1040-11-66 **Fabio Borges*** (borges@lncc.br), Av. Getulio Vargas, 333, Petropolis, Rio 25.651-075, Brazil.
This work shows how to provide security with Elliptic Curves. Through cryptographic algorithms, authentication methods could be improved, having impacts even in car anti-theft systems. Preliminary report.

An Elliptic Curve (EC) could be endowed with a special operation to form an abelian group. Let $\mathbb{F}$ be a field not of characteristic 2 or 3, and suppose $c, d \in \mathbb{F}$ and $y^2 = x^3 + cx + d$, if $4c^3 + 27d^2 \neq 0$ then a set of ordered pairs (x, y) together with a element called *point of infinite* ∞ yield an EC Group Ω. An interesting propriety for cryptography is the EC Discrete Logarithm Problem (ECDLP), which is similar to the discrete logarithm problem on integers, i.e. it is infeasible to find n in $b = na$ where $a, b \in \Omega$ and $n \in \mathbb{N}$. This property is used to improve the authentication, as far my knowledge goes, most part of security incidents involves logins. We could protect it joining login and password to form a bijection with $\mathbb{N}$. Next, we compute $b = na$ where a is a point with relatively large order, so we can validated b iif is equal to an identification previously stored in the computer. Currently, the authentication methods uses a hash function on password, and cannot be used with login because these functions are injective but not bijective. Another interesting application is to protect a vehicle with the authentication using EC, however, the car must have its own computer that must be unbreakable. (Received January 22, 2008)