1072-00-266 **S. Dov Gordon*** (ams@dovgordon.com). *Secure Computation.*

Playing chess over the telephone is easy. But what about playing poker? This seems much harder! How do you shuffle the cards? Do you need a trusted party to deal them? How do you know that your opponent has no aces up their sleeve?! Surprisingly, in 1981, Shamir, Rivest and Adleman answered these questions by demonstrating a protocol for playing "mental poker" that does not rely on any trusted party. (They used the same mathematics that appeared in their now-indispensable RSA encryption scheme.) The next year, Andrew Yao generalized the question to arbitrary functions: can two players, each holding private data, interact to compute some function of that data, F(x1, x2), without revealing anything more than the output? He provided an elegant solution, introducing the area of research that we now call "secure computation".

Yao's work was followed by thirty years of research in secure computation. Until recently, this line of work was mainly of theoretical interest. Today, technological advancement is creating both the need for secure computation, and, for the first time, the ability to use it. In this talk we will define secure computation, survey some of the early theoretical results, and describe some of the opportunities and challenges that face the field today. (Received June 29, 2011)