1 Pre-Election Audit: Two tables are posted online, with the content of each table entry encrypted (blue rectangles). Auditors randomly select rows of the first table for decryption (ballot numbers 2, 3, 6, 7, 9, shown after selection with blue removed). This reveals details of ballots (examples shown with red “X”) that would have been printed had those rows not been audited. Rows of the second table are then decrypted (rows 1, 3, 4, 5, 8, in the example) are printed and supplied to each voter at the polling place.

2 Polling-Place Voting: Those ballots not decrypted in audit (ballot numbers 1, 4, 5, 8, in the example) are printed and supplied to each voter at the polling place.

3 Post-Election Audit: After polls close, columns of orange dots record the side, left or right, of each mark scanned. Also, the letters that should be printed on the receipt are decrypted. The results are posted, for anyone to count, as purple dots. Audit is by decrypting randomly either the left or right side of second-table rows (in the example: right, left, right, left). Anyone can then check that green dots are on the same side of the column as the corresponding orange or purple dots for straight-through arrows, and on opposite sides for loop arrows. Randomness in the audit, not encryption, ensures with very high probability that posted marks are tallied correctly—but without linking results to ballots.

4 Verifying at Home: To check that his or her vote was posted correctly, a voter can use a browser to go to an election website and enter the serial number from the receipt. The image of the receipt should then be provided for download. Voters check that the two match and that marks are in the same positions on the display as on the paper receipt.