Crypto 2004

Stephen A. Weis
Massachusetts Institute of Technology

The International Association for Cryptologic Research (IACR; www.iacr.org) held its 24th annual International Cryptography Conference 15–19 August 2004 in Santa Barbara, California. Nicknamed Crypto, the conference attracted more than 400 researchers from academia, government, and industry. Several pioneers of modern cryptography attended, including Whitfield Diffie, co-inventor of the Diffie-Hellman key exchange, and Adi Shamir and Ronald Rivest of RSA algorithm fame. During the conference, Rivest and David Chaum, founder of DigiCash, were recognized as inaugural IACR fellows. The IACR named Shamir and Diffie honorary IACR fellows earlier in 2004.

The conference consisted of short sessions, invited talks, and presentations of conference papers for interested attendees.

Two invited speeches

Victor Shoup, associate professor of computer science at New York University, delivered an invited speech on the history and evolution of adaptive chosen-ciphertext security. Sometimes abbreviated as CCA2, it's a computational model for proving security in public-key cryptography. Shoup described the security model development and its latest efficient constructions and concisely summarized many incremental developments during the past 14 years.

Susan Landau, senior staff engineer at Sun Microsystems Laboratories, delivered an invited speech that focused on security, liberty, and electronic communications. She discussed US government surveillance in light of its "war on terrorism," presented a history of wiretapping, and explained the progression of wiretap laws over the past 20 years. Landau largely focused on the Communications Assistance for Law Enforcement Act (CALEA; www.askcalea.net/index.html)—specifically, its impact on new communications technologies such as voice over IP (VoIP).

Landau expressed that "freedom is important in the war on terror" and that government-mandated wiretap support designed into Internet technologies could ultimately weaken security. She suggested that cryptographers take a pragmatic view when lobbying government agencies about surveillance issues; they should sometimes be willing to compromise on privacy issues. She stated that other than accepting a draconian surveillance society, there's little to prevent individuals or small numbers of people from conducting terrorist attacks like the 1995 Oklahoma City bombing. However, she expressed that a multifaceted approach to electronic surveillance could help combat organized terrorist groups such as Al Qaeda.

Session highlights

Crypto held 15 sessions on topics varying from such esoteric subjects as zero-knowledge proofs and unbounded adversarial models to more applied topics such as efficient data representations, secure computation, and key management. In each session, several authors each presented their own peer-reviewed conference papers in 25-minute talks. The presenting authors offered new constructions and paradigms in public-key and symmetric cryptography as well as new cryptanalytic techniques and proofs of open problems.

In the group signatures session, Anna Lysyanskaya, assistant professor of computer science at Brown University, described new group signature and anonymous credential schemes based on bilinear maps. Coauthored by Jan Camenisch of IBM Zurich Research Laboratory, these developments have theoretical importance and potential practical applications. Trusted-computing platforms can use group signatures to verify the authenticity of executable code, and anonymous credentials might have applications in Internet voting or commerce systems.

A PhD student at Massachusetts Institute of Technology, David Woodruff, presented new representations of algebraic torus elements that are more efficient than previous constructions in his discussion on asymptotically optimal communication for torus-based cryptography. Coauthored with Marten van Dijk of Philips Research Laboratories, Eindhoven, the Netherlands, cryptosystems employing Woodruff and van Dijk's research might lower communication costs—in their work, elements can be represented in fewer bits, although the approach consumes more computation time. The effort is applicable to ElGamal signatures and encryption, Diffie-Hellman key exchange, and other discrete logarithm-based cryptosystems.

Storage costs are so low that adversaries probably could capture any man-made source of randomness.

In a session focused on public-key cryptanalysis, Alexander May of Paderborn University, Germany, factored an RSA modulus in deterministic polynomial time with knowledge only of an RSA public–private key pair. Previously, this problem could only be solved in probabilistic polynomial time. The question remains unanswered whether extracting the plaintext of an RSA-encrypted message is equivalent to factoring.

The stream cipher cryptanalysis session included a presentation by Yi Lu and Serge Vaudenay, researchers at École Polytechnique Fédérale de Lausanne, Switzerland. They describe fast correlation attacks against the E0 key-stream generator used in Bluetooth. The attack combines precomputation and coding theory techniques to yield the fastest known attack against E0. The attack takes 2^{39} time given 2^{39} consecutive samples and $O(2^{37})$ precomputation time.

During a session on public-key encryption, Xavier Boyen of Voltage Security presented a paper (coauthored with associate professor Dan Boneh of Stanford) that offered a new identity-based encryption (IBE) scheme with a stronger security proof. The first practical IBE scheme, designed by Boneh and Stanford's Matt Franklin (then at Stanford; now a professor at the University of California, Davis), relied on the random oracle heuristic in its security proof, and is incorporated into Voltage Security's commercial products. The random oracle heuristic is a convenient, but ultimately flawed model of proving cryptosystem security. The new Boyen and Boneh scheme avoids the random oracle model and requires only standard security assumptions. However, the new scheme is computationally inefficient. An open problem is to make it scheme efficient in practice.

Tel Aviv University's Tal Moran presented a noninteractive timestamping scheme in the bounded storage model—a task that's impossible in the standard cryptographic model, but feasible when an adversary's storage is limited. Moran coauthored this work with Ronen Shaltiel (then a post-doctoral student at the Weizmann Institute; now at the University of Haifa) and Amnon Ta-Shma of Tel Aviv University's School of Computer Science.

The bounded-storage model uses a public source of randomness streaming so quickly that no adversary could practically capture all bits. For example, a satellite might beam a constant stream of random bits to earth. Because real-world adversaries have bounded storage, other cryptographic applications that are impossible in unbounded settings might be feasible in real life. However, one attendee noted that storage costs are so low that adversaries probably could capture any man-made source of randomness.

Rump session

Crypto's traditional "rump session" lets attendees deliver informal, short, and often facetious talks. Internet rumors created considerable buzz over new hash function collision results presented during this year's session. Eli Biham, a professor at Technion Institute in Haifa, Israel, presented attacks to find near-collisions in the SHA-0 hash function, which was a flawed, earlier version of the standardized SHA-1 hash function that's used in many security applications. Biham also found near-collisions in the 34th round of SHA-1's 80 rounds of computation. Antoine Joux of the Central Information Systems Security Division (DCSSI; www.ssi.gouv.fr/en/dcssi/index.html) in France presented an attack that discovered a full collision in SHA-0, suggesting that similar attacks might be conducted against SHA-1. Joux's attack took 20 days to compute using 160 Intel Itanium processors, which is much faster than what a brute-force attack would be expected to take.

Xiaoyun Wang, from the Shandong University's School of Mathematics and System Science in China, presented widespread hash collision results, including those for the MD4, MD5, RIPEMD, HAVAL-128, HAVAL-160, and SHA-0 hash functions. Finding SHA-0 and HAVAL-160 collisions took a trivial amount of computation: 240 and 232 steps, respectively. She found MD5 and RIPEMD collisions in less than two hours, HAVAL-128 collisions took only 64 computations, and she was able compute MD4 collisions by hand. The attacks could affect systems that rely on hash functions' collision resistance, particularly MD4 and HAVAL-128. Wang presented no collision results for the commonly used SHA-1 hash function.

On a lighter note, Jean-Jacques Quisquater of the Université Catholique de Louvain, Belgium, Crypto Group discussed what he called a "corneal attack." Quisquater recorded close-up video of a computer user's eye and then extracted the computer monitor's image reflected in it. His attack captured an unsuspecting graduate student shirking her duties by surfing the Web.

International issues

Near the end of the conference, the IACR held its membership meeting to discuss administrative issues. One agenda topic scheduled for discussion involved about 10 international researchers who weren't able to attend the conference because of excessive delays in obtaining entry visas. Some members suggested that the IACR leadership lobby the US government to expedite visa applications for international researchers.

Another proposal considered changing the conference from its traditional US location to a country with more efficient visa controls. No action was taken and Crypto will remain in Santa Barbara for the foreseeable future (14–18 August 2005; www.iacr.org/conferences/crypto2005).

The papers presented at Crypto 2004 continued several nascent cryptographic research themes. In particular, there appear to be several open research questions regarding efficient constructions and security proofs for identity-based cryptosystems. There also appear to be many potential applications for bilinear maps, which are the underlying mathematical tool used in several identity-based system constructions. Further development of the universal composition, non-black box, and bounded-storage security models will likely continue as well.

The hash collision results raise questions about the practical security of commonly implemented hash functions. This might spur the adoption of stronger hash functions, like SHA-256, or the development of new, standardized hash functions. We'll need further investigation to determine the practical significance of these results. □

__Stephen A. Weis__ is a graduate PhD student at the Massachusetts Institute of Technology's Computer Science and Artificial Intelligence Laboratory. His research interests include cryptography and information security. He has an MSc in computer science from MIT and is a member of MIT's Cryptography and Information Security Group. Contact him at sweis@mit.edu.

Recruiting Conference Reporters for *IEEE Security & Privacy*

With so many security and privacy conferences these days, who can keep up with them all? Volunteering to provide summaries of discussions and events from the meetings. Please contact Carl E. Landwehr at clandweh@isr.umd.edu if you're interested.