به نام خدا

# سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه


# رمزنگاری کاملاً همریخت مبتنی بر مشبکه‌ها

## Fully Homomorphic Encryption Using Ideal Lattices

**دکتر سید مهدی سجادیه**

زمان: شنبه ۳۱ خرداد ماه ۱۳۹۳ ساعت ۳ عصر

مکان: دانشکده مهندسی کامپیوتر دانشگاه صنعتی شریف، طبقه چهارم، سالن ۴۰۴

یکی از آرزوهای محققان در زمینه رمزنگاری، توانایی در انجام محاسبات دلخواه و جستجو بر روی داده‌های رمزی بوده است. مسأله انجام محاسبات بر روی داده‌های رمزی سال‌ها به عنوان یک مسأله باز مهم مطرح بوده تا این که در سال ۲۰۰۹ سیستم رمزنگاری کاملاً همریخت به عنوان یک راه کار برای این مسأله ارائه شد. علاوه بر محاسبات ابری از دیگر کاربردهای این روش می‌توان به جستجوی‌های امن اینترنتی اشاره نمود.

در این سمینار ابتدا مفاهیم اولیه و کاربردهای رمزهای همریخت معرفی می‌شود و سپس به بررسی روش رمز همریخت مبتنی بر اعداد صحیح اشاره شده، و در نهایت رمز همریخت مبتنی بر مشبکه‌ها معرفی می‌شود.

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.

# سوابق علمی- پژوهشی

## سید مهدی سجادیه ، 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

محل کار: ایران، اصفهان، دانشگاه آزاد اسلامی واحد خوراسگان (اصفهان)، گروه برق الکترونیک

تلفن: ۰۳۱۱-۵۳۵۴۰۰۱

پست الکترونیکی: mahdisajadieh@yahoo.com , m.sajadieh@khuisf.ac.ir

## 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

(۱۳۸۵-۱۳۹۱) : 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 ،امنیت شبکه، امنیت نرم‌افزار، آشنایی با سیستم‌های رمز کلید عمومی، کدینگ کانال

## 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)
- همکاری با شرکت پیام پرداز از سال ۸۲ تاکنون

## پروژه کارشناسی ارشد:

حملهٔ جبری علیه سیستم‌های رمز دنباله‌ای

استاد راهنما : دکتر محمود مدرس هاشمی

## پروژه دکترا:

بررسی روش‌های طراحی تبدیل انتشار در رمزهای قالبی نوین

استاد راهنما : 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:

## مجله‌ها:

1- M.Sajadieh,M.Dakhilalian, H.Mala, , Behnaz Omoomi " On Construction of Involutory MDS Matrices from Vandermonde Matrices in GF($2^q$) " Design Codes and Cryptography 2011.

2- M.Sajadieh,M.Dakhilalian, H.Mala "Perfect Involutory Diffusion Layers Based on Invertibility of Some Linear Functions "iet information security 2011

3) M.Sajadieh,M.Dakhilalian,H.Mala,P.Sepehrdad "Perfect Recursive Diffusion Layers for Block Ciphers and Hash Functions." Journal of Cryptology 2013.

## کنفرانس‌ها

1) M.Sajadieh,M.Dakhilalian,H.Mala,P.Sepehrdad "Recursive Diffusion Layers for Block Ciphers and Hash Functions." FSE 2012: United States. (The best paper of FSE)

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

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

۹) ح.ملا، م.دخیل علیان، م.سجادیه"محاسبه دقیق وزن ورودی – خروجی برای ماتریس‌های MDS ابعاد ۴*۴ " هفتمین کنفرانس رمز ایران ۱۳۸۸ دانشگاه اصفهان

۱۰) م.ح.سجادیه، ح. خالقی ، م سجادیه "پیشنهادی برای افزایش امنیت تابع درهم ساز JH" دهمین کنفرانس رمز ایران ۱۳۹۱ دانشگاه تبریز

۱۱) م.یادگاری، م سجادیه، ع.زاغیان "یک طرح امضای کور هویت گرا مبتنی بر زوج نگار دو خطی" یازدهمین کنفرانس رمز ایران ۱۳۹۲ دانشگاه یزد

۱۲) م.مزروعی، ح. سعیدی، م. سجادیه، م. اخوان صراف "طراحی و تحلیل آشکار ساز اهداف بهبود بر اساس فاکتور بهبود" پانزدهمین کنفرانس برق ایران ۱۳۸۷.