

پژوهشگاه ارتباطات و فناوری اطلاعات

پیوست فراخوان ششمین دوره طرح پژوهانه
(۱۵ شهریور لغایت ۱۵ آبان ۱۴۰۵)

محورهای اصلی فراخوان

(۱) ارتباطات کوانتومی

- آزمایشگاه ارزیابی سامانه‌ها و شبکه‌های کوانتومی
 - تعیین حدود موفقیت/ شکست آزمون‌های ارزیابی عملکرد و امنیت سامانه‌های QKD به ازای پروتکل‌های مختلف
 - ارزیابی عملکرد و امنیت شبکه‌های توزیع کلید کوانتومی
- شبکه ارتباطات کوانتومی
 - بهینه‌سازی منابع و مسیرهای بازپخش کلید در شبکه‌های QKD
 - استفاده از هوش مصنوعی برای تشخیص حملات و بهینه‌سازی عملکرد شبکه QKD
 - ارزیابی شبکه‌های ارتباطات کوانتومی به روش تایید رسمی (formal verification)
 - کاربردهای روش‌های Zero Knowledge proof در QKD
 - ارائه معماری Zero Trust مبتنی بر QKD برای شبکه‌های حیاتی نسل آینده
 - استفاده توامان Blockchain و QKD برای مدیریت کلید و احراز هویت
 - بهبود معماری Blockchain با استفاده از مزایای QKD
 - استفاده از مزایای معماری Blockchain برای بهبود خدمات QKD
 - ارائه قابلیت‌های بهبود یافته ارکستراسیون در شبکه‌های SDN/NFV مبتنی بر معماری Zero Trust فعال شده با QKD
 - ارائه مدل‌های تحلیلی امنیت و کارایی برای معماری‌های مختلف QKD
 - ارزیابی امنیت کلید با توجه به مفروضات پیاده‌سازی واقعی
 - طراحی شبکه‌های کوانتومی با گره‌های غیر قابل اعتماد
 - مدلسازی و تحلیل امنیت شبکه‌های مبتنی بر درهم‌تنیدگی
 - طراحی الگوریتم مسیریابی برای شبکه‌های شامل گره‌های غیر قابل اعتماد
 - مدل تحلیلی برای سنجش قابلیت اعتماد و تحمل خطا
 - طراحی الگوریتم‌های مدیریت کلید و مسیریابی به صورت بدون اعتماد یا با حداقل دانش
- ماهواره کوانتومی
 - طراحی و ساخت سیستم جهت‌گیری (pointing) و ردیابی (tracking) در سامانه‌های ارتباطی با گره متحرک
 - شبیه‌سازی شبکه توزیع کلید کوانتومی با گره‌های متحرک
 - ارزیابی امنیت شبکه QKD مبتنی بر ماهواره
- تجهیزات کوانتومی
 - طراحی و ساخت تجهیزات مورد نیاز در شبکه‌های ارتباط کوانتومی (سامانه‌های توزیع کلید کوانتومی، مولد اعداد تصادفی کوانتومی، چشمه‌ها و آشکارسازهای کوانتومی، حافظه کوانتومی)
- حسگرهای کوانتومی
 - اندازه‌گیری و آشکارسازی سیگنال‌ها و میدان‌های الکترومغناطیسی

- مکان‌یابی، جهت‌یابی و ردیابی منابع و تجهیزات ارتباطی
- پایش، تشخیص و تأمین امنیت زیرساخت‌ها و سامانه‌های ارتباطی
- توسعه سامانه‌های هوشمند مبتنی بر حسگرهای کوانتومی و هوش مصنوعی برای کاربردهای ارتباطی
- هوش مصنوعی و ارتباطات کوانتومی
 - هوش مصنوعی برای طراحی، بهینه‌سازی و مدیریت شبکه‌های ارتباطات کوانتومی
 - هوش مصنوعی برای امنیت، تشخیص حملات و ارزیابی سامانه‌های ارتباطات کوانتومی
 - یادگیری ماشین برای بهبود عملکرد و بهینه‌سازی تجهیزات و سامانه‌های توزیع کلید کوانتومی
 - معماری‌ها و الگوریتم‌های هوشمند برای شبکه‌های کوانتومی نسل آینده
 - شبیه‌سازی، مدل‌سازی و دوقلو دیجیتال هوشمند برای طراحی و ارزیابی شبکه‌های ارتباطات کوانتومی
 - همگرایی هوش مصنوعی و ارتباطات کوانتومی با فناوری‌های ارتباطی نسل آینده

۲) رمزنگاری و احراز هویت پساکوانتومی

- آزمایشگاه ارزیابی شبکه و سامانه‌های پساکوانتومی
 - تعیین حدود موفقیت/ شکست آزمون‌های ارزیابی عملکرد و امنیت سامانه‌های PQC به ازای پروتکل‌های مختلف
 - ارزیابی عملکرد و امنیت شبکه‌های مبتنی بر PQC
 - طراحی سند راهبرد فناوری و معماری کلان آزمایشگاه ملی ارزیابی سامانه‌ها و شبکه‌های پساکوانتومی
 - طراحی Post-Quantum Migration Roadmap
- شبکه و ارتباطات پساکوانتومی
 - طراحی و بهینه‌سازی پروتکل‌های ارتباطی مقاوم در برابر کوانتوم مبتنی بر الگوریتم‌های PQC
 - طراحی پروتکل‌های TLS/DTLS پساکوانتومی
 - استفاده از الگوریتم‌های ML-KEM و ML-DSA در پروتکل‌های شبکه
 - بررسی و بهینه‌سازی Hybrid Cryptography شامل الگوریتم‌های کلاسیک و پساکوانتومی
 - طراحی سازوکارهای Crypto-Agility برای مهاجرت پویا بین الگوریتم‌های رمزنگاری
 - ارزیابی تأثیر PQC بر Latency، Throughput، CPU و Memory شبکه
 - بهینه‌سازی اندازه کلید، Ciphertext و Signature در الگوریتم‌های PQC
 - طراحی پروتکل‌های سبک‌وزن PQC برای تجهیزات محدودمنبع و IoT
 - ارائه معماری Zero Trust مبتنی بر PQC
 - طراحی Post-Quantum Zero Trust Architecture برای زیرساخت‌های حیاتی
 - استفاده از PQC برای احراز هویت کاربران، تجهیزات و سرویس‌ها در معماری Zero Trust
 - طراحی Post-Quantum Identity and Access Management
 - طراحی معماری Zero Trust Network Access (ZTNA) مقاوم در برابر کوانتوم
 - تحلیل ریسک‌های امنیتی در سیستم‌های رمزنگاری و احراز هویت کوانتومی/پساکوانتومی و طراحی راهکارهای بازایی
 - راهکار استفاده از امضای دیجیتال پساکوانتومی (Post-Quantum Digital Signature) در پروتکل‌های احراز هویت
 - طراحی یک چارچوب احراز هویت کوانتومی/پساکوانتومی برای سیستم‌های بانکی و مالی آینده
 - طراحی و پیاده‌سازی یک پروتکل احراز هویت کوانتومی/پساکوانتومی با قابلیت تشخیص نفوذ (QIA - Quantum Intrusion Detection Authentication)
 - طراحی یک سیستم احراز هویت دو عاملی (2FA) یا چند عاملی (MFA) ترکیبی با رمزنگاری پسا-کوانتومی و زیست‌سنجی
 - استفاده همزمان از Blockchain و PQC برای مدیریت کلید و احراز هویت

- استفاده از Blockchain برای مدیریت چرخه عمر کلیدهای PQC
- طراحی سازوکار Post-Quantum Identity مبتنی بر Blockchain
- بررسی استفاده از ML-DSA در Blockchain
- ارائه معماری SDN/NFV مقاوم در برابر کوانتوم
- طراحی Post-Quantum SDN Controller
- استفاده از PQC برای ایمن سازی ارتباط Controller و Network Devices
- طراحی ارکستراسیون Post-Quantum Network Functions
- ارائه قابلیت های Crypto-Agility در SDN/NFV
- تحلیل تأثیر PQC بر QoS و QoE
- طراحی معماری Post-Quantum Secure 6G
- استفاده از PQC در Edge Computing
- بررسی PQC در ارتباطات V2X
- هوش مصنوعی و پساکوانتوم
 - استفاده از هوش مصنوعی برای تشخیص حملات علیه سامانه های PQC
 - استفاده از AI برای انتخاب و بهینه سازی الگوریتم PQC متناسب با شرایط شبکه
 - پیش بینی سربار محاسباتی الگوریتم های PQC با استفاده از Machine Learning
 - تشخیص ناهنجاری در ترافیک رمزنگاری شده پساکوانتومی
 - استفاده از AI برای مدیریت Crypto-Agility
 - طراحی سامانه های AI-assisted PQC Security Assessment
- تجهیزات و سامانه های IoT پساکوانتومی
 - طراحی Lightweight PQC برای IoT
 - پیاده سازی PQC روی Microcontroller های محدودمنبع
 - ارزیابی مصرف انرژی الگوریتم های PQC در IoT
 - طراحی Post-Quantum Secure Boot
 - ایمن سازی ارتباطات Wireless IoT با PQC
 - بررسی PQC در شبکه های 5G/6G IoT
 - طراحی پروتکل های PQC برای تجهیزات پزشکی متصل
 - طراحی معماری Post-Quantum IoT Security
- سخت افزار و شتاب دهنده های پساکوانتومی
 - طراحی شتاب دهنده سخت افزاری ML-KEM
 - طراحی شتاب دهنده سخت افزاری ML-DSA
 - پیاده سازی PQC روی FPGA
 - طراحی ASIC برای الگوریتم های PQC
 - پیاده سازی PQC روی SoC
 - طراحی PQC Co-Processor
 - استفاده از GPU برای شتاب دهی محاسبات PQC
 - بهینه سازی مصرف توان شتاب دهنده های PQC
 - طراحی شتاب دهنده های مقاوم در برابر Side-Channel

- مقایسه معماری‌های FPGA/ASIC/GPU/SoC برای PQC
- ماهواره و ارتباطات پساکوانتومی
 - طراحی معماری Post-Quantum Secure Satellite Communication
 - شبیه‌سازی ارتباطات ماهواره‌ای مبتنی بر PQC
 - استفاده از PQC برای ایمن‌سازی Satellite-to-Ground Communication
 - استفاده از PQC برای ایمن‌سازی Inter-Satellite Links
 - طراحی احراز هویت پساکوانتومی در شبکه‌های ماهواره‌ای
 - بررسی اثر تأخیر زیاد ماهواره بر پروتکل‌های PQC
 - بهینه‌سازی حجم پیام‌های PQC در لینک‌های ماهواره‌ای
 - بهینه‌سازی Performance الگوریتم‌های PQC در کانال‌های ماهواره‌ای
 - طراحی Post-Quantum Secure Satellite Network
 - طراحی معماری ترکیبی (Hybrid Cryptography) Classical + PQC برای ارتباطات ماهواره‌ای
 - طراحی سازوکار Crypto-Agility در ماهواره‌ها

۳) رایانش کوانتومی

- ارایه خدمات شبیه‌سازی الگوریتم‌های کوانتومی بر بستر ابر (QCaaS)
 - طراحی و پیاده‌سازی سامانه مدیریت صف و ارکستراسیون برای اجرای الگوریتم‌های کوانتومی بر بستر ابر
 - توسعه یک محیط یکپارچه تحت وب برای طراحی و شبیه‌سازی مدارهای کوانتومی بر بستر ابر
 - پیاده‌سازی یک چارچوب جامع برای احراز هویت و کنترل دسترسی سرویس کوانتومی بر بستر ابر
 - طراحی و پیاده‌سازی سامانه پایش و مانیتورینگ مصرف منابع ابری در یک سرویس رایانش کوانتومی
 - یکپارچه‌سازی و ارائه سرویس شبیه‌سازی کوانتومی مبتنی بر فریم‌ورک Qiskit در یک بستر ابری
- طراحی و اقدامات لازم در راستای احداث آزمایشگاه توسعه رایانش کوانتومی
 - بررسی و ارزیابی فناوری‌های مختلف کیوبیت از منظر قابلیت ساخت و توسعه در ایران
 - طراحی سند راهبرد فناوری و معماری کلان آزمایشگاه ملی رایانش کوانتومی
 - طراحی و شبیه‌سازی سیستم یکپارچه کنترل و خوانش برای یک پلتفرم کیوبیت مشخص
 - مدیریت و یکپارچه‌سازی پروژه طراحی و راه‌اندازی آزمایشگاه کوانتومی
 - مطالعه و انتقال دانش فنی راه‌اندازی و بهره‌برداری از یک آزمایشگاه کوانتومی عملیاتی
 - مطالعه و بررسی ایجاد مجموعه دادگان کوانتومی جهت به کار گیری QAI در سکتورهای مختلف صنعتی

۴) امنیت اینترنت اشیا (IoT)، فناوری عملیاتی (OT) و زیرساخت‌های ارتباطی

- امنیت اینترنت اشیا (IoT Security)
 - امنیت تجهیزات و سخت‌افزار
 - امنیت سیستم‌عامل، ثابت‌افزار و میان‌افزار
 - امنیت ارتباطات، پروتکل‌ها و معماری IoT
 - امنیت پلتفرم، رایانش ابری و لبه
 - هویت، احراز اصالت و مدیریت دسترسی
 - رمزنگاری، حفاظت از داده و حریم خصوصی
 - پایش، تشخیص تهدید و پاسخ به رخداد

- امنیت چرخه عمر، به روزرسانی و زنجیره تأمین
- امنیت کاربردهای تخصصی IoT
- امنیت فناوری عملیاتی (OT Security)
 - امنیت سامانه‌ها و تجهیزات کنترل صنعتی
 - پایش، تشخیص، پاسخ و بازایی
 - امنیت شبکه‌ها، پروتکل‌ها و معماری صنعتی
 - مدیریت هویت، دسترسی و اعتماد
 - تاب‌آوری، ایمنی و مدیریت ریسک سایبری-فیزیکی
 - امنیت زنجیره تأمین، به روزرسانی و چرخه عمر تجهیزات
 - فناوری‌های نوین مانند هوش مصنوعی، دوقلوی دیجیتال، محاسبات لبه و روش‌های نوین رمزنگاری در امنیت OT
- امنیت زیرساخت‌های ارتباطی
 - امنیت شبکه‌های ثابت و سیار
 - امنیت شبکه‌های انتقال و دیتا در بخش دسترسی و هسته
 - امنیت شبکه‌های نرم‌افزارمحور و مجازی‌شده
 - امنیت مسیریابی، نام‌گذاری و خدمات پایه شبکه
 - امنیت مدیریت، اراکستراسیون و کنترل شبکه
 - پایش، تشخیص و پاسخ به تهدیدات شبکه
 - تاب‌آوری، تداوم خدمت و مقابله با حملات منع خدمت
 - امنیت تجهیزات و زنجیره تأمین ارتباطی

۵) هوش مصنوعی

- توسعه دادگان آموزشی، بنچمارک‌ها و چارچوب‌های ارزیابی برای مدل‌های زبانی بزرگ فارسی
 - طراحی و پیاده‌سازی پایپ‌لاین بومی جمع‌آوری، پالایش و اعتبارسنجی داده‌های آموزشی و ارزیابی برای مدل‌های زبانی بزرگ فارسی
 - ایجاد داده‌های آموزشی کنترل‌شده برای بهبود استدلال زنجیره‌ای در مدل‌های زبانی بزرگ فارسی
 - تولید و اعتبارسنجی داده‌های آموزشی مصنوعی برای خودآموزی کنترل‌شده (Controlled Self-Training) مدل‌های زبانی بزرگ فارسی
 - ایجاد بنچمارک استدلال چندمرحله‌ای برای ارزیابی مدل‌های زبانی بزرگ فارسی
 - ایجاد زیرساخت و بنچمارک جامع ارزیابی ایمنی، هم‌ترازی، استحکام، و اعتمادپذیری در مدل‌های زبانی بزرگ فارسی
 - ایجاد زیرساخت و بنچمارک ارزیابی مدل‌های زبانی مبتنی بر بازایی اطلاعات در حوزه‌های دانشی حساس (سلامت، مالی، حقوقی، ...) فارسی
- توسعه دادگان، بنچمارک و روش‌های ارزیابی سامانه‌های هوشمند احراز هویت
 - تهیه و اعتبارسنجی بنچمارک ارزیابی سامانه‌های تشخیص و تطبیق چهره در شرایط مختلف تصویربرداری
 - تهیه و اعتبارسنجی بنچمارک ارزیابی سامانه‌های تشخیص و تطبیق اثر انگشت
 - تهیه و اعتبارسنجی بنچمارک ارزیابی سامانه‌های تشخیص و تطبیق گوینده در شرایط مختلف صوتی
 - طراحی و پیاده‌سازی روش‌ها و سناریوهای آزمون برای ارزیابی دقت و استحکام سامانه‌های احراز هویت بیومتریک

- بررسی و ارزیابی مقاومت سامانه‌های احراز هویت چهره در برابر حملات جعل و ارائه تصویر و ویدئو
 - بررسی سوگیری و تفاوت عملکرد سامانه‌های احراز هویت بیومتریک در شرایط و گروه‌های مختلف
 - توسعه و ارزیابی روش‌های احراز هویت چندوجهی با ترکیب اطلاعات چهره، صدا یا اثر انگشت
 - طرح توسعه سرویس‌های بومی و اولویت‌دار بازارگاه هوش مصنوعی پژوهشگاه ارتباطات و فناوری اطلاعات
 - طراحی و پیاده‌سازی سرویس بومی پردازش و تحلیل زبان فارسی مبتنی بر مدل‌های یادگیری عمیق
 - توسعه سرویس تشخیص و تحلیل هوشمند تصاویر بومی در کاربردهای حاکمیتی
 - طراحی سرویس بومی تبدیل گفتار به متن و متن به گفتار فارسی
 - توسعه سرویس هوشمند تحلیل داده و پیش‌بینی مبتنی بر یادگیری ماشین
 - طراحی و پیاده‌سازی سرویس بومی تشخیص تقلب و ناهنجاری مبتنی بر هوش مصنوعی
 - خودران‌سازی در محیط‌های شبیه‌سازی شده
 - تولید داده‌های شبیه‌سازی شهری با استفاده از محیط AirSim
 - درک معنایی محیط و تشخیص موانع پویا با استفاده از یادگیری عمیق (Semantic Segmentation & Object Detection)
 - پیاده‌سازی عامل تبدیل داده‌های شبیه‌سازی (Sim) به داده‌های نزدیک به واقعیت (Real)
 - شبیه‌سازی اغتشاشات جوی و بادهای برشی (Wind Shear) برای ارزیابی پایداری ربات‌های هوایی در ارتفاع پایین
 - مدل‌سازی خودرانی برای پرند خودران در محیط‌های شهری شبیه‌سازی شده
- قابل ذکر است، در خصوص سایر موضوعات ارسالی، تنها مواردی که ذیل یکی از محورهای اصلی تدوین شده باشند، قابل بررسی و ارزیابی هستند.

پایان