Title (en)

VERIFIABLE ELECTRONIC VOTING METHOD

Title (de)

VERIFIZIERBARES ELEKTRONISCHES WÄHLVERFAHREN

Title (fr)

PROCÉDÉ DE VÉRIFICATION D'UN VOTE ÉLECTRONIQUE

Publication

EP 2382606 B1 20190213 (EN)

Application

EP 08875902 A 20081223

Priority

IB 2008055521 W 20081223

Abstract (en)

[origin: WO2010073065A1] The present invention allows a voter to verify that the votes he cast were properly counted while maintaining vote anonymity. Anonymity and transparency are balanced such that voters have proofs showing the votes they cast are properly counted, but the same proofs are meaningless to the others. In this way, transparency is successes without exposing voter privacy. While voters cast their votes, for example in a voting machine, a witness is required to verify that the vote is counted properly. A witness proving voter privacy is implemented by using a voter superiority over the voting system. This strength is used to solve transparency-anonymity problem: Voting system cannot guess next step of the voter, and when all steps are revealed, it is not allowed the system to get back. Voters present a random choice from a predetermined set of random choices together with each voting choice in the voting process, and he expects an algorithm output as a proof of including voting choices and random choices of the voting choices. After receiving algorithm output and making sure of it not to be changed in the coming steps, he presents all random choices of each possible choice, and gets the random choices from the voting system as he presents. Because, the voting system can not know random choices of the other possible choices, a possible malware code in the system can not dare to change voting choices of the voter. If it dares and the random choices of the not intended voting choices it selects is not as the random choices of the not intended voting choice entered following to receiving the algorithm output by the voter, then this illegal modification is revealed. The possibility of reveal increases exponentially, as the voting system's illegal modified votes increase. Algorithm output is an output of a cryptographic algorithm getting inputs that comprises voting choices and random choices of the voting choices and using a secret.

IPC 8 full level

G07C 13/00 (2006.01)

CPC (source: EP)

G07C 13/00 (2013.01)

Designated contracting state (EPC)

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MT NL NO PL PT RO SE SI SK TR

DOCDB simple family (publication)

WO 2010073065 A1 20100701; EP 2382606 A1 20111102; EP 2382606 B1 20190213; ES 2728313 T3 20191023

DOCDB simple family (application)

IB 2008055521 W 20081223; EP 08875902 A 20081223; ES 08875902 T 20081223