مجتبی بهرامیان

استادیار

دانشکده: دانشکده علوم ریاضی

گروه: ریاضی محض

سوابق تحصیلی

مقطع تحصیلی	سال اخذ مدرک	رشته و گرایش تحصیلی	دانشگاه
کارشناسی	۱۳۷۸	ریاضی	دانشگاه کاشان
کارشناسی ارشد	۱۳۸۰	ریاضی محض - جبر	دانشگاه صنعتی شریف
دکتری	۱۳۸۹	ریاضی محض - نظریه اعداد	دانشگاه کاشان

سوابق اجرایی

ردیف	نهاد اجرایی	تاریخ شروع	تاریخ پایان
1	عضو شورای فرهنگی دانشکده ریاضی	92/9/25	94/11/25
2	مدیر ارتباطات فرهنگی	94/6/23	95/9/20
3	دبیر شورای بدوی انضباطی	92/8/6	94/9/2
4	رئیس دبیرخانه کمیسیون بررسی موارد خاص	92/8/6	94/9/2

جوایز و تقدیر نامه ها

جوایز و تقدیرنامه‌ها

رتبه اول در بین دانشجویان فارغ‌التحصیل کارشناسی ریاضی دانشگاه کاشان 1378
دانشجوی نمونه دوره کارشناسی ریاضی دانشگاه کاشان
رتبه ممتاز مسابقات دانشجویی ریاضی 1376
رتبه ممتاز مسابقات دانشجویی ریاضی 1377
استاد نمونه آموزشی دانشگاه کاشان در سال 1390

موضوعات تدریس تخصصی

نظریه جبری اعداد، رمزنگاری خم‌های بیضوی

زمینه های تدریس

ریاضی عمومی 1و 2
مبانی ریاضیات
جبر 1و2و3
جبر خطی

نظریه اعداد
آموزش ریاضی
معادلات دیفرانسیل
ریاضی پایه

حساب خم‌های بیضوی
رمزنگاری 1و 2
الگوریتم و محاسبه
مباحث ویژه در رمزنگاری

آنالیز ریاضی 1
نظریه گراف
ریاضی کاربردی
نظریه جبری اعداد

همایش ها و کنفرانس ها

عضو کمیته‌ی اجرایی پنجمین کنفرانس ترکیبیات جبری و نظریه گراف (تیر ۹۱)

عضو کمیته‌ی اجرایی اولین کنفرانس نظریه محاسباتی اعداد و کاربردهای آن (آذر ۹۳)

عضو کمیته‌ی علمی اولین کنفرانس نظریه محاسباتی اعداد و کاربردهای آن (آذر ۹۳)

دبیر اجرایی دومین کنفرانس نظریه محاسباتی اعداد و کاربردهای آن (مهر ۹۴)

عضو کمیته‌ی علمی دومین کنفرانس نظریه محاسباتی اعداد و کاربردهای آن (مهر ۹۴)

دبیر اجرایی پنجاه و یکمین کنفرانس ریاضی ایران (بهمن ۹۹)

عضو کمیته‌ی علمی پنجاه و یکمین کنفرانس ریاضی ایران (بهمن ۹۹)

مقالات در همایش ها

۱. خدیجه اسلامی,مجتبی بهرامیان،A Threshold Multi-Secret Sharing Scheme Based on Shamir's Scheme،اولین کنفرانس بین المللی فناوریهای نوین در علوم،آمل،۲۰۱۷ ۹ ۷.
۲. مجتبی بهرامیان،رمزنگاری امن با خم‌های بیضوی،اولین کنفرانس بین المللی فناوریهای نوین در علوم،آمل،۲۰۱۷ ۹ ۷.
۳. خدیجه اسلامی,مجتبی بهرامیان،An Identity-Based Encryption Based on Pairings over Elliptic Curves،چهل و هشتمین کنفرانس ریاضی ایران،همدان،۲۰۱۷ ۸ ۲۲.
۴. مجتبی بهرامیان،RSA Scheme over the Ring of Gaussian Integers،چهل و هشتمین کنفرانس ریاضی ایران،همدان،۲۰۱۷ ۸ ۲۲.
۵. مجتبی بهرامیان،نظریه گروهها در رمزنگاری،۹-th Iranian Group Theory Conference (IGTC-۲۰۱۷)،کاشان،۲۰۱۷ ۲ ۱.
۶. مجتبی بهرامیان،نظریه گروهها در رمزنگاری،۹-th Iranian Group Theory Conference،کاشان،۲۰۱۷ ۲ ۱.
۷. خدیجه اسلامی,مجتبی بهرامیان،Secret Sharing Scheme،۹-th Iranian Group Theory Conference،کاشان،۲۰۱۷ ۲ ۱.
۸. خدیجه اسلامی,مجتبی بهرامیان،Secret Sharing Scheme،f9th Iranian Group Theory Conferenc،کاشان،۲۰۱۷ ۲ ۱.
۹. مجتبی بهرامیان,خدیجه اسلامی،GENERALIZED JACOBIAN CRYPTOSYSTEMS،First International Conference on Combinatorics, Cryptography and Computation،نور،۲۰۱۶ ۹ ۱.
۱۰. خدیجه اسلامی,مجتبی بهرامیان،Certificate-Based Encryption Scheme،First International Conference on Combinatorics, Cryptography and Computation،نور،۲۰۱۶ ۹ ۱.
۱۱. مجتبی بهرامیان،Jacobian group of Cocktail Party،The Second Conference on Computational Group Theory, Computational Number Theory and Applications،کاشان،۲۰۱۵ ۱۰ ۱۳.
۱۲. مجتبی بهرامیان,مریم شیخی گرجان،An identity-based encryption scheme،The Second Conference on Computational Group Theory, Computational Number Theory and Applications،کاشان،۲۰۱۵ ۱۰ ۱۳.

۱۳. مجتبی بهرامیان،The ۴۵th Annual Computing the Tate Pairing using Generalized Jacobians،Iranian Mathematics Conference،سمنان،۲۰۱۴ ۸ ۲۶.
۱۴. مجتبی بهرامیان,سمیه دیداری,حسن دقیق،The First Conference on Calculus on Elliptic Curves،Computational Group Theory, Computational Number Theory and Applications،کاشان،۲۰۱۴ ۱۲ ۱۷.
۱۵. حسن دقیق,مجتبی بهرامیان،The First Conference Constructing Elliptic Curves for Cryptography،on Computational Group Theory, Computational Number Theory and Applications،کاشان،۲۰۱۴ ۱۲ ۱۷.
۱۶. حسن دقیق,مجتبی بهرامیان,سمیه دیداری،نگاهی به برخی مسائل ریاضی در رمزنگاری،اولین کنفرانس جبر محاسباتی، نظریه محاسباتی اعداد و کاربردها،کاشان،۲۰۱۴ ۱۲ ۱۷.
۱۷. مجتبی بهرامیان,مریم شیخی گرجان,فاطمه سیفی شهپر،The Secret Sharing Based on Elliptic Curves،First Conference on Computational Group Theory, Computational Number Theory and Applications،کاشان،۲۰۱۴ ۱۲ ۱۷.
۱۸. مجتبی بهرامیان،۲۴th Iranian Algebra Seminar،Discrete logarithm Problem،کرج،۲۰۱۴ ۱۱ ۱۲.
۱۹. مریم رضایی کاشی، مجتبی بهرامیان،احراز هویت در رمزنگاری RSA،ششمین کنفرانس بین المللی ترکیبیات، رمزنگاری، علوم کامپیوتر و محاسبات،تهران،۲۰۲۱/۱۱/۱۷.
۲۰. الهام حاجی رضایی و مجتبی بهرامیان،رمزنگاری شناسه کاربری با استفاده از ژاکوبین تعمیم یافته خم‌های بیضوی،پنجاه و یکمین کنفرانس سالانه ریاضی ایران،کاشان،۱۳۹۹ ۱۱ ۲۸.
۲۱. مریم رضایی کاشی و مجتبی بهرامیان،انتقال بی‌اطلاع با استفاده از ژاکوبین تعمیم‌یافته خم‌های بیضوی،پنجاه و یکمین کنفرانس سالانه ریاضی ایران،کاشان،۱۳۹۹ ۱۱ ۲۸.
۲۲. مریم رضایی کاشی و مجتبی بهرامیان،کدهای رید-مولر روی میدان های متناهی و کاربرد آن ها در تسهیم راز،چهارمین کنفرانس بین المللی ترکیبیات، رمزنگاری، علوم کامپیوتر و محاسبات،تهران،۱۳۹۸.

مقالات در نشریات

1. مریم رضائی کاشی,مجتبی بهرامیان,A Post-Quantum Zero-Knowledge Identification Scheme,Mathematics Interdisciplinary Research,0000 00 00,ISC.
۲. مریم رضایی کاشی و مجتبی بهرامیان،اثبات دانستن عوامل اول یک عدد با استفاده از پروتکل دانش-صفر،مجله علوم ریاضی و انفورماتیک ایران (۲۰۲۱)،IJMSI.
۳. مجتبی بهرامیان،مروری بر رمزنگاری خم‌های بیضوی،فرهنگ و اندیشه ریاضی،۰ ۰ ۰۱.
4. Mojtaba Bahramian, Elham Hajirezaei,AN IDENTITY-BASED ENCRYPTION SCHEME USING ISOGENY OF ELLIPTIC CURVES,Facta Universitatis, Series: Mathematics and Informatics,pp. 1451-1460,2021 03 17.
5. 6. Khadijeh Eslami ,& Mojtaba Bahramian,An ECDLP-Based Verifiable Multi-Secret Sharing Scheme,Math. Interdisc. Res.,Vol. 5,pp. 193-206,2020.
6. Mojtaba Bahramian, Khadijeh Eslami,A New Verifiable Multi-Secret Sharing Scheme based on Elliptic Curves and Pairings,Italian journal of pure and applied mathematics,2019.
7. Mojtaba Bahramian, Maryam Sheyki, Christophe Doche,A Threshold Verifiable Multi-Secret Sharing Based on Elliptic Curves and Chinese Remainder Theorem,IET Research Journals (IET Information Security),2019.
8. Mojtaba Bahramian, Khadijeh Eslami,An Efficient threshold Verifiable Multi-secret Sharing Using Generalized Jacobian of Elliptic Curves,Algebraic Structures and Their Applications,Vol. 4,No. 2,pp. 45-55,2017.
9. Mojtaba Bahramian, Hassan Daghigh,A generalized fibonacci sequence and the diophantine equations,Iranian Journal of Mathematical Sciences and Informatics,Vol. 8,No. 2,pp. 111-121,2013,ISC.
10. Hassan Daghigh, Mojtaba Bahramian,Generalized Jacobian and Discrete logarithm Problem on Elliptic Curves,Iranian Journal of Mathematical Sciences and Informatics,Vol. 4,No. 2,pp. 55-64,2009,ISC.