基于循环移位置换的超伪随机置换的构造

余昭平 王晓东
(解放军信息工程大学电子技术学院 郑州 450004)

摘 要 为了优化 Luby 和 Rackoff 给出的 DES 型置换的构造，我们给出了一种基于循环移位置换的超伪随机置换的构造方法。新构造简化了构造的复杂性和基于随机预言模型的安全性证明，并指出：首末两轮循环移位置换和中间两轮 DES-型的随机置换的组合构造是超伪随机置换。新构造降低了区分优势的上界和敌手攻击成功的概率并降低了对首末轮函数的要求。

关键词 循环移位置换，伪随机性，超伪随机置换，随机预言模型
中图分类号：TN918 **文献标识码**：A **文章编号**：1000-5986(2006)05-0832-04

On the Construction of Super-Pseudorandom Permutations Based on the Rotation Permutations

Yu Zhao-ping Wang Xiao-dong
(*Institute of Electronic Technology, the PLA Information Engineering Universtity, Zhengzhou* 450004, *China*)

Abstract Towards making the construction method on the DES-model pseudorandom permutations given by Luby and Rackoff optimal and practical, a new construction method on pseudorandom permutations is provided. Based on the random oracle model by showing that two DES-model permutations are sufficient to be super-pseudorandom permutation together with initial and final rotation permutations, the complexity of construction is reduced samewhat and its proof of security is simplified The revised construction reduces the success probability of the adversary and the upper bound of advantage and also requirements of the first and the end functions.

Key words Rotation permutations, Pseudo-randomness, Super-pseudorandom permutations, Random oracle model

1 引言

Luby 和 Rackoff 在文献[1]中给出了一种包含四轮 DES 型置换的超伪随机置换 $\psi(f,g,h,e)$ 的构造，Goldreich 等人在文献[2]给出了基于伪随机发生器的伪随机函数的构造，Naor 和 Reingold[3] 给出基于陷门置换的构造。上述这些构造中都涉及非平凡计算(多项式时间)，因而试图最小化构造中所涉及伪随机函数的个数是有意义的。Moni Naor 和 Reingold 在文献[3]中提出 $\phi=h_1\circ\psi(f\circ g)\circ h_2$ 是超伪随机的，其中 h_1,h_2 是按位独立的置换。本文在此基础上给出了基于循环移位置换和 DES 型置换的超伪随机置换的构造模型，并改变了原有四轮 DES-型超伪随机置换构造模式，使得对第一和第四轮函数是随机或保密的通用散列函数的要求[4] 或第一和第四轮函数是按位独立置换的要求[3] 降低为 $\forall x\neq y$: $\mathrm{Prob}[h_1(x)_{|R}=h_1(x)_{|R}]\le 2^{-n}$ 和 $\mathrm{Prob}[h_2(x)_{|L}=h_2(x)_{|L}]\le 2^{-n}$，给出的循环移位置换满足上述要求并具有实用性，且使区分优势上界降低 $m^2/2^{2n}$ 。

2004-10-08 收到, 2005-04-07 改回
现代通信国家重点实验室基金 (5143601013JB0601) 资助课题

为节省篇幅，如无特别说明，本文中的有关定义和记号均与文献［3］和文献［4］相同。记 G 是预言机 M 可以询问的置换，M 的询问类型有两种:$(+,x)$ 表示询问“$G(x)$ 的值？”，$(-,y)$ 表示询问“$G^{-1}(y)$ 的值？”。记 M 的第 i 次询问应答结果为 $\langle x_i,y_i\rangle\in I_{2n}\times I_{2n}$，即 M 询问 $(+,x_i)$ 时得到的回答为 y_i，$(-,y_i)$ 时得到的回答为 x_i。记序列 $\{\langle x_1,y_1\rangle,\cdots,\langle x_m,y_m\rangle\}$ 为预言机 M 恰做 m 次询问的结果。记 M 的第 i 次询问的结果为前 $i-1$ 次询问结果对的函数 $C_M\left[\{\langle x_1,y_1\rangle,\cdots,\langle x_{i-1},y_{i-1}\rangle\}\right]$。

定义 1 令 $\rho=\{\langle x_1,y_1\rangle,\cdots,\langle x_m,y_m\rangle\}$ 是一个序列，对 $\forall i$, $1\le i\le m$，有 $\langle x_i,y_i\rangle\in I_{2n}\times I_{2n}$。若 ρ 满足对 $\forall i,1\le i\le m$，$C_M\left[\{\langle x_1,y_1\rangle,\cdots,\langle x_{i-1},y_{i-1}\rangle\}\right]\in\{(+,x),(-,y)\}$，则称 ρ 为 M 的可能的询问结果。

考虑对 M 询问应答的另外一种分布，考虑一个随机的过程 $\tilde{R}$，它关于 M 的第 i 次询问回答如下：

(1)如果 M 的第 i 次询问是 $(+,x)$，且存在某些 $1\le j<i$ 使得第 j 次询问的结果对是 $\langle x,y\rangle$，则 $\tilde{R}$ 的回答为 y。

(2)如果 M 的第 i 次询问是 $(-,y)$，且存在某些 $1\le j<i$ 使得第 j 次询问的结果对是 $\langle x,y\rangle$，则 $\tilde{R}$ 的回答为 x。

(3)如果 1，2 都不成立，则 M 的回答为一个均匀选择的 $2n$-比特串。

注：若 M 的询问结果中出现：$\langle x_j, y\rangle$和$\langle x_k, y\rangle (x_j \neq x_k)$或$\langle x, y_j\rangle$和$\langle x, y_k\rangle (y_j \neq y_k)$，则称 M 的询问结果是不一致的，否则称为是一致的。令 T_S 表示 M 的询问由 S 回答时的结果，T_R， $T_{\tilde{R}}$ 分别表示 M 的询问由 R 和 $\tilde{R}$ 回答时的结果，则 $M^{S,S^{-1}}(1^{2n}) = C_M(T_S)$， $M^{R,R^{-1}}(1^{2n}) = C_M(T_R)$。

定义 2　对于 $\forall f_1, f_2 \in H_n$ 和 $\delta_{i_1}, \delta_{i_2} \in P_{2n}$，记下述变换为 S，定义:

$$S = S(\delta_{i_1}, f_1, f_2, \delta_{i_2}) \overset{\text{def}}{=} \delta_{i_2}^{-1} \circ D_{2n,f_2} \circ D_{2n,f_1} \circ \delta_{i_1}$$。如图 1 所示。

$\forall i \geq 1$, $L_i = R_{i-1}$且$R_i = L_{i-1} \oplus f_i(R_{i-1})$，$\langle L_0, R_0\rangle = \delta_{i_1}(\text{Input})$且 $\text{Output} = \delta_{i_2}^{-1}(\langle L_2, R_2\rangle)$。

定义 3　对于特别选定的循环移位置换 $\delta_{i_1}, \delta_{i_2} \in P_{2n}$，定义 $\text{BAD}(\delta_{i_1}, \delta_{i_2})$ 为 M 的可能的且一致的询问结果 $\rho = \{\langle x_1, y_1\rangle, \cdots, \langle x_m, y_m\rangle\}$ 的集合，且 ρ 满足：$\exists 1 \leq i < j \leq m$ 使得 $\delta_{i_1}(x_i)_{|R} = \delta_{i_1}(x_j)_{|R}$ 或 $\delta_{i_2}(y_i)_{|L} = \delta_{i_2}(y_j)_{|L}$。

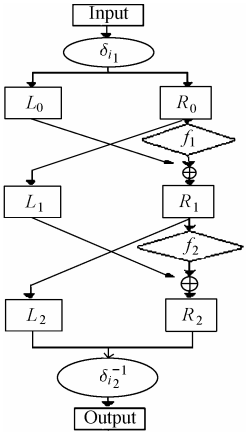

图 1　变换 S 构造示意图

Fig. 1 Construction of transform S

2　主要结果

命题 1　$\left|\text{Prob}_{\tilde{R}}[C_M(T_{\tilde{R}}) = 1] - \text{Prob}_R[C_M(T_R) = 1]\right| \leq m^2 / 2^{2n+1}$。

证明　对任意 M 的可能的且一致的询问结果 ρ 有：

$\text{Prob}[T_R = \rho] = (2^{2n} - m)! / 2^{2n}! = \text{Prob}_{\tilde{R}}[T_{\tilde{R}} = \rho | T_{\tilde{R}} \text{is consistent}]$，对于给定的 i，j，$T_{\tilde{R}}$ 不一致的概率至多是 2^{-2n}。$\text{Prob}_{\tilde{R}}[T_{\tilde{R}} \text{is inconsistent}] \leq C_m^2 2^{-2n} < m^2 / 2^{2n+1}$。从而

$$\left|\text{Prob}_{\tilde{R}}[C_M(T_{\tilde{R}}) = 1] - \text{Prob}_R[C_M(T_R) = 1]\right|$$
$$\leq \left|\text{Prob}_{\tilde{R}}[C_M(T_{\tilde{R}}) = 1 | T_{\tilde{R}} \text{isconsistent}] - \text{Prob}_R[C_M(T_R) = 1]\right| \cdot \text{Prob}[T_{\tilde{R}} \text{is consistent}] + \left|\text{Prob}_{\tilde{R}}[C_M(T_{\tilde{R}}) = 1 | T_{\tilde{R}} \text{is inconsistent}] - \text{Prob}_R[C_M(T_R) = 1]\right| \cdot \text{Prob}_{\tilde{R}}[T_{\tilde{R}} \text{is inconsistent}]$$
$$\leq \text{Prob}_{\tilde{R}}[T_{\tilde{R}} \text{is inconsistent}] < m^2 / 2^{2n+1}$$。　证毕

命题 2　若 $\delta_i \in P_{2n}$ 是一个循环移位置换，$\forall x_i \neq x_j \in I_{2n}$，有

$$\text{Prob}_{\delta_i}\left[\delta_i(x_i)_{|R} = \delta_i(x_j)_{|R}\right] = \text{Prob}_{\delta_i}\left[\delta_i(x_i)_{|L} = \delta_i(x_j)_{|L}\right] \leq (1 - 1/2^n) \cdot (1/2^n)$$

证明　对 $\forall x_i \neq x_j \in I_{2n}$，要使得 $\delta_i(x_i)_{|R} = \delta_i(x_j)_{|R}$，$x_i$与$x_j$ 的第 $n-i+1$ 到第 $2n-i$ 位必对应相等，它发生概率为 $1/2^n$，又因为 $x_i \neq x_j$，剩余 n 位至少有一比特不同，其概率为 $(1 - 1/2^n)$，故两事件同时发生概率不大于 $(1-1/2^n)\cdot(1/2^n)$。同理可证另式。　证毕

命题 3　若 $\delta_{i_1}, \delta_{i_2} \in P_{2n}$ 是循环移位置换，$\rho = \{\langle x_1, y_1\rangle, \cdots, \langle x_m, y_m\rangle\}$ 为 M 的任何可能的且一致的询问结果，那么 $\text{Prob}_{\delta_{i_1}, \delta_{i_2}}[\rho \in \text{BAD}(\delta_{i_1}, \delta_{i_2})] < (1 - 1/2^n) \cdot (m^2/2^n)$。

证明　由定义 $\rho \in \text{BAD}(\delta_{i_1}, \delta_{i_2})$，说明，$\exists 1 \leq i < j \leq m$ 使得 $\delta_{i_1}(x_i)_{|R} = \delta_{i_1}(x_j)_{|R}$ 或 $\delta_{i_2}(y_i)_{|L} = \delta_{i_2}(y_j)_{|L}$，由命题 2 知，对给定的 i，j 二者相等概率均不大于 $(1-1/2^n)\cdot(1/2^n)$。故

$$\text{Prob}_{\delta_{i_1}, \delta_{i_2}}\left[\rho \in \text{BAD}(\delta_{i_1}, \delta_{i_2})\right] \leq C_m^2 \cdot 2 \cdot (1 - 1/2^n)(1/2^n) < (1 - 1/2^n) \cdot (m^2/2^n)$$　证毕

命题 4　令 $\rho = \{\langle x_1, y_1\rangle, \cdots, \langle x_m, y_m\rangle\}$ 为 M 的任何可能且一致的询问结果，则

$$\text{Prob}_S\left[T_S = \rho \middle| \rho \notin \text{BAD}(\delta_{i_1}, \delta_{i_2})\right] = \text{Prob}_{\tilde{R}}[T_{\tilde{R}} = \rho]$$

证明　由于 ρ 为 M 的一个可能且一致的询问结果，所以对于 $1 \leq i \leq m$，有 $C_M\left[\{\langle x_1, y_1\rangle, \cdots, \langle x_{i-1}, y_{i-1}\rangle\}\right] \in \{(+, x_i), (-, y_i)\}$，因此 $T_{\tilde{R}} = \rho$ 当且仅当 $\tilde{R}$ 的第 i 次回答在 $C_M\left[\{\langle x_1, y_1\rangle, \cdots, \langle x_{i-1}, y_{i-1}\rangle\}\right] = (+, x_i)$成立的条件下是 y_i，$C_M\left[\{\langle x_1, y_1\rangle, \cdots, \langle x_{i-1}, y_{i-1}\rangle\}\right] = (-, y_i)$成立的条件下是 x_i。根据 ρ 是一致的和 $\tilde{R}$ 的定义，知 $\tilde{R}$ 的第 i 次回答是一个独立均匀的 $2n$-bi 串，从而 $\text{Prob}_{\tilde{R}}[T_{\tilde{R}} = \rho] = (2^{-2n})^m$。

由于 ρ 为 M 的一个可能的且一致的询问结果，要使 $T_S = \rho$ 当且仅当对于所有 $1 \leq i \leq m$，$y_i = S(x_i)$。对于选定的使得 $\rho \notin \text{BAD}(\delta_{i_1}, \delta_{i_2})$ 的循环移位置换 $\delta_{i_1}, \delta_{i_2} \in P_{2n}$，记 $(L_i^0, R_i^0) = \delta_{i_1}(x_i)$ 和 $(L_i^2, R_i^2) = \delta_{i_2}(y_i)$，由 S 定义，得：$y_i = S(x_i) \Leftrightarrow f_1(R_i^0) = L_i^0 \oplus L_i^2$ 且 $f_2(L_i^2) = R_i^0 \oplus R_i^2$，对于所有 $1 \leq i < j \leq m$，$R_i^0 \neq R_j^0$ 且 $L_i^2 \neq L_j^2$（否则 $\rho \in \text{BAD}(\delta_{i_1}, \delta_{i_2})$）。由于 f_1, f_2 是随机函数，$\rho \notin \text{BAD}(\delta_{i_1}, \delta_{i_2})$ 时，$f_1(R_i^0) = L_i^0 \oplus L_i^2$ 与 $f_2(L_i^2) = R_i^0 \oplus R_i^2$ 的发生概率均为 2^{-n}，故

$T_S=\rho$ 的概率恰是 2^{-2nm}。故 $\mathrm{Prob}_S\left[T_S=\rho\middle|\rho\notin \mathrm{BAD}\left(\delta_{i_1},\delta_{i_2}\right)\right]$ $=\mathrm{Prob}_{\tilde{R}}\left[T_{\tilde{R}}=\rho\right]$。 证毕

定理 1 令 $\delta_{i_1},\delta_{i_2}\in P_{2n}$ 是循环移位置换，$\forall f_1,f_2\in H_n$ 是随机函数，定义 $S=S\left(\delta_{i_1},f_1,f_2,\delta_{i_2}\right)$，$R\in P_{2n}$ 是一个随机置换，那么对于任意的至多做 $m=m(n)$ 次询问的预言机 M，有:

$\mathrm{adv}(M)=\left|\mathrm{Prob}\left[\mathrm{M}^{S,S^{-1}}\left(1^n\right)\right]=1-\mathrm{Prob}\left[M^{R,R^{-1}}\left(1^n\right)=1\right]\right|\le m^2/2^n$。

证明 令 Γ 为一切可能的且一致的，使得 $C_M(\rho)=1$ 的询问结果 ρ 的集合，记 Δ 为一切可能的且不一致的，使得 $C_M(\rho)=1$ 的询问结果 ρ 的集合，记 Ω 为一切可能的询问结果 ρ 的集合。那么

$$\left|\mathrm{Prob}_S\left[C_M\left(T_S\right)=1\right]-\mathrm{Prob}_{\tilde{R}}\left[C_M\left(T_{\tilde{R}}\right)=1\right]\right|$$

$$=\left|\sum_{\rho\in\Omega}\mathrm{Prob}_S\left[C_M(\rho)=1\right]\cdot\mathrm{Prob}_S\left[T_S=\rho\right]-\sum_{\rho\in\Omega}\mathrm{Prob}_{\tilde{R}}\left[C_M(\rho)=1\right]\cdot\mathrm{Prob}_{\tilde{R}}[T_{\tilde{R}}=\rho]\right|$$

$$\le\left|\sum_{\rho\in\Gamma}\left(\mathrm{Prob}_S[T_S=\rho]-\mathrm{Prob}_{\tilde{R}}[T_{\tilde{R}}=\rho]\right)\right|+\left|\sum_{\rho\in\Delta}\left(\mathrm{Prob}_S[T_S=\rho]-\mathrm{Prob}_{\tilde{R}}[T_{\tilde{R}}=\rho]\right)\right|$$

$$\le\left|\sum_{\rho\in\Gamma}\left(\mathrm{Prob}_S[T_S=\rho]-\mathrm{Prob}_{\tilde{R}}[T_{\tilde{R}}=\rho]\right)\right|+\mathrm{Prob}_{\tilde{R}}[T_{\tilde{R}}\text{is consistent}]$$

$$\le\left|\sum_{\rho\in\Gamma}\left(\mathrm{Prob}_S\left[T_S=\rho\middle|\rho\notin\mathrm{BAD}\left(\delta_{i_1},\delta_{i_2}\right)\right]-\mathrm{Prob}_{\tilde{R}}[T_{\tilde{R}}=\rho]\right)\right|\cdot\mathrm{Prob}_{\delta_{i_1},\delta_{i_2}}\left[\rho\notin\mathrm{BAD}\left(\delta_{i_1},\delta_{i_2}\right)\right]$$

$$+\left|\sum_{\rho\in\Gamma}\left(\mathrm{Prob}_S\left[T_S=\rho\middle|\rho\in\mathrm{BAD}\left(\delta_{i_1},\delta_{i_2}\right)\right]-\mathrm{Prob}_{\tilde{R}}[T_{\tilde{R}}=\rho]\right)\right|\cdot\mathrm{Prob}_{\delta_{i_1},\delta_{i_2}}\left[\rho\in\mathrm{BAD}\left(\delta_{i_1},\delta_{i_2}\right)\right]$$

$$+\mathrm{Prob}_{\tilde{R}}[T_{\tilde{R}}\text{is consistent}]=I_1+I_2+I_3$$

由命题 1 的证明过程知：$I_3=\mathrm{Prob}_{\tilde{R}}[T_{\tilde{R}}\text{is consistent}]<m^2/2^{2n+1}$，由命题 4 知 $I_1=0$。对于 I_2 有

$$I_2\le\max_{\delta_{i_1},\delta_{i_2}}\left\{\mathrm{Prob}_{\delta_{i_1},\delta_{i_2}}\left[\rho\in\mathrm{BAD}\left(\delta_{i_1},\delta_{i_2}\right)\right]\right\}\cdot\max\left\{\sum_{\rho\in\Gamma}\mathrm{Prob}_S[T_S=\rho]\middle|\rho\in\mathrm{BAD}\left(\delta_{i_1},\delta_{i_2}\right),\sum_{\rho\in\Gamma}\mathrm{Prob}_{\tilde{R}}[T_{\tilde{R}}=\rho]\right\}$$

$$\le\max_{\delta_{i_1},\delta_{i_2}}\left\{\mathrm{Prob}_{\delta_{i_1},\delta_{i_2}}\left[\rho\in\mathrm{BAD}\left(\delta_{i_1},\delta_{i_2}\right)\right]\right\}$$

$\le\left(1-1/2^n\right)\cdot\left(m^2/2^n\right)$(命题 3)。因此

$$\left|\mathrm{Prob}_S\left[C_M\left(T_S\right)=1\right]-\mathrm{Prob}_{\tilde{R}}[C_M\left(T_{\tilde{R}}\right)=1]\right|<m^2/2^{2n+1}+\left(1-1/2^n\right)\cdot\left(m^2/2^n\right)$$。由命题 1。

$$\mathrm{Adv}(M)=\left|\mathrm{Prob}_S\left[C_M\left(T_S\right)=1\right]-\mathrm{Prob}_R\left[C_M\left(T_R\right)=1\right]\right|$$

$$=\left|\mathrm{Prob}_S\left[C_M\left(T_S\right)=1\right]-\mathrm{Prob}_{\tilde{R}}\left[C_M\left(T_{\tilde{R}}\right)=1\right]\right|+\left|\mathrm{Prob}_{\tilde{R}}\left[C_M\left(T_{\tilde{R}}\right)=1\right]-\mathrm{Prob}_R\left[C_M\left(T_R\right)=1\right]\right|<m^2/2^{2n+1}+\left(1-1/2^n\right)\cdot\left(m^2/2^n\right)+m^2/2^{2n+1}=m^2/2^n$$ 证毕

定理 2 如果，$\forall\ \delta_{i_1},\delta_{i_2}\in P_{2n}$ 是循环移位置换，$\forall f_1,f_2\in H_n$ 是伪随机函数，$\delta_{i_1},\delta_{i_2},f_1,f_2$ 是独立选取的，则 $S=S\left(\delta_{i_1},f_1,f_2,\delta_{i_2}\right)$ 是超伪随机置换。而且，若不存在做至多 $m=m(n)$ 次询问，以 $\varepsilon=\varepsilon(n)$ 的优势区分伪随机函数与随机函数的预言机，则不存在做至多 $m=m(n)$ 次询问，以 $2\varepsilon+m^2/2^n$ 的优势区分 S 与随机置换的预言机。

证明 首先定义 3 个变量：$S_1=S\left(\delta_{i_1},f_1,f_2,\delta_{i_2}\right)$，这里 $\delta_{i_1},\delta_{i_2}\in P_{2n}$ 是循环移位置换，$f_1,f_2\in H_n$ 是伪随机函数；$S_2=S(\delta_{i_1},g_1,f_2,\delta_{i_2})$，这里 $\delta_{i_1},\delta_{i_2}\in P_{2n}$ 是循环移位置换，$f_2\in H_n$ 是伪随机函数，$g_1\in H_n$ 是随机函数；$S_3=S(\delta_{i_1},g_1,\ g_2,\delta_{i_2})$，这里 $\delta_{i_1},\delta_{i_2}\in P_{2n}$ 是循环移位置换，$g_1,g_2\in H_n$ 是随机函数，则对于每一个预言机 M 和几乎所有的整数 n，有

$$(1)\ \mathrm{adv}(M)=\left|\mathrm{Prob}\left[M^{S_1,S_1^{-1}}\left(1^{2n}\right)=1\right]-\mathrm{Prob}\left[M^{S_2,S_2^{-1}}\left(1^{2n}\right)=1\right]\le\varepsilon(n)\right|$$

$$(2)\ \mathrm{adv}(M)=\left|\mathrm{Prob}\left[M^{S_2,S_2^{-1}}\left(1^{2n}\right)=1\right]-\mathrm{Prob}\left[M^{S_3,S_3^{-1}}\left(1^{2n}\right)=1\right]\right|\le\varepsilon(n)$$

如果(1)或(2)不成立，则由文献［1］中定理 1 的证明知存在有效预言机 $\tilde{M}$ 能以大于 $\varepsilon(n)$ 的优势把 f_1与g_1 或 f_2与g_2 区分开。这与伪随机函数的定义相矛盾，故(1)和(2)成立。因此在定理 2 条件下有：

$$\mathrm{adv}(M)=\left|\mathrm{Prob}\left[M^{S,S^{-1}}\left(1^{2n}\right)=1\right]-\mathrm{Prob}\left[M^{R,R^{-1}}\left(1^{2n}\right)=1\right]\right|$$

$$\le\left|\mathrm{Prob}\left[M^{S_1,S_1^{-1}}\left(1^{2n}\right)=1\right]-\mathrm{Prob}\left[M^{S_2,S_2^{-1}}\left(1^{2n}\right)=1\right]\right|+\left|\mathrm{Prob}\left[M^{S_2,S_2^{-1}}\left(1^{2n}\right)=1\right]-\mathrm{Prob}\left[M^{S_3,S_3^{-1}}\left(1^{2n}\right)=1\right]\right|+\left|\mathrm{Prob}\left[M^{S_3,S_3^{-1}}\left(1^{2n}\right)=1\right]-\mathrm{Prob}\left[M^{R,R^{-1}}\left(1^{2n}\right)=1\right]\right|$$

$\le 2\varepsilon+m^2/2^n$。(注：s_1 相当于定理 2 的 s，s_3 相当于定理 1 的 s) 证毕

3 结束语

由以上论证可以看出，基于循环移位置换的超伪随机置

换的构造降低了区分优势的上界，其抗选择明密文攻击能力也提高相应的量级。

附录 有关定义和记号

I_n表示n-bit串的集合，$\{0,1\}^n$，$H_n=\{f\,|\,f:I_n\to I_n\}$，$P_n$表示 $I_n\to I_n$ 全体置换的集合，$P_n\subset H_n$。$x\oplus y$ 表示x与y的模 2 加，$\forall f,g\in H_n$, $f\circ g$ 表示 f 与 g 的复合，即 $f\circ g=f(g(x))$。对于 $x\in I_{2n}$，X_L 表示x的左边n bit，X_R 表示x的右边n bit。$x\in_r S$ 表示x均匀选自S。

定义 4 (DES 型置换) $\forall f\in{}_rH_n$，定义 DES 型置换 $D_{2n,f}\in P_{2n}$，$D_{2n,f}(L,R)=(R,\ L\oplus f(R))$，$L,\ R\in I_n$。注：DES 型置换是易于求逆的，$D_{2n,f}^{-1}=(R\oplus f(L),L)=\rho\circ D_{2n,f}\circ\rho$，其中 $\rho(L,\ R)\overset{\text{def}}{=}(R,\ L)$。

定义 5 (DES 型置换的复合) 设 $f_1f_2,\cdots,f_i\in{}_rH_n$，定义 DES 型置换的复合 $\psi\in P_{2n}$，

$$\psi(f_i,f_{i-1},\cdots,f_1)=D_{2n,f_i}\circ D_{2n,f_{i-1}}\circ\ldots\circ D_{2n,f_1}$$

定义 6 (函数总体) 设 $\mathrm{l}:N\to N$ 的函数，(例，$\mathrm{l}(n)=n$)一个 $\mathrm{l}(n)$ 位函数总体是一个随机变量序列 $F=\{F_n\}_{n\in N}$，F_n 在函数集 $H_{\mathrm{l}(n)}$ 上取值。如果 F_n 在 $H_{\mathrm{l}(n)}$ 上是均匀分布的，则称 F 为均匀函数总体。记 $\mathrm{l}(n)$ 位的均匀函数总体为 $R=\{R_n\}_{n\in N}$。一个置换总体是一个随机变量序列 $F=\{F_n\}_{n\in N}$，F_n 是置换集 P_n 上的随机变量，如果 F_n 是 P_n 上的均匀分布，则 F 称为均匀置换总体。

定义 7 (可有效计算的函数(置换)总体) 一个函数(或置换)总体 $F=\{F_n\}_{n\in N}$ 是可有效计算的，如果满足：

(1)有效取样：存在一个概率多项式时间算法 I 和一个由串到函数的映射 ϕ，使得 $\phi(I(1^n))$ 和 F_n 服从相同的分布。记对应于串 i 的函数为 f_i (即 $f_i\overset{\text{def}}{=}\phi(i)$)

(2)有效计算：存在一个概率多项式时间算法 V，使得对于 $\forall i\in I(1^n)$ 和 $x\in\{0,1\}^{\mathrm{l}(n)}$ 都有 $V(i,x)=f_i(x)$。

定义 8 (区分优势) 令 M 是一个预言机，$F=\{F_n\}_{n\in N}$ 和 $\tilde F=\{\tilde F_n\}_{n\in N}$ 是两个函数或置换总体。称函数 $\mathrm{Adv}(M)=\left|\mathrm{Prob}\left[M^{F_n}(1^n)=1\right]-\mathrm{Prob}\left[M^{\tilde F_n}(1^n)=1\right]\right|$ 为 M 区分 F 和 $\tilde F$ 时达到的优势。

令 $F=\{F_n\}_{n\in N}$ 和 $\tilde F=\{\tilde F_n\}_{n\in N}$ 是两个置换总体，F^{-1} 和 $\tilde F^{-1}$ 分别是 F 和 $\tilde F$ 的逆，则 $\mathrm{Adv}(M)=\left|\mathrm{Prob}\left[M^{F_n,F_n^{-1}}(1^n)=1\right]-\mathrm{Prob}\left[M^{\tilde F_n,\tilde F_n^{-1}}(1^n)=1\right]\right|$ 为 M 区分 $\langle F,F^{-1}\rangle$ 和 $\langle\tilde F,\tilde F^{-1}\rangle$ 时达到的优势。

定义 9 (可忽略不计函数) 若对任一正多项式 $P(\bullet)$，存在 N，当 $n>N$ 时满足 $\mu(n)<1/P(n)$，则称函数 $\mu:N\to N$ 是可忽略不计的。

定义 10 (伪随机函数总体) 一个 $\mathrm{l}(n)$ 位函数总体 $F=\{F_n\}_{n\in N}$ 称为是伪随机函数总体，如果对于每个概率多项式时间预言机 M，都有优势 $\mathrm{Adv}(M)=\left|\mathrm{Prob}\left[M^{F_n}(1^n)=1\right]-\mathrm{Prob}\left[M^{R_n}(1^n)=1\right]\right|$ 是可忽略不计的，其中 $R=\{R_n\}_{n\in N}$ 是 $\mathrm{l}(n)$ 位的均匀函数总体。

定义 11 (伪随机置换总体) 如果对于每个概率多项式时间预言机 M、某一置换总体 $P=\{P_n\}_{n\in N}$ 满足：$\mathrm{Adv}(M)=\left|\mathrm{Prob}\left[M^{F_n}(1^n)=1\right]-\mathrm{Prob}\left[M^{K_n}(1^n)=1\right]\right|$ 是可忽略不计的，其中 $K=\{K_n\}_{n\in N}$ 是均匀置换总体。则称此置换总体 $P=\{P_n\}_{n\in N}$ 是伪随机置换总体。

定义 12 (超伪随机置换总体) 如果对于每个概率多项式时间预言机 M、某一置换总体 $P=\{P_n\}_{n\in N}$ 满足：$\mathrm{adv}(M)=\left|\mathrm{Prob}\left[M^{P_n,P_n^{-1}}(1^n)=1\right]-\mathrm{Prob}\left[M^{K_n,K_n^{-1}}(1^n)=1\right]\right|$ 是可忽略不计的，其中 $K=\{K_n\}_{n\in N}$ 是均匀置换总体。则称此置换总体 $P=\{P_n\}_{n\in N}$ 是超伪随机置换总体。

定义 13 (循环移位置换) 令 δ_i 是 i 位 $(1\le i\le n-1)$ 循环移位置换，如果 δ_i 把第 k 比特变成第 $(k+i)\bmod n$ 比特，例如，如果 $x=X_1X_2\cdots X_n$，$x\in I_n$，则 $\delta_2(x)=X_{n-1},X_n,X_1\cdots X_{n-2}$，且 $\delta_i^{-1}=\delta_{n-i}$。

参 考 文 献

[1] Luby M, Rackoff C. How to construct pseudorandom permutations from pseudorandom functions. *SIAM J. Computing*, 1988, 17(2): 373 − 386.

[2] Goldreich O, Goldwasser S. How to construct random functions. *J. of the ACM*, 1986, 33(4): 792 − 807.

[3] Naor M, Reingold O. On the construction of pseudo-random permutation: Luby-Rackoff Revisited. (密码学电子刊物). http://eprint.iacr.org/ .1996(011).

[4] Iwata T, Yoshin T. Non-cryptographic primitive for pseudorandom permutation. *Theoretical Computer Science* 2003, 306(2): 139 − 154. http://www.elsevier.com/locate/tcs

余昭平：男, 1962 年生, 教授, 硕士生导师, 研究方向为密码理论、应用数学.

王晓东：男, 1973 年生, 硕士生, 研究方向为密码理论、应用数学.