# استخراج بیت‌های با نرخ بالا برای تولید کلید محرمانه مشترک با استفاده از تخمین فاز فیدینگ کانال‌های MIMO و کوانتیزاسیون چندسطحی

وجیهه زینلی فتح‌آبادی، حسین خالقی بیزکی و علی شهزادی

**چکیده: اخیراً روش‌های تولید کلید محرمانه مشترک با استفاده از مشخصات تصادفی‌بودن دامنه و فاز سیگنال دریافتی و تقارن کانال مشترک در سیستم‌های مخابراتی بی‌سیم، مورد توجه زیادی واقع شده است. پروتکل‌های تولید کلید بر اساس تخمین فاز سیگنال دریافتی، به علت توزیع یکنواخت فاز فیدینگ کانال، هم برای محیط‌های ساکن و هم سیار مناسب بوده و همچنین دارای نرخ تولید کلید بالاتری نسبت به پروتکل‌های تولید کلید بر اساس توان سیگنال دریافتی می‌باشند. علاوه بر این عموماً کارهای پیشین روی پروتکل تولید کلید روی سیستم‌های تک‌آنتنه (SISO) متمرکز بوده‌اند که دارای نرخ تولید کلید قابل توجهی نیستند. از این رو در این مقاله برای افزایش تصادفی‌بودن و نرخ تولید کلید از تخمین فاز سیگنال دریافتی روی سیستم‌های چندآنتنه (MIMO) برای تولید کلید محرمانه مشترک استفاده می‌شود، زیرا سیستم‌های MIMO دارای یک توانایی برای عرضه متغیرهای تصادفی بیشتر جهت تولید کلید نسبت به سیستم‌های SISO می‌باشند. نتایج شبیه‌سازی نشان‌دهنده این است که نرخ تولید کلید در حالتی که تعداد آنتن‌های فرستنده و گیرنده یکسان و برابر با ۲ و ۳ باشد، به ترتیب ٤ و ۹ برابر زمانی است که از ۱ آنتن فرستنده و گیرنده استفاده شود. همچنین هنگامی که جهت استخراج بیت‌های کلید محرمانه از کوانتیزاسیون چندسطحی استفاده شود، نرخ تولید کلید افزایش قابل ملاحظه‌ای پیدا خواهد کرد.**

**کلید واژه: کلید محرمانه مشترک، کانال فیدینگ MIMO، تخمین فاز، کوانتیزاسیون چندسطحی.**

## ۱- مقدمه

امنیت در مخابرات بی‌سیم نیازمند تبادل کلید محرمانه بین طرفین ارتباط است. تدبیرهای امنیتی رایج بر پایه ساختار سیستم‌های رمزنگاری کلید عمومی و الگوریتم‌های رمزنگاری با مدیریت کلیدهای رمزشده می‌باشد. اخیراً تعدادی از روش‌های تولید کلید با بهره‌گیری از اطلاعات و تکنیک‌های لایه فیزیکی شبکه‌های بی‌سیم به عنوان راه حلی دیگر برای تولید کلید در شبکه‌های بی‌سیم ارائه شده است.

این روش‌ها از ماهیت تصادفی‌بودن ذاتی فیدینگ کانال‌های بی‌سیم برای تولید کلید بهره برده‌اند. در مقایسه با پروتکل توافق کلید دیفی- هلمن [۱] که بر پایه محاسبه پیچیدگی استوار است، روش‌های بر پایه اطلاعات لایه فیزیکی دیگر بر فرض محدودبودن توان دشمن برای محاسبات پیچیده استوار نمی‌باشد و این بدین معنی است که امنیت چنین روش‌هایی دیگر امنیت محاسباتی نبوده، بلکه دارای امنیت کامل از نظر تئوری اطلاعات است [۲].

به طور کلی در روش‌های مبتنی بر اطلاعات لایه فیزیکی کانال از ۳ ویژگی فیدینگ کانال‌های بی‌سیم: ۱) تقارن کانال، ۲) تغییرات زمانی کانال و ۳) تغییرات مکانی کانال، جهت برقراری امنیت و تولید کلید محرمانه مشترک استفاده می‌شود [۲] تا [۱۳]. برخی از محققان با استفاده از کانال‌های چندمسیره به عنوان یک کانال تصادفی مشترک، از توان سیگنال دریافتی (RSS)[1] برای استخراج بیت‌های محرمانه مشترک بین واحدهای ارتباطی بهره برده‌اند [۲] تا [۷]. در حال حاضر مسئله قابل پیاده‌سازی بودن روش‌های بر پایه RSS ثابت شده اما این روش‌ها در برخی مسایل از قبیل مناسب‌نبودن برای محیط‌های ساکن، تعمیم به کلیدهای گروهی و نرخ پایین تولید کلید ضعف‌هایی دارند. از این رو چند طرح جهت بهبود نرخ تولید کلید وجود دارد [۷] و [۸]. مثلاً [۸] با بهره‌گیری از تکنیک دایورسیتی روی ۳ آنتن، به کلیدی با ۴ برابر افزایش نرخ تولید کلید دست یافته است.

دسته دیگری از طرح‌های تولید کلید مشترک بر مبنای مشخصه‌های فیدینگ کانال بی‌سیم در لایه فیزیکی، بیت‌های تصادفی مشترک خود را از تخمین فاز سیگنال دریافتی استخراج می‌کنند [۹] تا [۱۳]. در مقایسه با طرح‌های تولید کلید بر اساس مشخصات RSS، روش‌های بر پایه تخمین فاز سیگنال دریافتی، مزیت‌هایی را دارا هستند: اول این که به علت توزیع یکنواخت فاز کانال‌های فیدینگ، بیت‌های استخراجی متوسط آنتروپی بالاتری را دارا هستند، ثانیاً از نرخ تولید کلید بالاتری برخوردار می‌باشند و ثالثاً قابل پیاده‌سازی روی هر دو محیط ساکن و سیار بوده و در نهایت به علت قابلیت جمع‌پذیری فازهای تخمینی روی چندین گره، قادر به تولید کلیدهای گروهی می‌باشند. به طور مثال یک طرح تولید کلید بر پایه تخمین فاز کانال در [۹] پیشنهاد شده که علاوه بر تولید کلید بین دو گره، قابلیت تولید کلید بین چندین گره را دارد و در [۱۱] یک طرح تولید کلید بر اساس تخمین فاز کانال برای سیستم‌های OFDM پیشنهاد گردیده است. امنیت اطلاعاتی این طرح‌ها بر اساس این حقیقت ضمانت می‌شوند که برای دشمن واقع در مکان متفاوتی از فرستنده و گیرنده، به دست آوردن اطلاعات فاز یکسان برای تولید کلید، غیر عملی و نشدنی است [۹] تا [۱۲].

با توجه به مزیت‌های روش‌های بر پایه تخمین فاز سیگنال‌های

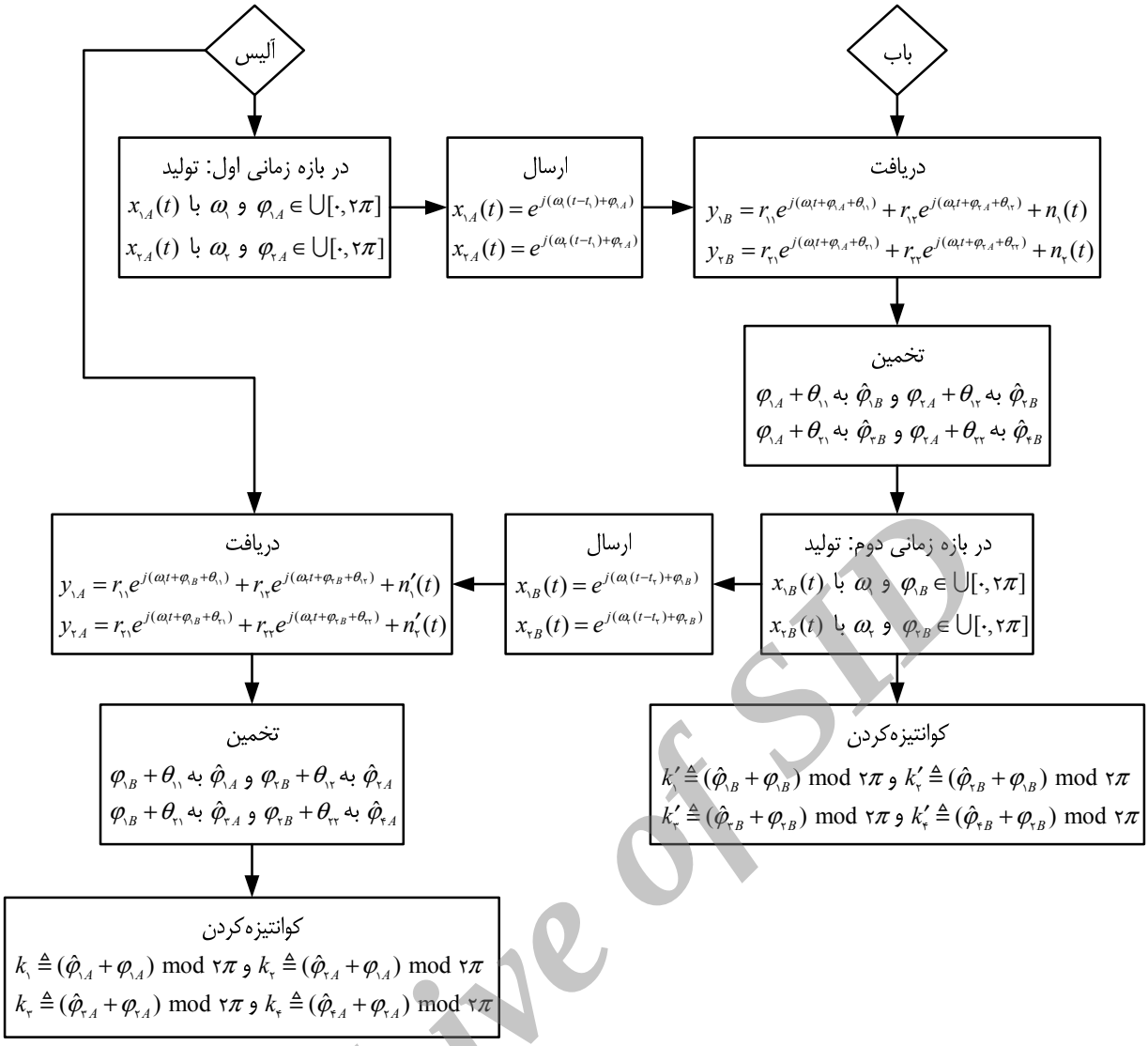
این مقاله در تاریخ ۱۲ دی ماه ۱۳۹۱ دریافت و در تاریخ ۱ مهر ماه ۱۳۹۳ بازنگری شد.

وجیهه زینلی فتح‌آبادی، مجتمع برق و الکترونیک، دانشگاه صنعتی مالک اشتر، تهران، (email: vzeinaly@yahoo.com).

حسین خالقی بیزکی، گروه مخابرات، مجتمع برق و الکترونیک، دانشگاه صنعتی مالک اشتر، تهران، (email: bizaki@ee.iust.ac.ir).

علی شهزادی، گروه مخابرات، دانشگاه سمنان، سمنان، (email: shahzadi@iust.ac.ir).

1. Received Signal Strength




شکل ۱: نحوه اجرای یک دور از پروتکل تولید کلید برای سیستم MIMO که $N_T = N_R = 2$ باشد.

دریافتی، در طرح پیشنهادی این مقاله از هم‌پاسخی فاز کانال استفاده شده است. علاوه بر این در این مقاله برای افزایش نرخ تولید کلید از یک سیستم چندورودی- چندخروجی (MIMO) استفاده گردیده است.

ادامه مقاله بدین صورت سازماندهی می‌شود: در بخش ۲ به معرفی مدل سیستم خواهیم پرداخت. جزئیات مراحل پروتکل تولید کلید شامل تست کانال، کوانتیزه‌کردن فازها و تطبیق کلید رمز و تقویت محرمانگی در بخش ۳ بیان می‌شوند. در بخش ۴ احتمال توافق کلید بررسی شده و در بخش ۵ در مورد تحلیل امنیت بحث می‌شود. در بخش ۶ نتایج شبیه‌سازی مورد تحلیل و بررسی قرار گرفته و در نهایت نتیجه‌گیری در بخش ۷ بیان می‌گردد.

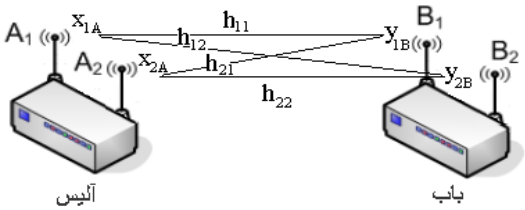
## ۲- مدل سیستم

مدل سیستمی که در اینجا برای تولید کلید محرمانه مشترک به کار گرفته شده است: فرض می‌شود آلیس و باب هر کدام دارای دو آنتن به صورت نیمه- دوطرفه بوده (به این معنا که هر یک از فرستنده و گیرنده قادر به ارسال و دریافت هم‌زمان سیگنال در یک فرکانس یکسان نمی‌باشند، یعنی یا ارسال و یا دریافت صورت می‌گیرد) و شنودگر (ایو) که قصد استراق سمع اطلاعات مخابره‌شده بین آلیس و باب را دارد نیز می‌تواند دارای یک یا دو آنتن باشد. یک فرض اساسی در مورد ایو این است که یک دشمن غیر فعال بوده و فقط قادر به شنود اطلاعات است نه تغییر و جعل اطلاعات. در پروتکل تولید کلید پیشنهادی برای انتقال سیگنال‌های راهنما بین گره‌ها از تقسیم زمانی استفاده شده و هر گره اطلاعات فاز کانال را تخمین زده و سپس مطابق با یک روش کوانتیزاسیون پیش‌فرض به بردارهای بیتی تبدیل می‌کند. علاوه بر این در این سیستم چندورودی- چندخروجی (MIMO) فرض می‌شود که برای تولید کلید در هر بازه زمانی که سیگنال راهنما به منظور تست کانال ارسال و دوباره دریافت می‌گردد، کانال ثابت بوده و از زمان همدوسی کانال تجاوز نکند. با توجه به فرضیات فوق، شرح پروتکل تولید کلید محرمانه مشترک در ادامه آمده است.

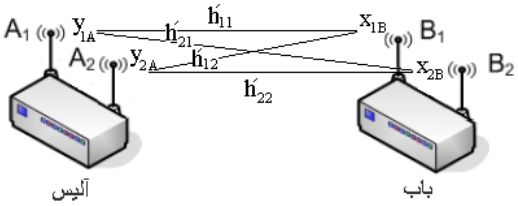
## ۳- پروتکل تولید کلید

### ۳-۱ تست کانال

در شکل ۱ به طور خلاصه مراحل پروتکل تولید کلید محرمانه مشترک پیشنهادی برای حالت ۲ آنتن فرستنده و ۲ آنتن گیرنده نشان داده شده است. برای اجرای هر دور از پروتکل تولید کلید، آلیس دو سیگنال راهنما جهت تست کانال به باب می‌فرستد و باب پس از دریافت سیگنال‌های ارسالی از طرف آلیس، فازهای سیگنال‌ها را تخمین زده و ثبت می‌کند. سپس مشابه همین کار را نیز باب انجام می‌دهد. به عبارت دیگر باب دو




(الف)




(ب)

شکل ۲: مدل سیستم، (الف) در بازه زمانی اول و (ب) در بازه زمانی دوم.

سیگنال راهنما جهت تست کانال به آلیس ارسال می‌کند و آلیس نیز فازهای سیگنال‌های دریافتی خود را تخمین زده و ثبت می‌کند. برای تولید یک کلید به طول خاص، نیاز به اجرای پروتکل در چندین دور می‌باشد و برای هر دور تولید کلید، دو بازه زمانی در نظر گرفته می‌شود به طوری که جمع این دو بازه زمانی از زمان همدوسی کانال تجاوز نکند. در اینجا بازه زمانی بدین صورت تعریف می‌شود: مدت زمانی که طول می‌کشد هر یک از طرفین، سیگنال‌هایی را جهت تست کانال به طرف مقابل ارسال کند و طرف مقابل نیز تخمین فاز انجام داده و مقادیر را ثبت کند.

در بازه زمانی اول، آلیس دو سیگنال تک‌فرکانس به طول $T_o$ را به عنوان سیگنال‌های راهنما برای تست کانال از طریق آنتن‌های $A_1$ و $A_2$ به ترتیب به صورت سیگنال‌های $x_{1A}(t)$ و $x_{2A}(t)$ به باب ارسال می‌کند به طوری که

$$x_{1A}(t)=e^{j(\omega_1(t-t_1)+\varphi_{1A})}$$
$$x_{2A}(t)=e^{j(\omega_2(t-t_1)+\varphi_{2A})} \qquad (۱)$$

که $t\in[t_1,t_1+T_o)$ بوده و $t_1$ زمان شروع ارسال سیگنال‌های راهنما می‌باشد که می‌توان برای سادگی $t_1=0$ را فرض کرد. $\varphi_{1A}$ و $\varphi_{2A}$ فازهای اولیه انتخابی است که توسط آلیس به صورت یکنواخت و تصادفی از فاصله $[0,2\pi)$ انتخاب شده‌اند و $\omega_1$ و $\omega_2$ فرکانس‌های حامل برای ارسال سیگنال‌ها روی هر آنتن می‌باشد. مدل سیستم در بازه زمانی اول (حالت رفت) در شکل ۲- الف آمده و مطابق شکل، سیگنال‌های دریافتی توسط باب از آنتن‌های $B_1$ و $B_2$ را به ترتیب $y_{1B}(t)$ و $y_{2B}(t)$ نامیده و به صورت زیر نوشته می‌شوند

$$\begin{bmatrix} y_{1B}(t)\\ y_{2B}(t)\end{bmatrix}=\begin{bmatrix} h_{11} & h_{12}\\ h_{21} & h_{22}\end{bmatrix}\begin{bmatrix} x_{1A}(t)\\ x_{2A}(t)\end{bmatrix}+\begin{bmatrix} n_1(t)\\ n_2(t)\end{bmatrix} \qquad (۲)$$

که در آن $n_1(t)$ و $n_2(t)$ معادل نویز گوسی جمع‌شونده با میانگین صفر و واریانس $\sigma^2$ می‌باشند. $h_{mn}(m,n=1,2)$ پاسخ ضربه مختلط فیدینگ کانال‌های چندمسیره از آلیس به باب هستند. اگر $\tau_{mn}$ معادل تأخیر کوتاه‌ترین مسیر در کانال $h_{mn}$ و $T_{d_{mn}}$ معادل گستره تأخیر کانال $h_{mn}$ در نظر گرفته شود، به منظور رسیدن به پاسخ حالت دائم، بایستی طول سیگنال‌های راهنما از گستره تأخیر هر کانال بیشتر باشد، یعنی $T_o>\max_{m,n=1,2} T_{d_{mn}}$. حال به جای $h_{mn}$ در (۲) قرار داده می‌شود $h_{mn}=r_{mn}e^{j\theta_{mn}}$ که $r_{mn}$ معادل اندازه ضریب کانال $h_{mn}$ با توزیع رایلی و $\theta_{mn}$ نشان‌دهنده فاز کانال $h_{mn}$ با توزیع یکنواخت بین $[0,2\pi]$ می‌باشد. بنابراین باب پس از زمانی مطلوب که پاسخ‌ها به حالت پایدار خود برسند، سیگنال‌های زیر را دریافت می‌کند

$$y_{1B}(t)=r_{11}e^{j(\omega_1 t+\varphi_{1A}+\theta_{11})}+r_{12}e^{j(\omega_2 t+\varphi_{2A}+\theta_{12})}+n_1(t) \qquad (۳)$$

$$y_{2B}(t)=r_{21}e^{j(\omega_1 t+\varphi_{1A}+\theta_{21})}+r_{22}e^{j(\omega_2 t+\varphi_{2A}+\theta_{22})}+n_2(t) \qquad (۴)$$

باب پس از دریافت سیگنال‌های $y_{1B}(t)$ و $y_{2B}(t)$ با استفاده از تخمین‌گر ML [۱۳]، فرکانس‌ها و فازهای سیگنال‌های مشاهده‌شده را تخمین زده و ثبت می‌کند. نحوه کوانتیزاسیون این مقادیر ثبت‌شده در بخش ۳-۲ توضیح داده خواهد شد.

در بازه زمانی دوم، باب سیگنال‌های تک‌فرکانس راهنمای $x_{1B}(t)$ و $x_{2B}(t)$ به طول $T_o$ را تولید کرده و از طریق آنتن‌های $B_1$ و $B_2$ به آلیس ارسال می‌کند به طوری که

$$x_{1B}(t)=e^{j(\omega_1(t-t_2)+\varphi_{1B})}$$
$$x_{2B}(t)=e^{j(\omega_2(t-t_2)+\varphi_{2B})} \qquad (۵)$$

که $t\in[t_2,t_2+T_o)$ بوده و $t_2$ زمان شروع ارسال سیگنال‌های راهنما در بازه زمانی دوم می‌باشد که بلافاصله پس از دریافت سیگنال‌ها در بازه زمانی اول است. $\varphi_{1B}$ و $\varphi_{2B}$ فازهای انتخابی باب هستند که به طور تصادفی و یکنواخت از فاصله $[0,2\pi)$ انتخاب می‌شوند. فرکانس‌های $\omega_1$ و $\omega_2$ در در دو بازه زمانی یکسان می‌باشند. مدل سیستم در بازه زمانی دوم (حالت برگشت) در شکل ۲- ب نشان داده شده و مطابق شکل، سیگنال‌های دریافتی توسط آلیس از آنتن‌های $A_1$ و $A_2$ را به ترتیب $y_{1A}(t)$ و $y_{2A}(t)$ نامیده و به صورت زیر می‌توان بیان نمود

$$\begin{bmatrix} y_{1A}(t)\\ y_{2A}(t)\end{bmatrix}=\begin{bmatrix} h'_{11} & h'_{12}\\ h'_{21} & h'_{22}\end{bmatrix}\begin{bmatrix} x_{1B}(t)\\ x_{2B}(t)\end{bmatrix}+\begin{bmatrix} n'_1(t)\\ n'_2(t)\end{bmatrix} \qquad (۶)$$

که در آن $n'_1(t)$ و $n'_2(t)$ معادل نویز گوسی جمع‌شونده با میانگین صفر و واریانس $\sigma^2$ می‌باشند و $h'_{mn}(m,n=1,2)$ پاسخ ضربه مختلط فیدینگ کانال‌های چندمسیره از باب به آلیس هستند. اگر $\tau'_{mn}$ معادل تأخیر کوتاه‌ترین مسیر در کانال $h'_{mn}$ و $T'_{d_{mn}}$ معادل گستره تأخیر کانال $h'_{mn}$ در نظر گرفته شود، به منظور رسیدن به پاسخ حالت دایم بایستی طول سیگنال‌های راهنما از گستره تأخیر هر کانال بیشتر باشد، یعنی $T_o>\max_{m,n=1,2} T'_{d_{mn}}$. حال به جای $h'_{mn}$ در (۶) قرار داده می‌شود $h'_{mn}=r'_{mn}e^{j\theta'_{mn}}$ که $r'_{mn}$ معادل اندازه ضریب کانال $h'_{mn}$ با توزیع رایلی و $\theta'_{mn}$ نشان‌دهنده فاز کانال $h'_{mn}$ با توزیع یکنواخت بین $[0,2\pi)$ است. بنابراین آلیس پس از زمانی مطلوب که پاسخ‌ها به حالت پایدار خود برسند، سیگنال‌های زیر را دریافت می‌کند

$$y_{1A}(t)=r'_{11}e^{j(\omega_1 t+\varphi_{1B}+\theta'_{11})}+r'_{12}e^{j(\omega_2 t+\varphi_{2B}+\theta'_{12})}+n'_1(t) \qquad (۷)$$

$$y_{2A}(t)=r'_{21}e^{j(\omega_1 t+\varphi_{1B}+\theta'_{21})}+r'_{22}e^{j(\omega_2 t+\varphi_{2B}+\theta'_{22})}+n'_2(t) \qquad (۸)$$

با فرض این که فاصله بین بازه زمانی اول و دوم از زمان همدوسی کانال کمتر باشد یعنی $TS_1+TS_2<\min_{m,n=1,2} T_{c_{mn}}$ که $T_{c_{mn}}$ زمان همدوسی کانال $h_{mn}$ و $TS_1$ و $TS_2$ به ترتیب طول بازه زمانی اول و دوم است، طبق اصل هم‌پاسخی کانال‌ها خواهیم داشت $h_{mn}\approx h'_{mn}$ و $T_{d_{mn}}\approx T'_{d_{mn}}$. بنابراین (۷) و (۸) به صورت زیر می‌توانند بیان شوند

$$y_{1A}(t)=r_{11}e^{j(\omega_1 t+\varphi_{1B}+\theta_{11})}+r_{21}e^{j(\omega_2 t+\varphi_{2B}+\theta_{21})}+n'_1(t) \qquad (۹)$$

$$y_{2A}(t)=r_{12}e^{j(\omega_1 t+\varphi_{1B}+\theta_{12})}+r_{22}e^{j(\omega_2 t+\varphi_{2B}+\theta_{22})}+n'_2(t) \qquad (۱۰)$$

آلیس پس از دریافت سیگنال‌های $y_{1A}(t)$ و $y_{2A}(t)$ با استفاده از تخمین‌گر ML [۱۳]، فرکانس‌ها و فازهای سیگنال‌های مشاهده‌شده را تخمین زده و ثبت می‌کند.

## ۳-۲ کوانتیزه‌کردن فازها

در پایان دور اول الگوریتم تولید کلید، آلیس از مشاهده $y_{1A}(t)$ و $y_{2A}(t)$ به ترتیب فازهای $\hat{\varphi}_{1A}$، $\hat{\varphi}_{2A}$ و $\hat{\varphi}_{3A}$، $\hat{\varphi}_{4A}$ و باب نیز از مشاهده $y_{1B}(t)$ و $y_{2B}(t)$ به ترتیب فازهای $\hat{\varphi}_{1B}$، $\hat{\varphi}_{2B}$ و $\hat{\varphi}_{3B}$، $\hat{\varphi}_{4B}$ را تخمین و ثبت می‌کند به طوری که

$$\begin{pmatrix}\hat{\varphi}_{1A}\approx\varphi_{1B}+\theta_{11}\\ \hat{\varphi}_{2A}\approx\varphi_{2B}+\theta_{12}\\ \hat{\varphi}_{3A}\approx\varphi_{1B}+\theta_{13}\\ \hat{\varphi}_{4A}\approx\varphi_{2B}+\theta_{14}\end{pmatrix},\quad \begin{pmatrix}\hat{\varphi}_{1B}\approx\varphi_{1A}+\theta_{11}\\ \hat{\varphi}_{2B}\approx\varphi_{2A}+\theta_{21}\\ \hat{\varphi}_{3B}\approx\varphi_{1A}+\theta_{31}\\ \hat{\varphi}_{4B}\approx\varphi_{2A}+\theta_{32}\end{pmatrix} \qquad (۱۱)$$

سپس آلیس و باب طبق الگوریتم زیر با اضافه‌کردن فازهای انتخابی خود به فازهای تخمینی، اندازه‌هایی را به دست می‌آورند که آماده برای کوانتیزه‌شدن می‌باشند

$$\begin{aligned}&\Phi^r_{1A}=(\hat{\varphi}_{1A}+\varphi_{1A})\bmod 2\pi\\ &\Phi^r_{2A}=(\hat{\varphi}_{2A}+\varphi_{1A})\bmod 2\pi\\ &\Phi^r_{3A}=(\hat{\varphi}_{3A}+\varphi_{2A})\bmod 2\pi\\ &\Phi^r_{4A}=(\hat{\varphi}_{4A}+\varphi_{2A})\bmod 2\pi\end{aligned} \qquad \text{برای آلیس:} \qquad (۱۲)$$

$$\begin{aligned}&\Phi^r_{1B}=(\hat{\varphi}_{1B}+\varphi_{B})\bmod 2\pi\\ &\Phi^r_{2B}=(\hat{\varphi}_{2B}+\varphi_{1B})\bmod 2\pi\\ &\Phi^r_{3B}=(\hat{\varphi}_{3B}+\varphi_{2B})\bmod 2\pi\\ &\Phi^r_{4B}=(\hat{\varphi}_{4B}+\varphi_{2B})\bmod 2\pi\end{aligned} \qquad \text{برای باب:} \qquad (۱۳)$$

که در آن $\Phi^r_{iP}$ نشان‌دهنده فاز $i$ام قبل از کوانتیزه‌شدن توسط گره $P$ $(P\in\{A,B\})$ در دور $r$ام می‌باشد. حال با استفاده از رابطه کوانتیزاسیون (۱۴)، فازهای (۱۲) و (۱۳) را کوانتیزه کرده و حاصل شاخص کوانتیزاسیون نامیده می‌شود

```
for i = 0,1,...,q-1
    if x ∈ [2πi/q, 2π(i+1)/q)
        Q(x) = i
    end
end
```
(۱۴)

که در آن $q$ بیانگر تعداد سطوح کوانتیزاسیون می‌باشد. برای استخراج بیت‌های کلید محرمانه مشترک با استفاده از کد گری[1] (معرف یک بیت اختلاف بین نواحی مجاور می‌باشد و برای کاهش در تعداد بیت‌های خطا به کار برده می‌شود) هر نمونه در ابتدا به $\log_2 q$ بیت تبدیل شده و سپس هر کدام از دنباله‌های بیتی به دست آمده را پشت سر هم قرار داده تا یک دنباله بیتی به اندازه $N_T\times N_R\times\log_2 q$ حاصل شود که در اینجا $N_T=N_R=2$ می‌باشد. در پایان هر دور آلیس $K^r_A=[k_1\ k_2\ k_3\ k_4]^T$ و باب $K^r_B=[k'_1 k'_2 k'_3 k'_4]^T$ را به دست خواهند آورد که $k_j$ها و $k'_j$ها $(j=1,\ldots,4)$ بردارهای بیتی حاصل از کوانتیزه‌کردن هر یک از فازهای ثبت‌شده در (۱۲) و (۱۳) می‌باشند. برای آن که باب بتواند به دنباله کلیدی مشابه دنباله کلید آلیس دست یابد، لازم است طبق الگوریتم زیر ترتیب پشت سر هم قرار گرفتن $k'_j$ها را تعیین کند

```
j_0 = 1
for n = 1 to N_r N_t - 1
    j_n = j_{n-1} + N_r
    if j_n > N_r N_t
        j_n = (j_{n-1} + N_r) mod (N_r N_t - 1)
    end
end
```
(۱۵)

باب پس از تعیین جایگاه هر دنباله کلید به دست آمده با استفاده از الگوریتم فوق، آنها را در $K^r_B$ قبلی جایگزین می‌کند و بنابراین در پایان هر دور، آلیس و باب دنباله‌ای از بیت‌های محرمانه مشترک به اندازه $4\times\log_2 q$ بیت را تولید کرده‌اند که البته این نتیجه خود بیانگر افزایش نرخ تولید کلید ۴ برابر بیشتر از یک سیستم تک‌آنتنه است. در [۹]، Wang و همکاران مشابه این کار را برای یک سیستم تک‌آنتنه اجرا کرده‌اند و نتایج نشان می‌دهد که نرخ تولید کلید ارائه‌شده در این مقاله ۴ برابر نرخی است که در [۹] به آن رسیده‌اند. در [۸] نویسندگان از یک سیستم فرستنده و گیرنده با سه آنتن استفاده کرده‌اند و توانسته‌اند به نرخ تولید کلید ۴برابری یک سیستم تک‌آنتنه دست یابند. این در حالی است که با استفاده از الگوریتم ارائه‌شده در این مقاله با یک سیستم MIMO $(3\times3)$ می‌توان به نرخ تولید کلید ۹برابری یک سیستم SISO دست یافت.

در آخر جهت تولید یک کلید به اندازه $|K|$، آلیس و باب هر کدام دنباله‌های به دست آمده از هر دور اجرای الگوریتم را به صورت متوالی قرار داده و بدین ترتیب کلید محرمانه و مشترک خود را تولید می‌کنند

$$K_A=[K_A^{1^T}\quad K_A^{2^T}\quad\ldots\quad K_A^{r^T}\quad\ldots\quad K_A^{R^T}]^T \qquad \text{آلیس:} \qquad (۱۶)$$

$$K_B=[K_B^{1^T}\quad K_B^{2^T}\quad\ldots\quad K_B^{r^T}\quad\ldots\quad K_B^{R^T}]^T \qquad \text{باب:} \qquad (۱۷)$$

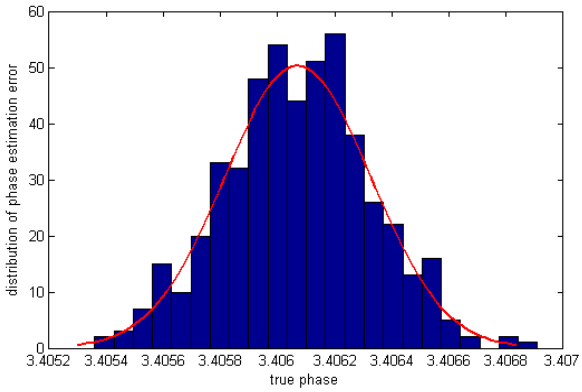
که در آن $R=|K|/(4\times\log_2 q)$ بیانگر تعداد دورهای لازم اجرای الگوریتم تولید کلید برای تولید کلیدی به اندازه $|K|$ می‌باشد. برای مثال برای رسیدن به کلیدی به اندازه $|K|=128$ بیت و با فرض این که تعداد سطوح کوانتیزاسیون $q=16$ باشد، تعداد دورهای اجرای الگوریتم $R=|K|/(4\times\log_2 q)=8$ دور می‌باشد و این در صورتی است که در حالت تک‌آنتنه به ۳۲ دور اجرای الگوریتم نیاز می‌باشد [۹].

## ۳-۳ تطبیق کلید رمز و تقویت محرمانگی

مطابق با اصل هم‌پاسخی، کلیدهای تولیدشده توسط آلیس و باب بایستی از نظر تئوری یکسان باشند اما این امکان وجود دارد که تعداد کمی از بیت‌ها به دلیل تأثیر نویز در تخمین فاز و تداخل و تغییرات سخت‌افزاری، یکسان و همانند نباشند. با توجه به راهکارهای نویسندگان برخی طرح‌های پیشین مانند [۹] و [۱۰] می‌توان برای تطبیق کلیدهای تولیدشده از یک الگوریتم رمزنگاری ساده که در ذیل تشریح می‌گردد، استفاده کرد.

فرض کنید دو گره $A$ و $B$ به ترتیب کلیدهای محرمانه $K$ و $K'$ را تولید کرده باشند و داشته باشیم $\mathrm{dis}(K,K')\le t$ که در اینجا $\mathrm{dis}(K,K')$ بیانگر تعداد مکان‌هایی است که $K$ و $K'$ با یکدیگر اختلاف دارند (فاصله همینگ). پیرو ساختار کد پیشنهادشده در [۱۰]، در اینجا نیز از یک کد تصحیح خطای $C[n,k,2t+1]_2$ برای تصحیح

1. Gray Code




شکل ۳: توزیع خطای تخمین ML فاز حول فاز صحیح در یک ناحیه کوانتیزاسیون.

خطاهای موجود در $K'$ استفاده می‌شود. بدین صورت که ابتدا گره $A$ به صورت تصادفی یک کلمه کد $c$ را از کد تصحیح خطای $C$ انتخاب کرده و عملیات $s = K \oplus c$ را انجام می‌دهد. سپس $s$ را از طریق کانال عمومی به گره $B$ ارسال می‌کند. گره $B$ به محض دریافت $s$، $c'$ را به صورت $c' = K' \oplus s$ محاسبه کرده و سپس با استفاده از کد بردار، $c$ را به دست می‌آورد. پس از به دست آوردن کلمه کد $c$، گره $B$ با انجام عملیات $K = c \oplus s$ به $K$ دست پیدا می‌کند. به عنوان مثال، فرض کنید که $|K| = ۷$ بیت باشد و $\mathrm{dis}(K, K') = ۱$ بیت باشد. در این مثال گره‌های $A$ و $B$ می‌توانند یک کد $BCH\_[۷,۴,۳]_۲$ را جهت تصحیح بیت‌های خطا به کار گیرند.

## ٤- احتمال توافق کلید

در پروتکل تولید کلید پیشنهادی، هر گره در هر دور، دو فاز تصادفی اولیه تولید کرده و چهار فاز از دو سیگنال مشاهده‌شده دریافتی را تخمین می‌زنند. در اینجا خطاهای تخمین فاز را به صورت زیر تعریف می‌کنیم: $\tilde{\varphi}_{jA} \triangleq \hat{\varphi}_{jA} - \varphi_{jA}$ و $\tilde{\varphi}_{jB} \triangleq \hat{\varphi}_{jB} - \varphi_{jB}$ برای $j = ۱,۲,۳,۴$. برای سادگی تحلیل فرض می‌گردد تخمین فاز در هر یک از گره‌ها از نوع بدون بایاس هستند. توجه داشته باشید که همه مشاهدات در بازه‌های زمانی مختلف و یا در گره‌های مختلف، تحت تأثیر نویزهای مستقل تحقق یافته‌اند. زمانی که تعداد نمونه‌ها در یک مشاهده زیاد باشد، خطاهای تخمین به متغیر تصادفی گوسی با متوسط صفر و واریانس $\sigma^۲_{\phi j}$، میل می‌کنند که واریانس‌های خطاهای تخمین فاز می‌توانند با استفاده از کران CRB[1]، کران‌دار شوند [۱۴].

حال برای به دست آوردن احتمال توافق کلید، $P_{QIA}$ را به عنوان احتمال این که هر دو گره در یک دور، شاخص کوانتیزاسیون یکسانی را تولید کرده باشند در نظر بگیرید. به عبارت دیگر $P_{QIA}$ احتمال توافق در شاخص کوانتیزاسیون (QIA)[2] می‌باشد. در دور $r$ام، فازهای $(\Phi^r_{۴A}, \Phi^r_{۳A}, \Phi^r_{۲A}, \Phi^r_{۱A})$ و $(\Phi^r_{۴B}, \Phi^r_{۳B}, \Phi^r_{۲B}, \Phi^r_{۱B})$ به سطح $q$ کوانتیزه می‌شوند و در نتیجه $۴\times\log_۲(q)$ بیت به دست می‌آید. بنابراین برای یک کلید مطلوب با اندازه $|K|$، احتمال این که هر دو گره کلید یکسانی را تولید کنند برابر است با حاصل‌ضرب احتمال توافق در شاخص کوانتیزاسیون هر جفت فاز متناظر به دست آمده در هر دور، به توان تعداد دورها که به صورت زیر داده می‌شود

$$p_{key} = \left(\prod_{j=۱}^{۴} P_{QIA_j}\right)^{\frac{|K|}{۴\log_۲(q)}} \qquad (۱۸)$$

که $P_{QIA_j}$ به ازای $j = ۱,\ldots,۴$ برابر با احتمال توافق در شاخص کوانتیزاسیون برای هر جفت فاز متناظر می‌باشد که می‌توان نشان داد به صورت زیر محاسبه می‌شود

$$P_{QIAj} = \int_{\frac{۲\pi i}{q}}^{\frac{۲\pi(i+۱)}{q}} P_i^۲(\phi_j)\frac{q}{۲\pi}\mathrm{d}\phi_j \quad , \quad j = ۱,۲,۳,۴ \qquad (۱۹)$$

که

$$P_i(\phi_j) = \int_{\frac{۲\pi i}{q}}^{\frac{۲\pi(i+۱)}{q}} \frac{۱}{\sqrt{۲\pi}\sigma_{\phi j}} e^{-\frac{(x-\phi_j)^۲}{۲\sigma^۲_{\phi j}}}\,\mathrm{d}x \qquad (۲۰)$$

که در آن $\sigma^۲_{\phi j}$ واریانس خطای تخمین فاز $j$ام می‌باشد و $j = ۱,\ldots,۴$.

اثبات: برای سادگی تحلیل فازهایی را تحت عنوان مقادیر صحیح فاز بدون خطای تخمین تعریف می‌کنیم $\phi_۱ \triangleq \theta_{۱۱} + \varphi_{۱A} + \varphi_{۱B}$، $\phi_۲ \triangleq \theta_{۱۲} + \varphi_{۲A} + \varphi_{۱B}$، $\phi_۳ \triangleq \theta_{۲۱} + \varphi_{۱A} + \varphi_{۲B}$ و $\phi_۴ \triangleq \theta_{۲۲} + \varphi_{۲A} + \varphi_{۲B}$. همان طور که قبلاً ذکر شد، در پروتکل پیشنهادی $\varphi_{۱A}$، $\varphi_{۲A}$ و $\varphi_{۱B}$، $\varphi_{۲B}$ به صورت تصادفی و یکنواخت روی فاصله $[۰,۲\pi]$ انتخاب می‌شوند و فاز کانال‌ها، $\theta_{۱۱}$، $\theta_{۱۲}$، $\theta_{۲۱}$ و $\theta_{۲۲}$ نیز روی فاصله $[۰,۲\pi]$ توزیع یکنواخت خواهند داشت. بر اساس قضیه اثبات‌شده در [۹]، توزیع مقادیر صحیح، $\phi_j$ها به صورت یکنواخت روی فاصله $[۰,۲\pi]$ می‌باشد. حال فرض کنید $\phi_j$ در سطح $i$ام کوانتیزاسیون قرار بگیرد یعنی در فاصله $(i = ۰,۱,\ldots,q-۱)$ , $[۲\pi i/q, ۲\pi(i+۱)/q)$. از آنجایی که خطاهای تخمین فاز مطابق با کران CRB گوسی و مستقل می‌باشند، احتمال این که $\hat{\phi}_j$ در سطح $[۲\pi i'/q, ۲\pi(i'+۱)/q)$ قرار بگیرد برابر است با

$$P_{i'}(\phi_j) = \int_{\frac{۲\pi i'}{q}}^{\frac{۲\pi(i'+۱)}{q}} \frac{۱}{\sqrt{۲\pi}\sigma_{\phi_j}} e^{-\frac{(x-\phi_j)^۲}{۲\sigma^۲_{\phi j}}}\,\mathrm{d}x \qquad (۲۱)$$

که در آن $i' \in \{۰,۱,\ldots,q-۱\}$. بنابراین $P_{QIAj}$ می‌تواند به صورت $P_{QIAj}(\phi_j) = \sum_{i'=۰}^{q-۱} P_{i'}(\phi_j)^۲$ محاسبه شود. شبیه‌سازی‌های صورت‌گرفته نشان می‌دهند که واریانس خطاهای تخمین فاز خیلی کوچک‌تر از یک می‌باشند و بنابراین برای $\phi_j \in [۲\pi i/q, ۲\pi(i+۱)/q)$، $P_{QIAj}(\phi_j)$ اساساً با $P_i(\phi_j)(i = i')$ تعیین می‌شود. در نتیجه متوسط احتمال توافق در شاخص کوانتیزاسیون برابر می‌شود با

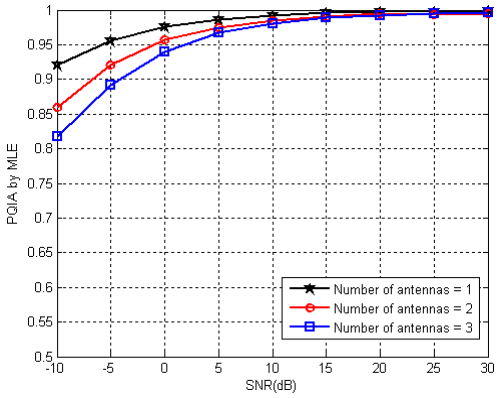
$$P_{QIAj}(\phi_j) = \int_{\frac{۲\pi i}{q}}^{\frac{۲\pi(i+۱)}{q}} P_i^۲(\phi_j)\frac{q}{۲\pi}\mathrm{d}\phi_j \qquad \blacksquare \qquad (۲۲)$$

همان طور که گفته شد، توزیع خطای تخمین فاز وقتی که تعداد نمونه‌ها زیاد باشد به توزیع گوسی میل می‌کند و گوسی شکل بودن توزیع خطای تخمین فاز حول فاز صحیح در شکل ۳ به خوبی قابل مشاهده است.

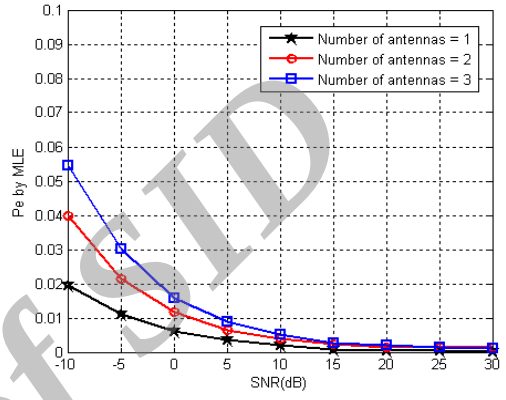
## ٥- تحلیل امنیت

امنیت و محرمانگی پروتکل پیشنهادشده در این مقاله با فرض ناهمبستگی مکانی ضمانت می‌شود و به عبارت دیگر بر اساس تئوری

1. Cramer - Rao
2. Quantization Index Agreement Probability




شکل ۴: $P_{QIA}$ بر حسب SNR برای حالت‌های SISO و MIMO.



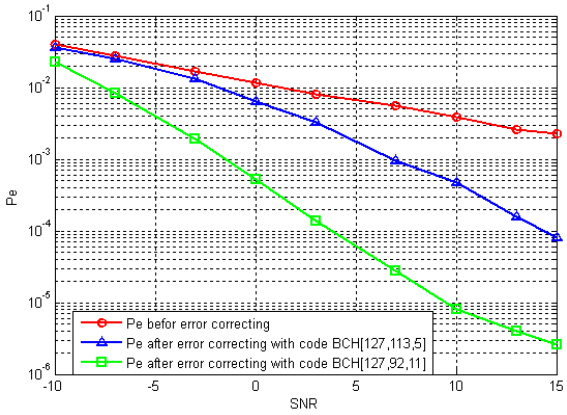

شکل ۵: $P_e$ بر حسب SNR برای حالت‌های SISO و MIMO.

مخابرات بی‌سیم، هر وسیله‌ای که به فاصله حداقل $\lambda/2$ ($\lambda$ طول موج می‌باشد) از گره‌های مجاز در حال ارتباط دورتر باشد، کانال فیدینگ متفاوتی را نسبت به گره‌های مجاز تجربه خواهد کرد که از نظر آماری نیز مستقل می‌باشد. این یک فرض مشترک بین همه پروتکل‌های تولید کلید با استفاده از مشخصات کانال‌های بی‌سیم مانند [۲]، [۳]، [۶] و [۹] است که از طریق آزمایشات واقعی نیز اثبات شده است.

## ۶- نتایج شبیه‌سازی

در این بخش نتایج شبیه‌سازی‌های انجام‌شده روی پروتکل تولید کلید بر اساس فاز سیگنال دریافتی تحت کانال‌های چندمسیره در یک سیستم MIMO ارائه می‌شود. فرض شده که فرکانس سیگنال‌های راهنمای اولیه، $f_{c1}=850\text{MHz}$ و $f_{c2}=900\text{MHz}$ و پارامترهای طول سیگنال‌های راهنما و تعداد سطوح کوانتیزاسیون به ترتیب $T_o=10\mu\text{s}$ و $q=16$ باشند. نتایج شبیه‌سازی $P_{QIA}$ و $P_e$ بر حسب SNR و برای سیستم‌هایی که دارای $N_T=N_R=1,2,3$ هستند به ترتیب در شکل ۴ و ۵ رسم شده است.

همان طور که در شکل ۴ پیداست، احتمال موفقیت در تولید کلید مشترک در SNR های پایین نیز مقدار بالایی بوده و به ترتیب هر چه تعداد آنتن‌ها افزایش پیدا می‌کند، احتمال توافق کلید کمتر می‌شود زیرا تخمین فاز از یک سیگنال تک‌فرکانس با خطای کمتری نسبت به تخمین فاز از یک سیگنال چندفرکانس به دست می‌آید [۱۴]. به علاوه احتمال توافق کلید در حالت MIMO به احتمال توافق در شاخص کوانتیزاسیون هر جفت فازهای متناظر بستگی دارد و بنا به دلایل بالا احتمال توافق کلید کاسته می‌شود. اما این نکته لازم به ذکر است که ۴ تا ۹ برابر افزایش نرخ تولید کلید در حالت MIMO به کاهش ۵ تا ۱۰ درصدی احتمال توافق کلید ارزش دارد.




شکل ۶: احتمال خطای بیت یک کلید ۱۲۸بیتی در سه حالت بدون تصحیح خطا، تصحیح خطا با کد $BCH$[۱۲۷,۱۱۳,۵] و تصحیح خطا با کد $BCH$[۱۲۷,۹۲,۱۱].

در شکل ۵ نرخ خطای بیت (BER) برای حالت کدنشده یک کلید با اندازه $|K|=144\,\text{bit}$ برای سیستم‌هایی که دارای $N_T=N_R=1,2,3$ هستند رسم شده است. در اینجا BER نسبت بیت‌های خطا به اندازه کلید تعریف شده و نتایج نشان‌دهنده این است که وقتی در شرایط SNR پایین (یعنی زیر ۱۰ dB) باشیم، می‌توان به BER خیلی کوچکی دست یافت. این به خاطر استفاده از کدهای گری است که یک عدم توافق بین شاخص‌های کوانتیزاسیون بین دو ناحیه مجاور، تنها منجر به تولید یک بیت خطا می‌شود. برای این قبیل BER های پایین، کدهای $BCH\_[n,k,2t+1]$ با قابلیت تصحیح حداکثر $t$ خطا برای تصحیح بیت‌های خطا می‌تواند به کار برده شود.

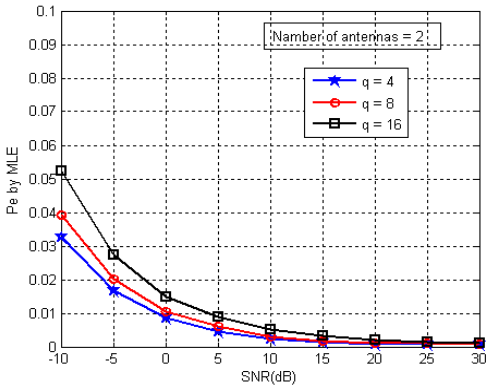
مطابق شکل ۵ در یک SNR ثابت با افزایش تعداد آنتن‌ها برای هر گره، احتمال خطا نیز افزایش پیدا می‌کند و دلایل این افزایش احتمال خطا همان دلایل کاهش احتمال توافق کلید می‌باشد. برای تطبیق بیت‌های خطا مطابق با آنچه در بخش ۳-۳ گفته شد، می‌توان پارامترهای کد تصحیح خطا را با استفاده از شکل ۵ به گونه زیر تعیین کرد:

اندازه کلید، بیانگر پارامتر $n$ یا همان طول کلمه کد می‌باشد. درصد خطای بیت در هر SNR با توجه به شکل ۵ تعیین‌کننده نسبت تصحیح خطای کد یعنی $t/n$ می‌باشد و در نهایت پارامتر $k$ را با توجه به $n$ و $t$ طوری تعیین می‌کنیم که احتمال نشت اطلاعات را در اجرای الگوریتم تطبیق کلید کمتر کند. به طور مثال برای $|K|=128$، $N_T=N_R=2$ و $SNR=5\,\text{dB}$، مطابق شکل ۴ درصد خطای بیت حدود ۰/۰۱ می‌باشد. در نتیجه می‌توان پارامترهای کد تصحیح خطا را به صورت زیر به دست آورد

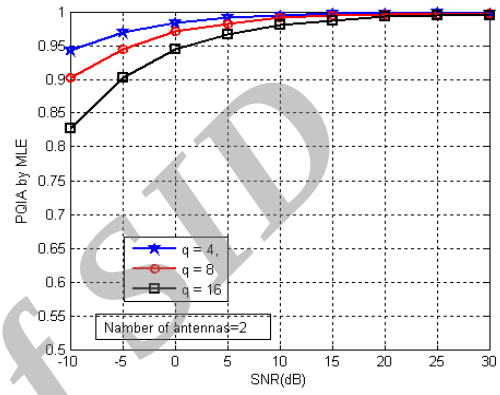
$$n=127\,,\ \frac{t}{n}=0/01\Rightarrow t=1/2\Rightarrow \\ t\approx 2\Rightarrow BCH[127,113,5] \qquad (23)$$

شکل ۶ اثر تصحیح خطا را با استفاده از کدهای تصحیح خطای $BCH$ روی احتمال خطای بیت نشان می‌دهد. جهت رسیدن به نتایج حاصل روی کلیدهای ۱۲۸بیتی به دست آمده از پروتکل تولید کلید روی یک سیستم MIMO (۲×۲)، با $q=16$، عملیات تطبیق کلید با دو کد مختلف با قدرت تصحیح خطای مختلف به کار گرفته شده است.

همچنین در شکل‌های ۷ و ۸ به ترتیب اثر احتمال خطای بیت و احتمال موفقیت کلید برای $|K|=128$ بیت بر حسب SNR در $q$ های مختلف برای MIMO (۲×۲) نشان داده شده است. همان طور که از شکل‌ها پیداست در یک SNR ثابت، احتمال خطای بیت وقتی از سطوح بیشتری برای کوانتیزاسیون استفاده می‌شود، بیشتر است و بالعکس در




شکل ۷: احتمال خطای بیت بر حسب SNR در $q$ های مختلف برای MIMO (۲×۲).




شکل ۸: احتمال توافق کلید بر حسب SNR در $q$ های مختلف برای MIMO (۲×۲).

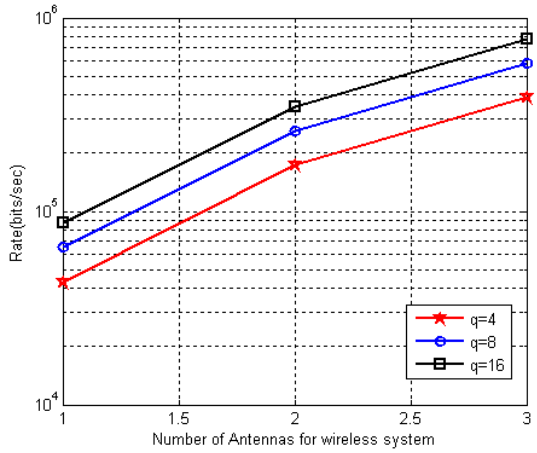
کوانتیزاسیون با سطوح بیشتر، احتمال موفقیت کلید کمتر می‌شود. زیرا هر چه نواحی سطوح کوانتیزاسون کوچک‌تر باشند، در حضور نویز، احتمال جابه‌جا شدن مقدار تخمینی از ناحیه صحیح به نواحی مجاور بیشتر از حالتی است که نواحی کوانتیزاسیون بزرگ‌تر هستند. با این حال هر چند $q$ کوچک‌تر مناسب‌تر به نظر می‌رسد، منتها به تعداد دورهای بیشتری برای رسیدن به یک کلید با اندازه ثابت نیاز دارد.

در شکل ۹ نرخ تولید کلید برای سیستم‌های SISO و MIMO در حالتی که $q$ های مختلف در نظر گرفته شوند نشان داده شده است. این نتیجه حاکی از این حقیقت است هر چند که با کوانتیزاسیون در سطوح بیشتر احتمال توافق کلید کمتر می‌شود اما در عوض نرخ تولید کلید افزایش پیدا می‌کند. در واقع در استفاده‌کردن کوانتیزاسیون در سطوح مختلف، بین احتمال توافق کلید و نرخ تولید کلید یک تعامل وجود دارد.

همان طور که در شکل ۹ آمده است، نرخ تولید کلید در حالت MIMO (۲×۲) تقریباً ۴ برابر نرخ تولید کلید یک سیستم تک‌آنتنه می‌باشد و این مقدار رشد نرخ وقتی که از یک سیستم با ۳ آنتن استفاده شود به ۹ برابر افزایش پیدا می‌کند.

حال به تأثیر حرکت گره‌ها روی پروتکل پیشنهادی می‌پردازیم. در یک سیستم سیار فرض کنید $|K|=۱۲۸$ بیت، $q=۱۶$، $T_o=۱۰۰\mu s$ و بیشترین فاصله بین گره‌ها $d=۱۰۰\,m$ باشد. اگر سرعت حرکت گره را برابر $v(m/s)$ در نظر بگیریم، آن گاه شیفت فرکانس داپلر برابر می‌شود با $f_d=v/\lambda=vf_c/c$ و در نتیجه زمان همدوسی کانال برابر است با $T_c=۰/۴۲۳/f_d=۰/۴۲۳C/vf_c$. برای ضمانت برقراری همپاسخی کانال در طی تولید کلید، بایستی زمان اجرای یک دور از الگوریتم از زمان همدوسی کانال کمتر باشد و به عبارت دیگر

$$۴(T_o+\tau+T_d)<T_c \qquad (۲۴)$$




شکل ۹: نرخ تولید کلید برای $q$ های مختلف در حالت‌های SISO و MIMO.

که $\tau=d/c=۰/۳۳\mu s$ تأخیر زمانی کانال و $T_d=۱/۲\mu s$ گستره تأخیر کانال هستند. بنابراین تا وقتی (۲۴) برای سرعت‌های مختلف (فرکانس داپلرهای مختلف) برقرار باشد، پروتکل تولید کلید به مشکلی برنمی‌خورد زیرا هم‌پاسخی کانال‌ها برقرار خواهد بود و در نتیجه فرستنده و گیرنده هر دو یک داپلر را خواهند دید و هر دو فاز یکسانی را مشاهده کرده و تخمین مشابهی از فاز دریافتی انجام می‌دهند. لذا حرکت فرستنده و گیرنده در این روش مشکلی را در روند تولید کلید به وجود نخواهد آورد زیرا هر دوی فرستنده و گیرنده فاز و فرکانس یکسانی را می‌بینند، خواه این فاز و فرکانسی برابر فاز و فرکانس اصلی باشد یا فاز و فرکانسی باشد که تحت تأثیر داپلر قرار گرفته است. برای مثال فرض کنید $v=۳۰\,m/s$ باشد، آن گاه $f_d=۹۰\,Hz$ و $T_c=۴/۷\,ms$ می‌شوند و این در حالی است که زمان اجرای هر دور حدود ۰/۴ ms طول می‌کشد. لازم به ذکر است شرط فیدینگ تخت در حوزه زمان و فرکانس همچنان برقرار می‌باشد، به عبارت دیگر هم زمان ارسال سیگنال از زمان همدوسی کانال تجاوز نمی‌کند $(T_o<T_c)$ و هم پهنای باند ارسالی از پهنای باند همدوسی کانال کمتر است $(B_s \triangleq ۱/T_o < B_{cb} \triangleq ۱/T_d)$.

## ۷- نتیجه‌گیری

در این مقاله، یک الگوریتم تولید کلید بر مبنای تخمین فاز کانال روی سیستم‌های MIMO با استفاده از اطلاعات فازهای یکنواخت پاسخ‌های کانال و فازهای انتخابی به صورت تصادفی و نیز به کارگیری از کوانتیزاسیون چندسطحی با قابلیت رشد نرخ تولید کلید چندین برابری ارائه شده، به طوری که بر اساس جستجوهای انجام‌شده در مقالات موجود، اگر تولید کلید بر مبنای الگوریتم دیگری غیر از الگوریتم ارائه‌شده صورت گیرد، دیگر نرخ تولید کلید برای یک سیستم MIMO (۲×۲)، ۴ برابر نرخ تولید کلید یک سیستم SISO نخواهد شد. نتایج شبیه‌سازی این رشد نرخ را به خوبی نمایش دادند و به علاوه در مقایسه با روش‌های بر پایه RSS، طرح پیشنهادشده قابلیت پیاده‌سازی روی هر دو محیط ثابت و سیار را دارد.

## مراجع

[1] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. on Information Theory*, vol. 22, no. 6, pp. 644-654, Nov. 1976.

[2] S. Mathur, W. Trappe, N. B. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: extracting a secret key from anunauthenticated wireless channel," in *Prof. ACMMOBICOM Conf.*, Sep. 2008.

[3] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wirelessnetworks," in *Proc.*

*of the 14th ACM Conf. on Computer and Communications Security*, *CCS'07,* pp. 401-410, Nov. 2007.

[4] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless secret key generation exploitingreactance-domain scalar response of multipath fadingchannels," *IEEE Trans. on Antennas and Propagation*, vol. 53, no. 11, pp. 3776-3784, Nov. 2005.

[5] M. G. Madiseh *et al.*, Secret Key extraction in ultra wideband channels for unsynchronized radios, in *Proc. 6th Annual Communication Networks and Services Research Conf, CNSR'08,* pp. 88-95, 5-8 May 2008.

[6] S. Jana, et al., "On the effectiveness of secret key extraction fromwireless signal strength in real environments," in *Proc. Proc. of the 15th Annual Int. Conf. on Mobile Computing and Networking, MOBICOM'09,* pp. 321-332, 2009.

[7] N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-rate uncorrelatedbit extraction for shared secret key generation from channel measurements," *IEEE Trans. on Mobile Computing*, vol. 9, no. 1, pp. 17-30, May 2010.

[8] K. Zeng *et al.*, "Exploiting multiple-antenna diversity for shared secret key generation in wireless networks," in *Proc. INFOCOM'10*, pp. 1837-1845, Mar. 2010.

[9] Q. Wang *et al.*, "Fast and scalable secret key generation exploiting channel phase randomness in wirelesss networks," in *Proc. IEEE INFOCOM'11*, pp. 1422-1430, Apr. 2011.

[10] Y. Dodis *et al.*, "Fuzzy extractors: how to generate strong keys from biometrics and other noisy data," *SIAM J. Comp.*, vol. 38, no. 1, pp. 97-139, 2008.

[11] A. A. Hassan *et al.*, "Cryptographic key agreement for mobile radio," *Digital Signal Processing*, vol. 6, no. 4, pp. 207-212, Oct. 1996.

[12] A. M. Sayeed and A. Perrig, "Secure wireless communications: secret keys through multipath," in *Proc. ICASSP'08*, pp. 321-332, Mar. 2008.

[13] Q. Wang, K. Xu, and K. Ren, "Cooperative secret key generation from phase estimation in narrowband fading channels," *IEEE Trans. on Selected Areas in Communications*, vol. 30, no. 9, pp. 1666-1674, Oct. 2012.

[14] D. C. Rife and R. R. Boorstyn, "Multiple tone parameters estimation from discrete-time observations," *Bell System Technical J.*, vol. 55, no. 9, pp. 1389-1410, Nov. 1976.

**وجیهه زینلی فتح‌آبادی** در سال ۱۳۸۶ مدرک کارشناسی مهندسی برق- مخابرات خود را از دانشگاه شاهد و در سال ۱۳۹۱ مدرک کارشناسی ارشد مهندسی مخابرات- گرایش رمز خود را با رتبه اول از دانشگاه صنعتی مالک اشتر تهران دریافت نمود. زمینه‌های تحقیقاتی مورد علاقه ایشان عبارتند از: رمزنگاری- امنیت سیستم های مخابراتی و MIMO.

**حسین خالقی بیزکی** مدرک دکتری خود را در رشته مهندسی برق گرایش مخابرات سیستم در سال ۱۳۸۶ از دانشگاه علم و صنعت ایران دریافت نمود. نام‌برده مولف بیش از ۳۰ مقاله ژورنال و کنفرانسی می‌باشد. علاقمندی‌های تحقیقاتی ایشان شامل تئوری اطلاعات و کدینگ، مخابرات سیار، سیستم‌های مخابراتی MIMO به ویژه نسل سوم و چهارم مخابرات سیار و دیگر زمینه‌های مرتبط با پردازش سیگنال‌ها و سیستم‌های مخابراتی دیجیتال می‌باشد.

**علی شهزادی** مدرک دکتری خود را در رشته مهندسی برق گرایش مخابرات سیستم در سال ۱۳۸۴ از دانشگاه علم و صنعت ایران دریافت نمود. ایشان هم‌اکنون عضو هیأت علمی گروه مهندسی مخابرات دانشکده مهندسی برق و کامپیوتر دانشگاه سمنان می‌باشد. از زمینه‌های تحقیقاتی مورد علاقه ایشان می‌توان به سیستم‌های رمزنگاری، مخابرات سیار به ویژه نسل سوم و چهارم، رادیو شناختگر و سیستم‌های مخابراتی دیجیتال را نام برد.