

Oops. Cryptographers cancel election results after losing decryption key.



One of the world's premier security organizations has canceled the results of its annual leadership election after an official lost an encryption key needed to unlock results stored in a verifiable and privacy-preserving voting system.

The International Association of Cryptologic Research (IACR) said Friday that the votes were submitted and tallied using Helios, an open source voting system that uses peer-reviewed cryptography to cast and count votes in a verifiable, confidential, and privacy-preserving way. Helios encrypts each vote in a way that assures each ballot is secret. Other cryptography used by Helios allows each voter to confirm their ballot was counted fairly.

An “honest but unfortunate human mistake”

Per the association’s bylaws, three members of the election committee act as independent trustees. To prevent two of them from colluding to cook the results, each trustee holds a third of the cryptographic key material needed to decrypt results.

“Unfortunately, one of the three trustees has irretrievably lost their private key, an honest but unfortunate human mistake, and therefore cannot compute their decryption share,” the IACR said. “As a result, Helios is unable to complete the decryption process, and it is technically impossible for us to obtain or verify the final outcome of this election.”

To prevent a similar incident, the IACR will adopt a new mechanism for managing private keys. Instead of requiring all three chunks of private key material, elections will now require only two. Moti Yung, the trustee who was unable to provide his third of the key material, has resigned. He’s being replaced by Michel Abdalla.

The IACR is a nonprofit scientific organization providing research in cryptology and related fields. Cryptology is the science and practice of designing computation and communication systems that remain secure in the presence of adversaries. The association is holding a new election that started Friday and runs through December 20.

<https://arstechnica.com/security/2025/11/cryptography-group-cancels-election-results-after-official-loses-secret-key/>