مروری بر پروتکل‌های مبتنی بر مسأله LPN در سامانه‌های RFID

نصور باقری[1] و رضا آقامحمدی۲

[1] استادیار دانشکده مهندسی برق، دانشگاه تربیت دبیر شهید رجایی، تهران، ایران
nbagheri@srttu.edu

[2] دانشجوی کارشناسی ارشد، دانشکده مهندسی برق، دانشگاه تربیت دبیر شهید رجایی، تهران، ایران
Re.aghamohammadi@gmail.com

چکیده

سامانهٔ RFID با استفاده از ارتباطات مبتنی بر فرکانس‌های رادیویی امکان شناسایی خودکار، ردیابی و مدیریت اشیا، انسان و حیوان را فراهم می‌کند. عملکرد RFID وابسته به دو دستگاه برچسب و بازخوان است که جهت برقراری ارتباط بین یکدیگر از امواج رادیویی استفاده می‌کنند. برای برقراری ارتباط امن بین برچسب و بازخوان از پروتکل‌های رمز نگاری استفاده می‌شود. مبنای اساسی برای امنیت یک پروتکل رمزنگاری بر اساس پیچیدگی محاسباتی مسأله است. به‌طور واضح‌تر یک پروتکل رمزنگاری زمانی امن گفته می‌شود که شکستن امنیت، به‌طور محاسباتی معادل حل یک مسأله خیلی سخت باشد. در این مقاله، در مورد مزایای استفاده از طراحی پروتکل‌های رمزنگاری برای برچسب‌های RFID بر اساس مسأله سخت غیر متعارف LPN بحث می‌کنیم.

واژگان کلیدی: احراز هویت، رمز نگاری سبک وزن HB, RFID, Authentication, LPN,

۱ – مقدّمه

شناسایی از طریق فرکانس رادیویی[1] (RFID) راهی برای شناسایی خودکار اجسام و دارایی به‌صورتی مفید و سریع است. با فناوری RFID، برچسب‌های RFID به اقلام مشتری متصل می‌شوند. این برچسب‌ها حاوی تراشه‌های رایانه‌ای کوچک ولی بادوام همراه با آنتن‌های بسیار کوچک هستند. برچسب‌های[2] غیرفعال با درخواست سیگنال با فرکانس رادیویی[3] که از بازخوان[4] می‌آید، فعال می‌شوند. درحالی‌که RFID فعال به کمک باتری روشن می‌شود. تراشهٔ رایانه‌ای کوچک حاوی شمارهٔ کد الکترونیکی محصول ((EPC[5] است که شیئی را که به آن چسبانده شده است، به‌صورت یکتا شناسایی می‌کند و آنتن به‌طور خودکار شماره EPC را بدون نیاز به در دیدرس‌بودن گیرنده، برای گیرنده می‌فرستد. تمام اطلاعات مرتبط با شماره EPC در شبکه‌ای از پایگاه داده ذخیره می‌شود که به آن سرویس اطلاعات EPC[6] یا سرور انتهایی گفته می‌شود [۱].

به‌تازگی امنیت و حریم خصوصی سامانه‌های RFID توجه بسیاری را به خود جلب کرده است. با وجود مزایای تعددی که RFID می‌تواند به ارمغان آورد، امنیت و حریم خصوصی از نگرانی‌های اصلی هستند که باعث کندی سرعت استقرار سریع و گستردهٔ این فناوری شده‌اند [۲]. برای حل این مشکلات امنیتی، محافظت از حریم خصوصی کاربران، جلوگیری از ارتباط غیر مجاز بین برچسب‌ها و بازخوان‌ها، نیاز به اجرای یک پروتکل امن میان برچسب و بازخوان

[1] Radio Frequency Identification
[2] Tag
[2] Radio-Frequency
[3] reader
[4] Electronic Product Code
[5] EPC-Information Services

براساس رمزنگاری است. برچسب‌های RFID دارای ظرفیت محاسباتی و حافظه پایینی هستند؛ بنابراین، استفاده از الگوریتم‌های رمزنگاری برای امن‌سازی پروتکلی که در آن‌ها استفاده می‌شود، غیر ممکن است [۳].

رمزنگاری سبک‌وزن[1] بخشی از حوزهٔ رمزنگاری است که درصورت استفاده از سخت‌افزار مناسب، در سامانه‌های ارزان‌قیمت، مثل کارت‌های هوشمند و برچسب‌های RFID غیرفعال، بسیار مورد تقاضا قرار دارد. مصالحه‌هایی در خصوص امنیت، حافظه و عملکرد باید در نظر گرفته شوند. در هریک از این مصالحه‌ها قیود مختلفی وجود دارد. به‌طورمثال AES و رمزهای دنباله‌ای را می‌توان به‌خوبی در سخت‌افزار پیاده‌سازی کرد ولی امنیت آن را نمی‌توان ثابت کرد. به‌تازگی در این زمینه سبک جدیدی که ساختن نمونه‌های نخستین رمزی از مسائل تئوری یادگیری است، مطرح شده است. مسائل مبتنی بر تئوری یادگیری مفاهیم پایه‌ای نظری پیچیده‌ای دارند که امنیت سامانه رمزی براساس آن‌ها است. پیاده‌سازی آن‌ها ساده و با بازدهٔ بالاست و درنتیجه در رمزنگاری سبک‌وزن بسیار مناسب هستند. یکی از محبوب‌ترین تلاش‌ها برای تحقق این نیاز پروتکل‌های خانواده HB است [۴].

در این مقاله، سعی کرده‌ایم پروتکل‌های مختلفی را که براساس مسأله LPN تاکنون ارائه شده، بررسی کرده و همچنین امنیت آنها را در مقابل حملات غیر فعال، فعال و مرد میانی مورد تجزیه و تحلیل قرار بدهیم.

مقاله به‌صورت زیر سازماندهی شده: ابتدا در بخش دو تاریخچه پروتکل‌های خانواده HB ارائه شده. در بخش سه مسأله LPN به‌طور دقیق مورد بررسی قرار گرفته. در بخش چهار پروتکل‌های خانواده HB به‌طوردقیق مورد تجزیه و تحلیل قرار گرفته و همچنین در بخش پنج سایر پروتوکل‌ها تجزیه و تحلیل شده‌اند و درنهایت نتیجه‌گیری در بخش شش آورده شده است.

۲- تاریخچهٔ پروتکل‌های مبتنی برمسئله LPN

در سال ۲۰۰۱ نخستین پروتکل از مجموعه پروتکل‌های بالا سبک HB توسط هاپر و به لوم[2] مبتنی برمسأله LPN ارائه شد. [۵] در این پروتکل سبک‌وزن تنها از ضرب نقطه‌ای بردارهای دودویی و یک بردار نوفهٔ تصادفی استفاده می‌شد. جولز و ویز[3] در سال ۲۰۰۵ نسخهٔ بهبودیافته آن به‌نام HB+ را با اضافه‌کردن یک کلید محرمانه دیگر و استفاده از توابع منطقی ANDو XOR با هدف حفظ امنیت در برابر حملات فعال ارائه کردند [۶]. در همان سال گیلبرت[4] حمله‌ای از نوع مرد میانی به نام GRS علیه این پروتکل مطرح کرد [۷]. در سال ۲۰۰۶ برینگر یک نسخهٔ بهبودیافته‌ای از HB+ ارائه داد که HB++ نامیده می‌شد. این پروتکل برای مقاومت در برابر حمله GRS طراحی شده بود. اگرچه در سال ۲۰۰۷ پیراموتا[5] [۸] ثابت کرد که پروتکل HB++ هنوز مقاومت کافی را در برابر دشمنی که وانمود می‌کند یک بازخوان قانونی هست ندارد، در سال ۲۰۰۷ مانیلا و پینادو[6] پروتکل دیگری پیشنهاد کردند. ابتدا پروتکلی با الهام از HB با نام HB-MP' ارائه شد. این پروتکل همان آسیب‌پذیری پروتکل HB+ نسبت به حمله مرد میانی را داشت. برای اجتناب از این ضعف، پروتکل دیگری با نام HB-MP ارائه شد. این پروتکل یک روش تازه برای مبادلهٔ پیام‌ها با استفاده از چرخش کلید محرمانه مطرح کرد و سعی در امن‌کردن خانواده پروتکل‌های HB داشت؛ اما هنوز پروتکل HB-MP نسبت به حملات مختلف از جمله حملهٔ مرد میانی، جعل و تکرار آسیب‌پذیر بود. در سال ۲۰۰۸ پروتکل HB-MP+ مطرح شد که نسبت به حملهٔ مرد میانی که همهٔ پروتکل‌های قبلی نسبت به آن آسیب‌پذیر بود، مقاوم است. در این پروتکل از تابع درهم‌ساز به‌منظور تصادفی‌کردن عمل چرخش استفاده شده است؛ اما در مورد این پروتکل نیز، هنوز بحث حملهٔ جعل و همچنین بعضی حملات غیر فعال مطرح است؛ اما در سال ۲۰۰۹ یون[7] نشان داد که این پروتکل نیز نمی‌تواند در برابرحملهٔ ردیابی مقاومت کند [۹]. همچنین در سال ۲۰۰۸ گیلبرت و همکارانش دو پروتکل جدید به نام‌های HB# و Random- HB# را برای غلبه بر بعضی از اشکالات عملی HB+ ارائه دادند [۱۰].

پروتکل HB# اجرای Random- HB# را با استفاده از ماتریس Toeplitze بهبود بخشید. از طرفی در سال ۲۰۰۸ اوافی[8] و همکارانش یک حمله مرد میانی را در برابر این دو

[1] Light weight cryptography
[2] Hopper and blum
[3] Jules and weis
[4] gilbert
[5] piramutha
[6] Munilla and peinado
[7] yoon
[8] ouafi

پروتکل ارائه کردند. در سال ۲۰۱۰ مدهاوان[1] یک نوع غیر خطی از HB را ارائه کردندکه NLHB نامیده شد. این پروتکل پیچیدگی کمتری نسبت به پروتکل HB از نظر اجرایی دارد؛ اما در همان سال ابیانه[2] [۱۱] نشان داد که پروتکل NLHB در برابر حملات غیر فعالی که به HB اعمال می‌شد آسیب‌پذیر است. بنا به راین پروتکل HBN[۱۲] در سال ۲۰۱۱ پیشنهاد شد. همچنین نوع دیگری از پروتکل HB به نام RCHB توسط علی و همکارانش در سال ۲۰۱۱ ارائه شد [۱۳]. پروتکل RCHB با معرفی عملکردهای چرخش و مکمل‌کردن روی کلید مخفی امنیت HB را بهبود بخشید. در همان سال کاو[3] و همکارانش [۱۴] پروتکل دیگری به نام F-HB را پیشنهاد دادند که از یک مسأله LPN و یک مولد شبه‌تصادفی تشکیل شده بود. در سال ۲۰۱۲ هیس[4] و همکارانش [۱۵] پروتکلی را بر اساس RING–LPN ارائه دادند. در سال ۲۰۱۳ لی و همکارانش [۱۶] پروتکل LCMQ را ارائه دادند. هستهٔ تکنیکی در این پروتکل استفاده از نوع خاصی از ماتریس گردشی و یک رمزنگاری امن است. در سال ۲۰۱۵ النا پگنین[5] و همکارانش پروتکلی را براساس مسأله LPN و محدودیت فاصله به نام HB+BD ارائه دادند که در این پروتکل علاوه‌بر برتری‌های پروتکل‌های HB به کانال ارتباطی بین برچسب و بازخوان نیز توجه شده است [۱۷].

۳- مسأله LPN

مسأله یادگیری در حضور نوفه (LWE) [6]به‌عنوان سخت‌ترین مسأله شناخته شده است [۱۸]، به‌طوری که عقیده بر این است که این مسأله به‌طور نمایی سخت است و حتی با رایانه‌های کوانتوم نیز قابل حل نیست. این مسأله بسیار قابل انعطاف است و پایه‌ای برای رمزنگاری امن و کارامد است. یک بردار نامعلوم s در Z_q^n را در نظر بگیرید، یک برنامه (که در آن مقدار s معلوم است)، برداری یک‌نواخت مانند a در Z_q^n و یک خطا مانند $e \in z$ با توزیع نرمال و انحراف معیار αq تولید می‌کند. خروجی برنامه به‌شکل روبه‌رو است.

$$(a, b = < a.s > + e \bmod q) \qquad (۱)$$

در این رابطه بردار s و بردار a در هم، ضرب نقطه‌ای شده‌اند و درنهایت نتیجه با یک مقدار خطا جمع شده است. این روش با همان s قبلی و a و e جدید تکرار می‌شود. وظیفهٔ ما یافتن s است. n مهم‌ترین پارامتر است که تعیین‌کننده دیمانسیون بردار s است.q نشان‌دهنده مدول بردار S است. q =poly(n)پارامتر q می‌تواند به‌صورت نمایی باشد، که‌دراین‌صورت اندازهٔ ورودی را افزایش داده و سختی مسأله بیش‌تر می‌شود.

اگر مقدار q، دو در نظر گرفته شود LPN ایجاد خواهد شد. که در واقع زیر مسأله‌ای از LWE است. پارامتر e یک نوفه با توزیع نرمال و انحراف معیار αq است (که به نزدیک‌ترین عدد صحیح گرد می‌شود).

مسأله LPN شامل ضرب داخلی دو عدد k بیتی است [۱۹]. دو عدد k بیتی $a=(a_0\ a_1 \ldots a_{k-1})$ و $x=(x_0\ x_1 \ldots x_{k-1})$ داده شده است، ضرب داخلی a و x به این شکل تعریف می‌شود:

$$a.\,x = (a_0.x_0) + (a_1.x_1) + \ldots + (a_{k-1}.x_{k-1}) \qquad (۲)$$

بدیهی است که این عملیات را می‌توان به‌راحتی در یک سخت‌افزار ارزان پیاده‌سازی کرد. علاوه‌بر این، همان‌طور که توسط جولز و ویز ذکر شده است، نیازی نیست که همه k بیت a و x برای ارزیابی (a.x) به‌طور هم‌زمان در هم ضرب شوند. بنابراین حافظه مورد نیاز برای این عملیات بسیار پایین است. نخستین‌بار اهمیت رمزنگاری با استفاده از عملیات ضرب داخلی توسط گلدریچ [7] و لوین[8] مطرح شد. آن‌ها ثابت کردند که اگر تنها x یا a داده شده باشد، حاصل (a. x) غیر قابل پیش‌بینی است این نتیجه پس از آن برای ساخت یک مولد عدد شبه‌تصادفی امن مورد استفاده قرار گرفت. مسأله LPN مسأله شناخته‌شده‌ای است [۲۱،۲۲،۲۵،۲۶،۵،۲۰]. فرض کنید $hw(v)$ نشان‌دهنده وزن همینگ بردار دودویی v باشد.

تعریف: فرض کنید A یک ماتریس تصادفی $q \times k$ از بردارهای دودویی باشد، فرض کنید x یک بردار k بیتی تصادفی بوده و $\varepsilon \in]0, \frac{1}{2}[$ ثابت پارامتر نوفه و v یک بردار تصادفی q بیتی باشد، به‌طوری که:

$$hw(v) < \varepsilon q \qquad (۳)$$

با معین‌بودن A، ε و $z = (A.x) \oplus v$ بردار k بیتی x' را به‌گونه‌ای پیدا کنید که:

[1] madhavan
[2] abyaneh
[3] cao
[4] heyse
[5] Elena pengin
[6] Learning with error
[7] Goldrich
[8] Luvin

$$hw(A.x' \oplus z) \leq \varepsilon q \qquad (۴)$$

سختی پیداکردن x (حل LPN) به‌خاطر این حقیقت است که هر بیت $A.x$ به‌طور مستقل با احتمال ε پرش دارد؛ از این‌رو داشتن سامانهٔ معادلات درست خطی در x که بتوان به‌راحتی با روش حذف گوسی آن را حل کرد سخت می‌شود. فرض کنید Ber_ε نشان‌دهنده توزیع برنولی با پارامتر ε باشد، به‌عنوان مثال:

$$(\nu \leftarrow Ber_\varepsilon, \Pr[\nu = 1] = 1 - \Pr[\nu = 0] = \varepsilon) \qquad (۵)$$

و فرض کنید $A_{x,\varepsilon}$ توزیعی باشد که با رابطهٔ زیر تعریف می‌شود.

$$\{a \leftarrow \{0,1\}^k; \nu \leftarrow Ber_\varepsilon : (a, a.x \oplus \nu)\} \qquad (۶)$$

یک نتیجه از سختی مسأله LPN با پارامتر نوفه ε این است که توزیع $A_{x,\varepsilon}$ از توزیع یکنواخت U_{k+1} روی رشته (k+1) بیتی، غیر قابل تشخیص است [۱۹]. اگرچه الگوریتم‌هایی به حل مساله LPN پرداخته‌اند [۲۲،۲۷]؛ اما الگوریتم به لوم کالایی و واسر من [۲۲] دارای زمان اجرای $2^{O(\frac{k}{logk})}$ است.

$$\begin{bmatrix} a_1^1 a_2^1 \dots a_n^1 \\ a_1^2 a_2^2 \dots a_n^2 \\ a_1^3 a_2^3 \dots a_n^3 \\ \dots \dots \dots \dots \\ a_1^r a_2^r \dots a_n^r \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ \dots \\ x_n \end{bmatrix} \oplus \begin{bmatrix} \nu_1 \\ \nu_2 \\ \nu_3 \\ \dots \\ \nu_r \end{bmatrix} = \begin{bmatrix} z_1 \\ z_2 \\ z_3 \\ \dots \\ z_r \end{bmatrix} \qquad (۷)$$

همان‌طور که در رابطهٔ ۷ مشاهده می‌شود، در مسأله LPN دشمن فقط به پارامترهای z و a که به‌طور یکنواخت غیر قابل تشخیص هستند، دسترسی دارد و منظور از حل مسأله LPN به‌دست‌آوردن بردار مخفی x است.

۴- پروتکل‌های خانواده HB

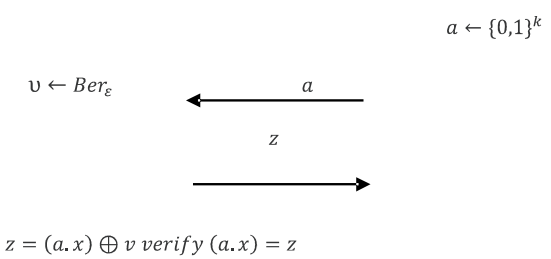
در این نوع از پروتکل‌های احراز هویت یک انسان می‌خواهد هویت خود را به یک دستگاه اثبات کند، درحالی‌که کانال ارتباطی ناامن است. به‌علاوه آن‌ها می‌خواهند از کلید مخفی که به اشتراک گذاشته‌اند، بارها برای احراز هویت استفاده کنند. در ادامه به بررسی برخی از پروتکل‌های خانوادهٔ HB می‌پردازیم:

۴-۱- پروتکل HB

نخستین پروتکل رمزنگاری براساس ضرب داخلی توسط هاپر و به لوم معرفی شد [۵]. آن‌ها یک پروتکل احراز هویت انسانی را ارائه دادند؛ به‌طوری که انسان نیاز به ارزیابی یک عمل ضرب داخلی دودویی دارد و یک بیت تصادفی تولید می‌کند. این پروتکل HB نامیده می‌شود و اثبات می‌شود که تحت شرایط خاصی که LPN نامیده می‌شود، ایمن است. در پروتکل HB، انسان و ماشین یک x مخفی را به‌طول k بیت به اشتراک می‌گذارند. پروتکل شامل چندین اجرا از یک (چالش – پاسخ) پایه است که در شکل زیر نمایش داده شده است.

Berε نشان دهندهٔ یک توزیع برنولی با امید ریاضی ε است که مقدار ε عددی است بین (0, 0.5) و عامل نوفه نامیده می‌شود (بیت v به عنوان بیت نوفه شناخته می‌شود و به‌طور مستقل برای هر دور پروتکل با احتمال ε برابر یک تولید می‌شود). هدف از v جلوگیری از استراق سمع دشمنان از استخراج x پس از مشاهده k جفت (z ، a)است. ماشین (بازخوان)، انسان (برچسب) را زمانی می‌پذیرد که مشخص شود از rدور پروتکل بالا ، اگر و تنها اگر انسان (برچسب) بیشینه $r\varepsilon$ پاسخ نادرست ایجاد کرده باشد.

واضح است که پروتکل HB، تنها درصورتی امن است که مشاهدهٔ پیام‌های رد و بدل شده بین H و C یک احتمال ناچیز از جعل هویت H باشد. به‌طور خیلی خاص، یک استراق‌سمع‌کننده مانند a، r جفت (a,z) فراهم می‌کند و سعی می‌کند تا x را که یک عدد k بیتی است، استنباط کند؛ به‌طوری که با استفاده از x پروتکل HB شناخته شده و a توسط c پذیرفته خواهد شد. مسأله پیداکردن x، مسأله LPN نامیده می‌شود.



(شکل ۱): یک دور از پروتکل HB

۴-۲ - بررسی امنیت پروتکل HB در برابرحملات غیر فعال:

از آن‌جا که این پروتکل مبتنی بر مسأله LPN طراحی شده است، حمله غیر فعال به این پروتکل از قبیل شنود و استراق‌سمع و به‌دست آوردن کلید مخفی از این طریق معادل با حل کردن مسأله LPN است. و از آن‌جا که مسأله LPN یک مسأله سخت است، بنابراین حملات غیر فعال بر این پروتکل کارساز نیست.

۴-۳- بررسی امنیت پروتکل HB در برابرحملات فعال:

به روش زیر می‌توان به پروتکل HB حمله کرد و مقدار کلید مخفی x را به‌دست آورد [۲۸]. اگر بردار تصادفی a از طرف یک بازخوان تقلبی همه به‌طور یکسان ارسال شوند، در آن صورت با توجه به این که بیشتر نوفه‌های v صفر هستند، پس می‌توان نتیجه گرفت که با توجه به‌رابطهٔ z=a.x و معلوم‌بودن مقدار a و z به‌راحتی می‌توان مقدار x را از طریق حذف گوسی به‌دست آورد. به‌بیانی دیگر دشمن فعال چالش زیر را برای برچسب می‌فرستد:

$$a=\begin{bmatrix}1000\ldots0\\1000\ldots0\\\ldots\\1000\ldots0\end{bmatrix} \qquad (۸)$$

همان‌طور که درقبل نیز توضیح داده شد، با توجه به این‌که بیش‌تر نوفه‌ها صفر هستند، بنابراین با ضرب ماتریس a دربردار مخفی x، پاسخ به‌دست‌آمده خیلی شبیه به بیت نخست x خواهد بود. و این کار برای بیت‌های بعدی هم تکرار می‌شود.

۴-۴ پروتکل HB^+

HB^+ پروتکل احراز هویت بر اساس مسأله LPN است و برای ابزار ارزان‌قیمت مانند برچسب‌های RFID استفاده می‌شود. پروتکل شامل r = r(k) دور تصدیق پاسخ میان برچسب و بازخوان است که دو کلید تصادفی x و y با طول k را به اشتراک می‌گذارند. یک دور شامل مراحل زیر است: شکل دو را برای نمایش گرافیکی مسأله مشاهده کنید:

برچسب به‌صورت تصادفی بردار $b \leftarrow \{0,1\}^k$ را که "عامل کورکننده" نامیده می‌شود، انتخاب و برای بازخوان ارسال می‌کند؛ سپس بازخوان به‌طور تصادفی بردار $a \leftarrow \{0,1\}^k$ را انتخاب کرده و برای برچسب ارسال می‌کند. در مرحلهٔ بعدی برچسب بیت ν را براساس توزیع Ber_ε ایجاد کرده و به بازخوان به‌وسیله ارسال یک بیت $z = a.x \oplus b.y \oplus \nu$ پاسخ می‌دهد. درنهایت بازخوان احراز هویت را اگر $a.x \oplus b.y = z$ برقرار باشد، قبول می‌کند. پارامترهای HB^+ عبارتند از: کلیدهای به اشتراک گذاشته‌شده x و y هر کدام به‌طول k ، تعداد دورهای r=r(k)، پارامتر برنولی ε و سطح آستانه u=u(k). سطح آستانه u طوری است که بزرگ‌تر از $\varepsilon.r$ است؛ بنابراین بازخوان زمانی برچسب را تأیید می‌کند که تعداد دورهای اجرای این پروتکل برای $a.x \oplus b.y = z$ که خطا را برمی‌گرداند، کمتر از u باشد. به‌دلیل وجود پارامتر نوفه ν در پاسخ z برچسب، احتمال این که یک دور احراز هویت حتی برای برچسب درست (صادق) موفقیت‌آمیز نباشد، صفر نیست. بنابراین پیشامد رد غلط که در آن بازخوان، برچسب صادق را رد می‌کند با احتمال زیر اتفاق می‌افتد:

$$P_{FR} = \sum_{i=t+1}^{r}\binom{r}{i}\varepsilon^i(1-\varepsilon)^{r-i} \qquad (۹)$$

در همین حین یک دشمن که در حال ارسال پاسخ تصادفی z به بازخوان است، می‌تواند با احتمال زیر پذیرفته شود.

$$P_{FA} = \sum_{i=0}^{t}\binom{r}{i} \qquad (۱۰)$$

این پیشامد پذیرش غلط نامیده می‌شود. خوش‌بختانه این احتمالات (P_{FR} و P_{FA}) در k قابل چشم‌پوشی هستند؛ زیرا r= r(k) (استفاده از کران چرنوف به فهم آن کمک می‌کند). جداول ۱ و ۲ احتمال رد و پذیرش اشتباه را با توجه به پارامترهای مختلف نشان می‌دهند.

۴-۵ بررسی امنیت پروتکل HB^+

HB^+ درحقیت بهبودیافتهٔ پروتکل *HB* است که در برابر حمله غیرفعال امن است؛ ولی در برابر حملات فعال امن نیست. در یک حمله فعال دشمن نقش یک بازخوان را بازی می‌کند و تلاش دارد کلیدهای مخفی را از برچسب دریافت کند. ثابت شده است که HB^+ در برابر این نوع حملات، امن است [۶،۱۹]؛ ولی در برابر دشمنان قدرت‌مندتر مانند "مرد میانی" (MIM) امن نیست. در چنین حملاتی دشمن میان

برچسب و بازخوان قرار می‌گیرد و دارای توانایی‌هایی برای دست‌کاری پیام‌ها است. در [۷]، گیلبرت، رابشاو و سیلبرت یک حمله MIM در برابر HB^+با نام حمله GRS ارائه کردند. این حمله در شکل ۳ نشان داده شده است. در حمله GRS، به‌منظور آشکارسازی کلید مخفی X، دشمن به اصلاح تمام پیام‌های مبادله‌شده میان برچسب و بازخوان نیاز ندارد و تنها به بردار a نیاز دارد. دشمن اخلال δ را به بردار a می‌افزاید و در نظر می‌گیرد که آیا روند احراز هویت موفقیت‌آمیز هست یا نه. باز خوان آن را درصورتی‌که $a'.x \oplus b.y = z$ برقرار شود، تصدیق می‌کند و در آن $\delta.x \oplus \nu = 0$ است. اگر برچسب مجاز هم‌چنان با احتمال شکست ناچیز(P_{FR}) احراز هویت شود، آن‌گاه تمامی روند احراز هویت مختل نمی‌شود و این بدین معنی است که $\delta.x = 0$ است؛ در غیر این‌صورت $\delta.x = 1$ است. با استفاده از $\delta = e_i$ بردار با مقدار یک در موقعیت i و صفرها در مکان‌های دیگر، دشمن بیت x_i از بردار X را به‌دست می‌آورد. با k تکرار حمله با δ متفاوت، دشمن تمام کلید مخفی X را به‌دست می‌آورد. حمله‌کننده تمام r دور چالش را با اضافه‌کردن (1,0,0,……,0) تغییر می‌دهد و برای برچسب می‌فرستد. برچسب مقدار z را به‌صورت زیر محاسبه کرده و دوباره برای بازخوان ارسال می‌کند.

$$\begin{aligned} Z &= ((a \oplus (1,0,0,\ldots,0)).x) \oplus (b.y) \oplus \upsilon \\ &= (a.x) \oplus ((1,0,0,\ldots,0).x) \oplus (b.y) \oplus \upsilon \\ &= (a.x) \oplus x_1 \oplus (b.y) \oplus \upsilon \end{aligned} \qquad (۱۱)$$

بنابراین تمام پاسخ‌ها با x_1 تغییر می‌کنند (یا همه تغییر می‌کنند یا هیچ‌کدام تغییر نمی‌کند) و حمله‌کننده با توجه به واکنش بازخوان اگر برچسب تأیید شود، بنابراین $x_1=0$ در غیر این‌صورت $x_1=1$ خواهد شد. و این کار برای بیت‌های x_2……..x_n انجام می‌شود.

$$\mathcal{T}(x, y, \varepsilon)\ \mathcal{R}(x, y)$$

$$b \leftarrow \{0,1\}^k\ b\ a \leftarrow \{0,1\}^k \xrightarrow{\quad\quad}$$

$$\upsilon \leftarrow Ber_\varepsilon \qquad \xleftarrow{\ a\ }$$

$$z = (a.x) \oplus (b.y)\ z\ verify\ (a.x) \oplus (b.y) = z \xrightarrow{\quad\quad}$$

(شکل ۲): یک دور از پروتکل HB^+

(جدول ۱): پارامترهای استفاده شده در پروتکل‌های خانواده HB

k	*طول کلیدهای مخفی*
r	*تعداد دورهای تکرار*
ε	*سطح نوفه*
t	*آستانه پذیرش برچسب*

(جدول ۲): نرخ خطا و هزینه انتقال برای پارامترهای مختلف که در پروتکل HB^{+} تنظیم شده است. آستانه پذیرش از رابطه $t = r\varepsilon$ به‌دست می‌آید.

هزینه انتقال (بیت) [مقدار داده شده k]	P_{FA} احتمال پذیرش اشتباه	P_{FR} احتمال رد اشتباه	r	ε	k
82000 [k=512]	4×10^{-6}	0.44	80	0.25	224
61500	6×10^{-5}	0.43	60224	0.25	
41000	1×10^{-3}	0.42	40	0.25	224
51250	2×10^{-8}	0.44	50	0.125	200
41000	7×10^{-9}	0.38	40	0.125	200

$$\mathcal{T}(x, y, \varepsilon)\ \mathcal{R}(x, y)$$

$$b \leftarrow \{0,1\}^k\ b\ a \leftarrow \{0,1\}^k \longrightarrow$$

$$\upsilon \leftarrow Ber_{\varepsilon} a' = a \oplus \delta \qquad a \text{ مرد میانی}$$

$$\longleftarrow \qquad \longleftarrow$$

$$z = (a'.x) \oplus (b.y) \oplus v\ z\ verify\ (a.x) \oplus (b.y) = z$$

$$\longrightarrow$$

(شکل ۳): حمله GRS. دشمن اخلالی در بردار a می‌افزاید و در نظر می‌گیرد که آیا تمامی روند احراز هویت مختل می‌شود یا نه

۴-۶ پروتکل HB++

پروتکل HB++ (۲۰۰۶) یک پروتکل احراز هویت سبک‌وزن در برابر برخی حملات می‌تواند به‌عنوان یک پروتکل HB+ در نظر گرفته شود که دوبار تحت کلید مخفی مستقلی در حال اجرا است؛ ولی با چالش‌های همبسته. علاوه‌بر این کلیدهای مخفی، در هر مرحله از احراز هویت نوسازی می‌شوند. تمام برچسب‌ها و بازخوان‌ها دو تابع f و h را به‌اشتراک می‌گذارند. اولی تابعی است که برای ارتباط‌دادن چالش‌های پروتکل به هم‌دیگر به‌کار رفته و دومی برای تعیین کلیدهای مخفی برای احراز هویت به‌کار می‌رود [۲۳]. تفاوت اصلی این پروتکل با اجدادش در این است که شامل عملیات مثلثاتی و چرخشی و تابع چکیده‌ساز (h) است. این ویژگی آخر این پروتکل را غیر عملی می‌سازد؛ زیرا طبق استاندارد نباید ازتوابع چکیده‌ساز در برچسب‌ها استفاده شود. در شکل ۴ یک دور پروتکل HB++ نشان داده شده است.

این پروتکل r بار تکرار می‌شود و اگر N و N' تعداد خطاها را در Z و Z' نشان‌دهند، زمانی احراز هویت موفقیت‌آمیز خواهد بود که $N \leq t$ و $N' \leq t$ باشد. t آستانهٔ پذیرش برچسب توسط بازخوان است. با توجه به شکل ۵ مشاهده می‌شود که کلیدهای مخفی با استفاده از یک تابع چکیده‌ساز در هر دور احراز هویت نوسازی می‌شوند که البته استفاده از تابع چکیده‌ساز در برچسب‌های RFID خارج از استاندارد است.

$$\mathcal{T}(x, y, x', y', \varepsilon)\ \mathcal{R}(x, y, x', y')$$

$b \leftarrow \{0,1\}^k\ b\ a \leftarrow \{0,1\}^k$

$\longrightarrow$

$v, v' \leftarrow Ber_\varepsilon$

a

$\longleftarrow$

$z = (a'.x) \oplus (b.y) \oplus v\ (z, z')\ verify\ (a.x) \oplus (b.y) = z$

$\longrightarrow$

$z = (f(a).x') \oplus (f(b).y') \oplus v'\ verify\ (f(a).x') \oplus (f(b).y') = z'$

(شکل ۴): یک دور از پروتکل HB++

$$\mathcal{T}(Z)\ \mathcal{R}(Z)$$

$B \leftarrow \{0,1\}^k\ B\ A \leftarrow \{0,1\}^k$

$\longrightarrow$

A

$\longleftarrow$

$(x, y, x', y') = h(Z, A, B)\ (x, y, x', y') = h(Z, A, B)$

(شکل ۵): نحوه نوسازی کلیدها در برچسب و بازخوان

۴-۷ بررسی امنیت پروتکل HB++

در پاسخ به حمله گیلبرت و همکاران (۲۰۰۵) به HB+، برینگر و همکاران (۲۰۰۶) دو پروتکل (HB++ [نخستین تلاش] (شکل ۴) و HB++ (شکل ۵)) را ارائه کردند که در برابر چنین حملات مردمیانی ایمن است. هرچند، این پروتکل‌ها هنوز هم در برابر حملات از سوی مهاجمی که تظاهر می‌کند که بازخوان قابل اعتماد است، ایمن نیستند. نشان داده شد که HB++ [نخستین تلاش] نسبت به حملات برینگر و همکاران (۲۰۰۶) ایمن نیست [۲۳].

یک ضعف دیگر ناشی از این حقیقت است که پروتکل‌های HB++ و HB++ [اولین تلاش] حاوی z هستند مثل HB+، و این z را می‌توان برای شناسایی رمزهای x و y استفاده کرد. این یک ضعف است، چون مهاجم می‌تواند مشخصات را با دانستن z دنبال کند که یک کانال کناری ایجاد می‌کند (فان و ین ۲۰۰۶). مهاجم می‌تواند به‌راحتی z را با استفاده از حملهٔ مرد میانی (گیلبرت و همکاران ۲۰۰۵) یا با وانمودکردن به این که یک خواننده معتبر است، آن‌طور که درقبل در همین بخش صحبت شد، محاسبه کند.

با صرف‌نظرکردن از احتمال حملهٔ کانال کناری، مهاجم نیاز دارد تا دو رمز دیگر را مشخص کند. اینجا، فرض بر این است که مهاجم، توانایی دریافت ارسال‌ها را از برچسب و جلوگیری‌کردن از رسیدن این ارسال‌ها به بازخوان دارد. مهاجم می‌تواند a را به نفع خود دست‌کاری تا کلیدهای رمز (x', y') را بازیابی کند. در ابتدا، مهاجم می‌تواند a=0 را بفرستد تا $f(b).y'$ را تعیین کند. به‌محض تمام‌شدن این کار، مهاجم می‌تواند a=1 را قرار دهد تا $1.x' \oplus f(b).y$ را مشخص و رمز x' را از روی $f(b).y'$ و $1.x' \oplus f(b).y$ تعیین کند.

در خلال دورهای بعدی پروتکل، مهاجم می‌تواند a=b را قرارا دهد و $f(b).(x' \oplus y')$ را تعیین کند. با دانستن $f(b).y'$ و x'، مهاجم می‌تواند y' را تعیین کند.

برینگر و همکاران (۲۰۰۶) HB++[نخستین تلاش] را تغییر دادند تا آسیب‌پذیری را که شناسایی کرده بودند، برطرف کنند و HB++ (شکل ۵) را ارائه کردند که در برابر این آسیب‌پذیری‌ها محافظ دارد. با این حال، HB++ هم مستعد چنین حملاتی که مهاجم وانمود می‌کند یک بازخوان معتبر است، هست. اینجا، دوباره، z را می‌توان برای بازیابی x' و y'مورد استفاده قرار داد، درست مانند HB+. برای بازیابی دو رمز $(x'$ و$y')$، باید فرضیات زیر را داشته باشیم: ρ در هر دور فقط یک‌بار به‌هنگام می‌شود، و دوری با این هدف با ارسال b توسط برچسب شروع و با بررسی z, z' توسط بازخوان تمام می‌شود. به‌هنگام‌سازی ρ به‌احتمال در ابتدای هر دور اتفاق می افتد. با این حال، یک مهاجم سریع می‌تواند بین دو ارسال موفق b، چندین مرتبه با برچسب ارتباط برقرار کند. تا هنگامی‌که b و ρ در زمان ارتباط مهاجم با برچسب ثابت باشند، نام‌برده در زیر، در آشکارکردن دو رمز (x', y') کمک خواهد کرد. فرض می‌شود که مهاجم توان تفسیر b ارسال شده توسط برچسب و جلوگیری از رسیدن b به بازخوان را دارد. مهاجم می‌تواند a را به نفع خودش دست‌کاری تا (x', y') را بازیابی کند. در ابتدا، مهاجم a=0 را می‌فرستد تا$rot(f(b), \rho).y'$ را تعیین کند. به‌محض انجام این کار، مهاجم قرار می‌دهد a=1 تا $1.x' \oplus rot(f(b), \rho).y''$ را تعیین و سپس مهاجم می‌تواند x' را از روی$rot(f(b), \rho).y'$ و $1.x' \oplus rot(f(b), \rho).y''$ مشخص کند.

در خلال دورهای بعدی پروتکل، مهاجم می‌تواند a=b قرار دهد و $rot(f(b), \rho).(x' \oplus y')$ را تعیین و با دانستن $rot(f(b), \rho).y'$ و x' می‌تواند y' را مشخص کند.

۴-۸ پروتکل HB*

این پروتکل r بار تکرار می‌شود و احراز هویت، زمانی موفق است که درنهایت t دور از r دور احراز هویت موفقیت‌آمیز نباشد [۳۰].

$$t > \varepsilon r \qquad (۱۲)$$

۴-۹- بررسی امنیت پروتکل HB*

حمله GRS : ثابت δ را به‌چالش a اضافه می‌کنیم؛ سپس اگر ε′ پایین باشد، بیشتر دورها از معادله a.x⊕b.y استفاده خواهند کرد که معادل است با پروتکل HB+. (زمانی درست است که$\varepsilon' = \frac{t-\varepsilon r}{r(1-r\varepsilon)}$) برعکس اگر ε′ نزدیک به$\frac{1}{2}$ باشد موارد زیر اتفاق می‌افتد:

اگر $\delta.y = 0$ و $\delta.x = 0$ باشد، بازخوان پذیرفته خواهد شد. در همه حالات دیگر بازخوان رد خواهد شد. بنابراین دشمن قادر خواهد بود فضای برداری <x,y> را به‌دست آورد. مراحل حمله به‌صورت زیر است. مقادیر خطی$\delta_1 \ldots\ldots \delta_{k-2}$ را به‌طوری پیدا کنید که احراز هویت انجام گیرد. به‌احتمال قریب به یقین این کار یک مجموعه نامرتب به‌صورت زیر می دهد {{c1 ,c2 ,c3} = {x,y,x⊕y}. سپس مقدار x⊕y را در مجموعه { c1 ,c2 ,c3} بوسیله درخواست برچسب واقعی با a=b در هر دور طوری تعیین کنید که z=a.(x⊕y)⊕υ شود. اولین جعل هویت با احتمال ۲/۱ پیش خواهد رفت. جعل هویت های بعدی با احتمال ۱ پیش خواهد رفت. پیچیدگی خطی : O(4K) احراز هویت مورد نیاز است [۲۴].

۴-۱۰ پروتکل random HB#

یک دور از پروتکل احراز هویت Random-HB# که در آن کلیدهای مخفی X و Y ماتریس‌های تصادفی دودویی هستند. مرحله تأیید نیاز به مقایسه دو بردار و به‌دست‌آوردن حکم رد یا قبول دارد.

$\mathcal{R}(\mathrm{x,y,s})$ بردارهای k بیتی مخفی $\mathcal{T}(\mathrm{x,y,s},\varepsilon)(\mathrm{x,y,s})$

$b \leftarrow \{0,1\}^k \ (b,w) \ a \leftarrow \{0,1\}^k$

$\longrightarrow$

$v \leftarrow Ber_\varepsilon$

$w = b.s \oplus v \ a$

$\longleftarrow$

$if \ v = 0$

$z = (a.x) \oplus (b.y) \oplus v \ z \ if \ b.s = w \ \ verify \ (a.x) \oplus (b.y) = z$

$\longrightarrow$

$elsez = \ (a.y) \oplus (b.x) \oplus v \ else \ verify \ z = \ (a.y) \oplus (b.x)$

(شکل ۶): یک دور از پروتکل HB^*.

پارامترها به‌کاررفته: $(\mathrm{k_x}, \mathrm{k_y}, m, \eta, u)$

$\mathcal{T}(X,Y) \ \mathcal{R}(\mathrm{X,Y})$

$v \in_R \{(0,1\}^m, (v_i{=}1){=}\eta$

$for \ 1 \le i \le m\} \ b \ a \leftarrow \{0,1\}^{k_x}$

$\longrightarrow$

$b \leftarrow \{0,1\}^{k_y} \ a$

$\longleftarrow$

$z = (a.X) \oplus (b.Y) \oplus v \ z \ Hwt[\ (a.X) \oplus (b.Y) \oplus z] \le um$

$\longrightarrow$

(شکل ۷): یک دور از پروتکل احراز هویت Random-HB#

۴-۱۱ پروتکل HB#

اشکال عمده Random-HB # این است که به حافظه زیادی در حدود ده‌ها کیلیو بیت که از طریق رابطه $(k_x+k_y).m$ به‌دست می‌آید احتیاج دارد. پروتکل HB# این مشکل را حل کرده و با توجه به این‌که از جهات دیگر شبیه پروتکل Random-HB # است، و تنها فرق آن این است که از فرم ماتریس آن توبلیتس است که دارای ویژگی‌های جالبی است و مقدار حافظه مورد نیاز را با توجه به رابطه (k_x+k_y+2m+2) به‌دست می‌آید، که به‌طور عملی حدود ۱/۵ کیلو بیت است. در جدول ۳ پارامترهای مختلف این پروتکل بر اساس طول کلیدهای X,Y و پارامترهای دیگر از قبیل ضریب نوفه (ε)، تعداد تکرار (t) و طول پارامتر نوفه ((m مورد بررسی قرار گرفته است.

(جدول ۳): پارامترهای عددی برای پروتکل

Storage (bits)	*Transmission (bits)*	*False accept rate* P_{FA}	*False reject rate* P_{FR}	*HB#* $K_X K_Y\ m\ \varepsilon\ t$
2918	*1756*	2^{-83}	2^{-45}	*80 512 1164 0.25 405*
1472	*1033*	2^{-83}	2^{-45}	*80 512 441 0.125 113*

۵- انواع دیگری از مسأله LPN

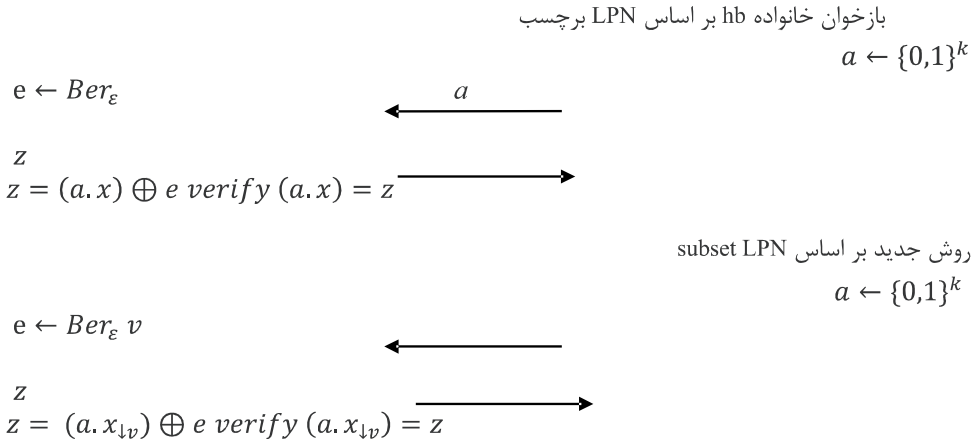
مسالهٔ LPN و گونه‌های تغییریافتهٔ آن به‌عنوان یک مسألهٔ در گسترهٔ وسیعی از سامانه‌های رمزی کلید عمومی و پروتکل‌های شناسایی و احراز هویت مورد استفاده قرار گرفته‌اند. در این قسمت برخی از انواع دیگر مسأله LPN و همچنین برخی از انواع دیگر پروتکل‌ها بر مبنای مسأله LPN را شرح می‌دهیم.

۵-۱ subset LPN

در این بخش یک پروتکل جدید دو دوری احراز هویت شرح داده می‌شود و امنیت آن در برابر حملات فعال تحت سختی مسأله $SLPN_{2,2l,d}$ اثبات می‌شود، که در آن d=l/(k+Y) برای مقدار ثابت Y>0 (به‌طور مشخص Y= ۰,۱ برای منظورهای عملی در نظر گرفته می‌شود) [۲۹].

۵-۲ مقایسه پروتکل subset LPN با پروتکل‌های خانواده HB

در این شکل پروتکل‌های خانواده HB با پروتکل‌های جدید مقایسه شده است. همان‌طور که در شکل ۸ مشاهده می‌شود در HB بردار a در s ضرب نقطه‌ای می‌شود؛ درحالی‌که در روش جدید بردار a در $s_{\downarrow V}$ ضرب نقطه‌ای می‌شود.



(شکل ۸): اساس کار پروتکل‌های جدید ومقایسه آن با خانواده HB

۵-۳ پارامترهای عمومی:

پروتکل‌های احراز هویت دارای پارامترهای زیر است که در آن T', T ثابت و n, l وابسته به پارامتر امنیتی λ هستند.

(جدول ۴): پارامترهای عمومی پروتکل subset LPN

طول کلمه رمز	$l \in \mathbb{N}\ s \in \mathbb{Z}_l^{2l}$
پارمتر توزیع برنولی	$Ber_\varepsilon\ \tau \in]0,1/2[$
آستانه پذیرش	$\tau' = 1/4 + \tau/2$
تعداد تکرارهای موازی	$n \in N$

$$\mathcal{T}(\mathrm{x}, \varepsilon)\ \tau = 0.1\ x \leftarrow \{0,1\}^{2l}\ \mathcal{R}(\mathrm{x})$$

$$a \leftarrow \{0,1\}^l\ V \leftarrow \{0,1\}^{2l}, \|V\|_1 = l$$

$$\mathrm{e} \leftarrow Ber_\varepsilon \qquad \xleftarrow{\quad v \quad}$$

$$z = (a.x_{\downarrow v}) \oplus e\ z\ acceptif\ \|(a.x_{\downarrow v}) \oplus z\|_1 \leq 0.2n$$

$$\xrightarrow{\quad}$$

(شکل ۹): یک دور از پروتکل جدید subset LPN

m=6, n=3
X= 1 0 0 0 1 1
V= 0 0 1 1 1 0
$X_{\downarrow v}$= 0 0 1

(شکل ۱۰): عملگری که در پروتکل جدید استفاده می‌شود.

۵-۴- تولید کلید:

الگوریتم KG (1^λ) از $x \leftarrow \{0,1\}^{2l}$ نمونه برداری کرده و x را به‌عنوان کلید محرمانه بر می‌گرداند. پروتکل احرازهویت دو دوری در شکل ۹ نشان داده شده است.

۵-۵- Toeplitz LPN

نخستین کاربرد واقعی مسالهٔ LPN در زمینهٔ رمزنگاری به سال ۲۰۰۱ برمی‌گردد که پروتکل احراز هویت HB پیشنهاد شد. این پروتکل که یک پروتکل مبتنی بر LPN است، طوری طراحی شد که انسان بتواند آن را فقط با کاغذ و خودکار اجرا کند. ازاین‌رو فقط در مدل حملهٔ غیرفعال، امن است. دو سال بعد، جولز و ویز[1]، به‌همراه کیتز و شین[2]، با بسط HB یک ساختار اصلاح‌شده پیشنهاد کردند. پروتکل اصلاح‌شده HB^+ نامیده شد. برخلاف مورد قبلی، HB^+ به‌گونه‌ای طراحی شد که در مدل حملهٔ فعال هم امن

[1] Julez and weis
[2] Kita and shin

باشد. ولی گیلبرت[1] و همکارانش فهمیدند که پروتکل HB^+ در خطر حملات مرد میانی قرار دارد که امنیت در مدل حملهٔ فعال را از بین می‌برد. پس از آن همین پژوهش‌گران شکل دیگری از پروتکل HB را با عنوان $HB^\#$ پیشنهاد کردند که جهت مقاوم‌بودن در برابر این حملات طراحی شده بود. علاوه‌بر اصلاح پروتکل، آن‌ها مشکل اندازهٔ بزرگ کلید یا پیچیدگی مخابراتی را با استفاده از یک پروتکل اندکی تغییریافته از LPN با عنوان TOEPLITZ-LPN حل کردند. با وجود این که ضعفی برای استفاده از TOEPLITZ-LPN گزارش نشده، ولی تاکنون در مورد سختی آن اطلاعاتی در دسترس نیست. در این نوع از مسأله LPN تنها تفاوت این است که برای ایجاد کلیدهای مخفی از ماتریس خاصی به نام توبلیتس[2] استفاده می‌شود.

۵-۶ Ring LPN

به‌تازگی هیس و همکارانش یک پروتکل شناسایی دو مرحله‌ای با عنوان Lapin پیشنهاد کردند. این پروتکل بیشتر براساس RING-LPN است تا LPN. با استفاده از خصوصیات ذاتی حلقه‌ها، پروتکل پیشنهادی برای استفاده در محیط‌های مقید خیلی مناسب است. در RING-LPN اراکل عناصر $v, v = s.r + e$ را از یک حلقهٔ چند جمله‌ای $Z_2[X]/(f)$ می‌دهد؛ یعنی. $v, s, r, e \in Z_2[X]/(f)$ این مسأله می‌تواند از یک چندجمله‌ای تقلیل‌ناپذیر f، یا یک چندجمله‌ای تقلیل‌پذیر استفاده کند. با انتخاب یک چندجمله‌ای تقلیل‌پذیر می‌توان از تئوری باقی‌ماندهٔ چینی (CRT) برای پیاده‌سازی مؤثر رمزنگاری استفاده کرد.

۵-۷ پروتکل HB بر اساس Ring LPN

تفاوت این نوع پروتکل با پروتکل معمولی HB در این است که پارامترهای کلید مخفی x و پارامتر چالشی a و همچنین پارامتر نوفه υ همگی متعلق به حلقه یا میدان چندجمله‌ای $Z_2[X]/(f)$ هستند.

۵-۸ پروتکل lapin بر اساس ring LPN

این پروتکل احراز هویت بر روی حلقه $R=Z_2[X]/(f(x))$ تعریف شده و شامل یک نگاشت مناسب $\pi\{0,1\} \to R$ است. پروتکل احراز هویت دارای پارامترهای عمومی زیر است، که در آن τ, τ' ثابت هستند و n بستگی به پارامتر امنیتی λ دارد. شکل ۱۲ یک دور از این پروتکل را نشان می‌دهد[۳۱].

۵-۹ پروتکل احراز هویت بر اساس توابع شبه تصادفی ضعیف از مسأله LPN:

از زمانی که هاپر و به لوم استفاده از LPN را آغاز کردند تاکنون، ساختارهای متعددی پیشنهاد شده است. به‌عنوان برخی از مهم‌ترین آن‌ها می‌توان پروتکل‌های پیشنهادی توسط کیلتز و همکارانش و دودیس و همکارانش را نام برد که نشان دادند چگونه می‌توان براساس LPN کدهای احراز هویت پیام را ساخت. وجود MAC ها امکان ارائهٔ روش‌های شناسایی‌ای را که در برابر حملات فعال، ایمن هستند، فراهم می‌کند. شکل ۱۳ این پروتکل را نمایش می‌دهد.

جدول ۶ مقایسه‌ای را بین پروتکل‌های مختلف و حملات صورت‌گرفته و سال حمله به آن‌ها را نشان می‌دهد. در این‌جا مشاهده می‌کنیم که اکثر پروتکل‌ها مورد حمله قرار گرفته‌اند و امنیت لازم را ندارند.

۶- جمع بندی و نتیجه‌گیری

با توجه به مطالبی که مطرح شد، مشاهده می‌کنیم که تلاش‌ها برای رسیدن به یک پروتکل سبک‌وزن که قابلیت پیاده‌سازی بر روی برچسب‌های RFID را داشته باشد و همچنین ایمنی کافی در برابر حملات مختلف به‌خصوص حمله مرد میانی را داشته باشند، همچنان ادامه دارد. در این راستا پروتوکل‌های بسیاری از طرف دانشمندان رمزنگاری ارائه شده است که بسیاری از آن‌ها در برابر حملات مرد میانی مقاومت کافی را نداشته‌اند و برخی نیز امنیت آن‌ها اثبات نشده است و همچنان پژوهش در این حوزه ادامه دارد.

[1] gilbert
[2] Toeplitz matrix

$\mathcal{T}(s)$ common secret **s** in$Z_2[X]/(f(x))$ $\mathcal{R}(s)$

$r \leftarrow Z_2[X]/(f(x))$

$e \leftarrow \beta_{\frac{1}{8}}^{n}$

r

$\longleftarrow$

t accept iff t+rs is 0 for more

$t = rs + e$ than 60% of the coefficients $\longrightarrow$

(شکل ۱۱): یک دور از پروتکل HB بر اساس Ring LPN

(جدول ۵): پارامترهای عمومی پروتکل lapin

n,R	و deg(f) =n R=Z_2[X]/(f)
$\pi:\{0,1\}^{\lambda}$	نگاشت R
$\tau \in (0,1)$	پارامتر توزیع برنولی
$\tau' \in (\tau, \frac{1}{2})$	آستانه پذیرش

$\mathcal{T}(s, s', \varepsilon)$ $\mathcal{R}(s, s')$

$c \leftarrow \{0,1\}^{\lambda}$

$e \leftarrow Ber_{\varepsilon}$

$r \leftarrow R^{*}$ c

$\longleftarrow$

(r, z)

$\longrightarrow$ *If* $r \notin R^{*}$ *reject*

$e' := z - r.(s.\pi(c) + s')$

$z = r.(s.\pi(c) + s') \oplus e$ *if* $wt(e') > n\,.\,\tau'$ *reject*

else accept

(شکل ۱۲): یک دور از پروتکل Lapin

$$\mathcal{T}(f,h,s)\ \mathcal{R}(f,h,s)$$
$$F: \mathbb{D} \to \mathbb{F} \textit{(a randomized weak-PRFfamily with noise X)}$$
$$H: \mathbb{D} \to \mathbb{F} \textit{(a pairwise-independent function family)}$$
$$\textit{Keys: } f \leftarrow F\ \ h \leftarrow H,\ \ s \leftarrow \mathbb{F}$$

$$r \leftarrow D\ r\ c \leftarrow F$$
$$\xrightarrow{\quad\quad}$$
$$\xleftarrow{\quad c \quad}$$
$$z = f^{x}(r)s + h(r)c\ accept\ iff$$
$$z\|f(r) - s^{-1}(z - h(r)c\| \le \tau'$$
$$\xrightarrow{\quad\quad}$$

(شکل ۱۳): پروتکل احراز هویت مبتنی بر توابع شبه تصادفی ضعیف.

جدول ۶: حملات انجام شده بر روی پروتکل‌های مختلف خانواده HB

(*) احتیاج به تعداد زیادی چالش – پاسخ دارد.

سال حمله	نوع حمله	سال پیشنهاد پروتکل	پروتکل
2001	فعال	2001	HB
2006	GRS	2005	HB+
2008	GRS	2006	HB++
2008	غیر فعال	2007	HB-MP
2008	GRS	2007	HB*
2008	غیر فعال	2008	HB-MP+
2009	MITM(*)	2008	Trusted-HB
2008		2008	HB#

۷- مراجع:

[1] Cho, J. S., & Park, J. J. (2012). High attack cost: Hash based RFID tag mutual authentication protocol. In 3rd international conference on computer science and its applications, lecture notes in electrical engineering (Vol. 114, pp. 113–120).

[2] Hernandez-Castro, J. C., Peris-Lopez, P., Safkhani, M., Bagheri, N., & Naderi, M. (2012). Another fallen hash-based RFID authentication protocol. In WISTP 2012, lecture notes in computer science (Vol. 7322, pp. 29–37).

[3] Zhou, S., Zhang, Z., Luo, Z., & Wong, E. C. (2010).Alightweight anti-desynchronization RFID authen-tication protocol. Information Systems Frontiers, 12(5), 521–528.

[4] Quafi, K., Overbock, R., & Vaudenay S. (2008). On the security of HB# against a man-in-the-middle attack. In Proceedings of 14th international conference on the theory and application of cryptology and information security, 2010 (Vol. 5350, pp. 108–124).

[5] Hopper, N. J., & Blum, M. (2001). Secure human identification protocols. In Cryptology–ASIACRYPT 2001, lecture notes in computer science (Vol. 2248, pp. 52–66).

[6] Juels, A., & Weis, S. (2005). Authenticating pervasive devices with human protocols. In Cryptology– crypto 2005, lecture notes in computer science (Vol. 3621, pp. 293–308).

[7] Gilbert, H., Robshaw, M., & Silbert, H. (2005). An active attack against HB+-a provable secure light-weighted authentication protocol. Cryptology ePrint archive,report2005/237.http:// eprint.iacr.-org

[8] Piramuthu, S. (2007). Protocols for RFID tag/ reader authentication. Decision Support Systems, 43(3), 897–914.

[9]Munilla, J., & Peinado, A. (2007). HP-MP: A further step in the HB-family of lightweight authentication protocols. Computer Networks, 51(9), 2262–2267.

[10] Leng, X., Mayes, K., & Markantonakis, K. (2008). HB-MP+ protocol: An improvement on the HB-MP protocol. In IEEE international conference on RFID (pp. 118–124), Apr 16–17 2008.

[11]Yoon, B., Sung, M. Y., Yeon, S., Oh, H. S., Kwon, Y., Kim, C., et al. (2009). HB- MP++ protocol: An

ultra light-weight authentication protocol for RFID system. In IEEE international conference on RFID (pp. 186–191), Apr 27–28 2009.
[12] Gilbert, H., Robshaw, M., & Seurin, Y. (2008). HB#: Increasing the security and efficiency of HB+. In EUROCRYPT 2008 (pp. 361–387).
[13] Madhavan, M., Thangaraj, A., Sankarasubramanian, Y., & Viswanathan, K. (2010). NLHB: A non-linear hopper-blum protocol. In Proceedings of IEEE international symposium on information theory, 2010(pp. 2498–2502).
[14] Abyaneh, M. R. S. (2010). On the security of non-linear HB (NLHB) protocol against passive attack. In Proceedings of IEEE/IFIP international conference on embedded and ubiquitous computing, 201(pp. 523–528)
[15] Bosley, C., Haralambiev, K., & Nicolosi, A. (2011). HBN: An HB-like protocol secure against man-in-the-middle attacks. Cryptology ePrint archive, report 2011/350.
[16] Ali, S. A., Mohamed, R. M., & Fahim, M. H. (2011). RCHB: Light-weight, provably-secure variants of the HB protocol using rotation and complementation. In Proceedings of 5th international conference on network and system security, 2011 (pp. 244–248).
[17] Cao, X., & O'Neill, M. (2011). F-HB: An efficient forward private protocol. In Proceedings of workshop on lightweight security and privacy: Devices, protocols, and applications, 2011 (pp. 53–60).
[18]Oded regev, the learning with error problem, 2010
[19]Jonathan Katz and Ji Sun Shin Parrallel and concurrent Secyrity of the HB and HB$^+$ Protocols Avilable at: http://eprint.iacr.org/2005/461
[20]E. R. Berlekamp, R. J. McEliece, and H. C. Van Tilborg. On the inherent intractability ofcertain coding problems. IEEE Transactions on Information Theory, 24(3):384{386, 1978.
[21] A. Blum, M. Furst, M. Kearns, and R. J. Lipton. Cryptographic primitives based on hard learning problems. In Advances in cryptology|CRYPTO-'93, pages 278{291. Springer,1994.
[22]A. Blum, A. Kalai, and H. Wasserman. Noise-tolerant learning, the parity problem, andthe statistical query model. Journal of the ACM (JACM), 50(4):506{519, 2003.
[23] J. Bringer, H. Chabanne, and E. Dottax. HB++: a lightweight authentication protocolsecureagainst some attacks. In Security, Privacy and Trust in Pervasive ndUbiquitousComputing, 2006. SecPerU 2006. Second International Workshop on, pages 28{33. IEEE,2006.7
[24] H. Gilbert, M. J. Robshaw, and Y. Seurin. Good variants of HB+ are hard to _nd. InFinancial Cryptography and Data Security, pages 156{170. Springer, 2008.
[25] N. J. Hopper and M. Blum. A secure human-computer authentication scheme.InTechnical Report CMU-CS-00-139. Carnegie Mellon University, 2000.
[26] M. Kearns. E_cient noise-tolerant learning from statistical queries. Journal of the ACM (JACM), 45(6):983{1006, 1998.
[27] E. Levieil and P. A. Fouque. An improved LPN algorithm. In Security and Cryptography for Networks, pages 348{359. Springer, 2006.
[28]J.Carrijo, R.Tonicelli, H.Imai, A.C.A.Nascimento. A Novel Probabilistic Passive Attack on the Protocols HB and HB+. Available from http: //eprint.iacr.org /2008/ 231.pdf.
[29]Eike Kiltz, Krzysztof Pietrzak, David Cash, Abhishek Jain and Daniele Venturi, the Effcient Authentication from Hard Learning Problems, 2007-2013.
[30]D. Duc and K. Kim, \Securing HB$^+$ against GRS Man-in-the-Middle Attack," in Proc. of Symposium on Cryptography and Information Security (SCIS), 2007.
[31]S.Heyse, E. Kiltz, K.Pietrzak,C.Paar,Lapin an Efficient Authentication Protocol Based on Ring-LPN Volume 7549 of the series Lecture Notes in Computer Science pp 346-365,2012.

نصـــور باقری هم‌اکنون به‌عنوان استاد یار در دانشکدظ مهندسی برق دانشگاه شـــهید رجایی فعالیت می‌کند. ایشـــان کارشـــناسـی خود را در رشتهٔ مهندسی برق از دانشـگاه مازندران و کارشـناسی ارشد و دکترای خود را در همین رشته از دانشـــگاه علم وصـــنعت دریافت کرده اســـت. علایق پژوهشـــی ایشـــان شـــامل تحلیل و طراحی طرح‌های رمز نگاری متقارن، فناوری RFID و پروتکل‌های امنیتی است.

رضـا آقامحمدی مدارک کارشناسی و کارشناسی ارشد خود را به‌ترتیب از دانشـگاه شـهید شمسی‌پور و دانشگاه شـــهیـد رجـایی، تهران، ایران در ســـال‌هـای ۷۹ و ۹۴ دریـافت کرده اســـت. زمینهٔ پژوهشـــی وی تحلیل امنیت پروتکل‌های احراز اصـــالت مبتنی بر مســـئله LPN برای سامانه‌های RFID است.