

---

# STUDIENARBEIT:

# REVERSE-ENGINEERING VON

# LOGIK-GATTERN IN INTEGRIERTEN

# SCHALTKREISEN

---



Humboldt-Universität zu Berlin  
Mathematisch-Naturwissenschaftliche Fakultät II  
Institut für Informatik

Martin Schobert  
Betreuer: Dipl.-Inf Henryk Plötz, Prof. Dr. rer. nat. Jens-Peter Redlich  
März 2010

# *Inhaltsverzeichnis*

<b>1 Einleitung</b>	<b>1</b>
1.1 Motivation . . . . .	2
1.2 Der Arbeitsablauf im Überblick . . . . .	4
1.3 Thematische Einschränkung . . . . .	4
<b>2 Aufwand und Kosten</b>	<b>6</b>
<b>3 Entkapselung</b>	<b>7</b>
3.1 Aufquellen von Thermoplasten . . . . .	7
3.2 Chip-Entkapselung in der Industrie . . . . .	8
3.3 Chip-Entkapselung mittels Kolophonium . . . . .	10
<b>4 Abtragung einzelner Schichten</b>	<b>13</b>
<b>5 Bildgewinnung</b>	<b>15</b>
5.1 Mikroskopierung . . . . .	15
5.2 Zusammenfügen und Nachbearbeitung der Bilddaten . . . . .	17
<b>6 Analyse von Integrierten Schaltkreisen anhand von Bilddaten</b>	<b>19</b>
6.1 Feldeffekt-Transistoren . . . . .	19
6.2 Komplementäre Verwendung von FETs . . . . .	21
6.3 Aufbau von Logik-Gattern . . . . .	23
6.4 Wiederverwendung von Logik-Gattern . . . . .	31
6.5 Gezielte Suche . . . . .	33
<b>7 Fazit</b>	<b>36</b>

<b>Literatur- und Quellenverzeichnis</b>	<b>37</b>
<b>Abbildungsverzeichnis</b>	<b>41</b>
<b>A Lizenzbedingungen</b>	<b>42</b>

---

# *1 Einleitung*

Im Dezember 2007 veröffentlichten Karsten Nohl und Henryk Plötz ihre Forschungsergebnisse über die Sicherheit des RFID-Systems Mifare Classic auf dem 24. Chaos Communication Congress [NP07b; NP07a]. Sie gewannen ihre Erkenntnisse über die Funktionsweise des Algorithmus Crypto1 durch Reverse-Engineering von Protokolldaten und der Integrierten Schaltkreise, die auf RFID-Transpondern vom Typ Mifare Classic eingebettet sind. Die im Vortrag dargestellten Erkenntnisse zeigen, dass für eine Analyse einfacher Schaltkreise „Küchentechnik“ genügt. Crypto1 wird unter anderem für Zugangskontrollen und Bezahlsysteme verwendet.

Der Bedarf an professioneller IC-Analyse ist groß. Jeder Hersteller von Integrierten Schaltkreisen benötigt dafür entsprechende Verfahren. Die Laboratorien verfügen über Werkzeuge, z.B. um festzustellen warum Prototypen nicht funktionieren. Auch andere Anwendungszwecken dienen diese Analysen. Die folgenden Beispiele sollen dies zeigen.

Einige Firmen, z.B. die kanadische Firma Chipworks [Chi], untersuchen Halbleiterbausteine und Mikroelektronik, um Auftraggeber über Technologien der Konkurrenz in Kenntnis zu setzen. Im Falle von Patentverletzungen haben die Auftraggeber damit Material in der Hand, um gegen die Konkurrenz juristisch vorzugehen. Detaillierte Informationen über Technologien helfen, Produkte unter Einsparung eigener Forschungsmittel zu verbessern.

Im Bereich der „nationalen Sicherheit“ besteht ebenfalls Bedarf an der Analyse Integrierter Schaltkreise. Militärische, nachrichtendienstliche und diplomatische Einrichtungen, die beispielsweise Chiffriertechnik oder hochtechnische Waffensysteme aus anderen Ländern einkaufen, haben ein Interesse an „hintertürfreier“ Hardware. Dahingehende Modifikationen können analysiert werden, auch wenn das einen größeren Aufwand darstellt. [Ade08; Str94; Kin+08]

Ein Projekt, dass die U.S.-amerikanische Defense Logistics Agency finanziert, ist das Advanced Microcircuit Emulation Program. Dabei geht es u. A. darum, Baupläne aus undokumentierten anwendungsspezifischen Schaltkreisen (ASICs) zurückzugewinnen. Anhand derer können Schaltkreise nachgebaut werden, z.B. weil der ursprüngliche Hersteller nicht mehr existiert. [Ave+02]

Den genannten Beispielen ist gemein, dass hinter den Programmen finanzstarke Institutionen stehen. Diese können Integrierte Schaltkreise analysieren – zur Fehlersuche, um etwas über die Fähigkeiten der Konkurrenz zu erfahren, um Manipulationen festzu-

stellen oder „auszuschließen“, um Sicherheitslöcher aufzuspüren, um geheime Chiffriermethoden aus Speichern auszulesen und dergleichen. Je nach Fragestellung kosten kommerzielle Chipanalysen fünf- bis sechsstellige Beträge.

Auf der anderen Seite können IC-Analysen mit einfachen Mitteln durchgeführt werden. Beispielsweise war das Reverse Engineering von Crypto1 ohne ein teures Labor mit einem zusammengerechneten Zeitaufwand in weniger als zwei Mannmonaten möglich. Mit einem fiktiven Tagessatz von 500 Euro wäre der Verschlüsselungsalgorithmus für etwa 30 Tausend Euro Kosten extrahiert. Mit den Erfahrungen aus dem Projekt wäre ein erneutes Reverse-Engineering von Crypto1 sogar in wenigen Tagen ohne nennenswerte Kosten möglich.

Im Rahmen des Mifare-Hacks entstand der Wunsch, das Reverse-Engineering von Integrierten Schaltkreisen werkzeuggestützt zu vereinfachen. Zu diesem Zweck wird eine Software namens degate entwickelt. Diese Software soll Gegenstand einer später zu schreibenden Diplomarbeit werden.

Diese Studienarbeit soll die Hintergründe des Reverse-Engineerings von Integrierten Schaltkreisen beleuchten und beschreiben wie man Schaltfunktionen von Logikgattern aus ICs rekonstruieren kann.

### 1.1 Motivation

Die Sicherheit des Verschlüsselungsverfahrens Crypto1 basiert auf dem Prinzip des „security by obscurity“, d.h. auf der Geheimhaltung des Verfahrens und weniger auf der Geheimhaltung der Schlüssel. Damit verletzt es Kerckhoffs’ Prinzip, welches besagt, dass die Sicherheit eines Systems nicht auf der Geheimhaltung des Verfahrens basieren darf. Üblicherweise ist die Geheimhaltung eines Verfahrens schwieriger als die von Schlüsseln zu gewährleisten. Im Falle einer Offenlegung lässt sich ein Verfahren nicht so leicht austauschen wie Chiffriermethoden. Das Kerckhoff’sche Prinzip wurde bereits 1883 aufgestellt. Allerdings wird es in der Praxis oftmals ignoriert. [Sch97, S. 8]

Wären regelmäßig hardwareimplementierte Verschlüsselungsverfahren einer Low-Cost-Analyse unterzogen, so müßte sich zwangsläufig das Sicherheitsniveau der Verfahren erhöhen. Kryptosysteme, deren Umgehung  $n$  Euro kosten, können keine Geheimnisse schützen, deren Umgehung  $n$  Euro Gewinn einbringt. Wenn die Umgehungskosten sinken, genügt es nicht mehr, ein potentiell knackbares Verschlüsselungsverfahren zu verwenden, dessen Sicherheit darin besteht, dass es niemand kennt.

Neben dem Verfahren Mifare Classic sind andere Verschlüsselungsverfahren von der Problematik des „Security by obscurity“ betroffen. Dazu zählen beispielsweise die proprietären RFID-System Legic prime und Felica sowie das Verschlüsselungsverfahren DECT Standard Cipher (DSC), das Kommunikation zwischen „Schnurlosetelefonen“ und deren Basisstation gegen unbefugtes Abhören sichern soll. Ebenfalls ist der Eurochip-Algorithmus geheim. Dieser ist ein Challenge-Response-Verfahren, mit dem Kartentelefone die Echtheit der Telefonkarten verifizieren. Der Algorithmus wurde in den 90er Jahren eingeführt, nachdem es zu viele Betrugsfälle mit Telefonkarten-Emulatoren gab. [Spi95]

Legic prime und der DSC sind seit dem 26. Chaos Communication Congress der Öffentlichkeit bekannt und gelten mittlerweile als unsicher. Die Verschlüsselungsalgorithmen wurden mittels Firmware-, Protokoll- und Chip-Reverse-Engineering ermittelt. [NP09; Tew09]

Das Enthüllen von proprietären Verschlüsselungsalgorithmen ist die hauptsächliche Motivation dafür, ein Verfahren zu entwickeln, mit der sich kostengünstig Analysen von Chips durchführen lassen. Kostengünstig bedeutet, dass für die Anschaffung aller notwendigen Geräte, keine höheren Kosten als etwa 1.000 bis 10.000 Euro entstehen.

Zahlreiche IT-sicherheitsrelevante Themen sind seit den 80er Jahren in den Fokus der zivilen Forschung gerückt, beispielsweise Betriebssysteme, Server-Software und Kryptographie. Dies hat maßgeblich zur Verbesserung von Sicherheitsstandards beigetragen. Sicherheitsstandards im Bereich Integrierter Schaltungen werden zwar ebenfalls besser, insbesondere bei Smartcards, es gibt aber nach wie vor fast keine öffentliche Sicherheitsforschung im Bereich Integrierter Schaltkreise. Dies ist insbesondere daran feststellbar, dass es nur sehr wenige Papers gibt, die speziell Reverse-Engineering von (Logik-)Schaltkreisen behandeln und diese dann defacto keine Details preisgeben.

Entwickler sicherheitsrelevanter Systeme überlegen sich zumeist, gegen welche Kategorien von Angreifern sie das System schützen wollen. Diese Kategorien orientieren sich i.d.R. an potentiellen Budgetgrößen, die den Angreifern zur Verfügung stehen. Diese Studienarbeit möchte darauf hinweisen, dass die Bewertung von Budgetgrößen ggf. kritisch betrachtet werden sollte.

### 1.2 *Der Arbeitsablauf im Überblick*

Ausgangspunkt für die Untersuchung von Integrierten Schaltkreisen sind Chips. Diese müssen zunächst entkapselt werden, um ein Plättchen aus Halbleitermaterial (engl. *die*) zu erhalten. ICs bestehen aus mehreren Schichten. Diese Schichten müssen Stück für Stück entfernt werden, um darunterliegende Schichten freizulegen. Jede Schicht wird fotografiert. Dabei entstehende Teilbilder werden zusammengesetzt. Die Fotografien der einzelnen Schichten müssen in Übereinstimmung gebracht werden, so dass man später den Verlauf von Leiterbahnen über mehrere Schichten hinweg nachvollziehen kann.

Diese Studienarbeit geht davon aus, das ein Chip-Layout überwiegend auf Standardzellen basiert. Diese Annahme ist statthaft, denn sie trifft auf den überwiegenden Teil von anwendungsspezifischen ICs zu. Zunächst wird die Bildrepräsentation von Standardzellen ermittelt. Die verschiedenen Instanzen von Standardzellen werden identifiziert. Anschließend wird deren Verdrahtung nachvollzogen. Man muss die Schaltfunktion der Standardzelltypen analysieren. Diese ergibt sich, wenn man die Verschaltung der einzelnen Transistoren auswertet.

Wenn diese Informationen ermittelt sind, kann man sich der Analyse auf “höherer Ebene” zuwenden. Bei der eingangs genannten Motivation, proprietäre Verschlüsselungsverfahren zu extrahieren, ist nie ein vollständiges Reverse-Engineering des gesamten Chips notwendig. Es genügt, sich auf relevante Bereiche zu konzentrieren. Diese Studienarbeit geht ebenfalls darauf ein, wie man diese relevanten Bereiche identifizieren kann.

### 1.3 *Thematische Einschränkung*

Das Reverse-Engineering von Integrierten Schaltkreisen ist ein beliebig komplexes Thema und umfasst konkrete Technologieaufklärung, etwa das Design von Flashspeichern, das optische Auslesen von Masken-ROMs, den vollständigen Nachbau von ICs oder das Auslesen von Speicherinhalten mittels Microprobing. Ebenfalls gehören invasive Angriffe in das Themenfeld, bei denen Strukturen auf einem Chip gezielt modifiziert werden, z.B. um Sicherungen zu deaktivieren, die ein Auslesen von Speichern verhindern sollen.

### ***1.3. THEMATISCHE EINSCHRÄNKUNG***

---

Der Schwerpunkt dieser Studienarbeit ist die statische Analyse von CMOS-basierten (digitalen) Logik-Schaltkreisen mit der Motivation, proprietäre Verschlüsselungsverfahren zu rekonstruieren. Die Analyse soll mit geringem Budget möglich sein.

---

## 2 Aufwand und Kosten

Der Reverse-Engineering-Prozess lässt sich grob in drei Abschnitte unterteilen: die Entkapselung, die Bildgewinnung und die Analyse der Schaltkreise. Jeder dieser Schritte kann bei externen Dienstleistern in Auftrag gegeben werden. Während eine Chip-Entkapselung im Labor im Wesentlichen eine Finanzierung des reinen Arbeitsaufwandes darstellt, sind darüber hinausgehende Analysen bei spezialisierten Firmen zumeist teuer. Diese Kosten können eingespart werden, wenn man die Analyse selbst durchführt.

Chip (analysierter Teil)	Anzahl Zell-Typen	Anzahl Zellen	Verbindungen
NXP Mifare Classic	40-70	600	1500
Logic prime	25	600	2100
DSC im SC14421CVF	26	300	1000

Tabelle 2.1: Komplexität des Reverse-Engineerings

Tabelle 2.1 gibt einen Überblick über die Komplexität des Reverse-Engineerings ausgewählter Integrierter Schaltkreise, bei der jeweils das Verschlüsselungsverfahren extrahiert wurde. Der Zeitaufwand für das Ermitteln der Zelltypen und jeweils deren Funktion beträgt etwa drei Tage und ist überwiegend von der Übung des Analysten abhängig. 300 bis 600 Platzierungen von Standardzellen kann man in maximal einer Woche halbautomatisiert ausfindig machen. Das manuelle Nachvollziehen von Leiterbahnen ist der aufwendigste Teil und beträgt ein bis zwei Wochen. Die letzten beiden zeitintensiven Schritte können schneller umgesetzt werden, wenn dereren Automatisierungsgrad höher ist. Eine weitere Verkürzung der Gesamtdauer ist durch kollaboratives Reverse-Engineering zu erreichen.

Die in der Einleitung veranschlagten 1.000 bis 10.000 Euro entfallen im Wesentlichen auf die Posten Mikroskop und Poliermaschine. Dabei handelt es sich um Einmalkosten, die eventuell vermeidbar sind. Poliermaschinen findet man z.B. in Geologie- oder Optik-Instituten, Mikroskope mit Digitalkameras in nahezu jeder materialwissenschaftlichen Einrichtung. Ein Labor mit Rauchabzug ist für die chemische Entkapselung mit konzentrierten Säuren notwendig. Wenn man ein Auftragslabor für die Entkapselung zur Hand hat, benötigt man dies nicht.

---

### 3 Entkapselung

Integrierte Schaltkreise werden je nach Anwendungsfall in verschiedenen Gehäusematerialien verpackt. Meistens handelt es sich um Epoxidverbindungen, Keramik oder Metall. Die hier beschriebene Methode bezieht sich auf die Entfernung von Epoxidverbindungen.

Epoxidverbindungen gehören zu den Duroplasten und zeichnen sich durch hohe chemische und mechanische Beständigkeit aus. Epoxide lassen sich nicht aufquellen und hauptsächlich nur durch aggressive Säuren oxidativ zersetzen. Der Anteil an Epoxiden in diesen Kunststoffgehäusen beträgt aber lediglich 20 bis 25 %. Mit zwei Dritteln bilden Quarzmehl und Glasfasern den überwiegenden Anteil. [HK02, S. 7]

In der Literatur werden zwei Fälle unterschieden: Mitunter wird nicht das gesamte Gehäuse entfernt, sondern lediglich das Gehäusematerial, welches über dem Siliziumplättchen ist, wenn die Funktionalität des Chips erhalten werden soll, insbesondere um den IC noch in einer Schaltung zu betreiben. Der andere Fall ist die Komplettentfernung des Gehäusematerials. Dieser Weg wird hier eingeschlagen. Durch das Herunterpolieren der einzelnen Schichten wird der Chip zerstört. Der Nachteil besteht darin, dass man die Bedeutung der *bond pads*, d.h. der Flächen auf dem Halbleiterplättchen, an denen die Leiterbahnen von den Pins des Chips befestigt sind, ggf. manuell ermitteln werden müssen.

Bei einer chemischen Entkapselung sollten mit jedem Durchgang mehrere Chips des gleichen Typs behandelt werden, damit bei misslungenem Politurvorgang noch Ersatzchips übrig sind.

Eine nahezu vollständige Beschreibung verschiedener Entkapselungsverfahren gibt Friedrich Beck. [Bec98]

#### 3.1 Aufquellen von Thermoplasten

Vergleichsweise ungefährlich ist das Aufquellen von Thermoplasten. Hersteller von Chipkarten (Telefonkarten, Mensa-Karten, Zugangskarten, ...) benutzen Thermoplaste, um den Chip einzubetten. Thermoplaste lassen sich mit Aceton aus dem Baumarkt aufquellen. Der Prozess dauert etwa 10 bis 20 Minuten. Das Material verliert dabei an Stabilität. Der Chip fällt dann heraus.

In Thermoplaste eingebettete Chips sind meist in einer weiteren Ummantelung aus Epoxid verpackt. In diesem Fall ist eine Behandlung mit Säuren unumgänglich.



Abbildung 3.1: Entfernen von Thermoplasten mittels Aceton

## 3.2 Chip-Entkapselung in der Industrie

Für die Entfernung von Epoxiden kann rauchende Salpetersäure [KK99] [Sko05] oder konzentrierte Schwefelsäure [Che08] verwendet werden. In einigen Anwendungsfällen wird eine Mischung aus konzentrierter Salpetersäure und konzentrierter Schwefelsäure benutzt. Das soll für einige Verpackungsmaterialien die Reaktion beschleunigen und das Silber in den Bond-Pads schonen.

Nick Chernyy beschreibt seine Methode in [Che08] wie folgt. Die Chips werden in ein Becherglas (40 ml) gelegt. Konzentrierte Schwefelsäure wird dazugegeben bis die Chips vollständig bedeckt sind. Erste Lösungserscheinungen sind sofort bemerkbar. Das Becherglas wird unter einem Rauchabzug erhitzt, um die Aktivität der Säure zu erhöhen. Die Temperatur ist unkritisch, etwa 60 °C bis 90 °C genügen. Die Siliziumscheibchen im Chip vertragen viel höhere Temperaturen und sind mit der Säuremethode praktisch nicht zerstörbar. Nach etwa 20 Minuten sollte der Kunststoffanteil

### **3.2. CHIP-ENTKAPSELUNG IN DER INDUSTRIE**

---

zersetzt sein. Er bleibt als mehr oder weniger schwarze Flüssigkeit bzw. als Schaum im Becherglas zurück.

In ein zweites Becherglas (500 ml) werden 400 ml Wasser gegeben. Der Inhalt des ersten Becherglases wird vorsichtig in das zweite Becherglas gefüllt. Das Mischen von Wasser und Säuren ist bekanntlich exotherm und führt bei Fehlanwendung zu Unfällen!

In ein drittes Becherglas (1000 ml) werden 400 ml Wasser gegeben. Der Inhalt des 500 ml-Becherglases wird vorsichtig in das Literglas gegossen, so dass die Siliziumplättchen mit anhaftenden Metallteilen im 500 ml-Becherglas verbleiben. Die Siliziumplättchen werden mit Wasser gereinigt, so dass keine Säure und kein Schmutz mehr anhaftet.

In einigen Fällen kann es passieren, dass die Kunststoffummantelung nicht vollständig entfernt ist. Dann ist eine erneute Behandlung mit Säure notwendig. Saubere Ergebnisse ergeben sich, wenn statt Schwefelsäure konzentrierte Salpetersäure verwendet wird. Die Rückstände sind dann nicht so trübe, dass die Chips im Becherglas nicht mehr sichtbar sind. Mit auf 90°C erhitzter Salpetersäure dauert die Entkapselung nur etwa fünf Minuten.

Das Experiment wurde mit rauchender Salpetersäure (mehr als 99,5%ige Konzentration) in einem Labor in Auftrag gegeben, um in Epoxidmasse eingeschlossene Chips aus einem RFID-Transponder zu entkapseln. Das Labor berichtete, dass die Reaktion bei Raumtemperatur sofort einsetzte und binnen kürzester Zeit abgeschlossen war.

Wenn das Gehäuse entfernt ist, ist noch eine Behandlung im Ultraschallbad notwendig, um eventuelle Anhaftungen zu entfernen. Dazu stellt man ein mit Aceton gefülltes Becherglas inklusive Chips in einen Ultraschallreiniger. Werden mehrere Chips gleichzeitig gereinigt, sollte die Reinigung nicht länger als eine halbe Minute andauern. Die Chips könnten aneinander reiben und gegenseitig die Oberflächen zerkratzen. Bei Einzelbehandlung dauert die Ultraschallreinigung drei bis fünf Minuten.

Ist keine geeignete Arbeitsumgebung vorhanden, unterlässt man die Entkapselung. Der Umgang mit konzentrierten Säuren ist gefährlich. Der Bedarf an einer geeigneten Arbeitsumgebung ist nicht aus Sicht der Bequemlichkeit zu verstehen. Wenn die Arbeitsumgebung nicht geeignet ist, entstehen zusätzliche Gefahren. Die genannten Säuren sind Standardchemikalien im Labor. Laboratorien verfügen über geeignete Arbeitsumgebungen. Eine Entkapselung im Auftragslabor ist preiswert verglichen damit, dass die Säure sonst selbst beschafft, transportiert, angewendet, gelagert und entsorgt

werden müsste. Für weniger als hundert Euro kann man Laboratorien mit der Chip-Entkapselungen beauftragen.

Im Ergebnis erhält man den Chip als Plättchen (engl. *die*), an dem meistens noch die Verbindungsdrähte zur Außenwelt hängen. Kleine Chips haben eine Abmessung von etwa einem Quadratmillimeter und eine Stärke von wenigen zehntel Millimetern.

### ***3.3 Chip-Entkapselung mittels Kolophonium***

Kolophonium nennt man den Rückstand des Baumharzes von Kiefern, bei dem Wasser und Terpentinöl abdestilliert wurden. Der Aggregatzustand von Kolophonium ist fest. Kolophonium selbst ist ungiftig, wenngleich dessen Dämpfe Allergien auslösen können. Kolophonium wird als z.B. als Flussmittel beim Löten, von Musikern zum Behandeln von Geigenbögen oder Gitarrensaiten und von Bergsteigern zur Erhöhung der Haftreibung verwendet. Kolophonium ist billig, leicht zu beschaffen, zu lagern, zu entsorgen und anzuwenden. Es ist ideal, um Chip-Entkapselungen durchzuführen, die keinen Laborstandards genügen.



Abbildung 3.2: IC-Entkapselung durch Kochen in Kolophonium

### 3.3. CHIP-ENTKAPSELUNG MITTELS KOLOPHONIUM

Friedrich Beck beschreibt eine Möglichkeit zum Enkapseln mittels Kolophonium: „Zum Öffnen wird das Bauteil im Drahtkörbchen in das auf 320 - 360 °C erwärmte Kolophonium getaucht, bis der Chip völlig freiliegt (5 - 10 Minuten); anschließend lässt sich mit trockenem Aceton das anhaftende Kolophonium entfernen.“ [Bec98, S. 19, 20] Beck schreibt ferner, dass die Kolophoniumdämpfe Rückstände im Abzug bilden, diesen verunreinigen und schwer zu entfernen sind. Dies sei der Grund, warum das Verfahren selten angewandt wird. Tatsächlich wird dieses Verfahren in aktuellen Quellen nicht mehr beschrieben. Die Zeitangabe von Herrn Beck konnte im Experiment nicht bestätigt werden. Tatsächlich sind die Kochzeiten sehr viel höher. Experimentell konnte jedoch bestätigt werden, dass das Verfahren prinzipiell funktioniert. [Sch10]

Zum Entkapseln nimmt man ein breites, langes und temperaturbeständiges Reagenzglas, füllt es mit Kolophonium und den Chips. Der Inhalt wird abhängig von der Chipgröße 30 bis 150 Minuten gekocht (Abbildung 3.2). Da das Halbleiterplättchen hohe Temperaturen verträgt, ist die Kochzeit unkritisch.



Abbildung 3.3: Reinigung der Halbleiterplättchen im Ultraschallreiniger

Den Inhalt des Reagenzglases lässt man anschließend auf Zimmertemperatur abkühlen, so dass das Kolophonium erstarrt. Man gibt dann etwa 10 ml Aceton oder Isopropanol (technische Reinheit genügt) in das Reagenzglas. Diese Chemikalien lösen das Kolophonium. Dieser Vorgang lässt sich durch Ultraschalleinwirkung erheblich beschleunigen.

### **3.3. CHIP-ENTKAPSELUNG MITTELS KOLOPHONIUM**

---

Den gelösten Reagenzglasinhalt filtriert man. Das Halbleiterplättchen bleibt fast immer im Reagenzglas haften. Mittels mehrfachem Nachspülen mit Aceton oder mit einem Holzstäbchen kann man das Plättchen vorsichtig aus dem Reagenzglas befördern.

Anschliessend sollte das Plättchen in ein oder mehreren Reinigungsgängen von anhaftenden Kolophonium- und Expoxid-Resten mittels Ultraschall befreit werden.

Bei dieser Form der Chip-Entkapselung entfallen die Probleme, wie sie sich im Umgang mit konzentrierten Säuren ergeben. Dennoch ist davon auszugehen, dass der Entkapselungsprozess gesundheitsgefährdend ist. Die Verwendung von Schutzbrillen ist hier unumgänglich, denn Kolophonium neigt zum Spritzen.

Mit etwa 40 Prozent ist Abietinsäure der hier wirksame Hauptbestandteil von Kolophonium. Abietinsäure hat ähnliche Konsistenzeigenschaften wie Kolophonium. Sie kann bei ausgewählten Chemikalienhändlern in Reinform erworben werden. Damit ließe sich der Entkapselungsprozess beschleunigen, was mangels an Privatpersonen liefernden Händlern experimentell bisher nicht bestätigt werden konnte.

---

## 4 Abtragung einzelner Schichten

Integrierte Schaltkreise sind mehrschichtig aufgebaut. Von jeder einzelnen Schicht werden Fotos aufgenommen. Dazu muss jede einzelne Schicht des Chips entfernt werden. Der Integrierte Schaltkreis besteht hauptsächlich aus Siliziumdioxid. Einzelne Schichten lassen sich chemisch oder mechanisch entfernen.

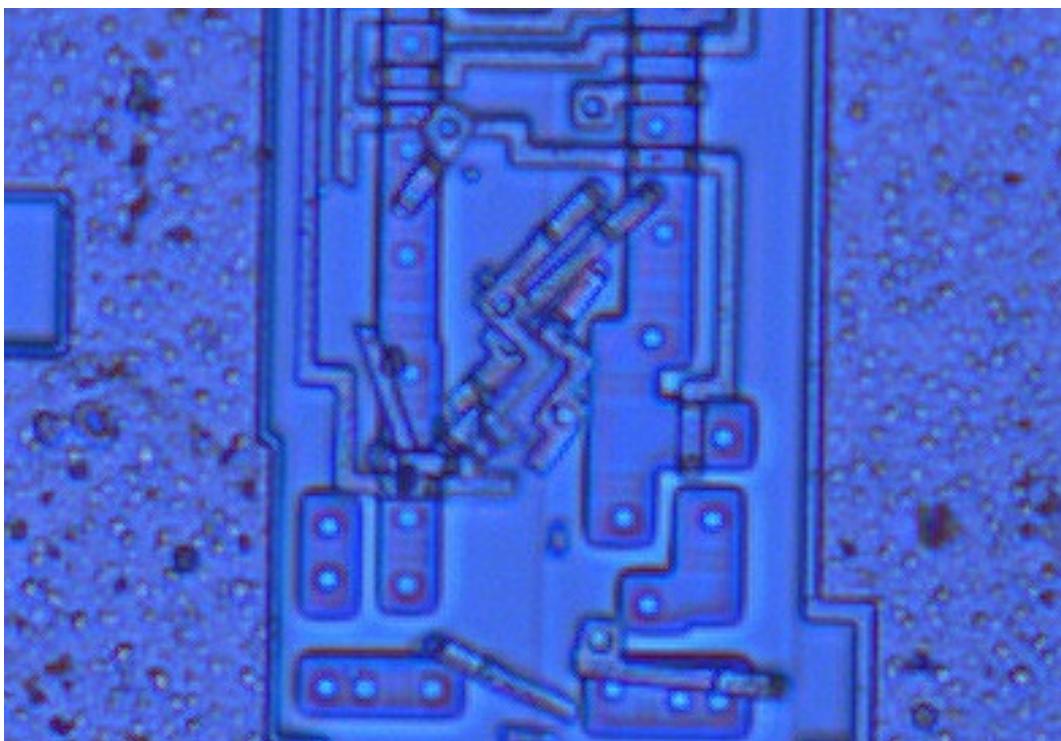


Abbildung 4.1: Unterätzung (Foto: Jan Krissler)

Die einzige Säure, die Siliziumdioxid angreift, ist die Flusssäure (Fluorwasserstoffsäure, HF). Flusssäure ist geeignet, um die Transistorschicht freizulegen. Der Nachteil besteht darin, dass Flusssäure auf den höheren Schichten zum Unterätzen neigt (Abbildung 4.1). Da Flusssäure schwierig zu handhaben ist, wird hier die mechanische Entfernung von Chip-Ebenen bevorzugt.

Für das Polieren von Oberflächen gibt es spezielle Poliermaschinen. Beispielsweise das Modell Phoenix 4000 der Firma Buehler GmbH (Abbildung 4.2). [Bue08] Mit mehreren tausend Euro ist das Gerät entsprechend teuer. Vergleichbare Geräte findet man an Universitäten in Geologie-Instituten.

Für den Poliervorgang benötigt man etwa 20 ml Poliersuspension mit einer Korngröße von  $0,1 \mu\text{m}$ .

Der Chip wird mit seiner Grundfläche auf eine Art Stempel geklebt. Dabei muss darauf geachtet werden, dass die Chipoberfläche parallel zur Polieroberfläche verläuft. An-

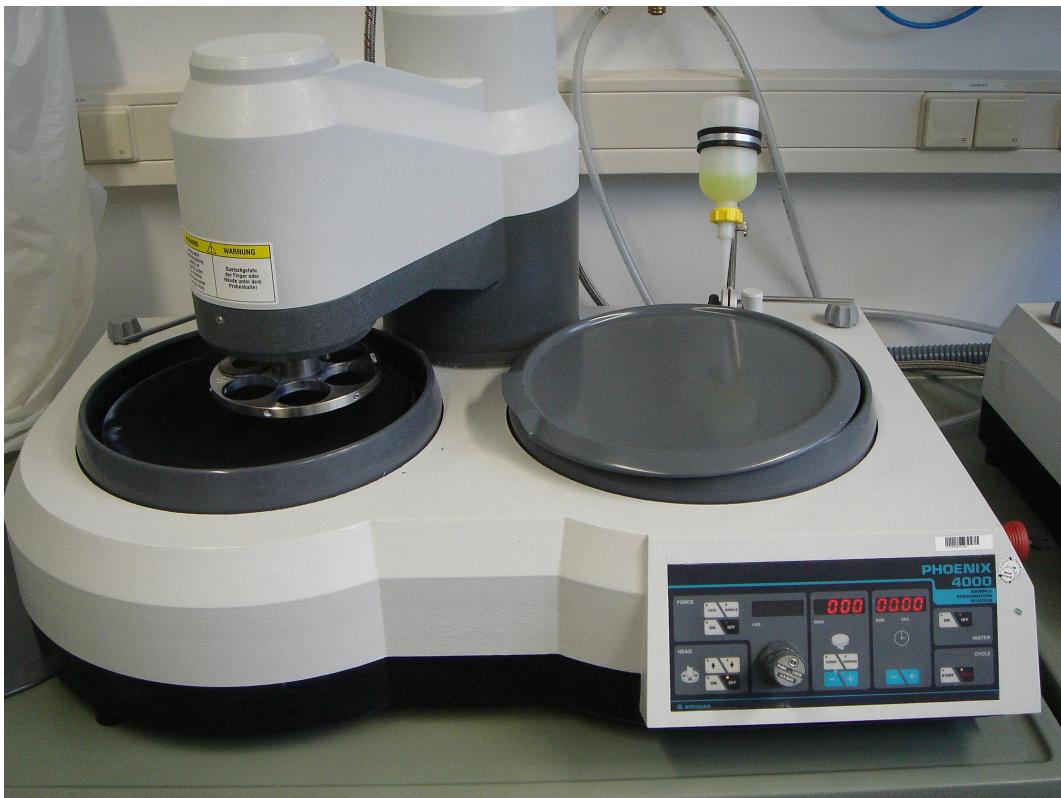


Abbildung 4.2: Poliermaschine Phoenix 4000 der Firma Buehler (Foto: Jan Krissler)

derenfalls ist der Materialabtrag beim Polieren unterschiedlich stark (vgl. Abbildung 6.6).

Es ist möglich, den Vorgang komplett manuell durchzuführen. Für das Polieren von Glasfaserkabelenden bietet der Fachhandel feinstes Polierpapier. Das ist zwar kostengünstig, der Nachteil besteht jedoch darin, dass sich Verschmierungen auf dem Chip bilden können.

Der Fortschritt des Polievorgangs muss regelmäßig unter einem Mikroskop kontrolliert werden. Wenn der Materialabtrag unterschiedlich stark ist, gibt es zwei Möglichkeiten. Entweder das Bildmaterial wird durch manuelle Nachbearbeitung korrigiert oder der Polievorgang wird mit einem weiteren Chip erneut gestartet.

---

## 5 Bildgewinnung

### 5.1 Mikroskopierung

Für die Aufnahme der Bilddaten benötigt man ein Mikroskop mit einem Kameramodul. Derartige Geräte kann man zwar für wenig Geld erwerben, jedoch ist nicht jedes Gerät geeignet. Für die Aufnahme der Bilddaten des Chiptyps Mifare Classic wurde ein Labormikroskop vom Typ Olympus BX61 (Abbildung 5.1) verwendet. [Oly08]



Abbildung 5.1: Mikroskop (Foto: Jan Krissler)

Das Mikroskop sollte eine 500- bis 2000-fache optische Vergrößerung erreichen. Das trifft in der Regel selbst auf die günstigsten Lichtmikroskope zu, jedoch muss das

Objektiv geeignet sein. Umso stärker die Objektivvergrößerung ist, desto kleiner ist der Arbeitsabstand zwischen Objektiv und Objekt.

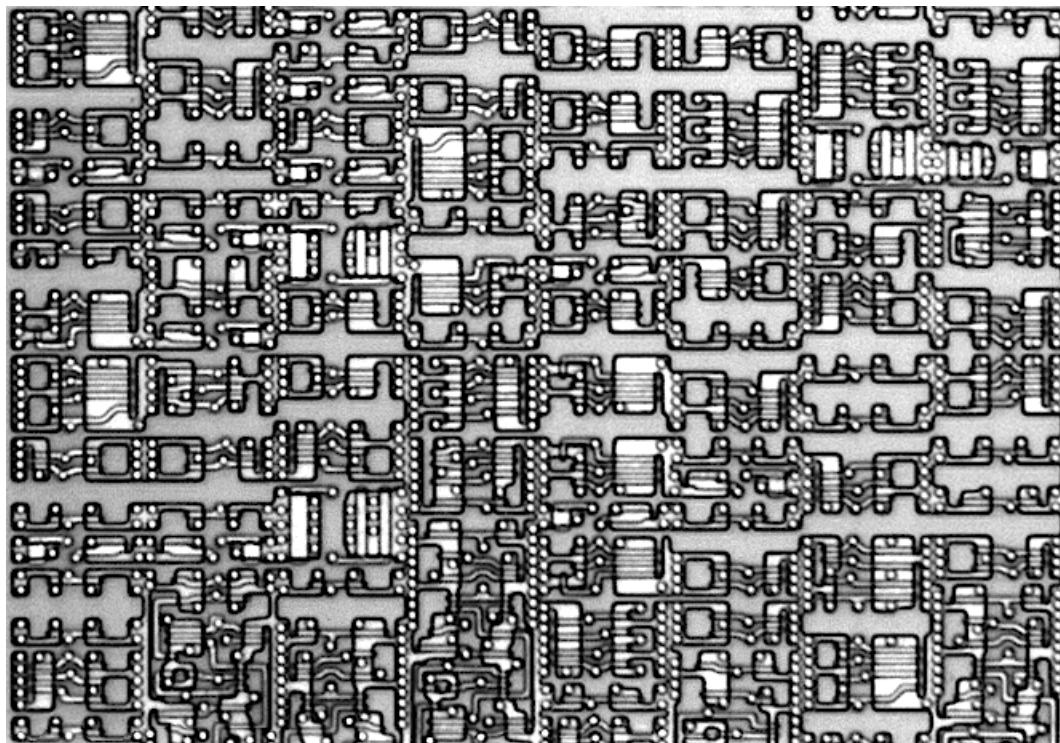


Abbildung 5.2: Bildausschnitt des Transistor-Layers eines Schaltkreises vom Typ Mifare Classic

Die Bilder werden mittels Auflichtmikroskopie gewonnen. Eine externe Lichtquelle beleuchtet die Chipoberfläche. Die Lichtstrahlen reflektieren in das Objektiv. Das Objektiv darf nicht zu nahe am Objekt sein, anderenfalls reflektiert nicht genug Licht. Für die Auflichtmikroskopie werden deshalb spezielle Objektive verkauft, die mit Beleuchtungsmöglichkeiten ausgestattet sind.

Das Mikroskop sollte mit einem XY-Tisch ausgestattet sein. Damit lässt sich die Probe einspannen und verfahren, ohne dass sie sich versehentlich verdreht. Wenn die Bilder mit verschiedenen Drehwinkeln aufgenommen werden, muss das vor dem Zusammensetzen der Bilddaten (manuell) korrigiert werden. Der Fachhandel bietet Mikroskope mit motorgetriebenen XY-Tischen an. Diese sind im Gesamtpaket mit mehreren tausend Euro jedoch teuer. Die besseren XY-Tische lassen sich drehen. Dadurch kann man die Probe bereits so auf dem Tisch orientieren, dass das Raster auf dem Chip parallel bzw. senkrecht zu den Bildrändern verläuft.

Ein Kameramodul mit zwei oder mehr Megapixeln ist erforderlich. Wenn man keine Mikroskopkamera hat, kann man diese ab etwa 200 Euro erwerben. In diesem Zusammenhang ist wichtig, dass sich die optische Gesamtvergrößerung multiplikativ aus der

Objektivvergrößerung und der optischen Vergrößerung durch die Kamera ergibt. Für günstige Mikroskopkameras ist oftmals keine optische Vergrößerung angegeben.

Als Strukturgröße in der Halbleitertechnik bezeichnet man die Abmessung der kleinsten anzutreffenden Bauteile. In der CMOS-Technik ist das die kleinste Gate-Länge eines CMOS-Transistors. Für die Analyse der Schaltkreise ist es hier nicht wesentlich, alle Details der Transistoren zu erkennen. Abbildung 5.2 zeigt Transistoren eines Schaltkreises vom Typ Mifare Classic unter dem Mikroskop bei 500-facher Vergrößerung. Mifare Classic wurde in einer Strukturgröße von etwa 500 nm gefertigt. Die einzelnen CMOS-Transistoren kann man gut erkennen.

Die Grenze der optischen Auflösung bei konventioneller Lichtmikroskopie hängt von der Wellenlänge der Beleuchtung und der Numerischen Apertur des Objektivs ab. Die Grenze liegt etwa bei 350 nm-Halbleiterprozessen. CPUs basierend auf dieser Strukturgröße wurden ab 1995 hergestellt. Im Vergleich - führende Halbleiterhersteller arbeiten derzeit an der Einführung von 22nm-Prozessen.

Um jenseits der Auflösungsgrenze operieren zu können, bedarf es anderer Mikroskopkonzepte. Beispielsweise lassen sich mittels Konfokalmikroskopie oder Rasterelektronenmikroskopie höhere Auflösungen erzielen.

## *5.2 Zusammenfügen und Nachbearbeitung der Bilddaten*

Die zu untersuchenden Schaltkreise sind größer als der Bildausschnitt im Mikroskop. Es müssen Einzelbilder zusammengefügt werden. Manuell kann man dazu Grafikbearbeitungsprogramme verwenden, beispielsweise das GNU Image Manipulation Program (gimp). Für das semi-automatische Zusammensetzen sind sogenannte Stitching-Programme geeignet. Man verwendet diese hauptsächlich zum Zusammensetzen von Fotos zu einer Panoramaaufnahme.

Als gerade so brauchbare freie Software hat sich das Programm Hugin erwiesen. Hugin ist die grafische Oberfläche zu den PanoTools. [Pan] Das kommerzielle Stitching-Programm PanaVue ImageAssembler 3 soll ebenfalls gute Ergebnisse beim Zusammensetzen von fotografierten Chip-Oberflächen liefern. Der PanaVue ImageAssembler ist in der Professional- und Enterprise-Edition für Bilddaten bis 100.000 x 100.000 Bildpunkte ausgelegt. Ferner ermöglicht die Software ein automatisiertes Zusammensetzen der Bilddaten, wenn genug Überlappung der Einzelbilder vorhanden ist. [Pan08]

## 5.2. ZUSAMMENFÜGEN UND NACHBEARBEITUNG DER BILDDATEN

Für das manuelle Zusammensetzen von Chip-Bildern anhand von Referenzpunkten hat Sven Kaden ein Programm geschrieben, dass ohne weiters Parameter-Tuning benutzt werden kann. [Kad09]

Wenn die Bilddaten zusammengesetzt sind, kann es für eine spätere automatisierte Bildanalyse sinnvoll sein, dass das Bildmaterial entrauscht wird. Dafür ist das quelloffene Werkzeug GREYCstoration geeignet. [Tsc08] Es entrauscht Bilddaten, versucht aber, wesentliche Merkmale des Bildes beizubehalten. Insbesondere bleiben dadurch Kanteninformationen erhalten.

---

## 6 Analyse von Integrierten Schaltkreisen anhand von Bilddaten

Dieses Kapitel soll sich der Fragestellung widmen, was anhand der Bilddaten zu erkennen ist. Es soll dargestellt werden, wie man bei vergleichsweise einfachen Schaltkreisen, etwa Chips vom Typ Mifare Classic, in Hardware umgesetzte Algorithmen findet.

Für eine detaillierte Einführung in die CMOS-Technik seien die einleitenden Kapitel aus dem Buch „CMOS VLSI Design“ empfohlen. [WH05] Das Buch erklärt anschaulich, wie CMOS-Technologie funktioniert und wie Designs erstellt und in Hardware umgesetzt werden. Die Darstellung hier fasst die wesentlichen Punkte aus der Sicht des Reverse-Engineerings zusammen.

### 6.1 Feldeffekt-Transistoren

Feldeffekt-Transistoren (FET) sind Halbleiterbausteine, die in Logikschaltkreisen als elektronische Schalter dienen. Abbildung 6.1 zeigt den Aufbau beider Typen auf einem gemeinsamen Substrat.

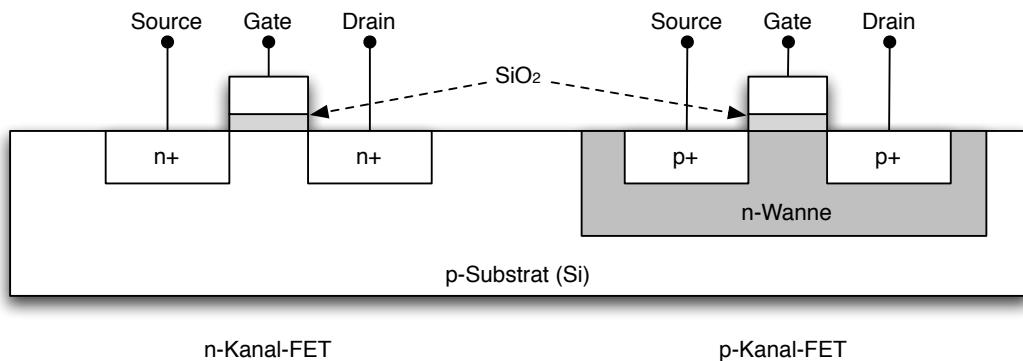


Abbildung 6.1: n-Kanal- und p-Kanal-FET auf einem gemeinsamen Substrat

Deren Funktionsweise besteht vereinfacht dargestellt darin, dass durch Anlegen einer Steuerspannung am Gate, die Region unter dem Gate an Ladungsträgern verarmt oder mit Ladungsträgern angereichert wird. Wenn genug Ladungsträger unter dem Gate-Anschluss vorhanden sind, entsteht ein elektrisch leitender Kanal zwischen den Anschlüssen Source und Drain. Zwei Typen von Feldeffekt-Transistoren unterscheidet man nach Art der Ladungsträger.

Feldeffekt-Transistoren des n-Kanal-Typs bestehen aus stark n-dotierten Bereichen<sup>1</sup> für Quelle und Abfluss und einem p-dotierten Substrat. Das Siliziumdioxid unter dem Gate-Kontakt stellt einen Isolator dar. Bei positiver Gatespannung bildet sich zwischen Gate und Substrat ein elektrisches Feld, so dass sich Elektronen unter dem Gate sammeln. Dadurch wird ein Stromfluss zwischen Source und Drain möglich.

Beim p-Kanaltyp dienen positiv geladene Defektelektronen modellhaft als Ladungsträger. Um einen leitenden Defektelektronen-Kanal zu erzeugen, muss die Gate-Spannung null sein. Dadurch sammeln sich Defektelektronen unter dem Gate. Source und Drain eines p-Kanal-FETs sind stark p-dotiert und dessen Substrat ist n-dotiert, d.h. genau anders herum wie beim n-Kanal-Typ. Um beide Transistorarten auf einem gemeinsamen Substrat betreiben zu können, werden bei der Chip-Herstellung sogenannte Wannen erzeugt.

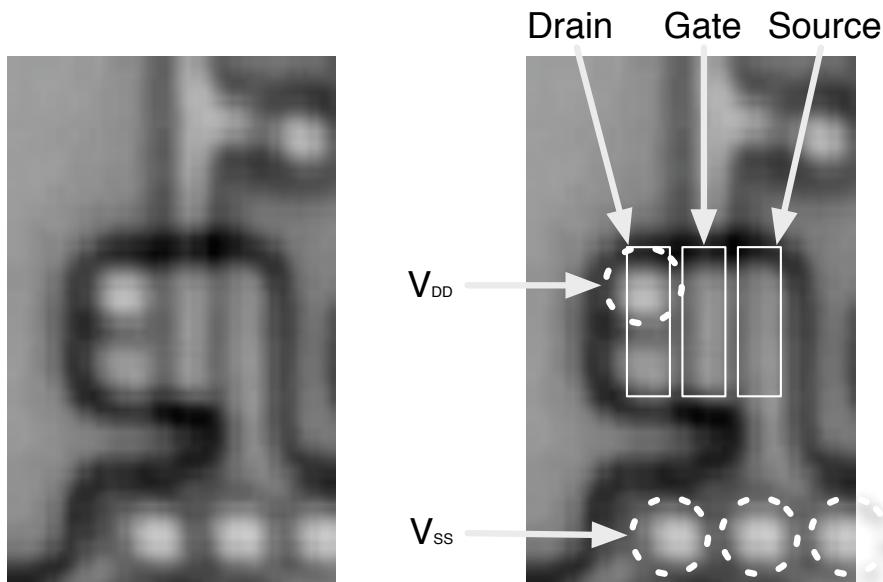


Abbildung 6.2: n-Kanal-FET unter dem Mikroskop (Chip: Mifare Classic)

Abbildung 6.2 zeigt ein Foto eines Feldeffekt-Transistors unter dem Mikroskop. Source, Gate und Drain sind durch zwei schmale vertikale Striche im Bild 6.2 links abgegrenzt.

Wenn sich benachbarte Transistoren einen Anschluss teilen, kann es schwierig sein, zu erkennen, welche Bereiche Source, Drain und Gate sind. Da der Gate-Anschluss immer als Signal-Eingang eines Transistors dient, ist dieser leichter zu identifizieren. Abbildung 6.3 zeigt drei in Reihe geschaltete p-Kanal-FETs. Zwischen den Gates befindet sich jeweils das gemeinsam genutzten Source und Drain.

<sup>1</sup>In Abbildungen wird die starke Dotierung mit einem Pluszeichen symbolisiert. Starke Dotierung bedeutet ein Verhältnis von  $10^4$  Siliziumatomen zu einem Donator bzw. Akzeptor. Bei mittleren Dotierungen ist das Verhältnis  $10^6$  Siliziumatome zu einem Akzeptor (p-Dotierung) bzw.  $10^7$  Siliziumatome zu einem Donator (n-Dotierung).

Feldeffekt-Transistoren sind symmetrisch aufgebaut. D.h. Source und Drain könnten vertauscht werden. Zumindest ist das bei den einfachen FETs der Fall und bei den Chips, von denen hier Bildmaterial gezeigt wird. Die Symmetrieeigenschaft lässt es zu, dass man bei der Analyse nicht Source und Drain explizit im Bild benennen muss. Es reicht die Vorstellung eines Schalters, mit dem man Source und Drain elektrisch verbinden kann.

In den Schaltkreisen wird Information als Spannungspotential gespeichert – LOW oder HIGH. Es ist deshalb nicht notwendig, sich zu überlegen, in welche Richtung der technische oder physikalische Strom fließt. Strom fließt im Gegensatz zu Bipolartransistoren hauptsächlich nur beim Umschaltvorgang.

Das Modell lautet also: Wenn das „passende“ Signal am Gate anliegt, sind Source und Drain elektrisch verbunden und der Transistor schaltet durch. Andernfalls sperrt der Transistor.

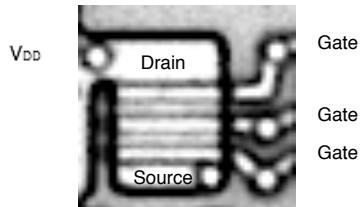


Abbildung 6.3: Drei p-Kanal-FETs in Reihenschaltung (Chip: Mifare Classic).

## 6.2 Komplementäre Verwendung von FETs

CMOS ist das Akronym für Complementary Metal Oxide Semiconductor. Feldeffekt-Transistoren werden in CMOS-Gattern nicht einzeln eingesetzt sondern immer komplementär geschaltet. In Schaltungen wird jedem p-Kanal-FET ein n-Kanal-FET gegenübergestellt. Der p-Kanal-FET ist Teil des Pull-up-Netzes, der n-Kanal-Typ ist Teil des Pull-down-Netzes. Je nach Steuerung hat ein Ausgang eines Gatters das Spannungspotential des Pull-up-Netzes oder auf das Potential des Pull-down-Netzes.

Beide Netze eines (Teil-)Gatters sind immer komplementär geschaltet. D.h. wenn das eine Netz gesperrt ist, ist das andere geöffnet und umgekehrt. Das sei am Beispiel des CMOS-Inverters aus Abbildung 6.4, der die logische Funktion NOT umsetzt, dargestellt.

Ist das Eingangssignal HIGH (positives Potential), entsteht ein leitender n-Kanal zwischen Source und Drain im Pull-down-Netz. Der Ausgang wird quasi geerdet. Gleichzeitig ist der p-Kanal-FET im Pull-up-Netz gesperrt, so dass keine leitende Verbindung zwischen dessen Source und Drain besteht. Ist das Eingangssignal LOW (0 V), ist der n-Kanal-FET gesperrt und der p-Kanal-FET offen. Der Ausgang hat dann das Potential  $V_{DD}$ .

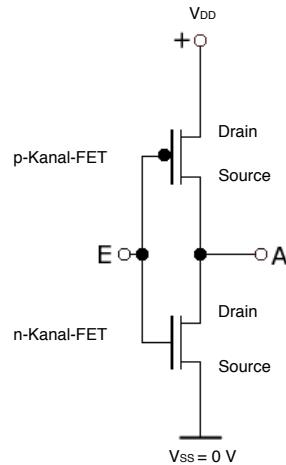


Abbildung 6.4: CMOS-Inverter

In der Umsetzung im Chip durchziehen parallele spannungsführende Leiterbahnen wie Schienen den Bereich, in dem die Logik-Gatter platziert sind. In Abbildung 6.5 sind das die dunkel markierten Streifen. Die Schienen für das Potential  $V_{DD}$  und  $V_{SS}$  wechseln sich dabei ab. Die Pull-up- und Pull-down-Netze sind zwischen den Leiterbahnen angeordnet.

Die hellen Punkte in Abbildung 6.5 sind Durchkontaktierungen zu höheren Schichten im Schaltkreis. Die Gate-Anschlüsse verlaufen zwischen den Transistorarten und sind jeweils mit einer Durchkontaktierung versehen.

Die z.T. haken- und ösenförmigen Transistoren weisen unterschiedliche Gate-Längen auf. P-Kanal-FETs haben meist eine größere Gate-Länge gegenüber n-Kanal-Typen. Das liegt daran, dass die Beweglichkeit der Löcher geringer ist als die der Elektronen. Um so größer der Kanalquerschnitt zwischen Source und Drain ist, desto mehr Defektelektronen können in der gleichen Zeit durch den Kanal driften.

Anhand der Zuordnung, auf welcher Seite jeweils die p-Kanal-Typen und auf welcher die n-Kanaltypen verlaufen kann man den Leiterbahnen Spannungspotentiale zuordnen. Am Drain des p-Kanal-FETs ist die Spannung  $V_{DD}$  angelegt, am Source des n-Kanal-FETs das Potential  $V_{SS}$ .

Tatsächlich ist es möglich, p- und n-Kanal-Typen vertauscht anzuwenden. N-Kanal-FETs können besser LOW-Signale weiterleiten. Dagegen leiten p-Kanal-FETs besser HIGH-Signale weiter. Beim Vertauschen der Typen, sind die Spannungspotentiale am Ausgang des Transistors etwas größer als  $V_{SS}$  bzw. etwas kleiner als  $V_{DD}$ . Man spricht dann von degradierten oder schwachen Signalen. Dies möchte man beim Design von CMOS-Schaltkreisen vermeiden. [WH05, S. 14ff]

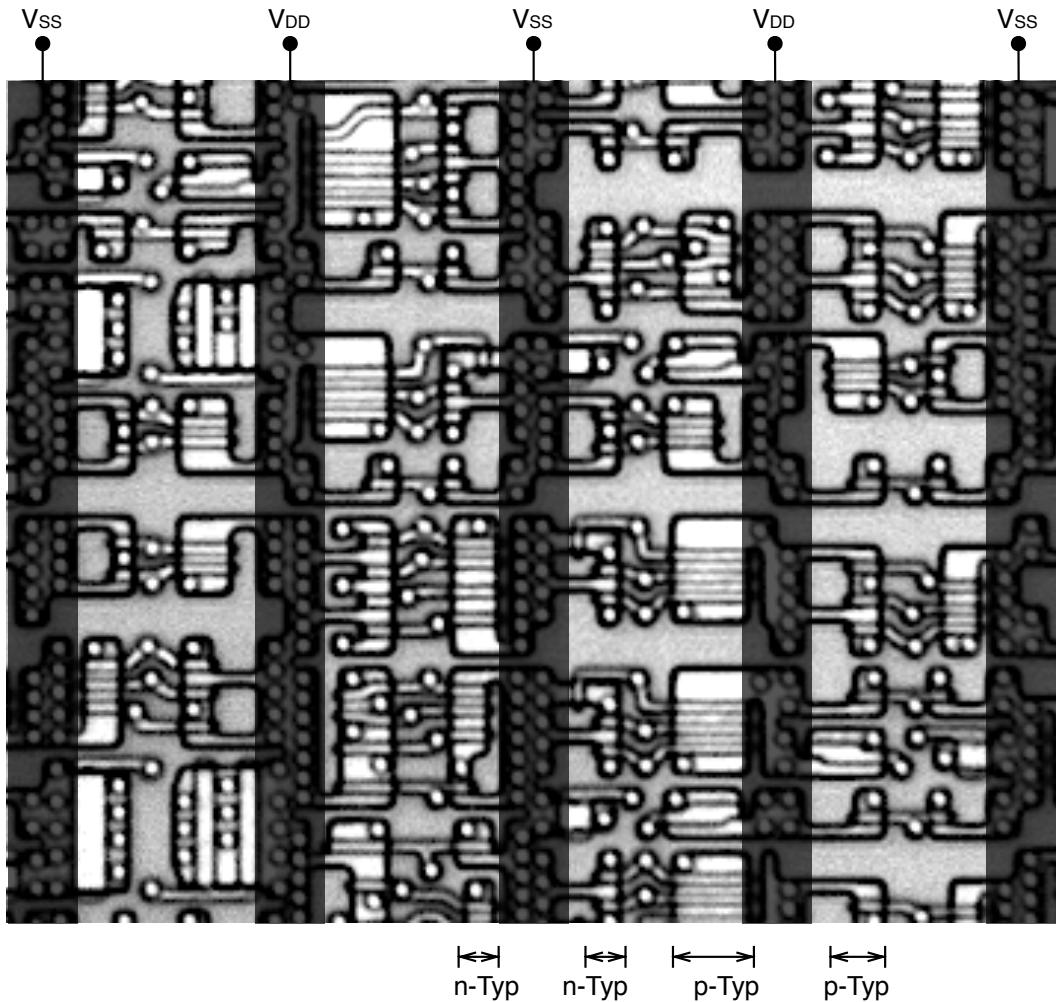


Abbildung 6.5: Typenweise Anordnung von p- und n-Kanal-Transistoren zwischen den Potentialschienen (Chip: Mifare Classic)

### 6.3 Aufbau von Logik-Gattern

In den letzten zwei Abschnitten ist beschrieben, wie man Transistoren als Schalter benutzt und wie Transistoren auf dem Substrat angeordnet sind. Herstellungsbedingt ist die Anordnung der Transistoren auf mehreren Schichten (*front-end-of-line*, FEOL) verteilt. Diese sollen hier zur Vereinfachung als Transistor-Layer bezeichnet werden. Um elementare Logik-Gatter aufzubauen, müssen mehrere Transistoren zusammengeschaltet werden. Auf dem Transistor-Layer sind bereits einzelne Leiterbahnen platziert. Die Leiterbahnen müssen kreuzungsfrei verlegt werden. Dazu sind zusätzliche Ebenen im Chip notwendig (*back-end-of-line*, BEOL).

Eine besondere Bedeutung kommt der ersten Verdrahtungsebene über dem Transistor-Layer zu. Sie bildet das Verbindungsgerüst, um aus den darunter liegenden Transistoren die logischen Grundfunktionen zu formen, beispielsweise NAND und NOR. Diese

Schicht wird Metal 1 oder kurz M1 genannt. Die Transistoren eines Gatters sind immer beieinander angeordnet.

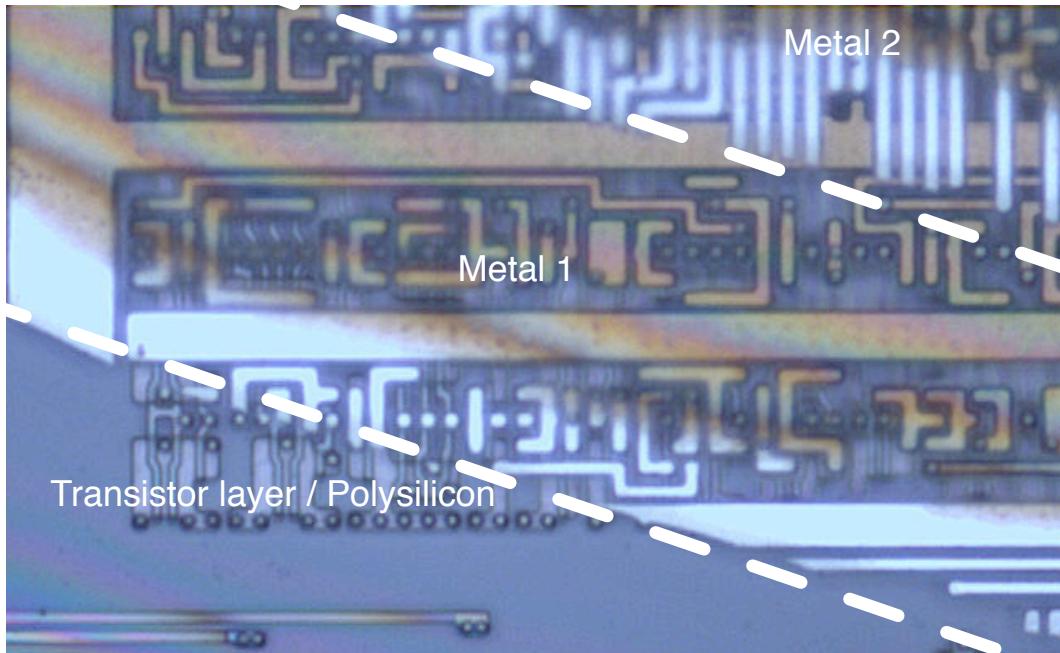


Abbildung 6.6: Der Materialabtrag beim Polieren der Chipoberfläche war nicht gleichmäßig. Dadurch ergibt sich eine Blick auf drei verschiedene Ebenen. (Mifare Classic)

Für die Anfertigung der Masken für den Herstellungsprozess können Chip-Designer grundlegende Funktionsblöcke aus vorgefertigten Bibliotheken verwenden. Bei Mifare Classic sind etwa 70 verschiedene Grundbausteine, u. A. etwas komplexere Typen wie Flipflops und Volladdierer, zu finden. Darunter sind aber einige Formen enthalten, die die gleiche logische Funktion umsetzen, nur dass leicht verschiedenen Masken zur Anwendung kommen. Im „Silicon Zoo“ zeigt Karsten Nohl die bei Mifare Classic verwendeten Grundbausteine. [Noh08b]

Abbildung 6.6 stellt den schichtweisen Aufbau von Logik-Schaltkreisen dar. In der Schicht M1 sind die fingerförmig angeordneten Leiterbahnen für  $V_{SS}$  und  $V_{DD}$  untergebracht. Über dem M1 sind weitere Schichten, die Leiterbahnen für die Verschaltung von Grundgattern beinhalten.

Wie kann man nun anhand von Bilddaten die Schaltfunktion eines Gatters ermitteln?

Die Abbildungen 6.7 und 6.8 zeigen beispielhaft zwei Grundgatter in CMOS-Technologie nebst Schaltbild. Die Funktionsweise des CMOS-Inverters wurde bereits beschrieben. In Abbildung 6.7 sieht man die beiden Transistoren, die Durchkontaktierungen und die Verbindungen mit  $V_{SS}$  und  $V_{DD}$ . Der Eingang E ist auf das Gate beider Transistoren geschaltet. Im Ausgang A sind Source des p-FETs und Drain des n-FETs vereint.

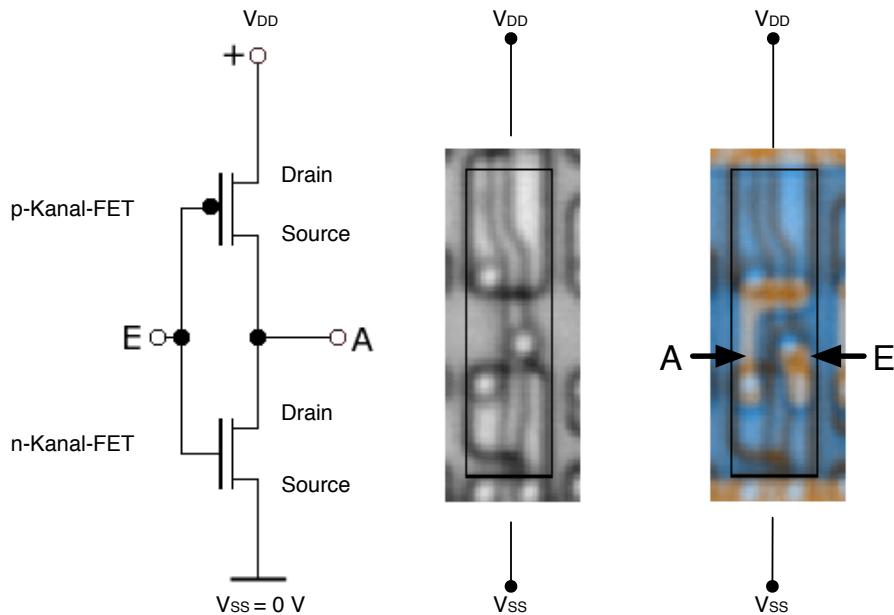


Abbildung 6.7: CMOS-Inverter (Mifare Classic)

In Abbildung 6.8 ist ein NAND aus insgesamt vier Transistoren dargestellt. Man beachte, dass die Gate-Längen im Pull-up-Netzwerk von Abbildung 6.8 nicht größer sind als im Pull-down-Netz, weil die beiden n-Kanal-FETs aus dem Pull-down-Netz seriell geschaltet sind und sich damit deren Widerstand verdoppelt. Die Driftgeschwindigkeiten der jeweiligen Majoritätsladungsträger ist damit in beiden Netzen etwa gleich.

Für das Reverse-Engineering einfacher Gatter ist es sinnvoll, die wenigen Transistoren und Leiterbahnen übersichtlich geordnet auf ein Blatt Papier zu skizzieren. Oft ist der Gattertyp sofort zu erkennen. Es kann sein, dass man aufgrund vorheriger Analyse anderer Gatter eine Grundstruktur wiedererkennt. Beispielsweise sieht ein 3-NAND, d.h. ein NAND für drei Eingänge<sup>2</sup>, nicht wesentlich anders aus als ein 2-NAND. Im Pull-up-Netz sind drei statt zwei Transistoren parallel geschaltet und im Pull-down-Netz sind drei FETs seriell verbunden (vgl. Abbildung 6.8).

Mitunter kann es hilfreich sein, eine Wahrheitstabelle aufzustellen, indem man für alle möglichen Belegungen der Eingänge den Wert am Ausgang ermittelt. Anhand der Wahrheitstabelle kann man eine Boolesche Funktion aufstellen. Tabelle 6.1 zeigt das beispielhaft für ein 3-NAND-Gatter. Für alle  $2^3 = 8$  möglichen Belegungen der Eingänge A, B, und C ist das Ergebnis der Booleschen Funktion in der letzten Spalte angegeben.

Aus der Tabelle kann man ablesen, dass die Schaltfunktion sich als  $\overline{(A \wedge B \wedge C)}$  darstellt. Das geht hier deshalb einfach, weil es nur eine Belegung gibt, bei der der Aus-

---

<sup>2</sup> $3 - \text{NAND}(A, B, C) = /AND(A, B, C)$

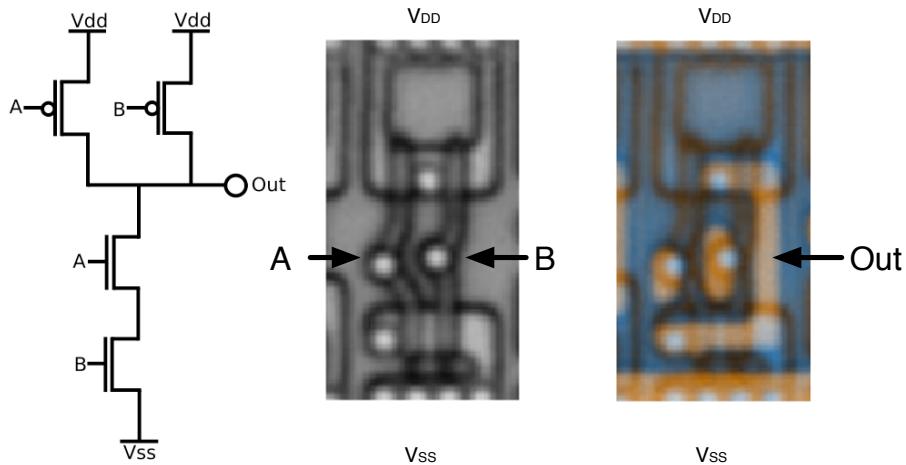


Abbildung 6.8: CMOS-NAND (Mifare Classic)

Eingang A	Eingang B	Eingang C	Ausgang NAND(A, B, C)
T	T	T	F
T	T	F	T
T	F	T	T
T	F	F	T
F	T	T	T
F	T	F	T
F	F	T	T
F	F	F	T

Tabelle 6.1: Wahrheitstabelle für einen 3-NAND

gang den Wert falsch annimmt. I.d.R. stellt man die Kanonische Alternative Normalform auf. Diese ist etwas sperrig und lautet  $\Phi(A, B, C) = (A \vee B \vee \bar{C}) \wedge (A \vee \bar{B} \vee C) \wedge (A \vee \bar{B} \vee \bar{C}) \wedge (\bar{A} \vee B \vee C) \wedge (\bar{A} \vee B \vee \bar{C}) \wedge (\bar{A} \vee \bar{B} \vee C) \wedge (\bar{A} \vee \bar{B} \vee \bar{C})$ . Diesen Ausdruck versucht man dann soweit zu vereinfachen, so dass möglichst wenig logische Operatoren auftreten.

Bei der Rekonstruktion einer Gatterfunktion mittels einer Wahrheitstabelle verliert diese an Anschaulichkeit. Insbesondere für den Fall, dass sich bei der Rekonstruktion Fehler einschleichen, sind diese schwierig festzustellen.

Abbildung 6.9 zeigt einen komplizierteren CMOS-Schaltkreis. Die Transistorschicht ist in der Abbildung oben dargestellt, darunter die Metallverbindungen, die die Transistoren zu einem Gatter verbinden. Die untere Darstellung zeigt beide Layer zu einem Bild vereint. Im Transistor-Layer sind 34 Transistoren zu erkennen: 17 p-Kanal-Transistoren oben und 17 n-Kanal-FETs unten. Der dargestellte Schaltkreis soll beispielhaft für eine Analyse herhalten.

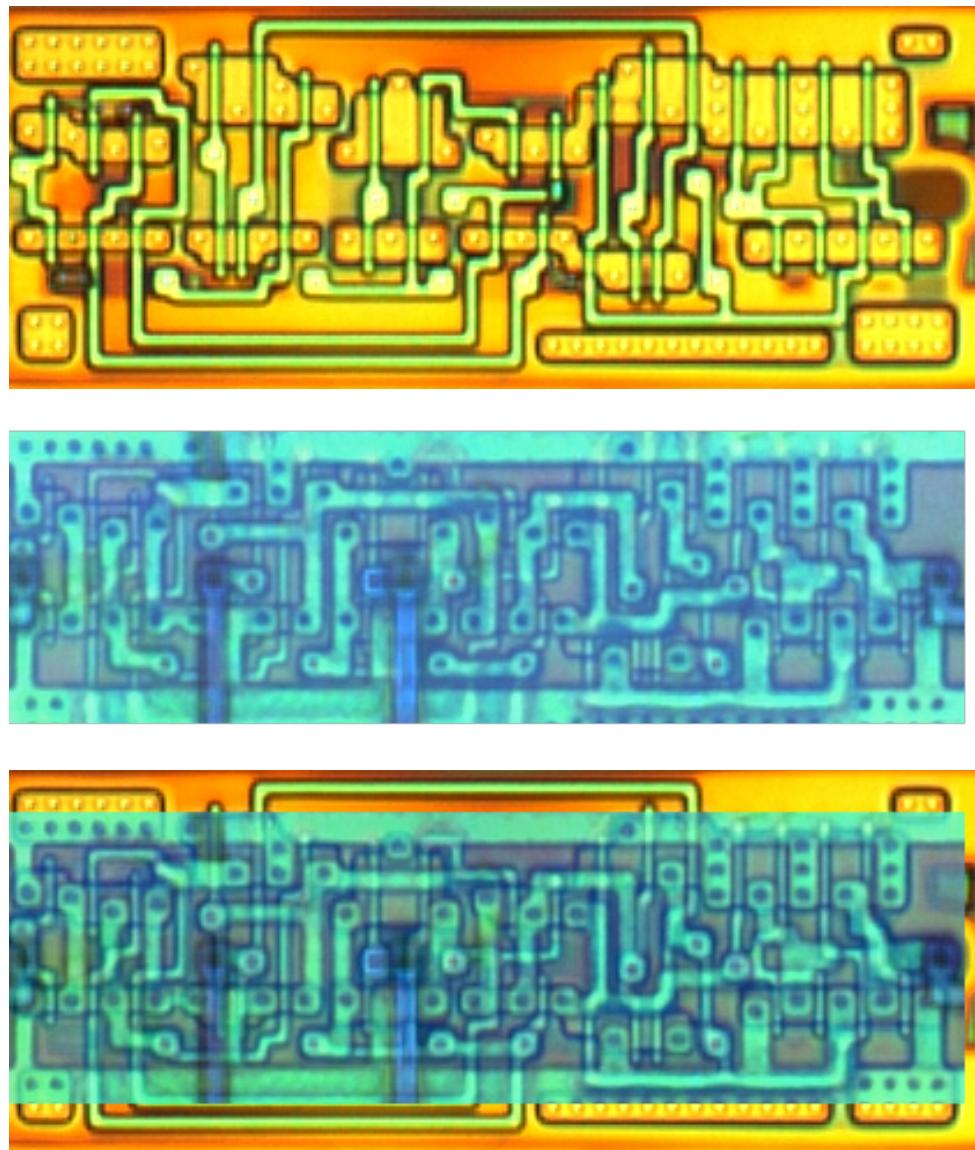


Abbildung 6.9: zu identifizierer CMOS-Schaltkreis [Noh08a]

Anhand der Transistorgrößen, genauer der Gate-Längen, ermittelt man, welche Seiten zum Pull-up-Netz gehören und welche zum Pull-down-Netz. P-Kanal-FETs müssen nicht zwangsläufig größer sein als n-Kanal-Typen. In Abbildung 6.9 (oben) sieht man, dass die p-Kanal-Transistoren an der oberen Seite angeordnet sind. In Bild 6.9 (mitte) sieht man am oberen und unteren Bildrand die Leiterbahnen für die Versorgungsspannung und Masse.  $V_{DD}$  ist oben,  $V_{SS}$  ist unten.

Die Transistoren findet man wieder anhand der Gates. Die Transistoren eines Gatters werden durchnummeriert. Z.B. von links nach rechts  $P1 \dots P17$  und  $N1 \dots N17$ . Dazu ist es hilfreich, das Bild in einem Grafikbearbeitungsprogramm zu öffnen und beispielsweise jedes fünfte Gate mit einer Beschriftung zu versehen.

Die Transistoren überträgt man auf ein Blatt Papier. Für jeden Transistor sind die Leiterbahnen zu verfolgen und in die Zeichnung zu übertragen. Für das Abzeichnen ist es empfehlenswert, die Transistoren wie im physischen Gatter anzurufen und die Gates zur Mitte hin zu zeichnen. Andernfalls hat man schnell zahlreiche unübersichtlich gekreuzte Leiterbahnen. Abbildung 6.10 zeigt den zu 6.9 gehörenden Schaltplan.

Beim Übertragen der Leiterbahnen aufs Papier werden sich durchaus Fehler einschleichen. Dann hilft es, nach offenen Transistoranschlüssen zu suchen. Durchkontaktierungen kann man anhand ihres punktförmigen Aussehens erkennen. Wenn man vermutet, dass zwei übereinander liegende Leiterbahnen elektrisch verbunden sind, dann muss es eine Durchkontaktierung geben. Weitere Fehler findet man evtl. bei der späteren Analyse. Wenn die Verschaltung mehrerer Transistorpaare keinen Sinn ergibt oder zu viele Transistoren effektiv nicht benutzt werden, lohnt sich ein erneuter Blick in das Ausgangsbild. Es ist möglich, dass nicht alle Transistoren eines Gatters verwendet werden. So werden beispielsweise die Transistoren  $P14, P15, N14$  und  $N15$  hier im Gatter nicht verwendet.

Die Ein- und Ausgänge des Gatters sind einfach zu finden. In Abbildung 6.9 (mitte) sind das die beiden senkrechten Striche, die von außen kommen und etwa bis zu Bildmitte verlaufen (blaue Färbung in der PDF-Version).<sup>3</sup> Im allgemeinen Fall findet man auf der Schicht M1 entsprechende Durchkontaktierungen und auf den darüberliegenden Verbindungslayern Leiterbahnen, die auf diese Kontakte geschaltet sind. Wenn eine Verbindung von außerhalb mit einem Gate verbunden ist, muss es sich um einen Eingang handeln. Wenn Verbindungen, die von einem Source oder Drain stammen in die Außenwelt des Gatters gerichtet sind, muss es sich um einen Gatterausgang handeln. Folglich sind die Anschlüsse A, B und C in Abbildung 6.10 Eingänge und X der Ausgang.

<sup>3</sup>Das Bild wurde mit einem Konfokalmikroskop aufgenommen, das verschiedenen Tiefen im Untersuchungsobjekt verschiedene Farben zuordnet.

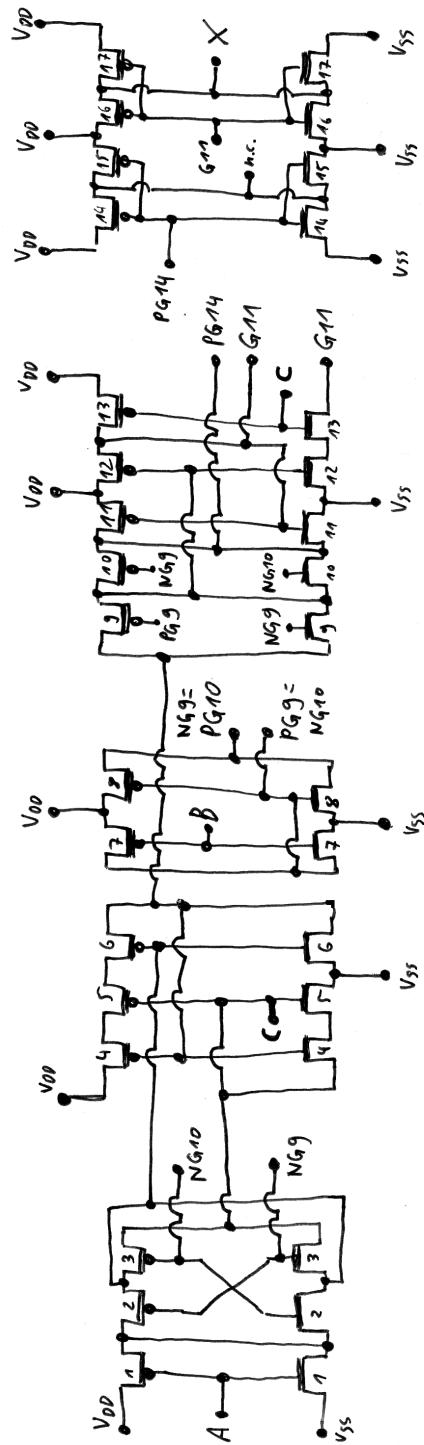


Abbildung 6.10: Rekonstruiertes Schaltbild des zu identifizierenden CMOS-Gatters

Bei einem Schaltplan wie in Abbildung 6.10, stellt sich die Frage, was die Schaltung bewirkt. Wie bereits beschrieben, wäre es möglich, dazu eine Wahrheitstabelle aufzustellen, beispielsweise unter Zuhilfenahme von Simulationspaketen wie etwa SPICE.

Intuitiver ist allerdings, zu versuchen, im Schaltbild Funktionsblöcke auszumachen<sup>4</sup>. Als Hinweis auf die Abgrenzung der Funktionsblöcke können die Zuführungen der Spannungspotentiale  $V_{DD}$  und  $V_{SS}$  dienen. In Abbildung 6.9 kann man im Transistor-Layer erkennen, dass seriell geschaltete Transistoren in Blöcken gruppiert sind. Diese Gruppierung spiegelt im Wesentlichen die Funktionsblöcke wieder.

Meistens hilft es, für jeden dieser Funktionsblöcke eine alternative „gewohnte“ grafische Darstellung zu finden. So sieht man beispielsweise, dass das Transistorpaar 4 und 5 ein NAND bildet und das Transistorpaar 6 einen Inverter darstellt. In vereinfachter Form gezeichnet entsteht ein Schaltplan wie in Abbildung 6.11.

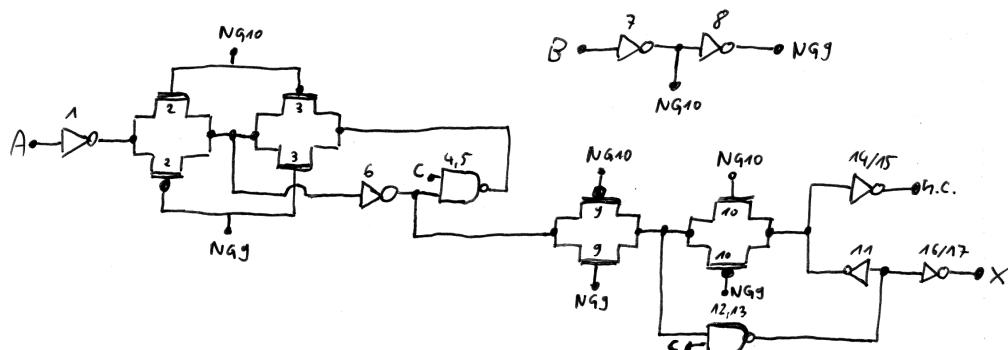


Abbildung 6.11: Schaltung eines Flipflops. Die angegebenen Zahlen geben an, welche Transistoren bzw. Transistorenpaare zum Teilgatter beitragen.

Der abgebildete Schaltkreis stellt einen taktflankengesteuerten Master/Slave-Flipflop dar. Das „Eingangsbit“ liegt an Eingang A an und das Taktsignal an Eingang B. Mit einem Signal auf Eingang C kann man den Informationsspeicher zurückstellen. Am Ausgang X liegt das gespeicherte Signal an. Das Gatter beinhaltet einen invertierten Ausgang. Der wird allerdings nicht genutzt.

Abbildung 6.11 zeigt zwei weitere Konstruktionsmechanismen, wie man sie des öfteren findet. Deshalb sollen sie hier kurz beschrieben werden.

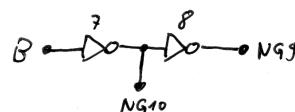


Abbildung 6.12: Doppelter Inverter zur Signalauffrischung.

<sup>4</sup>Für die Verifikation von Schaltkreisen existieren Werkzeuge, um auf dem Substrat angeordnete Gatter anhand von Netzlisten darauf zu prüfen, ob sie die intendierte Funktion erfüllen. In [BT94] wird beschrieben, wie man mittels eines Prolog-Programmes Schaltungen analysieren kann. Für das Reverse-Engineering wäre das ebenfalls praktisch.

Man sieht, dass die beiden Transistorenpaare 7 und 8 das Taktsignal B zweifach invertieren (Abbildung 6.12). Das Transistorpaar  $P_8$  und  $N_8$  erscheint überflüssig, da die doppelte Negation des Signals wieder das normale Taktsignal ist. Diese Konstruktion stellt einen Puffer dar. Wie bereits erwähnt, leiten p- und n-Kanal-FETs Signale unterschiedlich gut weiter. Insbesondere bei Serienschaltung mehrerer Transistoren, führt das intern zu Spannungsabfällen, so dass die Signalpegel nicht mehr ideal sind. Durch die genutzte Konstruktion wird das Taktsignal „aufgefrischt“ und hat wieder die idealen Spannungspegel  $V_{DD}$  oder  $V_{SS}$ . Der Nachteil besteht darin, dass diese zusätzlichen Gatter das Signal verzögern. Das Signal auf der Leiterbahn NG9 ist gegenüber dem Signal B phasenverschoben.

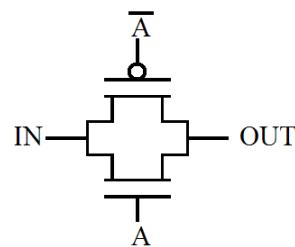


Abbildung 6.13: Transmission-Gate (Bildquelle: Wikipedia)

Als weiteres Konstruktionselement findet man in Abbildung 6.11 mehrere sogenannte Transmission-Gates. Ein Transmission-Gate besteht aus einem n- und einem p-Kanal Transistor, die wie in Abbildung 6.13 zusammengeschaltet sind. Ein n-FET schaltet bei positiver Gatespannung durch und ein p-FET sperrt bei positiver Gatespannung. Wenn das Signal am p-FET invertiert ist, dann schalten beide Transistoren bei HIGH durch und sperren beim LOW-Signal. Dadurch ergibt sich im Flipflop die taktflanken-gesteuerte Übernahme des Eingangssignals.

## 6.4 Wiederverwendung von Logik-Gattern

Wenn Ingenieure Schaltungen in Hardware umsetzen, erstellen sie nicht für jeden Chip-Typen ein vollständig neues Layout aller Transistoren, sondern nutzen vorgefertigte Grundgatter. Für diese Grundgatter existieren vorgefertigte Masken für den lithografischen Herstellungsprozess. Die sind weitgehend optimiert und wurden bereits auf Praxistauglichkeit hin untersucht.

Was man für Gattertypen auf einem Chip findet, hängt von den verwendeten Maskenbibliotheken ab. Es kann beispielsweise sein, dass man einen Halbaddierer als AND- und OR-Gatter getrennt realisiert findet. Es kann aber sein, dass die Maskenbibliothek

bereits einen Halbaddierer in Gänze beinhaltet und sich das auf dem Chip als eigenständiges Gatter widerspiegelt. Ferner ist es möglich, dass diese Maskenbibliotheken ganze Allzweck-CPUs oder speziell für die Signalverarbeitung geeignete Rechenwerke beinhalten. Das ist jedoch eher ein Sonderfall.

Die Wiederverwendung von Grundbausteinen ermöglicht beim Reverse-Engineering folgende Vereinfachung. Wenn man ein Gatter aus der Bibliothek bereits erkannt hat, ist es einfacher, diesen Gattertyp auf dem Chip wiederzufinden, als die Bedeutung aller Transistoren einzeln zu ermitteln.

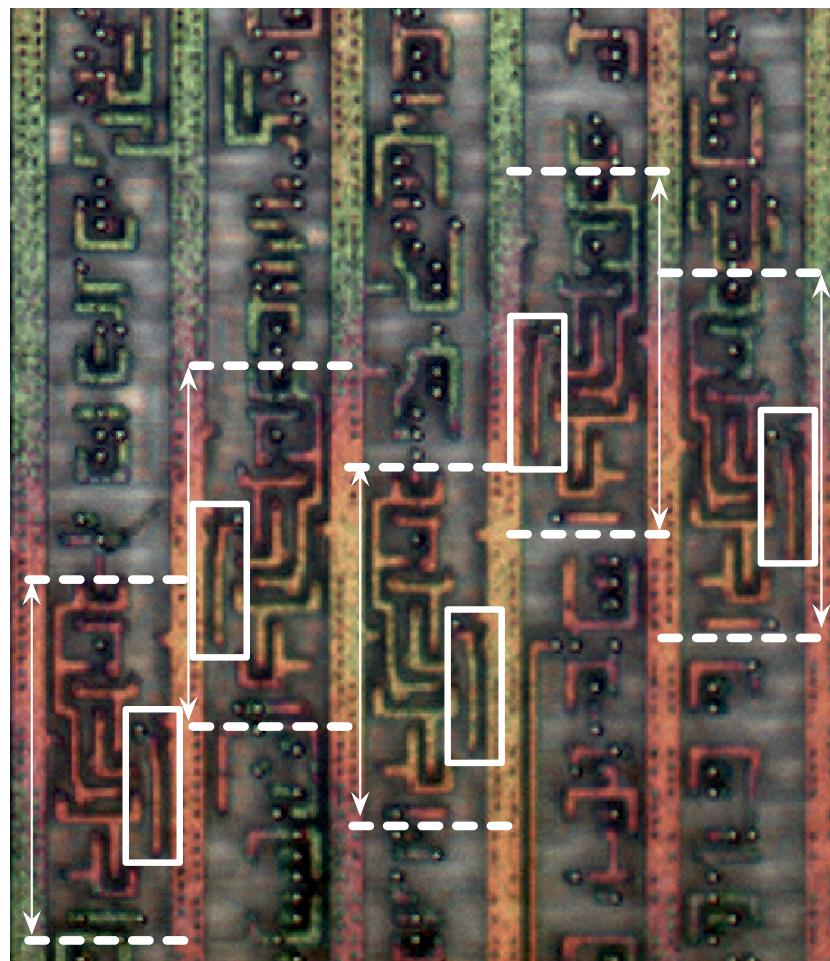


Abbildung 6.14: Wiederfinden markanter Muster (Chip: Mifare Classic).

Die dafür geeigneten Muster sind auf der Schicht M1 und auf dem Transistor-Layer. Meist ist M1 einfacher auszuwerten. Man sucht nach Mustern im Verdrahtungsflecht, die man an anderen Stellen auf dem Chip findet. Wenn man ein wiederkehrendes Muster identifiziert hat, beispielsweise der in Abbildung 6.14 mit Rechtecken hervorgehobene „Haken“, vergleicht man die verschiedenen Instanzen, um einen maximal konstanten Bildbereich zu finden. Die platzierten Gatter gehen nahtlos ineinander über, ohne dass eine definierte Abgrenzung vorhanden ist. Vergleicht man die

Instanzen, sieht man, welche Teile des Verdrahtungsgeflechts noch zum Gatter gehören. Idealerweise sucht man zuerst nach größeren Gattern.

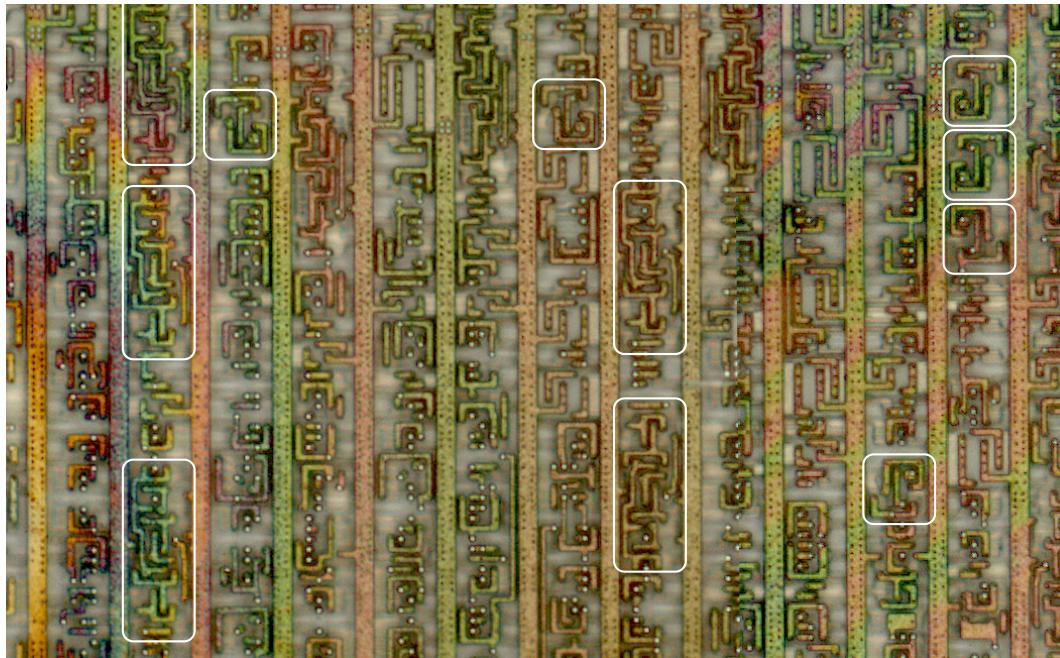


Abbildung 6.15: Manuelles Ermitteln der Gattergrenzen anhand von Verdrahtungsmasken (Chip: Mifare Classic)

Mittels normalisierter Kreuzkorrelation, einem Verfahren aus der Signalverarbeitung, ist es möglich, Bildmaterial an anderen Stellen wieder zu finden, an denen ein Muster ebenfalls auftritt. Die Schritte wendet man iterativ an bis man alle Gattertypen ermittelt hat.

## 6.5 Gezielte Suche

Das komplette Reverse-Engineering eines Chips ist zu aufwendig und nicht notwendig. Dies ist mit dem Reverse-Engineering von Software mittels Disassemblern vergleichbar. In der Regel sind vorab konkrete Fragestellungen gegeben, z.B. wie ein Verschlüsselungsverfahren implementiert ist. Deshalb muss kein Chip komplett analysiert werden.

Beispielsweise werden Stromchiffrierer mittels Schieberegister (Flipflops) konstruiert. Da funktional zusammenhängende Bereiche auf dem Chip benachbart platziert, muss man lediglich nach Bereichen suchen, in denen viele Flipflops zu sehen sind. Flipflops sind leicht zu erkennen, da sie innerhalb typischer Standardzellenbibliotheken die größten Elemente bilden. So beschreiben die markierten Bereiche in Abbildung 6.14

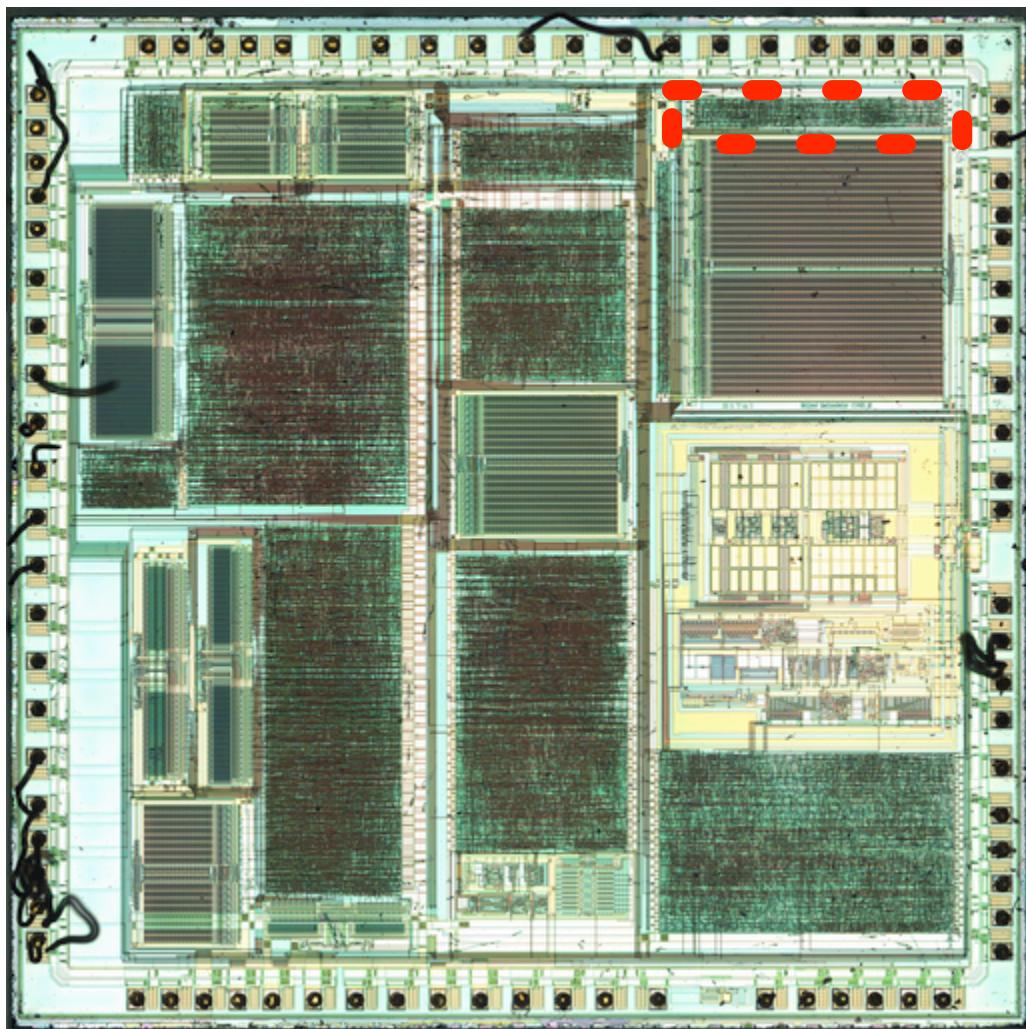


Abbildung 6.16: Übersicht des Dect-Chips SC14421CVF. Der Dect Standard Cipher ist innerhalb der Markierung im oberen rechten Bildbereich platziert.

Flipflops. Andere Gatter, die ebenfalls in der Abbildung zu sehen sind, z.T. sogar paarweise, sind vergleichsweise klein.

Dass die markierten Bereiche zu einem Standardzellentyp gehören ist ebenfalls am Grad der “Verzahnung” der Leiterbahnen auf der Schicht M1 zu erkennen. Wenn man ein Gefühl dafür entwickelt, wieviele Flipflops unter der Metall-Maske Platz finden, kann man die Maskengröße als Indiz dafür werten, dass es sich um einen Flipflop handelt. Diese Aussage ist jedoch nicht allgemeingültig. Es gibt Fälle, in denen auf der Schicht M1 Unterschiede in den Verdrahtungsmasken zu finden sind, obwohl es sich um den gleichen Typ Standardzelle handelt.

Kenntnisse von Schlüsselgrößen kryptografischer Routinen helfen ebenfalls. Wird der gesamte Schlüssel in der Hardware gespeichert, müssen sich mindestens entsprechend viele Flipflops finden lassen.

## 6.5. GEZIELTE SUCHE

Es ist möglich, dass die Schaltkreise in einem separaten Bereich platziert sind. Dies ist beispielsweise bei der Realisierung des Dect Standard Ciphers im SC14421CVF der Fall (Abbildung 6.16). Insbesondere sind in derartigen Bereichen hohe Flipflop-Konzentrationen leicht feststellbar.

Darüber hinaus können Masken einzelner Bereiche in Nachfolgern eines Chipdesigns übernommen werden, selbst wenn ein Technologiewechsel im Halbleiterprozess stattfindet. Dies ist nützlich, da man sich bei der Analyse auf Chips älteren Typs konzentrieren kann.

---

## 7 Fazit

Das Reverse-Engineering von Logikschaltungen in Integrierten Schaltkreisen ist mit einfachen finanziellen und technischen Mitteln möglich. Die Kosten für die Ausstattung hängen hauptsächlich davon ab, auf welche Geräte man Zugriff hat und welche Geräte man gegebenenfalls selbst bauen kann. Die Einstiegshürden sind deshalb vergleichsweise gering. Folglich ist die Annahme, dass in Integrierten Schaltungen verborgene Algorithmen gegen Angreifer mit geringem Budget geschützt sind, nicht haltbar.

Das Wissen, das für das Reverse-Engineering von Logik in ICs notwendig ist, kann innerhalb kurzer Zeit erlernt werden. Spezielle Vorkenntnisse sind dafür nicht notwendig.

Der Aufklärung von proprietären Verschlüsselungsverfahren sind im Rahmen des veranschlagten Budgets Grenzen gesetzt. Dieses Budget wird hier mit 1.000 bis 10.000 Euro bemessen. Die technischen Grenzen sind durch die optische Auflösung des Mikroskops festgelegt. Würde man ein größeres Budget veranschlagen, könnte diese Hürde überwunden werden. Für 20.000 bis 30.000 US-Dollar kann man gebrauchte Raster-elektronenmikroskope erwerben, die zur Analyse aktueller Halbleiterprozesse geeignet sind. Es ist ferner davon auszugehen, dass die Preise für Gebrauchtgeräte weiter fallen und geeignete Geräte in wenigen Jahren für unter 10.000 Euro gehandelt werden.

Für das Reverse-Engineering von Logikschaltkreisen gibt es kaum Software. Die wenigen Firmen, die in diesem Marktsegment tätig sind, machen ihre Softwarewerkzeuge nicht publik, da Programme Teil des Geschäftskonzeptes sind. Mangelnde Dokumentation der Prozesse und unzugängliche Software sind höchstwahrscheinlich Ursache dessen, dass dem Reverse-Engineering von ICs bisher kaum Beachtung zuteil wurde.

Das Reverse-Engineering von Logikschaltkreisen ist in vielen Teilen ein kreativer Prozess, der sich jedoch durch Computerunterstützung wesentlich beschleunigen lässt. Es ist daher unumgänglich, Software zu entwickeln, die zur Automatisierung beiträgt.

---

## Literatur- und Quellenverzeichnis

- [Ade08] Sally Adee. “The hunt for the kill switch”. In: *IEEE Spectrum* (Mai 2008). URL: <http://www.spectrum.ieee.org/print/6171> (besucht am 03.03.2010).
- [Ave+02] L. R. Avery u. a. *Reverse Engineering Complex Application-Specific Integrated Circuits (ASICs)*. 2002. URL: [http://www.gemes.com/company\\_info/reverse\\_engineering\\_complex\\_ASICS.pdf](http://www.gemes.com/company_info/reverse_engineering_complex_ASICS.pdf) (besucht am 03.03.2010).
- [Bec98] Friedrich Beck. *Präparationstechniken für die Fehleranalyse an integrierten Halbleiterschaltungen*. VCH Verlagsgesellschaft mbH, 1998. ISBN: 3-527-26879-9.
- [BT94] Inderpreet Bhasin und Joseph G. Tront. “Block-Level Logic Extraction from CMOS VLSI Layouts”. In: *VLSI Design* 1 (3 1994), S. 243–259. DOI: 10.1155/1994/67035. URL: <http://www.hindawi.com/getarticle.aspx?doi=10.1155/1994/67035> (besucht am 03.03.2010).
- [Bue08] Buehler GmbH. *Phoenix Grinder-Polishers*. 2008. URL: <http://www.buehler-met.de/produkte/schleifenpolieren.html> (besucht am 03.03.2010).
- [Che08] Nick Chernyy. *HOW TO: write an IC Friday post*. 2008. URL: <http://microblog.routed.net/2008/07/15/how-to-write-an-ic-friday-post/> (besucht am 03.03.2010).
- [Chi] Chipworks. *Webseiten der Firma Chipworks*. URL: <http://www.chipworks.com/> (besucht am 03.03.2010).
- [HK02] Prof. Dr. rer. nat. H. Kück. *Vorlesung: Aufbau- und Verbindungstechnik von Silizium-Mikrosystemen*. 2002. URL: [http://www.uni-stuttgart.de/izfm/lehre/AVT\\_Geh.pdf](http://www.uni-stuttgart.de/izfm/lehre/AVT_Geh.pdf) (besucht am 01.02.2010).
- [Kad09] Sven Kaden. *Image stitching*. 2009. URL: <http://degate.zfch.de/HAR2009/> (besucht am 03.03.2010).
- [Kin+08] Samuel T. King u. a. *Designing and implementing malicious hardware*. 2008. URL: [http://www.usenix.org/event/leet08/tech/full\\_papers/king/king.pdf](http://www.usenix.org/event/leet08/tech/full_papers/king/king.pdf) (besucht am 03.03.2010).
- [KK99] Oliver Kommerling und Markus G. Kuhn. *Design Principles for Tamper-Resistant Smartcard Processors*. 1999. URL: <http://www.cl.cam.ac.uk/~mgk25/sc99-tamper.pdf> (besucht am 03.03.2010).

- 
- [Noh08a] Karsten Nohl. *Reverse-Engineering Custom Logic (Part 1)*. Sep. 2008. URL: <http://www.flylogic.net/blog/?p=32> (besucht am 03.03.2010).
- [Noh08b] Karsten Nohl. *The Silicon Zoo*. 2008. URL: <http://www.siliconzoo.org/> (besucht am 03.03.2010).
- [NP07a] Karsten Nohl und Henryk Plötz. *24C3 Video Recordings: Mifare - Little Security, Despite Obscurity*. Dez. 2007. URL: [http://chaosradio.ccc.de/24c3\\_m4v\\_2378.html](http://chaosradio.ccc.de/24c3_m4v_2378.html) (besucht am 03.03.2010).
- [NP07b] Karsten Nohl und Henryk Plötz. *24th Chaos Communication Congress: Mifare - Little Security, Despite Obscurity*. Dez. 2007. URL: <http://events.ccc.de/congress/2007/Fahrplan/events/2378.en.html> (besucht am 02.02.2010).
- [NP09] Karsten Nohl und Henryk Plötz. *26th Chaos Communication Congress: Legic Prime - Obscurity in Depth*. Dez. 2009. URL: <http://events.ccc.de/congress/2009/Fahrplan/events/3709.en.html> (besucht am 03.02.2010).
- [Oly08] Olympus Europa Holding GmbH. *Olympus - Motorisiertes Forschungsmikroskop BX61*. 2008. URL: [http://www.olympus.de/microscopy/22\\_BX61.htm](http://www.olympus.de/microscopy/22_BX61.htm) (besucht am 03.03.2010).
- [Pan] Panorama Tools Portal. 2008. URL: <http://www.panotools.org> (besucht am 26.10.2008).
- [Pan08] PanaVue. *PanaVue ImageAssembler 3*. 2008. URL: <http://www.panavue.com/en/products/index.htm> (besucht am 03.03.2010).
- [Sch10] Martin Schobert. *Experiment: IC-Entkapselung mit Kolophonium*. 2010. URL: [https://berlin.ccc.de/mediawiki/index.php?title=Experiment:\\_IC-Entkapselung\\_mit\\_Kolophonium&oldid=7463](https://berlin.ccc.de/mediawiki/index.php?title=Experiment:_IC-Entkapselung_mit_Kolophonium&oldid=7463) (besucht am 03.03.2010).
- [Sch97] Bruce Schneier. *Angewandte Kryptographie. Protokolle, Algorithmen und Sourcecode in C*. 1. Auflage 1996 / 1., korrigierter Nachdruck 1997. Addison-Wesley, 1997. ISBN: 3-89319-854-7.
- [Sko05] Sergei P. Skorobogatov. *Semi-invasive attacks. A new approach to hardware security analysis*. Techn. Ber. UCAM-CL-TR-630. University of Cambridge, Computer Laboratory, 2005. URL: <http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-630.pdf> (besucht am 03.03.2010).

- 
- [Spi95] Der Spiegel. “Tip von Urmel”. In: *Der Spiegel*, 38/1995 (Sep. 1995). URL: <http://www.spiegel.de/spiegel/print/d-9221784.html> (besucht am 03.03.2010).
  - [Str94] Res Strehle. *Verschlüsselt – Der Fall Hans Bühler*. Werd Verlag, Zürich, 1994. ISBN: 978-3859321410.
  - [Tew09] Erik Tews. *26th Chaos Communication Congress: DECT (part II). What has changed in DECT security after one year*. Dez. 2009. URL: <http://events.ccc.de/congress/2009/Fahrplan/events/3648.en.html> (besucht am 03.02.2010).
  - [Tsc08] David Tschumperlé. *GREYCstoration. Open source algorithms for image denoising and interpolation*. 2008. URL: <http://cimg.sourceforge.net/greycstoration/> (besucht am 03.03.2010).
  - [WH05] Neil H. E. Weste und David Harris. *CMOS VLSI Design. A Circuits and Systems Perspective / International Edition*. 3. Aufl. Pearson Education, Inc., 2005. ISBN: 0-321-26977-2.

# *Abbildungsverzeichnis*

3.1	Entfernen von Thermoplasten mittels Aceton . . . . .	8
3.2	IC-Entkapselung durch Kochen in Kolophonium . . . . .	10
3.3	Reinigung der Halbleiterplättchen im Ultraschallreiniger . . . . .	11
4.1	Unterätzung (Foto: Jan Krissler) . . . . .	13
4.2	Poliermaschine Phoenix 4000 der Firma Buehler (Foto: Jan Krissler) .	14
5.1	Mikroskop (Foto: Jan Krissler) . . . . .	15
5.2	Bildausschnitt des Transistor-Layers eines Schaltkreises vom Typ Mi-fare Classic . . . . .	16
6.1	n-Kanal- und p-Kanal-FET auf einem gemeinsamen Substrat . . . . .	19
6.2	n-Kanal-FET unter dem Mikroskop (Chip: Mifare Classic) . . . . .	20
6.3	Drei p-Kanal-FETs in Reihenschaltung (Chip: Mifare Classic). . . . .	21
6.4	CMOS-Inverter . . . . .	22
6.5	Typenweise Anordnung von p- und n-Kanal-Transistoren zwischen den Potentialschienen (Chip: Mifare Classic) . . . . .	23
6.6	Der Materialabtrag beim Polieren der Chipoberfläche war nicht gleich-mäßig. Dadurch ergibt sich eine Blick auf drei verschiedene Ebenen. (Mifare Classic) . . . . .	24
6.7	CMOS-Inverter (Mifare Classic) . . . . .	25
6.8	CMOS-NAND (Mifare Classic) . . . . .	26
6.9	zu identifiziereder CMOS-Schaltkreis [Noh08a] . . . . .	27
6.10	Rekonstruiertes Schaltbild des zu identifizierenden CMOS-Gatters . .	29
6.11	Schaltung eines Flipflops. Die angegebenen Zahlen geben an, welche Transistoren bzw. Transistorenpaare zum Teilgatter beitragen. . . . .	30

## **ABBILDUNGSVERZEICHNIS**

---

6.12 Doppelter Inverter zur Signalauffrischung. . . . .	30
6.13 Transmission-Gate (Bildquelle: Wikipedia) . . . . .	31
6.14 Wiederfinden markanter Muster (Chip: Mifare Classic). . . . .	32
6.15 Manuelles Ermitteln der Gattergrenzen anhand von Verdrahtungsmas- ken (Chip: Mifare Classic) . . . . .	33
6.16 Übersicht des Dect-Chips SC14421CVF. Der Dect Standard Cipher ist innerhalb der Markierung im oberen rechten Bildbereich platziert. . .	34

---

## *A Lizenzbedingungen*

Diese Ausarbeitung ist unter Creative-Commons-Lizenz veröffentlicht (Namensnennung, keine kommerzielle Nutzung, keine Bearbeitung, Version 3.0 Deutschland). Es ist gestattet, das Werk zu vervielfältigen, zu verbreiten und öffentlich zugänglich zu machen. Sie müssen den Namen des Autors/Rechteinhabers in der von ihm festgelegten Weise nennen. Dieses Werk darf nicht für kommerzielle Zwecke verwendet werden. Dieses Werk darf nicht bearbeitet oder in anderer Weise verändert werden.

<http://creativecommons.org/licenses/by-nc-nd/3.0/de/>