میهمانان مدعو پژوهشگاه در بهار ۱۳۸۲

میهمانان پژوهشکده فیزیک

تئودوروس دوویسه از تاریخ ۱۸ خردادماه ۸۲ به‌مدت یک‌ماه و ژان پل گرییه از تاریخ ۱۸ خردادماه ۸۲ الی ۱۸ تیرماه ۸۲، میهمانان پژوهشکده فیزیک بودند. این افراد همکاران پروژهٔ سرن هستند.

شاهین محمدف نیز دیگر میهمان پژوهشکده فیزیک در بهار ۸۲ بوده است.

میهمان پژوهشکدهٔ ریاضیات

فیلیپ راگ‌اِوِی

پرفسور فیلیپ راگ‌اِوِی(Phillip Rogaway) از دانشگاه کالیفرنیا در دیویس، دو هفته میهمان پژوهشکدهٔ ریاضیات پژوهشگاه و دانشگاه صنعتی امیرکبیر بود. وی در طول اقامت خود در ایران دو سخنرانی در پژوهشکدهٔ ریاضیات و یک دورهٔ آموزشی-پژوهشی کوتاه مدت در دانشکدهٔ مهندسی کامپیوتر دانشگاه صنعتی امیرکبیر برگزار کرد. عناوین سخنرانیهای ایشان و توضیحاتی دربارهٔ آنها در زیر آمده است.

• نظری اجمالی بر مبحث امنیت اثبات‌پذیر در رمزنگاری (A Glimpse of Provable-Security Cryptography)

۱۷ اردیبهشت، پژوهشگاه

مبحث امنیت اثبات‌پذیر در رمزنگاری گرچه دانشی بیست ساله و مبتنی بر تعاریف و استنتاجات دقیق است، ولی هنوز مبحثی اسرارآمیز به‌شمار می‌رود.

هدف این سخنرانی، بحث دربارهٔ بعضی از جالب‌ترین ایده‌هایی بود که از رویکرد امنیت اثبات‌پذیر به رمزنگاری و نظریهٔ پیچیدگیِ مبتنی بر رمزنگاری سر برآورده است. سخنران بدون آنکه بخواهد جدیدترین نتایج را در این زمینه یا دستاوردهای خودش را تشریح کند، به توصیف چارچوب و زمینه‌ای پرداخت که سرچشمهٔ کارهای اوست.

• سازگار کردن دو دیدگاه در بارهٔ رمزنگاری(توجیه محاسباتی دیدگاه صوری)

(Reconciling Two Views of Cryptography(The Computational Soundness of Formal Encryption))

۲۴ اردیبهشت، پژوهشگاه

دو دیدگاه متمایز در رمزنگاری طی سالها در دو جامعهٔ مجزا شکل گرفته است. یکی از این دیدگاهها مبتنی بر چارچوب صوری(معمولاً جبری یا منطقی) است که ساده و مؤثر نیز هست. دیدگاه دیگر مبتنی بر مدل محاسباتی مبسوط و دقیق است که پیچیدگی و احتمال نیز در آن ملحوظ می‌شود. این دیدگاه با دنیای واقعی ارتباط پیدا می‌کند. سخنران که خود به رویکرد دوم اعتقاد دارد، کوشید پلی بین این دو دیدگاه بزند و با ارائهٔ توجیهی محاسباتی برای رویکرد صوری به رمزنگاری، از اختلاف دو دیدگاه بکاهد و آنها را به هم ربط دهد.

• امنیت اثبات‌پذیر به عنوان ابزاری برای طراحی قراردادهای عملی رمزنگاری

(Provable Security as a Tool for Designing Practical Cryptographic Protocols)

۲۱، ۲۲، ۲۳ اردیبهشت، دانشگاه صنعتی امیرکبیر

در این رشته سخنرانی، که در سه جلسه برگزار شد، سخنران به تشریح رویکرد امنیت اثبات‌پذیر به رمزنگاری پرداخت. این رویکرد که ابتدا مبحثی نظری بود، اکنون تبدیل به ابزاری اساسی در طراحی و تحلیل تکنیکهای عملی رمزنگارانه شده است. سخنران از جمله توضیح داد که چگونه به ابزاری دست یافته‌ایم که ایجاد قراردادهای رمزنگاری را(با کارایی و اطمینانی بیشتر از آنچه طراحیهای بی‌قاعده فراهم می‌کنند) تسهیل می‌کند. وی به منظور نشان دادن ایده‌های این رویکرد، از محرمانگی پیام و تصدیق اصالت آن در محیط کلید متقارن استفاده کرد.

انگیزهٔ سفر

از گزارش سفر راگ‌اِوِی به ایران

در ماه مه ۲۰۰۳ پس از سالها که اندیشهٔ سفر به ایران را در سر داشتم، سرانجام به آن کشور رفتم. تدارک این سفر کار دشواری نبود. دو تن از همکاران رشتهٔ تخصصی من، دکتر امین شکراللهی و دکتر ریحانه صفوی نایینی بین من و دکتر غلامرضا خسروشاهی از پژوهشگاه دانشهای بنیادی(IPM) و دکتر بابک صادقیان از دانشگاه صنعتی امیرکبیر(AUT) ارتباط برقرار کردند و من به مدت ۲/۵ هفته برای سخنرانی در این دو مؤسسه به ایران دعوت شدم.
تصورم این بود که سخنرانیها و درسهای من برای دانشجویان و پژوهشگران آنجا مفید خواهد بود. اما علاوه بر آن، انگیزه‌های شخصی نیز داشتم. بیست سال بود که نسبت به ایران کنجکاو بودم. بعضی از ایرانیان مقیم آمریکا را می‌شناختم و زندگیم مدتها با یکی از آنها گره خورده بود. به همین جهت به یادگیری زبان فارسی پرداختم، هر چند بیشترِ آنچه را که یاد گرفتم بعدها از یاد بردم. مادر و نامزدم با این سفر مخالف بودند. عقیدهٔ رایج در میان بسیاری از هم‌وطنانم این است که ایران جای خطرناکی است؛ کشوری است مملو از متعصبان مذهبی که ذهنشان مالامال از نفرت است. من می‌دانستم که این حرفها مهمل است. به‌علاوه، کشورم جنگ لفظی شدیدی علیه کشورهای منطقه راه انداخته بود و رئیس جمهور ایالات متحدهٔ آمریکا در تدارک جنگ افروزی خود، سه کشور کم قدرت جهان را، که ایران هم یکی از آنها بود، محور شرارت نامیده بود که به نظر من مضحک می‌نمود. با خود گفتم که اگر همین الان، در بحبوحهٔ بحران منطقه، به ایران بروم، این پیام را به ایرانیان خواهم رساند که همهٔ آمریکاییان، پرخاشگر، ناآگاه، و شوونیست نیستند.

.....

در پژوهشگاه دانشهای بنیادی و دانشگاه امیرکبیر، تقریباً همهٔ اعضای هیأت علمی تحصیلکردهٔ آمریکا یا اروپا(بیشتر، آمریکا) هستند. اغلب در دانشگاههای خوبی تحصیل کرده‌اند. می‌دانند کار پژوهش چگونه است، فرق بین کار خوب و کار بد را تشخیص می‌دهند، و ذائقهٔ علمی و فکری خوبی دارند. دانشجویانی که به آنها درس دادم، فوق‌العاده مشتاق یادگیری بودند. از قبل مقاله‌های مرا خوانده بودند و سؤالات عمیقی مطرح می کردند.

******

راگ‌اِوِی در گزارش ۶ صفحه‌ای خود از سفرش به ایران، نکات متعدد دیگری را نیز دربارهٔ فرهنگ‌دوستی ایرانیان، طرز رانندگی در تهران(که آن را به یک بازی ویدئویی تشبیه می‌کند!) و همچنین وضع زنان و مسائل اجتماعی و سیاسی دیگر مطرح کرده است.

از پایگاه اینترنتی پژوهشگاه در آدرس http://www.ipm.ac.ir دیدن نمایید.