2026.11.09.

KiRi 리포트

금융권의 양자내성암호 전환 과제

| 글로벌 이슈 |

임준수 연구원

요 약

공개키 암호를 해독할 수 있는 양자컴퓨터의 등장에 대비해, 금융권은 양자컴퓨터로도 해독하기 어려운 양자내성암호로의 전환을 준비하고 있음. 결제 및 인증 분야에서는 적용 시험과 도입이 진행되고 있으며, 해외 일부 보험회사에서는 관련 암호 관리방침을 정비하고 있음. 다만 양자내성암호로의 전환은 처리속도와 기존 시스템에 영향을 줄 수 있으므로 충분한 시험을 거쳐 단계적으로 추진할 필요가 있음

○ 양자컴퓨터가 발전하면 현재 금융거래에 사용되는 공개키[1] 암호가 해독될 가능성이 있어, 금융권에서는 양자내성암호로의 전환 준비가 중요해지고 있음

- 양자컴퓨터는 이미 클라우드를 통해 유료로 이용할 수 있으나 기존 공개키 암호를 해독할 수준에는 이르지 못했으며, 암호방식 전환에는 여러 해가 걸릴 수 있어 사전 준비가 필요함

○ 양자내성암호(Post-Quantum Cryptography; PQC)는 양자컴퓨터로도 해독하기 어렵도록 설계한 암호방식으로, 기존 컴퓨터 환경에서도 구현할 수 있음[2]

- 미국 국립표준기술연구소(NIST)는 2024년 양자내성암호 3종을 표준으로 확정하여, 보안업체와 금융회사가 제품 개발과 도입에 활용할 공통 기준을 마련함[3]

○ 양자컴퓨터를 이용한 암호 해독 위험은 개인정보 보호와 결제·인증의 신뢰에 영향을 미칠 수 있음[4]

- 공격자는 지금 암호화된 정보와 암호키 교환 기록을 빼돌려 보관해두었다가 나중에 키 공유에 쓰인 공개키 암호를 해독하는 방식으로 공격이 가능하며, 이를 '선 수집, 후 해독(Harvest Now, Decrypt Later)'이라고 함
- 건강정보 등 오랫동안 민감성이 유지되는 정보는 탈취 당시 암호화되어 있더라도 미래 해독 시점에 정보가 노출될 수 있어, 장기 고객정보를 취급하는 보험회사와 관련성이 큼
- 결제·인증에서는 전자서명으로 거래 메시지의 발신자와 변조 여부를 확인하므로, 공개키 암호의 취약성은 정보의 비밀 유지와 함께 금융거래의 신뢰성에도 영향을 미칠 수 있음

○ 금융권은 전자서명을 통해 거래 메시지의 발신자와 변조 여부를 확인하고 있어, 공개키 암호가 해독되면 결제·인증의 신뢰성이 훼손될 수 있으므로, 결제·인증과 정보 전송 분야에서 양자내성암호를 적용 가능성을 검증하기 위한 시험과 도입이 진행되고 있음

1) 다른 사람에게 알려도 되는 공개키와 자신만 보관하는 개인키를 한 쌍으로 사용하는 방식. RSA, ECC 등이 있음
2) NIST(2026. 2. 27.), "What Is Post-Quantum Cryptography?"
3) NIST(2024. 8. 13.), "NIST Releases First 3 Finalized Post-Quantum Encryption Standards"
4) BIS(2025. 12. 11.), "Project Leap Phase 2: Quantum-proofing Payment Systems", p. 6

- 국제결제은행(BIS)은 이탈리아·프랑스·독일 중앙은행, 네트워크 서비스 제공업체인 Swift·Nexi-Colt와 함께 유로시스템 거액결제시스템(T2)의 상용망과 분리된 환경에서 양자내성암호를 시험 적용함[5)]
- 시험에서 올바른 서명 확인과 잘못된 서명 차단, 서로 다른 암호 프로그램 간 호환에는 문제가 없었으나, 서명 검증시간은 0.0281초에서 0.2099초로 늘어나 약 7.5배를 기록함
- 다만, 측정 범위가 서명 검증 단계에 한정되고 암호키를 관리하는 실제 보안장비(HSM)의 영향도 반영되지 않았으므로, 실제 운영환경에서 발생하는 처리 지연은 별도로 확인할 필요가 있음
- 국내에서는 케이스마텍·금융결제원·블록에스가 3자 업무협약을 맺고 공동인증서를 이용한 본인 확인과 전자서명에 양자내성암호를 적용할 수 있는지 검증하기로 함[6)]
- 토스페이먼츠는 2026년 4월 결제창과 고객용 웹서비스 정보 전송에 양자내성암호를 도입함[7)]

○ **보험권에서는 건강정보 등 민감정보를 보호하기 위한 암호 관리방침과 고객정보를 처리하는 외부업체의 보안요건에 양자내성암호 적용을 추진하고 있음**

- 일본 메이지야스다생명은 건강정보 등 민감정보를 많이 취급한다는 점을 들어 2026년 3월 '안전한 암호의 이용·관리 방침'을 공개하고, 양자내성암호 등 안전한 암호로 이행한다는 방침을 제시함[8)]
- 미국 퍼시픽라이프(Pacific Life)는 자사 데이터를 취급하는 외부업체와 하도급사에 양자내성암호 채택 등 새로운 위험에 따른 암호 통제의 적시 갱신을 요구하여 위탁업체의 대응을 조달·관리 요건에 반영함[9)]

○ **금융권의 양자내성암호 전환은 처리 속도와 기존 시스템의 작동에 영향을 미칠 수 있으므로, 실제 업무환경을 반영한 충분한 시험을 거쳐 단계적으로 추진할 필요가 있음**

- BIS 시험에서는 새 암호가 작동하도록 여러 프로그램을 수정해야 했으며, 필요한 보안제품을 공급업체가 제공하는 시점도 금융회사의 전환 일정에 영향을 줄 수 있는 것으로 나타남
- 보험회사는 고객정보의 보호기간과 암호 사용현황을 점검하고, 계약 관리·보험금 지급 등 핵심 업무의 연속성을 고려한 전환계획을 마련할 필요가 있음
- G7 사이버전문가그룹은 가장 중요한 시스템은 2030~2032년, 전체는 2035년을 전환 참고 시점으로 제시했으며, 암호 사용현황을 파악하고 위험 노출도와 시스템의 중요도, 전환의 복잡성, 업무 중단 시 영향을 고려해 전환 순서를 정하도록 제안함[10)]
- NIST는 향후 추가적인 암호 교체에 대비해 보안과 업무 운영을 유지하면서 암호방식을 바꿀 수 있는 '암호 민첩성'[11)]을 시스템 전반에 반영하도록 권고함

---

5) BIS(2025. 12. 11.), "Project Leap Phase 2: Quantum-proofing Payment Systems", p. 21
6) 전자신문(2026. 7. 10.) "케이스마텍·금융결제원·블록에스, 공동인증서 환경에 양자내성암호(PQC) 적용 검증 나선다"
7) 토스페이먼츠(2026. 4. 3.), "토스페이먼츠, 국내 금융·IT 업계 최초 '양자내성암호' 전면 도입"
8) 메이지야스다생명(2026. 3. 11.), 「安全な暗号の利用・管理方針」の公表について
9) Pacific Life(2026. 5. 20.), "Third-Party Minimum Control Requirements", Encryption
10) G7 Cyber Expert Group(2026. 1. 12.), "Advancing a Coordinated Roadmap for the Transition to Post-Quantum Cryptography in the Financial Sector"
11) 보안을 유지하고 업무 중단을 최소화하면서, 사용 중인 암호방식을 다른 방식으로 교체할 수 있는 능력임