電子回路部品の偽造品を検出

コピーできないアナログ情報を利用する新手法

国際公開番号
WO2012/014623
(国際公開日：2012.2.2)

研究ユニット：

ナノエレクトロニクス研究部門

適用分野：

- 半導体分野
- 検査装置分野
- セキュリティ分野

目的と効果

深刻化する電子回路部品（LSIなど）の偽造品対策として、レーザーや特殊インクによって二次元バーコードをLSIパッケージや内部のシリコンチップにマーキングする技術が実用化されています。LSIごとにバーコードを付与する流通管理はとても効果的ですが、デジタルデータであるバーコードはコピーすることができます。この発明は、LSIの動作時の消費電力波形や放射電磁波形を測定･記録し、そのアナログデータをコピーできない情報として真贋判定に用いるものです。同じ論理回路のLSIでも、製造工場や製造時期の違いによりアナログ特性が異なるため、リバースエンジニアリング（製品の分解、解析）によって偽造したものを識別することが可能になりました。また、低速なプロセッサの表記を高速版と偽装する手口も、その特性の違いから検出することができます。

技術の概要

図１に示すように、LSI 製造時の検査過程で回路の動作波形を製造番号と共にデータベースに保存しておきます。真贋判定時には、LSI の製造番号をデータベースで検索し、動作波形を比較します。図２からわかるように、真贋を判定できます。また、同じ工場で同時期に作られた LSI のアナログ特性は、異なる工場で作られた偽物とは大きく異なるので、個々のLSIの動作波形ではなく、製造ロットごとに代表となる波形を登録することもできます。さらに真贋判定のための特徴のある電力・電磁波形を生成する専用回路を LSI 中に実装することが、この手法の実施にとても有効となります。

発明者からのメッセージ

LSI のばらつきから固有 ID を生成し、LSI の指紋のように利用する個体判別技術（PUF：Physically Unclonable Function）も偽造防止法として大きな期待が寄せられています。しかし、計算機で PUF による ID 生成を模擬することが可能な場合があります。一方、指紋認証装置では、指紋パターンをコピーしたゴム指などを排除するために生体検知が行われています。この発明を生体検知のように利用し、PUF のセキュリティをより強固なものにすることができました。PUF の技術は、利用が急拡大している IC カードに対する偽造対策として有望視されています。

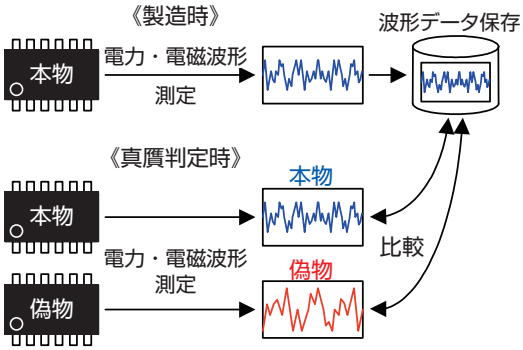

図1　LSIの製造時に電力･電磁波形を測定してデータベースに保存し、真贋判定時にはLSIを動作させて測定した波形をデータベースと照合する

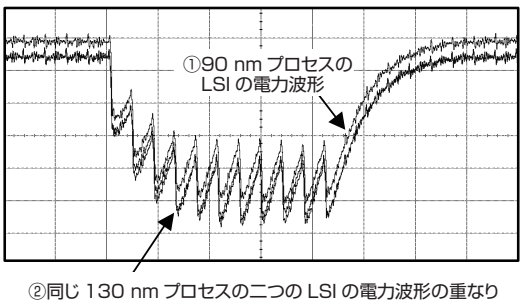

図2　異なる製造プロセスによって作られたLSI製品の電力波形
波形①と②のように、製造プロセスが異なると、同じ論理回路であっても電力波形が一致しない。一方、波形②のように、同じ製造プロセスで異なる時期に製造したLSI製品の動作時の波形は完全に一致している。

知的財産権公開システム（IDEA）は、皆様に産総研が開発した研究成果をご利用いただくことを目的に、産総研が保有する特許等の知的財産権を広く公開するものです。

IDEA
産総研が所有する特許のデータベース
http://www.aist.go.jp/aist-idea/