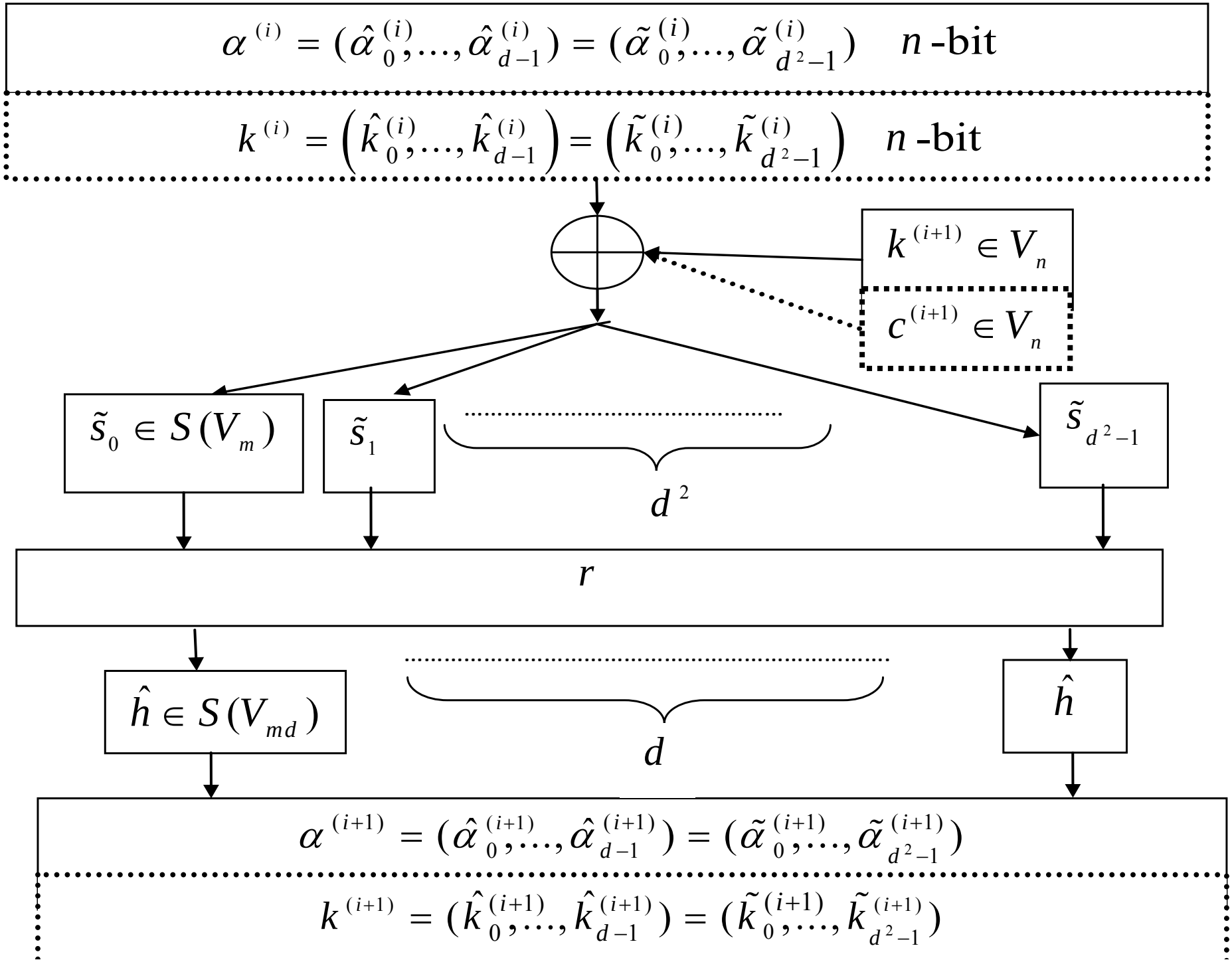
Differential attack on the family of block ciphers based on the SPN structure

Marina Pudovkina
National Research Nuclear University
(Moscow Engineering-Physics Institute)


$\alpha^{(i)} = (\hat{\alpha}_0^{(i)}, \ldots, \hat{\alpha}_{d-1}^{(i)}) = (\tilde{\alpha}_0^{(i)}, \ldots, \tilde{\alpha}_{d^2-1}^{(i)})$ n-bit
$k^{(i)} = (\hat{k}_0^{(i)}, \ldots, \hat{k}_{d-1}^{(i)}) = (\tilde{k}_0^{(i)}, \ldots, \tilde{k}_{d^2-1}^{(i)})$ n-bit
$k^{(i+1)} \in V_n$
$c^{(i+1)} \in V_n$
$\tilde{s}_0 \in S(V_m)$
$\tilde{s}_1$
$\tilde{s}_{d^2-1}$
d^2
r
$\hat{h} \in S(V_{md})$
d
$\hat{h}$
$\alpha^{(i+1)} = (\hat{\alpha}_0^{(i+1)}, \ldots, \hat{\alpha}_{d-1}^{(i+1)}) = (\tilde{\alpha}_0^{(i+1)}, \ldots, \tilde{\alpha}_{d^2-1}^{(i+1)})$
$k^{(i+1)} = (\hat{k}_0^{(i+1)}, \ldots, \hat{k}_{d-1}^{(i+1)}) = (\tilde{k}_0^{(i+1)}, \ldots, \tilde{k}_{d^2-1}^{(i+1)})$

Description of the family

1. *The key-schedule algorithm* $\varphi : k \mapsto (k^{(1)},\ldots,k^{(l)})$ is defined as

$$k^{(1)} = k,\quad k^{(j)} = hrs(c^{(j-1)} \oplus k^{(j-1)}) = g_{k^{(j-1)}}(c^{(j-1)}),$$

where $c^{(j-1)}$ is a fixed constant, $j = 2,\ldots,l$.

2. For a round key $k^{(i)} \in V_n$ *the round function* $g_{k^{(i)}} : V_n \to V_n$ is defined as

$$g_{k^{(i)}}(\alpha) = hrs(\alpha \oplus k^{(i)}).$$

3. *The encryption function* $g_k : V_n \to V_n$ is

$$f_k(\alpha) = \alpha^{(l)} = g_{k^{(1)}} \ldots g_{k^{(l)}}(\alpha).$$

6-rounds Whirlpool's block cipher belongs to the described family of block ciphers for $m = d = 8$.

Notations

- $n = m \cdot d^2; m, d \in \mathbb{N};$
- $\alpha = \left(\tilde{\alpha}_0, \ldots, \tilde{\alpha}_{d^2-1}\right) = \left(\hat{\alpha}_0, \ldots, \hat{\alpha}_{d-1}\right) \in V_n, \tilde{\alpha} \in V_m, \hat{\alpha} \in V_{md};$
- $s : \alpha = (\tilde{\alpha}_0, \ldots, \tilde{\alpha}_{d^2-1}) \mapsto (\hat{s}_0(\hat{\alpha}_0), \ldots, \hat{s}_{d-1}(\hat{\alpha}_{d-1})) = (\tilde{s}_0(\tilde{\alpha}_0), \ldots, \tilde{s}_{d^2-1}(\tilde{\alpha}_{d^2-1}));$
- $h : \alpha = (\tilde{\alpha}_0, \ldots, \tilde{\alpha}_{d^2-1}) \mapsto (\hat{h}(\hat{\alpha}_0), \ldots, \hat{h}(\hat{\alpha}_{d-1}))$ – the linear mapping;
- $\hat{r} \in S\left(\left\{0, \ldots, d-1\right\}\right), r(\tilde{\alpha}_0, \ldots, \tilde{\alpha}_{dq-1}) = \left(\tilde{\alpha}_{\hat{r}(0)}, \ldots, \tilde{\alpha}_{\hat{r}(d^2-1)}\right);$
- $X_i = \left\{id, \ldots, (i+1)d - 1\right\}, i = 0, \ldots, d-1;$
- $\hat{r}^{-1}(X_j) = \left\{v_j^{(1)}(0), \ldots, v_j^{(1)}(d-1)\right\}, id \le v_j^{(1)}(i) < (i+1)d;$
- $r^{-1}(\hat{\alpha}_i) = \hat{\alpha}_{i*}, r(\hat{\alpha}_i) = \hat{\alpha}_{i*}, i = 0, \ldots, d-1;$
- $\left|\hat{r}(X_i) \bigcap X_j\right| = 1, i, j \in \left\{0, \ldots, d-1\right\}.$

The idea attack

- Construct a differential characteristic for the first three rounds with $2m+1$ active s-boxes.
- Go through the last three rounds using the coincidence between the encryption function and the key-schedule algorithm.

Differential characteristic for the first three rounds

- Type $d-1-d$.

$$1.\delta^{(0)}=\left(\tilde{0},\ldots,\tilde{0},\tilde{\delta}^{(0)}_{v_j^{(1)}(0)},\tilde{0},\ldots,\tilde{0},\tilde{\delta}^{(0)}_{v_j^{(1)}(1)},\tilde{0},\ldots,\tilde{0},\tilde{\delta}^{(0)}_{v_j^{(1)}(d-1)},\tilde{0},\ldots,\tilde{0}\right)\rightarrow$$

$$\xrightarrow{g}\left(\hat{0},\ldots,\hat{0},\underbrace{\left(\tilde{0},\ldots,\tilde{0},\tilde{\delta}^{(1)}_{i+dj},\tilde{0},\ldots,\tilde{0}\right)}_{j},\hat{0},\ldots,\hat{0}\right),$$

$$2.\left(\hat{0},\ldots,\hat{0},\underbrace{\left(\tilde{0},\ldots,\tilde{0},\tilde{\delta}^{(1)}_{i+dj},\tilde{0},\ldots,\tilde{0}\right)}_{j},\hat{0},\ldots,\hat{0}\right)\xrightarrow{g}\left(\hat{0},\ldots,\hat{0},\hat{\delta}^{(2)}_{j'},\hat{0},\ldots,\hat{0}\right),$$

$$3.\left(\hat{0},\ldots,\hat{0},\hat{\delta}^{(2)}_{j'},\hat{0},\ldots,\hat{0}\right)\xrightarrow{sr}\left(\tilde{0},\ldots,\tilde{0},\tilde{\delta}'^{(2)}_{v_{j'}^{(2)}(0)},\tilde{0},\ldots,\tilde{0},\tilde{\delta}'^{(2)}_{v_{j'}^{(2)}(d-1)},\tilde{0},\ldots,\tilde{0}\right)\rightarrow$$

$$\xrightarrow{h,1}\delta^{(3)}$$

Properties of the differential characteristic

Proposition 1. Let $\alpha^{(0)}, k^{(1)}, k^{(2)}, k^{(3)} \in_U V_n$. Then there exists such differences $\delta^{(0)}, \delta^{(3)} \in V_n$ that

$$g_{k^{(3)}} g_{k^{(2)}} g_{k^{(1)}} \alpha^{(0)} \oplus g_{k^{(3)}} g_{k^{(2)}} g_{k^{(1)}} \left(\alpha^{(0)} \oplus \delta^{(0)}\right) = \delta^{(3)}$$

holds with probability $p_{char}(\delta^{(0)}, \delta^{(3)}) \geq 2^{-(m-1)(2d+1)}$.

The complexity of finding differences $\delta^{(0)}, \delta^{(3)}$ with the maximal $p_{char}(\delta^{(0)}, \delta^{(3)})$ is $O(d^2 \cdot 2^{3m})$.

Go through the last three rounds

Proposition. Let $\alpha^{(0)}$ be an arbitrary plain text from V_n and $\alpha^{(i)} = g_{k(i)} \dots g_{k(1)} \left(\alpha^{(0)}\right)$, $i \in \{1, \dots, 6\}$, k be an encryption key, $\varphi : k \to (k^{(1)}, \dots, k^{(l)})$, $l \geq 6$. Then

$$\hat{\alpha}_{j^*}^{(3)} = \hat{k}_j^{(5)\hat{h}^{-1}\hat{r}^{-1}\hat{s}^{-1}} \oplus \hat{c}_{j^*}^{(4)} \oplus$$

$$\overline{\oplus\left(\left(\alpha^{(6)h^{-1}r^{-1}s^{-1}h^{-1}r^{-1}} \oplus \left(\hat{k}_j^{(5)} \oplus c_j^{(5)}\right)^{\hat{s}_j}\right)^{\hat{s}_j^{-1}} \oplus \hat{k}_j^{(5)}\right)_j}^{\hat{h}^{-1}\hat{r}^{-1}\hat{s}^{-1}},$$

where $\alpha^b = b(\alpha), b \in S(V_n)$.

Corollary. Let k be an arbitrary key from V_n, $\varphi : k \to (k^{(1)},...,k^{(l)})$, $l \geq 6, \alpha^{(0)}, \alpha'^{(0)}$ be an arbitrary plaintexts from V_n, $\alpha^{(i)} = \left(\alpha^{(0)}\right)^{g_{k^{(1)}} \cdots g_{k^{(i)}}}, \alpha'^{(i)} = \left(\alpha'^{(0)}\right)^{g_{k^{(1)}} \cdots g_{k^{(i)}}}$, $i \in \overline{\{1,6\}}$. Then

$$\hat{\alpha}_{j*}^{(3)} \oplus \hat{\alpha}_{j*}^{(3)} = \sigma(\alpha^{(6)}, \alpha'^{(6)}, \hat{k}_j^{(5)}) = \left(\left(\alpha^{(6)h^{-1}r^{-1}s^{-1}h^{-1}r^{-1}} \oplus \left(\hat{k}_j^{(5)} \oplus c_j^{(5)} \right)^{\hat{s}_j} \right)^{\hat{s}_j^{-1}} \oplus \hat{k}_j^{(5)} \right)_j^{\hat{h}^{-1}r^{-1}\hat{s}^{-1}} \oplus$$

$$\oplus \left(\left(\alpha'^{(6)h^{-1}r^{-1}s^{-1}h^{-1}r^{-1}} \oplus \left(\hat{k}_j^{(5)} \oplus c_j^{(5)} \right)^{\hat{s}_j} \right)^{\hat{s}_j^{-1}} \oplus \hat{k}_j^{(5)} \right)_j^{\hat{h}^{-1}r^{-1}\hat{s}^{-1}}.$$

The attack on the family of block ciphers

1. Find differences $\delta^{(0)},\delta^{(3)}$ with the maximal $p_{char}(\delta^{(0)},\delta^{(3)})$.

2.For all $\left(\hat{k}_0^{(5)},\hat{k}_1^{(5)}\right)\in V_{dm}^2$ find

$$w\left(\hat{k}_0^{(5)},\hat{k}_1^{(5)}\right)=\left|\left\{j\in\left\{\overline{1,n_o}\right\}\middle|\sigma(\alpha^{(6,j)},\alpha'^{(6,j)},\hat{k}_0^{(5)})=\delta_{0*}^{(3)},\sigma(\alpha^{(6,j)},\alpha'^{(6,j)},\hat{k}_1^{(5)})=\delta_{1*}^{(3)}\right.\right.$$

3. (Finding true $\hat{k}_{0,true}^{(5)},\hat{k}_{1,true}^{(5)}$). Blocks $\hat{k}_{0,true}^{(5)},\hat{k}_{1,true}^{(5)}$ of the round key $k^{(5)}$ are true if

$$w\left(\hat{k}_{0,true}^{(5)},\hat{k}_{1,true}^{(5)}\right)=\max\left\{w\left(\hat{k}_0'^{(5)},\hat{k}_1'^{(5)}\right)\middle|\left(\hat{k}_0'^{(5)},\hat{k}_1'^{(5)}\right)\in V_{dm}^2\right\}.$$

4. For $i = 2,...,d-1$ do:

4.i.1. For all $\hat{k}_i^{(5)} \in V_{dm}$ find

$$w\left(\hat{k}_{i-1,true}^{(5)}, \hat{k}_i^{(5)}\right) = \left| \left\{ j \in \{1,...,n_o\} \middle| \begin{array}{l} \sigma(\alpha^{(6,j)}, \alpha'^{(6,j)}, \hat{k}_{i-1,true}^{(5)}) = \delta_{(i-1)*}^{(3)}, \\ \sigma(\alpha^{(6,j)}, \alpha'^{(6,j)}, \hat{k}_i^{(5)}) = \delta_{i*}^{(3)} \end{array} \right\} \right|$$

4.i.2. $\hat{k}_{i,true}^{(5)}$ is true if

$$w\left(\hat{k}_{i-1,true}^{(5)}, \hat{k}_{i,true}^{(5)}\right) = \max\left\{ w\left(\hat{k}_{i-1,true}^{(5)}, \hat{k}_i'^{(5)}\right) \middle| \left(\hat{k}_{i-1,true}^{(5)}, \hat{k}_i'^{(5)}\right) \in V_{dm}^2 \right\}.$$

5. Suppose $k^{(5)} = \left(\hat{k}_{0,true}^{(5)},...,\hat{k}_{d-1,true}^{(5)}\right)$ and using the key-schedule algorithm find $k^{(1)}$.

Output: the secret key $k^{(1)}$.

The complexity of the attack

n_o is the number of plaintexts.

- Let $p_{char} > 2^{-2dm}$ and $m \leq 2d$. The time complexity $2^{2dm+1} n_o + 2^{md+1} n_o (d-2)$.
- If $p_{char} \leq 2^{-2dm}$ then the time complexity $\leq 3 \cdot 2^{3dm} n_o + 3 \cdot 2^{md} n_o (d-3)$.

- The time complexity of Whirlpool's block cipher is smaller than $2^{236.3} \leq 2^{512/2}$.
- The probability of success is equal to 0.99.
- The number of plaintexts is $\leq 2^{107.3}$, $p_{char} \geq 2^{-(m-2)(2d+1)}$.

Table.
The upper bounds of the time complexity for different m, d.

m	d	$p_{char} \geq$	the time complexity $\leq$	p_{suc}	Brute force
8	8	$2^{-(m-1)(2d+1)}$	$2^{253.5}$	0.99	2^{512}
8	8	$2^{-(m-2)(2d+1)}$	$2^{236.3}$	0.99	2^{512}
4	8	$2^{-(m-1)(2d+1)}$	$2^{104.3}$	0.99	2^{256}
16	8	$2^{-(m-1)(2d+1)}$	$2^{519.7}$	0.99	2^{1024}
4	16	$2^{-(m-1)(2d+1)}$	$2^{233.3}$	0.99	2^{1024}

Thank you for your attention!