

عنوان مقاله:

تحلیل زمانی الگوریتم ضرب پیمانه‌های Blakley

محل انتشار:

یازدهمین کنفرانس سالانه انجمن کامپیوتر ایران (سال: 1384)

تعداد صفحات اصل مقاله: 10

نویسندگان:

بهادر بخشی - دانشکده کامپیوتر دانشگاه صنعتی امیرکبیر

بابک صادقیان - دانشکده کامپیوتر دانشگاه صنعتی امیرکبیر

خلاصه مقاله:

تحلیل زمانی تا کنون عمدتاً بر روی توانرسانی پیمانه‌های که دارای تغییرات زمانی زیادی است اعمال می‌شود. در این مقاله ما طرحی برای تحلیل زمانی الگوریتم ضرب پیمانه‌های Blakley که تغییرات زمانی آن در مقایسه با توانرسانی پیمانه‌های بسیار کمتر است، ارائه می‌کنیم. در این طرح، با فرض داشتن یکی از ورودیها و زمان اجرای الگوریتم و بدون در اختیار داشتن نتیجه عمل ضرب عملوند دیگر بدست می‌آید در کاربردهای مانند الگوریتم Digital Signature Standard این عملوند یکی از اجزای مخفی سیستم است. در اکثر تحلیل‌های زمانی برای کاهش پیچیدگی تحلیل، زمان اجرای مراحل الگوریتم مستقل از هم فرض می‌شود. در این مقاله نشان می‌دهیم که این فرض برای الگوریتم ضرب Blakley صادق نیست و مدل ریاضی همبستگیها و تاثیر آن در حمله زمانی را بررسی می‌کنیم. همچنین برای طرح تحلیل زمانی ارائه شده، مکانیزم تشخیص و تصحیح خطا تحلیل معرفی می‌کنیم.

کلمات کلیدی:

حمله زمانی، ضرب پیمانه‌های، الگوریتم Blakley، همبستگی

لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/127098>

