عنوان فارسی مقاله :

تجربیات کسب شده در زمینه طراحی و اجرای سخت افزار تروجان(Trojan)

عنوان انگلیسی مقاله :

Experiences in Hardware Trojan Design and Implementation

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.

II. Previous Detection Approaches

In order to overcome the shortages of traditional testing methods in Trojan detection, new low-cost testing schemes are of high priority to secure the whole design chain when the fabrication foundry is untrusted. Several Trojan detection schemes have already been proposed, among which two main techniques are functional testing and side-channel fingerprint generation. In [1], the author argues that attackers would only choose rarely occurring events as triggers and proposes equations to compute low frequency events as a complement to input patterns generated by commercial ATPG tools. The assumption here is quite weak, since as soon as attackers know the testing scheme, they will surely do the same computation and choose more frequently occurring patterns as triggers. [2] is the first paper to present the idea of differentiating Trojan-inserted chips by comparing the side-channel fingerprints of tested chips with those generated from gold models. It analyzed the common behavior of various types of Trojans and demonstrated the feasibility of building effective fingerprints for an IC family to detect Trojan-inserted ICs. Noise modeling was used to construct the fingerprint for an IC family and Karhunen-Loeve (KL) expansion was a computational tool to separate the randomness and the time-variation of a random process. This method is useful in detecting Trojans when the Trojan circuit is large enough compared to the whole chip area and the process variation is low. The false alarm rate will emerge and increase quickly if the Trojan only occupies a trivial percentage of the whole chip area and there is large process variation.

2. شیوه های تشخیص و آشکارسازی پیشین

به منظور غلبه بر موانع روشهای تست سنتی در زمینه تشخیص و آشکارسازی Trojan ، طرح های تست کم هزینه جدید برای اطمینان کل زنجیره طرح هنگامی که کارخانه تولید معتبر نباشد، از اولویت بالایی برخوردار می باشند. قبلاً طرح های تشخیص و آشکارسازی متعددی برای Trojan پیشنهاد شده است، در میان آنها می توان به دو شیوه مهم یعنی تست تابعی و تولید اثرانگشت کانال جانبی اشاره نمود. در بخش 1، مولف این گونه استدلال می کند که مهاجمین به ندرت پیش می آید که حوادث و رویدادها را به عنوان تریگر انتخاب کنند و برای محاسبه رویدادهای کم بسامد از معادلاتی به عنوان مکمل الگوهای ورودی ابزارهای تجاری ATPG استفاده می کنند. فرضیه مطرح شده در این جا بسیار ضعیف می باشد، زیرا به محض اینکه مهاجمین از طرح تست مطلع شدند، قطعاً شروع به محاسبه کرده و الگوهایی با بسامد بالا را به عنوان تریگر انتخاب می کنند. مقاله 2 اولین مقاله ای است که ایده تمایز تراشه های تعبیه شده Trojan از طریق مقایسه اثرانگشت کانال جانبی تراشه های تست شده با مدلهای طلا را مطرح می نماید. ایده مذکور رفتار معمول انواع و اقسام Trojan را آنالیز نموده و در مورد امکان ساخت اثرانگشت موثر برای یک خانواده IC جهت تشخیص و آشکارسازی IC های تعبیه شده Trojan توضیح داد. برای ارائه اثرانگشتی برای یک خانواده IC از روش مدل سازی نویز استفاده گردید و از روش بسط (Karhunen-Loeve (KL به عنوان یک ابزار محاسباتی برای جداکردن تصادفی بودن و تغییر زمانی فرایندتصادفی استفاده گردید. این روش در تشخیص و آشکارسازی Trojan زمانی مفید عمل می کند که مدار Trojan در مقایسه باکل مساحت تراشه به اندازه کافی بزرگ بوده و تغییر فرایند در حد کم باشد. اگر Trojan درصد جزئی از کل مساحت تراشه را به خود اختصاص داده و تغییر فرایند در حد زیاد باشد، آنگاه نرخ آژیر غلط در صورتی به صدا درآمده و به سرعت افزایش می یابد .