



بهره‌گیری از طیف تکانه زاویه مداری در رمزگذاری کانال مخابراتی با استفاده از فراسطح

چکیده

با افزایش روزافزون تقاضا برای انتقال ایمن اطلاعات، نیاز به پیشرفت در تکنیک‌های رمزگذاری ضروری است. تا به حال رمزگذاری‌ها عموماً نرم‌افزاری بوده و روی داده‌های سیگنال انجام می‌شده است؛ اما در این پژوهش قصد داریم به رمزگذار سخت‌افزاری بپردازیم که رمزگذاری روی مشخصات موج انتشاری انجام می‌شود. این مشخصات عبارت‌اند از فاز، دامنه، فرکانس، قطبش و جبهه موج. در این میان جبهه موج OAM به واسطه مودهای مختلف متعامدش می‌تواند در تئوری تا ظرفیت بی‌نهایت را برای ما ایجاد کند به این سبب قدرت رمزگذاری ما را فوق‌العاده افزایش می‌دهد و تا حدود زیادی محدودیت کانال‌های رمزگذاری را برطرف می‌کند. یکی از ادوات پرطرفدار به واسطه شکل‌دهی فوق‌العاده به موج، فراسطح‌ها هستند. فراسطح‌های رمزگذاری موج، رویکردی انقلابی برای محافظت از داده‌ها ارائه می‌دهند که از ویژگی‌های منحصربه‌فرد موج و طراحی نانو ساختار فراسطح‌ها بهره می‌برد. فراسطح‌ها ساختارهای مهندسی شده‌ای با ویژگی‌های زیر طول موج هستند که به روش‌های غیرمتعارف موج را دست‌کاری می‌کنند. در رمزگذاری، این فراسطح‌ها به‌عنوان کلیدهای ایستا و پویا عمل می‌کنند و موج را بر اساس اطلاعاتی که حمل می‌کند، تغییر می‌دهند. این دست‌کاری می‌تواند جبهه موج را به‌طور کلی تغییر دهد. تحقیقات در حال انجام به دنبال رفع محدودیت‌های رمزگذاری مشخصات موج به‌وسیله رمزگذاری الگوریتم است؛ اما این روش طراحی ساختار را هم پیچیده و گاهی حجیم‌تر می‌کند پس به سراغ روش پویا کردن فراسطح رفتیم تا بتوانند مشکل پیچیدگی ساختار را تا حد ممکن حل کنیم؛ در نهایت با ترکیب درجات آزادی موج، رمزگذاری سخت‌افزاری با ابعاد نامحدود طراحی کردیم از طرفی می‌دانیم که تا به امروز تحقیقات گسترده‌ای بر روی رمزگذاری نرم‌افزاری انجام شده است که منجر به پیشرفت‌های چشمگیری را در عرصه رمزگذاری شده است؛ اما در چند سال اخیر با توجه به گسترش تحقیقات بر روی سیستم‌های کوانتومی و پیشرفت کامپیوترهای کوانتومی سرعت محاسبات به‌صورت قابل‌توجهی افزایش یافته است. سیستم‌های توسعه‌یافته امروزی می‌توانند در زمان بسیار کوتاه‌تری رمزگذاری اطلاعات را بشکنند. در این میان روش‌هایی از جمله روش‌های رمزگذاری سخت‌افزاری در ترکیب با روش‌های نرم‌افزاری راه‌حل مناسبی برای غلبه برای این تهدید به نظر می‌رسد. برای اجرای این رویکرد ما با طراحی مناسب این ساختار قابلیت ترکیب شدن با روش نرم‌افزاری را اجرایی کردیم.

در ابعاد جزئی‌تر طراحی، برای جلوگیری از دسترسی افراد غیرمجاز به داده‌ها و ایمن‌سازی ارسال آن از یک ساختار فراسطح ایستا استفاده کردیم؛ اما با مهندسی موج ورودی توانستیم با طراحی این ساختار ایستا مناسب کاربردهای پویا را محقق کنیم. ما با ادغام هم‌زمان رمزگذاری در قطبش و جبهه موج OAM توانستیم این مدل رمزگذاری سخت‌افزاری را پیاده‌سازی کنیم. این رمزگذاری به‌ازای سه کانال مختلف پایه‌گذاری شده است. کانال اول به‌ازای قطبش \times ورودی و قطبش \times خروجی است که برایندهای $l=+1, -1$ در نقطه کانونی تولید می‌شود. در کانال دوم به‌ازای قطبش γ ورودی و قطبش γ خروجی است که برایندهای $l=+2, -2$ در نقطه کانونی قابل‌مشاهده است و در نهایت

کانال سوم به‌ازای قطبش γ ورودی و قطبش \times خروجی یا بلعکس، برایند موده‌های $L=+3, -3$ در نقطه کانونی دیده می‌شود. ما با قراردادن قطبش مایل به‌ازای زاویه‌ای خاص در ورودی ساختار، با یک وزن‌دهی خاص برایند $L=+1, -1$ و $L=+3, -3$ برای قطبش \times در نقطه کانونی خروجی و برایند $L=+2, -2$ و $L=+3, -3$ برای قطبش γ در همان نقطه کانونی خروجی تولید کردیم و سرانجام با کمک‌گرفتن از روش رمزگذاری DRPE یک روش رمزگذاری ترکیبی نرم‌افزاری و سخت‌افزاری را ارائه کردیم.

دانشجو: علی محمد اوبائی

استاد راهنما: دکتر محمد سلیمانی

استاد مشاور: دکتر محمدجواد حاجی احمدی

هیات داوری: دکتر سجاد ملایی؛ دکتر هادی علی اکبریان

تاریخ دفاع: شنبه ۱۴۰۳/۱۲/۴ ساعت: ۱۷

محل: سالن سمینار خوارزمی دانشکده برق