SAMSUNG SDS

Foresee

Techtonic 2021

Partner

Disrupt

정보유출 걱정없이 매칭하자!

안전한 데이터 매칭기술 PSI

문덕재, 손용하 프로

AGENDA

안전한 데이터 매칭기술(PSI) 이해하기

경쟁사 주요 적용사례 알아보기

SDS PSI 살펴보기 (데모시연)

SDS PSI 향후 계획 들어보기

SDS PSI

안전한 데이터 매칭기술(PSI) 이해하기

들어가며

기업내 보유 데이터를 활용한 서비스 時, 발생하는 유출사고를 방지하기 위한 규제강화, Privacy 강화 솔루션 출시 진행 중

개인정보 유출 및 오남용사고

- Facebook 5억3300만명 개인정보 유출 (`21년 4월)

facebook

- Amazon 고객정보 오남용으로 1조200억원 과징금 부과 (`21년 7월)

amazon

Privacy 규제 강화

- 전세계 80개국 이상 Privacy 관련 규제 제/개정 중

국가	규제명	시행일
유럽	GDPR	`18. 5.
미국	CCPA/CPRA	`20.1./`23.1.
캐나다	PIPEDA	`20. 4.
중국	CSL/PIPL	`16.11./`20.10.
싱가폴	PDPA	`20. 11.
일본	APPI	`20. 6.
한국	개인정보보호법	`20. 8.

Privacy 강화 솔루션 출시

Microsoft Google facebook VISA ENVEIL ENCRYPTED VEIL Duality baffle apheris AI inpher

안전한 데이터 매칭기술(PSI: Private Set Intersection)

데이터 소유자들이 원본 데이터 노출 걱정 없이 공통 데이터를 확인, 공통 데이터간 연산 및 분석을 지원하는 기술

Pain Point (Matching)

사용자

▼

고객 리스트, 계좌번호 등
개인정보 유출에 대한 우려

AS- IS

✔ Privacy 와 직결되는 PII* 정보
: 자유로운 활용이 어려움

A 社

번호	고객 ID
1	1
2	4
3	19
4	23
5	26
6	32
7	47

평문 매칭 불가

B 社

번호	고객 ID
1	2
2	5
3	16
4	19
5	23
6	32
7	47

TO-BE

✔ PET 기술을 활용한 PSI 적용으로
안전한 PII 매칭 가능

A 社

번호	고객 ID
5	26
1	1
7	47
4	23
6	32
2	4
3	19

암호문 매칭

B 社

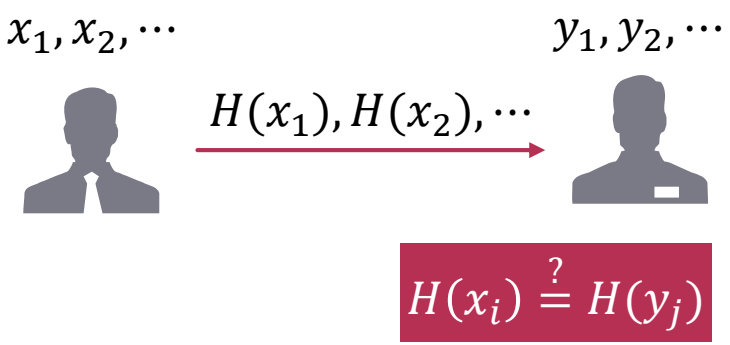
번호	고객 ID
6	32
5	23
3	16
7	47
1	2
2	5
4	19

* PII: Personally Identifiable Information

적용 요소기술 소개

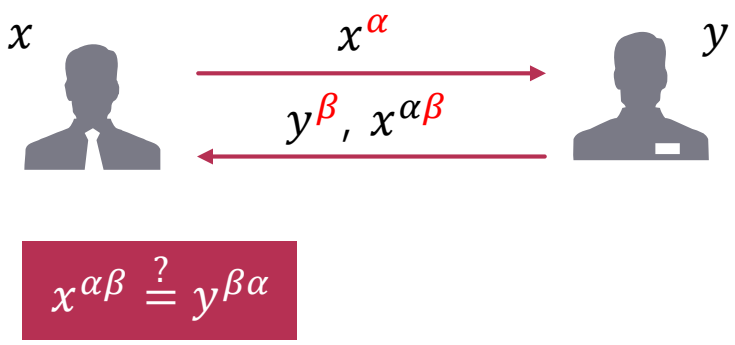
안전성, 구현속도 및 통신량을 모두 고려한 향상된 기술로 발전

① 기초 기술 (HASH)



Hash 함수의 역추적 가능성
→ 충분한 안전성 제공하지 못함

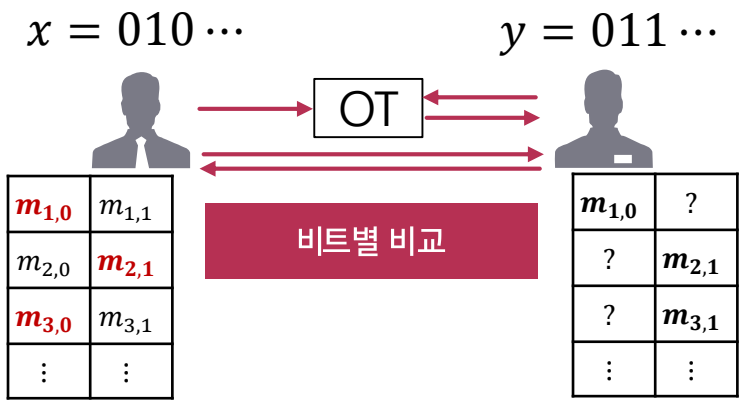
② 경쟁사 기술 (DDH*)



* DDH: Decisional Diffie-Helllman protocol

충분한 안전성 제공
지수 연산으로 인해 느린 구현속도
(Google/Facebook 社 적용 중)

③ SDS 기술 (HE + OT**)



**OT: Oblivious Transfer protocol

충분한 안전성 및 **월등한 구현속도**
비트 연산(OT)으로 인해 기본 통신량 증가
: 동형암호(HE)를 접목하여 통신량 절감

※ 동형암호기술 알아보기: Techtonic 2018(데이터가 돈이 되는 세상: Privacy Preserving Data Mining, https://www.samsungsds.com/kr/event/techtonic2018.html?referrer=https://www.google.com/)
Techtonic 2019(정보손실/유출없이 고객 데이터를 분석해 보자!, https://www.samsungsds.com/kr/event/techtonic2019.html?referrer=https://www.google.com/)

동형암호기반 PSI 기술 차별화 포인트

안전성을 유지하면서 경쟁사 대비 최소 65배 이상 빠른 구현 속도 제공

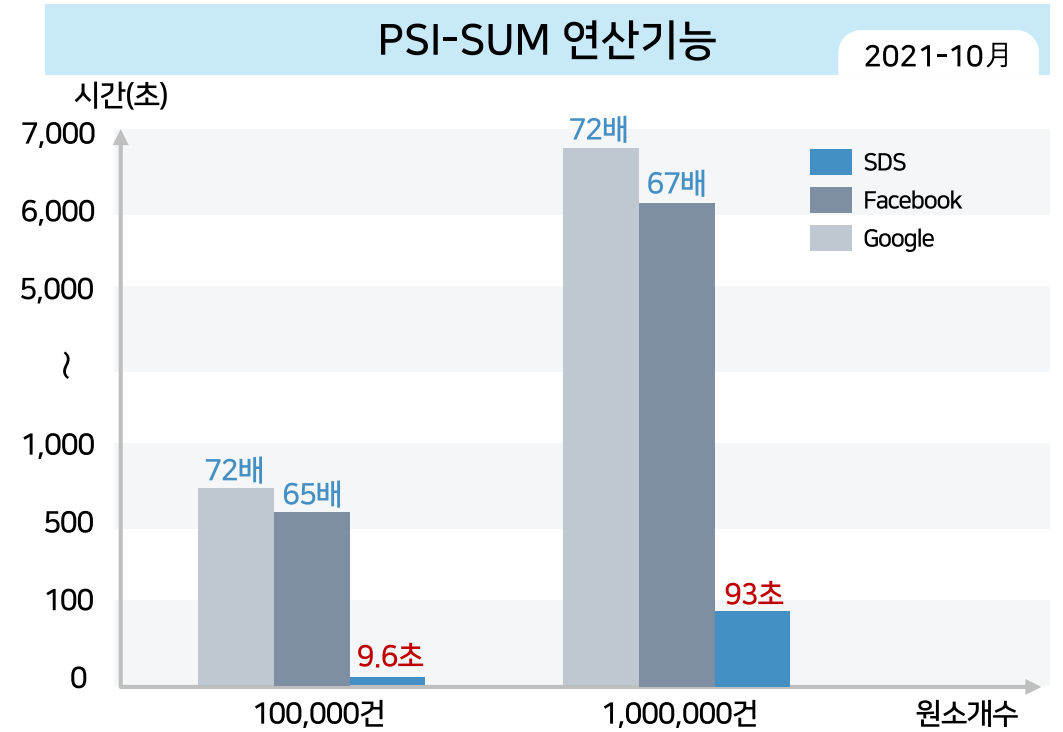
주요특징

- 다양한 상황에 적용 가능한 최적화 알고리즘 제공
  - 입력의 크기 (Balanced/Unbalanced) 별 최적화 버전 확보
  - 대역폭에 따른 최적화 버전 확보
- 경쟁사 대비 정량적 지표 우수 (`21. 10월 기준)
  - Google社/Facebook社 대비 72배/65배 이상 고속화
- 우수 기술에 대한 주요 IP 확보
  - HE기반 PSI 특허 출원완료/설계논리 대외검증(Top-tier) 진행 중

주요기능

단일정보 매칭	다중정보 매칭	
Cardinality 연산	SUM 연산	Threshold 연산

실환경에서 테스트 속도



※ 테스트 환경: MS Azure Cloud (Linux-Ubuntu 20.04, vCPU-Intel Xeon E5-2673 v4@2.30GHz 4Cores, 16GB RAM)

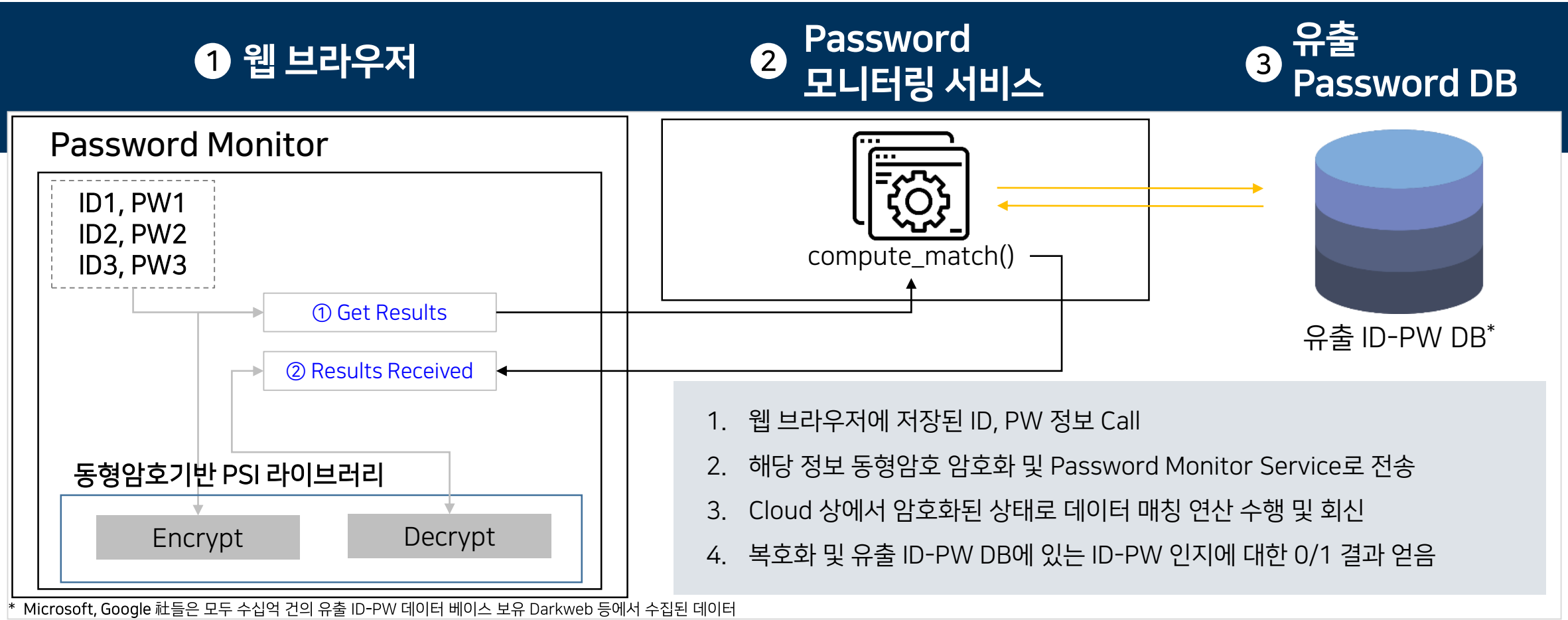
SDS PSI

경쟁사 주요 적용사례 알아보기

사례1

(MS, Google社) Password 모니터링 서비스

동형암호 기술을 이용한 안전한 Password 쿼리 보호



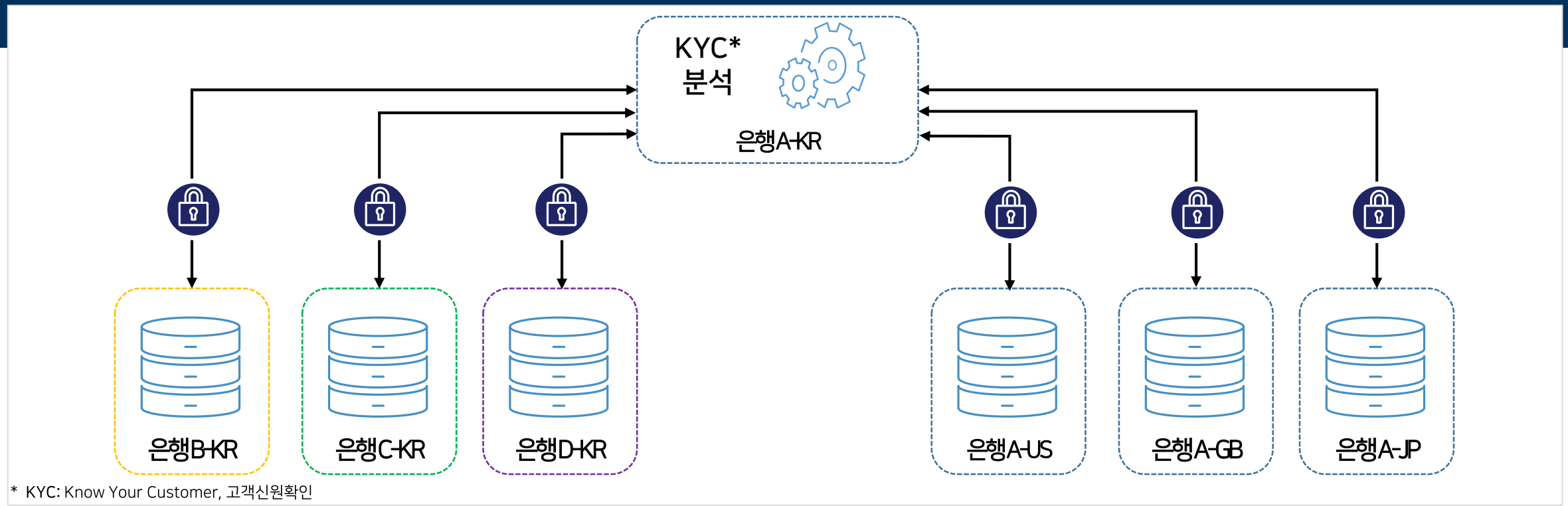
1. 웹 브라우저에 저장된 ID, PW 정보 Call
2. 해당 정보 동형암호 암호화 및 Password Monitor Service로 전송
3. Cloud 상에서 암호화된 상태로 데이터 매칭 연산 수행 및 회신
4. 복호화 및 유출 ID-PW DB에 있는 ID-PW 인지에 대한 0/1 결과 얻음

* Microsoft, Google 社들은 모두 수십억 건의 유출 ID-PW 데이터 베이스 보유 Darkweb 등에서 수집된 데이터

사례2

(Duality社) 자금세탁방지 및 사기검출

동형암호 기술기반 SQL 쿼리를 이용한 국내외 금융기관간 고객정보, 자금흐름 모니터링

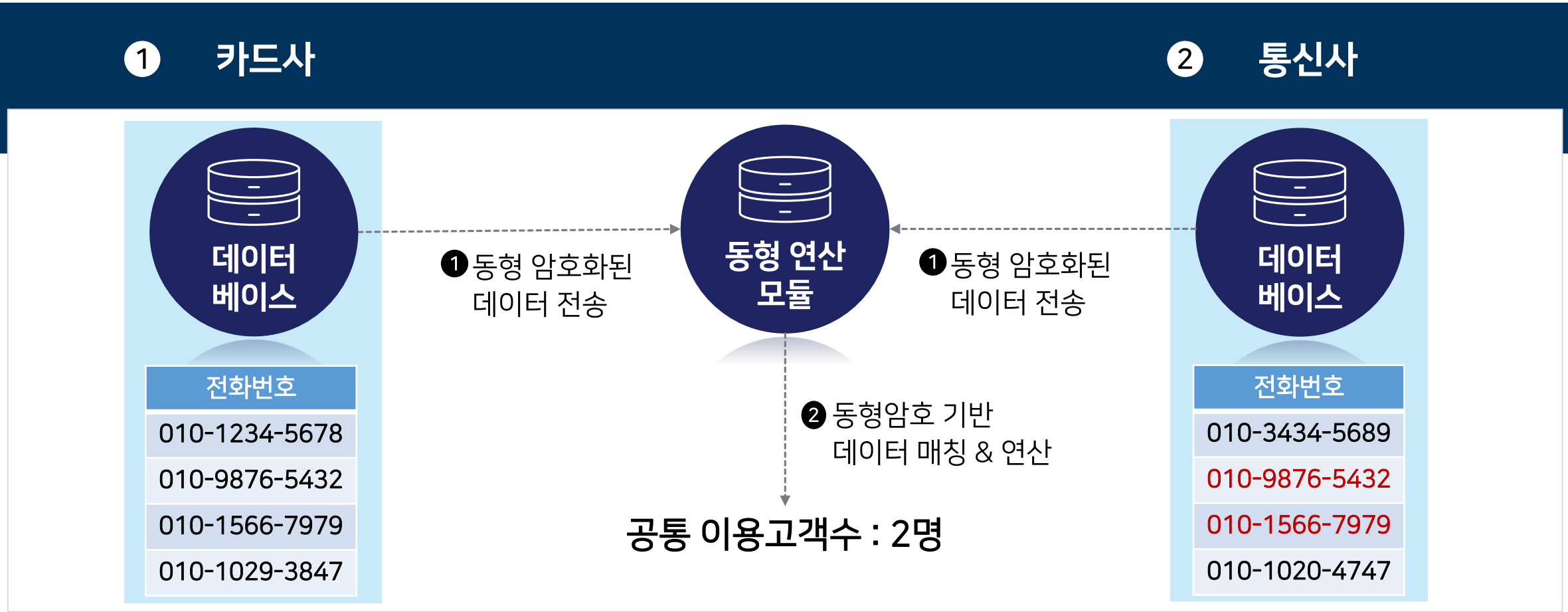


* KYC: Know Your Customer, 고객신원확인

사례3

(Enveil社) 제휴계약 사전성공률 / 데이터 모의결합, 결합률 확인

동형암호 기술을 이용한 안전한 데이터 매칭 및 기본연산(Cardinality) 을 통한 안전한 공통 데이터(고객 정보) 확인



사례4

(Google, Facebook社) 온라인 광고 효과 검증

동형암호 기술을 이용한 안전한 데이터 매칭 및 기본연산(SUM) 을 통한 안전한 광고 효과 검증

SDS PSI

SDS PSI 살펴보기 (데모시연)

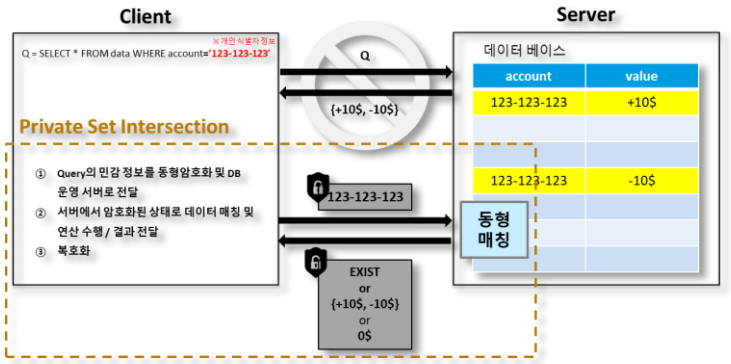
SDS PSI

SDS PSI 향후계획 들어보기

SDS PSI Compute System 적용 로드맵

독자적인 동형암호 기술기반 데이터 매칭기술을 다양한 데이터 활용 사업분야에 확대 적용

① 기본 매칭 서비스



- 단일 정보에 대한 매칭서비스
  . DB-query, Secure Search 등
- 다중 정보에 대한 매칭서비스
  . 결합 데이터 매칭

(보안, 의료 분야 등 적용)

② 연산지원 매칭 서비스

- 다양한 사업분야 요구사항에 따른 연산지원을 통한 서비스
  . 맴버십/데이터결합 효과검증
  . 온라인 광고/정책 사전효과 검증
  . 보험금/연금/포인트 중복수혜방지

(금융, 마케팅, 공공 분야로 확대적용)

③ 데이터 분석/거래 플랫폼 연계

AWS Data Exchange
금융데이터거래소 FINANCIAL DATA EXCHANGE
KDX 한국데이터거래소 KOREA DATA EXCHANGE
snowflake
NHN DATA

- 데이터 분석플랫폼 연계를 통한 결합분석 효과 극대화
- 데이터거래시 맞춤형 데이터 확인, 데이터 가공서비스 자동화, 고도화

(데이터활용 사업 전분야 확대적용)

Thank you

SAMSUNG SDS