用不可能差分法分析12轮ESF算法

高红杰 卫宏儒
(北京科技大学数理学院 北京 100083)

摘 要 轻量级分组密码算法ESF是一种具有广义Feistel结构的32轮迭代型分组密码,轮函数具有SPN结构,分组长度为64比特,密钥长度为80比特。为了研究ESF算法抵抗不可能差分攻击的能力,基于一条8轮不可能差分路径,根据轮密钥之间的关系,通过向前增加2轮、向后增加2轮的方式,对12轮ESF算法进行了攻击。计算结果表明,攻击12轮ESF算法所需的数据复杂度为$O(2^{53})$,时间复杂度为$O(2^{60.43})$,由此说明12轮的ESF算法对不可能差分密码分析是不免疫的。

关键词 分组密码,不可能差分密码分析,ESF,轻量级,复杂度
中图法分类号 TN918.1 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2017.10.028

Impossible Differential Attack on 12-round Block Cipher ESF

GAO Hong-jie WEI Hong-ru
(School of Mathematics and Physics, University of Science and Technology Beijing, Beijing 100083, China)

Abstract ESF is a lightweight block cipher algorithm with generalized Feistel structure of 32 rounds of iterated block ciphers. Its round function employs SPN structure. The block size of ESF is 64-bit and the key size is 80-bit. In order to analyze impossible differential cryptanalysis on the block cipher ESF, based on one 8-round impossible differential route, according to the relationship of the round keys, through adding two rounds in the front and adding two rounds in the end, 12-round ESF was attacked. Computing result shows that the attacks of 12-round ESF need $O(2^{53})$ data complexity, and $O(2^{60.43})$ time complexity, so 12-round ESF is not immune to impossible differential cryptanalysis.

Keywords Block cipher, Impossible differential cryptanalysis, ESF, Lightweight, Complexity

1 引言

不可能差分密码分析是差分密码分析的一种特殊形式,是一种十分有效的分析方法[1],最初是由Biham[2]和Keller[2]提出的,主要利用概率为0的差分,其基本思想是排除那些导致概率为0的特征或差分的候选密钥[3]。对于一条概率为0的差分路径,当用正确密钥解密密文对时不会得到符合该路径的差分;当用猜测密钥解密密文对时能得到符合该路径的差分,那么该密钥猜测值是错误的;从而筛除了所有的错误密钥猜测值,剩下的就是需要恢复的正确密钥[4]。近年来,该攻击方法被广泛运用于分组密码的分析中,如MIBS,LBlock,CLEFIA[5],SNAKE[6],Camellia,SMS4[7-8]等。

ESF算法是刘宣等在研究吴文玲学者设计的LBlock[9]算法之后提出的,他们发现通过对置换层进行按位置换的方式能够得到更好的置换层扩散性以及对较少轮数中的置换数据进行更快的扩散,这大大提升了分组密码抵抗攻击的能力。此外,基于算法PRESNT中P层置换的形式,借助数学公式对P层进行改善,于是得到了“八阵图算法”ESF算法[10-12]。这是一种具有广义Feistel结构的32轮迭代型分组密码,轮函数具有SPN结构,分组长度为64比特,密钥长度为80比特。

目前,对ESF算法的分析结果包括:文献[11]对ESF进行了11轮的不可能差分攻击,文献[12]对文献[11]中ESF的11轮不可能差分结果进行了改进,文献[13]对ESF算法进行了差分故障攻击。本文基于1条8轮不可能差分路径,根据轮密钥之间的关系,通过向前增加2轮、向后增加2轮的方式,对12轮ESF算法进行了不可能差分攻击。

2 ESF算法

2.1 符号及术语说明

M为64比特明文;C为64比特密文;K为80比特主密钥;K_r为32比特轮密钥;F为轮函数;s表示4×4 S盒;S为混淆层,包含8个4×4 S盒;⊕表示按位异或;P为扩散层;$\lll 7$表示循环左移7位;‖表示二进制字符联接;$[i]_2$为轮常数i的二进制表示。

2.2 ESF算法简介

ESF算法是一种Feistel型分组密码,分组长度为64比特,密钥长度为80比特,共有32轮。其加密结构如图1所

到稿日期:2016-09-13 返修日期:2016-12-23 本文受2016年国家自然科学基金项目:认证加密算法的设计和分析(61672509),2017年国家自然科学基金项目:面向网络空间的大数据安全与隐私保护研究(U1603116)资助。
高红杰(1992-),女,硕士生,主要研究方向为密码学与信息安全,E-mail:1532766237@qq.com;卫宏儒(1963-),男,副教授,硕士生导师,主要研究方向为数学、信息安全与密码学、物联网关键技术,E-mail:weihr@ustb.edu.cn。

示，每轮的轮函数 F 如图 2 所示，其中轮函数 F 包括轮子密钥加变换、非线性变换 S 盒和扩散变换 P。

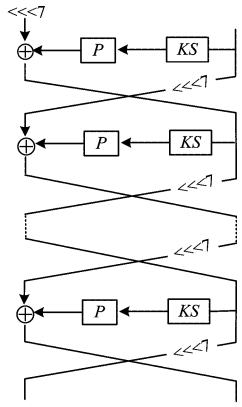

图 1 ESF 算法的加密流程

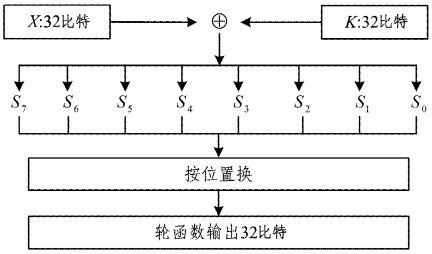

图 2 F 函数图

将 64 比特的明文分组为 L_0 和 R_0 两个 32 比特的值。设 L_{i-1} 和 R_{i-1} 是第 i 轮的输入，k_i 是 32 比特轮密钥，当 $1\leqslant i\leqslant 31$ 时，第 i 轮的迭代公式为：

$L_{i+1}=R_i$，$R_{i+1}=(L_{i-1}<<<7)\oplus F(R_i,K_i)$

经过 31 轮中间变换之后，当 $i=32$ 时，输出结果为：

$C=L_{32}\parallel R_{32}$

1)轮函数 F

$F:\{0,1\}^{32}\times\{0,1\}^{32}\rightarrow\{0,1\}^{32}$

$(R,k_i)\rightarrow Z=P(S(R\oplus k_i))$

2)非线性混淆层

ESF 算法的轮函数 F 采用典型的 SPN 结构，其中非线性变换 S 盒由 8 个并行的 4×4S 盒构成，表示为：$S=(S_1,S_2,S_3,S_4,S_5,S_6,S_7,S_8)$。

3)P 置换层

该层为线性变换，其构成如下：

①$P:\{0,1\}^{32}\rightarrow\{0,1\}^{32}$

$b=b_7\parallel b_6\parallel b_5\parallel b_4\parallel b_3\parallel b_2\parallel b_1\parallel b_0\rightarrow c=c_7\parallel c_6\parallel c_5\parallel c_4\parallel c_3\parallel c_2\parallel c_1\parallel c_0$

②当 $0\leqslant i\leqslant 8$ 时

$b_{4i}\parallel b_{4i+1}\parallel b_{4i+2}\parallel b_{4i+3}\rightarrow c_i\parallel c_{i+8}\parallel c_{i+16}\parallel c_{i+24}$

解密算法过程：对于 $r=31,30,\cdots,1,0$，计算：

1)$R_i=L_{i+1}$，$L_i=(F(L_{i+1},k_i)\oplus R_{i+1})>>>7$；

2)输出 $M=L_0\parallel R_0$ 为 64 比特明文。

2.3 ESF 的密钥编排

ESF 算法的密钥编排算法是通过对 80 比特的主密钥进行一系列运算的方式，使其产生 32 比特轮密钥的算法。将主密钥取为 $K=k_{79}k_{78}\cdots k_0$ 并存入密钥寄存器，将最左端存入 k_{79}，将最右端存入 k_0，取最左端的 32 比特密钥作为轮密钥 k_1，然后更新每轮轮密钥。对于 $i=1,2,3\cdots31$，按如下步骤更新密钥寄存器 K：

(1)$K<<<13$；

(2)密钥寄存器$[k_{79}k_{78}k_{77}k_{76}]=S_0[k_{79}k_{78}k_{77}k_{76}]$，$[k_{75}k_{74}k_{73}k_{72}]=S_0[k_{75}k_{74}k_{73}k_{72}]$；

(3)$[k_{47}k_{46}k_{45}k_{44}k_{43}]=[k_{47}k_{46}k_{45}k_{44}k_{43}]\oplus$轮常数 i；

(4)取当前寄存器 K 最左端的 32 比特作为轮密钥 K_{i+1} 的输出。

3 ESF 算法的不可能差分分析

3.1 ESF 算法的 8 轮不可能差分路径

利用文献[10]提出的 8 轮不可能差分路径：

(000a|bcd0|0000|0000|0000|0000|0000|0000|0000|0000|0000|0000|0000|0000|0000|0000)→(0000|0000|0000|0000|0000|0000|0000|0000|0000|0000|0000|0000|0000|0000|0000|0000|0efg|h000)

其中，a,b,c,d,e,f,g 是非零值，$h=1$。图 2 是 ESF 的 8 轮不可能差分路径，具体推导请参见文献[10]。

3.2 ESF 算法的 12 轮不可能差分攻击

利用上述的 8 轮不可能差分路径对 12 轮的 ESF 算法进行不可能差分攻击。其基本思想是：在 8 轮不可能差分路径的基础上，通过向前增加 2 轮、向后增加 2 轮的方式，进一步利用不可能差分将错误密钥进行淘汰，从而得到正确密钥。12 轮不可能差分攻击的过程如图 3 所示。

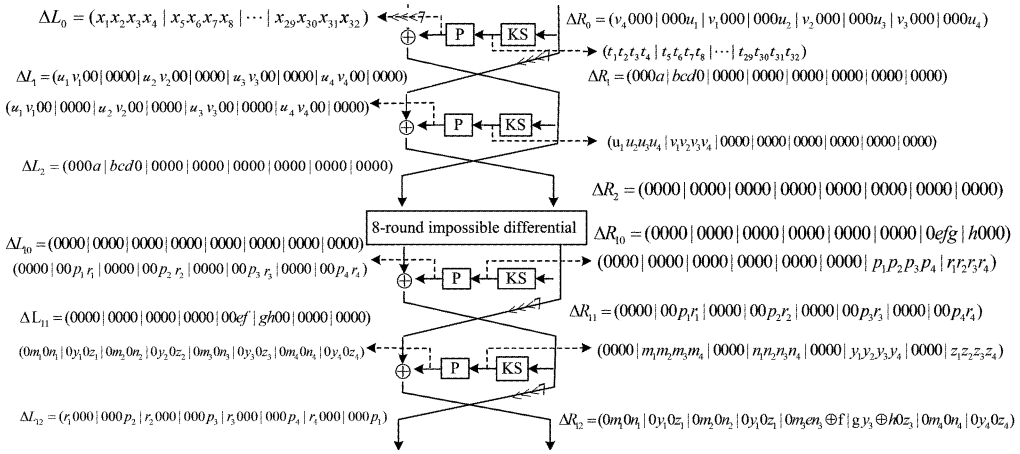

图 3 ESF 算法的 12 轮不可能差分分析路线

(1)选择明文结构

选择如下明文组：$L_0=(x_1x_2x_3x_4\,|\,x_5x_6x_7x_8\,|\cdots|\,x_{29}x_{30}x_{31}x_{32})$，$R_0=(y_1a_2a_3a_4\,|\,a_5a_6a_7y_8\,|\,y_9a_{10}a_{11}a_{12}\,|\,a_{13}a_{14}a_{15}y_{16}\,|\,y_{17}a_{18}a_{19}a_{20}\,|\,a_{21}a_{22}a_{23}y_{24}\,|\,y_{25}a_{26}a_{27}a_{28}\,|\,a_{29}a_{30}a_{31}y_{32})$，其中，$x_i(1\leqslant i\leqslant 32)$和 $y_i(i=1,8,9,16,17,24,25,32)$取所有可能值，$a_i$ 为常数。

该明文结构包括 2^{40} 个明文，可形成 2^{79} 个明文对，选取 2^N 个这样的结构进行 12 轮加密，则共有 2^{N+40} 个明文，可形成 2^{N+79} 个明密文对。

(2)过滤数据对

对这些明文对进行 12 轮加密，得到相应的密文对，选择满足如下差分形式的密文对：$\Delta L_{12}=(r_1000\,|\,000p_2\,|\,r_2000\,|\,000p_3\,|\,r_3000\,|\,000p_4\,|\,r_4000\,|\,000p_1)$，$\Delta R_{12}=(0m_10n_1\,|\,0y_10z_1\,|\,0m_20n_2\,|\,0y_20z_2\,|\,0m_3en_3\oplus f\,|\,gy_3\oplus h0z_3\,|\,0m_40n_4\,|\,0y_40z_4)$，其中 $p_i,r_i(i=1,2,3,4)$为非零值。因此满足条件的概率为 $p=2^{26}\times 2^{-64}=2^{-38}$，剩下的明密文对为 2^{N+41}。

(3)密钥恢复过程

1)猜测轮密钥 k_{12} 的 8 个比特值 $k_{12,7},k_{12,8},k_{12,15},k_{12,16},k_{12,23},k_{12,24},k_{12,31},k_{12,32}$，对上一步留下的任意一对密文计算满足 $s_2(L_{12,7}\oplus k_{12,7})\oplus s_2(L^*_{12,7}\oplus k_{12,7})=R_{12,7}\oplus R^*_{12,7}$，$s_2(L_{12,8}\oplus k_{12,8})\oplus s_2(L^*_{12,8}\oplus k_{12,8})=R_{12,8}\oplus R^*_{12,8}$，$s_4(L_{12,15}\oplus k_{12,15})\oplus s_4(L^*_{12,15}\oplus k_{12,15})=R_{12,15}\oplus R^*_{12,15}$，$s_4(L_{12,16}\oplus k_{12,16})\oplus s_4(L^*_{12,16}\oplus k_{12,16})=R_{12,16}\oplus R^*_{12,16}$，$s_6(L_{12,23}\oplus k_{12,23})\oplus s_6(L^*_{12,23}\oplus k_{12,23})=R_{12,23}\oplus R^*_{12,23}$，$s_6(L_{12,24}\oplus k_{12,24})\oplus s_6(L^*_{12,24}\oplus k_{12,24})=R_{12,24}\oplus R^*_{12,24}$，$s_8(L_{12,31}\oplus k_{12,31})\oplus s_8(L^*_{12,31}\oplus k_{12,31})=R_{12,31}\oplus R^*_{12,31}$，$s_8(L_{12,32}\oplus k_{12,32})\oplus s_8(L^*_{12,32}\oplus k_{12,32})=R_{12,32}\oplus R^*_{12,32}$的数据对，因此满足条件的概率为 2^{-8}，剩余数据对为 $2^{N+41}\times 2^{-8}=2^{N+33}$。

2)猜测轮密钥 k_{11} 的 4 个比特值 $k_{11,26},k_{11,27},k_{11,28},k_{11,29}$，对第 1)步留下的任意一对密文计算满足 $s_7(L_{11,26}\oplus k_{11,26})\oplus s_7(L^*_{11,26}\oplus k_{11,26})=R_{11,26}\oplus R^*_{11,26}$，$s_7(L_{11,27}\oplus k_{11,27})\oplus s_7(L^*_{11,27}\oplus k_{11,27})=R_{11,27}\oplus R^*_{11,27}$，$s_7(L_{11,28}\oplus k_{11,28})\oplus s_7(L^*_{11,28}\oplus k_{11,28})=R_{11,28}\oplus R^*_{11,28}$，$s_8(L_{11,29}\oplus k_{11,29})\oplus s_8(L^*_{11,29}\oplus k_{11,29})=R_{11,29}\oplus R^*_{11,29}$的数据对，因此满足条件的概率为 2^{-4}，剩余数据对为 2^{N+29}。

3)猜测轮密钥 k_1 的 1,8,9,16,17,24,25,32 这 8 个比特，针对第 2)步留下的每一个密文对相应的明文对(L_0,R_0)和(L_0^*,R_0^*)，$L_0=(x_1x_2x_3x_4\,|\,x_5x_6x_7x_8\,|\cdots|\,x_{29}x_{30}x_{31}x_{32})$，$R_0=y_1a_2a_3a_4\,|\,a_5a_6a_7y_8\,|\,y_9a_{10}a_{11}a_{12}\,|\,a_{13}a_{14}a_{15}y_{16}\,|\,y_{17}a_{18}a_{19}a_{20}\,|\,a_{21}a_{22}a_{23}y_{24}\,|\,y_{25}a_{26}a_{27}a_{28}\,|\,a_{29}a_{30}a_{31}y_{32})$，$L_0^*=(x_1^*x_2^*x_3^*x_4^*\,|\,x_5^*x_6^*x_7^*x_8^*\,|\cdots|\,x_{29}^*x_{30}^*x_{31}^*x_{32}^*)$，$R_0^*=(y_1^*a_2a_3a_4\,|\,a_5a_6a_7y_8^*\,|\,y_9^*a_{10}a_{11}a_{12}\,|\,a_{13}a_{14}a_{15}y_{16}^*\,|\,y_{17}^*a_{18}a_{19}a_{20}\,|\,a_{21}a_{22}a_{23}y_{24}^*\,|\,y_{25}^*a_{26}a_{27}a_{28}\,|\,a_{29}a_{30}a_{31}y_{32}^*)$，计算$(L_1,R_1)$和$(L_1^*,R_1^*)$，选择差分对 $R_1\oplus R_1^*=(000a\,|\,bcd0\,|\,0000\,|\,0000\,|\,0000\,|\,0000\,|\,0000\,|\,0000)$，其中 a,b,c,d 是非零值，因此满足条件的概率为 2^{-28}，此时剩余数据对为 2^{N+1}。

4)猜测轮密钥 k_2 的 4,5,6,7 这 4 个比特，做如下操作：针对上一步留下的每一对(L_0,R_0)和(L_0^*,R_0^*)，以及相应的(L_1,R_1)和(L_1^*,R_1^*)，$L_1=(y_1y_2a_3a_4\,|\,a_5a_6a_7a_8\,|\,y_9y_{10}a_{11}a_{12}\,|\,a_{13}a_{14}a_{15}a_{16}\,|\,y_{17}y_{18}a_{19}a_{20}\,|\,a_{21}a_{22}a_{23}a_{24}\,|\,y_{25}y_{26}a_{27}a_{28}\,|\,a_{29}a_{30}a_{31}a_{32})$，$R_1=(r_1r_2r_3z_4\,|\,z_5z_6z_7r_8\,|\,r_9r_{10}r_{11}r_{12}\,|\,r_{13}r_{14}r_{15}r_{16}\,|\,r_{17}r_{18}r_{19}r_{20}\,|\,r_{21}r_{22}r_{23}r_{24}\,|\,r_{25}r_{26}r_{27}r_{28}\,|\,r_{29}r_{30}r_{31}r_{32})$，$L_1^*=(y_1^*y_2^*a_2a_3a_4\,|\,a_5a_6a_7a_8\,|\,y_9^*y_{10}^*a_{11}a_{12}\,|\,a_{13}a_{14}a_{15}a_{16}\,|\,y_{17}^*y_{18}^*a_{19}a_{20}\,|\,a_{21}a_{22}a_{23}a_{24}\,|\,y_{25}^*y_{26}^*a_{27}a_{28}\,|\,a_{29}a_{30}a_{31}a_{32})$，$R_1^*=(r_1^*r_2^*r_3^*z_4^*\,|\,z_5^*z_6^*z_7^*r_8^*\,|\,r_9^*r_{10}^*r_{11}^*r_{12}^*\,|\,r_{13}^*r_{14}^*r_{15}^*r_{16}^*\,|\,r_{17}^*r_{18}^*r_{19}^*r_{20}^*\,|\,r_{21}^*r_{22}^*r_{23}^*r_{24}^*\,|\,r_{25}^*r_{26}^*r_{27}^*r_{28}^*\,|\,r_{29}^*r_{30}^*r_{31}^*r_{32}^*)$。计算 $s_1(z_4\oplus k_{2,4})\oplus s_1(z_4^*\oplus k_{2,4})=R_{2,4}\oplus R^*_{2,4}$，$s_2(z_5\oplus k_{2,5})\oplus s_2(z_5^*\oplus k_{2,5})=R_{2,5}\oplus R^*_{2,5}$，$s_2(z_6\oplus k_{2,6})\oplus s_2(z_6^*\oplus k_{2,6})=R_{2,6}\oplus R^*_{2,6}$，$s_2(z_7\oplus k_{2,7})\oplus s_2(z_7^*\oplus k_{2,7})=R_{2,7}\oplus R^*_{2,7}$，选择所有差分形式满足上述条件的数据对，因此满足条件的概率为 2^{-4}，此时剩余数据对为 2^{N-3}。

5)对上一步留下的每一个剩余对，判断 ΔR_2 是否等于$(0000\,|\,0000\,|\,0000\,|\,0000\,|\,0000\,|\,0000\,|\,0000\,|\,0000)$，若等于，则差分分析不可能成立，此时经过 2^{N-3} 个剩余明密文对，64 比特的密钥中剩余的错误密钥个数为 $2^{64}\times(1-2^{-4})^{2^{N-3}}<1$，即可恢复正确密钥，经过计算可得 $N\approx 13$。

攻击的复杂度计算过程如下：

步骤 1　$2\times 2^8\times 2^{N+41}=2^{63}$

步骤 2　$2\times 2^8\times 2^4\times 2^{N+33}\times(4/8)=2^{57}$

步骤 3　$2\times 2^8\times 2^4\times 2^8\times 2^{N+29}=2^{63}$

步骤 4　$2\times 2^8\times 2^4\times 2^8\times 2^4\times 2^{N+1}\times(4/8)=2^{37}$

因此该攻击的总时间复杂度为：$(2^{63}+2^{57}+2^{63}+2^{37})/12\approx 2^{60.43}$。

明文量为：$2^{N+40}=2^{13+40}=2^{53}$。

综上可得：总的时间复杂度为 $O(2^{60.43})$，数据复杂度为 $O(2^{53})$。

结束语　本文基于已有的 8 轮不可能差分路径，通过向前增加 2 轮、向后增加 2 轮的方式，构成了针对 12 轮 ESF 算法的不可能差分密码分析。通过计算数据复杂度和时间复杂度，获得了较好的结果。此外，通过寻找更好的不可能差分路径来改善目前已有的结果或者对更长轮数的 ESF 算法进行不可能差分攻击，以及用其他分析方法对 ESF 算法进行分析，将是之后对 ESF 算法进行研究的方向。

参 考 文 献

[1] CHEN Z, WANG N. Impossible Differential Cryptanalysis of SIMON[J]. Journal of Password, 2015, 2(6): 505-514. (in Chinese)
陈展，王宁. SIMON 算法的不可能差分分析[J]. 密码学报，2015，2(6)：505-514.

[2] CHEN J, HU Y P, ZHANG Y Y. Impossible differential attack on the 17-round block ciper SMS4[J]. Journal of Xidian University, 2008, 35(3): 455-458. (in Chinese)
陈杰，胡予濮，张跃宇. 用不可能差分法分析 17 轮 SMS4 算法[J]. 西安电子科技大学学报，2008，35(3)：455-458.

[3] WU W L, ZHANG W T, FENG D G. Impossible differential cryptanalysis of ARIA and Camellia[J]. Journal of Computer Science and Technology, 2007, 22(3): 449-456.

[4] 吴文玲，冯登国，张文涛. 分组密码的设计与分析[M]. 北京：清华大学出版社，2009：68-72.

[5] MALA H, DAKHILALIAN M. Impossible attacks on 13-round CLEFIA-128[J]. Journal of Computer Science and Technology, 2011, 26(4): 744-750.

(下转第 181 页)

关数据集上,Skyline 查询的平均通信消耗最大。

当数据维不变且网络规模不断增加时,节点数不断增加,导致数据元组的传输数量也在不断增加,从而导致最终的 Skyline 结果集增大。图 3 给出了当数据维度为默认值,分别在 3 种不同数据集进行实验,并且网络规模从 200m×200m 到 600m×600m 变化时,查询阶段的平均通信消耗。SWSKY 算法同样利用 F_{tuple} 进行元组过滤,在 3 种数据集下 SWSKY 查询算法都要明显优于 SkySensor 算法。

结束语　Skyline 查询在无线传感器网络中的应用日趋增多,减少能量的消耗依然是无线传感器网络的一个研究重点。本文提出的 SWSKY 算法在聚簇结构的基础上对过滤策略进行改进,在过滤时选取了支配力最强的过滤元组,它能有效地减少无效数据元组的传输,从而节省 WSN 能量,延长 WSN 的生命周期。

参 考 文 献

[1] 颜振亚,郑宝玉. 无线传感器网络[M]. 北京:清华大学出版社,2005.

[2] XIAO Y Y,CHEN Y G. Efficient distributed skyline queries for mobile applications[J]. Journal of Computer Science and Technology,2010,25(3):523-536.

[3] WANG H X,ZHENG J P,SONG B L. Skyline Query Processing in Wireless Sensor Networks[J]. Journal of Computer Science,2013,40(8):14-23. (in Chinese)
王海翔,郑吉平,宋保利. 无线传感器网络中的 Skyline 查询处理技术[J]. 计算机科学,2013,40(8):14-23.

[4] HOSE K,VLACHOU A. A survey of skyline processing in highly distributed environments[J]. Vldb Journal,2012,21(3):359-384.

[5] VLACHOU A,DOULKERIDIS C,KOTIDIS Y,et al. SKYPEER: Efficient Subspace Skyline Computation over Distributed Data[C]// 2014 IEEE 30th International Conference on Data Engineering. IEEE,2007:416-425.

[6] WU P,ZHANG C,FENG Y,et al. Parallelizing Skyline Queries for Scalable Distribution[C]// International Conference on Advances in Database Technology-edbt. 2006:112-130.

[7] WANG S,VU Q H,OOI B C,et al. Skyframe:A framework for skyline query processing in peer-to-peer systems[J]. Vldb Journal,2009,18(1):345-362.

[8] BALKE W T,GÜNTZER U,ZHENG J X. Efficient Distributed Skylining for Web Information Systems[J]. Lecture Notes in Computer Science,2004,2992:256-273.

[9] HUANG Z,JENSEN C S,LU H,et al. Skyline queries against mobile lightweight devices in MANETs[C]// International Conference on Data Engineering. 2006:66.

[10] CHEN H,ZHOU S,GUAN J. Towards Energy-Efficient Skyline Monitoring in Wireless Sensor Networks[C]// Wireless Sensor Networks,European Conference(Ewsn 2007). Delft,the Netherlands,2007:101-116.

[11] KWON Y,CHOI J H,CHUNG Y D,et al. In-Network Processing for Skyline Queries in Sensor Networks [J]. Ieice Transactions on Communications,2007,90(12):3452-3459.

[12] TAO Y,PAPADIAS D. Maintaining sliding window skylines on data streams[J]. IEEE Transactions on Knowledge & Data Engineering,2006,18(3):377-391.

[13] XIN J,WANG G,CHEN L,et al. Continuously Maintaining Sliding Window Skylines in a Sensor Network[C]// International Conference on Database Systems for Advanced Applications (DASFAA 2007). Bangkok,Thailand,2007:509-521.

[14] XIN J C,WANG G R. Continuous Skyline Nodes Query Processing over Wireless Sensor Networks[C]// NDBL 2012. 2012:2415-2430. (in Chinese)
信俊昌,王国仁. 无线传感器网络中 Skyline 节点连续查询算法[C]// 中国数据库学术会议. 2012:2415-2430.

[15] LI H,YOO J. An efficient scheme for continuous skyline query processing over dynamic data set[C]// International Conference on Big Data and Smart Computing. 2014:54-59.

[16] SU I F,CHUNG Y C,LEE C,et al. Efficient skyline query processing in wireless sensor networks[J]. Journal of Parallel & Distributed Computing,2010,70(6):680-698.

[17] KARP B,KUNG H T. GPSR:greedy perimeter stateless routing for wireless networks[C]// International Conference on Mobile Computing and Networking. ACM,2000:243-254.

(上接第 149 页)

[6] SUN B,QU L J,LI C. Impossible Differential Cryptanalysis of SNAKE[C]// Procof NSWCT'09. 2009:63-66.

[7] TOZ D,DUNKELMAN O. Analysis of two Attacks on Reduced-Round Versions of the SMS4[M]// Information and Communications Security. Springer Berlin Heidelberg, 2008: 141-156.

[8] WANG G L. Improved Impossible Differential Cryptanalysis on SMS4[C]// International Conference on Communications and Intelligence Information Security. IEEE,2010:105-108.

[9] LIU Y,GU D,LIN Z,et al. Impossible differential attacks on reduced-round Lblock [C]// ISPEC 2012. 2012:97-108.

[10] LIU X. The design and implementation of the lightweIght block ciper ESF[D]. Shandong: Shandong Normal University, 2014. (in Chinese)
刘宣. 轻量级分组密码 ESF 的设计与实现[D]. 山东:山东师范大学,2014.

[11] LIU X,LIU F,MENG S. Impossible differential cryptanalysis of lightweight block ciper ESF [J]. Computer and Engineering Science,2013,35(9):89-95. (in Chinese)
刘宣,刘枫,孟帅. 轻量级分组密码算法 ESF 的不可能差分析[J]. 计算机工程与科学,2013,35(9):89-95.

[12] CHEN Y L,WEI H R. Impossible Differential Cryptanalysis of ESF[J]. Computer Science,2016,43(8):89-91. (in Chinese)
陈玉磊,卫宏儒. ESF 算法的不可能差分密码分析[J]. 计算机科学,2016,43(8):89-91.

[13] XU P. Differential Fault Analysis on lightweight block ciper ESF[J]. Network Security Technology & Application, 2016(1):99-100. (in Chinese)
徐朋. 轻量级分组密码 ESF 的差分故障攻击[J]. 网络安全技术与应用,2016(1):99-100.