بخش جوایز بین‌المللی مهم از شمارهٔ بهار ۱۳۹۱ در نشریهٔ اخبار دایر شده و به معرفی برندگان معتبرترین جوایز علمی و دستاوردهای آنها در زمینه‌های مرتبط با کار پژوهشگاه می‌پردازد. این بخش را در این شماره به اعطای دو جایزهٔ مهم در بهار ۲۰۱۳، جایزهٔ گودل در علوم کامپیوتر نظری و جایزهٔ آبل در ریاضیات، اختصاص داده‌ایم. مطلب مربوط به جایزهٔ گودل را عمران احمدی عضو هیئت علمی پژوهشکدهٔ ریاضیات نوشته و شرح مربوط به جایزهٔ آبل در دفتر اخبار تهیه شده است.

اهدای جایزهٔ گودل ۲۰۱۳ به سه محقق رمزنگاری

عمران احمدی*

جایزهٔ گودل یکی از جوایز معتبر در علوم کامپیوتر نظری است که از سال ۱۹۹۳ هر سال به نویسندگان مقالات مهم و تأثیرگذار در این زمینه اهدا می‌شود. این جایزه به افتخار کورت گودل ریاضیدان، فیلسوف، و منطق‌دان برجستهٔ اطریشی-امریکایی نامگذاری شده و دو انجمن علوم کامپیوتر نظری اروپا (European Association for Theoretical Computer Science) و گروه الگوریتم و محاسبات انجمن ماشینهای محاسبه (Association for Computing Machinery, ACM) مشترکاً آن را اهدا می‌کنند.

برندگان سال ۲۰۱۳ جایزهٔ گودل سه نفر از محققان فعال در رمزنگاری، آنتوان ژو (Antoine Joux) از فرانسه و دن بونه (Dan Boneh) و متیو فرانکلین (Matthew Franklin) از امریکا هستند.

علت اهدای جایزه به آنتوان ژو، نگارش مقالهٔ «یک پروتکل 'یکباره' برای اشتراک کلید سه نفره[1]» و دلیل انتخاب دن بونه و متیو فرانکلین نگارش مقالهٔ مشترکی با عنوان «سیستم رمز مبتنی بر شناسه با استفاده از نگاشت دو دویی ویل (Weil)[2]» است. شرح مختصری از این مقالات در ادامه آورده می‌شود.

دستاورد آنتوان ژو

در سال ۱۹۷۶ دیفی (Diffie) و هلمن (Hellman) پروتکلی[3] ارائه دادند که با کمک آن، دو نفر می‌توانند بر روی کلیدی (اطلاعات غیرقابل کشف برای اغیار) توافق کنند که بعداً جهت رمزی کردن اطلاعاتی که با هم رد و بدل می‌کنند به کار رود. اهمیت این پروتکل در این بود که تمام اطلاعاتی که دو نفر با هم در مرحلهٔ توافق کلید رد و بدل می‌کنند در دسترس دیگران است، امری که پیش از آن ناممکن تلقی می‌شد. ارائهٔ پروتکل مزبور سرآغاز عصر جدیدی در رمزنگاری بود و منجر به پیدایش سیستم‌های رمز کلید عمومی شد.

آنتوان ژو

پروتکل ارائه شده توسط دیفی و هلمن بدین شرح است. فرض کنید یک گروه دوری G که توسط g تولید شده و n عضو دارد داده شده و دو شخص A و B می‌خواهند بر کلیدی توافق کنند که بعداً برای رمزی کردن اطلاعات مبادله شده بین یکدیگر از آن استفاده کنند. شخص A عدد a را که عددی بین یک و n است انتخاب کرده و g^a را محاسبه و به B ارسال می‌کند، در حالی که g^a در معرض مشاهدهٔ همگان است. به طور همزمان شخص B عدد b را انتخاب کرده و g^b را به A ارسال می‌کند. بعد از این مرحله، A با گرفتن g^b از B و داشتن a می‌تواند g^{ab} را محاسبه کند. شخص B نیز به طور مشابه g^{ab} را محاسبه می‌کند. پس از این مرحله از g^{ab} می‌توان به عنوان کلید استفاده کرد. به طور مثال، اگر A می‌خواهد پیغام m را به B بفرستد، کافی است که $m.g^{ab}$ را محاسبه کرده و به B ارسال کند. B با دریافت $m.g^{ab}$، $m.g^{ab}.g^{-ab}$ را محاسبه کرده و m را به دست می‌آورد. در این پروتکل، A تنها کسی است که a را می‌داند و B تنها کسی که b را. اگر گروه G به طور مناسب انتخاب شده باشد، غیر از A و B کس دیگری نمی‌تواند در زمان کوتاهی g^{ab} را محاسبه کند، علی‌رغم اینکه g، g^a و g^b در دسترس وی هستند.

پروتکل بالا بدین جهت 'یکباره' خوانده می‌شود که طرفین فعال در پروتکل برای توافق بر روی یک کلید فقط یک بار اقدام به ارسال اطلاعات به طرف فعال دیگر می‌کنند و پس از ارسال اطلاعات، کلید می‌تواند تولید شود.

بعد از ابداع پروتکل دیفی و هلمن، به طور طبیعی این سؤال مطرح شد که آیا می‌توان پروتکلی یکباره ارائه کرد که توسط آن، سه نفر بتوانند بر روی کلیدی توافق کنند؟ این مسأله به مدت بیش از دو دهه حل نشده باقیمانده بود تا اینکه آنتوان ژو توانست با استفاده از نگاشتهای دو دویی که بر خمهای بیضوی تعریف می‌شوند

*) پژوهشگاه

دن بونه

متیو فرانکلین

به سوال فوق پاسخ مثبت دهد. شرح پروتکل ارائه شده توسط ژو از حوصلهٔ این نوشته خارج است. علاقه‌مندان می‌توانند به مقالهٔ ژو[1] مراجعه کنند.

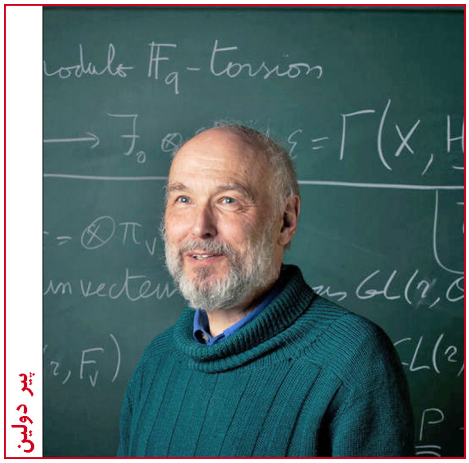
دستاورد دن بونه و متیو فرانکلین

سیستم‌های رمزنگاری به طورکلی به دو دسته تقسیم می‌شوند: سیستم‌های کلید خصوصی و سیستم‌های کلید عمومی. در سیستمهای کلید خصوصی یک کلید بین تمام کسانی که می‌خواهند ارتباط امن داشته باشند به اشتراک گذاشته می‌شود و از همان کلید برای رمزنگاری و رمزگشایی استفاده می‌شود. در سیستم‌های کلید عمومی، هر شخص یک کلید عمومی و یک کلید خصوصی دارد که اشخاص دیگر برای رمزی کردن اطلاعات ارسالی به وی از کلید عمومی او استفاده می‌کنند و خود شخص برای رمزگشایی از کلید خصوصی خود استفاده می‌کند. در ابتدای پیدایش سیستم‌های کلید عمومی نیاز به این بود که هر شخص برای خود یک کلید خصوصی و یک کلید عمومی تولید کرده و کلید عمومی خود را منتشر و قابل دسترس برای همگان کند. مسأله‌ای که در همان اوان مطرح شد این بود که آیا می‌توان یک سیستم رمزکلید عمومی طراحی کرد که با استفاده از آن برای افرادی که کلید عمومی برای خود منتشر نکرده‌اند پیغام امن فرستاد. مثلاً اگر A می‌خواهد به B پیغام بفرستد و کلید عمومی B در دسترس نیست، A از آدرس ایمیل B استفاده کند و پیغام خود را توسط آن رمزکرده و به B بفرستد. این مسأله به مدت بیش از دو دهه مطرح بود تا اینکه بونه و فرانکلین با الهام از کار آنتوان ژو آن را حل کردند. در کار بونه و فرانکلین نیز از نگاشت‌های دو خطی استفاده شده است.

مراجع

1. **A. Joux.** *A one round protocol for tripartite Diffie-Hellman*, J. Cryptology **17**(4) (2004) 263-276.
2. **D. Boneh** and **M. Franklin**, *Identity based encryption from the Weil pairing*, SIAM J. of Computing **32**(3) (2003) 586-615.
3. **W. Diffie** and **M. Hellman**, *New directions in cryptography*, IEEE Transaction on Information Theory **22**(6) (1976) 644-654.

جایزهٔ آبل ۲۰۱۳ برای پیر دولین•



پیر دولین

جایزهٔ آبل (چنانکه در شمارهٔ بهار ۹۱ اخبار توضیح داده شد) از سال ۲۰۰۳ هر سال به یک یا دو ریاضیدان برجسته اهدا می‌شود و امروز یکی از معتبرترین جوایز ریاضی به شمار می‌رود. این جایزه را فرهنگستان علوم و ادبیات نروژ اعطا می‌کند و علاوه بر اعتبارِ بسیار، مبلغ نقدی آن نیز (۶ میلیون کرون نروژ معادل تقریباً یک میلیون دلار امریکا) قابل مقایسه با جوایز نوبل است. در مقایسه با مدال فیلدز، که به ریاضیدانان برجستهٔ زیر چهل داده می‌شود تا مشوق آنان در پژوهشهای بعدی باشد، جایزهٔ آبل تاکنون به ریاضیدانانی کهنه‌کار و پرسابقه در اواخر دورهٔ کاری‌شان اهدا شده است.

فرهنگستان علوم و ادبیات نروژ جایزهٔ آبل ۲۰۱۳ را به پیر دولین (Pierre Deligne) ریاضیدان نامدار بلژیکی و استاد بازنشستهٔ انستیتوی مطالعات پیشرفته در پرینستن آمریکا اهدا کرد.

فرهنگستان نروژ دلیل اعطای این جایزه را به دولین، «دستاوردهای دوران‌ساز او در هندسهٔ جبری و تأثیر انقلابی این دستاوردها در نظریهٔ اعداد، نظریهٔ نمایشها، و مباحث وابسته» اعلام کرده است. در واقع، ایده‌های رهگشای دولین و نتایج حل بعضی از مسائل دیرینهٔ بسیار مهم توسط او چنان در این مباحث رخنه کرده‌اند که بخش مهمی از تحقیقات جاری در این زمینه‌ها را بدون ارجاع به کارهای او نمی‌توان فرموله کرد. به گفتهٔ پیتر سرنگ (Peter Sarnak) استاد پژوهشکدهٔ ریاضیات در انستیتوی مطالعات پیشرفته، «دستاورد دولین فراتر از اثبات چند حکم بنیادی ریاضی است؛ توجه او همچنین معطوف به درک این موضوع بوده است که چرا آن حکمها اساسی و اجتناب‌ناپذیرند، و با استدلال‌های انتزاعی بسیار هوشمندانه آنها را روشن و قابل فهم ساخته است. بسیاری از ابزارهای متعارف در هندسهٔ جبری مدرن، و قضیه‌ها، نظریه‌ها، اشیاء و ساختارهای ریاضی متعددِ مهمی نام او را بر خود دارند.»