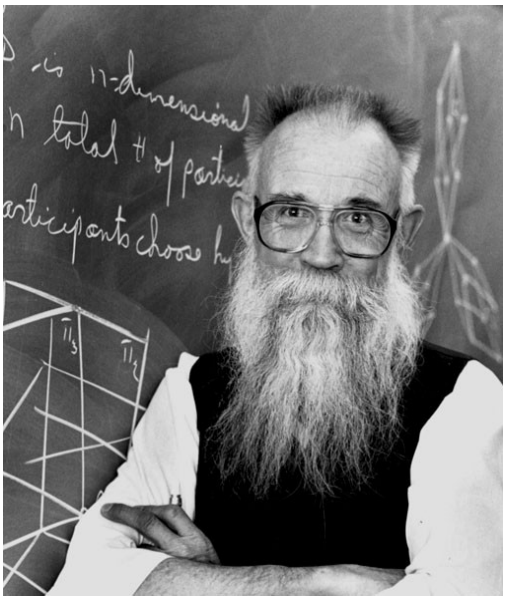
April 2001 Meeting: Gus Simmons, Zero-Knowledge Proofs

by John Geohegan



Gus Simmons

In the April Meeting, Dr. Gustavus Simmons introduced us to the significance and the mathematical basis of zero-knowledge proofs. Professing little knowledge of the mathematics, what follows is my understanding of the subject.

Since the time of Euclid some 2,300 years ago, the method of convincing someone you could prove a mathematical theorem has been to write out the proof and hand it to him. In the last 25 years, however, there has been a major change; it is now possible to convince someone that you have a proof in hand without giving him any knowledge! The new technique is an outgrowth of public-key cryptography which started in the 1970s. In 1986 Manuel Blum published a very readable paper titled "How to Prove a Theorem So No One Else Can Claim It", expanding on a paper the previous year by Goldwasser, Micali, and Rackoff. Blum showed that it was possible to devise a zero-knowledge proof for any provable theorem. Notice there's difference between proving a theorem and persuading someone else that you have the proof.

Writing in the Feb. 17, 1987, New York Times, James Gleick said "Although zero-knowledge proof began as an abstraction, computer scientists quickly realized its applicability to many everyday uses of secrecy. The issue arises whenever someone tears up credit-card carbons, looks over his shoulder while signing onto a computer or worries about the photocopying of a passport left with a hotel concierge."

Zero-knowledge proofs depend upon a series of interactions between the prover and the verifier that are more and more persuasive as the number of interactions increases, and upon the existence of a mathematical procedure that's easy in the forward direction but very difficult in reverse. In modular arithmetic it's easy to square a number but very difficult to extract the square root. For an everyday example, suppose I have a "smart card" that identifies me as knowing the modular square root of a large number, perhaps 200 digits long. In the blink of an eye, a verifying program could determine that

I truly know such a square root. The following "humanized" example illustrates the verification process using smaller numbers.

Prover: "I know the square root of 1251, modulo 1517, and I'll prove it without telling you what it is. I also know the square root of 247."

Verifier: "Prove to me you know the square root of 247."

Prover: "The square root of 247 is 42, modulo 1517.(This means that if 42 is squared, giving 1764, and divided by 1517, the remainder is 247. So 42 is called the square root of 247). I also know the square root of 821."

Verifier: "I can multiply 1251 times 821 and get 1,027,071 which leaves a remainder of 62 when divided by 1517. Since you claim to know the two square roots, you should be able to multiply them together and give me a square root of 62. What is it?"

Prover: "217 is a square root of 62. That means that if I square 217 and get 47089, then divide by 1517 I'll get a remainder of 62."

Verifier: "You're right, and I had no way of computing the square root of 62 because I didn't know the square root of either 1251 or 821. Let's do this a few more times and then I'll be very certain that you're giving me perfect square numbers and that you know the square root of 1251."

Explanation: The secret square root of 1251 is 94, and the square root of 821 is 83. When the Verifier asked for the square root of 62, the Prover multiplied 94 times 83, which leaves a remainder of 217 after dividing by 1517. For large numbers, it's easy to find a modular square but practically impossible to find a modular square root. A smart card can prove I know a large square root without giving away any information.

The name of Gus Simmons is sprinkled liberally through the literature of zero-knowledge proofs, validations, public-key cryptography, and factoring of large numbers. After hearing him speak I was inspired to come home and finally gain a rudimentary understanding of both public-keys and zero-knowledge. Our thanks to Bill Fienning and Dusty Cravens for promoting this most interesting meeting, and to Gus Simmons for a stimulating talk.