DOI:10.13471/j.cnki.acta.snus.2013.01.001

第 52 卷 第 1 期 中山大学学报（自然科学版） Vol. 52 No. 1
2013 年 1 月 ACTA SCIENTIARUM NATURALIUM UNIVERSITATIS SUNYATSENI Jan. 2013

基于混淆器的安全对称密码方案*

袁 征[1,2]，龚高翔[1,2]
（1. 北京电子科技学院，北京 100070；
2. 西安电子科技大学 通信工程学院，陕西 西安 710071）

摘 要： 提出基于多比特输出点函数混淆器的、具有“动态”密钥的对称密码方案。满足完全熵的多比特输出的点函数混淆器（MBPFO）等同于一个具有“错误密钥检测性”的语义安全的对称密码功能，该方案用此混淆器实现了对称密码方案，方案用双密钥通过敏感函数构造的“动态”密钥，可以实现类似“一次一密”的密码体制功能，因此该方案具有更高安全性，并且实现简单。

关键词： 混淆；对称密码；具有多比特输出点函数混淆器；敏感函数
中图分类号： TP309 **文献标志码：** A **文章编号：** 0529－6579（2013）01－0007－05

Secure Symmetric Encryption Scheme Based on Obfuscator

YUAN Zheng[1,2]，*GONG Gaoxiang*[1,2]
（1. Beijing Electronic Science & Technology Institute，Beijing 100070，China；
2. Communication Engineer Institute，Xidian University，Xi′an 710071，China）

Abstract: An symmetric encryption scheme with dynamic key based on obfuscation of point functions with multibit output（MBPF）is presented. A MBPF obfuscator with fully-entropic security，implying virtual black-box property（VBB），can be used to construct semantically secure encryption schemes with wrong key detection for $\alpha(n)$-weak keys. The symmetric encryption scheme is just the fully-entropic security MBPF obfuscator，whose key is deduced by a sensitive function . The sensitive function with two inputs，one is a secret key and another is a random key，and thus output key is random. The symmetric encryption scheme is more secure and implement simple.

Key words: obfuscation；symmetric encryption；Obfuscating point functions with multibit output；sensitive function

密码学中的对称密码算法具有速度快、容易实现、安全强度高、易于同步等特点，被广泛应用在互联网中。但是对称密码算法也存在密钥更换困难、用同一密钥加解密容易给敌手提供破解密钥的信息和时间等缺陷。本文利用混淆器设计了一个对称密码方案。所谓混淆器就是输入一个程序（例如，图林机，或者回路）[1]，输出一个与原始程序功能相同的新的程序的（有效的）算法，且输出的程序还具有“难以识别性”。此概念要求混淆器表现的像一个“黑盒”。由于具有多比特输出的点函数混淆器具有对称密码的特点和其它优点[2]，本文利用多比特输出的点函数混淆器构造的加密方案不仅具有很高的安全性，而且实现了“动态”密钥[3]。

* 收稿日期：2012－04－01
基金项目：国家自然科学基金资助项目（61070250）；北京市自然科学基金资助项目（4132066）；“十二五”国家密码基金资助项目（MMJJ201101026）；信息安全国家重点实验室基金资助项目（01－01，01－02－6）；中办信息安全重点实验室基金资助项目（YZDJ0905）
作者简介：袁征（1968 年生），女，教授；E-mail：yuanzheng@besti.edu.cn；zyuan@tsinghua.edu.cn

1 虚拟黑盒混淆与点函数混淆器

首先介绍混淆中最基础的概念——虚拟黑盒混淆[4]，然后介绍具有多比特输出点函数混淆器[2]。

1.1 虚拟黑盒混淆

一个算法 O，其输入为族 c 中的一个回路，输出一个新的回路，被称为族 c 的黑盒混淆器。如果算法 O 有如下三个特性，就被定义为虚拟黑盒混淆:

1) 保留功能性: 存在一个可以忽略的函数 $neg(n)$，使得对于任意输入长度 n 和每一个 $C \in C_n$，有:

$$Pr[\exists x \in \{0,1\}^n: O(C)(x) \neq C(x)] \leqslant neg(n) \tag{1}$$

式(1)是在随机 Oracle（预言机）和 O 的 coin（投硬币）上的概率。

2) 多项式递减性: 存在一个多项式 $p(n)$，使得对于所有有限多的输入长度和每一个 $C \in C_n$，混淆器 O 仅能把 C 扩大 p: $|O(C)| \leqslant p(|C|)$ 的一个因子。

3) 虚拟黑盒特性（VBB): 对于任意多项式大小回路敌手 A，存在一个多项式大小模拟器回路 S 和一个可以忽略的函数 $neg(n)$，使得对于每个输入长度为 n 和每个 $C \in C_n$，有:

$$|Pr[A(O(C)) = 1] - Pr[S^C(1^n) = 1]| \leqslant neg(n) \tag{2}$$

式(2)是在敌手、模拟器和混淆器的 coin（投硬币）上的概率。

虚拟黑盒混淆器 O 是运行在多项式时间内的，所以是有效的[5]。

1.2 具有多比特输出的点函数混淆

设 $I_{(k,m)}: \{0,1\}^* \cup \{\perp\} \to \{0,1\}^* \cup \perp$ 表示为函数:

$$I_{(k,m)}(x) = \begin{cases} m & x = k \\ \perp & \text{其它} \end{cases} \tag{3}$$

若给定密钥 k，式(3)输出消息 m，否则输出 $\perp$。设 $I = \{I_{(k,m)} \mid k,m \in \{0,1\}^*\}$ 为所有这样函数的族，被称为具有多比特输出点函数族，简称多比特点函数（MBPF)。

定义1（具有多比特输出的点函数混淆 MBPFO)[2] 一个多比特点函数（MBPF）混淆器是一个概率多项式时间算法 O，其输入 (k,m) 值，描述为一个函数 $I_{(k,m)} \in I$，输出一个回路 C，记为 $O(I_{(k,m)})$。但是这里一直假设 O 把 k 和 m 作为描绘的输入。满足如下条件:

1) 正确性: 对于所有的 $(k,m) \in \{0,1\}^*$，$|k| = n$，$|m| = poly(n)$，所有的 $x \in \{0,1\}^n$，满足:

$$Pr[C(x) \neq I_{(k,m)}(x) \mid C \leftarrow O(I_{(k,m)})] \leqslant negl(n) \tag{4}$$

式(4)是混淆器算法的随机性上的概率。

2) 多项式递减性: 对于任意的 k,m，回路 $C = O(I_{(k,m)})$ 的大小是在 $|k| + |m|$ 上的多项式。

3) 熵安全性: 如果对于任意有1比特输出的概率多项式时间敌手，任意多项式 $l(.)$，存在一个概率多项式时间模拟器 S，使得对于所有的联合分布 $\{X_n, Y_n\}_{n \in \mathbf{N}}$，(其中 $X_n \in \{0,1\}^n$，$Y_n \in \{0,1\}^{l(n)}$，$H_\infty(X_n) \geqslant \alpha(n)$)，满足式(5)，就说该方案具有 $\alpha(n)$ -熵安全性:

$$|Pr[A(O(I_{(k,m)})) = 1] - Pr[S^{I_{(k,m)}, l(.)}(1^n) = 1]| \leqslant negl(n) \tag{5}$$

式(5)是 $(k,m) \leftarrow (X_n, Y_n)$ 的随机性、混淆器 O 的随机性和 A,S 的随机性上的概率。

如果对于所有的 $\alpha(n) \in \omega(\log(n))$，方案具有 $\alpha(n)$ -熵安全，就说该方案具有完全熵安全性。完全熵安全性暗示着虚拟黑盒特性（VBB)，但反过来不一定。

2 构建一个基于混淆器的安全对称密码方案

本部分首先介绍具有多比特输出点函数混淆器与对称密码之间的关系。把一个公共私钥和一个随机密钥（公开的）作为输入，通过一个敏感函数产生“动态”密钥，然后构造出一个“随机”的多比特输出点函数混淆器，此混淆器具有“动态”密钥的对称密码功能。

2.1 具有多比特输出点函数混淆器（MBPFO）与对称密码之间的关系

此部分介绍了具有多比特输出点函数混淆器暗示了一个非常强对称密码类型（也叫着数字锁[7])。

定义2（错误密钥检测[8]） 如果对于所有的 $k \neq k' \in \{0,1\}^n$，所有 $m \in \{0,1\}^{poly(n)}$，有 $Pr[Dec_{k'}(Enc_k(m)) \neq \perp] \leqslant neg(n)$，就说这个加密方案满足错误密钥检测。

根据文献[8]，有如下定理。

定理1 令 $\alpha(n) \in w\{\log(n)\}$，对于 $\alpha(n)$ -弱密钥，存在满足错误密钥检测的语义安全加密

方案的充分必要条件是对于消息独立，存在 $\alpha(n)$ – 熵安全 MBPF 混淆器。用“完全”代替“$\alpha(n)$”，该定理也成立。

用定理 1 构造（MBPFO 到对称密码）。设 O 为一个消息独立的 MBPF 混淆器，定义（概率的）加密算法 $Enc_k(m) = O(I_{(k,m)})$ 和解密算法 $Dec_k(c) = C(k)$，其中 C 被理解为一个多比特输出点回路（MBPC），k 是从密钥 D_n 域中选取的一个密钥。

这里“MBPFO”和“对称密码”的概念是平等的: 首先它们满足相同的正确性，特别是给定密钥，加密方案允许恢复消息; 同样式（3）中给定 k，MBPFO 允许恢复 x。其次，它们有相似的保密要求，除非给定 k，式（3）的函数 $I_{(k,m)}(x)$ 混淆隐藏了特殊的输出 m; 同样除非敌手拥有密钥，对称密码隐藏了消息。但是，二者的不同是 MBPFO 的定义域是所有可能输入的 k，而对称密码不能定义在错误密钥上，换句话说，至少在概念上认为 MBPFO 为对称密码的特殊形式，通过解密算法，错误密钥被迅速检测出来。

2.2　基于混淆器的安全对称密码方案

与以前的对称密码相比，我们的对称密码方案的加密算法被一个具有对称密码功能的多比特输出的点函数混淆器所替代。而我们的加密方案的密钥是“动态”的，改变了以前对称密码方案中密钥的不变性。在敏感函数作用下产生的“动态”密钥，增加了我们的对称密码方案的安全性。

用户甲和乙协商确定多比特输出点函数混淆算法 O、私钥 k_1 和敏感函数 H，具体对称密码方案如下:

1）用户甲: 任意选择一个公开的密钥 k_2，并计算 $k = H(k_1, k_2)$;

2）用户甲: 用具有对称密码功能的多比特点函数混淆算法 O 和密钥 k，对需要混淆加密的明文 m 进行混淆加密，得到混淆后的密文 $c = Enc_k(m) = O(I_{(k,m)})$;

3）用户甲: 在公共信道上，把 k_2 和 c 同时传送给用户乙;

4）用户乙: 接收到密文 c 和密钥 k_2 后，根据私钥 k_1 和 k_2，计算 $k = H(k_1, k_2)$;

5）用户乙: 用以上的解密算法和 k，对密文 c 进行解密，得到明文 $m = Dec_k(c) = C(k)$。

以上方案中，私钥 k_1 需要通过秘密通道交换协商，密钥 k_2 在混淆加密时随机选择。k_1 和 k_2 的选择相互无关，无论给出多少个 k_2，都不会推出 k_1; k_1 和 k_2 对于 H（敏感函数）的敏感性，k_1 和 k_2 的细微变化都会引起 $k = H(k_1, k_2)$ 的明显变化，使产生的结果具有很好的扩散性与混淆性。

3　基于混淆器的对称密码方案的性能分析

3.1　对称密码方案的正确性

定理 2　基于 MBPFO 的对称密码方案是正确的。

证明　令加密密钥 $k = H(k_1, k_2)$、解密密钥为 $k' = H(k_1, k'_2)$，通过错误密钥检测证明正确性:

因为

$$Dec_{k'}(c) = C(k'), Enc_k(m) = O(I_{(k,m)}) \quad (6)$$

任取 $m \in \{0,1\}^{poly(n)}$，有:

$$m = Dec_{k'}(Enc_k(m)) = Dec_{k'}(O(I_{(k,m)})) \quad (7)$$

因为我们基于的多比特输出的点函数混淆器（MBPFO）是完全熵安全的，所以我们的对称密码方案满足错误密钥检测功能，即: 若 $k \neq k' \in \{0,1\}^n$，则: $pr[Dec_{k'}(Enc_k(m)) \neq \perp] \leqslant neg(n)$，

所以，当且仅当 $k = k'$ 时，$m = Dec_{k'}(Enc_k(m)) = Dec_{k'}(O(I_{(k,m)})) = C(k) = m$，正确。

3.2　“动态”密钥的安全性分析

“一次一密”密码体制的密钥是随机产生的，其明文、密文和密钥三者是相互独立的，敌手不能从密文中获得关于明文或者密钥的任何消息，即使敌手获得一些密文及所对应的明文，也只能得到相应的密钥，而不能得到其它密文对应的明文或者密钥。因此“一次一密”的密码体制在理论上被认为是绝对安全的[10]。

我们的对称密码方案虽然与传统的“一次一密”密码体制不同，但是通过随机密钥 k_2，可以实现类似于“随机”的密钥 k。我们的对称密码方案还解决了传统“一次一密”密码体制中密钥管理困难问题。实际上，如果函数 H 满足对私钥 k_1 和随机密钥 k_2 的单射性质，也就是:

当 $k_1 \neq k'_1$，或者 $k_2 \neq k'_2$ 时，$H(k_1, k_2) \neq H(k_1', k_2')$　　(8)

我们的对称密码方案的安全性最高。

由于敏感函数 H 具有很强的敏感性，一般从混沌系统中选取[11]。在混沌系统中的特性之一就是对初值的敏感依赖性。这样 H 对私钥 k_1 和动态密钥 k_2 是敏感的，k_1 或 k_2 的细微变化，$k = H(k_1, k_2)$ 都会产生巨大的变化。这正如洛伦兹在一次演讲中生动地指出: 一只蝴蝶在巴西煽动翅膀，就有

可能在美国的德克萨斯州引起一场风暴。由于密钥在每次加密都在不断地变化，从而使得密文与明文之间具有很高的非线性特性，从而提高了对称密码方案的安全性能。

敏感函数对初始密钥和随机密钥敏感性的实验分析。我们从敏感性很好的混沌系统中选取一个敏感函数 H，敏感函数 H 定义如下:

$$H(k_1,k_2) = \mathrm{mod}(abs(round(F_{k_1,T}(t)\times k_2)),256) \tag{9}$$

其中，k_1 为敏感函数的初始密钥; k_2 为随机密钥; T 为一种采样规定; $F_{k_1,T}(t)$ 为采样后的混沌信号; $round$ 是四舍五入运算，abs 是取绝对值; mod 是取余。敏感函数的输出值是在 [0，255] 上的整数序列。

1) 敏感函数对 k_1 的敏感性分析: 令 $H_i(k_1, k_2)$ 为 $H(k_1,k_2)$ 的第 i 个元素、Δk_1 为 k_1 的误差，敏感函数 H 产生一个长度为 t 的序列

$$s = \{s(1),\ldots,s(t)\}: s(i) = \begin{cases} 0 & H_i(k_1,k_2) = H_i(k_1+\Delta k_1,k_2) \\ 1 & \text{其它} \end{cases} \tag{10}$$

显然，密钥序列 s 表明了 $H(k_1+\Delta k_1,k_2)$ 和 $H(k_1,k_2)$ 之间对应元素的变动情况。

参数 $p = \sum_{i=1}^{t} s(i)/n \times 100\%$ 表示当 k_1 在产生误差 Δk_1 时，由敏感函数产生的混沌序列中发生变化的元素占序列元素总数的百分比。该参数表示敏感函数对密钥 k_1 的敏感性。Δk_1 分别取值 10^{-9}，10^{-10},...,10^{-15}，进行实验，实验结果如表1。

表1 敏感函数 H 对初始密钥 k_1 的敏感性

Table 1 Sensitivity of sensitive function H on initial key k_1

Δk_1	10^{-9}	10^{-10}	10^{-11}	10^{-12}	10^{-13}	10^{-14}	10^{-15}
p/%	99.58	99.54	99.56	99.68	99.63	99.66	99.52

由此实验可知，初始密钥 k_1 的细微变化，敏感函数产生的密钥序列都会发生 99.5% 的变化。

2) 同样，敏感函数对于随机密钥 k_2 的敏感性分析也可以采用以上的 p 作为评估标准，只是序列定义成为:

$$s(i) = \begin{cases} 0 & H_i(k_1,k_2) = H_i(k_1,k_2+\Delta k_2) \\ 1 & \text{其它} \end{cases} \tag{11}$$

通过实验，同样也可以得到，随机密钥 k_2 的细微变化，序列密钥都会发生 99.5% 以上的很大的变化。

综上所述，从混沌系统选取的敏感函数 H 对密钥 k_1 和 k_2 是非常敏感的，所以方案的安全性很高。

3.3 对称密码方案的安全性

定理3 如果 O 是一个满足完全熵的 MBPF 混淆器，则 O 也满足虚拟黑盒混淆。

说明 此定理的具体证明思路方法是改编的条件到多比特集[9]，证明思路分为三步:

1) 如果一个混淆器 O 满足完全安全，则其满足分布的不可辨别性。

2) 如果一个混淆器 O 满足分布的不可辨别性，则其满足 Oracle（预言机）不可辨别性。

3) 如果一个混淆器 O 满足 Oracle（预言机）不可辨别性，则其满足虚拟黑盒性能。

定理4 基于满足完全熵的 MBPFO 的对称密码方案是安全的。

证明 对称密码方案安全性主要依赖于满足完全熵的多比特输出的点函数混淆器（MBPFO）的安全性和“动态”密钥的安全性。

根据前面定理3，我们对称密码方案基于的满足完全熵的 MBPFO，也满足虚拟黑盒混淆，是安全的混淆器。

根据前面定理1，对于独立消息，存在 $\alpha(n)$ -熵安全的 MBPFO，也存在有错误密钥检测的语义安全加密方案。令 C 为多比特输出点回路（MB-PC），$\forall k \in D_n$，由该多比特输出的点函数混淆器 O 到对称密码的表示是:

$$Enc_k(m) = O(I_{(k,m)}), \text{和 } Dec_k(c) = C(k) \tag{12}$$

根据文献[8]，有以下结论: ①对于 $\alpha(n)$ -弱密钥，存在 CPA 安全的、具有“错误密钥检测性”的对称密码方案的充分必要条件是: 对于独立消息，存在 $\alpha(n)$ -熵安全的、自我可组合的 MBPF 混淆器; ②对于 $\alpha(n)$ -弱密钥，存在密钥独立消息（KDM）的、具有“错误密钥检测性”的语义安全对称密码方案的充分必要条件是: 对于独立消息的标准概念，存在 $\alpha(n)$ -熵安全的 MB-PF 混淆器。

另外，我们所基于的混淆器还有如下优点: ①混淆后函数的难以识别，这给敌手攻击增加难度，此性质可以增加安全性; ②该混淆器可以同时对多个回路进行串行作用，大大提高了混淆器的运行速度。③在文[12]中，多比特输出的点函数混淆器暗示非常强的对称密码，对于密钥依赖消息和随

机弱密钥是安全的。④该混淆器包含弱密钥抵抗，以及具有密钥依赖消息安全的[13]。

综上所述，我们的基于满足完全熵的 MBPFO 的对称密码方案选用的加密算法是具有很高安全性的多比特输出的点函数混淆器，混淆本身还有结果难以识别等优点；而只要密钥 k_1 和 k_2 有细微变化，用敏感函数 H 得到的“动态”密钥 k 都会产生 99.5% 以上的变化，所以我们的方案的安全性很高。

4 结　语

满足完全熵的多比特输出的点函数混淆器(MBPFO)等同于一个具有“错误密钥检测性”的语义安全的对称密码功能，因此本文提出了一个基于该混淆器的对称密码方案，方案具有虚拟黑盒性能，保证了混淆的安全性，可以抵抗各种混淆攻击。用敏感函数产生该对称密码方案的“动态”密钥，敏感函数的输入是私钥 k_1(混沌系统的初始条件)和随机密钥 k_2，k_1 和 k_2 中任意一个发生微小的变化，由敏感函数产生的“动态”密钥 k 将发生 99.5% 以上的改变。加密者通过改变 k_2 使得每次加密都用不同的密钥 k，从而实现类似“一次一密”的密码体制功能，使得我们对称密码方案从密钥和算法两方面更加安全。

参考文献:

[1] BOAZ B, ODED G, RUSSELL I, et al. On the (im) possibility of obfuscating program [M]. CRYPTO, 2001: 1 - 18.

[2] CANETTI R, DAKDOUK R R. Obfuscating point functions with multibit output [C] // EUROCRYPT, Lecture Notes in Computer Science, 2008, 4965: 489 - 508.

[3] 陈鲁生, 沈世镒. 现代密码学 [M]. 北京: 科学出版社, 2002: 36.

[4] GOLDWASSER S, ROTHBLUM G N. On best-possible obfuscation [C] // Vadhan, S. P. ed. TCC 2007. LNCS, Springer, Heidelberg, 2007, 4392: 194 - 213.

[5] 史扬. 曹立明. 王小平 混淆算法研究综述 [J]. 同济大学学报: 自然科学版, 2005(6): 813 - 819.

[6] NIR B, RAN C. On strong simulation and composable point obfuscation [C] // CRYPTO, advances in Cryptology-CRYPTO 2010, 30th Annual Cryptology conference, Santa Barbara, CA, USA, August 15 - 19, 2010. Proceedings, 2010: 520 - 537.

[7] NIR B, OMER P. Point obfuscation and 3 - round zero-knowledge [EB/OL]. (2011 - 09 - 21) [2012 - 03 - 28]. http://eprint.iacr.org.

[8] CANETTI R, KALAI Y T, VARIA M. On symmetric encryption and point obfuscation [C] // Micciancio, D. (ed.) TCC 2010. LNCS, Springer, Heidelberg, 2010, 5978: 52 - 71.

[9] CANETTI R. Towards realizing random oracles: Hash functions that hide all partial information [C] // CRYPTO, Lecture Notes in Computer Science, Springer, 1997, 1294: 455 - 469.

[10] SHANNON C E. Communication theory of secrecy systems [J]. Bell Systems Technical Journal, 1949, 28: 656 - 715.

[11] 廖晓峰, 肖迪, 陈勇, 等. 混沌密码学原理及其应用 [M]. 北京: 科学出版社, 2009: 2 - 18.

[12] BITANSKY N, CANETTI R. On strong simulation and composable point obfuscation [EB/OL]. (2010 - 07 - 25) [2012 - 03 - 28]. http://eprint.iacr.org.

[13] HAITNER I, HOLENSTEIN T. On the (im) possibility of key dependent encryption [C] // TCC, 2009: 202 - 219.