巻頭言

生成 AI と情報セキュリティ

吉浦紀晃
情報メディア基盤センター長

生成 AI の爆発的な普及により、私たちの日常のさまざまな場面で活用されるようになってきました。その一例が、検索エンジンに代わる情報収集手段としての利用です。これまでは、調べたいことがあると、Google などの検索エンジンで関連するキーワードを入力し、表示された Web ページのリストから必要な情報を探していました。しかし生成 AI の登場により、知りたいことを直接入力すれば、AI が即座に説明文を出力してくれるため、それを読むだけで十分な情報が得られるようになっています。つまり、検索行為が検索エンジンから生成 AI へと移行しつつあります。

Google もこの変化に対応するため、「AI Overview（AI による概要）」を検索結果の最上位に表示するなど、生成 AI への流出を防ぐ対策を講じています。ただし、AI Overview 自体が生成 AI の生成物であり、検索行為が生成 AI へと移っていくことには変わりません。

このような変化により、Web ページへのアクセス頻度が減少しています。従来の検索エンジンでは、検索結果から Web ページにアクセスすることで情報を取得していましたが、生成 AI ではその必要がなくなります。結果として、Web ページのアクセス数が減少します。これは、アクセス数が重要な指標となる Web ページ、例えば広告収入や販売促進を目的としたページにとって深刻な影響を与えます。また、検索結果で上位表示を目指すための SEO（Search Engine Optimization）の重要性も低下し、Web 関連の従来のビジネスモデルが大きく変わる可能性があります。実際に、生成 AI の普及とともに、Google 検索結果から Web ページへのアクセスが減少しているという報告も出始めています。

別の変化として、検索結果からの「削除の困難さ」が挙げられます。これまでは Web ページを公開しても、検索対象から除外することが可能でした。しかし生成 AI は Web ページを学習データとして取り込みます。一度学習された内容をあとから削除する Unlearning と呼ばれる技術は現在のところ存在せず、重要な課題となっています。

このことは情報セキュリティ上の問題を引き起こします。例えば、組織内部だけに公開するはずだった機密情報を誤ってインターネット上に公開してしまい、それを生成 AI が学習してしまった場合、その内容は AI の学習データに残り続け、後から取り除くことはほぼ不可能です。従来であれば、Web ページを削除し、検索エンジンの対象から除外することで一定の対処が可能でしたが、生成 AI 時代にはそれが通用しません。

このように、「うっかり」のミスや一時的な公開ですら取り返しのつかないリスクを伴う時代になりつつあります。生成 AI の利便性の裏にあるこのような危険性を理解し、適切な情報管理と慎重な対応がこれまで以上に求められています。

AlphaFold を用いた VHH 抗体構造アンサンブルの生成と検証

田實 元陽[1]、松永 康佑

1. 埼玉大学大学院理工学研究科

1. はじめに

タンパク質は、20 種類のアミノ酸がペプチド結合によって一本の鎖状につながったものであり、様々な立体構造をとることで生命活動維持に必要な機能を発揮している [1]。抗体はタンパク質の一種であり、抗原と結合することができるため免疫反応において重要な役割を果たす。抗体が特定の抗原に結合できるかどうかは抗体の構造、特に CDR(Complementarity determining region:相補性決定領域)と呼ばれるループ部分の構造によって決定される。抗体のなかでも、VHH 抗体または nanobody とよばれる分子は、ラクダ科の動物が持つ特殊な抗体である。人などの動物の持つ一般的な抗体は 2 本のタンパク質の鎖で構成されているのに対して、VHH 抗体は 1 本の鎖で構成されているため、工学的に扱いやすいという利点がある。一方で、CDR ループが一般の抗体よりも長いため構造予測が難しいという欠点がある。

抗体と抗原の結合を実験ではなくコンピュータを使って予測する場合、ドッキング計算と呼ばれる手法が用いられる。実験と比べて低コストで行えるが、多くのドッキング計算の計算を行うソフトウェアでは、タンパク質を剛体として扱っており、柔軟性を考慮していないことが多い。VHH 抗体ではループが長く構造変化がしやすいため、VHH 抗体を剛体として扱うシミュレーションでドッキング計算を行うと精度が下がってしまう。

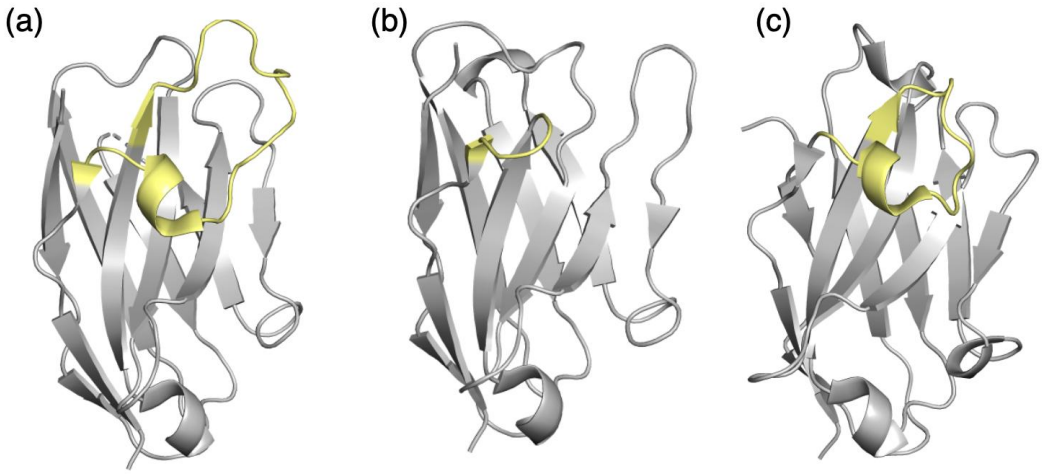

図 1: VHH 抗体の構造図。CDR H3 ループ箇所を黄色、その他の箇所を灰色で示している。(a) PDB ID: 4KRN。(b) PDB ID: 5E5M。(c) PDB ID: 6HEQ。

この問題に対して、アンサンブルドッキングと呼ばれる計算は、タンパク質の柔軟性を擬似的にドッキング計算に取り込む手法である。アンサンブルドッキングでは、まずシミュレーションなどを用いてターゲットとなる分子の代表構造(アンサンブル)を生成し、それを候補としてドッキング計算を行うため、もしシミュレーションで適切なアンサンブルを生成することができれば、高精度な複合体の結果が期待できる。実際に、VHH 抗体においても分子動力学(Molecular Dynamics; MD)シミュレーションを利用して生成したアンサンブルを用いたドッキング計算を行なったところ、アンサンブルを用いない場合と比較して、予測精度が向上したことが報告されている [2]。しかし課題として、MD シミュレーションに時間がかかりすぎるという点がある。実際、VHH 抗体の構造アンサンブルを生成するために 1 週間程度の計算時間がかかってしまう。

そこで本稿では、VHH 抗体のループ構造アンサンブルの予測計算時間を短くすることで、大量の抗体でドッキング計算を行えるようにすることを目的として、MD シミュレーションの代わりに AI ベースの構造予測モデルである AlphaFold を利用した構造アンサンブルの生成を検討し、その精度について報告する。AlphaFold は通常はひとつの構造のみを予測し、アンサンブル構造は生成しないが、いくつかの工夫をおこない構造アンサンブルを生成するようにし、その精度を MD シミュレーションの結果と比較検討する。

2. 手法

AlphaFold は Deep Mind 社が開発したタンパク質構造予測 AI であり、目的のタンパク質のアミノ酸配列を与えると高精度な構造予測結果を出力することができる [3]。多重配列アラインメント(Multiple Sequence Alignment; MSA)は、予測したいタンパク質の近縁の種のタンパク質のアミノ酸配列を並べたものである。MSA 内の複数の配列において同一の 2 箇所が相関を持って変異している場合、その箇所は立体構造上で近い可能性が高い、という考え方を共進化という。AlphaFold では MSA から共進化情報を取得し、その共進化情報をもとにタンパク質の立体構造を予測している。

AlphaFold は、通常の想定使用では、1 配列の入力に対して一つの構造しか出力することができない。しかし、複数回構造予測を行なって複数回構造を出力させることで、構造アンサンブルを生成するいくつかの手法が最近提案されている。本研究ではこの手法の 1 つである reduced MSA という手法を用いて構造アンサンブルを生成する [4]。AlphaFold では構造予測のための情報として MSA を用いていて、その MSA から共進化情報を取得し、構造予測を行なっている。Reduced MSA は AlphaFold で構造予測を行う際に使用する MSA をサブサンプリングし、意図的に配列の本数を減らすことで、予測に利用される共進化情報に統計的揺らぎを与え、結果として出力される立体構造に多様性を持たせるという手法である [4]。本研究ではこの多様性を CDR の動きとして扱い、サブサンプリングの乱数を変更しながら実行することで出力されるパターンを変更してタンパク質構造アンサンブルを生成する。

ここでは、AlphaFold の Google Colab 版の ColabFold の Local 環境版である LocalColabFold を利用して構造を生成した[5]。利用する MSA の配列数をサブサンプリングし、利用する配列数を変更しながらタンパク質構造アンサンブルを生成し、予測構造を主に主成分分析で低次元へ射影し、MD シミュレーションとの比較を通して、その精度を検証した。

Reduced MSA のよる構造アンサンブル生成は、東京医科歯科大学の森脇氏の記事(https://qiita.com/Ag_smith/items/fca48002fbdcb15145c0)を参考に、以下の例のようなシェルスクリプトを実行して予測結果を出力させた。このシェルスクリプトではまず、前半の mkdir から fi までの部分で構造予測をした結果を格納するフォルダを作っている。その後、colabfold_batch 以下の部分で、構造予測を行なっている。

```
#!/bin/bash

export PATH="/opt/localcolabfold/colabfold-conda/bin:$PATH" #LocalColabFoldのPATH
INPUTFILE="5e03/input.fasta"
OUTPUTDIR="5e03/output_recy3_msa512"

rm -rf ${OUTPUTDIR}
mkdir -p ${OUTPUTDIR}/0
for RANDOMSEED in `seq 0 99`; do
  if test ${RANDOMSEED} -ne 0 ;then
    mkdir -p ${OUTPUTDIR}/${RANDOMSEED}
    cp -rp 0/*_env ${RANDOMSEED}
  fi
  colabfold_batch \
    --num-recycle 20 \
    --num-models 5 \
    --model-order 1,2,3,4,5 \
    --amber \
    --templates \
    --custom-template-path "/data/moto/vhh/reduced_msa/5e03/templates/" \
    --use-dropout \
    --max-msa 512:5120 \
    --random-seed ${RANDOMSEED} \
    ${INPUTFILE} \
    ${OUTPUTDIR}/${RANDOMSEED}
done
```

図 2：Reduced MSA の計算に使用したスクリプト(PDB ID: 5E03 の場合)

INPUTFILE は構造予測を行いたいタンパク質の、アミノ酸配列情報が記述されているファイルのパスであり、OUTPUTDIR は出力結果を格納したいフォルダのパスである。colabfold_batch の各オプションは以下のようになっている。

- num-recycle の部分は AlphaFold の recycling の回数を指定していて、値を増やすことで精度が上がるが、時間もかかるようになる。AlphaFold のデフォルトの recycling の回数は 3 となっている。
- num-models は 1 回の構造予測で生成する予測構造の数であり、本研究では 1 フォルダ内に生成されるタンパク質立体構造ファイル(PDB ファイル)の数となっている。

model_order によって評価の高い順や低い順などに並べ替えることができる。本研究ではデフォルトである高い順となっている。また、評価基準も設定することができるが、同様にデフォルトのままで利用している。

- amber のオプションをつけることで構造最適化が行われる。
- templates のオプションを付けることで、ProteinDataBank (PDB)上に存在する実験構造をテンプレートとして仕様することができる。また custom-template-path をつけることで、自分で用意した立体構造ファイルをテンプレートとして用いることもできる。
- use-dropout のオプションを付けることで、機械学習の過学習を防ぐ Dropout という手法が適用され、出力が変化する。
- max-MSA は構造予測を行う際に利用する MSA の本数を制御している。:(コロン)より前の部分が AlphaFold の max_MSA_clusters に相当し、後ろの部分が max_extra_MSA に相当する。
- random-seed の値を変更しない限り、同条件で実行をすれば同じ出力となる。本研究では、フォルダ名と同じとなるようにしているため、同条件下では random-seed が同じになることは無いようになっている。
- random-seed 以降の部分では、はじめに用意した入力のファイルのパスと出力先のパスを指定している。

その後、主成分分析を行い、射影した低次元空間。atom_indices で CDR H3 ループの部分のみを選択し、for 文の内部で各アミノ酸残基ごとに隣り合っているもの以外で、残基番号が自身より後ろの他のアミノ酸残基との距離の配列を作成する。その後、事前に MD シミュレーションを行って得られたトラジェクトリを主成分分析して得られた主成分空間へ射影した。この処理を予測結果、単体構造、複合体構造の 3 つに対して行い、その結果を MD トラジェクトリと重ねてプロットした。比較対象として MD トラジェクトリは、レプリカ交換法を用いて MD シミュレーションを行った物の中から、温度 300K のデータのみを抽出した物である[6]。

3. 結果

PDB ID: 4KRN の構造アンブル生成結果

図 3 は PDB ID: 4KRN の MD シミュレーションで作成したアンサンブル、AlphaFold で生成したアンサンブル、PDB 上の実験構造を主成分分析しプロットしたものである。MD シミュレーションと AlphaFold の結果はどちらも 2 つのクラスタに分かれている等、大まかな特徴は似通っている。4KRN では AlphaFold の結果が MD シミュレーションの結果と同様に、2 状態に分かれていることを再現できた。しかし、AlphaFold の結果の内、実験構造から遠い方のクラスタが MD シミュレーションのものより全体的に実験構造側によっている部分や、プロットの左下のような AlphaFold では再現できていない部分もあり、もう少し大きな変化をさせることが将来的な課題と思われる。

4KRN の主成分分析の結果は、AlphaFold と MD シミュレーションのどちらも 2 つのクラスタに分かれている。その 2 つの状態を分ける要因について、4KRN の CDR H3 ループに存在するプロリンの影響を調査した。プロリンは trans 型だけでなく cis 型をとる確率も高く、構造が大きく変化しているところに存在することが多い。しかし、CDR 内に存在する残基番号 111 のプロリンをみると AlphaFold はともに trans 型であり、MD シミュレーションはともに cis 型であることから、残基番号 111 のプロリンは 2 状態を分ける要因にはなっていなかった。同じく CDR 内に存在する残基番号 114 のプロリンも、AlphaFold の 2 状態と MD シミュレーションの 2 状態は全て trans 型であり、こちらも 2 状態を分ける要因とはなっていない。そのため 4KRN の 2 状態を分ける要因はプロリンではなく、CDR H3 ループ内のプロリン以外のアミノ酸の協調的な主鎖構造の変化にあることがわかった。

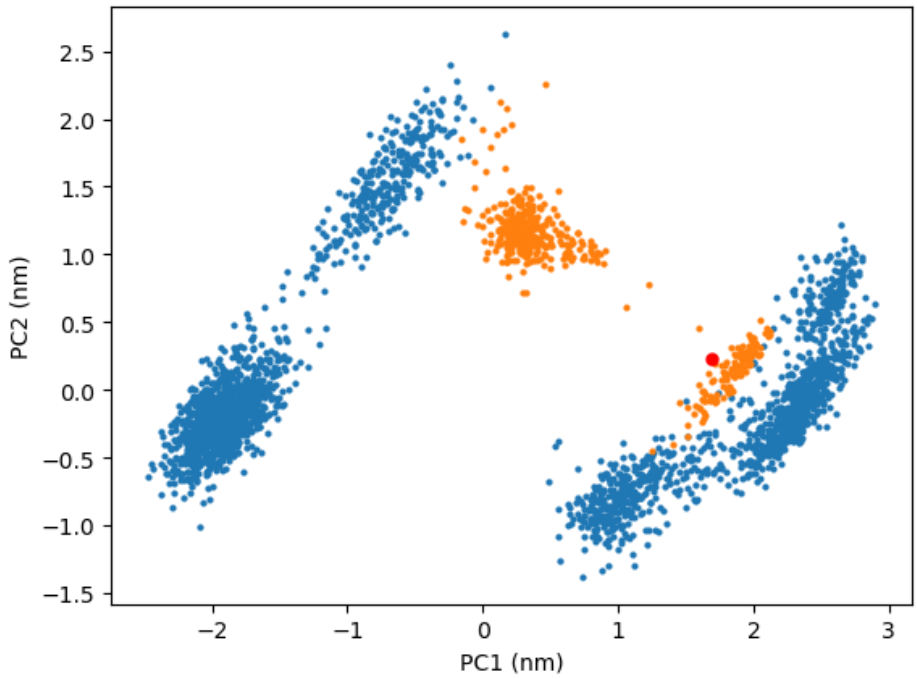

図 3: 4KRN の MD シミュレーションと AlphaFold の主成分空間での比較。オレンジが AlphaFold、青が MD シミュレーション、赤が実験構造となっている。AlphaFold は num-recycle:20、max-MSA:512:5120 で行った。

PDB ID: 5E03 の構造アンブル生成結果

図 4 は、PDB ID: 5E03 の MD シミュレーションで作成したアンサンブル、AlphaFold で生成したアンサンブル、PDB 上の単体の実験構造、また 5E03 と同じ VHH 抗体が抗原と結合している構造（PDB ID: 5E5M）を主成分空間へ射影したものである。5E03 では、複合体構造である 5E5M に近い構造をとっているものが多い。これは、AlphaFold の学習元のデータに複合体の構造が多いことで、複合体の構造の方を多く学習しているためと思われる。

また、図 5A のように template 構造を利用することで、5E5M（複合体構造）に近い構造の

みでなく 5E03（単体構造）に近い構造を取らせることもできる。図 5B は同じ VHH 抗体であるが 5E03 とはアミノ酸配列の異なる PDB ID: 4IDL を template として与えたものである。template を与えていない図 3 と比較するとほぼ変化のないことが分かる。これは、AlphaFold の能力として、MSA から取得した共進化情報から外れる構造は templates として採用しない、という機能が存在しているためであり、4IDL の構造は 5E03 のアミノ酸配列に対して不安定であると判断されたからであると考えることができる。したがって、AlphaFold は与えられた構造が安定かどうかを「知っては」いるが、正解構造を探す能力に乏しく、この点については未だ改善の余地があることがわかる。

5E03 においても 4KRN と同様にアンサンブルの広がりは MD シミュレーションと比較すると小さく、特定の構造に集中しやすい傾向にある。より広範な構造を含むアンサンブルを生成するためには、templates や MSA に対する将来的にさらなる工夫をする必要がある。

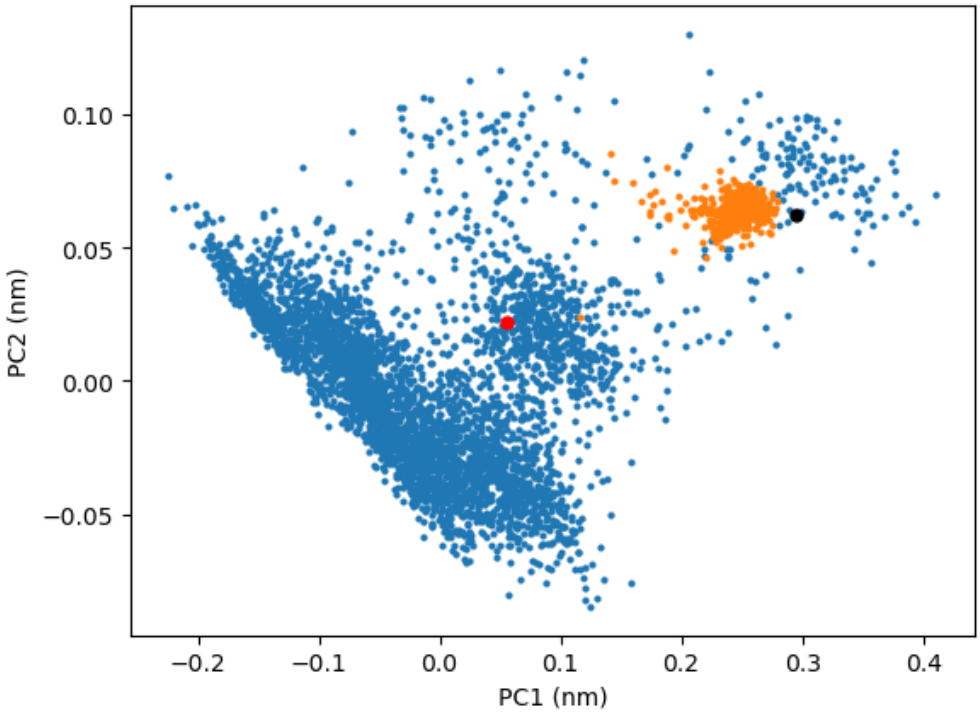

図 4: 5E03 の MD シミュレーションと AlphaFold の主成分空間での比較。オレンジが AlphaFold、青が MD シミュレーション、赤が実験構造、黒が複合体構造となっている。AlphaFold は num-recycle:20、max-MSA:512:5120 で行った。

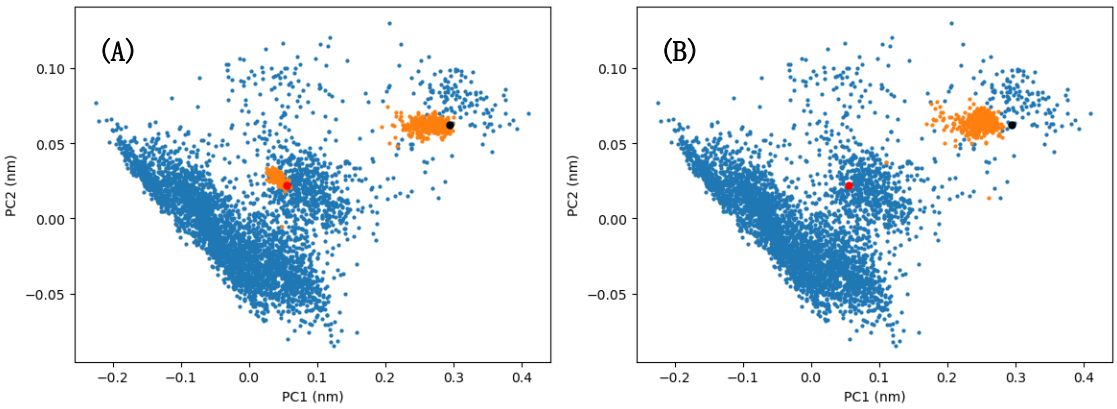

図 5: 5E03 において任意の template を追加して予測させた結果。(A) 5E03 の構造情報を templates として与えた結果。(B) 4IDL の構造情報を template として与えた結果。

PDB ID: 6HEQ の構造アンブル生成結果

図 6 は、PDB ID: 6HEQ の MD シミュレーションで作成したアンサンブル、AlphaFold で作成したアンサンブル、PDB 上の単体の実験構造、また 6HEQ と同じ VHH 抗体が抗原と結合している構造（PDB ID: 4N9O）を主成分空間へ射影したものである。AlphaFold で生成した構造は単体構造と複合体構造の中間のような位置に分布している。6HEQ はよって構造が変化するが、MD トラジェクトリの構造アンサンブルは変化後の構造も捉えており、変化後の構造がそもそも本来的に CDR H3 ループの揺らぎに内在していることがわかる。一方で AlphaFold による予測構造は両者の中間的な構造領域に集中しており、構造探索能力の低さのために、ループがとる典型構造に集中してしまっていると思われる。

図 7 は 6HEQ のアミノ酸配列を与えて AlphaFold でアンサンブルを生成する際に、templates として 6HEQ の構造情報を与えたもの(A)と、6HEQ の複合体構造である 4N9O の構造情報を与えたもの(B)である。どちらも templates として与えたものの構造の近辺に集まっていて、AlphaFold は 6HEQ と 4N9O がどちらも 6HEQ のアミノ酸配列に対して安定な構造であると判断していると考えられる。したがって、5E03 の結果と同じように AlphaFold は与えられた構造が安定化どうかは「知っている」が、それを探索する能力には以前課題があることがわかる。

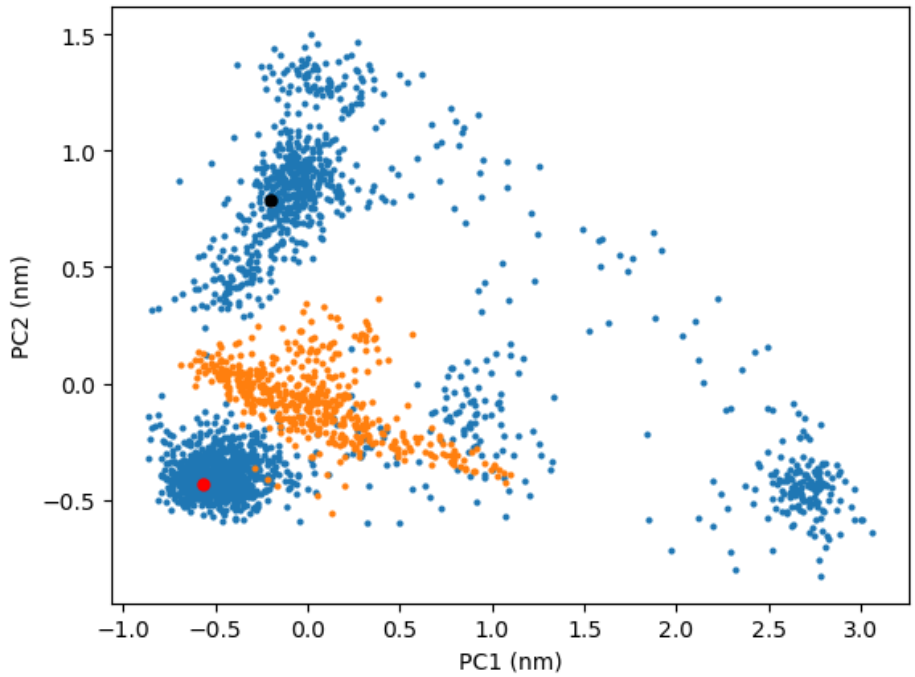

図 6: 6HEQ の MD シミュレーションと AlphaFold の主成分空間での比較。オレンジが AlphaFold、青が MD シミュレーション、赤が実験構造、黒が複合体構造となっている。 AlphaFold は num-recycle:20、max-MSA:512:5120 で行った。

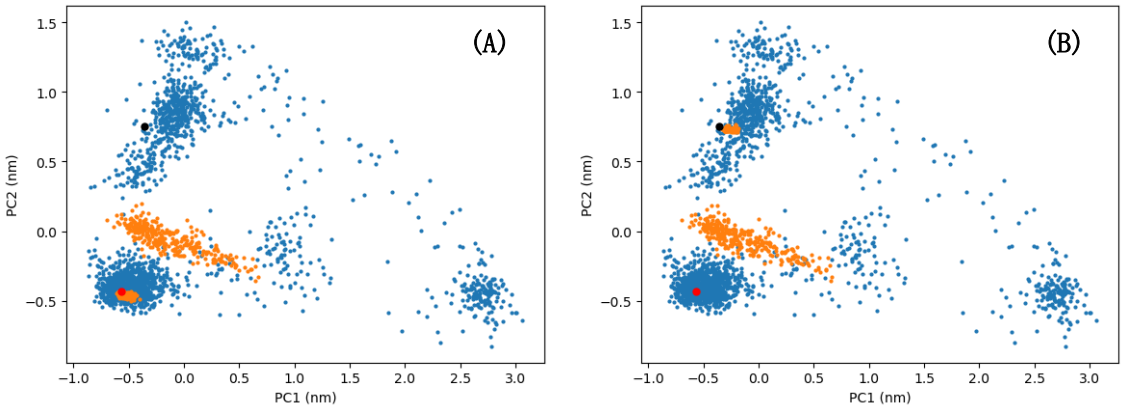

図 7: 6HEQ において任意の templates を追加して予測させた結果。(A) 6HEQ の構造情報を templates として与えた結果。(B) 4N9O の構造情報を templates として与えた結果。

4. まとめ

本論文では、結合予測計算に使用する VHH 抗体のタンパク質構造アンサンブルを AlphaFold を用いて生成し、MD シミュレーションで生成したものと比較、検証した。Reduced MSA を利用した手法では、4KRN の２つのクラスタを再現できたことなどの成果もあったが、構造が一定の位置に固まってしまいやすく、この手法によるアンサンブルの生

成には限界があることがわかった。Template を与えた調査では、template が実際に存在する安定構造だった場合は template にしたがって予測する一方で、template が実際に存在はしない不安定構造だった場合は、その他の安定構造を予測することがわかった。したがって、CDR H3 ループの構造の探索能力には課題があるが、ループ構造が安定かどうか判断する精度は十分に高いことがわかった。したがって、今後は Reduced MSA 的な共進化情報の揺らぎだけで構造を探索するのではなく、ループの物理モデルにしたがったよりアグレッシブな構造探索アルゴリズムと組み合わせることが有益と期待される。

5. 謝辞

本研究に有益なコメントをいただいた研究室メンバーに感謝いたします。また、VHH 抗体について様々なご助言をいただいた株式会社 Epsilon Molecular Engineering の皆様に感謝いたします。

参考文献

[1] 有坂 文雄, タンパク質科学： 生物物理学的なアプローチ, 裳華房, (2021).

[2] 山口 皓平, アンサンブルドッキングによる VHH 抗体の結合ポーズ予測,埼玉大学 理工学研究科 数理電子情報系専攻 情報システム工学コース修士論文 (2023).

[3] J. Jumper, et al., Highly accurate protein structure prediction with AlphaFold., *Nature*, **596**, 583–589 (2021)

[4] D. del Alamo, D. Sala, H. S. Mchaourab, J. Meiler, Sampling alternative conformational states of transporters and receptors with AlphaFold2.,*eLife*, **11**, e75751 (2022).

[5] M. Mirdita, K. Schütze, Y. Moriwaki, L. Heo, S. Ovchinnikov, M.Steinegger, ColabFold: making protein folding accessible to all., *Nat. Methods*, **19**, 679–682 (2022).

[6] 東田 連, レプリカ交換分子動力学法による VHH 抗体の構造予測, 埼玉大学 理工学研究科 数理電子情報系専攻 情報システム工学コース修士論文 (2023).

量子暗号通信の現状と課題

～ワイドギャップ半導体を用いたLED型単一光子発生デバイスの実現～

土方　泰斗

1.　はじめに

近年，インターネット上での電子商取引の発達する一方で，量子コンピュータといった超高速演算処理機による暗号の解読が懸念されている．また，ネットワークを介したいわゆる“サイバー攻撃”が，企業・自治体の情報漏洩，公開情報の改ざんを引き起こし，果ては国家安全保障にまで影響を及ぼす国際的な社会問題になっている．これらの対策の一つとして，不確定性原理に基づく絶対傍受不可能な量子暗号通信の実用化が有望視されている．しかし，微弱な光パルスを単一光子源として用いている現行方式では，パルス間の光子数バラつきによる脆弱性や，誤り訂正率増加に伴う通信速度の低下が問題となっている．このことが，量子暗号通信の普及を阻害し，その卓越的な暗号性能に見合うだけの導入実績に至らない要因として考えられる．

本報では，まず，量子暗号通信が絶対傍受不可能となる物理的根拠について平易な解説と共におさらいする．次に，量子暗号通信が普及するための主たるボトルネックとなっている光源の問題について，近年その解決方法として掲げられている「ワイドギャップ半導体量子光源」の開発状況について紹介していく．さらに，このような固体量子光源のさらなる応用先として，量子センシング，量子イメージング，量子コンピューティングといった各種量子技術を挙げ，当該分野の将来について展望していきたい．

2.　量子暗号通信の仕組み

現在広く用いられている暗号化技術は，RSA暗号を基調とする「桁数の非常に大きな素因数分解が現実的な時間で解くのは困難であろう」という予想を根拠としている．ところが，組み合わせ問題が得意な量子コンピュータ等を用いると，瞬時にこの暗号が破られてしまう危険性が指摘されている*[1]．

最近は２段階認証（２要素認証）といった，従来のパスワード方式に加えて複数の認証方式を併用することにより，ログイン認証やインターネット取引きの秘匿性を強化している．第二の認証方式として良く目にするのが“ワンタイムパッド”方式であり，「期限が短く，１回限り有効なパスワード」を用いることで，毎回変わるパスワードを短時間で解読するのは極めて難しいことを前提に秘匿性を保っている．しかし，この方式の欠点は，通信者間で秘密鍵を安全に共有するのが困難なことである（鍵配送問題）．そこで提案されたのが，秘

*[1] cf. 数学者 Peter Williston Shor のアルゴリズム, 1994 年

密鍵を量子の不確定性原理に基づき安全に共有する「量子鍵配送方式(Quantum Key Distribution; QKD)」，すなわち量子暗号通信である．

QKD が絶対傍受不可能な暗号通信と成り得る所以について大まかに説明する．現在，初期に提案された BB84 方式[1]に加え，E91 方式[2]などいくつかの暗号化方式が提案されており，基本的に後発の方がより暗号強度が強くなっている．ここでは紙面の都合により，最もオーソドックスな BB84 についてのみ解説したい．まず，最初に理解しなければならないのは，光源として“単一光子”という通常の光とは異なる性質を持つ光を暗号鍵のキャリアとして用いることである．私達が日常的に目にしている光は大きく分けて二つに分類され，一つは熱放射光と呼ばれる白熱電球や黒体放射で代表される光である．もう一つは，レーザ光に象徴されるコヒーレント光である．光の最小単位である光子としてこれらの光を記述すると，前者は一度に複数の光子を発し，光子を出さない休止期間がやや長い（図 1）．また，その光子数分布はゼロを起点にした指数分布に従い，分散は比較的大きい．一方，コヒーレント光はランダムのタイミング・数の光子を発し，その光子数分布は強度に応じてポアソン分布またはガウス分布を示す．ところで，これらの光はいずれも古典光という括りであるが，非古典光（量子光）として括られる第三の光がある．その一つが，BB84 等で利用される“単一光子”であり，その光子数は完全に 1 に限定される（このような光子数分布を Fock 状態と呼ぶ）．これらの光源を銃に例えて言うならば，古典光源が散弾銃，単一光子源が機関銃に対応する．

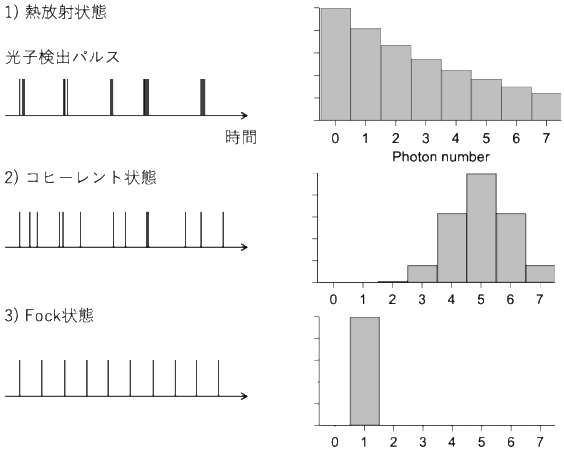

図 1．光子の 3 つの状態と光子数分布
＜熱放射状態＞一度に複数の光子を放出し，休止期間がやや長い，光子数は指数分布．黒体放射など．＜コヒーレント状態＞光子生成はランダム，光子数はポアソン分布．レーザー光など．＜Fock 状態＞光子生成は周期的，光子数は離散的．単一光子源，もつれ光子対などの非古典光．

その単一光子源を利用した暗号通信の秘匿性を説明するのに，良く，「単一光子はこれ以上分割できないので，傍受されれば直ぐにそれが解る」と述べられることがしばしばある．だがしかし，これは正しい説明ではない．正しくは，光の“量子状態の重ね合わせ”を利用する．この量子力学特有の物理現象が QKD を語る上で必要なもう一つの重要事項である．まず，“不確定性原理”についてヤングの二重スリット実験を参照しつつおさらいしたい．レーザー光線を二重スリットに入射すると背面側スクリーンに干渉縞ができることは周知

であるが，たとえレーザー光を電子線や単一光子などの粒子（量子）に置き換えても，同じように干渉縞が現れる．単一光子の場合，二つの光子がそれぞれ別のスリットを同時に通過する事は有り得ないはずだが，それなのに二つの波が重なって生じる干渉縞が現れるのはなぜなのか？さらに奇異な事に，何らかの方法で単一光子が「どちらのスリットを通過したか」を観測もしくはマーキングすると，途端に干渉縞が消え，２本のスリットを通過してできた２本の帯がスクリーンに現れる．このことが，量子が波と粒子の二重性を示す根拠となっている．しかし，この現象は数々の物理学者を悩ませ*2，明瞭かつ納得のいく統一的理論は未だ存在しない．諸説ある物理的解釈の内，比較的支持されているのが“コペンハーゲン解釈”であり，これは未観測の状態を確率的に解釈しようという説である．上述の２重スリットの例で考えると，どちらのスリットを通過したかの判定は，“50%：50%”という確率によって表現する．このように，五分五分の確率で２つの状態が共存する事を“量子重ね合わせ状態”と呼び，どちらの状態であるかは観測するまでは絶対に，誰にも判断することはできない．

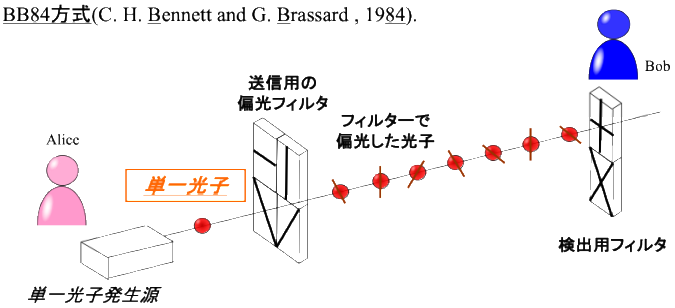

図２．代表的な量子暗号通信“BB84”方式の概念図[3]

前置きが長くなったが，いよいよ BB84 方式の核心部分を説明する．図２の送信側(Alice)に示すように，単一光子一つ一つにビットに対応した４方向の偏光状態を与える．ただし，0 または 1 のビットを与える方法は２通り有り，水平および垂直偏光を基底としている Z 基底，±45°偏光の X 基底がある．Z 基底か X 基底を選ぶかは“ランダムに”決める．ここで，

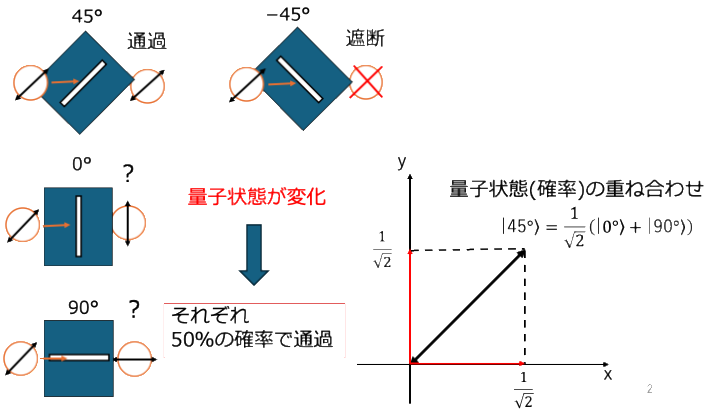

図 3. 45° 方向に偏光した光子を透過軸±45, 0 , 90° に傾けた偏光板に通した場合の概念図.
入射光子の偏光角と偏光板の透過軸が 45° 異なる場合（図中 0, 90° の場合），それぞれ 50%の確率で水平(X)及び垂直(Y)方向に偏光した光子が透過する．

*2 e.g. 「神はサイコロを振らない」by Albert Einstein.

Alice と Bob（受信側）の基底が同じになった場合，Bob は正しく暗号鍵を復号化できるが，問題は両者で基底が異なった場合である．一般的に，偏光子（検光子）透過軸と入射光の偏光角の違いθ によって透過光の強度 I は以下の式で表される(Malus' Law)：

$$I = I_0 \cos^2 \theta \tag{1}$$

従い，基底が合致しなかった場合（入射偏光角と透過軸が 45° ずれた場合），50%ずつの割合で互いに 90° 異なる光が透過することになる（図 3）．図 4 は，直交する 2 枚の偏光板を介した場合（左）と，その間にもう一枚 45° 傾けた偏光板を挿入した場合（右）の写真である．右の写真は，3 枚目の偏光板が挿入された領域のみ光が透過しており，そこで縦偏光と横偏光が五分五分の割合で透過していることが分かる．この現象は単一光子に対しても現れるので，これがいわゆる量子重ね合わせ状態として BB84 に利用される．

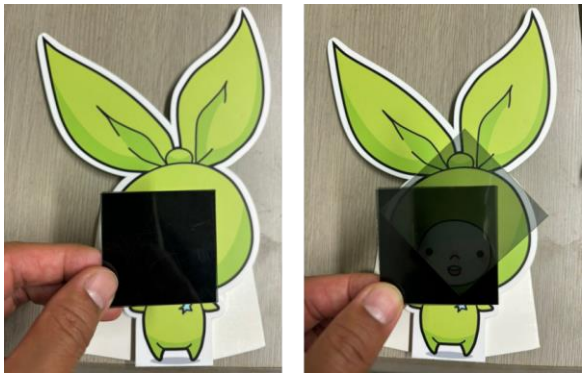

図 4. 透過軸が互いに直交する 2 枚の偏光板を置いた場合（左）と，その 2 枚の偏光板の間にもう 1 枚の偏光板を 45° 傾けて挿入した場合（右）の写真.
右の写真は偏光板が 1 枚多いにも関わらず，50%程度の透過光が見られる．45° 傾けた偏光板によって，この画像での縦と横方向の偏光が"重ね合わせ状態"になったことを示している．

BB84 方式は仕上げとして，Alice と Bob 間で“答え合わせ”を行い，秘密鍵の配送や盗聴の検出を行う．ここで，互いの基底が一致しなかった場合のビットは捨てて，一致した時のビットのみ利用する（通常，Z 基底を暗号鍵配送用，X 基底を盗聴者検出用といった具合に役割分担させる）．この時，もし盗聴者(Eve)がいた場合，基底が一致しているにも関わらず Alice と Bob のビットが異なるという結果が得られ，盗聴を検知できる．Eve は，自分がランダムに選んだ基底に基づきビットを復号し，コピーしたビット（光子）を Bob へ送り盗聴を見破られないようにする．従って，Alice と基底が同じになる確率が 1/2，基底が異なる場合でも当てずっぽうで 1/2 の確率で正解のビットを言い当てられる．すなわち，一つのビットに対する Eve の正答率は 3/4 となる．だが，読者の方々はこの正答率が高過ぎるのではないかと疑問に思うだろう．しかし，心配は無用である．確かに 1 つのビットから Eve を検知するのは難しく，そのビットは盗聴されてしまうかもしれないが，10 個のビットを使えば$(3/4)^{10}$=0.0563…，100 個なら~3.2×10^{-13} と，ビットを増やすことで現実的に不可能と言える正答率にまで下げることができる．以上要約すると，基底が異なった時の正答率 50%が不確定性原理に基づき“絶対に”保証されているので，QKD が絶対に盗聴不可能な暗号方式となる所以なのである．

3.　非古典光源の開発

3.1.　単一光子源の現状

現存する全ての量子暗号通信システムは，単一光子源として光強度を極度に絞ったレーザー光“擬似単一光子源”を用いている．しかし，2.で説明した通り，強度を絞ったとしても光子数分布は依然としてポアソン分布であり，Fock 状態には成り得ず，真の意味での単一光子源ではない．その結果，一つのパケットに光子が複数個入ってしまったり，空になる事態が発生し，暗号の秘匿性低下や誤り訂正率増加による鍵配送速度の低下が引き起こされる．従って，真の意味での単一光子源と，できればLED のように電池を繋ぐだけで使用できる汎用性の高い単一光子源の開発が急務となる．

これまで実証された単一光子源は，原子 1 個ないしは数個で構成される極めて微小な物質（すなわち量子）で構成されていた．そのため，単一光子という光は極めて人工的で普段一切関わりを持つことのできない特殊な光と思われがちだったが，最近その様相が変わりつつある．以前，確かに単一光子源は冷却原子，量子ドット，といった極めて特殊な人口物質で，しかも極低温（数 K）に冷却した状態でないと得ることができなかった．しかし近年，室温・常圧でも高レートで単一光子を発する材料・物質系が次々と発見されており，その一つがワイドギャップ半導体中の点欠陥（原子 数個単位の欠陥）または不純物である．読者の方々は，色がついている貴金属やステンドグラスの鮮やかな発色を見たことがあるだろう．これらは，いずれも結晶中の点欠陥や不純物による発光であり，カラーセンタ（色中心）と呼ばれている．近年，ダイヤモンドを始めとしたワイドギャップ半導体中のカラーセンタが，単一光子源として振る舞うことが発見され，それにより量子科学技術の開発機運が一気に高まっている．

3.2.　SiC 単一光子源

筆者らは，四半世紀にわたり炭化ケイ素(SiC)という半導体材料の研究に従事している．SiC とは，半導体の王様と評される Si と，地球上で最も強固な材料であるダイヤモンド(C)を“いいとこ取り”したような材料であり，近年パワー半導体として勢力的に実用化や量産化が進んでいる．例えば，最新鋭の電車や新型 N701S 系新幹線，電気自動車メーカートップの TESLA 社 MODEL3 やトヨタ社燃料電池車 MIRAI に SiC 半導体が搭載されており（図 5），さらにデータセンターの電源機器，家電製品など，応用範囲が多岐にわたり拡大

図 5. SiC パワーデバイスの豊富な実用化実績：電車・電気自動車・各種家電などに搭載

している．その SiC だが，2010 年頃からダイヤモンドと共に単一光子源や電子スピン源が次々と発見され，パワーデバイスだけでなく量子技術応用にも関心が高まって来た．SiC とダイヤモンドの共通する特徴として，堅牢でワイドギャップ半導体であることが挙げられ，これらの特徴は量子デバイスにとって非常に好ましい性質と言える．すなわち，堅牢であることは原子空孔のような原子が抜けた欠陥ができても潰れず構造安定性に寄与し，ワイドギャップであることは電子のエネルギーバンドへの熱流出を抑えるために室温高輝度発光の要因となる．さらに SiC に限れば，結晶成長技術の進歩により大口径（6 インチ以上）ウエハの量販化がなされ，パワーデバイスで培ったデバイス作製プロセス技術が成熟しているという，他の単一光子源材料にはない利点もある．また，実はあまり知られていない事だが，SiC は約 100 年前の 1927 年，人類初の発光ダイオード(LED)を実現させた材料でもある．加えて，GaN 系青色発光ダイオードが現在のように隆盛を極める前（1980 年代後半）においては，輝度に問題があったが，青色 LED をいち早く実用化させた経緯も有する．

以上より，SiC は量子応用技術の中でも，とりわけ“量子機能を有するデバイスや IC”を実現できる最有力候補として注目が集まっている．

SiC 半導体中に見つかった単一光子源の内，代表的なものを紹介しよう．まず，最も歴史が古く，開発が進んでいるのが Si 空孔と呼ばれる Si 原子が抜けてできた孔（あな）である．この単一光子源は波長 900nm 帯（近赤外域）の発光を有し，ダイヤモンド NV センタの可視域発光に比べて生体透過性が高いという特徴がある．また，光スピン操作を利用した nm オーダー領域の磁場または温度測定を可能にする量子センシングの実例も次々と報告されており，ダイヤモンド NV センタの強力なライバルとして挙げられている．他にも複空孔($V_{Si}V_C$)や SiC NV センタなど，様々な種類の単一光子源が開発されているが，詳細の説明は他書に譲りたい[4]．ところで，筆者らが数々の SiC 単一光子源の中でも特に注目しているのが，SiC 基板を酸化して SiO_2 膜を形成した際，SiC/SiO_2 界面に現れる単一光子源（以降，表面 SPS と呼ぶ）である（図 6）[5,6]．この表面 SPS は，通常単一光子源の形成に必要な高エネルギー粒子線照射が不要な上，極めて高輝度であり（ダイヤモンド NV センタの数倍の光子レート），かつ室温電気的制御が可能な点を特色としている．また，既に Si で培われた MOS デバイス・テクノロジーと相性が良く，新たな量子 MOS 型デバイスの創成や Si 系 MOS デバイスとの

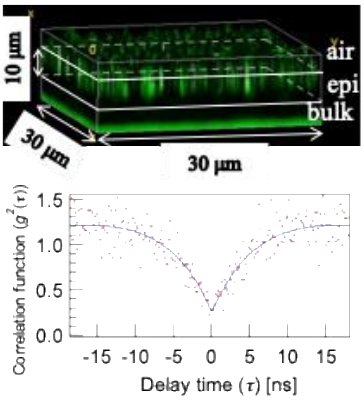

図 6. SiC エピ基板(図中 epi)上に形成された表面 SPS の 3D 画像（上）とその光子相関測定*3 結果（下）[6]．
τ= 0 でのディップ(anti-bunching)は同時に 2 つの検出器で光子が検出されないことを意味し，すなわち発光源が SPS（単一光子源）である事を表している．また，ディップ幅が数 ns と非常に狭いことは，高い単一光子放出レート(>100MHz)を示す．

*3 光子相関測定: 放出された光子を 2 つの経路に分岐し，それぞれの経路の 2 つの検出器で同時計数測定する．横軸は 2 つの検出器の時間差 τ，縦軸は自己相関関数 $g^2(\tau)$.

融合に期待が持てる．筆者らは，この表面 SPS を活用し，LED の如く電池に繋ぐだけで単一光子が発せられる“単一光子発生デバイス”を目下開発中である．本研究が成就した暁には，大規模な光学系が不要な小型かつ超高速・高純度の単一光子発生デバイスが完成するため，現行の擬似単一光子源と置き換えることで暗号性能と利便性を飛躍的に向上させたセキュリティネットワークが構築されると考えている．

4.　量子技術の応用展開

近年，量子技術の応用範囲は拡大の一途を辿っており，前出のワイドギャップ半導体がその主翼を担っている．既に述べた単一光子発生デバイス以外にもいくつかの応用例があるが，ここではその端緒について紹介していきたい．

当該分野で最も民生利用が近いと言われているのが主にワイドギャップ半導体を用いた“固体量子センサ”の開発である．基本的には単一光子源と同じ点欠陥を用いるのだが，点欠陥をカラーセンタではなく“電子スピン源”として利用する点が決定的に異なる．量子センサの検出原理だが，ここでは簡潔に述べるに留め，詳しくは既に数多く存在する文献を参照されたい[7]．電子スピン共鳴法(ESR)という元素分析手法があるが，量子センシングで用いる光検出磁気共鳴法(ODMR)はその派生版として考えて良い．ESR は，縮退していた up-spin と down-spin のエネルギー準位が外部磁場によってゼーマン分裂を起こすが，その分裂エネルギーに相当するエネルギーの電磁波（マイクロ波）を照射するとマイクロ波が吸収される（磁気共鳴）．その吸収されるマイクロ波周波数を測定して磁場や電流計測に応用したり，磁場を変えて試料の組成を同定したりする．一方 ODMR は，マイクロ波の吸収率ではなく蛍光強度の変化を用いる点で異なるが，磁気共鳴を利用して測定する原理は全く変わりない．量子センサは，点欠陥という原子サイズのセンサが構成でき，さらに量子状態が周囲環境に極めて敏感な事を利用し，超高感度化が図れる．現在，ダイヤモンド NV センタを筆頭に，量子技術の中でもとりわけホットなトピックである．

2019 年 10 月，Google の開発した量子コンピュータが世界最速スパコンでも 1 万年かかる計算をわずか 200 秒で実行したという，いわゆる“量子超越性”が Nature 誌に掲載された[8]．しかし，そこで用いた量子コンピュータは，超伝導量子ビットによって構成されているため，極低温への素子冷却が必要であり，システム上非常に大がかりなものとなる．その翌年，今度はフォトン量子ビットを用いた量子コンピュータの実証例が Science 誌に掲載され，脚光を浴びた[9]．量子コンピューティングの商業化は今まさに鰻上りに進んでおり，今後目が離せない分野である．ここでも筆者らは，SiC を用いて“手のひらサイズの量子コンピュータ”ができないかと，日々研究に邁進している．

最後に，量子イメージングについて紹介したい．量子イメージングは端的に言えば非古典

光源を照明として用いたイメージング手法であり，量子の性質を巧みに利用することで古典光を用いた場合よりも高分解能化やロバストな計測（光計測の大敵である振動や speckle ノイズ，迷光，さらには光学系の汚染などに耐性がある）が可能である．また，量子重ね合わせ状態や量子もつれを利用し，全く新しい概念に基づくイメージング法が提案されている．例えば，もつれ光子対を利用し，物理的に２つの光波を合わせることなく，光子対の時間相関によって干渉像を得る方法が提案された[10]．さらには，複数の非線形光学素子を設置し，素子で生成されるもつれ光子対がどの素子で生成されたかわからないよう光学系を配置することで，試料を通過していない光子で像を再生するという，まるで“心霊写真”のような現象を実証した例も報告されている[11]．これらに共通するのは光源として非古典光を用いていることであり，ここでも汎用性が高く高光子レートの単一光子源が重宝されると考えられる．

5. 最後に

近年ますます需要が高まっている量子暗号通信について，動作原理から現状の課題に至るまで俯瞰的に述べた．その中で，特に問題点として掲げられている単一光子源の現状について触れ，ワイドギャップ半導体による単一光子発生デバイスの実現が極めて有力な解決手段と成り得る事に言及した．また，量子暗号通信以外の量子応用分野についても紹介し，いずれの分野においても，筆者らが研究している LED 型単一光子発生デバイスが共通して有用であることを実例と共に述べた．筆者らは主に半導体量子デバイスなどのハードウェア開発に従事しているが，今後，量子情報処理や量子プロトコルなどのソフトウェア開発に関する研究者との連携を強化していきたいと切に願っている．

参考文献

[1] C.H. Bennett, G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing", Proceedings of IEEE Inter. Conf. Computers Systems and Signal Processing, Bangalore India, pp. 175-179 (1984).

[2] Ekert, Artur K, "Quantum cryptography based on Bell's theorem". Physical Review Letters. **67**: pp. 661-663 (1991).

[3] 高宮健吾：埼玉大学博士後期課程学位論文(2013).

[4] Takeshi Ohshima *et al.*, “Creation of silicon vacancy in silicon carbide by proton beam writing toward quantum sensing applications”, J. Phys. D: Appl. Phys. **51**: 333002 (2018).

[5] A. Lohrmann *et a.*, “Single-photon emitting diode in silicon carbide”, Nat. Commun.

6: 7783 (2015).

[6] Y. Hijikata, Y.-I. Matsushita, and T. Ohshima, "SiC thermal oxidation process and MOS interface characterizations: From carrier transportation to single-photon source" (Chapter 8) in "Handbook of Silicon Carbide Materials and Devices", Ed. Zhe C. Feng, Taylor & Francis, CRC (May 31, 2023).

[7] *For example*, Kai Bongs *et al.*, "Quantum sensors will start a revolution — if we deploy them right", Nature **617**: pp. 672-675 (2023).

[8] F. Arute *et al.*, "Quantum supremacy using a programmable superconducting processor", Nature **574**: pp. 505-510 (2019).

[9] H.-S. Zhong *et al.*, "Quantum computational advantage using photons", Science **370**: pp. 1460-1463 (2020).

[10] H. Defienne *et al.*, "Polarization entanglement-enabled quantum holography", Nat. phys. **17**: pp. 591-597 (2021).

[11] G.B. Lemos *et al.*, "Quantum imaging with undetected photons", Nature **512**: pp. 409-412 (2014).