2021/08/18, 2021 보안 심화 세미나

암호학과 네트워크 보안

- 1, 4부 서론, 암호 수학 -

우 승 찬(seungchan@pel.sejong.ac.kr)

세종대학교 프로토콜공학연구실

목 차

- 서론
- 암호 수학
  - 대수 구조
  - GF(2^n) 체

목 차

- 서론
- 암호 수학
  - 대수 구조
  - GF(2^n) 체

서론

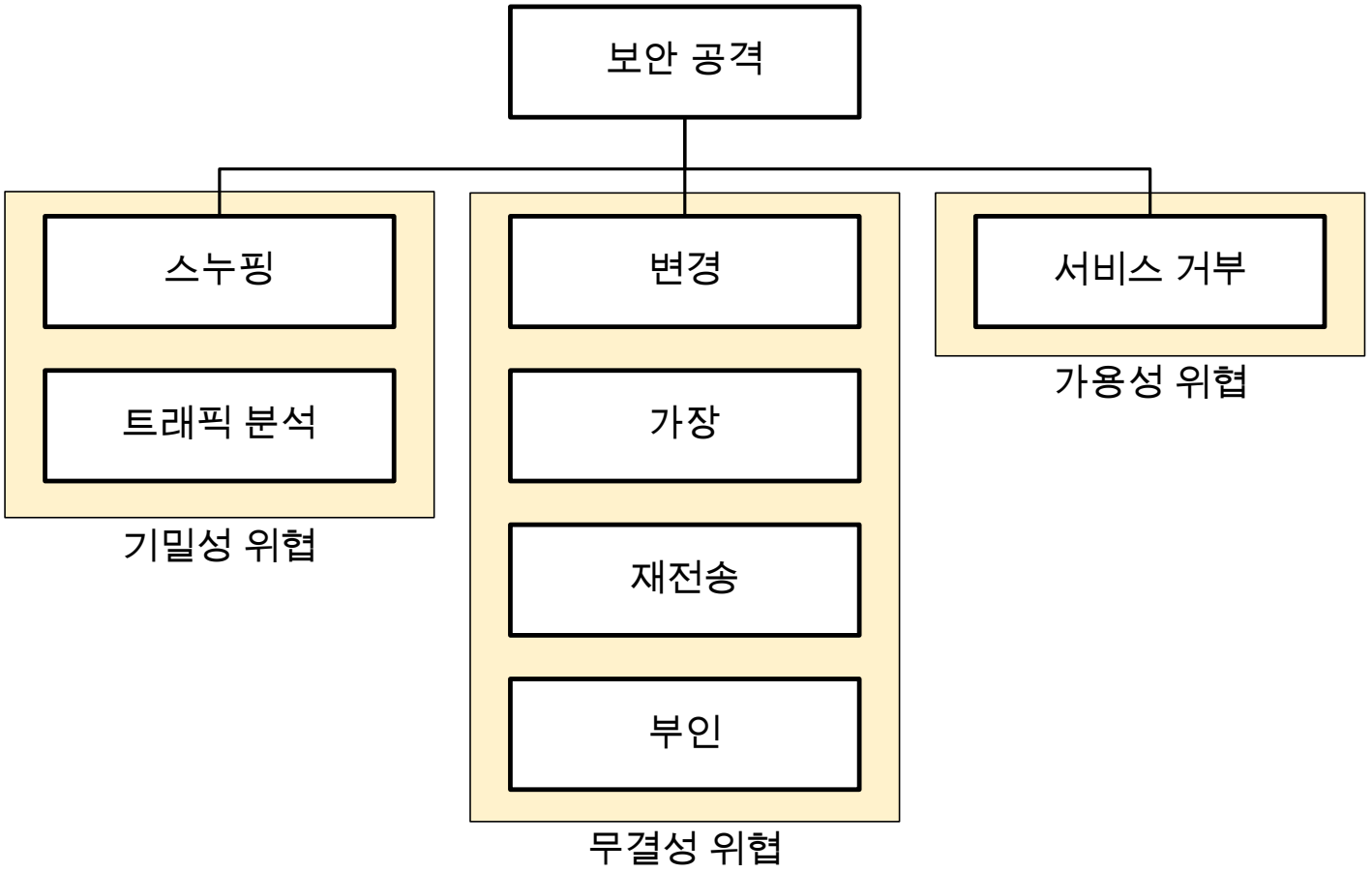
- 개요
  - 정보를 안전하게 보호하기 위해서는 보안 목표를 만족해야 한다.
  - 보안 목표
    - 기밀성, 무결성, 기용성

서론

- 보안 목표
  - 기밀성(Confidentiality)
    - 정보를 오직 인가된 사람들에게만 공개하는 것
      - 전송되는 데이터의 내용을 보호하여, 비인가자가 정보의 실제 내용에 접근하는 것을 방지함
  - 무결성(Integrity)
    - 정보가 변조되지 않고 그대로 전달되는 것
      - 데이터가 제3자에 의해 중간에 변조하는 것을 방지함
  - 가용성(Availability)
    - 정보를 인가된 자가 사용할 수 있도록 하는 것

서론

- 공격(Attack)
  - 보안의 세 가지 목표는 보안 공격에 의해서 위협받음



서론

- 공격(Attack)
  - 기밀성을 위협하는 공격
    - 스누핑(Snooping)
      - 데이터에 대한 비인가 접근하거나 탈취하는 것
        - e.g., 기밀 정보를 가지고 있는 메시지 탈취
    - 트래픽 분석(Traffic Analysis)
      - 암호화된 데이터의 트래픽을 분석함으로써 다른 형태의 정보를 얻는 것
        - e.g., 수신자와 송신자의 전자 주소를 알아내어 전송 성향을 추측하는데 도움이 되는 질의 응답 쌍 수집

서론

- 공격(Attack)
  - 무결성을 위협하는 공격
    - 변경(Modification)
      - 공격자가 정보를 획득한 후 자신에게 유리하도록 정보를 조작하는 것
    - 가장(Masquerading)
      - 공격자가 사용자로 위장을 하거나 공격자가 수신자로 위장하는 것
    - 재전송(Replaying)
      - 공격자가 사용자가 보낸 메시지 사본을 획득하고 다시 보내는 것
    - 부인(Repudiation)
      - 송신자가 메시지를 보냈다는 것을 부인하거나 수신자가 메시지를 받았다는 것을 부인하는 것

서론

- 공격(Attack)
  - 가용성을 위협하는 공격
    - 서비스 거부(DoS, Denial of Service)
      - 매우 일반적인 공격
      - 시스템의 서비스를 느리게 하거나 완전히 차단시키는 공격
      - 대량의 데이터 패킷을 통신망으로 보내 과부하를 일으킴
    - 분산 서비스 거부(DDoS,Distributed DoS)
      - 공격자를 분삭적으로 배치해 동시에 서비스 거부 공격을 하는 방법

서론

- 공격(Attack)
  - 공격은 소극적(Passive) 공격과 적극적(Active)공격이라는 두 그룹으로 분류함
    - 소극적 공격
      - 공격자의 목표는 단지 정보를 획득하는 것
      - 공격자가 데이터를 변경하거나 시스템에 해를 끼치지 않음
      - 공격을 탐지하기 힘들지만 암호화에 의해 막을 수 있음
    - 적극적 공격
      - 데이터를 바꾸거나 시스템에 해를 입힘
      - 공격자가 다양한 방법들을 사용하기 때문에 방어하기보다는 탐지하기가 쉬움

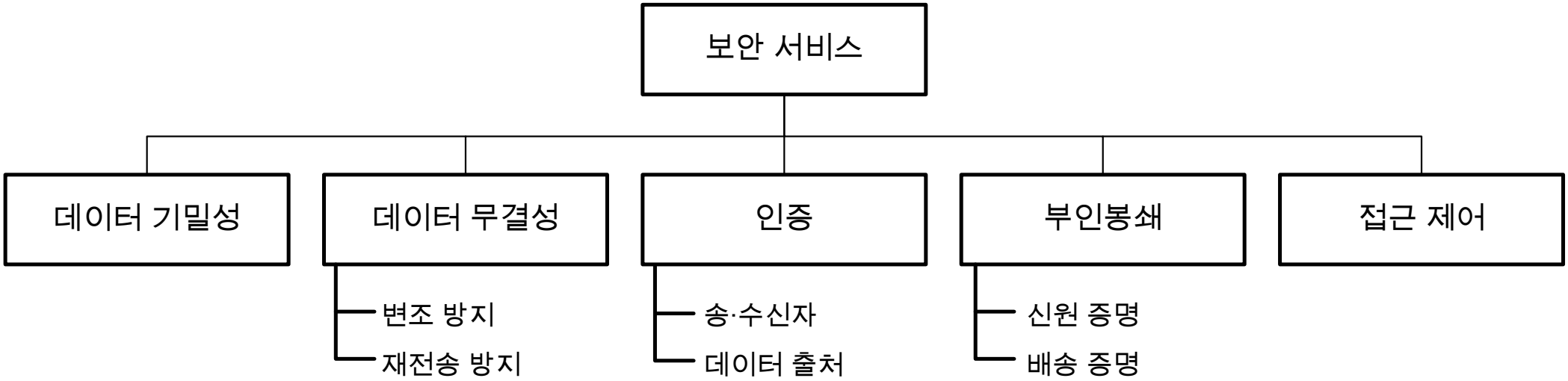
서론

- 소극적 공격과 적극적 공격

공격	적극성	위협
스누핑	소극적 공격	기밀성
트래픽 분석		
변경	적극적 공격	무결성
가장		
재전송		
부인		
서비스 거부	적극적 공격	가용성

서론

- 서비스와 메커니즘
  - 국제 통신 연합-통신표준화부문(ITU-T)에서 보안 서비스와 보안 메커니즘을 제시하였다.
  - 보안 서비스



서론

- 서비스와 메커니즘
  - 보안 서비스(1/2)
    - 데이터 기밀성(Data Confidentiality)
      - 노출 공격으로부터 데이터를 보호하기 위함
      - 메시지의 일부분이나 전체에 대한 기밀성을 포함
    - 데이터 무결성(Data Integrity)
      - 무결성을 위협하는 공격으로부터 메시지의 일부나 전부를 보호
    - 인증(Authentication)
      - 통신의 상대편에 대한 인증을 제공함
      - 연결형 통신에서 연결 설정 시 송신자 또는 수신자에 대한 인증
      - 비연결형 통신에서 데이터의 출처를 인증

서론

- 서비스와 메커니즘
  - 보안 서비스(2/2)
    - 부인봉쇄(Nonrepudiation)
      - 데이터의 송신자나 수신자가 부인하지 못하도록 함
      - 메시지가 잘 배송되었다는 증명을 제공함
    - 접근 제어(Access Control)
      - 비인가된 접근으로부터 데이터를 보호함
      - 일기, 쓰기, 프로그램 실행 등을 포함

서론

- 서비스와 메커니즘
  - 보안 메커니즘(1/2)
    - 암호화
      - 데이터를 숨기거나 보호하여 기밀성을 제공함
      - 암호와 스테가노그래피 기술을 이용
    - 데이터 무결성
      - 데이터에 데이터를 검사하는 값을 추가하고 그 검사 값이 같을, 때 데이터 무경성이 보장됨
    - 디지털 서명
      - 송신자가 데이터에 서명을 하고 수신자가 그 서명을 검증하는 방법
    - 인증 교환
      - 자신의 신원을 다른 사람에게 증명하기 위하여 메시지를 교환함

서론

- 서비스와 메커니즘
  - 보안 메커니즘(2/2)
    - 트래픽 패딩
      - 공격자가 트래픽 분석을 하지 못하도록 트래픽에 가짜 데이터를 삽입
    - 라우팅 제어
      - 공격자가 특정 경로에서 도청하지 못하도록 다른 경로를 선택하고 지속적으로 변화시켜줌
    - 공증
      - 두 사람 사이의 통신을 제어하기 위하여 신뢰할 수 있는 제 3자를 선택하는 것
      - 부인봉쇄에 사용됨
    - 접근 제어
      - 사용자가 시스템의 데이터나 데이터 출처에 대한 접근권을 가지는지 여부를 입증하기 위한 방법을 사용함
      - 패스워드, PIN

서론

- 서비스와 메커니즘
  - 서비스와 메커니즘의 관계

보안 서비스	보안 메커니즘
데이터 기밀성	암호화, 라우팅 제어
데이터 무결성	암호화, 디지털 서명, 데이터 무결성 메커니즘
인증	암호화, 디지털 서명, 인증 교환
부인봉쇄	디지털 서명, 데이터 무결성 메커니즘, 공증
접근 제어	접근 제어 메커니즘

서론

- 암호(Cryptography)
  - 대칭 키 암호화(Symmentric key Encipherment)
    - 암호화 하는 측과 복호화 하는 측이 하나의 암호 키를 사용함
  - 공개 키 암호화(Public key Encipherment)
    - 하나의 키 대신 두개의 키 쌍, 즉 공개 키(Public-key)와 개인 키(Private-key)를 사용함
    - 공개 키를 통하여 암호화를 하고 복호화는 개인 키를 사용함
  - 해싱(Hashing)
    - 키 값을 해시 함수(Hash Function)라는 수식에 대입시켜 계산하여 압축함
    - 데이터베이스 내의 항목들을 색인하고 검색하는데 사용

서론

- 스테가노그래피(Steganography)
  - 메시지를 다른 것으로 덮어서 감추는 것
  - 역사적 사용
    - 보이지 않는 잉크를 이용하여 메시지 행간이나 종이의 뒷면에 비밀 메시지를 적음
      - e.g., 양파 주스, 암모니아 소금
    - 일정 각도의 빛에 노출될 때 메시지가 나오도록 함
    - 무의미한 단순에서 각 단어의 첫 번째 또는 두 번째 문자가 비밀 메시지를 구성함
      - e.g., 세로드립

서론

- 스테가노그래피(Steganography)
  - 현대의 사용(1/2)
    - 텍스트 커버(Text Cover)
      - 텍스트를 이용하여 데이터를 숨김
      - e.g., A(0100001), HI(01001000 01001001)

This book is mostly about cryptography, not steganography

□ □□ □ □ □ □ □□

0 1 0 0 0 0 1

A friend called a doctor

0 10010 0001 0 01001

서론

- 스테가노그래피(Steganography)
  - 현대의 사용(2/2)
    - 이미지 커버(Image Cover)
      - 컬러 이미지 안에 데이터를 숨기는 것
      - 디지털 이미지는 3바이트의 픽셀로 구성됨
        - 빛의 삼원색(빨강, 녹색, 파랑)이 1바이트씩 표현
      - e.g., M

01010011	10111100	01010101
01011110	10111100	01100101
01111110	01001010	00010101

    - 다른 커버
      - 오디오나 비디오 안에도 데이터를 숨길 수 있음

서론

- 책의 구성
  - Part 1: 대칭-키 암호화
    - 대칭-키 암호를 사용한 고전 및 현대 암호들을 다룸
  - Part 2: 비대칭-키 암호화
    - 비대칭-키 암호, 즉 공개-키 암호를 이용한 암호화를 논함
  - Part 3: 무결성, 인증 및 키 관리
    - 해싱에 대해서 소개하며 무결성을 보장하기 위해 어떻게 암호화 방법들과 결합하는지 소개
  - Part 4: 네트워크 보안
    - 네트워크 보안을 달성하기 위해 앞서 소개한 방법들이 어떻게 결합되는 지 보여줌

목 차

- 서론
- 암호 수학
  - 대수 구조
  - GF(2^n) 체

암호 수학

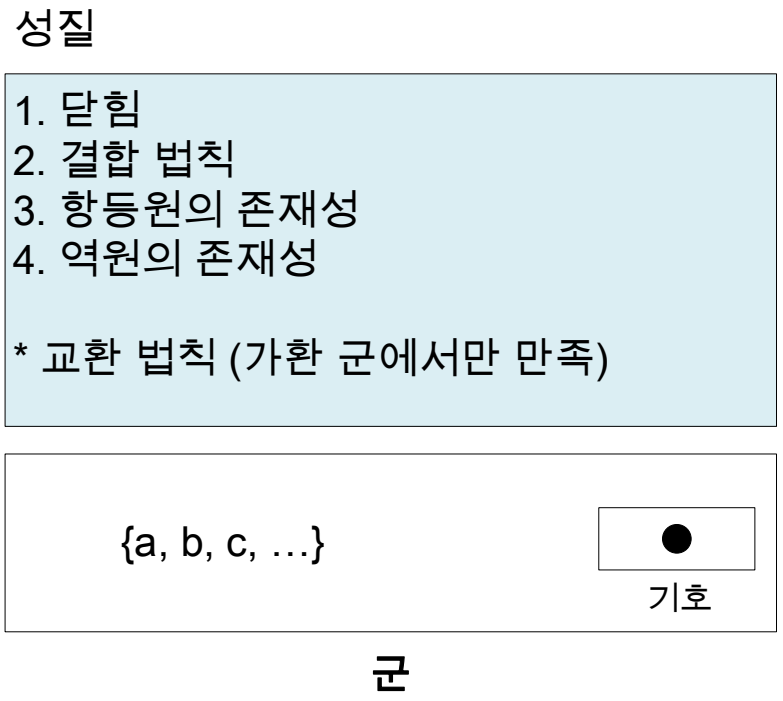
- 대수 구조(Algebraic Structure)
  - 집합과 집합에 포함된 원소들에 적용되는 연산
  - 일반적인 대수 구조

대수 구조

- 군(G, group)
  - 정의
    - 네 개의 성질을 만족하고 이항 연산 “•”이 정의된 원소들의 집합
  - 성질
    - 닫힘
      - 만약 a와 b가 G의 원소라면 $c = a \cdot b$ 또한 G의 원소
    - 결합 법칙
      - 만약 a, b, c가 G의 원소라면, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ 를 만족
    - 항등원의 존재성
      - G의 임의의 두 원수 a, b에 대하여, $e \cdot a = a \cdot e = a$ 를 만족하는 항등원(Identity element) e가 존재
    - 역원의 존재성
      - G의 원소 a에 대하여, $a \cdot a' = a' \cdot a = e$ 를 만족하는 a의 역원(Inverse)a' 존재

대수 구조

- 군(G, group)
  - 가환 군(Commutative group)
    - 군의 네 개의 성질에 교환 법칙을 추가로 만족하는 군
      - 교환 법칙
        - G의 임의의 두 원소 a, b에 대하여, $a \cdot b = b \cdot a$ 를 만족



대수 구조

- 군(G, group)
  - 응용
    - 덧셈 연산이 정의된 집합 G = $< Z_n, + >$ 는 가환 군임
      - 이 군은 새로운 원소를 추가하지 않고 덧셈과 뺄셈 모두 사용
    - 확인

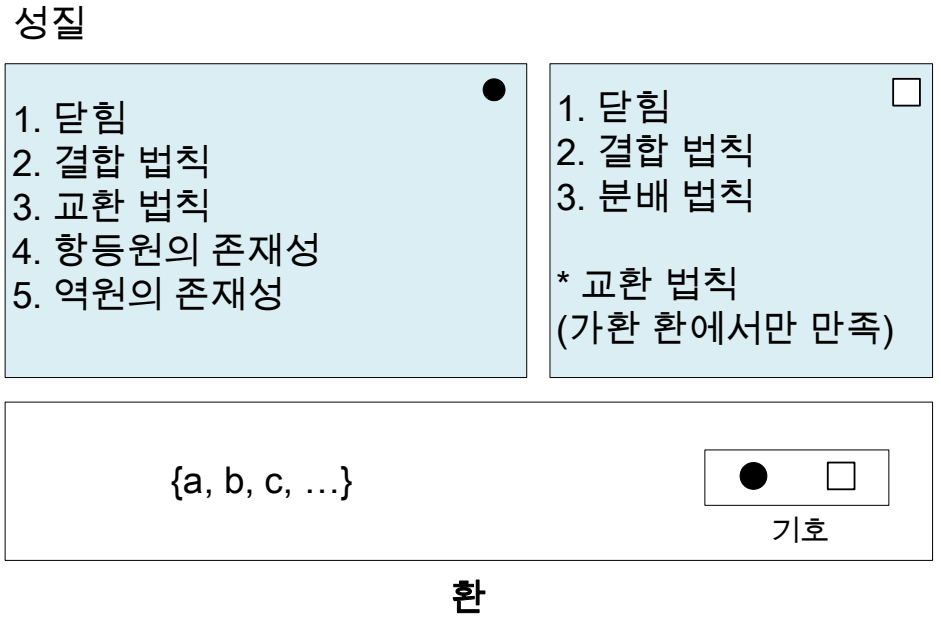
1. 집합은 연산에 대해 닫혀있음
   Z_n의 두 원소에 대한 합은 Z_n의 다른 값임
2. 결합 법칙을 만족함 e.g., 4+(3+2)=(4+3)+2
3. 교환 법칙을 만족함 e.g., 3+5=5+3
4. 항등원이 0으로 존재함 e.g., 3+0=0+3=3
5. 모든 원소는 덧셈에 대한 역원을 가짐
   이 역원으로 뺄셈 사용 가능
   e.g., 3의 역원은 -3이고 -3의 역원은 3임

대수 구조

- 군(G, group)
  - 군의 종류
    - 유한 군(Finite group)
      - 유한 개의 원소를 갖고 있음
    - 무한 군(Infinite group)
      - 무한 개의 원소를 갖고 있음
  - 군의 위수(Order)
    - 군에 있는 원소의 개수

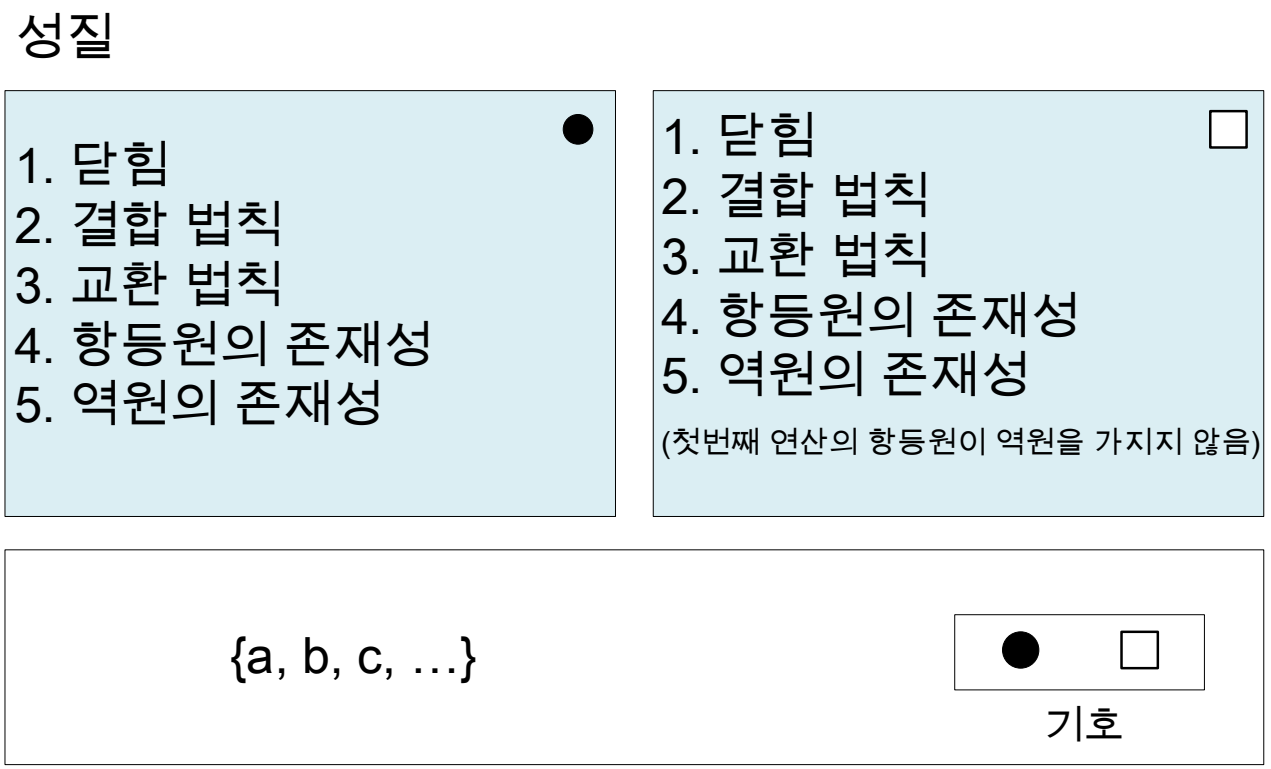
대수 구조

- 환(R, ring)
  - 두 개의 연산이 정의된 대수 구조 R = <{…},•, □> 로 표기
    - 첫 번째 연산은 가환 군에 요구되는 다섯 개 성질 만족
    - 두 번째 연산은 닫힘과 결합법칙을 만족하고 추가로 분배법칙을 만족함
    - 가환 환(Commutative ring)
      - 두 번째 연산에 교환 법칙까지 만족하는 환



대수 구조

- 체(F, field)
  - 특별한 두개의 성질을 만족하는 가환 환
  - F = <{…},•, □> 로 표기됨



대수 구조

- 체(F, field)
  - 유한 체(Finite field)
    - 유한개의 원소를 갖는 체
    - 유한 체가 암호에서 매우 중요한 구조
    - 유한개의 원소를 갖는 체의 원소의 개수는 P^n임
      - P는 소수, n은 양의 정수
    - 유한체는 보통 갈로아 체(Galois field)라고 불리고 GF(P^n)으로 표현됨

대수 구조

- 체(F, field)
  - GF(P)체
    - n이 1일 때의 갈로아 체
  - GF(2)체
    - 현재 암호에서 가장 널리 쓰이는 체이다.

GF(2)

{0.1} × +

+	0	1
0	0	1
1	1	0

Addition

XOR 연산

×	0	1
0	0	0
1	0	1

Multiplication

AND 연산

a	0	1
-a	1	0

a	0	1
a^{-1}	—	0

Inverses

대수 구조

- 정리
  - 군, 환, 체 세 대수 구조는 덧셈/뺄셈, 곱셈/나눗셈과 같은 비슷한 연산이 정의된 집합들을 사용할 수 있게 해준다.

대수 구조	사용하는 일반적인 기호	사용하는 일반적인 정수 집합
군(group)	(+ -) or (× ÷)	Z_n or Z_n*
환(ring)	(+ -) and (×)	Z
체(field)	(+ -) and (× ÷)	Z_p

목 차

- 서론
- 암호 수학
  - 대수 구조
  - GF(2^n) 체

GF(2^n)체

- GF(2^n)체
  - 암호학에서는 사칙연산(+ - × ÷) 이 모두 필요함
    즉, 암호학에서는 체를 사용
  - 컴퓨터로 연산을 할 때, 양의 정수들은 컴퓨터에 n-비트 워드로 저장됨
    - n은 보통 8, 16, 32, 64
  - 정수들의 범위는 0에서 $2^n - 1$이므로 모듈러는 2^n임

GF(2^n)체

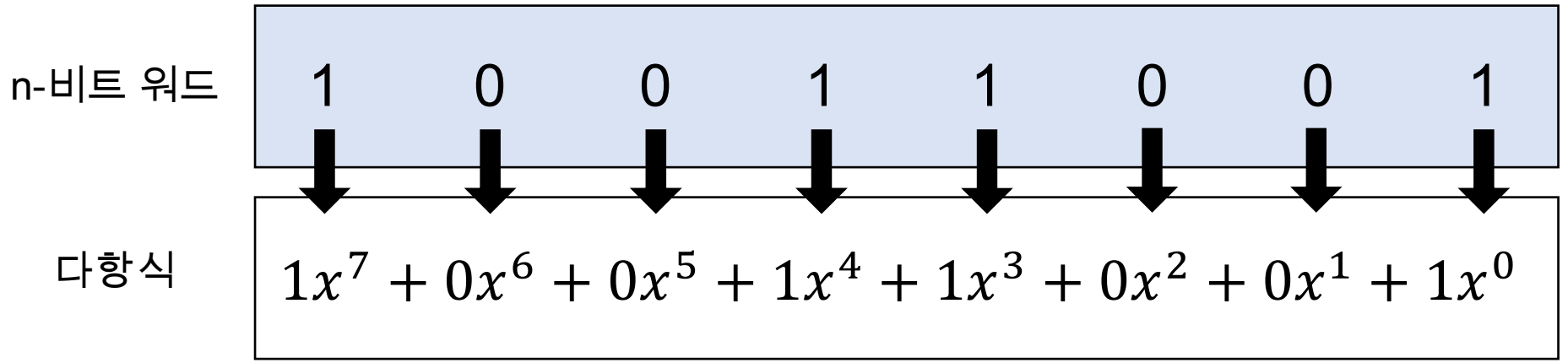
- 다항식
  - n-비트 워드들 위에서 GF(2^n)의 모든 성질들을 만족하는 연산 규칙을 정의할 수 있음
  - 차수 $n-1$의 다항식 형태로 표현하면 더욱 간단함.

$$f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x^1 + a_0x^0$$

  - n-비트 워드들을 다항식으로 표현하기 위한 규칙
    - x의 지수승은 n-비트 워드에서 비트들의 위치를 정의함
    - 항들의 계수는 비트들의 값으로써 정의됨
      - 비트는 0과 1의 값을 갖기 때문에 다항식의 계수는 0 또는 1임

GF(2^n)체

- 다항식
  - 예제



첫 번째 단순화

$$1x^7 + 1x^4 + 1x^3 + 1x^0$$

두 번째 단순화

$$x^7 + x^4 + x^3 + 1$$

GF(2^n)체

- 다항식
  - 연산
    - n-비트 워드들을 표현하는 다항식들은 두 개의 체 GF(2)와 GF(2^n)을 사용함
  - 모듈로
    - 두 다항식의 덧셈은 결코 그 집합에 속하지 않는 다항식을 생성하지 않음
    - 두 다항식의 곱셈은 n-1보다 큰 차수를 가지는 다항식을 생성할 수도 있음
      - 모듈로 논리에 따라 모듈로 다항식으로 나누고 나머지만 생각함

GF(2^n)체

- 다항식
  - 모듈로
    - 기약 다항식(Irreducible Polynomial)
      - 모듈로로써 정의되는 어떤 다항식으로도 나눌 수 없는 소수 다항식

차수	기약 다항식
1	$(x+1), (x)$
2	(x^2+x+1)
3	$(x^3+x^2+1), (x^3+x+1)$
4	$(x^4+x^3+x^2+x+1), (x^4+x^3+1), (x^4+x+1)$
5	$(x^5+x^2+1), (x^5+x^3+x^2+x+1), (x^5+x^4+x^3+x+1),$ $(x^5+x^4+x^3+x^2+1), (x^5+x^4+x^2+x+1)$

GF(2^n)체

- 다항식
  - 덧셈

$1x^7 + 0x^6 + 1x^5 + 0x^4 + 0x^3 + 1x^2 + 1x^1 + 0x^0$ ✚ (+는 XOR연산임)

$0x^7 + 0x^6 + 0x^5 + 0x^4 + 1x^3 + 1x^2 + 0x^1 + 1x^0$

$0x^7 + 0x^6 + 1x^5 + 0x^4 + 1x^3 + 1x^2 + 0x^1 + 1x^0$ → $x^5 + x^3 + x^1 + 1$

  - 덧셈에 대한 항등원
    - 다항식 자신을 더하는 것은 0의 다항식을 만듬
      - 덧셈에 대한 항등원은 0의 다항식임
  - 덧셈에 대한 역원
    - GF(2)에서 계수를 가지는 다항식의 덧셈의 역원은 자기 자신임
      - 따라서 다항식의 덧셈과 뺄셈 연산은 같은 연산임

GF(2^n)체

- 다항식
  - 곱셈
    - 기약다항식을 이용하여 차수를 줄어줌
    - 다항식 GF(2^5), 기약 다항식 $x^5 + x^2 + 1$
      - $(x^4 + x^3 + 1) \times (x^3 + x^2 + 1) =$
      - $x^4(x^3 + x^2 + 1) + x^3(x^3 + x^2 + 1) + (x^3 + x^2 + 1) =$
      - $x^7 + x^6 + x^4 + x^6 + x^5 + x^3 + x^3 + x^2 + 1 =$
      - $x^7 + x^5 + x^4 + x^2 + 1 =$
      - $(x^7 + x^5 + x^4 + x^2 + 1)\ mod\ (x^5 + x^2 + 1) =$
      - x^2
    - 곱셈에 대한 항등원
      - 항상 1임
    - 곱셈에 대한 역원
      - 두 다항식을 곱한 결과에 모듈로를 취했을 때의 나머지를 구함

GF(2^n)체

- 뺄셈
  - 덧셈과 뺄셈은 같은 연산임
- 나눗셈
  - 나눗셈은 곱셈 역원을 사용한 곱셈
- 정리
  - 유한체 GF(2^n)은 n-비트 워드들에 대한 덧셈, 뺄셈, 곱셈, 나눗셈의 네 개의 연산들을 정의하기 위해 사용될 수 있음

Thanks!

우 승 찬 (seungchan@pel.sejong.ac.kr)