PUFによる個体認証セキュリティ技術へのランダムテレグラフノイズの適用

Application of Random Telegraph Noise to Individual Authentication Technology Using Physical Unclonable Function (PUF)

陳　杰智　■CHEN Jiezhi
棚本　哲史　■TANAMOTO Tetsufumi
三谷　祐一郎　■MITANI Yuichiro

トランジスタの微細化に伴って，近年ランダムテレグラフノイズ（RTN）というトランジスタの動作電流が不規則に揺らぐ現象の影響が顕著になってきている。RTNは，CMOS（相補型金属酸化膜半導体）イメージセンサや，フラッシュメモリ，3次元構造のトランジスタなど，様々なデバイス（以下，チップと呼ぶ）の信頼性に影響を及ぼすことが懸念されている。

東芝はこれまで，RTNに寄与する欠陥の時定数に注目し，欠陥時定数のばらつき及びそのばらつきを支配している物理機構を実験的に明らかにしてきた。今回，その欠陥の時定数の特徴と事象のランダム性を利用して，情報セキュリティへの応用，特にPUF（Physical Unclonable Function）への適用を考案した。RTNを適用したPUFは，チップ個体のID（Identifier）を短時間で生成できるうえに，100万回以上利用しても安定してIDを生成できる高い耐性を持つことを実証した。

With the acceleration of downscaling technologies for transistors in recent years, random telegraph noise (RTN) has been attracting considerable attention due to its large impacts on transistor operating current fluctuations. The effects of RTN on the reliability of complementary metal-oxide semiconductor (CMOS) image sensors, flash memories, and three-dimensional transistors are a matter of concern.

Toshiba has been conducting studies on random variations in the time constants of traps that cause RTN and the dominant physical mechanisms of these variations through experiments, and confirmed that the time constants of RTN traps in individual chips are quite stable under electrical stressing. Focusing on highly stable and highly random characteristics of the time constants of RTN traps, we have applied RTN to a physical unclonable function (PUF) technology, one of the important security technologies for individual authentication. From the results of experiments using a newly developed algorithm, we have confirmed that the information of RTN traps can be successfully detected and that this RTN-based PUF technology can not only convert RTN into a chip ID in a sort time, but also achieve ID reading cycles of more than one million times by measuring the hamming distance (HD) as an index of stability.

1　まえがき

企業機密や個人情報の漏えいが問題になるなか，セキュリティの重要性がますます高まっている。エレクトロニクス分野でもスマートコミュニティにおけるクラウドサービスの展開に伴って，セキュリティの強化に関する研究開発が盛んになってきた。

PUF（Physical Unclonable Function）は，チップを構成する個々の素子特性のばらつきをそのまま“チップ指紋”として利用する情報セキュリティ技術である。PUFで生成したチップのID（以下，PUF IDと呼ぶ）を用いて作った暗号は，同じ指紋を持つチップでなければ復号できないため複製の不可能性が高く，更に低コストである点などから注目を集めている[(1), (2)]。PUFには，大きく分けてSRAM（Static RAM）型とArbiter型があり，どちらも製品化されている。オランダIntrinsic-ID社が開発したSRAM型のPUFは，電源を入れた直後のSRAMの初期値の個体差を利用するものであり，Arbiter型は回路内の配線遅延の差を利用する。これらの従来のPUFは，主にトランジスタのオン／オフを決定するしきい値電圧を基準としている。しかし，トランジスタのしきい値電圧は経時変化を伴うため，使用を繰り返すうちにPUF IDが初期に設定したものから徐々に変わってしまうことが問題になる。したがって，今後，PUFの実用化と普及が進むにつれて，経時変化の少ないPUFが重要になってくると考えられる。

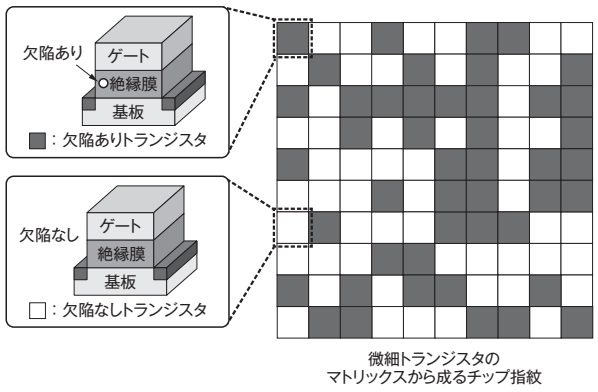


図1．絶縁膜中の欠陥分布を利用するPUFの概念 ― 微細トランジスタの欠陥分布をビット列化してチップ指紋を生成する。
Concept of PUF using trap distribution in dielectrics

東芝は，今回，トランジスタの信頼性上問題となってきたRTNに寄与する絶縁膜欠陥の時定数の安定性に注目し，逆

転の発想でこれを利用して，経時変化が少ないPUFを実現してセキュリティへ応用し，その有望性を見いだした。RTNを利用したPUFの概念を**図1**に示す。

ここでは，当社が考案した，RTNを用いたPUF IDの生成方法，及び多数回の使用に対する耐性を実証した結果について述べる。

2　RTN 現象と評価手法

近年，RTN現象は多くのチップにおいて報告されている。一般に観測されるRTN現象は，チャネルを流れる電子又は正孔の絶縁膜中欠陥への捕獲と放出によって発現すると考えられ，この欠陥をそれぞれ電子欠陥及び正孔欠陥と呼ぶ。通常，RTN現象を測定するには，一定のゲートバイアス電圧を印加しながらチャネル電流を測定して，欠陥がキャリアを捕獲するまでの時定数（τ_c）とキャリアを放出するまでの時定数（τ_e）それぞれの平均値，及び熱平衡状態での時定数（τ_0：$\tau_c=\tau_e$のときの時定数）を欠陥の特徴量として抽出する。

今回のRTN測定は，ノイズ評価専用の高速測定システムを用いて行った。サンプリングレートは最高1メガサンプル（MS）/sである。測定結果の例として，電流振動特性を**図2**(a)に，τ_c，τ_e，及びτ_0のゲートバイアス電圧V_gとの関係を図2(b)に示す。電流振動特性は，絶縁膜に存在するRTNに寄与する欠陥（以下，RTN欠陥と呼ぶ）のランダムな分布と測定時のV_gに依存しているので，結果として各チップのRTNはランダムな特性を示す。

また図2(c)には，式(1)で定義される，時定数のゲートバイアスカップリング$\alpha_{\tau c/\tau e}$とτ_0の関係を示す。

$$\alpha_{\tau c/\tau e}=(kT/q)\left(\partial \ln\left(\tau_c/\tau_e\right)/\partial V_g\right) \quad (1)$$

q：電子の電荷
k：ボルツマン定数
T：環境温度

$\alpha_{\tau c/\tau e}$は，界面からのRTN欠陥深さ（X_T）と式(2)に示す関係を持つとされている[3]。

$$X_T/T_{ox}=-\alpha_{\tau c/\tau e} \quad (2)$$

T_{ox}：ゲート絶縁膜の厚さ

$\alpha_{\tau c/\tau e}$が大きく，つまりRTN欠陥が界面から遠くなると，RTN欠陥とチャネルの電荷間のやり取りが遅くなり，時定数も長くなると考えられるが，図2(c)の実測データを見ると，τ_0と$\alpha_{\tau c/\tau e}$との間に有意な相関は見られず，このことからも，RTN欠陥がランダムに分布していることが裏づけられる。

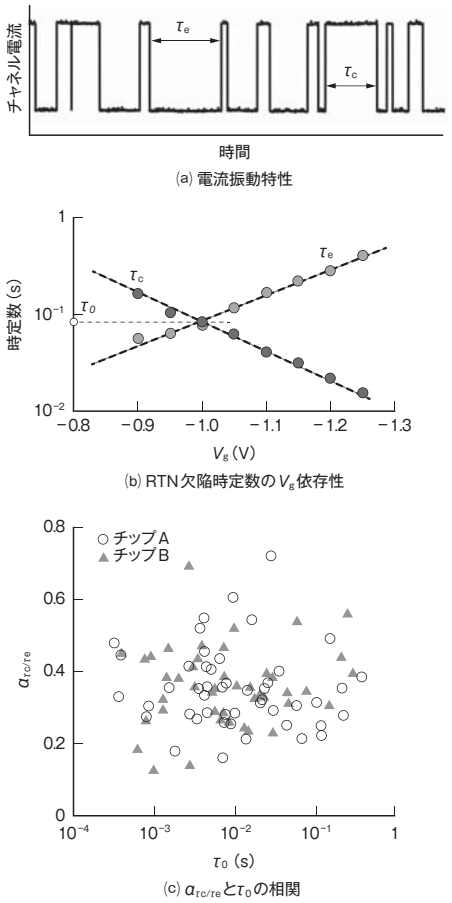
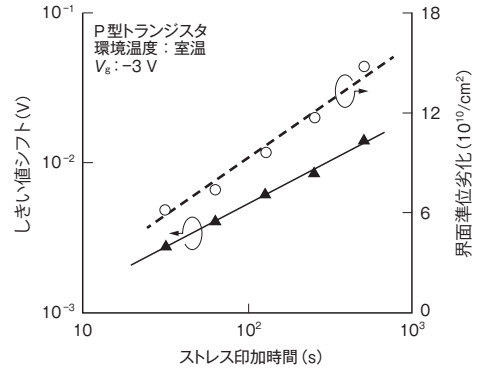


図2．RTN現象 ― RTNによる電流振動特性は，絶縁膜中の欠陥とゲートバイアス電圧に依存する。$\alpha_{\tau c/\tau e}$とτ_0の間に相関関係がないことから，欠陥が絶縁膜中でランダムに分布しているために，電流振動がランダムになることが裏づけられる。
Observed channel current fluctuations caused by RTN traps

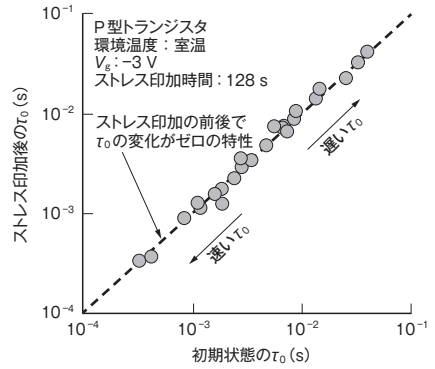
3　実験結果と考察

3.1　RTN欠陥のストレス耐性

まず，チップの特性を特徴づけるRTN欠陥の時定数に対して電気ストレス印加の前後で変化があるかどうかを評価した。実験方法として，ストレス印加前のτ_0を測定した後に，室温で電気ストレス（例えばトランジスタのゲートに-3 Vの一定電圧ストレスを印加）を長時間（例えば128 s間）印加し，その後のτ_0を測定した。電気ストレス印加に伴う界面準位の劣化としきい値の変動を**図3**(a)に，ストレス印加前後のτ_0の比較を図3(b)に，それぞれ示す。図3(a)に示すように，電気ストレスの印加はトランジスタの界面準位の劣化やしきい値変動などトランジスタ特性そのものに経時変化を引き起こす。しかしτ_0については，図3(b)に示すように，τ_0の大小にかかわらず電気ストレスによって変化しないことがわかる。更に，図3に示す正孔欠陥（p型トランジスタの場合）だけではなく，n型トランジスタのRTNに寄与する電子欠陥のτ_0についても同様の実験結果



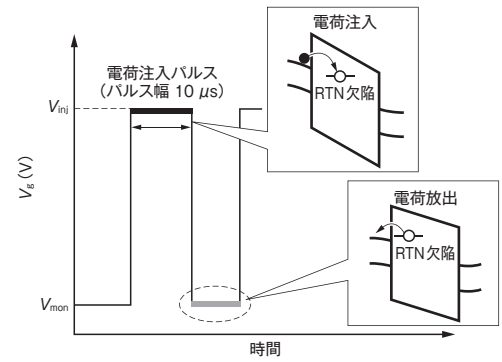
(a) ストレス印加によるトランジスタ特性の変化



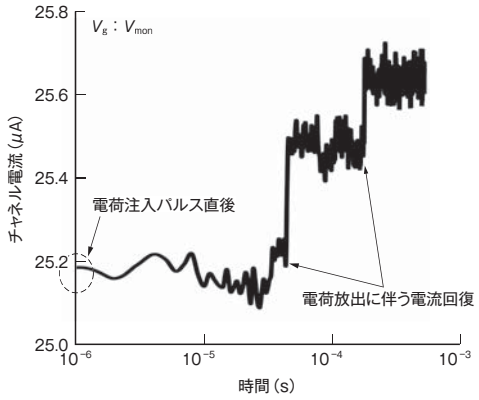
(b) ストレス印加前後のτ_0変化

図3. RTN欠陥の時定数のストレス耐性 — トランジスタ特性は電気ストレス印加によって変化するが，RTN欠陥の時定数は影響を受けず，ストレス耐性を持つことがわかる。

Stress-free properties of time constants of RTN traps



(a) RTN欠陥での電荷の注入と放出



(b) チャネル電流回復の例

図4. RTN欠陥によるチャネル電流回復現象 — 電荷注入パルスによってRTN欠陥に注入された電荷が，低バイアス電圧で放出されることによって，チャネル電流が階段状に回復する。

Channel current recovery phenomena caused by RTN traps

が得られている[4]。これらのことから，界面状態や界面準位の劣化（おそらく膜中準位の劣化も）はτ_0には影響せず，RTN欠陥としての特徴は，安定して維持されることが明らかになった。

3.2 PUFへのRTNの応用

当社は，RTN欠陥の時定数のランダム性及び電気ストレスに対する安定性を利用して，経時変化に強いPUFへ応用することを考案した。RTN特性のPUF応用を考えるうえで最初に考えなければならないのは，チップID 生成の時間である。従来のRTN評価では長時間のサンプリングが必要であった。しかしPUFへの応用を考えると，短い時間でRTNをチップIDに変換できるアルゴリズムが必要になる。

当社は今回，短時間でRTN欠陥を検知するための新たなアルゴリズムを考案した。その概要を**図4**に示す。まず，大きさV_{inj}の電荷注入パルス（パルス幅10 μs）を微細トランジスタのゲートに印加し，続いて低バイアス電圧（V_{mon}）でチャネル電流I_{inj}を測定する。電荷注入パルスによりRTN欠陥に電荷が注入され，続く低バイアス電圧でその電荷がRTN欠陥から放出されれば，チャネル電流の回復（階段的に初期電流より大きくなる）が観測される。

一方，RTN欠陥がない場合は，電荷が捕獲及び放出されないので，チャネル電流の回復は観測されない。このような特徴を利用してPUF IDを生成する方法を，次に述べる。

まず，チップを構成する微細トランジスタについて，式(3)で定義されるRを求める。

$$R = \Delta I_d / I_{ref} = (I_{ref} - I_{inj}) / I_{ref} \quad (3)$$

I_{ref}：電荷注入パルスがないときの参照電流

V_{mon}印加中に，ある基準値（例えば1 %）を超えるRが1回でも観測されれば欠陥を検知できたとして，微細トランジスタの出力信号が“1”のデジタル信号に変換される。一方，V_{mon}印加中に基準値を超えるRが観測されなければ，欠陥が検知できなかったとして，微細トランジスタの出力信号が“0”のデジタル信号に変換される。このとき，ランダム性を保障するために，電荷注入パルス条件に応じて基準値を調整する。更に，“1”又は“0”と変換されたデジタル信号の不安定性を低減するために，複数回の測定結果の多数決を取る。例えば，11回IDを読み込み，RTN欠陥が6 ～ 11回検知された場合に最終的に“1”の信号に変換する。

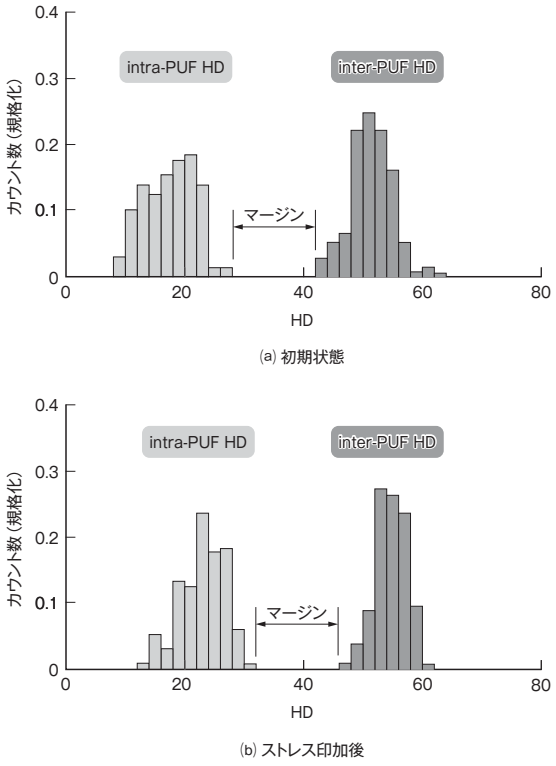


図5．RTNを適用したPUFの電気ストレス耐性 — 電気ストレスを100万回印加した後でもHDがほとんど劣化しないことから，RTNを適用したPUFは高い電気ストレス耐性を持つことがわかる。
Stress-free properties of RTN-based PUF

電荷注入パルスの印加時に，電気ストレスによってトランジスタの界面欠陥及び絶縁膜中の欠陥が増加するが，3.1節で述べたようにRTN欠陥の時定数は電気ストレス印加によって変動しないことから，IDは安定して取得できると考えらえる。

このアルゴリズムを検証するため，前述の電荷注入パルスを100万回繰り返してPUF信号を読み出すのと同等のストレスを想定し，同じ大きさV_{inj}の電気ストレスを100 s間印加して，ID生成の安定性を測定した。PUF IDの安定性に関する重要な指標として，ハミング距離（HD：二つのビット列を比較し，対応する位置のビット値が異なっている場所の数）を利用した。

同じチップでのHD（intra-PUF HD）と異なるチップのHD（inter-PUF HD）の測定結果の例を**図5**に示す。intra-PUF HDの最大値とinter-PUF HDの最小値の差を“マージン”と呼び，これが不十分であるとチップが自他のPUF IDを区別できず，暗号化や復号には利用できなくなってしまう。ストレス印加前後のHDを比較した結果，マージンの劣化はほとんど観測されなかった。従来のSRAM型PUFは，素子の劣化に伴ってしきい値ばらつきの相対値が変化することで，マージンが狭くなってPUF IDが認識できなくなることが問題であった。これに対し，RTN PUFは各素子のしきい値ばらつきに依存せず，また電気ストレスによる素子劣化が起こってもIDを安定して生成できることが実証された。

今後の課題は，IDの温度変化などの問題である。温度が変化すると，一定電荷注入パルスで検知できる欠陥の分布が変わるので，ID認識に制限が出てくる可能性がある。その対策として，例えば温度領域を切り分け，各温度領域にそれぞれのPUF IDを用意しておく方法などが考えられる。また，回路上でトランジスタをペアに接続して，二つのトランジスタ間のID分布の差を活用するなどの方法も考えられる。このような温度対策を含め，今後実用化に向けた検討を進める。

4　あとがき

クラウドサービスの展開に伴い，セキュリティの強化が非常に重要な課題となっている。今回，トランジスタのRTNに関連する信頼性評価及び解析の結果に基づき，短時間でチップのIDを生成でき，かつ繰り返し使用に対して高い耐性を持つRTN PUFの応用可能性を実証した。PUFの実用化と普及をいっそう加速していく。

文　献

(1) Su, Y. et al. "A 6.3pJ/b 96% Stable Chip-ID Generating Circuit using Process Variations". 2007 IEEE International Solid- State Circuits Conference (ISSCC). San Francisco, CA, USA, 2007-02, IEEE. 2007, p.406 - 407, 611.
(2) Mathew, S. K. et al, "A 0.19pJ/b PVT-Variation-Tolerant Hybrid Physically Unclonable Function Circuit for 100% Stable Secure Key Generation in 22nm CMOS". 2014 IEEE ISSCC. San Francisco, CA, USA, 2014-02, IEEE. 2014, p.278 - 279.
(3) 陳 杰智 他. 微細電界効果トランジスタにおけるランダムテレグラフノイズを引き起こす欠陥機構の解明. 東芝レビュー. **68**, 8, 2013, p.27 - 30.
(4) Chen, J. et al. "Further Understandings on Random Telegraph Signal Noise through Comprehensive Studies on Large Time Constant Variation and its Strong Correlations to Thermal Activation Energies". 2014 Symposium on VLSI Technologies. Honolulu, HI, USA, 2014-06, IEEE. 2014, p.202 - 203.

陳　　杰智　CHEN Jiezhi
研究開発統括部 研究開発センター LSI基盤技術ラボラトリー 研究主務。ゲート絶縁膜の信頼性技術の研究・開発に従事。応用物理学会会員。
Advanced LSI Technology Lab.

棚本　哲史　TANAMOTO Tetsufumi
研究開発統括部 研究開発センター LSI基盤技術ラボラトリー 主任研究員。半導体ナノデバイス集積回路及びそのセキュリティ応用の研究・開発に従事。日本物理学会，応用物理学会会員。
Advanced LSI Technology Lab.

三谷　祐一郎　MITANI Yuichiro
研究開発統括部 研究開発センター LSI基盤技術ラボラトリー 研究主幹。ゲート絶縁膜の信頼性技術の研究・開発に従事。応用物理学会会員。
Advanced LSI Technology Lab.