工業技術研究院
Industrial Technology
Research Institute

採購規範書

1. 產品/服務名稱：

   後量子密碼安全晶片整合下線製造先期驗證

2. 目的/用途說明：

   因應「晶片驅動產業創新再升級-後量子密碼應用發展計畫」116 年關鍵績效指標之需求，需進行後量子密碼公版矽智財晶片下線製造前之先期驗證與下線規劃，以確保116年後續後量子密碼安全晶片下線製造能順利進行。

3. 需求說明：

   本案將委託具備 PQC 安全晶片設計之專業廠商合作後量子密碼安全晶片整合下線製造前先期驗證與下線規劃，並進行後量子密碼運算正確性、效能與安全性(如：旁通道攻擊防護)進行下線製造前先期驗證，以確保未來後量子密碼晶片下線驗證能符合預期之效能與後量子資安應用能力。

4. 服務規格：

No.	品項	說明	備註
1	後量子密碼安全晶片SoC下線製造之前的先期驗證規畫	根據工研院所提供之公版矽智財(如：NIST FIPS 203/204/205標準演算法以及HQC演算法等)，進行後量子密碼安全晶片RISC-V SoC 設計與下線製造規畫，為確保符合未來後量子密碼安全晶片，能具備發展後量子資安應用能力，以及確保未來能夠下線製造(Tape out)，須交付專案執行計畫書，含：專案時程、後量子密碼安全晶片RISC-V SoC 架構規劃、驗證指標(正確性、效能、安全性)116年下線規劃(不含下線之執行)CAVP/CMVP送驗規劃(不含送驗之執行)、定期工作會議安排及專案執行簡報。	
2	後量子演算法公版矽智財晶片下線製造之SoC架構先期驗證	根據所規畫之後量子密碼安全晶片RISC-V SoC 架構，進行FPGA驗證，與ASIC模擬驗證數據，提交先期驗證報告書含：FPGA驗證成果，製程規劃(如：40奈米、180奈米等)、EDA工具驗證資料(如：製程、功耗、面積等效能分析)、符合NIST FIPS 203/204/205 標準與HQC演算之功能測試報告、旁通道測試、運算吞吐量評估等，並交付後量子演算法公版矽智財晶片下線先期驗證報告。	

5. 驗收標準：

   (1) NIST CAVP 測試案例驗證，完整支援 NIST FIPS 203/204/205 標準演算法

(2) NIST HQC 範例驗證，支援 HQC 演算法。

(3) 使用 RISC-V 架構作為後量子密碼安全晶片 SoC 中央處理器，除 PQC 以外，至少須含：TRNG、PUF、AES 256、I/O 等元件。

(4) NIST FIPS 203/204 運算吞吐量 100 TPS (Transactions Per Second) 以上。

6. 付款標準：

(1) 第一期款總金額之 40%：廠商須於 115 年 6 月 1 日前，提供專案執行計畫書與簡報（如第 4 點 No.1），作為付款依據。

(2) 第二期款總金額之 60%：廠商須於 115 年 9 月 30 日前，提供後量子演算法公版矽智財晶片下線先期驗證報告（如第 4 點 No.2），作為付款依據。

7. 訓練：□有 ■無

8. 保固：□有 ■無

9. 服務：■有 □無

(1) 廠商需提供即時技術支援。

(2) 若有未詳盡事宜得標廠商得全力配合本院進行補充。

(3) *完工時程若因為不可抗力因素需調整，得經主辦單位同意下進行異動。

10. 廠商交付文件：■有 □無

(1) 專案執行計畫書及簡報

(2) 後量子演算法公版矽智財晶片下線先期驗證報告

11. 其他注意事項

(1) 得標廠商得配合本院做設計變更，得標廠商不得拒絕。

(2) 若有未詳盡事宜得標廠商得全力配合委託方進行補充。

(3) 公共安全需符合委託方之相關規範。

(4) 本案所涉及之智慧財產權歸屬依附件 1 技術合作協議。

(5) 廠商需簽署保密協定（NDA），不得將計畫相關資訊外流。

(6) 委託方應提供符合雙方約定功能、介面、時脈及最低性能需求，且於合理整合至被委託方 SoC 後可達成本案驗收標準之 PQC 硬體模組及 HQC

硬體模組，並提供相關技術文件、測試依據及整合所需資訊。若委託方提供之硬體模組因原始性能不足、規格限制、介面瓶頸或架構限制，致使其於合理整合後仍無法達成本案驗收標準，則本規範書所定之相關驗收標準應由雙方另行協議調整，且不得據此認定被委託方有未履約、遲延履約或驗收未通過之情形。

(7) 委託方應於本案規定之被委託方交付日前至少二個月，提供可供整合驗證之完整 PQC 硬體模組及 HQC 硬體模組，並檢附相關技術文件、測試依據及整合所需資訊，以利被委託方有充足之時間完成 SoC 整合、測試與驗證作業。前述可供整合驗證，係指所提供模組及相關交付內容應具備功能正確性、完整性及可綜合（synthesis）性。若委託方提供之模組或相關交付內容存在錯誤語法、設計描述不完整或其他致使整合、綜合、測試或驗證作業延誤之情形，則因此所生之延誤應為被委託方所可接受，且本規範書所定之驗收時間及相關交付時程應按實際受影響期間合理展延，並由雙方另行協議調整。

工業技術研究院
Industrial Technology Research Institute

附件 1

技術合作協議

甲方：智能資安科技股份有限公司（以下稱「甲方」）
乙方：工研院（以下稱「乙方」）
鑑於：
乙方擁有 **後量子密碼學（Post-Quantum Cryptography, PQC）相關演算法與技術**；
甲方具有 **半導體晶片設計與整合能力**；
雙方同意合作將乙方之 PQC 技術實現於甲方之晶片設計平台中，爰訂立本契約，以資共同遵循。

第一條 契約目的

本契約之目的，在於建立雙方合作架構，以完成乙方之 PQC 技術於甲方所設計之晶片平台中之：

1. 技術整合
2. 硬體實現
3. 測試與驗證
4. 原型晶片或相關技術成果之開發

甲方於本契約下主要提供晶片設計、技術整合與驗證服務；乙方提供 PQC 演算法及相關技術資料。

第二條 定義

除本契約另有約定外，本契約名詞定義如下：

一、背景智慧財產權（Background Intellectual Property）

指任一方於本契約簽訂前即已擁有、控制或依法取得授權之所有智慧財產權，包括但不限於：

- 專利
- 著作權
- 營業秘密
- 技術文件
- 演算法
- 軟體
- 硬體設計
- 晶片架構

- RTL 程式碼
- EDA 設計流程

二、合作成果（Foreground Intellectual Property）

指雙方於本契約履行過程中所共同或單獨開發完成之技術成果。

三、晶片設計技術

指與半導體晶片設計相關之技術，包括但不限於：

- IC architecture
- RTL design
- layout design
- design flow
- verification environment
- tape-out preparation
- GDSII design data

第三條 合作範圍

雙方同意依本契約進行技術合作，其主要內容包括：

一、乙方提供 PQC 演算法及相關技術文件。

二、甲方依乙方提供之技術規格，進行晶片設計與硬體實現。

三、甲方協助進行設計整合、模擬、驗證及效能測試。

四、雙方共同進行技術驗證及成果評估。

第四條 背景智慧財產權

一、任一方於本契約簽訂前所擁有之背景智慧財產權，仍屬該方所有。

二、本契約之簽署或履行，不得解釋為任何一方將其背景智慧財產權移轉予另一方。

三、為達成本契約目的，雙方僅授予對方：

非專屬、不可轉讓、不可再授權、僅限本契約目的範圍內之使用權。

四、除本契約明示授權外，任何一方均不得主張取得對方背景智慧財產權之任何權利。

第五條 乙方 PQC 技術之權利

一、乙方所提供之 PQC 演算法、密碼學技術、數學模型、軟體實作、技術文件及其衍生技術，均屬乙方之智慧財產權。

二、甲方僅得於本契約目的範圍內使用前述技術，包括：

1. 晶片整合
2. 硬體實現

3. 測試與驗證

三、未經乙方書面同意，甲方不得：

1. 就該等技術申請專利
2. 對外授權或轉授權
3. 用於本契約以外之商業用途。

第六條 甲方晶片設計技術之權利

一、甲方於本契約履行過程中所使用或開發之晶片設計技術，包括但不限於：

- IC architecture
- RTL 程式碼
- layout 設計
- 設計流程
- 驗證系統
- EDA script

均屬甲方之智慧財產權。

二、乙方不得對前述技術：

1. 進行複製
2. 進行逆向工程
3. 提供予第三方使用

除非取得甲方書面同意。

第七條 合作成果之權利歸屬

一、合作成果若主要源自乙方 PQC 技術，其智慧財產權歸屬乙方所有。

二、合作成果若主要涉及晶片設計或硬體實現技術，其智慧財產權歸屬甲方所有。

三、若合作成果係由雙方共同完成且無法合理區分貢獻，則該成果之智慧財產權由雙方共有。

四、共有智慧財產權之商業利用，須經雙方書面同意。

第八條 Tape-out 與晶圓製造

一、晶片設計過程所產生之 GDSII 檔案、layout database、mask data 等資料，均屬甲方之機密資訊。

二、乙方不得自行或委託第三方：

1. 進行 tape-out

2. 提交晶圓廠製造

3. 使用前述資料製造晶片

除非經甲方書面同意。

第九條 Mask Work 保護

晶片之 layout 設計及 mask work 受相關智慧財產權法規保護。

未經權利人書面同意，任何一方不得複製、再製或利用該等設計於其他晶片產品。

第十條 逆向工程禁止

任一方不得對另一方提供之技術、晶片或相關成果進行：

1. 逆向工程

2. 反編譯

3. 結構分析

以取得該技術之核心資訊。

第十一條 無默示授權

除本契約明示授權外，本契約之任何內容均不得解釋為授予另一方任何默示授權（Implied License）。

第十二條 技術託管（Technology Escrow）

若甲方因破產、解散或其他原因無法繼續履行本契約之技術支援義務，雙方得同意將必要之技術文件交由第三方 escrow 機構保管。

在特定條件發生時，乙方得依 escrow 協議取得該等必要技術資料，以維持系統之基本運作。

第十三條 出口管制

雙方同意遵守適用之出口管制法規及加密技術相關法律。

任何涉及 PQC 或加密技術之跨境技術轉移，均須依相關法律規定辦理。

第十四條 政府研究成果權利條款

若乙方技術涉及政府資助之研究成果，乙方應確保：

1. 不影響甲方之晶片設計智慧財產權。

2. 不得主張對整體晶片產品之權利。

第十五條 技術移轉法遵循條款

若乙方之技術屬於政府研發成果，相關技術授權或移轉應符合：

科技基本法及相關技術移轉法規。

但該等規定不得影響甲方既有智慧財產權。

第十六條 研究成果發表條款

乙方得就本合作研究成果進行學術發表。

但發表前應提前 至少 60 日通知甲方。
甲方得要求刪除涉及：

- 營業秘密
- 晶片設計技術
- 商業機密

之內容。
第十七條 政府資金介入條款
若本合作計畫涉及政府補助或研究計畫資金：
雙方應遵守相關計畫管理規定。
但該等規定不得影響甲方對其晶片設計技術之權利。

第十八條 商品化優先授權條款
若合作成果具商業化價值：
乙方應優先與甲方協商授權條件。
甲方得於合理期間內取得優先授權權利。
第十九條 保密義務
雙方對於因本契約所取得之技術資料、設計文件、測試結果及其他機密資訊，均負保密義務。
本保密義務於本契約終止後仍持續有效五年至十年。
第二十條 商業化授權
若未來合作成果進入商業化階段，雙方得另行簽訂授權契約，以規範：

1. 晶片量產
2. PQC 技術授權
3. 權利金或分潤機制。

第二十一條 準據法與爭議解決
本契約以中華民國法律為準據法。
因本契約所生之爭議，雙方同意以**台灣新竹地方法院為管轄法院**。