<table>
<tr><td>RFP관리번호</td><td colspan="2">2025-융합-품목공모-2</td><td>공모유형</td><td colspan="3">품목공모형</td></tr>
<tr><td>해당여부</td><td colspan="5">■ 국가전략기술 □ 탄소중립 □ 글로벌 R&D □ 미래소재 □ 전략연구사업(MVP)(예정) □ 국방전략기술(예정)</td></tr>
<tr><td>국책연구기획
평가전문분야1</td><td>PM분야</td><td>정보·융합기술</td><td>RB분야</td><td>보안</td><td>RB세부분야</td><td>전 분야</td></tr>
<tr><td>사업명</td><td colspan="5">첨단융합기술개발사업 - 미래개척융합과학기술개발 - 미래유망융합기술파이오니어(도전형)</td></tr>
<tr><td>RFP명</td><td colspan="5">IoT 환경에 실제 적용이 가능한 하이브리드 PUF 보안기술 구현
(TRL : [시작] 2단계 ~ [종료] 5단계)</td></tr>
<tr><td rowspan="2">RFP유형코드</td><td>사업목적·내용</td><td>성과물 특성</td><td></td><td>지원대상</td><td rowspan="2">보안과제
분류</td><td rowspan="2">일반</td></tr>
<tr><td>R</td><td>1</td><td>-</td><td>1</td></tr>
</table>

1. 추진배경

□ 문제정의 및 배경

○ 사물인터넷(IoT) 시대의 도래와 함께 초연결 사회에서 네트워크와 디바이스를 대상으로 한 해킹 문제가 점차 심각해지고 있음. 특히, 스마트폰, 보안 카메라, IoT 통신 장비와 같은 소규모 기기들이 생성한 데이터를 네트워크 연결을 통해 전달하는 과정에서 위변조 된다면 비정상적인 정보 생성, 개인정보 유출을 넘어 개인의 생명과 직결된 위험을 초래할 수도 있음. 따라서, IoT 기기에 대한 인증 및 이를 활용한 보안 프로토콜의 활용이 필수적이나, 저비용의 경량 하드웨어를 탑재하는 IoT 기기의 특성상 해킹에 강인한 보안 기술을 적용하기 매우 어려움

○ IoT 기기에 대한 안전한 키 생성, 경량 인증 및 보안 프로토콜 등에 관해 많은 연구가 이루어지고 있지만, 소프트웨어 기반 기술은 해킹을 통한 복제 혹은 유출의 위험성을 가지고 있으며, TPM (Trusted Platform Module) 등 하드웨어 기반 방식은 비용이 높고 경량 IoT 기기에 적합하지 않아 적용되지 않는 경우가 일반적임. 앞으로 양자컴퓨팅 시대가 열린 후 양자내성암호가 널리 활용된다고 하더라도, 여전히 비밀키 자체를 복제하거나 유출할 수 있다면 해킹 문제로부터 자유로울 수 없음

○ 이와 관련하여 하드웨어 방식의 보안 기술인 물리적 복제 방지 기능(Physical Unclonable Function: PUF)에 관한 연구가 활발히 진행되고 있음. PUF는 제조 공정에서 발생하는 미세한 물리적 변동성을 활용하여 복제 불가능한 고유한 보안키를 생성하는 특징을 가지고 있음

○ 또한, PUF는 비밀키를 생성하거나 인증을 할 때 사용하는 일부 응답 데이터나 공개 데이터들을 안전하게 저장해야 하는 요구사항이 있지만 비밀키를 별도로 저장하지 않고 실시간으로 생성하므로 데이터베이스에서 키가 유출되는 공격에 일반적으로 강함. PUF는 추가적인 전력 소비가 거의 없고 소형화된 기기에서도 쉽게 구현 가능하다는 장점으로 인해, IoT 디바이스와 같은 저전력 환경에서도 유리한 보안 솔루션으로 평가받고 있음

○ PUF 관련 연구들은 각각의 방식과 관점에서 중요한 진전을 이루고 있지만, 여전히 단점과 한계가 존재함. 재료적 관점에서는 Optical PUF가 물리적 불규칙성을 활용해 예측 불가능성을 높임으로써 암호키의 엔트로피를 높일 수 있으며 비선형성 특성으로 AI 모델링 공격에 강한 저항성을 제공할 수지만, 환경적 요인에 민감할 수 있어 Optical PUF의 응답 값을 변동시켜 일관된 키를 생성하는 것이 어려울 수 있어 실시간 인증 및 키 생성에 관한 알고리즘 등의 문제가 있음. 반면 전기/전자적 관점에서는 Electrical/Electronic PUF는 전자 소자의 불규칙성을 이용해 효율적인 보안을 제공하지만, AI 기술을 활용한 키 예측 가능성과 엔트로피 소스의 부족이 주요한 약점으로 작용함. 정보/통신적 관점에서는 네트워크를 통한 키 관리와 전송 과정에서의 보안 위협이 문제로 제기되며, 이를 해결하기 위한 새로운 프로토콜 설계와 알고리즘적 보완이 필요함

○ 따라서, 각 기술의 단점을 보완하고 장점을 극대화하기 위해 재료적, 전기/전자적, 정보/통신적 접근 방식이 융합시킴으로써 단일 PUF 방식에 비해 보안성이 우수하고, 암호키의 엔트로피를 증가시키며 AI 모델링 공격에 강건한 하이브리드 PUF 개발이 필요함. 또한, 하이브리드 PUF를 기반으로 IoT 환경에서 활용될 수 있는 통합 보안 솔루션을 개발한다면 단일 PUF의 한계점을 극복할 뿐만 아니라, 양자컴퓨팅 시대에서도 상당 수준의 보안을 제공할 수 있는 기반을 마련할 수 있을 것으로 기대됨

□ 기획 주안점

○ IoT 환경에서도 사람의 생체 특징(지문, 홍채 등)과 같이 사물로부터 나온 물리적 특징을 추출하여 사물인증이 가능하도록 하는 기술 연구 필요

○ 기존 키 관리 방식의 한계(소프트웨어 방식: 키 유출・복제 등의 위험, 하드웨어 방식: 고비용, IoT 적용의 한계)를 극복한 저비용・고보안성 하드웨어 기반 암호키 기술 연구

○ 하드웨어 기반 하이브리드 PUF 보안소자 설계와 제작 및 이를 활용한 보안 프로토콜의 적용을 아우르는 융합적 연구가 기획되어야 함

2. 연구개발목표	

□ 최종목표

○ **소프트웨어 보안방식의 한계를 넘어, AI 모델링 공격에 강건한 하드웨어 방식의 하이브리드 PUF 보안 소자와 IoT 환경을 위한 보안 기술 개발 및 실증**

□ **세부목표**

ㅇ Optical PUF와 Electrical/Electronic PUF를 융합한 하이브리드 PUF 설계 및 개발

ㅇ 하이브리드 PUF 기반 사물지문 생성 및 인증 기술 개발

ㅇ IoT 환경에서 사물지문 기반 가상 HSM (Hardware Security Module) 구현 및 응용 개발・실증

3. 연구개발내용 및 성과목표	

□ **연구내용 및 범위**

ㅇ Optical PUF와 Electrical/Electronic PUF를 융합한 하이브리드 PUF 설계 및 개발

- AI 모델링 공격 및 물리적인 공격, 환경 등에 대한 내성을 가지는 광학적 소자 개발
- 광학 및 전자적 불규칙성을 함께 제공함으로써 암호키의 엔트로피를 증대시킬 수 있는 하이브리드 PUF 설계 및 개발

ㅇ 하이브리드 PUF 기반 사물지문* 생성 및 인증 기술 개발

* 사물지문(Things Fingerprint): 광매질이 부착된 사물의 고유 패턴을 기반으로 생성된 유일한 값

- Optical 및 Electrical/Electronic PUF 융합을 통한 고보안성* 사물지문 생성 및 오류완화 메커니즘

* 고보안성: AI 분석에 강인한 CRP(Challenge-Response Pair)를 생성하는 Strong PUF을 의미함

- 사물지문기반 사물인증용 암호키 생성* 및 인증 메커니즘 개발

* 암호키 생성: 하이브리드 PUF가 IoT 환경의 통합 보안 솔루션에 기본 요소로 활용될 수 있도록 하이브리드 PUF의 광학적 성질과 전자적 성질을 융합하여 암호키 생성

ㅇ IoT 환경에서 사물지문 기반 가상 HSM (Hardware Security Module) 구현 및 응용 개발・실증

- 사물지문 기반 가상 HSM* 기능 및 API 개발

* 사물지문 기반 가상 HSM: 사물지문을 활용하여 일반적인 HSM 기능을 소프트웨어로 제공하는 소프트웨어 모듈을 의미하며, 해당 모듈은 사물지문을 기반으로 PQC 개인키가 노출되지 않도록 저장하는 등 다양한 HSM 기능 및 이를 활용할 수 있는 API를 제공할 수 있어야 함

- 가상 HSM 적용 IoT 응용(예. 자동차/의료 등) 시나리오 제안 설계 및 실증

※ 제안자는 가상 HSM을 활용하여, 키유출 공격에 강인함을 요구하는 IoT 기반 응용 시나리오 및 기능·성능 목표를 제안하고 제안하는 응용 시나리오가 포함된 IoT 실증 환경 구축 후 보안 기능·성능 검증

□ **정량적 목표**

○ 하이브리드 PUF의 성능 평가를 위해서 Strong PUF 성능 평가에 활용되는 지표(유일성, 신뢰성, 비트-앨리어싱, 엔트로피, CRP 크기, 응답 시간, 전력 소비, AI 모델링 공격에 대한 저항성)들과 하드웨어 보안 소자의 구동 조건, Hamming distance, NIST test 결과 등을 포함하여 제안자가 도전적으로 제시

○ 가상 HSM이 가져야 하는 기능 및 성능에 대한 정량적 목표는 제안자가 제안하는 IoT 응용의 특성 및 기기 환경을 고려하여 도전적으로 제시하여 결정하되, 다음 항목을 선택적으로 포함할 것을 권장 (비밀키/공개키쌍 생성 시간, 저장된 비밀키/개인키 복구 시간, 대칭키 암호화 속도, 전자서명 속도, 전력 소비량, 메모리 사용량 등)

○ 제안된 하이브리드 PUF, 사물 지문 등의 우수성을 국제적으로 입증할 수 있는 최상급 국제 저명저널 및 국제 최우수 학술대회에 논문 10편 이상 게재 및 국제 특허 4건 이상 등록

□ **정성적 목표**

○ 연구성과 홍보, 확산 및 교류를 위한 산·학·연 국제 워크샵 개최

○ 국제 전시회 참여하여 성과 전시 및 홍보

○ 자체평가를 위한 자문회의 개최(연 1회 이상)

4. 지원기간/예산/추진체계

○ **기간** : 2025.4. ~ 2030.12. (5년 9개월)

○ **정부지원연구개발비** : 47억원 내외

구 분		연구 기간	연구비(단위과제당)
1단계 (21개월)	1년차(2025년)	'25.4.~'25.12.	3억원 내외
	2년차(2026년)	'26.1.~'26.12.	4억원 내외
2단계 (24개월)	3년차(2027년)	'27.1.~'27.12.	8억원 내외
	4년차(2028년)	'28.1.~'28.12.	8억원 내외
3단계 (24개월)	5년차(2029년)	'29.1.~'29.12.	12억원 내외
	6년차(2030년)	'30.1.~'30.12.	12억원 내외

※ 경쟁형 과제로 1단계 평가 후 2단계 진입 시 50% 내외 과제만 지원(단계평가 결과에 따라 연구비 조정 가능)

※ 연차별 연구비 규모 및 연구기간은 정부예산, 주제 발굴 및 기획 상황 등에 따라 변동 가능

○ **과제형태** : (일반)연구개발과제

5. 특기사항	

□ **과제 특성**

ㅇ 기존 연구에서 풀지 못했거나 시도하지 못했던 과학난제를 새로운 초융합을 통해 돌파하여(Breakthrough), 세계 최초로 시도하는 연구를 지향

□ **연구진 구성**

ㅇ 과학난제 해결의 실마리가 될 수 있는 개념 증명(PoC)을 위해 공동 밀착연구가 가능한 이종 이상 분야 융합을 권고

□ **필수 사항**

ㅇ 연구주제와 관련된 세계 선도적 연구기반(예시: 글로벌 최고 수준의 대표 참고문헌 자료 등)을 구체적으로 제시

- 난제 정의 및 도전목표를 제시하고 개념 증명을 실현하기 위한 과정 또는 방법론에 대해 구체적으로 기술하며 사업 기간 내 해결 가능한 수준을 제안
- 현재 수준 대비 차별성/도전성(세계 최초, 유일, 최고 등 수준 포함) 제시 및 관련 근거(문헌분석, 기술/연구 동향 분석 등) 제출

□ **기타 사항**

ㅇ 연구자가 제안한 정량적 목표는 과제 평가시 적합성 검토 후 조정 가능