



1

密码算法介绍

密码性能分析

4

总结

背景





01 PART 01

第一部分

研究背景

思科IBSG的最新白皮书估计,到2020年,将有500亿个设 备连接到互联网,这意味着在不远的将来,每个人都将被 数十种传感器设备所包围, 从互联网到物联网的这种演进 将对我们的日常生活产生巨大影响,并改变我们与周围的 物理世界的交互方式。 然而,显而易见的是,连接到 Internet的500亿智能设备给其所有者或用户的安全和隐私 带来了前所未有的挑战。众所周知,对称密码系统在物联 网的安全领域中扮演着重要角色, 但是物联网硬件设备的 计算和存储资源十分有限,这就需要对密码体系进行更加 细致有效的设计,保证在物联网设备中有限的资源上能够 稳定运行。

在本篇报告中,我们选取了3种在IoT设备中性能表现优异并且安全性较高的密码方案,即Chaskey、Simon和Speck,来进行简单的分析和介绍。



U REE



密码算法介绍——Chaskey



Chaskey主要用于克服现有密码算 法在微控制器上难以实现的问题。 它是基于排列的MAC算法



Chaskey算法中使用的密钥K长度 为128比特



Chaskey算法将消息M分成大小相 等的128比特的块进行置换π



Chaskey 的 置 换 采 用 Addition-Rotation-XOR设计方式



Chaskey的功能特点

Chaskey是用于32位微控制器体系结构的专用设计。加法和异或操作都是对于32bit的字为单位执行的,并且它们在32位的体系结构下都只需要通过一条指令就可以实现。

01 02 专用 设计 高效 抗计 实现 时攻 击 03

我们考虑到某些微控制器没有支持可变长度的位旋转和位平移。所以我们通过选择一些8的倍数作为旋转常数,使得这些操作可以通过寄存器上的8位或16位交换(swap)操作有效实现。

算法运行在ARM Cortex-M4上试验,对于长消息(≥128字节),Chaskey 算法运行仅需要7.0 cycles/byte,而 对于短消息(16字节)也仅需要10.6 cycles/byte,并且只占用了402bytes 的ROM。

在所有的微控制器架构上, Chaskey的每条指令的执行时间都 是固定的。且执行的时钟周期数 仅取决于消息的长度。因此, Chaskey具有固有的抵御计时攻击 的安全性。

Chaskey算法流程

消息M分成大小为n比特的块。然后我们以每n比特为单位对消息进行置换π的迭代,如下图所示。在最后一次的置换π的前后都使用了相同的子密钥进行异或操作,这使得子密钥可以一直保留在寄存器当中,减少装载(load)和存储(store)操作的次数。

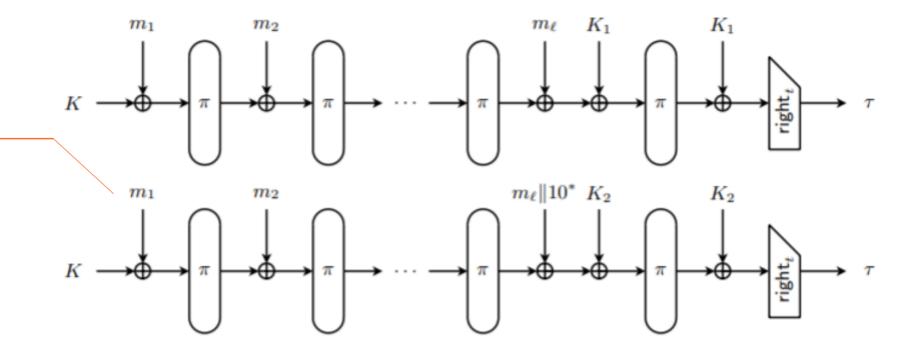
Chaskey使用n比特长度的密钥K为任意大小的消息M生成一个标签T,并且标签T的长度t小于等于n。我们通过算法1和2为密钥K生成两个子密钥K1和K2。

Algorithm 1 TimesTwo

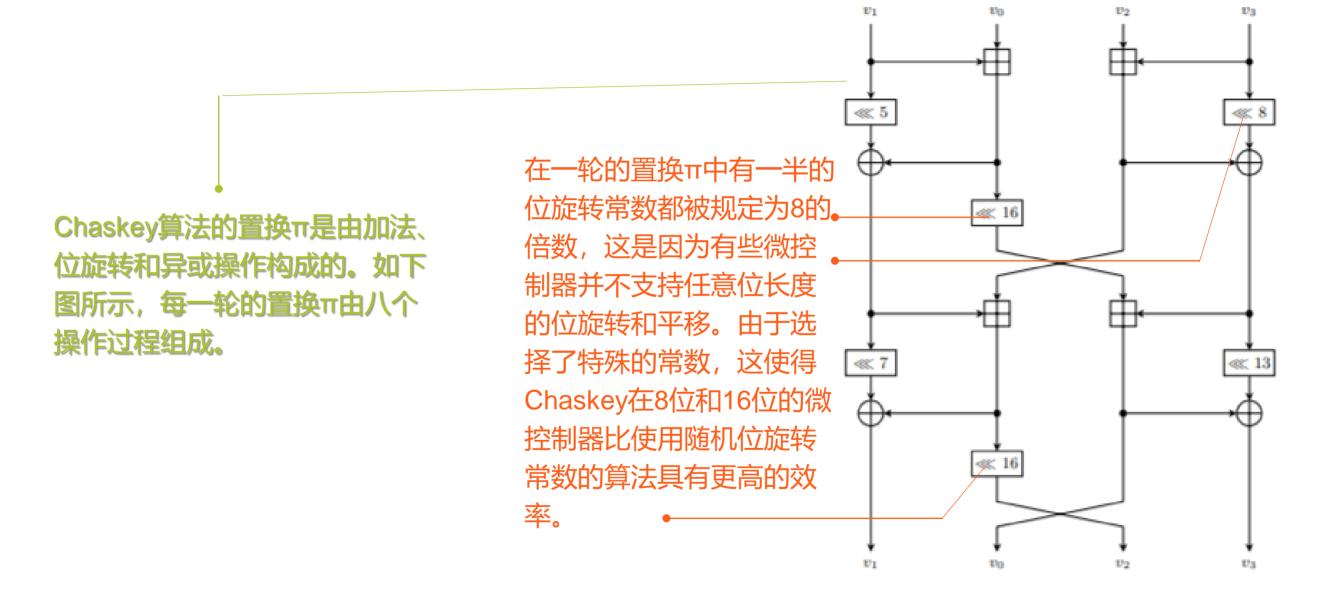
- 1: **procedure** TimesTwo(a)
- 2: **if** a[127] = 0 **then**
- 3: return $(a \ll 1) \oplus 0^{128}$
- 4: **else**
- 5: **return** $(a \ll 1) \oplus 0^{120}10000111$

Algorithm 2 SubKeys

- 1: **procedure** SubKeys(K)
- 2: $K_1 \leftarrow \text{TimesTwo}(K)$
- 3: $K_2 \leftarrow \text{TimesTwo}(K_1)$
- 4: **return** (K_1, K_2)



Chaskey算法流程



密码算法介绍——Simon & Speck



Simon和Speck密码是一种轻量级的分组密码,由美国国家安全局在2013年发布,主要为了实现平台的通用性



与其他轻量级分组密码算法不同, Simon和 Speck提供了多种分组长度以及每种分组可对 应的密钥长度来实现灵活性



Simon和Speck没有使用S盒,它采用的是 Feistel结构,可以在线性扩散和非线性混淆的 操作之间很好的平衡。



在扩散过程中,为了让密文中的每一位受明文中尽可能多的位影响,需要采用位置换。 Simon和Speck算法通过旋转来实现位置换, 在软件和硬件都达到良好的效果。





Simon对于软件进行优化, Speck 对硬件进行优化

Simon & Speck算法流程

Simon算法的轮函数为:

 $(x,y)\mapsto (y\oplus f(x)\oplus k,x)$

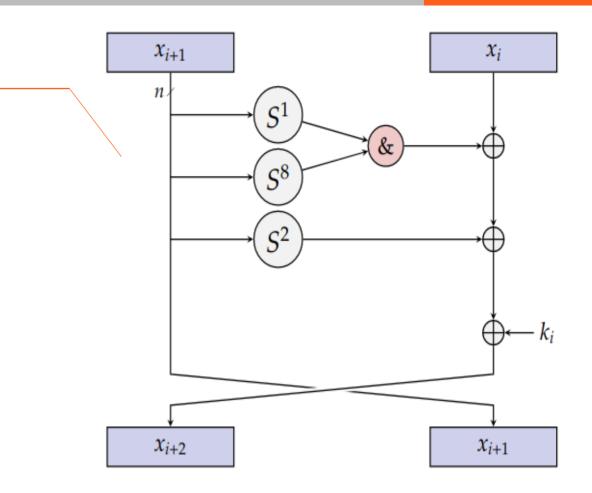
其中

 $f(x)=(Sx\& S^8 x)\oplus S^2 x$

S为左循环移位,上标表示移位的位数。

轮函数如右图所示。

根据密钥大小与块大小之间的倍数,可将所有情况分为三类: (块大小/密钥长度) 2倍 (96/96, 128/128), 3倍 (48/72, 64/96, 96/144, 128/192), 4倍 (32/64, 48/96, 64/128, 128/256)。这三类情况下, 轮密钥的产生公式如右图。其中, C、D、E都为常数, I是一个特殊的n×n矩阵, 维度等于块大小。

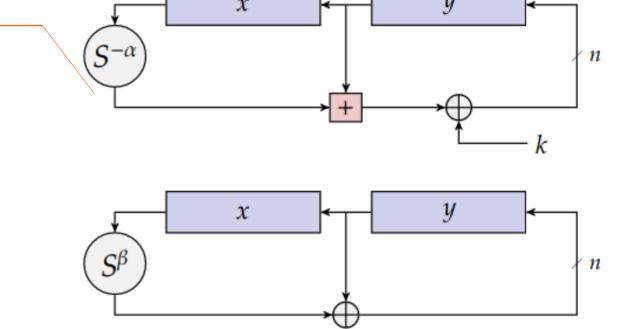


$$\begin{split} k_{i+2} &= k_i \oplus (I \oplus S^{-1}) S^{-3} k_{i+1} \oplus C_i \\ k_{i+3} &= k_i \oplus (I \oplus S^{-1}) S^{-3} k_{i+2} \oplus D_i \\ k_{i+4} &= k_i \oplus (I \oplus S^{-1}) (S^{-3} k_{i+3} \oplus k_{i+1}) \oplus E_i \end{split}$$

Simon & Speck算法流程

Speck算法的轮函数为:

 $(x,y)\mapsto ((S^{-\alpha} x+y)\oplus k, S^{-\beta} y\oplus (S^{-\alpha} x+y)\oplus k)$ 其中x和y的映射过程可以看做两个Feistel映射的组合,如右图所示。

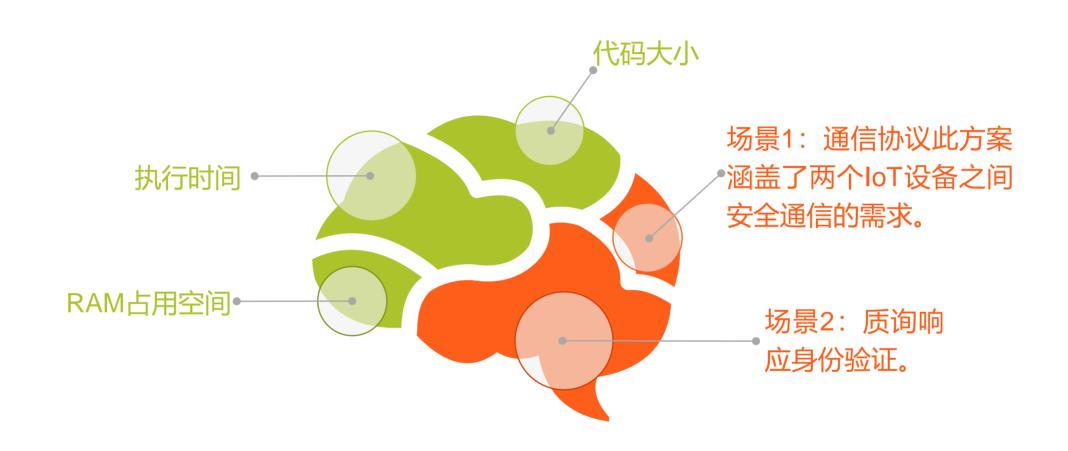


Speck算法的轮密钥生成函数是基于 轮函数得来的,公式如右图所示:

$$\begin{array}{ll} \ell_{i+m-1} &= (k_i + S^{-\alpha} \ell_i) \bigoplus i_{\leftarrow} \\ k_{i+1} &= S^{\beta} k_i \bigoplus \ell_{i+m-1} \end{array}$$



算法性能测试: 三个指标与两个场景



算法性能测试:实验数

Cipher

Chaskey

Speck

Speck

Chaskey-LTS

Table 2. Results for Scenario 1: Encryption and decryption of 128 bytes of data each platform, the results of the implementation with the best performance indishown. The Figure-of-Merit (FOM) is based on the performance indicators on a FOM value, the better the implementations of a cipher).

Block Key Code RAM

Simon

Simon

SPARX

SPARX

HIGHT

Robin

Robins

RC5-20

PRIDE

LBlock

RoadRunneR

RoadRunneR

PRESENT

PRINCE

TWINE

Piccolo

LED

Fantomas

AES

LEA

RECTANGLE

RECTANGLE

ъ

128 128

128

64

1084*

 1122^{*}

 1684°

1152*

1118*

1426*

1736*

3010*

1414*

5892

4944

5076

3706

3384

2504

2316

2954

 2160^{*}

5358

4236

1992

80 5156 574

3631

375

631'

352

353

 392°

753

408

333*

267

271

271

368

373

330

209

494

448°

374

646

314

LBlock

Piccolo

LED

TWINE

94557*

111677

146149

157205

252368

111155

144071

125635

183324

245232*

243396

297265

407269

2221555 7004

PRESENT

PRINCE

80

80

128

80

80

80

120215*

56788

76588

88804

386026

226135

235317

218909

263778

201549*

357423

387562

324221

2065695 3696

64

64

64

64

* Results for Assembly implementations

330*

234

238

238

378

380

338

362

324

450°

240

564

310

252

 1258^{*}

4164

3170

3312

1240

2918

3088

2952

1632

1838*

4174

3796

1354

1440

1294*

1362

1114

1528

2548

1444

4604

3572

3724

624

2240

2788

2504

2204

2528

4372

2456

1596

128

80

128

128

128

128

128

128

128

128

80

128

80

80

80

80

128

96

64 128

128

64

64128

64128

128

128

64

128

128

64

64

64

64

Table 1. Overview	of the 19	Speck	64	128	
key sizes are expres		Simon	64	96	
key setting to the to		Simon	64	128	
key seeming to the to	Juan Humin	RECTANGLE	64	80	
		RECTANGLE	64	128	
Cipher		LEA	128	128	
	Year	SPARX	64	128	
		SPARX	128	128	
AES	1998	HIGHT	64	128	1
Chaskey	2014	AES	128	128	
Fantomas	2014	Fantomas	128	128	
HIGHT	2006	Robin	128	128	
LBlock	2011	Robin*	128	128	
LEA	2013	RC5-20	64	128	
LED	2011	PRIDE	64	128	l
Piccolo	2011	RoadRunneR	64	80	
PRESENT	2007	RoadRunneR	64	128	
PRIDE	2014	LBlock	64	80	
PRINCE	2012	PRESENT	64	80	
$RC5^*$	1994	PRINCE	64	128	
RECTANGLE	2015	Piccolo	64	80	
RoadRunneR	2015	TWINE	64	80	
Robin/Robin*	2014	LED	64	80	
Simon	2013	* Results for Asse	ombler in	an los	
SPARX	2016	Results for Asse	emory in	ipiei	
Speck	2013	64 96/128 83	2/864	2	
TWINE	2011	64 80 1	1152		

^{*} We use RC5 with increased number of rounds, RC5-20.

Table 4. Results for Scenario 2: Encryption of 128 bits of data (pre-computed round keys). For each cipher and each platform, the results of the implementation with the best performance indicator according to Equation (II) are shown. The Figure-of-Merit (FOM) is based on the performance indicators on all three platforms (the smaller the

						FOM value, the be						mance n	idicator	on an	onrec pa	iciornis (c	ic sinai	ici tiic	
1: Encryption and decryption of 128 bytes of data the implementation with the best performance indi-			Cimbon			AVR			MSP			ARM			<u> </u>				
OM) is based on the performance indicators on :			Block	Key	Code	RAM	Time	Code	RAM	Time	Code	RAM '	l'ime	FOM					
ole	ementations of a ci	pner).					[b]	[b]	[B]	[B]	[cyc.]	[B]	[B]	[cyc.]	[B]	[B]	cyc.]		
	AVR			MSP		Chaskey	128	128	624*	80*	1465*	388*	70*	1153*	216*		524*	4.4	
	<u> </u>	—				Chaskey-LTS	128	128	624*	80*	2265*	390*	70*	1690*	216*	76*	648*	5.0	
y	Code RAM	Time	Code	RAM	Tim	Speck	64	96	506*	53*	2647*	328*	48*	1959*	256		1003	5.1	
_l l		leve l	[R]	[R]	leve	Speck	64	128	452*	53*	2917*	332*	48*	2013*	276	60	972	5.2	
Table 3. Results for Scenario 1: Encryption ar				Simon	64	96	600*	57*	4269*	460*	56*	2905*	416		1335	7.0			
each platform, the results of the implementation			Simon	64	128	608*	57*	4445*	468*	56*	3015*	388	64	1453	7.2				
shown, whereby different weights were assigne			LEA	128	128	906*	80*	4023*	722*	78*	2814*	520°	112*	1171*	8.0				
have a weight of 1, while the execution time h			time h	RECTANGLE	64	128	602*	Table	e 5. Resi	ults for S	Scenario	2: Encr	vntion o	f 128 bits	of data	(pre-co	m		
	important than t	he other	two n	etrics.	The F	RECTANGLE	64	80	606*	Table 5. Results for Scenario 2: Encryption of 128 bits of data (pre-ceach platform, the results of the implementation with the best performance)									
three platforms (the smaller the FOM value, t				due, t	SPARX	64	128	662*	shown, whereby different weights were assigned to the three metrics. Bot										
(SPARX	128	128	1184*			-							
•	Cipher			ı	AV	RC5-20	64	128	1068		have a weight of 2, while the execution time has a weight of 1, which more important than the execution time. The Figure-of-Merit (FOM								
5	Cipilei				AV	AES	128	128	1246*	three platforms (the smaller the FOM value, the better the imp									
į		Block	Key	Code	RAM	HIGHT	64	128	636*		pinerorin	. (diac, ui	a product th	e impre		
į		[b]	[b]	[B]	[B]	Fantomas	128	128	2496	Cip	hon			1	AV	D	1	MSF	,
į	cu i					Robin	128	128	2530	Cip	ner				AV	K.		MSF	_
į	Chaskey Chaskey-LTS	128 128	128 128	1328* 1328*	229° 229°	Robin* RoadRunneR	128 64	128 80	2580 1420			Ble	ock Ke	y Cod	e RAM	Time	Code	RAM	
į	Speck	64	96	966*	294	PRIDE	64	128	2064				[Ы] П	ы в	[B]	[cyc.]	[B]	[B]	
2	Speck	64	128	1112*	302	RoadRunneR	64	128	1184	CIL									-
2	Open	0.1	120	1112	002	reconstitution	OT	120	1101	Cha	skey		128 - 12	8 624	* 80*	1465°	388*	70*	

mputed round keys). For each cipher and ce indicator according to Equation (1) are th the memory consumption and code size eans the former two metrics are considered based on the performance indicators on all ions of a cipher).

Cipher			AVR				MSP					
	Block	Key	Code	RAM	Time	Code	RAM	Time	Code	RAM	Time	FON
	[b]	[b]	[B]	[B]	cyc.	[B]	[B]	[cyc.]	[B]	[B]	[cyc.]	
Chaskey	128	128	624*	80*	1465*	388*	70°	1153*	184*	76*	568*	7.
Speck	64	96	448*	53*	2829*	328*	48*	1959*	256	56	1003	7.
Speck	64	128	452*	53*	2917*	332*	48*	2013*	264	56	1029	7.
Chaskey-LTS	128	128	624*	80*	2265*	390*	70*	1690*	216*	76*	648*	7.
Simon	64	96	534*	57*	4521*	460*	56°	2905*	416	64	1335	9.
Simon	64	128	542*	57*	4709*	468*	56*	3015*	388	64	1453	10.
RECTANGLE	64	128	602*	56*	4381*	480*	54*	2651*	444*	76*	2365*	11.
RECTANGLE	64	80	606*	56*	4433*	480*	54*	2651*	444*	76*	2365*	11.
LEA	128	128	906*	80*	4023*	722*	78*	2814*	520*	112*	1171*	12.
SPARX	64	128	662*	51*	4397*	580*	52*	2261*	654*	72*	2338*	12
RC5-20	64	128	1068	63	8812	532	60	15925	372	64	1919	18.
SPARX	128	128	1184*	74*	5478*	904*	80*	3273*	932*	108*	4085*	19
HIGHT	64	128	636*	56*	6231*	636*	52*	7117*	670*	100*	5532*	19
AES	128	128	1246*	81*	3408*	1170*	80*	4497*	1348*	124*	4044*	21
Fantomas	128	128	1712	76	9689	1412	74	5506	1412	104	6484	27
Robin	128	128	1712	78	12499	1406	72	7051	1424	116	7686	30
PRIDE	64	128	958	60	11222	1842	68	13108	1592	148	7446	33
RoadRunneR	64	128	1184	59	6289	756	58	18067	1436	164	8573	33
RoadRunneR	64	80	1420	61	7329	1536	76	13034	1900	172	7234	33
Robin*	128	128	1754	80	14285	1980	80	5262	1472	116	9186	34
LBlock	64	80	1440	64	11183	804	58	16101	616	80	11818	34
PRESENT	64	80	1294*	56*	16849*	1072*	58*	12347*	1222*	80*	17105*	44.
Piccolo	64	80	1114	72	25820	784	70	20081	688	112	17965	48
PRINCE	64	128	1362	72	20060	1578	70	24375	1200	132	16270	51.
TWINE	64	80	1528	64	21701	1922	136	23662	1180	156	15673	52
LED	64	80	2602	91	143317	4422	104	121850	2172	352	35891	164

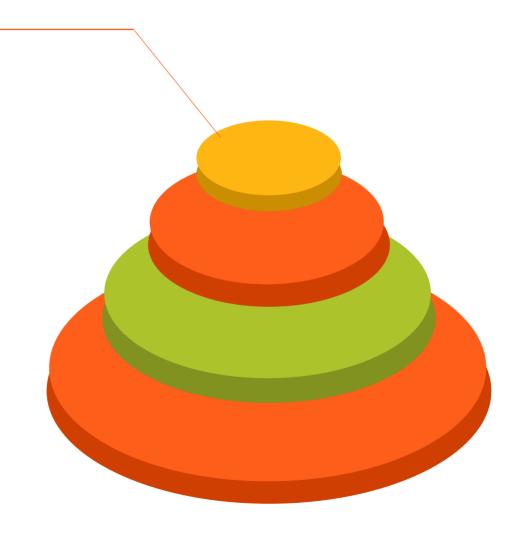
Results for Assembly implementations.

Chaskey	128	128	624*	80*	1465*	388*	70°	1153*	216*	76*	524*	4.4			
Chaskey-LTS	128	128	624*	80*	2265*	390*	70*	1690*	216*	76*	648*	5.0			
Speck	64	96	506*	53*	2647*	328*	48*	1959*	256	56	1003	5.1			
Speck	64	128	452*	53*	2917*	332*	48*	2013*	276	60	972	5.2			
Simon	64	96	600*	57*	4269*	460*	56*	2905*	416	64	1335	7.0			
Simon	64	128	608*	57*	4445*	468*	56*	3015*	388	64	1453	7.2			
LEA	128	128	906*	80*	4023*	722*	78*	2814*	520°	112*	1171*	8.0			
RECTANGLE	64	128	602*	Tabl	o 5 Ross	alte for S	Consti	2: Encry	ntion of	128 bit	te of date	a (pro-co	m		
RECTANGLE	64	80	606*					he implem	-			4.0			
SPARX	64	128	662*												
TEN A TRAF	2.05.05	2.05.05		shown, whereby different weights were assigned to the three metrics. Bot											

^{*} Results for Assembly implementations.

算法性能测试: 实验结果

结果表明,最新的ARX和类似ARX的设 计不仅非常快,而且在RAM空间占用量 和代码大小方面也非常小。以执行时间、 RAM占用空间和代码大小为基础的铁人 三项比赛的总冠军是Chaskey,紧随其 后的是Speck。 两者在两种使用情景下 以及在所有三个平台上始终表现良好。 这使它们成为保护物联网安全的轻量级 密码的强大候选者。当执行时间,RAM 占用空间和代码大小权重一样时, Simon等密码方案的FOM值也低于10.0, 也获得了很好的结果。





04 PART 04

第四部分

总结

总结



通过对三种适用于IoT设备的分组密码Chaskey、Simon和Speck进行分析总结,对它们的设计构造方案和安全性能有了进一步的认识。





通过对它们的性能测试部分的分析,分别得出了在资源受限的IoT设备中,三种密码方案的运行性能情况和对比其他密码方案的优势。





在以后的学习和研究带来了一些启发,在设计密码方案的时候,要尽可能考虑在实际运行环境下兼顾安全性和运行性能。





谢谢观看!

Merry Xmas and Happy New Year!!!!

|高亨利 1901210713|刘存展 1901210442|胡兆杰 1901210403|