Automated Ballot Stuffing with an Encrypted Vote

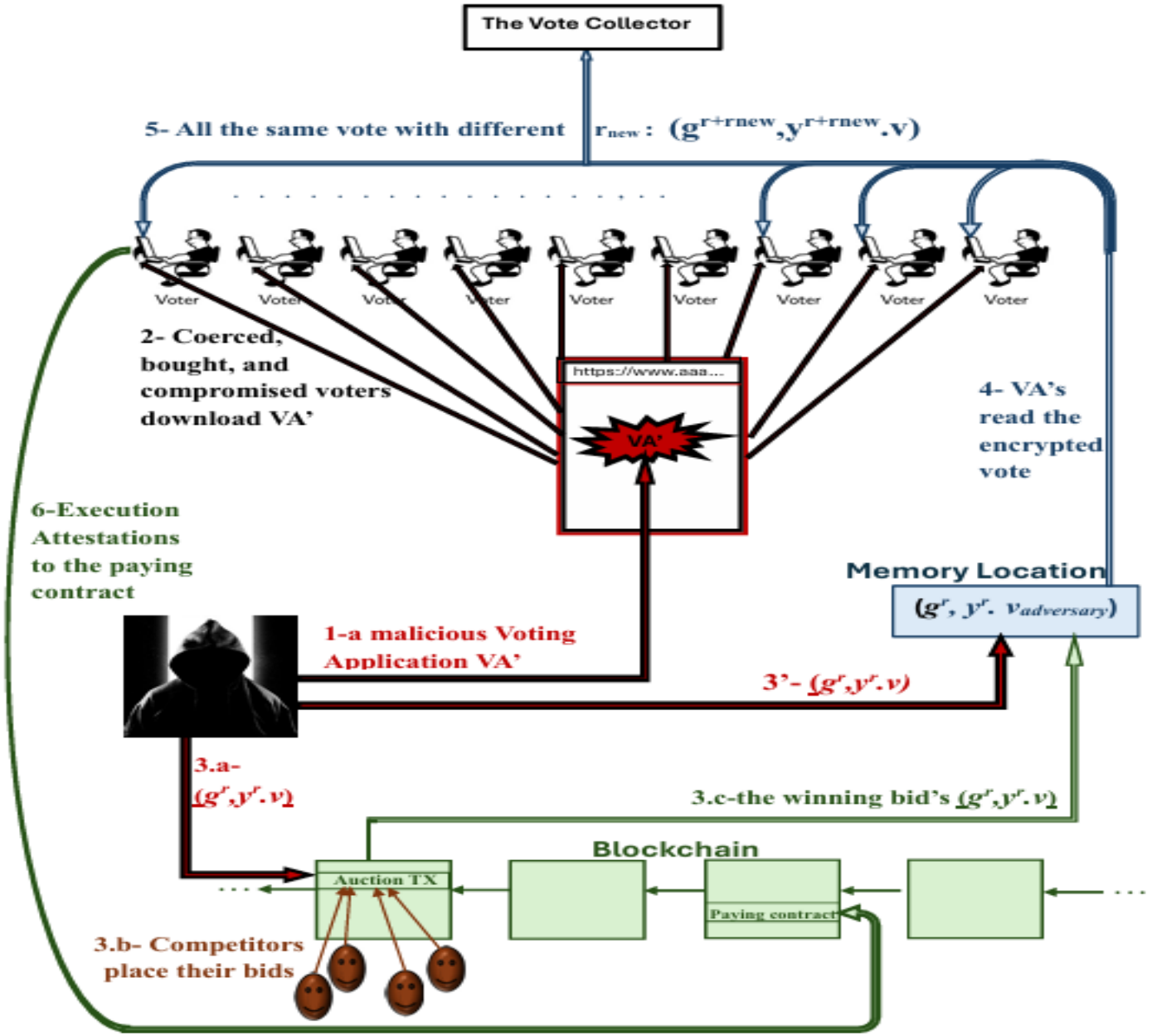
A Large-Scale Attack on the Estonian Internet Voting System (**IVXV**) and its Mitigation

Shymaa M. Arafat

Associate Professor (Independent, https://github.com/DrShymaa2022)
shar.academic@gmail.com, shymaa.arafat@gmail.com

Malicious Voting Application + Online Auctions + Execution Attestations =>

Cloning an anonymous vote



We put alarms on how online coding via smart contracts can add new threats to e-voting, and how severe could be not authenticating the Voting Application for IVXV (it is not just the Pereira attack)

Mitigations

1-Allow a *file digest* check for the Voting Application *batched into 1 button click*; still doesn't help dark web compromised voter credentials.

2-Assign an authentication key pair to the official voting application. *Allow only usage of pre-registered private voting applications with a stored public key at the voting server* after *scanning them for any malicious code.*

Both solutions can *use post-quantum hash based digital signatures*

Extra Safeguards:

-a *humanity check* for the Vote Collector to be sure the interaction process with VA is not automated (Swisspost).

-Let the verification application display an extra message "*You voted using (the official/a different) voting application*".

-a *"Reject all"* option for boycotters to minimize the effect of stolen credentials.