Paillier 陷门函数的两个变体的比特安全性分析

苏 东 王 克 吕克伟
(中国科学院研究生院信息安全国家重点实验室 北京 100049)

摘 要 文中对 Paillier 陷门函数两个变体——Rabin-Paillier 和 RSA-Paillier 进行了比特安全分析. 对于 Rabin-Paillier 陷门函数,文中证明了从密文计算其明文的$\lceil 3\sqrt{2n}/2\rceil+\lceil\log 2n\rceil$个最高有效位与对这个函数求逆一样困难,其中 n 为 RSA 模数 N 的二进制长度. 该结论的证明基于 Boneh 等人提出的素数域上的隐藏数问题的一个变体. 文中使用 Malykhin 在 2007 年得到的指数和的界把该变体扩展到了 Paillier 模数 N^2 的情况. 对于 RSA-Paillier 陷门函数,该文完善了 Morillo 等人对于该函数明文最低有效位的困难性证明. 通过设计一个随机化的算法使得 Morillo 等人提出的明文恢复算法在使用不完美的 LSB 预言机的时候也能工作.

关键词 比特安全;Paillier;Rabin-Paillier;RSA-Paillier;指数和的界;隐藏数问题
中图法分类号 TP309 **DOI 号**: 10.3724/SP.J.1016.2010.01050

The Bit Security of Two Variants of Paillier Trapdoor Function

SU Dong WANG Ke LV Ke-Wei
(*State Key Laboratory of Information Security, Graduate University of Chinese Academy of Sciences, Beijing* 100049)

Abstract This paper gives the bit security analysis of two variants of Paillier's trapdoor function, Rabin-Paillier and RSA-Paillier. For Rabin-Paillier trapdoor function, it is shown that computing the $\lceil 3\sqrt{2n}/2\rceil+\lceil\log 2n\rceil$ most significant bits (MSB) of its plaintext is as hard as inverting this function. The proof is based on a variant of Hidden Number Problem (HNP) over prime field introduced by Boneh et al. The authors extend this variant to Paillier modulus N^2 case by using a new bound of exponential sum given by Malykhin in 2007. For the RSA-Paillier trapdoor function, the authors complete Morillo et al.'s proof on the hardness of the least significant bit of plaintext, and devise a randomization procedure to make their algorithm workable in an imperfect oracle case.

Keywords bit security; Paillier; Rabin-Paillier; RSA-Paillier; bounds of exponential sums; hidden number problem

1 引 言

单向(陷门)函数的存在是现代密码学的基础. 称一个函数是单向的,如果它是求值容易而求逆困难. 与单向函数紧密相关的一个概念是 hard-core 谓词,是由 Blum 和 Micali[1] 在 1984 年提出的. 一个多项式时间算法 $B:\{0,1\}^*\rightarrow\{0,1\}$ 被称为是单向函数 f 的 hard-core 谓词,如果已知可计算的函数 $f(x)$,对于任意的有效算法,它猜对 $B(x)$ 的概率仅比 1/2 多出一个可忽略的量. 换句话说,如果 x 是随机选取的,即使已知 $f(x)$,$B(x)$ 也是随机的. Blum

收稿日期:2010-01-25;最终修改稿收到日期:2010-05-18. 本课题得到国家自然科学基金(60970154)与国家"九七三"重点基础研究发展规划项目基金(2007CB311202)资助.苏 东,男,1982 年生,硕士研究生,研究方向为公钥密码学与计算机安全. E-mail: sudong.tom@gmail.com. 王 克,男,1985 年生,硕士研究生,研究方向为公钥密码学. 吕克伟,男,1970 年生,博士,副教授,研究方向为公钥密码学、密码协议.

和 Micali[1] 证明了对于有限域 $\mathbb{F}_p$ 和其乘法群 $\mathbb{F}_p^*$ 的生成元 g，离散指数函数的 $\mathrm{Exp}(x)=g^x \bmod p$ 的输入 x 的最高有效位(Most Significant Bit，MSB)是一个 hard-core 谓词，这就把离散指数函数的求逆问题归约到以不可忽略的优势猜测 x 的最高有效位上. 在 1988 年，Alexi、Chor、Goldreich 和 Schnorr[2] 证明了 RSA/Rabin 加密消息的最低有效位(Least Significant Bit，LSB)是一个 hard-core 谓词. 在 2000 年，Fischlin 和 Schnorr[3] 给出了一个更为高效的 RSA/Rabin 函数求逆算法. Håstad 和 Näslund[4] 证明了 RSA/Rabin 加密消息的所有比特都单独是 hard-core 比特. 而在 1989 年，Goldreich 和 Levin[5] 证明了每个单向函数都有一个 hard-core 谓词. 尽管已经有这样的一般性结果，对于特定的单向函数，依然有必要寻找它们的 hard-core 谓词.

在 1999 年欧密会上，Paillier[6] 提出了一个 $\mathbb{Z}_{N^2}^*$ 上新的同态陷门置换 $P_{N,g}(\cdot,\cdot)$，其中 N 为 RSA 模数，g 为 $\mathbb{Z}_{N^2}^*$ 中阶为 N 非零整数倍的元素. 他使用该置换构造了一个概率公钥加密方案. 为了加密一个消息 $c\in\mathbb{Z}_N$，先选择一个随机的整数 $y\in\mathbb{Z}_N^*$ 然后计算 $w=g^c y^N \bmod N^2$. c 被称为 w 相对于 N 和 g 的类(Class)，记作 $Class_{N,g}(w)$. 文献[6]已证明，如果已知 N 的分解，计算 $Class_{N,g}(w)=c$ 是容易的. 对于 N 和 g，Paillier 定义了计算合数剩余类问题，记作 Class$[N,g]$. 此问题是，已知 N,g 和 w，计算类 c. Paillier 假定这个问题是困难的，称作计算合数剩余类假设. 为了方便起见，也把它称作标准 Paillier 假设. Paillier 单向陷门函数的一个重要性质是同态性，即

$$P_{N,g}(c_1,y_1)P_{N,g}(c_2,y_2)\equiv P_{N,g}(c_1+c_2,y_1y_2)\bmod N^2.$$

该性质使得 Paillier 单向陷门函数在构造密码协议方面有着广泛的用途. 在 2001 年，Catalano，Gennaro 和 Howgrave-Graham[7] 分析了 Paillier 陷门函数的比特安全性并且证明了在假设计算合数剩余类是困难的情况下，类 c 的 LSB 是一个 hard-core 谓词. 他们也证明了 Paillier 陷门函数同时隐藏了 $n-b$(或者说 $O(n)$)个类比特. 这一同时安全性的结论所基于的假设是：如果 $c<B=2^b$，从随机的 $w\in\mathbb{Z}_{N^2}^*$ 计算 c 依然是困难的. 这个假设也被称为 B-困难假设，它比标准 Paillier 假设要强.

在 2001 年，Catalano、Gennaro、Howgrave-Grahm 和 Nguyen[8] 提出了 Paillier 陷门函数的一个高效的变体，称为 RSA-Paillier 陷门函数. 它是基于置换

$$E_{N,e}:\mathbb{Z}_N^*\times\mathbb{Z}_N\to\mathbb{Z}_{N^2}^*,$$

$$E_{N,e}(r,m)\equiv r^e(1+mN)\bmod N^2,$$

其中 N 为两个等长的不相同的大素数的乘积，$e\in\mathbb{Z}_N$，$gcd(e,\lambda(N^2))=1$. 为了加密消息 $m\in\mathbb{Z}_N$，首先选择随机数 $r\in\mathbb{Z}_N^*$，然后计算 $w=E_{N,e}(r,m)$. 对于密文 w，如果知道私钥 d 或者 N 的分解，$ed\equiv 1 \bmod \lambda(N^2)$，则可以首先算出 $r=(w \bmod N)^d$，然后计算 $m=L(wr^{-e} \bmod N^2)$. 该置换的单向性和对 RSA 函数求逆的困难性等价[9]. 基于这个置换的加密方案在选择明文攻击下的语义安全性是由判定的小 e 次剩余假设所决定的[9]. 至于同态性，RSA-Paillier 陷门函数则没有 Paillier 陷门函数那么好的性质了，

$$E_{N,e}(r_1,m_1)E_{N,e}(r_2,m_2)\neq E_{N,e}(r_1r_2,m_1+m_2)\bmod N^2.$$

但是，它还是保持了部分的同态性：

$$E_{N,e}(r,m_1)E_{N,e}(1,m_2)\equiv r^e(1+(m_1+m_2)N)\bmod N^2,$$

$$E_{N,e}(r_1,m)E_{N,e}(r_2,0)\equiv(r_1r_2)^e(1+mN)\bmod N^2.$$

对于 RSA-Paillier 陷门函数的比特安全性，Morillo、Ràfols 和 Soler[10] 首先声称该函数明文的 LSB 是一个 hard-core 比特. 然而，他们的证明是不完善的. 他们的明文恢复算法，也称为 MRS 算法，只在 LSB 预言机能够以概率 1 正确回答查询时才能工作. 因此，当预言机只能相对于随机猜测以一个不可忽略的优势正确回答 LSB 时，该函数明文的 LSB 的困难性依然是一个有待进一步研究的问题.

在 2003 年，Galindo、Mollevi、Morillo 和 Villar[11] 提出了另外一个变体，称作 Rabin-Paillier 陷门函数. 它是基于置换

$$F_{N,e}:\mathbb{Z}_N\times Q_N\to Q_{N^2},$$

$$F_{N,e}(m,r)=mN+r^{2e} \bmod N^2,$$

其中 Q_N 为模 N 的二次剩余集合，$Q_{N^2}=\{x+yN\mid x\in Q_N, y\in\mathbb{Z}_N\}$. 其中 N 为两个等长的大素数的乘积，$e\in\mathbb{Z}_N$，$gcd(e,\lambda(N))=1$. 为了加密消息 $m\in\mathbb{Z}_N$，首先选择随机数 $r\in Q_N$，然后计算 $w=F_{N,e}(m,r)$. 对于密文 w，如果知道私钥 d 和 N 的分解，$ed\equiv 1 \bmod \lambda(N)$，则可以首先算出 $r\equiv(w \bmod N)^{2^{-1}d} \bmod N$，然后计算 $r\equiv w-r^{2e} \bmod N^2$. Galindo 等人[11] 证明了它的单向性与分解 Blum 整数等价. 基于这个置换的加密方案在选择明文攻击下的语义安全性是由判定的小 $2e$ 次剩余假设所决定的[11]. 虽然在 Paillier 陷门函数变体中，Rabin-Paillier 的单向性是最强的，但是它完全丧失了同态性. 这也就限制了该变体在密码系统构造上的应用. 因此对于其比特安全性的研究来说，传统的“零化和移位”的方法也对其失

效.在本文中,我们使用研究比特安全的另一种工具——隐藏数问题,来分析 Rabin-Paillier 陷门函数的比特安全性.

隐藏数问题(Hidden Number Problem(HNP))首先由 Boneh 和 Venkatesan[12] 于 1996 年中提出.他们使用这个模型证明了在 Diffie-Hellman 密钥交换协议中,计算出秘密密钥的$O(\sqrt{n})$个 MSB 与计算出整个秘密密钥一样困难,其中 n 为素模数 p 的二进制长度.他们首先设计了一个隐藏数问题,$\mathbb{F}_p$-HNP:已知 d 个数对$(t_i, MSB_k([\alpha t_i]_p))$, $i=1,2,\cdots,d$,其中 $k>0$ 以及 $t_1\cdots t_d \in_R \mathbb{F}_p^*$,目标是恢复出隐藏数 $\alpha\in\mathbb{F}_p$.然后构造了隐藏数恢复的算法并把它应用到 Diffie-Hellman 密钥交换协议上.作为$\mathbb{F}_p$-HNP 的一个自然扩展,他们也提出了一个含有两个未知数的隐藏数问题变体,$\mathbb{F}_p$-HNP-2U:已知$(t_i, MSB_k([\alpha t_i+\beta]_p))$,$i=1,2,\cdots,d$,恢复出 $\alpha,\beta\in\mathbb{F}_p$.隐藏数问题在研究很多密码系统的安全性上发挥着重要的作用[13].在 2007 年,Garefalakis[14] 把文献[12]的模素数隐藏数问题扩展到了无平方因子合数模数(square-free composite moduli)情况.

我们的贡献

首先,对于 Rabin-Paillier 陷门函数,我们使用了 Malykhin[15] 证明的$\mathbb{Z}_{p^2}^*$子群上的指数和的界来把$\mathbb{F}_p$-HNP-2U 扩展到了 Paillier 模数 N^2 的情况.这是一个带平方因子的合数模数.然后应用这个新的隐藏数问题变体证明了计算 Rabin-Paillier 陷门函数明文的$\lceil 3\sqrt{2n}/2\rceil+\lceil\log 2n\rceil$个最高有效位和对整个函数求逆一样困难.

其次,对于 RSA-Paillier 函数,我们完善了文献[10]的关于明文 LSB 困难性的证明.通过为 RSA-Paillier 函数设计一个能够放大不完美 LSB 预言机的预测优势的随机化算法,使得文献[10]中的明文恢复算法在使用不完美的预言机时也能工作.

本文的结构

本文第 2 节简要介绍 hard-core 谓词,Paillier 加密方案、RSA-Paillier 加密方案和 Rabin-Paillier 加密方案.第 3 节给出 Rabin-Paillier 陷门函数的比特安全性分析.在第 4 节中,我们讨论 RSA-Paillier 陷门函数的比特安全性.

记号和约定

令 $a\leftarrow A$ 表示从有限集 A 中随机均匀地选取一个元素 a.对于一个整数 x,令$[x]_N\in[0,N)$记 $x \bmod N$最小的非负剩余,令 $LSB(x)$表示 x 的最低有效位,$MSB(x)$记为 x 的最高有效位.对于 $x\in\mathbb{Z}_{N^2}^*$,我们使用 $\mathrm{ord}_{N^2}(x)$来记 x 模 N^2 的乘法阶.令 N_n表示 n 比特长的合数 $N=PQ$ 的集合,其中 P 和 Q 为两个等长的大素数.令 P_n表示对$\langle N,g\rangle$的集合,其中 $N\in N_n$,并且 g 为$\mathbb{Z}_{N^2}^*$中的一个元素,它的乘法阶为 N 的非零整数倍.我们使用 log 来表示以 2 为底的对数函数.我们使用 $\varepsilon(n)$来表示一些不可忽略函数,即对于某个多项式 $p(n)$,$\varepsilon(n)>1/p(n)$.为了简单起见,我们使用 ε 来替代 $\varepsilon(n)$.我们用关系 $P_1\Rightarrow P_2$($P_1\Leftrightarrow P_2$)来表示问题 P_1 可以被多项式时间归约到(等价于)问题 P_2.按照传统,向量以列形式存在,并且用粗体小写字母表示,比如 $\boldsymbol{u}$.第 i 个分量记作 $\boldsymbol{u}_i$.向量 $\boldsymbol{u}$ 的长度可以用欧式范数表示:$\|\boldsymbol{u}\|=\sqrt{\boldsymbol{u}^{\mathrm{T}}\boldsymbol{u}}$.令 $\varphi(\cdot)$表示欧拉函数,并且令 $\lambda(\cdot)$表示 Carmichael 函数,它的定义如下

$$\lambda(n)=\begin{cases}\varphi(n), & n=p^\alpha, p=2, \alpha\le 2 \text{ 或 } p\ge 3\\ \varphi(n)/2, & n=2^\alpha, \alpha\ge 3\\ lcm(\lambda(p_1^{\alpha_1}),\cdots,\lambda(p_k^{\alpha_k})), & n=\prod_{i=1}^k p_i^{\alpha_i}\end{cases}$$

对于 $N\in N_n$以及 $\gcd(e,\varphi(N))=1$,用 $RSA_{N,e}$来表示 RSA 函数,用 RSA$[N,e]$来表示 RSA 问题.类似的,对于 $N=PQ$、$P\equiv Q\equiv 3 \bmod 4$ 以及$P\neq Q$,我们用 $Rabin_N$来表示 Rabin 函数,用 Rabin$[N]$来表示 Rabin 问题.

2 预备知识

2.1 几个基本的密码学定义

定义 1[15]. Hard-Core 谓词. 对于函数 $f:\{0,1\}^*\to\{0,1\}^*$,它的 hard-core 谓词为一个布尔谓词 $B:\{0,1\}^*\to\{0,1\}$,满足

1. $\exists$概率多项式时间算法 A,满足 $\forall x\in\{0,1\}^*$,$A(x)=B(x)$;

2. $\forall$概率多项式时间算法 G, $\forall$常数 c, $\exists k_0$,满足

$\forall k>k_0$, $\Pr[G(f(x))=B(x)]<1/2+1/k^c$.

对于一个单向函数 f,一种证明谓词 B 为 hard-core 谓词的方法是:假设存在一个高效的算法 A,它能够从 $y=f(x)$以高于 1/2 的不可忽略的概率猜出 $B(x)$的值,则我们能够构造另一个高效的算法 A′,它能够在概率多项式时间内从输入 y 以不可忽略的概率计算出 x.

2.2 Paillier 加密方案

在文献[6]中,Paillier 提出了一个新的概率加

密方案. 这一方案是基于群$\mathbb{Z}_{N^2}^*$中的运算的，其中 N 为一个 RSA 模数. 该方案是同态的，在选择明文攻击下是语义安全的，而且有高效的解密运算. 具体地说，对于$\langle N,g\rangle\in P_n$，考虑如下映射：

$$P_{N,g}:\mathbb{Z}_N\times\mathbb{Z}_N^*\to\mathbb{Z}_{N^2}^*,$$
$$P_{N,g}(c,y)=g^c y^N \bmod N^2.$$

Paillier 证明了 $P_{N,g}$为一个单向陷门置换. 陷门信息是 N 的分解. 由 P_n为双射，已知$\langle N,g\rangle\in P_n$，对于一个元素 $w\in\mathbb{Z}_{N^2}^*$，存在唯一的$(c,y)\in\mathbb{Z}_N\times\mathbb{Z}_N^*$，满足 $w=g^c y^N \bmod N^2$. c 被称为 w 相对于 N 和 g 的类，记作 $Class_{N,g}(w)$. 定义计算合数剩余类问题为已知 w 计算 c，并认为这个问题是难解的.

Paillier 加密方案的具体描述如下.

密钥生成. 已知一个安全参数 n，随机选择两个不同的 $n/2$ 比特长的素数 P 和 Q，选择一个整数 $g\in\mathbb{Z}_{N^2}^*$，满足 $N\mid \mathrm{ord}_{N^2}(g)$，则公钥为$\langle N,g\rangle$，其中 $N=PQ$；私钥是$\langle P,Q\rangle$. 我们用 $\mathrm{Paillier}_{\mathrm{pk}}(n)$来记安全参数为 n 的该方案的公钥的集合.

加密. 对于明文 $c\in\mathbb{Z}_N$，选择一个随机值 $y\in\mathbb{Z}_N^*$. 通过计算 $w=P_{N,g}(c,y)$来对 c 进行加密. 我们把这个加密过程记作 $\mathrm{PEnc}_{N,g}(c)$. y 的选择可以看作这个加密过程的随机掷币.

解密. 可以通过 $L(w^\lambda \bmod N^2)/L(g^\lambda \bmod N^2)$来从密文恢复出明文 c，其中 $L(u)=(u-1)/N$ 且 $\lambda(N)=\mathrm{lcm}(P-1,Q-1)$.

定义 2[7]. 计算剩余类的困难性. 称计算函数 $Class_{N,g}(\cdot)$是困难的，如果对于任意的概率多项式时间算法 A，都存在一个可忽略函数 $\mathrm{negl}(\cdot)$，满足

$$\Pr[\langle N,g\rangle\in\mathrm{Paillier}_{\mathrm{pk}},\ c\leftarrow\mathbb{Z}_N,y\leftarrow\mathbb{Z}_N^*;$$
$$w=g^c y^N \bmod N^2;\mathrm{A}(N,g,w)=c]\le\mathrm{negl}(n).$$

如果 $N=PQ$ 的分解已知，则函数 $Class_{N,g}(\cdot)$是可以计算的. 令 $\lambda=\lambda(N)=\mathrm{lcm}(P-1,Q-1)$，则 $Class_{N,g}(\cdot)=L(w^\lambda \bmod N^2)/L(g^\lambda \bmod N^2)$，其中 $L(u)=(u-1)/N$. 另一方面，如果 N 的分解未知，到目前为止还没有找到计算 $Class_{N,g}(\cdot)$的多项式时间算法. 因此，有如下假设.

假设 1[7]. 计算合数剩余类假设. 如果 N 的分解未知，则不存在概率多项式时间算法能够解计算合数剩余类问题.

我们把 $P_{N,g}$的单向性记为 $\mathrm{Paillier}_1[N,g]$. 这也就是计算合数剩余类的困难性，即 $\mathrm{Paillier}_1[N,g]\Leftrightarrow\mathrm{Class}[N,g]$.

上述 Paillier 加密方案也存在一个确定性的变体，即把随机掷币 y 也做成消息的一部分. 这样对于消息 $m\in\mathbb{Z}_{N^2}$，$m=m_1+m_2N$，其中 $m_2\in\mathbb{Z}_N^*$，可以通过计算 $w=g^{m_1}m_2^N \bmod N^2$来实现对 m 的加密. 把这个加密方案的单向性记作 $\mathrm{Paillier}_2[N,g]$，有如下定义.

定义 3. 对于任意的概率多项式时间算法 A，都存在一个可忽略的函数 $\mathrm{negl}(\cdot)$，使得

$$\Pr[\langle N,g\rangle\in\mathrm{Paillier}_{\mathrm{pk}},m_1\leftarrow\mathbb{Z}_N,m_2\leftarrow\mathbb{Z}_N^*;$$
$$w=g^{m_1}m_2^N \bmod N^2;\mathrm{A}(N,g,w)=(m_1,m_2)]$$
$$\le\mathrm{negl}(n).$$

Paillier[6] 也证明了，对于$\langle N,g\rangle\in\mathrm{Paillier}_{\mathrm{pk}}$，

$$\mathrm{Class}[N,g]\ \Rightarrow\ \mathrm{RSA}[N,N]\Rightarrow\mathrm{Fact}[N]$$
$$\Updownarrow\qquad\qquad\Updownarrow$$
$$\mathrm{Paillier}_1[N,g]\quad\mathrm{Paillier}_2[N,g].$$

2.3 RSA-Paillier 加密方案

在 2001 年，Catalano 等人[8]提出了 Paillier 加密方案的一个高效的变体. 其加密的效率近似于 RSA 加密方案. 他们首先定义了 RSA-Paillier 陷门函数.

定义 4[8]. RSA-Paillier 陷门函数.

$$E_{N,e}:\mathbb{Z}_N^*\times\mathbb{Z}_N\to Z_{N^2}^*,$$
$$E_{N,e}(r,m)=r^e(1+mN)\bmod N^2.$$

其中 $N=PQ$ 为 RSA 模数，$e\in\mathbb{Z}_N$，满足 $\gcd(e,\lambda(N^2))=1$ 和 $e>2$.

Catalano 等人[8]证明了 $E_{N,e}$是一个陷门置换，并且构造了如下的 RSA-Paillier 加密方案.

密钥生成. 给定一个安全参数 n，随机选择两个 $n/2$ 长的不同的素数 P 和 Q. 选择一个整数 $e\in\mathbb{Z}_N$，满足 $\gcd(e,\lambda(N^2))=1$ 且 $e>2$，则公钥是$\langle N,e\rangle$，其中 $N=PQ$. 私钥是$\langle P,Q,d\rangle$，其中 $d\in\mathbb{Z}_N^*$，满足 $ed\equiv1 \bmod\lambda(N^2)$. 用 $\mathrm{RSA\text{-}Paillier}_{\mathrm{pk}}(n)$来记安全参数为 n 的公钥集合.

加密. 对于消息 $m\in\mathbb{Z}_N$，选择一个随机值 $r\in\mathbb{Z}_N^*$，计算 $w=E_{N,e}(r,m)$.

解密. 消息 m 可以通过计算 $r=(w \bmod N)^d$和 $m=L(wr^{-e} \bmod N^2)$恢复出来.

$E_{N,e}$的单向性，记作 $\mathrm{RSA\text{-}Paillier}[N,e]$，定义如下.

定义 5. 对于任意的概率多项式时间算法 A，都存在一个可忽略的函数 $\mathrm{negl}()$，使得

$$\Pr[\langle N,e\rangle\in\mathrm{RSA\text{-}Paillier}_{\mathrm{pk}},\ m\leftarrow\mathbb{Z}_N,r\leftarrow\mathbb{Z}_N^*;$$
$$w=(1+mN)r^e \bmod N^2;\mathrm{A}(N,e,w)=m]\le\mathrm{negl}(n),$$

此外，Catalano 等人[8]定义了一个计算困难问题，称作计算小 e 次剩余问题(CSeR).

定义 6[8]. 计算小 e 次剩余问题的困难性. 对于任意的概率多项式时间算法 A,都存在一个可忽略的函数 negl(),使得

$$\Pr[\langle N,e\rangle\in \text{RSA-Paillier}_{pk}, m\leftarrow\mathbb{Z}_N, w=m^e \bmod N^2; \text{A}(N,e,w)=m]\leq \text{negl}(n).$$

Catalano 等人[8]证明了对于 $\langle N,e\rangle\in \text{RSA-Paillier}_{pk}$, $\text{CSeR}[N,e]\Leftrightarrow\text{RSA-Paillier}[N,e]\Leftrightarrow\text{RSA}[N,e]$. 此外,Catalano 等人[8]提出了 Hensel-RSA 问题,对于 $\langle N,e\rangle\in \text{RSA-Paillier}_{pk}$,已知 $c=r^e \bmod N$,计算 $r^e \bmod N^l$ for $l>1$. 更为正式地讲,他们定义了 $\mathbb{Z}_N^*$ 到 $\mathbb{Z}_{N^l}^*$ 的映射 $\text{Hensel-RSA}[N,e,l](r^e \bmod N)=r^e \bmod N^l$. 并证明了,$\text{Hensel-RSA}[N,N,3]\Leftrightarrow\text{RSA}[N,N]$ 和 $\text{Hensel-RSA}[N,N,2]\Leftrightarrow\text{Class}[N,g]$.

2.4 Rabin-Paillier 加密方案

在 2003 年,Galindo 等人[11]提出了 Paillier 陷门函数另外一个变体,称作 Rabin-Paillier 陷门函数. 他们首先定义了 Rabin-Paillier 陷门函数.

定义 7[11]. Rabin-Paillier 陷门函数

$$F_{N,e}:\mathbb{Z}_N\times Q_N\rightarrow Q_{N^2},$$

$$F_{N,e}(m,r)=mN+r^{2e} \bmod N^2,$$

其中 Q_N 为模 N 的二次剩余集合,$Q_{N^2}=\{x+yN\mid x\in Q_N, y\in\mathbb{Z}_N\}$. $N=PQ$ 为一个 RSA 模数,$e\in\mathbb{Z}_N^*$,满足 $\gcd(e,\lambda(N))=1$ 和 $e>2$.

Galindo 等人[11]证明了 $F_{N,e}$ 是一个陷门函数并且构造了如下的 Rabin-Paillier 加密方案,

密钥生成. 已知一个安全参数 n,随机选择两个不同的 $n/2$ 长的随机数 P 和 Q,满足 $P\equiv Q\equiv 3 \bmod 4$. 选择一个整数 $e\in\mathbb{Z}_N^*$,满足 $\gcd(e,\lambda(N))=1$ 和 $e>2$. 则公钥为 $\langle N,e\rangle$,其中 $N=PQ$. 私钥为 $\langle P,Q,d\rangle$,其中 $d\in\mathbb{Z}_N^*$ 和 $ed\equiv 1 \bmod \lambda(N)$. 我们用 $\text{Rabin-Paillier}_{pk}(n)$ 来记安全参数为 n 的公钥集合.

加密. 令 $m\in\mathbb{Z}_N$,选择一个随机值 $r\in Q_N$,然后计算 $w=F_{N,e}(m,r)$.

解密. 消息 m 可以通过如下计算来恢复,$t=RSA_{N,e}^{-1}(w \bmod N)$, $r=Rabin_N^{-1}(t)$, $m=(w-r^{2e} \bmod N^2)/N$.

Rabin-Paillier 方案的构造是基于 Rabin-Williams 函数的:

$$RW_{N,e}:Q_N\rightarrow Q_N,$$

$$RW_{N,e}(m)=m^{2e} \bmod N.$$

这个函数在分解假设下是陷门单向置换.

$F_{N,e}$ 单向性,记作 Rabin-Paillier$[N,e]$,可以按如下定义.

定义 8. Rabin-Paillier 陷门函数的单向性. 对于任意的概率多项式时间算法 A,都存在一个可忽略的函数 negl(),使得

$$\Pr[\langle N,e\rangle\in \text{Rabin-Paillier}_{pk}, m\leftarrow\mathbb{Z}_N, r\leftarrow Q_N; w=mN+r^{2e} \bmod N^2; \text{A}(N,e,w)=m]\leq \text{negl}(n).$$

Galindo 等人[11]也定义了 Hensel 提升问题的另外一个版本,称作 Hensel-RW 问题:对 $\langle N,e\rangle\in \text{Rabin-Paillier}_{pk}$,已知 $r^{2e} \bmod N$,对于 $l>1$,计算 $r^{2e} \bmod N^l$. 这个问题也可以记为 Hensel-RW$[N,e,l]$. 他们也证明了对于 $\langle N,e\rangle\in \text{Rabin-paillier}_{pk}$,

$$\text{Rabin-Paillier}[N,e]\Leftrightarrow \text{Hensel-RW}[N,e,2]\Leftrightarrow\text{Fact}[N].$$

我们把上文中出现的主要的困难问题总结到图 1 中. 该图蕴含了一个有意思的公开问题:Catalano 等人[9]指出问题 Class$[N,g]$ 与问题 RSA$[N,N]$ 的困难性也许并不等价. 由于 $\text{Hensel-RSA}[N,N,3]\Leftrightarrow\text{RSA}[N,N]$, $\text{Hensel-RSA}[N,N,2]\Leftrightarrow\text{Class}[N,g]$,Hensel 提升问题的第 3 个参数也许是 Class$[N,g]$ 和 RSA$[N,N]$ 困难程度的指示器.

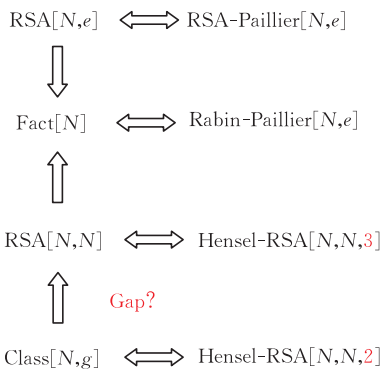

图 1 Paillier 变体困难问题之间的归约关系

3 Rabin-Paillier 陷门函数的比特安全性分析

在本节中我们使用隐藏数问题来分析 Rabin-Paillier 陷门函数的比特安全性. 对于整数 $k\geq 1$,定义 $MSB_k(t)$ 为满足下列不等式的非负整数 $(MSB_k(t)-1)N^2/2^k\leq t \bmod N^2\leq MSB_k(t)N^2/2^k$. 不正式地讲,$MSB_k(t)$ 为 $t \bmod N^2$ 的前 k 个 MSB 所对应的整数.

为了研究 Rabin-Paillier 的比特安全性,我们把隐藏数问题的变体 $\mathbb{F}_p$-HNP-2U[12] 扩展到模 N^2 的情况. 首先使用一个指数和的界的最新结果[15]和中

国剩余定理来估计分布的 $x\in\mathbb{Z}_{N^2}^*$ 均匀性，其中 $\lambda x\equiv y \bmod N^2$，$y\in[r+1,r+h]$. 剩下的就是按照文献[17]中的证明框架来构建新的隐藏数问题变体. 我们的新隐藏数问题变体的正式定义如下.

定义 9.　固定 N 和 k，对于任意的 $\alpha,\beta\in\mathbb{Z}_{N^2}^*$，令 $O_{\alpha,\beta}(\cdot)$ 为一个隐藏数预言机，输入是整数 t，输出是 $\alpha t+\beta \bmod N^2$ 的 k 个 MSB，$O_{\alpha,\beta}(t)=MSB_k(\alpha t+\beta \bmod N^2)$. 任务是利用预言机 $O_{\alpha,\beta}(\cdot)$，在期望多项式时间内计算隐藏数 $\alpha \bmod N^2$ 和 $\beta \bmod N^2$.

根据文献[12]，已知随机整数 $t_1,\cdots,t_d\in\mathbb{Z}_{N^2}^*$，首先用下述矩阵 $\boldsymbol{M}$ 来构造一个 $d+2$ 维的格 $L_{N^2}(t_1,\cdots,t_d)$，

$$\boldsymbol{M}=\begin{pmatrix} N^2 & 0 & 0 & \cdots & 0 & 0 & 0\\ 0 & N^2 & 0 & \cdots & 0 & 0 & 0\\ & \vdots & & & & \vdots & \\ 0 & 0 & 0 & \cdots & N^2 & 0 & 0\\ t_1 & t_2 & t_3 & \cdots & t_d & 1/N^2 & 0\\ 1 & 1 & 1 & \cdots & 1 & 0 & 1/N^2 \end{pmatrix}.$$

称 $\boldsymbol{M}$ 的前 d 个行向量为 N^2-向量. 这个格是整个隐藏数恢复算法的关键. 接下来，使用文献[15]给出的指数和的界来把文献[12]的模素数隐藏数问题的结论扩展到 Paillier 模数 N^2 的情况.

引理 1[15].　令 p 为一个素数，G 为 $\mathbb{Z}_{p^2}^*$ 的任意一个子群，而且 $\sharp G=t$. 记

$$S(G):=\max_{a\in\mathbb{Z}_{p^2}^*}\left|\sum_{x\in G}\exp(2\pi i ax/p^2)\right|.$$

如果 $t\geq p$，则 $S(G)=0$；否则

$$S(G)=\begin{cases}(p^7t^{26})^{1/36}, & p^{7/10}<t<p^{3/4}(\log p)^{-1},\\ p^{1/9}t^{5/6}(\log p)^{1/9}, & p^{3/4}(\log p)^{-1}<t<p^{7/9},\\ (p^5t^{17})^{1/24}(\log p)^{1/12}, & p^{7/9}<t<p^{4/5},\\ p^{3/8}t^{1/2}, & p^{4/5}<t<p.\end{cases}$$

令 $M_\lambda(r,h)$ 为方程 $\lambda x\equiv y \bmod N^2$ 的解的个数，其中 $x\in\mathbb{Z}_{N^2}^*$，$y\in[r+1,r+h]$. 下述引理表明 $M_\lambda(r,h)$ 接近于其期望值 $\varphi(N^2)h/N^2=\varphi(N)h/N$.

引理 2.　对于任意的 $\varepsilon>0$，都存在 $\delta>0$，满足界

$$\max_{0\leq r,h<N^2-1}\max_{\gcd(\lambda,N^2)=1}\left|M_\lambda(r,h)-\frac{\varphi(N)h}{N}\right|=O(N^{1-\delta}).$$

容易看出，$M_\lambda(r,h)$ 可以使用指数和来进行计数，这是因为

$$\frac{1}{m}\sum_{a=0}^{m-1}\exp(2\pi iau/m)=\begin{cases}1, & m\mid u\\ 0, & \text{否则}\end{cases}$$

其中，m 和 u 为任意整数. 我们有

$$\begin{aligned}M_\lambda(r,h)&=\frac{1}{N^2}\sum_{x\in\mathbb{Z}_{N^2}^*}\sum_{y=r+1}^{r+h}\sum_{c=0}^{N^2-1}\exp(2\pi ic(\lambda x-y)/N^2)\\&=\frac{1}{N^2}\sum_{c=0}^{N^2-1}\Big(\sum_{x\in\mathbb{Z}_{N^2}^*}\exp(2\pi ic\lambda x/N^2)\cdot\sum_{y=r+1}^{r+h}\exp(-2\pi icy/N^2)\Big).\end{aligned}$$

因此，

$$\left|M_\lambda(r,h)-\frac{\varphi(N)h}{N}\right|\leq\frac{1}{N^2}\sum_{c=1}^{N^2-1}\Big(\Big|\sum_{x\in\mathbb{Z}_{N^2}^*}\exp(2\pi ic\lambda x/N^2)\Big|\cdot\Big|\sum_{y=r+1}^{r+h}\exp(-2\pi icy/N^2)\Big|\Big).$$

如果 $\gcd(c,N^2)=1$，可以使用引理 1 中的界以及中国剩余定理来估计上述和式在 $x\in\mathbb{Z}_{N^2}^*$ 上的上界

$$\begin{aligned}&\sum_{x\in\mathbb{Z}_{N^2}^*}\exp\Big(\frac{2\pi icx}{N^2}\Big)\\&=\sum_{a\in\mathbb{Z}_{Q^2}^*}\sum_{b\in\mathbb{Z}_{P^2}^*}\exp\Big(\frac{2\pi ic(aP^2+bQ^2)}{P^2Q^2}\Big)\\&=\sum_{a\in\mathbb{Z}_{Q^2}^*}\exp\Big(\frac{2\pi ica}{Q^2}\Big)\sum_{b\in\mathbb{Z}_{P^2}^*}\exp\Big(\frac{2\pi icb}{P^2}\Big)\\&<P^{7/8}Q^{7/8}=N^{7/8}.\end{aligned}$$

在 $c\in\mathbb{Z}_N\backslash\mathbb{Z}_N^*$ 和 $y\in[r+1,r+h]$ 上的和式可以用文献[18]中第 3 章的练习 11.c 来进行估计.

$$\sum_{a=1}^{m-1}\left|\sum_{x=M(a)}^{M(a)+P(a)-1}\exp\Big(2\pi i\frac{a}{m}x\Big)\right|<m\ln m-m,\ \text{for } m>60$$

其中 m 为一个整数，$m>1$. 函数 $M(a)$ 和 $P(a)$ 取整数值，而且对于 $a=1,2,\cdots,m-1$，$P(a)>0$. 因此，

$$\begin{aligned}&\max_{0\leq r,h<N^2}\left|M_\lambda(r,h)-\frac{\varphi(N)h}{N}\right|\\&\leq\frac{1}{N^2}\Big(\sum_{c\in\mathbb{Z}_{N^2}^*}\left|\sum_{x\in\mathbb{Z}_{N^2}^*}\exp\Big(\frac{2\pi ic\lambda x}{N^2}\Big)\right|+\\&\sum_{c\in\mathbb{Z}_{N^2}\backslash\mathbb{Z}_{N^2}^*}\left|\sum_{x\in\mathbb{Z}_{N^2}^*}\exp\Big(\frac{2\pi ic\lambda x}{N^2}\Big)\right|\Big)\cdot\left|\sum_{y=r+1}^{r+h}\exp\Big(\frac{2\pi icy}{N^2}\Big)\right|\\&=\frac{1}{N^2}(\varphi(N^2)N^{7/8}(2\log N)+N(P+Q-1)(2\log N)^2)\\&=N^{7/8}\Big(1-\frac{1}{P}\Big)\Big(1-\frac{1}{Q}\Big)(2\log N)+\frac{P+Q-1}{N}(2\log N)^2\\&<O(N^{7/8}\log N)=O(N^{1-\delta}),\end{aligned}$$

其中 δ 为一个大于零的常数.　　证毕.

有了这个引理就可以证明唯一性定理了. 它的证明类似于文献[17]中引理 3.2 的证明. 为了本文的完整，我们也把全部的证明写在这里了. 稍有不同的是，要对 μ 和 k 稍加放大. 这是为了使得在新的隐藏数问题中隐藏数恢复算法的成功概率依然能够充

分地大.

定理 1. 唯一性定理. 令 $d=2\lceil\sqrt{2n}\rceil$, $\mu=\sqrt{2n}+3$, $\delta>0$. 令 $\alpha,\beta\in\mathbb{Z}_{N^2}^*$. 在 $\mathbb{Z}_{N^2}^*$ 中独立且均匀地选择整数 $t_1,\cdots,t_d$. 则对于满足

$$\Big(\sum_{i=1}^{d}((\alpha t_i+\beta)-u_i)^2\Big)^{1/2}$$

任意的向量 $\boldsymbol{u}=(u_1,\cdots,u_d,0,0)$, 满足

$$\Big(\sum_{i=1}^{d}(v_i-u_i)^2\Big)^{1/2}\le N^2 2^{-\mu}$$

的所有的向量 $\boldsymbol{v}=(v_1,\cdots,v_{d+2})\in L_{N^2}(t_1,\cdots,t_d)$ 可以至少以概率 $1-2^{-\sqrt{2n}}$ 具有形式

$\boldsymbol{v}=([\alpha' t_1+\beta']_{N^2},\cdots,[\alpha' t_d+\beta']_{N^2},\alpha'/N^2,\beta'/N^2)$, 其中 $\alpha\equiv\alpha' \bmod N^2$, $\beta\equiv\beta' \bmod N^2$.

证明. 首先定义两个整数 a 和 b 在模 N^2 下的距离

$$\begin{aligned}\mathrm{dist}_{N^2}(a,b)&=\min_{c\in Z}|a-b-cN^2|\\&=\min\{[a-b]_{N^2},N^2-[a-b]_{N^2}\}.\end{aligned}$$

令 t 为一个从 $\mathbb{Z}_N^*$ 中随机均匀选取的整数. 由引理 2 可知, 对于任意的 $a_1\neq a_2 \bmod N^2$ 和 $b_1\neq b_2 \bmod N^2$, 事件 $\mathrm{dist}_{N^2}(a_1t+b_1,a_2t+b_2)>N^2 2^{-\mu+1}$ 发生的概率为 $1-2^{-\mu+2}+O(N^{-\delta})\ge 1-5/2^{\mu}$.

因此, 对于任意的 $a_1\neq a_2 \bmod N^2$ 和 $b_1\neq b_2 \bmod N^2$,

$$\begin{aligned}&\Pr[\mathrm{dist}_{N^2}(a_1t_i+b_1,a_2t_i+b_2)\\&>N^2 2^{-\mu+1}\mid \forall a_1\neq a_2 \bmod N^2,\\&\quad b_1\neq b_2 \bmod N^2,\ \exists i\in[1,d]]\\&\ge 1-(N^2-1)(5/2^{\mu})>1-2^{-\sqrt{2n}},\end{aligned}$$

其中概率取自从 $\mathbb{Z}_{N^2}^*$ 中独立均匀选取的 d 个整数 $t_1,\cdots,t_d$.

固定整数 $t_1,\cdots,t_d$,

$$\min_{\substack{a_1\neq a_2 \bmod N^2\\ b_1\neq b_2 \bmod N^2}}\ \min_{i\in[1,d]}\mathrm{dist}_{N^2}(a_1t_i+b_1,a_2t_i+b_2)>N^2 2^{-\mu+1}\tag{1}$$

令 $\boldsymbol{v}$ 为满足 $\|\boldsymbol{v}-\boldsymbol{u}\|\le N^2 2^{-\mu}$ 的向量. 由于 $\boldsymbol{v}\in L_{N^2}(t_1,\cdots,t_d)$, 则有整数 $\alpha',\beta',z_1,\cdots,z_d$, 满足

$$\begin{aligned}\boldsymbol{v}=(&\alpha' t_1+\beta'-z_1N^2,\cdots,\alpha' t_d+\beta'-z_dN^2,\\&\alpha'/N^2,\beta'/N^2).\end{aligned}$$

如果 $\alpha\equiv\alpha' \bmod N^2$ 和 $\beta\equiv\beta' \bmod N^2$, 则对于所有的 $i=1,2,\cdots,d$, 我们有 $\alpha' t_i+\beta'-z_iN^2=[\alpha' t_i+\beta']_{N^2}$, 否则会存在一个 $j\in[1,d]$, 满足 $|v_j-u_j|>N^2 2^{-\mu}$.

现在假设 $\alpha\neq\alpha' \bmod N^2$ 和 $\beta\neq\beta' \bmod N^2$, 我们有

$$\begin{aligned}&\Big(\sum_{i=1}^{d}(v_i-u_i)^2\Big)^{1/2}\\&\ge\min_{i\in[1,d]}\mathrm{dist}_{N^2}(\alpha' t_i+\beta',u_i)\\&\ge\min_{i\in[1,d]}(\mathrm{dist}_{N^2}(\alpha' t_i+\beta',\alpha t_i+\beta)-\\&\quad\mathrm{dist}_{N^2}(\alpha t_i+\beta,u_i))\\&\ge N^2 2^{-\mu+1}-N^2 2^{-\mu}=N^2 2^{-\mu}.\end{aligned}$$

这个就与假设相矛盾了. 因此条件(1)至少可以以概率 $1-2^{-\sqrt{2n}}$ 成立. 证毕.

定理 2. 令 $d=2\lceil\sqrt{2n}\rceil$, $k=\lceil 3\sqrt{2n}/2\rceil+\lceil\log 2n\rceil$, 则存在一个确定的多项式时间算法 A, 满足对于任何整数 $\alpha,\beta\in\mathbb{Z}_{N^2}$, 已知 $2d$ 个整数

$$(t_i,s_i=MSB_k(\alpha t_i+\beta)),\ i=1,2,\cdots,d,$$

A 都能以概率

$$\Pr_{t_1,\cdots,t_d}[A(t_1,\cdots,t_d;s_1,\cdots,s_d)=(\alpha,\beta)]\ge 1-2^{-\sqrt{2n}}$$

成功地输出隐藏数 α 和 β.

证明. 本定理的证明借鉴了文献[17]中引理 3.3 的证明. 已知随机整数 $t_1,\cdots,t_d\in\mathbb{Z}_{N^2}^*$, 考虑向量 $\boldsymbol{r}=(r_1,\cdots,r_d,0,0)$, 其中 $r_i=s_iN^2/2^k$, $i=1,2,\cdots,d$. 然后把矩阵 $\boldsymbol{M}$ 的第 $(d+1)$ 行向量 $(t_1,\cdots,t_d,1/N^2,0)$ 乘上 α, 把 $\boldsymbol{M}$ 的 $(d+2)$ 行 $(1,\cdots,1,0,1/N^2)$ 乘上 β.

把上述乘法的结果减去 N^2-向量的相应倍数, 然后得到一个格点

$\boldsymbol{u}_{\alpha,\beta}=(u_1,\cdots,u_d,\alpha/N^2,\beta/N^2)\in L_{N^2}(t_1,\cdots,t_d)$, 满足 $|u_i-r_i|<N^2 2^{-k}$, $i=1,2,\cdots,d$.

现在使用文献[14]的引理 4 提到的 LLL 算法来在多项式时间内找到一个格向量 $\boldsymbol{w}=(w_1,\cdots,w_{d+2})$, 满足

$$\begin{aligned}\|\boldsymbol{w}-\boldsymbol{r}\|&\le 2^{(d+2)/4}\min\{\|\boldsymbol{z}-\boldsymbol{r}\|,\boldsymbol{z}\in L_{N^2}(t_1,\cdots,t_d)\}\\&\le 2^{(d+2)/4}N^2(d+2)^{1/2}2^{-k}\le N^2 2^{-\mu-1}\end{aligned}$$

其中 $\mu=\sqrt{2n}+3$.

由于已经有 $\|\boldsymbol{u}_{\alpha,\beta}-\boldsymbol{r}\|\le N^2 d^{1/2}2^{-k}\le N^2 2^{-\mu-1}$, 因此 $\|\boldsymbol{w}-\boldsymbol{u}_{\alpha,\beta}\|\le N^2 2^{-\mu}$. 应用定理 1, 可以以概率 $1-2^{-\sqrt{2n}}$ 得到 $\boldsymbol{w}=\boldsymbol{u}_{\alpha,\beta}$. 因此也就能够从 $\boldsymbol{w}$ 最后的两个分量得到 α 和 β. 证毕.

定理 3. 令 $k=\lceil 3\sqrt{2n}/2\rceil+\lceil\log 2n\rceil$, $d=2\lceil\sqrt{2n}\rceil$, $\langle N,e\rangle\in\text{Rabin-Paillier}_{\mathrm{pk}}$. 存在一个概率多项式时间算法 B, 已知公钥和 $w\in\mathbb{Z}_{N^2}^*$, 它通过调用预言机 $O_{\alpha,\beta}2\lceil\sqrt{2n}\rceil$ 次, 至少以概率 $1-2^{-\sqrt{2n}}$ 计算出值 $m \bmod N^2$ 和 $r^{2e} \bmod N^2$.

证明. 令 $\alpha:=mN \bmod N^2$ 和 $\beta:=r^{2e} \bmod N^2$. 可以构造算法 B:

1. 选择随机数 $t_1,\cdots,t_d\in\mathbb{Z}_{N^2}^*$；

2. 查询预言机，并得到 $s_i:=O_{\alpha,\beta}(t_i)$，$i=1,2,\cdots,d$；

3. 调用定理 2 的多项式时间算法 A；

4. 输出 α 和 β；

5. $m:=\alpha/N$，$r^{2e}:=\beta$；

应用定理 2，上述算法能够至少以概率

$$\Pr[A(t_1,\cdots,t_d;s_1,\cdots,s_d)=(\alpha,\beta)]\geq 1-2^{-\sqrt{2n}}$$

返回 m 和 r^{2e}. 证毕.

定理 4. 令 $k=\lceil 3\sqrt{2n}/2\rceil+\lceil\log 2n\rceil$，$\langle N,e\rangle\in$ Rabin-Paillier$_{pk}$. 对于 Rabin-Paillier 陷门函数，计算明文 m 的前 k 个 MSB 和分解 Blum 整数 N 是一样困难的.

证明.

($\Rightarrow$) 如果敌手能在多项式时间内分解 Blum 整数 $N=PQ$，则它能够计算 $d\in\mathbb{Z}_N^*$，其中 $ed\equiv 1 \bmod \lambda(N)$. 因此，所有的私钥都能够被计算出来.

($\Leftarrow$) 敌手的目标是分解 N. 在预言机 $O_{\alpha,\beta}$ 的辅助下，它首先调用定理 3 中的多项式时间算法 B. 当算法 B 返回 m 和 $r^{2e} \bmod N^2$，敌手需要找到 r 来分解 N，即敌手已知 $r^{2e} \bmod N$，需要对 Rabin-Williams 函数求逆. 敌手依照文献[11]中的命题 6 来完成剩下的攻击. 算法 B 能够模拟预言机 Hensel-RW$[N,e,2]$. 敌手首先从 Q_N 中随机选取一个数 a，计算 $r^{2e}a^{2e} \bmod N$. 然后，敌手至少能够以概率 $(1-2^{-\sqrt{2n}})^2\geq 1-2^{-\sqrt{2n}+1}$ 知道 $r^{2e} \bmod N$，$r^{2e} \bmod N^2$ 和 $\mu^{2e}=(ar)^{2e} \bmod N^2$，其中 $\mu=ar \bmod N$. 因此存在一个 $z\in\mathbb{Z}_N$，满足

$$ar\equiv\mu(1+zN)\bmod N^2 \qquad (2)$$

把这个等式升到 $2e$ 次幂，敌手得到等式 $a^{2e}r^{2e}\equiv\mu^{2e}(1+2ezN) \bmod N^2$. 从这个式子就能计算出 z，因为其它的值都已经知道了. 最后，敌手可以利用文献[9]中的定理 1 的证明中的格约减算法来解等式(2)从而得到 r. 这一步约用时 $O(\log^4 N)$. 证毕.

4 RSA-Paillier 陷门函数的比特安全性分析

在本节中，我们研究 RSA-Paillier 陷门函数明文的比特安全性. Morillo 等人在文献[10]中声称 RSA-Paillier 陷门函数的明文的最低有效位(LSB)是 hard-core 比特. 他们的证明采用的是反证法：如果明文的 LSB 不是困难的，即存在一个预言机，输入给它密文它能返回对应明文的 LSB. 则可以用这个预言机构造一个算法，它能够在概率多项式时间内对 RSA-Paillier 函数求逆. 换句话说，已知 $w\in\mathbb{Z}_{N^2}^*$，满足 $w=E_{N,e}(r,m)$. 任务是在预言机 $O(w)=LSB(m)$ 的帮助下，在概率多项式时间内恢复出明文 m. 证明通常依据预言机能否正确回答查询而分为两种情况. 在第一种情况是假定敌手拥有一个完美的 LSB 预言机，$\Pr_w[O(w)=LSB(m)]=1$. Morillo 等人考虑了这种情况并且给出了一个借助完美 LSB 预言机恢复明文的算法，称作 MRS 算法. 但是他们的证明忽略掉了不完美 LSB 预言机的情况，$\Pr_w[O(w)=LSB(m)]\geq 1/2+\varepsilon(n)$，其中 $\varepsilon(n)>1/p(n)$，$p(n)$ 为某个多项式. 我们通过构造了一个随机化算法来使得 MRS 算法在不完美预言机下也能工作，从而完善了 RSA-Paillier 明文 LSB 的安全性证明.

4.1 完美预言机的情况

MRS 算法类似于经典的二分搜索算法. 这个算法寻找一个值 t，$t=N-m-1$，而不是先找未知的明文 m. 循环不变量是：在每次 while 循环的开始，有 $\beta=\alpha+d$ 和 $\alpha\leq N-m-1\leq\beta$. 当算法终止时，while 循环终止于 $\beta=\alpha$. 目标值是 $t=\alpha$，则有 $m=N-\alpha-1$. MRS 算法运行时间是 $O(\log N)$. 这是由于在每次迭代中，α 和 β 的距离减半，而它们的初始距离是 $(N-1)/2$. 图 2 给出了这个算法的详细描述.

```
MRS 算法(N,e,w,O)}
1. α:=0, β:=(N−1)/2, d:=(N−1)/2;
2. while (β−α≥1) do
3. b′:=O(w(1+βN))=LSB(m+β);
4. if (b′=LSB(m)+LSB(α+d)mod2)
5. then α:=β;
6. else if (d≠1)
7.     then d:=⌈d/2⌉;
8.     else d:=0;
9. end if
10. β:=α+d;
11. end while
12. return N−α−1;
```

图 2　MRS 算法

4.2 不完美预言机的情况

在本节中，我们展示如何使用一个不完美的预言机来恢复出明文. 关键的技术就是使用随机化方法来放大这个预言机猜测比特的统计优势. 首先给出我们的结论.

定理 5. 令 $\langle N,e\rangle\in$ RSA-Paillier$_{pk}$. 已知 $w\in\mathbb{Z}_{N^2}^*$，如果假定函数 $E_{N,e}(\cdot,\cdot)$ 为一个陷门置换，则 w

对应明文的 LSB 是函数 $E_{N,e}(\cdot,\cdot)$ 的一个 hard-core 谓词.

证明. 在这种情况下,上一节中的算法无法使用,因为不能保证在 MRS 算法(图 2)的任意一个循环中 b' 就是正确的比特.这就需要使用一个随机化的过程,称为随机化查询算法(图 3),来放大这个预言机在猜测比特上的统计优势.所以我们使用随机化查询算法来替换掉 MRS 算法中预言机调用的步骤(图 2 第 3 行).

```
随机化查询(N,e,w,O)
1. l:=2n/ε²;
2. countZero:=0, countOne:=0;
3. for (i=1 to l)
4.    m'←ℤ_N, s←ℤ_N^*;
5.    w1=r^e≡w mod N;
6.    w2≡w1 s^e≡(rs)^e mod N;
7.    ŵ≡w2(1+m'N)
        ≡(1+(m+m')N)(rs)^e mod N²;
8.    b=O(ŵ)
9.    if (b=LSB(m'))
10.     countZero:=countZero+1;
11.   else
12.     countOne:=countOne+1;
13. end for
14. if(countZero>countOne)
15.   return 0;
16. else
17.   return 1;
```

图 3 随机化查询算法

对于 $w=(1+mN)r^e \bmod N^2$,由于 m 与 r 独立,可以利用 RSA-Paillier 函数的部分同态性分别对它们进行随机化.具体地说,首先随机化 r.已知 $m'\leftarrow\mathbb{Z}_N$, $s\leftarrow\mathbb{Z}_N^*$,计算 $w_1:=r^e\equiv w \bmod N$ 和 $w_2:=w_1 s^e\equiv(rs)^e \bmod N$.然后通过计算 $\hat{w}\equiv w_2(1+m'N)\equiv(1+(m+m')N)(rs)^e \bmod N^2$ 来实现 m 的随机化.随机化要重复 l 次,来输出一个对 LSB 的投票,进而以很高的概率得出 LSB 的正确的值.这个投票的过程也称为多数决策.并且每次 for 循环(图 3 行 3~13)的调用被称为一次度量.l 的取值将在下文中得到解释.

下面是使用不完美预言机的明文恢复算法的概率和时间分析.对于 $i=1,2,\cdots,l$,定义取值为 0 和 1 的随机变量 X_i,表示在随机化查询算法中第 i 次查询的是否出错,即 $X_i=1$ iff $O(\hat{w})\neq LSB(m+m')$.由于 m' 和 s 在每次测量中的选取是相互独立的,则 X_i 之间也是相互独立的.由于 $\Pr_w[O(w)=LSB(m)]\geq 1/2+\varepsilon(n)$,可以有 $E[X_i]\leq 1/2-\varepsilon$.一个多数决策是错误的,只有当 $(1/l)\sum_{k=1}^{l}X_i\geq 1/2$,或等价地 $(1/l)\sum_{k=1}^{l}X_i\geq E[X]+\varepsilon$.因此定义事件 $\mathrm{MAJErrs}=\left[(1/l)\sum_{k=1}^{l}X_i\geq E[X]+\varepsilon\right]$.多数决策错误概率的上届可以使用 Chebyshev 不等式来估计:

$$\Pr[\mathrm{MAJErrs}]\leq \Pr\left[\left|\frac{1}{l}\sum_{k=1}^{l}X_i-E[X]\right|\geq\varepsilon\right]\leq\varepsilon^{-2}Var\left[\frac{1}{l}\sum_{k=1}^{l}X_i\right]\leq\frac{1}{l\varepsilon^2}.$$

最后一个不等式成立时因为

$$Var\left[\sum_{k=1}^{l}X_i/l\right]=\sum_{k=1}^{l}Var[X_i]/l^2 \text{ 和 } Var[X_i]<1.$$

如何确定测量的次数 l?只要每次随机化查询算法都返回正确的比特,m 就可以被正确地计算出来.这个事件发生的概率大于 $(1-1/l\varepsilon^2)^n>1/2$.因此如果取 $l=2n/\varepsilon^2$,则上述条件可以满足.因此,明文恢复算法可以在调用预言机 $O(\log N\cdot 2n/\varepsilon^2)=O(n^2/\varepsilon^2)$ 次后找出 m. 证毕.

5 结论及展望

本文分析了 Paillier 陷门函数两个变体的比特安全性.对于 Rabin-Paillier 陷门函数,我们使用了隐藏数问题证明了计算明文的 $\lceil 3\sqrt{2n}/2\rceil+\lceil\log 2n\rceil$ 个 MSB 和计算整个明文一样困难.对于 RSA-Paillier 陷门函数,本文给出了明文 LSB 困难性的完整的证明.

本文的研究还有若干个未解决的问题.对于 Rabin-Paillier 陷门函数,能否把困难比特的数目由 $O(\lceil\sqrt{2n}\rceil)$ 提升到 $O(n)$.对于 RSA-Paillier 陷门函数,构造出新的隐藏数问题的变体来研究明文连续比特困难性也是一个有意思的问题.

参 考 文 献

[1] Blum M, Micali S. How to generate cryptographically strong sequences of pseudo-random bits. SIAM Journal on Computing, 1984, 13(4): 850-864

[2] Alexi W, Chor B, Goldreich O, Schnorr C. RSA and Rabin functions: Certain parts are as hard as the whole. SIAM J. Computing, 1988, 17(2): 194-209

[3] Fischlin R, Schnorr C. Stronger security proofs for RSA and Rabin bits. Journal of Cryptology, 2000, 13(2), 221-244

[4] Håstad J, Näslund M. The security of individual RSA bits// Proceedings of the IEEE Symposium on Foundation of Computer Science. Palo Alto, California, USA, 1998: 510-521

[5] Goldreich O, Levin L. A hard-core predicate for all one-way functions//Proceedings of the 21st ACM Symposium on Theory of Computing. Seattle, Washington, USA, 1989: 25-32

[6] Paillier P. Public-key cryptosystems based on composite degree residuosity class//Proceedings of the Eurocrypt'99. Prague, Czech Republic, 1999: 223-238

[7] Catalano D, Gennaro R, Howgrave-Graham N. Paillier's trapdoor function hides up to n bits. Journal of Cryptology, 2002, 15(4): 251-269

[8] Catalano D, Gennaro R, Howgrave-Graham N, Nguyen P Q. Paillier's cryptosystem revisited//Proceedings of the ACM Conference on Computer and Communications Security 2001. Philadelphia, USA, 2001: 206-214

[9] Catalano D, Nguyen P Q, Stern J. The hardness of Hensel lifting: The case of RSA and discrete logarithm//Proceedings of the Asiacrypt'02. Queenstown, New Zealand, 2002: 299-310

[10] Morillo P, Ràfols C, Soler R. Seguridad del último bit del mensaje del esquema de S-Paillier//Proceedings of Conference on Discrete Mathematics and Algorithms. Valladolid, Spain, 2006: 343-350

[11] Galindo D, Mollevi S, Morillo P, Villar J. A practical public key cryptosystem from Paillier and Rabin schemes//Proceedings of the PKC 2003. Miami, Florida, USA, 2003: 279-291

[12] Boneh D, Venkatesan R. Hardness of computing the most significant bits of secret keys in Diffie-Hellman and related schemes//Proceedings of the Crypto'96. Santa Barbara, California, USA, 1996: 129-142

[13] Shparlinski I E. Playing 'Hide-and-Seek' in finite fields: Hidden number problem and its applications//Proceedings of the 7th Spanish Meeting on Cryptology and Information Security, 2002: 49-72

[14] Garefalakis T. The hidden number problem with non-prime modulus. JP Journal of Algebra, Number Theory and Applications, 2007, 8(2): 193-211

[15] Malykhin Y V. Bounds for exponential sums modulo p^2. Journal of Mathematical Sciences, 2007, 146(2): 5686-5696

[16] Goldreich O. Fundations of Cryptography — Basic Tools. Cambridge, United Kingdom: Cambridge University Press, 2001

[17] González Vasco M I, Shparlinski I E. On the security of diffie-hellman bits//Proceedings of the Workshop on Cryptography and Computational Number Theory. Birkhäuser, 2001: 257-268

[18] Vinogradov I M. Elements of Number Theory. New York: Dover Publications, 1954

SU Dong, born in 1982, M. S. candidate. His current research interests are public-key cryptography and computer security.

WANG Ke, born in 1985, M. S. candidate. His research interests focus on public-key cryptography.

LV Ke-Wei, born in 1970, Ph. D., associate professor. His research interests include public-key cryptography, cryptographic protocols.

Background

This work is partially supported by the National Natural Science Foundation of China (No. 60970154) and the National Basic Research Program of China (No. 2007CB311202).

At Eurocrypt'99, Paillier proposed a new homomorphic trapdoor permutation over $\mathbb{Z}_{N^2}^*$, where N is an RSA modulus, and used it to construct a probabilistic public key encryption scheme. Paillier defined Computational Composite Residuosity Class Problem and thought it is hard to be solved. He showed that the one-wayness of Paillier's trapdoor function is equivalent to the hardness of this problem. In Eurocrypt '01 Catalano et al. showed that the least significant bit of the class of Paillier's Trapdoor Function is a hard-core predicate under the assumption that computing residuosity class is hard. From 2001, several variants of Paillier's trapdoor function were proposed, including RSA-Paillier and Rabin-Paillier. So, what is the bit security of these new trapdoor functions? Can we get stronger bit security results for them? These questions are the motivations of this paper.

For RSA-Paillier trapdoor function, the authors correct the proof of the hardness of least significant bit of this function. The proof was given by Morillo, Ràfols and Soler in 2006. They only consider the perfect oracle case. For Rabin-Paillier trapdoor function, the authors use hidden number problem to show its bit security, which is the formal model of lattice attacks. The authors show that for Rabin-Paillier trapdoor function, computing the $\lceil 3\sqrt{2n}/2\rceil+\lceil\log 2n\rceil$ most significant bits of the plaintext is as hard as inverting this function, where n is the length of an RSA modulus N.