The Gödel Price 2012

Laudatio for

Antoine Joux, Dan Boneh and Matthew K. Franklin

The 2013 Gödel Prize for outstanding papers in Theoretical Computer Science is awarded jointly to the following two papers:

Antoine Joux
A One Round Protocol for Tripartite Diffie-Hellman
Journal of Cryptology, 17(4): 263-276, 2004.
(Conference version: ANTS 2000)

Dan Boneh and Matthew K. Franklin
Identity-Based Encryption from the Weil Pairing
SIAM Journal on Computing, 32(3): 586-615, 2003.
(Conference version: CRYPTO 2001)

ACM's Special Interest Group on Algorithms and Computation Theory (SIGACT) together with the European Association for Theoretical Computer Science (EATCS) will recognize three researchers for their contributions to cryptographic concepts and schemes that provide greater efficiency, flexibility, and security. Their respective papers established the field of pairing-based cryptography by supplying a precise definition of the security of this approach, and providing compelling new applications for it. These applications include better methods for users to exchange the cryptographic keys that enable them to communicate privately and securely with each other. The papers' authors are Antoine Joux, and the team of Dan Boneh and Matthew K. Franklin. They will receive the 2013 Gödel Prize for outstanding papers in theoretical computer science at the ACM Symposium on the Theory of Computing (STOC) June 1-4, in Palo Alto, CA.

In his paper *A One Round Protocol for Tripartite Diffie-Hellman*, Joux's work generalized the two-party key agreement to the multi-party key agreement protocol of Diffie and Hellman, with a focus on the three-party case. His work uses an approach to public-key cryptography based on the algebraic structure of elliptic curves. Joux showed how to implement an elegant tripartite key agreement protocol using pairings on elliptic curves developed by Weil and Tate, and demonstrated that only one broadcast is required for each party.

Boneh and Franklin, in their paper *Identity-Based Encryption from the Weil Pairing*, used Weil pairings on elliptic curves to develop a fully functional identity-based encryption scheme (IBE). It relies on a type of public-key encryption in which the user's public key can be simply the user's identity or email address combined with a single master public key common to all users. This approach replaces the sender's need to obtain a user's public key by direct interaction with the user or via a published database of user public keys, which may be susceptible to corruption.

Antoine Joux is a part-time professor at the Université de Versailles Saint-Quentin-en-Yvelines and a part-time senior security engineer at CryptoExperts. A former member of the Computer Science Department at L'Ecole Normale Supérieure in Paris, he was deputy scientific director of the Central Directorate of Security of Information Systems in France.

Dan Boneh is a professor Computer Science and Electrical Engineering at Stanford University. An editor of the Journal of the ACM, he received a Ph.D. degree in Computer Science from Princeton University. He is a recipient of the Packard Award, the Alfred P. Sloan Award, the Terman Award, and the RSA Award.

A professor of Computer Science at the University of California, Davis, Matthew Franklin is a graduate of Columbia University with a Ph.D. degree in Computer Science. He received an M.A. degree in Mathematics from the University of California, Berkeley, and a B.A. degree in Mathematics from Pomona College. He is editor-in-chief of the Journal of Cryptology. He received a National Science Foundation Career Award, and was an AT&T Bell Labs Ph.D. Scholar.