دانشکده‌ی فنی و مهندسی
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

نام خانوادگي دانشجو: عسگری چناقلو
نام: میثم

عنوان پایان‌نامه:
یک تابع درهم‌ساز کلیددار کارا مبتنی بر نظریه آشوب

استاد راهنما: دکتر شهرام جمالی
استاد مشاور: دکتر رضا اسودی

مقطع تحصیلی: **کارشناسی ارشد**
رشته: مهندسی کامپیوتر
گرایش: معماری کامپیوتر
دانشگاه: **محقق اردبیلي**
دانشکده: فنی و مهندسی تاریخ دفاع: 94/06/31
تعداد صفحات: 106

چکیده:
تابع درهم‌ساز یکی از ابزارهای مهم در رمزنگاری و تشخیص اصالت پیام محسوب می‌شود که فرم کلیددار این تابع برای MAC و فرم بدون کلید آن در MDC مورداستفاده قرار می‌گیرد. در طراحی این‌گونه توابع، سرعت و امنیت پارامترهای مهمی برای کاربردهای مختلف رمزنگاری می‌باشند. توابع درهم‌ساز پرکاربرد در این زمینه MD5، SHA-0، SHA-1 و SHA-2 می‌باشند که به شکل‌های مختلف موردحمله قرار گرفته‌اند. توابع یاد شده، با ساختار مرکل-دامگارد و با توابع درونی دودویی طراحی شده‌اند. یک روش دیگر برای طراحی چنین توابعی استفاده از نگاشت‌های آشوب می‌باشد. در این رساله، ابتدا یک سیستم آشوب با قابلیت فشرده‌سازی معرفی و با استفاده از آن یک تابع درهم‌ساز فازی طراحی گشته است. ساختار درهم‌سازی معرفی شده قابلیت پیاده‌سازی به صورت موازی را داشته و طول خروجی متغیری را دارا است. این تابع درهم‌ساز از یک کلید 256 بیتی بهره می‌برد که طول آن می‌تواند افزایش یابد. بررسی کارایی تابع درهم‌ساز پیشنهادی با استفاده از پارامترهای کارایی، تحلیل امنیتی و سرعت صورت گرفته استکه از آن جمله می‌توان به بررسی حساسیت تابع درهم‌ساز به پیام ورودی و تغییر شرایط اولیه، بررسی آماری اغتشاش و انتشار و مقاومت در برابر برخورد یاد کرد. تابع درهم‌ساز طراحی‌شده به لحاظ پارامترهای کارایی بیان شده با برخی توابع درهم‌ساز مبتنی برآشوب نیز مقایسه و بر اساس حملات عمومی صورت گرفته بر روی توابع درهم‌ساز مورد بحث و بررسی قرار گرفته است.

کلید واژه‌ها: تابع درهم‌ساز، نظریه آشوب، حملات رمزنگاری، سیستم آشوب.

فهرست مطالب

شماره و عنوان مطالب **صفحه**

فصل سوم: نظریه آشوب و توابع درهم‌ساز مبتنی بر آن

فصل چهارم: یک سیستم آشوب ترکیبی جدید با قابلیت فشرده‌سازی

فصل پنجم: الگوریتم درهم‌سازی فازی مبتنی بر سیستم آشوبناک DCS

فصل ششم: نتایج به‌دست آمده

فصل هفتم: نتیجه‌گیری و بحث

فهرست جدول‌ها

شماره و عنوان جدول **صفحه**

فهرست شکل‌ها

شماره و عنوان شکل **صفحه**

فهرست علائم اختصاری

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

فصل اول:

مقدمه

1-1- مقدمه

عدم ارتباط بین اطلاعات و رسانه انتقال آن، به بزرگترین مزیت اطلاعات دیجیتال بدل گشته است، به‌طوری‌که 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 Ethernet، Wi-Fi و GSM و یا ارتباط ماهواره‌ای ارسال و دریافت کرد.

این امر به‌نوبه خود می‌تواند نفوذپذیری بزرگی را فراهم آورد، به شکلی که دیگر نمی‌توان فقط با استناد به رسانه فیزیکی، صحت اطلاعات را تصدیق[1] نمود. جهت تصدیق این اطلاعات، رمزنگارها[2] 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).

ازاین‌رو، در ارتباطات امن به شیوه مدرن امروزی، امضای دیجیتال[3]، MAC[4] و MDC[5] از اهمیت بسیاری برخوردار گشته‌اند و ارتباطات مدرن نیازمند برقراری چنین ساختاری برای حفظ اصالت پیام[6]، تائید هویت فرستنده[7] و عدم انکار از سوی فرستنده[8] می‌باشند.

توابع درهم‌ساز در امضای دیجیتال، MAC، MDC، جدول کلیدواژه، تشخیص ویروس[9]، PRF[10] و PRNG[11] کارکردهای فراوانی دارند. این توابع در بسیاری از پروتکل‌های بی-سیم همچون WAP[12] نیز به‌طور گسترده‌ای استفاده‌شده‌اند (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

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

بر اساس نظریه اغتشاش و انتشار[1]، 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 شده‌است 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 قرارگرفته‌اند که (den ؛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.

به‌جز توابع مرسوم نامبرده شده، راهبردهای مختلفی در زمینه طراحی توابع درهم‌ساز مورد تحقیق و بررسی قرارگرفته‌اند. یکی از این راهبردها استفاده از نظریه آشوب[2] در این زمینه می‌باشد. نگاشت‌های آشوب[3] با توجه به خصوصیت‌های حساسیت به مقادیر اولیه ورودی، ارگودیسیتی[4] 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 نگاشت‌ها، 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 تولد[1] مقاوم‌تر می‌باشد.

یک سیستم مبتنی بر نظریه آشوب ازنقطه‌نظر ریاضی سامانه‌ای دینامیک می‌باشد که رفتار آن در یک بازه قابل پیش‌بینی بوده و رفتار آن در خارج از بازه‌ی مزبور غیرقابل‌پیش‌بینی است و یا اینکه به‌صورت اتفاقی و قابل‌تشخیص با خطای غیرقابل‌چشم‌پوشی می‌باشد. سیستم آشوب را می‌توان به‌صورت بی‌نظمی 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 باشد[2]

3- چرخش‌های دوره‌ای چگال داشته باشد[3] (Kellert, 1993)

یک تابع درهم‌ساز مبتنی برآشوب، از یک سیستم یا نگاشت مبتنی برآشوب و یک الگوریتم درهم‌سازی تشکیل شده است. با استفاده از سیستم آشوب، با یک ورودی به‌عنوان کلید، یک توالی از بیت‌ها به دست می‌آید که خاصیت آشوب را دارا هستند. با استفاده از توالی به دست آمده و ترکیب آن با ورودی با اندازه نامعلوم، می‌توان خروجی را به اندازه معلوم فشرده کرد. نکته اساسی در چنین توابع درهم‌ساز، خاصیت حساسیت به مقادیر اولیه سیستم آشوب و همچنین نحوه استفاده از آن در ایجاد حساسیت به مقادیر ورودی در خروجی تابع درهم‌ساز می‌باشد (Kocarev & Lian, 2011).

طراحی یک تابع درهم‌ساز مبتنی برآشوب به لحاظ امنیتی نسبت به توابعی مانند MD5، SHA-0، SHA-1 و SHA-2 می‌تواند بهبودهای امنیتی بسیاری را از جهت حساسیت به مقادیر ورودی و هم چنین اغتشاش و انتشار به دست دهد. بهینه‌سازی روی چنین توابعی می‌تواند آن‌ها را به لحاظ سرعت پردازش نسبت به سایر توابع درهم‌ساز مبتنی برآشوب بهبود بخشد. همچنین این توابع می‌توانند به‌صورت کلیددار و بدون کلید برای استفاده در کاربردهای MAC و MDC طراحی شوند.

2-1- بیان مسئله

طراحی توابع درهم‌ساز یک مسئله‌ی باز در زمینه رمزنگاری می‌باشد. زیرا توابع طراحی شده به مرور مورد حمله قرار خواهند گرفت و علت این امر در رشد سرعت پردازش رایانه‌ها و روش‌های حملات رمزنگاری می‌باشد. از این حیث، علاوه بر اهمیت موضوع در حیطه 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 بوته آزمایش گزارده شده و موفقیت‌هایی در حملات نیز کسب‌شده است که در (De Cannière & Oechslin, ؛ 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 (Biryukov & et al, 2011؛ Biham & Chen, 2004) به برخی از این حملات بر روی توابع درهم‌ساز MD5، SHA-0، SHA-1 و SHA-2 اشاره‌شده 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 ؛ Deng & et al, 2010؛ Kwok & Tang, 2003؛ Wong, 2003؛ Kanso & et al, 2012؛ Xiao & et al, ؛ Wang & et al, 2008؛ Wang & Hu, 2007؛ Xiao & et al, 2005؛ Yi, 2005 Deng & et al, ؛ Xiao & et al, 2006؛ Zhang & et al, 2007؛ Xiao & et al, 2009؛ 2008 (Kanso & Ghebleh, 2013؛ Akhshan & et al, 2009؛ Akhavan & et al, 2009؛ 2009 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 موردبررسی قرارگرفته‌اند.

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 موردنظر 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 نگاشت‌های آشوب و یا ترکیب آن‌ها برای ایجاد یک تابع درهم‌ساز مبتنی بر آشوب مناسب است؟
- چگونه می‌توان تابع درهم‌ساز مبتنی برآشوب 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 خصوصیاتی 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 $\overline{B}$ ، 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 مرکل-دامگارد و ساختار اسفنجی و تحلیل انعطاف پذیری می‌باشد.

1-5- ساختار پایان‌نامه

ساختار ادامه این پایان نامه 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

Abstract:

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.

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