; \mathrm{m})$ 是具有辅助随机向量 r 的 $|\mathrm{m}|$ 元陷门单向函数, r 是一个随机向量 $(r_1, \cdots, r_{|\mathrm{r}|})$, $|\mathrm{r}|$ 是 r 的维数, $\mathrm{m} = (m_1, \cdots, m_{|\mathrm{m}|})$, $|\mathrm{m}|$ 表示 m 的元数, 若 $f(\mathrm{r}; \mathrm{m})$ 满足以下三个条件:

1° 辅助陷门单向性:当 r 是一个随机向量时, $f(\mathrm{r}; \mathrm{m})$ 是一个 $|\mathrm{m}|$ 元陷门单向函数, 其对应的陷门信息为 t_f; 而当 r 对敌手是确定的时, $f(\mathrm{r}; \mathrm{m})$ 不是单向的.

2° r 处于辅助地位:知道陷门信息 t_f 的任何敌手, 不需要知道有关 r 的任何信息量, 就可以由 $f(\mathrm{r}; \mathrm{m})$ 求得 m. 求出 m 后可以求出 r, 但在求出 m 之前一定不能先求出 r.

3° r 的完整性:如果敌手知道 r 所取的值, 则 m 也完全暴露了, 但是如果敌手只知道 r 的一些分量所取的值, 则不能得到 m.

当然该定义可能还有疏漏之处(譬如说, 知道 r 的一些分量所取的值是否会暴露 m 的某些分量), 原因在于我们目前还没有找到这样的函数, 有一些性质暂时无法描述. 这种函数在密码学中有一定的用途. 为此, 我们将对两个极端的例子进行简单地讨论.

如果 $|\mathrm{r}| = 1$, $|\mathrm{m}| = n$, 也就是说得到的函数是 $f(r; m_1, \cdots, m_n)$, 这样就可以用一个会话密钥一次加密 n 个消息. 解密者不需要知道 r, 就可以由陷门信息恢复 $m_1, \cdots, m_n$, 这可以是并行地分别恢复 $m_1, \cdots, m_n$, 也可以是恢复出 $m_1, \cdots, m_i$, 才能恢复 m_{i+1}, 从而得到 $m_1, \cdots, m_n$, 就相当于"层层剥开"的效果. 不管怎样, 这样的函数都能在密码学中找到合适的用途.

如果| r| = n,| m| = 1,也就是说得到的函数是 $f(r_1, \cdots, r_n; m)$,这样的函数至少可以增大密文空间,即增大密文的不确定性.而且该函数可以用于构造(有仲裁的)秘密共享方案.

5 小结

本文研究了 NTRU 陷门单向函数的特殊性,提出了一种新的陷门单向函数定义,从而拓宽了概率公钥加密的模型,如果能够找到其他的此类函数实例,必将在实际中有重要用途.

参考文献:

[1] S Goldwasser, S Micali. Probabilistic encryption[J]. Computer and System Sciences, 1984, 28(2): 270 - 299.

[2] J Hoffstein, J Pipher, J H Silverman. NTRU: A ring based public key cryptosystem[A]. ANTS'3, LNCS 1423[C]. Berlin: Springer-Verlag, 1998. 267 - 288.

[3] M Bellare, P Rogaway. Optimal asymmetric encryption-how to encrypt with RSA[A]. Eurocrypt'94: LNCS 950[C]. Berlin: Springer - Verlag, 1994. 92 - 111.

[4] R Cramer, V Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack[A]. Crypto'98: LNCS 1462[C]. Berlin: Springer-Verlag, 1998. 13 - 25.

[5] Phong Q Nguyen, D Pointcheval. Analysis and improvements of NTRU encryption paddings [A]. Crypt'2002: LNCS 2442 [C]. Berlin: Springer-Verlag, 2002. 210 - 225.

[6] O Goldreich. Foundations of Cryptography: Basic Tools[M]. New York: Cambridge University Press, 2001.

作者简介:

陈 原 女,1978 年出生于新疆阿克苏,博士研究生,主要研究方向为信息安全和密码学. E-mail: didy_chen@tom.com

肖国镇 男,1934 年出生于吉林四平,教授,博士生导师,主要研究方向为信息论、编码学和密码学.

王育民 男,1936 年出生于北京,教授,博士生导师,主要研究方向为信息论、编码与密码、网络安全.