بسمه تعالی

سوابق علمی- پژوهشی

سید مهدی سجادیه ، دانشجوی دکترای مهندسی برق

نام و نام خانوادگی: سید مهدی سجادیه

محل تحصیل: ایران، اصفهان، دانشگاه صنعتی اصفهان، دانشکده برق و کامپیوتر، آزمایشگاه تحقیقاتی رمزنگاری و امنیت سیستم‌ها

سوابق تحصیلی:

(۱۳۷۴-۱۳۷۸) : دبیرستان مرکز پرورش استعدادهای درخشان، واحد اصفهان، رشته ریاضی

(۱۳۷۸-۱۳۸۲) : کارشناسی مهندسی برق، گرایش الکترونیک، دانشگاه صنعتی اصفهان

(۱۳۸۲-۱۳۸۵) : کارشناسی ارشد مهندسی برق، گرایش مخابرات سیستم، دانشگاه صنعتی اصفهان

(مهر ۱۳۸۵) : دکترای مهندسی برق، گرایش، دانشگاه صنعتی اصفهان

افتخارات علمی:

کسب رتبه ۳۷۴ در آزمون سراسری سال ۱۳۷۸ در رشته ریاضی-فیزیک

کسب رتبه ۱۶۲ در آزمون کارشناسی ارشد سال ۱۳۸۲

زمینه تحقیقاتی:

رمزنگاری، طراحی و تحلیل رمزهای قالبی، طراحی و تحلیل رمزهای دنباله‌ای ،آشنایی با سیستم‌های رمز کلید عمومی، کدینگ کانال

دروس گذرانده در دوره کارشناسی ارشد و دکترا:

- فرآیندهای تصادفی
- کدینگ کانال
- پردازش سیگنال‌های دیجیتال
- تئوری پیشرفته مخابرات

- رمزنگاری
- پردازش سیگنال‌های دیجیتال پیشرفته (تبدیل موجک)
- امنیت شبکه
- تئوری اطلاعات و کدینگ منبع
- تئوری گراف
- تئوری بازی
- سیستم‌های رادار
- شناسایی آماری الگو
- ریاضی مهندسی پیشرفته
- رادیوی نرم‌افزاری (software defined radio)
- رمزنگاری پیشرفته (خم بیضوی و تحلیل رمزهای قالبی)

پروژه‌های تحقیقاتی درسی:

- تولید اعداد تصادفی (برای درس تئوری اطلاعات)
- پیاده سازی Turbo Code(درس کدینگ کانال)
- پروتکل‌های تبادل کلید (درس رمزنگاری)
- کاربرد تئوری گراف در تئوری اطلاعات (درس تئوری گراف)
- تئوری بازی و رادیوی هوشمند (درس رادیو نرم‌افزاری)
- حمله جبری، حمله همبستگی، حمله زمان حافظه (درس رمزنگاری پیشرفته)

پروژه‌های انجام شده:

- بررسی الگوریتم‌های دنباله‌ای جدید و حملات مهم (دانشگاه صنعتی اصفهان_صافاوا)
- بررسی الگوریتم‌های قالبی جدید و حملات مهم (دانشگاه صنعتی اصفهان_صافاوا)

پروژه کارشناسی ارشد:

حملهٔ جبری علیه سیستم‌های رمز دنباله‌ای

استاد راهنما : دکتر محمود مدرس هاشمی استاد مشاور: دکتر محمد دخیل‌علیان

سخنرانی دعوتی:

"بررسی حملات علیه A5/1"، دانشگاه صنعتی اصفهان، اسفند ۱۳۸۶.

بررسی حملات علیه A5/1"، دانشگاه صنعتی شریف، خرداد ۱۳۸۷.

مقالات:

م. سجادیه، م. مدرس هاشمی" روشی برای شمار ش تعداد معادلات افزوده شده در روش خطی سازی تکراری برای سیستمهای رمز دنباله ای" سومین کنفرانس رمز ایران ۱۳۸۴ دانشگاه صنعتی اصفهان

۲)م.مزروعی،م.سجادیه،ع.شهرکی،م اخوان"بررسی نگاشتهای کاهش نمونه در آشکاری سازی رادار"شانزدهمین کنفرانس برق ایران ۱۳۸۶ مرکز مخابرات ایران

۳)م.سجادیه، م. دخیل علیان،و.نحوی" بررسی اثر نویز در حملات علیه سیستمهای رمز دنباله ای"چهارمین کنفرانس رمز ایران ۱۳۸۶ دانشگاه علم و صنعت

4-M.sheikh,A.fanian,M.sajadieh,P.khadivi,M.berenjkub"A Distributed certificate authority and key establishment protocol for mobile ad hoc network" ICACT2008,korea.

5-M.sheikh,A.fanian,M.sajadieh,P.khadivi,M.berenjkub"A cluster based key establishment protocol for wireless mobile ad hoc networks" CSICC2008,iran.kish

۶-م.سجادیه، م مدرس هاشمی"مقایسهٔ امنیت سیستم رمز نگار دنباله‌ای BSRA و مولد جمعی از لحاظ حملهٔ جبری"پنجمین کنفرانس رمز ایران ۱۳۸۷دانشگاه صنعتی مالک اشتر

7- H.Mala,M.Dakhilalian,M.Sajadieh,"Provable security for a 4 blocked unbalanced Feistel Structure against differential cryptanalysis"iscisc2008

سابقهٔ تدریس

- دانشگاه صنعتی اصفهان (بهمن۸۲ تا کنون)

  آزمایشگاه‌های مدار۱، منطقی، الکترونیک۲، پالس، مخابرات دیجیتال و مدارهای مخابراتی
- دانشگاه آزاد اسامی واحد خوراسگان (بهمن۸۵ تا کنون)

  دروس مدار۱، ریاضی مهندسی، احتمال مهندسی، تجزیه و تحلیل سیستم‌ها و تکنیک پالس