doi:10.3969/j.issn.1000-436x.2014.06.023

分组密码 TWIS 的三子集中间相遇攻击

郑雅菲，卫宏儒
(北京科技大学 数理学院，北京 100083)

摘 要：对轻量级分组密码 TWIS 的安全性做进一步分析，将三子集中间相遇攻击应用于忽略后期白化过程的 10 轮 TWIS。基于 TWIS 密钥生成策略中存在的缺陷，即其实际密钥长度仅为 62 bit 且初始密钥混淆速度慢，攻击恢复 10 轮 TWIS 全部 62 bit 密钥的计算复杂度为 2^{45}，数据复杂度达到最低，仅为一个已知明密文对。分析结果表明 TWIS 在三子集中间相遇攻击下是不安全的。
关键词：分组密码；TWIS；中间相遇攻击；复杂度
中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2014)06-0180-05

3-subset meet-in-the-middle attack on block cipher TWIS

ZHENG Ya-fei, WEI Hong-ru
(School of Mathematics and Physics, University of Science and Technology Beijing, Beijing 100083, China)

Abstract: To do further analysis of the security of lightweight block cipher TWIS, 3-subset meet-in-the-middle attack was applied to 10-round TWIS without the final whitening. Based on the weakness in the key schedule of TWIS：its actual key size was only 62-bit and the confusion speed of the initial key was rather slow, the time complexity to recover the whole 62-bit key of 10-round TWIS was 2^{45}, and the data complexity was low enough with only one known plaintext-ciphertext pair. The result shows that block cipher TWIS is not secure under 3-subset meet-in-the-middle attack.
Key words: block cipher; TWIS; meet-in-the-middle attack; complexity

1 引言

TWIS 是由 Ojha 等人于 2009 年提出的轻量级分组密码算法[1]，设计思想基于 CLEFIA[2]，采用广义 Feistel 结构，设计者称其分组长度与密钥长度均为 128 bit，加密轮数为 10 轮。算法的设计文章未给出任何密钥恢复攻击。Su Bozhan 等人首先对其进行了安全性分析，通过构造 10 轮差分区分器，给出全 10 轮 TWIS 不抵抗差分分析的结论[3]。随后，Onur Kocak 与 Nese Oztop 给出了 TWIS 安全性的进一步研究，差分分析全 10 轮的 TWIS，恢复 12 bit 末轮轮密钥的计算复杂度为 2^{21}；构造了 9.5 轮的不可能差分区分器与线性区分器；指出 TWIS 的实际密钥长度仅为 62 bit，而不是设计者宣称的 128 bit[4]。

中间相遇攻击(meet-in-the-middle attack)由 Diffie 与 Hellman 于 1977 年针对 DES 的安全性提出[5]。其基本思想为寻找轮数尽可能长的独立密钥，对已知明密文对分别进行加密与解密操作，再选定中间变量进行匹配，筛选正确密钥。中间相遇攻击对算法结构、密钥生成策略有较严格的要求，具有数据复杂度极低的优点。中间相遇攻击目前已应用于 DES、AES、Keeloq 等分组密码算法的安全性分析中，详细过程与结果可参见文献[6~10]。

基于传统的中间相遇攻击，产生了很多改进后的攻击方法，例如，三子集中间相遇攻击。三子集中间相遇攻击由 Andrey Bogdanov 等人在轻

收稿日期：2013-03-05；**修回日期**：2013-11-20
基金项目：国家自然科学基金资助项目（61272476）；内蒙古自治区科技创新引导奖励资金基金资助项目（2012）
Foundation Items: The National Natural Science Foundation of China (61272476); The Oriented Award Foundation for Science and Technological Innovation, Inner Mongolia Autonomous Region (2012)

量级分组密码 KTANTAN[11]的安全性分析中首次提出，通过改进密钥子集合的选取与部分匹配技术的应用，增加了传统中间相遇攻击可分析的轮数。将三子集中间相遇攻击应用于全轮 KTANTAN32、KTANTAN48，攻击的数据复杂度分别为 3/2 个明密文对，计算复杂度分别为 $2^{75.044}$ / $2^{75.584}$ [12]。三子集中间相遇攻击有效地拓宽了中间相遇攻击在分组密码安全性分析中的应用。其他应用可参见 Gautham Sekar 等人对 XTEA 算法的安全性分析[13]。

本文通过研究分组密码 TWIS 轮密钥生成的缺陷，对忽略后期白化过程的全 10 轮 TWIS 应用三子集中间相遇攻击。恢复实际全部 62 bit 密钥信息的计算复杂度为 2^{45}，数据复杂度仅为一个已知明密文对，攻击结果表示 TWIS 算法不抵抗三子集中间相遇攻击。本文的计算复杂度与数据复杂度均优于 TWIS 现有的安全性分析结果。

2　分组密码 TWIS 介绍

2.1　符号说明

$A_{(l)}$：A 的长度为 l bit。

$<<< i$：左循环移位 i bit。

$>>> j$：右循环移位 j bit。

$A \oplus B$：A 和 B 按比特取异或和。

$A \wedge B$：A 和 B 按比特取与。

$|A|$：集合 A 中的元素个数。

$\varphi_{i,j}$：第 i 轮到第 j 轮的加密过程。

2.2　分组密码 TWIS

TWIS 是轻量级分组密码，其分组长度与密钥长度均为 128 bit，算法结构为 2-分支的广义 Feistel 结构，迭代轮数为 10，每轮的轮密钥长度为 32 bit。令 $P_{(128)}=(P_0,P_1,P_2,P_3)$ 表示 128 bit 明文输入，$C_{(128)}=(C_0,C_1,C_2,C_3)$ 表示 128 bit 密文输出，$RK_i(i=0,1,\cdots,10)$ 表示轮密钥，则 TWIS 的加密过程如下

$$(T_0,T_1,T_2,T_3)=(P_0\oplus RK_0,P_1,P_2,P_3\oplus RK_1)$$
$$\text{for } i=1 \text{ to } 10 \text{ do}$$
$$(X_0,X_1)=G(RK_{i-1},T_0,T_1)$$
$$T_2=X_0\oplus T_2 \quad T_3=X_1\oplus T_3$$
$$T_1=T_1<<<8 \quad T_3=T_3>>>1$$
$$(T_0,T_1,T_2,T_3)=(T_2,T_3,T_0,T_1)$$
$$(X_0,X_1)=G(RK_i,T_0,T_3)$$
$$T_1=X_0\oplus T_1 \quad T_2=X_1\oplus T_2$$
$$T_2=T_2>>>1 \quad T_3=T_3<<<8$$
$$\text{end for}$$
$$(C_0,C_1,C_2,C_3)=(T_0\oplus RK_2,T_1,T_2,T_3\oplus RK_3)$$

其中，轮函数 G 的输入为 3 个 32 bit 的分组，包括 2 个 32 bit 分支及一个 32 bit 轮密钥，输出为 2 个 32 bit 的分组。

$$G(RK,X_0,X_1)=(Y_0,Y_1)$$
$$Y_1=X_1\oplus F(RK,X_0)$$
$$Y_0=X_1$$

F 函数实现算法的密钥混合，本文攻击不涉及其具体计算，故不进行详细介绍，可参见文献[1]。

TWIS 算法通过密钥生成策略由 128 bit 的初始密钥 K 得到 11 个 32 bit 的轮密钥 $RK_i(i=0,1,\cdots,10)$，其中 RK_0 与 RK_1 为初始白化密钥，RK_2 与 RK_3 为最后的白化密钥。

各轮轮密钥的具体生成过程为

$$K=(k_1,k_2,\cdots,k_{16})$$
$$\text{for } i=1 \text{ to } 11 \text{ do}$$
$$K=K<<<3$$
$$k_1=S(k_1\wedge 0\text{x3f})$$
$$k_{15}=S(k_{15}\wedge 0\text{x3f})$$
$$k_{16}=k_{16}\oplus i$$
$$RK_{i-1}^t=\boldsymbol{M}(k_{13}k_{14}k_{15}k_{16})^t$$
$$\text{end}$$

其中，S 与 F 函数中用到的 S 盒相同，$\boldsymbol{M}$ 为混淆矩阵。

3　三子集中间相遇攻击简介

三子集中间相遇攻击是中间相遇攻击的一种改进方法，通过放宽选取密钥子集合的严格要求，使得攻击的应用范围变广。与传统中间相遇攻击将密钥空间划分为 2 个完全独立的子密钥集合不同，三子集中间相遇攻击将密钥空间划分为 3 个子密钥集合。

如图 1 所示，令 l 为密钥长度，$K=k_0k_1\cdots k_{l-1}$ 表示初始密钥。定义 $K_1=\{k_i\,|\,$应用于 $\varphi_{1,\alpha}$ 的密钥比特集合$\}$，$K_2=\{k_i:$应用于 $\varphi_{R-\beta+1,R}$ 的密钥比特集合$\}$，$A_0=K_1\cap K_2$ 表示加密过程 $\varphi_{1,\alpha}$ 与 $\varphi_{R-\beta+1,R}$ 的共用密钥集合，则 $A_1=K_1\setminus K_1\cap K_2$ 与 $A_2=K_2\setminus K_1\cap K_2$ 表示仅在 $\varphi_{1,\alpha}$ 与 $\varphi_{R-\beta+1,R}$ 中使用的密钥集合，并有 $K=K_1\cup K_2$。

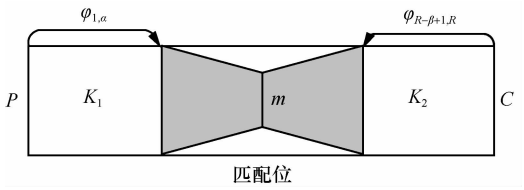

图 1 三子集中间相遇结构

当 $R-\beta+1=\alpha$ 时，三子集中间相遇攻击等价于中间相遇攻击。

三子集中间相遇攻击的过程包括 2 个步骤：首先建立三子集中间相遇结构，并利用该结构过滤部分错误密钥，减小密钥空间；然后通过进一步的密钥筛选寻找正确密钥。

首先建立三子集中间相遇结构。

记 (P,C) 为一个明密文对，对 A_0 的每种猜测值。

1) 猜测 A_1 中密钥的所有可能值，计算 $v=\varphi_{1,\ \alpha}(P)$；

2) 猜测 A_2 中密钥的所有可能值，计算 $u=\varphi^{-1}_{R-\beta+1,\ R}(C)$；

3) 确定进行中间匹配的轮数，对 v 与 u 分别进行加密与解密运算，得到匹配轮数处对应的加密结果 v'与解密结果 u'的 $m(1\leqslant m\leqslant b)$ 个比特，并对 m 个比特值进行匹配，若 m 个比特值不完全相同，则认为是错误密钥。该步对密钥的筛选概率为 2^{-m}，即经过该步筛选后剩余密钥数为 2^{l-m}。

该步的计算复杂度为

$$2^{|A_0|}(2^{|A_1|}+2^{|A_2|})$$

接下来，进一步对剩余所有密钥进行筛选。

穷举搜索剩余的所有密钥候选值，利用明密文对 (P,C) 计算中间匹配轮数处 v'与 u'的值，并对其全部 b 比特值进行匹配，若 b 比特值不完全相同，则认为是错误密钥。一次匹配可删除 2^b 个错误密钥。对剩余的 2^{l-m-b} 个可能密钥候选值重复该过程，直到得出唯一的正确密钥。

该步的计算复杂度为

$$2^{l-m}+2^{l-m-b}+2^{l-m-2b}+\cdots$$

综上所述，完整三子集中间相遇攻击的计算复杂度可表示为

$$2^{|A_0|}(2^{|A_1|}+2^{|A_2|})+(2^{l-m}+2^{l-m-b}+2^{l-m-2b}+\cdots)$$

在对密钥子集合的划分中，只要 $|A_1|+|A_2|>2$，即可得到优于穷举搜索的计算复杂度。

在密钥筛选阶段，共需要进行 $\lceil l/b\rceil$ 次匹配来筛选得到正确密钥，而每次匹配需要一个明密文对，即攻击所需数据量依赖于密钥长度 l 与分组长度 b，且 $DC=\lceil l/b\rceil$。

4 TWIS 的三子集中间相遇攻击

TWIS 算法的设计者称其密钥长度为 128 bit，但是观察其密钥生成策略可以发现，每轮变换循环移位仅 3 bit，值改变的量仅为 24 bit。这使得初始密钥的混淆速度非常慢。经过推导可发现其实际密钥长度仅为 62 bit，且忽略后期白化后，算法首尾两端可找到较长轮数的独立密钥。

本文攻击利用该特点，通过推测各轮的轮密钥，对忽略后期白化过程的全 10 轮 TWIS 应用三

表 1 **TWIS 各轮轮密钥**

轮数	RK_{i-1}	RK_i
前期白化	$\{k_0,k_1,k_2,k_{99},k_{100},\cdots,k_{127}\}$	$\{k_0,k_1,\cdots,k_5,k_{102},k_{103},\cdots,k_{127}\}$
i=1	$\{k_0,k_1,k_2,k_{99},k_{100},\cdots,k_{127}\}$	$\{k_0,k_1,\cdots,k_5,k_{102},k_{103},\cdots,k_{127}\}$
i=2	$\{k_0,k_1,\cdots,k_5,k_{102},k_{103},\cdots,k_{127}\}$	$\{k_0,k_1,\cdots,k_8,k_{105},k_{106},\cdots,k_{127}\}$
i=3	$\{k_0,k_1,\cdots,k_8,k_{105},k_{106},\cdots,k_{127}\}$	$\{k_0,k_1,\cdots,k_{11},k_{108},k_{109},\cdots,k_{127}\}$
i=4	$\{k_0,k_1,\cdots,k_{11},k_{108},k_{109},\cdots,k_{127}\}$	$\{k_0,k_1,\cdots,k_{14},k_{111},k_{112},\cdots,k_{127}\}$
i=5	$\{k_0,k_1,\cdots,k_{14},k_{111},k_{112},\cdots,k_{127}\}$	$\{k_0,k_1,\cdots,k_{17},k_{114},k_{115},\cdots,k_{127}\}$
i=6	$\{k_0,k_1,\cdots,k_{17},k_{114},k_{115},\cdots,k_{127}\}$	$\{k_0,k_1,\cdots,k_{20},k_{117},k_{118},\cdots,k_{127}\}$
i=7	$\{k_0,k_1,\cdots,k_{20},k_{117},k_{118},\cdots,k_{127}\}$	$\{k_0,k_1,\cdots,k_{23},k_{120},k_{121},\cdots,k_{127}\}$
i=8	$\{k_0,k_1,\cdots,k_{23},k_{120},k_{121},\cdots,k_{127}\}$	$\{k_0,k_1,\cdots,k_{26},k_{123},k_{124},\cdots,k_{127}\}$
i=9	$\{k_0,k_1,\cdots,k_{26},k_{123},k_{124},\cdots,k_{127}\}$	$\{k_0,k_1,\cdots,k_{29},k_{126},k_{127}\}$
i=10	$\{k_0,k_1,\cdots,k_{29},k_{126},k_{127}\}$	$\{k_1,k_2,\cdots,k_{32}\}$
后期白化	$\{k_0,k_1,\cdots,k_8,k_{105},k_{106},\cdots,k_{127}\}$	$\{k_0,k_1,\cdots,k_{11},k_{108},k_{109},\cdots,k_{127}\}$

子集中间相遇攻击。

4.1　轮密钥推导

三子集中间相遇攻击利用 TWIS 一些密钥比特在连续的多轮加密过程中未被使用的特点。所以为了建立 TWIS 的三子集中间相遇结构，首先推导各轮加密使用的轮密钥。根据 TWIS 密钥生成策略得到的各轮轮密钥的使用情况如表 1 所示。

观察各轮轮密钥的使用情况可以发现，虽然 TWIS 的设计者称其密钥长度为 128 bit，但实际有效的密钥长度仅为 62 bit，即在轮密钥生成过程中，仅使用了初始密钥的 $\{k_0,k_1,\cdots,k_{32},k_{99},k_{100},\cdots,k_{127}\}$ 这 62 bit，而其他 66 bit 无效。这使得对 TWIS 的穷举搜索复杂度由 2^{128} 降为 2^{62}。记实际密钥空间为 $K'=\{k_0,k_1,\cdots,k_{32},k_{99},k_{100},\cdots,k_{127}\}$。

4.2　10 轮 TWIS 的三子集中间相遇攻击

在 TWIS 实际密钥长度 l=62 的基础上应用三子集中间相遇攻击，使得复杂度进一步降低。

考虑初始白化密钥，忽略后期白化密钥，观察各轮轮密钥可有如下发现。

从第 0 轮至第 4 轮的轮密钥涉及的密钥比特集合为 $\{k_0,k_1,\cdots,k_{14},k_{99},k_{100},\cdots,k_{127}\}$，未使用实际密钥的 18 个比特集合为 $\{k_{15},k_{16},\cdots,k_{31},k_{32}\}$。

从第 7 轮至第 10 轮的轮密钥涉及的密钥比特集合为 $\{k_0,k_1,\cdots,k_{32},k_{117},k_{118},\cdots,k_{127}\}$，未使用实际密钥的 18 比特集合为 $\{k_{99},k_{100},\cdots,k_{115},k_{116}\}$。

利用 TWIS 轮密钥的上述 2 个重要特点，根据第 3 节中对三子集中间相遇攻击思想与过程的介绍，选取 $\alpha=4$，$\beta=7$，即可将实际密钥空间划分为 3 个子集合 A_0、A_1 和 A_2，划分方式如下

$$K^{'}=\{k_0,k_1,\cdots,k_{32},k_{99},k_{100},\cdots,k_{127}\}$$

$$\begin{aligned}K_1&=K^{'}\setminus\{k_{15},k_{16},\cdots,k_{31},k_{32}\}\\&=\{k_0,k_1,\cdots,k_{14},k_{99},k_{100},\cdots,k_{127}\}\end{aligned}$$

$$\begin{aligned}K_2&=K^{'}\setminus\{k_{99},k_{100},\cdots,k_{115},k_{116}\}\\&=\{k_0,k_1,\cdots,k_{32},k_{117},k_{118},\cdots,k_{127}\}\end{aligned}$$

$$A_0=K_1\cap K_2=\{k_0,k_1,\cdots,k_{14},k_{117},k_{118},\cdots,k_{127}\}$$

$$A_1=K_1\setminus A_0=\{k_{99},k_{100},\cdots,k_{116}\}$$

$$A_2=K_2\setminus A_0=\{k_{15},k_{16},\cdots,k_{32}\}$$

$$|A_1|=|A_2|=18,|A_0|=26$$

利用这些参数即可得到 10 轮 TWIS 的三子集中间相遇结构，并对密钥进行初步筛选。具体过程如下。

已知一个明密文对(P,C)，对 A_0 的 2^{26} 种可能值。

1) 猜测 A_1 中密钥的所有 2^{18} 种可能值，计算 $v=\varphi_{1,4}(P)$。

2) 猜测 A_2 中密钥的所有 2^{18} 种可能值，计算 $u=\varphi_{7,10}^{-1}(C)$。

3) 选择第 5 轮为中间匹配轮数，得到第 5 轮处的 v'与 u'，具体推导过程如图 2 所示。图中黑色部分表示受独立密钥 A_1、A_2 影响，白色部分表示不受影响。对 v'与 u'均不受独立密钥影响的 32 个比特值进行匹配，若 32 个比特值不完全相同，则认为是错误密钥，筛选概率为 2^{-32}。

该步的计算复杂度为：$2^{26}(2^{18}+2^{18})=2^{45}$。

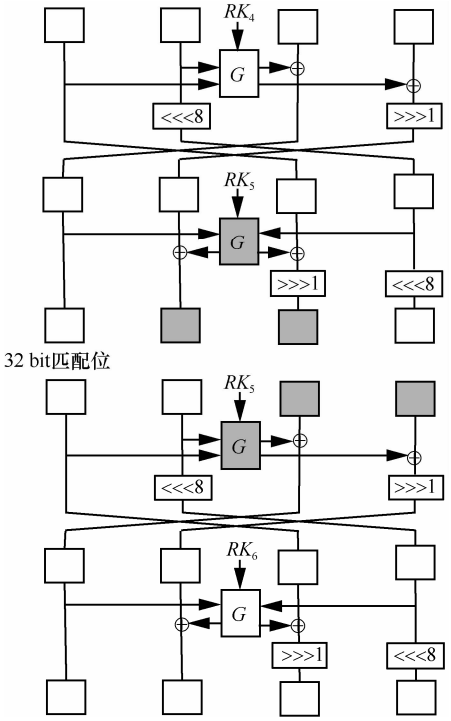

图 2　中间匹配过程

接下来，穷举搜索剩余 $2^{l-m}=2^{30}$ 个密钥候选值，利用明密文对(P,C)重新计算 v'与 u'的值，并对其 128 bit 值进行匹配，若 128 bit 值不完全相同，则认为是错误密钥，该步的筛选概率为 2^{-128}。重复该步骤，直到得到满足 v'=u'的唯一正确密钥。

该步的计算复杂度为

$$\begin{aligned}&2^{l-m}+2^{l-m-b}+2^{l-m-2b}+\cdots\\&=2^{30}+2^{-98}+\cdots\\&\approx 2^{30}\end{aligned}$$

观察上式可发现，对 TWIS 只需要一步筛选即

可期待淘汰所有错误密钥，得到唯一的正确密钥。

4.3 复杂度分析

根据第 3 节中对三子集中间相遇攻击复杂度计算的介绍，恢复 10 轮 TWIS 实际全部 62 bit 密钥信息的计算复杂度为

$$\begin{aligned}&2^{|A_0|}(2^{|A_1|}+2^{|A_2|})+2^{l-m}+2^{l-m-b}+\cdots\\&=2^{26}(2^{18}+2^{18})+2^{30}+2^{-98}+\cdots\\&\approx 2^{45}\end{aligned}$$

数据复杂度为 $DC=\left\lceil\frac{l}{b}\right\rceil=\left\lceil\frac{62}{128}\right\rceil=1$。

5 结束语

如表 2 所示，针对 TWIS 算法密钥生成策略中存在的缺陷，本文首次对忽略后期白化的全 10 轮 TWIS 应用了三子集中间相遇攻击。恢复实际密钥的全部 62 bit 密钥信息的数据复杂度仅为一个明密文对，计算复杂度为 2^{45}，分析结果表明忽略后期白化的全 10 轮 TWIS 算法不抵抗三子集中间相遇攻击。本文结果优于文献[4]中 Onur Kocak 等人差分攻击 10 轮 TWIS 得到的结果。

表 2 TWIS 安全性分析结果

算法	轮数	恢复密钥比特	计算复杂度	数据复杂度	攻击方法
本文	10	62	2^{45}	1	三子集 MITM
文献[4]	10	12	2^{21}	2^{21}	差分攻击

参考文献：

[1] OJHA S K, KUMAR N, JAIN K. TWIS–a lightweight block cipher[A]. Information Systems Security[C]. Berlin: Springer Heidelberg, 2009.280-291.

[2] SHIRAI T, SHIBUTANI K, AKISHITA T, *et al*. The 128 bit block cipher CLEFIA[A]. Fast Software Encryption[C]. Berlin: Springer Heidelberg, 2007.181-195.

[3] SU B Z, WU W L, ZHANG L, *et al*. Full-round differential attack on TWIS block cipher[A]. Information Security Applications[C]. Berlin: Springer Heidelberg, 2011.234-242.

[4] KOCAK O, OZTOP N. Cryptanalysis of TWIS block cipher[A]. Research in Cryptology[C]. Berlin: Springer Heidelberg, 2012.109-121.

[5] DIFFIE W, HELLMAN M E. Special feature exhaustive cryptanalysis of the NBS data encryption standard[J]. Computer, 1977, 10(6): 74-84.

[6] CHAUM D, EVERTSE J H. Cryptanalysis of DES with a reduced number of rounds[A]. Cryptology-CRYPTO'85 Proceedings[C]. Berlin: Springer Heidelberg, 1986.192-211.

[7] DEMIRCI H, SELCUK A A. A meet-in-the-middle attack on 8-round AES[A]. Fast Software Encryption[C]. Berlin: Springer Heidelberg, 2008.116-126.

[8] DEMIRCI H, TASKM İ, COBAN M, *et al*. Improved meet-in-the-middle attacks on AES[A]. Progress in Cryptology- INDOCRYPT 2009[C]. Berlin: Springer Heidelberg, 2009.144-156.

[9] DUNKELMAN O, SEKAR G, PRENEEL B. Improved meet-in-the-middle attacks on reduced-round DES[A]. Progress in Cryptology–INDOCRYPT 2007[C]. Berlin: Springer Heidelberg, 2007.86-100.

[10] INDESTEEGE S, KELLER N, DUNKELMAN O, *et al*. A practical attack on keeloq[A]. Cryptology-EUROCRYPT 2008[C]. Berlin: Springer Heidelberg, 2008.1-18.

[11] DE C C, DUNKELMAN O, KNEZEVIC M. KATAN and KTANTAN—a family of small and efficient hardware-oriented block ciphers[A]. Cryptographic Hardware and Embedded Systems-CHES 2009[C]. Berlin: Springer Heidelberg, 2009.272-288.

[12] BOGDANOV A, RECHBERGER C. A 3-subset meet-in-the-middle attack: cryptanalysis of the lightweight block cipher KTANTAN[A]. Selected Areas in Cryptography[C]. Berlin: Springer Heidelberg, 2011.229-240.

[13] SEKAR G, MOUHA N, VELICHKOV V, *et al*. Meet-in-the-middle attacks on reduced-round XTEA[A]. Topics in Cryptology–CT-RSA 2011[C]. Berlin: Springer Heidelberg, 2011.250-267.

作者简介：

郑雅菲（1988-），女，河北任丘人，北京科技大学硕士生，主要研究方向为密码学。

卫宏儒（1963-），男，陕西扶风人，北京科技大学副教授，主要研究方向为数学、信息安全与密码学、物联网关键技术。