بخشی از ترجمه مقاله

عنوان فارسی مقاله :

ALE: رمزگذاری سبک تصدیق شده مبتنی بر AES

عنوان انگلیسی مقاله :

ALE: AES-Based Lightweight Authenticated Encryption

توجه !

این فایل تنها قسمتی از ترجمه میباشد. برای تهیه مقاله ترجمه شده کامل

با فرمت ورد (قابل ویرایش) همراه با نسخه انگلیسی مقاله، اینجا کلیک نمایید.

بخشی از ترجمه مقاله

6 Conclusion

In this paper, we have proposed ALE – a new Authenticated Lightweight Encryption algorithm based on AES. It is a single-pass nonce-based online scheme that combines some ideas of Pelican MAC, LEX and ASC-1 in a highly lightweight manner. ALE is about half the size of ASC-1 and in terms of speed in the lightweight implementation, it is about 4.5 times faster than ASC-1 in its smallest implementation.

By requiring only 2.5 kGE of area in lightweight ASIC hardware ALE is actually significantly smaller than most other authentication encryption modes including the popular modes AES-OCB and AES-CCM. In terms of speed in the lightweight implementation, ALE is about 2.5 times faster than AES-OCB and about 5 times faster than AES-CCM. When using the parallel AES-NI instructions, ALE outperforms AES-GCM, AES-CCM and ASC-1 by a considerable margin, providing a throughput close to that of AES-OCB, which is a patented scheme.

6. نتیجه گیری

در این مقاله، ما ALE - یک الگوریتم رمزگذاری سبک وزن معتبر جدید بر اساس AES را پیشنهاد داده ایم. آن یک طرح برخط مبتنی بر وضعیت فعلی تک مسیره است که بعضی از نظریه های پلیکان MAC، LEX، و ASC-1 را به شیوه ای بسیار سبک وزن ترکیب می کند. ALE در حدود نصف اندازه ASC-1 و بر حسب سرعت در پیاده سازی سبک وزن می باشد، آن در حدود 4.5 برابر سریع تر از ASC-1 در کوچک ترین پیاده سازی خود است.

با نیاز به فقط 2.5 کیلو GE از منطقه در ASIC سبک وزن ALE سخت افزار به طور بسیار چشمگیری کوچکتر از بیشتر حالت های رمزگذاری معتبر دیگر است که حالت های عمومی AES-OCB و AES-CCM را در بر می گیرد. بر حسب سرعت در پیاده سازی سبک وزن، ALE در حدود 2.5 بار سریع تر از AES-OCB و در حدود 5 بار سریع تر از AES-CCM است. هنگام استفاده از دستورالعمل های AES-NI موازی،ALE عملکرد بهتری نسبت به AES-GCM، AES-CCM و ASC-1 با در نظر گرفتن حاشیه، فراهم کردن توان عملیاتی نزدیک به AES-OCB، که طرحی انحصاری است، دارد.