Quantum Differential and Linear Cryptanalysis

Denis Denisenko

17.09.2020

Structure of the report

1. Quantum algoritms (Grover, quantum counting).
2. Quantum differential cryptanalysis.
3. Quantum counting as subprogram of Grover's search.
4. Quantum linear cryptanalysis.

Grover's quantum algorithm

Let $N = 2^n$, we want to «find» arbitrary solution among M possible solutions, $M < N/2$.

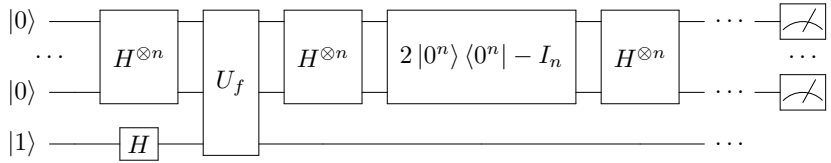


Figure 1: Grover's iteration «G» relatively the boolean function f.

- If $|\alpha\rangle \equiv \frac{1}{\sqrt{N-M}} \sum_x'' |x\rangle$, $|\beta\rangle \equiv \frac{1}{\sqrt{M}} \sum_x' |x\rangle$, then $|\psi\rangle = \sqrt{\frac{N-M}{N}}\,|\alpha\rangle + \sqrt{\frac{M}{N}}\,|\beta\rangle$.
- $|\psi\rangle = cos(\frac{\theta}{2})\,|\alpha\rangle + sin(\frac{\theta}{2})\,|\beta\rangle$, after measurement $|\psi\rangle$ we get random solution with probability $sin^2(\frac{\theta}{2})$.
- After k Grover's iterations we get

$$G^k\,|\psi\rangle = cos\left(\frac{2k+1}{2}\theta\right)|\alpha\rangle + sin\left(\frac{2k+1}{2}\theta\right)|\beta\rangle\,.$$

Quantum counting

Problem: For random boolean function $f : V_n \to V_1$, we have to estimate $M = \left|f^{-1}(1)\right|$ – number of arguments x on which $f(x) = 1$.
We could estimate $\theta = 2 \arcsin \sqrt{M/N}$ by quantum circuit on fig. 2, $M = \sin^2(\frac{\theta}{2})N$.

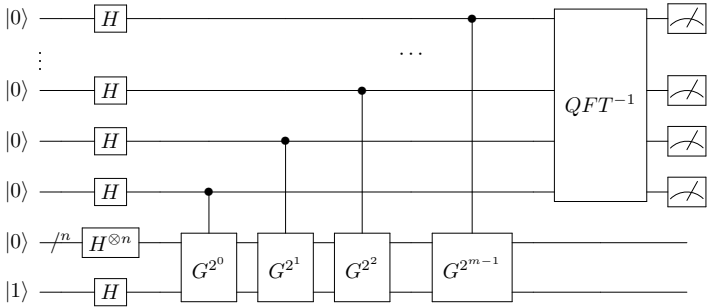


Figure 2: Quantum counting circuit. The control register contains m qubits.

If $m \approx n/2$ we could get $|f^{-1}(1)|$ by $\approx O(\sqrt{2^n})$ quantum operations with constant error rate and sucsses probability at least $4/\pi^2 = 0.405285$.

Quantum differential cryptanalysis

Problems

1. Difference relations search – Bernstein-Vazirani quantum algorithm ([1], [2], [3]).
2. Iteration key search is described in [4], [5].

- For $E : V_n \times V_m \to V_m$, $C = E(key, P)$, we have difference (a, b) with probability $p_{(a,b)}$. It is assumed that on the secret key key:

$$P(E(key, P) \oplus E(key, P \oplus a) = b) = p_{(a,b)}, \qquad p_{(a,b)} = \max_{a,b \in V_m \setminus \overrightarrow{0}} p_{(a,b)}.$$

- We have N pairs (P_i, C_i), received on the same secret key.
- According to [4], the quantum complexity of key search is $O(\sqrt{N}) + O(\sqrt{K})$, while the classical complexity is estimated as $O(N) + O(K)$ (in [4] $key \in V_{log_2 K}$).

Quantum differential cryptanalysis

- Check K_1, estimate $\tilde{p}_{(a,b)_{R-1}}$, if it close to $p_{(a,b)_{R-1}}$, then we have candidate for K_1.
- If we find K_1, for K_2 searching we need $(a,b)_{R-2}$ with $p_{(a,b)_{R-2}}$;
- Usually $p_{(a,b)_{R-1}} < p_{(a,b)_{R-2}}$.

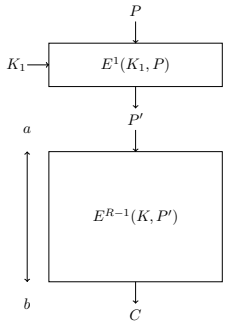


Figure 3: K_1 searching.

Quantum differential cryptanalysis (main idea)

- Since $p_{(a,b)_{R-1}} = \max_{x,y \in V_m \setminus \{0\}} p_{(x,y)_{R-1}}$, it is required to find $K_1 \in V_k$ $(k < n)$ that

$$Prob(\text{"}If\ \{P'_i \oplus P'_j = a\},\ then\ \{C_i \oplus C_j = b\}\text{"}) \to \max,$$

$P'_i = E^1(K_1, P_i)$.

- Let

$$Z(K_1) = \sum_{i,j=0}^{2^m-1} Ind(C_i \oplus C_j = b | P'_i \oplus P'_j = a),$$

$C_i = E^{R-1}(key, P'_i)$, then

$$Z(K_1) = \sum_{i=0}^{2^m-1} Ind(E^{R-1}(key, P'_i) \oplus E^{R-1}(key, P'_i \oplus a) = b).$$

If on the round key K_1 the probability of the difference (a, b) is maximum, then on the round key K_1 the value of $Z(K_1)$ also is maximum.

Quantum differential cryptanalysis (main idea)

- Searching probable K_1 is equivalent optimizing $Z(K_1)$, i.e. searching such round key K_1 on which $Z(K_1) \to max$.

- In the classical case, in order to find $Z(K_1)$ it is necessary to check all known possible pairs (P_i, C_i), i.e. for each pair of blocks (P_i, C_i), calculate $P_i' = E^1(K_1, P_i)$ and check if the property "If $P_i' \oplus P_j' = a$, then $C_i \oplus C_j = b$ " is performed.

- In the quantum case, we want to use quantum parallelism, i.e. get a superposition of all possible iterative keys K_1 and the corresponding values $Z(K_1)$.
  We want to get
  $$\sum_{K_1} \frac{1}{\sqrt{2^k}} |K_1\rangle |Z(K_1)\rangle ,$$
  to which we will apply the amplitude amplification procedure for searching K_1 candidates.

Quantum differential key searching by [4]

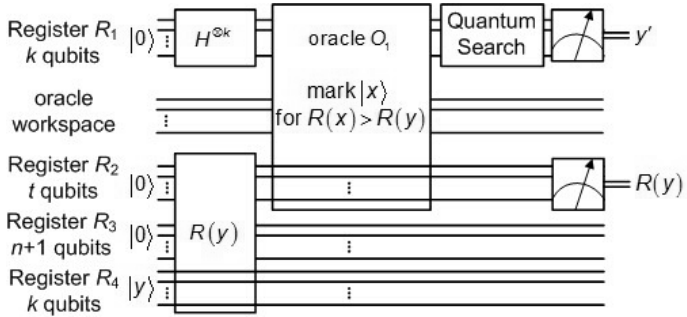


Figure 4: Schematic circuit for the quantum differential cryptanalysis

Quantum differential key searching by [4]

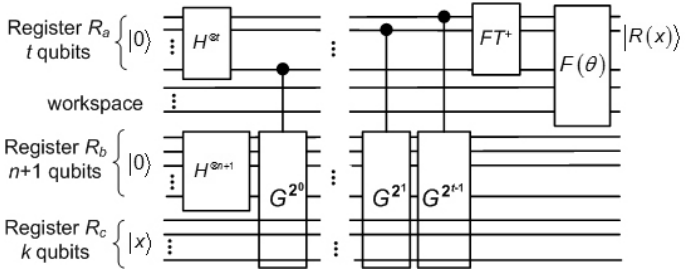


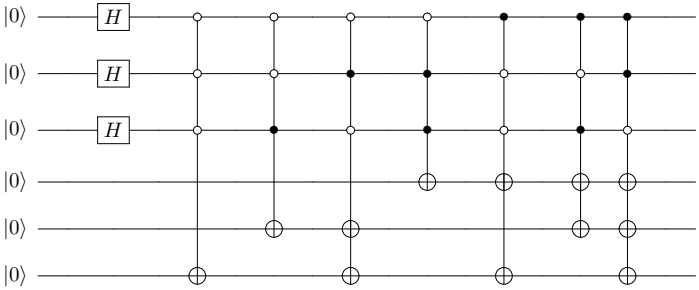
Figure 5: Circuit for calculating $R(x)$

Quantum differential cryptanalysis (data preparation)

- We know $N = 2^m$ pairs of blocks (P_i, C_i), $i \in \overline{0, N-1}$, we want to prepare $\sum_{i=0}^{2^m-1} \frac{1}{\sqrt{2^m}} |P_i\rangle |C_i\rangle$.

Example:

№ of pair i	P_i	C_i
0	000	001
1	001	010
2	010	011
3	011	100
4	100	101
5	101	110
6	110	111
7	111	000



Quantum differential cryptanalysis (make $|K_1\rangle\,|Z(K_1)\rangle$)

For prepare $|K_1\rangle\,|Z(K_1)\rangle$ we want to estimate $Z(K_1)$ using the quantum counting algorithm.
We have to realize the boolean function f_{K_1} and estimate $|f_{K_1}^{-1}(1)|$:

Number of a pair P_i, C_i	$x_1\ x_2\ \ldots\ x_m$	$f(x_1, x_2, \ldots, x_m)$
$i = 0$	$00\ldots00$	$Ind(E^{R-1}(key, P'_0) \oplus E^{R-1}(key, P'_0 \oplus a) = b)$
$i = 1$	$00\ldots01$	$Ind(E^{R-1}(key, P'_1) \oplus E^{R-1}(key, P'_1 \oplus a) = b)$
$i = 2$	$00\ldots10$	$Ind(E^{R-1}(key, P'_2) \oplus E^{R-1}(key, P'_2 \oplus a) = b)$
$i = 3$	$00\ldots11$	$Ind(E^{R-1}(key, P'_3) \oplus E^{R-1}(key, P'_3 \oplus a) = b)$
$\vdots$	$\vdots$	$\vdots$
$i = N-1$	$11\ldots11$	$Ind(E^{R-1}(key, P'_{N-1}) \oplus E^{R-1}(key, P'_{N-1} \oplus a) = b)$

Table 1: The table of values of the boolean function f_{K_1}.

For preparing $\sum_{i=0}^{N-1} \frac{1}{\sqrt{N}} |P_i\rangle\,|C_i\rangle$, we need $O(N)$ quantum operations.

To implement f_{K_1}, we have to prepare $\sum_{i=0}^{N-1} \frac{1}{\sqrt{N}} |P_i\rangle\,|C_i\rangle$ twice.

Quantum differential cryptanalysis (make $|K_1\rangle\,|Z(K_1)\rangle$)

Quantum circuit that implements f_{K_1}:

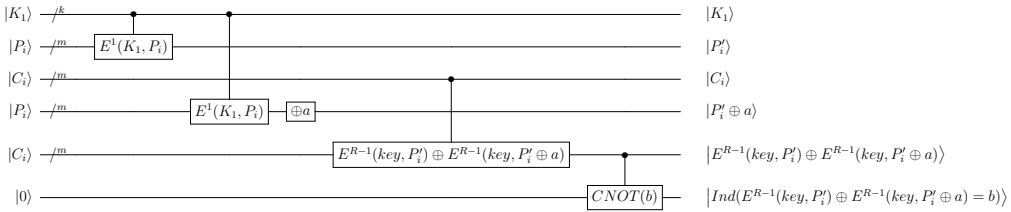


Figure 6: Implementation of f_{K_1} as a quantum circuit. $E^1(K_1, P_i)$ - one iteration of the encryption function on K_1 and P_i. The operation $\oplus a$ is the application of one-qubit gates X on those qubits whose numbers correspond to "1" bits of the difference $a \in V_m$. The operation $E^{R-1}(key, P_i') \oplus E^{R-1}(key, P_i' \oplus a)$ is performed using m standard two-qubit operations $CNOT$, and $CNOT(b)$ - generalized $CNOT$, inverting the lower qubit, in which the difference $b \in V_m$ acts as a control vector.

Quantum differential cryptanalysis (problem)

Input. Block cipher with round encryption $E : V_k \times V_m \to V_m$, $N = 2^m$ pairs of blocks (P_i, C_i), $P_i, C_i \in V_m$, $i \in \overline{0, 2^m - 1}$ received on the same secret key, difference relation $(a, b)_{R-1}$ with $p_{(a,b)_{R-1}}$, such that two simple hypotheses can be distinguished by classical statistical methods

$$H_0 : P(\text{"If } P'_i \oplus P'_j = a, \text{ then } C_i \oplus C_j = b\text{"}) \sim Be(1/2^{m-1});$$

$$H_1 : P(\text{"If } P'_i \oplus P'_j = a, \text{ then } C_i \oplus C_j = b\text{"}) \sim Be(p_{(a,b)_{R-1}}),$$

provided $1/2^{m-1} < p_{(a,b)_{R-1}}$, with acceptable error probabilities.
The case when $p_{(a,b)_r} = \min_{x,y \in V_m \setminus \{0\}} p_{(x,y)_r}$ and $p_{(a,b)_{R-1}} = 0$ is known as the impossible differential method.
Output. Round key K_1 with a maximum value of $Z(K_1)$.

Quantum differential cryptanalysis (Preparation step)

1. Prepare two registers with quantum states $\sum_{i=0}^{N-1} \frac{1}{\sqrt{N}} |P_i\rangle |C_i\rangle$. Complexity is $O(N)$ quantum operations.

2. Select a random round key K, calculate the value of $Z(K)$.
   - $O(2^m)$ classical operations – find exact value of $Z(K)$ by analysing all N pairs (P_i, C_i); calculate the initial value $\theta_{current} := \theta_K = 2 \arcsin \sqrt{\frac{Z(K)}{N}}$.
   - $O(2^{\lceil \frac{m}{2} \rceil + 3})$ quantum operations – quantum counting with relatively the boolean function f_K, with a probability of at least $4/\pi^2$ estimate $\widetilde{\theta}_{current}$, which has a predicted error level $\Delta\widetilde{\theta}_{current} \leq 2^{-3}$ (see [7, 8, 9]).

Quantum differential cryptanalysis (Search procedure, part 1/4)

1. Initialize k qubits in state $|0\rangle$, apply the $H^{\otimes k}$, we obtain $\sum_{K_1} \frac{1}{\sqrt{2^k}} |K_1\rangle$.

2. Execute quantum counting as in the figure 2 relatively $f_{K_1} : V_k \times V_m \to V_1$, with using $w_N = \lceil m/2 \rceil + 3$ control qubits, to determine $||f_{K_1}||$ without measurements.

$$f_{K_1}(P_i) = Ind(E^{R-1}(key, P_i') \oplus E^{R-1}(key, P_i' \oplus a) = b).$$

A quantum circuit implementing f_{K_1} is shown in the figure 6.

The complexity of the quantum counting is $O(2^{w_N})$, we get a superposition of the estimates $\widetilde{\theta}_{K_1}$ which has a predicted error level $\Delta\widetilde{\theta}_{K_1} \leq 2^{-3}$ with a probability of at least $4/\pi^2$.

Thus, after quantum counting we obtain a superposition of round keys and the corresponding estimates $\sum_{K_1} \frac{1}{\sqrt{2^k}} |K_1\rangle \left|\widetilde{\theta}_{K_1}\right\rangle$ (other registers are omitted for clarity, because they are not involved in the further search procedure), at this step we need $k + 4m + 1 + w_N$ logical qubits.

Quantum differential cryptanalysis (Search procedure, part 2/4)

3. The value $\theta_{current}$ is used as a threshold value, the set of all possible round keys $K \in V_k$ is divided into two classes: the first class of "bad" keys $\theta_K \leq \theta_{current}$ and the second class of "good" keys $\theta_K > \theta_{current}$.
This classification can be realized by the boolean function $g : V_{w_N} \times V_{w_N} \to V_1$,

$$g(\widetilde{\theta}_{K_1}, \theta_{current}) = Ind(\widetilde{\theta}_{K_1} > \theta_{current}).$$

The boolean function $g(\widetilde{\theta}_{K_1}, \theta_{current})$ can be implemented as follows:
- We could initialize one ancilla qubit $|q\rangle = |1\rangle$, and consider it as high order bit of binary decomposition $\theta_{current}$.
- If after subtraction in the binary number system $\theta_{current} - \widetilde{\theta}_{K_1}$, the high order bit is changed and will be "zero" (we get $|q\rangle = |0\rangle$), then $\widetilde{\theta}_{K_1} > \theta_{current}$.

Quantum counting relatively g as in the figure 2 with using $w_K = \lceil k/2 \rceil + 3$ control qubits – complexity $O(2^{w_K})$ Grover iterations, with a probability of at least $4/\pi^2$ we obtain the estimate θ_g, by which we find

$$||g|| \approx \widetilde{M}_g = 2^k \cdot \sin^2\left(\frac{\theta_g}{2}\right).$$

Quantum differential cryptanalysis (Search procedure, part 3/4)

4. Apply the Grover algorithm relatively the boolean function g.

   After $\left[\frac{\pi}{4}\sqrt{\frac{2^k}{\widetilde{M}_g}}\right]$ Grover iterations with probability $\sin^2\left(\frac{2\left[\frac{\pi}{4}\sqrt{\frac{2^k}{\widetilde{M}_g}}\right]+1}{2}\theta_g\right)$ we get one from $\widetilde{M}_g$ possible solutions, i.e. such K_1' on which $\theta_{K_1'} > \theta_{current}$.

   Reset $\theta_{current} = \theta_{K_1'}$ and repeat the search procedure again.

   To implement the Grover algorithm relatively g we need $k + 4m + 1 + w_N + 2$ logical qubits, one ancilla qubit needs to implement the subtraction with implementation of g and another one qubit needs to implement the Grover iteration.

Quantum differential cryptanalysis (Search procedure, part 4/4)

If each quantum counting procedure execute correctly, then to search for the key K with the maximum value θ_K, i.e. with the maximum value of $Z(K)$, it is required no more than $\widetilde{M}_g$ iterations of the search procedure (for $\widetilde{M}_g$ obtained at the first start of the search procedure).

The lower bound of searching success probability could be estimated by $\frac{4}{\pi^2} \cdot \frac{4}{\pi^2} \cdot 0.5 = 0.0821279$ (this estimate is for the case when the quantum counting procedure performed only twice and the success probability of the Grover's algorithm for searching maximum > 0.5), i.e. on average, it will take about 12 starts to find the new value of $\theta_{current}$.

Thus, the complexity of each searching procedure is at least

$$O\left(2^{w_N} + 2^{w_K} + \left[\frac{\pi}{4}\sqrt{\frac{2^k}{\widetilde{M}_g}}\right]\right)$$

quantum operations.

Remarks

1. The correct quantum circuit for implementing one Grover iteration:

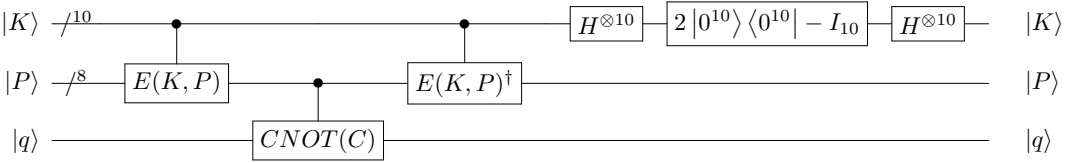


Figure 7: One iteration of the Grover's algorithm for SDES key searching ([10]).

2. The results of experiments in Quipper quantum simulator indicate that quantum circuit in figure 8 does not lead to success, i.e. "inversion about mean" doesn't increase the amplitude of target secret key.
We have to implement $E(K,P)$ and $E(K,P)^{\dagger}$ at each iteration of the Grover's algorithm.

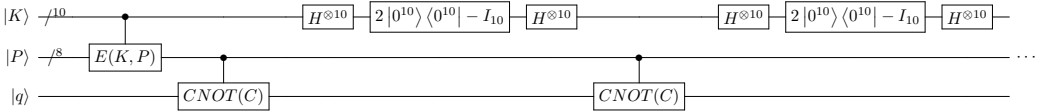


Figure 8: Wrong iteration of the Grover's algorithm for SDES key searching.

Remarks

3. Therefore, at step 4 of presented search procedure, quantum counting relatively f_{K_1} for preparing $\sum_{K_1} \frac{1}{\sqrt{2^k}} |K_1\rangle \left|\widetilde{\theta}_{K_1}\right\rangle$ should be performed at each Grover iteration!
   Correct quantum circuit:

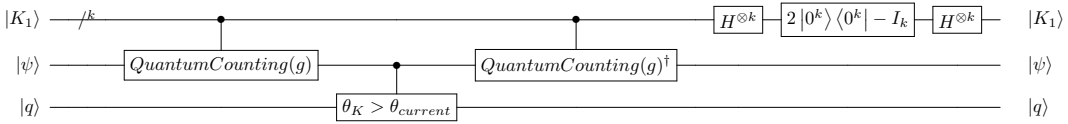


Figure 9: The correct implementation of one Grover's algorithm iteration with using quantum counting as a "subroutine".

Conclusion

- Quantum counting as a "subroutine" of Grover's algorithm eliminate quantum acceleration, since
$$O(\sqrt{K}) \cdot O(\sqrt{K}) \approx O(K).$$
- The success probability of Grover's algorithm should be multiplied by $\left(\frac{4}{\pi^2}\right)^{\left[\frac{\pi}{4}\sqrt{\frac{K}{M}}\right]}$.

Complexity of the quantum differential cryptanalysis (key search)

Conditions	The complexity of the quantum differential cryptanalysis (number of quantum operations)
1.At step 4, quantum counting is performed only once (false)	$O(N + 2^{w_N} + 2^{w_K} + 2^{w_K} \cdot 1 + \left\lceil \frac{\pi}{4} \sqrt{\frac{2^k}{\widetilde{M}_g}} \right\rceil)$
2.At step 4, quantum counting and its inversion are performed at each Grover iteration **(true)**.	$O(N + 2^{w_N} + 2^{w_K} + 2^{w_K+1} \cdot \left\lceil \frac{\pi}{4} \sqrt{\frac{2^k}{\widetilde{M}_g}} \right\rceil)$

Table 2: Estimates of the complexity of the quantum differential cryptanalysis:
1) $O(N + 2^{w_N} + 2^{w_K} + 2^{w_K} \cdot 1 + \left\lceil \frac{\pi}{4} \sqrt{\frac{2^k}{\widetilde{M}_g}} \right\rceil)$ - an understated estimates of the complexity, optimistic from the point of view of a quantum cryptanalyst.
2) $O(N + 2^{w_N} + 2^{w_K} + 2^{w_K+1} \cdot \left\lceil \frac{\pi}{4} \sqrt{\frac{2^k}{\widetilde{M}_g}} \right\rceil)$ - the correct estimate.
3) Required at least $k + 4m + 1 + w_N + (w_K + 3)$ logical qubits, where $w_N = \lceil m/2 \rceil + 3$, $w_K = \lceil k/2 \rceil + 3$.

Quantum linear cryptanalysis

Suppose we have a linear relations $(a,b)_r$, $a,b \in V_m$, $r \in \overline{1,R}$ for $E^r : V_k \times V_m \to V_m$.

$$Prob(\langle P,a\rangle = \langle E^r(key,P),b\rangle) = p_{(a,b)_r} = \frac{1}{2} + \delta,\ \delta \in [-0.5, 0.5], \tag{1}$$

$\langle x,y\rangle$ - dot product $x,y \in V_m$. We consider the case $\delta > 0$.

$$p_{(a,b)_r} = \max_{x,y \in V_m \setminus \{0\}} p_{(x,y)_r}.$$

$K_r \in V_k$ – iteration key on the r-th round;

Problems

1. Find linear relations $(a,b)_r$ with characteristic $p_{(a,b)_r}$ ([2]);
2. Search iterative keys by a statistical method (under the assumption that the secret key is "weak", i.e., such that $(a,b)_r$ with the probability $p_{(a,b)_r} = \frac{1}{2} + \delta$ takes place.

Quantum linear cryptanalysis

The key searching procedure is the same as in quantum differential cryptanalysis with one exception: definition $Z(K_1)$.

Let $Z(K_1)$ is the number of pairs (P'_i, C_i), $i \in \overline{0, 2^m - 1}$ on which the linear relation $\langle P'_i, a\rangle = \langle C_i, b\rangle$ is realized,

$$Z(K_1) = \sum_{i=0}^{2^m-1} Ind(\langle P'_i, a\rangle = \langle C_i, b\rangle),$$

where $Ind(x) \in \{0, 1\}$ is an indicator that the logical expression x is satisfied.

Quantum linear cryptanalysis (make $|K_1\rangle\,|Z(K_1)\rangle$)

Let's consider a way to prepare the state $|K_1\rangle\,|Z(K_1)\rangle$ for an arbitrary first round key $K_1 \in V_k$. We estimate $Z(K_1)$ using the quantum counting algorithm, for which it is necessary to set the corresponding boolean function f_{K_1} and evaluate $|f_{K_1}^{-1}(1)|$:

Number of a pair P_i, C_i	$x_1\ x_2\ \ldots\ x_m$	$f(x_1, x_2, \ldots, x_m)$
$i = 0$	$00\ldots00$	$Ind(\langle P'_0, a\rangle = \langle C_0, b\rangle)$
$i = 1$	$00\ldots01$	$Ind(\langle P'_1, a\rangle = \langle C_1, b\rangle)$
$i = 2$	$00\ldots10$	$Ind(\langle P'_2, a\rangle = \langle C_2, b\rangle)$
$i = 3$	$00\ldots11$	$Ind(\langle P'_3, a\rangle = \langle C_3, b\rangle)$
$\vdots$	$\vdots$	$\vdots$
$i = N-1$	$11\ldots11$	$Ind(\langle P'_{N-1}, a\rangle = \langle C_{N-1}, b\rangle)$

Table 3: The table of values of the boolean function f_{K_1}, by which we evaluate the value of $Z(K_1)$. $P'_i = E^1(K_1, P_i)$ - the result of applying one iteration of the encryption algorithm to the known plaintext block P_i on the iteration key K_1.

Quantum linear cryptanalysis (make $|K_1\rangle\,|Z(K_1)\rangle$)

To prepare the quantum state $\sum_{i=0}^{N-1} \frac{1}{\sqrt{N}} |P_i\rangle\,|C_i\rangle$, $O(N)$ we need quantum operations.

To implement f_{K_1}, the state $\sum_{i=0}^{N-1} \frac{1}{\sqrt{N}} |P_i\rangle\,|C_i\rangle$ have to be prepared once.

Quantum circuit that implements f_{K_1}:

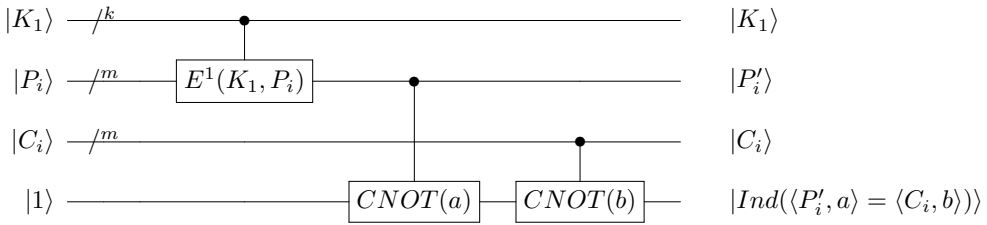


Figure 10: Implementation of f_{K_1} as a quantum circuit. $E^1(K_1, P_i)$ - one iteration of the encryption function on the key K_1 and the plaintext block P_i, which is theoretically possible without the use of ancilla qubits (see [11], [12]) Here the operations $CNOT(a)$ and $CNOT(b)$ are sets of $||a||$ and $||b||$ of standard two-qubit gates $CNOT$, for which control bits correspond to "1" bits in binary representation of $a \in V_m$ and $b \in V_m$.

Complexity of the quantum linear cryptanalysis

Conditions	The complexity of the quantum linear cryptanalysis (number of quantum operations)
1.At step 4, quantum counting is performed only once (false).	$O(N + 2^{w_N} + 2^{w_K} + 2^{w_K} \cdot 1 + \left[\frac{\pi}{4}\sqrt{\frac{2^k}{\widetilde{M}_g}}\right])$
2.At step 4, quantum counting and it's inversion are performed at each Grover iteration **(true)**.	$O(N + 2^{w_N} + 2^{w_K} + 2^{w_K+1} \cdot \left[\frac{\pi}{4}\sqrt{\frac{2^k}{\widetilde{M}_g}}\right])$

Table 4: Estimates of the complexity of the quantum linear cryptanalysis:

1) $O(N + 2^{w_N} + 2^{w_K} + 2^{w_K} \cdot 1 + \left[\frac{\pi}{4}\sqrt{\frac{2^k}{\widetilde{M}_g}}\right])$ - an understated estimates of the complexity, optimistic from the point of view of a quantum cryptanalyst.

2) $O(N + 2^{w_N} + 2^{w_K} + 2^{w_K+1} \cdot \left[\frac{\pi}{4}\sqrt{\frac{2^k}{\widetilde{M}_g}}\right])$ - the correct estimate.

3) Required at least $k + 2m + 1 + w_N + (w_K + 3)$ logical qubits, where $w_N = \lceil m/2 \rceil + 3$, $w_K = \lceil k/2 \rceil + 3$.

Conclusions

1. For a quantum linear cryptanalysis we need fewer logical qubits than to implement a quantum differential crypanalysis.
2. The complexity of the quantum differential and linear crypanalysis may turn out to be less than the complexity of key searching by the Grover's algorithm, if $E : V_n \times V_m \to V_m$ and $m < n/2$.
3. In case number of pairs $N < 2^m$, the schemes for applying the quantum differential and linear crypanalysis do not change, it is possible to reduce the complexity at the preparatory stage. The required number of logical qubits remains the same as in the case of $N = 2^m$.
4. Acceleration of computations due to "quantum parallelism" in the quantum differential and linear cryptanalysis, when we talk about key search, is apparently absent. Using quantum counting as a "subprogram" of the Grover algorithm eliminates quantum acceleration, since the main part of computation complexity described by $O(\sqrt{K}) \cdot O(\sqrt{K}) \approx O(K)$ quantum operations.

Thank your for attention!

[1] Hong-Wei Li, Li Yang. *Quantum differential cryptanalysis to the block ciphers.* https://arXiv.org/pdf/1511.08800.pdf, 2015.

[2] Hong-Wei Li, Li Yang. A quantum algorithm to approximate the linear structures of boolean functions. DOI:10.1017/S0960129516000013, https://arxiv.org/abs/1404.0611, 2015.

[3] Huiqin Xie, Li Yang. Using Bernstein-Vazirani algorithm to attack block ciphers, arXiv:1711.00853v3 [quant-ph], 2018.

[4] Zhou Q., Lu S., Zhang A., Sun J. *Quantum differential cryptanalysis,.* https://arxiv.org/abs/1811.09931, 2019.

[5] Kaplan M., Leurent G., Leverrier A., Naya-Plasencia M. Quantum Differential and Linear Cryptanalysis. IACR Transactions on Symmetric Cryptology, 2016, 71-94. https://doi.org/10.13154/tosc.v2016.i1.71-94; FSE 2017. http://www.iacr.org/workshops/fse2017/slides/10-03.pdf

[6] Huiqin Xie, Li Yang *Quantum impossible differential and truncated differential cryptanalysis*, arXiv:1712.06997v2 [quant-ph], 2018.

[7] Brassard G., Hoyer P., Tapp A. Quantum Counting. Physical Review Letters, http://arxiv.org/abs/quant-ph/9805082v1 1998.

[8] Denisenko D.V. Application of the Quantum counting to Estimation the Weights of Boolean Functions in Quipper. ZhETF, DOI: 10.1134/S1063776120040032, 2020.

[9] Nielsen M.A., Chuang I.L. Quantum computation and quantum information. Cambridge Univ. Press., http://csis.pace.edu/ctappert/cs837-18spring/QC-textbook.pdf, 2010.

[10] Denisenko D.V., Nikitenkova M.V. Application of Grover's Quantum Algorithm for SDES Key Searching. ZhETF. DOI:10.1134/S1063776118120142 2019.

[11] Denisenko D.V. Quantum circuits for S-box implementation without ancilla qubits. ZhETF, DOI:10.1134/S004445101906004X, 2019.

[12] Denisenko D.V., Nikitenkova M.V. Optimization of S-boxes GOST R 34.12-2015 "Magma" quantum circuits without ancilla qubits.
https://ctcrypt.ru/files/files/2019/materials/12_Denisenko.pdf, CTCrypt 2019.