work/queries to obtain next ciphertexts  $2^{104}$ total work/queries 2<sup>86</sup>  $2^{68}$ 2<sup>50</sup> 2<sup>32</sup> work  $2^{14}$ query 2<sup>3</sup> available failing ciphertexts