بسمه تعالی

سوابق علمی و اجرایی

۱۳۹۹/۱۰/۲۵

مصطفی زارع خورمیزی

دانشگاه دامغان، دانشکدهٔ ریاضی و علوم کامپیوتر

تلفن: ۰۲۳۳۵۲۲۰۰۹۲

فکس: ۰۲۳۳۵۲۲۰۰۹۲

ایمیل: mostafazaare@du.ac.ir

سوابق تحصیلی

۱۳۸۳–۱۳۸۸	دکتری، منطق ریاضی، دانشگاه شهید بهشتی، تهران
۱۳۸۱–۱۳۸۳	کارشناسی ارشد، ریاضی محض، دانشگاه صنعتی اصفهان
۱۳۷۷–۱۳۸۱	کارشناسی، ریاضی محض، دانشگاه صنعتی اصفهان

رسالهٔ دکتری

عنوان	توسعهٔ نظریهٔ مدل‌های کریپکی منطق مرتبهٔ اول شهودی
استاد راهنما	دکتر مرتضی منیری

پایان‌نامه کارشناسی ارشد

عنوان	قواعد پذیرفتنی منطق شهودی گزاره‌ای
استاد راهنما	دکتر مجتبی آقایی

سوابق شغلی

مهر ۱۳۸۸ تا کنون	استادیار دانشکده ریاضی و علوم کامپیوتر دانشگاه دامغان
دی ۱۳۹۶ تا کنون	رئیس گروه نظارت، ارزیابی و تضمین کیفیت دانشگاه دامغان
آبان ۱۳۹۲ تا مهر ۱۳۹۳	مدیر برنامه‌ریزی فرهنگی و اجتماعی دانشگاه دامغان
آبان ۱۳۹۰ تا مهر ۱۳۹۲	مدیر امور فرهنگی دانشگاه دامغان

علایق پژوهشی

- رمزنگاری: تحلیل الگوریتم‌ها و پروتکل‌های رمزنگاری، رمزنگاری کوانتومی، رمزهای پساکوانتومی، امنیت شبکه
- منطق ریاضی: منطق شهودی، منطق شناختی، منطق کوانتومی
- نظریهٔ محاسبه، نظریهٔ پیچیدگی

مقالات مجله

- “Elementary Extensions of Kripke models”, Preprint.
- “An intuitionistic analogue of the Keisler sandwich theorem”, Preprint.
- With M. Moniri, “Fragments of epistemic and intuitionistic arithmetic”, Preprint.
- With F. Gorji, “A differential fault attack on the LED lightweight block cipher”, Submitted.
- With M. Abiri and M. Moniri, “Forcing and satisfaction in Kripke models of intuitionistic arithmetic”, To appear in *Logic Journal of the IGPL*.

- With M. Abiri and M. Moniri, “From forcing to satisfaction in Kripke models of intuitionistic predicate logic”, *Logic Journal of the IGPL*, Volume 26, Issue 5, 464–474, 2018.
- Extensions of Kripke models, *Logic Journal of the IGPL*, Volume 25, No. 5, 697-699, 2017.
- With M. Moniri, Homomorphisms and chains of Kripke models, Archive for Mathematical Logic, Vol. 50, 431-443, 2011.
- With M. Moniri, Preservation theorems for Kripke models, Mathematical Logic Quarterly, Vol. 55, 177-184, 2009.
- درستی‌یابی پروتکل‌های رمزنگاری با استفاده از برنامه‌سازی منطق، مجله علمی ـ پژوهشی «پدافند الکترونیکی و سایبری»، ویژه‌نامه اولین کنفرانس بین‌المللی ترکیبیات، رمزنگاری و محاسبات، دانشگاه امام حسین (ع)، شماره ۱، ۱۳۹۶

مقالات کنفرانس

- فرس به صدق در مدل‌های کریپکی منطق محمولات شهودی، مشترک با مرتضی منیری و مریم عبیری، چهل و نهمین کنفرانس ریاضی ایران، دانشگاه علم و صنعت ایران، ۱–۴ شهریور ۱۳۹۷
- حمله‌ی خطای تفاضلی به طرح کلید رمز PRESENT، مشترک با فرشاد گرجی، دومین کنفرانس ملی ترکیبیات، رمزنگاری و محاسبات، دانشگاه علم و صنعت ایران، ۱۶ و ۱۷ آذر ۱۳۹۶
- تروژان‌های سخت‌افزاری MAPLE، مشترک با سیدهاشم طبسی و فاطمه قربان‌پور، چهارمین کنفرانس ملی و دومین کنفرانس بین‌المللی پژوهش‌های کاربردی در مهندسی برق، مکانیک و مکاترونیک، دانشگاه صنعتی مالک اشتر، ۲۹ بهمن ۱۳۹۵
- حمله خطای چند مرحله‌ای به PRINCE، مشترک با سیدهاشم طبسی و فاطمه ولادتی، چهارمین کنفرانس ملی و دومین کنفرانس بین‌المللی پژوهش‌های کاربردی در مهندسی برق، مکانیک و مکاترونیک، دانشگاه صنعتی مالک اشتر، ۲۹ بهمن ۱۳۹۵
- حمله‌ی خطای تروجان به الگوریتم رمز PRINCE، مشترک با سید هاشم طبسی و فاطمه قربان‌پور، چهارمین کنفرانس بین‌المللی مهندسی برق و کامپیوتر، دانشگاه تهران، ۲۳ دی ۱۳۹۵
- حمله خطای چند مرحله‌ای به LED-128، مشترک با سیدهاشم طبسی و فاطمه ولادتی، چهارمین کنفرانس بین‌المللی مهندسی برق و کامپیوتر، دانشگاه تهران، ۲۳ دی ۱۳۹۵
- درستی‌یابی خودکار پروتکل‌های رمزنگاری با استفاده از برنامه‌سازی منطق، اولین کنفرانس بین‌المللی ترکیبیات، رمزنگاری و محاسبات، دانشگاه علم و صنعت واحد نور، ۱۱ و ۱۲ شهریور ۱۳۹۵
- حمله جبری به AES با استفاده از حل‌کننده‌های SAT، مشترک با سمیه معتمدی، دومین همایش ملی علوم محاسباتی، دانشگاه دامغان، ۷ و ۸ شهریور ۱۳۹۵
- ساندویچ‌های مدل‌های کریپکی، چهل و سومین کنفرانس ریاضی ایران، دانشگاه تبریز، ۹–۶ شهریور ۱۳۹۱
- زیرنظریه‌های حساب شناختی، همایش منطق ریاضی و کاربردهای آن، دانشگاه اصفهان، ۹ و ۱۰ آذر ۱۳۹۰
- زنجیرهای مدل‌های کریپکی، چهل و دومین کنفرانس ریاضی ایران، دانشگاه ولی عصر (عج) رفسنجان، ۱۷–۱۴ شهریور ۱۳۹۰
- مدل‌های کریپکی منطق مرتبهٔ اول شهودی، همایش منطق ریاضی تبریز، دانشگاه تبریز، ۵ و ۶ آبان ۱۳۸۹
- قضایای حفظ برای مدل‌های کریپکی، همایش منطق ریاضی، پژوهشگاه دانش‌های بنیادی، دی ۱۳۸۸
- توسیع‌ها و اجتماع زنجیرهای مدل‌های کریپکی، چهلمین کنفرانس ریاضی ایران، دانشگاه صنعتی شریف، ۲۹–۲۶ مرداد ۱۳۸۸
- Preservation theorems for intuitionistic first-order logic, Logic Colloquium 2009, Sofia University, Bulgaria, July 31-August 5

طرح‌های پژوهشی

- تحلیل خودکار خطی و تفاضلی رمزهای مبتنی بر ARX با استفاده از حل‌کننده‌های SAT، تیر ۱۳۹۷ لغایت دی ۱۳۹۹
- طراحی، تحلیل و پیاده‌سازی حمله‌های خطا به الگوریتم‌های رمزنگاری و حمله‌های جبری منطقی به توابع چکیده‌ساز، مهر ۱۳۹۵ لغایت شهریور ۱۳۹۶
- تحلیل الگوریتم‌ها و پروتکل‌های رمزنگاری کوانتومی، تیر ۱۳۹۲ لغایت شهریور ۱۳۹۴
- نظریهٔ مدل‌های برخی منطق‌های غیرکلاسیک، پژوهشگاه دانش‌های بنیادی، تیر ۱۳۹۰ لغایت خرداد ۱۳۹۱
- ساندویچ‌های مدل‌های کریپکی، بنیاد ملی علم ایران، بهمن ۱۳۸۹ لغایت خرداد ۱۳۹۱
- گسترش نظریهٔ مدل‌های کریپکی، پژوهشگاه دانش‌های بنیادی، تیر ۱۳۸۹ لغایت خرداد ۱۳۹۰

- نتایجی دربارهٔ مدل‌های کریپکی منطق مرتبهٔ اول شهودی، دانشگاه دامغان، خرداد ۱۳۸۹ لغایت آذر ۱۳۸۹
- اجتماع زنجیرهای مدل‌های کریپکی نظریه‌های شهودی، بنیاد ملی علم ایران، تیر ۱۳۸۷ لغایت خرداد ۱۳۸۹

جوایز علمی

- پرداخت هزینهٔ سفر جهت شرکت و ارائه سخنرانی در کنفرانس Logic Colloquium 2009 در شهر صوفیه کشور بلغارستان توسط Association for Symbolic Logic
- لوح تقدیر و بورس تحصیلی به عنوان فارغ التحصیل ممتاز دوره کارشناسی توسط دانشگاه صنعتی اصفهان

سوابق تدریس

کارشناسی ارشد و دکتری:

- رمزنگاری
- نظریه کدها و رمزها
- نظریهٔ علوم کامپیوتر
- الگوریتم‌های پیشرفته
- نظریه اثبات و ریاضیات ساختنی
- مبانی ریاضی در رمزنگاری
- نظریه محاسبه پیشرفته
- الگوریتم و محاسبه
- مباحثی در منطق ریاضی

کارشناسی:

- مبانی علوم ریاضی
- مبانی منطق و نظریه مجموعه‌ها
- نظریه محاسبه
- مقدمه‌ای بر رمزنگاری
- مبانی نظریهٔ محاسبه
- ریاضی عمومی

مهارت‌ها

- C, C++, C#
- Maple
- Prolog
- HTML, CSS, JavaScript
- SAT/SMT Solver

عضویت در انجمن‌های علمی

- انجمن ریاضی ایران
- گروه منطق ریاضی، پژوهشکده ریاضیات، پژوهشگاه دانش‌های بنیادی
- گروه تدوین سرفصل دروس دروه کارشناسی ارشد پدافند غیرعامل (گرایش فناوری اطلاعات و ارتباطات) دانشگاه دامغان با همکاری دانشگاه صنعتی مالک اشتر

پایان‌نامه‌های کارشناسی ارشد راهنمایی شده

- جعفر محمدی، تحلیل خطای ملاقات در میانه غیر ممکن رمز سبک LED، مهر ۱۳۹۹
- میلاد سلاحی، کاربرد کدهای قالبی خطی در رمزنگاری، مهر ۱۳۹۹
- مازیار فراتی، تحلیل خطای تفاضلی رمز قالبی KLEIN ، مهر ۱۳۹۹
- علی حمدی‌پور، بهبود تحلیل خطای تفاضلی رمزهای سبک با ساختار شبکه فایستل توسعه یافته، مهر ۱۳۹۹
- علی ملک‌برمی، تحلیل یک حمله خطای بهینه روی رمز سبک LED-64، بهمن ۱۳۹۸
- هدا صالحی جهرمی، حمله خطای تفاضلی به رمز سبک LBlock، شهریور ۱۳۹۸
- سیدعلی مرتضوی، حمله خطای تفاضلی به AES، مهر ۱۳۹۷
- سیدمحسن احترامی نودهی، حمله خطای تفاضلی به LEA، مهر ۱۳۹۷
- فرشاد گرجی، تحلیل خطای تفاضلی رمزهای قالبی، تیر ۱۳۹۷

- سیدعرفان اسدی، کاربرد تسهیم راز اجتماعی در امنیت رایانش ابری، بهمن ۱۳۹۶
- فاطمه قربان‌پور، حمله‌های القای خطا روی سخت‌افزارهای رمزنگاری، بهمن ۱۳۹۵
- فاطمه ولادتی، حمله‌های خطای چند مرحله‌ای به رمزهای قالبی، بهمن ۱۳۹۵
- مژگان حاجی‌پروانه، تحلیل منطقی توابع درهم‌ساز، بهمن ۱۳۹۵
- سحر هادیان کمرودی، تحلیل جایگشت‌ها در رمزهای شبه AES، بهمن ۱۳۹۵
- سعید خراسانی، کاربرد حل‌کننده‌های SAT در رمزشکنی توابع درهم‌ساز، بهمن ۱۳۹۵
- فرزانه اسماعیلی، یک حمله خطا و خطای جبری به رمز قالبی LED، خرداد ۱۳۹۵
- سیدحسین عبداللهی، پیاده‌سازی مدار دوکیوبیتی کوانتومی، شهریور ۱۳۹۴
- محمدعلی خندان، بررسی پیاده‌سازی فیزیکی گیت CNOT و یک الگوریتم جستجوی کوانتومی برای مسأله 3SAT، بهمن ۱۳۹۳
- عادله مهرافروز، یک الگوریتم اکتشافی کوانتومی برای مسأله فروشنده دوره‌گرد، بهمن ۱۳۹۳
- رضا بابایی، تحلیل پروتکل‌های امنیت با استفاده از منطق AUTLOG، بهمن ۱۳۹۳
- محمد طباخ، تحلیل پروتکل‌های امنیت با استفاده از منطق SVD، بهمن ۱۳۹۳
- فاطمه کاشانی، تحلیل پروتکل‌های امنیت با استفاده از منطق AT، بهمن ۱۳۹۳
- مصطفی شمس‌الدینی‌فرد، تحلیل پروتکل‌های امنیت با استفاده از منطق‌های VO و SVO، آذر ۱۳۹۳
- الهام منجزی، تحلیل پروتکل‌های امنیت با استفاده از منطق GNY، شهریور ۱۳۹۳
- سمیه حیدری سورشجانی، بررسی تصمیم‌پذیری محرمانگی در پروتکل‌های امنیت، بهمن ۱۳۹۲
- نسیم نعمتی، الگوریتمی برای درستی‌یابی محرمانگی در پروتکل‌های امنیت، بهمن ۱۳۹۲
- مرجان میثاق، تحلیل پروتکل‌های امنیت با استفاده از منطق BAN، شهریور ۱۳۹۲
- ملیحه شیوا، بروز رسانی معناشناسی پروتکل‌های امنیت، بهمن ۱۳۹۱
- مهدی بردیده، تحلیل پروتکل‌های امنیت با استفاده از منطق زمانی توزیع شده، شهریور ۱۳۹۱
- حسین کلاته سیفری، درستی‌یابی گمنامی در منطق شناختی، شهریور ۱۳۹۱
- پریسا دلیری حسن‌جانی، قضایای حفظ برای منطق محمولات شهودی، بهمن ۱۳۹۰
- مریم عبیری، نظریه‌های عمومی در منطق مرتبهٔ اول شهودی، شهریور ۱۳۹۰