بررسی کلاسهای متفاوت پروتکل های تصدیق RFID

چکیده:

سامانه بازشناسی با امواج رادیویی (RFID) تکنولوژی به روز و در حال پیشرفتی است. محدودیت های اصلی تکنولوژی RFID موارد امنیتی و حریم شخصی هستند. بسیاری از روش ها، از جمله رمزنگاری، تصدیق و تکنیکهای سخت افزاری، برای گذر از مشکلات امنیتی و حریم شخصی ارائه شده اند. این مقاله روی پروتکلهای تصدیق یا تایید متمرکز شده است. ترکیب محبوبیت تکنولوژِی RFID و نا امن بودن آن منجر به سیل پروتکلهای مشترک تصدیق شده است. پروتکلهای تصدیق به عنوان کامل، ساده، سبک و فوق سبک طبقه بندی می شوند. از سال 2002 تا به الان، تحقیقات مهمی انجام شده و پروتکلهای بسیاری نیز عرضه شده اند که برخی از این پروتکلها نیاز به ارتقا دارند. مقاله پیش رو پروتکلهای تصدیق مشترک RFID اخیرا ارائه شده را طبق کلاس تصدیق آن با جزئیات کامل بررسی می نماید. پروتکلهای که اکثرا بر اساس امنیت، تکنیک مقایسه شده اند مبتنی بر پروتکل هایی هستند که پروتکلهای ارائه شده با آنها و در نهایت، روش های تایید پروتکلها با یکدیگر مقایسه شده اند. نکات مهم این مقایسه در دو جدول تجمیع شده اند.

کلمات کلیدی: پروتکلهای تصدیق، سامانه بازشناسی با امواج رادیویی ، حمله های شناسایی فرکانس های رادیویی، پروتکلهای تاییده شده سامانه بازشناسی با امواج رادیویی

مقدمه:

سامانه بازشناسی با امواج رادیویی (RFID)

برای شناسایی اشیا با برچسبی کوچک در حال ایجاد است. این تکنولوژی به عنوان یکی از ضروری ترین تکنولوژی های این چند دهه قلمداد می شود[1]. سیستمهای RFID از یک برچسب، یک برچسب خوان و یک سرور دیتابیس پشت خط تشکیل شده است. برچسب خوان شناساگر های نشگانگر های RFID را خوانده و هویت جستجو ها را برای سرور پشت خط می فرستند. اطلاعات بدست آمده از برچسب ورودی به پایگاه داده پشت خط خواهد بود.

برچسب ها در سه طبقه بسته به نوع تغذیه آنها دسته بندی میشوند: برچسب های فعال، نیمه فعال و غیر فعال. برچسب های RFID فعال نیازمند یک باتری داخلی برای تغذیه اجزای الکترونیکی خود و تولید سیگنال برای برچسب خوان هستند. برچسب های نیمه فعال و یا به عبارتی نیمه غیر فعال تنها از قدرت باتری برای روشن کردن مدار میکروچیپ استفاده می کنند و انرژی ساخت سیگنال پاسخ برای برچسب خوان را از سیگنال رادیویی برچسب خوان بدست می اورند. برچسب های غیر فعال تمام انرژی خود را از برچسب خوان بدست می آورند. علاوه بر این برچسب های RFID در سه بازه فرکانسی دسته بندی می شوند: فرکانس ضعیف(125-KHz134) فرکانس بالا(KHz13.56) و فرکانس فوق بالا(860-KHz960)[2]. برچسب های غیر فعالRFID (کم هزینه) که با پهنا های فرکانس فوق بالا کار می کنند امکان نو آوری را در حوزه های کاربرد روزانه، مثل ساخت اکسس کنترل، مدیریت زنجیره تجهیزات و موقعیت یابی کالا ها فراهم کرده اند. استاندارد کد الکترونیکی کالا(EPC) کلاس 1 (C1) نسل دوم(Gen2) مثالی از تکنولوژی های غیر فعال RFID است[3].

برخی متخصصین بر این باورند که بارکد های دیداری با برچسب های RFID ارزان قیمت متصل به کالاهای مورد مصرف جایگزین می شوند[4]. با این حال، به خاطر طبیعت رابطه بی سیم بین برچسب و برچسب خوان، این تکنولوژی تهدیدات بزرگی در زمینه امنیت و حریم شخصی دارد. پروتکل های تایید شده مشترک معمولا برای غلبه به حمله های امنیتی بین برچسب و برچسب خوان استفاده می شوند. از سال 2002 تحقیقات بسیاری انجام شده و پروتکلهای بی شماری ارائه شده اند اما برخی از آنها همچنان نیاز به ارتقا دارند.

---

[1] دپارتمان مهندسی کامپیوتر، دانشگاه دوکوز ایلل، ازمیر 35160، ترکیه

در بخش هایی که در ادامه خواهیم خواند بخش 2 در مورد پروتکل های تایید شده و اهدف آنها بحث و توضیح خواهد داد. بخش 3 پروتکل ها را با توجه به طبقه خود بررسی و مقایسه می کند. بخش 4 مقایسه را ارزیابی می کند. بخش 5 نتایج حاصل از بررسی پروتکل های احراز هویت را ارائه می دهد.

2. پروتکل های تأیید شده

لوپز و همکاران [5] راه حل های بسیاری برای غلبه بر مسائل امنیتی و خطرات مرتبط با سیستم های RFID را معرفی کردند.

در این مطالعه، ما قصد داریم تا پروتکل های تأیید شده را عمیق تر کنیم. تأییدیه اولین قدم در دفاع در مقابل حملات بی سیم به سیستم هایRFID می باشد. هنگامی که سرور هویت برچسب RFID را تأیید می کند، اعتماد به برچسب آغاز می شود.

پس از تاییده، خواننده می تواند به محتویات برچسب های تأیید شده دسترسی پیدا کند.

2.1 دسته های (کلاس های) پروتکل های تأیید شده

چین [6] اظهار داشت که پروتکل های تاییدی به چهار دسته با توجه به هزینه محاسبات برچسب و عملیات پشتیبانی شده تقسیم می شوند.

•پروتکل های کاملا پیشرفته: پروتکل هایی که از رمزگذاری متقارن و نامتقارن و تابع یک طرفه پشتیبانی می کند. مثالها در [7، 8] هستند.

•پروتکل های ساده: پروتکل هایی که از تابع هش و مولد عدد تصادفی پشتیبانی می کند(RNG) . نمونه هایی از این دسته در [9، 10] ارائه شده است.

•پروتکل های سبک: پروتکل هایی که از بررسی افزونگی چرخه ای (CRC)و RNG پشتیبانی می کند. مثالها در [11-14] ارائه شده است.

•پروتکل فوق العاده سبک: پروتکل هایی که به ویژه برای دستگاه های بسیار محدود طراحی شده اند. اینها

پروتکل ها فقط شامل عملیات ساده بیتی (مانندAND ، OR، XOR) در برچسب ها می باشند. مثالها در [15، 16] داده شده است.

2.2 اهداف پروتکل های تأییدشده

با توجه به انواع تهدیدات بالقوه، یک پروتکل تاییدی، در هر دسته ای، باید همه یا بیشتر تهدیدها و خدمات امنیتی زیر را بررسی کند.

تهدیدات امنیتی

•ردیابی حمله: مهاجم می تواند اطلاعات مرتبط با یک برچسب مشخص شده را ردیابی کند.

• حمله عدم سرویس دهی (DoS): آن تلاشی برای تخریب تگ ها با داشتن خوانندگان مخرب که آنها را با اطلاعات بیشتر بجای کنترل آنها بارگذاری می کند.

•حمله غیرهمگامی: مهاجم خواننده و تگ را غیرهمگام می کند.

•حمله مرد میانی: این کنترل جریان پیام را می گیرد.

•حمله جعل هویت: مهاجم یک برچسب معتبر را جعل میکند و به عنوان یک برچسب معتبر عمل می کند.

•حمله کلونینگ: مهاجم اعتقاد خواننده را فریب می دهد که داده ها را از برچسب قانونی دریافت می کند.

•حمله افشاء کامل: مهاجم تمام اطلاعات مخفی تگ را به خطر می اندازد.

•استراق سمع: مهاجم در کانال های ارتباطاتی استراق سمع می کند.

•حمله بازپخش: مأمور یا مهاجم، احتمالا به عنوان بخشی از حمله تظاهرگونه توسط جایگزینی بسته، اطلاعات را قطع و دوباره انتقال می دهد.

خدمات امنیتی

• تایید متقابل: ویژگی که هر دو برچسب و سرور به یکدیگر اعتبار می دهند.

•محرمانه بودن: املاک که تمام اطلاعات مخفی به طور ایمن منتقل می شود.

• در دسترس بودن: ویژگی که طرفین مورد تایید همیشه برای برقراری ارتباط در دسترس است.

•امنیت جلو / عقب: ویژگی که مهاجم نمی تواند اطلاعات محرمانه قبلی / فعلی را به خطر بیاندازد حتی اگر اطلاعات محرمانه فعلی / قبلی را به دست آورد.

•مالکیت قابل انتقال: ویژگی که حریم خصوصی صاحبان فعلی و جدید نقض نمی شود زمانی که صاحب فعلی داده های لازم را به صاحب جدید منتقل می کند.

• ناشناس بودن برچسب: ویژگی که مهاجم نمیتواند از طریق گوش دادن به کانال، یک برچسب را پیدا کند.

• قابل ردیابی: صاحب برچسب می تواند با استفاده از اطلاعات حریم خصوصی محل ذخیره شده در برچسب شناسایی شود.

• مکان خصوصی محل: ویژگی که مهاجم نمی تواند در مورد شیء ردیابی از اطلاعات یک برچسب قضاوت کند.

•حریم خصوصی اطلاعات: ویژگی که تنها خواننده قانونی می تواند به اطلاعات ذخیره شده در برچسب دسترسی داشته باشد.

3. بررسی و مقایسه پروتکل های تأییدی

بر خلاف مطالعه و بررسی سو [17] که در آن پروتکل ها با توجه به خدمات ارائه شده و الگوریتم های استفاده شده طبقه بندی شده اند، این بخش، 22 پروتکل تایید شده پیشنهادی اخیرا RFID را با توجه به کلاس

خود معرفی می کند؛ برخی از پروتکل ها به طور دقیق مورد بررسی و توضیح قرار می گیرند در حالی که سایر پروتوکل ها در جداول به دلیل فضای محدود ارائه شده اند

ستون اول جدول 1 ، 22 پروتکل را بر اساس کلاس خود فهرست می کند که از تمام پیشرفته شروع می شود و به پروتکل فوق العاده سبک ختم می شود .ستون دوم تابعی را ارائه می دهد که پروتکل بر آن مبتنی است. ستون سوم ابزار تأییدیه مورد استفاده برای تصدیق را ارائه می دهد.

جدول1: تکنیکها، تایید و دسته ها پروتوکل تاییدی (پروتوکل، C دسته، F کاملا پیشرفته، S ساده، L سبک، وزن فوق العاده سبک UL)

P	تابع مبتنی بر	تایید شده توسط	EPC	مقایسه با	C
[31]	ECC	**.....**	X	[27, 28, 30]	F
[37]	رمزنگاری کلید عمومی	منطق BAN	X	[38-42]	F
[32]	ECC	مدل پیشگو تصادفی	X	[25، 28، 30،43]	F
[33]	ECC & AES	تست و تحقق آن در دستگاه ها واقعی	X	[25, 28–30]	F
[44]	افزایش فضای کلیدی با استفاده از نانس ها	AVISPA	X	[45–47]	F
[48]	برچسب های NFC حمایت شده از نظر رمزنویسی در داروها	به صورت دستی در [49]	X	[49]	F
[50]	تابع هش یک طرفه و رمزگذاری نیمه تصادفی کلیدها	به صورت دستی در [51]	X	[9, 10, 36, 51, 52]	F
[53]	مبتنی بر هش	.....	X	[36, 51, 54]	S
[55]	مبتنی بر هش	**بصورت دستی**	X	[6, 56–61]	S
[62]	مبتنی بر هش و PRNG	منطق[63]GNY	√	[64-66]	S
[67]	پیچیدگی زمان ثابت	**مدل رقابتی** بیزانتینی[52]	X	[68]	S
[69]	عملیات هش وRNG	منطق[63]GNY	X	[10, 70–75]	S
[76]	تابع هش یک طرفه	منطق[63]GNY	X	[10, 77, 78]	S

[79]	مبتنی بر XOR ، PRNG و CRC	بصورت دستی	√	[42, 80]	L
[81]	مبتنی بر XOR، PRNG	بصورت دستی همانند [82]	√	[83–86]	L
[87]	شاخص برچسب سریع، PRNG وCRC	برنامه شبیه سازی شده	√	[10, 73, 77, 88–91]	L
[92]	یادگیری یکسان با نویز	بصورت دستی همانند[93]	√	[93–96]	L
[97]	یک ژنراتور شبه تصادفی بین خوانندگان و برچسب ها به اشتراک گذاشته شد	AVISPA	√	[98-103]	L
[104]	**جایگزینی و** CRC	**مفسر ساده پروملا**(SPIN)	√	[6, 38, 56, 105]	L
[106]	تبدیل یک بیتی فوق العاده سبک	به صورت دستی	√	[6, 38, 57, 58, 64, 105, 107]	UL
[108]	**مبتنی بر چرخش بیتی XOR**	به صورت دستی	√	[6, 38, 56–58, 105]	UL
[109]	توابع غیرقابل پنهان فیزیکی	PUF	√	[110–112]	UL

ستون EPC فهرست می کند که آیا پروتکل سازگار با EPC Gen2 است یا خیر. ستون "در مقایسه با" پروتکل های دیگر را فهرست می کند که پروتکل با آن مقایسه شده است. آخرین ستون دسته پروتکل تاییدی را ارائه می دهد. مقایسه پروتکل ها بر اساس تهدیدات امنیتی و خدمات امنیتی در جدول 2 ارائه شده است در حالی که جدول 3 نام های مقاله مورد بررسی و سال انتشار را همراه با منابع خود ارائه می دهد.

3-1- پروتکل‌های کاملا پیشرفته

دسته کاملا تکامل‌یافته (پیشرفته) [ی پروتکل‌ها] شامل الگوریتم‌های رمزنگاری است که عمدتا به دو گروه الگوریتم‌های متقارن و نامتقارن تقسیم می‌شوند. الگوریتم‌های نامتقارن مبتنی بر رمزنگاری منحنی بیضی‌شکل (ECC)، از جهت سرویس‌ها و میزان امنیتی که ارائه می‌کنند، قوی به حساب می‌آیند. در مقایسه با سیستم

شیوه‌ای رمزنگاری به روش کلید عمومی (RSA)، سیستم‌های بر پایه‌ی ECC، کوچکتر (کم حجم‌تر)، سریع‌تر و با مصرف انرژی پایین‌تری هستند. از این رو برای سیستم‌های با محدودیت منابع، الگوریتم‌های مبتنی بر ECC انتخاب بهتری نسبت به الگوریتم RSA هستند. اشاره شده است که سیستم RSA، یک متغیّر مبتنی بر ECC دارد. به همین جهت بسیاری از پروتکل‌های تاییده شده بر پایه‌ی ECC، برای اجرای تگ‌هایی یا برچسب هایی (کدهای برنامه‌نویسی) دارای محدودیت شدید ارائه شده‌اند.

در سال 2006، تویلز و همکاران با استفاده از پروتکل شناسایی Schnorr، یک پروتکل شناسایی RFID برپایه‌ی ECC را ارائه کردند. آنها ادعا کردند که این پروتکل، در مقابل جعل‌سازی تگ مقاوم است. با این حال در سال 2008، لی و همکاران نشان دادند که پروتکل تویلز و همکاران، در برابر ردیابی موقعیت مکانی بی‌دفاع است، تایید متقابل و امنیت پیشرو را تضمین نمی‌کند و در مقیاس‌پذیری با نقصان روبه‌رو است. در سال 2007، باتینا و همکاران، بر مبنای پروتکل احراز هویت اوکاماتو، یک پروتکل شناسایی RFID برپایه‌ی ECC را ارائه و اشاره کردند که طرح پیشنهادی آنان (پروتکل ارائه شده‌ی آنان) می‌تواند در مقابل حملات فعال ایمن باشد. با این حال لی و همکاران اظهار داشتند که این پروتکل از منظر حمله‌ی ردیابی موقعیت مکانی و امینت پیشرو آسیب‌پذیر است و همچنین فاقد مقیاس‌پذیری است. لی و همکاران ادعا کردند که سه مشکل یادشده را مرتفع ساخته‌اند، اما مطالعات منتشرشده در سال 2008 نشان داد که طرح پیشنهادی لی و همکاران، در برابر حملات جعل اطلاعات و ردیابی بی‌دفاع است و احراز تایید متقابل را نیز تأمین نمی‌کند.

جدول2. مقایسه پروتکل های تایید از منظر تهدیدهای امنیتی و خدمات امنیتی (F تمام و کمال، S ساده، L خفیف، UL بسیار خفیف)

پروتکل	31	37	32	33	44	48	50	53	55	62	66	67	69	76	79	81	87	92	97	104	106	108	109
تهدیدات امنیتی																							
ردیابی حمله				√			√		√			√	√		√					√	√		

DoS	√	√		√	√	√	√						√	√			√		√			√
همگام سازی	√	√		√	√	√	√	√	√		√	√			√	√	√			√		
مردمیانی	√	√	√	√	√	√	√	√							√		√				√	
حمله عدم پذیرش سرویس	√		√	√	√	√		√	√		√		√	√		√						√
حمله کلونسازی	√			√		√			√		√	√	√									
حمله افشای کامل				√		√			√										√	√	√	
استراق سمع		√		√				√									√	√				
حمله بازپخش	√	√	√	√	√	√		√		√	√	√	√	√	√	√	√		√		√	√
سرویس امنیتی																						
احرازهویت متقابل	√	√	√	√	√	√	√	√			√		√	√	√			√			√	√
محرمانه بودن	√	√		√	√	√	√			√		√				√		√			√	
در دسترس	√				√																	

بودن امنیت رو به جلو	√	√	√	√		√	√	√		√	√	√	√	√	√	√	√	√	√			
امنیت رو به عقب	√			√	√		√	√					√	√		√	√					√
مالکیت قابل انتقال							√															
ناشناس بودن	√		√										√							√		
برچسب قابلیت ردیابی	√	√	√	√		√	√	√		√		√		√	√	√	√					
اختفای موقعیت			√	√						√		√		√	√							
اختفای اطلاعات	√			√	√					√		√		√		√	√					
کلاس																						
کلاس	F	F	F	F	F	F	F	F	F	S	S	S	S	S	S	L	L	L	L	L	L	L
																				UL	UL	UL

در سال 2009، با بازسازی سه مولفه لگاریتم مجزای دارای انحنای بیضی شکل بر اساس دسترسی کنترل شده تصادفی (EC-RAC) [18]؛ طرح های انتقالی شناسه و رمزعبور امن، و تایید هویت سرور با توجه به الزامات

سیستم و ویژگی های امنیتی، لی و همکارانش [22] 6 پروتکل مختلف برای حداقل سازی حجم محاسبات مربوط به برچسب ها، ارائه نموده اند.

در سال 2010، لی و همکارانش [23] پروتکل مبنی بر ECC که به مشکلات ردیابی موجود در پروتکل های ارائه شده در [7، 19] اشاره نموده است را معرفی نموده اند. این طرح تنها برچسب مربوط برای شناسایی خواننده را درنظر گرفته و برچسب تایید اعتبار را نادیده گرفته است. در سال 2011، ژانگ و همکارانش [24] پروتکلی تصادفی و کلیدی مبنی بر ECC را معرفی نموده اند که در واقع شکل بهبود و اصلاح یافته از طرح های لی و همکارانش و تولس و همکارانش، می باشد. این پروتکل در برابر برخی از حملات مربوطه ایمن بوده اما همچنان قادر به ارائه تایید متقابل نمی باشد.

در سال 2014، به منظور دستیابی به تایید متقابل، لائو و همکارانش [25] پروتکل ایمن تایید مبنی بر توانایی ECC همراه با پروتکل انتقال شناسه بازبینی شده، را معرفی نموده اند. با این حال، مطالعات [26- 28] چنین نشان داده اند که پیشنهاد لائو و همکارانش دارای نقص های امنیتی و عملکردی ضعیف می باشد. بعدها در همان سال، با بهره گیری از ECC، چوو [29] پروتکلی برای تایید ارائه کرده و چنین اعلام داشته است که این پروتکل پیشنهادی در برابر حملات مختلف، دارای مقاومت می باشد. با این حال، ژانگ و چی [30] چنین نشان داده اند که پروتکل پیشنهادی توسط چوو از منظر ضمیمه نمودن اطلاعات حریم خصوصی و امکان ردیابی رو به عقب و رو به جلو دارای نقوص و مشکلاتی می باشد. سپس در سال 2015، جین و همکارانش [31] پروتکل تایید متقابل برای محیط های درمانی و بهداشتی مبنی بر ECC پیشنهاد نموده و چنین بیان نموده اند که این پروتکل پیشنهادی در برابر حملات مختلف مقاوم بوده و نسبت به طرح های ارائه شده در [27، 28، 30] عملکرد بهتری از خود ارائه می نماید.

در سال 2016، فاراش و همکارانش [32] چنین نشان داده اند که طرح پیشنهادی توسط ژانگ و همکارانش [30] محافظت پیش فرضی از خود ارائه نمی نماید. اخیرا در سال 2017، ابراهیم و همکارانش [33] پروتکل توانمند و قدرتمند از تایید متقابل بر اساس ECC ارائه و کارآیی این پروتکل با بهره گیری از آخرین نسخه بازبینی شده از تعیین هویت بی سیم و پلاتفورم حسگر (WISP5) ثابت شده است. در پروتکل پیشنهادی، تایید

متقابل تنها در دو مرحله انجام گرفته و در برابر تمامی حملات معمول مقاومت نموده و تمامی الزامات سیستم های امنیتی RFID را برآورد می نماید.

به دلیل زمانبر بودن الگوریتم های نامتقارن، تنها گزینه برای سیستم های RFID این الگوریتم ها، نمی باشند. علاوه بر این، اجرا و پیاده سازی سیستم های RFID همچنان امری چالش برانگیز می باشد. از این رو، برخی از محققین توجه خود را بر طرح های متقارن که شامل دو گروه اصلی: متون رمزی بلوک شده و متون رمزی در جریان، می باشند، متمرکز نموده اند.

جدول 3 منبع شماره و اسامی پروتکل های بررسی شده

شماره مرجع	اسم مقاله و سال انتشار
[31]	پروتکل بازشناسی مشترک RFID برای محیط های درمانی با استفاده از منحنی رمزگذاری بیضی (2015)
[37]	پروتکل بازشناسی مشترک RFID جدید با پیچیدگی پایین و امنیت بالا(2014)
[32]	پروتکل بازشناسی اثبات شده ایمن بر مبنای منحنی های بیضوی در محیط های درمانی(2016)
[33]	استاندارد رمزگذاری پیشرفته پروتکل بازشناسی مشترک بر مبنای رمزنگاری منحنی بیضوی برای RFID اثبات شده با WISP(2017)
[44]	افزایش فضای کلید ها با هزینه ای کم برای بازشناسی RFID
[48]	برچسب های NFC با پشتیبانی از رمزنگاری در دارو ها برای امنیت بیشتر در بیمار(2014)
[50]	HPAP طرح جدید بازشناسی برای سیستمهای RFID(2013)
[53]	پروتکل بازشناسی مشترک برچسب RFID بر مبنای هاش در سیستمهای اطلاعاتی دارو های مراقبت از راه دور (2015
[55]	پروتکل بازشناسی موثر ارائه دهنده امنیت و حریم خصوصی بالا(2016)
[62]	کشف رمزی پروتکل LMAP: یک پروتکل بازشناسی RFID ارزان قیمت(2017)
[67]	پروتکل بازشناسی RFID کاربردی و خصوصی با پشتیبانی از انتقال مالکیت (2013)

[69] RSEL: طرح بازشناسایی RFID سبک، ایمن، کاربردی و ابطال پذیر(2014)

[76] تابع یک سویه هاش بر مبنای پروتکل بازشناسی مشترک سبک RFID (2013

[79] طرح جدیدی برای بازشناسی مشترک سیستم های RFID ارزان قیمت (2016)

[81] پروتکل کاربردی بازشناسی RFID سبک با امنیت حریم خصوصی خط سیر (2017)

[87] ایمن و کاربردی پروتکل بازشناسی RFID سبک بر مبنای فهرست بندی سریع برچسب (2014)

[92] پیشرفتی در پروتکل های بازشناسی سبک خانواده HB برای استفاده کاربردی در سیستمهای RFID (2013)

[97] KEDGEN2: پروتکل ثبت کلید و استخراج برای سیستم های EPC Gen2 RFID (2014)

[104] پروتکل بازشناسی فوق سبک RFID با CRC و جایگشت (2014)

[106] SLAP: پروتکل بازشناسی سبک و فشرده برای سیستمهای RFID ارزان قیمت

[108] کشف رمز پروتکل جدید بازشناسی مشترک فوق سبک برای دستگاه های IoT با استفاده از برچسب های RFID (2017)

[109] امنیت قوی K برای شناسایی پروتکلهای بازشناسی بر مبنای توابع غیر قابل جعل فیزیکی

رمز نگارهای جریان داده سری سریعتر هستند و اعمال آن ساده تر است ولی در مقایسه با رمز گذاری بلاکی ضعیف تر هستند. لذا رمز گذاری های بلاکی محبوب تر هستند و محبوب ترین رمزگذاری بلوکی استاندارد پیشرفته رمزگذاری(AES) است.

شایان ذکر است که فلدهوفر و همکارانش[8] اعمال موفقی از AES را در سال 2004 معرفی کردند. با این حال در سال 2008 کاپس[34] متوجه شد که استفاده از الگوریتم گسترده رمزگذاری ظریف(XTEA) قدرت و منابع کمتری نسبت به AES نیاز دارد. علاوه بر این تحقیقاتی که از AES استفاده می کنند بیشتر به تعداد درگاه ها اشاره می کنند نه اهداف امنیتی پروتکل های بازشناسی، که سوژه اصلی مقاله حاضر است.

3.2 پروتکل های ساده

کلاس پروتکل های ساده شامل پروتکل هایی است که از RNG و یک تابع هش یکسویه پشتیبانی می کنند. اکوبا و همکارانش[35] در سال 2003 به پروتکل قدرتمندی به عنوان مثالی از پروتکل های بر پایه هش دست یافتند. با این حال هزینه جستجو برای برچسب توسط سرور برای این پروتکل بالا است. در همان سال این پروپوزال توسط ویز و همکارانش[10] تحت عنوان پروتکل hash-lock ارتقا یافت و اگر چه پروتکل hash-lock در جایگذاری تگ و کاربردی بودن سرور خوب عمل کرده است، ولی در زمینه امنیت بسیار ضعیف عمل کرده اند. در سال 2006 سودیک مدعی شد که هنوز یک پروتکل بازشناسی RFID ناچیز(YA-TRAP) [9] در مقابل حملات موقعیت یابی مقاومت کرده است.

با این حال در سال 2007 سودیک متوجه نقایص پروتکل قبلی خود شد و پروتکل جدیدی[36] را معرفی کرد، اگر چه پروتکل جدید وی هدف اصلی او را نشان نمی دهد و در مقابل حمله پاسخگویی نفوذ پذیر است. در سال 2011 شین و همکارانش[113] طرحی را نشان دادند که در [9]در مقابل حملات پاسخ گویی و DoS نفوذپذیر بوده ارائه شده و نسخه ای ایمن را معرفی کردند. در همان سال لوپز و همکارانش[114] مدعی شدند که مطلب مطرح شده توسط شین و همکارانش[113] در مقابل حملات جعل هویت و پاسخ گویی بی دفاع است و مفهوم جدیدی را تحت عنوان سیستم هایRFID امنیت ناشکیبا (IS-RFID) معرفی کردند.

در سال 2012، ین و همکارانش[115] متوجه شدند که مدارک داروی تولید شده توسط IS-RFID به راحتی توسط بیمارستان قابل تغییر است. در سال 2012 شن و همکارانش[116] پیشنهاد پروتکل مقاومت جعلی دادند که در مقابل حملات جعل هویت، عدم همگام سازی، و ردیابی پذیری مقاومت کند. در سال 2012 چو و همکارانش[65] به پروتکل بازشناسی مشترک بر مبنای تابع هش دست پیدا کردند که از کار قبلی وی[54] نشأت گرفته بود. در سال 2012 و 2013 طرح چو و همکارانش[65] توسط کیم و همکارانش[117،118] مورد آنالیز قرار گرفت و ضعف شدید آن در مقابل حملات عدم همگام سازی کشف شد.

در سال 2014 صف خانی و همکارانش[119] نیز طرح چو و همکارانش[65] را آنالیز کردند و نشان دادند که در مقابل عدم همگام سازی، جعل هویت برچسب و برچسب خوان نفوذ پذیر است. علاوه بر این، طرحی که در [117،118] بر مبنای فعالیت های انجام شده در [65] مطرح شد توسط [119] آنالیز شد و نیز همان نواقص را داشت. در سال 2015 پروتکل باز شناسی مشترک دیگری بر مبنای تابع هش توسط سیرواستاوا و

همکارانش [53] معرفی شد و از نظر کیفی با پروتکل های معرفی شده در [36،51،54] مقایسه و برتر از آنها شناخته شد. در سال 2016 شن و همکارانش[55] پروتکل بازشناسی RFID کاربردی(ERAP) را معرفی و ادعا کردند در مقایسه با تحقیقات پیشین، پروتکل آنها در مقابل انواع مختلف حملات با هزینه کم مقاومت می کند،که نیازهای برچسب های RFID با منابع اجباری بالا را برآورده می کند. در نهایت در سال 2017 ، لی و همکارانش[62] که پروتکل بازشناسی مشترک سبک(LMAP) [120] در مقابل برخی حملات و تمامیت اطلاعات نفوذ پذیر است. برای بهبود وضعیت امنیت و حریم خصوصیLMAP، نسخه ارتقا یافته ای از LMAP را معرفی کرده و مدعی شدند که پروتکل آنها تمام نیاز های برنامه های RFID را برطرف کرده و در مقابل حملات رایج مقاومت می کند.

از دیگر پروتکل هاییی که ممکن است در این دسته قرار بگیرد و ارزش اشاره به آن را داشته باشد خانواده پروتکل هوپر و بلوم(HB) است. در سال 2001 هوپر و بلوم پروتکل سبک فوق العاده ای را مطرح کردند که تنها از اپرتور های AND و XOR در بردارهای باینایری و یک بیت نویز به نام بیت HB [94] استفاده می کند و می توان آن را از طریق یک رویداد فیزیکی تولید کرد. برای مقاومت در برابر حملات ضمنی، پروتکل وابسته به پیچیدگی محاسباتی یاددگیری پاریتی به همراه مشکل نویز است.

پروتکل HB برای FRID طراحی نشده بود و به عنوان سبک یا فوق سبک طبقه بندی نشده بود. بعد از آن خانواده پروتکل های سبک بر مبنای پروتکل HB معرفی شد. از آنجایی که پروتکل HB در مقابل حملات ضمنی مقاومت می کند، جولز و ویز در سال 2005 پروتکل تغییر یافته شده ای را تحت عنوان پروتکل +HB [93] معرفی کردند که در مقابل حملات فعال مقاومت کند. آنها مدعی شدند که پروتکل آنها سبک ولی ممکن است نتوان بر روی برچسب های RFID اعمال کرد و استفاده از نسخه دو دوری آن ممکن است ایمن نباشد. همچنین در سال 2005، گیلبرت و همکارانش [14] اذعان داشتند که پروتکل +HB در مقابل حملات فعال زمان خطی بی دفاع است.

در سال 2006، برینگر و همکارانش[11] پروتکل +HB را بهینه سازی کردند تا به پروتکل ++HB دست پیدا کنند که در مقابل حمله گیلبرت و همکارانش مقاومت کند. با این حال، برای شناسایی حملات، نیازمند توابع یونیورسال هش و محتوای کلید های امنیتی مضاعف هستند. در سال 2007 مونیلا و همکارانش[95] ایده رند

کردن را معرفی کرده و پروتکل جدیدی تحت عنوان HB-MP ارئه دادند که در مقابل نقایص پروتکل های HB و +HB موثر است.

در سال 2008 گیلبرت و همکارانش[121] کشف کردند که یک حمله غیر فعال ساده می تواند هویت یک برچسب واقعی را با استراق سمع یک مکالمه جعل کند. در سال 2008 پروتکل #HB به عنوان نسخه ارتقا یافته در زمینه پروتکل #HB تصادفی معرفی که در همان مقاله[122] توضیح داده شد. پروتکل #HB در مقابل کلاس گسترده ای از حملات فعال شامل حمله فعال گیلبرت و همکارانش به پروتکلهای HB و HB-MP مقاومت است و بر خلاف پروتکل ++HB، پروتکل #HB نیازمند سخت افزار اضافه که پیچیدگی پروتکل HB را افزایش دهد نیست. همچنین در سال 2008 لنگ و همکارانش[96] پروتکل HB-MP را با معرفی پروتکل HB-MP+ ارتقا دادند. یون و همکارانش[123] متوجه شدند که پروتکل HB-MP+ کارایی دفاعی واقعی در مقابل حملات فعال پیشرفته یا روش های قوی ای برای مقابله با مشکل ردیابی ندارد، و به دنبال آن پروتکل HB-MP++ را معرفی کردند. باز هم در سال 2008 کوافی و همکارانش[124] یک حمله با حضور یک انسان در آن روی پروتکل #HB انجام دادند و یک راز به اشتراک گذاشته شده بین طرفین در حال کالمه را بدست آوردند.

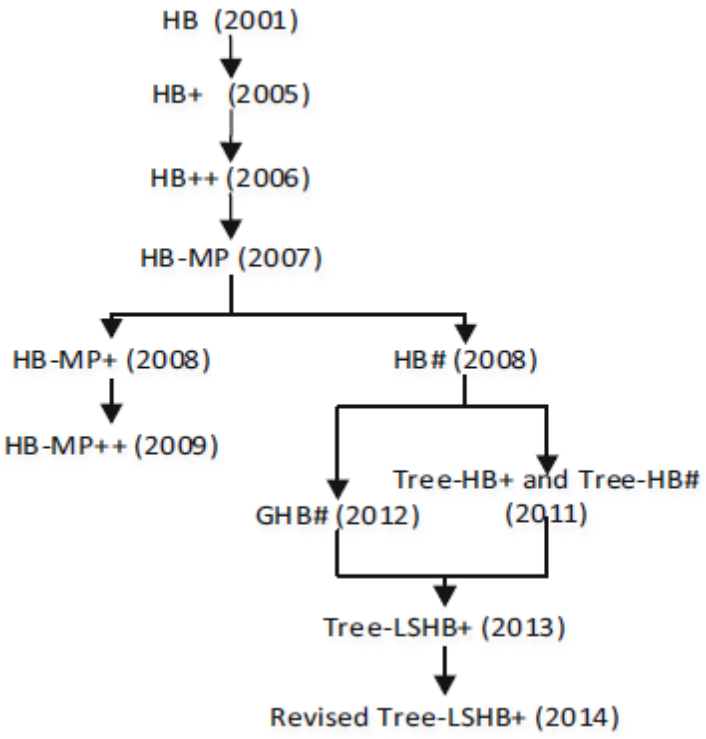
در سال 2009 هالوی و همکارانش[125] نشان دادند که پروتکل های PRF محور از جمله پروتکل های +HB و #HB برای برچسب های ارزان قیمت کارایی ندارد و پروتکل های درختی +HB و درختی #HB را معرفی کردند. در سال 2012 پروتکل GBH# [126] ایجاد و ادعا شد می تواند در مقابل حملات با حضور یک انسان مقاومت کند، حمله ای که یک حمله موثر برای پروتکل #HB بود. با این حال، با معرفی پروتکل درختی LSHB+ [128] در سال 2013 دنگ و همکارانش مدعی شدند که پروتکل های درختی و پروتکلهای HB معمولی تنها بازشناسی یک سویه دارند، تنها برچسب توسط برچسب خوان بازشناسی می شوند و آنها بازشناسی مشترک را اضافه کردند. در نهایت پروتکل LSHB+ درختی نمی تواند در مقابل حملات افشای اسرار، عدم همگامسازی، و قابل ردیابی بودن مقاومت کند[128]. در [128] نسخه بازبینی شده ای از LSHB+ درختی ارائه و ادعا شد نسبت به پروتکل LSHB+ درختی قبلی برتری دارد. تکامل خانواده پروتکل های HB در شکل یک نشان داده شده است. دیگر پروتکل های بررسی شده رد جدول 1 و2 نشان ارائه شده اند.

3.3 پروتکل های سبک

کلاس پروتکل های سبک شامل پروتکلهایی است که نیازمند توابع ساده ای از جمله کد CRC و یک RNG هستند و بیشتر شامل پروتکل های است که تایید کننده استاندارد های EPC C1 Gen 2 هستند. کارکردهایی که از EPC C1 Gen2 پشتیبانی می کنند ممکن است برای مسائل امنیتی زیاد کاربردی نباشد و از همین جهت ارتقای آنها از اهمیت بالایی برخوردار است. علاوه بر این برخورد با مشکلات جدید در زمان حل مشکلات مد نظر امری طبیعی به شمار می رود. در پروتکل های تایید شده با استاندارد EPC C1 Gen2 مشکل امنیتی اصلیCRC-16 است(که به موجب ضعف جبری CRC است

$$((a \oplus b) = CRC\ (a) \oplus CRC(b)$$

در سال 2005 جولز[129] جز اولین افرادی بود که راه حل مورد تایید EPC C1 Gen2 را ارائه داد و مدعی شد که در مقابل شبیه سازی و کلاه برداری مقاوم است. در همان سال کارثیکیان و همکارانش[130] پروتکلی معرفی و از XOR و توابع ماتریس استفاده کردند تا قابل ردیابی نباشند و از تایمر و بروزرسانی کلید برای دستیابی به بازشناسی مشترک استفاده کردند.



شکل 1 – تکامل خانواده HB

در سال 2006، دوک و همکاران[13] نشان داد که طرح جولز[129] دچار درز های اطلاعاتی و حریم خصوصی است. علاوه بر این پروتکل جدیدی را معرفی کردند که از CRC، XOR، و یک تولید کننده اعداد شبه تصادفی(PRNG) برای تضمین امنیت اطلاعات تعاملی استفاده می کند، تا به بازشناسی و همگام سازی بروز رسانی های کلید های امنیت دست پیدا کند. با این حال، پروتکل آنها در مورد حمله DoS و امنیت پیشرونده نفوذ پذیر است.

در سال 2007، شین و همکارانش[12] هم تحقیقات کاثیکیان و همکاران[130] و دوک و همکارانش[13] دست خوش تغییر کردند تا پروتکل جدیدی به نام پروتکل شین و چن (CC) را معرفی کنند که مدعی هستند به امنیت پیشرونده و همچنین مقاومت در برابر حمله های DoS بدست آورده اند؛ با این حال اشتباه بودن اهداف امنیتی مورد نظر با استفاده از ویژگی خطی عمل CRC استفاده شده در پروتکل، ثابت شد. در همان سال، لو و همکارانش[131] پروتکل CC در زمینه امنیت دیتا حریم خصوصی و کارایی بهبود بخشید ولی پروتکل CC همچنان نسبت به استراق سمع و ردیابی موقعیت جغرافیایی نفوذ پذیر است.

در سال 2009، لوپز و همکارانش[132] متوجه شدند که پروتکل CC نمی تواند در مقابل جعل هویت برچسب و برچسب خوان، عدم همگام سازی و حملات ردیابی مقاومت کند. در سال 2010، یه و همکارانش[133] پروتکل جدیدی را تحت عنوان پروتکل رمز ایمن از راه دور(SRP) ارائه دادند که پیاده سازی آن ساده و سریع بوده و ادعا کرده اند که نه تنها مشکلات پروتکل CC را رفع کرده است بلکه دقت عملکرد کلی را نیز افزایش داده است. با این حال حبیبی و همکارانش[83و134] متوجه شدند که پروتکل SRP در مقابل حملات ردیابی و درز اطاعات بی دفاع است و اینکه پیچیدگی یک حمله موفق تنها 2^{16} است و آنها SRP را بهبود بخشیده و نسخه جدیدی از آن را معرفی کرده اند.

در سال 2014، محمدی و همکارانش[120] طرحی که در [83] معرفی شده بود را مطالعه و نشان دادند که در مقابل حمله ای که پارامترهای رمزی را نشان بدهد، حمله جعل هویت برچسب، حمله عدم همگام سازی دیتا، حمله ردیابی نفوذ پذیر است. به علاوه آنها طرحی که در [83] ارائه شده بود را ارتقا داده و طرحی را مطرح کردند که به آن پروتکل سبک بازشناسی مشترک ارتقا یافته(ILMAP) می گویند. بعدها در سال 2014 علوی و همکارانش[135] پروتکل ILMAP را بررسی و نشان دادند که در مقابل حمله ای که پارامترهای مخفی آن را

نشان دهد، حمله به یکپارچگی اطلاعات، حمله کشف اطلاعات پیشرونده برچسب خوان، حمله ردیابی و حمله های ردیابی رو به جلو و رو به عقب نفوذ پذیر است. علاوه بر آن در سال 2013 پنگ و همکارانش [136] با تغییر پروسه هایی در ILMAP از مبنای پروتکل SRP پروتکل بازشناسی ای به نام +SRP معرفی کردند و ادعا کردند بر ضعف های پروتکل SRP غلبه کرده و پیچیدگی یک حمله موفق را به 2^{23} افزایش داده اند.

با این حال در سال 2015 ونگ و همکارانش[137] پروتکل +SRP را آنالیز کرده و نشان دادند که به خاطر نقص معروف عملکرد CFC در مقابل حمله های عدم همگام سازی و در مقابل حمله ی افشای منفعل با ضریب پیچیدگی O (2^{16}) نفوذ پذیر است. علاوه بر آن، نسخه بروز رسانی شده +SRP به نام ++SRP معرفی شد و ادعا شد می تواند د مقابل حملات افشا کننده با ضریب پیچیدگی O(2^{23}) مقاومت کند و این به معنی ارائه امنیتی بالاتر از نسخه اسبق خود را داراست.

در سال 2016 معروف و همکارانش[79] طرح بازشناسی مشترک جدیدی را مطرح کردند که مطابق با استاندارد EPC C1 Gen2 بود. آنها اینطور می گفتند که طرح آنها در زمینه حملات امنیتی مقاوم است، از طرح های قبلی بهتر بوده و به علت استفاده از اپراتور های ساده (XOR، CRC و PRNG) به راحتی می توان در سیستمهای RFID اعمال کرد. در نهایت در سال 2017 ژانگ و همکارانش[81] پروتکل بازشناسی RFID سبکی را با مسیر امنیت حریم شخصی قوی(LAP-STP) معرفی کردند. آنها اینطور اطلاع رسانی کردند که پروتکل آنها می تواند حملات متفاوتی را تحمل کرده و ضامن مسیر حریم شخصی قوی باشد. دیگر پروتکل های بررسی شده در جداول 1و 2 ارائه شده اند.

3.4 پروتکل های فوق سبک

پروتکل های فوق سبک مخصوصا برای دستگاه های بسیار ضروری ساخته شده اند که تنها از اپراتور های بیتی (مثلXOR، OR،AND)در آنها استفاده شد. بعد از عرضه Gen2 در سال 2006، لوپز و همکارانش پروتکل های RFID سبکی را تحت عنوان پروتکل های بازشناسی مشترک فوق سبک (UMAPها) را معرفی کردند و پروتکل بازشناسی مشترک ساده گرا(M^2AP)،[56] پروتکل بازشناسی مشترک سبک(LMAP) [57] و پروتکل بازشناسی مشترک موثر(EMAP) [58] که فقط از توابع مثلثاتی(∨،∧،⊕) و جمع استفاده می کند را در بر گرفتند.این خانواده از نظر هزینه محاسباتی و هزینه نگهداری مناسب برچسب های RFID ارزان قیمت هستند.

با این حال در سال 2007 لی و همکارانش[15،16] حملات متعددی را به M^2AP، LMAP و EMAP ارائه دادند. در همان سال شین[6] گفت UMAP ها در مقابل حملات بسیاری نفوذ پذیر هستند، عملیات چرخش را معرفی کرد و بازشناسی قوی و یکپارچگی قوی(SASI) را معرفی کرد. با این حال به خاطر استفاده از توابع مثلثاتی(⊕،∨)، و تعداد محدود چرخش ها و جمع بستن ها، پروتکل SASI در مقابل حملات متعددی نفوذپذیر است و این امر توسط [138،139] نشان داده شده است. بعد ها در سال 2009 لوپز و همکارانش[105] از XOR که در توابع و جمع های تو در تو نگه داری شده استفاده و پروتکل تار عنکبوت را معرفی کردند که نشأت گرفته از پروتکل SASI بود.

با این حال در سال 2010 تاگرا و همکارانش حمله ی عدم همگام سازی را برروی تار عنکبوت انجام دادند. بعد از تار عنکبوت، لوپز و همکارانش[141] قدری LMAP را ارتقا داده و پروتکل بازشناسی فوق سبکی (ULAP) را معرفی کردند که برای غلبه بر حملات ضمنی تنها از جمع و توابع مثلثاتی استفاده می کند. در همین حال ریال در سال 2010 حمله ای ضمنی بروس ULAP توسط ونگ و همکارانش[142] انجام شد.

در سال 2012 تیان و همکارانش[38] پروتکل بازشناسی RFID فوق سبک جالبی را تحت عنوان پروتکل بازشناسی RFID با جایگشت(RAPP) را معرفی کردند که فقط سه عملیات شامل XOR بیتی، چرخش به چپ و جایگشت است. با این حال وزن همینگ چرخش و جاگشت تغییر ناپذیر است(یعنی وزن همینگ خروجی دو عملیات با وزن همینگ اولین پارامتر برابر است) به خاطر ویژگی های جایگشت، ژوانگ و همکارانش[143] در سال 2013 دو حمله به RAPP داشت که باعث می شود برچسب علاوه بر حملات عدم همگام سازی و پاسخگویی به حالت DoS در بیاید.

علاوه بر این در سال 2013 ژوان و همکارانش[144] با استفاده از عملیات های تجمیع(تجمیع دو رشته بیتی) و تفکیک(عکس تجمیع) پروتکل بازشناسی جدید را تحت عنوان پروتکل بازشناسی RFID فوق سبک کاربردی(EURFID) معرفی کنند. با این حال، در همان سال همان نویسنده[66] کشف کرد که پروتکل EURFID درشرایط تداخل برچسب ها به خوبی عمل نمی کند و پروتکل بازشناسی RFID را برای برچسب های ارزان قیمت(RAPLT) معرفی کرد که عملیات تجمیع و تفکیک جدیدی بر مبنای پروتکل فوق سبک است. با این وجود،طبق گفته های ژوانگ و همکارانش[145] RAPLT در مقابل حملات پاسخگویی و عدم همگام

سازی، و محافظت از یکپارچگی اطلاعات و حریم خصوصی کاربر نفوذ پذیر است. در سال 2015 ونگ و همکارانش[137] حمله افشا سازی را بر روی RAPLT [66] با استفاده از ویژگی خطی عملیات تجمیع و حمله عدم همگام سازی را روی +SRP [136] را با استفاده از ویژگی خطی عملیات CRC انجام دادند. آنها نسخه ای بهینه شده و کاربردی از پروتکل +SRP را که با استاندارد EPC C1 Gen2 همخوانی دارد و توسط ++SRP را معرفی کردند. آنها مدعی شدند که این پروتکل می تواند در مقابل حمله کامل جستجو مقاومت کند.

در سال 2016ریال لوو و همکارانش[106] پروتکل بازشناسی مشترک فوق سبک جدیدی را بر مبنای تبدیل ایمن بیتی فوق سبک ارائه دادند. هدف از این کار ارتقای بازشناسی فوق سبک در مقابل مقاومت امنیتی ضعیف در پروتکل های اخیر که بود که در منابع [107] و [64] ذکر شده است. پروتکل آنها تنها از 3 عملکرد بیتی استفاده می کند: XOR، چرخش به چپ و تبدیل. آنها ادعا می کنند پروتکل آنها امن تر از دیگر پروتکلهای مورد مقایسه است، میتواند در مقابل حملات موجود مقاومت کند و نسبت به پروتکل های مورد مقایسه برای سیستمهای RFID ارزان قیمت مناسب تر است. در نهایت در سال 2017 تواری و همکارانش[108] پروتکل بازشناسی مشترک فوق سبکی را ارائه دادند که از XOR بیتی و چرخش به چپ استفاده می کند. آنها اذعان داشتند که پروتکل آنها از تمامیت اطلاعات، یکپارچگی اطلاعات، بی نامی برچسب ها اطمینان حاصل می کند و در مقابل حملات ردیابی و حملات دیگر مقاومت می کند. دیگر پروتکل های ارزیابی شده در این کلاس در جداول 1 و 2 ارائه شده اند.

3.5 روش های بازشناسایی جدید تر

ذکر این موضوع که از روش های بروز تری از جمله استفاده از جستجوی جامع برای فعال کردن حفاظت امنیتی نیز استفاده می شود خالی از لطف نیست. مانیسم تصادفی کردن شناسه گر های برچسب ها برای محافظ از حریم شخصی آنها اولین بار در سال 2003 توسط ویز و همکارانش [10] مطرح شد. با استفاده از یک نانس که توسط یک برچسب و مقدار مخفی، شناسه گر را شناسایی می کنند. در همان سال اکوبا و همکارانش [35] در سال 2005 آویون و همکارانش[146] این ایده را با روشی متفاوت بهبود بخشیدند؛ که در آن کلید جدید پیغامی بود که در پیام قبل ارسال شده بود.

در سال 2008، هنریکی و همکارانش[147] روش اکوبا و همکارانش[35] و آویون و همکارانش[146] را استفاده کردند ولی کلید جدید با استفاده از زنجیره های هش قبلی تولید می شد. مشکل اصلی شناسه گر های تصادفی برچسب ها در قسمت سرور است که شناسه گر باید در بین حجم بزرگی از دیتا جستجو شود. راه حلی برای این مشکل روش ساختار جستجوی درختی است که توسط مولنار و همکارانش[70]، مولنار و همکارانش[148] و دیمیتریو[149] استفاده شده است. در این مقاله، شاخه ها کلید های مشخصی دارند و هر برچسبی مجموعه از کلید ها را دارد. برای شناسایی برچسب، کلید هر قسمت و بر روی شاخه خاصی استفاده می شود.

با این حال در سال 2010، آویون و همکارانش[150] اینطور ذکر کردند که پروتکل هایی که از جستجوی جامع استفاده می کنند در معرض حمله تمام وقت هستند. در سال 2014، فیگویردو و همکارانش[151] پروتکلی را معرفی کردند که برچسب های RFID در خودرو ها استفاده شده بودند. برچسب از کلیدی که در آن قرار داده شده استفاده و دو مقدار تصادفی تولید شده توسط برچسب خوان و برچسب استفاده می کند تا شناساگر تصادفی بدلی تولید کند. نرم افزار های شناسایی جستجوی جامعی انجام می دهند تا برچسبی که شناساگر را تولید کرده کشف کنند.

فیگویردو و همکارانش[151] اینطور گفتند که روش های[35، 147،146] مشکلات همگام سازی شدیدی نرم افزار های شناسایی و برچسب ها بوجود می آورد. آنها همچنین اذعان کردند که روشهای ساختاری استفاده شده در [149،148،70] محاسبات درون برچسب را زیاد می کند و میزان جواب برچسب را طولانی می کند. در نهایت، اینطور بیان کردند که مشکلات فوق را رفع کرده، و اطلاع دادند که هدف آنها از این پروپوزال ایجاد بهترین امنیت برای صاحبان برچسب ها نیست بلکه نشان دادن امکان جستجوی جامع کلید بدون استفاده مستقیم یا مشخص از شناساگر ها در زمان بازشناسی برچسب است.

جدول شماره 4 بررسی کلی محصولات MIFARE

Products	Authentication	Confidentiality
MIFARE Classic EV1	CRYPTO1	CRYPTO1
MIFARE Plus	AES	CRYPTO1 + AES
MIFARE Plus SE	AES	CRYPTO1 + AES (Optional)
MIFARE Plus EV1	AES	AES
MIFARE Ultralight C	3DES	–
MIFARE Ultralight EV1	–	–
MIFARE Ultralight Nano	–	–
MIFARE DESFire EV1	AES + 3DES + DES	AES + 3DES + DES
MIFARE DESFire EV2	AES + 3DES + DES	AES + 3DES + DES

ارزیابی قیاسی

در جدول 2، پروتکل ها با یکدیکر در زمینه تهدیدات امنیتی و خدمات با یکدیگر مقایسه شده اند. هر کدام از پروتکل های مورد مقایسه قابلیت ویژه ای در حل مشکلات امنیتی و حریم خصوصی دارد. بعد از اینکه تعداد تیک ها از جدول شمرده شد، کلاسی که بر بیشتر تهدیدات فایق آمده و بیشترین خدمات را ارائه دهد به تکامل رسیده است و کلاسی که بر کمترین تهدیدات فایق آمده و کمترین خدمات را ارائه می دهد کلاس فوق سبک است. پروتکلی که در [33] ارائه شده است که که بهترین امنیت را ارائه می دهد کامل است و بر 9 مورد از تهدیدات غلبه کرده و 9 خدمت را ارائه می دهد. پروتکلی که در [106] ارائه شده است، که کمترین امنیت را به همراه دارد فوق سبک بوده و بر 3 تهدید غلب کرده و تعداد 0 خدمت را ارائه می دهد. انتظار می رود که تعریفات کلاس های بازشناسی را مد نظر قرار دهید. به عبارت دیگر، کمترین دست آورد را زمانی از یک پروتکل بازشناسی خواهیم داشت که قدرت سخت افزاری برچسب ضعیف است. جای تعجب ندارد که بیشتر برنامه های RFID محور از جمله دسترسی کنترل ساختمان[152]، پاسپورت هی الکترونیک[153]، عوارضی الکترونیکی[154] و جریمه الکترونیک[155] از کلاس به تکامل رسیده استفاده می کنند. علاوه بر این تکنولوژی هایی که در حجم گسترده در این حوزه استفاده می شوند، مثل کالیپسو[156] و بیشتر نسلهای MIFARE [157] از کلاس به تکامل رسیده استفاده می کنند. وقتی که مسئله زندگی یک شخص و حریم خصوصی است، اینگونه انتظار می رود. با این حال، هزینه ها باید کاهش داشته باشد و نیاز برای پروتکلهای سبک و فوق سبک بیشتر و قوی تری بر همگام واضح است. برای خوانندگانی که نیاز به تعمق در مورد ویژگی های خاصی هستند، لطفا [158] را بررسی نمایید.

5 نتیجه گیری

استفاده از پروتکل های بازشناسی اولین مرحله در در مقابله با حملات بیسیم به سیستمهای RFID است. مقاله پیش رو برخی از پروتکل های بازشناسی RFID اخیر را بررسی و مقایسه کرده است. نکات اصلی این مقایسه در جداول 1 و 2 ارائه شده است. جدول 1 نشان می دهد که برای مقابله با با این حملات و حصول اطمینان از امنیت و حریم شخصی، پروتکل های بازشناسی بررسی شده روش های متفاوتی را پیش گرفته اند ، مثل ECC، توابع هاش، تولید کنندگان اعداد تصادفی و تلفیق، تفکیک، بیت ترکیبی و عملیات های چرخش؛ و متد های تایید متفاوتی برای تایید پروتکل های معرفی شده استفاده شده اند. با اینکه برچسب های RFID ارزان قیمت به شدت محدود به سخت افزار خود هستند، در زمینه های ذخیره سازی و ظرفیت پردازش، ولی اکثر پروپوزال های بررسی شده در کلاس تکامل یافته قرار دارند و تعداد کمی از آنها در کلاس فوق سبک قرار می گیرند.

جدول 2 نشان داده که هرکدام از پروتکلهای بررسی شده قابلیت خاصی برای مواجهه با مسائل امنیتی و حریم خصوصی است. پروتکل های تکامل یافته بسیاری از تهدیدات را پشت سر می گذارند خدمات بسیاری نسبت به دیگر پروتکل ها ارائه میدهند. با در نظر گرفتن تعاریف کلاس های بازشناسی و هدفی که پروتکلهای بازشناسی باید به آن دست پیدا کنند، چنین نتیجه ای انتظار میرود.

مقاله حاضر اینچنین نتیجه می گیرد که نیاز برای پروتکل های بازشناسی قوی تر وجود دارد، علی الخصوص در زمینه پروتکل های بازشناسی فوق سبک. لذا ضروریست پروتکل بازشناسی قوی تری ارائه شود که روش یکپارچه ای برای مواجهه با همه یا حداقل بیشتر تهدیدات را نسبت به پروتکل های ارائه شده در این مقاله را در کارآتی خود داشته باشد.

References

1. Chinese RFID technology policy white paper, 2006. 15 Ministries and Commissions including Ministry of Science and Technology of PRC.

2. Karmakar, N. C. (Ed.). (2011). *Handbook of smart antennas for RFID systems*. New York: Wiley.
3. EPCglobal. (2015). EPC radio frequency identity protocols Class-1 Generation-2 UHF RFID protocol for communications at 860–960 MHz. Technical report, Version 2.0.1. https://www.gs1.org/sites/default/files/docs/epc/Gen2_Protocol_Standard.pdf. Accessed 03 Sept 2017.
4. Vajda, I., & Buttyán, L. (2003). Lightweight authentication protocols for low-cost RFID tags. In *Second workshop on security in ubicomp* (Vol. 2003, pp. 1–10).
5. Peris-Lopez, P., Hernandez-Castro, J. C., Estevez-Tapiador, J. M., & Ribagorda, A. (2006). RFID systems: A survey on security threats and proposed solutions. In *IFIP international conference on personal wireless communications* (pp. 159–170). Springer, Berlin, Heidelberg.
6. Chien, H. Y. (2007). Sasi: A new ultralightweight rfid authentication protocol providing strong authentication and strong integrity. *IEEE Transactions on Dependable and Secure Computing, 4*(4), 337–340.
7. Tuyls, P., & Batina, L. (2006). RFID tags for anti-counterfeiting. In D. Pointcheval (Ed.), *Topics in cryptology–CT-RSA 2006* (pp. 115–131). Berlin: Springer.
8. Feldhofer, M., Dominikus, S., & Wolkerstorfer, J. (2004). Strong authentication for RFID systems using the AES algorithm. In M. Joye & J.-J. Quisquater (Eds.), *Cryptographic hardware and embedded systems CHES 2004* (pp. 357–370). Berlin: Springer.
9. Tsudik, G. (2006). YA-TRAP: Yet another trivial RFID authentication protocol. In *Fourth annual IEEE international conference on pervasive computing and communications workshops, PerCom Workshops 2006*. IEEE.
10. Weis, S. A., Sarma, S. E., Rivest, R. L., & Engels, D. W. (2004). Security and privacy aspects of low-cost radio frequency identification systems. In D. Hutter, G. Müller, W. Stephan, & M. Ullmann (Eds.), *Security in pervasive computing* (pp. 201–212). Berlin, Heidelberg: Springer.
11. Bringer, J., Chabanne, H., & Dottax, E. (2006). HB++: A lightweight authentication protocol secure against some attacks. In *Second international workshop on security, privacy and trust in pervasive and ubiquitous computing, 2006* (pp. 28–33). IEEE.
12. Chien, H. Y., & Chen, C. H. (2007). Mutual authentication protocol for RFID conforming to EPC Class 1 Generation 2 standards. *Computer Standards & Interfaces, 29*(2), 254–259.
13. Duc, D., Park J., & Lee, H. (2006). Enhancing security of EPCglobal gen-2 RFID tag against traceability and cloning. In *2006 symposium on cryptography and information security* (pp. 17–20).
14. Gilbert, H., Robshaw, M., & Sibert, H. (2005). Active attack against HB+: A provably secure lightweight authentication protocol. *Electronics Letters, 41*(21), 1169–1170.
15. Li, T., & Deng, R. (2007). Vulnerability analysis of EMAP-an efficient RFID mutual authentication protocol. In *The second international conference on availability, reliability and security, 2007. ARES 2007* (pp. 238–245). IEEE.
16. Li, T., & Wang, G. (2007). Security analysis of two ultralightweight RFID authentication protocols. In H. Venter, M. Eloff, L. Labuschagne, J. Eloff, & R. von Solms (Eds.), *New approaches for security, privacy and trust in complex environments* (pp. 109–120). New York: Springer.
17. Soos, M. (2009). An overview of RFID security protocols. Ph.D. Thesis. https://www.msoos.org/wordpress/wp-content/uploads/2012/03/soos_thesis_v3.pdf. Accessed 01 Sept 2017.
18. Lee, Y. K., Batina, L., & Verbauwhede, I. (2008). EC-RAC (ECDLP based randomized access control): Provably secure RFID authentication protocol. In *2008 IEEE international conference on RFID,* (pp. 97–104). IEEE.
19. Batina, L., Guajardo, J., Kerins, T., Mentens, N., Tuyls, P., & Verbauwhede, I. (2007). Public-key cryptography for RFID-tags. In *Fifth annual IEEE international conference on pervasive computing and communications workshops, 2007* (pp. 217–222). IEEE.
20. Van Deursen, T., & Radomirovic, S. (2008). Attacks on RFID Protocols. *IACR Cryptology ePrint Archive, 2008*(310), 1–56.
21. Bringer, J., Chabanne, H., & Icart, T. (2008). Cryptanalysis of EC-RAC, a RFID identification protocol. In *Cryptology and network security* (pp. 149–161). Springer, Berlin, Heidelberg.
22. Lee, Y. K., Batina, L., & Verbauwhede, I. (2009). Untraceable RFID authentication protocols: Revision of EC-RAC. In *2009 IEEE international conference on RFID* (pp. 178–185). IEEE.
23. Lee, Y. K., Batina, L., Singelee, D., Preneel, B., & Verbauwhede, I. (2010). Anti-counterfeiting, untraceability and other security challenges for RFID systems: Public-key-based protocols and hardware. In A.-R. Sadeghi & D. Naccache (Eds.), *Towards hardware intrinsic security* (pp. 237–257). Berlin, Heidelberg: Springer.
24. Zhang, X., Li, J., Wu, Y., & Zhang, Q. (2011). An ECDLP based randomized key RFID authentication protocol. In *2011 international conference on network computing and information security (NCIS)* (Vol. 2, pp. 146–149). IEEE.
25. Liao, Y. P., & Hsiao, C. M. (2014). A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol. *Ad Hoc Networks, 18,* 133–146.
26. Moosavi, S. R., Nigussie, E., Virtanen, S., & Isoaho, J. (2014). An elliptic curve-based mutual authentication scheme for RFID implant systems. *Procedia Computer Science, 32,* 198–206.
27. He, D., Kumar, N., Chilamkurti, N., & Lee, J. H. (2014). Lightweight ECC based RFID authentication integrated with an ID verifier transfer protocol. *Journal of Medical Systems, 38*(10), 1–6.
28. Zhao, Z. (2014). A secure RFID authentication protocol for healthcare environments using elliptic curve cryptosystem. *Journal of Medical Systems, 38*(5), 1–7.
29. Chou, J. S. (2014). A secure RFID authentication protocol to enhance patient medication safety using elliptic curve cryptography. *The Journal of Supercomputing, 70*(1), 75–94.
30. Zhang, Z., & Qi, Q. (2014). An efficient RFID authentication protocol to enhance patient medication safety using elliptic curve cryptography. *Journal of Medical Systems, 38*(5), 1–7.
31. Jin, C., Xu, C., Zhang, X., & Zhao, J. (2015). A secure RFID mutual authentication protocol for healthcare environments using elliptic curve cryptography. *Journal of Medical Systems, 39*(3), 1–8.
32. Farash, M. S., Nawaz, O., Mahmood, K., Chaudhry, S. A., & Khan, M. K. (2016). A provably secure RFID authentication protocol based on elliptic curve for healthcare environments. *Journal of Medical Systems, 40*(7), 1–7.
33. Ibrahim, A., & Dalkilic, G. (2017). An advanced encryption standard powered mutual authentication protocol based on elliptic curve cryptography for RFID, proven on WISP. *Journal of Sensors*, Article ID 2367312.
34. Kaps, J. P. (2008). Chaitea, cryptographic hardware implementations of xtea. In D. R. Chowdhury, V. Rijmen, & A. Das (Eds.), *Progress in cryptology-INDOCRYPT 2008* (pp. 363–375). Berlin, Heidelberg: Springer.
35. Ohkubo, M., Suzuki, K., & Kinoshita, S. (2003). Cryptographic approach to "privacy-friendly" tags. In *RFID privacy workshop* (Vol. 82).
36. Tsudik, G. (2007). A family of dunces: Trivial RFID identification and authentication protocols. In *Privacy enhancing technologies* (pp. 45–61). Springer, Berlin, Heidelberg.
37. Rostampour, S., Namin, M. E., & Hosseinzadeh, M. (2014). A novel mutual RFID authentication protocol with low complexity

and high security. *International Journal of Modern Education and Computer Science (IJMECS), 6*(1), 17–24.
38. Tian, Y., Chen, G., & Li, J. (2012). A new ultralightweight RFID authentication protocol with permutation. *IEEE Communications Letters, 16*(5), 702–705.
39. Qian, Z., Chen, C., You, I., & Lu, S. (2012). ACSP: A novel security protocol against counting attack for UHF RFID systems. *Computers & Mathematics with Applications, 63*(2), 492–500.
40. Han, S., Potdar, V., & Chang, E. (2007). Mutual authentication protocol for RFID tags based on synchronized secret information with monitor. In *Computational science and its applications–ICCSA 2007* (pp. 227–238). Springer, Berlin, Heidelberg.
41. Qingling, C., Yiju, Z., & Yonghua, W. (2008). A minimalist mutual authentication protocol for RFID system & BAN logic analysis. In *ISECS international colloquium on computing, communication, control, and management* (Vol. 2, pp. 449–453). IEEE.
42. Chen, C. L., & Deng, Y. Y. (2009). Conformation of EPC class 1 generation 2 standards RFID system with mutual authentication and privacy protection. *Engineering Applications of Artificial Intelligence, 22*(8), 1284–1291.
43. Chou, J. S. (2014). An efficient mutual authentication RFID scheme based on elliptic curve cryptography. *The Journal of Supercomputing, 70*(1), 75–94.
44. Dalkiliç, G., Özcanhan, M. H., & Çakır, H. Ş. (2014). Increasing key space at little extra cost in RFID authentications. *Turkish Journal of Electrical Engineering & Computer Sciences, 22*(1), 155–165.
45. Liu, Y. (2008). An efficient RFID authentication protocol for low-cost tags. In *IEEE/IFIP international conference on embedded and ubiquitous computing* (Vol. 2, pp. 180–185). IEEE.
46. Toiruul, B., & Lee, K. (2006). An advanced mutual authentication algorithm using AES for RFID systems. *International Journal of Computer Science and Network Security, 6*(9), 156–162.
47. Ha, J., Moon, S., Nieto, J. M. G., & Boyd, C. (2007). Low-cost and strong-security RFID authentication protocol. In *Emerging directions in embedded and ubiquitous computing* (pp. 795–807). Springer, Berlin, Heidelberg.
48. Özcanhan, M. H., Dalkılıç, G., & Utku, S. (2014). Cryptographically supported NFC tags in medication for better inpatient safety. *Journal of Medical Systems, 38*(8), 1–15.
49. Peris-Lopez, P., Safkhanim, M., Bagheri, N., & Naderi, M. (2013). RFID in eHealth: How combat medications errors and strengthen patient safety. *Journal of Medical and Biological Engineering, 33,* 363–372.
50. Hakeem, M. J., Raahemifar, K., & Khan, G. N. (2013). HPAP: A novel authentication scheme for RFID systems. In *26th annual ieee canadian conference on electrical and computer engineering* (pp. 1–6). IEEE.
51. Chatmon, C., Le, T. V., & Burmester, M. (2006). Secure anonymous RFID authentication protocols (pp. 1–10). *Technical Report* TR-060112, Florida State Univeristy, Tallahassee.
52. Changqing, O., Jixiong, W., Zhengyan, L., & Shengye, H. (2008). An enhanced security authentication protocol based on hash-lock for low-cost RFID. In *2nd international conference on anti-counterfeiting, security and identification* (pp. 416–419). IEEE.
53. Srivastava, K., Awasthi, A. K., Kaul, S. D., & Mittal, R. C. (2015). A hash based mutual RFID tag authentication protocol in telecare medicine information system. *Journal of Medical Systems, 39*(1), 1–5.
54. Cho, J. S., Yeo, S. S., & Kim, S. K. (2011). Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value. *Computer Communications, 34*(3), 391–397.
55. Shen, J., Tan, H., Moh, S., Chung, I., & Wang, J. (2016). An efficient RFID authentication protocol providing strong privacy and security. *Journal of Internet Technology, 17*(3), 443–455.
56. Peris-Lopez, P., Hernandez-Castro, J. C., Estevez-Tapiador, J. M., & Ribagor-da, A. (2006). M2AP: A minimalist mutual authentication protocol for low-cost RFID tags. In *Ubiquitous intelligence and computing* (pp. 912–923). Springer, Berlin, Heidelberg.
57. Peris-Lopez, P., Hernandez-Castro, J. C., Estévez-Tapiador, J. M., & Ribagorda, A. (2006). LMAP: A real lightweight mutual authentication protocol for low-cost RFID tags. In *Workshop on RFID security* (pp. 12–14).
58. Peris-Lopez, P., Hernandez-Castro, J. C., Estevez-Tapiador, J. M., & Ribagorda, A. (2006). EMAP: An efficient mutual-authentication protocol for low-cost RFID tags. In *On the move to meaningful internet systems 2006: OTM 2006 workshops* (pp. 352–361). Springer, Berlin, Heidelberg.
59. Tan, C. C., Sheng, B., & Li, Q. (2008). Secure and serverless RFID authentication and search protocols. *IEEE Transactions on Wireless Communications, 7*(4), 1400–1407.
60. He, L., Jin, S. H., Zhang, T., & Li, N. N. (2009). An enhanced 2-pass optimistic anonymous RFID authentication protocol with forward security. In *5th International conference on wireless communications, networking and mobile computing* (pp. 1–4). IEEE.
61. Rahman, M. S., Soshi, M., & Miyaji, A. (2009). A secure RFID authentication protocol with low communication cost. In *International conference on complex, intelligent and software intensive systems, 2009, CISIS'09* (pp. 559–564). IEEE.
62. Li, J., Zhou, Z., & Wang, P. (2017). Cryptanalysis of the LMAP protocol: A low-cost RFID authentication protocol. In *29th Chinese control and decision conference (CCDC)* (pp. 7292–7297). IEEE.
63. Zhu, S., Yang, B., & Zhang, M. (2007). Research on RFID protocols and security. In *Information security and confidentiality of communications* (pp. 168–170).
64. Mujahid, U., Najam-ul-Islam, M., & Shami, M. A. (2015). RCIA: A new ultralightweight rfid authentication protocol using recursive hash. *International Journal of Distributed Sensor Networks, 11*(1), Article ID 642180.
65. Cho, J. S., Jeong, Y. S., & Park, S. O. (2015). Consideration on the brute-force attack cost and retrieval cost: A hash-based radio-frequency identification (RFID) tag mutual authentication protocol. *Computers & Mathematics with Applications, 69*(1), 58–65.
66. Jeon, I. S., & Yoon, E. J. (2013). A new ultralightweight RFID authentication protocol using merge and separation operations. *International Journal of Mathematical Analysis, 7*(52), 2583–2593.
67. Kardaş, S., Çelik, S., Arslan, A., & Levi, A. (2013). An efficient and private RFID authentication protocol supporting ownership transfer. In *Lightweight cryptography for security and privacy* (pp. 130–141). Springer, Berlin, Heidelberg.
68. Kardas, S., Levi, A., & Murat, E. (2011). Providing resistance against server information leakage in RFID systems. In *4th IFIP international conference on new technologies, mobility and security* (pp. 1–7). IEEE.
69. Fan, K., Li, J., Li, H., Liang, X., Shen, X. S., & Yang, Y. (2014). RSEL: revocable secure efficient lightweight RFID authentication scheme. *Concurrency and Computation: Practice and Experience, 26*(5), 1084–1096.
70. Molnar, D., & Wagner, D. (2004). Privacy and security in library RFID: Issues, practices, and architectures. In

Proceedings of the 11th ACM conference on Computer and Communications Security (pp. 210–219). ACM.
71. Sarma, S. E., Weis, S. A., & Engels, D. W. (2003). RFID systems and security and privacy implications. In *Cryptographic hardware and embedded systems CHES 2002* (pp. 454–469). Springer, Berlin, Heidelberg.
72. Ohkubo, M., Suzuki, K., & Kinoshita, S. (2004). Hash-chain based forward-secure privacy protection scheme for low-cost RFID. In *Proceedings of the SCIS* (Vol. 2004, pp. 719–724).
73. Henrici, D., & Muller, P. (2004). Hash-based enhancement of location privacy for radio frequency identification devices using varying identifiers. In *Proceedings of the second IEEE annual conference on pervasive computing and communications workshops* (pp. 149–153). IEEE.
74. Gao, X., Xiang, Z., Wang, H., Shen, J., Huang, J., & Song, S. (2004). An approach to security and privacy of RFID system for supply chain. In *IEEE international conference on e-commerce technology for dynamic e-business* (pp. 164–168). IEEE.
75. Li, Y., & Ding, X. (2007). Protecting RFID communications in supply chains. In *Proceedings of the 2nd ACM symposium on information, computer and communications security* (pp. 234–241). ACM.
76. Ren, X., Xu, X., & Li, Y. (2013). An one-way hash function based lightweight mutual authentication rfid protocol. *Journal of Computers, 8*(9), 2405–2412.
77. Song, B., & Mitchell, C. J. (2008). RFID authentication protocol for low-cost tags. In *Proceedings of the first ACM conference on wireless network security* (pp. 140–147). ACM.
78. Ning, H., Liu, H., Mao, J., & Zhang, Y. (2011). Scalable and distributed key array authentication protocol in radio frequency identification-based sensor systems. *IET Communications, 5*(12), 1755–1768.
79. Maarof, A., Labbi, Z., Senhadji, M., & Belkasmi, M. (2016). A novel mutual authentication scheme for low-cost RFID systems. In *2016 international conference on wireless networks and mobile communications (WINCOM)* (pp. 240–245). IEEE.
80. Huang, Y. C., & Jiang, J. R. (2012). An ultralightweight mutual authentication protocol for EPC C1G2 RFID tags. In *2012 fifth international symposium on parallel architectures, algorithms and programming (PAAP)* (pp. 133–140). IEEE.
81. Zhang, W., Liu, S., Wang, S., Yi, B., & Wu, L. (2017). An efficient lightweight RFID authentication protocol with strong trajectory privacy protection. *Wireless Personal Communications, 96*(1), 1215–1228.
82. Zhang, W., Wu, L., Liu, S., Huang, T., Guo, Y., & Hsu, C. (2016). A trajectory privacy model for radio-frequency identification system. *Wireless Personal Communications, 90*(3), 1121–1134.
83. Habibi, M. H., Alagheband, M. R., & Aref, M. R. (2011). Attacks on a lightweight mutual authentication protocol under EPC C-1 G-2 standard. In *Information security theory and practice. Security and privacy of mobile devices in wireless communication* (pp. 254–263). Springer, Berlin, Heidelberg.
84. Xiao, F., Zhou, Y. J., Zhou, J. X., & Niu, X. X. (2013). Provable secure mutual authentication protocol for RFID in the standard model. *Journal on Communications, 34*(4), 82–87.
85. Ha, J. C., Ha, J. H., Moon, S. J., & Boyd, C. (2006). LRMAP: Lightweight and resynchronous mutual authentication protocol for RFID system. In *International conference on ubiquitous convergence technology* (Vol. 4412, pp. 80–89). Springer.
86. Alomair, B., Clark, A., Cuellar, J., & Poovendran, R. (2012). Scalable RFID systems: a privacy-preserving protocol with constant-time identification. *IEEE Transactions on Parallel and Distributed Systems, 23*(8), 1536–1550.
87. Pang, L., Li, H., He, L., Alramadhan, A., & Wang, Y. (2014). Secure and efficient lightweight RFID authentication protocol based on fast tag indexing. *International Journal of Communication Systems, 27*(11), 3244–3254.
88. Zhang, Z., Zhou, S., & Luo, Z. (2008). Design and analysis for RFID authentication protocol. In *IEEE international conference on e-business engineering* (pp. 574–577). IEEE.
89. Zhou, S., Zhang, Z., Luo, Z., & Wong, E. C. (2010). A lightweight anti desynchronization RFID authentication protocol. *Information Systems Frontiers, 12*(5), 521–528.
90. Choi, E. Y., Lee, S. M., & Lee, D. H. (2005). Efficient RFID authentication protocol for ubiquitous computing environment. In *Embedded and ubiquitous computing–EUC 2005 workshops* (pp. 945–954). Springer, Berlin, Heidelberg.
91. Dimitriou, T. (2005). A lightweight RFID protocol to protect against traceability and cloning attacks. In *First international conference on security and privacy for emerging areas in communications networks* (pp. 59–66). IEEE.
92. Lin, Z., & Song, J. S. (2013). An improvement in HB-family lightweight authentication protocols for practical use of RFID system. *Journal of Advances in Computer Networks, 1*(1), 61–65.
93. Juels, A., & Weis, S. A. (2005). Authenticating pervasive devices with human protocols. In *Advances in cryptology–CRYPTO 2005* (pp. 293–308). Springer, Berlin, Heidelberg.
94. Hopper, N. J., & Blum, M. (2001). Secure human identification protocols. In *Advances in cryptology—ASIACRYPT 2001* (pp. 52–66). Springer, Berlin, Heidelberg.
95. Munilla, J., & Peinado, A. (2007). HB-MP: A further step in the HB-family of lightweight authentication protocols. *Computer Networks, 51*(9), 2262–2267.
96. Leng, X., Mayes, K., & Markantonakis, K. (2008). HB-MP+ protocol: An improvement on the HB-MP protocol. In *2008 IEEE international conference on RFID* (pp. 118–124). IEEE.
97. Tounsi, W., Cuppens-Boulahia, N., Garcia-Alfaro, J., Chevalier, Y., & Cuppens, F. (2014). KEDGEN2: A key establishment and derivation protocol for EPC Gen2 RFID systems. *Journal of Network and Computer Applications, 39,* 152–166.
98. Van Le, T., Burmester, M., & De Medeiros, B. (2007). Universally composable and forward secure RFID authentication and authenticated key exchange. In *Proceedings of the 2nd ACM symposium on information, computer and communications security* (pp. 242–252). ACM.
99. Burmester, M., & Munilla, J. (2011). Lightweight RFID authentication with forward and backward security. *ACM Transactions on Information and System Security (TISSEC), 14*(1), 11–16.
100. HanataniI, Y., Ohkubo, M., Matsuo, S. I., Sakiyama, K., & Ohta, K. (2012). A study on computational formal verification for practical cryptographic protocol: The case of synchronous RFID authentication. In *Financial cryptography and data security* (pp. 70–87). Springer, Berlin, Heidelberg.
101. Brusó, M., Chatzikokolakis, K., & Den Hartog, J. (2010). Formal verification of privacy for RFID systems. In *23rd IEEE computer security foundations symposium* (pp. 75–88). IEEE.
102. Kim, H. S., Oh, J. H., Kim, J. B., Jeong, Y. O., & Choi, J. Y. (2008). Formal verification of cryptographic protocol for secure RFID system. In *Fourth international conference on networked computing and advanced information management* (Vol. 2, pp. 470–477). IEEE.
103. Asadpour, M., & Dashti, M. T. (2011). A privacy-friendly RFID protocol using reusable anonymous tickets. In *IEEE 10th international conference on trust, security and privacy in computing and communications (TrustCom)* (pp. 206–213). IEEE.
104. Gao, L., Ma, M., Shu, Y., & Wei, Y. (2014). An ultralightweight RFID authentication protocol with CRC and permutation. *Journal of Network and Computer Applications, 41,* 37–46.

105. Peris-Lopez, P., Hernandez-Castro, J. C., Tapiador, J. M., & Ribagorda, A. (2009). Advances in ultralightweight cryptography for low-cost RFID tags: Gossamer protocol. In *Information security applications* (pp. 56–68). Springer, Berlin, Heidelberg.
106. Luo, H., Wen, G., Su, J., & Huang, Z. (2016). SLAP: Succinct and lightweight authentication protocol for low-cost RFID system. *Wireless Networks, 22*, 1–10.
107. Zhuang, X., Zhu, Y., & Chang, C. C. (2014). A new ultralightweight RFID protocol for low-cost tags: R^2AP. *Wireless Personal Communications, 79*(3), 1787–1802.
108. Tewari, A., & Gupta, B. B. (2017). Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for IoT devices using RFID tags. *The Journal of Supercomputing, 73*(3), 1085–1102.
109. Kardaş, S., Çelik, S., Bingöl, M. A., Kiraz, M. S., Demirci, H., & Levi, A. (2015). K-strong privacy for radio frequency identification authentication protocols based on physically unclonable functions. *Wireless Communications and Mobile Computing, 15*(18), 2150–2166.
110. Ranasinghe, D., Engels, D., & Cole, P. (2004). Security and privacy: Modest proposals for low-cost RFID systems. In *Auto-ID labs research workshop, Zurich, Switzerland.*
111. Tuyls, P., & Batina, L. (2006). RFID-tags for anti-counterfeiting. In *Topics in cryptology–CT-RSA 2006* (pp. 115–131). Springer Berlin Heidelberg.
112. Bassil, R., El-Beaino, W., Itani, W., Kayssi, A., & Chehab, A. (2012). PUMAP: A PUF-based ultra-lightweight mutual authentication RFID protocol. *International Journal of RFID Security and Cryptography, 1*(1/2), 58–66.
113. Chien, H. Y., Yang, C. C., Wu, T. C., & Lee, C. F. (2011). Two RFID-based solutions to enhance inpatient medication safety. *Journal of Medical Systems, 35*(3), 369–375.
114. Peris-Lopez, P., Orfila, A., Mitrokotsa, A., & Van der Lubbe, J. C. (2011). A comprehensive RFID solution to enhance inpatient medication safety. *International Journal of Medical Informatics, 80*(1), 13–24.
115. Yen, Y. C., Lo, N. W., & Wu, T. C. (2012). Two RFID-based solutions for secure inpatient medication administration. *Journal of Medical Systems, 36*(5), 2769–2778.
116. Chen, Y. Y., Huang, D. C., Tsai, M. L., & Jan, J. K. (2012). A design of tamper resistant prescription RFID access control system. *Journal of Medical Systems, 36*(5), 2795–2801.
117. Kim, H. (2012). Enhanced hash-based RFID mutual authentication protocol. In *Computer applications for security, control and system engineering* (pp. 70–77). Springer, Berlin, Heidelberg.
118. Kim, H. (2013). RFID mutual authentication protocol based on synchronized secret. *International Journal of Security and Its Applications, 7*(4), 37–50.
119. Safkhani, M., Peris-Lopez, P., Castro, J. C. H., & Bagheri, N. (2014). Cryptanalysis of Cho et al'.s protocol, A hash-based mutual authentication protocol for RFID systems. *Journal of Computational and Applied Mathematics, 259*, 571–577.
120. Mohammadi, M., Hosseinzadeh, M., & Esmaeildoust, M. (2014). Analysis and improvement of the lightweight mutual authentication protocol under EPC C-1 G-2 standard. *Advances in Computer Science: An International Journal, 3*(2), 10–16.
121. Gilbert, H., Robshaw, M. J., & Seurin, Y. (2008). Good variants of HB+ are hard to find. In *Financial cryptography and data security* (pp. 156–170). Springer, Berlin, Heidelberg.
122. Gilbert, H., Robshaw, M. J., & Seurin, Y. (2008).: HB#: Increasing the security and efficiency of HB+. In *Advances in cryptology–EUROCRYPT 2008* (pp. 361–378). Springer, Berlin, Heidelberg.
123. Yoon, B., Sung, M. Y., Yeon, S., & Oh, H. S. (2009). HB-MP++ protocol: An ultralightweight authentication protocol for RFID system. In *Proceedings of IEEE international conference on RFID* (pp. 186–191). IEEE.
124. Ouafi, K., Overbeck, R., & Vaudenay, S. (2008). On the security of HB# against a man-in-the-middle attack. In *Advances in cryptology-ASIACRYPT 2008* (pp. 108–124). Springer, Berlin, Heidelberg.
125. Halevi, T., Saxena, N., & Halevi, S. (2011). Tree-based HB protocols for privacy-preserving authentication of RFID tags. *Journal of Computer Security, 19*(2), 343–363.
126. Rizomiliotis, P., & Gritzalis, S. (2012). GHB#: A provably secure HB-like lightweight authentication protocol. In *Applied cryptography and network security* (pp. 489–506). Springer, Berlin, Heidelberg.
127. Deng, G., Li, H., Zhang, Y., & Wang, J. (2013). Tree-LSHB+: An LPN-based lightweight mutual authentication RFID protocol. *Wireless Personal Communications, 72*(1), 159–174.
128. Qian, X., Liu, X., Yang, S., & Zuo, C. (2014). Security and privacy analysis of tree-LSHB+ protocol. *Wireless Personal Communications, 77*(4), 3125–3141.
129. Juels, A. (2005). Strengthening EPC tags against cloning. In *Proceedings of the 4th ACM workshop on wireless security* (pp. 67–76). ACM.
130. Karthikeyan, S., & Nesterenko, M. (2005). RFID security without extensive cryptography. In *Proceedings of the 3rd ACM workshop on security of* ad hoc *and sensor networks* (pp. 63–67). ACM.
131. Lo, N. W., & Yeh, K. H. (2007). An efficient mutual authentication scheme for EPCglobal class-1 generation-2 RFID system. In *Emerging directions in embedded and ubiquitous computing* (pp. 43–56). Springer, Berlin, Heidelberg.
132. Peris-Lopez, P., Hernandez-Castro, J. C., Estevez-Tapiador, J. M., & Ribagorda, A. (2009). Cryptanalysis of a novel authentication protocol conforming to EPC-C1G2 standard. *Computer Standards & Interfaces, 31*(2), 372–380.
133. Yeh, T. C., Wang, Y. J., Kuo, T. C., & Wang, S. S. (2010). Securing RFID systems conforming to EPC Class 1 Generation 2 standard. *Expert Systems with Applications, 37*(12), 7678–7683.
134. Habibi, M. H., Gardeshi, M., & Alaghband, M. R. (2011). Practical attacks on a RFID authentication protocol conforming to EPC C-1 G-2 standard. *arXiv preprint* arXiv:1102.0763.
135. Alavi, S. M., Baghery, K., & Abdolmaleki, B. (2014). Security and privacy flaws in a recent authentication protocol for EPC C1 G2 RFID tags. *Advances in Computer Science: an International Journal (ACSIJ), 3*(5), 44–52.
136. Pang, L., He, L., Pei, Q., & Wang, Y. (2013). Secure and efficient mutual authentication protocol for RFID conforming to the EPC C-1 G-2 standard. In *2013 IEEE Wireless communications and networking conference (WCNC)* (pp. 1870–1875). IEEE.
137. Wang, S., Liu, S., & Chen, D. (2015). Security analysis and improvement on two RFID authentication protocols. *Wireless Personal Communications, 82*(1), 21–33.
138. Phan, R. C. W. (2009). Cryptanalysis of a new ultralightweight RFID authentication protocol—SASI. *IEEE Transactions on Dependable and Secure Computing, 6*(4), 316–320.
139. Hernandez-Castro, J. C., Tapiador, J. M., Peris-Lopez, P., & Quisquater, J. J. (2009). Cryptanalysis of the SASI ultralightweight RFID authentication protocol with modular rotations. In *International workshop on coding and cryptography*.
140. Tagra, D., Rahman, M., & Sampalli, S. (2010). Flaws in a recent ultralightweight RFID protocol. In *International conference on software telecommunications and computer networks, Croatia* (pp. 6–10).
141. Peris-Lopez, P., Hernandez-Castro, J., Estevez-Tapiador, J., & Ribagorda, A. (2009). An ultra-light authentication protocol

resistant to passive attacks under the Gen-2 specification. *Journal of Information Science and Engineering, 25*(1), 33–57.
142. Wang, S. H., & Wang, G. L. (2010). Analysis of passive attack on RFID authentication protocol ULAP. *Networks and Communications, 36,* 17–19.
143. Zhuang, X., Wang, Z. H., Chang, C. C., & Zhu, Y. (2013). Security analysis of a new ultralightweight RFID protocol and its improvement. *Journal of Information Hiding and Multimedia Signal Processing, 4*(3), 165–180.
144. Jeon, I. S., & Yoon, E. J. (2013). Cryptanalysis and improvement of a new ultralightweight rfid authentication protocol with permutation. *Applied Mathematical Sciences, 7,* 3433–3444.
145. Zhuang, X., Zhu, Y., & Chang, C.C. (2013). Security analysis of ultralightweight RFID protocols. *Technique Report.*
146. Avoine, G., & Oechslin, P. (2005). A scalable and provably secure hash-based RFID protocol. In *Proceedings of the third IEEE international conference on pervasive computing and communications workshops* (pp. 110–114). IEEE.
147. Henrici, D., & Müller, P. (2008). Providing security and privacy in RFID systems using triggered hash chains. In *Proceedings of the sixth annual IEEE international conference on pervasive computing and communications* (pp. 50–59). IEEE.
148. Molnar, D., Soppera, A., & Wagner, D. (2005). A scalable, delegatable pseudonym protocol enabling ownership transfer of RFID tags. In *International workshop on selected areas in cryptography* (pp. 276–290). Springer, Berlin, Heidelberg.
149. Dimitriou, T. (2006). A secure and efficient RFID protocol that could make big brother (partially) obsolete. In *Fourth annual ieee international conference on pervasive computing and communications* (pp. 6). IEEE.
150. Avoine, G., Coisel, I., & Martin, T. (2010). Time measurement threatens privacy-friendly RFID authentication protocols. In *International workshop on radio frequency identification: Security and privacy issues* (pp. 138–157). Springer, Berlin, Heidelberg.
151. Figueiredo, R., Zúquete, A., & e Silva, T. O. (2014). Massively parallel identification of privacy-preserving vehicle RFID tags. In *International workshop on radio frequency identification: Security and privacy issues* (pp. 36–53). Springer International Publishing.
152. Rohr, A., Nohl, K., & Plötz, H. (2010). *Establishing Security Best Practices in Access Control*. Berlin, Germany: Security Research Labs.
153. Kumar, V. N., & Srinivasan, B. (2012). Evolution of electronic passport scheme using cryptographic protocol along with biometrics authentication system. *International Journal of Computer Network and Information Security, 4*(2), 50.
154. Hwang, R. J., Su, F. F., & Tsai, Y. C. (2010). Efficient electronic toll collection protocol for intelligent transport system. *Journal of Computer Science, 21*(3), 18–26.
155. Nair, L. S., Arun, V. S., & Joseph, S. (2015). Secure e-ticketing system based on mutual authentication using RFID. In *Proceedings of the third international symposium on women in computing and informatics* (pp. 673–677). ACM.
156. Calypso Secure (2014). https://www.calypsonet asso.org/secure. Accessed 09 March 2017.
157. Schalk, G. H. (2013). *RFID: MIFARE and contactless cards in application*. Limbricht: Elektor Publishing.
158. UCODE. http://www.nxp.com/products/identification-and-security/smart-label-and-tag-ics/ucode:MC_50483. Accessed 20 March 2017.