仕　様　書

1.件名:相関乱数生成 ASIC 駆動用ボード設計及び製造作業

2.研究の概要

国立研究開発法人産業技術総合研究所サイバーフィジカルセキュリティ研究部門（以下、「産総研」という。）では、内閣府による戦略的イノベーション創造プログラム（SIP）第３期の課題「先進的量子技術基盤の社会課題への応用促進」において、「プライバシーなどを保護しつつデータ解析ができる秘密計算などの活用に関する研究」（以下、「本研究」という。）を実施している。秘密計算技術は、量子暗号を補完し、セキュアなデータ解析を実現する手段として非常に有用である。しかし、秘密計算の実行には、豊富な計算リソースとネットワーク帯域が必要とされており、それが当該技術の社会展開を阻む一因となっている。そこで、本研究では秘密計算の省リソース化により、この課題を解決することが目的の１つとなっている。産総研では、その手段として、秘密計算実行に必要な乱数生成を専用かつ安全なハードウェア（以下、「相関乱数生成 ASIC」という。）で行うことで、従来必要とされる計算リソースとネットワーク帯域を大幅に低減する計画を進めている。

3.作業の概要

本作業は、相関乱数生成 ASIC 駆動するためのボードを設計及び製造する作業である。ボードにはソケットを実装し、相関乱数生成 ASIC はソケットに設置できるようにすること。本ボードは AMD 製 VPK120 と FMC で接続できるように製造すること。

4.作業の構成

4-1: 相関乱数生成 ASIC 駆動用ボード設計及び製造作業

5.作業構成別仕様

5-1: 相関乱数生成 ASIC 駆動用ボード設計及び製造作業

5-1-1:相関乱数生成 ASIC は Taiwan Semiconductor Manufacturing Company 社製の 65nm プロセス、208pin QFP で製造したものであり、これに対応するソケットをボード上に実装すること。

5-1-2:本ボードは AMD 製 VPK120 の FMC ポートに接続し、FPGA から駆動用信号を送信する予定である。ボード上に対応する FMC コネクタを実装し、ソケットから FMC コネクタまでを適切に配線すること。

5-1-3:FPGA から ASIC へは最大 70MHz のシングルエンド信号を伝送する。少なくとも 50MHz のシングルエンド信号が伝送できるように設計を行うこと。

5-1-4:FMC から ASIC までの伝送が適切に行われるよう、コンデンサなどの部品を適切にボード上に配置すること。また必要があれば電源端子やクロック源をボード上に配置すること。

5-1-5:ボードの納入数は 5 枚とする。

5-1-6:ボード設計に利用したガーバーデータも納入すること。

6.特記事項

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。

7.出荷前検査

受注者は、納入に先立って、自己の標準的な検査項目に準じて出荷前検査を実施し、その結果を性能試験成績書として、本装置の納品時に提出する。

8.納入物品

8-1: 相関乱数生成 ASIC 駆動用ボード　5 枚

8-2: 相関乱数生成 ASIC 駆動用ボード用ガーバーデータ　一式（電子媒体）

8-3: 性能試験成績書　1 部（電子媒体）

※電子媒体は原則としてメール・ファイル転送サービスなどの電子的手段で納入すること。

9.納入場所

〒135-0064 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

サイバーフィジカルセキュリティ研究部門

臨海副都心センター本館 1 階 1110 室

10.納入の完了

本件は「8.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。

11.納入期限

2026 年 3 月 13 日（金）

12.成果の取り扱い

12-1:産総研は、受注者が本契約の履行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。

12-2:受注者は、成果物の著作権（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、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。

12-3: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。

13.セキュリティ要件

13-1: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。

13-2: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。

14.付帯事項

14-1:本仕様書の技術的内容及び知り得た情報については、守秘義務を負うものとする。

14-2: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。また、本仕様書に定めのない事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。

14-3:本業務に起因する不具合等に関しては、原因究明に関し、納入の完了後1年間は無償で対応を行うこと。

14-4:請負者の責において及ぼした損害は、請負者が賠償すること。

別紙

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。