高度情報セキュリティ向け 超小型乱数生成回路

Ultrasmall Random Number Generators for High-Level Information Security

藤田　忍　内田　建　安田　心一

■FUJITA Shinobu　■UCHIDA Ken　■YASUDA Shinichi

情報セキュリティを支える暗号・認証技術において，高品質な乱数は不可欠な要素の一つであり，乱数の品質が全体の安全性を大きく左右する。実際に利用されている乱数は，ソフトウェアによる算術乱数か物理現象を利用した物理乱数に属する。モバイル機器ではハードウェア上の制約が強く，乱数生成にも超小型の専用回路が必要である。

東芝は，LSIを構成するナノスケールのシリコンデバイスに発生する物理的な揺らぎ信号を利用した，高品質の乱数生成が可能な超小型回路を開発した。

High-level random number generators (RNGs) are required for information security systems such as authentication and cipher systems. In engineering use, random numbers are generated either arithmetically or physically. Especially for mobile devices, small RNGs are essential as the hardware resources are strictly limited.

Toshiba has developed ultrasmall RNGs that can generate high-quality random numbers. In these circuits, fluctuating signals observed in nano-scale silicon devices are utilized as the origin of randomness.

1 まえがき

ネットワーク上でやり取りされる情報のセキュリティを保つのに，暗号技術，認証技術，アクセス制御技術などが用いられる。乱数は，これらにかかわる基盤技術である。例えば，チャレンジレスポンスなどによる機器間の認証手続き，ID（IDentification）やパスワードといった個人の認識情報の生成，暗号の鍵生成などに乱数が使われる。セキュリティシステムに要求される乱数の本質は，予測の困難性に尽きる。理想的な乱数生成器とは，生成器の設計者ですら出力を予想できないものを意味する。予測困難性という性質は，デジタル機器に内蔵されている機密情報の読取り，改ざんの防止技術，耐タンパ技術にも幅広く応用することができる。

ここでは，理想に近い乱数が生成でき，かつ，モバイル情報機器にも搭載可能な超小型物理乱数回路技術について述べる。超小型物理乱数回路技術は，情報セキュリティが利用できる範囲を大幅に拡張すると期待される。

2 乱数生成回路の動向

情報セキュリティ技術で利用される乱数とは，通常，0と1のビットがランダムに並んだビット列のことを意味する。理想的な乱数は真正乱数と呼ばれ，0と1の分布，ビット間の相関，周期性などの規則性をいっさい持たないものを指す。従来，算術的に作った擬似的な乱数が利用されてきたが，今後は，一段と高い品質の乱数が必要となる。

2.1 算術乱数と物理乱数

実際に利用される乱数には，物理現象に基づいて作られる物理乱数と，一定のアルゴリズムで作られる算術乱数がある。後者では，基本的にある種の初期値設定が必要で，同じ初期値に対して同じ乱数列を作り出す再現性がある。更に，同じビット列を繰り返す周期性があり，真正乱数ではないという意味で，擬似乱数とも呼ばれる。擬似乱数生成方式としては，フィードバックレジスタ回路で生成されるM系列（線形最大周期列）と呼ばれる擬似乱数が有名である。算術乱数を情報セキュリティに使う場合には，この周期を十分長くすることと，初期値自身を毎回変更する工夫が必要である。

それに対して物理乱数は，大きな自由度を持った物理現象を利用し，外界と予測不能な相互作用を持つので，周期性や再現性は存在せず，初期値設定も不要である。ビット間の相関をなくすことも，物理量を適切に選ぶことで，原理的には実現可能である。以下で，物理乱数の生成源として熱雑音，量子光学（偏光），発振回路を利用した生成方式について述べる。

2.2 熱雑音を利用した物理乱数生成

電子が導体内を粒子として移動する際に，電子個々に生じるランダムな運動が，電気信号にノイズを発生させる。これが熱雑音で，ジョンソンノイズとも呼ばれる。熱雑音は，大きい場合でも数十μVで，演算増幅器や差動アンプを使い

4～5けた程度信号増幅してAD（Analog to Digital）変換する。更に一様性（0と1の均等性）や自己相関性を改善するためのデジタル処理が行われる。基本的にアナログ回路であり，回路サイズが大きくなる。しかし，熱雑音増幅型の物理乱数回路は，情報セキュリティ用に利用されている乱数生成回路の中でもっとも高度なものであり，生成された乱数は，数学的に真の乱数（真性乱数）に近い。これは，サーバやクライアントPC（パソコン）の一部に使われている。東芝からも，既にワークステーションやデスクトップPC向けに製品化されている。

2.3 量子光学を利用した物理乱数生成

量子光学を利用した乱数生成回路も開発されている。単一の光子の偏光方向は，観察するときに初めて決定され，その方向は完全にランダムであるという量子光学の原理に基づく。この量子光学乱数生成器は，光学機器の一種なので，信号をデジタル乱数化するための補正回路も必要であり，生成器自体の大きさは熱雑音増幅型乱数生成器よりも更に大きい。

2.4 発振回路を利用した物理乱数生成

物理乱数生成回路に準じるものとして，発振回路型乱数回路がある。これは，高速で発振する回路に対して，非同期の低速カウンタで1ビットデータとして読み込み，それを平滑化（0,1の出現を均等化すること）することで乱数化するもので[(1)]，古くから知られている。増幅が不要なので，熱雑音増幅型回路よりは小さいものの，回路はやや大きめになる。発振回路が持つ周期性が乱数に残ってしまう傾向があり，熱雑音増幅型よりも乱数の質は落ちる。また消費電流が大きいという欠点もある。

2.5 乱数の品質と回路サイズの関係

回路の乱数の質（規則性がないほど，一様性が良いほど，自己相関性が弱いほど，質が高い）を縦軸に，回路サイズを横軸に取って，各乱数回路のおおよその性能を**図1**に示した。これらの乱数生成器を比較すると，回路の大きさが大きいほど乱数の質が高いというトレードオフが存在していることがわかる。

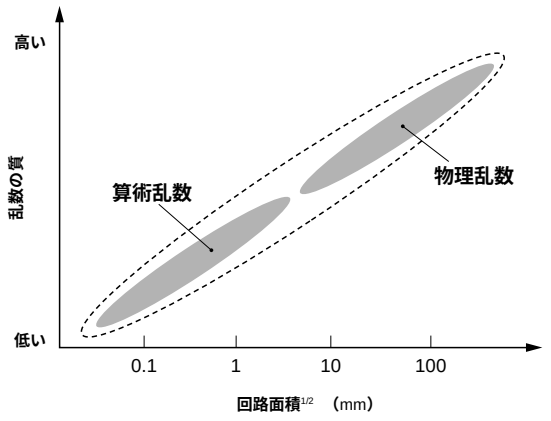


図1．従来型乱数生成回路のトレードオフ ― これまでの技術では，乱数の質を高めるためには回路を大きくする必要があった。
Trade-off of conventional RNG

3 小型乱数生成回路の開発

ICカード，携帯電話，PDA（携帯情報端末）などモバイル情報機器の利用が急速に拡大しつつある。このような機器では，情報の信頼性を保ち，盗聴や紛失などによる情報漏洩（ろうえい）のリスクに対処するため，暗号化と認証の機能が不可欠である。

モバイル機器では，従来，実装上の制約から小型の算術乱数回路しか搭載できなかった。この場合，乱数のレベルを上げるために，この周期を十分長くすることと，初期値自身を毎回変更するための回路や，生成した乱数を再度暗号モジュールで再攪拌（かくはん）するための回路が必要である。しかし，これらの付属回路は，算術乱数回路自体よりも大きいため，結局，搭載不可能となる場合が多い。したがって，モバイル機器では高いセキュリティレベルを提供する乱数回路を実現することが困難であった。

ここで，仮に物理乱数生成回路がモバイル機器に搭載可能な程度に小型化できると，余分な付属回路なしに品質の高い乱数が利用できることになる。このためには，先に説明したトレードオフを破る技術開発が必要となる。

当社では，一定入力に対して出力が確率的に決定される特殊な論理回路を設計し，これをもとに論理回路だけから成る乱数回路の技術を開発した。これは，物理乱数回路の原理を模倣したもので，出力の性質は物理乱数に近い。動作が確率的であるため，初期値設定も不要で，周期性もない。論理ゲート数は1ビット当たり100程度であり，擬似乱数回路でない高品質乱数生成回路としては，もっとも小型の乱数生成回路である。この乱数生成回路は，新型のICカード用マイコンのエンジニアリングサンプルに搭載されており，2003年にリリースされる。

更に，乱数源となる新しい素子を開発して，熱雑音増幅型乱数生成器に迫るような高品質乱数の生成を超小型回路で実現しようとしている。このため，シリコントランジスタに付随するナノスケール物理現象で見られる“揺らぎ”や“不確定性”を利用して乱数を作り出すことを試みている。今回は，擬似破壊酸化膜を利用した乱数生成と，単一電子素子を用いた乱数生成について紹介する。

3.1 擬似破壊酸化膜を利用した乱数生成

物理乱数生成回路は，物理現象に基づくランダムな信号を発する乱数源の部分と，ランダムな信号を所定のクロックで

読み出すデジタル乱数に変換する回路部とから成る。回路の小型化ということを考えた場合，乱数源の信号は，増幅が必要ない程度に大きく揺らいでいることが望ましい。当社は，シリコン上に形成した酸化膜が擬似破壊した後に流れる電流が，大きな揺らぎを示すことに注目して，これを乱数源とすることを試みた。**図2**は，電流揺らぎからフーリエ変換により求めたパワースペクトル密度分布である。周波数(f)に反比例してパワースペクトルが減少する1/f的な特性を示している。真性乱数を一定間隔で発生させる仮想的回路の信号を逆フーリエ変換すると，周波数依存性のないホワイトスペクトルとなる。1/f的な特性のままでは得られる乱数にも1/f特性を反映した規則性が現れてしまう。

当社は，次に示す方法によりデジタル化することで，この規則性を取り除いた乱数を得た[(2)]。**図3**は，乱数回路全体の概略図である。まず，擬似破壊後のシリコン酸化膜を抵抗値がランダムに変化する抵抗とみなして，これをデジタル発振回路であるマルチバイブレータの抵抗に用いて，電気特性の揺らぎを矩形(くけい)波の周期の揺らぎに変換した。次に，この揺らいでいる周期の一つ一つをカウンタで1ビット化することで，ノイズ源の1/f特性による規則性を取り除いた乱数列を得た。周期の揺らぎ方は1/f特性を持っているが，それを周波数に関係なく0と1に細分化して分けてしまうことで，周波数特性を実効的に除去したことになる。回路は20程度の論理ゲートと，いくつかの受動素子だけで形成され，かなり小型な回路である。この回路により，高品質の乱数生成が確認できた。品質評価に関しては，後述する。

なお，この回路の乱数源の部分には，基本的に大きな揺らぎ信号を持つあらゆる種類の素子を使うことができる。例えば，将来トランジスタが小型化していくにつれて，現在のトランジスタ構造のままだと揺らぎ信号が大きくなることが予測されている。揺らぎ信号を抑える構造を開発中であるが，逆に今の構造をそのまま使えば，乱数源素子としてこの乱数生成回路内で使うこともできる。

3.2 単一電子素子を利用した乱数生成

前節で乱数源素子の揺らぎ信号が大きいと，乱数生成回路を小型化できることを示した。更に，ナノスケールのトランジスタ構造において特徴的に現れる単一電子現象を利用することで，統計的にランダムで，かつ巨大な揺らぎ信号を発生させることができることを見いだし，高品質の乱数生成を実証した[(3)]。

当社で開発した単一電子素子の模式図を**図4**に示す。基本的な構造は電界効果トランジスタと同じで，ソース，ドレイン，ゲート電極を持つ。特徴的なのは，ゲート電極下の電子チャネル部分で，厚さが約2.6 nmの極薄SOI(Silicon-On-Insulator)層をエッチングで荒らして，数 nmの起伏を形成している。このトランジスタの各電極に適当な電圧を加えると，**図5**に示すようなポテンシャルエネルギーが低い部分が

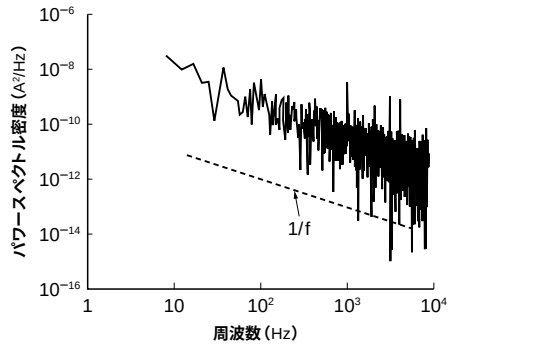


図2．パワースペクトル密度の周波数依存性 ― 擬似破壊酸化膜を流れる電流揺らぎ成分は，1/f特性を示す。

Dependence of power spectrum density on frequency

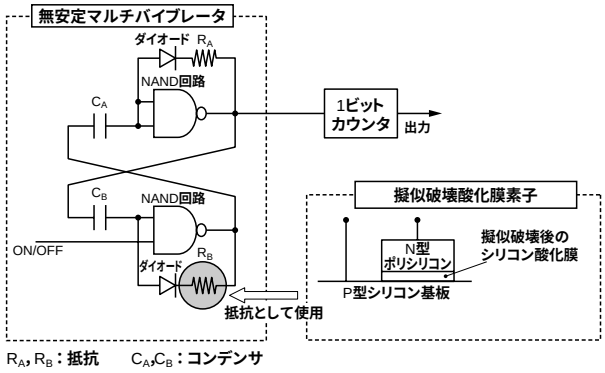


図3．擬似破壊酸化膜素子を用いた乱数生成回路 ― 無安定マルチバイブレータの抵抗を擬似破壊酸化膜素子で置き換えることで，素子抵抗の揺らぎをデジタル信号に変換する。

Random number generating circuit using oxide film after soft breakdown

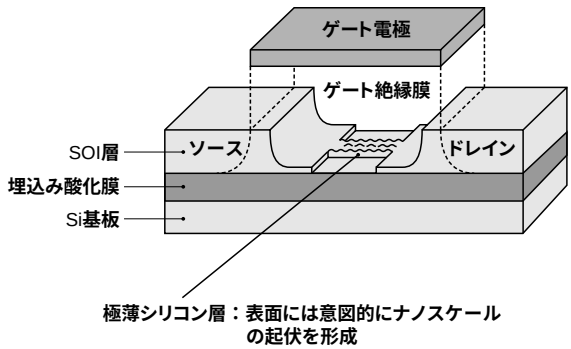


図4．単一電子素子の模式図 ― 基本的な構造は電界効果トランジスタと同じだが，特徴的なのはゲート電極下の電子チャネル部分で，厚さが約2.6 nmの極薄シリコン層をエッチングで荒らして，数 nmの起伏を形成している。

Schematic view of single-electron device for random number generation

ライン状につながり，谷間を流れる川のように単一電子の通路が形成される。更にゲート電圧を微調整すると，この通路のそばに，単一電子を捕獲する電子トラップを一個だけ形成することができる。

電子1個が，準安定な電子トラップに，ランダムに出入りする。電子がトラップされると，その周辺のポテンシャルエネルギーが上昇して，ライン状に流れていた電子の伝導度が低下する。この結果，電子チャネルの抵抗率が変化する。一定電流をチャネルに流れるようにすると，トランジスタの出力電圧（ドレイン電圧）が，電子チャネルの抵抗率変化に応じて変化する。出力電圧の時間変化を**図6**に示す。この図に示すように，単一電子素子は，電子一個の検出感度が極めて高いためにトランジスタの出力が大きいので，電圧増幅回路が不要である。かつ電子1個が出入りする現象なので，信号は始めから量子化，つまりデジタル化されており，AD変換の必要がない。したがって，乱数生成回路は，単一電子素子とシステムクロックに合わせて信号を取り出すラッチ回路だけでよい。これは，究極の小型乱数生成回路である。単一電子素子を用いているため，従来の物理乱数生成回路に比べて，消費電流も7けた小さくなっている。

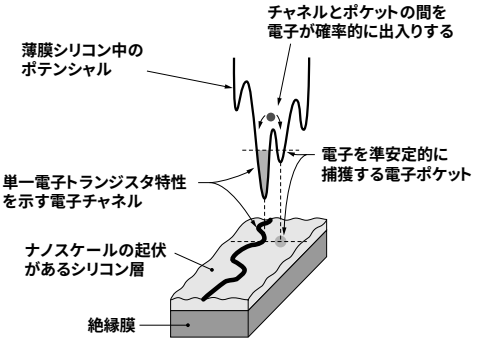
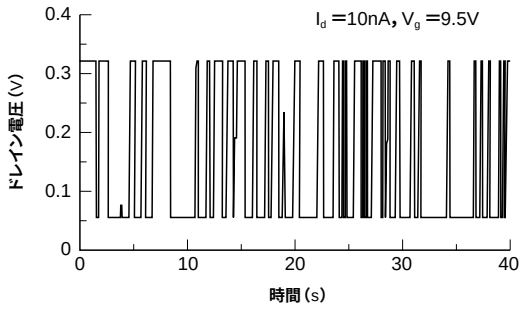


図5．単一電子素子内部のポテンシャルエネルギー ― ポテンシャルエネルギーが低い部分がライン状につながり，単一電子の通路が形成され，通路の側に電子トラップが形成される。

Potential energy diagram of single-electron device



I_d：ドレイン電流　　V_g：ゲート電圧

図6．乱数生成用単一電子素子の出力電圧の時間変化 ― トランジスタの出力電圧（ドレイン電圧）が，電子チャネルの抵抗率変化に応じて時間的に変化する。

Time dependence of drain voltage of single-electron device for random number generation

3.3 乱数品質の評価

擬似破壊酸化膜を利用した乱数生成回路と，単一電子素子を利用した乱数生成回路でそれぞれ生成した乱数列の検定結果を**表1**に示す。FIPS PUB（Federal Information Processing Standards Publication）140-2で推奨された検定[4]の結果とNIST（National Institute of Standard and Technology）の標準的な検定[4]の結果である。比較のために，熱雑音増幅

表1．乱数列の検定結果

Results of statistical tests

	テスト項目	合格条件	乱数生成回路		
			擬似破壊酸化膜	単一電子素子	熱雑音増幅
FIPS PUB 140-2	モノビットテスト	9725～10275	9885	10043	10044
	ポーカーテスト	2.16～46.17	11.52	15.8848	8.8
	ランテスト				
	“0”が1個連続	2315～2685	2532	2462	2474
	“0”が2個連続	1114～1386	1292	1243	1285
	“0”が3個連続	527～723	613	647	617
	“0”が4個連続	240～384	281	290	289
	“0”が5個連続	103～209	165	147	157
	“0”が6個以上連続	103～209	174	166	155
	“1”が1個連続	2315～2685	2557	2409	2443
	“1”が2個連続	1114～1386	1269	1296	1238
	“1”が3個連続	527～723	636	586	675
	“1”が4個連続	240～384	323	329	318
	“1”が5個連続	103～209	145	177	160
	“1”が6個以上連続	103～209	126	158	144
	ロングランテスト				
	“0”が最長連続	＜26	13	14	15
	“1”が最長連続	＜26	11	14	14
NIST SP 800-22	χ^2テスト	＞0.05	0.103876	0.543113	0.533775
	連の検定 pix1	＜0.014142	0.005750	0.002150	0.002200
	連の検定 Pv	＞0.01	0.111001	0.207205	0.531968
	ブロック内一様分布検定	＞0.05	0.634655	0.197144	0.607922
	一様分布検定	＞0.05	0.714937	0.389749	0.887740
	系列相関検定	－0.014194～0.014094	－0.011536	0.008983	0.004381
	系列検定	＞0.05	0.357106	0.379094	0.290657
	ポーカー検定	＞0.05	0.585999	0.627154	0.452948
	クーポン検定	＞0.05	0.471937	0.542948	0.741871
	間隔検定				
	“0”の間隔	＞0.05	0.369666	0.303893	0.723682
	“1”の間隔	＞0.05	0.942435	0.691953	0.426996
	“2”の間隔	＞0.05	0.800761	0.403905	0.556573
	“3”の間隔	＞0.05	0.378751	0.123166	0.373852
	“4”の間隔	＞0.05	0.456733	0.975941	0.603550
	“5”の間隔	＞0.05	0.787486	0.094254	0.529814
	“6”の間隔	＞0.05	0.396691	0.900630	0.577889
	“7”の間隔	＞0.05	0.999443	0.921356	0.888357
	“8”の間隔	＞0.05	0.405245	0.821125	0.773621
	“9”の間隔	＞0.05	0.320215	0.790492	0.803654
	“10”の間隔	＞0.05	0.244123	0.308909	0.326773
	“11”の間隔	＞0.05	0.442690	0.942683	0.754963
	“12”の間隔	＞0.05	0.420807	0.554840	0.609826
	“13”の間隔	＞0.05	0.895869	0.191812	0.589233
	“14”の間隔	＞0.05	0.979323	0.654739	0.531294
	“15”の間隔	＞0.05	0.304458	0.312341	0.866731

型の結果も示している。新たに開発した乱数生成回路で生成した乱数は，熱雑音増幅型と同様にすべての検定に合格している。

図7は，乱数列を8ビットずつに区切って，前後の相関をプロットしたもので，乱数列が一様であるほど均等かつ密に点がグラフを埋めていく。Aは擬似破壊酸化膜を利用した乱数生成回路，Bは単一電子素子を利用した乱数生成回路，Cは熱雑音増幅型乱数生成回路，Dは16段の線型フィードバックシフトレジスタ，それぞれの回路で生成した乱数の結果である。AとBの結果は，Cの熱雑音増幅型乱数生成回路と比べてそん色なく，規則性を持たない乱数列となっていることがわかる。

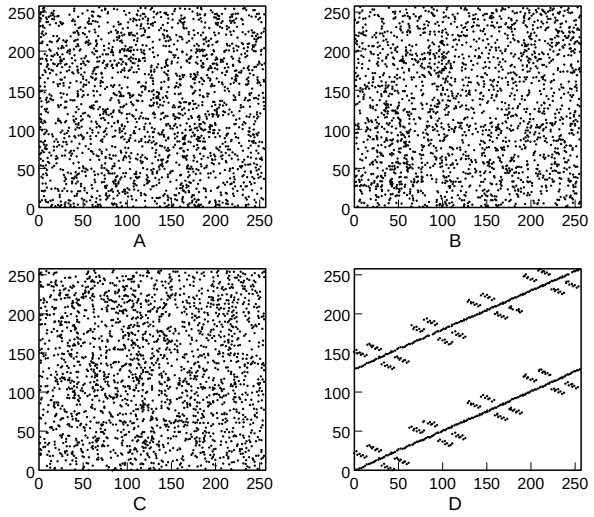


図7．乱数の相関性の比較 ― 新たに開発したA,Bは熱雑音増幅型（C）とそん色ない乱数になっている。

Comparison of correlations among random numbers

4 あとがき

情報セキュリティ用の乱数生成技術を概観し，モバイル情報機器で高度なセキュリティを実現するのに有望な，小型物理乱数生成回路の設計技術について述べた。

当社は，生成原理が物理乱数回路に近い乱数生成回路を論理回路だけで構成する技術を開発し，回路規模が論理ゲート数で100程度という小型化を実現した。また，乱数源となる新しい素子を開発して，より小型で，より高品質の乱数生成が可能であることを実証した。擬似破壊酸化膜を利用した乱数生成では，論理ゲート数で20程度であり，単一電子素子を利用した乱数生成では，ラッチ回路一つだけの究極の小型回路である。今後，これらの新型乱数生成回路を実際にシステムLSIに適用するため，技術開発を進めていく。

これらの技術は，ハードウェアの制約が厳しく，これまで適用が困難だった状況での情報セキュリティ機能利用に，大きく道を開くものと期待される。

謝　辞

擬似破壊酸化膜を利用した乱数生成と，単一電子素子を利用した乱数生成に関する研究の一部は，通信・放送機構からの2000～2003年度の“高度情報セキュリティに向けた真正乱数生成用集積回路の研究開発”の委託を受け，当社が研究開発しているシステムに関するものである。

関係者各位のご支援に感謝する。

文　献

(1) 岡本栄司. 暗号理論入門. 共立出版, 1993, 66p.
(2) Yasuda, S., et al. Novel Random Number Generator Using MOS Gate after Soft-Breakdown. 2002 International Conference on Solid State Devices and Materials. The Japan Society of Applied Physics. 2002, p.250－251.
(3) Uchida, K., et al. Single-Electron Random-Number Generator for Highly Secure Ubiquitous Computing Applications. IEEE International Electron Devices Meeting Technical Digest. IEEE. 2002, p.47－50.
(4) National Institute of Standards and Technology. Federal Information Processing Standards Publication: FIPS PUB 140-2（現在，乱数評価に関して改訂中）, NIST SP 800-2214.

藤田　忍 FUJITA Shinobu
研究開発センター LSI基盤技術ラボラトリー主任研究員。
システムLSI用半導体ナノデバイスの研究・開発に従事。
応用物理学会，IEEE会員。
Advanced LSI Technology Lab.

内田　建 UCHIDA Ken
研究開発センター LSI基盤技術ラボラトリー研究主務。
半導体ナノデバイスの研究・開発に従事。応用物理学会，IEEE会員。
Advanced LSI Technology Lab.

安田　心一 YASUDA Shinichi
研究開発センター LSI基盤技術ラボラトリー。
システムLSI用半導体ナノデバイスの研究・開発に従事。
応用物理学会会員。
Advanced LSI Technology Lab.