دانشکده مهندسی کامپیوتر

طراحی سیستم‌های دیجیتال

مستند پروژه

بررسی الگوریتم درهم‌سازی skein

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

۱۷ خرداد ۱۳۹۸

فهرست مطالب

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 ادامهٔ این مستند شرح و توضیح آن آمده است الگوریتم درهم سازی skein یا skein 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. [۱]. طبق ادعای طراحان الگوریتم این الگوریتم می‌تواند در ۱.۶ کلاک در بایت داده‌ها را هش کند، که به این معنیست که در پردازندهٔ دوهسته‌ای ۶۴ بیتی با فرکانس پردازشی ۱.۳ گیگاهرتز می‌تواند با سرعت ۵۰۰ مگابایت بر ثانیه داده‌ها را هش کند.

کتاب‌نامه

[۱]