

دانشکده مهندسی کامپیوتر  
طراحی سیستم‌های دیجیتال  
مستند پروژه

---

## بررسی الگوریتم درهم‌سازی skein

---

نگارندگان:  
حسن سندانی  
محمد صالح سعیدی  
مریم حاک  
محمد مهدی عرفانیان  
علی جندقی

۱۹ خرداد ۱۳۹۸



# فهرست مطالب

۲	۱	مقدمه
۳	۱.۱	توضیح الگوریتم
۳	۱.۱.۱	مثالهایی از درهم‌سازی

# فصل ۱

## مقدمه

توضیحی اولیه مشتمل بر تعریف الگوریتم، نحوه کلی عملکرد الگوریتم، پایه‌های ریاضی، کاربردها و استانداردها

## ۱.۱ توضیح الگوریتم

الگوریتمی که در ادامه این مستند شرح و توضیح آن آمده است الگوریتم درهم سازی skein یا cryptographic hash function است. این الگوریتم از سری الگوریتم‌های درهم‌سازی امنیتی یا cryptographic hash function و یکی از نامزدهای نهایی مسابقه انتخاب بهترین تابع درهم‌سازی NIST می‌باشد. این مسابقه برای انتخاب بهترین الگوریتم درهم‌سازی برای استاندارد جدید SHA-3 برگزار شد. طبق ادعای طراحان الگوریتم این الگوریتم می‌تواند در 6.1 کلاک در بایت داده‌ها را هش کند، که به این معنیست که در پردازنده دوهسته‌ای 64 بیتی با فرکانس پردازشی 3.1 GHz می‌تواند با سرعت 500 مگابایت بر ثانیه داده‌ها را هش کند. این مقدار سرعت تقریباً دو برابر سرعت هش کردن داده الگوریتم SHA-512 است. همچنین با گزینه درخت درهم‌سازی که می‌تواند به صورت اختیازی در الگوریتم پیاده‌سازی شود می‌توان در پیاده‌سازی موازی الگوریتم سرعت را به بیش از این هم رساند. نکته دیگری که در مورد الگوریتم skein لازم به ذکر است این است که این الگوریتم پیاده‌سازی آسان و ساده‌ای دارد و فقط از سه عملگر اصلی برای محاسبه هش استفاده می‌کند و نحوه عملکرد الگوریتم به راحتی قابل به خاطر سپاری و یادگیری است.

الگوریتم درهم‌سازی skein برای حالت‌های ورودی ۲۵۶، ۵۱۲ و ۱۰۲۴ بیتی و هر مقداری خروجی پیاده‌سازی شده است که این خاصیت در انعطاف الگوریتم در حالت‌های مختلف بسیار حیاتی است.

در پیاده‌سازی سخت‌افزاری نیز این الگوریتم قوی عمل می‌کند، برای پیاده‌سازی skein-512 بر سخت‌افزار به حدود ۲۰۰ بایت فضای مموری نیاز داریم، برای skein-256 این مقدار به حدود ۱۰۰ بایت کاهش پیاده می‌کند که این الگوریتم را به یک الگوریتم مناسب برای پیاده‌سازی‌های روی قطعات کوچک سخت‌افزاری تبدیل می‌کند، مثلاً می‌توان از skein-256 در پیاده‌سازی smart card استفاده کرد. [۱]

### ۱.۱.۱ مثال‌هایی از درهم‌سازی

• Skein-256-256(“”)

c8877087da56e072870daa843f176e9453115929094c3a40c463a196c29bf7ba

• Skein-512-256(“”)

39ccc4554a8b31853b9de7a1fe638a24cce6b35a55f2431009e18780335d2621

• Skein-512-512(“”)

bc5b4c50925519c290cc634277ae3d6257212395cba733bbad37a4af0fa06af4  
1fca7903d06564fea7a2d3730dbdb80c1f85562dfcc070334ea4d1d9e72cba7a

# کتاب نامه

<http://www.skein-hash.info/about> [۱]