椭圆曲线Diffie-Hellman密钥交换协议的比特安全性研究

魏 伟[①] 陈佳哲[①] 李 丹[③] 张宝峰*[①②]

[①](中国信息安全测评中心 北京 100085)

[②](清华大学 北京 100084)

[③](国家开放大学 北京 100039)

摘 要：椭圆曲线Diffie-Hellman密钥交换协议与其他公钥密码体制相比，能够以较小的密钥尺寸来达到相同的安全强度，因此在实际应用中对带宽和存储的要求较低，从而在很多计算资源受限的环境中有更多应用价值。该文从理论和应用角度，评估该类型协议共享密钥建立过程中的部分信息泄漏对安全性的威胁至关重要。基于隐藏数问题和格分析技术，该文讨论了椭圆曲线Diffie-Hellman密钥交换协议的比特安全性，启发式地证明了椭圆曲线Diffie-Hellman共享密钥的x坐标的中间11/12 bit的计算困难性近似于恢复整个密钥。进一步地，给出了信息泄露量与泄漏位置的显式关系式。该文的研究结果放松了对泄露比特位置的限制，更加符合应用场景，显著改进了以往工作中得出的结论。

关键词：椭圆曲线Diffie-Hellman；比特安全；信息泄露；格；隐藏数问题

中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2020)08-1820-08

DOI: 10.11999/JEIT190845

Research on the Bit Security of Elliptic Curve Diffie-Hellman

WEI Wei[①] CHEN Jiazhe[①] LI Dan[③] ZHANG Baofeng*[①②]

[①](*China Information Technology Security Evaluation Center*, *Beijing* 100085, *China*)

[②](*Tsinghua University*, *Beijing* 100084, *China*)

[③](*The Open University of China*, *Beijing* 100039, *China*)

Abstract: The elliptic curve Diffie-Hellman key exchange protocol enjoys great advantages since it could achieve the same security level with significantly smaller size of parameters compared with other public key cryptosystems. In real-world scenarios, this type of protocol requires less bandwidth and storage which leads to more application especially to computing resource constrained environments. Hence, it is important to evaluate the threat aroused by the partial information leakage during the establishment of shared keys. In this paper, the bit security of elliptic curve Diffie-Hellman with knowledge of partial inner bits based on the combination of hidden number problem and lattice-based cryptanalysis technique is recisited. 11/12 of the inner bits of the x-coordinate of the elliptic curve Diffie-Hellman key are approximately as hard to compute as the entire key. Moreover, the explicit relationship between the leakage fraction and the leakage position is elaborated. This result which relaxes the restriction on the location of leakage position dramatically improves the trivial one which stemmed from prior work.

Key words: Elliptic curve Diffie-Hellman; Bit security; Information leakage; Lattice; Hidden Number Problem(HNP)

收稿日期：2019-11-01；改回日期：2020-04-16；网络出版：2020-04-24

*通信作者： 张宝峰 zhangbf@itsec.gov.cn

基金项目：国家重点研发计划(2016YFB0800902)，国家自然科学基金(61802439, U1936209)

Foundation Items: The National Key Research and Development Program of China (2016YFB0800902), The National Natural Science Foundation of China (61802439, U1936209)

1　引言

1976年提出的Diffie-Hellman密钥交换协议开启了公钥密码学的新时代。椭圆曲线Diffie-Hellman密钥交换协议基于椭圆曲线上的离散对数问题(Elliptic Curve Discrete Logarithm Problem, ECDLP)而设计。由于ECDLP问题当前还未发现亚指数时间算法，因此与其他公钥密钥体制相比，椭圆曲线密码算法通常能够以更小的密钥尺寸来满足相同的安全要求，从而在很多计算资源受限的环境中(如智能卡、移动通信、无限设备等)有更多应用价值，这也是椭圆曲线公钥密码体制最突出的优势之一。椭圆曲线最初分别由Koblitz[1]和Miller[2]引入到公钥密码学的研究中，近年来，很多基于ECDLP所设计的具有不同安全功能的密码体制被提出，如椭圆曲线Diffie-Hellman密钥交换协议、椭圆曲线数字签名方案、椭圆曲线公钥加密方案等。其中，椭圆曲线Diffie-Hellman密钥交换协议是本文的主要研究内容。

在现实场景中，除了理论假设之外，实现过程的安全性通常也会严重影响密码系统的整体安全性。随着侧信道等针对密码算法实现过程的攻击技术的研究进展，评估会话密钥建立中的部分信息泄漏对安全性的威胁愈发重要。Diffie-Hellman密钥交换协议安全性的研究起始于定义在有限域上的相关方案。1996年，Boneh和Venkatesan[3]首次研究了$G=\mathbb{Z}_p^*$上的Diffie-Hellman密钥交换协议及其他相关方案的比特安全性。该结论基于隐藏数问题(Hidden Number Problem, HNP)与格分析技术的巧妙运用。HNP问题是一种丢番图不等式方程组的求解问题。直观上，给定某些随机选取的$t\in\mathbb{F}_q$(为素数)，在已知$t\alpha$的部分信息的条件下，HNP问题旨在恢复隐藏的$\alpha\in\mathbb{F}_q$。通常，HNP问题反映了待恢复的未知目标与其相关的随机逼近之间的关系。此外，HNP问题在SM2, OpenSSL, ECDSA, PUF等包含DSA类算法的标准和实现的攻击中都发挥了重要作用[4–9]。

近年来，为提高解决实际密码方案安全分析的适用性，HNP问题从各个角度得以推广，许多相应的变种问题被提出。例如，模逆隐藏数问题(Modular Inverse Hidden Number Problem, MIHNP)[10,11]、椭圆曲线隐藏数问题(Elliptic Curve Hidden Number Problem, EC-HNP)[12,13]、扩展的隐藏数问题(Extended Hidden Number Problem, EHNP)[14,15]。这些变种问题与HNP问题密切相关，在密码设计和分析中都发挥了重要的作用。其中，EC-HNP问题在文献[12]中被用于研究椭圆曲线Diffie-Hellman密钥交换协议的比特安全性。该项工作证明，计算椭圆曲线Diffie-Hellman共享密钥的x坐标最高(或最低)5/6比例的比特位与计算整个共享密钥一样困难。最近，文献[16]改进了这一结果：在基于某个假设的条件下将椭圆曲线Diffie-Hellman比特安全的结果改进到了最高(或最低)1/2 bit。

在文献[14]的基础上，本文进一步研究了椭圆曲线Diffie-Hellman密钥交换协议的比特安全性。与以往工作不同的是，本文研究的内容包含了信息泄露发生在中间位置时的情形。本文的工作主要有两大挑战：(1)椭圆曲线有理点群运算的非线性性质使得运用HNP的技术手段对Diffie-Hellman密钥交换协议的安全性分析结果并不理想，同样的原因使得当前文献中基于MIHNP问题的分析结果比线性的HNP问题的分析结果差很多，这也是椭圆曲线Diffie-Hellman相比于有限域Diffie-Hellman安全性分析结论更少的原因之一。(2)本文放松了对信息泄露发生位置的限制，并不局限于只发生在比特数据串的两端。当前几乎所有基于HNP问题来分析密码体制安全性的技术都假设nonce的部分泄露信息发生在比特数据串的两端。此外，也存在少量针对中间部分的比特信息发生泄露的研究结果。例如，Nguyen 和Shparlinski[17]利用了连分数技术将其研究结果推广到了内部比特信息泄露的情形。他们指出，为达到恢复密钥的目的，从中间部位发生的信息泄露所需要的比特数是从最高或最低比特开始泄露所需要的比特数的两倍。在文献[12]中，作者指出椭圆曲线Diffie-Hellman密钥交换协议中，共享密钥的x坐标的5/6-最高(或最低)比特安全决定了整体的安全性。然而，当考虑泄露信息发生在中间部位时，至少需要获得中间部位$2\times5/6$部分的泄露信息，该结论显然是平凡的。即使基于文献[13]的改进结果，在基于某个假设的条件下，恢复密钥也至少需要获得中间部位$2\times1/2$部分的泄露信息，结论仍然是平凡的。

本文主要研究了椭圆曲线Diffie-Hellman密钥交换协议的比特安全性，取得了以下成果：

(1) 针对部分信息泄露发生在中间位置的情况，对已有方法和结果进行了推广和改进。不同于以往工作中直接利用HNP来进行密码分析[16]，本文首先基于多次调用改进的EC-HNP获得的已知信息，构建一组具有小根的同余方程组，然后构造了一个特殊结构的格，使得该格具有一个能够表示同余方程组解的短向量，且该短向量的长度远小于Gaussian heuristic估计值。从而，该问题被启发式地转化为一个特殊格上的最短向量求解问题，进而可以利用

当前研究已经相对成熟的格基约化算法来求解。由于泄漏的位置发生在中间，因此每一个方程都包含更多的变量，这将导致格的维数较大。但是本文的工作仍然改进了基于文献[12,13]得出的结论。

(2) 具体地，本文指出在椭圆曲线Diffie-Hellman密钥交换协议中，恢复共享密钥的x坐标的中间11/12部分比特与恢复整个密钥一样困难。

(3) 此外，本文还给出了信息泄露量与泄漏位置的显式关系式。该结果基于Gaussian heuristic假设，严格的比特安全性证明可以参考文献[12]来给出。

本文接下来的组织结构如下：第2节是相关背景知识的介绍，包含椭圆曲线基本知识及Diffie-Hellman密钥交换协议、格基本知识以及椭圆曲线HNP及其变种问题等；第3节，本文将给出椭圆曲线Diffie-Hellman密钥交换协议的中间部位比特安全性的结论；第4节进行了总结。

2 预备知识

本节介绍了本文中所用到的一些预备知识，分为3部分内容。首先是椭圆曲线Diffie-Hellman密钥交换协议及背景知识的介绍。第2节给出了格上一类主要的困难问题的定义以及相关的格基约化算法结论。第3节简要介绍了HNP问题的研究历程以及椭圆曲线HNP问题的定义。

为方便读者理解，给出主要符号对照表如表1所示。

2.1 椭圆曲线Diffie-Hellman背景知识

本文主要研究定义在有限素域$\mathbb{F}_p$(其中素数$p>3$)上的椭圆曲线。给定参数$a,b\in\mathbb{F}_p$满足$4a^3+27b^2\neq 0$，$\mathbb{E}$是定义在$\mathbb{F}_p$上的椭圆曲线。那么由椭圆曲线$\mathbb{E}$在$\mathbb{F}_p$中的所有有理点构成的Abelian群$\mathbb{E}(\mathbb{F}_p)$可定义为

$$\mathbb{E}(\mathbb{F}_p)=\{\boldsymbol{P}=(x,y)\mid y^2=x^3+ax+b \bmod p,\ x,y\in\mathbb{F}_p\}\cup\{\mathcal{O}\} \tag{1}$$

其中，$\mathcal{O}$表示无穷远点。

给定有理点$\boldsymbol{P}\in\mathbb{E}(\mathbb{F}_p)$，分别记$x_{\boldsymbol{P}}$和$y_{\boldsymbol{P}}$为$\boldsymbol{P}$的$x$坐标和$y$坐标。对$\mathbb{E}(\mathbb{F}_p)$中的任意两个有理点$\boldsymbol{P}=(x_{\boldsymbol{P}},y_{\boldsymbol{P}})$和$\boldsymbol{Q}=(x_{\boldsymbol{Q}},y_{\boldsymbol{Q}})$，其中$\boldsymbol{P}\neq\pm\boldsymbol{Q}$，二者的加法可以定义为$\boldsymbol{P}+\boldsymbol{Q}=(x_{\boldsymbol{P}+\boldsymbol{Q}},y_{\boldsymbol{P}+\boldsymbol{Q}})$，其中

$$\left.\begin{aligned}x_{P+Q}&=s^2-x_P-x_Q \bmod p\\ y_{P+Q}&=-(y_P+s(x_{P+Q}-x_P)) \bmod p\end{aligned}\right\} \tag{2}$$

式(2)中，$s=(y_{\boldsymbol{P}}-y_{\boldsymbol{Q}})/(x_{\boldsymbol{P}}-x_{\boldsymbol{Q}})$。对于任意的整数$n$，用$n\boldsymbol{P}$表示的点$\boldsymbol{P}$的数量乘法，它定义为$\boldsymbol{P}$的连续$n$次加法。

下面简要介绍椭圆曲线Diffie-Hellman密钥交换协议。取椭圆曲线上的有理点$\boldsymbol{G}\in\mathbb{E}(\mathbb{F}_p)$，记其阶为$g$。协议双方分别记为用户A和B。用户A随机选择$u$, $1\le u\le g-1$，保密u，计算$u\boldsymbol{G}$并发送给用户B；用户B随机选择v, $1\le v\le g-1$，保密v，计算$v\boldsymbol{G}$并发送给用户A；用户B接收$u\boldsymbol{G}$并计算共享密钥$v(u\boldsymbol{G})$；用户A接收$v\boldsymbol{G}$并计算共享密钥$u(v\boldsymbol{G})$。

2.2 格

给定$\mathbb{R}^m$中n个线性无关的向量$\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_n$，由它们的整系数线性组合所构成的离散加法子群

$$\mathcal{L}(\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_n)=\left\{\sum_{i=1}^{n}x_i\boldsymbol{b}_i : x_i\in\mathbb{Z}\right\} \tag{3}$$

称为格。称$\boldsymbol{B}=[\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_n]$为一组格基。

格理论的研究在现代密码应用中主要有两个方面：一是基于格困难问题的公钥密码体制的设计[18]，二是运用近似格困难问题的快速求解算法分析各种公钥密码体制的安全性。目前，最受关注的两大困难问题为最短向量问题(Shortest Vector Problem, SVP)和最近向量问题(Closest Vector Problem, CVP)。简单来说，SVP 问题是指寻找由格基$\boldsymbol{B}$生成的格中的一个非0最短向量；CVP 问题指给定格基$\boldsymbol{B}$和目标向量$\boldsymbol{t}$，寻找距离$\boldsymbol{t}$最近的格向量。

LLL算法是求解近似SVP问题最基本的算法之一，该算法在1982年由Lenstra等人[19]提出。当前实际中最有效的求解近似最短向量问题的格基约化算法是BKZ算法[20]。

引理1[19,21] 给定n维整数格基$\boldsymbol{B}=[\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_n]$，由其生成的格记为$L$，那么存在一个多项式时间算法，可在$O(n^4\lg\max\limits_{1\le i\le n}\|\boldsymbol{b}_i\|)$时间复杂度内输出一个非0格向量$\boldsymbol{x}$，满足$\|\boldsymbol{x}\|\le(2/\sqrt{3})^n\lambda_1(L)$，其中$\lambda_1(L)$表示格$L$的最短格向量的长度。

对于n维随机格，Gaussian heuristic给出了平均意义下最短格向量长度的一个估计值。

定义1[22] Gaussian Heuristic：设L是$\mathbb{R}^n$中的一个满秩格，C是$\mathbb{R}^n$的一个可测子集。Gaussian Heuristic指出，$L\cap C$中格点的个数约为$\mathrm{vol}(C)/\mathrm{vol}(L)$，其中vol表示体积。

表 1 主要符号对照表

符号	代表意义
$\mathbb{R}^m$	m维实数向量空间
$\mathbb{Z}$	整数集
$\mathbb{F}_p$	p元有限域
$\mathbb{E}(\mathbb{F}_p)$	椭圆曲线$\mathbb{E}$在$\mathbb{F}_p$中的有理点群
$\|\cdot\|$	欧几里得范数
$\det(L)$	格L的基本域体积
$\lambda_1(L)$	格L的最短格向量的长度
$\boldsymbol{B}^{\mathrm{T}}$	矩阵$\boldsymbol{B}$的转置矩阵

因此，对于一个n维格L, Gaussian Heuristic估计出的最短格向量的长度约为

$$\sigma(L)=\sqrt{\frac{n}{2\pi \mathrm{e}}}(\det(\mathrm{L}))^{1/n} \tag{4}$$

一般来说，随着最短向量长度和Gaussian Heuristic之间差距的增加，实际的最短格向量更容易被找到。Gaussian Heuristic的意义在于，如果最短向量长度显著地小于$\sigma(L)$，则可以利用LLL算法或其他相关近似短向量求解算法在多项式时间内找到最短向量。基于此，Gaussian Heuristic在格困难问题求解算法的研究中具有重要应用。例如，枚举算法是求解SVP问题研究最早也是最多的确定性算法，在带裁剪的枚举算法中，Gaussian Heuristic被用来估计枚举球中的格点数目，进而估计算法的复杂度，并得到了理论和实验的吻合[23,24]。本文对椭圆曲线Diffie-Hellman的比特安全性的启发式证明中，运用了Gaussian Heuristic的结论。

2.3 椭圆曲线上的HNP问题

1996年，Boneh和Venkatesan引入了隐藏数问题HNP，并将该问题应用到DSA类签名体制及其在OpenSSL等相关实现中的密钥恢复问题[3]。HNP问题可简要描述如下：对于任意实数z和素数n，符号$|\cdot|_n$表示$|z|_n=\min_{b\in\mathbb{Z}}|z-bn|$。对任意有理数$l$和$m$，用$\mathrm{APP}_{l,n}(m)$表示使得$|m-r|_n\le n/2^{l+1}$成立的任意有理数$r$。那么，HNP问题可以定义为：给定参数$n,d\in\mathbb{Z}$，从$[1,n-1]$随机均匀选取$\{t_i\}_{i=1}^d$，对于隐藏的$\alpha\in\mathbb{Z}_n$，在已知$\{t_i\}_{i=1}^d$及相应的$\mathrm{APP}_{l,n}(\alpha t_i)$的条件下，求解$\alpha$。

本文通过放宽对已知比特位置的限制，修改了文献[14]中提出的EC-HNP$_x$问题。对于定义在有限域$\mathbb{F}_p$(p为素数)上的椭圆曲线Diffie-Hellman密钥交换协议，定义$\boldsymbol{P}=(x_{\boldsymbol{P}},y_{\boldsymbol{P}})$为协议双方最终建立的共享密钥，并记$m$为素数$p$的比特长度。修改后的EC-HNP$_x$问题的定义如下：

定义2　EC-HNP$_x$：给定有限域$\mathbb{F}_p$(p为素数，其比特长度为m)，满足$1\le k+j\le m$的正整数k和j，定义在$\mathbb{F}_p$上的椭圆曲线$\mathbb{E}(\mathbb{F}_p)$以及有理点$\boldsymbol{R}\in\mathbb{E}(\mathbb{F}_p)$。设$\boldsymbol{P}\in\mathbb{E}(\mathbb{F}_p)$是一个隐藏的有理点，对于任意的整数输入$t$，预言机$\mathcal{O}_{k,j}(t)$可输出有理点$\boldsymbol{P}+t\boldsymbol{R}$的$x$坐标的一段比特串，该比特串从低$j$比特位开始，长度为$k$。给定对预言机$\mathcal{O}_{k,j}(t)$的询问权限，EC-HNP$_x$问题的目标是寻找隐藏的有理点$\boldsymbol{P}$。

不难发现，EC-HNP$_x$问题的求解将直接推出椭圆曲线Diffie-Hellman的共享密钥的比特安全性结论。在该协议中，u和v由用户双方分别保密，$u\boldsymbol{G}$和$v\boldsymbol{G}$是公开的，$\boldsymbol{P}=uv\boldsymbol{G}$是协议最终建立的共享密钥。假设攻击者具有预言机，使其能够从$a\boldsymbol{G}$和$b\boldsymbol{G}$获取到$ab\boldsymbol{G}$的部分信息(这里，a, b为任意的未知整数)。对随机选择的整数t, $u\boldsymbol{G}+t\boldsymbol{G}=(u+t)\boldsymbol{G}$是可以计算的。记$\boldsymbol{R}=v\boldsymbol{G}$，则$\boldsymbol{P}+t\boldsymbol{R}=(u+t)v\boldsymbol{G}$的部分信息可被获取。对于输入$\boldsymbol{P}$和$\boldsymbol{R}$，若攻击者可以通过$\boldsymbol{P}+t\boldsymbol{R}$的已知部分比特信息求解EC-HNP$_x$问题，则可恢复密钥$\boldsymbol{P}$。因此，椭圆曲线Diffie-Hellman密钥交换协议的比特安全性分析可以转化为求解EC-HNP$_x$问题。

3　椭圆曲线Diffie-Hellman密钥交换协议的比特安全

本节将给出对椭圆曲线Diffie-Hellman密钥交换协议的比特安全性的改进结果。基于改进的EC-HNP$_x$问题，主要讨论了泄露的部分信息位于中间位置的情况。首先构造一个同余方程组，并将密钥恢复转化为求解方程组的问题。然后构造一个特殊结构的格，进而将方程组求解问题转化为求解该格的最短向量问题。定理1给出了本节的主要结论。

定理1　设$\mathbb{E}$是定义在$\mathbb{F}_p$(其中素数$p>3$，其比特长度为m)上的椭圆曲线，正整数k和j满足$1\le k+j\le m$。在$\mathbb{E}(\mathbb{F}_p)$上的椭圆曲线Diffie-Hellman密钥交换协议中，设$\boldsymbol{P}=(x_{\boldsymbol{P}},y_{\boldsymbol{P}})\in\mathbb{E}(\mathbb{F}_p)$是协议双方建立的共享密钥，预言机$\mathcal{O}_{k,j}(t)$可输出有理点$\boldsymbol{P}+t\boldsymbol{R}$($\boldsymbol{R}$为已知有理点，$t$为任意整数)的$x$坐标的一段比特串，该比特串从低$j$比特位开始，长度为$k$。基于Gaussian heuristic，若$k$和$j$满足以下关系，则存在多项式时间算法，在$2n+1(n=\mathrm{poly}(m))$次询问$\mathcal{O}_{k,j}(t)$后可恢复出共享密钥$\boldsymbol{P}$的$x$坐标$x_{\boldsymbol{P}}$，进而可恢复共享密钥$\boldsymbol{P}=(x_{\boldsymbol{P}},\sqrt{x_{\boldsymbol{P}}^3+ax_{\boldsymbol{P}}+b})$或$\boldsymbol{P}=(x_{\boldsymbol{P}},-\sqrt{x_{\boldsymbol{P}}^3+ax_{\boldsymbol{P}}+b})$，

$$k\ge\begin{cases}\dfrac{5}{6}m, & j=0\\ \dfrac{11}{12}m+\dfrac{j}{12}+\dfrac{11}{12}, & 0<j<\dfrac{1}{25}m-\dfrac{11}{25}\\ \dfrac{12}{13}m-\dfrac{1}{13}j+\dfrac{11}{13}, & \dfrac{1}{25}m-\dfrac{11}{25}\le j<\dfrac{1}{12}m\\ \dfrac{5}{6}m, & j=\dfrac{1}{6}m\end{cases} \tag{5}$$

证明：下面分3小节给出定理1的完整证明。在3.1节中本文基于对预言机$\mathcal{O}_{k,j}(t)$的$2n+1$次询问结果，构造了由n个同余多项式方程组成的方程组，该方程组的解隐含共享密钥的x坐标；在3.2节中，构造了一个具有特殊结构的$12n+6$维格，将方程组的求解问题转化为该格的短向量的求解问题；3.3节分析了信息泄露发生在对称位置的情况，完善了所需泄露信息量与泄露发生位置的显示表达。

3.1 构造同余多项式方程组

记共享密钥$\boldsymbol{P}$的x坐标为$x_P = 2^{k+j}x_0 + h_0 + e_0$，其中$2^j < h_0 < 2^{k+j}$为通过预言机$\mathcal{O}_{k,j}(t)$(取$t=0$时)获得的已知信息，$0 < e_0 < 2^j$和$0 < x_0 < 2^{m-(k+j)}$是未知的。只要求解出$e_0$和$x_0$即可恢复共享密钥$\boldsymbol{P}$。

对于椭圆曲线上的任意有理点$\boldsymbol{Q} = (x_{\boldsymbol{Q}}, y_{\boldsymbol{Q}}) \in \mathbb{E}(\mathbb{F}_p)$，将以下两个相关的表达式进行组合以消除$y_{\boldsymbol{P}}$的显式表达

$$\begin{aligned} & x_{\boldsymbol{P}+\boldsymbol{Q}} + x_{\boldsymbol{P}-\boldsymbol{Q}} \\ &= 2\left(\frac{y_{\boldsymbol{P}}^2 + y_{\boldsymbol{Q}}^2}{(x_{\boldsymbol{P}} - x_{\boldsymbol{Q}})^2} - x_{\boldsymbol{P}} - x_{\boldsymbol{Q}}\right) \\ &= 2\left(\frac{x_{\boldsymbol{Q}}x_{\boldsymbol{P}}^2 + (a + x_{\boldsymbol{Q}}^2)x_{\boldsymbol{P}} + ax_{\boldsymbol{Q}} + 2b}{(x_{\boldsymbol{P}} - x_{\boldsymbol{Q}})^2}\right) \end{aligned} \tag{6}$$

对于椭圆曲线上的任意有理点$\boldsymbol{Q} = (x_{\boldsymbol{Q}}, y_{\boldsymbol{Q}}) \in \mathbb{E}(\mathbb{F}_p)$，记

$$\left.\begin{aligned} x_{\boldsymbol{P}+\boldsymbol{Q}_i} &= 2^{k+j}x_i^{\boldsymbol{P}+\boldsymbol{Q}_i} + h_i + e_i \\ x_{\boldsymbol{P}-\boldsymbol{Q}_i} &= 2^{k+j}x_i^{\boldsymbol{P}-\boldsymbol{Q}_i} + h_i' + e_i' \end{aligned}\right\} \tag{7}$$

其中，h_i和h_i'是已知的部分比特信息，$x_i^{\boldsymbol{P}+\boldsymbol{Q}_i}$和$x_i^{\boldsymbol{P}-\boldsymbol{Q}_i}$分别表示$\boldsymbol{P}+\boldsymbol{Q}_i$和$\boldsymbol{P}-\boldsymbol{Q}_i$的高比特信息。令$\tilde{h}_i = h_i + h_i'$, $\tilde{e}_i = e_i + e_i'$, $\tilde{x}_i = x_i^{\boldsymbol{P}+\boldsymbol{Q}_i} + x_i^{\boldsymbol{P}-\boldsymbol{Q}_i}$。则有

$$\begin{aligned} & \tilde{h}_i + \tilde{e}_i + 2^{k+j}\tilde{x}_i \\ &= x_{\boldsymbol{P}+\boldsymbol{Q}_i} + x_{\boldsymbol{P}-\boldsymbol{Q}_i} \\ &= 2\left(\frac{x_{\boldsymbol{Q}_i}x_{\boldsymbol{P}}^2 + (a + x_{\boldsymbol{Q}_i}^2)x_{\boldsymbol{P}} + ax_{\boldsymbol{Q}_i} + 2b}{(2^{k+j}x_0 + h_0 + e_0 - x_{\boldsymbol{Q}_i})^2}\right) \end{aligned} \tag{8}$$

对于输入$\{t_i, -t_i\}_{i=1}^n$，记$\boldsymbol{Q}_i = t_i\boldsymbol{R}, -\boldsymbol{Q}_i = -t_i\boldsymbol{R}$，独立地重复询问$2n$($n$为正整数)次预言机$\mathcal{O}_{k,j}(t)$，并用变量符号集合$\{X, Y_i, Z_i, U\}_{i=1}^n$来分别对应地表示未知变量集合$\{e_0, \tilde{e}_i, \tilde{x}_i, x_0\}_{i=1}^n$。重写式(8)，可以得到如式(9)的多项式

$$\begin{aligned} F_i(X, Y_i, Z_i, U) =& a_{1,i}X^2Y_i + a_{2,i}X^2Z_i + a_{3,i}XY_iU \\ &+ a_{4,i}XZ_iU + a_{5,i}Z_iU^2 + b_{1,i}X^2 \\ &+ b_{2,i}XY_i + b_{3,i}XZ_i + b_{4,i}XU \\ &+ b_{5,i}Y_iU + b_{6,i}Z_iU + b_{7,i}U^2 \\ &+ c_{1,i}X + c_{2,i}Y_i + c_{3,i}Z_i + c_{4,i}U \\ &+ d_i \bmod p \end{aligned} \tag{9}$$

且满足$F_i(e_0, \tilde{e}_i, \tilde{x}_i, x_0) = 0 \bmod p (1 \le i \le n)$。需要说明的是，在式(9)中$\{a_{i,j}, b_{i,j}, c_{i,j}\}$均为关于$\{h_0, \tilde{h}_i, x_{Q_i}, a, b\}$的已知系数参数，其具体的数值表达式并不影响对方程组的求解能力，因此在下文中略去具体表达式的计算。

注意到，X和U在以上n个方程中保持不变；Y_i和Z_i由于与有理点$\boldsymbol{Q}_i$的选择相关，$\boldsymbol{Q}_i$又基于对预言机$\mathcal{O}_{k,j}(t)$的n次独立询问而产生，因此Y_i和Z_i在以上n个方程中是不同的。

根据已知条件，对$1 \le i \le n$，有

$$\left.\begin{aligned} & 0 < e_0 < 2^j, 0 < \tilde{e}_i = e_i + e_i' < 2^{j+1} \\ & 0 < \tilde{x}_i = x_i^{\boldsymbol{P}+\boldsymbol{Q}} + x_i^{\boldsymbol{P}-\boldsymbol{Q}} < 2^{m-(k+j)+1} \\ & 0 < x_0 < 2^{m-(k+j)} \end{aligned}\right\} \tag{10}$$

这给出了方程组$F_i(X, Y_i, Z_i, U) = 0 \bmod p (1 \le i \le n)$中一组解的上界。因此，恢复$e_0$和$x_0$的问题转化为了求解方程组$F_i(X, Y_i, Z_i, U) = 0 \bmod p (1 \le i \le n)$的一组小整数解问题。

3.2 构造格求解同余方程组

随着求解SVP和CVP等格问题的快速算法的研究发展，基于格的密码分析技术在求解同余方程组的有界解中发挥了越来越重要的作用。本小节将给出具体的格基构造方法，以求解上节中提出的同余方程组。

定义由以下格基$\boldsymbol{B}$生成的格为L

$$\boldsymbol{B} = \begin{pmatrix} \boldsymbol{E} & \boldsymbol{R} \\ \boldsymbol{0} & \boldsymbol{P} \end{pmatrix} \tag{11}$$

其中，矩阵$\boldsymbol{R}$由式(9)中的变量系数构成，是一个$(11n+6) \times n$维的矩阵。例如，当$n=2$时，$\boldsymbol{R}$可写成表达式为

$$\boldsymbol{R} = \begin{pmatrix} d_1 & c_{4,1} & c_{3,1} & 0 & c_{2,1} & 0 & c_{1,1} & b_{7,1} & b_{6,1} & 0 & b_{5,1} & 0 & b_{4,1} & b_{3,1} & 0 & b_{2,1} & 0 & b_{1,1} & a_{5,1} & 0 & a_{4,1} & 0 & a_{3,1} & 0 & a_{2,1} & 0 & a_{1,1} & 0 \\ d_2 & c_{4,2} & 0 & c_{3,2} & 0 & c_{2,2} & c_{1,2} & b_{7,2} & 0 & b_{6,2} & 0 & b_{5,2} & b_{4,2} & 0 & b_{3,2} & 0 & b_{2,2} & b_{1,2} & 0 & a_{5,2} & 0 & a_{4,2} & 0 & a_{3,2} & 0 & a_{2,2} & 0 & a_{1,2} \end{pmatrix}^{\mathrm{T}} \tag{12}$$

矩阵$\boldsymbol{E}$是一个$11n+6$-维的对角方阵，根据矩阵$\boldsymbol{R}$中系数所对应的序列，矩阵$\boldsymbol{E}$的元素与多项式方程组(2)中相应变量的上界相关。类似地，当$n=2$时，其对角元素按顺序可列为

$$\begin{aligned} \{& 1, 2^{k+j-m}, 2^{k+j-m-1}, 2^{k+j-m-1}, 2^{-j-1}, 2^{-j-1}, 2^{-j}, 2^{2(k+j-m)}, 2^{2(k+j-m)-1}, 2^{2(k+j-m)-1}, \\ & 2^{k-m-1}, 2^{k-m-1}, 2^{k-m}, 2^{k-m-1}, 2^{k-m-1}, 2^{-2j-1}, 2^{-2j-1}, 2^{-2j}, 2^{3k+3j-3m-1}, 2^{3k+3j-3m-1}, \\ & 2^{2k+j-2m-1}, 2^{2k+j-2m-1}, 2^{k-j-m-1}, 2^{k-j-m-1}, 2^{k-j-m-1}, 2^{k-j-m-1}, 2^{-3j-1}, 2^{-3j-1}\} \end{aligned} \tag{13}$$

矩阵$\boldsymbol{P}$是一个n维对角方阵，其对角元素均为素数p。因此，格基矩阵$\boldsymbol{B}$的维数为$12n+6$，其行列式可以计算为

$$\det(L)=\frac{p^n}{2^{n(12m-12k+j+11)+4(m-k)}} \tag{14}$$

那么由格基$\boldsymbol{B}$生成的格L中存在一个格向量$\boldsymbol{v}=\boldsymbol{wB}$，其系数向量为

$$\begin{aligned}\boldsymbol{w}=(&1,x_0,\tilde{x}_1,\cdots,\tilde{x}_n,\tilde{e}_1,\cdots,\\&\tilde{e}_n,e_0,x_0^2,\tilde{x}_1x_0,\cdots,\tilde{x}_nx_0,\ \tilde{e}_1x_0,\cdots,\\&\tilde{e}_nx_0,e_0x_0,e_0\tilde{x}_1,\cdots,e_0\tilde{x}_n,e_0\tilde{e}_1,\cdots,\\&e_0\tilde{e}_n,e_0^2,\tilde{x}_1x_0^2,\cdots,\tilde{x}_nx_0^2,e_0\tilde{x}_1x_0,\cdots,\\&e_0\tilde{x}_nx_0,e_0\tilde{e}_1x_0,\cdots,e_0\tilde{e}_nx_0,e_0^2\tilde{x}_1,\cdots,\\&e_0^2\tilde{x}_n,e_0^2\tilde{e}_1,\cdots,e_0^2\tilde{e}_n,k_1,\cdots,k_n)\end{aligned} \tag{15}$$

其中，$k_1,k_2,\cdots,k_n$是使得等式(16)成立的整数序列

$$\begin{aligned}\boldsymbol{v}=\Bigg(&1,\frac{x_0}{2^{m-k-j}},\frac{\tilde{x}_1}{2^{m-k-j+1}},\cdots,\frac{\tilde{x}_n}{2^{m-k-j+1}},\frac{\tilde{e}_1}{2^{j+1}},\cdots,\\&\frac{\tilde{e}_n}{2^{j+1}},\frac{e_0}{2^j},\frac{x_0^2}{2^{2(m-k-j)}},\frac{\tilde{x}_1x_0}{2^{2(m-k-j)+1}},\cdots,\\&\frac{\tilde{x}_nx_0}{2^{2(m-k-j)+1}},\frac{\tilde{e}_1x_0}{2^{m-k+1}},\cdots,\frac{\tilde{e}_nx_0}{2^{m-k+1}},\frac{e_0x_0}{2^{m-k}},\\&\frac{e_0\tilde{x}_1}{2^{m-k+1}},\cdots,\frac{e_0\tilde{x}_n}{2^{m-k+1}},\frac{e_0\tilde{e}_1}{2^{2j+1}},\cdots,\frac{e_0\tilde{e}_n}{2^{2j+1}},\frac{e_0^2}{2^{2j}},\\&\frac{\tilde{x}_1x_0^2}{2^{3m-3k-3j+1}},\cdots,\frac{\tilde{x}_nx_0^2}{2^{3m-3k-3j+1}},\frac{e_0\tilde{x}_1x_0}{2^{2m-2k-j+1}},\cdots,\\&\frac{e_0\tilde{x}_nx_0}{2^{2m-2k-j+1}},\frac{e_0\tilde{e}_1x_0}{2^{m-k+j+1}},\cdots,\frac{e_0\tilde{e}_nx_0}{2^{m-k+j+1}},\frac{e_0^2\tilde{x}_1}{2^{m-k+j+1}},\\&\cdots,\frac{e_0^2\tilde{x}_n}{2^{m-k+j+1}},\frac{e_0^2\tilde{e}_1}{2^{3j+1}},\cdots,\frac{e_0^2\tilde{e}_n}{2^{3j+1}},0,\cdots,0\Bigg)\end{aligned} \tag{16}$$

从$\{e_0,\tilde{e}_i,\tilde{x}_i,x_0\}$的上界容易计算得到格向量$\boldsymbol{v}$的长度的上界

$$\parallel v\parallel\le\sqrt{11n+6} \tag{17}$$

根据Gaussian heuristic，若

$$\parallel\boldsymbol{v}\parallel\ll\sqrt{12n+6}\det(L)^{\frac{1}{12n+6}} \tag{18}$$

则格向量$\boldsymbol{v}$将作为格L的一个最短向量通过格基约化算法在多项式时间内被输出。

整理不等式(18)可得

$$\sqrt{\frac{11n+6}{12n+6}}\ll\left(\frac{p^n}{2^{n(12m-12k+j+11)+4(m-k)}}\right)^{\frac{1}{12n+6}} \tag{19}$$

最终有

$$k\ge\frac{11}{12}m+\frac{1}{12}j+\frac{11}{12},\ 0\le j\le m \tag{20}$$

此外，受$k+j<m$条件的限制，本文指出，当$0<j<m/13$时，最多获取$\frac{11}{12}m+\frac{1}{12}j+\frac{11}{12}$的内部比特信息，共享密钥可被恢复。

3.3 信息泄露的对称情形分析

本小节将针对信息泄露发生在对称位置的情况给出相关的分析。对于任意输入t及有理点$\boldsymbol{R}\in\mathbb{E}(\mathbb{F}_p)$，假设问询预言机后返回从高$j'$比特位开始，长度为$k$的$\boldsymbol{P}+t\boldsymbol{R}$的$x$坐标的部分比特信息。当参数$t=0$时，记

$$x_{\boldsymbol{P}}=x_0+h_0+2^{m-j'}e_0 \tag{21}$$

其中，h_0是已知的部分比特信息。

同理，对于椭圆曲线上的任意有理点$\boldsymbol{Q}_i=(x_{\boldsymbol{Q}_i},y_{\boldsymbol{Q}_i})\in\mathbb{E}(\mathbb{F}_p)$，记

$$\left.\begin{aligned}x_{\boldsymbol{P}+\boldsymbol{Q}_i}&=x_i^{\boldsymbol{P}+\boldsymbol{Q}_i}+h_i+2^{m-j'}e_i\\x_{\boldsymbol{P}-\boldsymbol{Q}_i}&=x_i^{\boldsymbol{P}-\boldsymbol{Q}_i}+h_i'+2^{m-j'}e_i'\end{aligned}\right\} \tag{22}$$

其中，h_i和h_i'是已知的部分比特信息。令$\tilde{h}_i=h_i+h_i'$，$\tilde{e}_i=e_i+e_i'$，$\tilde{x}_i=x_i^{\boldsymbol{P}+\boldsymbol{Q}_i}+x_i^{\boldsymbol{P}-\boldsymbol{Q}_i}$，则有

$$\begin{aligned}&\tilde{h}_i+2^{m-j'}\tilde{e}_i+\tilde{x}_i=x_{\boldsymbol{P}+\boldsymbol{Q}_i}+x_{\boldsymbol{P}-\boldsymbol{Q}_i}\\&\quad=2\left(\frac{x_{Q_i}x_P^2+(a+x_{Q_i}^2)x_P+ax_{Q_i}+2b}{\left(x_0+h_0+2^{m-j}e_0-x_{Q_i}\right)^2}\right)\end{aligned} \tag{23}$$

除某些变量的系数不同以外，式(23)与式(8)基本类似。同理，独立地重复询问$2n$次预言机，并用$\{X,Y_i,Z_i,U\}_{i=1}^n$来分别对应地表示未知变量集合$\{e_0,\tilde{e}_i,\tilde{x}_i,x_0\}_{i=1}^n$。重写式(23)，可以得到$n$个多项式为

$$\begin{aligned}G_i(X,Y_i,Z_i,U)=&a'_{1,i}X^2Y_i+a'_{2,i}X^2Z_i\\&+a'_{3,i}XY_iU+a'_{4,i}XZ_iU\\&+a'_{5,i}Z_iU^2+b'_{1,i}X^2+b'_{2,i}XY_i\\&+b'_{3,i}XZ_i+b'_{4,i}XU+b'_{5,i}Y_iU\\&+b'_{6,i}Z_iU+b'_{7,i}U^2+c'_{1,i}X\\&+c'_{2,i}Y_i+c'_{3,i}Z_i+c'_{4,i}U\\&+d'_i\bmod p\end{aligned} \tag{24}$$

其中，$1\le i\le n$。该组多项式满足

$$G_i(e_0,\tilde{e}_i,\tilde{x}_i,x_0)=0\bmod p\ (1\le i\le n) \tag{25}$$

类似于3.2节的格L和格向量$\boldsymbol{v}$的构造方法，本文构造格$\boldsymbol{\Lambda}$和相应的格向量$\boldsymbol{v}'\in\boldsymbol{\Lambda}$，具体的构造方法此处略去。注意到，式(24)和式(9)具有相同的结构，结合格基的构造方式，容易得到格$\boldsymbol{\Lambda}$和格$\boldsymbol{L}$具有相同的行列式，格向量$\boldsymbol{v}'$和$\boldsymbol{v}$具有相同的长度上界。从而可以通过求解式(24)的一组小整数解来恢复共享密钥$\boldsymbol{P}$的x坐标。然后，将式(24)的小根求解问题转化为寻找格$\boldsymbol{\Lambda}$的一个短向量$\boldsymbol{v}'$的问题。短向量$\boldsymbol{v}'$的长度需满足

$$\parallel\boldsymbol{v}'\parallel\ll\sqrt{12n+6}\det(\boldsymbol{\Lambda})^{\frac{1}{12n+6}} \tag{26}$$

计算可得，

$$k\ge\frac{11}{12}m+\frac{1}{12}j'+\frac{11}{12},\ 0\le j'\le\frac{m}{13} \tag{27}$$

统一起见，本文仍记j为部分信息泄露比特段的低起始比特，那么

$$j+k+j'=m \tag{28}$$

因此

$$k\geq\frac{12}{13}m-\frac{1}{13}j+\frac{11}{13},\ 0<j<\frac{1}{12}m \tag{29}$$

结合式(24)和式(29)，本文改进了文献[19]中对于泄露比特位置发生在内部的情形的结论。具体地，关于泄露信息量与泄露发生的位置的关系，有如式(30)的结论

$$k\geq\begin{cases}\dfrac{5}{6}m, & j=0\\ \dfrac{11}{12}m+\dfrac{j}{12}+\dfrac{11}{12}, & 0<j<\dfrac{1}{25}m-\dfrac{11}{25}\\ \dfrac{12}{13}m-\dfrac{1}{13}j+\dfrac{11}{13}, & \dfrac{1}{25}m-\dfrac{11}{25}\leq j<\dfrac{1}{12}m\\ \dfrac{5}{6}m, & j=\dfrac{1}{6}m\end{cases} \tag{30}$$

因此，定理1得到证明。

4 结论

本文基于EC-HNP问题，针对信息泄露发生在中间部位的情形，研究了椭圆曲线Diffie-Hellman的比特安全性。具体来说，本文证明了椭圆曲线Diffie-Hellman密钥交换协议的x坐标的内部11/12 bit位近似和整个密钥一样难以计算。此外，本文还建立了信息泄漏率与信息泄漏位置的显式关系，并结合实际的椭圆曲线Diffie-Hellman密钥交换协议，分析了本结果的应用。本文的研究结果显著改进了以往文献中的平凡结论。

参 考 文 献

[1] KOBLITZ N. Elliptic curve cryptosystems[J]. *Mathematics of Computation*, 1987, 48(177): 203–209. doi: 10.1090/S0025-5718-1987-0866109-5.

[2] MILLER V S. Use of elliptic curves in cryptography[C]. Proceedings of Conference on the Theory and Application of Cryptographic Techniques, California, USA, 1986: 417–426.

[3] BONEH D and VENKATESAN R. Hardness of computing the most significant bits of secret keys in Diffie-Hellman and related schemes[C]. The 16th Annual International Cryptology Conference, California, USA, 1996: 129–142.

[4] LIU Mingjie, CHEN Jiazhe, and LI Hexin. Partially known nonces and fault injection attacks on SM2 signature algorithm[C]. The 9th International Conference on Information Security and Cryptology, Guangzhou, China, 2014: 343–358.

[5] NGUYEN P Q and SHPARLINSKI I E. The insecurity of the elliptic curve digital signature algorithm with partially known nonces[J]. *Designs, Codes and Cryptography*, 2003, 30(2): 201–217. doi: 10.1023/A:1025436905711.

[6] FAN Shuqin, WANG Wenbo, and CHENG Qingfeng. Attacking OpenSSL implementation of ECDSA with a few signatures[C]. 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 2016: 1505–1515.

[7] GANJI F, KRÄMER J, SEIFERT J P, *et al*. Lattice basis reduction attack against physically unclonable functions[C]. The 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, USA, 2015: 1070–1080.

[8] BREITNER J and HENINGER N. Biased nonce sense: lattice attacks against weak ECDSA signatures in cryptocurrencies[J]. *Financial Cryptography and Data Security*, 2019: 3–20.

[9] MOGHUMI D, SUNAR B, EISENBARTH T, *et al*. TPM-FAIL: TPM meets timing and lattice attacks[J]. arXiv: 2019, 1911.05673.

[10] BONEH D, HALEVI S, and HOWGRAVE-GRAHAM N. The modular inversion hidden number problem[C]. The 7th International Conference on the Theory and Application of Cryptology and Information Security, Gold Coast, Australia, 2001: 36–51.

[11] XU Jun, SARKAR S, HU Lei, *et al*. New results on modular inversion hidden number problem and inversive congruential generator[C]. The 39th Annual International Cryptology Conference, Santa Barbara, USA, 2019: 297–321.

[12] SHANI B. On the bit security of elliptic curve Diffie-Hellman[C]. The 20th IACR International Conference on Practice and Theory in Public-Key Cryptography, Amsterdam, The Netherlands, 2017: 361–387.

[13] XU Jun, HU Lei, and SARKAR S. Cryptanalysis of elliptic curve hidden number problem from PKC 2017[J]. *Designs, Codes and Cryptography*, 2020, 88(2): 341–361. doi: 10.1007/s10623-019-00685-y.

[14] HLAVÁČ M and ROSA T. Extended hidden number problem and its cryptanalytic applications[C]. The 13th International Workshop on Selected Areas in Cryptography, Montreal, Canada, 2007: 114–133.

[15] WEI Wei, CHEN Jiazhe, LI Dan, *et al*. Partially known information attack on SM2 key exchange protocol[J]. *Science China Information Sciences*, 2019, 62(3): 032105. doi: 10.1007/s11432-018-9515-9.

[16] 张江, 范淑琴. 关于非对称含错学习问题的困难性研究[J]. 电子与信息学报, 2020, 42(2): 327–332. doi: 10.11999/JEIT190685.

ZHANG Jiang and FAN Shuqin. On the hardness of the asymmetric learning with errors problem[J]. *Journal of Electronics & Information Technology*, 2020, 42(2): 327–332. doi: 10.11999/JEIT190685.

[17] NGUYEN P Q and SHPARLINSKI I E. The insecurity of

the digital signature algorithm with partially known nonces[J]. *Journal of Cryptology*, 2002, 15(3): 151–176. doi: 10.1007/s00145-002-0021-3.

[18] 谢天元, 李昊宇, 朱熠名, 等. FatSeal: 一种基于格的高效签名算法[J]. 电子与信息学报, 2020, 42(2): 333–340. doi: 10.11999/JEIT190678.
XIE Tianyuan, LI Haoyu, ZHU Yiming, *et al*. FatSeal: An efficient lattice-based signature algorithm[J]. *Journal of Electronics & Information Technology*, 2020, 42(2): 333–340. doi: 10.11999/JEIT190678.

[19] LENSTRA A K, LENSTRA H W JR, and LOVÁSZ L. Factoring polynomials with rational coefficients[J]. *Mathematische Annalen*, 1982, 261(4): 515–534. doi: 10.1007/BF01457454.

[20] SCHNORR C P. A hierarchy of polynomial time lattice basis reduction algorithms[J]. *Theoretical Computer Science*, 1987, 53(2/3): 201–224.

[21] MICCIANCIO D and GOLDWASSER S. Complexity of Lattice Problems: A Cryptographic Perspective[M]. Boston, USA: Kluwer Academic Publishers, 2002.

[22] NGUYEN P Q. Hermite's Constant and Lattice Algorithms[M]. NGUYEN P Q and VALLÉE B. The LLL Algorithm: Survey and Applications. Berlin, Germany: Springer, 2009: 19–69.

[23] GAMA N, NGUYEN P Q, and REGEV O. Lattice enumeration using extreme pruning[C]. The 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, France, 2010: 257–278.

[24] AONO Y and NGUYEN P Q. Random sampling revisited: Lattice enumeration with discrete pruning[C]. The 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, 2017: 65–102.

魏　伟：女，1985年生，助理研究员，研究方向为密码学.
陈佳哲：男，1985年生，副研究员，研究方向为密码学.
李　丹：女，1991年生，讲师，研究方向为侧信道分析技术.
张宝峰：男，1983年生，副研究员，研究方向为信息技术产品的安全测评.

责任编辑：余　蓉