RBI Quantum Hackathon Workbench

Tomas Rosa* and Jiri Pavlu, CBCC of RBI in Prague

*) corresponding author

Revision History

- 22/04/2019/Tom, direct application of BV elaborated
- 24/04/2019/Tom, S-Box indices permuted to reflect actual Qiskit implementation
- 5/05/2019/Tom, periodisation details, cryptography runtime models
- 9/05/2019/Tom, entanglement masking

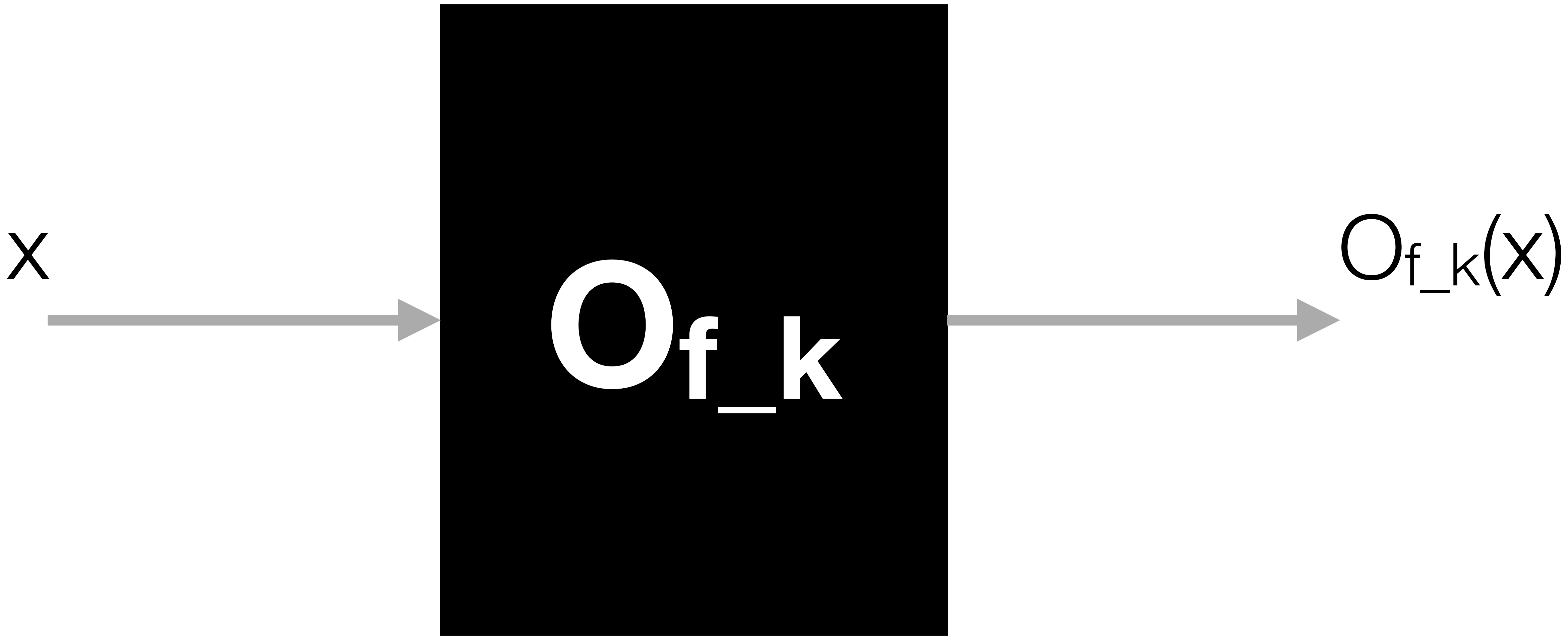
Notation Notes

- $\oplus$ denotes (vector) addition modulo 2
  - when clear from the context, we use simply + and $\oplus$ interchangeably

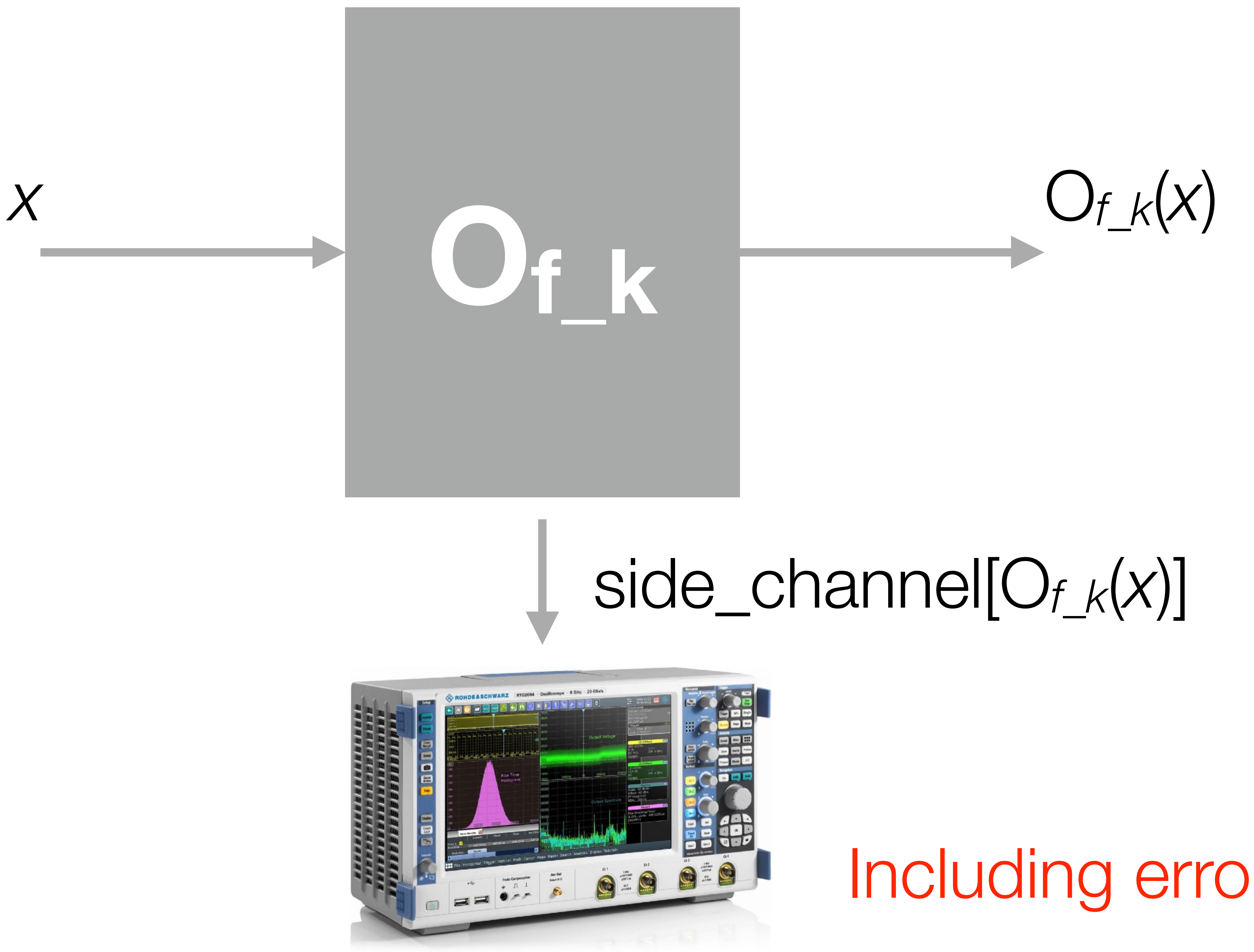
Runtime Models

- These models capture the context in which the cryptographic scheme shall remain secure
- They affect the formal definition and assumptions used for the security proof
  - however, the correspondence is not one-to-one
  - there are consensual rules of what to use when

Black Box Runtime Model

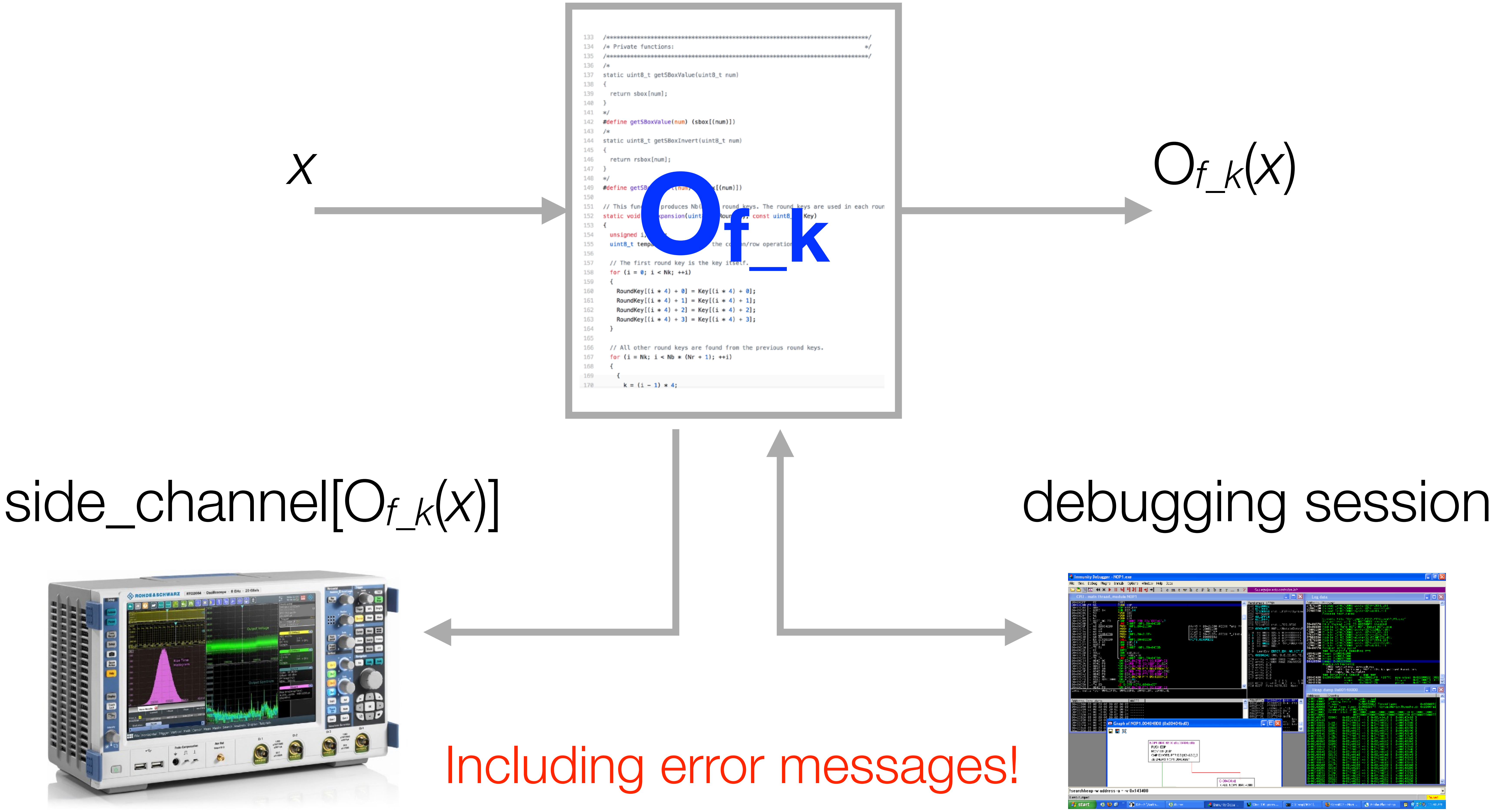


Grey Box Model

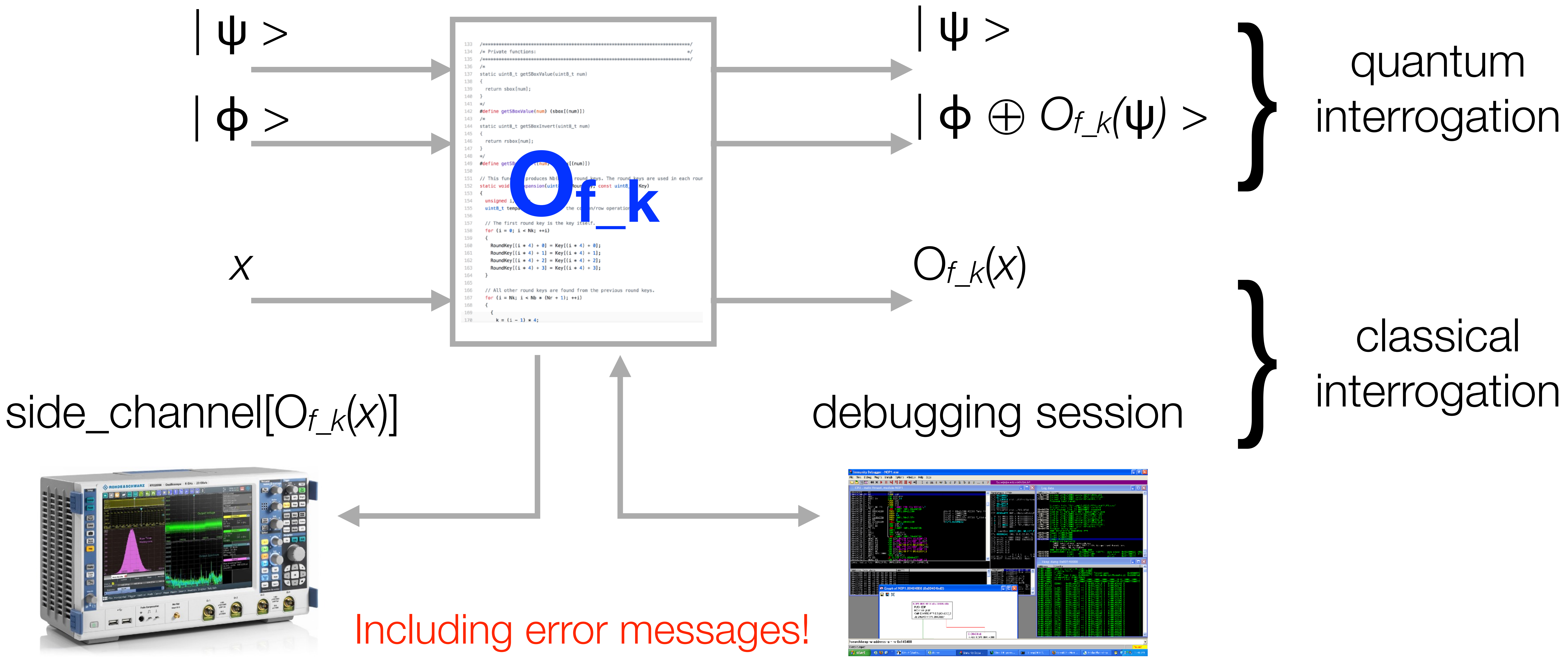


Including error messages!

White Box Model



Quantum Box Model



Even-Mansour Cipher

$$c = E(m) = P[m \oplus k^{(1)}] \oplus k^{(2)}$$

- P is (pseudo)random permutation (S-box)
- $k^{(1)}$ is the first part of the key
- $k^{(2)}$ is the second part of the key
- m is the input plaintext, c is the output ciphertext

Periodisation of the Even-Mansour Cipher

$$y = f(x) = E(x) \oplus P[x] = P[x \oplus k^{(1)}] \oplus k^{(2)} \oplus P[x]$$

$$\Rightarrow f(x \oplus k^{(1)}) = f(x)$$

- So, $k^{(1)}$ is can be found as the period of f(x)
  - also called a linear structure, here
- $k^{(2)}$ is then determined easily from a simple linear equation

Vector Oriented Description of $y = E(x)$, 3-bit Example

$$\begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} P_1[(x_1, x_2, x_3) + (k_1^{(1)}, k_2^{(1)}, k_3^{(1)})] \\ P_2[(x_1, x_2, x_3) + (k_1^{(1)}, k_2^{(1)}, k_3^{(1)})] \\ P_3[(x_1, x_2, x_3) + (k_1^{(1)}, k_2^{(1)}, k_3^{(1)})] \end{pmatrix} + \begin{pmatrix} k_1^{(2)} \\ k_2^{(2)} \\ k_3^{(2)} \end{pmatrix}$$

S-boxes for 3-bit Example

$$P_1[(x_1, x_2, x_3)] = x_3 + \overline{x_1} x_2 = x_2 + x_3 + x_1 x_2$$

$$P_2[(x_1, x_2, x_3)] = x_1 + \overline{x_2} x_3 = x_1 + x_3 + x_2 x_3$$

$$P_3[(x_1, x_2, x_3)] = x_2 + x_1 \overline{x_3} = x_1 + x_2 + x_1 x_3$$

Vector Description of the Periodisation

$$\begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} P_1[(x_1,x_2,x_3)+(k_1^{(1)},k_2^{(1)},k_3^{(1)})] \\ P_2[(x_1,x_2,x_3)+(k_1^{(1)},k_2^{(1)},k_3^{(1)})] \\ P_3[(x_1,x_2,x_3)+(k_1^{(1)},k_2^{(1)},k_3^{(1)})] \end{pmatrix} + \begin{pmatrix} k_1^{(2)} \\ k_2^{(2)} \\ k_3^{(2)} \end{pmatrix} + \begin{pmatrix} P_1[(x_1,x_2,x_3)] \\ P_2[(x_1,x_2,x_3)] \\ P_3[(x_1,x_2,x_3)] \end{pmatrix}$$

Periodisation per One Index (Bit-by-Bit)

Let $\vec{x} = (x_1, x_2, x_3) \in F_2^{\,3}$.

$$f_1(\vec{x}) = E_1(\vec{x}) + P_1(\vec{x})$$
$$= P_1[(x_1, x_2, x_3) + (k_1^{(1)}, k_2^{(1)}, k_3^{(1)})] + P_1[(x_1, x_2, x_3)] + k_1^{(2)}$$
$$= x_2 + k_2^{(1)} + x_3 + k_3^{(1)} + (x_1 + k_1^{(1)})(x_2 + k_2^{(1)}) + x_2 + x_3 + x_1 x_2 + k_1^{(2)}$$
$$= k_2^{(1)} x_1 + k_1^{(1)} x_2 + k_2^{(1)} + k_3^{(1)} + k_1^{(1)} k_2^{(1)} + k_1^{(2)}$$
$$= (k_2^{(1)}, k_1^{(1)}, 0) \cdot (x_1, x_2, x_3) + k_2^{(1)} + k_3^{(1)} + k_1^{(1)} k_2^{(1)} + k_1^{(2)}$$
$$= \vec{a_1} \cdot \vec{x} + \zeta_1$$

In General - Periodisation Index by Index

$$f_i(\vec{x}) = \vec{a_i} \cdot \vec{x} + \zeta_i, \ 1 \leq i \leq n$$

for our experiment $n = 3$

In Particular

$$\overrightarrow{a_1} = (k_2{}^{(1)}, k_1{}^{(1)}, 0),\ \zeta_1 = k_2{}^{(1)} + k_3{}^{(1)} + k_1{}^{(1)} k_2{}^{(1)} + k_1{}^{(2)}$$

$$\overrightarrow{a_2} = (0, k_3{}^{(1)}, k_2{}^{(1)}),\ \zeta_2 = k_1{}^{(1)} + k_3{}^{(1)} + k_2{}^{(1)} k_3{}^{(1)} + k_2{}^{(2)}$$

$$\overrightarrow{a_3} = (k_3{}^{(1)}, 0, k_1{}^{(1)}),\ \zeta_3 = k_1{}^{(1)} + k_2{}^{(1)} + k_1{}^{(1)} k_3{}^{(1)} + k_3{}^{(2)}$$

$\overrightarrow{a_i} \in F_2{}^3,\ \zeta_i \in F_2$

We start with the BV-style superposition

$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{\vec{x} \in F_2{}^n} |x\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

We apply the quantum oracle operator for $f_i(x)$, $1 \leq i \leq n$, $n = 3$

$$|x\rangle \otimes |w\rangle \mapsto |x\rangle \otimes \left|w \oplus f_i(\vec{x})\right\rangle, \text{ where } f_i(\vec{x}) = \vec{a}_i \cdot \vec{x} + \zeta_i$$

$$|\psi_{2,i}\rangle = \frac{1}{\sqrt{2^n}} \sum_{\vec{x} \in F_2{}^n} \underbrace{(-1)^{\vec{a}_i \cdot \vec{x} + \zeta_i}} |x\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

phase kickback effect

We use the final Hadamard transform on the first part of the register for the desired interference

$$|\psi_{3,i}\rangle = \frac{1}{2^n}\sum_{\vec{y}\in F_2^{\,n}}\sum_{\vec{x}\in F_2^{\,n}}(-1)^{\vec{a}_i\cdot\vec{x}+\zeta_i}(-1)^{\vec{x}\cdot\vec{y}}|y\rangle\otimes\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

$$= (-1)^{\zeta_i}\frac{1}{2^n}\sum_{\vec{y}\in F_2^{\,n}}\sum_{\vec{x}\in F_2^{\,n}}(-1)^{(\vec{a}_i+\vec{y})\cdot\vec{x}}|y\rangle\otimes\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

$$= \underbrace{(-1)^{\zeta_i}}_{\text{global phase}}\underbrace{|a_i\rangle}_{\text{direct key bits}}\otimes\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

global phase direct key bits

Entanglement Masking - the Idea

- If there is the oracle $E(x)$ on a quantum computer implemented for some authorised reason (e.g. as a communication sub-module), then the honest calling of this module would be with an eigenstate, not with the equal superposition inputs.

- So, we are searching for such a modification that will on one hand work with eigenstates in the unchanged way, so $E(x)$ still does what it shall do.

- On the other hand, the masking shall defeat the attacking algorithm when there is the input superposition entered.

- We achieve this through entanglement with internal (to $E(x)$) working qubits that breaks the desired interference in the final Hadamard transform of our attack.

Masking the *E*(*x*) Oracle via Internal Input Entanglement
- the initial BV superposition then becomes this

$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}}\left(\sum_{\vec{x}\in F_2{}^n} \underbrace{|x\rangle}_{\text{original input}} \otimes \underbrace{|x\rangle}_{\text{entangled sibling}}\right) \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

Entanglement corrupts the final Hadamard transform interference

$$\left|\psi_{3,i}\right\rangle = (-1)^{\zeta_i} \frac{1}{2^n} \left[\sum_{\vec{x} \in F_2^{\,n}} \left(\sum_{\vec{y} \in F_2^{\,n}} (-1)^{(\vec{a}_i + \vec{y}) \cdot \vec{x}} \left| y \right\rangle \right) \otimes \underbrace{\left| x \right\rangle} \right] \otimes \left(\frac{\left|0\right\rangle - \left|1\right\rangle}{\sqrt{2}} \right)$$

the entangled |x> sibling prevents the desired interference to occur,
so, we end up with an equal superposition with respect to the first part of the register