

**České vysoké učení technické v Praze
Fakulta elektrotechnická
Katedra telekomunikační techniky**

A7B32KBE 5. přednáška

Moderní blokové šifry III

Ing. Tomáš Vaněk, Ph.D. tomas.vanek@fel.cvut.cz





CAMELLIA

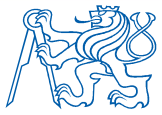
Autoři: Nippon Telegraph and Telephone Corporation
Mitsubishi Electric Corporation

- sestrojena v roce 2000
- 2003 zařazena mezi doporučené bezpečné kryptografické primitivy v programu EU NESSIE (New European Schemes for Signatures, Integrity and Encryption).
- v Japonsku zařazena na seznam doporučených programů pro využití pro vládní účely
- odolná proti diferenciální a lineární kryptoanalýze
- šifra Feistelova typu
- vhodná jak pro SW i HW implementaci (32 bitové procesory), tak i pro čipové karty (8 bitové procesory)



CAMELLIA – základní informace

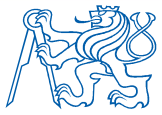
- symetrická bloková šifra
 - patentovaná, ale volně k dispozici (royalty-free licence)
 - délka bloku: 128 bitů
 - délka klíče: 128, 192, a 256-bitů
 - počet rund - 18 pro klíč délky 128 bitů
 - 24 pro klíče délky 192, 256 bitů
 - každých 6 rund vloženy přídatné funkce FL, FL⁻¹
 - čtyři 64bitové S-boxy
 - bílení klíče
 - lineární transformace založeny na MDS
 - operace v algoritmu CAMELLIA lze popsat pomocí multivarietních polynomů - $GF((2^8))^8$
-



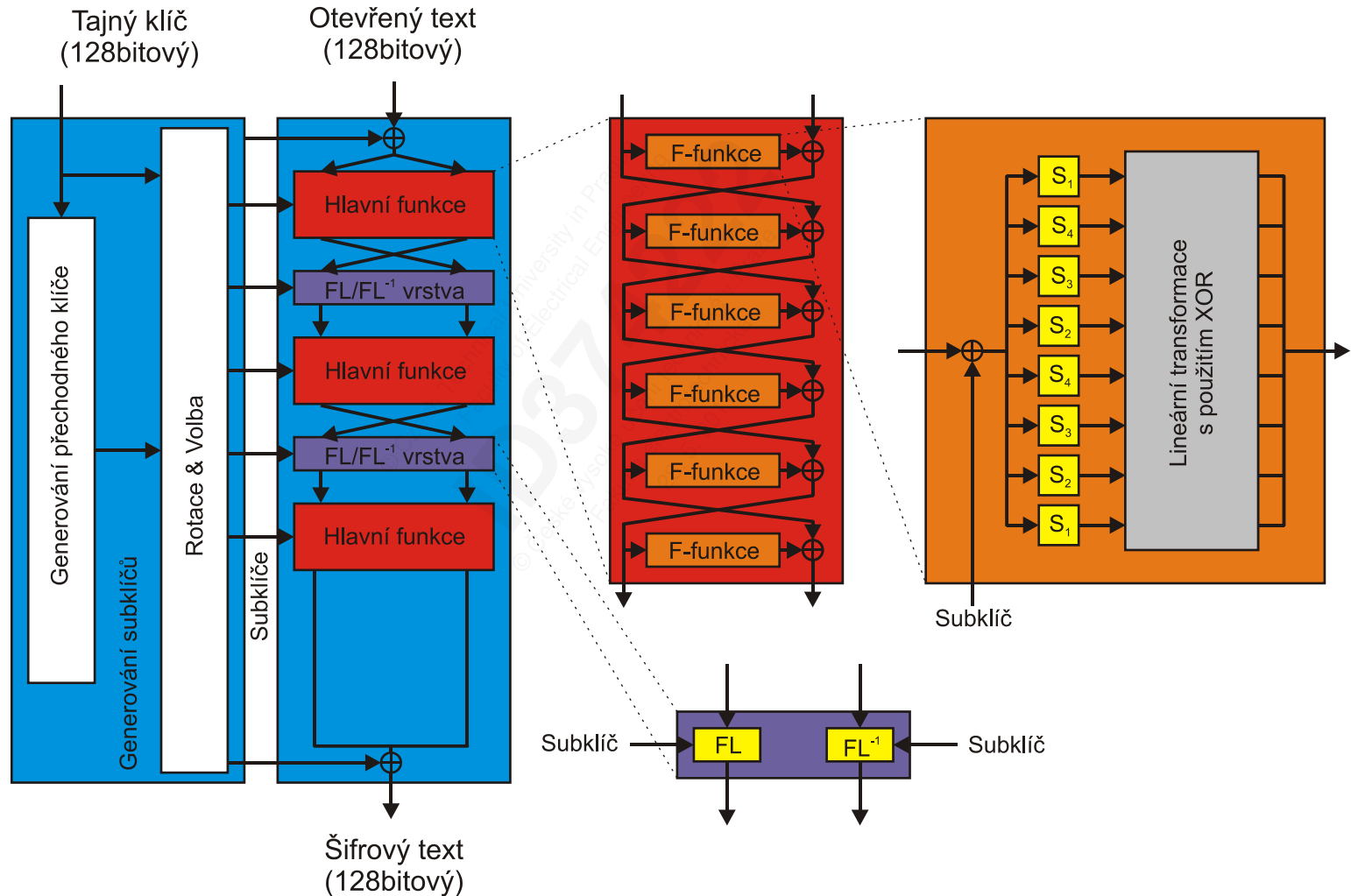
CAMELLIA – základní informace

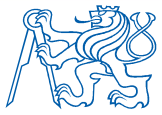
Algoritmus Camellia je podporován v řadě standardů a doporučení:

- IPsec - RFC 4312
- SSL/TLS - RFC 4132
- S/MIME – RFC 3657
- XML security URI – RFC 4051
- OpenSSL
- ISO/IEC18033-3
- PKCS#11
- GnuTLS



CAMELLIA – šifrování s 128bitovým klíčem





CAMELLIA

Blok OT délky 128 bitů M je pomocí operace XOR sloučen se dvěma 64bitovými podklíči $kw_1 \parallel kw_2$ a dále je rozdělen do dvou 64bitových datových větví L_0 a R_0 .

Následující operace jsou prováděny od $r = 1$ do 18, kromě $r = 6$ a 12:

$$L_r = R_{r-1} \oplus F(\llcorner_{r-1}, k_r)$$

$$R_r = L_{r-1}.$$

Pro $r = 6$ a 12 je prováděno podle vztahů:

$$L'_r = R_{r-1} \oplus F(\llcorner_{r-1}, k_r)$$

$$R'_r = L_{r-1}$$

$$L_r = FL(\llcorner'_r, kl_{r/3-1})$$

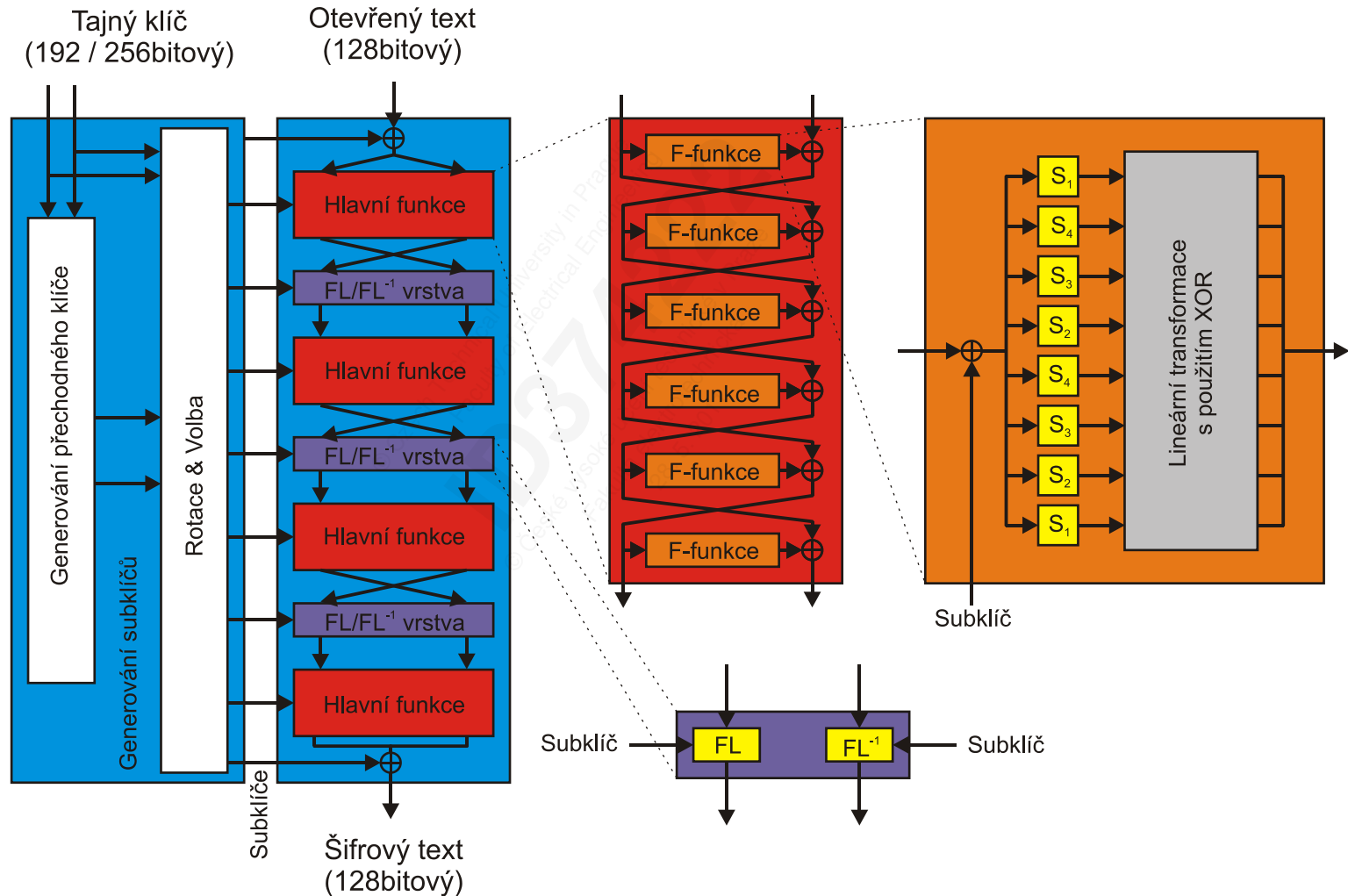
$$R_r = FL^{-1}(\llcorner'_r, kl_{r/3})$$

Poslední poloviny R_{18} a L_{18} jsou kaskádní a pomocí operace XOR sloučeny s 64bitovými podklíči $kw_3 \parallel kw_4$.

Výsledkem 128bitový blok ŠT.



CAMELLIA – šifrování s 192/256bitovým klíčem



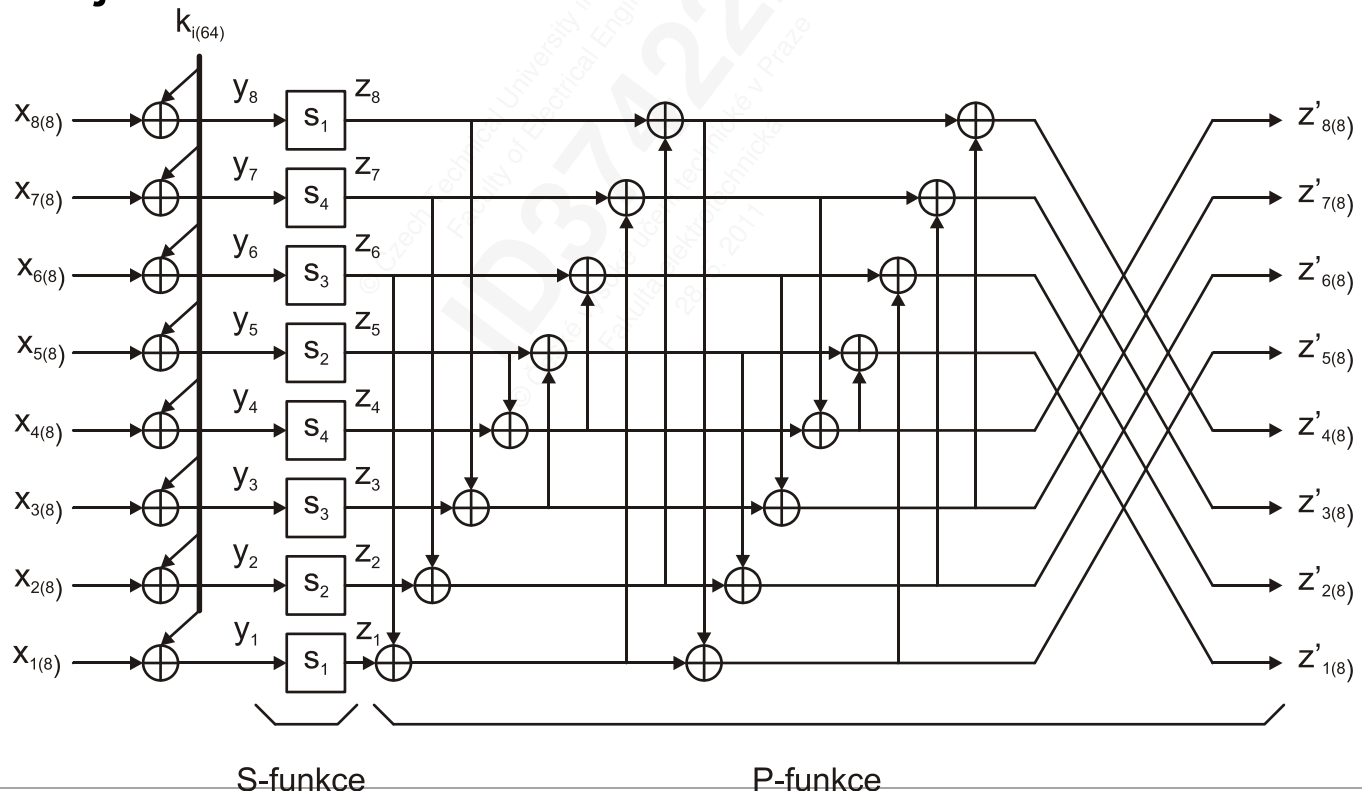


CAMELLIA

- Schéma procesu šifrování pro 192 a 256bitové klíče je stejné jako v případě použití 128bitového klíče s tím rozdílem, že obsahuje navíc jednu hlavní funkci a jednu FL/FL^{-1} vrstvu.
- Dešifrování probíhá stejně jako šifrování, pouze jednotlivé rundové podklíče se zadávají ve zpětném pořadí.
- Každých 6 rund je vložena vrstva FL/FL^{-1}

CAMELLIA – schéma F-funkce

- F-funkce má SPN strukturu
- S-funkce je nelineární vrstva
- P-funkce je lineární vrstva





CAMELLIA - popis P-funkce

- P-funkce je definována následovně:

$$P: (GF((2)^8)^8 \rightarrow (GF((2)^8)^8, (z_1, z_2, \dots, z_8) \mapsto (z'_1, z'_2, \dots, z'_8),$$

kde

$$z'_1 = z_1 \oplus z_3 \oplus z_4 \oplus z_6 \oplus z_7 \oplus z_8$$

$$z'_2 = z_1 \oplus z_2 \oplus z_4 \oplus z_5 \oplus z_7 \oplus z_8$$

$$z'_3 = z_1 \oplus z_2 \oplus z_3 \oplus z_5 \oplus z_6 \oplus z_8$$

$$z'_4 = z_2 \oplus z_3 \oplus z_4 \oplus z_5 \oplus z_6 \oplus z_7$$

$$z'_5 = z_1 \oplus z_2 \oplus z_6 \oplus z_7 \oplus z_8$$

$$z'_6 = z_2 \oplus z_3 \oplus z_5 \oplus z_7 \oplus z_8$$

$$z'_7 = z_3 \oplus z_4 \oplus z_5 \oplus z_6 \oplus z_8$$

$$z'_8 = z_1 \oplus z_4 \oplus z_5 \oplus z_6 \oplus z_7.$$

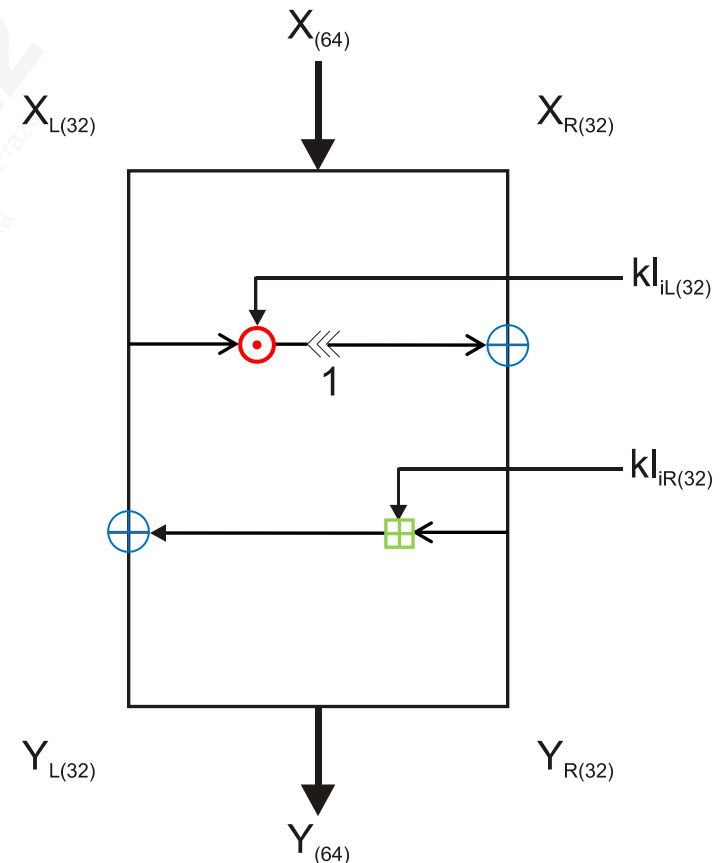


CAMELLIA – schéma FL-funkce

Definice: $FL: GF(2)^{64} \times GF(2)^{64} \rightarrow GF(2)^{64}, (X_L \parallel X_R, kl_L \parallel kl_R) \mapsto Y_L \parallel Y_R$,

kde $Y_R = ((X_L \odot kl_L) \lll_1) \oplus X_R$

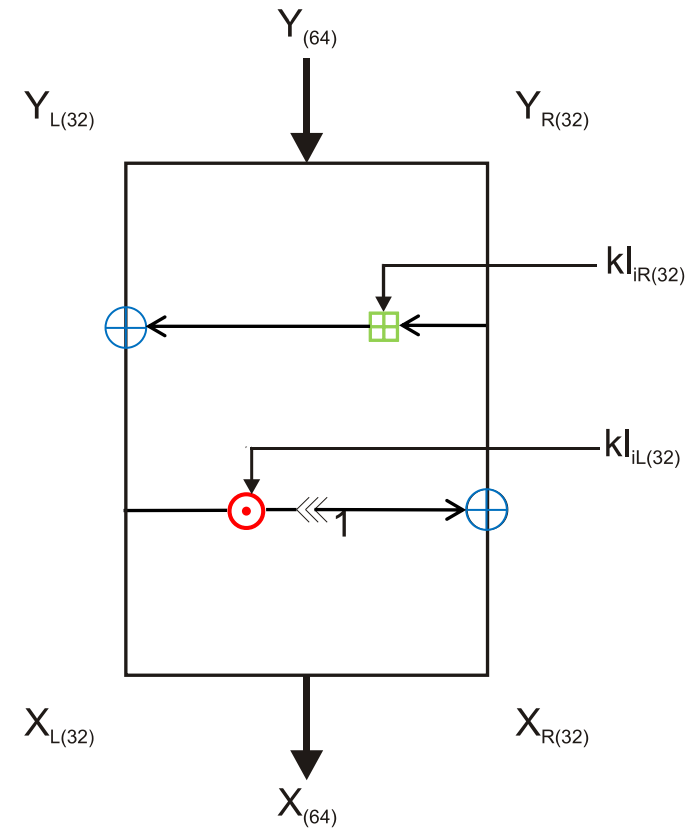
$Y_L = (Y_R \boxplus kl_R) \oplus X_L$.

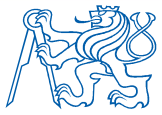




CAMELLIA – schéma FL^{-1} -funkce

$$FL^{-1} = (FL(x, k), k) = x.$$





CAMELLIA - bezpečnost

- nejsou známe žádné efektivní útoky
- celý algoritmus lze popsat pomocí 6224 rovnic s 3584 proměnnými, které celkem obsahují 17920 lineárních a kvadratických členů
- **teoreticky** možné použít XLS útok

CAMELLIA vs. AES

- CAMELLIA má Feistelovu strukturu → efektivnější implementace v čipových kartách
- srovnatelná úroveň bezpečnosti i rychlosti s AES

Dotazy



Právní doložka (licence) k tomuto Dílu (elektronický materiál)

České vysoké učení technické v Praze (dále jen ČVUT) je ve smyslu autorského zákona vykonavatelem majetkových práv k Dílu či držitelem licence k užití Díla. Užívat Dílo smí pouze student nebo zaměstnanec ČVUT (dále jen Uživatel), a to za podmínek dále uvedených.

ČVUT poskytuje podle autorského zákona, v platném znění, oprávnění k užití tohoto Díla pouze Uživateli a pouze ke studijním nebo pedagogickým účelům na ČVUT. Toto Dílo ani jeho část nesmí být dále šířena (elektronicky, tiskově, vizuálně, audiem a jiným způsobem), rozmnožována (elektronicky, tiskově, vizuálně, audiem a jiným způsobem), využívána na školení, a to ani jako doplňkový materiál. Dílo nebo jeho část nesmí být bez souhlasu ČVUT využívána ke komerčním účelům. Uživateli je povoleno ponechat si Dílo i po skončení studia či pedagogické činnosti na ČVUT, výhradně pro vlastní osobní potřebu. Tím není dotčeno právo zákazu výše zmíněného užití Díla bez souhlasu ČVUT. Současně není dovoleno jakýmkoliv způsobem manipulovat s obsahem materiálu, zejména měnit jeho obsah včetně elektronických popisných dat, odstraňovat nebo měnit zabezpečení včetně vodoznaku a odstraňovat nebo měnit tyto licenční podmínky.

V případě, že Uživatel nebo jiná osoba, která drží toto Dílo (Držitel díla), nesouhlasí s touto licencí, nebo je touto licencí vyloučena z užití Díla, je jeho povinností zdržet se užívání Díla a je povinen toto Dílo trvale odstranit včetně veškerých kopií (elektronické, tiskové, vizuální, audio a zhotovených jiným způsobem) z elektronického zařízení a všech záznamových zařízení, na které jej Držitel díla umístil.