Lineární kryptoanalýza

V následujícím textu bude $f = f_N \circ \ldots \circ f_1$ složení booleovských funkcí $f_i : \mathbb{F}_2^n \to \mathbb{F}_2^n$, $i = 1, \ldots, N$.

Definice. *Lineární cesta* nad f je $(N+1)$-tice vektorů $U = (u^{(0)}, \ldots, u^{(N)})$, $u^{(i)} \in \mathbb{F}_2^n$, $i = 0, \ldots, N$. Dvojice $(u^{(i-1)}, u^{(i)})$, $i = 1, \ldots, N$, se nazývají *lineární kroky* cesty U, *korelace lineárního kroku* je hodnota korelační matice $\mathrm{C}^{f_i}_{u^{(i)},u^{(i-1)}}$.

Pokud lineární cesta $U = (u^{(0)}, \ldots, u^{(N)})$ začíná vektorem $v = u^{(0)}$ a končí vektorem $u = u^{(N)}$, řekneme, že je to cesta od v k u.

Definice. *Korelační příspěvek* lineární cesty $U = (u^{(0)}, \ldots, u^{(N)})$ nad f je součin korelací jejích kroků, tedy

$$\mathrm{C_p}(U) = \prod_{i=1}^{N} \mathrm{C}^{f_i}_{u^{(i)},u^{(i-1)}}$$

Zřejmě platí $\mathrm{C_p}(U) \in \langle -1, 1 \rangle$.

Věta (*o skládání lineárních cest*). Pro $u, v \in \mathbb{F}_2^n$ platí

$$\mathrm{C}^f_{u,v} = \sum_{\substack{U \text{ lin. cesta nad } f \\ \text{od } v \text{ k } u}} \mathrm{C_p}(U)$$

Důkaz. Pro $N = 1$ tvrzení platí. Předpokládejme, že věta platí pro $N-1$ a položme $g = f_{N-1} \circ \ldots \circ f_1$. Pro korelační matici $f = f_N \circ g$ pak dostaneme rovnost $\mathrm{C}^f = \mathrm{C}^{f_N} \cdot \mathrm{C}^g$, tedy:

$$\begin{aligned}
\mathrm{C}^f_{u,v} &= \sum_{w \in \mathbb{F}_2^n} \mathrm{C}^{f_N}_{u,w} \cdot \mathrm{C}^g_{w,v} \\
&= \sum_{w \in \mathbb{F}_2^n} \mathrm{C}^{f_N}_{u,w} \cdot \left(\sum_{\substack{\tilde{U} \text{ lin. cesta nad } g \\ \text{od } v \text{ k } w}} \mathrm{C_p}(\tilde{U}) \right) \\
&= \sum_{w \in \mathbb{F}_2^n} \sum_{\substack{\tilde{U} \text{ lin. cesta nad } g \\ \text{od } v \text{ k } w}} \mathrm{C}^{f_N}_{u,w} \cdot \mathrm{C_p}(\tilde{U}) \\
&= \sum_{w \in \mathbb{F}_2^n} \sum_{\substack{U \text{ lin. cesta nad } f \\ U = (v, \ldots, w, u)}} \mathrm{C_p}(U) \\
&= \sum_{\substack{U \text{ lin. cesta nad } f \\ \text{od } v \text{ k } u}} \mathrm{C_p}(U)
\end{aligned}$$

□

Korelační příspěvky lineárních cest mohou mít různá znaménka. Nalezení lineární cesty s velkou hodnotou $|\mathrm{C_p}(U)|$ tedy nemusí vždy vést k výrazné korelaci složené funkce f. Z pohledu iterovaných kryptosystémů můžeme booleovské funkce f_i chápat jako kolová šifrovací zobrazení pro konkrétní hodnoty kolových klíčů. Lineární útok na iterovaný kryptosystém může z uvedeného důvodu pro konkrétní hodnoty kolových klíčů selhat. V pozici útočníka ovšem kolové klíče neznáme. Důvod úspěšnosti lineárního útoku při náhodné volbě kolových klíčů popíšeme v závěru tohoto textu.

Korelační příspěvek lineární cesty nad klíč alternující šifrou. Tvar šifrovacího zobrazení N-kolové klíč alternující šifry pro dané kolové klíče $K_1, \ldots, K_{N+1}$ je

$$f = \left(\tau_{K_{N+1}} \circ \beta_N \circ \tau_{K_N}\right) \circ \left(\beta_{N-1} \circ \tau_{K_{N-1}}\right) \circ \ \ldots \ \circ \left(\beta_1 \circ \tau_{K_1}\right)$$

kde $\tau_{K_i} : \mathbb{F}_2^n \to \mathbb{F}_2^n$, $i = 1, \ldots, N+1$, jsou přičtení kolových klíčů a $\beta_i : \mathbb{F}_2^n \to \mathbb{F}_2^n$, $i = 1, \ldots, N$, nezávisí na klíčích. Mezi šifrovací algoritmy tohoto typu patří AES a také SPN.
Pro $f_i = \beta_i \circ \tau_{K_i}$, $i = 1, \ldots, N-1$, platí $\mathrm{C}^{f_i} = \mathrm{C}^{\beta_i} \cdot \mathrm{C}^{\tau_{K_i}}$. Víme, že $\mathrm{C}^{\tau_{K_i}}$ je diagonální s hodnotami na diagonále ± 1. Pro vektory $u, v \in \mathbb{F}_2^n$ tedy platí $\left|\mathrm{C}^{f_i}_{u,v}\right| = \left|\mathrm{C}^{\beta_i}_{u,v}\right|$.
V posledním kole $f_N = \tau_{K_{N+1}} \circ \beta_N \circ \tau_{K_N}$ dostaneme $\mathrm{C}^{f_N} = \mathrm{C}^{\tau_{K_{N+1}}} \cdot \mathrm{C}^{\beta_N} \cdot \mathrm{C}^{\tau_{K_N}}$. Opět pro vektory $u, v \in \mathbb{F}_2^n$ platí $\left|\mathrm{C}^{f_N}_{u,v}\right| = \left|\mathrm{C}^{\beta_N}_{u,v}\right|$.
Pro lineární cestu $U = (u^{(0)}, \ldots, u^{(N)})$ nad f pak bude

$$|\mathrm{C_p}(U)| \ = \ \left|\prod_{i=1}^{N} \mathrm{C}^{f_i}_{u^{(i)},u^{(i-1)}}\right| \ = \ \prod_{i=1}^{N} \left|\mathrm{C}^{f_i}_{u^{(i)},u^{(i-1)}}\right| \ = \ \prod_{i=1}^{N} \left|\mathrm{C}^{\beta_i}_{u^{(i)},u^{(i-1)}}\right|$$

Nad klíč alternující šifrou tedy $|\mathrm{C_p}(U)|$ nezávisí na hodnotách klíčů.

Příklad konstrukce lineární cesty. Budeme pracovat nad substitučně-permutační sítí se 4-bitovým S-boxem π_S:

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
8	F	3	0	A	5	9	6	C	1	E	2	7	4	D	B

Substituční vrstva σ bude obsahovat čtyři S-boxy. Tabulka permutace π_P:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	3	11	5	8	0	15	9	1	12	4	7	13	6	14	10

Zkonstruujeme lineární cestu $U = (u^{(0)}, \ldots, u^{(3)})$ nad prvními třemi koly 4-kolové verze SPN. V korelační matici π_S zvolíme jednu z výraznějších hodnot, například pro vektory $\mathtt{0x3}, \mathtt{0xC} \in \mathbb{F}_2^4$ je $\mathrm{C}^{\pi_\mathrm{S}}_{\mathtt{0x3},\mathtt{0xC}} = \frac{3}{4}$. Řekněme, že začneme těmito paritami na druhém S-boxu substituční vrstvy. Položíme $u^{(0)} = \mathtt{0x0C00}$ a označíme $w^{(1)} = \mathtt{0x0300}$, vektory v $\mathbb{F}_2^{16}$. Pro $u^{(1)} = e_{\pi_\mathrm{P}}(w^{(1)}) = \mathtt{0x0041}$ platí:

$$\mathrm{C}^{e_{\pi_\mathrm{P}} \circ \sigma}_{u^{(1)},u^{(0)}} = \mathrm{C}(\mathrm{p}_{u^{(1)}} \circ (e_{\pi_\mathrm{P}} \circ \sigma), \mathrm{p}_{u^{(0)}}) = \mathrm{C}((\mathrm{p}_{e_{\pi_\mathrm{P}}(w^{(1)})} \circ e_{\pi_\mathrm{P}}) \circ \sigma, \mathrm{p}_{u^{(0)}}) = \mathrm{C}(\mathrm{p}_{w^{(1)}} \circ \sigma, \mathrm{p}_{u^{(0)}}) = \mathrm{C}^{\sigma}_{w^{(1)},u^{(0)}}$$

Pro bricklayer funkci σ dostaneme:

$$\mathrm{C}^{e_{\pi_\mathrm{P}}\circ\sigma}_{u^{(1)},u^{(0)}} = \mathrm{C}^{\sigma}_{w^{(1)},u^{(0)}} = \mathrm{C}^{\pi_\mathrm{S}}_{0,0}\cdot\mathrm{C}^{\pi_\mathrm{S}}_{\mathtt{0x3,0xC}}\cdot\mathrm{C}^{\pi_\mathrm{S}}_{0,0}\cdot\mathrm{C}^{\pi_\mathrm{S}}_{0,0} = \mathrm{C}^{\pi_\mathrm{S}}_{\mathtt{0x3,0xC}} = \frac{3}{4}$$

Určili jsme, až na znaménko, hodnotu korelace prvního lineárního kroku. Budeme pokračovat volbou výstupních parit na druhé vrstvě S-boxů.
Na třetím S-boxu zvolme například $\mathrm{C}^{\pi_\mathrm{S}}_{\mathtt{0xC,0x4}} = \frac{3}{4}$ a na čtvrtém S-boxu $\mathrm{C}^{\pi_\mathrm{S}}_{\mathtt{0x8,0x1}} = -\frac{1}{2}$. Položme $w^{(2)} = \mathtt{0x00C8},\ u^{(2)} = e_{\pi_\mathrm{P}}(w^{(2)}) = \mathtt{0x400C}$. V druhém kroku dostaneme korelaci:

$$\mathrm{C}^{e_{\pi_\mathrm{P}}\circ\sigma}_{u^{(2)},u^{(1)}} = \mathrm{C}^{\sigma}_{w^{(2)},u^{(1)}} = \mathrm{C}^{\pi_\mathrm{S}}_{0,0}\cdot\mathrm{C}^{\pi_\mathrm{S}}_{0,0}\cdot\mathrm{C}^{\pi_\mathrm{S}}_{\mathtt{0xC,0x4}}\cdot\mathrm{C}^{\pi_\mathrm{S}}_{\mathtt{0x8,0x1}} = \frac{3}{4}\cdot\left(-\frac{1}{2}\right) = -\frac{3}{8}$$

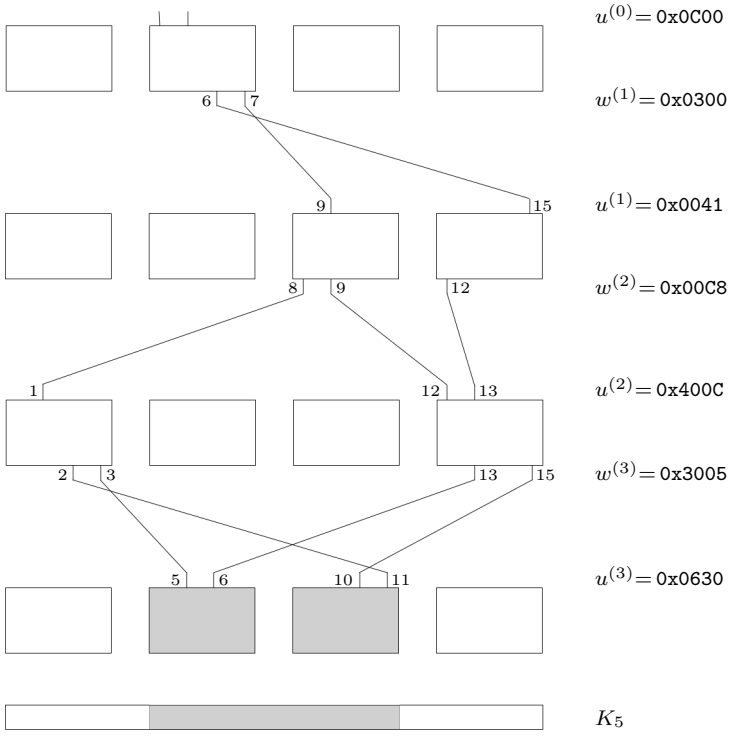
Na třetí vrstvě S-boxů zvolme $\mathrm{C}^{\pi_\mathrm{S}}_{\mathtt{0x3,0x4}} = \frac{1}{4}$ pro první S-box a $\mathrm{C}^{\pi_\mathrm{S}}_{\mathtt{0x5,0xC}} = \frac{1}{4}$ pro čtvrtý S-box. Tedy $w^{(3)} = \mathtt{0x3005}$, $u^{(3)} = e_{\pi_\mathrm{P}}(w^{(3)}) = \mathtt{0x0630}$ a korelace třetího kroku:

$$\mathrm{C}^{e_{\pi_\mathrm{P}}\circ\sigma}_{u^{(3)},u^{(2)}} = \mathrm{C}^{\sigma}_{w^{(3)},u^{(2)}} = \mathrm{C}^{\pi_\mathrm{S}}_{\mathtt{0x3,0x4}}\cdot\mathrm{C}^{\pi_\mathrm{S}}_{0,0}\cdot\mathrm{C}^{\pi_\mathrm{S}}_{0,0}\cdot\mathrm{C}^{\pi_\mathrm{S}}_{\mathtt{0x5,0xC}} = \frac{1}{4}\cdot\frac{1}{4} = \frac{1}{16}$$

Pro korelační příspěvek cesty U tedy platí:

$$|\mathrm{C_p}(U)| = \frac{3}{4}\cdot\frac{3}{8}\cdot\frac{1}{16} = \frac{9}{512}$$

Během konstrukce se snažíme udržet cestu v malém počtu S-boxů, v opačném případě bychom pravděpodobně zhoršili její korelační příspěvek. Jak dále uvidíme, při útoku na poslední kolový klíč je také žádoucí, abychom cestu zakončili v malém počtu S-boxů. V našem příkladu cesta končí na druhém a třetím S-boxu.



Lineární útok na substitučně-permutační síť. Popíšeme lineární útok na SPN, jehož cílem je získat část posledního kolového klíče. Postup útoku na N-kolovou verzi:

1. Konstrukce lineární cesty $U = (u^{(0)}, \ldots, u^{(N-1)})$ nad prvními $N-1$ koly SPN s výraznou hodnotou $|\mathrm{C_p}(U)|$. Označíme $v = u^{(0)}$, $u = u^{(N-1)}$.

2. Nasbírání množiny vzorků $T = \{(x, f(x))\}$, kde f je šifrovací zobrazení N-kolové SPN (pro neznámé ale pevně dané klíče). Odhaduje se, že počet vzorků by měl zhruba odpovídat hodnotě $\frac{1}{\mathrm{C_p^2}(U)}$.

3. Na indexech těch S-boxů, na kterých je vektor u nenulový (tedy na S-boxech, na kterých končí cesta U), tipujeme část posledního kolového klíče K_{N+1}. Pro každý takový tip $\tilde{K}$ spočítáme

$$\mathrm{C}_{\tilde{K}} = 2 \cdot \frac{\left|\left\{(x,y) \in T\,;\ \mathrm{p}_u(\sigma^{-1}(y + \tilde{K})) = \mathrm{p}_v(x)\right\}\right|}{|T|} - 1$$

   Pro korektní výpočet bychom měli rozšířit $\tilde{K}$ na celou délku kolového klíče, nicméně na zbylých S-boxech je vektor u nulový a tedy výsledek parity p_u na těchto hodnotách nezávisí. Je-li tip na klíč správný, můžeme $\mathrm{C}_{\tilde{K}}$ chápat jako aproximaci korelace $\mathrm{C}^{f'}_{u,v}$ na množině vzorků, kde f' je šifrovací zobrazení prvních $N-1$ kol.

Tipy na část K_{N+1} s výraznou hodnotou $|\mathrm{C}_{\tilde{K}}|$ jsou kandidáty na hledaný výsledek.

Poznámky. 1) Kromě určité míry náhodnosti plaintextů nevyžadujeme žádnou specifickou vlastnost sbíraných vzorků. Proto v tomto případě mluvíme o *known plaintext* útoku.

2) Lineární útok lze považovat za úspěšný, pokud je mezi nalezenými kandidáty správný tip na částečný klíč a případně malý počet false positive výsledků. Z tohoto pohledu je důležité, aby lineární cesta končila v malém počtu S-boxů. Jednak musí být vyhodnocení všech možností pro částečný klíč výpočetně zvládnutelné a také by nemělo projít příliš mnoho false positive výsledků.

3) Pokud bychom s lineární cestou prošli i přes poslední vrstvu S-boxů, při vyhodnocování tipů na klíč bychom k ciphertextu pouze přičetli příslušný tip na klíč a spočítali hodnotu parity. Víme, že přičtení klíče mění pouze znaménka vstupů původní korelační matice. Tímto způsobem bychom tedy špatné tipy neodlišili. Lineární útok spoléhá na 'náhodné' chování S-boxů, které při zpětném průchodu poslední substituční vrstvou tipy na klíč dostatečně rozliší.

4) Popsaným postupem můžeme útočit na krajní kolové klíče. Podobně můžeme v případě úspěchu získat část prvního kolového klíče.

Pro booleovskou funkci $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ a vektory $v \in \mathbb{F}_2^n$, $u \in \mathbb{F}_2^m$, značíme $\mathrm{CP}^f_{u,v}$ korelační potenciál $\mathrm{p}_u \circ f$ ve v, tedy $\mathrm{CP}^f_{u,v} = \mathrm{C}^2(\mathrm{p}_u \circ f, \mathrm{p}_v)$.
Ve znění následujícího tvrzení chápeme klíč alternující šifru $f = f_N \circ \ldots \circ f_1$ jako produkt kolových kryptosystémů, zatímco po dosazení konkrétní $(N+1)$-tice kolových klíčů dostáváme booleovské funkce $f, f_1, \ldots, f_N : \mathbb{F}_2^n \to \mathbb{F}_2^n$.

Věta (*průměrný korelační potenciál*). Ať $f = f_N \circ \ldots \circ f_1$ je klíč alternující šifra. Pak pro vektory $u, v \in \mathbb{F}_2^n$ platí

$$\mathrm{E}(\mathrm{CP}^f_{u,v}) = \sum_{\substack{U \text{ lin. cesta nad } f \\ \text{od } v \text{ k } u}} \mathrm{C}_\mathrm{p}^2(U)$$

kde $\mathrm{E}(\mathrm{CP}^f_{u,v})$ je průměrný korelační potenciál, tedy aritmetický průměr hodnot $\mathrm{CP}^f_{u,v}$ na množině všech $(N+1)$-tic kolových klíčů.

Důkaz. Pro $U = (u^{(0)}, \ldots, u^{(N)})$ lineární cestu nad f označme $\tilde{\mathrm{C}}_\mathrm{p}(U)$ korelační příspěvek cesty U nad algoritmem f s vynecháním kolových klíčů. Korelační příspěvek U pro kolové klíče $K_1, \ldots, K_{N+1}$ pak můžeme vyjádřit:

$$\begin{aligned}
\mathrm{C}_\mathrm{p}(U) &= \mathrm{C}^{\tau_{K_{N+1}} \circ \beta_N \circ \tau_{K_N}}_{u^{(N)},u^{(N-1)}} \cdot \quad \cdots \quad \cdot \mathrm{C}^{\beta_1 \circ \tau_{K_1}}_{u^{(1)},u^{(0)}} \\
&= \left(\mathrm{C}^{\tau_{K_{N+1}}}_{u^{(N)},u^{(N)}} \cdot \mathrm{C}^{\beta_N}_{u^{(N)},u^{(N-1)}} \cdot \mathrm{C}^{\tau_{K_N}}_{u^{(N-1)},u^{(N-1)}}\right) \cdot \quad \cdots \quad \cdot \left(\mathrm{C}^{\beta_1}_{u^{(1)},u^{(0)}} \cdot \mathrm{C}^{\tau_{K_1}}_{u^{(0)},u^{(0)}}\right) \\
&= (-1)^{u^{(N)} \cdot K_{N+1}} \cdot \mathrm{C}^{\beta_N}_{u^{(N)},u^{(N-1)}} \cdot (-1)^{u^{(N-1)} \cdot K_N} \cdot \quad \cdots \quad \cdot \left(\mathrm{C}^{\beta_1}_{u^{(1)},u^{(0)}} \cdot (-1)^{u^{(0)} \cdot K_1}\right) \\
&= (-1)^{\sum_{i=0}^{N} u^{(i)} \cdot K_{i+1}} \cdot \tilde{\mathrm{C}}_\mathrm{p}(U) \\
&= (-1)^{U \cdot K} \cdot \tilde{\mathrm{C}}_\mathrm{p}(U)
\end{aligned}$$

kde U chápeme jako konkatenaci svých vektorů a K je konkatenace klíčů $K_1, \ldots, K_{N+1}$.
Nyní upravme vyjádření průměrného korelačního potenciálu:

$$\begin{aligned}
\mathrm{E}(\mathrm{CP}^f_{u,v}) &= \frac{1}{2^{(N+1)\cdot n}} \cdot \sum_{K_1,\ldots,K_{N+1} \in \mathbb{F}_2^n} \mathrm{CP}^f_{u,v} \\
&= \frac{1}{2^{(N+1)\cdot n}} \cdot \sum_{K_1,\ldots,K_{N+1} \in \mathbb{F}_2^n} \left(\mathrm{C}^f_{u,v}\right)^2 \\
&= \frac{1}{2^{(N+1)\cdot n}} \cdot \sum_{K_1,\ldots,K_{N+1} \in \mathbb{F}_2^n} \left(\sum_{\substack{U \text{ lin. cesta nad } f \\ \text{od } v \text{ k } u}} \mathrm{C}_\mathrm{p}(U) \right)^2 \\
&= \frac{1}{2^{(N+1)\cdot n}} \cdot \sum_{K_1,\ldots,K_{N+1} \in \mathbb{F}_2^n} \quad \sum_{\substack{U \text{ lin. cesta nad } f \\ \text{od } v \text{ k } u}} \quad \sum_{\substack{V \text{ lin. cesta nad } f \\ \text{od } v \text{ k } u}} \mathrm{C}_\mathrm{p}(U) \cdot \mathrm{C}_\mathrm{p}(V) \\
&= \frac{1}{2^{(N+1)\cdot n}} \cdot \sum_{\substack{U \text{ lin. cesta nad } f \\ \text{od } v \text{ k } u}} \quad \sum_{\substack{V \text{ lin. cesta nad } f \\ \text{od } v \text{ k } u}} \quad \sum_{K \in \mathbb{F}_2^{(N+1)\cdot n}} \widehat{\mathrm{p}}_U(K) \cdot \tilde{\mathrm{C}}_\mathrm{p}(U) \cdot \widehat{\mathrm{p}}_V(K) \cdot \tilde{\mathrm{C}}_\mathrm{p}(V) \\
&= \frac{1}{2^{(N+1)\cdot n}} \cdot \sum_{\substack{U \text{ lin. cesta nad } f \\ \text{od } v \text{ k } u}} \quad \sum_{\substack{V \text{ lin. cesta nad } f \\ \text{od } v \text{ k } u}} \tilde{\mathrm{C}}_\mathrm{p}(U) \cdot \tilde{\mathrm{C}}_\mathrm{p}(V) \cdot \sum_{K \in \mathbb{F}_2^{(N+1)\cdot n}} \widehat{\mathrm{p}}_U(K) \cdot \widehat{\mathrm{p}}_V(K) \\
&= \frac{1}{2^{(N+1)\cdot n}} \cdot \sum_{\substack{U \text{ lin. cesta nad } f \\ \text{od } v \text{ k } u}} \quad \sum_{\substack{V \text{ lin. cesta nad } f \\ \text{od } v \text{ k } u}} \tilde{\mathrm{C}}_\mathrm{p}(U) \cdot \tilde{\mathrm{C}}_\mathrm{p}(V) \cdot (\widehat{\mathrm{p}}_U, \widehat{\mathrm{p}}_V)
\end{aligned}$$

$$= \frac{1}{2^{(N+1)\cdot n}} \cdot \sum_{\substack{U \text{ lin. cesta nad } f \\ \text{od } v \text{ k } u}} \left(\tilde{\mathrm{C}}_{\mathrm{p}}(U)\right)^2 \cdot 2^{(N+1)\cdot n}$$

$$= \sum_{\substack{U \text{ lin. cesta nad } f \\ \text{od } v \text{ k } u}} \mathrm{C}_{\mathrm{p}}^2(U)$$

□

Poznámka. Má-li být lineární útok úspěšný, musí nalezená lineární cesta s výrazným korelačním příspěvkem svědčit o výrazné korelaci. To nemusí vždy platit, ale předchozí věta ukazuje, že pro průměrnou (náhodnou) volbu kolových klíčů se korelační příspěvky lineárních cest musí projevit.