



نام و نام خانوادگی : **علیرضا شفیعی نژاد**

سال تولد : ۱۳۵۶

۱. مشغول به کار:

استادیار دانشکده برق و کامپیوتر، دانشگاه تربیت مدرس، مهر ۹۴ - تاکنون

مدیرعامل، شرکت مهندسی پدیدآوران نرم افزار آپادانا، مهر ۹۱-مهر ۹۴، مهر ۹۷ - تاکنون

۲. تحصیلات :

مدرک تحصیلی	رشته تحصیلی	محل تحصیل	تاریخ
دکتری	مهندسی برق مخابرات-شبکه	دانشگاه صنعتی اصفهان	۱۳۸۵-۱۳۹۱
کارشناسی ارشد	معماری سیستمهای کامپیوتری	دانشگاه صنعتی اصفهان	۱۳۷۸-۱۳۸۱
کارشناسی	مهندسی کامپیوتر-سخت افزار	دانشگاه صنعتی شریف	۱۳۷۴-۱۳۷۸

۳. زمینه های تحقیقاتی :

- رایانش ابری امن (رمزنگاری و ویژگی مبنا و زنجیره قالبها)
- امنیت سخت افزار با روشهای واریسی مدل (کشف تروجان)
- شبکه های نسل پنجم و ششم موبایل (بازطراحی با زنجیره قالبها)
- کشف آسیب پذیری و تشخیص بد افزار با روشهای یادگیری ماشین
- مسیریابی حرکت پهپاد در شبکه های اینترنت اشیا

۴. تألیف و تحقیق:

پایان نامه‌ها

۱) علیرضا شفیعی نژاد، کدینگ شبکه برای مسیریابی تک بخشی در شبکه‌های بی‌سیم چندکاناله-چندواسطه، رساله دکترا، دانشگاه صنعتی اصفهان، بهمن ماه ۱۳۹۱

نکته ۱: دفاع با نمره عالی

نکته ۲: قرار گرفتن جزء پایان‌نامه‌های برتر و نوآور و کسب جایزه مرکز تحقیقات مخابرات

۲) علیرضا شفیعی نژاد، تحلیل رمزنگار قالبی *FDE* و پیاده‌سازی سریع آن در نرم‌افزار، پایان نامه کارشناسی ارشد، دانشگاه صنعتی اصفهان، تیرماه ۱۳۸۱

۳) علیرضا شفیعی نژاد، طراحی و پیاده‌سازی پایانه *WYSE*، دانشگاه صنعتی شریف، پایان نامه کارشناسی، اسفند ۱۳۷۸

مقاله‌ها (ژورنال):

3) *A Shafieinejad, M Almasian, Secure Cloud File Sharing Scheme Using Blockchain and Attribute-Based Encryption, Accepted for publication in Elsevier Computer Standard and Interface, 2023*

4) *Sajjad Palanki; Alireza Shafieinejad, Attribute-Based Encryption with Efficient Attribute Revocation, Decryption Outsourcing, and Multi-Keyword Searching in Cloud Storage, The ISC International Journal of Information Security (ISecure), Vol. 4, No.3, October 2022, Pages 135-149, 5)*

5) *M Hojjati, A Shafieinejad, H Yanikomeroğlu, A blockchain-based authentication and key agreement (AKA) protocol for 5G networks, IEEE Access 8, 216461-216476, 2020*

۴) محمد پیام الماسیان، علیرضا شفیعی نژاد و مهدی سجادیه، "چارچوب کنترل دسترسی مبتنی بر بلاک‌چین و رمزنگاری ویژگی *MP Almasian, A Shafieinejad, A Blockchain* (7مین)، فصلنامه صنایع الکترونیک ایران، فروردین ۱۳۹۹

8) *A. Shafieinejad and F. Hendessi, "Analysis of Inter-flow Network Coding in Lossy Wireless Networks", The Modares Journal of Electrical Engineering, 16(2), pp.62-71 (2016)*

9) *A. Shafieinejad, N. Motamedi, F. Hendessi and M. Mahdavi, "INCP: Practical Wireless Network Coding for Multiple Unicast Sessions". Springer Wireless Personal Communications, 91(2), pp.623-651 (2016)*

10) *A. Shafieinejad, F. Hendessi and F. Fekri, "Network Coding for multiple unicast sessions in wireless networks", Springer Wireless Networks, Vo. 19, No. 5, pp. 891-911 (2013)*

11) *A. Shafieinejad, F. Hendessi and F. Fekri, "Star Structure etwork Coding for multiple unicast sessions in wireless mesh networks", Springer Wireless personal communications, 72(4), 2185-2214*

12) *A. Shafieinejad, F. Hendessi and T. A. Gulliver, "A Structure for Fast Data*

Encryption”, *International Journal of Contemp. Math. Sciences*, Vol. 2, 2007, no. 29, 1401 – 1424

13) **A. Shafieinejad, F. Hendessi and T. A. Gulliver**, “**On the Security and performance of the FDE block cipher**”, *Contemporary Engineering Sciences*, July 2009, no. 5, 209-238

مقالات منتشر شده در کنفرانس ها :

14) **M. Fouladian, F. Hendessi, A. Shafieinejad**, “**A New Vertical Handoff Method for 3G/WLAN Networks**”, *Proceeding of ICACC 2009, International Conference on Advanced Computer Control Singapore January 22-24, 2009, Singapore Institute of Electronics*

15) **M.Fouladian, F. Hendessi, A. Shafieinejad**, “**A New Method for Vertical Handoff between WLANs and UMTS in Boundary Conditions**”, *Proceeding of ICCET 2009, International Conference on Computer Engineering and Technology, Singapore Institute of Electronics*

16) **Shafieinezhad A, Hendessi F, N.Azmi**, “**Security of FDE against Differential and Linear attacks**”, *ISCC 2007, Oct 2007*

۱۷) ع.فانیان، م. برنجکوب و ع. شفیعی نژاد، "ارائه‌ی یک مدل جدید برای امن‌سازی کاربردهای تحت بر وب"، سومین همایش امنیت اطلاعات و جنگ الکترونیک، آبان‌ماه ۱۳۸۵

18) **Shafieinezhad A, Hendessi F**, “**Fast C-Implementation of FDE in Software**”, *ISCC’2003 (The 2th Iranian Society of Cryptology Conference on Cryptology, Comunicatons & Computer Security), Oct 2003, pp 11-25*

۱۹) ع. شفیعی نژاد و ف. هندسی، "بررسی شبه‌تصادفی بودن *FDE* با آزمونهای آماری"، مجموعه مقالات دومین کنفرانس انجمن رمز ایران، مهر ماه ۱۳۸۳

۲۰) ع. شفیعی نژاد، ف. هندسی و م. اسماعیلی، "تکمیل ساختار *FDE* با طراحی *Sbox* های قوی"، مجموعه مقالات یازدهمین کنفرانس برق ایران، اردیبهشت ماه ۱۳۸۲

۲۱) ع. شفیعی نژاد، ف. هندسی و م. اسماعیلی "پیاپی‌سازی سریع *FDE* به روش *Bitslicing*"، مجموعه مقالات هفتمین کنفرانس کامپیوتر ایران، اسفند ۱۳۸۰

۴. سوابق اجرایی

محل کار	پروژه	سمت	زمان
دانشگاه تربیت مدرس	بازطراحی شبکه زیرساخت فیبر نوری ارتقا مرکز پردازش سریع با افزودن سرویس <i>GPU</i> بازطراحی پورتال بازطراحی امنیت شبکه دانشگاه راه اندازی سرویسهای یادگیری الکترونیکی و آموزش راه دور	مدیر	اسفند ۹۶ - مهر ۱۴۰۱
دانشگاه تربیت مدرس	مدیر مرکز پژوهشی امن اندیشان با همکاری شرکت صافتا	مدیر	اصفند ۹۷ - تاکنون
شرکت مهندسی پدید آوران نرم افزار		مدیرعامل	مهر ۹۷ - تاکنون

مهر ۹۷	همکار	برگزاری دوره های ارزیابی امنیتی و کدنویسی امن برای کارشناسان وزارت دفاع	دانشگاه تربیت مدرس
۹۵-۸۹	مدیر پروژه	ساخت رمز کننده بومی شبکه (لایه دوم و سوم) (<i>net-to-net VPN</i>)	شرکت مهندسی پدید آوران نرم افزار
۹۲-۹۱	مدیر پروژه	ارزیابی امنیتی سامانه کارت هوشمند سلامت	شرکت مهندسی پدید آوران نرم افزار
۹۳-۹۰	همکار	ساخت <i>UTM</i> بومی	شرکت مهندسی پدید آوران نرم افزار
۸۹	مدیر پروژه	تهیه <i>RFP</i> برای زیر ساخت کلید عمومی	شرکت مهندسی پدید آوران نرم افزار
۸۸-۸۹	همکار پروژه	ارزیابی پروتکل های احراز اصالت	دانشگاه صنعتی اصفهان
۸۸-۸۷	مدیر پروژه	طراحی و پیاده سازی شتاب دهنده رمزنگاری سخت افزاری مبتنی بر <i>PCI-Express</i>	شرکت مهندسی پیام پرداز
۸۷-۸۴	مسوول فنی	طراحی و پیاده سازی سامانه امن ساز شبکه کیهان	شرکت مهندسی پیام پرداز

۵. موفقیت های تحصیلی، علمی و اجتماعی:

تاریخ و محل	شرح	نوع موفقیت
تابستان ۱۳۹۵	مجله علمی-پژوهشی دانشکده برق دانشگاه تربیت مدرس با موضوع "رمزنگاری و امنیت شبکه"	مسوول ویرایش نسخه ویژه
۱۳۹۱-دانشگاه صنعتی اصفهان	کسب جایزه مرکز تحقیقات مخابرات برای رساله دکترا	رساله برتر و نوآور
۱۳۷۴	عضو بنیاد ملی نخبگان	نخبه کشوری
۱۳۷۸	کنکور کارشناسی ارشد	رتبه ۴۲
۱۳۷۳ دانشگاه فردوسی مشهد	مدال برنز مرحله کشوری - نفر اول مرحله استانی	المپیاد ریاضی

۶. تدریس:

محل تدریس	عنوان درس	مقطع تدریس	ترم شروع
دانشگاه تربیت مدرس	رمزنگاری کاربردی	کارشناسی ارشد - رایانش امن	۹۳ تا کنون (نیمسالهای فرد)
دانشگاه تربیت مدرس	توسعه امن نرم افزار	کارشناسی ارشد - رایانش امن	۹۳ تا کنون (نیمسالهای زوج)
دانشگاه تربیت مدرس	معماری کامپیوتر پیشرفته	کارشناسی ارشد - معماری	نیمسال اول ۹۵-۹۶
دانشگاه تربیت مدرس	سنتز مدارهای دیجیتال	کارشناسی ارشد - معماری	نیمسال دوم ۹۵-۹۶
دانشگاه تربیت مدرس	طراحی پردازنده های خاص شبکه	کارشناسی ارشد - معماری	نیمسال دوم ۹۵-۹۶
دانشگاه صنعتی اصفهان	شبکه های کامپیوتری	کارشناسی	نیمسال دوم ۹۱-۹۲
دانشگاه صنعتی اصفهان	ساختمان داده ها	کارشناسی	نیمسال اول ۸۹-۸۸

نیمسال اول ۸۸-۸۹	کارشناسی	مبانی برنامه نویسی به ++C	دانشگاه صنعتی اصفهان
نیمسال دوم ۸۸-۸۹	کارشناسی	فناوری اطلاعات	دانشگاه صنعتی اصفهان