强安全可调加密方案的两个密码特性

郭 瑞* 金晨辉
(解放军信息工程大学电子技术学院 郑州 450004)

摘 要：该文在同时具备选择明文攻击和选择密文攻击的条件下，给出了可调加密方案的分类攻击安全和广义分类攻击安全的概念，并证明了二者的等价性；证明了抗基本区分攻击安全和抗左右不可区分攻击安全的可调加密方案一定是分类攻击安全和广义分类攻击安全的，从而揭示了强安全可调加密方案一定具有分类攻击安全和广义分类攻击安全这两个密码特性。

关键词：密码学；可调加密方案；分类攻击安全；广义分类攻击安全
中图分类号：TN918 **文献标识码**： A **文章编号**：1009-5896(2011)07-1761-04
DOI: 10.3724/SP.J.1146.2010.01110

Two Cryptographic Properties of Strong Security Tweakable Enciphering Scheme

Guo Rui Jin Chen-hui
(*Electronic Technology Institute*, *PLA Information Engineering University*, *Zhengzhou* 450004, *China*)

Abstract: This paper presents the concepts of sorted-attack security and generalized sorted-attack security of tweakable enciphering schemes under chosen-plaintext and chosen-ciphertext attacks. Firstly, it is proved that those two notions are equivalence. Secondly, it is proved that the basic distinguishing attack security and the left-or-right distinguishing attack security guarantee sorted-attack security and generalized sorted-attack security, therefore reveals that a strong tweakable enciphering scheme have those two cryptographic properties.

Key words: Cryptography; Tweakable enciphering scheme; Sorted-attack security; Generalized sorted-attack security

1 引言

可调加密方案是由 Halevi 等人[1]以磁盘加密为背景提出的一类特殊的分组密码加密方案。可调加密方案本质上是由调柄参数决定的一簇加密算法，且不同的调柄对应的加密算法具有独立的加密效果。此外，与传统的加密算法相比，由于可调加密方案多了一个调柄参数，从而使其更具有灵活性[2]。在磁盘加密时，可将磁盘的扇区地址作为调柄参数，从而保证了即使两个扇区的明文相同，对应的密文也是独立的[1]。

考察密码算法的安全性刻画方法是密码学研究的一个重要内容。例如，在公钥密码和对称密码中，人们可利用基本区分攻击安全[3]、左右区分攻击安全[3,4]和语义安全[4,5]等概念，刻画对这些密码算法的攻击方法及密码算法的安全性。在可调加密方案的安全性定义研究方面，文献[1]在提出可调加密方案的概念的同时，给出了基本区分攻击安全和左右区分攻击安全的定义，并证明了这两个安全性定义在保持安全规约意义下等价，且将抗基本区分攻击安全的可调加密方案称为强安全可调加密方案[1]。目前，这两个安全性定义已成为分析可调加密方案的安全性的基本工具[6–11]。语义安全本质上考察的是密文的获得能否有助于获得明文的信息[3,4]，本文则从对未知密文分类的角度考察可调加密方案的安全性。本文将针对可调加密方案，在两个明文的对应密文未知的条件下，考察能否将密文分入不同类的方法，刻画可调加密方案的安全性。给出分类攻击安全和广义分类攻击安全的定义，并证明二者的等价性，证明基本区分攻击安全和左右区分攻击安全的可调加密方案一定是分类攻击安全和广义分类攻击安全的，从而揭示了强安全可调加密方案一定具有分类攻击安全和广义分类攻击安全这两个密码特征。

2 可调加密方案的分类攻击安全和广义分类攻击安全及其等价性

本节首先介绍可调加密方案的定义，并给出可

2010-10-15 收到， 2011-05-06 改回
河南省杰出青年科学基金(0312001800)资助课题
*通信作者：郭瑞 guorui201@sohu.com

调加密方案分类攻击安全和广义分类攻击安全的定义，证明二者的等价性。

定义 1[1] 设 $\mathcal{M}=\bigcup_{i\geq 1}\{0,1\}^i$ 是消息空间，$\mathcal{K}$ 为密钥空间，$\mathcal{T}$ 为调柄空间，且 $\forall T\in\mathcal{T},\forall K\in\mathcal{K}$, $E(T,K,\cdot)$ 都是加密算法，则称 E: $\mathcal{T}\times\mathcal{K}\times\mathcal{M}\to\mathcal{M}$ 为一个可调加密方案。

对于可调加密方案，调柄可以是公开的，但要求不同的调柄对应的加密算法可视为独立的。下面给出可调加密方案分类攻击安全和广义分类攻击安全的定义，它们反映了任意两个明文的对应密文本质上属于同一类。以下我们用 $K\in_R\mathcal{K}$ 表示 K 在 $\mathcal{K}$ 按均匀分布选取。

定义 2 (分类攻击安全) 设 E: $\mathcal{T}\times\mathcal{K}\times\mathcal{M}\to\mathcal{M}$ 是一个可调加密方案，$A_{\text{find}}^{E_K,D_K}$ 和 $A_{\text{guess}}^{E_K,D_K}$ 是以加密预言机 $E_K(T,m)$ 和脱密预言机 $D_K(T,c)$ 的预言结果为输入的两个算法，且 $(T_0,X_0,T_1,X_1,s)=A_{\text{find}}^{E_K,D_K}$ 和 $A_{\text{guess}}^{E_K,D_K}(y_i,s)\in\{0,1\}$，其中 $y_i=E_K(T_i,X_i),\ i=0,1$。定义

$$\begin{aligned}\text{Adv}_E(A)=\Big|&\Pr[K\in_R\mathcal{K}:A_{\text{guess}}^{E_K,D_K}(y_0,s)=1]\\&-\Pr[K\in_R\mathcal{K}:A_{\text{guess}}^{E_K,D_K}(y_1,s)=1]\Big|\end{aligned}\quad(1)$$

则称 $A=(A_{\text{find}}^{E_K,D_K},A_{\text{guess}}^{E_K,D_K})$ 是一个优势为 $\text{Adv}_E(A)$，攻击能力为 $R=(t,q,\mu)$ 的分类攻击算法，这里 t 是攻击算法的时间复杂度，q 是加密预言机和脱密预言机的总询问次数，μ 是询问得到的总比特数。如果攻击能力为 $R=(t,q,\mu)$ 的分类攻击算法的优势都小于 ε，则称 E 是 (t,q,μ)-ε 分类攻击安全的可调加密方案。

由于算法 A 可将输入根据其输出的取值分为两类，因而本质上就是对密文的一种分类方法。因此，能够抵抗分类攻击，意味着对于在计算能力范围内构造出的任意两个调柄、任意两个明文、任意一个辅助参数和任何分类攻击方法 A，当密钥均匀分布时，对应的两个密文落入同一类的概率都没有明显的差异，因而本质上都是同一类。

定义 3 (广义分类攻击安全) 设 E: $\mathcal{T}\times\mathcal{K}\times\mathcal{M}\to\mathcal{M}$ 是一个可调加密方案，$A_{\text{select}}^{E_K,D_K}$ 是以加密预言机 $E_k(T,m)$ 和脱密预言机 $D_k(T,c)$ 的预言结果为输入的算法，$A_{\text{predict}}^{E_K,D_K}(y,s)$ 是以加密预言机 $E_k(T,m)$ 和脱密预言机 $D_k(T,c)$ 的预言结果及 (y,s) 为输入的算法，$(f,T,X_0,X_1,s)=A_{\text{select}}^{E_K,D_K}$，这里 $T\in\mathcal{T}$, $X_0,X_1\in\mathcal{M}$, f: $\mathcal{T}\times\mathcal{M}\to\mathcal{M}$。对于 $i=0,1$，记 $p_i=\Pr[K\in_R\mathcal{K}:A_{\text{predict}}^{E_K,D_K}(E_k(T,X_i),s)=f(T,X_i)]$，则称 $A=(A_{\text{select}},A_{\text{predict}})$ 是一个优势为 $|p_0-p_1|$，攻击能力为 $R=(t,q,\mu)$ 的广义分类攻击算法，这里 t 是攻击算法的时间复杂度，q 是加密预言机和脱密预言机的总询问次数，μ 是询问得到的总比特数。如果攻击能力为 $R=(t,q,\mu)$ 的广义分类攻击算法的优势都小于 ε，则称 E 是 (t,q,μ)-ε 广义分类攻击安全的可调加密方案。

在分类攻击中，我们是利用 $A_{\text{guess}}^{E_K,D_K}(y_i,s)$ 的输出值为 0 或 1 将明文 X_i 对应的 y_i 进行分类；在广义分类攻击中，则是利用 $A_{\text{predict}}^{E_K,D_K}(y_i,s)$ 的输出值与由明文和调柄计算出的 $f(T,X_i)$ 是否相等对密文进行分类的，因而是种动态的分类方法，是分类攻击的一般化。

定理 1 如果可调加密方案 E: $\mathcal{T}\times\mathcal{K}\times\mathcal{M}\to\mathcal{M}$ 是 (t,q,μ)-ε 分类攻击安全的，则此方案一定是 (t,q,μ)-ε 广义分类攻击安全的。

证明 假设存在攻击能力为 $R=(t,q,\mu)$ 的广义分类攻击算法 $(A_{\text{select}}^{E_K,D_K},A_{\text{predict}}^{E_K,D_K}(y,s))$ 以大于等于 ε 的优势成功攻击了可调加密方案 E。下面证明，可以构造一个攻击能力为 $R=(t,q,\mu)$ 的分类攻击算法 $A_P=(A_{\text{find}},A_{\text{guess}})$ 大于等于 ε 的优势成功攻击 E。该分类攻击算法 A_P 设计如下：

算法 $A_{\text{find}}^{E_K,D_K}$：

步骤 1 计算出 $(f,T,X_0,X_1,s)=A_{\text{select}}^{E_K,D_K}$；

步骤 2 输出 (T,X_0,T,X_1,s)。

算法 $A_{\text{guess}}^{E_K,D_K}(y,s)$：

步骤 1 以 (T,X_0) 和 (T,X_1) 为输入向 $E_K(\cdot,\cdot)$ 询问，得到 $y_0=E_K(T,X_0)$ 和 $y_1=E_K(T,X_1)$；

步骤 2 计算出 $\alpha_0=A_{\text{predict}}^{E_K,D_K}(y_0,s),\alpha_1=A_{\text{predict}}^{E_K,D_K}(y_1,s)$；

步骤 3 对于 $i=0,1$，当 $\alpha_i=f(T,X_i)$ 时令 $A_{\text{guess}}^{E_K,D_K}(y_i,s)=1$，否则令 $A_{\text{guess}}^{E_K,D_K}(y_i,s)=0$。

显然，上述分类攻击算法与广义分类攻击算法相比，二者的预言机询问次数、询问的总消息长度和时间复杂度都相同，即其攻击能力为 $R=(t,q,\mu)$。此外，有

$$\begin{aligned}\text{Adv}_E(A_p)=&|\Pr[K\in_R\mathcal{K}:A_{\text{guess}}^{E_K,D_K}(E_K(T,X_0),s)=1]\\&-\Pr[K\in_R\mathcal{K}:A_{\text{guess}}^{E_K,D_K}(E_K(T,X_1),s)=1]\|\\=&|\Pr[K\in_R\mathcal{K}:\alpha_0=f(T,X_0)]\\&-\Pr[K\in_R\mathcal{K}:\alpha_1=f(T,X_1)]\|\\=&|\Pr[K\in_R\mathcal{K}:A_{\text{predict}}^{E_K,D_K}(E_K(T,X_0),s)\\&=f(T,X_0)]-\Pr[K\in_R\mathcal{K}:A_{\text{predict}}^{E_K,D_K}(E_K\\&\cdot(T,X_1),s)=f(T,X_1)]\|\geq\varepsilon\end{aligned}\quad(2)$$

即上述分类攻击算法的优势大于等于 ε。这说明本定理成立。 证毕

定理 2 如果可调加密方案 E: $\mathcal{T}\times\mathcal{K}\times\mathcal{M}\to\mathcal{M}$ 是 (t,q,μ)-ε 广义分类攻击安全的，则此方案一定

是 (t,q,μ)-ε 分类攻击安全的。

证明　假设存在攻击能力为 $R=(t,q,\mu)$ 的分类攻击算法 $A_p=(A_{\text{find}},A_{\text{guess}})$ 以大于等于 ε 的优势成功攻击了可调加密方案 E。下面证明，一定可以构造一个攻击能力为 $R=(t,q,\mu)$ 的广义分类攻击算法 $A=(A_{\text{select}},A_{\text{predict}})$ 以大于等于 ε 的优势成功攻击可调加密方案 E。令

$$d=\begin{cases}1, & \text{若 } \Pr[K\in_R\mathcal{K}:A_{\text{guess}}^{E_K,D_K}(y_0,s)=1]\\ & \quad>\Pr[K\in_R\mathcal{K}:A_{\text{guess}}^{E_K,D_K}(y_1,s)=1]\\ 0, & \text{其它}\end{cases}\tag{3}$$

并设计广义分类攻击算法 $(A_{\text{select}}^{E_K,D_K},A_{\text{predict}}^{E_K,D_K}(y,s))$ 如下：

算法 $A_{\text{select}}^{E_K,D_K}$：

步骤 1　计算出 $(T_0,X_0,T_1,X_1,s')=A_{\text{find}}^{E_K,D_K}$；

步骤 2　以 (T_1,X_1) 为输入向 $E_K(\cdot,\cdot)$ 询问，得到 $y_1=E_K(T_1,X_1)$，并令 $s=(s',y_1)$；

步骤 3　令 f: $\mathcal{T}\times\mathcal{M}\to\mathcal{M}$ 使 $\forall X\in\mathcal{M},\forall T\in\mathcal{T}$ 都有 $f(T,X)=X$；

步骤 4　输出 (f,T_0,X_0,X_1,s)。

由定义 1 和分类攻击算法 A_p 的优势大于等于 ε 知 $X_0\neq X_1$。再设计算法 $A_{\text{predict}}^{E_K,D_K}(y,s)$ 如下：

步骤 1　计算出 $(f,T_0,X_0,X_1,s)=A_{\text{select}}^{E_K,D_K}$；

步骤 2　以 (T_0,X_0) 为输入向 $E_K(\cdot,\cdot)$ 询问，得到 $y_0=E_K(T_0,X_0)$；

步骤 3　令　$A_{\text{predict}}^{E_K,D_K}(y_0,s)=A_{\text{predict}}^{E_K,D_K}(y_1,s)=X_{(b_{d\oplus1}\oplus1)\wedge b_d}$，其中 $b_0=A_{\text{guess}}^{E_K,D_K}(y_0,s')$, $b_1=A_{\text{guess}}^{E_K,D_K}(y_1,s)$。

显然，上述分类攻击算法与广义分类攻击算法相比，二者的预言机询问次数、询问的总消息长度和时间复杂度都相同，即其攻击能力为 $R=(t,q,\mu)$。此外，还有

$$\begin{aligned}|p_0-p_1|&=|\Pr[K\in_R\mathcal{K}:A_{\text{predict}}^{E_K,D_K}(E_k(T,X_0),s)\\&\quad=f(T,X_0)]-\Pr[K\in_R\mathcal{K}:A_{\text{predict}}^{E_K,D_K}(E_k\\&\quad\cdot(T,X_1),s)=f(T,X_1)]\|\\&=|\Pr[K\in_R\mathcal{K}:X_{(b_{d\oplus1}\oplus1)\wedge b_d}=X_0]\\&\quad-\Pr[K\in_R\mathcal{K}:X_{(b_{d\oplus1}\oplus1)\wedge b_d}=X_1]\|\\&=|\Pr[K\in_R\mathcal{K}:(b_{d\oplus1}\oplus1)\wedge b_d=0]\\&\quad-\Pr[K\in_R\mathcal{K}:(b_{d\oplus1}\oplus1)\wedge b_d=1]\|\\&=|\Pr[K\in_R\mathcal{K}:(b_{d\oplus1}=1)\cup(b_d=0)]\\&\quad-\Pr[K\in_R\mathcal{K}:b_{d\oplus1}=0,b_d=1]\|\end{aligned}\tag{4}$$

记事件 $b_{d\oplus1}=0$ 为 A、事件 $b_d=0$ 为 B，则由 d 的定义知 $\Pr(K\in_R\mathcal{K}:b_{d\oplus1}=1)>\Pr(K\in_R\mathcal{K}:b_d=1)$，即 $\Pr(\overline{A})\geq\Pr(\overline{B})$。再由 $\Pr(B)-\Pr(\overline{A}\cup B)\leq0\leq\Pr(A)-\Pr(A\cap\overline{B})=\Pr(A\cap B)$ 知 $\Pr(\overline{A}\cup B)-\Pr(A\cap\overline{B})\geq\Pr(B)-\Pr(A)=\Pr(\overline{A})-\Pr(\overline{B})\geq0$，故有

$$\begin{aligned}|p_0-p_1|&=|\Pr(\overline{A}\cup B)-\Pr(A\cap\overline{B})|\\&=\Pr(\overline{A}\cup B)-\Pr(A\cap\overline{B})\geq\Pr(\overline{A})-\Pr(\overline{B})\\&=\Pr[K\in_R\mathcal{K}:A_{\text{guess}}^{E_K,D_K}(y_{d\oplus1},s)=1]\\&\quad-\Pr[K\in_R\mathcal{K}:A_{\text{guess}}^{E_K,D_K}(y_d,s)=1]\geq\varepsilon\end{aligned}\tag{5}$$

即上述广义分类攻击算法的优势大于等于 ε。这说明本定理成立。　　证毕

定理 1 和定理 2 说明可调加密方案的广义分类攻击安全和分类攻击安全这两个定义等价。

3　分类攻击安全和广义分类攻击安全与强安全可调加密方案的关系

利用可调加密方案与可调随机置换的区分优势刻画可调加密方案的安全性是一种常用的基本方法[1]。文献[1]给出了可调加密方案抗基本区分攻击安全、抗左右区分攻击安全的可调加密方案的定义，并证明了这两个定义的等价性。抗基本区分攻击安全的可调加密方案又称为强安全可调加密方案。下面证明强安全可调加密方案一定是分类攻击安全和广义分类攻击安全的。

定义 4[1](抗左右区分攻击安全)　设 E: $\mathcal{T}\times\mathcal{K}\times\mathcal{M}\to\mathcal{M}$ 是一个可调加密方案，$A_{\text{construct}}^{E_K,D_K}$ 是以加密预言机 $E_k(T,m)$ 和脱密预言机 $D_k(T,c)$ 的预言结果为输入的算法，$(T_0,T_1,X_0,X_1,C_0,C_1)=A_{\text{construct}}^{E_K,D_K}$，且 $A_{\text{output}}^{E_K(T_0,X_0),D_K(T_0,C_0)},A_{\text{output}}^{E_K(T_1,X_1),D_K(T_1,C_1)}\in\{0,1\}$。定义

$$\begin{aligned}\text{Adv}_E(A)=|&\Pr[K\in_R\mathcal{K}:A_{\text{output}}^{E_K(T_0,X_0),D_K(T_0,C_0)}=1]\\&-\Pr[K\in_R\mathcal{K}:A_{\text{output}}^{E_K(T_1,X_1),D_K(T_1,C_1)}=1]\|\end{aligned}\tag{6}$$

则称 A 是一个优势为 $\text{Adv}_E(A)$，攻击能力 $R=(t,q,\mu)$ 的左右区分攻击算法，其中 t 是该算法的时间复杂度，q 是加密预言机和脱密预言机的总询问次数，μ 是询问得到的总比特数。如果攻击能力为 $R=(t,q,\mu)$ 的左右区分攻击算法的优势都小于 ε，则称 E 是 (t,q,μ)-ε 左右区分攻击安全的可调加密方案。

定理 3　设可调加密方案 E: $\mathcal{T}\times\mathcal{K}\times\mathcal{M}\to\mathcal{M}$ 是 (t,q,μ)-ε 左右区分攻击安全的，则该方案一定是 (t,q,μ)-ε 分类攻击安全的。

证明　假设存在攻击能力为 $R=(t,q,\mu)$ 的分类攻击算法 $A_p=(A_{\text{find}},A_{\text{guess}})$ 以大于等于 ε 的优势成功攻击了可调加密方案 E。下面证明，一定可以构造一个攻击能力 $R=(t,q,\mu)$ 的左右区分攻击算法 A 以大于等于 ε 的优势成功攻击可调加密方案 E。具体的左右区分攻击算法 A 设计如下：

步骤 1　计算出 $(T_0,X_0,T_1,X_1,s)=A_{\text{find}}^{E_K,D_K}$；

步骤 2　以 (T_0,X_0) 和 (T_1,X_1) 为输入向 $E_K(\cdot,\cdot)$

询问，得到 $y_0 = E_K(T_0, X_0)$ 和 $y_1 = E_K(T_1, X_1)$；

步骤 3 计 算 出 $b_0 = A_{\text{guess}}^{E_K, D_K}(y_0, s)$ 和 $b_1 = A_{\text{guess}}^{E_K, D_K} \cdot (y_1, s)$；

步骤 4 输 出 $A^{E_K(T_0,X_0), D_K(T_0,C_0)} = b_0$ 和 $A^{E_K(T_1,X_1), D_K(T_1,C_1)} = b_1$。

显然，上述左右区分攻击算法中预言机的询问次数、询问的总消息长度以及时间复杂度都与分类攻击算法相同，因而其攻击能力为 $R = (t, q, \mu)$。此外，还有

$$\begin{aligned}\text{Adv}_E(A) &= |\Pr[K \in_R \mathcal{K} : A^{E_K(T_1,X_1), D_K(T_1,C_1)} = 1] \\ &\quad - \Pr[K \in_R \mathcal{K} : A^{E_K(T_0,X_0), D_K(T_0,C_0)} = 1]\| \\ &= |\Pr[K \in_R \mathcal{K} : b_1 = 1] - \Pr[K \in_R \mathcal{K} : b_0 = 1]\| \\ &= |\Pr[K \in_R \mathcal{K} : A_{\text{guess}}^{E_K, D_K}(y_0, s) = 1] \\ &\quad - \Pr[K \in_R \mathcal{K} : A_{\text{guess}}^{E_K, D_K}(y_1, s) = 1]\| \geq \varepsilon \end{aligned} \quad (7)$$

即上述左右区分攻击算法的优势大于等于 ε。这说明本定理成立。 证毕

定理 3 说明左右区分攻击安全的可调加密方案一定是分类攻击安全和广义分类攻击安全的。因此，分类攻击安全和广义分类攻击安全是强安全可调加密方法的两个密码特征。

5 结束语

本文针对可调加密方案，给出分类攻击安全和广义分类攻击安全的形式化定义，并证明了二者的等价性。还证明了强安全可调加密方案一定是分类攻击安全和广义分类攻击安全的，从而揭示了分类攻击安全和广义分类攻击安全是强安全可调加密方案的密码特征。上述结论有助于理解和认识强安全可调加密方案的安全特征。

参 考 文 献

[1] Halevi S and Rogaway P. A tweakable enciphering mode[C]. CRYPTO'03, Berlin, 2003, LNCS 2729: 482–499.

[2] 王鹏, 冯登国. TAE 模式的分析和改进[J]. 软件学报, 2006, 17(2): 333–338.
Wang P and Feng D G. Cryptanalysis of the TAE mode and its improvement[J]. *Journal of Software*, 2006, 17(2): 333–338.

[3] Bellare M, Desai A, Jokipii E, and Rogaway P. A concrete security treatment of symmetric encryption[C]. IEEE Computer Society, Washington, D.C, 1997: 394–403.

[4] 陈原, 白恩健, 肖国镇. 两种语义安全性定义的等价性[J]. 电子学报, 2009, 37(10): 2149–2153.
Chen Yuan, Bai En-jian, and Xiao Guo-zhen. Equivalence between two definitions of semantic security[J]. *Acta Electronica Sinica*, 2009, 37(10): 2149–2153.

[5] Goldwasser S. Probabilistic encryption [J]. *Journal of Computer and System Science*, 1984, 28(2): 270–299.

[6] Sarkar P. Tweakable enciphering schemes from stream ciphers with IV [EB/OL]. Cryptology ePrint Archive, Report 2009/312, 2009.

[7] Wang Peng, Feng Dengguo, and Wu Wen-ling. HCTR: a variable-input-length enciphering mode [C]. CISC, Berlin, 2005, LNCS 3822: 175–188.

[8] Chakraborty D and Sarkar P. HCH: a new tweakable enciphering scheme using the hash-counter-hash approach[J]. *IEEE Transactions on Information Theory*, 2008, 54(4): 1683–1699.

[9] Sarkar P. Efficient tweakable enciphering schemes from (block-wise) universal hash functions[J]. *IEEE Transactions on Information Theory*, 2009, 55(10): 4749–4760.

[10] Martin Gagné, Pascal Lafourcade, Yassine Lakhnech, and Reihaneh Safavi-Naini. Automated security proof for symmetric encryption modes[C]. ASIAN'09, 2009, Berlin, LNCS 5913: 39–53.

[11] Cuauhtemoc Mancillas-López, Chakraborty D, Francisco Rodríguez-Henríquez. Reconfigurable hardware implementations of tweakable enciphering schemes[J]. *IEEE Transactions on Computers*, 2010, 59(11): 1547–1561.

[12] Kazuhiko Minematsu. Beyond-birthday-bound security based on tweakable block cipher[C]. Fast Software Encyption'09, Belgium, 2009, LNCS 5665: 308–326.

[13] Dinur I and Shamir A. Cube attacks on tweakable black box polynomials[C]. Cryptology Eurocrypt'09. Germany, 2009, LNCS 5479: 278–299.

郭 瑞： 男，1985 年生，硕士生，研究方向为密码学.

金晨辉： 男，1965 年生，教授，博士生导师，研究方向为密码学与信息安全.