ETH zürich

ETH Library

Secure testing of VLSI cryptrographic equipment

Doctoral Thesis

Author(s):
Bonnenberg, Heinz

Publication date:
1993

Permanent link:
https://doi.org/https://doi.org/10.3929/ethz-a-000904787

Rights / license:
In Copyright - Non-Commercial Use Permitted

This page was generated automatically upon download from the ETH Zurich Research Collection.
For more information, please consult the Terms of use.

Diss. ETH No. 10204

Secure Testing of VLSI Cryptographic Equipment

A dissertation submitted to the
SWISS FEDERAL INSTITUTE OF TECHNOLOGY
ZURICH

for the degree of
Doctor of technical sciences

presented by
HEINZ BONNENBERG
Dipl. Inform.
born 20. 12. 1960
citizen of Germany

accepted on the recommendation of
Prof. Dr. W. Fichtner, examiner
Prof. Dr. J. L. Massey, co-examiner

1993

Abstract

Advances in cryptology and the ability to integrate complex functionality into a single device has led to an intensive use of hardware cryptographic equipment. Modern ciphers require an extraordinary amount of both time and equipment to be broken and thus are unbreakable from a practical point of view. As a consequence, potential eavesdroppers focus their attacks on the weaknesses of the electronic systems performing the encryption and decryption operations.

Susceptibility to physical system intrusion can never be totally prevented. However, miniaturization by VLSI integration is one of a number of appropriate measures to protect sensitive information to a satisfactory degree.

Circuitry of the complexity achieved by VLSI requires specific design for testability (DfT). The large variety of potential device-internal defects contrasts with the small number of external interconnects that can be utilized for testing purposes. Conventional DfT techniques are based on an external test stimuli generation and test response analysis and thus rely on the observability and controllability of internal nodes. This requirement for accessibility strongly conflicts with the cryptographic demand of hiding chip-internal sensitive information.

A way around this fundamental antagonism between security and testability is the choice of a built-in self-test (BIST). BIST requires the integration of stimuli generators and response evaluation on-chip. Non-sensitive information about the BIST process in advance and BIST results are then the only available information that can be acquired from the device.

For most applications, BIST is too expensive with regard to both designer effort and silicon area consumption. However, exploitation of specific cipher properties allows the integration of a high-quality self-test scheme with a

minimum area consumption.

The practical feasibility of utilizing such specific cipher properties with regard to BIST is demonstrated by a VLSI implementation of the new secret key block cipher IDEA. The new VINCI chip has been provided with two kinds of self-test operation: an off-line mode including the complete chip hardware to achieve maximum fault coverage, and an on-line self-test that concurrently controls data transformation and immediately indicates any failure. By this compound test scheme, VINCI fully conforms to the demands of existing security standards.

Test response evaluation during BIST is frequently performed by compressing a large number of test results into a single signature. As a consequence, self-testing devices lack fault localization capabilities in most cases because a faulty signature tells little about the time of occurrence and the number of faults. In contrast, substantial fault localization capability on VINCI has been realized by monitoring all intermediate self-test results continuously and triggering an immediate alarm in case of a failure.

Zusammenfassung

Kryptographie findet heute immer breiteren Einsatz bei der Übertragung vertraulicher Daten. Neue Verschlüsselungsverfahren bieten hier größtmögliche theoretische Sicherheit in Verbindung mit immer höheren Datentransformationsraten. In einem Umfeld, in dem Verfahren angewendet werden, die nur noch mit einem praktisch nicht zu realisierenden Aufwand gebrochen werden können, richtet sich das Augenmerk potentieller Lauscher daher am ehesten auf die Schwächen der elektronischen (Sub-) Systeme, die die benötigte Ver- oder Entschlüsselung ausführen.

In jedes physikalische System kann – wenn auch möglicherweise nur unter extremem Aufwand – eingebrochen werden. Eine Miniaturisierung durch Höchstintegration in einen VLSI-Schaltkreis bietet immerhin guten Schutz vor dem Zugang zu internen Strukturen. Bei komplexen ICs besteht jedoch generell die Notwendigkeit der Testbarkeit, die im Normalfall durch Maßnahmen zur Erhöhung der Beobachtbarkeit und Kontrollierbarkeit interner Strukturen erreicht wird. Gerade dies aber steht dem Gebot der Abschirmung interner Strukturen, die Rückschluß auf den geheimen Schlüssel oder Klartext zulassen, entgegen. Hier eröffnet die Möglichkeit des automatischen, eingebauten Selbsttests einen Ausweg.

Für konventionelle Anwendungen erweist sich ein automatischer Selbsttest oft als zu teuer, weil er neben hohem Entwurfsaufwand viel Fläche für die ebenfalls zu integrierenden Stimuligeneratoren und Analysierer der Testantworten beansprucht. Die in dieser Dissertation behandelten Blockchiffrierungsverfahren besitzen jedoch eine Reihe von – auch theoretisch nachweisbaren – Eigenschaften, die sich hervorragend eignen, um einen Selbsttest hoher Qualität mit geringsten Ansprüchen in bezug auf Siliziumfläche zu integrieren.

Die praktische Anwendbarkeit der besonderen Chiffren-Eigenschaften im Zusammenhang mit einem effizienten Selbsttest wird anhand einer VLSI-Implementierung des neuen Verschlüsselungsverfahrens IDEA demonstriert. VINCI, der neue Baustein hoher Komplexität, ist mit zwei Arten von Selbsttest ausgestattet, um den Forderungen existierender Sicherheitsnormen zu genügen: mit einem *off line* Test, der exklusiv die gesamte Chiphardware einbezieht, um eine hohe Fehlerüberdeckung zu erreichen, und mit einem *on line* Selbsttest, der im laufenden Betrieb, also auch während des *off line* Selbsttests, ständig sämtliche Ver- oder Entschlüsselungen kontrolliert und allfällige Ausfälle ohne Verzögerung meldet.

Das Konzept der Signaturanalyse erlaubt eine höchst effiziente Auswertung von Selbsttestergebnissen. Allerdings geht bei der Kompression von Testresultaten zu einer Signatur die Lokalisierbarkeit von Fehlern meist verloren. Bei VINCI ist die Lokalisierbarkeit von Fehlern jedoch durch die ständige Überwachung aller Zwischenwerte, die nicht zuletzt durch Einbeziehung des *on line* Selbsttests erreicht wird, weitgehend aufrecht erhalten worden.