انجمن رمز ایران
Iranian Society of Cryptology

Masking as a Side-Channel Countermeasure in Hardware

Side-channel attacks are a major threat to the security of modern embedded devices. If no particular attention is paid, the exploitation of physical leakages such as the power consumption and the electromagnetic radiation of a cryptographic implementation can lead to successful key recoveries. Examples include KeeLoq, FPGA bitstream encryption, Atmel CryptoMemory, and GSM Simcards. As a consequence, the topic has been followed by a vast literature on potential solutions to defeat such attacks. The countermeasures against side-channel attacks range from ad hoc to formal, and are defined to be applied at various abstraction levels. For instance, time randomizations (based on random delay insertion or shuffling) are frequently-used low-overhead heuristic-based approaches (mainly) for software-based applications. These hiding schemes are not limited to only those which randomize the computations in time, but covers the approaches that add noise resources as well as those aiming to equalize the power consumption. On the other hand, probably the most investigated and best understood protection against side-channel attacks is masking. The underlying principle of masking is to represent any sensitive variable in the implementation by d shares in such a way that the computations are performed only on these shares. Assuming that the leakage of the shares are independent of each other, a successful key-recovery attack needs to observe at least the dth-order statistical moment of the leakage distributions, where the corresponding complexity increases exponentially with d. However, the independence of leakages associated to the shares is an assumption which is usually violated in hardware applications. As an example, the first masked AES Sbox designs failed in practice to satisfy the desired first-order security. Instead, based on Boolean masking and multiparty computation, **threshold implementations** (TI) can ensure first-order resistance in the presence of glitches. In this tutorial, the basics and challenges of realizing masking in hardware platforms are explained, and the core topic - with respect to threshold implementation - is how to protect hardware implementation of symmetric cryptographic primitives.

انجمن رمز ایران
Iranian Society of Cryptology

نقاب گذاری به عنوان یک روش مقابله با حملات کانال جانبی در سخت افزار

حملات کانال جانبی یک تحدید مهم برای امنیت سیستم‌های نهفته به شمار میروند. اگر دقت کافی در طراحی چنین سیستم‌هایی نشود، استفاده از نشت فیزیکی اطلاعات همچون توان مصرفی و یا تشاشعات الکترومغناطیسی مربوط به دستگاه رمزنگاری می‌تواند منجر به حملاتی موفقیت آمیز برای یافتن کلید شود. به عنوان مثال می‌توان به مواردی چون KeeLoq، رمزنگاری پیکربندی FPGAها، حافظه رمزگذاری شده Atmel و سیم کارت‌های GSM اشاره کرد. در نتیجه، موضوع حمالات کانال جانبی به شکلی وسیع توسط محققین دنبال شده و راه حل‌هایی برای مقابله با آن‌ها ارائه شده‌اند. روش‌های مقابله با حملات کانال جانبی طیف وسیعی از روش‌های موردی و تفصیلی را در بر می‌گیرند که می‌توانند در سطوح مختلفی از پیاده‌سازی به کار گرفته شوند. به عنوان مثال، تصادفی‌سازی در حوزه زمان (توسط اضافه کردن تصادفی تاخیر و یا به هم ریختن ترتیب اجرای عملیات) روش‌های ابتکاریی و کم هزینه هستند که عمدتاً در پیاده‌سازی‌های نرم افزاری مورد استفاده قرار می‌گیرند. این روش‌های مبتنی بر "مخفی سازی" به تصادفی سازی در حوزه زمان محدود نمی‌شوند، بلکه شامل روش‌هایی همچون اضافه کردن منابع نویز و یا یکسان سازی توان مصرفی نیز می‌شوند.

از طرف دیگر، "نقاب گذاری" در مقایسه با دیگر روش‌های مقابله، بیشتر مورد بررسی و شناخت قرار گرفته است. اساس نقاب گذاری مبتنی بر ارائه مقادیر میانی پیاده‌سازی (رمزنگاری) توسط d سهم می‌باشد، به طوری که تمامی محاسبات فقط بر روی سهم‌ها انجام می‌گیرند. با فرض این که نشت اطلاعاتی مربوط به سهم‌ها مستقل از یکدیگر می‌باشند، یک حمله موفقیت‌آمیز برای کشف کلید نیازمند بررسی گشتاور مرتبه d ام توزیع احتمال نشت اطلاعاتی است. در این حالت، پیچیدگی حمله با افزایش d به شکل نمایی زیاد می‌شود. اما فرض استقلال نشت اطلاعاتی مربوط به سهم‌ها عموماً در پیاده‌سازی‌های سخت افزاری نقض می‌شود. به عنوان مثال، اولین تلاش‌ها برای پیاده‌سازی جدول جانشینی نقاب گذاری شده الگوریتم AES در عمل منجر به شکست شدند. در مقابل، **پیاده‌سازی آستانه‌ای** (TI) که بر اساس نقاب گذاری بولی و محاسبات چند جانبه است، می‌تواند در حضور glitch (تغییرات گذرا در مدارهای منطقی ترکیبی) در مقابل حملات کانال جانبی مرتبه اول مقاومت ایجاد کند.

در این کارگاه آموزشی، مبانی و چالش‌های مربوط به محقق سازی نقاب گذاری در پیاده‌سازی‌های سخت افزاری مورد بحث قرار خواهند گرفت. موضوع اصلی کارگاه – با توجه به پیاده‌سازی آستانه‌ای – نحوه ایجاد مقاومت در پیاده‌سازی سخت افزاری الگوریتم‌های رمزنگاری متقارن در برابر حملات کانال جانبی است.