김일성종합대학학보
수 학

주체109(2020)년
제66권 제1호

비공개성을 보장하는 RFID인증체계의 한가지 모형

김 철 은

론문에서는 최근에 신분확인수단으로 널리 리용되는 RFID태그에 기초한 다양한 인증체계(RFID인증체계)를 보다 정확히 모형화할수 있는 한가지 수학적모형을 연구하였다.

RFID인증체계에 대한 연구에서는 체계가 여러개의 태그들과 1개의 태그읽기장치로 이루어지고 RFID인증규약은 개별적인 태그와 읽기장치사이의 2실체인증규약으로 간주해도 일반성을 잃지 않는다.[6, 8]

RFID인증체계는 완전성(정확성)과 믿음성(안전성), 비공개성을 갖추어야 한다.[1, 7]

선행연구[2]에서는 처음으로 《구별불가능성》에 기초하여 RFID체계의 비공개성(privacy)에 대한 엄밀한 정의를 갖춘 RFID체계모형(Avoine모형)을 제기하였다. Avoine모형은 선행연구[3, 6]에서 일반화되였다.

선행연구[7]에서는 《모의가능성》에 의거한 비공개성과 완전성, 믿음성개념까지 갖춘 비교적 《성숙된》 체계모형(V07모형)을 제기하였다. V07모형은 선행연구[1, 2] 등에서 확장, 개선되였다. 이 모형들에서는 일련의 본질적인 결함[4, 8]들이 제기되였다.

한편 선행연구[5]에서는 《구별불가능성》에 기초한 선행연구결과를 개선하여 새로운 모형(HPVP모형)을 제기하였다. 이 모형은 선행연구[4, 5] 등에서 확장, 개선되였다.

HPVP모형과 그 확장판들에서 나타난 심각한 문제는 태그함락공격을 표현하는 Corrupt 오러클이 직관적표상과 어긋나게 정의된것이다.

론문에서는 선행연구들에서 제기한 RFID인증체계모형의 결함을 극복한 개선된 RFID인증체계모형을 제기하였다.

우선 RFID인증체계의 서술에 리용할 몇가지 기호들과 용어들을 약속한다.

$A(b_1, \cdots, b_m) \mapsto a$: 입력값 $b_1, \cdots, b_m$ 에서의 확률적알고리듬(확률적튜링기계) A 의 실행결과를 a 에 대입

$a \leftarrow A(b_1, \cdots, b_m)$: 입력값 $b_1, \cdots, b_m$ 에서의 확정적알고리듬(확정적튜링기계) A 의 실행결과를 a 에 대입

A^B : 확률적알고리듬 A가 실행과정에 다른 알고리듬(오러클이라고 부른다.) B를 호출하여 그 결과를 리용할수 있으며 더우기 B를 호출하여 그 결과를 받아오는데는 한결음의 시간만 소비하는 오러클알고리듬(오러클튜링기계)

$\perp$: null값. 실패 또는 거짓(false)을 의미하는 기호로도 사용한다.

$\varnothing$: 빈 문자렬 또는 빈모임(구체적인 의미는 문맥에 따라 달라진다.)

$\{0, 1\}^{\lambda}$: 길이가 λ인 2진비트렬전부의 모임

RFID인증체계는 다음과 같이 정의한다.

정의 1 보안파라메터 λ를 가진 RFID인증체계 $\mathbb{S}(\lambda, \mathfrak{I}, \mathfrak{R}, DB, \pi)$는

ㄱ) $\mathfrak{I} := \{T_1, \cdots, T_l\}$ ($l = l(\lambda)$는 λ에 관한 다항식) : 태그 $T \in \mathfrak{I}$는 λ에 관한 확률적다항식시간대화형알고리듬(대화형튜링기계)

ㄴ) $\mathfrak{R}$: 태그읽기장치, λ에 관한 확률적다항식시간대화형알고리듬

ㄷ) DB : 태그읽기장치 $\mathfrak{R}$의 인증정보자료기지

를 구성요소로 하고있으며 다음과 같은 확률적다항식시간알고리듬들을 갖추고있다.

① $\mathrm{SetupReader}(1^{\lambda}) \mapsto (P_{\Re}, K_{\Re})$: 태그읽기장치 $\Re$의 공개파라메터 $P_{\Re}$와 비공개파라메터(비공개열쇠와 내부상태값) $K_{\Re}$를 생성하고 체계의 모든 태그들의 식별자와 비밀자료를 보관하기 위한 인증정보자료기지 DB를 초기화하고 $P_{\Re}$는 공개된다. $K_{\Re}$는 읽기장치(인증봉사기)에 비밀로 보관한다.

② $\mathrm{SetupTag}(P_{\Re}, ID_T) \mapsto (P_T, K_T, S_T)$: $P_{\Re}$와 태그 $T \in \Im$의 식별자 ID_T를 입력파라메터로 줄 때 태그 T의 공개파라메터(공개열쇠) P_T, 초기비밀정보 K_T, 초기상태 S_T를 생성

③ $\pi(\Re, T) \mapsto (\mathrm{Out}_{\Re}, \mathrm{Out}_T)$: 읽기장치 $\Re$와 태그 T 사이의 다항식시간규약. $\mathrm{Out}_{\Re}$는 $\Re$의 대화실행결과, Out_T는 T의 대화실행결과

$\pi(\Re, T)$의 출력결과는 다음과 같은 의미를 가진다.

ㄱ) $\mathrm{Out}_{\Re} = \mathrm{ID}_T$: 규약실행과정에 읽기장치 $\Re$가 (대화상대방인) 태그 T의 신분확인에 성공(태그 T가 합법적이라는 결론에 도달)

ㄴ) $\mathrm{Out}_{\Re} = \perp$: 규약실행과정에 읽기장치 $\Re$가 (대화상대방인) 태그 T의 신분확인에 실패(태그 T가 비법적이라는 결론에 도달)

ㄷ) $\mathrm{Out}_T =$《접수》: 규약실행과정에 태그 T가 (대화상대방인) 읽기장치 $\Re$의 신분확인에 성공(읽기장치 $\Re$가 합법적이라는 결론에 도달)

ㄹ) $\mathrm{Out}_T = \perp$: 규약실행과정에 태그 T가 (대화상대방인) 읽기장치 $\Re$의 신분확인에 실패(읽기장치 $\Re$가 비법적이라는 결론에 도달)

ㅁ) 기타 경우 : 미정

규약 π의 매개 실행(과정)을 (인증)대화(session)라고 부른다.

식별자가 sid인 인증대화에서 태그 T와 태그읽기장치 $\Re$의 최종출력결과를 각각 $\mathrm{Out}_{T,sid}$와 $\mathrm{Out}_{\Re,sid}$로 표시한다.

정의 2 RFID인증체계 $\mathbb{S}(\lambda, \Im, \Re, DB, \pi)$에 대한 공격자 $\boldsymbol{A}$는 공개파라메터 $P_{\Re}$ 및 $P_{T'}$ ($T' \in \mathcal{T}$), 1^{λ}들을 입력값으로 하고 다음과 같은 대면부(오러클호출부)를 갖춘 확률적 오러클알고리듬이다.

① $\mathrm{CreateTag(ID)} \mapsto T$: 유일식별자 ID를 가지는 합법적인 태그 T를 작성한다. 즉 $\mathrm{SetupTag}(P_{\Re}, ID)$를 호출하며 $T \in \mathcal{T}$이다. 반환값에는 T의 비밀정보가 포함되지 않는다.

② $\mathrm{DrawTag}^b(T_0, T_1) \mapsto vtag$: 입력값 T_0과 T_1은 합법적인 태그들이다. 공격자가 공격대상으로 될 태그를 선발할 때 리용하는 오러클이다. $vtag$는 b가 0일 때에는 왼쪽태그 T_0을, 1일 때에는 오른쪽태그 T_1을 가리키는《가상태그식별자》또는 $\perp$이다. $\mathrm{DrawTag}^b$의 반환결과 $vtag$가 $\perp$가 아닐 때 3원조 ($vtag$, T_0, T_1)을 선발태그표 DT에 보관한다. $\mathrm{DrawTag}^b$는 DT에 T_0 또는 T_1이 포함된 3원조가 이미 존재하면 $vtag$를 $\perp$로 설정하고 DT에는 아무런 정보도 추가하지 않는다. $T_0 = T_1$일수도 있다. $T_0 \neq T_1$일 때 T_0과 T_1을 도전태그라고 부른다. 도전태그로 선발되는 태그들의 식별자는 도전태그표 QT에 보관한다.

③ $\mathrm{Free}^b(vtag)$: 선발태그표 DT에서 $vtag$가 들어있는 3원조 ($vtag$, T_0, T_1)을 검색하여 삭제한다. b가 0일 때에는 왼쪽태그 T_0, 1일 때에는 오른쪽태그 T_1의 림시기억기를 초기화한다.

④ $\mathrm{Corrupt}(vtag) \mapsto S_T$: 선발태그표 DT에서 $vtag$를 포함하는 유일한 기록이 ($vtag$,

T, T)일 때 T의 비밀정보(상태) S_T를, 그렇지 않을 때에는 $\perp$를 반환한다. 함락된 태그들의 식별자는 함락태그표 CT에 보관한다.

⑤ $\text{Launch}^b(vtag) \mapsto (sid,\ m,\ m')$: 가상태그식별자 $vtag$로 참조되는 태그 T와 읽기장치사이에 π에 기초한 새로운 대화를 개시하게 한다. m과 $\mathcal{R}$로부터 나오는 대화식별자 sid, 응답통보문 m'를 반환한다. 태그 T는 응답대기상태에 진입한다. 응답대기상태는 응답을 접수하든가, $\text{Free}^b(vtag)$로 선발해제될 때까지 유지된다.

⑥ $\text{SendTag}^b(vtag,\ m) \mapsto m'$: 가상태그식별자 $vtag$로 참조되는 태그 T에 규약통보문 m을 전송한다. T로부터 나오는 응답통보문 m'를 반환한다. 응답통보문이 없거나 $vtag$로 참조되는 태그 T를 찾지 못하면 $\perp$를 반환한다.

⑦ $\text{SendReader}(sid,\ m) \mapsto m'$: 대화 sid에서 읽기장치 $\Re$에 통보문 m을 전송하고 그것의 응답통보문 m'를 반환한다. 읽기장치가 현재 진행중인 대화들중에 식별자가 sid인 것이 없으면 $\perp$를 반환한다.

⑧ $\text{Excute}^b(vtag) \mapsto (sid,\ t_{sid})$: 가상태그식별자 $vtag$로 참조되는 합법적인 태그 T와 합법적인 읽기장치 $\Re$사이에 규약 π에 기초한 인증대화를 진행하고 대화식별자 sid 및 대화대본 t_{sid}를 반환한다.

⑨ $\text{Result}(sid) \mapsto x$: 대화 sid에서 $\text{Out}_{\Re,\,sid} \neq \perp$이고 $\text{Out}_{T,\,sid}$ =《접수》이거나 $\text{Out}_{\Re,\,sid} = \text{ID}_T$이고 $\text{Out}_{T,\,sid} \neq \perp$일 때 1을, $\text{Out}_{\Re,sid} = \perp$이거나 $\text{Out}_{T,\,sid} = \perp$이면 0을, 기타 경우는 미정값을 반환한다.

정의 3 공격자를 다음과 같이 분류한다.

RFID인증체계의 공격자를 Result대면부를 갖추고있는가 그렇지 못한가에 따라 자유(wide)공격자(간단히 w급공격자)와 제한(narrow)공격자(간단히 n급공격자)로 구분한다.[5, 6]

또한 공격자의 태그함락공격능력 즉 공격자가 Corrupt대면부를 어떻게 리용하는가에 따라 다음과 같이 8가지로 구분한다.

강(strong)공격자(간단히 s급공격자): 아무런 제한없이 Corrupt오러클을 리용할수 있는 공격자

강중간(strong-middle)공격자(간단히 sm급공격자): $QT \cap CT = \varnothing$라는 제한을 가진 강공격자

파괴적(destructive)공격자(간단히 d급공격자): 임의의 태그에 대하여 Corrupt오러클을 한번만 호출할수 있으며 Corrupt오러클을 적용한 태그는 파괴된다.

파괴적중간(destructive-middle)공격자(간단히 dm급공격자): $QT \cap CT = \varnothing$라는 제한을 가진 파괴적공격자 즉 도전태그에 대하여서는 함락공격을 할수 없다.

전방(forward)공격자(간단히 f급공격자): 일단 어떤 태그에 대하여 Corrupt오러클을 적용한 후에는 다른 태그들을 함락하는 Corrupt오러클외에 다른 오러클들을 리용할수 없다.

전방중간(forward-middle)공격자(간단히 fm급공격자): $QT \cap CT = \varnothing$라는 제한을 가진 전방공격자 즉 도전태그에 대하여서는 함락공격을 할수 없다.

약(weak)공격자(간단히 e급공격자): Corrupt대면부를 갖추지 못한 공격자 즉 태그에 대한 물리적공격능력이 전혀 없는 공격자

피동(passive)공격자(간단히 p급공격자): DrawTag, Free, Execute대면부만 갖추고있는 공격자 즉 인증체계에 대한 도청능력만 있고 주동공격능력이 전혀 없는 공격자

RFID인증체계 $\mathbb{S}(\lambda,\ \Im,\ \Re,\ DB,\ \pi)$에 대한 공격자 $\boldsymbol{A}$가 c급공격자라는것을 $\boldsymbol{A}_c$로 표

시한다. 여기서

$c \in \{w, s, ws, wsm, wd, wdm, wf, wfm, we, wp, ns, nsm, nf, nfm, ne, np\}$

정의로부터 곧 알수 있는바와 같이 ws급공격자의 공격능력이 가장 강하고 np급공격자가 가장 약하다.

론문에서 제기한 모형의 공격표현력을 선행모형들과 비교하면 표와 같다.

표. 론문의 모형과 기타 모형들의 공격자의 공격표현력비교

모형 / 공격	Avoine[2]	JW[9]	V07[10, 11]	CCEG[3]	HPVP[7, 8]	론문의 모형
태그작성	×	×	√	√	√	√
모든 태그와 대화가능	×	×	√	√	×	√
도전태그 선택	×	√	없음	없음	없음	√
임의태그 함락	×	×	√	√	√	√
도전태그 함락	√	×	없음	없음	없음	√
자유/제한공격	제한	자유	자유/제한	자유	자유/제한	자유/제한
공격등급설정	없음	없음	8	3	10	16

×는 해당한 조작이 모형에서 허용되지 않는다는것을, √는 허용된다는것, 《없음》은 아무런 론의도 없다는것을 의미한다.

참 고 문 헌

[1] A. Arslana et al.; Cryptology ePrint Archive: Report, 1130, 1, 2016.
[2] S. Canard et al.; Cryptology ePrint Archive: Report, 405, 1, 2010.
[3] I. Damgård et al.; LNCS, 4964, 318, 2008.
[4] H. Gross et al.; LNCS, 9476, 32, 2015.
[5] J. Hermans et al.; IEEE Transactions on Mobile Computing, 13, 12, 2888, 2014.
[6] A. Juels et al.; ACM Transactions on Information and System Security, 13, 1, 1. 2009.
[7] S. Vaudenay; LNCS, 4833, 68, 2007.
[8] S. Vaudenay; LNCS, 9451, 3, 2015.

주체108(2019)년 9월 15일 원고접수

A Model for Privacy-Preserving RFID Systems

Kim Chol Un

We propose a new model for privacy-preserving RFID systems which supports unilateral and mutual authentication protocols—it includes the notion of soundness, completeness and privacy.

Keywords: RFID system model, authentication, privacy