保留格式加密模型研究

刘哲理，贾春福，李经纬
（南开大学 信息技术科学学院，天津 300071）

摘 要：对保留格式加密（FPE, format preserving encryption）进行了研究，指出加密模型的设计思想正向如何降低问题域的复杂性发展；提出了编码后加密（CtE, coding-then-encipher）的新模型，描述了工作原理及算法，分析了安全性；最后提出了 CtE 模型在 $chars^n$ 域内的一个应用方案，介绍了使用的编解码算法，分析了其效率。

关键词：保留格式加密；排序后加密；编码后加密；随机基准值加密
中图分类号：TP393.08 **文献标识码：**A **文章编号：**1000-436X(2011)06-0184-07

Research on the format-preserving encryption modes

LIU Zhe-li , JIA Chun-fu, LI Jing-wei
(College of Information Technical Science, Nankai University, Tianjin 300071, China)

Abstract: FPE (format-preserving encryption) was discussed, and it was shown that how to reduce domain complexity was the direction of designing FPE modes. A new FPE mode named coding-then-encipher mode was proposed and its operating principle and security were described in detail, and it was pointed out that the key for this mode was finding efficient *encode* and *decode* algorithms on domain. Furthermore, a scheme under coding-then-encipher mode which can resolve FPE problem in $chars^n$ was presented, the *encode* and *decode* algorithms were described, and their efficiency were analyzed.

Key words: format-preserving encryption; rank-then-encipher; coding-then-encipher; random reference-based encryption

1 引言

支付卡行业数据安全标准[1](PCI DSS, payment card industry data security standard)的提出与应用及消费者保护个人隐私意识的提高，促使人们探索发现新的技术来加密信用卡号等个人识别信息(PII, personally identifiable information)，以最小化数据意外丢失所造成的影响。使用已有的加密方法对 PII 进行加密，最大的问题在于它们通常会扩展密文，使密文的数据长度或类型等发生变化，这就需要修改数据库结构或应用程序来适应密文的变化，成本非常高。

上述的加密问题，要求密文与明文具有相同的格式，这是一类新的加密技术，称为“保留格式加密”(FPE, format-preserving encryption)。FPE 的初衷是为了解决数据库或者应用系统中的 PII 加密问题，随着技术的发展，其应用并不仅限于此。比如，FPE 可以应用于数据遮蔽[2](data masking)领域，通过对原始数据进行加密，输出一个和原始数据格式一模一样的数据，用来进行功能测试、性能测试和模拟测试等；另外，FPE 对于网络数据安全一样有用，可以使数据报在不改变格式的情况下在传输过程中受到保护。

目前，国外已公开发表多篇有关 FPE 的理论研

收稿日期：2010-08-23；修回日期：2010-12-21
基金项目：国家自然科学基金资助项目（60973141）；天津市自然科学基金资助项目（09JCYBJ00300）；高等学校博士学科点专项科研基金资助项目（20100031110030）
Foundation Items: The National Natural Science Foundation of China (60973141); The National Science Foundation of Tianjin (09JCYBJ00300); The Specialized Research Fund for the Doctoral Program of Higher Education of China (20100031110030)

究成果[3~11]。2002 年，Black 和 Rogaway[5]首次从密码学角度研究了 FPE 问题，认为核心是设计某密码 $F: K \times X \to X$，其中 K 是密钥空间，X 是有限的消息空间。他们关注于整数域 $Z_n = \{0,1,\text{L},n-1\}$ 上的 FPE 问题，提出了 3 种构建方法：Prefix、Cycle-walking 和 Generalized-Feistel。Prefix 方法通过在内存中建立一个伪随机置换来加密数据，仅适合于较小有限域。Cycle-walking 方法可以保证明文被加密到期望范围内，其原理可以简单地描述如下：要加密明文 $x \in \{0,1,\text{L},n-1\}$，选用分组密码 E(如 AES)，设 $y = E(x)$，如果 $y \in \{0,1,\text{L},n-1\}$ 则返回 y，否则循环执行 $y = E(y)$，直到有 $\{0,1,\text{L},n-1\}$ 范围内的密文 y 产生为止。可见，Cycle-walking 方法在加密不同数据时，调用 E 的次数可能不同，其效率具有不确定性。Generalized-Feistel 则利用 Luby-Rackoff 结构[12]，构造分组大小为 $2m$ 的分组密码，并结合 Cycle–walking 方法，理论上能对任意大小的集合进行加密。基于这些 FPE 基本构建方法，一些 FPE 加密模型陆续被提出，包括 FFSEM[8]、RtE[9]、FFX[10] 及 BPS[11]模型等。

本文关注于已有的 FPE 模型构造方法的研究，并致力于提出新的 FPE 模型。

2　FPE 的定义

定义 1(基本 FPE)。FPE 可以简单描述为构造一种密码 $E: K \times X \to X$，其中 K 是密钥空间，X 是明文和密文空间。

基本 FPE 强调明文和密文处于相同的消息空间，即具有相同的格式。以信用卡号为例，要求密文和明文是具有相同长度的十进制数。事实上，分组密码算法本身就是某种形式的 FPE，它是由分组长度 m 决定的$\{0,1\}^m$ 字符串集合上的置换，然而 FPE 的概念远远超出了分组密码的范畴，FPE 要处理的待加密消息空间更加复杂。比如日历表 YYYY-MM-DD 不仅具有长度为 10 的字符串的限制，还需要满足特定位置是字符 '–' 以及年、月、日在合理范围内等格式要求。

为了完整地描述 FPE 问题，定义集合 W 为格式空间，对于任意给定的格式 $w \in W$，其对应于待加密消息空间的子空间 X_w，FPE 与集合 $\{X_w\}_{w \in W}$ 有关。把 X_w 叫作由格式 w 决定的待加密消息空间的一个分片，每个分片都是一个有限集。当给定密钥 k，格式 w 和调整因子 t 后，FPE 就是一个定义在 X_w 上的置换 $E_k^{w,t}$。

定义 2(一般化 FPE)。一般化 FPE 问题可以描述为一个函数 $E: K \times W \times X \times T \to X \cup \{\perp\}$，其中 K 为密钥空间，O 为格式空间，T 为调整因子空间[13]，X 为消息空间，所有空间都非空且 $\perp \notin X$。

一般化 FPE 可以通过算法三元组 *fpe* = (*setup, encryption, decryption*)来描述。

算法 ***setup***。初始化系统参数 *params*，不同 FPE 模型需要初始化的系统参数有所差异，但通常包含以下 3 部分内容。

1) 初始化具有足够安全性的对称加密算法所需的参数，通常包括轮次数、轮函数和分组长度等。

2) 初始化待解决的问题域，包括明确格式 w 及由其确定的待加密消息空间 X_w。

3) 初始化用于加解密的对称密钥 k，该对称密钥需要安全存储，不对外公开。

算法 ***encryption***。输入为调整因子 t 和明文 x，返回一个在分片 X_w 内的密文 y 或者 $\perp$。该算法执行 $E_K^{W,T}(X) = E(K,W,T,X)$ 的过程，$E_K^{W,T}(\cdot)$ 是 X_W 上的一个置换。如果 $x \in X_w$，则返回 $y = E_k^{w,t}(x)$；否则返回 $\perp$。

算法 ***decryption***。输入为调整因子 t 和密文 y，返回相同分片 X_w 内的明文 x 或者 $\perp$。该算法是 *encryption* 的逆运算，定义如下：$y \in X_w$，则返回 $D_k^{w,t}(y) = x$，否则返回 $\perp$。

3　加密模型分析

Black 和 Rogaway[5]提出的 3 种构建 FPE 方案的基本方法，成为后来 FPE 模型设计的主要参照。已提出的 FPE 模型或方案及其所采用的基本方法如表 1 所示。

由表 1 可以看出如下结果。

1) Generalized-Feistel 方法得到了更多的关注。

FFSEM、FFX 和 BPS 等模型都使用了 Feistel 网络[12]来设计对称密码，在 Feistel 网络中所使用的伪随机函数通常用到了传统的分组密码，比如 AES、3DES 等，具备可证明的安全性和实用性。

Feistel 网络是目前主流的分组密码设计模式之一，其最大优点是保证了加解密的相似性：解密过程就是对密文逆序使用子密钥的加密过程，这使得在实际应用中不需要对加解密算法分别实现，降低了成本。Feistel 网络由于 DES 的公布而广为人知，当前已被许多分组密码所采用。

表 1 保留格式加密模型或方案

年份	模型或方案	问题域	基本方法			
			Prefix	Cycle-walking	Generalized-Feistel	Others
2008	A scheme for Social Security Numbers[7]	Social Security Numbers	√		√	
2008	FFSEM[8]	Integer field Z_n={0, 1, 2, …, n-1}		√	√	
2009	Rank-then-Encipher[9]	Arbitrary regular language				√
	Integer FPE[9]	Integer field Z_n={0, 1, 2, …, n-1}			√	
2009	FFX[10]	$chars^n$ where *chars* is a finite alphabet			√	
2009	A scheme based on Thorp Shuffle[6]	Integer field Z_n={0,1, … ,n-1} where $2^{20}\leq n\leq 2^{50}$			√	
2010	BPS[11]	$chars^n$ where *chars* is a finite alphabet			√	

基于 Feistel 网络的 FPE 加密模型通常具有以下特点。

① 通常与 Cycle-walking 方法结合使用。在表 1 中，只有 FFSEM 在内部构造中结合了 Cycle-walking 方法，事实上在使用基于 Feistel 网络的加密模型解决任意有限域上的 FPE 问题时，与 Cycle-walking 方法相结合是一种通用的做法。

② Luby 和 Rackoff[12]证明了当 Feistel 密码的分组长度为 $2m$ 且攻击者拥有的明文密文对少于 $2^{m/2}$ 时，基于 Feistel 网络的分组密码是安全的。如果用更多轮次运算替代 Generalized-Feistel 方法中的 3 轮运算，攻击者至少拥有 2^m 的明文密文对才可能破译密码[14]。

2) FPE 模型的设计思想逐渐向如何降低问题域的复杂性方向发展。

FPE 问题的复杂性除了表现在保留数据格式上外，还表现在待解决消息空间的复杂性上，这种复杂性使得研究人员很难发现广泛适用于不同消息空间的通用解决办法。待解决消息空间越复杂，FPE 问题也就越难解决。

2002 年提出的构建 FPE 的基本方法已经一定程度上解决了整数域内的 FPE 问题，近年来提出的模型则将解决的问题域由整数域 Z_n 扩展到 $chars^n$。但是，已提出的模型只能解决一般 $chars^n$ 上的 FPE 问题，在更复杂的有限制的 $chars^n$ 问题域上，这些模型并没有太好的解决办法，通常需要结合 Cycle-walking 方法来解决。2009 年提出的 RtE 模型[9]，即 rank-then-encipher（排序后加密）模型，则将问题域进一步扩展到由任意正则语言描述的消息空间。

在解决复杂问题域上的 FPE 问题时，2 个典型的 FPE 模型，即 RtE 模型和 FFX 模型，它们都不是在复杂的问题域上直接寻求 FPE 问题的解决办法，而是将 FPE 问题转移到等价的具有较低复杂度的整数域上。

RtE 模型的基本思想在于对消息空间内的元素先排序后加密，将解决复杂有限域上的 FPE 问题转化到建立索引与元素的对应关系和设计整数 FPE 算法上来。为了实现对元素的排序，需要有效地描述消息空间，对于消息空间的一种描述方式是采用正则语言。Martinez[15]对可用正则语言描述的消息空间，介绍了高效的 *rank* 和 *unrank* 算法。

RtE 模型如图 1 所示，加密过程首先执行 *rank* 算法，获得明文 x 在消息空间中的索引 i；然后利用整数 FPE 方案加密 i 为 j；最后使用 *unrank* 算法，返回消息空间中索引为 j 的元素 y 作为对 x 加密的结果。

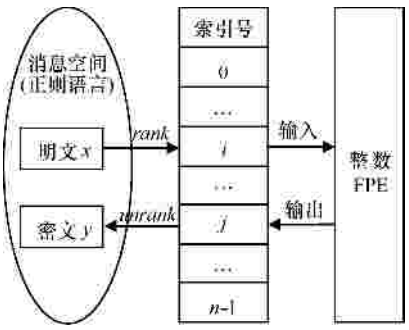

图 1 RtE 模型

解决 $chars^n$ 上 FPE 问题的 FFX 模型的主要思想则在于：给定字母表并描述为 $chars=\{a_0,a_1,a_2,\cdots,a_{radix-1}\}$，表中元素个数为 *radix*，称之为阶数；然后，将字母表重定义为 $chars=\{0,1,2,\cdots,radix-1\}$，这样就建立了字符 a_i 与数字 i 的一一映射关系。

FFX 模型如图 2 所示，加密过程首先根据建立的映射，将 n 位长度的明文 x 中的每个字符替换为

其在 $chars=\{0,1,2,\cdots,radix-1\}$ 中对应的数值，从而可将明文 x 映射为 $(Z_{radix})^n$ 中的字符串 i，将字符串 i 作为输入参与指定类型和轮数的 Feistel 网络运算，输出为 $(Z_{radix})^n$ 域内的另一元素 j，然后重新替换为字母表中的字母而得到密文。

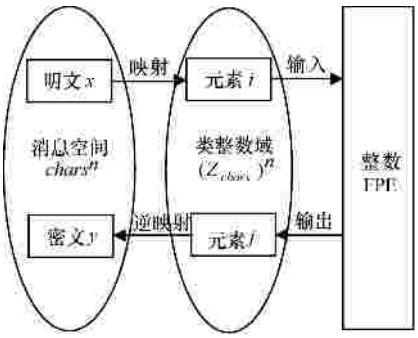

图 2　FFX 模型

4　编码后加密的 FPE 模型

RtE 模型和 FFX 模型的共同点在于：在解决待加密消息空间内的 FPE 问题时，以某种合理的方式，建立问题域与整数域的双射关系，从而将原始 FPE 问题转化到整数域上。事实上，FFX 模型中非平衡 Feistel 网络的运算过程的输入输出可视为固定长度为 n 的 $radix$ 进制数，是一种类整数域上的 FPE 问题的解决过程，不需要特别区分对待。

这种建立双射的过程是一种“编码”的过程，即将原始待加密消息空间内的元素，以合理的方式，映射为整数域内的唯一值。这种将复杂问题域上的 FPE 问题，通过编码方式转化到整数域上的 FPE 问题的办法，是一种通用的全新的 FPE 加密模型，称为“编码后加密”(coding-then-encipher)模型，简称为 CtE 模型。

4.1　CtE 模型

CtE 模型如图 3 所示。该模型包括 2 部分：编码部分，将消息空间内的元素，以某种合理的编码手段，建立其与整数域内数值的一一对应关系；整数 FPE 部分，将整数域内某个元素的编码加密成另外的整数。

编码部分由可逆的编码运算和解码运算组成，编码运算将消息空间 X 内的元素映射为整数域内的整数，解码运算将整数反射为消息空间 X 内的元素。

能否在待加密消息空间内找到高效的编解码算法是该模型的关键，使用 CtE 模型的前提也在于设计高效的编解码算法。幸运的是，已有的研究成果，包括 FFX、RtE 等模型，为此提供了有益的参考：FFX 用字母在字母表中的位置来编解码；RtE 用 $rank$ 和 $unrank$ 过程来编解码。因此，从这个角度来说，RtE 和 FFX 都属于 CtE 范畴，而且 FFX 模型的编解码效率明显优于基于排序的 RtE 模型编解码效率。

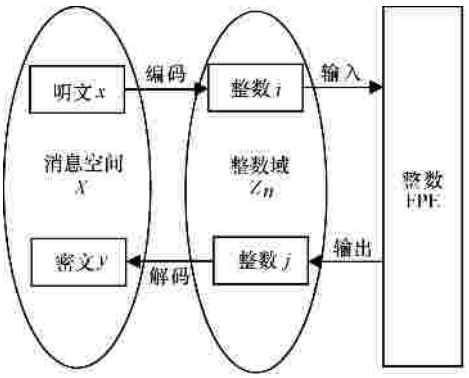

图 3　编码后加密模型

整数 FPE 部分并不限制所采用的整数 FPE 方案，目前已提出的 FFSEM、Generalized-Feistel 等方法都可以适用，当然，也可以基于 Feistel 网络自行设计安全高效的整数 FPE 方案。

4.1.1　算法描述

CtE 模型具体的算法描述如下。

算法 *setup*。初始化阶段主要确定。

1) 格式 w 及由其确定的待加密消息空间 X_w。

2) 编码和解码函数。对于待加密消息空间的分片 X_w，其上的编码函数可以描述为映射 $encode_w: X \to Z_{|X_w|} \cup \{\perp\}$，通过 $encode_w$ 算法可以将 X_w 内的元素 $x \in X_w$ 编码为 $i \in Z_{|X_w|}$，如果 $x \notin X_w$，则 $encode_w(x) = \perp$。与此对应，X_w 上的解码函数将一个整数映射为其在 X_w 中对应的元素，描述为 $decode_w: N \to X_w \cup \{\perp\}$。$decode_w$ 算法可以将 $j \in Z_{|X_w|}$ 解码为 X_w 内对应的元素 $y \in X_w$，如果 $j \notin Z_{|X_w|}$，则 $decode_w(j) = \perp$。

3) 用于解决整数域内 FPE 问题的方案 $integer\_fpe$。

算法 *encryption*。输入为 $integer\_fpe$ 方案所需的密钥 k、明文 x，输出为满足格式要求的密文 y。

加密过程可以用以下算法三元组来描述：$fpe\_encryption = (encode, integer\_fpe, decode)$。

算法 *encode*。输入为一明文 x，输出为其对应的编码 Cx。

$$Cx \leftarrow encode(x)$$

算法 *integer_fpe*。输入为明文的编码 Cx 和密钥 k，输出为密文的编码 Cy。

$$Cy \leftarrow integer\_fpe(k, Cx)$$

算法 *decode*。输入为密文的编码 Cy，返回密文 y。

$$y \leftarrow decode(Cy)$$

4.1.2 安全性分析

保留格式加密是一种特殊的对称密码，由于对称密码体制的基础模块是伪随机置换和伪随机函数，安全性通常可以归约到基础模块的安全性上，因此，对称密码体制的一个重要的安全目标是伪随机性。2002 年，Black 和 Rogaway[5]首次描述了保留格式加密的安全性，认为标准的安全目标就是 PRP（pseudorandom permutation）安全，要求攻击者不能区分是保留格式加密方案还是消息空间内置换集合中的某个随机置换。

设 $\mathrm{Perm}(X_w)$ 表示分片 X_w 上的所有置换的集合，$P \xleftarrow{R} \mathrm{Perm}(X_w)$ 表示随机抽取一个置换 P。设 A^f 是一个可以查询预言机 f 的攻击者，f 要么是 CtE 模型的加密预言 $E_k(\cdot)$，要么是一个随机置换预言 $P(\cdot)$。

为了定量描述攻击者区分保留格式加密方案和随机置换的能力，首先从 $\{0,1\}$ 中随机选择一个值：$b \xleftarrow{R} \{0,1\}$，然后从消息空间 X_w 上的置换集合 $\mathrm{Perm}(X_w)$ 中随机选取一个置换 P。

为了给攻击者足够多的攻击优势，允许攻击者执行两类查询：编解码查询及加密查询，并分别以编解码运算预言机 $Oracle(Coding)$ 和加密预言机 $Oracle(Enc)$ 对两类查询进行响应。编解码查询给予攻击者足够多的优势，允许其查询消息的编码或者根据编码来获得消息；加密查询则允许攻击者伪造任何的明文来获得加密后的密文，进而拥有足够多的明文密文对来获得对于攻击者有利的信息。

对于攻击者 A 的加密查询，加密预言机 $Oracle(Enc)$ 根据随机选取的 b 来决定采用 CtE 模型的加密预言还是随机置换来响应：如果 $b=0$，$Oracle(Enc)$ 以随机置换预言 $P(\cdot)$ 响应；如果 $b=1$，$Oracle(Enc)$ 以 CtE 模型的加密预言 $E_k(\cdot)$ 响应。

攻击者 A 的目标是：在执行一定次数的加密查询后，判定 $Oracle(Enc)$ 使用的是加密预言 $E_k(\cdot)$ 还是随机置换 $P(\cdot)$，也就是输出一个判定值 b'。如果 $b'=b$，说明攻击者 A 判定成功，相反失败。攻击者 A 在攻击过程中具有的优势可以描述为：$\mathrm{Adv}^{\mathrm{prp}}_{\mathrm{CtE}}(A) = 2\Pr[\mathrm{PRP}^A_{\mathrm{CtE}} \Rightarrow \mathrm{true}] - 1$，$\Pr[\mathrm{PRP}^A_{\mathrm{CtE}} \Rightarrow \mathrm{true}]$ 表示攻击者判定成功的概率。

因为 CtE 模型的加密预言 $E_k(\cdot)$ 实质上是整数 FPE 方案 *integer_fpe*，由其完成了整数域内消息编码的置换，所以上述攻击过程中攻击者 A 的对手实质上是整数 FPE 方案 *integer_fpe*，其具有的优势等同于：$\mathrm{Adv}^{\mathrm{prp}}_{\mathrm{CtE}}(A) = 2\Pr[\mathrm{PRP}^A_{integer\_fpe} \Rightarrow \mathrm{true}] - 1$。

可见，如果 *integer_fpe* 是随机置换，那么攻击者无法从 *integer_fpe* 中获得足够的优势。也就是说，CtE 模型的安全性依赖于所选择的整数 FPE 方案，如果采用安全的整数 FPE 方案，那么该模型就达到了 PRP 安全。

4.2 随机基准值的加密方案

下面将描述一个 CtE 模型的具体方案，称为“随机基准值的加密方案”，用于解决 $chars^n$ 上的 FPE 问题。基本思想是：在待加密消息空间中产生随机字符串作为基准值，通过设计合理的编解码算法，将 $chars^n$ 内的元素基于该基准值编码为整数域内某个数值，然后在整数域内执行整数 FPE 算法，最后根据解码运算，将加密后的整数解码成消息空间内的元素。

4.2.1 算法描述

由于 CtE 模型的重点在于编解码算法的设计，因此下面重点描述编解码算法。

该加密方案将在初始化阶段确定有限字母表 *chars* 及由其决定的消息空间 $X=chars^n$、调整空间 T 和密钥空间 K 等，然后随机选取消息空间内某元素作为基准值 rB，进而确定采用的编解码运算为基于基准值求偏移量的算法 *pos* 和 *unpos*。

为了有效地将 $chars^n$ 内的元素映射到整数域，一个可采纳的 *pos* 和 *unpos* 方案(如图 4 所示)描述如下。

1) 为待加密消息空间 $chars^n$ 任意指定一种全序“p”，$m = |chars^n|$ 表示 $chars^n$ 中的元素数目，$p_x = |\{y \in chars^n : y \,\mathsf{p}\, x\}|$ 表示“p”顺序下字符串 x 在 $chars^n$ 中的位置。

2) 通过计算相对于随机基准值的模 m 偏移量，可以建立从整个待加密消息空间到整数集合 $\{0,1,\cdots,m-1\}$ 的双射。

```
Algorithm pos(x, rB, m)
    Cx? m+p_x - p_rB    mod m;
 return Cx;

Algorithm unpos(Cy, rB, m)
    Cy? Cy + p_rB    mod m;
    C is the Cy-th string in chars^n ;
```

图 4　*pos* 和 *unpos* 算法

例如，当 $chars = \{a, b, c, d, \cdots, z\}$，$n = 3$ 时，假设随机生成的基准值 $rB = aap$，为 $chars^n$ 所指定的“ｐ”为字典序，即 a ｐ b ｐ Ｌ ｐ z。考虑利用随机基准值加密方案对字符串 *abc* 进行加密。首先通过字典序可以计算 $p_{rB}=l_a\times|chars|^2+l_a\times|chars|^1+l_p\times|chars|^0=15$，$p_{abc}=l_a\times|chars|^2+l_b\times|chars|^1+l_c\times|chars|^0=26+2=28$，这里 l_x 表示字符 x 在字符表 *chars* 中的位置。因此字符串 *abc* 进行 *pos* 后的结果为 $(|chars^n| + p_{abc} - p_{rB}) \bmod |chars^n| = 13$，执行整数 FPE 算法后有 $Cy = integer\_fpe(13, k)=1\ 987$，再执行 *unpos* 操作，$Cy = (Cy + p_{rB}) \bmod |chars^n| = 2\ 002$，对应于 $chars^n$ 中的字符串 *cza*。由此可得 *abc* 的加密结果为 *cza*。

需要说明的是，以上的偏移量算法只适合于元素呈线性分布并且任意 2 个相邻合法元素的距离都相等的消息空间。$chars^n$ 的这种元素线性等距的特性可以保证在指定基准元素和任意 2 个相邻元素的距离为单位长度后，消息空间中的任意点都可以通过其相对于该基准元素的距离偏移量来表示，从而把 $chars^n$ 双射到了整数域中。

但是，并不是所有的消息空间都具有元素线性等距的特性，例如 Bellare [10] 就提出了这样一个问题：设 validSSN(x)是一个谓词，可根据固定的有效性标准，对任意给定的 9 位十进制数 x，返回 true 或 false。那么，该问题的待加密消息空间由满足 validSSN(x)为 true 的 9 位十进制数的字符串 x 组成。此消息空间中的点都是线性的（存在数值上的线性关系），但是任意相邻两点并不一定等距，当得到密文的偏移量时，无法通过基准值找到其对应的密文，因此在此情况下，随机基准值的加密方案并不适用。

还有更复杂的元素非线性或距离不可度量的消息空间，在此类空间中相对于基准值的同一偏移量可能与多个点相对应（元素非线性）或者消息空间中任意两点的距离无法度量（不可度量），基于随机基准值的加密方案也是不适用的。

4.2.2　效率分析

CtE 模型的提出，使得研究者只需要关注从原始消息空间到整数域的双射的建立和整数 FPE 算法的设计。如果有高效的编解码算法将待加密元素映射为某个整数，以及将加密后的整数值映射回原始消息空间，那么 CtE 方法将是高效的。也就是说，CtE 方法的重点在于待加密消息空间中分片的 *encode* 和 *decode* 算法。

作为 CtE 模型的实现形式，RtE 模型采用了基于 *rank* 和 *unrank* 的编解码方法，Bellare[9]给出了一种适用于任意正则语言的排序算法，利用该排序算法对原始消息空间中的元素进行排序，可以将其一一映射到整数域中；FFX 模型利用输入字符串中字母在字母表中的位置来进行编解码，该模型通过将字母表重定义为 $chars=\{0,1,2,\cdots,radix\text{-}1\}$，建立字符 a_i 与数字 i 的一一映射关系，从而可把取自于字母表 *chars* 中的长度为 n 的字符串映射到一个类整数域中。随机基准值加密方案，类似于 FFX，将字母表重定义为 $chars=\{0,1,2,\cdots,radix\text{-}1\}$，并将输入字符串视为长度为 n 的 *radix* 进制数，在消息空间内随机产生一个基准字符串，通过相对该基准字符串所对应 *radix* 进制数的模 $radix^n$ 偏移量的计算，可以将原始消息空间映射到 Z_{radix^n} 中。

此 3 种方法在处理 $chars^n$ 上 FPE 问题时，其编解码算法的时间复杂度如表 2 所示。

表 2　FPE 方案的编解码算法时间复杂度

FPE 方案	时间复杂度
基于 RtE 的 $chars^n$ 解决方案	$O(n\|chars\|)$
基于 FFX 的 $chars^n$ 解决方案	$O(1)$
随机基准值加密方案	$O(1)$

由表 2 可知，在处理 $chars^n$ 上的 FPE 问题时，随机基准值加密方案的 *encode* 和 *decode* 算法均可在 $O(1)$时间复杂度下完成，与 FFX 模型具有相似的时间复杂度，而比 RtE 模型中基于排序的 *rank* 和 *unrank* 有大幅度的效率提升。

5　结束语

随着 2008 年 Voltage 公司 FPE 白皮书[7]的公布，FPE 问题逐渐成为密码学领域中的一个研究热点。当前已经有了一些研究成果：已提出的 FPE 模型为特定领域内的 FPE 问题提供了较好的解决办法，尤

其是整数域内的FPE问题已经具有成熟、安全、高效的解决方案；对于更复杂的 $chars^n$ 问题域上的FPE问题，也已经提出了多个相关的加密模型，这些已提出的模型多数在构造过程中使用了Feistel网络。通常要解决的问题域复杂度越高，FPE问题越难解决，因此，FPE模型的设计思想逐渐向如何降低问题域的复杂性方向发展，无论是RtE模型还是FFX模型，它们都不是在复杂的问题域上直接寻求FPE问题的解决办法，而是将FPE问题转移到等价的具有较低复杂度的整数域上。

本文研究分析了已提出的FPE模型的特性，进而提出了“编码后加密”的FPE模型，该加密模型主要包括2部分：编码部分和整数FPE部分。编码部分由编码运算和解码运算组成，编码运算将消息空间 X 内的元素映射为某个整数，解码运算将整数反射为消息空间 X 内的元素，能否在待加密消息空间内找到高效的编解码算法是该模型的关键；整数FPE部分则用于解决整数域内的FPE问题。进而，提出了该模型在 $chars^n$ 问题域的典型方案：基于随机基准值的加密方案，指出该方案具有较高的效率，并深入分析了编解码运算的算法设计，指出这种基于偏移量计算的编解码方法只适合于元素线性等距的消息空间，而对于元素线性变距消息空间，以及更复杂的元素非线性或距离不可度量的消息空间，本文提出的偏移量的编解码方法并不适用。

对于任意有限域上的FPE问题，本文所提出的FPE模型并没有突出贡献，同FFX和RtE模型一样，需要结合Cycle-walking来实现，除此之外，Bellare认为密集编码对解决该问题也非常有用[10]。本文也没有深入研究消息空间的编码理论，以及如何设计高效的编解码算法，这些相关研究对于更复杂问题域上的FPE问题解决都是有实际意义的。

参考文献：

[1] PCI Security Standards Council. Payment Card Industry Data Security Standard[S]. 2006.

[2] RADHAKRISHNAN R, KHARRAZI M, MEMON N. Data masking: a new approach for steganography[J]. Journal of VLSI Signal Processing, 2005, 41(3): 293-303.

[3] National Bureau of Standards. FIPS PUB 74. Guidelines Implementing and Using the NBS Data Encryption Standard[S]. 1981.

[4] SMITH H, BRIGHTWELL M. Using datatype-preserving encryption to enhance data warehouse security[A]. NIST 20th National Information Systems Security Conference[C]. 1997. 141.

[5] BLACK P, ROGAWAY P. Ciphers with arbitrary finite domains[A]. Topics in Cryptology-CT-RSA'02[C]. Springer, 2002. 114-130.

[6] MORRIS B, ROGAWAY P, STEGERS T. How to encipher messages on a small domain[A]. Cryptology-CRYPTO'09[C]. 2009.

[7] SPIES T. Format preserving encryption unpublished white paper[EB/OL]. http://www.voltage.com, 2008.

[8] SPIES T. Feistel finite set encryption mode[EB/OL]. http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/ffsem/ffsem-spec.pdf.

[9] BELLARE M, RISTENPART T, ROGAWAY P, *et al*. Format- preserving encryption[A]. Selected Areas in Cryptography (SAC 2009)[C]. Springer, 2009.

[10] BELLARE M, ROGAWAY P, SPIES T. The FFX mode of operation for format-preserving encryption[EB/OL]. http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/ffx/ffx-spec.pdf.

[11] BRIER E, PEYRIN T, STERN J. BPS: a format-preserving encryption proposal[EB/OL]. http://brutus.ncsl.nist. gov/groups/ ST/toolkit/BCM/documents/proposedmodes/bps/bps-spec.pdf.

[12] LUBY M, RACKOFF C. How to construct pseudorandom permutations and pseudorandom functions[J]. SIAM J, Computing, 1988,17(3): 373-386.

[13] LISKOV M, RIVEST R, WAGNER D. Tweakable block ciphers[A]. CRYPTO 2002[C]. Springer,2002. 31-46.

[14] PATARIN J. Security of random Feistel schemes with 5 or more rounds[A]. Cryptology–CRYPTO'04[C]. Springer, 2004. 106-122.

[15] MARTINEZ A. Topics in Formal Languages: String Enumeration, Unary NFAs and State Complexity[D]. University of Waterloo, 2002.

作者简介：

刘哲理（1978-），男，山东潍坊人，博士，南开大学博士后，主要研究方向为密码学、智能卡操作系统。

贾春福（1967-），男，河北文安人，博士，南开大学教授、博士生导师，主要研究方向为息安全与可信计算、恶意代码发现与分析。

李经纬（1987-），男，四川成都人，南开大学硕士生，主要研究方向为密码学。