



تحلیلی امنیت تابع چکیده ساز SHA-3

تألیف: سید احسان حسینی نژاد



کتاب ریرا

۱۳۹۸

سرشناسه	:	حسینی نژاد، سیداحسان، ۱۳۷۰ -
عنوان و نام پدیدآور	:	تحلیل امنیت تابع چکیده‌ساز SHA-3 / تألیف سیداحسان حسینی نژاد.
مشخصات نشر	:	تهران: کتاب ریرا، ۱۳۹۸.
مشخصات ظاهری	:	۱۱۸ ص.
شابک	:	978-622-6706-19-3
وضعیت فهرست نویسی	:	فپا
یادداشت	:	کتابنامه: ص. [۱۰۹] - ۱۱۲.
موضوع	:	رمزگذاری داده‌ها — ریاضیات
ژانر	:	Data encryption (Computer science) -- Mathematics
موضوع	:	رمزنگاری — ریاضیات
موضوع	:	Cryptography -- Mathematics
موضوع	:	الگوریتم‌های کامپیوتری
موضوع	:	Computer algorithms
رده بندی کنگره	:	QA۷۶/۹
رده بندی دیویی	:	۰۰۵/۸۲
شماره کتابشناسی ملی	:	۵۷۳۷۳۳۹

تحلیل امنیت تابع چکیده‌ساز SHA-3

تألیف: سید احسان حسینی نژاد

نوبت چاپ: اول ۱۳۹۸

شمارگان: ۱۰۰۰ نسخه

شابک: ۹۷۸-۶۲۲-۶۷۰۶-۱۹-۳

قیمت: ۱۵۰۰۰ تومان



کتاب ریرا

انتشارات کتاب ریرا

نشانی: خیابان انقلاب، خیابان دانشگاه، خیابان روانمهر، کوچه بهار، پلاک ۳

تلفن: ۶۶۴۹۳۳۴۸

فهرست مطالب

فصل اول : آشنایی با امنیت و تحلیل داده	۵
رمزنگاری باستانی	۶
رمزنگاری نوین	۱۳
رمزنگاری و اهداف آن	۱۶
تحلیل رمز	۲۰
امنیت در توابع چکیده ساز	۲۴
سطح امنیت	۲۴
جمع بندی	۲۶
فصل دوم : الگوریتم چکیده ساز امن - ۳	۲۸
کچک	۳۱
تبدیل رشته داده به حالت داخلی	۳۳
تبدیل حالت داخلی به رشته داده	۳۵
اعمال کچک	۴۶
مشخصات لایه گذاری چند نرخی	۴۷
مشخصات خانواده کچک	۴۷
ساختار اسفنجی	۴۸
مشخصات توابع SHA-3	۵۱
تحلیل امنیتی	۵۳
تحلیل امنیتی تابع کچک	۵۴
سطح امنیتی	۵۴
امنیت توابع خروجی قابل گسترش	۵۶
جمع بندی	۵۹

فصل سوم: توسعه و بهبود نتایج حمله تحلیل خطای تفاضلی روی SHA-3	۶۱
رفتار تفاضلی دور محدود SHA-3	۶۳
ویژگی‌های تفاضلی عملگرها	۶۳
عملگر XOR	۶۴
عملگر ضرب بیتی	۶۶
توزیع تفاضلی در کچک	۶۸
توزیع تفاضلی دور در و بازیابی از حالت داخلی	۷۲
تشخیص خطای تزریقی	۷۵
حمله بازیابی حالت داخلی	۷۶
نتایج حمله به روش مقالات قبل توسعه آن	۷۷
روشهای بهبود نتایج	۷۹
الگو X و تشخیص خطای تزریقی	۸۱
ساخت الگو X	۸۳
شیوهی استفاده از روابط یک الگو X در بررسی مقدار خطا	۸۷
تشخیص خطای تزریقی با الگو X	۸۹
محدودیت‌های تشخیص خطای تزریقی با الگو X	۹۴
روش تفاضل معکوس و بازیابی صفحه ناقص در چکیده خروجی	۹۶
استفاده از روش جبری	۱۰۲
شبیه سازی حملهی بهبود یافته	۱۰۳
بحث روی نتایج	۱۰۶
سخن پایانی	۱۰۷
منابع	۱۰۹
پیوست ۱: لغات و اصطلاحات	۱۱۳