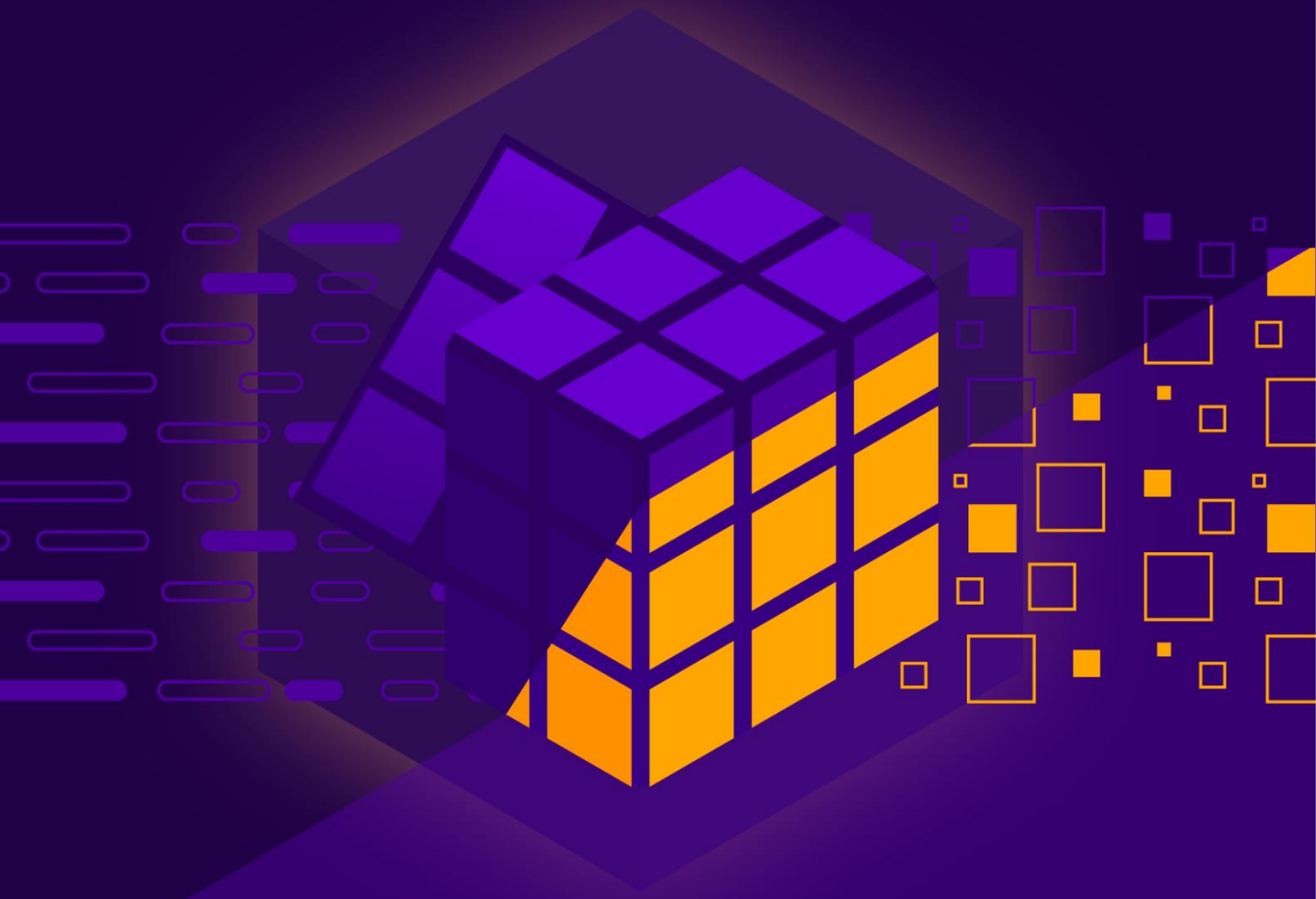
完全準同型暗号：
サイバーセキュリティ専門家のための包括的ガイド



CSAJC cloud security alliance Japan Chapter

CSA cloud security alliance®

Fully Homomorphic Encryption Working Groupの恒久的かつ正式な場所は https://cloudsecurityalliance.org/research/working-groups/fully-homomorphic-encryptionです。

© 2025 Cloud Security Alliance – All Rights Reserved.You may download, store, display on your computer, view, print, and link to the Cloud Security Alliance at https://cloudsecurityalliance.org subject to the following: (a) the draft may be used solely for your personal, informational, noncommercial use; (b) the draft may not be modified or altered in any way; (c) the draft may not be redistributed; and (d) the trademark, copyright or other notices may not be removed.You may quote portions of the draft as permitted by the Fair Use provisions of the United States Copyright Act, provided that you attribute the portions to the Cloud Security Alliance.

Acknowledgments

Lead Authors

Jez Goldstone
Joseph Wilson

Contributors

Songbo Bu
Nigel Smart
Asif Suleman

Reviewers

Harie Srinivasa Bangalore
William Butler
Sahil Dhir
Rahul Kalva
Eve Maler
Prateek Mittal
Venkata Nedunoori
Mithilesh Ramaswamy
Anand Sarangam

CSA Global Staff

Ryan Gifford
Stephen Smith

© Copyright 2025, Cloud Security Alliance.All rights reserved.

日本語版提供に際しての告知及び注意事項

本書「完全準同型暗号：サイバーセキュリティ専門家のための包括的ガイド」は、Cloud Security Alliance (CSA)が公開している「Fully Homomorphic Encryption: A Comprehensive Guide for Cybersecurity Professionals」の日本語訳です。本書は、CSAジャパンが、CSAの許可を得て翻訳し、公開するものです。原文と日本語版の内容に相違があった場合には、原文が優先されます。
翻訳に際しては、原文の意味および意図するところを、極力正確に日本語で表すことを心がけていますが、翻訳の正確性および原文への忠実性について、CSAジャパンは何らの保証をするものではありません。この翻訳版は予告なく変更される場合があります。以下の変更履歴（日付、バージョン、変更内容）をご確認ください。

変更履歴

日付	バージョン	変更内容
2025年02月12日	日本語版1.0	初版発行

本翻訳の著作権はCSAジャパンに帰属します。引用に際しては、出典を明記してください。無断転載を禁止します。転載および商用利用に際しては、事前にCSAジャパンにご相談ください。
本翻訳の原著作物の著作権は、CSAまたは執筆者に帰属します。CSAジャパンはこれら権利者を代理しません。原著作物における著作権表示と、利用に関する許容・制限事項の日本語訳は、前ページに記したとおりです。なお、本日本語訳は参考用であり、転載等の利用に際しては、原文の記載をご確認下さい。

CSAジャパン成果物の提供に際しての制限事項

日本クラウドセキュリティアライアンス（CSAジャパン）は、本書の提供に際し、以下のことをお断りし、またお願いします。以下の内容に同意いただけない場合、本書の閲覧および利用をお断りします。

１．　責任の限定
CSAジャパンおよび本書の執筆・作成・講義その他による提供に関わった主体は、本書に関して、以下のことに対する責任を負いません。また、以下のことに起因するいかなる直接・間接の損害に対しても、一切の対応、是正、支払、賠償の責めを負いません。
(1)　本書の内容の真正性、正確性、無誤謬性
(2)　本書の内容が第三者の権利に抵触しもしくは権利を侵害していないこと
(3)　本書の内容に基づいて行われた判断や行為がもたらす結果
(4)　本書で引用、参照、紹介された第三者の文献等の適切性、真正性、正確性、無誤謬性および他者権利の侵害の可能性

２．　二次譲渡の制限
本書は、利用者がもっぱら自らの用のために利用するものとし、第三者へのいかなる方法による提供も、行わないものとします。他者との共有が可能な場所に本書やそのコピーを置くこと、利用者以外のものに送付・送信・提供を行うことは禁止されます。また本書を、営利・非営利を問わず、事業活動の材料または資料として、そのまま直接利用することはお断りします。
ただし、以下の場合は本項の例外とします。
(1)　本書の一部を、著作物の利用における「引用」の形で引用すること。この場合、出典を明記してください。
(2)　本書を、企業、団体その他の組織が利用する場合は、その利用に必要な範囲内で、自組織内に限定して利用すること。
(3)　CSAジャパンの書面による許可を得て、事業活動に使用すること。この許可は、文書単位で得るものとします。
(4)　転載、再掲、複製の作成と配布等について、CSAジャパンの書面による許可・承認を得た場合。この許可・承認は、原則として文書単位で得るものとします。

© Copyright 2025, Cloud Security Alliance.All rights reserved.

３．　本書の適切な管理
(1)　本書を入手した者は、それを適切に管理し、第三者による不正アクセス、不正利用から保護するために必要かつ適切な措置を講じるものとします。
(2)　本書を入手し利用する企業、団体その他の組織は、本書の管理責任者を定め、この確認事項を順守させるものとします。また、当該責任者は、本書の電子ファイルを適切に管理し、その複製の散逸を防ぎ、指定された利用条件を遵守する（組織内の利用者に順守させることを含む）ようにしなければなりません。
(3)　本書をダウンロードした者は、CSAジャパンからの文書（電子メールを含む）による要求があった場合には、そのダウンロードしまたは複製した本書のファイルのすべてを消去し、削除し、再生や復元ができない状態にするものとします。この要求は理由によりまたは理由なく行われることがあり、この要求を受けた者は、それを拒否できないものとします。
(4)　本書を印刷した者は、CSAジャパンからの文書（電子メールを含む）による要求があった場合には、その印刷物のすべてについて、シュレッダーその他の方法により、再利用不可能な形で処分するものとします。

４．　原典がある場合の制限事項等
本書がCloud Security Alliance, Inc.の著作物等の翻訳である場合には、原典に明記された制限事項、免責事項は、英語その他の言語で表記されている場合も含め、すべてここに記載の制限事項に優先して適用されます。

５．　その他
その他、本書の利用等について本書の他の場所に記載された条件、制限事項および免責事項は、すべてここに記載の制限事項と並行して順守されるべきものとします。本書およびこの制限事項に記載のないことで、本書の利用に関して疑義が生じた場合は、CSAジャパンと利用者は誠意をもって話し合いの上、解決を図るものとします。

その他本件に関するお問合せは、info@cloudsecurityalliance.jp までお願いします。

© Copyright 2025, Cloud Security Alliance.All rights reserved.

日本語版作成に際しての謝辞

「完全準同型暗号：サイバーセキュリティ専門家のための包括的ガイド」は、CSAジャパン会員の有志により行われました。作業は全て、個人の無償の貢献としての私的労力提供により行われました。なお、企業会員からの参加者の貢献には、会員企業としての貢献も与っていることを付記いたします。
以下に、翻訳に参加された方々の氏名を記します。（氏名あいうえお順・敬称略）

高橋　久緒
松浦　一郎, CISSP, CISM, CDPSE
満田　淳
諸角　昌宏
米山　努

© Copyright 2025, Cloud Security Alliance.All rights reserved.

目次

© Copyright 2025, Cloud Security Alliance.All rights reserved.

はじめに

クラウドコンピューティングへの依存が高まる中、処理中のデータを保護することは重要な課題となっています。従来の暗号化方式は、保存中や転送中のデータは保護しますが、データをセキュアに処理しなければならない場合、特にAIによる攻撃や量子コンピューティングのような複雑で新たな脅威を伴う環境では不十分です。完全準同型暗号（FHE）は、暗号化されたデータを復号することなく計算できるようにすることで、画期的なソリューションを提供します。本書は、FHEの詳細な概要、その重要性、課題、サイバーセキュリティ専門家のためのベストプラクティスを提供します。

目的

この文書の主な目的は以下の通りです。

1. 完全準同型暗号の概念と仕組みを説明します。
2. クラウド、ブロックチェーン、データベース、そしてより広範なデータ経済におけるデータセキュリティとプライバシーの強化におけるFHEの重要性を強調します。
3. FHEに関連する課題を特定し、潜在的な解決策を提案します。
4. 実際のアプリケーションでFHEを実施するためのベストプラクティスを提供します。

このガイドを読み終わる頃には、サイバーセキュリティの専門家はFHEを完全に理解し、処理中の機密情報を保護するためにFHEを活用する方法を理解できます。

完全準同型暗号の理解 暗号化

完全準同型暗号とは？

完全準同型暗号（FHE）とは、暗号文に対して計算を実行し、暗号化された結果を生成することを可能にする暗号技術であり、復号されたときに、平文に対して実行されたのと同等の演算の結果と一致します。このコンセプトは2009年、Craig Gentryによって初めて実現され、データのライフサイクルを通じて暗号化を維持することを可能にすることで、暗号の分野に革命をもたらしました。

FHEの仕組み どのように機能するか？

FHEは、格子に基づく暗号と多項式演算の数学的原理に基づいています。以下は、FHEスキームの核となる構成要素です。

1. 鍵生成：このプロセスにより、暗号化用の公開鍵と復号用の秘密鍵が生成されます。これは、ス

© Copyright 2025, Cloud Security Alliance.All rights reserved.

キームのセキュリティパラメータに基づいて鍵ペアを作成することです。これは通常クライアントサイドで行われます。

2. 暗号化：公開鍵を用いて平文データを暗号文に変換します。このステップにより、データは暗号化され、セキュアな保護を確実にします。これもクライアント側の操作です。

3. 評価：暗号文に対して直接計算を行います。このコンポーネントはFHEの中核であり、暗号化されたデータを復号せずに操作できるようにします。FHEのセキュリティモデルでは、評価操作は多くの場合、クライアントの境界の外、サーバーサイドで実行されます。

4. 復号：得られた暗号文を、秘密鍵を使って平文に戻します。このステップでは、あたかも元の平文データに対して実行されたかのような計算結果を明らかにします。これはクライアントサイドで実行されることが多いですが、マルチパーティのFHEプロトコルの中には、協調的な復号フェーズを含むものもあります。

作業モデル：対称鍵 FHE

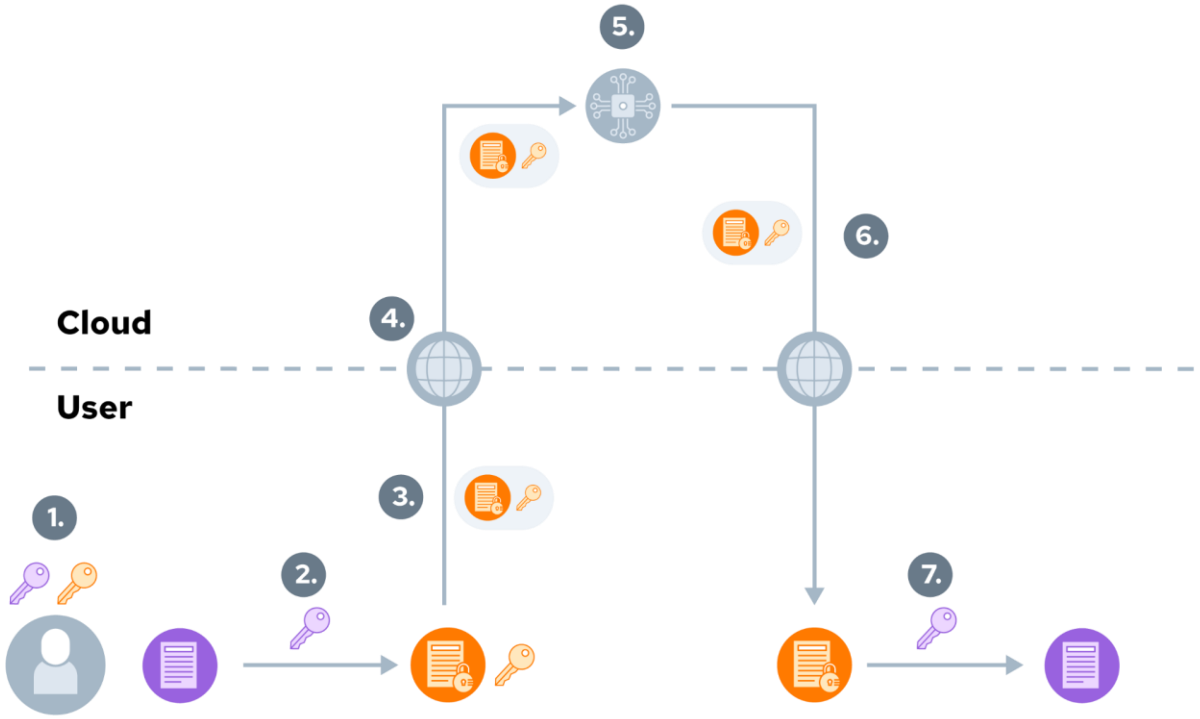


図1:対称鍵FHEのワークフロー

この作業モデルでは、ユーザーはデータを公開することなく、クラウド上の計算処理にデータを送ることを求めています。例えば、他では利用できないような高品質のデータ分析プラットフォームや機械学習モデルを活用したいと考えるかもしれません。

最初に、ユーザーは2つの鍵を生成します：(1.)秘密鍵（紫）と「サーバー」鍵（橙）。サーバー鍵は、FHE計算を行う際に適用される補助的な情報であり、暗号的な機密性はありません。

© Copyright 2025, Cloud Security Alliance.All rights reserved.

ユーザーは、FHE暗号化スキームの対称鍵バリアントを使用して、自分の秘密鍵を平文データ（紫）に適用し、暗号文（鍵のシンボルが付いた橙）に変換します（2.）その後、ユーザーは(3.)暗号文とサーバー鍵を(4.)インターネット経由でリモートのクラウドサーバーに送信することができます。

ユーザーから送られたデータは、一連のFHE演算処理によって処理されます。あらかじめ定義されたFHE計算のシーケンスの命名法は、(5.)「circuit」です。この処理は元の暗号文とサーバー鍵の両方を取り込み、元のデータに対して行われた処理の出力を含む新しい暗号文を返します(6.)。データが復号されることはありません。

その後、データはユーザーに返され、ユーザーは自分の秘密鍵を利用して出力された暗号文を復号（7.）します。

上記のモデルでは、暗号文へのデータのエンコードと、データが暗号化されるパラメータは、circuitを構築するために使用されるFHEスキームと演算に対応しなければなりません。クライアント側のアプリケーションは、このメタデータに従ってデータのエンコードと暗号化処理を行うことが期待されます。

FHEの共通鍵モデルは、公開鍵モデルにも拡張することができ、多人数による計算を可能にします。

完全準同型暗号

FHEは、暗号化されたデータに対する計算をサポートする、より広範な暗号システムの特殊なケースです。より広範な準同型暗号化スキームには、以下のようなものがあります。

- 部分準同型暗号（PHE）：足し算か掛け算のどちらかをサポートしますが、両方はサポートしません。暗号システムの例としては、RSA（乗法）、Paillier（加法）などがあります。
- サムホワット型準同型暗号（SHE）：限られた数の加算と乗算をサポートします。
- Leveled完全準同型暗号 (Leveled FHE)：鍵生成時に決定される一定数のオペレーションをサポートします。
- 完全準同型暗号(FHE)：無制限の加算と乗算をサポートし、暗号文に対する任意の計算を可能にします。

なぜ完全準同型暗号が重要なのか？

FHEは、信頼された境界の外でも情報を暗号的にセキュアに保つことを可能にすることで、斬新なデータ利用の機会を豊富に提供します。特に、セキュリティを犠牲にすることなく、他のデータ保有者と協力する能力です。以下では、望ましいアプリケーションを可能にするFHEの重要な側面について説明します。

エンドツーエンド セキュリティ

© Copyright 2025, Cloud Security Alliance.All rights reserved.

機密データは常に暗号化されているため、セキュリティインシデントの影響は大幅に軽減される可能性があります。認可されたコンポーネントは、何らかの理由で機密データにアクセスする必要が生じる可能性があるため、このメリットの程度は、エンドツーエンドのシステム全体で考慮する必要があります。

アタックサーフェスの大幅な削減

このリスクの範囲は、機密情報を知る必要を持つ認可されたアクセスが有するコンポーネントのみに大幅に縮小され、リスクの可能性はさらに減少します。

データプライバシー強化

クラウドコンピューティングでは、データはリモートサーバーで処理されることが多く、潜在的な脅威にさらされます。従来の暗号化方式では、データを処理する前に復号する必要があるため、データが脆弱になります。FHEは、暗号化されたデータの計算を可能にすることで、このリスクを排除し、データのライフサイクル全体を通してデータのプライベート性とセキュリティを確保します。

実用的な観点から見ると、FHEの利点は、信頼された環境の外（移動中、保存中、使用中を含む）にあるデータのエンドツーエンドのセキュリティを確保することで、鍵管理の問題を縮小できることです。これにより、アタックサーフェスを大幅に削減します。

低帯域幅での秘匿マルチパーティ計算

FHEは秘匿マルチパーティ計算（SMPC）を促進し、複数のパーティがプライバシーを維持しながら、入力に対する関数を共同で計算することを可能にします。特に、異なるソースからの機密データの機密性を維持しなければならない、連携学習や共同分析のようなシナリオではそうです。暗号化されたデータ上で計算を可能にすることで、FHEは処理中に機密情報が決して漏洩しないことを保証します。SMPCを可能にする他の方法とは異なり、FHEを介したSMPCの方法は、低帯域幅の要件でSMPCを可能にします。

General Data Protection Regulation（GDPR）、Digital Operational Resilience Act（DORA）、California Consumer Privacy Act（CCPA）などの厳しいデータ保護規制により、企業はユーザーのデータのプライバシーを確保しなければなりません。FHEは、処理中のデータを保護することにより、これらの規制要件を満たす堅牢なソリューションを提供します。これにより、データ侵害やコンプライアンス違反による罰則のリスクが軽減され、FHEは機密情報を扱う組織にとって魅力的な選択肢となります。

クラウドの信頼性を高めるサービス

より多くの組織がクラウドに移行する中で、クラウドサービスプロバイダーに対する信頼は最も重要です。FHEは、クラウドプロバイダーでさえも処理中のデータにアクセスできないようにすることで、この信頼性を高めています。これにより、企業はデータセキュリティを犠牲にすることなく、クラウドサービスの拡張性と柔軟性を活用することができます。

© Copyright 2025, Cloud Security Alliance.All rights reserved.

潜在的な課題と解決策

計算オーバーヘッド

FHEの主な課題のひとつは、計算オーバーヘッドが大きいことです。暗号化されたデータに対する操作は、平文データに対して行われる操作よりも本質的に計算集約的でリソースを必要とするため、特に大規模システムやリアルタイムアプリケーションでは、パフォーマンスのトレードオフが顕著になります。この課題を軽減するアプローチは以下のようにいくつか存在します。

1. **最適化のテクニック**：FHEワークフローのデータ符号化と暗号計算フェーズのアルゴリズムを最適化することで、FHE circuitの複雑さを軽減し、性能を向上できます。これらの最適化は、通常、FHEライブラリやその他のユーティリティに取り込まれています。
2. **ハードウェアアクセラレーション**：グラフィックスプロセッシングユニット（GPU）やFPGA（Feld Programmable Gate Array）などのハードウェアアクセラレータを活用することで、計算を大幅に高速化することができます。これらのデバイスは並列処理に適しており、FHEで使用される多項式演算に有益です。専門的なFHEハードウェアアクセラレータ（ASICなど）が開発されており、現在は商業化前のフェーズにあります。
3. **効率的なスキーム**：CKKS（近似演算向け）やBGV（厳密演算向け）のようなFHEスキームは、より効率的な並列計算を提供できます。アプリケーションの要件に基づいて適切なスキームを選択することで、パフォーマンスを向上させることが可能です。アプリケーションの要件によっては、スキームの選択は開発者の権限に属する場合もあれば、FHEを扱うための特定のツールやフレームワークの使用に固有の場合もあります。

鍵管理

データプロバイダーとFHEサービスの間で交換されるFHE鍵（「サーバー鍵」）は、暗号的に不活性です。これらはFHE処理に従事するために必要ですが、クラウド上の情報を復号するために使用することはできません。

FHEで暗号化された結果に、その後も繰り返しアクセスする必要がある使用例があるかもしません。そのような場合には、継続的なアクセスを確保するため、および／または、後続の関係者にアクセスを許可するための適切な鍵管理プロセスが必要となります。複数の関係者が関与する場合は、閾値方式やマルチキー方式など、適切な鍵管理・鍵拠出方式の導入を検討しなければならなりません。プロトコルとソリューションの要件によっては、セキュアなアプライアンスや鍵管理ソリューションに関して追加の考慮が必要になる場合があります。これらの検討は、データが継続的にどのようにアクセスされるかを考慮した縦断的データアクセス要件に適合するように設計される必要があります。

© Copyright 2025, Cloud Security Alliance.All rights reserved.

ノイズマネジメント

FHEにおいて「ノイズ」とは、暗号化されたメッセージに意図的に導入されたランダムな要素であり、そのセキュリティを保証するものです。ノイズは暗号化されたメッセージにビットベクトルとして付加され、高次ビットにメッセージが格納されます。

クラウドの専門家は一般的に、FHEの実装におけるノイズ管理の詳細を直接考慮する必要はないでしょう。とはいえ、FHEコンピューティングにおけるノイズの重要性と影響を考慮し、以下に主要な用語と概念をリストします。

ノイズの増加

暗号化された値に対して操作が行われるたびに、ノイズは増加します。これは加算演算よりも乗算演算の方が顕著です。

ノイズによる破損

ノイズが大きくなりすぎると、メッセージと重なり、その値を破損してしまいます。

ブートストラッピング

「ブートストラッピング」は、実装の違いはあるにせよ、すべてのFHE方式でサポートされている操作です。ブートストラップ操作により、暗号文のノイズが大幅に低減され、ブートストラップを繰り返し使用することで無限に計算を実行することができます。したがって、ブートストラップは*完全*準同型暗号を達成するために不可欠です。

典型的なFHEプログラムは、ノイズを管理するために、ブートストラップに続いて一連の操作を実行し、この操作のサイクルを繰り返します。ブートストラップが必要な頻度は、FHEスキーム、アプリケーション、および暗号パラメータの関数であり、ブートストラップスケジュールを最適化するには、専門家の知識と実装が必要となります。

ブートストラッピングには、ゲートブートストラップやファンクショナルブートストラップ、プログラマブルブートストラップなどの種類があります。

現在、計算負荷を軽減する、より効率的なブートストラップ処理方法の開発に向けた研究が進められています。特定のアプリケーション向けの近似ブートストラップなどの技術は、過剰なオーバーヘッドを発生させることなく、ノイズを管理するのに役立ちます。

その他のノイズ管理アプローチ

ブートストラッピングは、FHEにおけるノイズ管理の主要なアプローチです。しかし、計算コストが高く

© Copyright 2025, Cloud Security Alliance.All rights reserved.

なることも多く、時には過度にコストがかかることもあります。そのため、多くの方式では、ノイズ管理に役立つ補助的なアプローチ（Leveledモード演算やモジュラスイッチングなど）もサポートしています。

ハイブリッドアプローチ

FHEをマルチパーティコンピューティング（MPC）や機械学習（ML）アルゴリズムなどの他の暗号技術と統合することで、クラウドコンピューティングやエッジコンピューティングのような複雑な環境におけるノイズの軽減、パフォーマンスの最適化、計算効率の向上に役立ちます。これらのハイブリッドアプローチは、異なる手法の長所を活用することで、より優れたパフォーマンスとセキュリティを実現します。

実装の複雑さ

FHEを実装するには、暗号の原理を深く理解し、既存のシステムと慎重に統合する必要があります。ユーザーフレンドリーなライブラリやツールの開発により、このプロセスが簡素化されています：

1. **FHEライブラリ**：OpenFHE、Lattigo、TFHE-rs、Microsoft Seal、HELib、Pyfhel、TenSEAL、Sunscreen、cuFHE、NuFHEなどのライブラリは、暗号や数学的プリミティブ、その他のユーティリティの低レベル実装を開発者に提供しています。
2. **FHEコンパイラとツールチェーン**：HEIR、HECO、HELayers、EVA、Concreteのような高レベルのユーティリティは、開発者に高レベルのインターフェースを提供し、暗号学の専門知識や専門家の理解を必要とせずに、より複雑なFHEアプリケーションを開発することを可能にします。
3. **教育リソース**：包括的なドキュメント、チュートリアル、コミュニティサポートは、FHEの実装を学ぶ開発者にとって極めて重要です。FHEの導入を促進するために、組織や学術機関がこうしたリソースを提供するケースが増加しています。

セキュリティ上の考慮事項

FHEは、関連するセキュリティモデルの中では強固なセキュリティを提供しますが、それでも注意は必要です。FHE実装のセキュリティ確保には、以下のセキュリティ上の考慮事項への対応が必要です。

1. **サイドチャネル攻撃**：FHEは計算中のデータを保護しますが、暗号化または復号の時点におけるサイドチャネル攻撃は依然として脅威となりえます。これらの攻撃を軽減するには、セキュアなハードウェアやセキュアなソフトウェアの開発手法が必要です。これらは、暗号ライブラリと、FIPS-140のような標準規格が定める標準的なセキュアハードウェア設計手法の両方によって確保されるべきです。
2. **パラメータの選択**：FHEスキームに適切なパラメータを選択することは、セキュリティとパフォーマンスを確保するために非常に重要です。パラメータを適切に選択することで、セキュリティ、パフォーマンス、ノイズ管理のトレードオフのバランスを取ることができます。ほとんどの暗号ライブラリは、指定された計算に適切なパラメータを自動的に選択するユーティリティを提供しています。

© Copyright 2025, Cloud Security Alliance.All rights reserved.

3. **サイバーセキュリティの実践**：FHEは特に、使用中のデータ保護と機密性を確保するための強力なセキュリティモデルを提供します。恐喝を伴うランサムウェアに対しては、データの外部流出を制限することで、ある程度の防御は可能ですが、ランサムウェアのような他の破壊的サイバー攻撃に対しては防御できません。FHEのワークフローを設計する際にも、現代のサイバーセキュリティの慣行に従うべきです。

4. **アクセス制御**：FHEは入力保護の一形態です。データ入力への不正なアクセスは防ぐことはできますが、計算の出力自体に機密情報が含まれないという保証はありません。計算の潜在的な出力（例えば、返される名前のリスト）とその重要性は前もって理解されるべきであり、これらの出力に機密情報が含まれると予想される場合は、アクセスを制限するために適切なアクセス制御が行われるべきです。結果を公表する場合は、差分プライバシーなどのアウトプット保護アプローチと合わせてFHEの使用を検討することが必要です。

法律と倫理に関する考慮事項

- **データ所有権と管理責任**：組織は、FHEソリューションを導入する際、データの所有権、データ処理に対する同意、説明責任に関する法的な意味を考慮しなければなりません。GDPRのような規制の遵守は、データ取扱実務における信頼と合法性を維持するために不可欠です。
- **データの倫理的使用**：研究や分析における暗号化データの倫理的使用に関するガイドラインを確立することは、データ分析による誤用や意図しない結果を防ぐために重要です。

完全準同型暗号のベストプラクティス

適切な**FHE**スキームの選択

さまざまなFHEスキームは、それぞれ異なる長所と短所を示しています。アプリケーションの要件に基づいて適切なスキームを選択することは、パフォーマンスにとって極めて重要であり、現在のところ専門家の見識が必要です。しかし、FHEのソフトウェアエコシステムが成熟するにつれて、適切なスキームとパラメータの選択は、実際の実装から得られたベストプラクティスによって導かれ、場合によってはコンパイラレベルで完全に自動化されることが期待されます。以下に既存のスキームの概要を記載します。

1. BGV/BFV：正確な算術演算に適しており、高精度を必要とする用途に最適。
2. CKKS：近似演算に最適化されており、ある程度の近似が許容される機械学習などのアプリケーションに便利。
3. TFHE：Boolean circuitや、小さなデータ項目に対するルックアップテーブルとして表現可能な関数に対して効率的。

パフォーマンス最適化

© Copyright 2025, Cloud Security Alliance.All rights reserved.

FHEのパフォーマンスオーバーヘッドを軽減するために、以下の最適化アプローチを検討します。

1. **ハードウェアアクセラレーション**：GPU、FPGA、または専用のハードウェアアプライアンスを使用して計算を高速化します。GPUやFPGAは並列処理や専門的なcircuit実装に優れており、FHEで使用される多項式演算に有益です。専用ソリューションは、FHEコンピューティング運用のために明確に設計されたハードウェアを特徴とします。

2. **コストの最適化**：FHEは必要な場合にのみ使用し、計算やデータ処理は可能な限り事前にクリアな状態で実施します。FHEプロセスの要件に適合するデータサニタイゼーションワークフローは、早期に特定されるべきであり、FHEアプリケーションのライフサイクルを通じて一貫性を保つことが理想的です。

セキュリティとコンプライアンスの確保：

FHEを実装する際には、セキュリティが最も重要です。堅牢なセキュリティを確保するために、以下のベストプラクティスに従ってください。

1. **定期的な監査**：FHE実装の暗号ライブラリとツールを定期的に監査し、脆弱性がなく、期待通りに動作することを確認してください。外部の検査に対してオープンであり、査読を受けた暗号解読の対象となる暗号スキームを実装したライブラリ上に構築されたソリューションのみを使用してください。

2. **パラメータの選択**：セキュリティ、パフォーマンス、およびノイズ管理のバランスを取るために、FHEスキームのパラメータを慎重に選択します。FHEコミュニティが提供するガイドラインやベストプラクティスを参照し、可能であればFHEライブラリやツールチェーンの自動パラメータ生成機能を活用してください。

3. **警戒**：FHEは、信頼されていないコンピューティングシステムにおけるデータの機密性の課題に対処することができます。しかし、FHEを利用することですべてのサイバーセキュリティの脅威（ランサムウェアなど）がなくなるわけではなく、FHEは、コンピューティングシステムの完全性を確保するための従来のメカニズムやプロセスと並行して活用されるべきです。

拡張性と柔軟性を備えた設計

- **将来の拡張計画**：FHEの実装が、データ量の増加や計算の複雑さに応じて拡張できることを確認してください。これには、将来の機能拡張やデータ処理ニーズの変更に対応可能な、柔軟なアーキテクチャを選択することが含まれます。

- **既存システムとの相互運用性**：既存および将来のアプリケーションとの統合を検討します。これには、システムの特性（特に、計算に関与するデータタイプと情報フォーマット）を正式に記録する必要があります。また、暗号化/復号ルーチンをコードベースに分離し、必要に応じて暗号アジリティを可能にすることについても検討する必要があります。これらの慣行は、将来的なシステムとの統合を容易にし、該当する場合には、異なるプラットフォーム間での幅広い採用を支援するものでなければなりません。

© Copyright 2025, Cloud Security Alliance.All rights reserved.

定期的なアップデートと教育

1. **継続的な学習**：学術論文、業界会議、およびオンラインコースを通じて、FHEの最新の進歩を常に把握することができます。新しい技術やツールに後れを取らないことは、最も効率的でセキュアなソリューションの導入に役立ちます。

2. **コミュニティへの関与**：フォーラムや専門家グループなど、FHEや暗号技術のコミュニティに参加してください。他の専門家と関わることで、洞察やサポート、協力の機会を得ることができます。

健全な実装戦略

1. **要件を特定する**：データガバナンスの改善や簡素化、コラボレーションやデータ活用の新たな機会、市場内での革新や差別化など、FHEが付加価値を提供する場所を特定します。

2. **解決策を特定する**：特定された要件によっては、解決策（プロトコル、セキュアな計算の原型、あるいは製品）がすでに存在しているかもしれません。例えば、2つの異なるデータベースに共通する要素を秘密裏に特定する能力が要求される場合、これは*秘匿積集合の例であり*、FHEの下で実行可能で、すでにプロトコルやソリューションが存在するプライベートコンピューティングの原型です。

3. **プロトタイプとテスト**：特に、モノのインターネット（IoT）やエッジコンピューティングのような急速なスケーリングが必要なシナリオでは、小規模なプロトタイプから始めて、特定のユースケースにおけるFHEの実現可能性、パフォーマンス、およびスケーラビリティを評価します。これにより、本格的な導入前に潜在的な課題を特定し、対処することができます。

4. **反復的に改善する**：FHEを段階的に導入し、ソリューションを継続的に最適化し、再調整します。各段階からのフィードバックを次の段階の改善に利用し、堅牢で効率的な最終的な実装を確実にします。

実社会における実装上の課題

どのような変化であれ、その導入には独自の課題が伴います。以下は、私たちが直面する可能性のある課題の一部です。

1. **統合の複雑さ**：FHEを既存のシステムやワークフローに組み込むことは複雑で、慎重な検討が必要です。

2. **必要な専門知識**：複雑な暗号化を抽出する共通ライブラリが利用できるようになったことで、参入障壁は低下しています。セキュリティパラメータを適切に使用することは、セキュアな実装のために不可欠です。業界は標準化と抽象化に積極的に取り組んでおり、FHEはこれまで以上に利用しやすくなっています。

3. **パフォーマンスのオーバーヘッド**：ハードウェアとソフトウェアの最適化における継続的な進歩は、処理速度を著しく向上させています。他のシステムコンポーネントと同様に、採用する側もパ

© Copyright 2025, Cloud Security Alliance.All rights reserved.

フォーマンスの必要性を考慮する必要があります。

4. **ユーザー・アドプション**：明確なコミュニケーションとトレーニングは、組織がこれらの技術を採用するのに役立ちます。

結論

完全準同型暗号は、暗号学の分野において画期的な進歩であり、プライバシーを侵害することなく暗号化されたデータ上で計算を実行する能力を提供します。この技術は、特にクラウドコンピューティングや共同作業環境におけるデータセキュリティの重要な課題に対処するものです。FHEには、計算オーバーヘッドや実装の複雑さといった課題がありますが、現在進行中の研究や技術の進歩により、今後ますます実用的で効率的になっていくでしょう。

サイバーセキュリティの専門家にとって、FHEを理解し活用することは、データプライバシーを強化し、規制コンプライアンスを確保し、クラウドサービスに対する信頼を構築することにつながります。ベストプラクティスに従い、最新の動向を把握することで、専門家は進化し続けるデジタル環境において、FHEを効果的に導入し、機密情報を保護することができます。組織がデータセキュリティとプライバシーをますます優先するようになるにつれ、FHEはこうした要求に応え、クラウドコンピューティングとその先の将来のセキュリティを確保するための重要なツールとして浮上しています。

完全準同型暗号をしっかりと理解することで、サイバーセキュリティの専門家は、現代のデータ保護の複雑な状況を自信を持ってナビゲートし、より安全でセキュアなデジタル世界に貢献することができます。

© Copyright 2025, Cloud Security Alliance.All rights reserved.