حسن دقیق

دانشیار

دانشکده: دانشکده علوم ریاضی

گروه: ریاضی محض

سوابق تحصیلی

مقطع تحصیلی	سال اخذ مدرک	رشته و گرایش تحصیلی	دانشگاه
کارشناسی	۱۳۵۹	ریاضی	دانشگاه کاشان
کارشناسی ارشد	۱۳۶۷	ریاضی	دانشگاه تربیت مدرس
دکتری	۱۳۷۶	ریاضی	دانشگاه مک گیل

سوابق اجرایی

- معاون آموزشی دانشگاه کاشان 1369 - 1367
- معاون اداری و مالی دانشگاه کاشان 1379- 1377
- رئیس دانشگاه کاشان 1386-1381
- معاون مدیر کل بورس دانشجویان خارج 1381-1380
- عضو کمیته بورس وزارت علوم و تحقیقات و فناوری 1382- 1380
- عضو کمیته ارزشیابی وزارت علوم و تحقیقات و فناوری 1386 تا کنون
- مدیر گروه ریاضی ، آمار و علوم کامپیوتر دانشگاه کاشان 1387 تا
- دبیر کنفرانس ریاضی شیمی – 1388
- دبیر چهاردهمین دوره مسابقات دانشجویی ریاضی کشور - 1389
- معاون مالی و اداری دانشگاه کاشان 1395 تا 1396
- رئیس دانشکده علوم ریاضی- 1397-

جوایز و تقدیر نامه ها

1. استاد نمونه آموزشی دانشگاه کاشان در سال های 86، 87، 88 و 90
2. استاد نمونه پژوهشی دانشگاه کاشان در سال

موضوعات تدریس تخصصی

جبر 1و2و3 – آنالیز 1و2- نظریه اعداد- توپولوژی عمومی – رمزنگاری

جبر پیشرفته- هندسه منیفلد- نظریه جبری اعداد – جبر جابجایی- نظریه جبری رمزنگاری - حساب روی خمهای بیضوی

مقالات در همایش ها

۱. حسن دقیق , مجتبی بهرامیان , سمیه دیداری،نگاهی به برخی مسائل ریاضی در رمزنگاری،اولین کنفرانس جبر محاسباتی، نظریه محاسباتی اعداد و کاربردها،;hahk،۱۳۹۳.
۲. حسن دقیق و مهرداد خزلی،الگوریتمی برای بدست آوردن نقاط گویای خم های بیضوی E/Q با رتبه یک،بیستمین سمینار جبر،تهران،۱۳۸۸.
3. حسن دقیق , روح الله خداکرمیان گیلان , سمیه دیداری ,A key exchange protocol based on endomorphism ring of elliptic curves ,The Second Conference on Computational Group Theory, Computational Number Theory and Applications ,کاشان ,2015.
4. سمیه دیداری , مجتبی بهرامیان , حسن دقیق ,A Sharp Height Estimate for a Specific Family of Elliptic Curves ,The First Conference on Computational Group Theory ,کاشان ,2014.
5. حسن دقیق ,& سمیه دیداری ,Factoring RSA numbers using elliptic curves ,The Second Conference on Computational Group Theory, Computational Number Theory and Applications ,کاشان ,2015.
6. حسن دقیق , سمیه دیداری , روح الله خداکرمیان گیلان ,A deterministic algorithm for Discrete logarithm on some special elliptic curves over rational numbers ,12th International ISC Conference on Information Security and Cryptology ,گیلان ,2015.
7. حسن دقیق ,& فاطمه سیفی شهپر ,Constructing Elliptic Curves with Prescribed Torsion using Halving ,Computational Algebra, Computational Number Theory and Applications ,کاشان ,2015.
8. حسن دقیق , امیرمهدی یزدانی کاشانی , روح الله خداکرمیان گیلان ,Primality test for Mersenne numbers using elliptic curves ,International ISC Conference on Information Security and Cryptolog ,تهران ,2014.
9. حسن دقیق ,& سمیه دیداری ,The mordell-weil group of a special family of elliptic curves ,The 45th Annual Iranian Mathematics Conference ,سمنان ,2014.
10. حسن دقیق ,& روح الله خداکرمیان گیلان ,Computing minimal polynomial of parametric numbers in number fields ,The 45th Annual Iranian Mathematics Conference ,سمنان ,2014.
11. حسن دقیق , سمیه دیداری , فاطمه سیفی شهپر ,Elliptic curves and cryptography ,The 45th Annual Iranian Mathematics Conference ,سمنان ,2014.
12. حسن دقیق , سمیه دیداری , فاطمه سیفی شهپر ,Computing Elliptic Curve Discrete Logarithm via Lifting ,10th International ISC Conference on Information Security and Cryptology ,یزد ,2013.
13. حسن دقیق ,Special Values of L-functions, غیاث الدین جمشید کاشانی ,کاشان ,1378.
۱۴. امیرمهدی یزدانی کاشانی,حسن دقیق،The ۴۶th Annual Iranian Mathematics Conference،یزد،۲۰۱۵ ۸ ۲۵ ،a simple methos for hashing to elliptic curves.
۱۵. حسن دقیق,امیرمهدی یزدانی کاشانی،The Second Conference on Computational Group Theory, Computational Number Theory and Applications،کاشان،۲۰۱۵ ۱۰ ۱۳ ،An efficient method for encoding to elliptic curves.
۱۶. حسن دقیق,رضا کابلی نوش آبادی،اثبات ناتراوای دانش،دومین کنفرانس جبر محاسباتی، نظریه محاسباتی اعداد و کاربردهای آن،کاشان،۲۰۱۵ ۱۰ ۱۳.
۱۷. عبدالکریم الهی,حسن دقیق،مروری بر امنیت کتابخانه های دیجیتال،همایش ملی مهندسی رایانه و مدیریت فناوری اطلاعات،تهران،۲۰۱۴ ۵ ۲۹.
۱۸. بهزاد سلیمانی نیسیانی,روح اله خداکرمیان گیلان,حسن دقیق،مقاومت مسئله لگاریتم گسسته در برابر حملات ژنتیک،کنفرانس امنیت سامانه‌های نرم‌افزاری،شیراز،۲۰۱۴ ۵ ۱۵.
۱۹. مجتبی بهرامیان,سمیه دیداری,حسن دقیق،The First Conference on Computational Group Theory, Computational Number Theory and Applications،کاشان،۲۰۱۴ ۱۲ ۱۷ ،Calculus on Elliptic Curves.
۲۰. حسن دقیق,مهرداد خزلی،الگوریتمی برای بدست آوردن نقاط گویای خم های بیضوی E/Q با رتبه یک،بیستمین سمینار جبر،تهران،۲۰۰۹ ۴ ۲۲.
۲۱. سمیه دیداری,حسن دقیق,مجتبی بهرامیان،The First Conference on Computational Group Theory, Computational Number Theory and Applications،کاشان،۲۰۱۴ ۱۲ ۱۷ ،Constructing Elliptic Curves for Cryptography.
۲۲. Hassan Daghigh, Fatemeh Seifi Shahpar, Ruhollah Khodakaramian،Constructing Elliptic

Curves with Prescribed Torsion using Halving،The First Conferenceon Computational Group Theory, Computational Number Theory and Applications،۲۰۱۴.

23. Amir Mehdi Yazdani Kashani, Hassan Daghigh ,A Simple Method For Hashing To Elliptic Curves ,46th Annual Iranian Mathematics Conference ,2015.

مقالات در نشریات

1. H. Daghigh ,& M. Bahramian,Generalized Jacobian and Discrete logarithm Problem on Elliptic Curves,Iranian Journal of Mathematical Sciences and Informatics,2009 11 01,ISC.
2. A. Astaneh Asl ,& H. Daghigh,Independence of Heegner points For Nonmaximal Orders,INT J NUMBER THEORY,2011 5 01,ISI.
3. M. Bahramian ,& H. Daghigh,A generalized fibonacci sequence and the diophantine equations,Iranian Journal of Mathematical Sciences and Informatics,2013 10 01,ISC.
4. H. Daghigh ,& S. Didari,On The Elliptic Curves of The Form y^2=x^3-3px,Bulletin of the Iranian Mathematical Society,2014,ISI ,ISC.
5. H. Daghigh ,& S. Didari,On The Elliptic Curves of The Form y^2=x^3-pqx,Iranian Journal of Mathematical Sciences and Informatics,2015 10 01,ISC.
6. H. Daghigh ,& S. Didari,Complete Characterization of the Mordell- Weil Group of some families of elliptic curves,B IRAN MATH SOC,2016,ISI ,ISC.
7. H. Daghigh , R. Khodakaramian Gilan , F. Seifi Shahpar,Diffie-Hellman type key exchange protocols based on isogenies,Bulletin of the Iranian Mathematical Society,2017,ISI ,ISC.
۸. Amirmehdi Yazdani Kashani and Hassan Daghigh،EMBEDDING FINITE FIELDS INTO ELLIPTIC CURVES،FACTA UNIVERSITATIS،۲۰۱۹.
۹. Mehrdad Khazali and Hassan Daghigh،FAMILY OF ELLIPTIC CURVES E(p,q): y^۲=x^۳- p^۲x+q^۲،FACTA UNIVERSITATIS،۲۰۱۹.
10. HASSAN DAGHIGH* AND RUHOLLA KHODAKARAMIAN GILAN,ISOGENY-BASED CERTIFICATELESS IDENTIFICATION SCHEME,Journal ofAlgebraic Structures and Their Applications,2019.
11. Amirmehdi Yazdani Kashani and Hassan Daghigh,EFFICIENT ENCODINGS TO HYPERELLIPTIC CURVES OVER FINITE FIELDS,FACTA UNIVERSITATIS,2018.