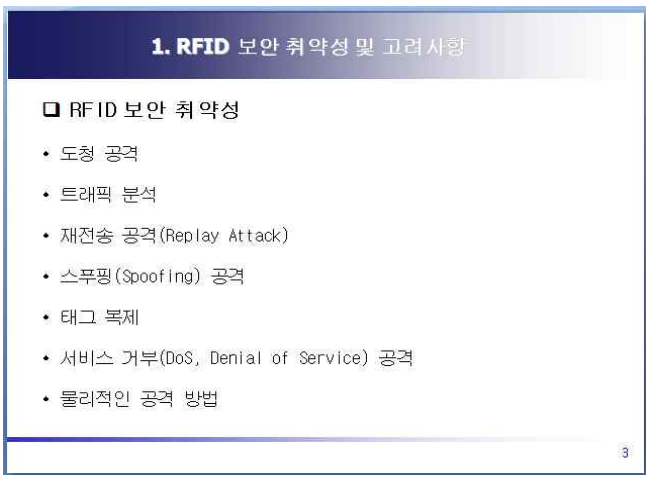
RFID 보안 알고리즘 동향 분석

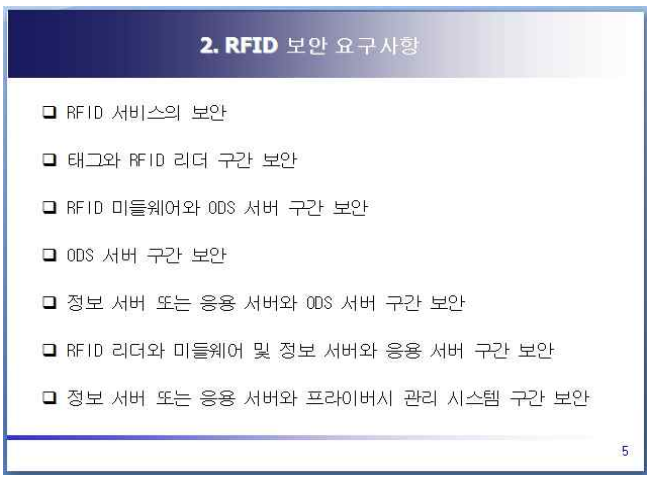
† 박 두진

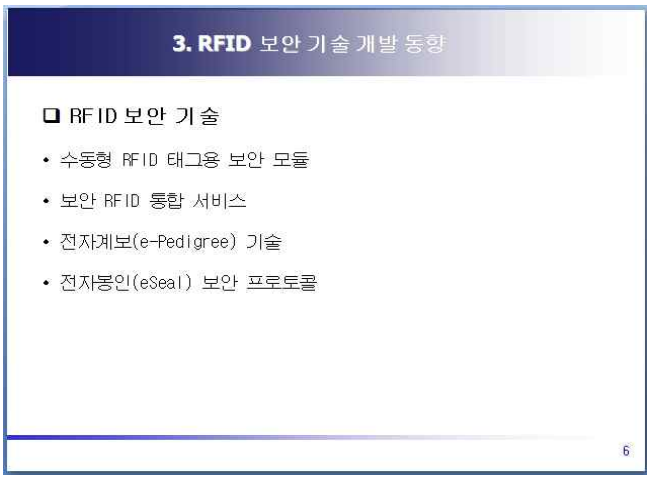
† 동명대학교 중소기업직업훈련컨소시엄사업단 팀장

요 약 : 다양한 물류분야에 적용되는 RFID 기술이 보다 확산되기 위해서는 RFID 의 정보의 보안이 선행되어야 한다. 본 발표에서는 RFID 기술의 보안의 취약성과 이를 해결할 수 있는 보안 요구사항을 분석하였다. 또한 RFID 보안 기술과 보안 알고리즘 동향을 분석하였다.

핵심용어 : RFID, 보안, 알고리즘, 메모리맵







† 교신저자 정회원) djpark@tu.ac.kr

3. RFID 보안 기술 개발 동향

❑ 모바일 RFID 보안 기술

- 모바일 RFID 정보보호 통합 프레임워크
- 모바일 RFID 보안 라이브러리
- 모바일 RFID 보안 미들웨어
- 모바일 WIPI 확장 보안 미들웨어 기술
- 모바일 RFID 프라이버시 보호 서비스
- 보안 응용 포탈 게이트웨이 기술
- 정책 프로파일 기반 개인 프라이버시 보호 기술

4. RFID 보안 알고리즘동향

❑ RFID 태그와 리더간 보안 알고리즘

- 태그와 리드간 도청 방지 기법
  - 트리워킹 알고리즘
  - 난수적 트리워킹 알고리즘
- 태그와 리더간 인정 기법
  - 해쉬락 기법
  - 비대칭키 동의(Asymmetry Key Agreement) 기법

4. RFID 보안 알고리즘동향

❑ 트리기반 RFID 보안 알고리즘

- TW (Tree-walking) 알고리즘
- QT (Query Tree) 알고리즘
- AQT (Advanced Query Tree) 알고리즘

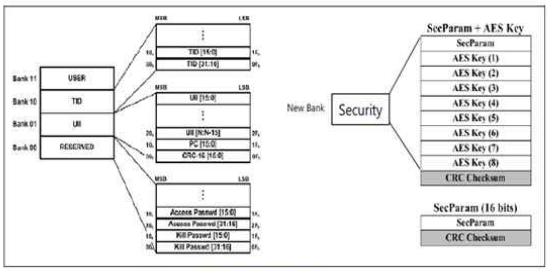
4. RFID 보안 알고리즘동향

❑ 수동형 RFID 태그와 리더 보안 알고리즘

- 수동형 RFID 태그 메모리맵 정보
- 수동형 RFID 보안 명령/응답 메시지
- 수동형 RFID 보안 프로토콜 동작

4. RFID 보안 알고리즘동향

• 수동형 RFID 태그 메모리맵 정보



수동형 RFID 보안태그 메모리맵 구조

4. RFID 보안 알고리즘동향

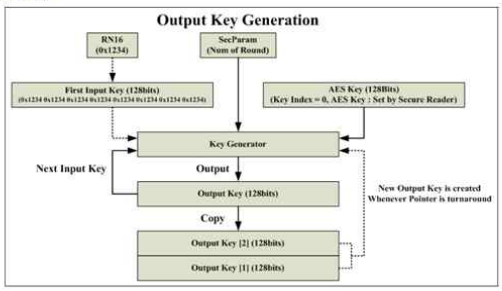
• SecParam

Bit	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
SecParam	SF	KS	RFU[0:1]		Round [0:3]				Key Index [0:7] (EBV)							

- SF(Secure Function) 비트
- KS(Key Setting) 비트
- Round[0:3]
- Key Index[0:7]

4. RFID 보안 알고리즘동향

• **AESKey**



세션 키 생성 방법

13

4. RFID 보안 알고리즘동향

• **ACK 명령의 태그 보안 응답 메시지**

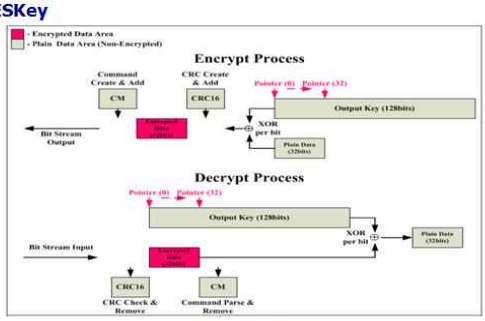
Ack 명령에 따른 기존 응답

Ack 명령에 따른 보안 응답

16

4. RFID 보안 알고리즘동향

• **AESKey**

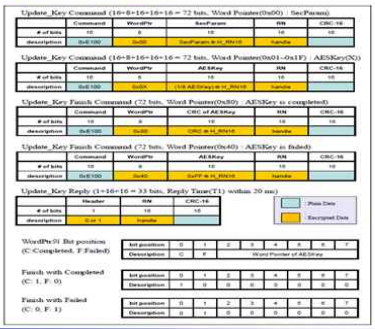


암호화 / 복호화 방법

14

4. RFID 보안 알고리즘동향

• **Update_Key 명령/응답 메시지**



17

4. RFID 보안 알고리즘동향

• **수동형 RFID 보안 명령/응답 메시지**

- ACK 명령의 태그 보안 응답 메시지
- Update_Key 명령과 응답 메시지
- Get_SecParam 명령과 응답 메시지
- Sec_ReqRN 명령과 응답 메시지
- Req_Auth 명령과 응답 메시지

15

4. RFID 보안 알고리즘동향

• **Get_SecParam 명령/응답 메시지**

Get_SecParam Command (16+16+16 = 48 bits)

	Command	RN	CRC-16
# of bits	16	16	16
description	0xE101	handle	

: Plain Data
: Encrypted Data

Get_SecParam Reply (1+16+16+16 = 49 bits)

	Header	SecParam	RN	CRC-16
# of bits	1	16	16	16
description	0 or 1	SecParam	handle	

18

4. RFID 보안 알고리즘 동향

• **Sec_ReqRN** 명령/응답 메시지

Sec_ReqRN Command (16+16+16+16 = 64 bits)

	Command	Challenge	RN	CRC-16
# of bits	16	16	16	16
description	0xE102	RN16	handle	

Sec_ReqRN reply (16+16+16 = 48 bits)

	Challenge	RN	CRC-16
# of bits	16	16	16
description	RN16	handle	

: Plain Data

: Encrypted Data

19

4. RFID 보안 알고리즘 동향

• **Req_Auth** 명령과 응답 메시지

Req_Auth Command (16+16+16 = 48 bits)

	Command	Handle	CRC-16
# of bits	16	16	16
description	0xE103	Encrypted newRN16	

Req_Auth reply (16+16 = 32 bits)

	Auth_data	CRC-16
# of bits	16	16
description	Ch16 ⊕ newRN16	

: Plain Data

: Encrypted Data

20