حمله به یک پروتکل احراز اصالت در سامانه های RFID

محمد حسن حبیبی
محمود گردشی

دانشگاه جامع امام حسین- دانشکده فناوری اطلاعات و ارتباطات

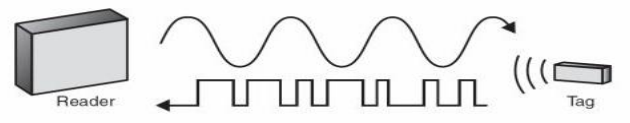
رئوس مطالب

- مقدمه
- سامانه های RFID
- انواع حملات بر روی پروتکل های RFID
- توصیف پروتکل LY
- حملات پیشنهادی به پروتکل LY
- نتیجه گیری
- مراجع

مقدمه

- فناوری شناسایی از طریق امواج رادیویی

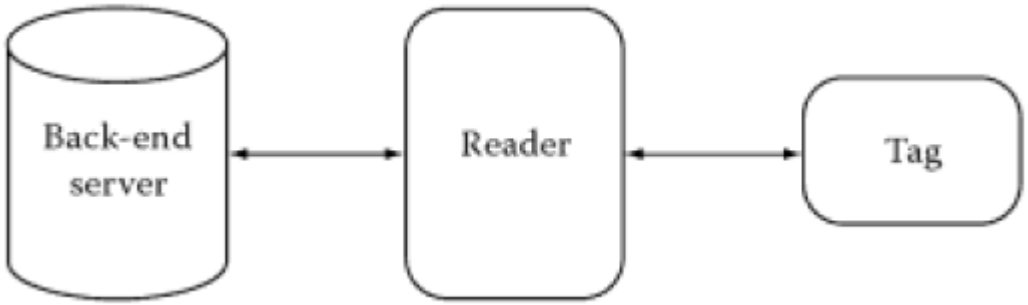
RFID : Radio Frequency Identification



- اولین بار در جنگ جهانی دوم
- رشد روز افزون در یک دهه گذشته
- مزایا:
- افزایش سرعت و صرفه جویی دروقت
- انجام احراز هویت در مقیاسهای بزرگ
- کاهش هزینه

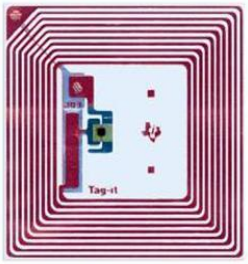
اجزای یک سامانه RFID

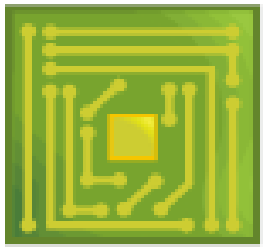
- سه جزء اساسی :
- برچسبهای RFID یا Tag ها
- کارتخوان ها یا Readerها
- سرویس دهنده نهایی یا back-end server



برچسبهای RFID

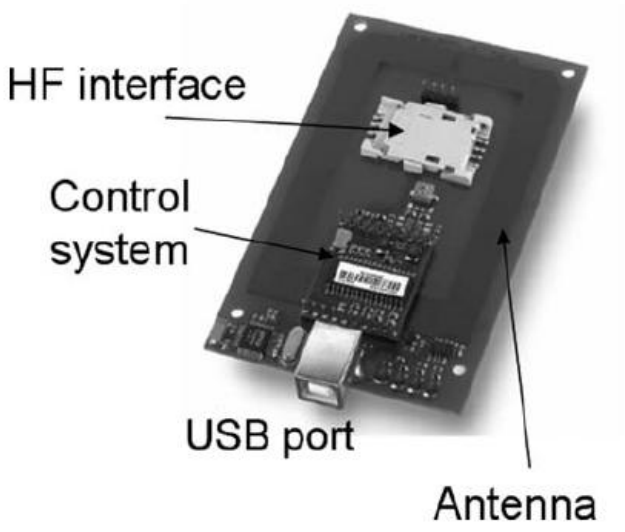
- روی هر هدف یک برچسب نصب می شود
- هر برچسب شامل: آنتن،حافظه،ریزتراشه
- هر برچسب دارای یك شناسه (ID)یکتا
- در صورت نیاز به تامین سطح امنیتی مناسب
- توابع درهم ساز،مولد اعداد شبه تصادفی، اولیه های سبک وزن





کارت خوان

- برقراری ارتباط با برچسب ها به صورت بی سیم
- دارای یك پورت USB برای ارتباط با سرور
- صرفا یك واسطه ارتباطی بین سرور و برچسبها
- عدم پردازش و ذخیره سازی داده ها

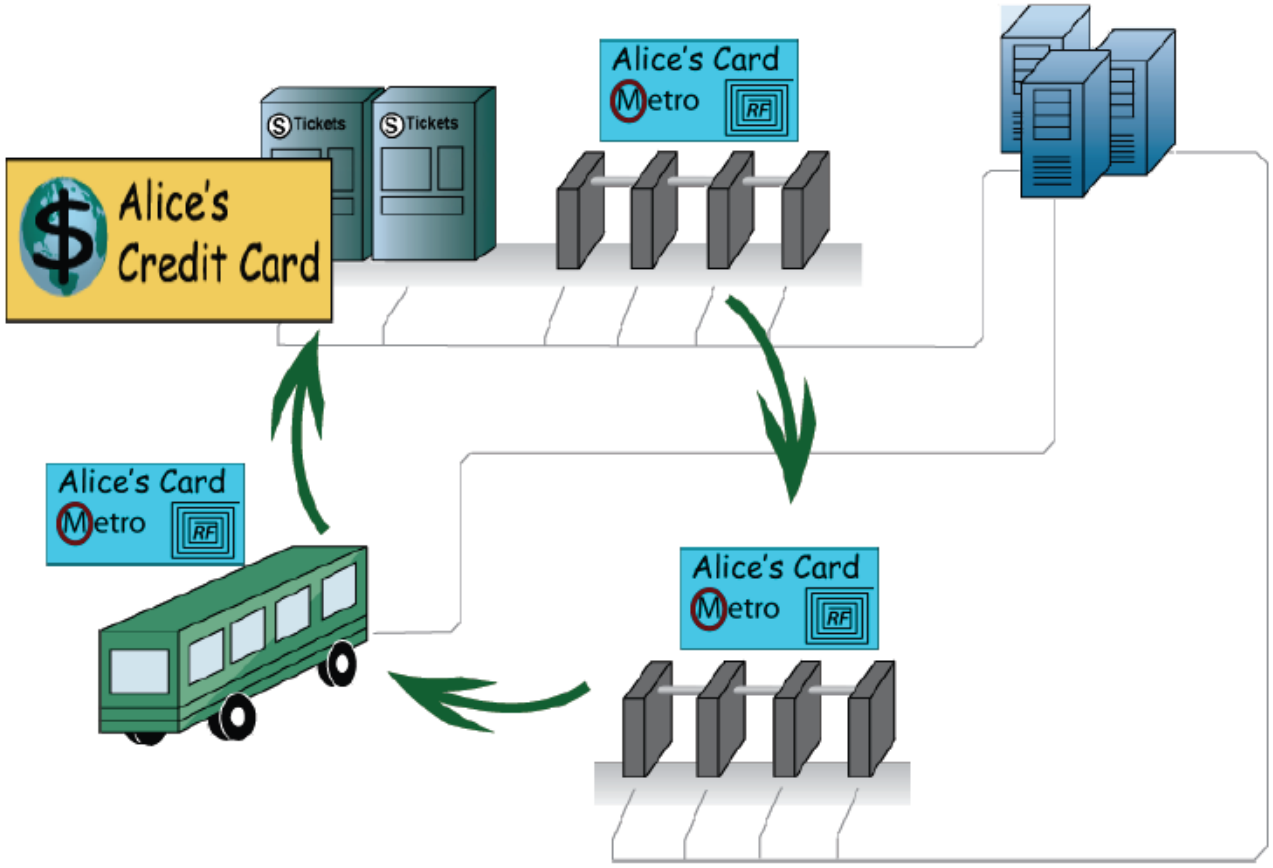


سرور نهایی

- یك database و چند پردازنده پرقدرت
- database حاوی اطلاعات مربوط به همه برچسبها
- همه محاسبات در پردازنده های سرور

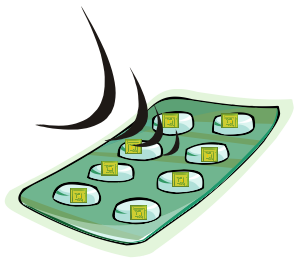
یک سیستم نمونه

An architecture for public transit



کاربردها

- پاسپورتهای الکترونیکی
- شبکه حمل و نقل عمومی
- صنعت خودروسازی
- کاربرد نظامی
- بارکدهای الکترونیکی
- علامت گذاری حیوانات
- کاربردهای پزشکی
- کارتهای اعتباری



شناسایی واحراز اصالت در RFID

- تامین امنیت: استفاده از پروتکل احراز اصالت (شناسایی)
- انجام رمزنگاری داده ها در دل پروتکل مورد استفاده
- امنیت کل سیستم وابسته به میزان امن بودن پروتکل احراز اصالت

انواع حملات

- ✓ کشف کلید و شناسه
- ➢ جعل هویت برچسب یا کارت خوان
- ✓ ردیابی برچسبها
- ✓ ناهمزمان سازی طرفین

توصیف پروتکل LY

- **منطبق با استاندارد EPC C-1 G-2**
- **فاز مقدماتی**
  - ✓ توابع CRC و PRNG با خروجی 16 بیتی روی هربرچسب و کارت خوان
  - ✓ روی هر برچسب یک شناسه 96 بیتی، یک کلید 16 بیتی:

Tag: (flag, K_x, EPC_x)

- Flag = 0 or 1

  - ✓ متناظر با هر برچسب یک سه تایی در کارت خوان:

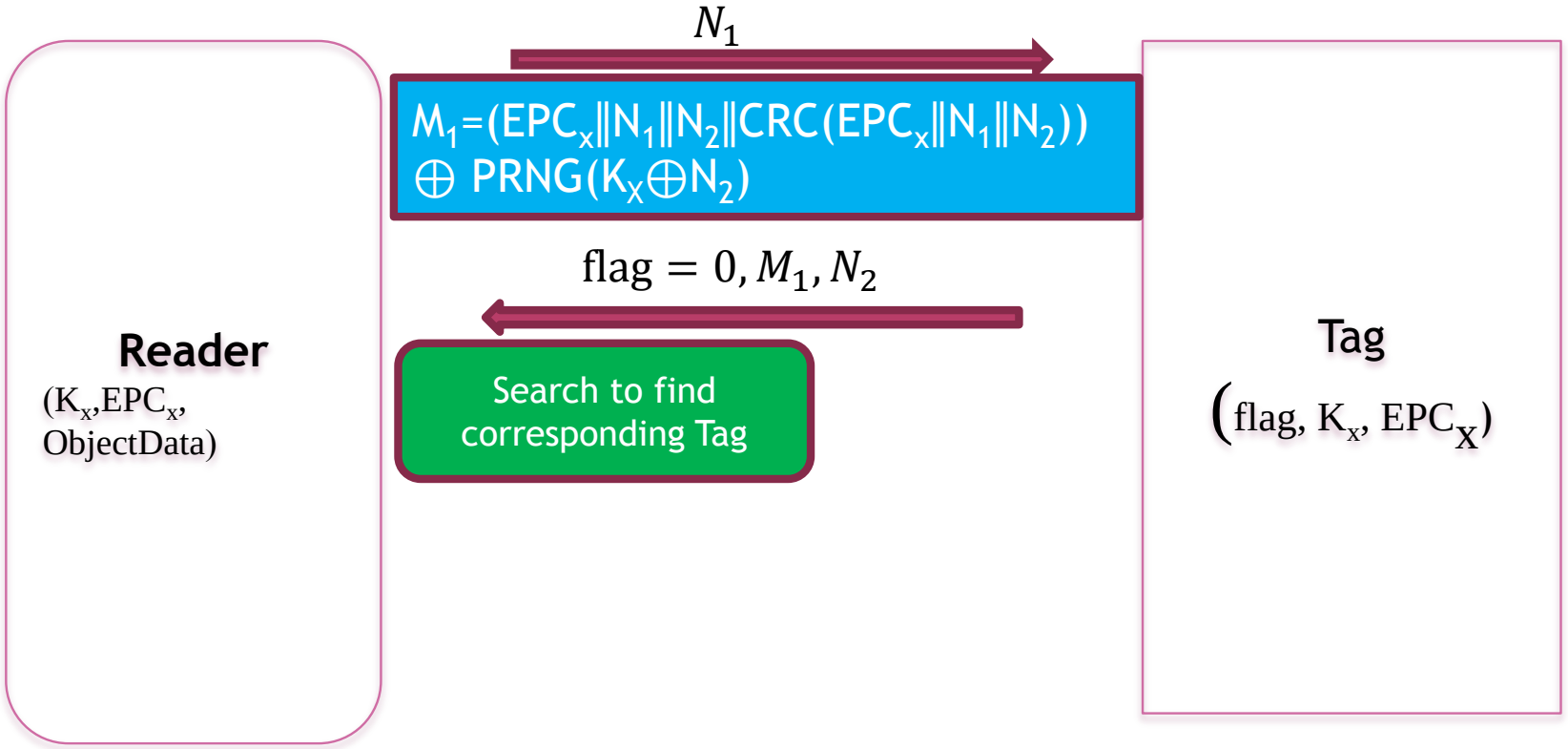
Reader: ($K_{x\text{-}DB}$, $EPC_{x\text{-}DB}$, ObjectData)

توصیف پروتکل LY

- **فاز مقدماتی**
- روش XOR کردن مقادیر با طول بیت‌های متفاوت
- مثلا: $(EPC_x||N_1||N_2||CRC(x)) \oplus PRNG(N_1 \oplus N_2)$
- رشته اول: 96+16+16+16=144 بیت و رشته دوم: 16 بیت
- $Q = PRNG(N_1 \oplus N_2) || \ldots.. || PRNG(N_1 \oplus N_2)$ (9 مرتبه)
- $(EPC_x||N_1||N_2||CRC(x)) \oplus Q$

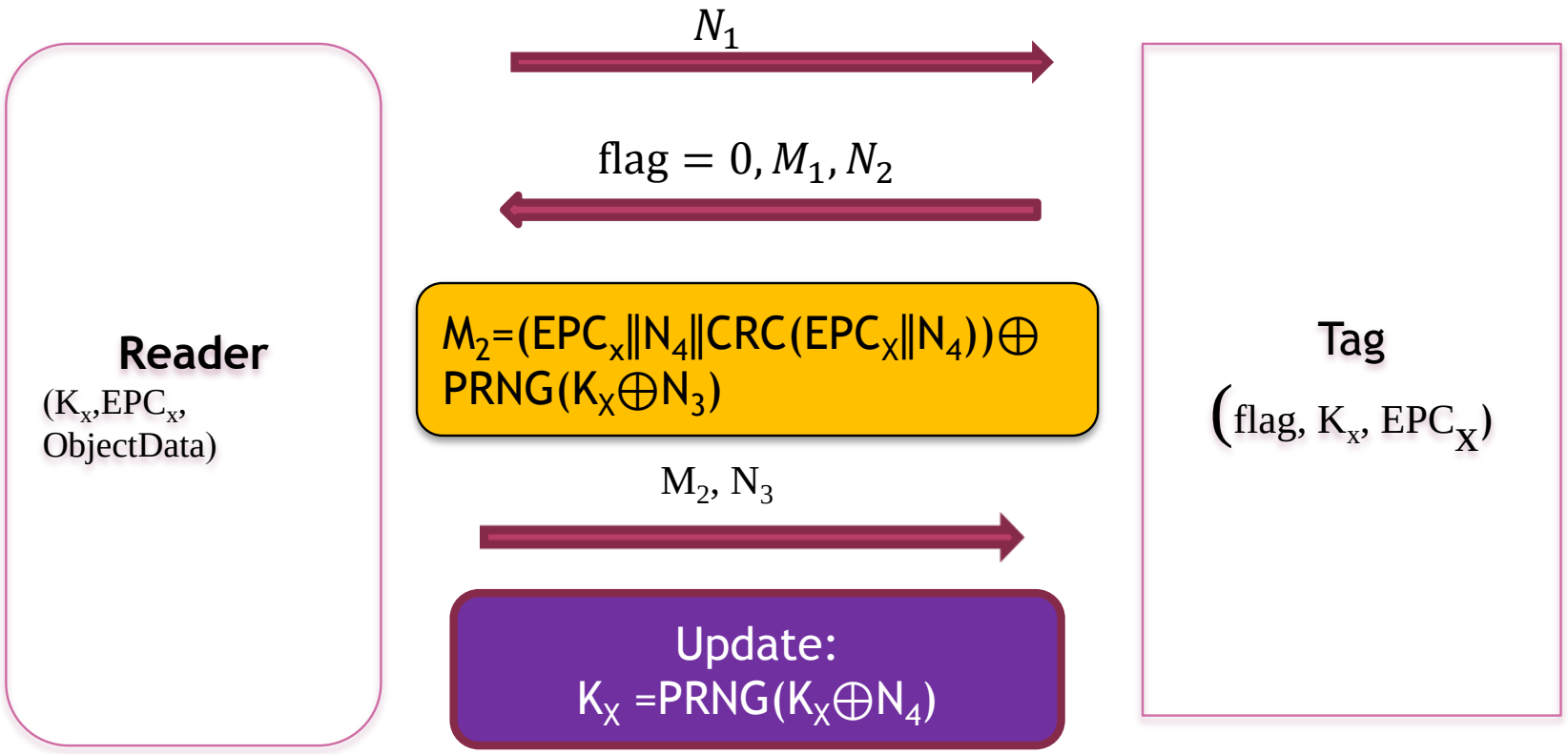
توصیف پروتکل LY

- فاز احراز اصالت(حالت0= flag)



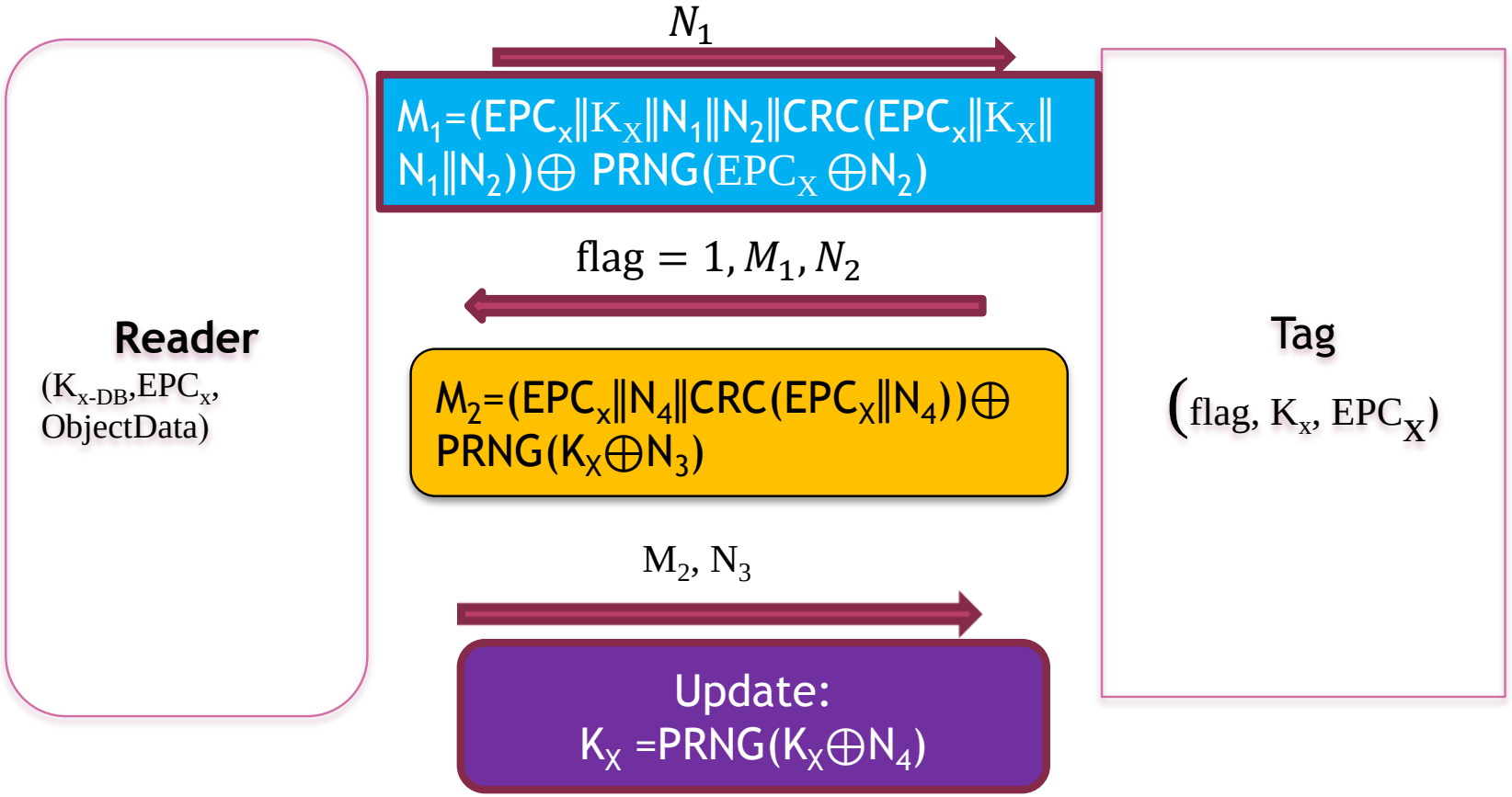
توصیف پروتکل LY

- فاز احراز اصالت(حالت0= flag)



توصیف پروتکل LY

- فاز احراز اصالت(حالت flag=1)

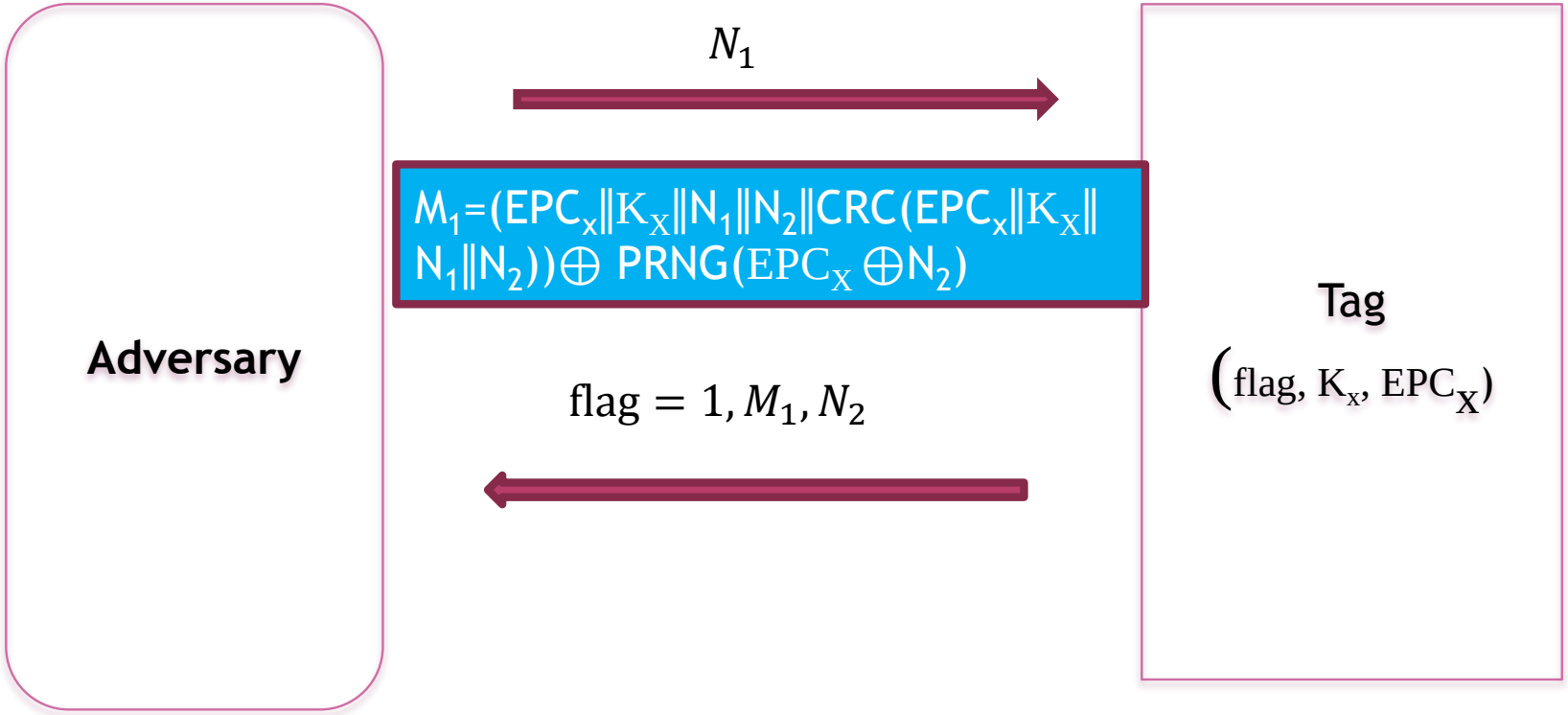


حملات پیشنهادی

- **جعل هویت یک برچسب مجاز**
- نقطه ضعف: ساختار پیام M_1 از الحاق چند رشته بیت و XOR کردن آنهابا یک رشته دیگر بدست می‌آید
- عملگرهای الحاق و XOR دارای خواص امنیتی ضعیفی هستند

حملات پیشنهادی

- جعل هویت یک برچسب مجاز
- بایک نشست ناتمام، برچسب را به flag =1



حملات پیشنهادی

- جعل هویت یک برچسب مجاز
- می توان نوشت:

$$M_1=(EPC_X \| K_X \| N_1 \| N_2 \| CRC(EPC_X \| K_X \| N_1 \| N_2)) \oplus PRNG(EPC_X \oplus N_2) = EPC_X \oplus [PRNG(EPC_X \oplus N_2) \| \ldots \| PRNG(EPC_X \oplus N_2)] \| K_X \oplus PRNG(EPC_X \oplus N_2) \| N_1 \oplus PRNG(EPC_X \oplus N_2) \| N_2 \oplus PRNG(EPC_X \oplus N_2) \| CRC(EPC_X \| K_X \| N_1 \| N_2) \oplus PRNG(EPC_X \oplus N_2)$$

- با توجه با ساختار پیام M_1 داریم:

$$M_{1[112\text{-}127]} \oplus N_1 = PRNG(EPC_X \oplus N_2)$$

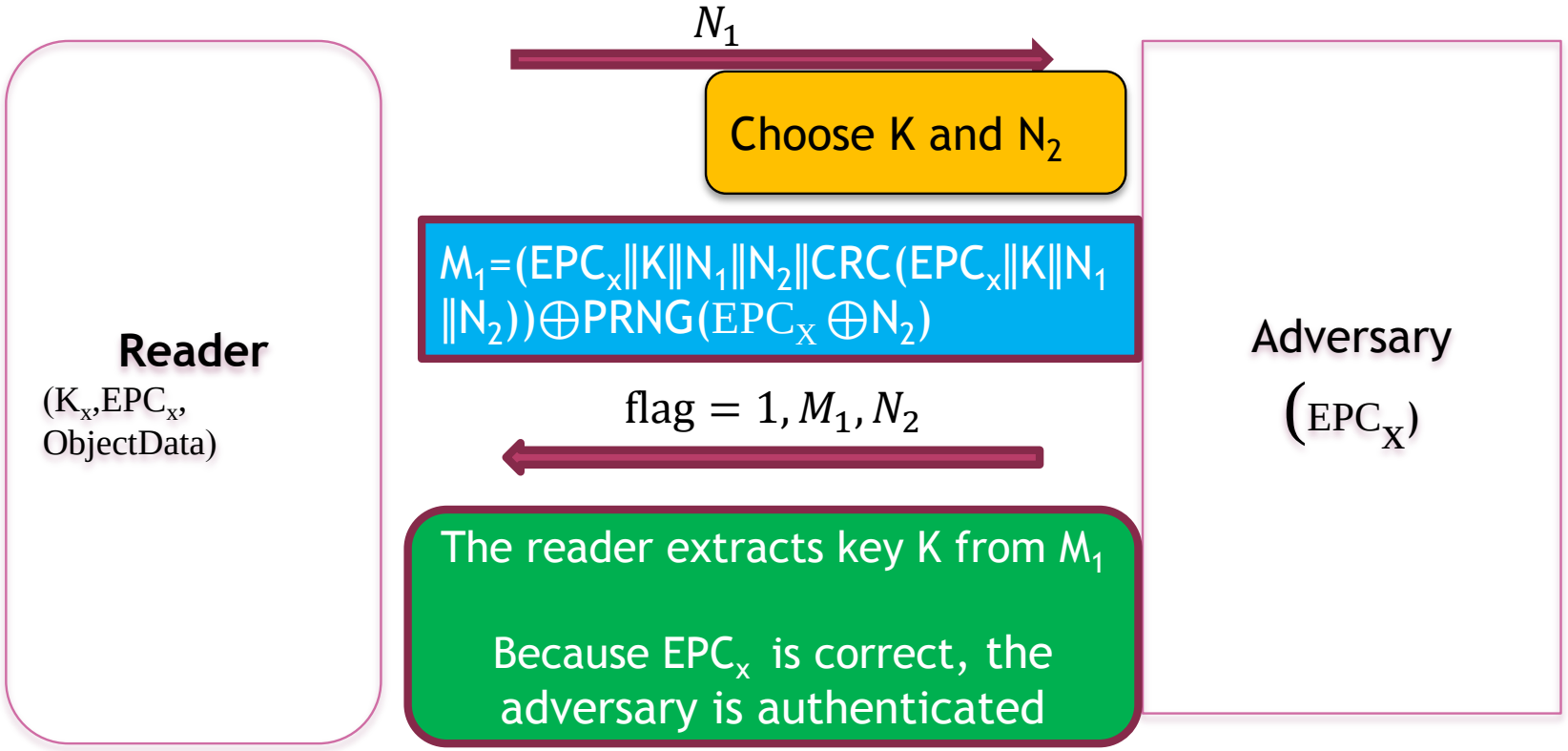
- مهاجم شناسه برچسب را محاسبه می کند:

$$EPC_X = M_{1[0\text{-}95]} \oplus (\underbrace{PRNG(EPC_X \oplus N_2) \| \ldots \| PRNG(EPC_X \oplus N_2)}_{\text{6مرتبه}})$$

- با داشتن شناسه، او در هر زمانی قادر است تا هویت این برچسب را جعل کند.

حملات پیشنهادی

- جعل هویت یک برچسب مجاز



نتیجه گیری

- تحلیل امنیتی پروتکل LY در دو حالت flag=0 و flag=1
- استفاده از یک ضعف ساختاری در طراحی پیامهای پروتکل
- کشف و محاسبه شناسه دائمی برچسب
- انجام حمله جعل هویت برچسب
- امکان حمله جعل هویت کارتخوان با توجه با در اختیار داشتن شناسه

مراجع

[1] J. Banks, M. Pachano. L. Thompson, and D. Hanny, “RFID applied”, JOHN WILEY & SONS, Inc, 2007.

[2] D. Henrici, “RFID Security and privacy: concepts, protocols and architectures“, Springer-Verlag Berlin Heidelberg, Lecture Notes Electrical Engineering, Volume17, 2008.

[3] S. Konomi and G. Roussos, “Ubiquitous computing in the real world: lessons learnt from large scale RFID deployments”, Pers. Ubiq. Computing, 2007.

[4] N.W. Lo and K-H. Yeh, “A secure communication protocol for EPCglobal Class 1 Generation 2 RFID systems”, 24th International Conference on Advanced Information Networking and Applications Workshops, IEEE computer society, Perth, Australia, April 2010, pp. 562-566.

[5] G. Roussos, “Networked RFID: Systems, software and services”, Springer-Verlag London, Computer communications and networks series, 2008.

با تشکر از توجه شما
سوال؟؟؟