HOW TO SHARE A SECRET

Prof. Franck Leprevost

Humanity needs safe communications for a very large set of reasons: the protection of State secrets, the efficiency of military plans, or the discretion of a secret love. Whatever the reason is, an appropriate technology is required. During thousands of years, symmetric-key cryptology was the single approach, knowing of course an increasing sophistication with time. However, at the very core of its concept resides a difficulty: the initial key exchange. In the mid-1970's a new concept emerged: public-key cryptology. Difife and Hellman proposed a key-exchange protocol to solve the draw-back of symmetric-key cryptology. The security of this protocol relies on the difficulty to solve a mathematical problem, the so-called Discrete Logarithm Problem (DLP) in a cyclic group G. Diffie-Hellman proposed to use for G the group $\Fp^*$ of non-zero elements of the finite field $\Fp$ for a large prime p. DLP over $\Fp^*$ can be solved in sub-exponential time, what leads, even nowadays, to a fairly secure key-exchange protocol based on $\Fp^*$. Since DLP can be expressed in any cyclic group, it was natural to look for alternatives.

In the mid-1980's, Koblitz and Miller (independently) proposed to use elliptic curves defined over a finite field, and defined the Elliptic Curve Discrete Logarithm Problem (ECDLP). According to today's knowledge, ECDLP in general can not be solved with methods faster than exponential. This leads to an even more secure key-exchange protocol than the original one proposed by Diffie and Hellman. However, some very specific attacks have been designed in the past decades, using very sophisticated mathematics. But no general attack has been developed so far. To do so, probably a new idea is necessary. This talk starts gently, but aims at presenting the state-of-the-art regarding ECDLP over $\Fp$ for a large prime p. Hence its second half is quite technical.

Lecture co-financed by the European Union in scope of the European Social Fund

HUMAN CAPITAL
HUMAN – BEST INVESTMENT!

EUROPEAN UNION
EUROPEAN
SOCIAL FUND