work/queries to obtain next ciphertexts  $2^{103}$ total work/queries 2<sup>85</sup> 2<sup>67</sup>  $2^{49}$ 2<sup>31</sup> work 2<sup>13</sup> query  $2^{1}$ 23 available failing ciphertexts