

بررسی امنیت کوانتومی یک طرح احراز هویت امن RFID پهنپادی در آماد و پشتیبانی دفاعی

علی نخعی امرودی، محمد حسین تقدیری، روح الله جلایی صلات

۱-دکتری رمز، دانشکده رایانه، دانشگاه جامع امام حسین

۲-ارشد مخابرات، دانشکده برق دانشگاه جامع امام حسین

۳-دکتری ریاضی و رمز، دانشکده رایانه، دانشگاه جامع امام حسین

چکیده

مزایای توابع غیرقابل شبیه سازی فیزیکی (PUF) منجر به ظهور تعداد قابل توجهی از سیستم های جدید مبتنی بر شناسایی و احراز هویت مانند شناسایی فرکانس رادیویی (RFID) شده است. که انتظار می رود به دلیل مزایایی مانند تشخیص به موقع تعداد قابل توجهی از اشیاء، جایگزین سیستم شناسایی بارکد معمولی شود. به عنوان مثال ، RFID می تواند برای شناسایی یک وسیله نقلیه هوایی بدون سرنشین (UAV) هنگامی که با برجسب متصل است ، استفاده شود . در این مقاله ، ما یک طرح احراز اصالت ناشناس جدید برای برنامه های پهنپادی مجهز به RFID با استفاده از توابع غیرقابل تکثیر فیزیکی پیشنهاد می دهیم .امنیت و تجزیه و تحلیل عملکرد نشان می دهد که طرح پیشنهادی ما در برابر حملات کوانتومی نیز ایمن و کارآمد است .از این رو ، می تواند برای چندین سیستم کاربردی مبتنی بر RFID مفید باشد.

واژگان کلیدی:احراز هویت، حملات کوانتومی، RFID، پهنپاد، آماد و پشتیبانی.

۱- مقدمه

شناسایی فرکانس رادیویی یا RFID در حال حاضر به یک فناوری ضروری برای شناسایی و ردیابی اشیاء تبدیل شده است. [۳-۱] RFID ازگیرنده و فرستنده سیگنال رادیویی دو طرفه برای بازخوانها استفاده می کند. سیگنالهای رادیویی به برچسب متصل به جسم فیزیکی ارسال می شوند و بازخوان یا ریدر مسئول پاسخگویی هستند. دستگاه RFID Reader یک دستگاه متصل به شبکه (قابل حمل یا ثابت) همراه با آنتن است که وظیفه انتقال توان، داده و همچنین دستورات را به برچسب های اشیاء برعهده دارد. تطبیق پذیری فناوری RFID آن را برای استفاده در شناسایی و احراز هویت هواپیماهای بدون سرنشین (پهپادها) [۴] در هر دو حالت تجاری و یا نظامی ایده آل می کند. در اینجا ما نمونه ای از سناریوی نظامی را پیشنهاد می کنیم که در آن باید پهپاد قبل از اجازه فعالیت در یک فضای هوایی امن احراز هویت شود.

در جنگ مدرن، هواپیماهای بدون سرنشین پهپادی منبعی هستند که معمولاً مورد استفاده قرار می گیرند و می توانند کارهای شناسایی و سایر کارهای مفید را انجام دهند. به دلیل کاربرد گسترده آنها، پرسنل نظامی باید اطمینان حاصل کنند که هواپیماهای بدون سرنشین که وارد حریم هوایی امن می شوند توسط دشمنانشان اداره نمی شوند. در این حالت، می توان این پهپادها را با برچسب های RFID مجهز کرد و لازم است که از طریق یک ایستگاه بازخوانی (خواننده) عبور کنند تا برچسب آن اسکن شده و اعتبار آن برای تأیید به یک واحد سرور امن ارسال شود. یا پهپاد احراز هویت می شود و اگر نه، می توان آن را رهگیری کرد. این سناریو در شکل ۱ نیز نشان داده شده است. با توجه به محدودیت منابع RFID که نیاز به پروتکل هایی با سربار محاسباتی محدود را ارائه می دهد، ما یک راه حل با استفاده از عملکردهای غیر کلون شده فیزیکی برای کاهش هزینه و پیچیدگی در حالی که حفظ امنیت کافی برای سناریوهای احراز هویت مبتنی بر پهپاد است، پیشنهاد می کنیم.

اکنون، به عنوان محلی ساز و ردیاب، سیستم مبتنی بر [۳] RFID از دیگر سیستم های محلی سازی بهتر عمل می کند. با این حال، در برابر ناشناس بودن و حملات حریم خصوصی مکان [۴،۵] آسیب پذیر است زیرا برچسب های RFID اطلاعات شناسایی و مکان خود را به عنوان متن ساده به خواننده های RFID منتقل می کنند. بنابراین، هر مهاجمی می تواند برچسب ها را با شناسایی آنها به راحتی ردیابی کند. ایمن سازی سیستم های مبتنی بر RFID یک کار چالش برانگیز است زیرا توانایی محاسباتی برچسب های RFID بسیار محدود است [۶،۷].

علاوه بر این، راه حل های موجود اغلب بدون در نظر گرفتن مکانیسم های محافظت سخت افزاری از برچسب های کم هزینه استفاده می کنند. در نتیجه، رمزهای ذخیره شده در این برچسب ها می توانند از طریق کانال اصلی جانبی و حملات تهاجمی بازایی شوند [۸]، که امکان جعل اطلاعات برچسب (مانند مانده بدهی بلیط) را فراهم می کند. برای پرداختن به این موضوع، اخیراً مفهوم فناوری تابع غیرقابل تکتیرفیزیکی (PUF)، ارائه شده است [۹،۱۰]. (PUF) تابعی است که از ویژگی فیزیکی حاصل می شود و هدف اصلی PUF تولید یک خروجی مخصوص دستگاه برای هر ورودی مانند اثر انگشت است. ظهور PUF چاشنی و طعم جدیدی در فناوری شناسایی فرکانس رادیویی (RFID) ایجاد کرده است. با در نظر گرفتن PUF، RFID می تواند امنیت سخت افزار را تضمین کند.

۲-۱- کار و انگیزه

به طور کلی، مفهوم فناوری PUF را می توان برای اطمینان از درجه بالاتری از امنیت و کارایی مورد استفاده قرار داد . در چند سال گذشته، برخی از طرح های احراز هویت جالب مبتنی بر PUF پیشنهاد شده اند. می توانیم آنها را به دو دسته تقسیم کنیم:

(i) طرح های مبتنی بر PUF ایده آل [۱۸، ۱۱]، (ii) طرح های مبتنی بر PUF نوپزی [۲۱، ۱۹]

برینگر و همکاران یک پروتکل احراز هویت طرح مبتنی بر PUF ایده آل را با استفاده از PUF های ایده آل در [۱۱] معرفی کرد ؛ با این حال، پروتکل نمی تواند امنیت را در برابر حملات DoS و جعل هویت فراهم کند [۱۲] صادقی و همکاران [۱۲].

برای تضمین حریم خصوصی مخرب با در نظر گرفتن مدل امنیتی Vaudenay از یک PUF ایده آل در ساخت احراز هویت RFID استفاده کرد [۱۷].

بلافاصله پس از آن ، کولسنگ و همکاران [۱۳] طرح جدیدی را پیشنهاد کرد که از ترکیب PUF و یک شیفت رجیستر با بازخورد خطی (LFSR) استفاده می کند . این پروتکل از چهار دور تشکیل شده است و برای هر دور برچسب با استفاده از عملکرد XOR و یک کلید مخفی مشترک ، هویت آن را رمزگذاری می کند . در پایان هر جلسه ، کلید توسط سرور و برچسب ها به روز می شود . با این حال ، امنیت آن با توجه به حفاظت از شناسه (محرمانه بودن) و حمله غیرهمگام سازی مورد بازنگری و ارتقاء قرار گرفت [۱۵، ۱۴] .

در سال ۲۰۱۵ ، لی و همکاران طرحی جدید را تحت شرایط جدید حریم خصوصی پیشنهاد کرد [۱۶]؛ با این حال، ساخت آن بر اساس رمزگذاری امن با کلید عمومی است . در سال ۲۰۱۷ ، طرح جدیدی توسط Pandey و همکاران پیشنهاد شد. نویسندگان از ترکیب PUF با رمزنگاری آستانه استفاده کردند . در اینجا ، نویسندگان روش به اشتراک گذاری مخفیانه برای خنثی کردن حملات سازنده برچسب را پیشنهاد کردند [۱۸] . با این حال، در پروتکل آنها، برچسب نیاز به انجام برخی عملیات گران قیمت محاسباتی دارد، که برای دستگاه های برچسب محدود منابع غیرقابل اجرا است .

اگرچه مکانیزم های طراحی دیفرانسیل می توانند قابلیت اطمینان را بهبود بخشند ، نویز هنوز به عنوان عاملی در طراحی PUF ظاهر می شود ، که ممکن است باعث شود چندین بیت خروجی برای هر چالش نادرست باشد. هرویگ و همکاران [۱۹] یک پروتکل احراز هویت با در نظر گرفتن شرایط پر نویز PUF را پیشنهاد کردند ؛ با این حال ، پس از بررسی دقیق رویکرد آنها ، نقاط ضعف زیر را در این طرح ها پی بردیم . به عنوان مثال ، در [۱۹]، یک برچسب باید هویت خود را آشکار کند تا به تأیید کننده در یافتن خروجی PUF قبلی Z کمک کند، بنابراین این طرح نمی تواند ویژگی ناشناس بودن را تضمین کند. در سال ۲۰۱۴ ، موریاما و همکاران [۲۰] با استفاده از PUF پروتکل احراز هویت جدیدی را برای سیستم های RFID پیشنهاد کردند . این پروتکل به بازخوان اجازه می دهد تا اسرار وضعیت تصادفی را به روز کند، و سپس یک برچسب برای هر جلسه S دریافت می کند . اما در طرح آنها یک برچسب نیاز به ذخیره داده های کمکی برای بازسازی خروجی، که باعث سربار

ذخیره سازی بالا در سمت برچسب می شود را دارد. علاوه بر این، اجرای بازسازی خروجی بر روی دستگاه مبتنی بر PUF در بسیاری از کاربردها یک نقطه ضعف است. اخیراً گوپ و همکاران، یک پروتکل احراز هویت جدید [۲۲] با استفاده از شرایط PUF نوین پیشنهاد کرد. اما مانند [۲۰]، در طرح آنها، یک برچسب نیاز به اجرای تابع بازسازی گران قیمت محاسباتی و ذخیره داده های کمکی برای بازسازی خروجی دارد، که باعث هزینه ذخیره سازی بالایی نیز می شود. برای حل این مسئله، در CHES 2015، آیسو و همکاران یک پروتکل جدید مبتنی بر [۲۱] PUF با استفاده از استخراج کننده فازی معکوس معرفی کردند؛ با این حال، طبق [۲۲]، پروتکل ارائه شده در [۲۱] نمی تواند حریم خصوصی را فراهم کند، که یکی از الزامات امنیتی اصلی در سیستم مبتنی بر RFID است. علاوه بر این، در تمام پروتکل های احراز هویت ناشناس مبتنی بر PUF (از جمله [۱۹-۲۱])، برای شناسایی دستگاه، واحد خواننده - سرور نیاز به انجام یک عملیات جستجوی کامل دارد. بنابراین، آنها برای سناریوهای کاربردی پایگاه داده در مقیاس بزرگ مناسب نیستند.

به طور خلاصه، در تمام طرح های فوق الذکر، سرور برای شناسایی برچسب نیاز به جستجوی جامع دارد. که برای برنامه های کاربردی با پایگاه داده های بزرگتر مناسب نیست. هدف این مقاله پرداختن به همه موارد بالا با ارائه یک پروتکل احراز هویت واقعی برای حفظ پروتکل احراز هویت با استفاده از PUF است. ما می توانیم سهم خود را در این مقاله به صورت زیر خلاصه کنیم:

- ما یک طرح احراز هویت جدید را برای شرایط PUF نوینی پیشنهاد می دهیم.
- طرح پیشنهادی ما قادر خواهد بود از ویژگیهای مهم امنیتی مانند ناشناس ماندن، محافظت در برابر حملات DoS و غیره اطمینان حاصل کند، که برای هر برنامه و سرویس اینترنت اشیا ضروری است.
- یکی از ویژگی های قابل توجه طرح پیشنهادی این است که در طرح ما، سرور قادر خواهد بود برچسب را بدون انجام عملیات جستجوی جامع شناسایی کند.

۳-۱- استخراج کننده فازی

یک استخراج کننده فازی [۲۳]، [۲۴]، [۲۵-۲۷] ترکیبی از دو تابع است، یعنی $FE.Gen(.)$ [تولیدکننده کلید]

و $FE.Rec(0)$ [تابع تولید مثل یا تکثیر] (reproduction function).

می توانیم $FE.Gen(0)$ را به عنوان یک الگوریتم احتمالی برای تولید کلید K و داده های کمکی hd ،

یعنی $(K, hd) = FE.Gen(R)$ روی یک رشته بیت ورودی داده شده R در نظر بگیریم.

$FE.Rec(.)$ یک تابع قطعی است که یک ورودی نوین R' و داده کمکی hd را می گیرد و سپس کلید K را تولید می کند، یعنی $K = FE.Rec(R')$ ، زمانی که فاصله همینگ بین R' و R حداکثر d باشد.

۴-۱- استخراج کننده فازی معکوس

به منظور اطمینان از اجرای سریع طرح امن و استخراج کننده های فازی ، می توان از مفهوم استخراج کننده فازی معکوس استفاده کرد .در این زمینه ، دستگاه های RFID دارای PUF نیازی به اجرای هر الگوریتم بازسازی فشرده و شدید محاسباتی ندارند .در عوض ، دستگاه باید الگوریتم تولید داده کمکی را اجرا کند.

۵-۱- عملکرد فیزیکی غیرقابل شبیه سازی

یک تابع فیزیکی غیرقابل تکثیر (PUF) یک سیستم فیزیکی است که برای یک ورودی داده شده (چالش) یک خروجی (پاسخ) را ارائه می دهد، که می تواند به عنوان یک شناسه منحصر به فرد امن (اثر انگشت دیجیتال) برای دستگاه ها عمل کند .هر پاسخی که برای هر چالشی ایجاد می شود، کاملاً منحصر به فرد و غیرقابل پیش بینی است .آنتروپی برای جفت های چالش/پاسخ (CRP) Pufs به میکرو واریانس فیزیکی در هر تراشه ایجاد شده در طول فرآیند تولید نسبت داده می شود که تفاوت های رفتاری منحصر به فردی را بین هر PUF ایجاد می کند و شبیه سازی آنها را بسیار دشوار می کند.

نتیجه این امر تولید امن چالش ها و پاسخ هایی است که نیازی به رمزنگاری پیچیده و گران قیمت ندارد .این ماهیت سبک وزن PUF ها آنها را برای فعال کردن احراز هویت ایمن برای سیستم های محدود به منابع مانند RFID بسیار مناسب می کند.

ما می توانیم PUF را به عنوان یک جفت CRP تعریف کنیم .برای یک چالش ورودی معین C ، PUF یک رشته تصادفی $R = P(C)$ یعنی R را خروجی می دهد . به یک P PUF گفته می شود $(d, n, l, \lambda, \epsilon)$ - اگر شرایط زیر برقرار باشد، ایمن است:

۱. تصور کنید ، دو PUF وجود دارد $P_1(\cdot)$ و $P_2(\cdot)$ ، و برای هر یک ورودی $C_1 \in \{0,1\}^k$ ، $\Pr[HD(P_1(C_1), P_2(C_1)) > d] \geq 1 - \epsilon$

۲. برای یک PUF معین $P_i(\cdot)$ و برای هر ورودی $C_1, C_2, \dots, C_n \in \{0,1\}^k$ ، $\Pr[HD(P_i(C_1), P_i(C_2)) > d] \geq 1 - \epsilon$.

۳. با توجه به، دو PUF $P_i(\cdot)$ و $P_j(\cdot)$ ، و برای هر ورودی $C_1, C_2, \dots, C_n$ ،

$$\Pr[H^\infty(P_i(C_k), P_j(C_k)) > d] \geq 1 - \epsilon, \quad i \neq j, \quad k \leq n$$

۶-۱- تابع شبه تصادفی

یک تابع شبه تصادفی PRF: $\{0,1\}^k \times \{0,1\}^* \rightarrow \{0,1\}^k$ که یک پارامتر امنیتی مخفی $K \in \{0,1\}^k$ و یک پیام $M \in \{0,1\}^*$ می گیرد به عنوان ورودی و یک رشته دلخواه $PRF(K, M)$ را ارائه می دهد که از رشته تصادفی قابل تشخیص نیست .

حال، فرض کنید h یک تابع چند جمله ای شبه تصادفی قابل محاسبه باشد.

برای تشخیص h ، یک دشمن احتمالی چند جمله ای زمان (PPT) A ممکن است پرس و جوهای محدود چند جمله ای را با ورودی های انتخابی خود درخواست کند و خروجی های محاسبه شده توسط h را برای آموزش بدست آورد.

بعد از مرحله آموزش، به A تابعی داده می شود که یا h است یا یک تابع کاملاً تصادفی است. می گوییم h یک تابع شبه تصادفی است، اگر از یک تابع واقعاً تصادفی در زیر A قابل تشخیص نباشد.

یعنی، A با توجه به یک بیت تصادفی $\{0, 1\}$ یا h یا یک تابع واقعاً تصادفی داده می شود و فقط احتمال $0.5 + \epsilon$ را دارد تا h را متمایز کند.

۲- طرح پیشنهادی ما

این بخش احراز هویت ناشناس واقعی ما را معرفی می کند، طرحی که از دو مرحله تشکیل شده است: مرحله راه اندازی و مرحله احراز هویت. در اینجا سرور را با نماد S و برچسب RFID را با نماد T نشان می دهیم.

۲-۱- مرحله راه اندازی

✓ سرور به طور تصادفی یک چالش C_i را برای دور i ام و همچنین مجموعه ای از چالش های اضطراری

$$C_{em} = \{C_1, \dots, C_n\}$$

را تولید میکند که می توانیم بعداً برای جلوگیری از برهم ریختن همگام سازی بین واحد سرور- بازخوان و برچسب از آن استفاده کنیم.

✓ سپس سرور $\{C_{em}, C_i\}$ را به برچسب T می فرستد.

✓ سپس T خروجی های PUF را به شرح زیر استخراج می کند:

$$R_i, R_{em} = P_T(C_i, C_{em})$$

✓ حال $\{R_{em}, R_i\}$ را به واحد سرور خواننده S ارسال می کند.

✓ سپس S ابتدا یک مقدار که هویت سایه ای نامیده می شود به صورت زیر ایجاد می کند

$$SID_T = h(R_i \parallel MK)$$

که در آن h یک تابع درهمساز است؛ MK نیز کلید اصلی^۱ سرور است.

✓ سپس S یک کلید مخفی sk نیز می سازد.

✓ سپس S مجموعه‌ای از جفت‌های کلید اضطراری و شبه ID یکتا

$$(PID, Kem) = \{(sid_1, K_{em1}), \dots, (sid_n, K_{emn})\}$$

را تولید می کند و به تگ T ارسال می کند.

✓ در نهایت، برای هر تگ، سرور

$$\{(SID_T^i, SK), C_i, R_i, C_{em}, R_{em}, (PID, K_{em})\}$$

را در پایگاه داده خود ذخیره می کند.

✓ اکنون سرور تگ

$$\{(PID, K_{em}), (SK, SID_T^i)\}$$

را برای T ارسال می کند.

✓ T مقدار $\{(PID, K_{em}), (SK, SID_T^i)\}$ را ذخیره می کند.

جزئیات این مرحله در شکل ۲ نشان داده شده است.

۲-۲- مرحله احراز هویت

✓ برچسب آمین مشخصه سایه‌ای خود یعنی SID_T^i را انتخاب و سپس عدد تصادفی N_t را تولید و در

نهایت یک پیام درخواستی $\{SID_T^i, N_t\}$ را به سرور S ارسال می کند.

✓ سرور S پس از دریافت پیام درخواست M_1 ، ابتدا SID_T^i را در پایگاه داده خود پیدا می کند و

^۱ Master Key

^۲ Secret Key

✓ $\{ (C_i, R_i), sk \}$ را در حافظه خود بارگذاری می کند (می خواند).

✓ بعد از آن، سرور S مقدار تصادفی N_s را تولید می کند

✓ سرور S مقدار $sk \oplus N_s N_s^* =$ ، محاسبه می کند.

✓ سرور S مقدار خروجی کلید هش

$$= h(N_s || sk || N_s^*) Res_S$$

محاسبه می کند.

✓ حال سرور مقادیر $\{ C_i, N_s^*, Res_S \}$

را به برچسب ارسال می کند.

✓ سپس برچسب خروجی PUF را به صورت $R'_i = P_T(C_i)$ استخراج می کند

✓ و خروجی کلید هش Res_S را مجدداً بر اساس مقادیری که از قبل ذخیره داشته است (بین خود و

سرور رد و بدل کرده است) را بررسی می کند تا سرور را احراز اصالت نماید.

✓ اگر معتبر باشد، تگ موارد زیر را محاسبه می کند:

Compute :
 $N_s = sk \oplus N_s^*$
 $(K_i, hd_i) = FE.Gen(R'_i)$
 $hd^* = h(sk || N_s) \oplus hd_i$
 $C_{i+1} = h(C_i || K_i)$
 $R'_{i+1} = P_T(C_{i+1})$
 $R_{i+1}^* = K_i \oplus R'_{i+1}$
 $Res_T = h(N_s || K_i || R_{i+1}^* || hd^*)$
 $SID_T^{i+1} = h(SID_T^i || K_i)$
 $sk = h(sk || K_i)$
Store : $\{SID_T^{i+1}, sk\}$

✓ سپس، تگ یک پیام پاسخ M_3 ساخته و به سرور S می‌فرستد:

$$M_3: \{R_{i+1}^*, Res_T, hd^*\}$$

✓ پس از دریافت پیام پاسخ M_3 ، سرور S ابتدا hd_i را محاسبه می‌کند:

$$hd_i = h(sk_i \parallel N_s) \oplus hd^*$$

✓ سپس سرور مقدار $K_i = FE.Rec(R_i, hd_i)$ را محاسبه می‌کند.

✓ و سپس سرور خروجی تابع درهمساز Res_T را محاسبه و T را تأیید می‌کند.

✓ اگر تأیید موفقیت آمیز باشد، S محاسبه ذیل را انجام می‌دهد:

$$C_{i+1} = h(C_i \parallel K_i), R'_{i+1} = K_i \oplus R_{i+1}^*, SID_T^{i+1} = h(SID_T^i \parallel K_i), h(sk \parallel K_i)$$

✓ سپس سرور sk و (C_{i+1}, R'_{i+1}) را برای دور بعدی احراز هویت $(i+1)$ ذخیره می‌کند.

در غیر این صورت، S روند احراز هویت را خاتمه می‌دهد و از برچسب می‌خواهد که با استفاده از یکی از جفت‌های بلااستفاده $(pid_x, k_{emx}) \in (PID, k_{em})$ دوباره امتحان کند.

هر بار که از یک جفت استفاده می‌شود، باید از هر دو انتها حذف شود. در این حالت، سرور S یکی از جفت‌های اضطراری بلااستفاده، را از (C_{em}, R_{em}) انتخاب می‌کند و یک هویت سایه‌ای جدید به برچسب T ارائه می‌شود. سرانجام، جفت استفاده شده از جفت‌های اضطراری نیز باید از (C_{em}, R_{em}) حذف شود.

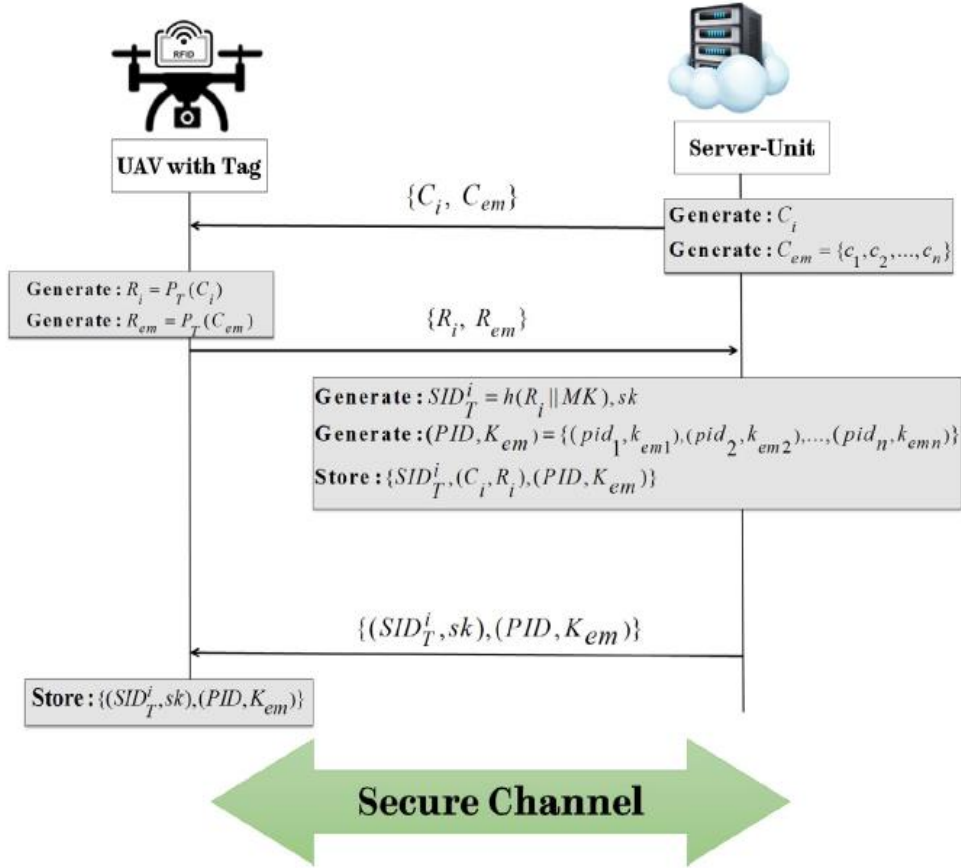


Fig. 2. Setup Phase of the Proposed Scheme.

در طرح پیشنهادی ما، برچسب فقط می‌تواند از تعداد t جفت‌های (PID, k_{em}) و (C_{em}, R_{em}) استفاده نشده استفاده کند جای که $t \leq n-1$ باشد. پس از آن، تگ باید درخواست بارگذاری مجدد کند.

در این صورت، تگ باید هویت سایه $(n+1)$ خود را همراه با $nonce Nt$ و پیام (بارگذاری مجدد) "Re-Load" در درخواست احراز هویت M_1 وارد کند. سپس، پس از استنتاج کردن از برچسب، سرور S مجموعه‌ای از جفت‌های جدید را تولید می‌کند و سپس از کلید جلسه K_i برای رمزگذاری آنها استفاده می‌کند و متعاقباً آنها را به تگ ارسال می‌کند. جزئیات مرحله احراز هویت ما در شکل ۳ ارائه شده است.

حمله کوانتومی به پروتکل:

➤ حمله کننده یا دشمن Res_s را در میانه می‌گیرد.

➤ سپس به کمک کامپیوتر کوانتومی (به کمک الگوریتم سایمون) یک Y پیدا می‌شود که به صورت زیر است:

$$h(Y) = h(N_t \| sk \| N_s^*)$$

➤ حال ما Y را بصورت زیر بدست آوردیم:

$$Y = N_t \| sk \| N_s^*$$

➤ اکنون با جستجوی کامل sk را مییابیم.

➤ با توجه به کار صورت گرفته در مرجع [۲۱] جدول شماره ۱ در بهترین حالت sk ، ۱۲۸ بیتی است که به کمک الگوریتم گراور (روی کامپیوتر کوانتومی) با جستجوی کامل 2^{64} حالت شکسته می‌شود.

➤ بنابراین برای اینکه این پروتکل در برابر حملات کوانتومی نیز مقاوم باشد می‌بایستی طول کلید sk به اندازه کافی بزرگ در نظر گرفته شود. مثلاً طول آن حداقل ۵۱۲ بیت باشد.

۳- تجزیه و تحلیل امنیتی

در این بخش، ما به طور رسمی امنیت طرح احراز هویت ناشناس سبک وزن واقعی پیشنهادی را در مورد الزامات امنیتی اصلی تجزیه و تحلیل می‌کنیم.

۳-۱- مدل امنیتی

اکنون مدل امنیتی Ouafi و Phan [۲۸] را برای تحلیل امنیت و حریم خصوصی طرح پیشنهادی در نظر می‌گیریم. این مدل به حریف A اجازه می‌دهد تا ارتباط رادیویی بین تگ و خواننده را پنهان کند. علاوه بر این، دشمن همچنین می‌تواند هر گونه حمله فعال یا غیرفعال را انجام دهد. در این راستا، A نیاز به مدل سازی پرس و جوهای زیر در زمان چند جمله ای دارد.

اجرا کردن (S, T, i) : این پرس و جو مدل سازی حملات غیر فعال را نشان می‌دهد. در این زمینه، حریف تمام پیام‌های ارسال شده بین تگ T و واحد خواننده-سرور S را در جلسه i استراق سمع می‌کند. در نتیجه، مهاجم باید بتواند تمام داده های رد و بدل شده بین تگ T و واحد خواننده-سرور S را به دست آورد.

ارسال (U, V, m, i) : این پرس و جو مدلسازی حملات فعال را نشان می‌دهد. در اینجا، یک حریف A مجاز است در جلسه یکم به عنوان خواننده قانونی U جعل کند و یک پیام m را به تگ V ارسال می‌کند.

پرس و جو (T, m_1, m_2) : این پرس و جو توانایی حریف را برای بررسی یک برچسب مدل می‌کند. برای این کار، m_1 را به T می‌فرستد و m_2 را از T دریافت می‌کند.

مسدود کردن (A): این پرس و جو توانایی دشمن را برای راه اندازی یک حمله DoS مدل می کند. در اینجا، حریف A مجاز است بخشی از پروتکل را مسدود کند و همگام سازی بین تگ T و سرور S را قطع کند.

خراب کردن (T, K): در این پرس و جو، مهاجم A اجازه دسترسی به اطلاعات مخفی (K) ذخیره شده در حافظه تگ را دارد.

امتحان (T_0 و T_1 و T_2): این پرس و جو مفهوم غیر قابل تشخیص حریم خصوصی غیرقابل ردیابی (UPriv) را تعریف می کند. اگر طرف یک پرسش آزمایشی را پذیرفته باشد و از او خواسته شود، بسته به یک بیت $b \in \{0, 1\}$ ، که به طور تصادفی انتخاب شده است، توسط دشمن T_b از مجموعه $\{T_0, T_1\}$ داده می شود.

می گوییم، اگر A بتواند بیت b را به درستی حدس بزند، برنده بازی می شود. برای اینکه مفهوم معنادار باشد، مهم است که یک جلسه آزمون باید به معنای تعریف ۲ تازه باشد.

۴- نتیجه گیری

در این مقاله یک پروتکل جدید احراز هویت مبتنی بر PUF برای حفظ حریم خصوصی برای یک سیستم پهنپاد مجهز به RFID ارائه کردیم که می تواند چندین ویژگی امنیتی ضروری را تضمین کند. انعطاف پذیری در برابر حملات انسان در وسط، حریم خصوصی در برابر استراق سمع و غیره (همانطور که در بخش ۳ مورد بحث قرار گرفت)، که برای هر برنامه مبتنی بر RFID ضروری است. امنیت و تجزیه و تحلیل عملکرد نشان می دهد که طرح احراز هویت پیشنهادی ما ایمن و کارآمد است. از این رو، می تواند برای چندین راه حل امنیتی عملی مبتنی بر RFID با استفاده از PUF مفید باشد. همچنین نشان داده شد که این پروتکل در برابر حملات کوانتومی نیز ایمن است.

- [١] A. Grover, H. Berghel, A survey of RFID deployment and security issues, Inf. Process. Syst. 7 (4) (2011) 561–580.
- [٢] J. Banks, D. Hanny, M. Pachano, L. Thompson, RFID Applied, Wiley, 2007.
- [٣] P. Gope, et al., An enhanced secure delegation-based anonymous authentication protocol for PCSs, Int. J. Commun. Syst. (2019).
- [٤] P. Gope, B. Sikdar, An efficient privacy-preserving authenticated key agreement scheme for edge-assisted internet of drones, IEEE Trans. Veh. Technol. (2020) <http://dx.doi.org/10.1109/TVT.2020.301877>, 2020.
- [٥] P. Gope, et al., A secure IoT-based modern healthcare system with fault-tolerant decision-making process, IEEE J. Biomed. Health Inf. (2020) <http://dx.doi.org/10.1109/JBHI.2020.3007488>.
- [٦] A. Khattab, Z. Jeddi, E. Amini, M. Bayoumi, RFID Security Threats and Basic Solutions, Springer International Publishing, Cham, 2017, pp. 27–41.
- [٧] P. Peris-Lopez, J.C. Hernandez-Castro, J.M. Estevez-Tapiador, A. Ribagorda, RFID Systems: A Survey on Security Threats and Proposed Solutions, Springer Berlin Heidelberg, Berlin, Heidelberg, 2006, pp. 159–170.
- [٨] P. Kocher, J. Jaffe, B. Jun, Differential power analysis, in: Proc. CRYPTO'99, in: LNCS, vol. 1666, Springer-Verlag, 1999, pp. 388–397.
- [٩] P.S. Ravikanth, Physical One-Way Functions (Ph.D. thesis), Massachusetts Institute of Technology, 2001.
- [١٠] G. Suh, S. Devadas, Physical unclonable functions for device authentication and secret key generation, in: Design Automation Conference, 2007, DAC '07, 44th ACM/IEEE, 2007, pp. 9–14.
- [١١] J. Bringer, H. Chabanne, T. Icart, Improved privacy of the tree-based hash protocols using physically unclonable function, in: Proceedings of the 6th

International Conference on Security and Cryptography for Networks, SCN '08, Springer-Verlag, Berlin, Heidelberg, 2008, pp. 77–91.

[15] A.-R. Sadeghi, I. Visconti, C. Wachsmann, PUF-enhanced RFID security and privacy, in: Secure Component and System Identification – SECSI'10, Cologne, Germany, 2010.

[16] L. Kulseng, Z. Yu, Y. Wei, Y. Guan, Lightweight mutual authentication and ownership transfer for RFID systems, in: Proceedings of the IEEE Conference on INFOCOM 2010, RFIDSec'11, Springer-Verlag, Berlin, 2010.

[17] M. Akgun, M.U. Caglayan, Puf based scalable private RFID authentication, in: Proceedings of the 2011 Sixth International Conference on Availability/Reliability and Security, ARES '11, IEEE Computer Society, Washington, DC, USA, 2011, pp. 473–478.

[18] S. Kardas, S. elikc, M. Yıldız, A. Levi, Puf-enhanced offline RFID security and privacy, J. Netw. Comput. Appl. 35 (6) (2012) 2059–2067.

[19] K. Lee, J.G. Nieto, C. Boyd, A state-aware RFID privacy model with reader corruption, in: Cyberspace Safety and Security, in: LNCS, vol. 7672, Springer, 2012, pp. 324–338.

[20] S. Vaudenay, On privacy models for RFID, in: AsiaCrypt 2007, in: LNCS, vol. 4833, Springer, 2007, pp. 68–87.

[21] S. Pandey, S. Deyati, A. Singh, A. Chatterjee, Noise-resilient SRAM physically unclonable function design for security, in: IEEE 25th Asian Test Symposium, ATS, Hiroshima, 2016, pp. 55–60. <http://dx.doi.org/10.1109/ATS.2016.65>.

[22] A.V. Herrewewege, S. Katzenbeisser, R. Maes, R. Peeters, et al., Reverse fuzzy extractors: Enabling lightweight mutual authentication for PUF-enabled RFIDs, in: A.D. Keromytis (Ed.), FC 2012, in: LNCS, vol. 7397, Springer, Heidelberg, 2012, pp. 374–389.

[۲۰]D. Moriyama, S. Matsuo, M. Yung, PUF-Based RFID authentication secure and private under complete memory leakage, in: IACR Cryptology ePrint Archive, ۲۰۱۳Vol. 712, 2013, <http://eprint.iacr.org/2013/712>.

[۲۱]A. Aysu, E. Gulca, D. Moriyama, P. Schaumont, M. Yung, End-to-end design of a PUF-based privacy preserving authentication protocol, in: Cryptographic Hardware and Embedded Systems, CHES, in: LNCS, vol. 9293, 2015, pp.

۵۷۶–۵۵۵

[۲۲]P. Gope, J. Lee, T.Q.S. Quek, Lightweight and practical anonymous authentication protocol for RFID systems using physically unclonable functions, IEEE Trans. Inf. Forensics Secur. 13 (11) (2018) 2831–2843.

[۲۳]Y. Dodis, J. Katz, L. Reyzin, A. Smith, Robust fuzzy extractors and authenticated key agreement from close secrets, in: Advances in Cryptology, CRYPTO, in: LNCS, vol. 4117, Springer, 2006, pp. 232–250.

[۲۴]Y. Dodis, L. Reyzin, A. Smith, Fuzzy extractors: How to generate strong keys from biometrics and other noisy data, in: Advances in Cryptology, EUROCRYPT, in: LNCS, vol. 3027, 2004, pp. 523–540.

[۲۵]X. Boyen, Reusable cryptographic fuzzy extractors, in: ACM Conference on Computer and Communications Security, ACM CCS, ACM, 2004, pp. 82–91.

[۲۶]C. Bosch, J. Guajardo, A.R. Sadeghi, J. Shokrollahi, P. Tuyls, Efficient helper data key extractor on FPGAs, in: Cryptographic Hardware and Embedded Systems, CHES, in: LNCS, vol. 5154, Springer, 2008, pp. 181–197.

[۲۷]J. Delvau, D. Gu, I. Verbauwhede, M. Hiller, J. Yu, Efficient fuzzy extraction of PUF-induced secrets: Theory and applications, in: Cryptographic Hardware and Embedded Systems, CHES, in: LNCS, vol. 8913, Springer, 2016, pp. 412–430.

[۲۸]K. Ouafi, R.C.-W. Phan, Privacy of recent RFID authentication protocols, in: Information Security Practice and Experience, Springer, 2008, pp. 263–277.