

New electronic voting system for future elections invented

Submitted by: BlueSky Public Relations Ltd

Wednesday, 31 May 2017

PRESS RELEASE: FOR IMMEDIATE RELEASE

New electronic voting system for future elections invented

A new secure electronic voting system has been designed by a team of mathematicians from Université Paris-Saclay (<https://www.universite-paris-saclay.fr/en>)'s University of Versailles, Inpher, Gemalto and CEA LIST.

The new protocol could be used in elections across the globe.

Inspired by existing e-voting systems, the researchers present a simple and transparent scheme that easily confirms the correctness of the final election result, guarantees privacy and allows verifiability.

The scheme follows the essential components for an e-voting protocol; no one should be able to retrieve the vote of a particular user, each voter should be able to verify that their vote was included, and the final vote count should correspond with the sum of all the legitimate votes. Their system also publicly detects any attempt to cheat.

“Designing security for electronic based systems is much more intricate than traditional paper-based systems,” Ilaria Chillotti, from Université Paris-Saclay. “Until now, all designs were based on assumptions that could be compromised by advanced quantum computers. Our design is the first step to achieving a quantum resistant e-voting scheme.

“Our scheme differs from existing e-voting protocols that have been used for medium-scale elections by changing the underlying design with a lattice-based fully homomorphic encryption design.”

Fully homomorphic encryption allows computations to be carried out on encrypted information.

The paper was published in Post-Quantum Cryptography 2016, part of the Lecture Notes in Computer Science (<https://link.springer.com/bookseries/558>) book series.

/ENDS

For more information, a copy of the paper, or to speak to the authors, contact Stephanie Mullins at BlueSky PR on smullins@bluesky-pr.com or call +44 (0)1582 790 706.