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.

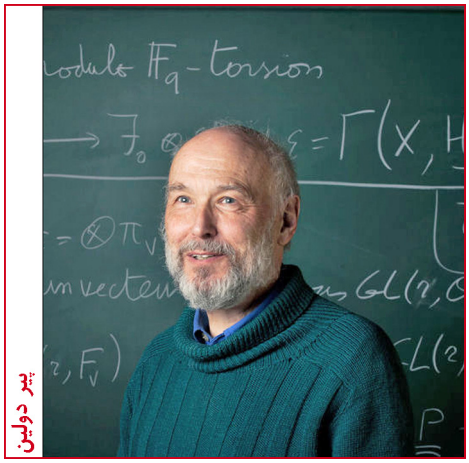
دستاورد دن بونه و متیو فرانکلین

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.»

حال نگاهی دقیق‌تر به دستاوردهای دولین:

اشیای هندسه از قبیل خط، دایره، و کره را می‌توان با معادله‌های جبری ساده‌ای توصیف کرد. ارتباط بنیادیِ حاصل بین هندسه و جبر به پیدایش هندسهٔ جبری انجامیده است که در آن از روشهای هندسی برای بررسی جوابهای معادلات چندجمله‌ای استفاده می‌شود و به عکس، روشهای جبری برای تحلیل اشیای هندسی به کار می‌روند.

هندسهٔ جبری طی زمان دستخوش دگرگونی‌ها و بسط و گسترش‌هایی شده و به صورت رشته‌ای مرکزی در ریاضیات درآمده که ارتباطات عمیقی با تقریباً هر مبحث ریاضی دارد. پیر دولین نقش اساسی در بسیاری از این تحولات داشته است.

معروفترین دستاورد دولین حل و فصل آخرین و عمیق‌ترین حدس از رشته حدسهای ویل (Weil) یعنی اثبات فرضیهٔ ریمان در مورد واریته‌های جبری روی یک میدان متناهی است. ویل گمان می‌برد که اثبات این حدسها نیازمند روشهایی از توپولوژی جبری است. بر این اساس، گروتندیک (Grothendieck) و اعضای مکتب او نظریهٔ کوهومولوژی lـآدیک را پدید آوردند که بعدها ابزار اساسی دولین در اثبات معروفش بود، اثباتی که یک شاهکار واقعی است و پرتو جدیدی بر کوهومولوژی واریته‌های جبری افکنده است. حدسهای ویل کاربردهای مهمی در نظریهٔ اعداد، از جمله در حل و فصل حدس رامانوجان-پیترسن و براورد مجموعه‌های نمایی داشته است.

دولین در یک رشته مقاله نشان داد که کوهومولوژی واریته‌های تکین و نافشرده دارای یک ساختار آمیختهٔ هاج (Hodge) هستند. نظریهٔ ساختارهای آمیختهٔ هاج امروز ابزار اساسی و نیرومندی در هندسهٔ جبری است و امکان درک عمیقتری از کوهومولوژی را فراهم کرده است. همچنین، دولین، کاتانی (Cattani) و کاپلان (Kaplan) از این نظریه برای اثبات یک قضیهٔ جبری استفاده کردند که گواه محکمی برای درستی حدس هاج به‌شمار می‌آید.

دولین همچنین به اتفاق بلینسن (Beilinson)، برنستاین (Bernstein)، و گابر (Gabber) پژوهشهای مهمی در نظریهٔ بافه‌های انحراف (perverse sheaves) انجام داد. این نظریه نقش مهمی در اثبات اخیر لم بنیادی به وسیلهٔ نگو (Ngo، برندهٔ مدال فیلدز در سال ۲۰۱۰) داشته است. خودِ دولین نیز برای روشن کردن ماهیت تناظر ریمان-هیلبرت، که تعمیم‌دهندهٔ مسألهٔ ۲۱ ام هیلبرت به ابعاد بالاتر است، استفادهٔ زیادی از این نظریه کرده است. همچنین از کوهومولوژی lـآدیک برای ساخت نمایشهای خطی برای گروه‌های متناهی کلی از نوع لی بهره برده است. وی (به اتفاق مامفرد) مفهوم پشتهٔ جبری (algebraic stack) را برای اثبات فشردگی فضای پیمانه‌ایِ خمهای پایدار معرفی کرد. اینها و بسیاری از دستاوردهای دیگر او، تأثیر عمیقی در هندسهٔ جبری و مباحث وابسته داشته است.

تأثیر مفاهیم، ایده‌ها، نتایج، و روشهای دولین در پیشبرد هندسهٔ جبری، و ریاضیات به طور کلی، همچنان ادامه دارد.

پیر دولین در چهارم اکتبر ۱۹۴۴ در بروکسل، پایتخت بلژیک، به دنیا آمد. ۱۲ ساله بود که شروع به مطالعهٔ کتابهای ریاضی دانشگاهیِ برادر بزرگترش کرد. دبیر ریاضی او که علاقهٔ دولینِ نوجوان را به ریاضیات می‌دید چند جلد از سری مبانی ریاضیات، نوشتهٔ گروه بورباکی، را به او داد. آشنایی با این کتابها مسیر زندگی آتی او را تعیین کرد و علی‌رغم میل پدرش که می‌خواست او مهندس شود و زندگی مرفهی داشته باشد تصمیم گرفت دنبال رشتهٔ مورد علاقه‌اش ــ ریاضیات ــ برود. وی به تحصیل ریاضی در دانشگاه بروکسل پرداخت و دوره‌های کارشناسی و دکتری را، به ترتیب در سالهای ۱۹۶۶ و ۱۹۶۸، در آنجا به پایان رساند. بعداً، در سال ۱۹۷۲ درجهٔ دکتری دولتی علوم ریاضی را در دانشگاه پاریس جنوب II، زیر نظر الکساندر گروتندیک، گرفت.

دولین در سالهای ۱۹۶۷-۱۹۶۸ همزمان بورسیهٔ بنیاد ملی پژوهشهای علمی بلژیک و پژوهشگر میهمان در مرکز مطالعات عالی علمی (IHÉS) فرانسه بود. سپس از ۱۹۶۸ تا ۱۹۷۰ عضو میهمان این مرکز بود و در این سال به عضویت دائم برگزیده شد. در سال ۱۹۸۴ به عضویت دائم انستیتوی مطالعات پیشرفتهٔ پرینستن انتخاب شد و تا زمان بازنشستگی در ۲۰۰۸ در این سمت باقی ماند.

جامعهٔ علمی بین‌المللی انواع جوایز و نشانها را برای تقدیر از خدمات علمی دولین به او اهدا کرده است که از آن جمله‌اند مدال هانری پوانکاره از فرهنگستان علوم فرانسه (۱۹۷۴)، مدال فیلدز (۱۹۷۸)، جایزهٔ کرافورد از فرهنگستان سوئد (۱۹۸۸، به اتفاق الکساندر گروتندیک)، جایزهٔ بالزان (۲۰۰۴)، و جایزهٔ ولف (۲۰۰۸، به اتفاق فیلیپ گریفیت و دیوید مامفرد). دولین عضو بسیاری از فرهنگستانها و انجمنهای علمی مهم دنیاست، از جمله عضو افتخاری انجمن ریاضی مسکو و انجمن ریاضی لندن، عضو خارجی فرهنگستان علوم و هنرهای آمریکا، و عضو خارجی فرهنگستان سلطنتی علوم سوئد.

******

• برگرفته از وبگاه جایزهٔ آبل و

Deligne Awarded 2013 Abel Prize, Notices of the AMS **60**(6) (June/July 2013) 760-761.