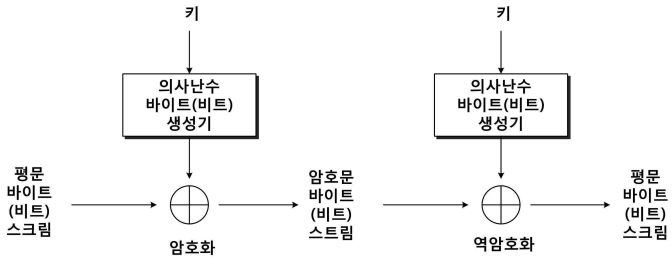
무선통신 비트 오류 최소화를 위한 클럭조절형 랜덤 암호 발생기

CLOCK CONTROLLED RANDOM PASSWORD GENERATOR FOR MINIMIZING BIT ERROR RATE IN WIRELESS COMMUNICATION



[기본적인 스트림 암호 알고리즘을 설명하기 위한 예시도]

발명자	이훈재, 김기환, 이정규, 이상곤, 김태용, 장원태
출원번호	10-2016-0123457
출원일자	2016-09-26
등록번호	10-1881143 (KR)
등록일자	2018-07-17

기술아젠다

- ✓ 사회 안전 확보 - 사이버 안전 및 정보보호

과학기술분류

- ✓ 공통 보안기술(L0301)
- ✓ 네트워크 시스템 보안(L0302)
- ✓ 서비스/응용보안(L0303)

표준산업분류

- ✓ 컴퓨터 프로그래밍 서비스업(KSIC 62010)

신성장동력 • 원천기술분야

- ✓ 융합 보안 - 미래컴퓨팅 응용·보안기술

기술개요 DSU+

- 무작위 난수생성을 알고리즘을 통한 무선통신비트오류에 대응할 수 있음
- 충분한 크기의 LFSR을 난수발생에 있어서 안전한 수준의 무작위수열을 생성할 수 있는 효과를 제공함
- 비선형성을 증가시켜 상관 공격 등을 통한 악의적 암호 해독을 어렵게 하도록 할 수 있음

기술의 요지

- 클럭을 제공하는 클럭제공부(400b); 클럭제공부(400b)가 제공하는 클럭에 따라 출력비트를 출력하는 제 1 LFSR(100c); 클럭제공부(400b)가 제공하는 클럭에 따라 출력비트를 출력하는 제 2 LFSR(100d); 이전 캐리값을 제공받아 저장하는 제 1 비트 메모리(200c); 이전 메모리 상태값을 제공받아 저장하는 제 2 비트 메모리(200d); 및 제 1 및 제 2 LFSR(100c, 100d)의 출력비트와 제 1 및 제 2 비트 메모리(200c, 200d)가 저장한 이전 캐리값과 이전 메모리 상태값을 제공받아 출력 키수열 및 현재 캐리값 및 현재 메모리 상태값을 생성하고, 출력 키수열은 암호로서 출력하고 현재 캐리값 및 현재 메모리 상태값을 제 1 및 제 2 비트 메모리(200c, 200d)로 제공하는 연산기(300b);를 구비하는 무선통신 비트 오류 최소화를 위한 클럭조절형 랜덤 암호 발생기에 있어서, 제 1 LFSR(100c)은, 255 비트의 난수발생 함수를 갖으며, 제 2 LFSR(100d)은, 257 비트의 난수발생 함수를 갖음

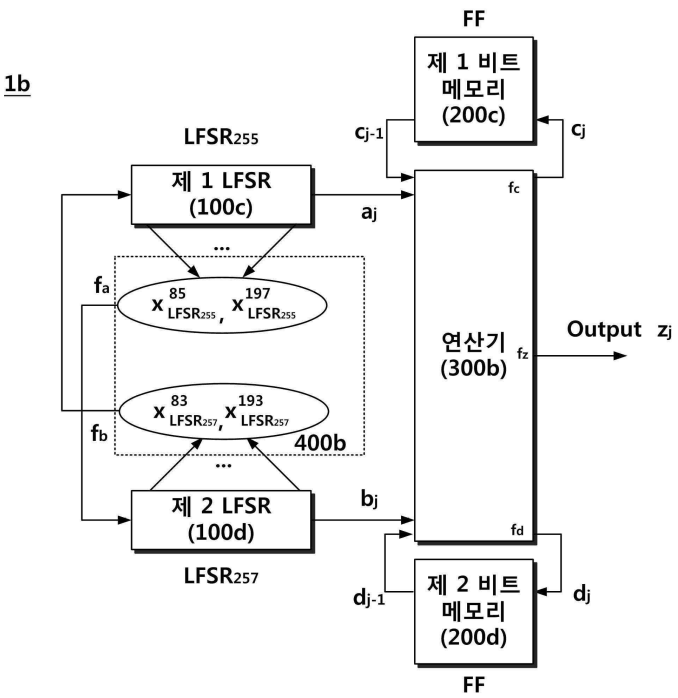
기존 기술의 문제점

- 사물인터넷과 개인인증 방식이 근거리 무선통신(NFC, Blue tooth, ...)을 기반으로 변화하는 추세에 맞추어 데이터의 유출을 보호하기 위해 암호화가 필수적으로 요구되고 있음
- 블록암호의 경우 특정 블록이 정확하게 전달되지 못할 경우 메시지 해독 전체에 영향을 줄 수 있기 때문에 문제가 될 수 있음. 이에 1 비트(bit) 기반의 상대적으로 작은 전송으로 암호화가 이루어지는 스트림 암호가 필요함

개발 기술의 효과

- 무작위 난수생성을 알고리즘을 통한 무선통신 비트 오류에 대응할 수 있는 효과를 제공함
- 충분한 크기의 LFSR을 난수발생에 있어서 안전한 수준의 무작위수열을 생성할 수 있는 효과를 제공함
- 비선형성을 증가시켜 상관 공격 등을 통한 악의적 암호 해독을 어렵게 하도록 할 수 있는 효과를 제공함

대표 도면



[무선통신 비트 오류 최소화를 위한 클럭조절형 랜덤 암호 발생기(1b)를 나타내는 블록도]

기술의 작용

- 무선통신 비트 오류 최소화를 위한 클럭조절형 랜덤 암호 발생기(1b)는 제 1 LFSR(100c), 제 2 LFSR(100d), 제 1 비트 메모리(200c), 제 2 비트 메모리(200d), 연산기(300b) 및 클럭 제공부(400b)를 구비함
- 무선통신 비트 오류 최소화를 위한 클럭조절형 랜덤 암호 발생기(1b)는 제 1 LFSR(100c)와 제 2 LFSR(100d)에서 사용된 다항식에 해당하는 정보를 이용함
- 제 1 LFSR(100c)와 제 2 LFSR(100d) 각각에서 사용하는 255 비트의 16탭, 257 비트의 16 탭으로 이루어진 2개의 원시 다항식(two primitive polynomials)으로 정의됨
- 제 1 LFSR(100a) 및 제 2 LFSR(100b)을 구비한 클럭조절형 랜덤 암호 발생기(1a)가 충분한 크기의 LFSR을 난수발생에 사용한다면 안전한 수준의 무작위수열을 생성할 수 있음
- 이를 위해 무선통신 비트 오류 최소화를 위한 클럭조절형 랜덤 암호 발생기(1)는 LFSR 255 비트의 난수발생 함수를 갖는 제 1 LFSR(100c)와 LFSR 257 비트의 난수발생 함수를 갖는 제 2 LFSR(100d)을 사용함
- 256 비트의 함수를 사용하는 무선통신 비트 오류 최소화를 위한 클럭조절형 랜덤 암호 발생기(1b)는 무작위 난수가 생성됨
- 또한 무선통신 비트 오류 최소화를 위한 클럭조절형 랜덤 암호 발생기(1b)는 각각의 LFSR 함수가 정해진 크기를 가지고 있는 단점을 보안하기 위하여 상대방의 상태값을 이용하여 출력순서에 변화를 줌

적용 시장 DSU+

- 컴퓨터 프로그래밍 서비스업(KSIC 62010) 시장 – 특정 고객의 요구에 의하여 주문형 소프트웨어를 자문, 개발 및 공급하는 산업활동을 말함
- 미국은 SW개발 및 공급업(5112) 시장

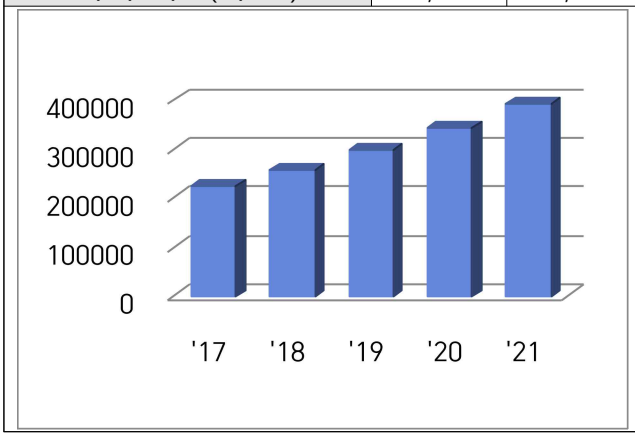
시장 규모

- SW개발 및 공급업(5112)의 미국 시장 규모는 2017년 224,400백만 달러에서 증가(CAGR 15%)되어, 2021년에는 392,300백만 달러에 달할 것으로 예측
- 컴퓨터 프로그래밍 서비스업(KSIC 62010)의 국내 시장 규모는 2017년 42,367억 원에서 증가(CAGR 6.7%)하여, 2021년에는 54,907억 원에 달할 것으로 예측

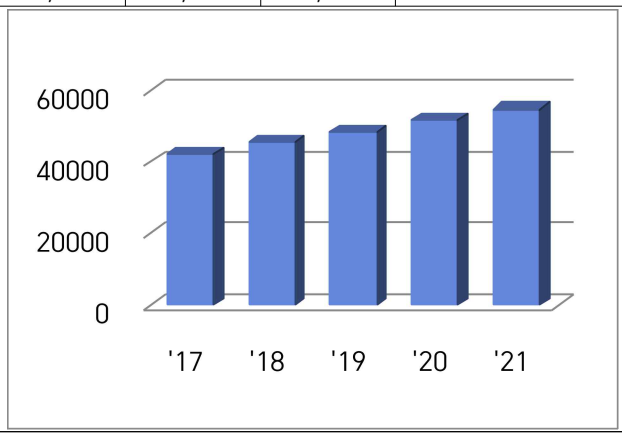
[표] 미국/국내 컴퓨터 프로그래밍 서비스업 분야의 시장규모 추이

단위: 억 원, 백만 달러, %

구분	'17	'18	'19	'20	'21	CAGR(17~21)
미국 시장(백만 달러)	224,400	257,900	296,600	341,100	392,300	15%
국내 시장(억 원)	42,367	45,502	48,637	51,772	54,907	6.7%



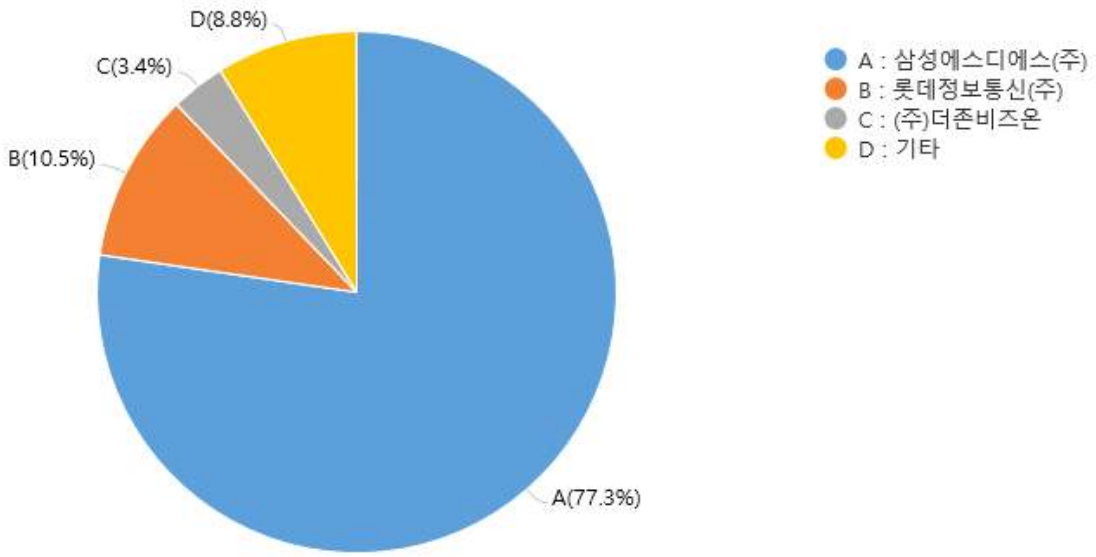
[미국 시장]



[국내 시장]

*출처: 한국은 한국과학기술정보연구원(2019), 미국은 정보통신정책연구원(2017), '미국 SW산업 매출 현황' 재가공

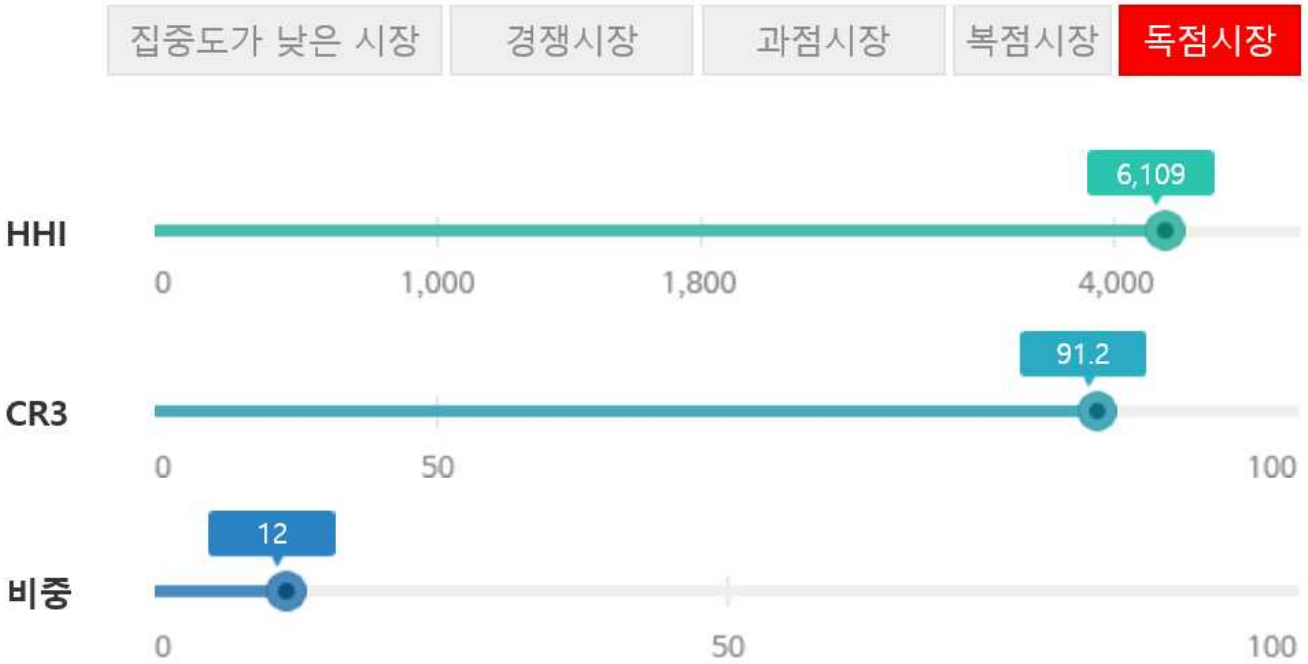
국내 시장 점유율



*출처: 한국과학기술정보연구원(2019, 2018년도 기준으로 작성)

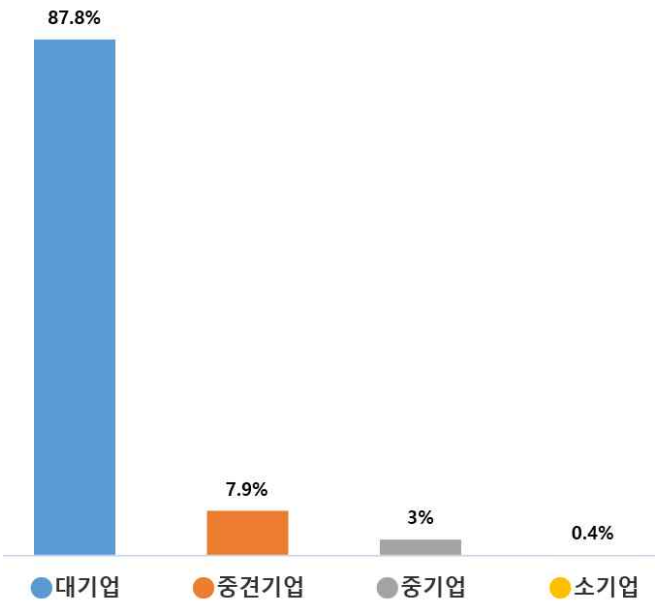
시장 집중도

- 기업집중도를 보면, 컴퓨터 프로그래밍 서비스업(KSIC 62010) 시장에서 허핀달-허쉬만 지수(Herfindahl Hirschman Index, HHI. 시장집중도 측정방법으로 기업의 시장점유율의 제곱을 모두 합산한 지수)가 6,109이고, 상위 3대 기업 집중도(Concentration Ratio3, CR3. 시장점유율 1~3위 기업의 시장점유율의 합)는 91.2%를 차지하며 중소, 중견기업 매출 비중이 12%를 차지하는 시장으로 독점 시장에 해당함



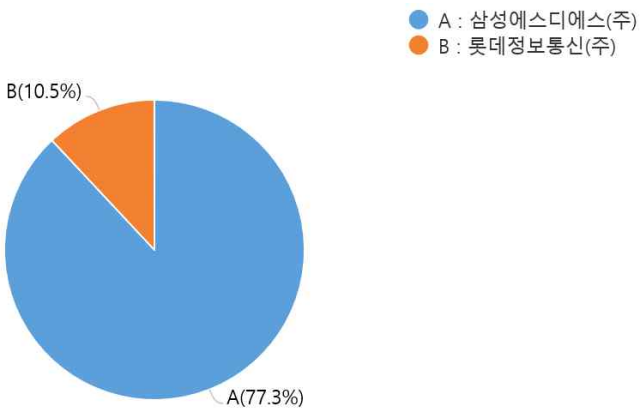
*출처: 한국과학기술정보연구원(2019)

규모별 시장 점유율



*출처: 한국과학기술정보연구원(2019)

대기업 경쟁구조



*출처: 한국과학기술정보연구원(2019)

기술동향 DSU+

- 초지연성·초고속·초연결을 구현하는 5G 기술은 스마트폰의 경계를 넘어 집과 이동 수단, 일터, 제조 시설, 사회 인프라에 걸쳐 폭넓게 적용되며, 개인의 삶과 기업 생산성, ICT 분야에 큰 변화를 불러일으키는 변곡점이 될 것으로 예측되고 있음.
- 이처럼 무선통신 기술이 고도화, 범용화되면서, 암호화 기술의 중요성도 커지고 있음

국내외 기술 동향

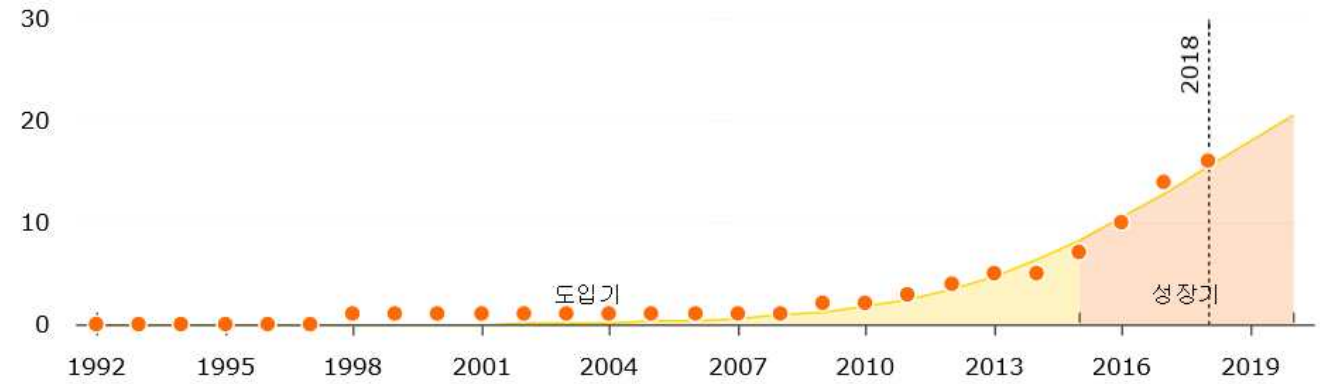
- 초고속 광대역 전송 서비스, 초저지연 서비스, 사물인터넷과의 융합, 클라우드에 대한 의존성 증가, 다양한 모바일 융합 서비스 등장 등 초연결 지능화 인프라의 근간이 되는 5G는 이동통신 서비스의 다양한 메가트렌드가 총망라될 것으로 전망되고 있음
- 고품질의 이동통신 서비스가 안전하게 운용되기 위해서는 기본적으로 가입자의 개인 정보와 통신의 기밀성 및 무결성을 보호하는 것 외에도 다양한 사이버 공격에 대한 네트워크 자체 보호가 무엇보다 중요함
- 5G 기술을 통해 PC와 모바일 기기는 물론 스마트 빌딩, 자율주행차 등 다양한 사물인터넷 기기들이 수많은 사용자와 연결되는 만큼, 이에 대한 통제권을 뺏길 경우에는 중요 정보를 탈취당하거나 금전적 피해를 입는 것에서 더 나아가 사람의 생명과 안전을 위협할 수 있는 공격이 발생할 수도 있기 때문임
- 이에, 보안 전문가들은 5G 상용화도 중요하지만, 보안성 담보에도 힘을 기울일 것을 강조하고 있음
- 상용화를 추진하는 5G 망과 관련해 유럽네트워크정보보호원(ENISA) 등은 기존 2G~4G 망 환경에 알려진 취약점이 5G 망에서도 적용 가능성이 짙다고 발표함
- 보안이 무너지면 원격의료나 자율주행차 등 사람 목숨이 걸린 사고로까지 이어질 수 있기 때문에 사업 전체가 송두리째 위기를 맞게 될 위험이 있음. 그래서 보안 리스크 관리가 다른 그 무엇보다도 중요한 사업 경쟁력이 됨.
- 5G 보안 해법으로 KT는 블록체인을, SKT는 양자암호를 내세우는데, 결국엔 모든 기술이 복합적으로 통합 적용되어야 할 것임.
- 전통적으로 모바일 기기의 오픈소스 취약점을 어떻게 해결할 것인지도 큰 문제임. 다른 망 환경보다 표준화를 빨리 이룬 5G의 경우 오픈소스의 사용이 많아질 것이며 이는 오픈소스 보안관리를 철저히 해서 극복할 문제이기도 함

관련 기술의 미래 부상성

No.	Product family	K-Index	특허수	국내기업 점유율	기업 독점도	파급도	복합도	미래 부상성
1	PASSWORD MANAGEMENT SYSTEM	87.26	16	0.00%	1,833.91	0	0	7.41
2	AUTHENTICATION PASSWORD	71.42	5	0.00%	2,000.00	0.22	0	3.96
3	PASSWORD INPUT DEVICE	72.45	7	0.00%	1,400.00	0.02	0.09	2.84
4	BIOS PASSWORD	56.86	2	0.00%	5,000.00	0	0	2.79
5	LOG-IN PASSWORD	71.36	8	0.00%	1,875.00	0	0	2.31
6	PASSWORD GENERATOR	73.37	11	9.09%	1,404.96	0.38	0.55	1.98
7	1-TIME PASSWORD GENERATOR	41.27	2	0.00%	5,000.00	0.2	0	0.45
8	VOICE-MAIL PASSWORD	50.89	5	20.00%	4,400.00	0.5	0	0.36
9	ID PASSWORD	37.87	3	66.67%	5,555.56	0	0	0.05
10	SECRET PASSWORD	34.58	4	0.00%	6,250.00	0	0	0

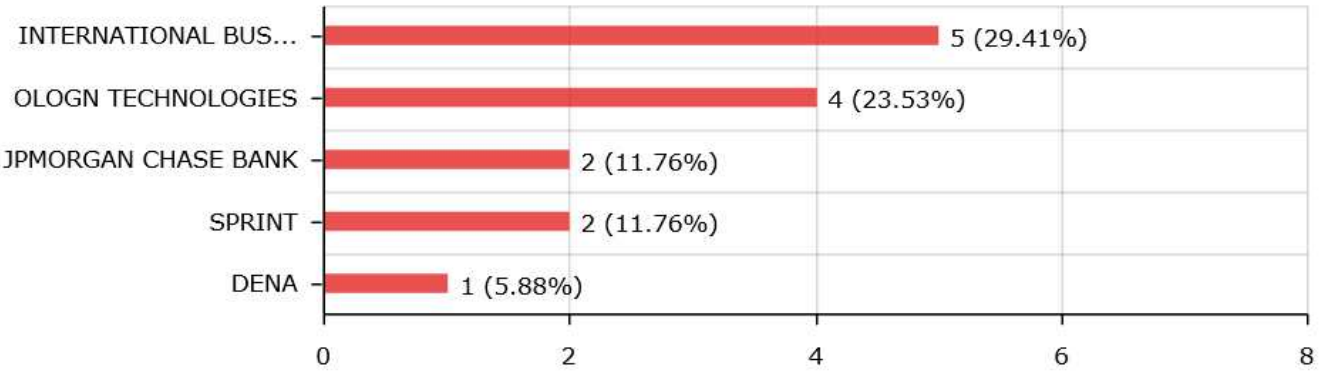
*출처: 한국과학기술정보연구원(2019), TOD(Technology Opportunity Discovery)

주요 Product family인 PASSWORD MANAGEMENT SYSTEM 분야의 특허수 성장성 예측



*출처: 한국과학기술정보연구원(2019), TOD

주요 Product family인 PASSWORD MANAGEMENT SYSTEM 분야의 주요 특허 출원인



*출처: 한국과학기술정보연구원(2019), TOD

문의처 DSU+

- ✓ 담당자 : 기술경영센터
- ✓ 전화번호 : 010-4312-3972
- ✓ 이메일 : sem903@dongseo.ac.kr
- ✓ 주소 : (47011) 부산시 사상구 주례로 47 동서대학교 산학력력단 기술경영센터