<주요 Q&A>

정보유출 걱정 없이 매칭하자!
안전한 매칭기술 PSI(Private Set Intersection)

Q1. PSI 기술이 블록체인 기반기술인것인가요?

블록체인 기술은 아니고, 암호기술이며 향후 블록체인 기술에도 적용해볼 수 있지 않을까 생각됩니다.

Q2. 정말 노출 없는 기술인가요?

네 각 사용자가 보유한 정보는 전혀 노출하지 않고 교집합이나 특정 정보를 계산할 수 있는 암호기술입니다.

Q3. 협업하는 기관들이 공통 데이터를 목적에 따라 안전하게 활용하기 위해서 구비해야 할 사항들에 대해서 질문 드립니다.

두가지로 상황으로 나누어 답변드리겠습니다.

1. 제 3자 데이터 제공 동의받은 데이터의 경우: 협업하는 기관에 데이터를 직접 제공하여 활용할 수 있습니다.

2. 미동의받은 데이터의 경우: 원본 데이터에 개인정보보호법에서 명시된 기준에 따라 가명화 및 익명화 기술을 적용하여 협업기관과 데이터를 활용할 수 있습니다. 이런 경우 이번 세션에서 소개드리는 PSI 기술을 포함한 다양한 비식별화 기술들을 활용과 법령에 의거 데이터 전문기관의 도움을 통해 진행될 수 있습니다.

Q4. 동형암호 에 대한 간단한 정의나 설명 링크 알 수 있을까요

2018, 2019년 테크토닉 행사에 자세히 소개되어 있습니다. (발표자료 7페이지 참고)

SAMSUNG SDS

Q5. HE가 무엇의 약자인가요?

Homomorphic Encrytion 동형암호 약어입니다.

Q6. https://www.koreascience.or.kr/article/JAKO201317748766296.pdf 이 자료를 참조하면 될까요?

네 해당자료도 좋구요.. 동형암호 표준화단체에서 제공하는 기술문서들을 보셔도 좋습니다. (http://homomorphicencryption.org/standard/)

Q7. G사의 경우 두 개의 암호화 기술을 합해 자료들은 암호화 된 상태에서 보호한다고 알고 있는데요. 삼성 SDS에서의 기술적 부분은 한단계 업그레이드 되었다고 봐도 될까요?

네. 맞습니다. 기존 기술에 동형암호의 장점을 추가하여 업그레이드 되었다고 보시면 됩니다.

Q8. 양자 컴퓨팅 기술과 접목을 시켜 볼 순 없나요?

우선 기존 컴퓨팅 기술로도 충분한 효율성을 달성할 수 있으므로 구현적인 면에서 접목시킬 필요성은 매우 낮아 보입니다. 다른 방향으로 양자 컴퓨팅 시대에 암호기술에 영향을 주는 부분이 안전성 분석분야인데요. 추가된 동형암호기술은 양자내성암호기술이므로 양자 컴퓨터시대에도 안전하게 사용가능합니다.

Q9. 해킹 위험이 전혀 없는건가요

암호화는 공개키로 암호화되고, 공격자가 쉽게 접근할 수 있는 연산과정은 암호화된 상태에서 진행되므로 해킹에 문제가 없고, 복호화는 각 사용자만 보유하고 있는 복호화키로 진행되므로 매우 안전합니다.

Q10. 뭔가 애플 기기의 비밀번호 유출 모니터링 서비스 같네요 특정 패스워드 유출 위험을 알려주더라구요

네. 비슷한 서비스로 보시면 됩니다.

Q11. 저런 것을 위해 요새 오픈뱅킹 서비스가 확대되는 것인가요?

오픈 뱅킹은 사용자 동의기반 서비스로 각 국가별 서비스로 적용됩니다. 하여 해당 기술적용과는 조금 거리가 있습니다.

Q12. 모든 보안은 창과 방패 싸움인데 향후 뚫릴수 있는 가능성을 두고 생체정보를 활용한 2차 보안 기능이 필요하지 않을 까요?

네 주신 의견에 동의합니다. 보안기술은 하나의 완벽한 기술로 방어가 불가하므로 다중 보안기술 적용이 더 좋습니다.

Q13. 저희 동형암호 기술이라고 한다면 이 기술특허가 삼성에 있는 건가요?

네 글로벌 회사와 함께 저희 회사도 독자적인 기술특허들을 많이 보유하고 있습니다.

Q14. 혹시 개인정보결합전문기관으로써 본 기술이 활용이 되고 있나요?

현재 해당기술 적용을 위한 논의가 진행중에 있습니다.

Q15. 개인정보 비식별화 (익명처리, 가명처리)는 회사 내부 자체 검증 시 불법인지요?

각 사에서 사용될 데이터에 대한 자체 검증은 문제가 없으며, 대부분의 회사들이 자체 기술/기준으로 검증하고 있습니다. 다만, 외부 협업시에는 좀더 세밀한 검증이 필요하며, 이를 위해 전문기관을 통해 진행하기도 합니다.

Q16. 앞으로 사이버보안이 더욱 더 중요해질 것 같은데 PSI기술이특화된부분은?

해당 기술을 주기적으로 활용한다면 최신성까지는 필요하지 않을듯 싶고, 보유한 데이터를 각사와 협업시 식별할 수 있는 공통의 실별자 항목만 보유된다면 적용 가능합니다.

Q18. 특정 로그인 사용자 인증 정보 및 사용환경이 안전한지 여부를 확인 가능한 암호화 프로토콜은 삼성SDS 독자적 기술인가요? 아니면 범용적인 기술인가요?

공개된 기술들도 있으나 저희 기술이 최신/고보안/초고속 기술이 적용된 솔루션이라고 보시면 됩니다.