

## تصدیق صحت مبتنی بر توابع غیرهمسان فیزیکی در سیستم‌های ارتباطی زیرآبی

مسعود کاوه<sup>۱</sup>، سید محمدرضا موسوی میرکلایی<sup>۲</sup> و هومان علائیان<sup>۳</sup>

۱- دانشجوی دکتری دانشکده مهندسی برق دانشگاه علم و صنعت ایران

۲- استاد دانشکده مهندسی برق دانشگاه علم و صنعت ایران

۳- دانشجوی کارشناسی دانشکده مهندسی برق دانشگاه علم و صنعت ایران

### چکیده

ویژگی‌های منحصر به فرد و محدودیت‌های موجود در کانال‌های زیرآبی موجب می‌شود تا ارتباطات در این محیط در مقابل حملات بدخواهانه بسیار آسیب‌پذیر باشند. بنابراین موضوع امنیت جز چالش‌های بسیار مهم در سیستم‌های ارتباطی زیرآبی محسوب می‌شود. از طرفی مولفه‌های زیرآبی از لحاظ منابع محاسباتی، ارتباطی و انرژی بسیار محدودند و این موارد در کنار چالش‌های محیطی زیر آب، کار را برای ارائه راه‌کارهای امنیتی مناسب مشکل‌تر می‌سازد. به همین علت استفاده از روش‌های رمزنگاری موجود مانند الگوریتم‌های کلید همگانی به علت سربار مخابراتی و محاسباتی زیاد برای سیستم‌های ارتباطی زیرآبی غیرممکن می‌باشد. این مقاله استفاده از توابع غیرهمسان فیزیکی (PUF) را برای اولین بار در سیستم‌های امنیتی زیرآبی پیشنهاد می‌دهد. در این فناوری با استفاده از ویژگی‌های فیزیکی هر تراشه، کلیدهای منحصر به فرد و قدرتمندی تولید می‌شود که می‌تواند به خوبی تصدیق صحت در سیستم‌های زیرآبی را ارضا نماید. تحلیل‌های امنیتی و عملکردی نشان می‌دهند که روش ارائه شده در این مقاله علاوه بر قدرت مقاومت بسیار بالا در برابر حملات ممکن و ایجاد امنیت بیشتر نسبت به روش‌های موجود، بسیار مناسب محیط زیرآب با همه محدودیت‌هایش بوده و نسبت به روش‌های سنتی رمزنگاری، عملکرد بهینه‌تری را در سه پارامتر مصرف انرژی، سربار مخابراتی و هزینه محاسباتی از خود به جای می‌گذارد.

**کلمات کلیدی:** ارتباطات زیرآبی امن، تصدیق صحت، تهدیدات زیرآبی، فناوری PUF.

### ۱. مقدمه

ارتباطات زیرآبی همواره با چالش‌های بیشتری نسبت به ارتباطات در هوا روبه‌رو بوده است. به دلیل جذب بالای انرژی توسط آب، باید از سیگنال‌های آکوستیکی به جای سیگنال‌های رادیویی یا نوری در زیر آب استفاده نمود که این امر سبب روبرویی با مشکلاتی از قبیل تداخل‌های چندمسیره [۱ و ۲]، پهنای باند بسیار محدود [۳]، تاخیرهای بسیار زیاد [۴]، نرخ خطای بیت بزرگ [۵ و ۶] و محیط بسیار نویزی در زیر آب [۷ و ۸] می‌شود. به دلیل وجود این چالش‌ها و ویژگی‌های منحصر

\* [m\\_mosavi@iust.ac.ir](mailto:m_mosavi@iust.ac.ir)

به فرد، ارتباطات زیرآبی می‌تواند به راحتی در معرض حملات بدخواهانه قرار گیرد. بنابراین در سال‌های اخیر تلاش‌های زیادی در راستای ایجاد ارتباطی امن به دور از انواع مختلفی از حملات ممکن در سیستم‌های زیرآبی صورت گرفته است [۹-۱۱] که از قبیل این سیستم‌ها می‌توان به شبکه‌های سگ‌زیرآبی اشاره نمود [۱۲-۱۶] که چالش‌ها و راه‌کارهای امنیتی در لایه‌های مختلف این شبکه‌ها توسط دانشمندان مورد بررسی قرار گرفته و هنوز هم یک زمینه تحقیقاتی باز می‌باشد [۱۷-۲۱].

سیستمی که در این مقاله مورد بررسی قرار می‌گیرد، شامل تعداد مشخصی از زیرسطحی‌ها شامل AUV<sup>۱</sup> و زیردریایی‌های خودی می‌باشد که گزارش‌های زیرآبی را به یک مرکز فرماندهی سطحی<sup>۲</sup> می‌فرستند. هر یک از AUV‌ها می‌تواند خود اطلاعات زیرآبی را به دست آورده و یا اطلاعات از حسگرهای زیرآبی جمع‌آوری نماید و سپس برای SCC بفرستد. همچنین یک حمله‌گر بیرونی<sup>۳</sup> نیز در سیستم وجود دارد که می‌تواند حمله‌های بازپخش<sup>۴</sup>، حمله ارسال پیام‌های جعلی<sup>۵</sup>، حمله تحلیل پیام<sup>۶</sup> و حمله اصلاح پیام<sup>۷</sup> را انجام دهد. هدف این مقاله ارائه یک روش امن و بهینه با توجه به حمله‌ها و محدودیت‌های موجود در محیط زیر آب می‌باشد. امن به این معنا که روش پیشنهادی در برابر حملات مذکور مقاوم بوده و سه شرط تصدیق صحت، محرمانگی و بی‌عیبی پیام را ارضاء نماید. بهینه نیز به این معنا است که روش‌های امنیتی اضافه شده بر سیستم دارای کمترین میزان سربرابر مخابراتی و کمترین میزان مصرف انرژی و محاسباتی باشند. بنابراین یک روش تصدیق صحت مبتنی بر توابع غیرهمسان فیزیکی<sup>۸</sup> [۲۲-۲۵] در این مقاله ارائه می‌گردد.

با توجه به تصادفی بودن و تغییرات بسیار عمیق در فرآیند تولید تراشه‌ها، هر ترانزیستور در یک مدار مجتمع ویژگی‌های فیزیکی متفاوت و مخصوص به خود را دارد. از آنجایی که این تغییرات در حین فرآیند ساخت، غیرقابل کنترل است، خواص فیزیکی دستگاه، یا به عبارتی همان اثر انگشت آن تراشه، نه قابل کپی‌برداری و نه قابل همسان‌سازی است. اثر انگشت الکترونیکی برای تولید یک کلید رمزنگاری امن و قابل اطمینان مخصوص همان تراشه (به صورت یکتا) به کار رفته و نیاز به ذخیره‌سازی هر نوع کلید حساس در حافظه غیرقابل انعطاف<sup>۹</sup> را از بین می‌برد. کلید تولید شده در روش PUF غیرقابل مشاهده برای مهاجمان بوده و در هر دستگاه منحصر به فرد است و می‌تواند برای تأیید اعتبار و تصدیق صحت تراشه، اطلاعات تراشه، دستگاه و حتی کل سیستم قابل استفاده باشد.

میزان بهینه بودن این روش در سه پارامتر مصرف انرژی، سربرابر مخابراتی و هزینه‌های محاسباتی با روش RSA<sup>۱۰</sup> مورد مقایسه قرار می‌گیرد. تحلیل امنیتی نشان می‌دهد که روش پیشنهادی در برابر حملات مذکور مقاوم بوده و سه شرط اصلی امن بودن پیام را برآورده می‌سازد. همچنین در بخش ارزیابی عملکرد این مقاله ثابت می‌شود که روش ارائه شده با توجه به محدودیت‌های محیط زیرآب، بسیار مناسب بوده و نسبت به روش RSA، عملکرد بهینه‌تری را در پارامترهای مصرف انرژی، سربرابر مخابراتی و هزینه‌های محاسباتی از خود به جای می‌گذارد. سازمان‌دهی مقاله به این شرح می‌باشد: بخش دوم به تحلیل فناوری PUF می‌پردازد. بخش سوم مدل سیستم و تهدیدات را نشان داده و بخش چهارم روش ارائه شده را مورد

<sup>1</sup> Autonomous Underwater Vehicles

<sup>2</sup> Surface Command Center (SCC)

<sup>3</sup> External Adversary (EA)

<sup>4</sup> Replay Attack

<sup>5</sup> Fabricated Message Attack

<sup>6</sup> Analyst Attack

<sup>7</sup> Message Modification Attack

<sup>8</sup> Physical Unclonable Function (PUF)

<sup>9</sup> Non-volatile Memory (NVM)

<sup>10</sup> Rivest-Shamir-Adleman

بررسی قرار می‌دهد. همچنین تحلیل امنیتی و ارزیابی عملکرد روش پیشنهادی به ترتیب در بخش‌های پنجم و ششم قرار گرفته و در انتها نیز یک نتیجه‌گیری قرار می‌گیرد.

## ۲. فناوری PUF

ساختارهای خازن شانه‌ای به هم متصل سطحی<sup>۱</sup> یک ابزار بسیار مناسب برای اندازه‌گیری و ارزیابی ویژگی‌های لایه سطحی با روش‌های مختلف می‌باشند. این ساختارهای شانه‌ای به راحتی در آخرین مرحله لایه فلزکاری تولید تراشه‌های استاندارد ساخته می‌شوند. مرحله روکش‌بندی به منظور به حداکثر رساندن مقدار ظرفیت سازه‌های خازنی شانه‌ای، بهینه سازی شده است. این افزایش در مقدار ظرفیت خازنی اندازه‌گیری شده می‌تواند برای پیاده‌سازی یک فناوری به نام PUF مورد استفاده قرار گیرد. PUF یک تابع تصادفی است که تنها می‌توان آن را به کمک یک سیستم فیزیکی ارزیابی نمود. یک PUF می‌تواند برای برقراری امنیت تراشه و ذخیره اطلاعات به کار رود که در آن الگوریتم گشودن کلید توسط خازن‌هایی که در تراشه وجود دارند، تولید می‌شود. با افزایش ظرفیت خازنی و دقت اندازه‌گیری آن‌ها، قدرت کلیدهای تولید شده افزایش می‌یابد.

در روش PUF می‌توان کلیدهای بسیار زیادی را به توجه به تغییرات بیت چالش<sup>۲</sup> تولید نمود. آزمایش‌هایی که در آن مدارهای یکسان با طرح‌بندی‌های یکسان روی تراشه‌های مختلف قرار داده شده، نشان می‌دهند که تاخیر مسیر<sup>۳</sup> به اندازه کافی در طول تراشه‌ها متفاوت است تا از آن‌ها برای شناسایی استفاده شود. شکل ۱ روند تولید کلید در روش PUF را نشان می‌دهد. هر بیت چالش دو مسیر از طریق مدار می‌سازد که به صورت همزمان ایجاد می‌شوند. پاسخ‌های دیجیتالی صفر و یک بر اساس مقایسه بین مسیرهای تاخیر و توسط داور<sup>۴</sup> مشخص می‌شود. در نتیجه می‌توان پاسخ‌های  $n$  بیتی را از این مدار با  $n$  بار تکرار مدار و یا استفاده از  $n$  چالش‌های مختلف به دست آورد. در اینجا بهتر است تنها از منطق دیجیتال استاندارد استفاده گردد. به دلیل وابستگی به ساختار فیزیکی و مداری این روش، پارامترهایی مانند دما و ولتاژ نیز می‌توانند بر خروجی سیستم تاثیر بگذارند. این روش دارای چند مزیت امنیتی می‌باشد که می‌توان به موارد زیر اشاره نمود:

- کلیدها با توجه به درخواست یا نیاز تولید می‌شوند.
- می‌توان کلیدهای اصلی چندتایی<sup>۵</sup> تولید نمود.
- به علت تغییرات فرآیند تصادفی، هیچ دو مدار مجتمعی حتی با طرح‌بندی<sup>۶</sup> یکسان برابر نبوده و در نتیجه کلیدهای یکسان تولید نمی‌کنند. این تنوع در فرآیند تولید یک ویژگی ذاتی می‌باشد.
- کلیدهای تولید شده در این روش قابل زدودن یا پیش‌بینی نبوده و تنوع نسبی با پیشرفت فرآیند تولید افزایش می‌یابد.

کلید تولید شده در این روش غیرقابل مشاهده برای مهاجمان بوده و در هر دستگاه منحصر به فرد است و می‌تواند برای تأیید اعتبار و تصدیق صحت کل سیستم قابل استفاده باشد. کلیدهای رمزنگاری منحصر به فردی که توسط فناوری PUF تولید می‌شود می‌تواند گزینه بسیار مناسبی برای حل مسأله امنیت برای سیستم‌های ارتباطی زیرآبی باشد. PUF از الگوهای تصادفی منحصر به فرد دستگاه برای تشخیص تراشه‌ها از یکدیگر استفاده می‌کند.

<sup>۱</sup> Planar Inter-digitated Comb Capacitor Structures

<sup>۲</sup> Challenge Bits

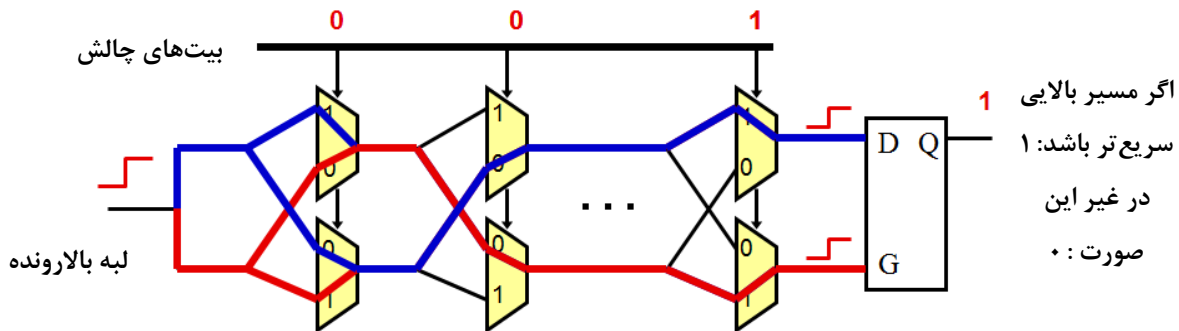
<sup>۳</sup> Path Delays

<sup>۴</sup> Arbiter

<sup>۵</sup> Multiple Master Keys

<sup>۶</sup> Layouts

PUF و به‌طور خاص SRAM PUF طراحی شده است تا امکان کپی، همسان‌سازی و یا پیش‌بینی آن غیرممکن باشد. این کار آن را برای برنامه‌های کاربردی مانند تولید و ذخیره کلید امن، احراز هویت دستگاه، تولید انعطاف‌پذیر کلید و مدیریت قدرتمند کلیدهای تولید شده در هر تراشه بسیار مناسب می‌کند.



شکل ۱- روند تولید کلید در روش PUF.

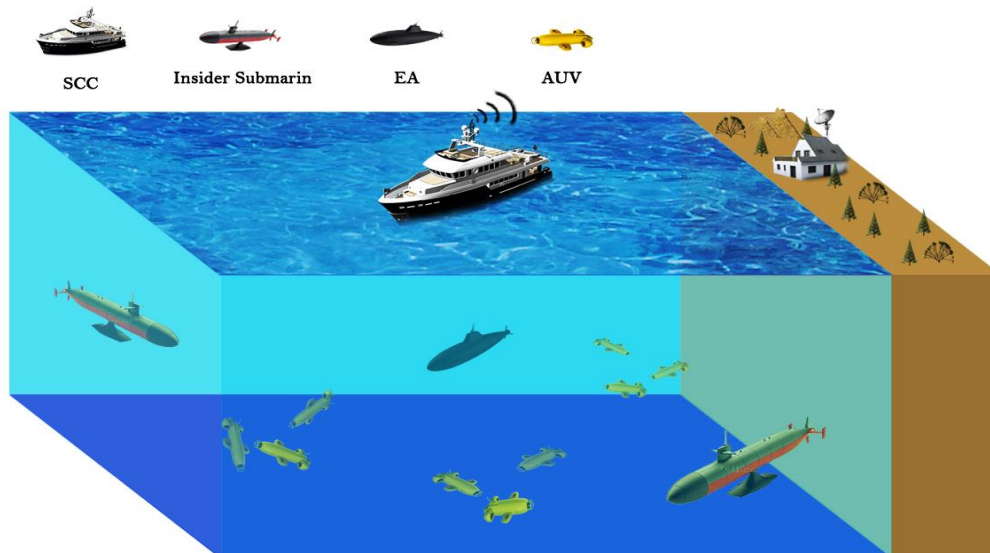
PUF به‌طور فعال تحریک شده و اجرا می‌شود تا از حالات تصادفی در رفتار آن بهره‌برداری گردد. یک روش خوب برای نگاه کردن به یک PUF می‌تواند به عنوان یک اثر انگشت برای هر دستگاه باشد. رفتار نویزی اثر انگشت هر دستگاه نیز به نفع سیستم استفاده می‌شود. آنتروپی نویز می‌تواند برای تولید اعداد تصادفی قوی و مستقل با آنتروپی بالا استفاده شود. ژنراتورهای مستقل و قوی اعداد تصادفی در هر نوع پروتکل رمزنگاری مورد نیاز هستند و اغلب ضعیف‌ترین لینک در پیاده‌سازی‌های مربوط به رمزنگاری می‌باشند.

### ۳. مدل سیستم و تهدیدهای موجود

شکل ۲ یک سیستم ارتباطات آکوستیک زیرآبی شامل چند AUV و زیردریایی خودی، یک مرکز فرماندهی سطحی (SCC) و یک حمله‌گر (EA) را نشان می‌دهد. در این سیستم هر یک از زیرسطحی‌ها دارای محدودیت انرژی و محاسباتی می‌باشند. زیرا منابع انرژی و محاسباتی آن‌ها (خصوصاً AUV) محدود می‌باشد. گزارشات هر یک از زیرسطحی‌ها را جمع‌آوری نموده و به تحلیل آن‌ها می‌پردازد. به دلیل رسیدن پیام‌های بسیار زیاد به SCC توسط همه زیرسطحی‌ها، در نظر گرفتن هزینه‌های محاسباتی برای SCC نیز یک مساله چالش‌برانگیز محسوب می‌شود. هرچند که فرض می‌شود SCC هیچ‌گونه محدودیتی در مصرف منابع انرژی نداشته باشد. همچنین ذکر این نکته ضروریست که تمام اطلاعات و گزارش‌هایی که زیرسطحی‌ها برای SCC می‌فرستند در یک فرمت خاص بوده و البته SCC این فرمت را می‌داند. همچنین این سیستم می‌تواند توسط EA مورد حمله قرار گرفته که در مورد محیط زیرآبی و ارتباطات در آن شناخت کاملی داشته می‌تواند پیام‌های ارسالی را در بین راه ضبط کرده و یا به دام بیندازد. حال فرض می‌شود که EA حملات زیر را به سیستم اعمال کند:

- **حمله بازپخش:** در این نوع از حمله، EA می‌تواند پیام‌های ارسال شده توسط زیرسطحی‌ها را ضبط کرده و دوباره برای SCC ارسال نماید. در واقع SCC پیام‌هایی را دریافت می‌کند که از تاریخشان گذشته است. لذا در نظر گرفتن یک روش تصدیق صحت برای آشکارسازی پیام‌های منقضی ضروریست.

- **حمله ار سال پیام جعلی:** در اینجا SCC یک پیام جعلی از EA دریافت کرده که با توجه به نوع پیام دریافتی و در صورت عدم آشکارسازی می‌تواند موجب گرفتن تصمیماتی به نفع دشمن گردد. بنابراین تدوین روشی مبتنی بر تصدیق صحت برای آشکارسازی فرستنده پیام‌های دریافتی در SCC ضروری می‌باشد.



شکل ۲- مدل سیستم ارتباطات زیرآبی و تهدیدات موجود در این مقاله.

- **حمله تحلیل پیام:** در این روش EA پیام ار سالی را دریافت کرده و به گشودن و تحلیل آن برای یافتن جزئیات هر چه بیشتر اهتمام می‌ورزد. بنابراین استفاده از روش‌های رمزنگاری جهت مقابله با حمله‌های ضدمحرمانگی لازم است.
- **حمله اصلاح پیام:** پیام‌های ار سالی در کانال ممکن توسط EA گیر افتاده و مورد تغییر و اصلاح قرار گیرند. در این صورت SCC امکان دستیابی به پیام‌های صحیح را از دست می‌دهد. لذا باید از تکنیک‌های حفظ بی‌عیبی پیام استفاده شود.

در ادامه توضیح مدل سیستم و تهدیدات موجود، به بررسی اهداف طراحی پرداخته می‌شود. در واقع همانطور قبلاً اشاره گردید، هدف از ارائه روش پیشنهادی در این مقاله، طراحی یک پروتکل "امن" و "بهینه" برای سیستم مورد نظر با استفاده از فناوری PUF است.

#### ۴. روش امن پیشنهادی

روش امن و بهینه ارائه شده در این مقاله بر پایه فناوری PUF و توابع رمزنگاری چکیده ساز شکل می‌گیرد. به دلیل استفاده از توابع رمزنگاری چکیده ساز، لازم است تا در ابتدا ثابت شود که هیچ گونه تصادمی<sup>۱</sup> صورت نمی‌گیرد. برای مثال اگر داشته باشیم  $h_i = \text{Hash}(D_i)$  که در آن  $D_i$  متن پیام و Hash تابع رمزنگاری چکیده ساز باشد، آنگاه نباید پیام جعلی  $D'_i$  پیدا کرد که در آن  $h_i = \text{Hash}(D'_i)$  به عبارت دیگر باید ثابت نمود که احتمال اتفاق یک تصادم تقریب برابر

<sup>1</sup> Collision

صفر است. اگر  $h$  یک تابع چکیده ساز بوده که بتواند خروجی چکیده ساز رمز شده‌ای برابر  $z$ -bit ( $z = 2^q$ ,  $q \in \{1, 2, \dots\}$ ) تولید نماید، بنابراین برای یک پیام تصادفی  $D$ ،  $2^z$  پیام چکیده ساز شده مختلف توسط  $h(D)$  تولید می‌شود. در اینجا می‌توان ثابت نمود که چند پیام جعلی باید توسط EA ساخته و فرستاده شود تا در SCC یک تصادم رخ دهد.

اگر فرض شود که  $P(l)$  احتمال رخ دادن یک تصادم بعد فرستادن  $l$  پیام جعلی باشد، داریم:

$$Pr[E_i] = \frac{i-1}{2^z} \quad (1)$$

$$P(l) = Pr[E_1 \vee E_2 \vee \dots \vee E_l] \leq Pr[E_1] \vee Pr[E_2] \vee \dots \vee Pr[E_l] \leq \frac{0}{2^z} + \frac{1}{2^z} + \dots + \frac{l-1}{2^z} = \frac{l(l-1)}{2^{z+1}} \quad (2)$$

که در آن،  $E_i$  احتمال رخ دادن  $i$ امین تصادم بعد از فرستادن  $D_i$  می‌باشد. طبق رابطه (۲)، کران بالایی  $P(l)$  با عبارت  $O(2^{-z-1}l^2)$  رشد می‌کند. برای مثال اگر  $P(l) = 0.5$  و  $z = 128$ -bit،  $z$ ، آنگاه برای تولید یک تصادم با شانس ۵۰٪ (که خود شانس بالایی محسوب می‌شود)، EA نیاز دارد تا  $2^{64}$  پیام جعلی را برای SCC بفرستد! اما  $D_i$  در فاصله‌های زمانی کوتاه تغییر می‌کند که با این شرایط، احتمال روی دادن یک تصادم، به اندازه بسیار بزرگی کافی، قابل صرف نظر کردن است. حال هر زیر سطحی  $S_j$  یک کلید خصوصی یکتا و قدرتمند  $K_{prvt_j}$  را با استفاده از تراشه موجود و فناوری PUF پایگاه داده خود می‌سازد. سپس  $S_j$  با استفاده از رابطه زیر کلید عمومی  $K_{pub_j} = Hash(K_{prvt_j})$  را تولید نموده، آن را با کلید خصوصی خود رمز کرده و به کل سیستم ارسال می‌نماید. هر  $S_j$  نیز به مقدار مورد نیاز، پیام‌های رمز شده‌ای به صورت رابطه زیر تولید می‌نماید:

$$C'_i = Enc_{K_{prvt_j}}(m_i || TS_i) \quad (3)$$

که در آن،  $m_i$  و  $TS_i$  به ترتیب متن اصلی و مهر زمانی<sup>۱</sup> و  $Enc$  به معنای تابع رمزنگاری تحت کلید خصوصی  $K_{prvt_j}$  می‌باشد. حال  $S_j$  با استفاده از کلید عمومی  $SCC(K_{pub_{SCC}})$ ،  $C'_i$  را طبق رابطه زیر رمز می‌نماید:

$$C_i = Enc_{K_{pub_{SCC}}}(C'_i) \quad (4)$$

در نهایت  $S_j$  طبق رابطه زیر مقدار چکیده ساز پیام رمز شده را محاسبه کرده و آن را برای SCC می‌فرستد.

$$h_i = Hash(C_i) \quad (5)$$

به دلیل جمع و ارتباطات بلادرنگ، وجود مهر زمانی برای هر پیام ضروریست. همچنین در ادامه مشاهده خواهد شد که با کمک مهر زمانی، می‌توان اثر بعضی از تهدیدات را خنثی نمود. در حالت کلی، هر پیام ارسالی توسط  $S_j$  می‌تواند با توجه به ثانیه، دقیقه، روز، ماه و سال ارسال آن پیام تاریخ‌گذاری شده و به وسیله این تاریخ، مهر زمانی منحصر به فرد برای هر پیام تولید گردد. در ادامه به منظور دریافت معتبر پیام‌ها، SCC می‌تواند مراحل زیر را به اجرا برساند:

(۱) SCC می‌تواند حمله بازپخش را با مقایسه مجموعه چکیده ساز پیام‌های دریافتی قبلی و چکیده ساز پیام دریافت شده آشکار نماید. برای مثال فرض شود که  $S_1$   $C_i$  را برای SCC می‌فرستد که مقدار چکیده ساز  $C_i$  برابر با  $Hash$

<sup>1</sup> Time Stamp

$(C_i) = d$  می‌باشد. سپس به پایگاه داده خود رجوع کرده و تمامی مقادیر چکیده سازهای رسیده شده قبل را فراخوانی می‌نماید. اگر  $d$  عضو مجموعه چکیده سازهای دریافتی قبلی تا آن لحظه باشد، آن‌گاه حمله بازپخش آشکار شده و پیام دریافت شده رد می‌گردد. برای مثال فرض شود که مجموعه پیام‌های چکیده ساز شده دریافتی قبلی برابر با  $\{c, d, e, f\}$  باشد. حال با توجه به اینکه  $d$  عضوی از این مجموعه است، لذا پیام دریافتی یک پیام بازپخش شده بود و آن را رد می‌کند.

(۲) پس از دریافت  $h_i$  و اطمینان از عدم حمله بازپخش، به پایگاه داده خود رجوع نموده و مقدار  $C_i$  را می‌یابد. با توجه به اینکه تابع چکیده ساز استفاده شده امن می‌باشد [۲۶]، هر گونه حمله ضد بی‌عیبی آشکار می‌شود. همچنین با توجه به رابطه (۲) حمله‌های مبتنی بر تصادم نیز غیرممکن خواهد بود.

(۳) پس از دریافت  $C_i$  و با توجه به رابطه زیر مقدار  $C'_i$  را به دست می‌آورد که در آن  $Dec$  تابع رمزگشایی می‌باشد. با توجه به اینکه  $C'_i$  با استفاده از کلید عمومی  $SCC$  رمز شده است، حال  $C'_i$  تنها با دانستن کلید خصوصی  $SCC$  ( $K_{prvtSCC}$ ) قابل گشودن است. از آنجایی که کلید خصوصی  $SCC$  تنها در اختیار  $SCC$  می‌باشد (این نیز با استفاده از فناوری PUF در خود  $SCC$  تولید می‌شود)، لذا فقط  $SCC$  به  $C'_i$  دسترسی داشته و حملات ضد محرمانگی خنثی می‌گردد.

$$C'_i = Dec_{K_{prvtSCC}}(C_i) \quad (۶)$$

(۴) همچنین  $SCC$  برای اعتباربخشی به پیام، باید بتواند منبع فرستنده پیام را نیز شناسایی نماید. به عبارت دیگر  $SCC$  باید بداند که پیامی که دریافت می‌کند از سمت یکی از زیر سطحی‌ها ارسال شده و یا  $EA$  آن را ارسال نموده است.  $SCC$  با در اختیار داشتن  $C'_i$  و همچنین کلید عمومی  $S_j(K_{pub_j})$ ، مقدار  $m_i|TS_i$  را طبق رابطه زیر محاسبه می‌نماید. ذکر این نکته ضروریست که به دلیل اینکه تنها  $S_j$  کلید خصوصی خود ( $K_{prvt_j}$ ) را در اختیار دارد، لذا فقط  $S_j$  می‌تواند پیامی از جانب خود برای  $SCC$  بفرستد و بنابراین هر گونه حمله ضد احراز اصالت آشکار خواهد شد.

$$m_i|TS_i = Dec_{K_{pub_j}}(C'_i) \quad (۷)$$

(۵) به دلیل تاخیر انتشار موجود در کانال آکوستیک زیرآبی، ابتدا  $SCC$  تازگی پیام را با توجه به رابطه (۸) مورد بررسی قرار می‌دهد که در آن  $TS_{local}$  مهر زمانی محلی در  $SCC$  و  $\theta$  یک مقدار آستانه از پیش تعریف شده می‌باشد. اگر رابطه (۸) برقرار نباشد،  $SCC$  پیام را رد می‌کند. در غیر این صورت متن اصلی  $m_i$  را با فرمتی که در پایگاه داده خود ذخیره دارد، مقایسه می‌نماید. اگر فرمت پیام‌ها یکی بود، پیام پذیرفته شده و در غیر این صورت رد می‌گردد. به این ترتیب، روش ارائه شده در این مقاله، بی‌عیبی و تازه بودن پیام را نیز مورد ارزیابی قرار می‌دهد.

$$|TS_i - TS_{local}| \leq \theta \quad (۸)$$

## ۵. تحلیل امنیتی

ویژگی‌های امنیتی روش پیشنهادی در این مقاله، در این بخش مورد بررسی قرار می‌گیرد. به عبارتی دیگر، میزان مقاوم بودن این روش در مقابل حملات بازپخش، از سال پیام جعلی، تحلیل پیام و اصلاح پیام مورد ارزیابی قرار می‌گیرد. در واقع در این بخش فارغ از میزان بهینه بودن روش پیشنهادی، تنها امنیت آن مورد بررسی قرار می‌گیرد و در بخش بعدی، به بررسی بهینه بودن تصدیق صحت مبتنی بر PUF پرداخته خواهد شد.

### ۵-۱. مقاومت در برابر حمله بازپخش

با توجه به توضیحات ارائه شده در قدم اول بررسی اعتبار پیام، SCC می‌تواند حمله بازپخش را با پس از دریافت  $C_i$  آشکار نماید. برای توضیح بیشتر، ابتدا SCC مقدار  $Hash(C_i)$  را محاسبه نموده و سپس آن را با مقادیر چکیده ساز دریافتی در پایگاه داده خود مقایسه می‌نماید. اگر هیچ یک از اعضای مجموعه چکیده ساز دریافتی قبلی، برابر با چکیده ساز پیام دریافتی جدید نباشند، آن‌گاه می‌توان به این نتیجه رسید که حمله بازپخش صورت نگرفته است، در غیر این صورت حمله بازپخش آشکار شده است، بنابراین روش پیشنهادی در برابر حمله بازپخش مقاوم می‌باشد.

### ۵-۲. مقاومت در برابر حمله تحلیل پیام

در روش پیشنهادی، هر زیرسطحی پیام مورد نظر خود را ابتدا طبق رابطه (۴) و با استفاده از کلید عمومی SCC ( $K_{pub_{SCC}}$ )، رمز می‌کند. کلید عمومی SCC نیز طبق رابطه ( $K_{pub_j} = Hash(K_{prvt_j})$ )، از چکیده ساز کردن کلید خصوصی آن به دست می‌آید. با توجه به یکتا بودن کلید خصوصی تولید شده توسط فناوری PUF در تراشه موجود در SCC و خواص امن، یک‌راهه بودن و عدم تصادم تابع چکیده ساز مورد استفاده، کلید عمومی به کار رفته نیز یکتا بوده و تنها با کلید خصوصی SCC گشوده می‌شود. از آنجایی که کلید خصوصی SCC تنها در اختیار SCC بوده (تولید شده با PUF و ذخیره شده در حافظه SCC) و مطلقاً غیرقابل دسترس و یا کشف برای هر موجودیت دیگری غیر از SCC اعم از حمله‌گر می‌باشد، لذا امکان آشکارسازی و تحلیل پیام توسط حمله‌گر وجود نداشته و بنابراین روش پیشنهادی در این مقاله در برابر حمله تحلیل پیام، امن می‌باشد.

### ۵-۳. مقاومت در برابر حمله ارسال پیام جعلی

SCC می‌تواند با در اختیار داشتن  $C'_i$  و با استفاده از رابطه (۷) یعنی؛ استفاده از کلید عمومی  $S_j(K_{pub_j})$ ، مقدار  $m_i|TS_i$  را به دست آورد. از آنجایی که تنها  $S_j$  کلید خصوصی خود ( $K_{prvt_j}$ ) را در اختیار دارد، لذا فقط  $S_j$  می‌تواند پیامی از جانب خود با امضا  $S_j(K_{prvt_j})$  برای SCC بفرستد و هر پیامی که با استفاده از  $K_{prvt_j}$  رمز شده باشد، قطعاً از طرف  $S_j$  ارسال شده است، زیرا  $K_{prvt_j}$  کلید یکتایی است که توسط PUF تولید شده و هیچ موجودیتی به جز خود  $S_j$  به آن دسترسی و یا قدرت کشف آن را ندارد. بنابراین SCC می‌تواند منبع پیام  $m_i|TS_i$  را با استفاده از  $K_{pub_j}$  شناسایی نموده و هر گونه حمله ضدحراز اصالت را خنثی سازد.

### ۵-۴. مقاومت در برابر حمله اصلاح پیام



پس از تصدیق صحت پیام و منبع آن، SCC رمز  $C'_i$  را با استفاده از رابطه (۷) گشوده و  $m_i|TS_i$  را به دست می‌آورد. همانطور که قبلاً ذکر شد، تمام پیام‌هایی که زیر سطحی‌ها برای SCC می‌فرستند در قالب یک فرمت بوده و این فرمت در پایگاه داده SCC قرار دارد. حال SCC پس از گشودن رمز پیام، متن اصلی به دست آمده را با فرمت موجود در پایگاه داده خود مقایسه می‌نماید. اگر پیام گشوده شده در قالب فرمت ذخیره شده در SCC بود، آنگاه پیام پذیرفته می‌شود، در غیر این صورت پیام به نحوی دچار تغییر شده و بی‌عیبی آن زیر سوال می‌رود. به این ترتیب حمله اصلاح پیام آشکار شده و SCC پیام را رد می‌کند. همچنین با توجه به اینکه تابع چکیده ساز استفاده شده امن می‌باشد، هر گونه حمله ضد بی‌عیبی آشکار می‌شود.

## ۶. ارزیابی عملکرد و میزان بهینگی

در قسمت قبل ثابت شد که روش ارائه شده امن بوده و در مقابل همه تهدیدات مقاوم است. اما میزان بهینگی روش ارائه شده نیز با توجه به محدودیت‌های موجود در سیستم‌ها و کانال‌های زیرآبی از اهمیت به‌سزایی برخوردار است. لذا در این بخش ارزیابی عملکرد و بهینگی روش پیشنهادی در سه پارامتر مصرف انرژی، سربار مخابراتی و هزینه محاسباتی با روش RSA مقایسه می‌شود.

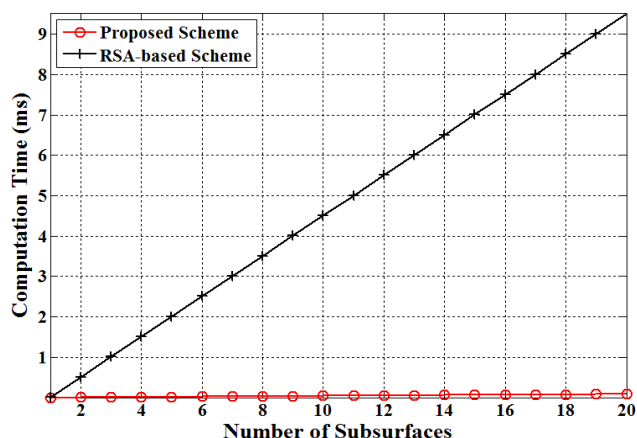
### ۶-۱. مصرف انرژی

همانطور که در قسمت‌های قبل ذکر شد، کمبود منابع انرژی از مهم‌ترین چالش‌ها در ارتباطات زیرآبی می‌باشد. به همین دلیل روش‌های رمزنگاری که به منظور برقراری امنیت به سیستم اضافه می‌شوند باید دارای کمترین سربار انرژی باشند که در عمل عکس این بوده و معمولاً روش‌هایی مانند RSA به دلیل داشتن فرآیندهایی با محاسبات بسیار زیاد و پیچیده مانند انتخاب یک جفت عدد اول بزرگ، امضا RSA و غیره، اغلب انرژی زیادی را از سیستم مصرف می‌کنند. اما در روش پیشنهادی مبتنی بر PUF، عملیات منطقی بر روی تراشه موجود برای رسیدن به یک عدد تصادفی که همان کلید خصوصی می‌باشد، تنها فرآیند موجود در این روش است که مصرف انرژی آن در مقابله با فرآیندهای پیچیده موجود در الگوریتم RSA قابل مقایسه نمی‌باشد.

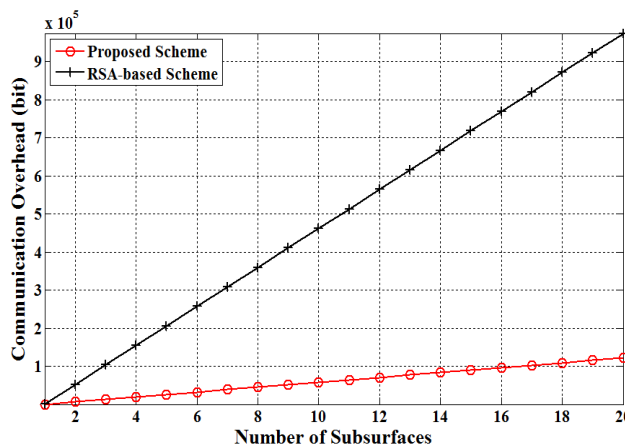
### ۶-۲. سربار مخابراتی

به دلیل پهنای باند کم در ارتباطات آکو استیک زیرآبی، در نظر گرفتن سربار مخابراتی مساله‌ای بسیار مهم می‌باشد. بنابراین سربار مخابراتی اضافه شده به سیستم توسط روش امن ارائه شده در این مقاله با روش RSA مقایسه می‌شود. در روش RSA که در آن  $S_j$  یک امضا RSA برای SCC می‌فرستد، مقدار سربار مخابراتی به طور معمول (حداقل) برابر  $1024$  بیت می‌باشد. در حالی که در روش پیشنهادی در این مقاله، پس از رمز کردن پیام با استفاده از کلیدهای تولید شده توسط PUF و همچنین به دست آوردن چکیده ساز آن (رابطه (۹))، مقدار سربار مخابراتی حاصل برابر  $128$  بیت خواهد بود (در این مقاله فرض بر استفاده از یک تابع تولید چکیده ساز  $128$  بیتی می‌باشد). اما این اختلاف با افزایش تعداد زیر سطحی‌ها محسوس‌تر خواهند شد، زیرا در یک سیستم مخابرات آکو استیک زیرآبی، هر SCC با تعداد زیادی از زیر سطحی‌ها در ارتباط می‌باشد. شکل ۳ برتری عملکرد روش پیشنهادی نسبت به روش RSA را با افزایش تعداد زیر سطحی‌ها نشان می‌دهد.

$$\text{Hash}(\text{Enc}_{\text{pub}_{\text{SCC}}}(\text{Enc}_{\text{K}_{\text{prvt}_j}}(m_i|TS_i))) \quad (9)$$



شکل ۴- هزینه محاسباتی در روش پیشنهادی و روش RSA در SCC.



شکل ۳- مقایسه سربار مخابراتی بین روش پیشنهادی و روش RSA.

### ۳-۶. هزینه محاسباتی

در این بخش، هزینه محاسباتی بین دو روش مذکور در زیرسطحی‌ها و در SCC آورده می‌شود. جدول ۱ نتایج مشاهدات حاصل از اجرای یک تابع رمزنگاری چکیده ساز، یک امضا RSA و یک تصدیق امضا RSA را نشان می‌دهد که در ماشین Intel Pentium IV 3.0-GHz به اجرا در آمده اند [۲۷].

جدول ۱- زمان اجرای عملگرهای رمزنگاری.

عملگر رمزنگاری	زمان مورد نیاز برای اجرا
تابع چکیده ساز یک‌طرفه	0.000092 ms
یک امضا RSA	2.25 ms
یک تصدیق امضا RSA	0.1 ms

در سیستم ارتباطی زیرآبی، هر زیرسطحی تنها عملیات جمع‌آوری اطلاعات و عملیات منطقی مانند XOR را انجام می‌دهد. همچنین هر امضا الگوریتم RSA نیز طبق جدول ۱ به 2.25 ms زمان نیاز دارد. در نتیجه برای ارسال هر پیام در فرستنده، هزینه محاسباتی برای هر زیرسطحی در روش PUF نسبت به روش RSA مقداری قابل چشم‌پوشی است. بنابراین روش تصدیق صحت مبتنی بر PUF ارائه شده در این مقاله دارای هزینه محاسباتی بسیار کمتری نسبت به روش RSA در زیرسطحی‌ها می‌باشد.

در گیرنده، برای اینکه منبع پیام توسط SCC تصدیق گردد، نیاز است تا مقدار تابع چکیده ساز ارسالی محاسبه شده و سپس با استفاده از کلید خصوصی و عمومی، متن اصلی استخراج گردد. حال با توجه به جدول ۱ مقدار زمان مورد نیاز برای تولید یک مقدار چکیده ساز و برای هر پیام در روش ارائه شده برابر 0.000092 ms می‌باشد. در حالی که طبق جدول ۱ و در روش اعتبار بخشیدن به امضا RSA، پیچیدگی محاسباتی برابر 0.1 ms خواهد بود. شکل ۴ هزینه محاسباتی در

SCC را با استفاده از دو روش ارائه شده در این مقاله و RSA نشان می‌دهد. با توجه به نتایج مشخص است که روش تصدیق صحت مبتنی بر PUF دارای هزینه محاسباتی بسیار کمتری نسبت به روش RSA در SCC می‌باشد. همچنین در روش ارائه شده در این مقاله بر خلاف روش RSA علاوه بر تصدیق صحت، شرط‌های محرمانگی و بی‌عیبی پیام نیز برآورده می‌شود. در حالی که برای محرمانگی از الگوریتم‌های متقارن مانند الگوریتم<sup>۱</sup> AES استفاده نشده است که این خود علاوه بر اینکه از بار محاسباتی سیستم می‌کاهد، در مصرف انرژی صرفه‌جویی شده و همچنین سربارهایی مانند تولید، توزیع و مدیریت کلید برای الگوریتم متقارن را در خود ندارد. همچنین بی‌عیبی در این روش تنها به تابع رمزنگاری چکیده ساز بستگی داشته که علاوه بر بار محاسباتی و پردازشی پایین، به دلیل امن بودن تابع چکیده ساز، هر گونه حمله ضد بی‌عیبی نیز خنثی می‌گرداند. جدول ۲ یک مقایسه کلی بین روش ارائه شده در این مقاله و روش RSA ارائه می‌دهد.

جدول ۲- مقایسه بین روش ارائه شده در این مقاله و روش RSA برای امنیت سیستم‌های ارتباطی زیرآبی.

RSA	روش مبتنی بر PUF	
وابسته به کلید	بسیار بالا	امنیت
زیاد	کم	سربار مخابراتی
زیاد	کم	مصرف انرژی
زیاد	کم	هزینه پردازشی
دارد	ندارد	مدیریت کلید
خیر	بله	مقیاس پذیری
کم	زیاد	طول عمر

## ۷. نتیجه‌گیری

در این مقاله یک روش امن و بهینه مبتنی فناوری PUF برای ارتباطات آکوستیک زیرآبی ارائه شده است. به دلیل ویژگی‌های بسیار مناسب مناسب فناوری PUF مانند تولید کلیدهای بسیار تصادفی و قدرتمند، عدم دسترسی و کشف کلید خصوصی حتی در صورت دسترسی فیزیکی به سیستم و همچنین تولید کلیدهای یکتا برای هر دستگاه موجب شد تا در این مقاله از این فناوری برای تصدیق صحت در ارتباطات زیرآبی استفاده گردد. همچنین روش پیشنهادی در این مقاله (پروتکل ارائه شده مبتنی بر تابع رمزنگاری چکیده ساز و فناوری PUF) با بخشیدن امنیت کامل به سیستم و با مقاومت در برابر همه تهدیدات موجود در کانال زیرآبی (حملات بازپخش، ارسال پیام جعلی، تحلیل پیام و اصلاح پیام)، نشان داد که سه شرط مهم تصدیق صحت، محرمانگی و بی‌عیبی را برآورده می‌سازد. همچنین این روش با توجه به محدودیت‌های موجود در محیط زیر آب، نسبت به روش RSA در سه پارامتر مصرف انرژی، سرریز مخابراتی و هزینه محاسباتی، عملکرد بهتری داشته است. لذا با استفاده از تکنولوژی PUF می‌توان خط پایانی بر چالش‌های امنیتی در سیستم‌های ارتباطی زیرآبی به خصوص از دیدگاه عملی کشید.

<sup>۱</sup> Advanced Encryption Standard

## ۸. مراجع

- [1] A. Falahati, B. Woodward, and S. C. Bateman, "Underwater Acoustic Channel Models for 4800 b/s QPSK Signals," *IEEE J. Oceanic Engineering*, vol. 19, no. 1, pp. 12–20, 1991.
- [2] A. Zielinski, Y. Yoon, and L. Wu, "Performance Analysis of Digital Acoustic Communication in a Shallow Water Channel," *IEEE J. Oceanic Engineering*, vol. 20, no. 4, pp. 293–299, 1995.
- [3] P. A. Walree, and R. Otnes, "Ultrawideband Underwater Acoustic Communication Channels," *IEEE J. Oceanic Engineering*, vol. 38, no. 4, pp. 678–688, 2013.
- [4] A. C. Singer, J. K. Nelson, and S. S. Kozat, "Signal Processing for Underwater Acoustic Communications," *IEEE Communication Magazine*, vol. 47, no. 1, pp. 90–96, 2009.
- [5] T. C. Yang, "Correlation-Based Decision-Feedback Equalizer for Underwater Acoustic Communications," *IEEE J. Oceanic Engineering*, vol. 30, no. 4, pp. 865–880, 2005.
- [6] S. Hwang, and P. Schniter, "Efficient Multicarrier Communication for Highly Spread Underwater Acoustic Channels," *IEEE J. Selected Areas in Communications*, vol. 26, no. 9, pp. 1674–1683, 2008.
- [7] M. Stojanovic, and J. Preisig, "Underwater Acoustic Communication Channels: Propagation Models and Statistical Characterization," *IEEE Communication Magazine*, vol. 47, no. 1, pp. 84–89, 2009.
- [8] M. Khishe, M. R. Mosavi and M. Kaveh, "Improved Migration Models of Biogeography-Based Optimization for Sonar Dataset Classification by using Neural Network," *J. Applied Acoustics*, vol. 118, no. 3, pp. 15–29, 2017.
- [9] B. G. Mobasser, and R. S. Lynch, "Information Embedding in Sonar by Modifications of Time-Frequency Properties," *IEEE J. Oceanic Engineering*, vol. 41, no. 1, pp. 139–154, 2016.
- [10] M. C. Domingo, "Securing Underwater Wireless Communication Networks," *IEEE Communication Magazine*, vol. 8, no. 1, pp. 22–28, 2011.
- [11] G. Han, J. Jiang, N. Sun, and L. Shu, "Secure Communication for Underwater Acoustic Sensor Networks," *IEEE Communication Magazine*, vol. 53, no. 8, pp. 54–60, 2015.
- [12] G. Dini, and A. L. Duca, "A Secure Communication Suite for Underwater Acoustic Sensor Networks," *Sensors- Basel*, vol. 12, no. 11, pp. 133–58, 2012.
- [13] Y. Chen, Y. Lin, and S. Lee, "A Mobicast Routing Protocol in Underwater Sensor Networks," *IEEE Conf. Wireless Communications and Networking*, pp. 510–515, 2011.
- [14] S. Misra, S. Dash, M. Khatua, A.V. Vasilakos, and M. S. Obaidat, "Jamming in Underwater Sensor Networks: Detection and Mitigation," *IET Commun.*, vol. 6, no. 14, pp. 2178–88, 2012.
- [15] X. Lu, and Z. Yonghua, "Modeling The Wormhole Attack in Underwater Sensor Network," *IEEE 8th International Conf. Wireless Communications, Networking and Mobile Computing*, pp. 1–4, 2012.
- [16] Y. Luo, L. Pu, Z. Peng, and Z. Shi, "RSS-Based Secret Key Generation in Underwater Acoustic Networks: Advantages, Challenges, and Performance Improvements," *IEEE Communication Magazine*, vol. 54, no. 2, pp. 32–38, 2016.
- [17] C. Lal, R. Petrocci, M. Conti, and J. Alves, "Secure Underwater Acoustic Networks: Current and Future Research Directions," *IEEE 3th Conf. Underwater Communications and Networking*, pp. 1–5, 2016.
- [18] H. Li, Y. He, X. Cheng, H. Zhu, and L. Sun, "Security and Privacy in Localization for Underwater Sensor Networks," *IEEE Communication Magazine*, vol. 53, no. 11, pp. 56–62, 2015.
- [19] G. Ateniese, et al., "SecFUN: Security Framework for Underwater Acoustic Sensor Networks," *IEEE 3th Conf. Oceans*, pp. 1–9, 2015.
- [20] M. Ahmed, M. Salleh, and M. Channa, "Routing Protocols Based on Node Mobility for Underwater Wireless Sensor Network : A Survey," *J. Network and Computer Applications*, vol. 78, pp. 242–252, 2017.
- [21] Y. Chen, and Y. Lin, "Mobicast Routing Protocol for Underwater Sensor Networks," *IEEE Sensors Journal*, vol. 13, no. 2, p. 737–749, 2013.
- [22] Johnson, Anju P., Rajat Subhra Chakraborty, and Debdeep Mukhopadhyay. "A PUF-Enabled Secure Architecture for FPGA-based IoT Applications." *IEEE Transactions on Multi-Scale Computing Systems*, Vol. 1, No .2, pp. 110-122, 2015.
- [23] U. Siam, M. Majzoubi, and F. Koushanfar. "A Built-in-Self-Test Scheme for Online Evaluation of Physical Unclonable Functions and True Random Number Generators." *IEEE Transactions on Multi-Scale Computing Systems*, Vol. 2, No .1, pp. 2-16, 2016.
- [24] R. Deepu, et al. "Comb Capacitor Structures for On-Chip Physical Unclonable Function." *IEEE Transactions on Semiconductor Manufacturing*, Vol. 22, No. 1, pp. 96-102, 2009.



- [25] M. Debdeep. "PUFs as Promising Tools for Security in Internet of Things." IEEE Design & Test, Vol. 33, No. 3, pp. 103-115, 2016.
- [26] R. Rivest, "RFC 1321: The MD5 Message-Digest Algorithm," in *Internet Activities Board*. Gaithersburg, MD, USA: National Institute of Standards and Technology, 1992.
- [27] W. Dai, Crypto++ 5.6.2 Benchmarks 2013. [Online]. Available: [http:// www.cryptopp.com/](http://www.cryptopp.com/).