미래 대비

Quantum-Safe 보안을 향한 여정

Vanguard 보고서

2022년 4월

의뢰:

IBM

451 Research

S&P Global
Market Intelligence

작성자 소개

John Abbott

4SIGHT 수석 연구 분석가

S&P Global Market Intelligence의 한 부서인 451 Research를 위한 시스템, 스토리지, 소프트웨어 인프라 주제를 다룹니다. 30년 이상의 경력을 쌓아온 베테랑으로 Unix, 슈퍼컴퓨팅, 시스템 아키텍처, 소프트웨어 개발, 스토리지와 같은 분야에서 전문 기술 분야를 개척해 왔습니다.

1999년 10월, 451 Group의 공동 설립자 중 한 사람으로, 샌프란시스코 지점에서 분석 업무를 담당했습니다. 스토리지 가상화와 블레이드 서버에 대한 보고서를 포함해 451 Research의 수많은 특별 보고서를 작성했으며, 이 두 주제 중 하나에 관한 최초의 종합 설문조사가 발표된 바 있습니다. 최근에는 융합 인프라, 새 시스템 아키텍처, AI, 딥 러닝 가속기와 같은 주제를 주로 다뤄왔습니다. 신기술의 미래 지향적이고 장기적인 적용을 위해 451 Research 프레임워크인 4SIGHT 구축에도 참여했습니다.

기술 관련 보고서 작성자로서의 이력과 메인프레임, 초기 PC 및 Unix 워크스테이션을 사용한 직접적인 참여를 기반으로 1984년부터 기술 분야를 다루기 시작했습니다. 프리랜스 저널리스트로서 Computing, Computer Weekly, Financial Times, The Times 등에 기고했습니다. 1987년 ComputerWire의 주간 Unix 뉴스레터인 Unigram.X의 편집자로 임명되었으며, 그후 처음에는 런던에서, 이후에는 샌프란시스코에서 이 회사의 일간 Computergram International 서비스의 편집자 직을 역임했습니다. 샌프란시스코에 451 Research 지사를 세우고 10년 넘게 거주해 오고 있습니다.

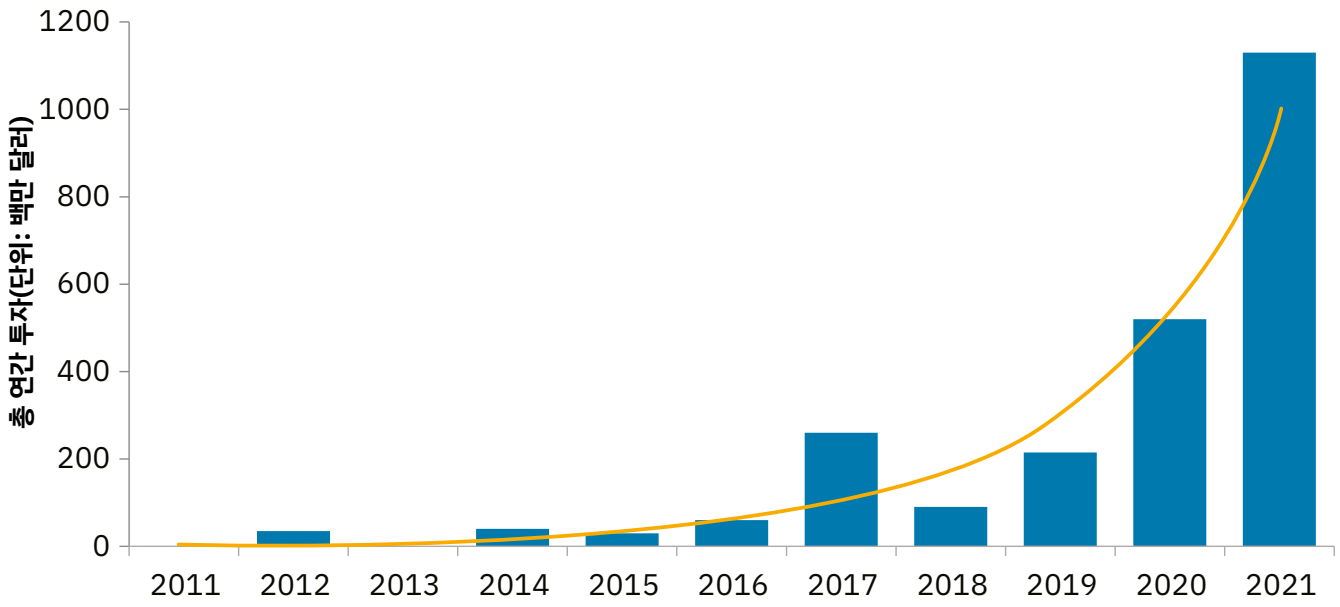
Keele 대학에서 음악을 전공하고 런던 대학교에서 현대 영문학 석사 학위를 받았습니다.

소개

오늘날의 양자 컴퓨팅이란 고위험, 고수익 투자라고 말할 수 있습니다. 우리 생에 동안 보편적이고 실용적인 양자 컴퓨터가 실현될 수 있다는 보장은 없습니다. 그러나 수 많은 연구소와 기술 부문의 점점 더 많은 민간 기업이 매일매일 어려움을 극복하면서 첨단 과학을 끊임 없이 발전시키고 있습니다. 그리고 기존 슈퍼컴퓨터의 능력으로 처리할 수 없는 문제를 해결해 내는 엄청난 결과를 가져올 수도 있습니다. 따라서 판매자와 사용자 모두가 변혁적일 수 있는 기술을 활용할 수 있는 기회를 잡을 수 있습니다. 자료 1에 표시된 S&P Capital IP Pro의 데이터에 따르면, 양자 스타트업 기업들은 지난 10년 동안 24억 달러의 투자를 받았습니다. 2021년은 양자 기업에 대해 11억 달러의 투자가 몰리면서 관심사가 집중된 한 해였습니다. 하지만 이 데이터는 IBM, Amazon, Google, Honeywell을 포함한 기존 IT 회사들에 의한 막대한 투자는 포함되지 않은 것입니다.

이 분야는 기회와 함께 몇 가지 주요 우려 사항이 있는데, 아마도 가장 중요한 문제는 오늘날의 보안 관행에 대한 위협일 것입니다. 양자 컴퓨터를 사용하는 악성 공격자는 디지털 서명을 위조하고 현재 전 세계 IT 시스템에 깊숙이 숨겨져 있는 공용 키 인프라를 포함하여 현 수준의 암호기법과 암호화를 해독할 수 있습니다. 더욱 우려되는 것은, 실제 양자 컴퓨팅이 등장하면 현재 보호되고 있는 암호화된 데이터라도 저장해 놓고 나중에 복호화할 수 있다는 점입니다. 이는 더 이상 지체할 수 없는 시급한 문제입니다. 하루 빨리 대처하지 않으면 더 많은 데이터가 위험에 처할 것입니다.

자료 1: 양자 컴퓨팅 스타트업 기업 투자



출처: S&P Capital IQ Pro

451 테이크

Shor의 알고리즘을 효과적으로 실행할 수 있는 양자 컴퓨터가 언제쯤이면 널리 보급되어 악의적인 공격자가 액세스할 수 있을지에 대해서는 정확히 예측할 수 없습니다. 지금까지 어떤 IT 공급업체도 양자 컴퓨팅이 기존 컴퓨터를 상당 수준 능가할 지에 대해 명확한 시기를 제시하지 않았습니다. 그러나 지난 5년 동안의 급속한 기술 발전과 현재 진행 중인 상당한 투자를 고려해 보면 그 날은 아마도 2020년대 말 쯤이 될 것입니다. 그렇게 되면 현재 공용 키 알고리즘으로 보호되는 모든 정보가 노출될 위험이 있습니다. 국가 방위와 정보 기관, 고객이 규제 대상 산업에 속한 클라우드 서비스 제공업체와 시스템 공급업체의 경우 그 위험은 무시할 수 없을 정도로 이미 심각해졌습니다. 1999년에서 2000년으로 연도가 바뀌면서 널리 사용되는 컴퓨터 프로그래밍 단축키가 혼란을 일으킬 것이라고 위협한 Y2K를 되돌아 보십시오. 이처럼 과거의 잘못된 경고와 미래에 대한 불투명성에도 불구하고 한 가지는 분명합니다. 오늘날 사이버 공격의 위험은 막대한 문제이며 위협과 취약성의 본질은 끊임없이 진화하고 있습니다. 보안 정책은 지속적으로 검토하고 업데이트해야 하며 암호화 민첩성 및 암호화 인벤토리의 구현과 함께 Quantum-safe 암호화 기술은 이제 현실적으로 중요한 부분입니다.

Quantum-Resistant 및 Quantum-Safe 시나리오

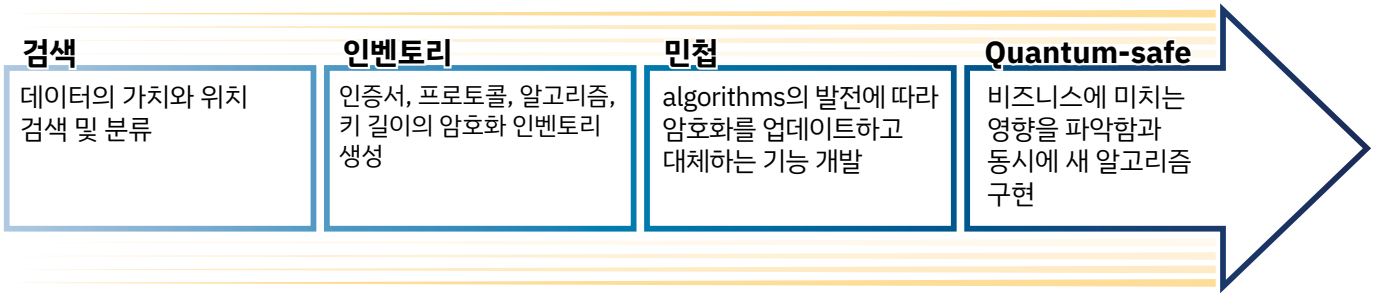
문제: 널리 사용되고 있는 현 세대의 보안 알고리즘은 난해한 수학적 문제를 기반으로 하므로 기존 컴퓨터로는 파헤치기가 매우 어렵습니다. 그러나 이러한 문제는 충분한 능력 갖춘 양자 컴퓨터로 쉽게 해결할 수 있습니다. 이 전제는 미국 수학자 Peter Shor가 현재 Shor의 알고리즘이라고 알려진 다항 시간 알고리즘을 발견한 1994년 이후 널리 받아들여져 왔습니다. 최초의 양자 컴퓨터는 그 후 3년 뒤에 제작되었고, Quantum-safe 알고리즘의 개발은 지난 10년 동안 꾸준히 진행되었습니다. 그러나 오늘날 정부 기관과 산업 전반에서 널리 사용되는 공용 키 암호화 시스템에서 새 알고리즘 세트로 전환하는 것은 수십 년이 걸릴 수 있습니다.

그렇기 때문에 미국 국립표준기술연구소(NIST) 및 국토안보부(DHS)와 같은 조직에서는 알고리즘 자체에 대한 표준화 프로세스와 기업이 양자 후 암호화로 전환을 준비하는 데 도움이 되는 권장사항을 마련하고 있습니다. 이 작업에 따라 지난 1월 국가 방위와 정보 서비스의 전환을 시작하도록 명령하는 백악관 각서가 작성되었습니다.

오늘날 시중에 나와 있는 가장 강력한 컴퓨터에서 (소인수를 찾아서) 2,024비트 합성수를 해독하려면 수백만 년이 걸립니다. 양자 컴퓨터에서는 이론적으로 몇 시간이면 끝낼 수 있습니다. Shor의 알고리즘에 의해 깨진 현재 공용 키 체계에는 현재 45년이 되었지만 여전히 거의 모든 인터넷 기반 거래에 사용되는 유서 깊은 RSA 알고리즘과 데이터 보안 표준, Paillier 암호 시스템, 타원 곡선 디지털 서명 알고리즘, 타원 곡선 Diffie-Hellman 및 ElGamal 암호화가 포함됩니다. NIST, ISO/IEC, ETSI, IETF에서 제정한 수 많은 표준이 영향을 받게 되어 전 세계적인 문제가 될 것입니다. 중국 SM2 디지털 서명 알고리즘과 SM9 국가 암호화 표준도 깨졌습니다.

제안 요청에 따라 2016년에 시작된 NIST 표준 프로세스를 통해 새 Quantum-resistant(양자 저항) 후보 세트가 식별되었습니다. 격자, 다변수, 해시 또는 코드 기반 암호화와 같은 다양한 접근 방식으로 분류되는 이 프로세스에는 격자 기반 CRYSTALS-Kyber 키 캡슐화 메커니즘(KEM), McEliece(코드 기반 KEM), Falcon(격자 기반), Rainbow(다변수) 양자 후 서명 체계가 포함됩니다. 이러한 체계와 여타 및 최종 후보들은 현재 완료된 3라운드 경쟁을 마치고 초안 표준화 과정을 거치고 있습니다. 대체 알고리즘과 추가 서명 체계에 대한 요청을 포함한 4라운드가 올해 시작되어 2024년 말 완료될 예정입니다.

자료 2: Quantum-Safe를 향한 성숙도 단계



출처: 451 연구

Quantum-Safe 암호화로 가는 길

조직은 향후 10년 동안 자사의 정보 보안 아키텍처에 Quantum-safe 암호화를 통합하기 위해 지금 어떤 조치를 취해야 할까요? 이미 진행 중이지만 첫 번째 단계는 표준화 프로세스에 참여하는 것입니다. 사기 인증 방지, 암호화 무결성 보호, 디지털 서명 손상 방지에 이해 관계가 있는 모든 조직이 적극적으로 참여하여 승인된 최종 알고리즘, 프로세서 및 도구 목록에 따라 요구 사항이 충족되는지 확인하는 것이 중요합니다. 표준화 기관에서 상당한 진전을 이루고 있긴 하지만, 여전히 계속 진행 중인 작업으로, 더 많은 알고리즘이 필요합니다. 그 외에도 다음과 같은 성숙도 단계가 Quantum-safe로 이어집니다.

- **데이터 검색 및 분류:** 중요 데이터 인벤토리 가져오기. 무엇이 가치가 가장 높은가? 데이터는 어디에 있나? 준수 요구사항은 무엇인가? 많은 조직들이 무엇을 소유했는지 또는 소유하고 있는 것의 가치를 완전히 인식하지 못하기 때문에 이를 올바르게 이해하는 것이 중요합니다. 이러한 지식 없이는 가장 심각한 취약점을 파악할 수 없습니다. 조직은 소유권이 정의된 데이터 인벤토리를 만들고 관리해야 합니다.
- **암호화 인벤토리:** 암호화 인벤토리에는 취약한 공용 키 암호화가 사용되는 위치와 방법에 대해 자세히 설명되어 있으며, 인증서, 암호화 프로토콜, 알고리즘, 키 길이와 같은 세부정보가 포함됩니다. 인벤토리는 인증서와 암호화 키의 전체 수명 주기에 걸쳐 관리해야 합니다.
- **암호화 민첩성**: 조직은 계획 및 전환 프로세스 내에서 암호화 민첩성을 고려해야만 기술이 발전하고 상황이 변화하면서 문제를 줄이고 조정할 수 있습니다. 또한 현 세대 암호화를 업데이트하거나 교체한 후 제대로 정의된 리드타임 내에 더 쉽게 테스트할 수 있도록 프로세스를 설계하고 수립해야 합니다.
- **Quantum-safe**: 조직은 Quantum-safe 암호화가 비즈니스에 미치는 잠재적인 성능 영향을 인식하고 새 알고리즘을 구현해야 합니다.

조직은 제각각 다를 뿐더러 모든 조직이 비용이나 수명주기 관리 문제 등으로 인해 모든 것을 바꿀 수 있는 상황에 있거나 의지를 가지고 있는 것은 아닙니다. 하지만 보안 프로토콜을 업데이트하거나 교체하는 기능을 설계하는 것은 장단기적인 관점에서 모두 중요합니다. 시스템 인프라와 밀접하게 관련되어 있으므로 암호화 민첩성을 달성하려면 시스템 설계자와 애플리케이션 개발자, 보안 전문가의 협력이 필요합니다. 히지만 현재 이 프로세스에 필요한 도구가 부족한 실정입니다.

조직은 다양한 요소를 사용하여 보호되는 자산의 가치, 보호 대상의 취약성(예: 키 저장소, 암호), 영향을 받게 될 연결된 시스템(예: 연방 기관을 포함한 외부 기관과의 정보 공유), 데이터 보호 기간을 비롯한 Quantum-safe 암호화 대안의 우선 순위를 정할 것입니다. 오랜 전환 기간 동안에 걸쳐 기존 알고리즘과 Quantum-safe 알고리즘을 결합한 하이브리드 체계가 필요합니다.

구현, 동기, 동인

장비와 인프라가 미션 크리티컬 엔터프라이즈 워크로드를 호스팅하는 대규모 클라우드 서비스 제공업체와 시스템 공급업체의 경우, Quantum-safe 암호화 표준이 완전히 마무리될 때까지 기다릴 여유가 없습니다. 해당 업체들은 이 문제에 대해 수 년 동안 연구해 왔으며, 2024년까지 최종 표준 목록을 만들기 위한 최선의 알고리즘과 프로토콜을 선택하는 데 기여해 왔습니다. 이미 다수의 클라우드 기반 키 관리 서비스에서 2차, 3차 알고리즘을 지원하고 있습니다. 고객은 이러한 서비스를 사용하여 대역폭 사용률과 대기 시간에 대한 추가 오버헤드 가능성이 있는 애플리케이션의 성능에 미치는 잠재적 영향을 측정하고 전송 수준 보안 프록시 계층에서 발생할 수 있는 연결 실패를 완화하고 있습니다. 그러나 관련 표준과 기술이 발전함에 따라 Quantum-safe로의 전환은 수 년 동안 계속 진행될 것이며, 이 전환 과정에서는 핵심 인프라 확보가 중요하다는 것에 모두가 동의합니다.

시스템 분야에서 메인프레임은 여전히 초대형 은행, 보험 회사, 통신, 소매, 운송 업계를 위한 가용성과 보안성이 높은 핵심 인프라로 널리 사용되고 있으며 이러한 경향은 반세기 넘게 유지되어 왔습니다. 최신 세대의 메인프레임에는 새로운 양자 저항 알고리즘을 위한 업데이트된 운영 체제 구성 요소, 키 관리 API, 지원과 함께 작동하는 Quantum-safe 하드웨어 보안 모듈이 내장되어 있습니다. 하드웨어 트러스트 루트가 있는 Quantum-safe 보안 부트 기술은 시스템 부트 펌웨어의 무결성을 보호하는 데 사용되며 파트너사와 암호화 키를 안전하게 교환하기 위한 Quantum-safe 메커니즘은 애플리케이션 프로그래밍 인터페이스를 통해 제공됩니다.클라우드 서비스 제공업체와 공급업체는 고객이 Quantum-safe 암호화로 전환할 수 있도록 충분히 지원해야 합니다. 규정 선언 자체만으로는 불충분한데, 일부 이유로는 자체적으로 상당한 전문 지식이 없는 사용자 조직에 명확한 지침을 제공할 만큼 권위가 부족하기 때문입니다.

이미 미션 크리티컬 인프라의 중심에 있는 공급업체는 활성화를 위한 시스템 수준의 추가 변경 없이 핵심 비즈니스 시스템 보호를 제공하여 프로세스를 더 쉽게 만들 수 있습니다. 또한 암호화 애플리케이션 분석을 위해 반드시 필요한 검색 도구도 제공할 수 있습니다. 오늘날의 기존 알고리즘으로 암호화된 데이터가 미래의 고급 양자 컴퓨터로 해독될 수 있기 때문에 데이터를 담당하는 조직은 현재 뿐 아니라 미래의 수명주기 전반에 걸쳐 데이터를 보호해야 합니다. 해당 데이터를 20년 동안 보호해야 하는 경우라면 2040년대가 될 것입니다. 몇 년 안에는 양자 컴퓨팅이 실용화되지 않을 것이라고 믿는 회의론자들도 현재의 발전 속도를 감안하여 그때 쯤에는 가능성이 크게 높아질 것이라는 것을 인정해야 합니다.

결론

양자 컴퓨팅에 대한 비즈니스 사례는 매우 확실합니다. 양자 컴퓨터가 완전히 실현되면 화학, 기계 학습, 금융, 운송, 의료 등이 크게 발전할 수 있습니다. 양자 컴퓨터는 현재 사용되는 고전적이고 결정론적인 컴퓨터로는 실행이 비현실적인 방정식의 처리를 어마어마한 속도로 가속화할 것입니다.

반면에 양자 컴퓨팅으로 인해 데이터와 개인정보에 대한 사이버 공격의 위협이 더 커질 수 있습니다. 데이터의 비즈니스 가치가 증가함에 따라 데이터 보호 요구 사항의 규모와 비용도 증가합니다. 그리고 데이터의 가치는 오래 지속되기 때문에 가까운 미래에 양자 컴퓨팅이 실제 현실이 될 가능성이 높은 점도 고려해야 합니다. 더 늦기 전에 조치를 취하면 Quantum-safe 코어 인프라, 현재 응용프로그램 계층 취약성을 찾을 수 있는 도구 구현, 조직 전체에서 사용되는 키 교환 시스템 보호, 데이터에 보관된 장기간 암호의 지속적인 보호가 가능해 집니다.

연락처

미주
+1 877 863 1306
market.intelligence@spglobal.com

유럽·중동·아프리카
+44 20 7176 1234
market.intelligence@spglobal.com

아시아 태평양
+852 2533 3565
market.intelligence@spglobal.com

www.spglobal.com/marketintelligence