ARB RIDER AWG-7000 シリーズ

QKD と量子センサのための AWG

アプリケーションノート

任意信号発生器

はじめに

デジタル時代において、金融取引から政府の機密データに至るまで、機密情報はかつてない速度でネットワークを流れています。しかしながら、数学的アルゴリズムに依存する従来の暗号化方式は、量子コンピュータによって存続そのものが脅威に直面しています。
量子コンピュータは、十分な性能を獲得すれば、これらの暗号化コードを容易に解読できる可能性があります。したがって、量子耐性暗号手法の開発が急務となっており、QKD（量子鍵配送）はこの取り組みの最前線に位置しています。

量子力学の法則は、私たちの通信やデータを保護するだけでなく、前例のない詳細さで周囲の世界を理解するためにも用いられています。
光、温度、圧力、熱だけでなく、従来のセンサでは感知できないものも、量子センサによって測定可能になります。
量子センサは自然定数に依存するため、信頼性が低下することはなく、自己校正機能を備えています。従来のセンサのように測定値が時間とともにずれることもありません。

AWG-7000 シリーズ任意信号発生器のような高性能な AWG は、こうした新興の画期的な技術の設計・開発において非常に人気が高まっています

課題：

- 量子センサおよび QKD アプリケーションのためのパルス生成

解決策：

- AWG-7000 シリーズ任意信号発生器

結果：

- 量子センサ・光学部品・フォトニクスシステムの試験・信頼性評価・特性評価を加速。
- 電気光学変調器および量子システム向けのパルス生成および制御信号生成時間の短縮

Active Technologies

QKD：Quantum Key Distribution（量子鍵配送）

量子鍵配送（Quantum Key Distribution, QKD）は、共有する当事者間でのみ知られる暗号鍵を交換するための安全な通信手法です。これは、量子物理学に基づく特性を利用して暗号鍵を交換し、その安全性を証明可能で、かつ保証する方法です。
QKD は、2 者間でメッセージの暗号化と復号に使用する鍵を生成・共有することを可能にします。具体的には、QKD は鍵を当事者間で**配送**する方法です。

従来の鍵配送は、膨大な計算能力を必要とする複雑な数学的計算を用いた公開鍵暗号に依存しています。しかし、公開鍵暗号の有効性にはいくつかの問題があります。例えば、攻撃手法の絶え間ない進化、弱い乱数生成器、そして計算能力の進歩です。さらに、量子コンピュータの登場により、現在のほとんどの公開鍵暗号方式は**安全ではなくなる**でしょう。

QKD は、数学に依存するのではなく、自然界の基本的な法則に基づいてデータを保護する量子システムを利用する点で、従来の鍵配送とは異なります。

QKD は、光ファイバーケーブルを介して多数の光粒子（フォトン）を送信することで動作します。各フォトンはランダムな量子状態を持ち、送信されたフォトン全体で 1 と 0 のストリームを形成します。この 1 と 0 のストリームは量子ビット（qubit）と呼ばれ、二進法におけるビットに相当します。フォトンが受信側に到達すると、ビームスプリッターを通過し、フォトンはランダムにどちらかの経路を選び、フォトンコレクターに入ります。

その後、受信者は送信者に対して送信されたフォトンの順序に関するデータを返し、送信者はそれを発光側の情報と照合します。

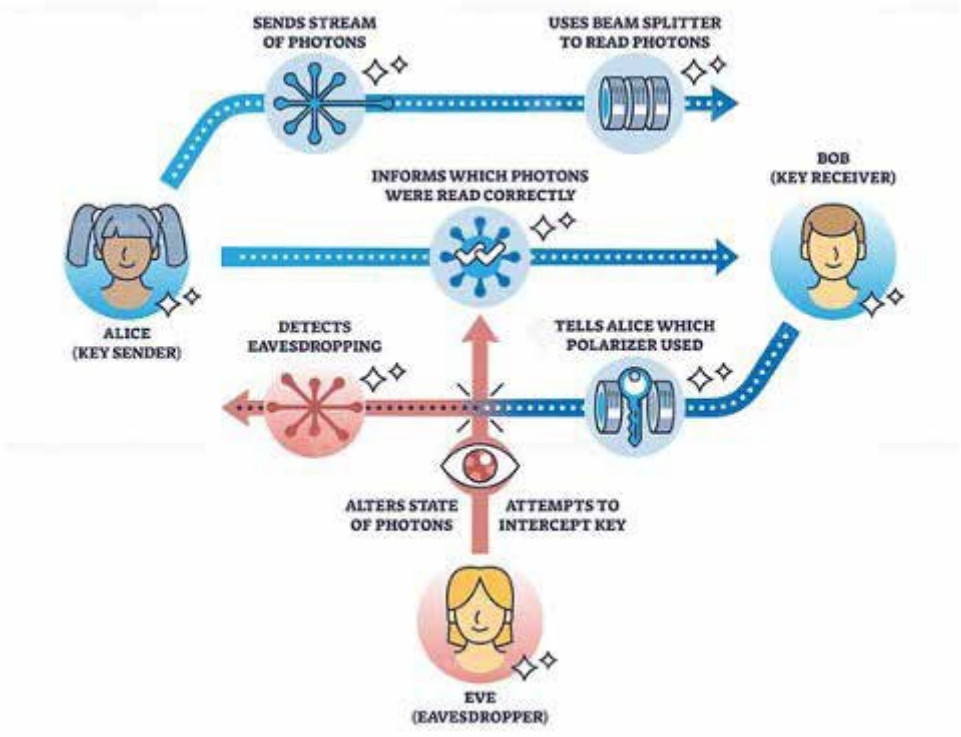

図 1：アリスとボブとイブ

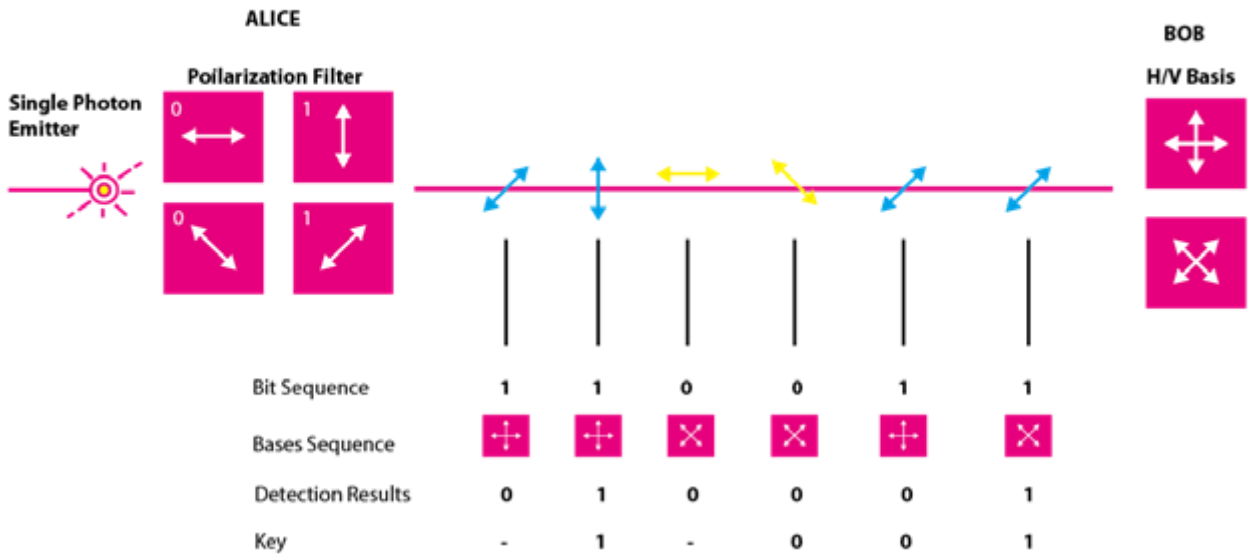

図 2：アリスとボブがフォトンを送信

誤ったビームコレクターに入ったフォトンは破棄され、残ったものは特定のビット列になります。このビット列はデータを暗号化するための鍵として使用できます。誤りやデータ漏洩は、誤り訂正やその他の後処理の段階で取り除かれます。

これを行うために、アリスは光の最小単位であるフォトンをボブに送ります。フォトンは粒子であるだけでなく波でもあるため、振動します。フォトンはさまざまな方向に振動できますが、1 方向だけに振動する場合、それは偏光と呼ばれます。

偏光フィルターを使うことで、フォトンを選別できます。例えば、上下方向に振動するフォトンだけを通過させることができ、これらは垂直偏光と呼ばれます。

量子力学の助けを借りることで、単一のフォトンを送信することが可能になります。アリスは偏光したフォトンをボブに送り、ボブがアリスの偏光方向と同じ向きにフィルターを保持していれば、光はフィルターを通過します。

一方で、ボブが偏光方向に対してフィルターを交差させて保持した場合、フォトンは通過せず、各フォトンは一度しか測定できません。

では、ボブがフィルターをアリスの偏光方向に対して少し斜めに回転させた場合はどうなるでしょうか？

この場合、フォトンがフィルターを通過することもあれば、通過しないこともあります。もし両者が同じ方向に斜め偏光させた場合、フォトンは再びすべて通過します。しかし、異なる斜め方向に偏光させた場合、フォトンはボブのフィルターを通過しなくなります。

量子鍵交換（Quantum Key Exchange, QKD）

アリスは自分が送信したフォトンの偏光方向を記録し、ボブは自分がフィルターをどのように保持したか、そして光を受信できたかどうかを記録します。

これで、2 人は公開の場で、アリスがどのようにフォトンを偏光させたか、ボブがどのようにフィルターを保持したかについて話し合うことができます。この会話は誰でも聞くことができます。一方がフィルターを斜めに使い、もう一方が垂直または水平に使った場合、その部分は常に削除され、残った部分から鍵を構築します。

攻撃者（中間者攻撃者）であるイヴが、偏光フィルターを使ってフォトンを読み取ろうとした場合、彼女はその後ボブに新しいフォトンを送信しなければなりません。

イヴは自分がフィルターを正しく保持したかどうかを知りません。光が見えなければ、彼女はフィルターをアリスのフィルターに対して交差させて保持したか、あるいは少し違う角度で保持した可能性がありますが、フォトンは通過しませんでした。
光が見えたとしても、それはフォトンがフィルターを少し回転させた状態で通過したためかもしれず、イヴは依然としてフィルターを正しく保持していなかった可能性があります。
イヴはフィルターを斜めに保持することが正しかったかどうかを知ることができません。

フォトンは複製できず、一度しか測定できないため、イヴはボブに送るフォトンを頻繁に推測しなければなりません。
アリスとボブは後で、自分たちがどのようにフィルターを使ったか、そして鍵に使える部分についてだけを話し合います。
しかしイヴは、公開の会話なしに、斜めか非斜めかを事前に決定しなければならず、どのように進めるかを推測するため、しばしば間違いを犯します。
ボブもイヴと同じくらい間違えますが、ボブの間違いは単に削除されます。アリスとボブが鍵を構築する前に、彼らは個々のビットを比較します。
それらは鍵には使われませんが、もし一致しなければ、誰かが盗聴していることがわかります。したがって、量子暗号は鍵の合意に使用されます。
この方法は、フォトンがわずかに回転したフィルターを通過できるかどうかという量子力学のランダム性に基づいているため、解読不可能と考えられています。

図 3：量子暗号

QKD の種類

QKD にはさまざまな種類がありますが、主に 2 つのカテゴリーに分けられます。それは、準備・測定プロトコル（prepare-and-measure protocols）とエンタングルメント（量子もつれ）ベースのプロトコル（entanglement-based protocols）です。

準備・測定プロトコルは、未知の量子状態を測定することに焦点を当てています。これにより、盗聴の検出や、どれだけのデータが傍受された可能性があるかを確認できます。
エンタングルメントベースのプロトコルは、2 つの物体が結びついて一体の量子状態を形成する量子状態に焦点を当てています。エンタングルメントの概念は、一方の物体を測定すると、もう一方に影響を与えるというものです。もし盗聴者が以前信頼されていたノードにアクセスして何かを変更した場合、関係する他の当事者はそれを知ることができます。
量子もつれや量子重ね合わせを実装することで、フォトンを観測しようとする行為自体がシステムを変化させ、侵入を検出可能にします。

QKD の理想的なインフラを構築することは困難です。理論的には完全に安全ですが、実際には単一フォトン検出器などのツールの不完全さがセキュリティの脆弱性を生みます。そのため、セキュリティ分析を常に考慮することが重要です。

現代の光ファイバーケーブルは、フォトンを伝送できる距離に制限があります。通常、その範囲は 100km 以上です。一部のグループや組織は、QKD の実装に向けてこの範囲を拡大することに成功しています。例えば、ジュネーブ大学と Corning 社は協力して、理想的な条件下で 307km のフォトン伝送が可能なシステムを構築しました。

QKD のもう一つの課題は、古典的に認証された通信チャネルを確立する必要があることです。これは、参加するユーザーの一方が最初に対称鍵を交換し、十分なレベルのセキュリティを確保することを意味します。高度な暗号化標準を使用することで、QKD なしでもシステムを十分に安全にすることは可能です。しかし、量子コンピュータの利用が増えるにつれて、攻撃者が量子計算を使って現在の暗号方式を突破する可能性が高まり、QKD の重要性が高まります。

QKD の攻撃手法

QKD は理論的には安全ですが、QKD の不完全な実装はセキュリティを損なう可能性があります。実際の応用において、QKD システムを突破する技術が発見されています。例えば、BB84 プロトコルは安全であるはずですが、現時点ではそれを完全に実装する方法はありません。
フェーズリマッピング攻撃は、盗聴者のためのバックドアを作るために考案されました。この攻撃は、参加者の一方が信号をデバイスに出入りさせなければならないという事実を利用します。このプロセスは、多くの商用 QKD システムで広く使用されている方法を悪用します。

もう一つの攻撃手法はフォトン数分割攻撃（Photon Number Splitting Attack）です。理想的な状況では、ユーザーは一度に 1 つのフォトンを相手に送信できるべきです。しかし、実際にはほとんどの場合、追加の類似フォトンが送信されます。これらのフォトンは、当事者が気づかないまま傍受される可能性があります。この種の攻撃に対抗するために、BB84 プロトコルの改良版であるデコイ状態 QKD（Decoy State QKD）が実装されました。これは、意図された BB84 信号にデコイ信号を混ぜることで、両者が盗聴者の存在を検出できるようにする仕組みです。

QKD の実装方法

QKD を実装するには、2 つの異なるアプローチがあります。

1. 離散変数方式（DV-QKD）：単一フォトンにランダムなデータを符号化して送信する方法です。
2. 連続変数方式（CV-QKD）：光の波動性を利用し、電磁場の四重項（quadrature）に情報を符号化する方法です。CV-QKD では、コヒーレントなホモダイン検出またはヘテロダイン検出を用いて、信号の四重項値を連続的に取得し、鍵を読み取ります。

市場には、通信の送信側（アリス）に対するさまざまな変調ソリューションがあり、受信側（ボブ）には光ハイブリッド復調器を使用できます。
最も技術的に進んだ強度変調器の一つは Exail NIR-MX800 です。$LiNbO_3$（ニオブ酸リチウム）変調の固有で比類のない利点により、高帯域幅、高コントラスト、使いやすさを提供します。

図 4：電気工学変調器

以下の文章を日本語に翻訳しました。

Arb Rider AWG-7000 および AWG-5000 シリーズの任意信号発生器は、これらの種類の電気光学変調器（Electro-Optic Modulator）を直接制御し、非常に短い光パルスを生成することを可能にします。
50 ピコ秒の立ち上がり／立ち下がり時間、100 ピコ秒のパルス幅、5Vpp の振幅でパルスを生成するという独自の機能により、外部アンプを使用せずに EOM を駆動するソリューションを提供します。

図 5：Active Technologies AWG-7000

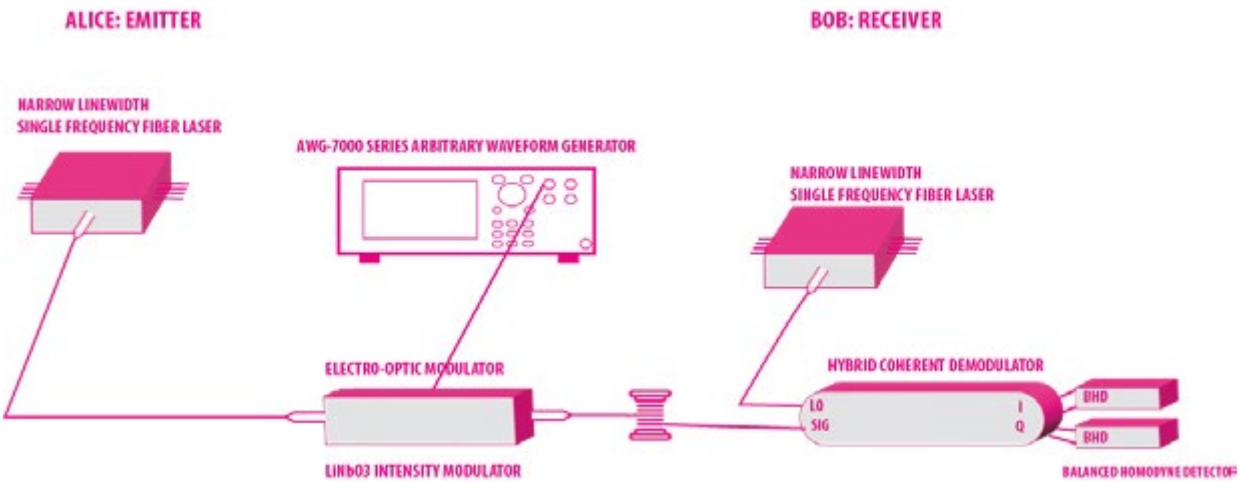

図 6: Arb Rider AWG-7000 による短光パルス生成

上の図は、任意信号発生器 AWG-7000 と、短い光パルスを生成するために使用される最初の変調ブロックとの典型的な接続を示しています。
例えば、Exail 社の NIR-MX800 と Active Technologies 社の AWG-7000 を使用することで、850nm、1310nm、1550nm の各波長で、100 ピコ秒からの非常に短い光パルス幅を実現できます。
重要な点として、AWG-7000 と強度変調器（Intensity Modulator）の接続図では、外部アンプは使用されていません。これは、AWG-7000 が、下の図に示すように、振幅 5Vpp で幅 100 ピコ秒の非常に狭いパルスを生成できるためです。

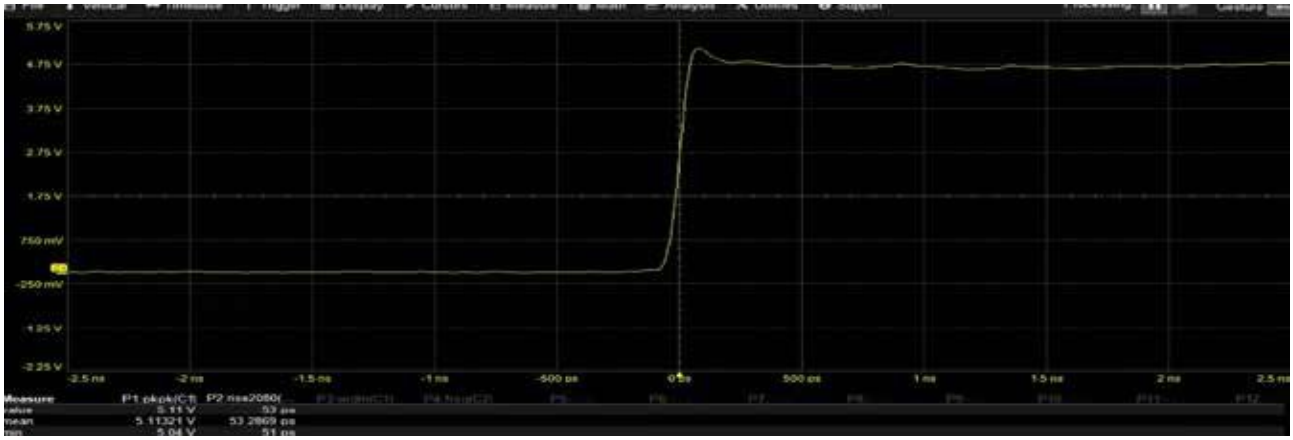

図 7：振幅 5Vpp、立ち上がり時間 50ps

図 8：振幅 5Vpp、パルス幅 100ps

量子センサ

量子センサは、私たちの周囲の世界をこれまでにない詳細なレベルで理解することを可能にします。
その高度なセンサ技術により、運動や電場・磁場の変化を感知することで、測定、ナビゲーション、研究、探索、視覚、そして世界との相互作用の精度が大幅に向上します。
解析されたデータは原子レベルで収集されます。この「繊細な」データを原子レベルで収集するということは、古典物理学で行われるような膨大な原子の集合体から情報を得るのではなく、個々の原子から情報を抽出することを意味します。

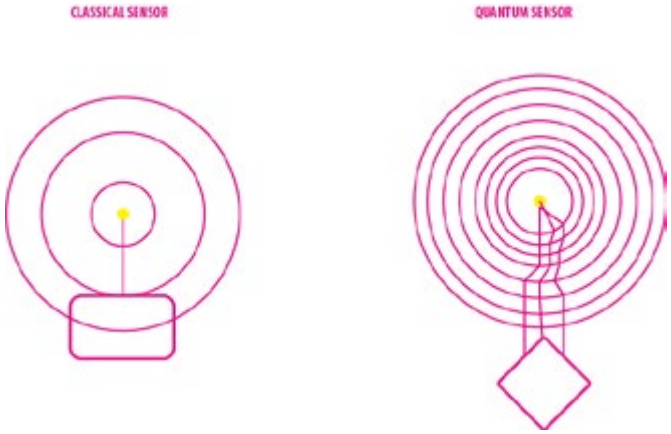

図 9：古典的なセンサと量子センサ

これにより、量子センサは私たちの技術デバイスを飛躍的に高精度、より徹底的、より効率的、そしてより生産的にすることができます。さらに、量子センシングを利用するデバイスは、従来のセンサと同じ物理的制約を受けないため、卓越した信頼性を実現し、今日の光や音に基づくデータセンサでますます一般的になっている信号妨害やその他の電磁干渉に対する脆弱性が低くなります。

量子センシングは、原子の性質を利用して物理世界の活動を測定するため、日常生活において次のような役立ち方があります：

- 現在の衛星依存型 GPS デバイスよりも高速で、より正確で、より信頼性の高い位置情報取得が可能になり、制約が大幅に減少します。
- 医師に対して、より詳細で正確な医療診断画像を低コストで提供し、患者への副作用の可能性を減らします。
- 地上、空中、海上での自律走行車のより安全で優れたナビゲーションを実現し、交通量の多い場所や予期しない障害物周辺でも対応可能です。
- 宇宙、水中、そして RF 信号が溢れる領域でのより正確で耐干渉性の高い誘導システムを提供します。

- 地下環境の信頼性の高い検出、画像化、マッピング（交通トンネル、下水道、水道管、古代遺跡、鉱山、地下生息地など）。
- 重力変化や地殻変動のより深く、より動的なセンシングにより、雪崩、地震、火山噴火、津波、気候変動活動の予兆や発生を検知できます。

磁気共鳴画像法（MRI）

MRI 量子センサは数十年前から存在しています。例えば、MRI 装置は量子センサを使用しており、1970 年代から利用されています。これらの装置の内部では、あなたの体内の原子そのものが個々の量子センサに変わります。

MRI は、磁場を利用して体内の原子に存在するスピンと呼ばれる量子特性を操作し、そのスピンが磁場に応答する様子を測定し、画像に変換します。

図 10：MRI 装置

窒素空孔センター（NV センター）磁力計

原子時計は、もう一つの種類の量子センサであり、1950 年代から存在しています。原子時計は GPS 衛星で時刻を保持し、SI 単位系における「秒」の公式定義にも使われていますが、その後技術は進化しました。

現代の革新により、新しい量子センサと応用が可能になっています。その一つが窒素空孔センター（NV センター）を利用する技術で、これはダイヤモンド内に存在する、または人工的に作られる構造です。

純粋なダイヤモンドは、炭素原子の完全な格子構造でできています。このうち隣接する 2 つの炭素原子を取り除き、そのうち 1 つを窒素原子に置き換えると、窒素と空孔（欠損部分）が組み合わさり、非常に高感度な磁力計として機能します。

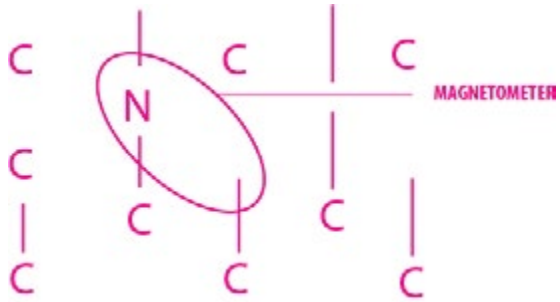

図 11：磁力計

この磁力計は、電子スピンを利用して磁場の微小な変化を検出します。実際、NV センターは地球の磁場の強さの 5,000 万分の 1 の変化を検出できるほど高感度です。さらに驚くべきことに、地球の磁場が背景に存在していても、その微小な変化を正確に検出できます。

ダイヤモンドは炭素原子の集合体であり、それぞれが 4 つの炭素と結合して規則的な結晶構造を形成しています。しかし、時にはこの構造に「欠陥」が生じます。別の元素の原子が入り込んだり、炭素原子が欠けて空間ができたりすることがあります。これらの欠陥はダイヤモンドを異なる色調で輝かせる原因となり、カラーセンター（色中心）と呼ばれます。

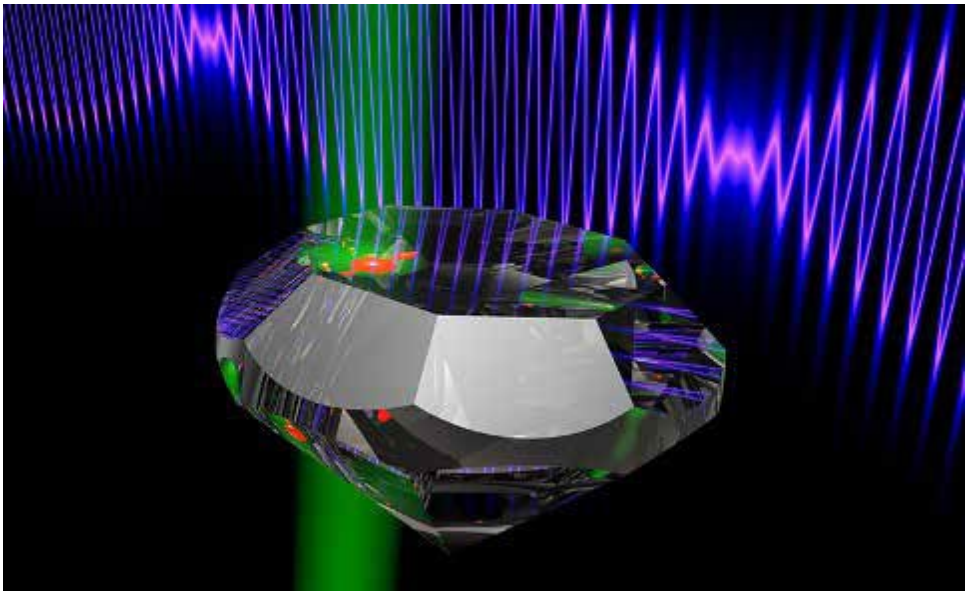

図 12：ダイヤモンド内の窒素空孔（NV）センター

特に興味深い欠陥は、結晶中の炭素原子が窒素原子に置き換えられ、隣接する炭素原子が欠けている場合に発生します。この欠陥は**窒素空孔（NV）センター**として知られ、独自の量子スピンを持ちます。このスピンは回転する磁石のように考えることができます。ダイヤモンドは主にスピンが中性な炭素 12 原子で構成されているため、NV センターのスピンは近傍の原子の影響を受けません。また、ダイヤモンドの格子構造は非常に硬いため、室温では原子が十分に動かず、スピンが別の状態に変わることはありません。

しかし、このスピンは電磁放射や磁場によって変化させることができ、この性質により NV センターを持つダイヤモンドはセンサとして利用可能になります。さらに、NV センターは光励起発光性（フォトルミネセンス）を持ち、緑色の光を当てると赤い光を発します。NV センターのスピン状態はダイヤモンドの蛍光強度を決定するため、科学者は明るさの変化を利用して、マイクロ波や磁場によるスピン状態の変化を監視できます。どの周波数が光の変化を引き起こすかを調べることで、研究者はダイヤモンドを使って磁場の強さを測定することもできます。この技術は光検出磁気共鳴（Optically Detected Magnetic Resonance）と呼ばれます。

Arb-Rider AWG-7000 シリーズは、ダイヤモンド内の単一のスズ空孔センターを操作するために使用される実験的パルスシーケンスを制御するために利用されています。
AWG-7000 は、最大 5Vpp の高振幅で狭い電気的矩形パルスを生成し、電気光学振幅変調器（Electro-Optical Amplitude Modulator）を制御して短いレーザーパルスを生成することができます。
この仕組みを使用することで、ガウス形状に近い光パルスを生成でき、半値全幅（FWHM）が 130 ピコ秒程度の狭いパルスを実現します。
さらに、AWG-7000 は**電気光学位相変調器**（**Electro-Optical Phase Modulator**）を駆動し、約 7GHz までの周波数サイドバンドを生成することが可能です。これにより、位相が安定したレーザーフィールドで 2 つの光学遷移を駆動できます。

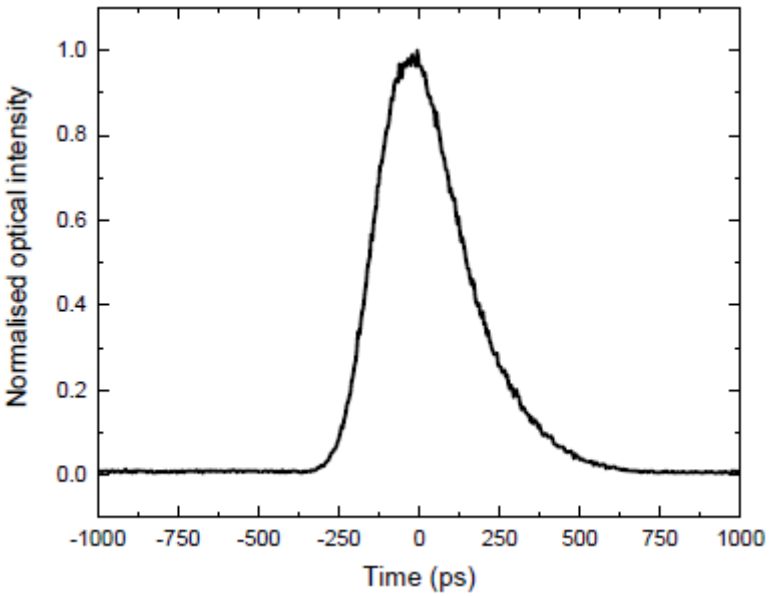

図 13：ガウス・パルス

AWG-7000 のデジタル出力チャネルは、音響光学振幅変調器（Acousto-Optical Amplitude Modulator）の制御や、実験シーケンスのタイミングを取るためのトリガーパルス生成に使用できます。
将来的には、シーケンス内の特定の読み出し結果に応じて、測定プロトコルをリアルタイムで制御することが必要になるでしょう。

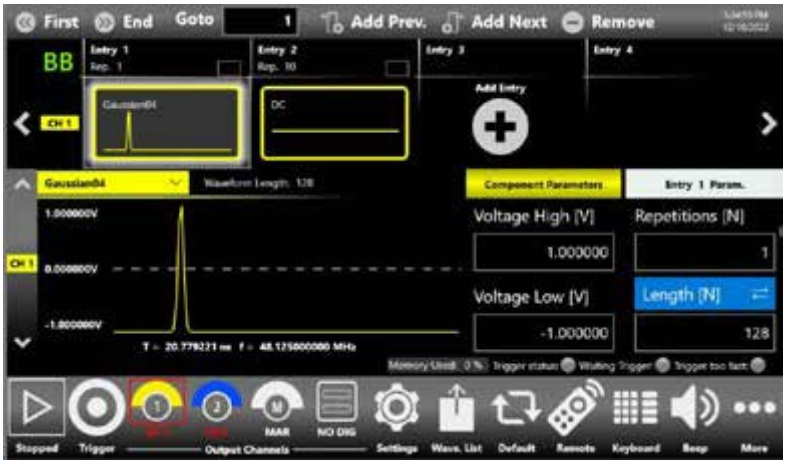

図 14：True-Arb の UI

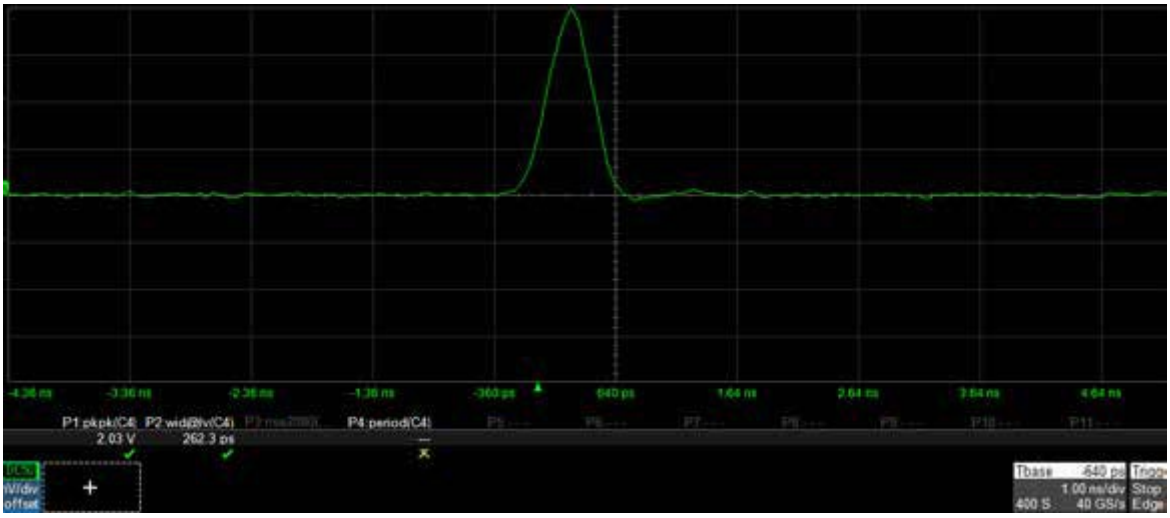

図 15：AWG-7000 シリーズの狭ガウス・パルス