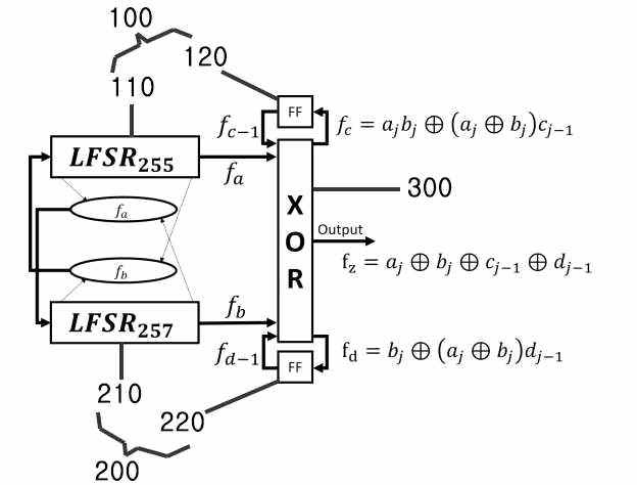
양방향성 상호 클럭조절방식을 이용한 랜덤 이진수열 발생방법

random binary number column generating method using bidirectional mutual clock control way



[대상 기술의 양방향성 상호 클럭조절방식을 이용한 랜덤 이진수열 발생방법의 개념도]

발명자	이훈재, 최윤정, 김기환, 이상곤
출원번호	10-2017-0147725
출원일자	2017-11-08
등록번호	10-1995133 (KR)
등록일자	2019-06-25

기술아젠다

- ✓ 풍요로운 지식 창조 및 활용 – 시공간상의 원활한 정보교환

과학기술분류

- ✓ 디지털 영상(HE1404)
- ✓ 공통 보안기술(EE0301)
- ✓ 정보시스템보안(SC1108)

표준산업분류

- ✓ 응용 소프트웨어 개발 및 공급업(KSIC 58222)

신성장동력 • 원천기술분야

- ✓ 인공지능 - 시각이해 기술

기술개요 DSU+

- 2개의 LFSR의 메모리에 저장되는 초기값을 모두 0이 아닌 임의의 값으로 변경한 후, 각각의 LFSR의 1비트를 저장하는 캐쉬메모리를 사용하여 상호클럭조절 함수를 구성하되, LFSR의 탭 길이가 가변클록의 횟수에 영향을 주게 되고, 가변클록의 횟수의 변화에 의해 선형복잡도가 증가하며 주기가 길어지는 것으로, 암호화된 긴 메시지를 사용하여 전달할 때, Berlekamp-Massey 알고리즘을 이용한 공격 등의 컴퓨터 공격에 대해서 안전하게 함

기술의 요지

- 2개의 LFSR(100, 200)이 서로 상호작용 하면서 클럭을 랜덤(Random)으로 조절하여 데이터를 획득하는 데이터획득단계; 획득한 데이터를 논리회로부(300)에서 이진수열로 변환하여 발생시킨 후 최종 출력결과를 획득하는 출력결과획득단계; 로 이루어짐
- 2개의 LFSR(Linear feedback shift register, 선형 되먹임 시프트 레지스터)의 메모리에 저장되는 초기값을 모두 0이 아닌 임의의 값으로 변경한 후, 각각의 LFSR의 1비트를 저장하는 캐쉬메모리를 사용하여 상호클럭조절 함수를 구성하되, LFSR의 탭 길이가 가변클록의 횟수에 영향을 주게 되고, 가변클록의 횟수의 변화에 의해 선형복잡도가 증가하며 주기가 길어지는 것으로, 암호화된 긴 메시지를 사용하여 전달할 때, Berlekamp-Massey 알고리즘을 이용한 공격 등의 컴퓨터 공격에 대해서 안전하게 함

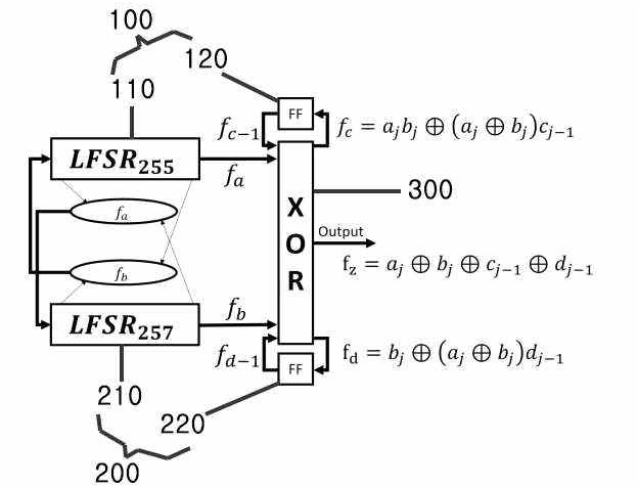
기존 기술의 문제점

- 종래의 상호보완 이진 수열을 이용한 영상 디블러링 방법은 양방향성 상호 클럭조절방식을 제공하지 못하여 가변클록을 제공하지 못하며, 선형복잡도가 낮고, 주기가 짧아서 컴퓨터 공격에 대한 안정성이 낮은 단점이 있었음

개발 기술의 효과

- 2개의 LFSR의 메모리에 저장되는 초기값을 모두 0이 아닌 임의의 값으로 변경한 후, 각각의 LFSR의 1비트를 저장하는 캐쉬메모리를 사용하여 상호클럭조절 함수를 구성하되, LFSR의 탭 길이가 가변클록의 횟수에 영향을 주게 되고, 가변클록의 횟수의 변화에 의해 선형복잡도가 증가하며 주기가 길어지는 것으로, 암호화된 긴 메시지를 사용하여 전달할 때, Berlekamp-Massey 알고리즘을 이용한 공격 등의 컴퓨터 공격에 대해서 안전하게 하는 현저한 효과가 있음

대표 도면



[양방향성 상호 클럭조절방식을 이용한 랜덤 이진수열 발생방법의 개념도]

기술의 작용

- 2개의 LFSR(100, 200)이 서로 상호작용하면서 클럭을 랜덤(Random)으로 조절하여 데이터를 획득하는 데이터획득 단계; 획득한 데이터를 논리회로부(300)에서 이진수열로 변환하여 발생시킨 후 최종 출력결과 를 획득하는 출력결과획득단계; 로 이루어짐
- 2개의 LFSR(100, 200)는 제1LFSR(100)과 제2LFSR(200)로 구분되되, 각각은 메인 메모리(110, 210)와, 1비트(bit)의 공간을 가지며 이전에 저장된 데이터를 담아두는 캐쉬 메모리(120, 220)로 이루어지되, 제1LFSR(100)와 제2LFSR(200)은 서로 다른 비트(bit)의 메인 메모리를 가지는 것이며, 2개의 LFSR(100, 200)는 초기에 초기화를 위한 초기화 단계를 실시하는 것으로, 초기화 단계에서 키(key)와 초기화 벡터(IV, Initialization Vector)로부터 내부상태가 채워지되, 각 데이터는 '0'아 아닌 임의의 값으로 채우고, 캐리함수와 메모리함수를 초기화하고, 이후 각각의 LFSR(100, 200)에서 임의의 2개 비트를 사용하여 상호클럭조절 함수를 적용함
- 내부상태의 길이가 키(key) 길이보다 더 길기 때문에, 키 확장을 하여 내부상태를 채우는 것이며, 가변클럭의 횟수를 임의의 지정된 횟수로 지정하여 사용하거나, 각각의 LFSR(100, 200)의 원시다항식을 변경하여 출력 순서를 변경하는 것으로, 안전성을 향상시킬 수 있음

적용 시장 DSU+

- 응용 소프트웨어 개발 및 공급업(KSIC 58222) 시장 – 컴퓨터에서 특정한 업무 처리를 위하여 기능 및 프로세스를 프로그램화 하여 자동적으로 처리하는 범용성의 응용 소프트웨어를 개발하는 산업활동을 말함. 인터넷, 휴대폰 및 PDA 등에 사용하는 모바일용 응용 소프트웨어를 개발·공급하는 산업활동도 포함
- 미국은 SW개발 및 공급업(5112) 시장

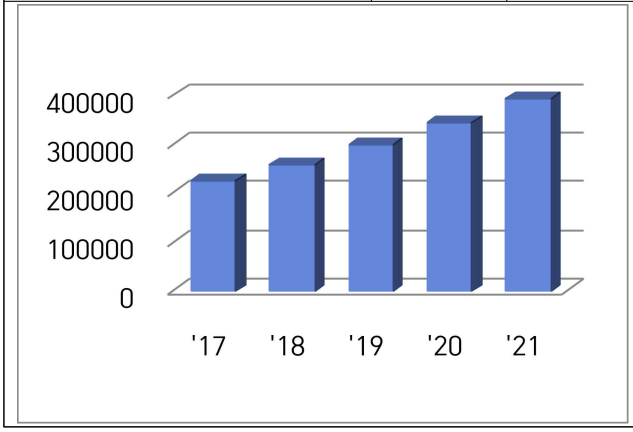
시장 규모

- SW개발 및 공급업(5112)의 미국 시장 규모는 2017년 224,400백만 달러에서 증가(CAGR 15%)되어, 2021년에는 392,300백만 달러에 달할 것으로 예측
- 응용 소프트웨어 개발 및 공급업(KSIC 58222)의 국내 시장 규모는 2017년 104,201억 원에서 증가(CAGR 2.9%)하여, 2021년에는 116,948억 원에 달할 것으로 예측

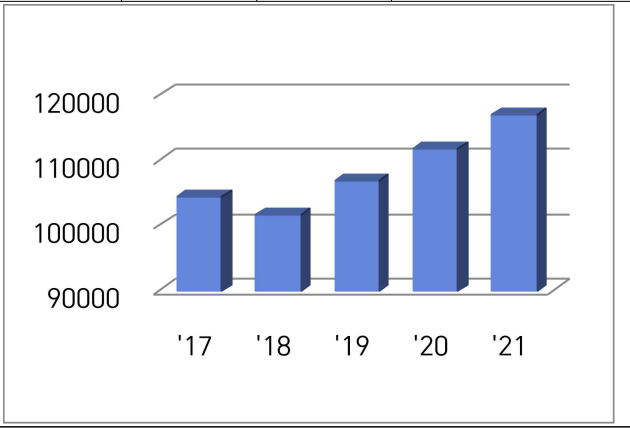
[표] 미국/국내 응용 소프트웨어 개발 및 공급업 분야의 시장규모 추이

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)	104,201	101,514	106,659	111,804	116,948	2.9%



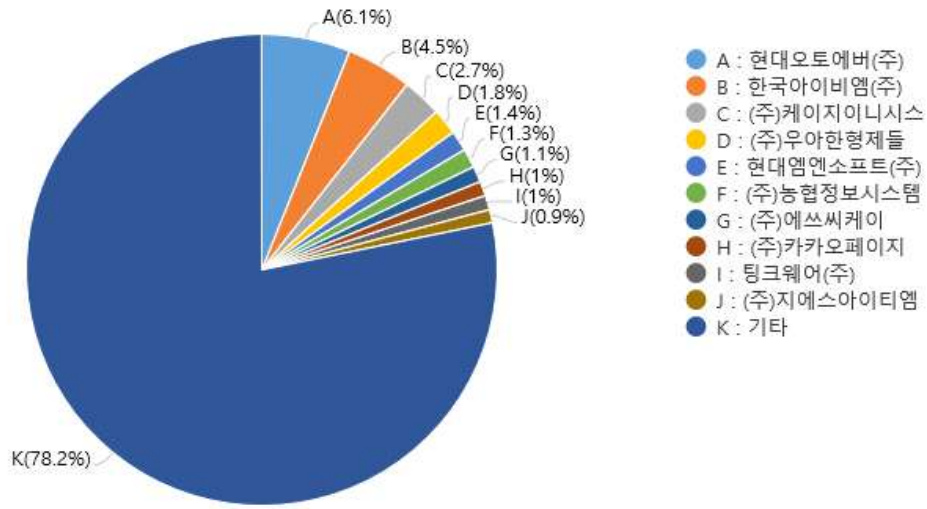
[미국 시장]



[국내 시장]

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

국내 시장 점유율



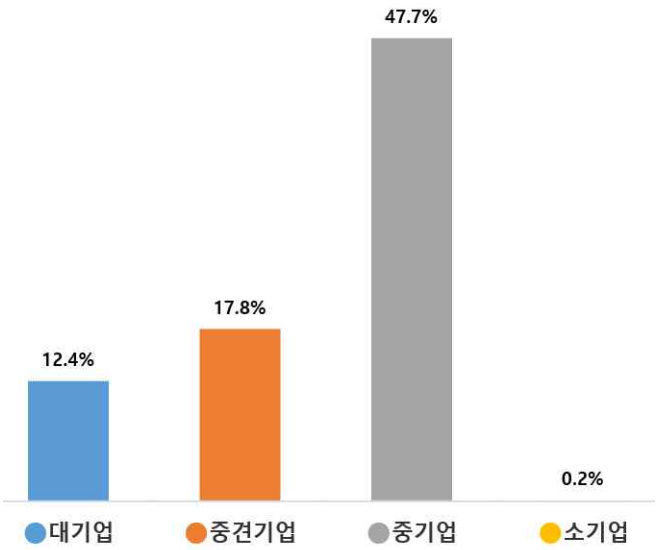
*출처: 한국과학기술정보연구원(2019, 2018년도 기준으로 작성)

시장 집중도

- 기업집중도를 보면, 응용 소프트웨어 개발 및 공급업(KSIC 58222) 시장에서 허핀달-허쉬만 지수(Herfindahl Hirschman Index, HHI. 시장집중도 측정방법으로 기업의 시장점유율의 제곱을 모두 합산한 지수)가 90이고, 상위 3대 기업 집중도(Concentration Ratio3, CR3. 시장점유율 1~3위 기업의 시장점유율의 합)는 13.3%를 차지하며 중소, 중견기업 매출 비중이 88%를 차지하는 시장으로 집중도가 낮은 시장에 해당함

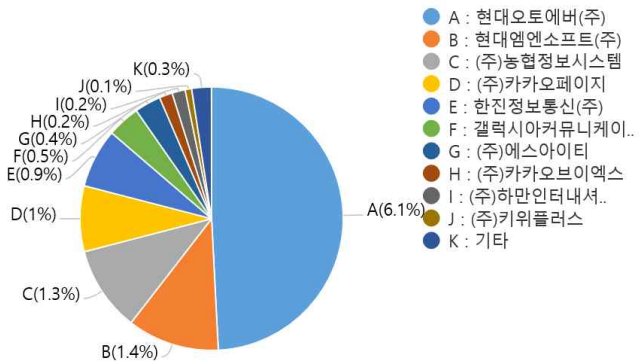
*출처: 한국과학기술정보연구원(2019)

규모별 시장 점유율



*출처: 한국과학기술정보연구원(2019)

중견기업 경쟁구조



*출처: 한국과학기술정보연구원(2019)

기술동향 DSU+

- 벌러캠프-매시(Berlekamp-Massey) 알고리즘은 주어진 수열을 만들 수 있는 가장 작은 선형 귀환 시프트 레지스터를 찾는 알고리즘임. 즉, 선형 점화식의 최소 다항식을 구하는 알고리즘임

국내외 기술 동향

- 본 기술은 Berlekamp-Massey 알고리즘을 이용한 공격 등의 컴퓨터 공격에 대해서 안전하게 함
- 또한 본 기술에서 사용하는 선형 되먹임 시프트 레지스터(Linear feedback shift register, LFSR)는 시프트 레지스터의 일종으로, 레지스터에 입력되는 값이 이전 상태 값들의 선형 함수로 계산되는 구조를 가지고 있음. 이때 사용되는 선형 함수는 주로 배타적 논리합(XOR)이다. LFSR의 초기 비트 값은 시드(seed)라고 부름
- LFSR의 동작은 결정론적이기 때문에, LFSR로 생성되는 값의 수열은 그 이전 값에 의해 결정됨. 또한, 레지스터가 가질 수 있는 값의 개수는 유한하기 때문에, 이 수열은 특정한 주기에 의해 반복됨. 하지만 선형 함수를 잘 선택한다면 주기가 길고 무작위적으로 보이는 수열을 생성할 수 있음
- LFSR는 의사 난수, 의사 난수 잡음(PRN), 빠른 디지털 카운터, 백지화 수열 등의 분야에서 사용됨
- LFSR는 하드웨어로 구현할 수 있고, 직접 시퀀스 확산 스펙트럼(DSSS) 무선같은, 매우 빠른 의사 난수 수열의 생성이 요구되는 응용에 유용하게 사용됨. 위성항법장치는 시간 보정과 관련된 고정밀 위치를 가리키는 수열을 신속하게 전송하기 위해서 LFSR을 사용함
- 또한 LFSR은 디지털 방송과 통신에서도 사용함.
- 그래서 분선 형태로부터 짧게 반복되는 수열(예시, 0이나 1의 흐름)을 방지하는 것은 수신기가 부호를 추적하는 것을 복잡하게 하거나 다른 전송을 방해할 것이며, 선형 되먹임 레지스터는 종종 전송된 비트 스트림을 "임의화"하는데 사용됨. 임의화는 복조후에 수신기에서 제거됨. LFSR이 전송하는 부호스트림과 동일한 속도로 실행될때, 이 기술은 스크램블러처럼 사용됨. LFSR이 부호스트림보다 상당히 빠르게 실행되면, 전송하는 신호의 대역폭이 증가되고, 이것이 DSSS(직접 시퀀스 확산 스펙트럼)임.

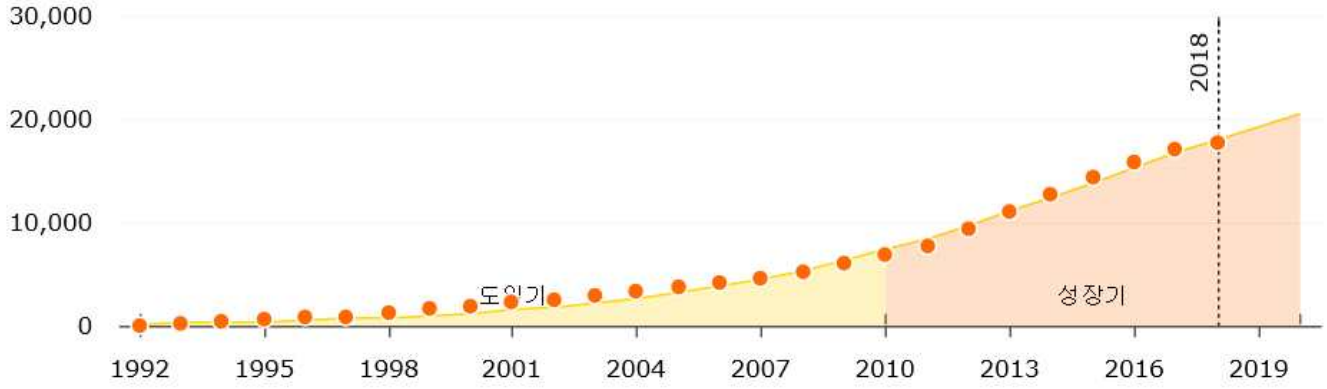
관련 기술의 미래 부상성

No.	Product family	K-Index	특허수	국내기업 점유율	기업 독점도	파급도	복합도	미래 부상성
1	IMAGE PROCESSING TERMINAL	80.66	9	22.22%	1,358.02	0	0.05	5.48
2	MEDICAL IMAGE PROCESSOR	97.38	178	1.12%	2,332.07	0	2.55	4.8
3	★IMAGE CAPTURE DEVICE	98.52	2,813	1.71%	130.37	17.49	65.32	4.43
4	IMAGE PROCESSING UNIT	98.16	676	4.73%	412.11	13.36	6.46	4.41
5	IMAGE PROCESSING TOOL	80.78	10	0.00%	1,400.00	0	0.01	4.18
6	IMAGE PROCESSING COMPONENT	79.31	9	0.00%	1,358.02	0.12	0.04	4.06
7	IMAGE PROCESSOR	98.02	17,808	3.85%	864.18	30.24	213.12	4.02
8	IMAGE PROCESSING FILTER	76.92	8	0.00%	1,250.00	0	0.06	3.62
9	DIGITAL IMAGE PROCESSOR	94.12	193	47.67%	1,550.91	0.29	4.77	3.18
10	IMAGE SIGNAL PROCESSOR	94.36	413	15.74%	759.25	0.78	12.06	3.02

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

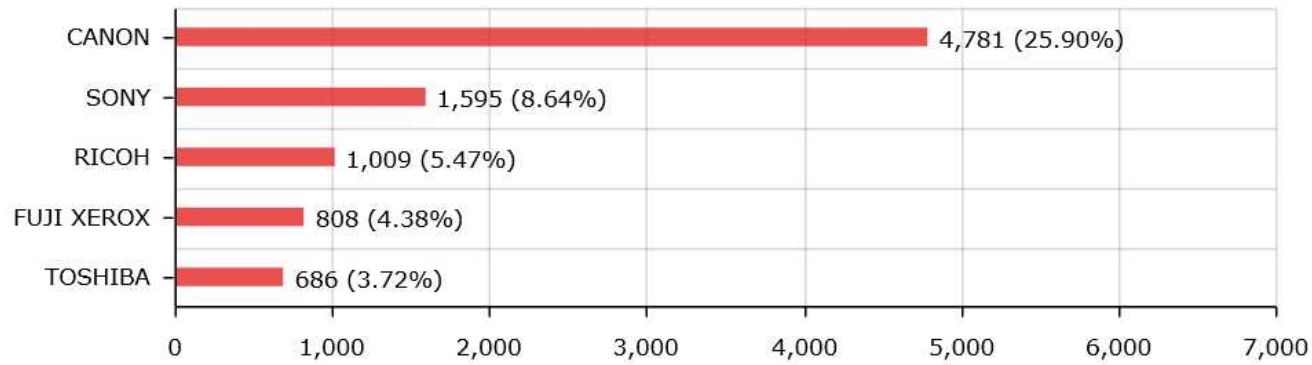
★는 KISTI 선정 'TOP 2000 부상제품'

주요 Product family인 IMAGE PROCESSOR 분야의 특허수 성장성 예측



*출처: 한국과학기술정보연구원(2019), TOD

주요 Product family인 IMAGE PROCESSOR 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