## Appendix

The full table of our key classification experiments is shown below.

Symbols $p_1, q_1, p_2, q_2$ denote the proportions of keys that meet the conditions in corresponding groups. For simplicity, we use the common $v_2[k-1]$ to represent four groups: $v_2[k] = 0 \& v_3[k-1] = 0$ (with $p_1$), $v_2[k] = 0 \& v_3[k-1] = 1$ (with $q_1$), $v_2[k] = 1 \& v_3[k-1] = 0$ (with $p_2$) and $v_2[k] = 1 \& v_3[k-1] = 1$ (with $p_2$).

Analysis of the expected success rate (for both of $k_0$ and $k_1$) has been presented in the paper.

**Table 1.** Results of key classification experiments (full table)

| $k$ | conditions | boundline | $p_1$ | $q_1$ | $p_2$ | $q_2$ | $k_0$ | $k_1$ |
|---|---|---|---|---|---|---|---|---|
| 0 | / | $e_{26} \leq -5.255$ | 0% | / | 100% | / | 100% | / |
| 1 | $v_2[k-1] = 0$ | $e_{27} \leq -5.285$ | 0% | 0% | 100% | 100% | 100% | 50% |
| 1 | $v_2[k-1] = 1$ | $e_{30} \leq -7.635$ | 19.5% | 51.0% | 49.7% | 16.7% | 51.2% | 61.8% |
| 2 | $v_2[k-1] = 0$ | $e_{44} \leq -6.465$ | 0% | 0.6% | 99.6% | 51.1% | 99.6% | 62.2% |
| 2 | $v_2[k-1] = 1$ | $e_{44} \leq -6.535$ | 0.3% | 98.7% | 48.5% | 0% | 75.1% | 86.6% |
| 3 | $v_2[k-1] = 0$ | $e_{29} \leq -5.485$ | 0% | 3.8% | 96.4% | 27.5% | 96.8% | 67.0% |
| 3 | $v_2[k-1] = 1$ | $e_{29} \leq -5.475$ | 4.1% | 97.1% | 28.4% | 0% | 84.4% | 79.0% |
| 4 | $v_2[k-1] = 0$ | $e_{46} \leq -6.515$ | 0% | 10.5% | 97.2% | 23.1% | 93.7% | 70.1% |
| 4 | $v_2[k-1] = 1$ | $e_{46} \leq -6.525$ | 11.4% | 96.6% | 22.0% | 0% | 87.5% | 75.4% |
| 5 | $v_2[k-1] = 0$ | $e_{47} \leq -6.505$ | 0% | 13.3% | 97.6% | 19.9% | 92.4% | 71.9% |
| 5 | $v_2[k-1] = 1$ | $e_{31} \leq -5.685$ | 13.1% | 96.3% | 17.4% | 0% | 89.7% | 73.7% |
| 6 | $v_2[k-1] = 0$ | $e_{32} \leq -4.825$ | 0% | 13.2% | 96.4% | 15.9% | 91.9% | 72.0% |
| 6 | $v_2[k-1] = 1$ | $e_{32} \leq -4.825$ | 14.1% | 96.4% | 16.0% | 0% | 90.4% | 73.2% |
| 7 | $v_2[k-1] = 0$ | $e_{33} \leq -4.745$ | 0% | 15.4% | 96.5% | 15.6% | 90.8% | 72.7% |
| 7 | $v_2[k-1] = 1$ | $e_{33} \leq -4.725$ | 16.5% | 98.0% | 16.6% | 0% | 90.9% | 73.8% |
| 8 | $v_2[k-1] = 0$ | $e_{34} \leq -4.835$ | 0% | 15.3% | 96.4% | 16.4% | 90.9% | 72.5% |
| 8 | $v_2[k-1] = 1$ | $e_{34} \leq -4.845$ | 15.3% | 96.2% | 15.5% | 0% | 90.6% | 72.6% |
| 9 | $v_2[k-1] = 0$ | $e_{51} \leq -6.515$ | 0% | 16.7% | 97.3% | 15.7% | 90.5% | 73.5% |
| 9 | $v_2[k-1] = 1$ | $e_{51} \leq -6.545$ | 15.8% | 95.7% | 15.3% | 0% | 90.6% | 72.2% |
| 10 | $v_2[k-1] = 0$ | $e_{52} \leq -6.515$ | 0% | 15.9% | 97.1% | 15.8% | 90.8% | 73.2% |
| 10 | $v_2[k-1] = 1$ | $e_{52} \leq -6.505$ | 16.5% | 97.2% | 16.3% | 0% | 90.7% | 73.2% |
| 11 | $v_2[k-1] = 0$ | $e_{53} \leq -6.515$ | 0% | 16.2% | 97.2% | 17.9% | 90.8% | 72.8% |
| 11 | $v_2[k-1] = 1$ | $e_{53} \leq -6.535$ | 16.4% | 96.3% | 15.6% | 0% | 90.7% | 72.5% |
| 12 | $v_2[k-1] = 0$ | $e_{54} \leq -6.525$ | 0% | 14.8% | 96.4% | 16.5% | 91.1% | 72.3% |
| 12 | $v_2[k-1] = 1$ | $e_{54} \leq -6.565$ | 14.8% | 94.9% | 15.0% | 0% | 90.3% | 71.9% |
| 13 | $v_2[k-1] = 0$ | $e_{55} \leq -6.515$ | 0% | 18.0% | 97.0% | 16.3% | 89.8% | 73.5% |
| 13 | $v_2[k-1] = 1$ | $e_{55} \leq -6.485$ | 17.9% | 97.7% | 17.5% | 0% | 90.3% | 73.4% |
| 14 | $v_2[k-1] = 0$ | $e_{56} \leq -6.565$ | 0% | 14.5% | 94.4% | 13.8% | 90.3% | 71.6% |
| 14 | $v_2[k-1] = 1$ | $e_{56} \leq -6.515$ | 16.2% | 96.8% | 17.3% | 0% | 90.0% | 73.2% |
| 15 | $v_2[k-1] = 0$ | $e_{57} \leq -6.525$ | 0% | 15.9% | 96.5% | 15.5% | 90.6% | 72.9% |
| 15 | $v_2[k-1] = 1$ | $e_{57} \leq -6.505$ | 17.4% | 97.2% | 17.0% | 0% | 90.3% | 73.1% |
| 16 | $v_2[k-1] = 0$ | $e_{42} \leq -5.585$ | 0% | 14.4% | 96.3% | 14.9% | 91.2% | 72.5% |
| 16 | $v_2[k-1] = 1$ | $e_{42} \leq -5.565$ | 16.2% | 97.1% | 15.5% | 0% | 91.0% | 73.0% |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 17 | $v_2[k-1]=0$ | $e_{43} \leq -5.575$ | 0% | 13.8% | 95.6% | 16.0% | 91.2% | 71.7% |
| 17 | $v_2[k-1]=1$ | $e_{59} \leq -6.545$ | 15.3% | 96.3% | 15.0% | 0% | 90.9% | 72.6% |
| 18 | $v_2[k-1]=0$ | $e_{60} \leq -6.515$ | 0% | 16.8% | 96.5% | 16.8% | 90.2% | 72.8% |
| 18 | $v_2[k-1]=1$ | $e_{60} \leq -6.535$ | 15.7% | 96.6% | 15.9% | 0% | 90.6% | 72.9% |
| 19 | $v_2[k-1]=0$ | $e_{61} \leq -6.515$ | 0% | 16.5% | 96.9% | 17.5% | 90.5% | 72.8% |
| 19 | $v_2[k-1]=1$ | $e_{61} \leq -6.535$ | 16.5% | 96.3% | 15.7% | 0% | 90.6% | 72.5% |
| 20 | $v_2[k-1]=0$ | $e_{62} \leq -6.535$ | 0% | 16.2% | 96.5% | 15.6% | 90.4% | 72.9% |
| 20 | $v_2[k-1]=1$ | $e_{46} \leq -5.485$ | 15.1% | 96.5% | 16.0% | 0% | 90.5% | 73.0% |
| 21 | $v_2[k-1]=0$ | $e_{63} \leq -6.515$ | 0% | 16.4% | 97.2% | 16.5% | 90.6% | 73.2% |
| 21 | $v_2[k-1]=1$ | $e_{47} \leq -5.455$ | 16.0% | 97.3% | 15.7% | 0% | 91.0% | 73.2% |
| 22 | $v_2[k-1]=0$ | $e_{48} \leq -5.465$ | 0% | 16.4% | 96.6% | 16.7% | 90.4% | 72.8% |
| 22 | $v_2[k-1]=1$ | $e_{48} \leq -5.445$ | 17.7% | 97.4% | 18.1% | 0% | 89.9% | 73.4% |
| 23 | $v_2[k-1]=0$ | $e_{49} \leq -5.455$ | 0% | 17.5% | 96.8% | 17.7% | 89.9% | 72.9% |
| 23 | $v_2[k-1]=1$ | $e_{49} \leq -5.475$ | 16.0% | 96.0% | 16.4% | 0% | 90.1% | 72.6% |
| 24 | $v_2[k-1]=0$ | $e_{50} \leq -5.485$ | 0% | 14.1% | 96.1% | 15.7% | 91.3% | 72.1% |
| 24 | $v_2[k-1]=1$ | $e_{50} \leq -5.465$ | 15.5% | 96.9% | 16.3% | 0% | 90.5% | 73.2% |
| 25 | $v_2[k-1]=0$ | $e_{51} \leq -5.455$ | 0% | 16.0% | 97.2% | 16.7% | 90.8% | 73.0% |
| 25 | $v_2[k-1]=1$ | $e_{51} \leq -5.465$ | 16.4% | 96.9% | 16.2% | 0% | 90.6% | 73.0% |
| 26 | $v_2[k-1]=0$ | $e_3 \leq -8.635$ | 0% | 8.3% | 98.2% | 8.8% | 95.0% | 73.6% |
| 26 | $v_2[k-1]=1$ | $e_3 \leq -8.605$ | 9.2% | 98.6% | 8.7% | 0% | 95.0% | 73.9% |
| 27 | $v_2[k-1]=0$ | $e_5 \leq -6.515$ | 0% | 15.7% | 96.1% | 16.9% | 90.5% | 72.3% |
| 27 | $v_2[k-1]=1$ | $e_5 \leq -6.525$ | 15.8% | 96.5% | 14.8% | 0% | 91.1% | 72.6% |
| 28 | $v_2[k-1]=0$ | $e_{17} \leq -8.995$ | 0% | 15.9% | 100% | 15.9% | 92.0% | 75.0% |
| 28 | $v_2[k-1]=1$ | $e_{17} \leq -8.995$ | 16.5% | 100% | 17.5% | 0% | 91.2% | 75.3% |
| 29 | $v_2[k-1]=0$ | $e_7 \leq -6.525$ | 0% | 16.2% | 96.8% | 15.6% | 90.6% | 73.1% |
| 29 | $v_2[k-1]=1$ | $e_7 \leq -6.535$ | 16.3% | 96.1% | 15.8% | 0% | 90.5% | 72.4% |
| 30 | $v_2[k-1]=0$ | $e_8 \leq -6.515$ | 0% | 15.7% | 97.3% | 15.7% | 91.0% | 73.3% |
| 30 | $v_2[k-1]=1$ | $e_8 \leq -6.535$ | 16.9% | 96.3% | 15.6% | 0% | 90.7% | 72.3% |
| 31 | $v_2[k-1]=0$ | $e_9 \leq -6.505$ | 0% | 16.8% | 97.3% | 17.1% | 90.5% | 73.2% |
| 31 | $v_2[k-1]=1$ | $e_9 \leq -6.525$ | 15.8% | 96.3% | 16.3% | 0% | 90.3% | 72.8% |
| 32 | $v_2[k-1]=0$ | $e_{58} \leq -5.485$ | 0% | 15.6% | 96.6% | 16.5% | 90.8% | 72.6% |
| 32 | $v_2[k-1]=1$ | $e_{10} \leq -6.515$ | 16.6% | 97.4% | 16.4% | 0% | 90.7% | 73.3% |
| 33 | $v_2[k-1]=0$ | $e_{59} \leq -5.495$ | 0% | 14.7% | 96.3% | 16.0% | 91.1% | 72.3% |
| 33 | $v_2[k-1]=1$ | $e_{11} \leq -6.525$ | 16.7% | 96.7% | 16.3% | 0% | 90.5% | 72.8% |
| 34 | $v_2[k-1]=0$ | $e_{12} \leq -6.535$ | 0% | 15.6% | 96.8% | 16.0% | 90.8% | 72.8% |
| 34 | $v_2[k-1]=1$ | $e_{60} \leq -5.485$ | 17.0% | 96.6% | 15.9% | 0% | 90.7% | 72.6% |
| 35 | $v_2[k-1]=0$ | $e_{61} \leq -5.495$ | 0% | 15.0% | 96.2% | 15.4% | 90.9% | 72.5% |
| 35 | $v_2[k-1]=1$ | $e_{61} \leq -5.495$ | 14.8% | 96.0% | 16.0% | 0% | 90.3% | 72.8% |
| 36 | $v_2[k-1]=0$ | $e_{14} \leq -6.555$ | 0% | 15.3% | 95.6% | 15.7% | 90.5% | 72.1% |
| 36 | $v_2[k-1]=1$ | $e_{14} \leq -6.525$ | 17.6% | 96.9% | 17.8% | 0% | 89.8% | 73.1% |
| 37 | $v_2[k-1]=0$ | $e_{15} \leq -6.565$ | 0% | 14.9% | 95.3% | 15.1% | 90.6% | 72.0% |
| 37 | $v_2[k-1]=1$ | $e_{63} \leq -5.485$ | 16.3% | 96.4% | 15.9% | 0% | 90.5% | 72.6% |
| 38 | $v_2[k-1]=0$ | $e_{16} \leq -6.535$ | 0% | 16.3% | 97.0% | 16.0% | 90.6% | 73.1% |
| 38 | $v_2[k-1]=1$ | $e_{16} \leq -6.565$ | 14.6% | 96.3% | 15.1% | 0% | 90.9% | 72.8% |
| 39 | $v_2[k-1]=0$ | $e_{16} \leq -8.995$ | 0% | 19.4% | 93.0% | 20.3% | 87.5% | 70.7% |
| 39 | $v_2[k-1]=1$ | $e_{16} \leq -8.985$ | 18.7% | 94.0% | 19.1% | 0% | 88.0% | 71.5% |
| 40 | $v_2[k-1]=0$ | $e_2 \leq -3.925$ | 0% | 23.9% | 90.8% | 24.1% | 84.5% | 69.9% |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 40 | $v_2[k-1]=1$ | $e_{17} \leq -6.155$ | 23.4% | 90.4% | 22.4% | 0% | 85.1% | 69.4% |
| 41 | $v_2[k-1]=0$ | $e_3 \leq -4.195$ | 0% | 21.3% | 93.3% | 20.7% | 86.7% | 71.3% |
| 41 | $v_2[k-1]=1$ | $e_3 \leq -4.185$ | 21.1% | 93.3% | 21.9% | 0% | 86.4% | 71.3% |
| 42 | $v_2[k-1]=0$ | $e_{19} \leq -8.995$ | 0% | 5.1% | 99.4% | 4.9% | 97.2% | 74.6% |
| 42 | $v_2[k-1]=1$ | $e_{19} \leq -8.965$ | 5.2% | 99.6% | 5.4% | 0% | 97.1% | 74.8% |
| 43 | $v_2[k-1]=0$ | $e_{21} \leq -5.995$ | 0% | 12.8% | 96.6% | 13.1% | 92.2% | 72.7% |
| 43 | $v_2[k-1]=1$ | $e_{21} \leq -5.955$ | 13.8% | 97.7% | 13.7% | 0% | 92.1% | 73.4% |
| 44 | $v_2[k-1]=0$ | $e_{22} \leq -5.815$ | 0% | 12.4% | 98.6% | 12.2% | 93.2% | 74.1% |
| 44 | $v_2[k-1]=1$ | $e_{22} \leq -5.855$ | 11.1% | 96.5% | 11.4% | 0% | 92.7% | 72.8% |
| 45 | $v_2[k-1]=0$ | $e_{23} \leq -5.765$ | 0% | 12.3% | 98.1% | 14.0% | 93.0% | 73.3% |
| 45 | $v_2[k-1]=1$ | $e_{23} \leq -5.775$ | 12.3% | 97.9% | 13.3% | 0% | 92.4% | 73.9% |
| 46 | $v_2[k-1]=0$ | $e_8 \leq -5.415$ | 0% | 14.0% | 97.0% | 15.2% | 91.7% | 72.8% |
| 46 | $v_2[k-1]=1$ | $e_8 \leq -5.415$ | 14.4% | 97.5% | 14.5% | 0% | 91.7% | 73.4% |
| 47 | $v_2[k-1]=0$ | $e_{25} \leq -6.165$ | 0% | 9.4% | 98.7% | 9.5% | 94.7% | 74.1% |
| 47 | $v_2[k-1]=1$ | $e_{25} \leq -6.135$ | 10.7% | 99.4% | 10.5% | 0% | 94.5% | 74.5% |
| 48 | $v_2[k-1]=0$ | $e_{10} \leq -5.435$ | 0% | 20.2% | 96.2% | 20.5% | 88.4% | 72.6% |
| 48 | $v_2[k-1]=1$ | $e_{10} \leq -5.445$ | 19.6% | 95.2% | 18.7% | 0% | 88.7% | 71.8% |
| 49 | $v_2[k-1]=0$ | $e_{11} \leq -5.495$ | 0% | 15.9% | 94.8% | 16.1% | 89.9% | 71.7% |
| 49 | $v_2[k-1]=1$ | $e_{11} \leq -5.475$ | 16.6% | 96.0% | 16.2% | 0% | 90.2% | 72.4% |
| 50 | $v_2[k-1]=0$ | $e_{12} \leq -5.495$ | 0% | 16.3% | 96.2% | 15.1% | 90.3% | 72.9% |
| 50 | $v_2[k-1]=1$ | $e_{12} \leq -5.505$ | 15.1% | 95.6% | 15.6% | 0% | 90.3% | 72.3% |
| 51 | $v_2[k-1]=0$ | $e_{29} \leq -6.535$ | 0% | 15.8% | 96.4% | 15.7% | 90.6% | 72.7% |
| 51 | $v_2[k-1]=1$ | $e_{13} \leq -5.495$ | 15.2% | 95.7% | 15.7% | 0% | 90.3% | 72.4% |
| 52 | $v_2[k-1]=0$ | $e_{30} \leq -6.535$ | 0% | 16.3% | 95.9% | 16.1% | 90.1% | 72.5% |
| 52 | $v_2[k-1]=1$ | $e_{14} \leq -5.495$ | 15.1% | 96.1% | 15.6% | 0% | 90.6% | 72.7% |
| 53 | $v_2[k-1]=0$ | $e_{31} \leq -6.555$ | 0% | 14.9% | 95.1% | 15.8% | 90.5% | 71.7% |
| 53 | $v_2[k-1]=1$ | $e_{31} \leq -6.495$ | 17.4% | 97.9% | 18.3% | 0% | 90.0% | 73.8% |
| 54 | $v_2[k-1]=0$ | $e_{32} \leq -6.375$ | 0% | 16.3% | 97.2% | 17.2% | 90.7% | 73.0% |
| 54 | $v_2[k-1]=1$ | $e_{16} \leq -5.515$ | 13.9% | 94.6% | 14.1% | 0% | 90.6% | 71.6% |
| 55 | $v_2[k-1]=0$ | $e_{17} \leq -5.285$ | 0% | 16.6% | 97.9% | 16.1% | 90.8% | 73.8% |
| 55 | $v_2[k-1]=1$ | $e_{17} \leq -5.315$ | 14.2% | 96.6% | 15.4% | 0% | 90.8% | 73.1% |
| 56 | $v_2[k-1]=0$ | $e_{18} \leq -5.255$ | 0% | 18.1% | 98.2% | 14.7% | 90.2% | 74.6% |
| 56 | $v_2[k-1]=1$ | $e_{18} \leq -5.275$ | 15.6% | 96.7% | 15.1% | 0% | 91.1% | 72.8% |
| 57 | $v_2[k-1]=0$ | $e_{19} \leq -5.255$ | 0% | 15.1% | 97.5% | 13.8% | 91.4% | 73.7% |
| 57 | $v_2[k-1]=1$ | $e_{19} \leq -5.265$ | 15.6% | 96.5% | 14.3% | 0% | 91.4% | 72.4% |
| 58 | $v_2[k-1]=0$ | $e_{20} \leq -5.275$ | 0% | 13.8% | 94.6% | 13.2% | 90.8% | 71.8% |
| 58 | $v_2[k-1]=1$ | $e_{20} \leq -5.235$ | 15.2% | 97.7% | 15.9% | 0% | 91.1% | 73.7% |
| 59 | $v_2[k-1]=0$ | $e_{37} \leq -5.815$ | 0% | 14.9% | 97.4% | 14.3% | 91.4% | 73.4% |
| 59 | $v_2[k-1]=1$ | $e_{37} \leq -5.835$ | 13.5% | 96.4% | 14.7% | 0% | 91.1% | 73.0% |
| 60 | $v_2[k-1]=0$ | $e_{37} \leq -7.985$ | 0% | 11.0% | 95.6% | 10.8% | 92.5% | 72.1% |
| 60 | $v_2[k-1]=1$ | $e_{37} \leq -7.925$ | 13.3% | 97.4% | 13.6% | 0% | 92.1% | 73.4% |
| 61 | $v_2[k-1]=0$ | $e_{39} \leq -5.545$ | 0% | 14.1% | 98.4% | 12.8% | 92.2% | 74.2% |
| 61 | $v_2[k-1]=1$ | $e_{39} \leq -5.535$ | 14.7% | 98.2% | 13.0% | 0% | 92.7% | 73.4% |
| 62 | $v_2[k-1]=0$ | $e_{39} \leq -7.085$ | 0% | 21.7% | 90.8% | 20.6% | 85.5% | 70.1% |
| 62 | $v_2[k-1]=1$ | $e_{39} \leq -7.065$ | 21.1% | 93.1% | 21.9% | 0% | 86.3% | 71.2% |
| 63 | $v_2[k-1]=0$ | $e_{41} \leq -3.935$ | 88.8% | 88.8% | 90.3% | 89.3% | 50.9% | 50.2% |
| 63 | $v_2[k-1]=1$ | $e_{44} \leq -5.095$ | 28.3% | 29.1% | 29.9% | 30.9% | 51.2% | 50.3% |