Una aplicación de los códigos correctores en criptografía: el problema de las votaciones electrónicas

Policarpo Abascal Fuentes

Dpto. de Matemáticas
Universidad de Oviedo
Edificio de Energía. Campus de Viesques. 33203-Gijón
abascal@epsig.uniovi.es

Ante la demanda del uso de servicios telemáticos para abordar situaciones y problemas que, tradicionalmente, han venido apoyándose en el intercambio de información sobre papel y otras formas convencionales de comunicación, la criptografía ha tomado un papel muy relevante.

La cuestión de las votaciones también ha sucumbido ante tal empuje, pero notemos que en un proceso de votación son muchos los requisitos que se necesitan para certificar un seguro funcionamiento. Se trata, entonces, de que los sistemas de votaciones electrónicas avalen, al menos, las mismas condiciones ya garantizadas por el sistema tradicional de voto presencial: transparencia, democracia, privacidad, verificabilidad, ...

Ya han sido propuestos diversos esquemas de votación electrónica. Aquí proponemos, con los códigos correctores de errores, sistemas en los que se garanticen las propiedades de privacidad y verificabilidad.

Nuestro objetivo es seguir trabajando en la construcción de un protocolo satisfactorio en el sentido de cumplir la mayor cantidad de condicionantes democráticos tradicionales trasladados al caso electrónico.