Quantum-enhanced symmetric cryptanalysis for S-AES

A speedrun for

Alexey Moiseevskiy
Grover’s algorithm

Quadratic speedup is provided

$O(2^n) \rightarrow O(2^{n/2})$

Twice longer key required
Standard encryption routine

S-AES:
- 16-bit text
- 16-bit key
- 2 rounds

32 qubits – too many
Optimized encryption routine
Conclusions

- 23 qubits for general attack
- 19, 17, 15 or 11 qubits for attack with partial key leak
- Few enough for GPU-accelerated simulations or data-center format QPU
- The new algorithm is scalable and can be adapted for full AES attack
Thank you!
Alexey Moiseevskiy
+7 968 016 97 32
Aleksey.Moiseevsky@infotecs.ru
amoiseevskiy@gmail.com