第 48 卷第 5 期
2016 年 10 月

南 京 航 空 航 天 大 学 学 报
Journal of Nanjing University of Aeronautics & Astronautics

Vol. 48 No. 5
Oct. 2016

DOI:10.16356/j.1005-2615.2016.05.008

基于新加密结构和 Sponge 结构的轻量级 Hash 函数 CHF

黄玉划[1,2]　代学俊[1]　陈帮春[1]　苏　菲[2]　刘宁钟[1]　曾庆喜[3]

(1.南京航空航天大学计算机科学与技术学院,南京,211106;2.苏州中科启慧软件技术有限公司,苏州,215500;
3.南京航空航天大学能源与动力学院,南京,210016)

摘要:针对能耗等资源受限环境对密码算法的需求,基于 Sponge 迭代结构,采用基于新加密结构(命名为 MS 结构)的 CLEFIA-128*(轻量级分组密码国际标准的修订算法)作为压缩函数,设计了一个轻量级 Hash 函数 CHF。效率测试和分析表明 CHF 算法的软件效率高于常见轻量级 Hash 函数,并兼顾了硬件效率,既能满足射频识别(Radio frequency identification, RFID)等资源极端受限环境对硬件的使用需求,也可以满足其他一些诸如嵌入式系统和单片机等环境对软件实现的需求,适用范围更广。依赖性测试和安全分析表明,该算法能够满足轻量级 Hash 函数的安全需求,也从侧面论证了 MS 结构的安全性。

关键词:轻量级 Hash 函数;Sponge 结构;CLEFIA 算法;依赖性测试;密码分析

中图分类号:TP309;TN918　　**文献标志码**:A　　**文章编号**:1005-2615(2016)05-0662-06

Lightweight Hash Function CHF Based on New Encryption and Sponge Structures

Huang Yuhua[1,2], *Dai Xuejun*[1], *Chen Bangchun*[1], *Su Fei*[2], *Liu Ningzhong*[1], *Zeng Qingxi*[3]

(1. College of Computer Science & Technology, Nanjing University of Aeronautics & Astronautics, Nanjing, 211106, China; 2. Suzhou Chinsdom Co. Ltd., Suzhou, 215500, China;
3. College of Energy and Power Engineering, Nanjing University of Aeronautics & Astronautics, Nanjing, 210016, China)

Abstract: To meet the application requirement for cipher algorithms in the resource-constrained terminal system such as the limited energy supply etc, a lightweight Hash function named CHF is designed. CHF adopts the Sponge structure as its iterative structure, and it uses the CLEFIA-128* as its compression function, which adopts a new encryption structure named MS. Test and analysis results show that the software efficiency of CHF is better than that of common lightweight hash functions, and its hardware efficiency is also taken into account. That is, the CHF algorithm fulfills the application requirements for hardware in the resource-constrained system such as radio frequency identification(RFID) and for software in embedded system & monolithic processor. Thus the CHF has wider application. The dependency test and security analysis results show that the CHF algorithm satisfies the security requirements of the lightweight Hash function. Thus the security of MS structure is proved from sideway.

Key words: lightweight Hash function; Sponge structure; CLEFIA algorithm; dependence test; crypt analysis

基金项目:国家自然科学基金(61375021)资助项目;江苏省科技支撑计划(BE2013879)资助项目;江苏省自然科学基金(SBK201322136)资助项目;南京航空航天大学青年科技创新基金(NS2010097)资助项目。

收稿日期:2016-01-01;**修订日期**:2016-08-30

通信作者:黄玉划,男,副教授,E-mail:hyuhua2k@163.com。

引用格式:黄玉划,代学俊,陈帮春,等. 基于新加密结构和 Sponge 结构的轻量级 Hash 函数 CHF[J]. 南京航空航天大学学报,2016,48(5):662-667. Huang Yuhua, Dai Xuejun, Chen Bangchun, et al. Lightweight Hash function CHF based on new encryption and Sponge structures[J]. Journal of Nanjing University of Aeronautics & Astronautics, 2016,48(5):662-667.

Hash 函数是密码学的重要分支，是一种将任意长度的输入消息压缩成固定长度输出摘要的函数，它在数字签名、身份认证与密钥交换、数据校验与消息认证及伪随机数生成等领域具有广泛的应用。随着无线通信与网络技术的发展，普通的 Hash 函数难以满足无线终端资源受限环境的应用需求，轻量级 Hash 函数的设计与分析成为当前的研究热点，比较有代表性的有 SQUASH，DM-PRESENT，H-PRESENT，Vortex，QUARK，PHOTON，SPONGENT，Lesamnta-LW，GLUON 和 ARMADILLO 等。其中，DM-PRESENT，H-PRESENT 和 SPONGENT 的压缩函数均采用轻量级分组密码国际标准 PRESENT[1-2]，只是结构不同。

SQUASH[3]是 Shamir 在 FSE 2008 上提出的轻量级 Hash 函数。它是针对射频识别（Radio frequency identification，RFID）标签等资源极端受限环境设计的，迭代结构采用的是 Rabin 结构，压缩函数采用的是非线性反馈移位寄存器（Nonlinear feedback shift register，NFSR）。这种设计使得该算法可以应用于任何资源极端受限的环境，因为它也可以根据处理器的倍数来调整算法的吞吐率，例如将算法从 8 位平台换到 32 位或者 64 位平台的话，它的速率将会大大地提高。

DM-PRESENT[4]和 H-PRESENT[5]是 Bogdanov 等在 CHES 2008 上提出的轻量级 Hash 函数。它们都采用轻量级分组密码 PRESENT 作为压缩函数，在迭代结构的选择上 DM-PRESENT 使用 DM 结构，而 H-PRESENT 使用 Hirose 结构。DM-PRESENT 的摘要长度为 64 bit，H-PRESENT 的摘要长度为 128 bit。在硬件实现时，DM-PRESENT 最少需要 1 600 个门电路（GE），而 H-PRESENT 最少需要 2 330 个 GE，都可用于 RFID 标签等环境。

Vortex[6]是 Gueron 和 Kounavis 在 ISC 2008 上提出的一种轻量级 Hash 函数。它可将任意长度的消息压缩成 256 bit 的消息摘要。在设计时采用 MD 结构，压缩函数采用类似高级加密标准（Advanced encryption standard，AES）的轮，在扩散层设计时通过使用有限域 GF(2)上的乘法实现，这种方式提高了扩散的速度。虽然只采用了 3 个 AES 型的轮，但是设计者通过增加压缩函数的密钥编排算法的强度来保证算法的安全。设计者声称该算法的安全性与 SHA-256 相当，同时速度是优于 SHA-256 的。

QUARK[7]是 Aumasson 等在 CHES 2010 上提出的一种轻量级的 Hash 函数。它设计时采用 Sponge 结构[8]，压缩函数的设计基于轻量级密码 Grain 和 KANTAN。它分为 U-QUARK，D-QUARK 和 T-QUARK，并且都有着不错的效率。最小的 U-QUARK 提供 2^{64} 的安全强度，硬件实现能控制在 1 379 个 GE。最大的 T-QUARK 能提供 2^{112} 的安全强度，也仅需要 2 296 个 GE 就可实现。

PHOTON[9]是 Guo 等在 CRYPTO 2011 上提出的一种轻量级 Hash 函数。它设计时采用 Sponge 结构，压缩函数采用 AES 型的设计。一般来说，AES 并不适合于资源极端受限环境，但是设计者采用一种序列化的方法，巧妙地降低了算法实现时对 GE 数的需求。在提供 2^{64} 安全强度的情况下，该算法最少可用 1 120 GE 实现。

SPONGENT[10]是 Bogdanov 等在 CHES 2011 上提出的一种轻量级 Hash 函数。它设计时迭代结构采用 Sponge 结构，压缩函数采用轻量级分组密码 PRESENT。这种设计能够大大提高硬件的实现效率。该算法能提供 88，128，160，224 和 256 五种不同的摘要长度，它们的硬件实现的 GE 数分别为 738，1 060，1 329，1 728 和 1 950。该算法是一种硬件实现效率非常优秀的轻量级 Hash 函数，具有很好的前景。

GLUON[11]是 Berger 等在 AFRICACRYPT 2012 上提出的一种轻量级 Hash 函数。它在设计时采用 Sponge 结构，并以两个流密码为基础设计压缩函数。设计者声称它的最小版本能用 2 071 个 GE 实现，且能达到 2^{64} 的安全强度。它是个相当有竞争力的轻量级 Hash 函数，而且引入流密码的设计理念也是它的一大特色。

ARMADILLO[12]是由 Badel 等在 CHES 2010 上提出的一种专门面向硬件设计的迭代的轻量级 Hash 函数。它在设计时采用了数据依赖置换技术，该技术因为在 RC6 和 MARS 设计时的应用而受到重视，由于具体过程中采用的更易硬件实现的移位操作，所以硬件实现效率很高，最小的硬件实现能达到 2 923 个 GE。

Wu 等设计了一个轻量级 Hash 函数 LHash[13]，硬件实现需要 989～1 200 个 GE，符合超轻量级密码的硬件需求，性能较好。

总体而言，现有轻量级 Hash 函数一般是面向硬件的，没有兼顾软件效率，难以满足嵌入式系统和单片机等环境对软件实现的需求。目前轻量级

Hash 函数尚未制定相应的国际标准。本文设计了一种综合性能较好的轻量级 Hash 函数。

1 轻量级 Hash 函数 CHF 设计

为了满足资源受限环境的应用需求，基于目前比较流行的 Sponge 迭代结构，采用轻量级分组密码国际标准 CLEFIA-128 的变形算法 CLEFIA-128* 作为压缩函数，设计了一个轻量级 Hash 函数 CHF。

1.1 符号注释

$GF(m^n)=\{0,\cdots,m-1\}^n$ 表示 n 位 m 进制有限域；

$A\times B=\{<x,\ y>|x(A,\ y\in B\}$ 表示集合 A 与 B 的笛卡积；

$A\rightarrow B$ 表示集合 A 到 B 的映射；

$x\ |\rightarrow\ y$ 表示元素 x 映射到 y；

$x_{(n)}$ 表示长度为 n-bit 的 x；

GE 表示门电路；

$a\leftarrow b$ 表示用 b 的值更新 a 的值；

$a\oplus b$ 表示按位异或运算；

$a|b\ =\ (a,b)$ 表示连接运算；

$X[a\sim b]$ 表示 X 的第 a 到 b 比特；

$x<<<i$ 表示 x 循环左移 i 位；

$x>>>j$ 表示 x 循环右移 j 位。

1.2 CHF 算法参数设计与迭代结构

CHF 算法设计了 3 种版本，对应的消息摘要长度分别为 72，88 和 128 bit。具体设计时，统一取内部状态宽度 $b=128$ bit；吞吐率 $r=8$ bit；容量 $c=120$ bit，即提供 2^{120} 的抗原像攻击能力；迭代轮数 $R=18$ 轮。

CHF 算法的迭代结构采用目前比较流行的 Sponge 迭代结构[8]，如图 1 所示。

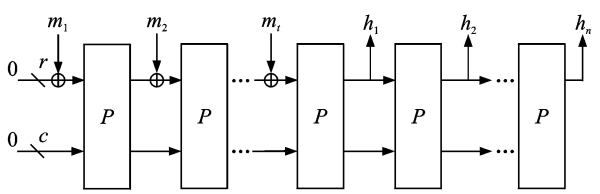

图 1 Sponge 结构

Fig. 1 Sponge structure

Sponge 结构采用简单的迭代设计，通过一个固定 b 比特长度的内部状态和一个置换函数 P 将不定长度的消息压缩成任意长度的消息摘要。它的内部状态 $b=r+c\geqslant n$ 为宽度，r 为吞吐率，c 为容量，n 为消息摘要的长度。Sponge 结构因为没有前向反馈，硬件实现时所需的 GE 数更少，更加符合轻量级 Hash 函数的设计要求。

1.3 CHF 算法的压缩函数——变形算法 CLEFIA-128* 介绍

测试和分析表明，轻量级分组密码国际标准 CLEFIA-128 算法[14]存在以下可改进空间[15]：首先它需要 5 轮才能基本实现伪随机性，扩散效果并不明显；其次它每一轮使用两个轮函数的设计降低了算法的软硬件实现效率。因此，可从加密结构和轮函数两个方面对其进行改进。

(1)修改加密结构

变形算法 CLEFIA-128* 的加密结构如图 2 所示(结合 Mars 和 SMS4，命名为 MS 结构)，将原来的加密结构更改为每一轮用 3 个分支去更新另外一个分支，然后再用更新结果去更新另外两个分支，迭代的轮数不变，即 $r=18$。整个加密过程中共用到了 r 个 32 bit 的轮密钥(RK_0，RK_1，RK_2，…，RK_{r-1})和 2 个 32 bit 的白化子密钥(WK_0，WK_1)。详细过程可参阅文献[15]。

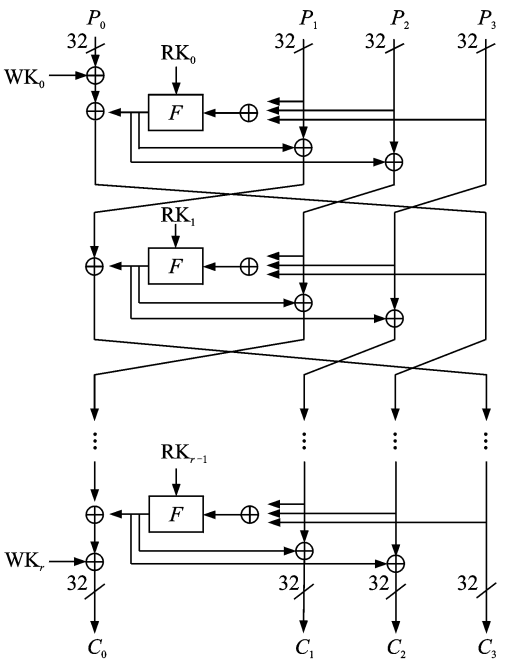

图 2 CLEFIA-128* 所采用的 MS 加密结构示意图

Fig. 2 MS structure in CLEFIA-128*

(2)修改轮函数

CLEFIA-128 使用了两个不同的轮函数 F_0，F_1，CLEFIA-128* 只使用一个轮函数 F，如图 3 所示。

CLEFIA-128 选用了两个不同的 S 盒 S_0，S_1，各使用两次。由于 Camellia 算法(欧洲第二代普通型分组密码标准)[16]采用的 S 盒适用于小硬件设

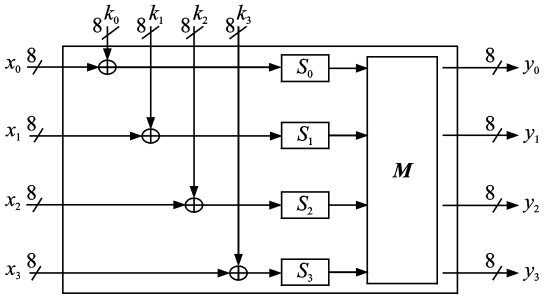

图 3　CLEFIA-128* 中轮函数 F 示意图

Fig. 3　Round function F in CLEFIA-128*

计，CLEFIA-128* 轮函数 F 中混淆层的 4 个 S 盒采用 Camellia 中的 4 个 8 位 S 盒并行，扩散层矩阵 $\boldsymbol{M}$ 仍然使用 CLEFIA-128 中的 Hadamard 矩阵，选择 CLEFIA-128 中 $\boldsymbol{M}_0$ 或 $\boldsymbol{M}_1$ 均可。

Camellia/ CLEFIA-128* 算法轮函数 F 的 4 个 S 盒可参阅文献[16]。

2　CHF 算法效率分析与测试

(1)硬件实现效率

依据文献[17]所讲述的硬件实现效率的评估方法来计算 CHF 系列算法的硬件实现效率。CHF 算法的硬件实现大约需要 2 240.96 GE，可以较好地应用到 RFID 等环境。为了进一步降低所需的 GE 数，可以采用 S 盒序列化的方法，只需约 1 640.96 GE就可实现 CHF 算法。这样做的缺点就是吞吐率将减小，算法的执行时间延长，在实际应用时可根据具体需求来决定采用何种实现方式。

文献[6]总结了当前一些轻量级 Hash 函数的硬件实现效率，如表 1 所示。

表 1　一些轻量级 Hash 函数的硬件实现效率

Tab. 1　Hardware efficiency of some Hash functions

算法	GE 数	算法	GE 数
SQUASH	2 646	SPONGENT-88	738
DM-PRESENT-80	1 600/2 213	SPONGENT-128	1 060
DM-PRESENT-128	1 886/2 530	SPONGENT-160	1 329
H-PRESENT-128	2 330/4 256	SPONGENT-224	1 728
C-PRESENT-192	4 600/8 048	SPONGENT-256	1 950
PHOTON-80	865/ 1168	GLUON-64	2 071
PHOTON-128	1 122/1 708	GLUON-80	2 799
PHOTN-160	1 396/2 117	GLUON-112	4 724
U-QUARK	1 379/2 392	Lesamnta-LW	8 240
D-QUARK	1 702/2 819	ARMADILLO	2 923
S-QUARK	2 296/4 640		

(2)软件实现效率

在 Intel (R) Core (TM) i5-2520 M 2.5 GHz Windows 7 64-bit 平台下用 C 语言编程对 CHF 算法进行了实现，并将它们与典型轻量级 Hash 函数 SPONGENT-88 算法的软件实现效率进行对比，如表 2 所示，CHF 的软件效率是 SPONGENT 的 4 倍。

表 2　CHF 系列算法和 SPONGENT 的软件实现效率对比

Tab. 2　Software efficiency of CHF and SPONGENT

算法	速度/(Kb·s^{-1})	
	128 bit	512 bit
CHF-72	815.29	2.97
CHF-88	688.67	2.70
CHF-128	461.60	1.81
SPONGENT-88	170.31	0.68

(3) 效率分析比较

CHF 算法的硬件实现能达到 2 000 GE 以下的数量级，与 SQUASH，H-PRESENT 和 GLUON 等算法相当，虽尚不及 SPONGENT 和 PHOTON，但明显优于 C-PRESENT 和 Lesamnta-LW。通常来讲，2 000 GE 可作为衡量一个轻量级密码是否能够应用 RFID 环境的标准，文中设计的超轻量级的 U-CHF 完全能够达到这一标准。虽然典型轻量级 Hash 函数 SPONGENT 算法具有更佳的硬件实现，但是它采用了 PRESENT 类型的压缩函数设计，大量位操作使得它的软件实现效率不高，而 CHF 系列算法的压缩函数采用的是广义的 Feistel 结构，具有更高的软件实现效率，如表 2 所示。

总的来说，CHF 算法兼顾了软件和硬件实现，既能满足 RFID 等资源极端受限环境的硬件使用需求，也可以满足其他的一些诸如嵌入式、单片机等环境对软件实现的需求，适用范围更广。

3　CHF 算法安全性测试与分析

(1)依赖性测试

密码算法的依赖性包括算法的完备性、雪崩效应和严格雪崩准则等方面。一个密码算法具有良好的依赖性是指它满足完备度 $d_c=1$，雪崩效应度 $d_a\approx1$，严格雪崩效应度 $d_{sac}\approx1$。任取 100 000 个 128 bit 的样本对 CHF 算法的依赖性做测试，结果如表 3 所示。

可以看出，两种算法的输出改变的平均位数非常接近理想值 50%，即输入几乎每改变一位，就会引起输出一半的值的改变。因此，该算法的混淆和扩散效果好。

表3 CHF依赖性测试结果

Tab. 3 Dependency test of CHF

指标	CHF
完备度 d_c	1.000 000
雪崩效应度 d_a	0.999 997
严格雪崩准则度 d_{sa}	0.997 501
输出改变的位数	49～78
输出改变的平均位数	63.997 285
输出位改变的概率	0.499 549～0.500 378
输出位改变的平均概率	0.499 979

(2)抗碰撞、原像和第二原像分析

Bertoni等[18]论证了Sponge结构与随机预言机是不可区别的,并给出了该结构抗碰撞、原像及第二原像攻击的能力。抗碰撞攻击:$\min\{2^{n/2}, 2^{c/2}\}$;抗原像攻击:$\min\{2^n, 2^c, \max\{2^{n-r}, 2^{c/2}\}\}$;抗第二原像攻击:$\min\{2^n, 2^{c/2}\}$。

文献[15]证明了压缩函数CLEFIA-128*的安全性,因此,CHF-72,CHF-88和CHF-128抗碰撞攻击的能力分别为2^{36},2^{44}和2^{60},抗原像攻击的能力分别为2^{64},2^{80}和2^{120},抗第二原像攻击的能力均为2^{60}。

(3)差分和线性分析

CLEFIA-128算法在设计轮函数的混淆层时选用了两个不同的S盒S_0,S_1,各使用两次,其中S_0的最大差分概率$DP_{max}^{S_0}=2^{-4.67}$,最大线性概率$LP_{max}^{S_0}=2^{-4.38}$,相比之下S_1具有更低的最大差分和线性概率,安全性更高。CHF算法采用的4个8位的S盒都满足$DP_{max}^{S_i}=LP_{max}^{S_i}=2^{-6}$,$0\leqslant i<4$,安全性都比$S_0$更高,与$S_1$相当。差分和线性分析表明CHF算法每一轮的最大差分和线性活动S盒的个数如表4所示。

表4 CHF算法的活动S盒情况

Tab. 4 Active S-box of CHF

轮	差分S盒	线性S盒	轮	差分S盒	线性S盒
1	0	0	10	27	36
2	3	4	11	30	40
3	6	8	12	33	44
4	9	12	13	36	48
5	12	16	14	39	52
6	15	20	15	42	56
7	18	24	16	45	60
8	21	28	17	48	64
9	24	32	18	51	68

9轮压缩函数的最大差分概率为$DCP_{max}^{9r}\leqslant 2^{24\times(-6)}=2^{-144}<2^{-128}$,7轮压缩函数的最大线性概率为$LCP_{max}^{7r}\leqslant 2^{24\times(-6)}=2^{-144}<2^{-128}$,由此可见,18轮的设计是足以抵抗差分和线性分析的。

(4)不可能差分分析

运用矩阵的方法对CHF算法的压缩函数CLEFIA-128*进行不可能差分分析[19],只能攻击到第4轮,可以找到如下的6条不可能差分路径:

$$(\alpha,0,0,0)\overset{4r}{\nrightarrow}(\alpha,0,0,0)\quad p=1;$$

$$(0,0,\alpha,0)\overset{4r}{\nrightarrow}(0,0,\alpha,0)\quad p=1;$$

$$(0,0,\alpha,0)\overset{4r}{\nrightarrow}(\alpha,0,\alpha,0)\quad p=1;$$

$$(\alpha,\alpha,0,0)\overset{4r}{\nrightarrow}(\alpha,0,0,0)\quad p=1;$$

$$(\alpha,0,\alpha,0)\overset{4r}{\nrightarrow}(\alpha,0,0,0)\quad p=1;$$

$$(\alpha,0,0,\alpha)\overset{4r}{\nrightarrow}(\alpha,0,0,0)\quad p=1。$$

其中,$\alpha(GF(2^{32}))$表示非零的差分。因此,CHF系列算法是能够抵抗不可能差分分析的。

4 结束语

为了满足能耗等资源受限环境的应用需求,本文基于Sponge迭代结构,采用CLEFIA-128*算法作为压缩函数,设计了一个轻量级Hash函数CHF。其硬件实现能达到2 000GE以下的数量级。与典型轻量级Hash函数SPONGENT相比,CHF算法具有更好的软件实现效率;其硬件实现效率与现有轻量级Hash函数也可比,可以说它兼顾了软硬件实现效率,适用范围更广。最后,对CHF算法作了依赖性测试和安全性分析,它具有良好的混淆和扩散效果,并能抵抗现有的攻击。实际上,CLEFIA-128*与CLEFIA-128总体迭代加密结构并不相同,只是轮函数结构相同,轮函数采用的S盒也不相同。之所以采用已有的轮函数结构和S盒,是为了方便同行感知和验证CLEFIA-128*所采用的迭代加密结构MS及CHF算法的安全性,而Camellia算法为CLEFIA-128*和CHF算法提供了4个现成的S盒。实际上,4个S盒可自行设计,通过伪随机方式产生或通过不可约多项式产生。

参考文献:

[1] ISO/IEC 29192-2. Information technology - security techniques - lightweight cryptography - Part 2: Block ciphers[S]. Switzerland: ISO/IEC, 2012.

[2] Bogdanov A, Knezevic M, Leander G, et al. SPONGENT: The design space of lightweight cryptographic hashing[J]. IEEE Transactions on Computers,

2013，62(10)：2041-2053.

[3] Shamir A. SQUASH—A new MAC with provable security properties for highly constrained device such as RFID Tags[C]// FSE 2008，LNCS 5086. Berlin Heidelberg：Springer-Verlag，2008：144-157.

[4] Koyama T，Sasaki Y，Kunihiro N. Multi-differential cryptanalysis on reduced DM-PRESENT-80：Collisions and other differential properties[J]. Lecture Notes in Computer Science，2013，7839：352-367.

[5] Bogdanov A，Leander G，Paar C，et al. Hash functions and RFID tags：Mind the gap[C]// CHES 2008，LNCS 5154. Berlin Heidelberg：Springer-Verlag，2008：283-299.

[6] Gueron S，Kounavis M K. Vortex：A new family of one-way hash functions based on AES rounds and carry-less application[C]// ISC 2008，LNCS 5222. Berlin Heidelberg：Springer-Verlag，2008：331-340.

[7] Aumasson J P，Henzen L，Meier W，et al. QUARK：A lightweight Hash[J]. Journal of Cryptology，2013，26(2)：313-339.

[8] Bertoni G，Daemen J，Peeters M，et al. Sponge functions[C]// ENCRYPT Hash Workshop 2007. Berlin Heidelberg：Springer-Verlag，2007：1-22.

[9] Guo J，Peyrin T，Poschmann A. The PHOTON family of lightweight hash functions[C]// CRYPTO 2011，LNCS 6841. Berlin Heidelberg：Springer-Verlag，2011：222-239.

[10] Bogdanov A，Leander G，Toz D，et al. SPONGENT：A lightweight hash function[C]// CHES 2011，LNCS 6917. Berlin Heidelberg：Springer-Verlag，2011：312-325.

[11] Berger T P，Hayer J D，Marquet K，et al. The GLUON family：A lightweight Hash function family based on FCSRs[C]// AFRICACRYPT 2012，LNCS 7374. Berlin Heidelberg：Springer-Verlag，2012：306-323.

[12] Badel S，Dagtekin N，Jr JN，et al. ARMADILLO：A multi-purpose cryptographic primitive dedicated to hardware[C]// CHES 2010，LNCS 6225. Berlin Heidelberg：Springer-Verlag，2010：398-412.

[13] Wu Wenling，Wu Shuang，Zhang Lei，et al. LHash：A lightweight hash function[J]. Lecture Notes in Computer Science，2014，8567：291-308.

[14] Shirai T，Shibutani K，Akishita T，et al. The 128-bit blockcipher CLEFIA(Extended abstract)[C]// FSE 2007，LNCS 4593. Berlin Heidelberg：Springer-Verlag，2007：181-195.

[15] 陈帮春. 物联网终端系统安全机制研究与设计[D]. 南京：南京航空航天大学，2014.
Chen Bangchun. Research and design of terminal system security mechanism in IoT[D]. Nanjing：Nanjing University of Aeronautics and Astronautics，2014.

[16] Aoki K，Ichikawa T，Kanda M，et al. Specification of Camellia—A 128-bit block cipher[EB/OL]. https：// www. cosic. esat. kuleuven. ac. be/nessie/workshop/submissions/Camellia. zip，2016-10-12.

[17] Axel Y P B. Lightweight cryptography：Cryptographic engineering for a pervasive world [D]. Bochum：Ruhr-University Bochum，2009.

[18] Bertoni G，Daemen J，Peeters M，et al. On the indifferentiability of the Sponge construction[C]// EUROCRYPT 2008，LNCS 4965. Berlin Heidelberg：Springer-Verlag，2008：181-197.

[19] Azimi S A，Ahmadian Z，Mohajeri J，et al. Impossible differential cryptanalysis of Piccolo lightweight block cipher[C]// 11th International Conference on Information Security and Cryptology. Berlin Heidelberg：Springer-Verlag，2014：89-94.