Electronic Voting Protocols
How can we trust this technology?

Did you say « Protocols »?
Yes, we use cryptographic protocols which allow us to vote electronically using our computers or voting machines.

They consist in a list of predefined steps (like a cooking recipe) to accomplish a goal (in this case, to vote) which use different cryptographic related functions (such as encryption, electronic signatures, ...)

The everyday life provides us with a lot of examples:
- Credit cards
- Secured Internet (https)

Sounds risky, no?
Indeed, your vote is a sensitive data that needs to be protected. To achieve this, there is a need of guarantees that come from different security properties.

One of the most important is privacy. It is better to be sure that there is no possibility (for someone else) to learn how you voted.

There is also integrity: The result of the election must accurately reflect all the votes that have been cast during the voting process.

Is it really more convenient?
There are several benefits:

You can sometimes vote directly from your home, a benefit which can reduce the number of abstainers. This « new » way of voting can motivate people, especially the youngest.

It is also more efficient. Computers count much faster (and with no mistakes!) the results. This prevents human errors in counting.

Is it really safe?
Yes and no… Each system is different. It depends on how it works and how they are implemented. Some are vulnerable:

- Machines Diebold (USA) (Attack by Candice Hoke, 2008.)
- Paperless Voting Machines (India) (Attack by A. Halderman, R. Gonggrijp, 2010.)

Others are safe and satisfies good security properties like Helios, Civitas, …

How can we prove that a protocol satisfies a security property?
To do so, you can use formal analysis, a symbolic study of your system and property. This mathematical approach and reasoning provides you with a proof describing if your system satisfies (or not) the property.

Here is how you can do it:

As a first step, you model the system and your property. This should be as precise as you can, to ensure the accuracy of your result.

Then, you perform a proof, a mathematical one, which looks almost like the others.

Finally, you have your answer: the system satisfies (or not) your property.

What is your thesis about?
In my thesis, Formal Analysis of E-Voting Protocols, I study the security of existing voting systems. (One of them was used to vote using Internet in Norway in 2012 and is still in use.)

I also develop a new software tool to deal automatically with these (often) complicated systems instead of doing all the proofs by hand by myself. It is always better to make a computer doing the hard work! (As I said before, there are less human errors. 😊)

What should I remember?
A non-verified system can be dangerous. You’ll never use a poor safe to protect valuable assets, and prefer a safe that brings warranties. It should be the same with your vote and electronic voting in general. We must ensure the security of a system before using it, especially if it is deployed for important elections.