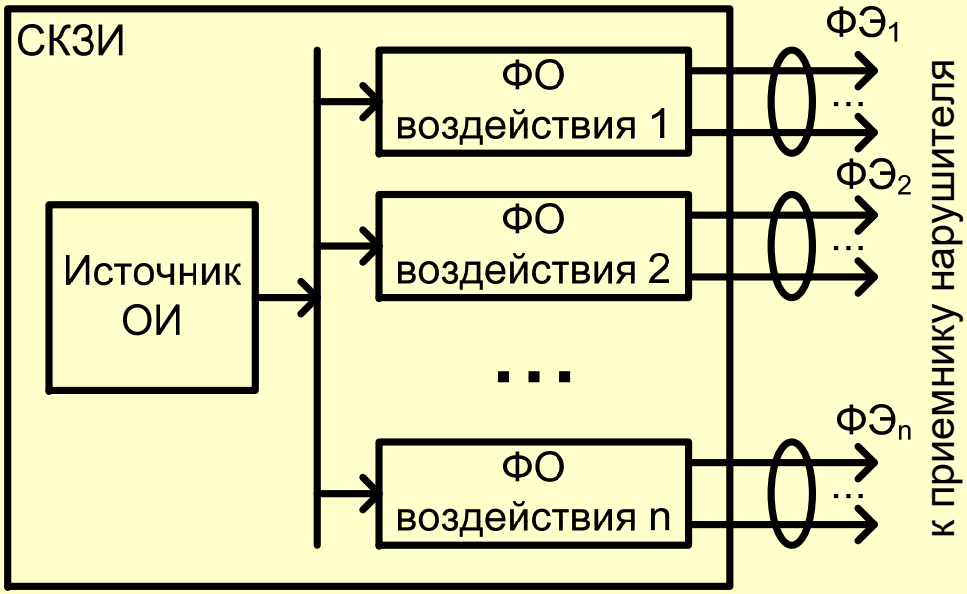
ЗАЩИТА КЛЮЧЕВОЙ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО КАНАЛУ ПЭМИН

В. М. Амербаев, ИППМ РАН

А. В. Шарамок, ООО Фирма «АНКАД»

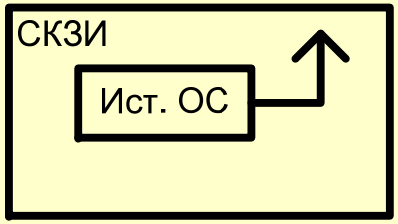
Причины появления каналов ПЭМИН



ОИ – опасная информация;
ФО – физический объект;
ФЭ – физический эффект.

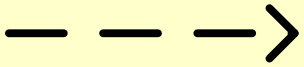
Методы борьбы с утечками по каналам ПЭМИН

на передатчик побочного канала



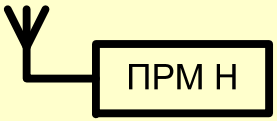
понижением мощности излучаемого сигнала

на среду передачи



увеличением затухания в побочном канале за счет изменения свойств среды передачи

на приемник побочного канала



созданием активных помех

Задача защиты ключевой информации

ГОСТ 28147-89	сложение по модулю 2^{32};
AES	сложение по модулю 2;
IDEA	умножение по модулю $(2^{16} + 1)$ и сложение по модулю 2^{16}.

Сложение по модулю 2^{32} при использовании ГОСТ 28147-89

(**1**) Маскированный раундовый подключ и использованную маску хранят в памяти раздельно;

(**2**) При выполнении сложения в регистр аккумулятор помещают маскированный раундовый подключ;

(**3**) Осуществляют сложение по модулю 2 использованной маски с содержимым регистра аккумулятора с сохранением результата в регистре аккумулятора;

(**4**) Осуществляют сложение по модулю 2^{32} преобразовываемого подблока данных с содержимым регистра аккумулятора с сохранением результата в регистре аккумулятора.

Традиционный алгоритм суммирования

K, ***X***, и **Г** - ***n***-разрядные целые числа, такие, что $0 \le K < q^n$, $0 \le X < q^n$ и $0 \le \Gamma < q^n$;

$$\begin{array}{l} K = k_0 + k_1 q + k_2 q^2 + k_3 q^3 + \ldots + k_{n-1} q^{n-1} \\ + \\ X = x_0 + x_1 q + x_2 q^2 + x_3 q^3 + \ldots + x_{n-1} q^{n-1} \\ \hline S = s_0 + s_1 q + s_2 q^2 + s_3 q^3 + \ldots + s_{n-1} q^{n-1} \end{array},$$

$$s_0 = \left| k_0 + x_0 \right|_q, \qquad \eta_0 = \left\lfloor \frac{k_0 + x_0}{q} \right\rfloor;$$

$$s_1 = \left| k_1 + x_1 + \eta_0 \right|_q, \qquad \eta_1 = \left\lfloor \frac{k_1 + x_1 + \eta_0}{q} \right\rfloor;$$

$$s_2 = \left| k_2 + x_2 + \eta_1 \right|_q, \qquad \eta_2 = \left\lfloor \frac{k_2 + x_2 + \eta_1}{q} \right\rfloor;$$

$$s_r = \left| k_r + x_r + \eta_{r-1} \right|_q, \qquad \eta_r = \left\lfloor \frac{k_r + x_r + \eta_{r-1}}{q} \right\rfloor;$$

$$s_{n-1} = \left| k_{n-1} + x_{n-1} + \eta_{n-2} \right|_q, \qquad \eta_{n-1} = \left\lfloor \frac{k_{n-1} + x_{n-1} + \eta_{n-2}}{q} \right\rfloor.$$

k_i и x_i – *i*-ые разряды операндов;

s_i – *i*-ый разряд результата;

η_r – перенос из *r*-го разряда;

$\lfloor\ \rfloor$ – наибольшее целое число, не превосходящее аргумент.

Поразрядная сумма по модулю q

$\widetilde{K} = K \otimes \Gamma$ $\otimes$ – операция поразрядного сложения по модулю ***q***;

$$
\begin{array}{l}
\otimes \quad K = k_0 + \quad k_1 q + \quad k_2 q^2 + \quad k_3 q^3 + \ldots \quad + k_{n-1} q^{n-1} \\
\quad\;\; \Gamma = \gamma_0 + \quad \gamma_1 q + \quad \gamma_2 q^2 + \quad \gamma_3 q^3 + \ldots \quad + \gamma_{n-1} q^{n-1} \\
\hline
\widetilde{K} = \left|k_0 + \gamma_0\right|_q + \left|k_1 + \gamma_1\right|_q q + \left|k_2 + \gamma_2\right|_q q^2 + \left|k_3 + \gamma_3\right|_q q^3 + \ldots + \left|k_{n-1} + \gamma_{n-1}\right|_q q^{n-1}
\end{array}
$$

Алгоритм скрытного суммирования

$$s'_0 = \left|\widetilde{k}_0 + x_0\right|_q, \qquad \eta_0 = \left\lfloor \frac{\left|\widetilde{k}_0 - \gamma_0\right|_q + x_0}{q} \right\rfloor;$$

$$s'_1 = \left|\widetilde{k}_1 + x_1 + \eta_0\right|_q, \qquad \eta_1 = \left\lfloor \frac{\left|\widetilde{k}_1 - \gamma_1\right|_q + x_1 + \eta_0}{q} \right\rfloor;$$

$$s'_2 = \left|\widetilde{k}_2 + x_2 + \eta_1\right|_q, \qquad \eta_2 = \left\lfloor \frac{\left|\widetilde{k}_2 - \gamma_2\right|_q + x_2 + \eta_1}{q} \right\rfloor;$$

$$s'_r = \left|\widetilde{k}_r + x_r + \eta_{r-1}\right|_q, \qquad \eta_r = \left\lfloor \frac{\left|\widetilde{k}_r - \gamma_r\right|_q + x_r + \eta_{r-1}}{q} \right\rfloor;$$

$$s'_{n-1} = \left|\widetilde{k}_{n-1} + x_{n-1} + \eta_{n-2}\right|_q, \qquad \eta_{n-1} = \left\lfloor \frac{\left|\widetilde{k}_{n-1} - \gamma_{n-1}\right|_q + x_{n-1} + \eta_{n-2}}{q} \right\rfloor.$$

$$\left|s'_r - \gamma_r\right|_q = \left\|\widetilde{k}_r + x_r + \eta_{r-1}\right|_q - \gamma_r\Big|_q =$$

$$= \left|\widetilde{k}_r + x_r + \eta_{r-1} - \gamma_r\right|_q = \left\|k_r + \gamma_r\right| + x_r + \eta_{r-1} - \gamma_r\Big|_q =$$

$$= \left|k_r + \gamma_r + x_r + \eta_{r-1} - \gamma_r\right|_q = \left|k_r + x_r + \eta_{r-1}\right|_q = s_r.$$

Алгоритм скрытного суммирования

Если при сложении двух операндов $\widetilde{K}$ и ***X***, один из которых является маскированным гаммой ***Г***, перенос в старшие разряды формировать по правилу:

$$\eta_r = \left\lfloor \frac{\left|\widetilde{k}_r - \gamma_r\right|_q + x_r + \eta_{r-1}}{q} \right\rfloor,$$

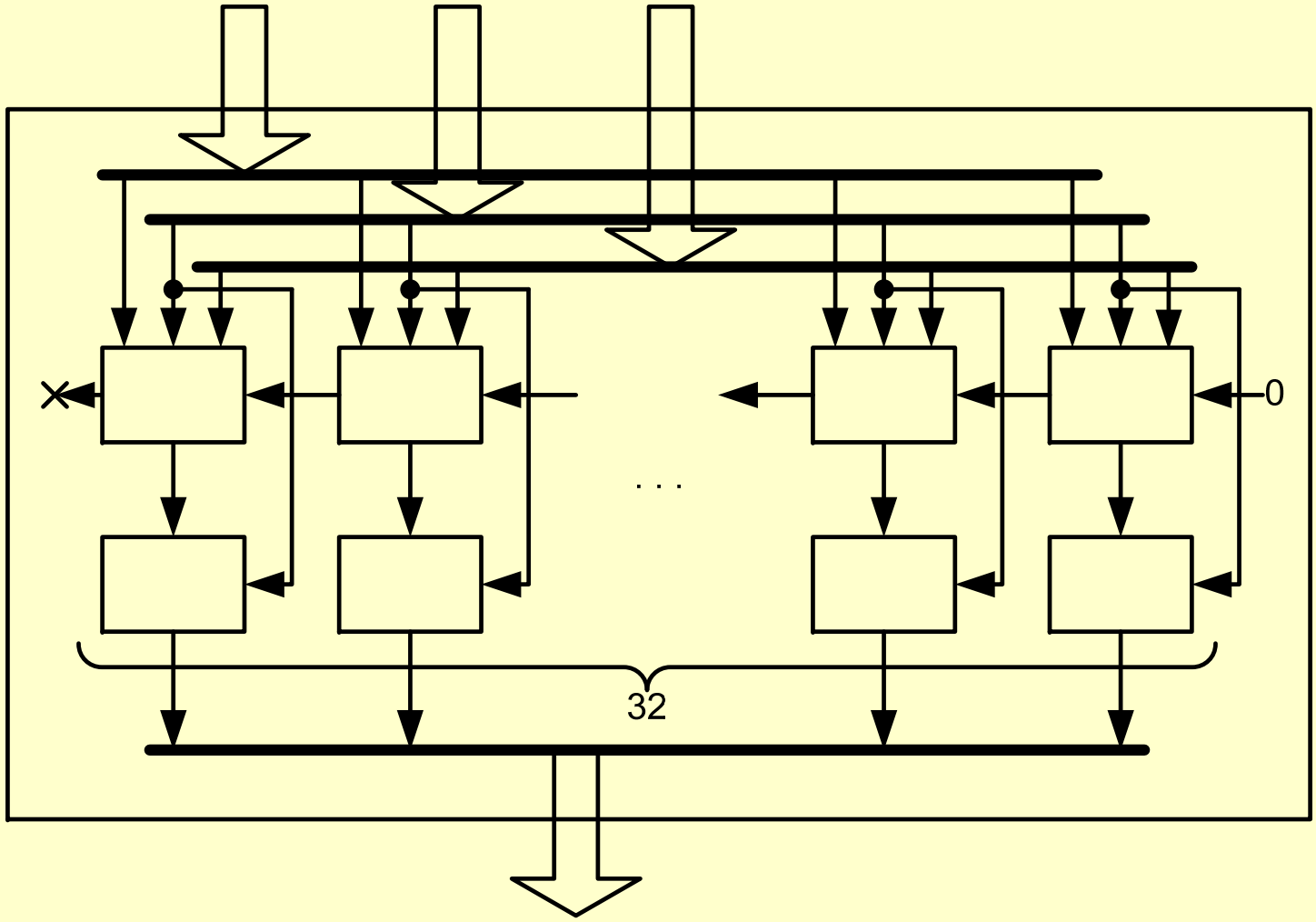
то при поразрядном вычитании по модулю основания ***q*** использованной ранее маски ***Г*** из результата ***S'***, будет получена сумма ***S*** по модулю q^n двух не маскированных операндов ***K*** и ***X***.

Для двоичной системы счисления

$$s'_r = \left|\widetilde{k}_r + x_r + \eta_{r-1}\right|_2, \qquad \eta_r = \left\lfloor \frac{\left|\widetilde{k}_r + \gamma_r\right|_2 + x_r + \eta_{r-1}}{2} \right\rfloor;$$

$$s'_r = \left|s'_r + \gamma_r\right|_2.$$

Сумматор скрытного сложения



Вопросы?