عنوان مقاله:

Applying TMR for Trojan Masking: Challenges, Guidelines and New Solutions

محل انتشار:

اولین همایش ملی رایانش نرم و هوش محاسباتی (سال: 1400)

تعداد صفحات اصل مقاله: 17

نویسندگان:

Seyed Mohammadhossein Shekarian, - *Factually of Engineering, Department of Computer Engineering, University of Guilan, Rasht, Iran*

Arman Hajishafieha, - *Factually of Engineering, Department of Computer Engineering, University of Guilan, Rasht, Iran*

خلاصه مقاله:

Hardware Trojans are among the most critical threats to the security and trustworthiness of computing systems. To protect circuits against Trojans, many detection methods and design-for-hardware-trust techniques are provided in the literature, including triple modular redundancy (TMR). However, most available TMR techniques can be easily neutralized if the Trojan is implemented at the output of the voting module. We previously introduced OTMR (TMR with obfuscated voter) to overcome this challenge. In this paper, we present a more thorough discussion on the limitations and challenges of applying TMR for Trojan masking. We highlight the importance of controlling TMR overhead to keep the Trojan-to-background effect ratio as large as possible. We also provide algorithms for the effective application of OTMR on low-observable, low-controllable and functionally-critical signals. We conducted experiments on general and crypto benchmarks to validate the effectiveness of our approach. The result confirms that, if wisely used, OTMR can mask Trojans and improve the Trojan detection probability by side-channel analysis at .the same time

کلمات کلیدی:

Hardware Trojans, Triple Modular Redundancy (TMR), Obfuscated TMR (OTMR), Security Critical Signals

لینک ثابت مقاله در پایگاه سیویلیکا: