仕　様　書

１．件名

楕円曲線に基づく暗号技術の安全性評価プログラムの高速実装作業

２．研究の概要

国立研究開発法人産業技術総合研究所（以下、「産総研」という。）サイバーフィジカルセキュリティ研究部門では、国立研究開発法人科学技術振興機構が主催する戦略的創造研究推進事業の CREST「サステナブルな分散型秘密計算基盤」(JPMJCR22M1）として、秘密計算技術に関する研究を実施しており、その関連研究として楕円曲線に基づく暗号技術（以下、「ECC」という。）の安全性評価についても研究を行っている。特に、計算機実験による安全性評価を実施しており、この実験には大きな計算能力や計算資源が必要となるため、安全性評価を行うプログラムの高効率化、大規模な計算機環境を効果的に活用して実験を行う必要がある。

本件は、ECC の安全性評価プログラムを、調達請求者の指示に基づきスーパーコンピュータ環境向けに高速実装し、これを用いた実験作業を行うものである。

３．作業項目

（１）　楕円曲線に基づく暗号技術の安全性評価プログラムの高速実装

（２）　楕円曲線に基づく暗号技術の安全性評価プログラムを用いた実験

４．作業項目別仕様

受注者は、作業を実施するにあたり、次の事項に対応すること。

- 調達請求者と定期的に意見交換や議論・協議を行い、作業に関する情報や得られた情報や必要なノウハウの詳細を適宜共有して解説すること。
- 作成したデータ、実施予定及び実施した作業の報告書及び意見交換や議論・協議に関する議事録を作成し提出すること。

（１）　楕円曲線に基づく暗号技術の安全性評価プログラムの高速実装

- 受注者は、調達請求者が貸与するサンプルプログラムと指示に基づき、分散計算環境における高速計算技術・アルゴリズム・ソフトウェア・システムに関する技術動向、関連する文献、プログラムやソフトウェア、ライブ

ラリ、ソースコードの調査を行いつつ、楕円曲線に基づく暗号技術の安全性評価を高速に行うためのプログラムを作成する。

- 受注者は、プログラムの作成において必要な開発環境を構築し、作成したプログラムの正しさを確認するためのテストプログラムや、性能を評価するためのベンチマークプログラム、さらにこれら結果の解析と、必要な場合はその結果を可視化するための統計処理・可視化処理プログラムも作成する。
- 受注者によるプログラム作成において使用するプログラミング言語は、C++言語を想定しているが、調達請求者と協議の上で、必要に応じて適宜 C 言語や Python、SageMath、アセンブラなど他の言語を使用してもよい。
- 受注者が作成するプログラムについて、その動作環境は、ABCI 3.0 と、OS として Ubuntu 24.04 LTS が動作する x86-64 とその拡張命令セットアーキテクチャ及び CUDA による GPGPU 環境とする。なお、本作業の実施のために、ABCI 3.0 の利用グループの使用権限を受注者に貸与する。
- このプログラムは、GCC や LLVM などの Linux と GPGPU 環境で一般的に用いられているツールチェインにより実行可能であること。
- このプログラムは、上記の環境に加えて、Ubuntu 以外の他の一般的な Linux 環境でも動作する互換性を備えること。加えて、可能な場合は、Windows 11 以降や macOS 14 以降の環境でも動作すること。互換性の確保のために、Docker コンテナなどを使用してもよいが、この場合は、容易にプログラムの実行や実験の再現が可能となるように、設定や実行方法についての詳細な文書とスクリプトを作成して納品すること。
- 受注者は、作成したプログラムのソースコード及びその解説書を「１０. 納入期限及び納入場所」に記載の期限までに納入すること。

（２） 楕円曲線に基づく暗号技術の安全性評価プログラムを用いた実験

- 受注者は、調達請求者の指示に基づき、上記（１）で作成したプログラムを使用した実験の実施と得られたデータの収集及び分析を行う。例えば、調達請求者が計測対象と収集データや統計処理などの仕様を指示するので、受注者はこれに従い、実験実行スクリプトの作成作業などを行う。
- 受注者は、実施する作業や統計情報の生成作業及びその可視化といった作業は、例えばスクリプトを作成するなど再現可能な形式で実施し、これを納入物品に含めること。
- 受注者は、作成したスクリプトをソースコードの一部として、スクリプトの使用方法や実験結果を作業報告書や解説書の一部として納入物品に含めて、「１０. 納入期限及び納入場所」に記載の期限までに納入すること。

６．特記事項

（１） 「サプライチェーン・リスクに対応するため、別紙に記載する事項に従って契約を履行しなければならない。」

（２） 受注者は以下の技能を有すること。

・ 本調達で実施する作業では本研究に関する専門知識、特に楕円曲線に関する理論や関連する数論及び代数学などの数学的理論と関連するアルゴリズムと、要求仕様に基づく高速実装の技能、例えば漸近計算量などの理論だけでなく、プロファイリングなどの実験と使用計算環境の知識に基づく高速実装の技能が求められるため、以下に示す受注者に求める技能・実績に関する技術や計算環境、技能に関する十分な知識を有し、以下に示す計算環境におけるソフトウェア開発や高速実装について 3 年以上の業務実績または 3 年未満の場合は同等以上と認められる業務実績を有すること。さらに、関連する技術及びその分野について、付随する英文マニュアルや英文論文等を判読できる十分な英語能力を有し、英語のみで提供される情報源に基づき、独立して設計及び実装にかかる文献調査、プログラム調査、実験環境構築、評価実験、プログラムの作成を遂行できること。

- プログラミング言語 C、C++及び Python によるソフトウェア開発の実績。
- CUDA による GPGPU プログラミングやソフトウェア開発の実績。
- SIMD（主に AVX2、AVX512）プログラミングやソフトウェア開発の実績。
- 楕円曲線に基づく暗号技術に関する高速実装及びソフトウェア開発の実績。特に、有限体演算の高速実装の技能を有すること。
- 耐量子計算機暗号技術に関するソフトウェア開発の実績（楕円曲線に基づく暗号技術と耐量子計算機暗号技術は異なる技術だが、本作業の遂行には暗号技術とその数理的構造への理解、数論及び代数処理の実装経験や実績を有することが望ましい）。
- マルチスレッド及びマルチコアによる並列プログラミング及びソフトウェア開発の実績。
- スーパーコンピュータ環境における MPI による大規模並列分散計算及び高性能計算に関するプログラミング及びソフトウェア開発の実績。
- 高速性と可用性・保守性・移植性のバランスを考慮したプログラミングやソフトウェア開発の実績。

・ 調達請求者と議論、協議を行いながら作業を実施できること。

７．納入物品

（１） 作業報告書（議事録含む） 1 部（電子媒体）
（２） ソースコード 一式（電子媒体）
（３） 解説書 一式（電子媒体）

※電子媒体の場合、原則として USB メモリ等の外部電磁的記録媒体は用いないこと。

８．貸与品

（１） ABCI 利用グループの使用権限
（２） サンプルプログラム

９．納入の完了

「７．納入物品」に記載された納入物品が過不足なく納入され、仕様書を満たしていることを確認して、納入の完了とする。受注者は、確認に係る作業を支援すること。

１０．納入期限及び納入場所

納入期限：2025 年 11 月 14 日
納入場所：東京都江東区青海 2-3-26
国立研究開発法人産業技術総合研究所
臨海副都心センター　本館　1104 号室
サイバーフィジカルセキュリティ研究部門

１１．成果の取扱い

（１） 産総研は、受注者がプログラム作成により得られた技術上の成果のうち産総研が指示するもの（以下「成果」という。）についての利用及び処分に関する権利を専有するものとする。
（２） 受注者は、成果に係るソフトウェアの著作権（著作権法第 27 条及び第 28 条に規定する権利を含む。）及び意匠登録を受ける権利を産総研に譲渡するものとし（譲渡対価は契約金額に含まれるものとする。）、著作者人格権を行使しないものとする。ただし、パッケージ製品に係るものは除く。
（３） 受注者は、契約条項に定める検査に合格後、直ちに別紙様式による著作者財産権譲渡証書及び著作者人格権不行使証書を産総研に提出しな

ければならない。

（４） 受注者は、産総研に対し、納品した成果品が第三者の知的財産権を侵害しないことを保証するものとする。なお、納品した成果品について、第三者の権利侵害の問題が生じ、その結果、産総研又は第三者に費用や損害が生じた場合は、受注者は、その責任と負担においてこれを処理するものとする。

１２．セキュリティ要件

（１） 受注者に求める資格要件

情報セキュリティマネジメントシステム(ISO/IEC 27001/JIS Q 27001)の資格を有していることを推奨する。

（２） 情報セキュリティポリシーに関する要件

①本業務の遂行に当たっては、産総研の情報セキュリティポリシー（別途定める読み替え条項に従うものとする。以下同じ。）を遵守するとともに、情報セキュリティポリシーにおいて産総研に求められる水準の情報セキュリティ対策を講じること。産総研の情報セキュリティ規程については、下記 URL を参照のこと。その他の情報セキュリティポリシーの詳細については受注者決定後に提示する。

【国立研究開発法人産業技術総合研究所情報セキュリティ規程】
https://www.aist.go.jp/Portals/0/resource_images/aist_j/outline/comp-legal/pdf/securitykitei.pdf

②産総研の情報セキュリティポリシーの見直しが行われた場合は、見直しの内容に応じた情報セキュリティ対策を講じること。なお、対応内容については調達請求者に事前に報告し承認を得ること。

（３） その他セキュリティに関する事項

①受注者は、本業務の履行に際して、秘密である旨を示されて貸与を受けた秘密情報を秘密として適切に保持することとし、第三者に開示又は漏洩してはならない。

②受注者は、本業務の履行によって知った一切の情報を本業務の履行以外の目的に利用してはならない。契約終了後も同様とする。

③貸与品及び提供する資料は、調達請求者の了解なしに所外に持ち出しまたは複製してはならない。

④産総研の所外へ持ち出しまたは複製した貸与品及び提供する資料については一覧表を作成し、調達請求者に提出すること。なお、契約終了後、速やかに返却又は廃棄し、その旨を調達請求者に報告して確認を得たうえで一覧表からの削除を行うこと。
⑤受注者は、契約締結後、情報セキュリティ管理体制を記載したドキュメントを産総研担当者に提出すること。
⑥受注者は、本業務において、受注者の従業員若しくはその他の者によって、意図せざる変更が加えられない管理体制とすること。
⑦受注者は、産総研の求めに応じて、資本関係、役員等の情報、委託事業の実施場所並びに委託事業従事者の所属、専門性（情報セキュリティに係る資格・研修実績等）、実績及び国籍に関する情報提供を行うこと。
⑧本業務にかかる情報に関する情報セキュリティインシデントが生じた場合、速やかに報告の上、原因の分析を実施し、産総研担当者と対処内容及び再発防止策を検討すること。当該インシデントへの対処を実施するにあたっては、事前に産総研担当者の確認を得ること。
⑨情報セキュリティインシデントが生じたことで、受注者の作業環境等の確認が必要となった場合には、産総研の調査に協力を行うこと。
⑩産総研で情報セキュリティインシデントが発生した場合、速やかに調査及び復旧に協力を行うこと。
⑪履行期間が半年以上の場合、本業務の遂行における情報セキュリティ対策の履行状況を確認するため、産総研が提示するチェックリストの内容に基づき、適宜情報セキュリティ対策の履行状況を報告すること。
⑫産総研担当者より、情報セキュリティ対策の履行が不十分であると指摘された場合は、速やかに是正処置を講ずること。
⑬本業務の遂行における情報セキュリティ対策の履行状況を確認するために、産総研が情報セキュリティ監査の実施を必要と判断した場合、受注者は、産総研が定めた実施内容（監査内容、対象範囲、実施者等）に基づく情報セキュリティ監査を受け入れること。
⑭受注者は、産総研の許可なく、本業務の一部又は全部を第三者（再委託先）に請け負わせてはならない。ただし、受注者に求めている情報セキュリティ対策を、再委託先が実施することを再委託先に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を産総研に提供し、承認申請書を提出して、事前に産総研の書面による承認を受けた場合はこの限りではない。
⑮本業務の履行においては、十分な秘密保持を行うこと。
⑯サプライチェーン・リスクに係る情報セキュリティ上の事象が発生した

場合、受注者は原因調査などについて産総研担当者と協議の上、主導的に解決を図ること。

⑰受注者は、受注先及び再委託先において作成した委託事業に係る成果物（システム構成・設定情報、等を含む。産総研に帰属しない著作物を除く。）の納入の完了後速やかに、当該成果物を産総研担当者の許可を得て、抹消すること。また、受注者は、産総研担当者の指示に従い、当該成果物の抹消の確認を受けること。

⑱サプライチェーン・リスクに係る情報セキュリティ上の事象が発生した場合、受注者は原因調査などについて産総研担当者と協議の上、主導的に解決を図ること。

⑲受注者は、受注先及び再委託先において作成した委託事業に係る成果物（システム構成・設定情報、等を含む。産総研に帰属しない著作物を除く。）の納入の完了後速やかに、当該成果物を産総研担当者の許可を得て、抹消すること。また、受注者は、産総研担当者の指示に従い、当該成果物の抹消の確認を受けること。

１３．付帯事項

- 受注者は、調達請求者の求めにより、作業の進捗状況及び作業内容について報告しなければならない。
- 納入されたプログラム等における産総研側の責めによらない納入の完了後１年以内の動作不良等不具合については、その補修、調整等責任をもって無償で速やかに行うこと。
- 本仕様書の技術的内容及び知り得た情報に関しては、守秘義務を負うものとする。
- 本仕様書の技術的内容に関する質問等については、調達請求者と協議すること。
- 本仕様書に定めのないこと項及び疑義が生じた場合は、調達担当者と協議のうえ決定する。

サプライチェーン・リスク対応に係る特記事項

1. サプライチェーン・リスクへの対応

受注者は、機器等の意図的な不正改造及び情報システム又はソフトウェアに不正なプログラムを埋め込むなど、国立研究開発法人産業技術総合研究所（以下、「産総研」という。）の意図しない変更が加えられたときに生じ得る情報の漏えい若しくは破壊又は機能の不正な停止、暴走その他の障害等の情報セキュリティ上のリスク（以下「サプライチェーン・リスク」という。）に対応するため、受注者は「IT 調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ」（平成 30 年 12 月 10 日関係省庁申合せ）に基づく対応を図らねばならない。

2. 意図しない変更に対する対策

①受注者は、本業務の履行に際して、サプライチェーン・リスクが潜在すると知り、又は知り得るべきソースコード、プログラム等（以下「ソースコード等」という。）の埋込み又は組込みその他産総研担当者の意図しない変更を行ってはならない。

②受注者は、本業務の履行に際して、サプライチェーン・リスクが潜在すると知り、又は知り得るべきソースコード等の埋込み又は組込みその他産総研担当者の意図しない変更が行われないように相応の注意をもって管理しなければならない。

③受注者は、本業務の履行に際して、情報の窃取等により研究所の業務を妨害しようとする第三者から不当な影響を受けるおそれのある者が開発、設計又は製作したソースコード等（受注者がその存在を認知し、かつ、サプライチェーン・リスクが潜在すると知り、又は知り得るべきものに限り、主要国において広く普遍的に受け入れられているものを除く。）を直接又は間接に導入し、又は組み込む場合には、これによってサプライチェーン・リスクを有意に増大しないことを調査、試験その他の任意の方法により確認又は判定するものとする。

3. サプライチェーン・リスクにかかる調査の受入れ体制

①受注者は、本業務に産総研担当者の意図しない変更が行われるなど不正が見つかったときは、追跡調査や立入検査等、産総研と連携して原因を調査し、サプライチェーン・リスクを排除するための手順及び体制を整備し、当該手順及び体制を示した書面を産総研担当者に提出しなければならない。

4. サプライチェーン・リスクを低減するための対策

①受注者は、サプライチェーン・リスクを低減する対策として、本業務の設計、構築、運用・保守の各工程における不正行為の有無について定期的または必要に応じて監査を行う体制を整備するとともに、本業務により産総研に納入する納入物品に対して意図しない変更が行われるリスクを回避するための試験を行わなければならない。当該試験の項目は、情報セキュリティ技術の趨勢、対象の情報システムの特性等を踏まえ、受注者において適切に設定するものとする。

②機器の納入であり、かつ、設計、構築、運用・保守の各工程が存在しない場合は、4. ①の対応は不要。

5. 受注者の業務責任者等

①受注者は、本業務の履行に従事する業務責任者及び業務従事者（契約社員、派遣社員等の雇用形態を問わず、本業務の履行に従事する全ての従業員をいう。以下同じ。）を必要最低限の範囲に限るものとする。

②機器納入であり、かつ、設計、構築、運用・保守の各工程が存在しない場合は、5. ①の対応は不要。

6. 再委託

6.1 本業務の第三者への委託の制限

受注者は、産総研の許可なく、本業務の一部又は全部を第三者（再委託先）に請け負わせてはならない。ただし、6.2 に定める事項を遵守する場合はこの限りではない。

6.2 第三者への委託に係る要件

①受注者は、本業務の一部又は全部を第三者に再委託するときは、再委託先の事業者名、住所、再委託対象とする業務の範囲、再委託する必要性について記載した承認申請書を、委託元である産総研に提出し、書面による事前承認を受けなければならない。

②受注者は、本業務の一部又は全部を第三者に再委託するときは、再委託した業務に伴う再委託者の行為について、全ての責任を負わなければならない。

③受注者は、知的財産権、情報セキュリティ（機密保持を含む。）及びガバナンス等に関して、本仕様書が定める受注者の責務を再委託先も負うよう、必要な処置を実施し、その内容について委託元である産総研の承認を得なければならない。

④受注者は、受注者がこの仕様書の定めを遵守するために必要な事項について本仕様書を準用して、再委託者と約定しなければならない。

⑤受注者は、前号に掲げる情報の提供に加えて、再委託先において本委託事業に関わる要員の所属、専門性（情報セキュリティに係る資格・研修実績等）、実績及び国籍についての情報を委託元である産総研へ提出すること。

⑥受注者は、再委託先において、産総研の意図しない変更が加えられないための管理体制について委託元である産総研に報告し、許可又は確認（立入調査）を得ること。

7. その他

①提出された資料等により産総研担当者に報告された内容について、サプライチェーン・リスクが懸念され、これを低減するための措置を講じる必要があると認められる場合に、調達担当者は受注者に是正を求めることがあり、受注者は相当の理由があると認められるときを除きこれに応じなければならない。

②産総研は、受注者の責めに帰すべき事由により、本情報システムに産総研担当者の意図しない変更が行われるなど不正が見つかった場合は、契約条項に定める契約の解除及び違約金の規定を適用し、本業務契約の全部又は一部を解除することができる。

別紙様式（第１０条関係）

年　　月　　日

著作者財産権譲渡証書

国立研究開発法人産業技術総合研究所　殿

請　負　者
住　　所
会　社　名
代　表　者
役職・氏名　　印

ソフトウェア作成請負契約（　　年　　月　　日　契約）
件　名　　楕円曲線に基づく暗号技術の安全性評価プログラムの高速実装作業

上記契約により作成したソフトウェアの所有権及び著作権（著作権法第27条及び第28条に規定する権利を含む）は、ソフトウェア作成請負契約条項第10条第２項の規定により国立研究開発法人産業技術総合研究所に譲渡したことに相違ありません。ただし、上記契約締結前に自己所有していた権利は除くものとします。

別紙様式（第１０条関係）

年　　月　　日

著作者人格権不行使証書

国立研究開発法人産業技術総合研究所　殿

請　負　者
住　　所
会　社　名
代　表　者
役職・氏名　　印

ソフトウェア作成請負契約（　　年　　月　　日　契約）
件　名　　楕円曲線に基づく暗号技術の安全性評価プログラムの高速実装作業

上記契約により作成したソフトウェアの著作権（著作権法第27条及び第28条に規定する権利を含む）に係わる著作者人格権をソフトウェア作成請負契約条項第10条第２項の規定により行使しないことを約束します。

なお、著作者人格権を行使しようとする場合は、国立研究開発法人産業技術総合研究所の承認を得るものとします。