Speicherqualifzierung – Datensicherheit in Flash-Speichern

HTV Halbleiter-Test & Vertriebs-GmbH, Bensheim, Deutschland

Kurzfassung

Die weltweit eingesetzte Elektronik befindet sich in einem starken Wandel. Auch Speicherbausteine sind hiervon betroffen. Die aktuelle Entwicklung bei digitalen Speicherbausteinen zielt darauf ab, deren Geschwindigkeit und Datenübertragung zu steigern, den Energieverbrauch zu senken und gleichzeitig die gespeicherte Datenmenge pro Flächeneinheit immer weiter zu erhöhen. Mit diesem Trend geht jedoch auch einher, dass immer weniger Elektronen in einer Speicherzelle eine Information bzw. ein Bit (0 oder 1) repräsentieren. Für die spätere Applikation ist es daher elementar, die Qualität der eingesetzten Speichertechnologie zu kennen, um einen sicheren Betrieb über die gesamte Produktlebensdauer sicherstellen zu können. Die Bensheimer HTV GmbH, einer der weltweiten Marktführer im Bereich Test, Bauteilprogrammierung, Langzeitkonservierung und -lagerung, Analytik sowie Bearbeitung elektronischer Komponenten, qualifiziert und vergleicht, beispielsweise im Auftrag des BSI (Bundesamt für Sicherheit in der Informationstechnik), unterschiedliche Speichertechnologien für Anwendungen mit einer hohen funktionalen Sicherheit.

In dieser Studie werden Flash-Speicher mit unterschiedlichen Technologien von unterschiedlichen Herstellern analysiert (vgl. Tabelle 1).

Tabelle 1: Ausgewählte Flash-Speicher (Angaben aus dem Datenblatt)

Kurzname	Technologie*	Strukturbreite	Bit pro Zelle	Endurance** (min. Anzahl)	Data Retention*** (Jahre)	Speichergröße/ Chipgröße
FG-NOR-320	Floating Gate NOR	320 nm	1	1.000.000	20 (bei 125°C) 10 (150°C)	4 Megabit / 13,62 mm^2
FG-NOR-110	Floating Gate NOR	110 nm	1	1.000.000	20	8 Megabit / 7,63 mm^2
SLC-NAND-34	SLC-NAND	34 nm	1	100.000	10	2 Gigabit / 34,02 mm^2
MLC-NAND-34	MLC-NAND	34 nm	2	3.000	JESD47	32 Gigabit / 85,64 mm^2

* Beim SLC- und MLC-NAND konnte die Strukturbreite nicht exakt aus dem Datenblatt ermittelt werden und wurde geschätzt
** Minimale Anzahl an Lösch-/Programmierzyklen pro Speicherzelle
*** Lagerungszeit nach der die Daten in einer Speicherzelle ohne Betriebsspannung immer noch sicher ausgelesen werden können

Speichertechnologien

Flash-Speicher bzw. Flash-EEPROMs sind aktuell die meist eingesetzten, nicht flüchtigen Speicher in mobilen Geräten. Nicht flüchtig (engl. non volatile) bedeutet, dass Daten, auch nach dem Abschalten der Versorgungsspannung, in der Regel für Jahre im Speicher erhalten bleiben. Sie sind eine Untergruppe der Halbleiterspeicher, kommen z. B. in Speicherkarten und USB-Sticks vor und können sogar in einem Mikrocontroller integriert sein. Ebenso finden sie auch in den sogenannten SSD-Festplatten (Solid-State-Disk) Anwendung.

Aufbau und Funktionsweise einer Speicherzelle mit Floating Gate

Eine einzelne Speicherzelle ist bei einem Flash-Speicher standardmäßig als CMOS-Transistor aufgebaut.

Den logischen Zustand einer Speicherzelle (0 oder 1) repräsentieren dabei die Elektronen im sogenannten Floating Gate des Transistors. Diese beeinflussen die Schwellspannung des Transistors, bei der dieser vom Source- zum Drain-Anschluss leitend wird und einen Stromfluss zulässt.

Im Programmierschritt (engl. program, write) werden vom Source-Anschluss Elektronen in das Floating Gate eingebracht, das vom restlichen Silizium-Substrat über eine Oxid-Schicht isoliert ist. Diese Elektronen hindern anschließend durch ihr elektromagnetisches Feld den Stromfluss im Kanal zwischen dem Source- und Drain-Anschluss.

Der Transistor ist jetzt programmiert und befindet sich der Definition nach im logischen Zustand „0“ (vgl. Abbildung 1).

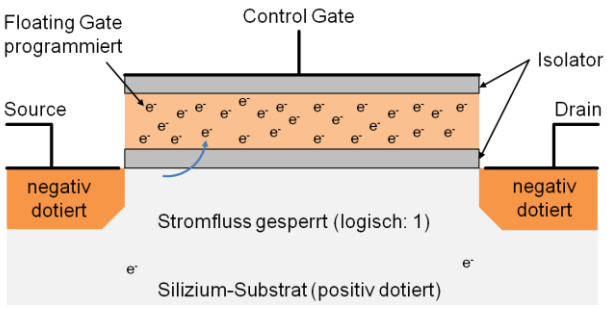

Abbildung 1: CMOS-Transistor (n-Kanal-MOSFET) mit programmiertem Floating Gate (Zustand: 0).

Das Entfernen von Elektronen aus dem Floating Gate wird als Löschen (engl. erase) bezeichnet. Ein Stromfluss durch den Transistor von Source nach Drain ist jetzt aufgrund der geringeren Schwellspannung wieder möglich und sein logischer Zustand ist dann „1“ (vgl. Abbildung 2).

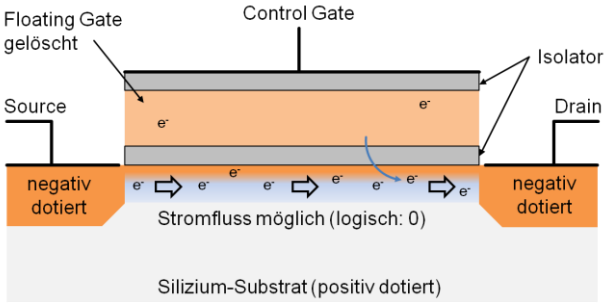

Abbildung 2: CMOS-Transistor (n-Kanal-MOSFET) mit gelöschtem Floating Gate (Zustand: 1).

Der Stromfluss im Transistor ist damit das Maß für die Anzahl von Ladungsträgern im Floating Gate. Er wird beim Lesevorgang über eine interne Spannungsmessung erfasst und anschließend als logischer Zustand interpretiert.

NAND- und NOR-Architektur

Die unterschiedlichen Anforderungen an Flash-Speicher ergeben in der Praxis unterschiedliche Architekturen bzw. Anordnungen einzelner Speicherzellen miteinander. In der NOR-Architektur können Zellen einzeln an beliebiger Stelle im Speicher ausgelesen werden. Diese Eigenschaft benötigen Programme, die Daten direkt vom Speicher abrufen und ausführen müssen.
Die NAND-Architektur verschaltet dagegen mehrere Zellen miteinander (8, 16 oder 32 Zellen), die anschließend nur als Gruppe ausgelesen werden können. Diese Architektur eignet sich gut zum Speichern großer Datenmengen (z. B. als Massenspeicher in einem USB-Stick oder einer SSD-Festplatte), da durch die Verknüpfungen Steuerleitungen entfallen und so Platz auf dem Chip eingespart wird.

Die NAND- und NOR-Architektur sind mit etwa 70% Marktanteil die am häufigsten vertretenen Flash-Speicher Architekturen.

Alterung der Speicherzellen

Damit die Elektronen vom Floating Gate nach dem Programmieren nicht mehr abfließen können, ist das Floating Gate durch eine Oxidschicht (SiO_2) vom Source-Drain-Kanal und Control Gate getrennt.
Programmieren und Löschen sind dabei Operationen mit hoher Spannung und führen neben anderen Effekten zu einer stückweisen Schädigung der Oxidschicht, sodass mit einer zunehmenden Anzahl von Schreib- und Löschzyklen immer mehr Elektronen aus dem Floating Gate über die Zeit abfließen können.
Lesezugriffe erfolgen bei wesentlich niedrigeren Spannungen und tragen daher nur sehr gering zu Alterungseffekten der Speicherzellen bei.
Die Lebensdauer (engl. endurance) einer Speicherzelle ist definiert als ihre maximale Anzahl von Schreib- und Löschzyklen (engl. write/erase cycling Endurance), bei der sie die gespeicherten Daten noch für eine definierte Mindestzeit ohne Spannungsversorgung halten kann. Diese Zeit wird als „Data Retention“ bezeichnet.

Immer weniger Elektronen repräsentieren heutzutage ein Bit

Reduktion der Transistorgröße:
Zur Reduzierung von Kosten und Chip-Fläche werden die Speicherstrukturen bei Flash-Speichern auf einer immer kleineren Fläche realisiert. Der Vergleich der Speicher in Tabelle 1 verdeutlicht diese Tatsache.
Während der Speicher mit Floating Gate NOR-Architektur noch eine Strukturbreite von 320nm aufweist, liegt die Strukturbriete des MLC-NAND-Speichers nur noch bei 34nm.
Aktuelle Speicher können bereits mit Strukturbreiten zwischen 7nm und 5nm gefertigt werden.

Erhöhung der Bitanzahl pro Speicherzelle:
Anfänglich wurde in einer Speicherzelle nur ein Bit (Zustand: „0“ oder „1“) gespeichert. Diese Zellen werden als SLC (engl. single-level cell) bezeichnet. Um die Speicherdichte der Flash-Speicher aber weiter zu erhöhen, ohne physikalisch die Speicherzellen ändern zu müssen, werden weitere Spannungsniveaus innerhalb einer Zelle bzw. eines Transistors definiert. Dadurch wird es möglich, mehrere Bits in einem Transistor in Form unterschiedlicher Spannungsniveaus zu realisieren. Intel führte solche MLC-Speicher (engl. multi-level cell) unter der Bezeichnung „StrataFlash“ erstmals

1997 im Markt ein. Inzwischen gibt es bereits MLC-Zellen, die bis zu 4 Bits speichern können.
Die Verkleinerung der Flash-Zellen und die mehrfache Speicherung von Bits pro Zelle führen dazu, dass immer weniger Elektronen ein Bit repräsentieren. Während in der Vergangenheit über 100.000 Elektronen ein Bit repräsentierten, sind es bei aktuellen MLC-NAND-Flash-Speichern nur noch wenige Tausend.
Die Betrachtung der Speicher aus Tabelle 1 verdeutlicht diesen Trend. Während bei der Floating Gate NOR-Architektur mit einer Strukturbreite von 320nm nur 0,3 Megabit/mm^2 gespeichert werden, sind es beim genannten MLC-NAND-Speicher mit einer Strukturbreite von 34nm bereits 373,7Megabit/mm^2 (vgl. Abbildung 3).

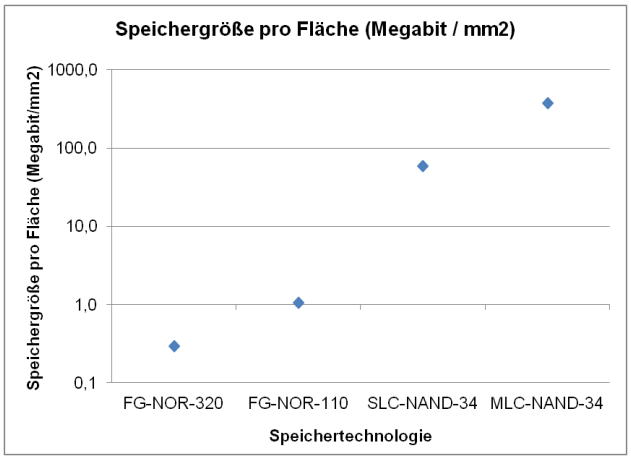

Abbildung 3: Speichergröße pro Fläche.

Moderne NAND-Flash-Speicher weisen daher eine immer geringere Endurance und kürzere Data Retention auf (vgl. Tabelle 1). Waren bei der Floating Gate NOR-Architektur noch mindestens 1.000.000 Schreibzyklen zulässig, sind es beim vorgestellten MLC-NAND-Speicher nur noch 3.000 Lösch- und Schreibzyklen!
Inzwischen kommt es daher auch immer häufiger vor, dass kosmische Strahlung die Elektronen eines Transistors aus dem Floating Gate herausschlägt und es dadurch zu einem Bitkippen kommt. Dieser Effekt wird als Single Event Upset (SEU) bezeichnet.

Defekte Zellen von Anfang an

Aufgrund ihrer Größe und gleichzeitig feinen Strukturen können NAND-Flash-Speicher nicht mehr fehlerfrei gefertigt werden. Daher weisen NAND-Flash-Speicher bereits bei der Auslieferung fehlerhafte Speicherbereiche (engl. bad block) auf. SLC-Speicherzellen weisen ca. 2% und MLC-Speicherzellen ca. 5% fehlerhaft Speicherbereiche auf, die im Chip entsprechend gekennzeichnet sind und nicht verwendet werden dürfen.

Flash Management zur Linderung

Um die moderne NAND-Technologie trotz ihrer Anfälligkeit in Bezug auf Bitfehler und geringer Lebensdauer dennoch nutzen zu können, muss ein aufwändiges Flash-Management verwendet werden, um Datenverlust durch beschädigte Zellen vorzubeugen und so die Lebensdauer des Speichers zu maximieren. Das Flash-Management hat dabei folgende Aufgaben:

- Alle Speicherbereiche werden gleichmäßig abgenutzt (engl. wear leveling).
- Datenfehler bei Schreib- und Lesezyklen werden über Prüfsummen erkannt und korrigiert.
- Fehlerhafte Speicherbereiche (engl. bad block) werden markiert und deren weitere Verwendung verhindert.

Praktische Messreihen

Für den praktischen Vergleich der Speicher aus Tabelle 1 wurde beim Testspezialisten HTV eine Speicherqualifikation mit folgendem Vorgehen durchgeführt:

- Einzelne Speicherbereiche bzw. Blöcke werden mit einer unterschiedlichen Anzahl von Lösch- und Schreibzyklen gealtert (Gebrauchsalterung).
- Anschließend werden die gealterten Blöcke mit Testdaten programmiert.
- Für den beschleunigten Abfluss von Elektronen aus dem Floating Gate werden die Bauteile dann bei einer Temperatur von 150°C gelagert und zyklisch nach einer Zeit von 24h ausgelesen und der Speicherinhalt auf Bitfehler bzw. Bitkipper untersucht.

Ergebnisse der Floating Gate NOR-Architektur (320nm und 110nm):
Für die Floating Gate NOR-Architektur mit einer Strukturbreite von 320nm und 110nm ergeben sich selbst in Blöcken mit einer Gebrauchsalterung von 70.000 Lösch- und Schreibzyklen auch nach einer Zeit von 8 Tagen keine Bitkipper.
Dieses Ergebnis war zu erwarten, da diese Bauteile laut Datenblatt eine Endurance von 1.000.000 Lösch- und Schreibzyklen und eine Data Retention von 20 Jahren aufweisen.

Ergebnisse SLC-NAND-Architektur (34nm):
Einen deutlichen Anstieg bei den Bitkippern zeigen dagegen die NAND-Speicher. Bei einer Strukturbreite von 34nm zeigt sich bereits eine deutliche Zunahme von Bitkippern während der Beschleunigten Alterung der Zellen (vgl. Abbildung 4).

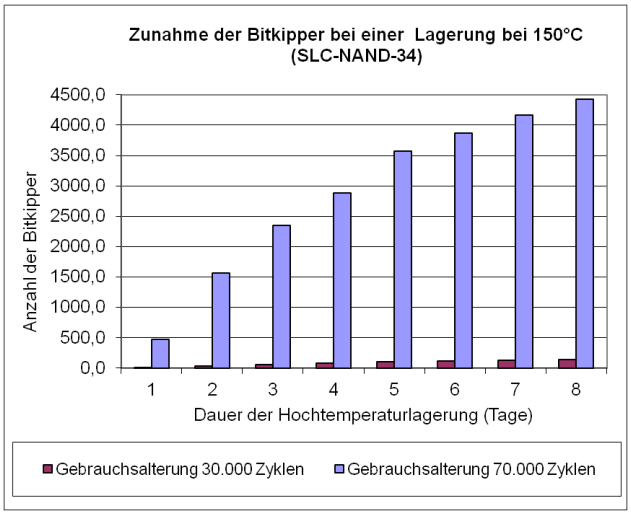

Abbildung 4: Bitkipper in Abhängigkeit von der Gebrauchsalterung (Mittelwert von 8 Bauteilen).

Ergebnisse MLC-NAND-Architektur (34nm):
Die MLC-NAND-Speicher mit einer Strukturbreite von 34nm weisen im Vergleich zu den SLC-NAND-Speichern eine noch weitaus höhere Anzahl von Bitkippern auf und haben damit die geringste Data Retention aller in dieser Studie vorgestellten Speicher. Eine deutliche Zunahme von Bitkippern kann hier bereits schon bei Zellen festgestellt werden, die nur einmalig programmiert wurden (vgl. Abbildung 5).

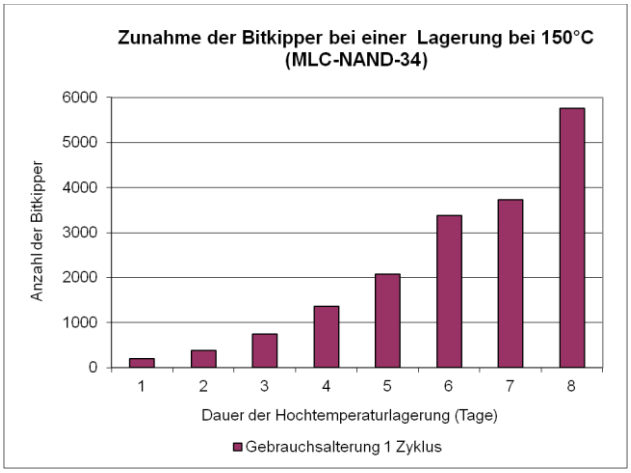

Abbildung 5: Viele Bitkipper in Zellen mit nur einmaliger Programmierung (Mittelwert von 8 Bauteilen).

Fazit

Zur Einschätzung der Qualität eines nicht flüchtigen Speichers stellen die Endurance und die Data Retention wichtige Parameter da.
Aktuelle Flash-Speichertechnologien nutzen sich mit der Zeit ab. Für Neuentwicklungen elektronischer Geräte sollte daher das Speicherkonzept passend zur Lebensdauer des Produktes ausgelegt werden.
HTV unterstützt seine Kunden sowohl bei der Speicherqualifikationen als auch der Auswahl eines passenden Speicherkonzeptes.
Zusätzlich können bei HTV elektronische Speicher für die Serienfertigung sowohl programmiert als auch kundenspezifisch konfektioniert und markiert werden.