



مهندسی

دانشکده‌ی فنی و

گروه آموزشی مهندسی کامپیوتر و فناوری اطلاعات

پایان‌نامه برای دریافت درجه‌ی کارشناسی ارشد
در رشته‌ی مهندسی کامپیوتر گرایش معماری کامپیوتر

عنوان:

یک تابع درهم‌ساز کلیددار کارا مبتنی بر نظریه
آشوب

استاد راهنما:

دکتر شهرام جمالی

استاد مشاور:

دکتر رضا اسودی

پژوهشگر:

میثم عسگری چناقلو

تابستان 1394

<p>نام خانوادگی دانشجو: عسگری چناقلو نام: میثم</p>
<p>عنوان پایان نامه: یک تابع درهم ساز کلیددار کارا مبتنی بر نظریه آشوب</p>
<p>استاد راهنما: دکتر شهرام جمالی استاد مشاور: دکتر رضا اسودی</p>
<p>مقطع تحصیلی: کارشناسی ارشد رشته: مهندسی کامپیوتر گرایش: معماری کامپیوتر دانشگاه: محقق اردبیلی دانشکده: فنی و مهندسی تاریخ دفاع: تعداد صفحات: 106</p>
<p>94/06/31 چکیده:</p> <p>تابع درهم ساز یکی از ابزارهای مهم در رمزنگاری و تشخیص اصالت پیام محسوب می شود که فرم کلیددار این تابع برای MAC و فرم بدون کلید آن در MDC مورد استفاده قرار می گیرد. در طراحی اینگونه توابع، سرعت و امنیت پارامترهای مهمی برای کاربردهای مختلف رمزنگاری می باشند. توابع درهم ساز پرکاربرد در این زمینه MD5، SHA-0، SHA-1 و SHA-2 می باشند که به شکل های مختلف مورد حمله قرار گرفته اند. توابع یاد شده، با ساختار مرکب- دامگارد و با توابع درونی دودویی طراحی شده اند. یک روش دیگر برای طراحی چنین توابعی استفاده از نگاشت های آشوب می باشد. در این رساله، ابتدا یک سیستم آشوب با قابلیت فشرده سازی معرفی و با استفاده از آن یک تابع درهم ساز فازی طراحی گشته است. ساختار درهم سازی معرفی شده قابلیت پیاده سازی به صورت موازی را داشته و طول خروجی متغیری را دارا است. این تابع درهم ساز از یک کلید 256 بیتی بهره می برد که طول آن می تواند افزایش یابد. بررسی کارایی تابع درهم ساز پیشنهادی با استفاده از پارامترهای کارایی، تحلیل امنیتی و سرعت صورت گرفته است که از آن جمله می توان به بررسی حساسیت تابع درهم ساز به پیام ورودی و تغییر شرایط اولیه، بررسی آماری اغتشاش و انتشار و مقاومت در برابر برخورد یاد کرد. تابع درهم ساز طراحی شده به لحاظ پارامترهای کارایی بیان شده با برخی توابع درهم ساز مبتنی بر آشوب نیز مقایسه و بر اساس حملات عمومی صورت گرفته بر روی توابع درهم ساز مورد بحث و بررسی قرار گرفته است.</p> <p>کلید واژه ها: تابع درهم ساز، نظریه آشوب، حملات رمزنگاری، سیستم آشوب.</p>

فهرست مطالب

شماره و عنوان مطالب

صفحه

فصل اول: مقدمه

1-1-1	مقدمه	2
1-2-1	بیان مسئله	4
1-3-1	اهداف پژوهش	6
1-4-1	معیارهای ارزیابی	6
1-5-1	ساختار پایان‌نامه	6

فصل دوم: اصول نظری توابع درهم‌ساز

1-2-1	مقدمه	9
2-2-1	مروری بر توابع درهم‌ساز	9
2-2-2-1	توابع درهم‌ساز بدون کلید	11
2-2-2-2	توابع درهم‌ساز کلیددار	13
2-3-1	انواع توابع درهم‌ساز بر اساس راهکارهای مختلف	14
2-3-2-1	توابع درهم‌ساز مبتنی بر رمزنگارهای بلوکی	15
2-3-2-1-1	روش Davies-Meyer	16
2-3-2-2	روش Matyas-Meyer-Oseas	17
2-3-2-3	روش Miyaguchi-Preneel	17
2-3-2-4	روش MDC-2 و MDC-4	18
2-3-2-2	توابع درهم‌ساز مرسوم	18
2-3-2-1-2	ساختار مرکب-دامگارد	19
2-3-2-2-2	تابع درهم‌ساز MD5	19
2-3-2-3-2	تابع درهم‌ساز SHA-1	21
2-4-1	انواع حملات رمزنگاری بر روی توابع درهم‌ساز	24
2-4-1-1	حملات مستقل از الگوریتم درهم‌سازی	25
2-4-1-1-1	حمله تصادفی	25

- 26.....2-1-4-2 شبه حمله
- 26.....3-1-4-2 جستجوی نا آگاهانه کلید
- 27.....4-1-4-2 حمله روز تولد
- 27.....2-4-2 حملات وابسته به الگوریتم درهم سازی
- 28.....1-2-4-2 حمله MITM
- 28.....2-2-4-2 حمله MITM محدود
- 28.....3-2-4-2 حمله اصلاح بلوک
- 28.....4-2-4-2 حمله نقطه ثابت
- 29.....5-2-4-2 حمله دیفرانسیلی یا تفاضلی
- 29.....3-4-2 حملات وابسته به رمزنگار بلوکی
- 30.....4-4-2 حملات سطح بالا
- 30.....1-4-4-2 حمله بازپخش
- 30.....1-4-4-2 حمله قطعه بندی
- 30.....5-2-5-2 ضعف ساختاری مرکل-دامگارد
- 31.....1-5-2 حمله گسترش پیام
- 31.....2-5-2 حمله چندین-برخوردی جوکس
- 31.....3-5-2 حمله نقطه ثابت توسط Dean و نسخه توسعه یافته آن توسط
Schneier و Kesley
- 32.....4-5-2 حمله گله داری توسط کلسی و کوهنو
- 33.....5-5-2 حملات اخیر انجام شده بر روی توابع درهم ساز
- 35.....6-2-6 پارامترهای آماری کارایی توابع درهم ساز
- 37.....7-2-7 اعداد تصادفی و توابع تولید کننده آن
- 37.....1-7-2 اصول اولیه اعداد تصادفی
- 39.....2-7-2 آزمون اعداد تصادفی
- 40.....1-2-7-2 آزمون فراوانی
- 40.....2-2-7-2 آزمون تکرار متوالی
- 40.....3-2-7-2 آزمون طولانی ترین تکرار متوالی یکها
- 41.....4-2-7-2 آزمون رتبه ماتریس دودویی
- 41.....5-2-7-2 آزمون تبدیل فوریه گسسته
- 41.....6-2-7-2 آزمون الگوی غیر متداخل
- 41.....7-2-7-2 آزمون الگوی متداخل

42.....	2-7-2-8- آزمون آماری جهانی مائورر
42.....	2-7-2-9- آزمون پیچیدگی خطی
42.....	2-7-2-10- آزمون ردیفی
42.....	2-7-2-11- آزمون آنتروپی تقریبی
42.....	2-7-2-12- آزمون جمع تجمعی
43.....	2-7-2-13- آزمون گردش‌های تصادفی
43.....	2-7-2-14- جمع‌بندی آزمون‌های توابع PRNG و RNG
44.....	2-8- جمع‌بندی

فصل سوم: نظریه آشوب و توابع درهم‌ساز مبتنی بر آن

46.....	3-1- مقدمه
46.....	3-2- نظریه آشوب
47.....	3-2-1- رفتار پیچیده در نگاشتهای تک بعدی
49.....	3-2-2- نگاشت لجستیک
51.....	3-3- استفاده از نظریه آشوب در رمزنگاری
52.....	3-3-1- توابع درهم‌ساز مبتنی بر نگاشتهای ساده
52.....	3-3-1-1- الگوریتم درهم‌سازی چن و هوانگ
53.....	3-3-1-2- الگوریتم درهم‌سازی لیو و همکارانش
55.....	3-3-1-3- الگوریتم درهم‌سازی ژیاوو و همکارانش
56.....	3-3-2- توابع درهم‌ساز مبتنی بر شبکه عصبی آشوبناک
60.....	3-3-3- تابع درهم‌ساز کلیددار موازی مبتنی بر نظریه آشوب
64.....	3-4- جمع‌بندی

فصل چهارم: یک سیستم آشوب ترکیبی جدید با قابلیت فشرده‌سازی

66.....	4-1- مقدمه
66.....	4-2- سیستم‌های آشوب
68.....	4-2- سیستم آشوب معرفی شده با قابلیت فشرده‌سازی
70.....	4-3- بررسی رفتار آشوب سیستم DCS

4-4- جمع‌بندی 73

فصل پنجم: الگوریتم درهم‌سازی فازی مبتنی بر سیستم آشوبناک

DCS

- 5-1- مقدمه 75
- 5-2- تابع درهم‌ساز پیشنهادی 75
- 5-2-1- ساختار کلی تابع درهم‌ساز پیشنهادی 75
- 5-2-2- فرم‌دهی و قطعه‌بندی پیام ورودی 77
- 5-2-3- توزیع بلوک‌های پیام 77
- 5-2-4- توابع درونی F_i 78
- 5-2-5- تابع جهش ژنتیکی کلید یا mutate 80
- 5-2-6- تابع SortBlocks و آرایه دینامیک توابع F_i 81
- 5-2-7- تابع HSum 81
- 5-2-8- روابط فازی weak و strong 82
- 5-3- اندازه خروجی متغیر 83
- 5-4- جمع‌بندی الگوریتم پیشنهادی 83

فصل ششم: نتایج به‌دست آمده

- 6-1- مقدمه 85
- 6-2- تحلیل آماری سیستم DCS 85
- 6-2-1- نتایج مجموعه آزمون‌های اعداد تصادفی بر روی DCS 85
- 6-2-2- مزایای سیستم DCS 85
- 6-3- تحلیل تابع درهم‌ساز پیشنهادی 87
- 6-3-1- تحلیل آماری 87
- 6-3-1-1- خروجی درهم‌سازی شده 87
- 6-3-1-2- خروجی درهم‌سازی شده برای مجموعه‌هایی از رشته‌ها 88
- 6-3-2- تحلیل امنیتی 91
- 6-3-2-1- تحلیل امنیتی کلید با جستجوی ناآگاهانه کلید 92
- 6-3-2-2- حمله تصادفی 92

93	6-3-2-3- تحلیل حمله روز تولد.....
93	6-3-2-4- تحلیل حمله نقطه ثابت.....
93	6-3-2-5- حمله MITM و نسخه محدود شده آن.....
93	6-3-2-6- حمله دیفرانسیلی یا تفاضلی.....
94	6-4- سرعت پردازش.....
95	6-5- انعطاف پذیری.....
96	6-6- ملاحظات پیاده‌سازی امن.....
96	6-7- مقایسه ساختار پیشنهادی با مرکز دامگارد و ساختار اسفنجی.....
97	6-8- مقایسه با سایر توابع درهم‌ساز مبتنی بر آشوب و مرسوم

فصل هفتم: نتیجه‌گیری و بحث

100	7-1- نتیجه‌گیری.....
100	7-2- پیشنهادات.....
102	منابع و مآخذ.....

فهرست جدول‌ها

شماره و عنوان جدول

صفحه

جدول 2-1: توابع غیرخطی درونی الگوریتم درهم‌سازی MD5	21
جدول 2-2: توابع غیرخطی درونی الگوریتم درهم‌سازی SHA-1	23
جدول 2-3: برخورد برای تابع درهم‌ساز MD4	34
جدول 2-4: برخورد برای تابع درهم‌ساز MD5	35
جدول 3-1: نگاشت مقادیر X_i به مقادیر دودویی	53
جدول 5-1: 32 بیت اول مجذور اعداد اول 2 تا 19	77
جدول 5-2: توابع Z_i	79
جدول 6-1: نتایج بدست آمده از آزمون NIST برای 10^6 سری تولید شده 100 بیتی	86
جدول 6-2: پیام‌های 1 تا 6	88
جدول 6-3: خروجی درهم‌سازی شده پیام‌های 1 تا 6	88
جدول 6-4: نتایج آماری برای خروجی‌های درهم‌سازی شده 256، 512، 1024 و 2048 تایی تصادفی	89
جدول 6-5: نتایج آماری برای خروجی‌های درهم‌سازی شده 256، 512، 1024 و 2048 تایی از متن انگلیسی	89
جدول 6-6: بهبود کارایی ایجاد شده توسط اجرای چندنخی نسبت به اجرای عادی	95
جدول 6-7: مقایسه الگوریتم پیشنهادی نسبت به سایر روش‌ها	98

فهرست شکل‌ها

شماره و عنوان شکل	صفحه
شکل 2-1: برخورد در توابع درهم‌ساز	10
شکل 2-2: تشخیص خطا به وسیله تابع درهم‌ساز	12
شکل 2-3: ساختار کلی توابع درهم‌ساز مبتنی بر رمزنگارهای بلوکی	16
شکل 2-4: روش Davies-Meyer	17
شکل 2-5: روش Matyas-Meyer-Oseas	17
شکل 2-6: روش Miyaguchi-Preneel	18
شکل 2-7: ساختار مرکب-دامگارد	19
شکل 2-8: دیاگرام تابع درهم‌ساز MD5	21
شکل 2-9: دیاگرام تابع درهم‌ساز SHA-1	23
شکل 2-10: نقطه ثابت برای یک تابع فشرده‌ساز	29
شکل 3-1: نمودار دوشاخه نگاشت لجستیک	50
شکل 3-2: روند کار تابع درهم‌ساز مبتنی بر شبکه عصبی آشوبناک	57
شکل 3-3: شبکه عصبی آشوبناک	58
شکل 3-4: تابع درهم‌ساز موازی مبتنی بر SEN	60
شکل 3-5: شبکه SEN مربوط به فاز پیش‌پردازش	62
شکل 3-6: نگاشت آشوب PWNLCM	62
شکل 3-7: تابع ترکیب‌کننده	64
شکل 4-1: ساختار سیستم آشوب ترکیبی LS	67
شکل 4-2: نمودار دو شاخه سیستم آشوب ترکیبی LS	67
شکل 4-3: هیستوگرام نمودار دوشاخه سیستم آشوب ترکیبی LS	68
شکل 4-4: دو سری تولید شده به وسیله DCS و با کمترین اختلاف	70
شکل 4-5: نمودار دوشاخه سیستم DCS : ماتریس DM_1	71
شکل 4-6: نمودار دوشاخه سیستم DCS : ماتریس DM_6	71
شکل 4-7: نمودار دوشاخه بزرگنمایی شده سیستم DCS	72
شکل 4-8: هیستوگرام مربوط به نمودار دوشاخه DCS	72

- شکل 5-1: الگوریتم درهم‌سازی پیشنهادی 76
- شکل 5-2: فلوچارت توابع F_i 80
- شکل 5-3: روابط قوی و ضعیف برقرار شده بین F_3 و توابع F_2 و F_4 83
- شکل 6-1: هیستوگرام کاراکترهای خروجی توزیع شده برای 35000 پیام درهم‌سازی شده از متن انگلیسی 89
- شکل 6-2: هیستوگرام خروجی B_i مربوط به 1000 فایل 185 KB با اختلاف یک بیت نسبت به فایل اصلی 90
- شکل 6-3: برخوردهای خروجی درهم‌سازی شده در فرمت ASCII مربوط به 1000 فایل 185 KB با اختلاف یک بیت نسبت به فایل اصلی... 91
- شکل 6-4: خروجی در حالت 512 بیتی 91
- شکل 6-5: هیستوگرام کاراکترهای خروجی توزیع شده برای 1000 پیام یکسان درهم‌سازی شده با اختلاف کلید یک بیت 92
- شکل 6-6: سرعت اجرای تابع درهم‌ساز پیشنهادی در دو حالت عادی و چند نخه 94

فهرست علائم اختصاری

مفهوم	علامت اختصاری
پیام ورودی	M
کلید	K
خروجی درهم‌سازی	H
تابع درهم‌ساز بدون کلید	$h(M)$
تابع درهم‌ساز کلید دار	$h_k(M)$
ورودی نگاشت آشوب در زمان n	X_n
نگاشت لجستیک	$L(r, X_n)$
نگاشت سینوسی	$Sine(r, X_n)$
سیستم یا نگاشت لجستیک-سینوسی	LS
سیستم آشوبناک دینامیک	DCS
شیفت به چپ چرخشی به اندازه N بیت	\lll_N
OR منطقی	\vee
AND منطقی	\wedge
جمع در پیمانی اعشاری و بازگرداندن حاصل جمع به همان پیمانه	\boxplus
XOR منطقی	\oplus
کاهش به پیمانه یا محاسبه باقیمانده	mod
محاسبه بخش اعشاری عدد	mod 1
تابع مولد اعداد تصادفی	RNG
تابع مولد اعداد شبه تصادفی	PRNG

فصل اول :

مقدمه

1-1- مقدمه

عدم ارتباط بین اطلاعات و رسانه انتقال آن، به بزرگترین مزیت اطلاعات دیجیتال بدل گشته است، به طوری که می‌توان نسخه‌های مختلفی از اطلاعات را بدون از بین رفتن کیفیت آن به سهولت به دست آورد. این اطلاعات را می‌توان بر روی دیسک سخت، گوشی همراه ذخیره و یا حتی بر روی یک شبکه Wi-Fi، Ethernet، GSM و یا ارتباط ماهواره‌ای ارسال و دریافت کرد.

این امر به نوبه خود می‌تواند نفوذپذیری بزرگی را فراهم آورد، به شکلی که دیگر نمی‌توان فقط با استناد به رسانه فیزیکی، صحت اطلاعات را تصدیق¹ نمود. جهت تصدیق این اطلاعات، رمزنگارها² نیازمند تسامح بر روی یک کلید می‌باشند. با در نظر داشتن خیل عظیمی از گروه‌ها که نیازمند برقراری ارتباط با یکدیگر هستند، برقراری و ذخیره گذرواژه برای تمامی ارتباطات ممکن بین گروه‌ها، پرهزینه خواهد بود (Stevens, 2012).

از این رو، در ارتباطات امن به شیوه مدرن امروزی، امضای دیجیتال³، MAC⁴ و MDC⁵ از اهمیت بسیاری برخوردار گشته‌اند و ارتباطات مدرن نیازمند برقراری چنین ساختاری برای حفظ اصالت پیام⁶، تائید هویت فرستنده⁷ و عدم انکار از سوی فرستنده⁸ می‌باشند.

توابع درهم‌ساز در امضای دیجیتال، MAC، MDC، جدول کلیدواژه، تشخیص ویروس⁹، PRF¹⁰ و PRNG¹¹ کارکردهای فراوانی دارند. این توابع در بسیاری از پروتکل‌های بی-سیم همچون WAP¹² نیز به طور گسترده‌ای استفاده شده‌اند (Mironov, 2005).

این توابع یک اثرانگشت از پیام ایجاد می‌کنند که در صورت هرگونه تغییر پیام با استفاده از آن می‌توان تغییر در پیام دریافتی را تشخیص داد. این توابع در یک تعریف اجمالی، یک ورودی با اندازه دلخواه را دریافت کرده و یک خروجی با اندازه معلوم تولید می‌کنند. توابع درهم‌ساز

¹ Authentication

² Ciphers

³ Digital signature

⁴ Message Authentication Code

⁵ Manipulation Detection Code

⁶ Integrity of a message

⁷ Validating identity of originator

⁸ Non-repudiation of origin (dispute resolution)

⁹ Intrusion detection, Virus detection

¹⁰ Pseudorandom function

¹¹ Pseudorandom number generator

¹² Wireless Application Protocol

به صورت کلیددار برای MAC و به صورت بدون کلید برای MDC مورد استفاده قرار می‌گیرند.

بر اساس نظریه اغتشاش و انتشار¹، تغییر یک کاراکتر در ورودی یک سیستم رمزنگار باید تغییر بزرگی در خروجی رمزنگار ایجاد کند (انتشار) و هم چنین ارتباط بین کلید و خروجی رمزنگار، باید یک ارتباط پیچیده و توأم باشد (اغتشاش) (Shannon, 1949).

همان‌طور که بیان شد، یک تابع درهم‌ساز باید خصوصیت اغتشاش و انتشار را دارا باشد. این خصوصیت برای یک تابع درهم‌ساز با سه خاصیت زیر به‌طور عمومی بیان می‌شود:

1- خاصیت یکطرفه بودن یا مقاوم در برابر پیش تصویر اول (preimage resistance)

2- مقاوم در برابر پیش تصویر دوم (Second preimage resistance)

3- مقاوم در برابر برخورد (Collision resistance) (Stallings, 1999)

راهکارهای مختلفی برای طراحی این توابع ارائه شده است که می‌توان این توابع را بر اساس راهکار طراحی آنها دسته‌بندی کرد. اکثر توابع درهم‌ساز طراحی شده از عملگرهای منطقی با تکرارهای متوالی استفاده می‌کنند که به این توابع درهم‌ساز، توابع درهم‌ساز مرسوم گفته می‌شود.

توابع درهم‌ساز مرسوم مانند MD5 و SHA مورد حملات مختلفی نیز قرار گرفته‌اند که (De Cannière & Rechberger, 2008)؛ Wang & Yu, 2005؛ Oechslin, 2003؛ Sasaki & Aoki, 2009؛ Boer & Bosselaers, 1994؛ Khovratovich & et al, 2012؛ Chabaud & Joux, 1998؛ De Cannière & et al, 2007؛ Biryukov؛ Biham & Chen, 2004؛ Nikolić & Biryukov, 2008؛ Sanadhya & Sarkar, 2008 (& et al, 2011) نمونه‌ای از حملات انجام‌شده بر روی آنها می‌باشند.

به جز توابع مرسوم نامبرده شده، راهبردهای مختلفی در زمینه طراحی توابع درهم‌ساز مورد تحقیق و بررسی قرار گرفته‌اند. یکی از این راهبردها استفاده از نظریه آشوب² در این زمینه می‌باشد. نگاشتهای آشوب³ با توجه به خصوصیت‌های حساسیت به مقادیر اولیه ورودی، ارگودیسیتی⁴ و اغتشاش و انتشار، در زمینه رمزنگاری و بخصوص توابع درهم‌ساز کاربردهای فراوانی دارند (Amin & et al, 2009). توابع درهم‌ساز طراحی‌شده با استفاده از این نگاشتهای، در مقابل برخورد می‌توانند مقاوم باشند. تابع درهم‌ساز آشوب طراحی شده در (Kanso & et al, 2012) که اندازه خروجی درهم‌سازی شده

¹ Confusion and diffusion

² Chaos Theory

³ Chaotic-maps

⁴ Ergodicity

متغیری دارد و در مقابل حمله روز تولد¹ مقاومتر می-باشد.

یک سیستم مبتنی بر نظریه آشوب از نقطه نظر ریاضی سامانه ای دینامیک می باشد که رفتار آن در یک بازه قابل پیش بینی بوده و رفتار آن در خارج از بازه ی مزبور غیرقابل پیش بینی است و یا اینکه به صورت اتفاقی و قابل تشخیص با خطای غیرقابل چشم پوشی می باشد. سیستم آشوب را می توان به صورت بی نظمی در نظر گرفت که به لحاظ ریاضی این سه اصل را دارا باشد:

1- حساس به شرایط اولیه باشد

2- خاصیت مرکب بودن به لحاظ توپولوژیکی را دارا

باشد²

3- چرخش های دوره ای چگال داشته باشد³ (Kellert, 1993)

یک تابع درهم ساز مبتنی بر آشوب، از یک سیستم یا نگاشت مبتنی بر آشوب و یک الگوریتم درهم سازی تشکیل شده است. با استفاده از سیستم آشوب، با یک ورودی به عنوان کلید، یک توالی از بیت ها به دست می آید که خاصیت آشوب را دارا هستند. با استفاده از توالی به دست آمده و ترکیب آن با ورودی با اندازه نامعلوم، می توان خروجی را به اندازه معلوم فشرده کرد. نکته اساسی در چنین توابع درهم ساز، خاصیت حساسیت به مقادیر اولیه سیستم آشوب و همچنین نحوه استفاده از آن در ایجاد حساسیت به مقادیر ورودی در خروجی تابع درهم ساز می باشد (Kocarev & Lian, 2011).

طراحی یک تابع درهم ساز مبتنی بر آشوب به لحاظ امنیتی نسبت به توابعی مانند MD5، SHA-0، SHA-1 و SHA-2 می تواند بهبودهای امنیتی بسیاری را از جهت حساسیت به مقادیر ورودی و هم چنین اغتشاش و انتشار به دست دهد. بهینه سازی روی چنین توابعی می تواند آن ها را به لحاظ سرعت پردازش نسبت به سایر توابع درهم ساز مبتنی بر آشوب بهبود بخشد. همچنین این توابع می توانند به صورت کلیددار و بدون کلید برای استفاده در کاربردهای MAC و MDC طراحی شوند.

1-2- بیان مسئله

طراحی توابع درهم ساز یک مسئله ی باز در زمینه رمزنگاری می باشد. زیرا توابع طراحی شده به مرور مورد حمله قرار خواهند گرفت و علت این امر در رشد سرعت پردازش رایانه ها و روش های حملات رمزنگاری می باشد. از این حیث، علاوه بر اهمیت موضوع در حیطة امنیت اطلاعات و

¹ Birthday attack

2- Topologically mixing

3- Dense periodic orbits

توسعه حملات صورت گرفته، نیاز به یک تابع درهم‌ساز کارا و سریع احساس می‌شود.

ضعف امنیتی یک تابع درهم‌ساز می‌تواند خطرات زیادی را در تصدیق پیام ایجاد کند و تغییر آن را توسط یک عامل سوم مانند هکر، ویروس و یا حتی خطای ایجادشده در مسیر انتقال پیام ممکن سازد.

امنیت توابع درهم‌ساز به لحاظ کارکردهای مختلف و متنوع آن به شکلی که توصیف شد، از اهمیت بسیار بالایی در دنیای ارتباطات دیجیتال امروزی برخوردار است. امنیت این توابع با حملاتی همچون حمله تصادفی، شبه حمله، جستجوی ناآگاهانه کلید، حمله روز تولد، حمله MITM، حمله اصلاح بلوک، حمله نقطه ثابت، حمله تفاضلی، حمله بازپخش و حمله قطعه بندی به بوتله آزمایش گزارده شده و موفقیت‌هایی در حملات نیز کسب‌شده است که در (De Cannière & Oechslin, 2008 ; Sasaki & Aoki, 2009 ; den Boer & Bosselaers, 1994 ; Rechberger, 2008 ; Chabaud & Joux, 1998 ; De Cannière & et al, 2007 ; Wang & Yu, 2005 ; 2003 ; Nikolić & Biryukov, 2008 ; Sanadhya & Sarkar, 2008 ; Khovratovich & et al, 2012 ; Biham & Chen, 2004 ; Biryukov & et al, 2011) به برخی از این حملات بر روی توابع درهم‌ساز MD5، SHA-0، SHA-1 و SHA-2 اشاره شده است.

سرعت نیز پارامتر مهمی در طراحی این توابع می‌باشد، به شکلی که سهولت پردازش به‌عنوان یکی از اصول اولیه توابع درهم‌ساز است (Menezes & et al, 1996).

در مورد توابع رمزنگاری، از طرفی افزایش سرعت، خود باعث کاهش امنیت می‌شود. علت این امر در افزایش روز به روز سرعت پردازش رایانه‌ها و در به‌کارگیری حملات مختلف است که همگی به پیچیدگی زمانی تابع درهم‌ساز وابسته هستند.

توابع درهم‌ساز با استفاده از نظریه آشوب در (Amin & et al, 2009 ; Kwok & Tang, 2003 ; Wong, 2003 ; Kanso & et al, 2012 ; al, 2009 ; Xiao & et al, 2005 ; Yi, 2005 ; Wang & et al, 2008 ; Wang & Hu, 2007 ; Xiao & et al, 2005 ; 2008 ; Zhang & et al, 2007 ; Xiao & et al, 2009 ; Deng & et al, 2006 ; Xiao & et al, 2009 ; Akhshan & et al, 2009 ; Akhavan & et al, 2009 ; Kanso & Ghebleh, 2013) طراحی‌شده‌اند و به لحاظ آنالیز کارایی در زمینه‌هایی مانند خروجی مقدار درهم‌سازی شده تابع، آنالیز انتشار و اغتشاش، حمله روز تولد، حمله MITM و آنالیز سرعت و انعطاف‌پذیری مورد بررسی قرار گرفته‌اند.

توابعی که مبتنی بر نظریه آشوب طراحی می‌شوند، به لحاظ امنیت، از بعد نگاشت آشوب و خاصیت آشوب‌گونه خروجی آن، نسبت به توابع مرسوم برتری نسبی دارند. اما نکته بسیار مهم، انتخاب یک نگاشت آشوب مناسب برای عملیات رمزنگاری مورد نظر و استفاده از آن با یک الگوریتم درهم‌سازی مناسب و ایمن می‌باشد.

در این پژوهش، در صدد هستیم تا پاسخ مناسبی برای سوال‌های زیر پیدا کنیم.

- کدامیک از نگاشته‌های آشوب و یا ترکیب آن‌ها برای ایجاد یک تابع درهم‌ساز مبتنی بر آشوب مناسب است؟

- چگونه می‌توان تابع درهم‌ساز مبتنی بر آشوب را مطابق با پارامترهای ارزیابی طراحی کرد؟

- تابع درهم‌ساز مبتنی بر آشوب چه برتری‌های امنیتی نسبت به توابع درهم‌ساز مرسوم MD5، SHA-0 و SHA-1 خواهد داشت؟

1-3- اهداف پژوهش

هدف از این پایان‌نامه طراحی یک تابع درهم‌ساز مبتنی بر نظریه آشوب است که بتواند پارامترهای ارزیابی موجود در این زمینه را برآورده کند. از این رو، انتظار می‌رود که با استفاده از ترکیب یک یا چند نگاشت آشوب بتوان یک سیستم جدید آشوبناک به دست آورد و همچنین تابع درهم‌ساز ارائه شده که مبتنی بر این سیستم می‌باشد، بتواند خصوصیتی مانند کلیددار و بدون کلید بودن و پشتیبانی از طول خروجی متغیر را فراهم کند. افزون بر این، تابع ارائه شده باید مشکلات موجود در ساختار درهم‌سازی مرکل-دامگارد را مرتفع و پارامترهای ارزیابی را ارضا کند.

1-4- معیارهای ارزیابی

ارزیابی کارایی یک تابع درهم‌ساز به سه دسته اصلی آماری، سرعت و امنیت دسته بندی می‌شود که به لحاظ آماری، تحلیل اغتشاش و انتشار مهم‌ترین عامل می‌باشد. این عامل با پارامترهایی مانند تعداد بیت‌های تغییر یافته B_i با تغییر یک بیت از پیام، میانگین احتمال تغییر P ، میانگین بیت‌های تغییر یافته \bar{B} ، انحراف معیار بیت-های تغییر یافته در اجراهای مختلف ΔB و همچنین انحراف معیار احتمال تغییر بیت‌ها ΔP اندازه‌گیری می‌شود.

ارزیابی سرعت با استفاده از محاسبه مدت زمان لازم برای پردازش ورودی‌های مختلف بیان می‌شود و تحلیل رمزنگاری شامل موارد تحلیل حمله روز تولد، تحلیل حمله

MITM، مقایسه با ساختار مرکز-دامگارد و ساختار اسفنجی و تحلیل انعطاف پذیری می‌باشد.

1-5- ساختار پایان‌نامه

ساختار ادامه این پایان‌نامه به این شکل است که در فصل دوم، به بررسی اصول اولیه توابع درهم‌ساز، RNG و PRNG پرداخته می‌شود و هم چنین نحوه ارزیابی و پارامترهای ارزیابی بیان می‌گردد. در فصل سوم، کارهای مرتبط در این زمینه بررسی می‌شود. فصل چهارم و پنجم به معرفی سیستم آشوب و تابع درهم‌ساز جدید پرداخته می‌شود. فصل ششم نتایج حاصل از ارزیابی الگوریتم پیشنهادی را بیان می‌کند و در نهایت، در فصل هفتم به نتیجه‌گیری و ارائه پیشنهادات برای ادامه کار پرداخته می‌شود.

Family name: Asgari Chenaghlu	Name: Meysam
Title of Thesis : An Efficient Chaos-Based Keyed Hash Function	
Supervisor: Shahram Jamali	
Advisor: Reza Asvadi	
Graduate Degree M.Sc.	
Major: Computer Architecture	Specialty: Computer Engineering
University: Mohaghegh Ardabili	Faculty: Technical Engineering
Graduation date: 2015/07/22	Number of pages: 106
<p>Abstract:</p> <p>Hash function as one of primitive tools of cryptography and message authentication, is used in keyed and unkeyed forms for MDC and MAC. Hashing speed and security are the most important qualities of these functions for various cryptographic applications. Commonly used hash functions in field of cryptography are MD5, SHA-0, SHA-1 and SHA-2 that has been attacked in different ways. These functions use Merkle-Damgard scheme with iterating over internal binary functions. Another way to design such functions is using chaos theory. In this document, first a chaotic system with compression ability is proposed and a fuzzy hashing scheme based on this system has been developed. Hashing structure of proposed scheme can be run on multi-threading. Use of 256 bits long key improves its security against generic attacks. Simulation results such as statistical analysis, speed analysis and cryptanalysis deductions, shows its good performance and reliability. Proposed function is compared to other chaotic hash functions by statistical parameters and is discussed in cryptanalysis matters.</p>	
Keywords: Hash function, Chaos theory, Cryptanalysis, Chaotic system	



Faculty of Technical Engineering
Department of Computer Engineering and Information Technology

Thesis submitted in partial fulfilment of the requirements for the degree of
M.Sc. in Computer Engineering

Title:

An Efficient Chaos-Based Keyed Hash Function

Supervisor:

Dr. Shahram Jamali (Ph. D)

Advisor:

Dr. Reza Asvadi (Ph. D)

By:

Meysam Asgari Chenaghlu

September – 2015