عنوان مقاله:

An Investigation through Different B its Leakage in Power Analysis Attacks

محل انتشار:

چهارمین کنفرانس انجمن رمز ایران (سال: 1386)

تعداد صفحات اصل مقاله: 6

نویسندگان:

Ehsan Rahimi - *Electrical Engineering Department, Iran University of Science & Technology, Tehran, Iran*

Ali Sadr - *Electrical Engineering Department, Iran University of Science & Technology, Tehran, Iran*

خلاصه مقاله:

Since the introduction of side-channel attacks, cryptographic devices are highly susceptible to power and electromagnetic analysis attacks, because these attacks require only relatively inexpensive equipments. Unless adequate countermeasures are implemented, side channel attacks allow an unauthorized person to reveal the private key of a cryptographic module. For attackers it is really prominent to attack a module with less number of measurements. Choosing an appropriate intermediate result is often of high importance and enables them to reveal the secret key with less number of measurements and in a short duration of time. In this paper a differential power analysis attack on different bits of an intermediate result on software implementation of AES- 128 on an 8051-compatible microcontroller has been carried out. The results show that specific bits leak information that is detectable with given 200 measurements. The other bits do not leak enough information that could be exploitable with 200 measurements in this particular attack. Consequently attackers should be aware that different bits in the same register .in a processor leak different amount of information

کلمات کلیدی:

Side Channel Attacks, Diferential Power Analysis Attack, Cryptographic Processors, Intermediate Result