Rekonstruktion integrierter Schaltungen mittels Degate

Martin Schobert
martin@degate.org

21. Oktober 2011

Zusammenfassung

Die Diplomarbeit „Softwaregestütztes Reverse-Engineering von Logik-Gattern in integrierten Schaltkreisen“ beschreibt einen semi-automatischen Arbeitsprozess, mit dem digitale Logikschaltkreise in einem Chip rekonstruiert werden können. Dieser Prozess ist notwendig, um Aussagen über geheimgehaltene Sicherheitsmechanismen, z. B. in Smartcard-Chips, treffen zu können. In der Open-Source-Software Degate ist dieser Arbeitsprozess implementiert. Als Eingabedaten dienen mikroskopische Aufnahmen der einzelnen Chipebenen. Mittels Degate können die darin enthaltenen Informationen interaktiv rekonstruiert und in Form von Hardwarebeschreibungssprachen exportiert werden. Damit lässt sich eine Schaltung analysieren, simulieren und erneut synthetisieren.

1 Motivation

Auf dem Hardwaremarkt existieren zahlreiche Anwendungen, z.B. in Form integrierter Schaltkreise, die geheimgehaltene Verschlüsselungsverfahren einsetzen. Oft besteht für Forscher im Bereich der IT-Sicherheit keine Möglichkeit diese Verschlüsselungsverfahren zu untersuchen, da die Verfahren nicht bekannt sind. Weil Halbleiterstrukturen ohne Weiteres nicht sichtbar sind, wird entsprechenden Hardwarerealisierungen ein Sicherheitsniveau unterstellt, welches nur mit hohem Aufwand analysierbar sei. Verschiedene Veröffentlichungen in den letzten Jahren haben jedoch gezeigt, dass diese Annahme nicht statthaft ist.

Der Schlüssel zur Bewältigung der Komplexität einer IC-Analyse liegt in Software, die den Prozess soweit wie möglich automatisiert. International marktführende Firmen, die kommerziell Reverse-Engineering im Halbleitersektor betreiben, haben eigene, proprietäre Softwarewerkzeuge entwickelt. Deren Werkzeuge sind für die Allgemeinheit nicht oder nur zu sehr hohen Lizenzkosten verfügbar. Im Open-Source-Bereich gab es bisher keine Software, mit der man anhand von Bildmaterial integrierte Schaltungen rekonstruieren kann und die den Reverse-Engineering-Prozess maßgeblich unterstützt. Frei verfügbare Software kann Forschern helfen, einen niederschwelligen Einstieg in das Reverse-Engineering von Schaltkreisen zu finden. Forscher können Degate kostenfrei verwenden und Funktionen erweitern bzw. an eigene Bedürfnisse anpassen.

Ebenfalls ermöglicht eine Rekonstruktion proprietärer Verfahren, diese für Open-Source-Software oder für offene Hardwaresysteme nachzuimplementieren. So sind beispielsweise einige gängige Kommu-

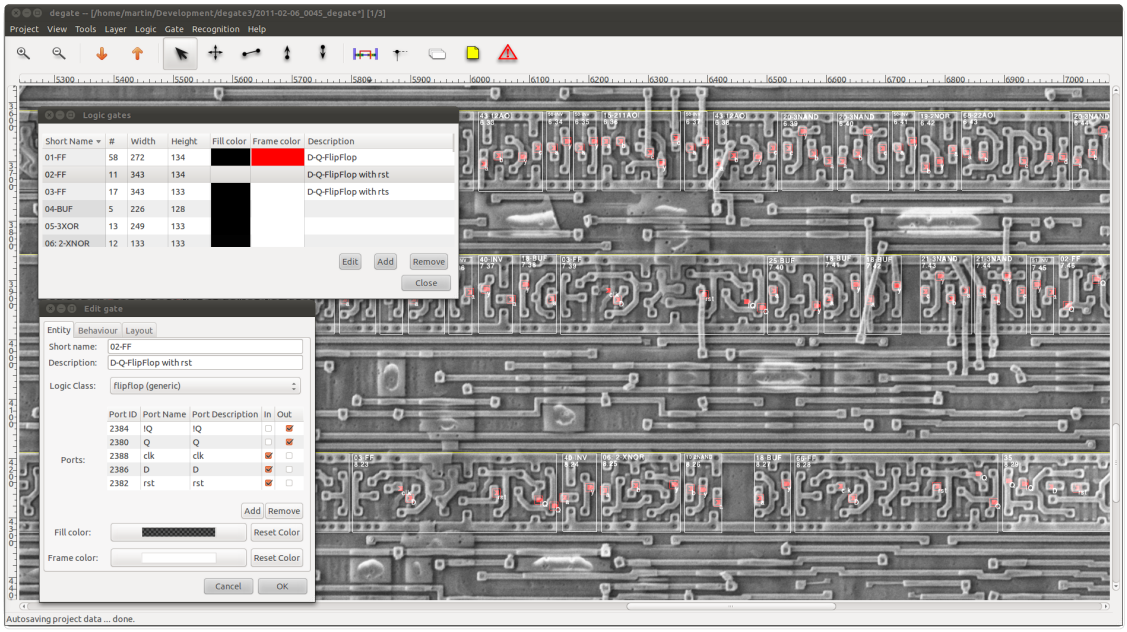

Abbildung 1: Bildschirmfoto der interaktiven Benutzeroberfläche

nikationsstandards nicht vollständig publiziert – u. A. die Verschlüsselungsverfahren von GPRS (1 und 2) und des Schnurlostelefonstandards DECT.

2 Auswirkungen

Degate wurde bereits für mehrere Reverse-Engineering-Projekte eingesetzt: Das lange Zeit geheimgehaltene Verschlüsselungsverfahren des RFID-Systems Legic Prime, welches in z. B. in Zugangskontrollsystemen Verwendung findet, wurde mit Degate rekonstruiert. Die Rekonstruktion ergab, dass das Legic-Prime-Verfahren keinen Schutz bietet. Durch die Kenntnis des Verschlüsselungsverfahrens war es möglich, dass Kommunikationsprotokoll von Legic Prime zu analysieren und es in die Open-Source-Firmware des Proxmark-Projektes[1] zu integrieren. Dadurch kann die Proxmark-Hardware mittlerweile auch mit Transpondern vom Typ Legic Prime kommunizieren.

Ferner wurde Degate verwendet, um den DECT Standard Cipher zu rekonstruieren, welcher Kommunikationsdaten zwischen Schnurlostelefonen und der Basisstation verschlüsselt. Zuletzt haben Forscher mittels Degate die proprietäre Speicherverschlüsselung einer Infineon SLE66-Smartcard rekonstruiert[2].

3 Lizenz und Publikation

Die Software Degate steht unter der GNU Public License Version 3 und ist im Internet[3] veröffentlicht. Die Diplomarbeit ist unter der Creative-Commons-Lizenz auf der Projektwebseite publiziert[4].

[1] http://www.proxmark.org
[2] Heise: Open-Source-Tool ermöglicht Sicherheitstests von Chipkarten, http://heise.de/-1344069, 15.09.2011
[3] http://github.com/nitram2342/degate
[4] http://degate.org/documentation/diplomarbeit.pdf