work/queries to obtain next ciphertexts  $2^{110}$ total work/queries  $2^{91}$ 2<sup>72</sup> 2<sup>53</sup> 2<sup>34</sup> work  $2^{15}$ query 2<sup>3</sup> available failing ciphertexts