暗号システム向けの理想的な乱数実現へ ―“パリティ対称性”利用が有効― ★

Toward Realization of Ideal Random Number Generator for Cryptographic Systems ―Effective Use of "Parity Symmetry"―

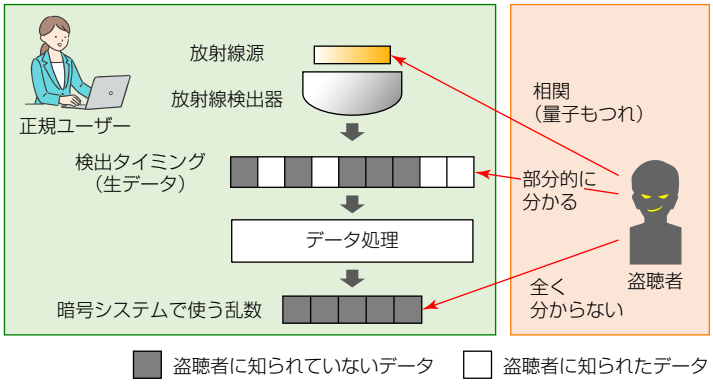
暗号や認証には，安全な(つまりランダムかつ秘匿性な)乱数が必須である。しかし現在普及している乱数生成方式は，その安全性の根拠が明確ではない。この問題を最終的に解決すると期待されているのが量子乱数生成器である。

放射線を用いた乱数生成器も，その量子乱数生成器の一種である。これまで半世紀以上にわたって，原子核の崩壊タイミングは量子現象として本質的にランダムであると予想されてきており，その予想に基づく乱数生成器の方式が提案されてきた。しかしそこでも，安全性の厳密な証明はやはり知られていなかった。これを受けて当社は，東京大学，大学共同利用機関法人 高エネルギー加速器研究機構(高エネ研)との共同研究を実施し，その厳密な証明に世界で初めて(*1)成功した。成功の理由は，ある種の核崩壊の持つ自然界の基本的な“パリティ対称性”に着目し，さらに当社が長年培った量子暗号の理論的知見を適用したことである。

この成果の適用対象である“パリティ対称性”を持つ放射線源には様々なものがあるが，その一例にアメリシウムがあり，これを使った乱数生成器は古くから実装されている。さらに近年では数ミリ角サイズのチップとして発表されている例もある。

それらに今回の成果を適用すれば，小型かつ安全性が厳密に保証された乱数生成器の実用化が期待できる(*2)。

＊1　2022年７月７日，当社調べ
＊2　詳細は東京大学工学部，高エネ研のプレスリリース参照
https://www.t.u-tokyo.ac.jp/press/pr2022-07-07-002/
https://www.kek.jp/ja/press/202207071401/

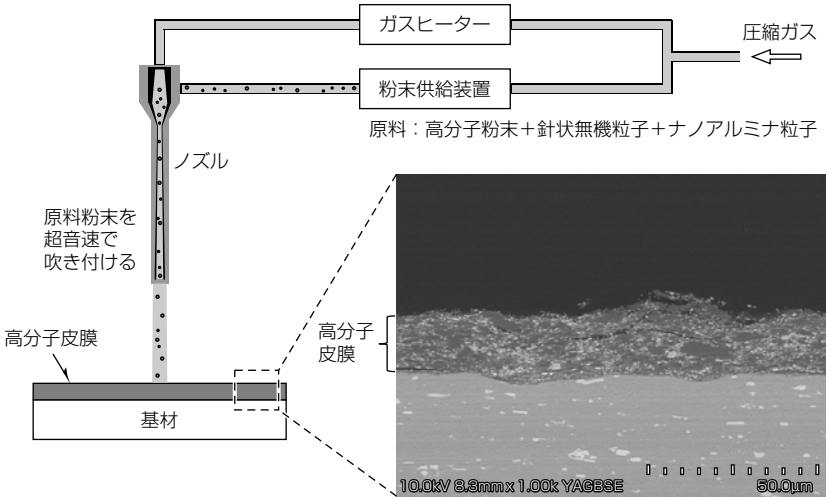


放射線の検出タイミングを基に秘密の乱数を生成

コールドスプレー法を用いた難加工な高分子材料の成膜技術

Deposition Technique for Hard-to-process Polymeric Materials Using Cold Spray Method

スーパーエンジニアリングプラスチックなどの難加工な高分子材料の成膜技術を東北大学と共同で確立した。加工が容易ではない高分子材料は皮膜形成が難しいが，コールドスプレー法を利用することで，原料粉末を固相状態のまま超音速で基材に吹き付けて皮膜化できる。今回の開発では，分子動力学法を駆使して，高分子粒子が基材に衝突するプロセスを解析し，高分子鎖の凝集力と界面への密着力が課題であることを見いだした。その解析結果を基にして，凝集力を向上させる針状無機粒子と，界面への密着力を向上させるナノアルミナ粒子を高分子粉末に添加することで，強固な成膜を実現した。この技術によって，各種製品で耐久性の高い保護皮膜の形成が期待できる。



コールドスプレー法を用いた高分子材料の成膜技術の概略図

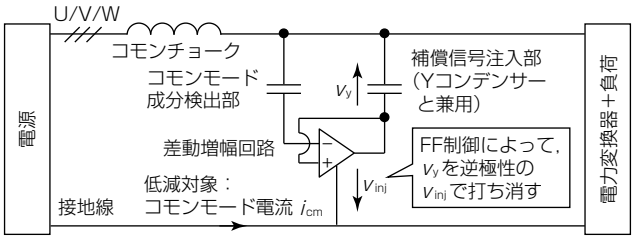
広帯域コモンモード成分を補償する小型・低コストなアクティブEMIフィルター

Compact and Low-cost Active EMI Filter Compensating Wideband Common-mode Component

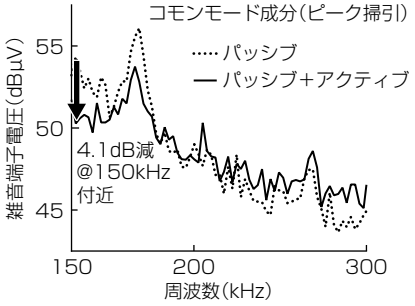
広帯域にコモンモード成分を一括補償する小型・低コストなアクティブEMI(Electro Magnetic Interference)フィルターを開発した。

コモンモード成分検出部と補償信号注入部をコイルでなくコンデンサーで構成することで，回路の小型・低コスト化を可能にした。かつフィードフォワード(FF)制御を採用することで，パッシブフィルターとの組合せ状態で生じていた共振の影響を回避し，150kHz帯の雑音端子電圧と1kHz帯の漏えい電流の一括補償を可能にした。

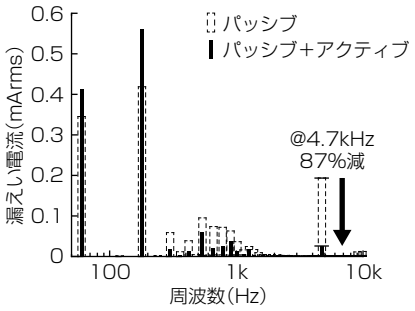
実機評価の結果，雑音端子電圧では150kHz付近で4.1dB減と漏えい電流は4.7kHz付近で87%減になり，低減両立の達成を確認した。



今回開発のアクティブEMIフィルター



雑音端子電圧の結果



漏えい電流の結果

テラヘルツ波センシング応用技術

Sensing Technology Using Terahertz Waves in 300GHz Band

光の高解像度と電波の透過性を併せ持つテラヘルツ波は障害物の背後に隠れたものを高精度に可視化でき，新たなアプリケーション応用が期待されている。

今回，MIMO(Multiple Input Multiple Output)レーダーの概念を活用し，簡素なアレーアンテナで，対象物体の高解像度な断層撮像を行うセンシング方式を開発した。電力を集中させたビームによる走査が不要で，1回測定を行えば，計算機上の信号処理によって任意の深さで断層画像を切り出すことができ，多様な用途に対応可能である。**図1**はセキュリティーゲートでの金属探知を想定した測定結果である。キャスター付きカバンの内側にアルミ箔(はく)で作った“イ”の字，外側のポケットに金属製のハサミを入れ，正面から測定を行った。切り出す断層面を信号処理で変えることによって，カバン奥の金属シャフトの影響を受けることなく，ハサミ層，“イ”の字層の独立したイメージが得られる。**図2**は食品異物検査を想定した測定結果であり，左下の単純な反射波イメージでは容器表面の強い反射でボルトが視認困難になっている。右下は今回開発したセンシング方式を用いて，表面反射の影響が少ない断層面で切り出したイメージで，カップ麺内部の異物を明瞭に検出できる。

図1-金属検知を想定したテラヘルツ波測定結果

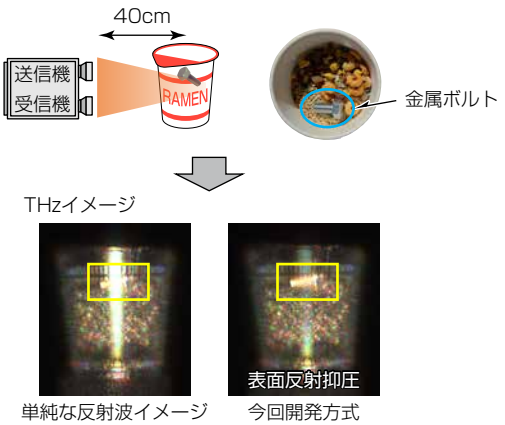


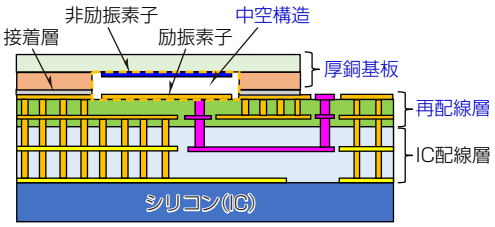
図2-食品異物検査を想定したテラヘルツ波測定結果

超高精度センシングを可能にするサブテラヘルツ帯アンテナ

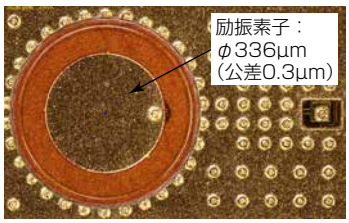
Sub-THz Band Antenna for Ultra High-Resolution Sensing

従来のミリ波帯を用いた電波センサーよりも高精度なセンチメータ級センシングを可能にする超小形サブテラヘルツ帯(*1)アンテナを開発した。半導体製造の後工程で用いられる加工精度が高い再配線プロセスと厚銅基板製造プロセスの適用によって誘電損失がない中空構造を形成し，製造公差が極めて小さく低損失な超小形アンテナ(サイズ：φ336μm)を実現した。このアンテナは空港等で用いられているウォークスルー型危険物検知センサーや工場検査ラインの非破壊検査センサー，ヘルスケア用途の見守りセンサー等への適用が期待されている。

＊1　約300GHz，波長約1mm



サブテラヘルツ帯アンテナの断面イメージ

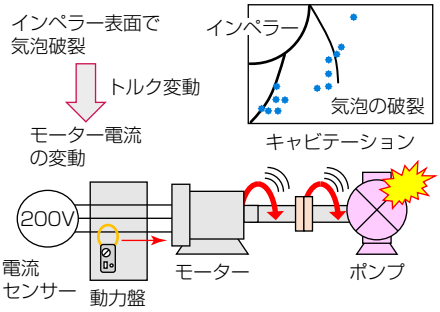


試作したアンテナ(再配線部分)

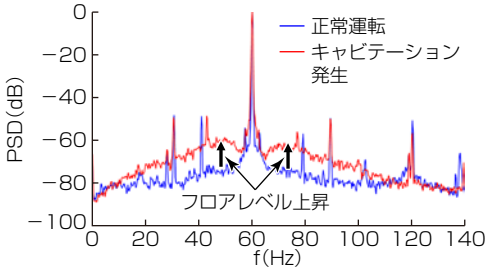
モーター電流解析によるポンプの異常検知

Pump Fault Detection by Motor Current Signal Analysis

ポンプを駆動するモーターの電流信号を用いて，ポンプの運転中にインペラー(羽根車)の損傷の原因になるキャビテーション現象を検知する技術を開発した。キャビテーションの気泡がインペラー表面で破裂する際に生じるトルクの摂動が，モーター電流のパワースペクトル密度(PSD)でのフロアレベルを増加させる。この原理を用いて，正常運転時のフロアレベルを評価基準として設定することによって，電流信号からキャビテーションの発生を検知する新たな手法を見いだした。これによって，モーターやポンプ本体に新たにセンサーを設置・追加することなく，動力盤内の電流センサーの信号だけで低コストにポンプの異常運転状態の発生を検知することが可能になり，ポンプ損傷の未然防止につなげることができる。



モーター電流解析によるポンプ異常検知の原理

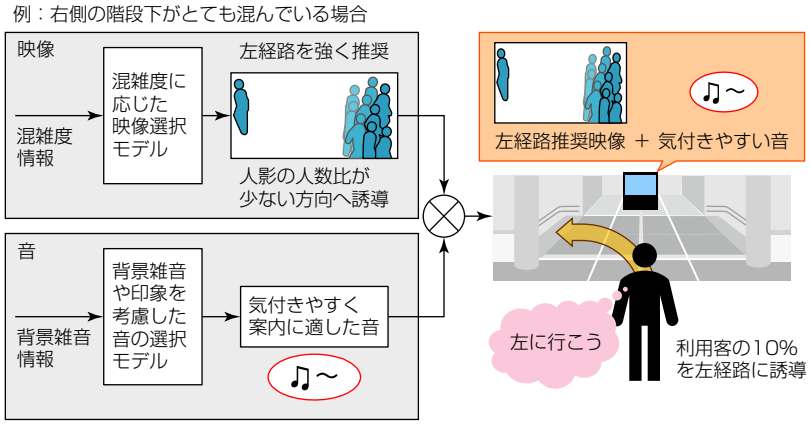


正常運転時とキャビテーション発生時の電流パワースペクトル密度

音・映像コンテンツを用いた人流誘導技術

Nudge Technology for Route Selection Using Audio-Visual Contents

混雑の平滑化を目的とした駅構内での人流の誘導は，これまで駅務員が担っており，負担になっていた。そこで，サイネージの映像と音によって人の行動変容を実現する人流誘導技術を開発した。映像については混雑度に応じて左右に分岐する人影の比率を制御することによって，ナッジと呼ばれる行動支援方法を活用した誘導を実現した。音については雑音下で気付きやすい周波数及びメロディを提示可能にした。これによって，音でサイネージに注意を向けて，映像で経路選択を支援する。駅での実証実験で，この技術によって利用客の10％を意図した方向に誘導できることを確認した。この技術を複数の分岐点に適用することによって，駅ホームの混雑の平準化と駅員の負担軽減が期待できる。



音・映像を用いた人流誘導の仕組み

AI SPEC：AIと共に生きる未来を考える取組み

AI SPEC: Speculation on Possible Futures with AI

近年，身近な製品やサービスにAI技術が広がる一方，倫理的な社会課題も顕在化してきた。そこでデザイナーとAI研究者が中心になり，AI倫理の議論を活性化するプロジェクト“AI SPEC”を開始した。これは，AIが生活に入り込んだ未来の起こり得るストーリーをマンガで描き，誰もが参加しやすい議論の場を提供する活動で，マンガを起点としたワークショップや展示，ウェブ発信を実施した。社内外の人々を議論に巻き込んで幅広い視点を得るとともに，社会全体のAI倫理リテラシー向上に貢献する目的である。今後も最新のAI技術動向を踏まえた社会課題を探索し，新たな問いを投げかけながら，一人ひとりがAI倫理を自分事として考える風土の醸成を目指して活動を進める。

AI SPECが提供する様々な議論の場

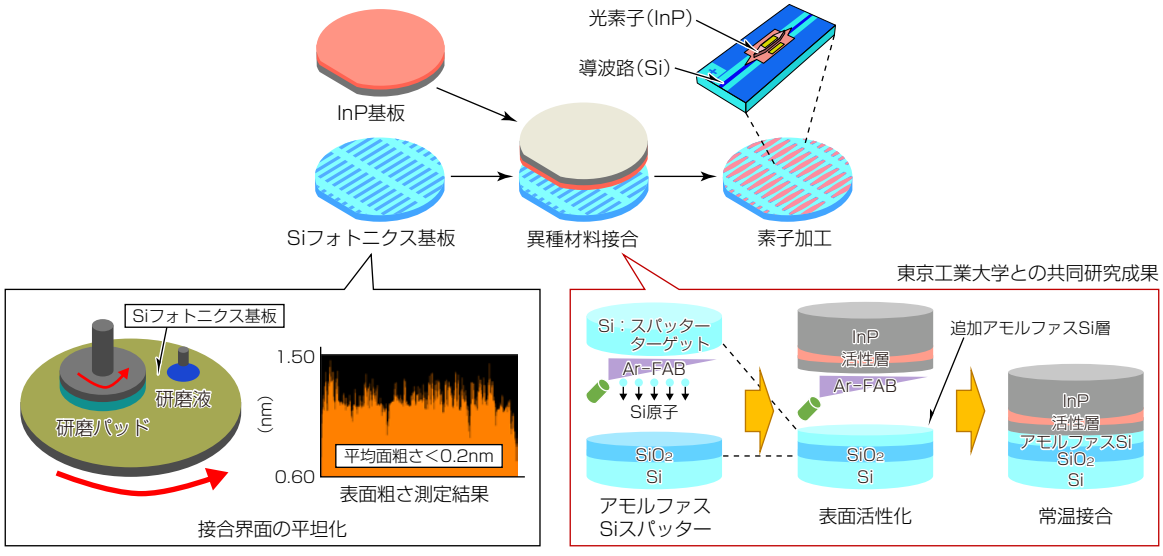
InPとSiフォトニクスの異種材料集積技術

InP/Si Heterogeneous Material Integration Technology

Si(シリコン)フォトニクスはデータセンター，センサーシステム，IOWN基盤，5G(第５世代移動通信システム)／6G(第６世代移動通信システム)モバイル光収容，光コンピューティング等，幅広い市場を支える集積光デバイス技術として期待されている。Siフォトニクスの利点は，シリコン基板上に多種の光デバイスを集積することで多様な機能を小型・安価に提供できる点にある。一方，Siは現行光デバイスの主要半導体材料であるInP(インジウムリン)に対して動作効率が低く，集積化に伴う消費電力増大が大きな課題である。

この課題を解決するため，光デバイスの機能をInPの1/2～1/5サイズで実現できるSiと，動作電力をSiの1/25で実現できるInPの二つの異種材料を表面活性化接合によって集積するSiフォトニクス／InP集積技術を開発した。表面活性化接合では平均面粗さ１nm以下が要求される。今回，Siフォトニクスの接合界面を平坦(へいたん)化することで，0.2nm以下の平均面粗さを達成した。また，東京工業大学西山研究室と共同で，接合性の高いアモルファスSi層を介した異種材料接合を実証した。この二つの技術の導入によって，従来の水酸基を用いた接合と比較して，大幅に接合面積を向上させ，より量産性の高い集積基板を作製可能になった。

この技術によって，今後一層の小型化，低消費電力化が要求される集積光デバイスの新市場領域展開に貢献する。



Ar-FAB：高速アルゴン原子線照射，SiO_2：二酸化ケイ素

Siフォトニクス／InP集積技術