Internet voting: the heart of the matter

Internet voting is a key tool when trying to improve electoral processes in democratic countries: allows voters who due to their personal circumstances are not able to vote in paper to participate, improves the accuracy of the results and reduces the logistic and financial cost of organizing an election. Nevertheless, it also introduces new techonlogical and security challenges which are not present in traditional elections. Some risks that tend to be highlighted include: that someone knows how a voter has voted, that the voting device modifies the selections made by the voter, or that a voter is impersonated. Some are unique to Internet voting, while other require mitigation measures regardless of the voting channel. In that sense, mathematics is essential when making internet voting systems secure.

Encryption, digital signatures, zero-knowledge proofs and secret sharing schemes are some of the cryptographic primitives which are used to meet security requirements such as voter's privacy, vote integrity or verifiabiliaty. Voting options might be encrypted using the ElGamal cryptosystem instantiated over finiste fields or elliptic curves, and the resulting ciphertext can be signed using the RSA cryptosystem whose security is based on the hardness of factoring the product of two large primes. Then, the private key can be distributed among a number of authorities using a Shamir secret sharing scheme based on polynomial interpolation over finite fields. Thus, cryptography and consequently mathematics are a fundamental piece of secure internet voting systems.

As any other application running online and making use of public-key cryptography, internet voting systems are also vulnerable to the increasingly well-known quantum computing attacks. If large-scale quantum computers are ever built, they would commpletely break many public-key cryptosystems, including RSA and elliptic curves. For this reason, there are several alternatives which have been proposed, all of them ensuring security against both quantum and classical computers. Probably, the most promising one is lattice-based cryptography, whose securtiy relies on the hardness of solving lattice problems such as the shortest vector problem. In the internet voting context, quantum computers pose a risk for privacy in the long-term. Data published during an election (such as encrypted votes), must be protected by using quantum-resistant algorithms if voter's privacy is to be preserved in the future from a quantum adversary. LPR encryption scheme, CRYSTALS-Dilithium and BKLP commitment scheme are some of the lattice-based algorithms proposed for substituting current cryptography used in internet voting systems.