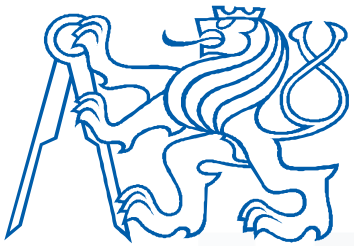
České vysoké učení technické v Praze
Fakulta elektrotechnická
Katedra telekomunikační techniky

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

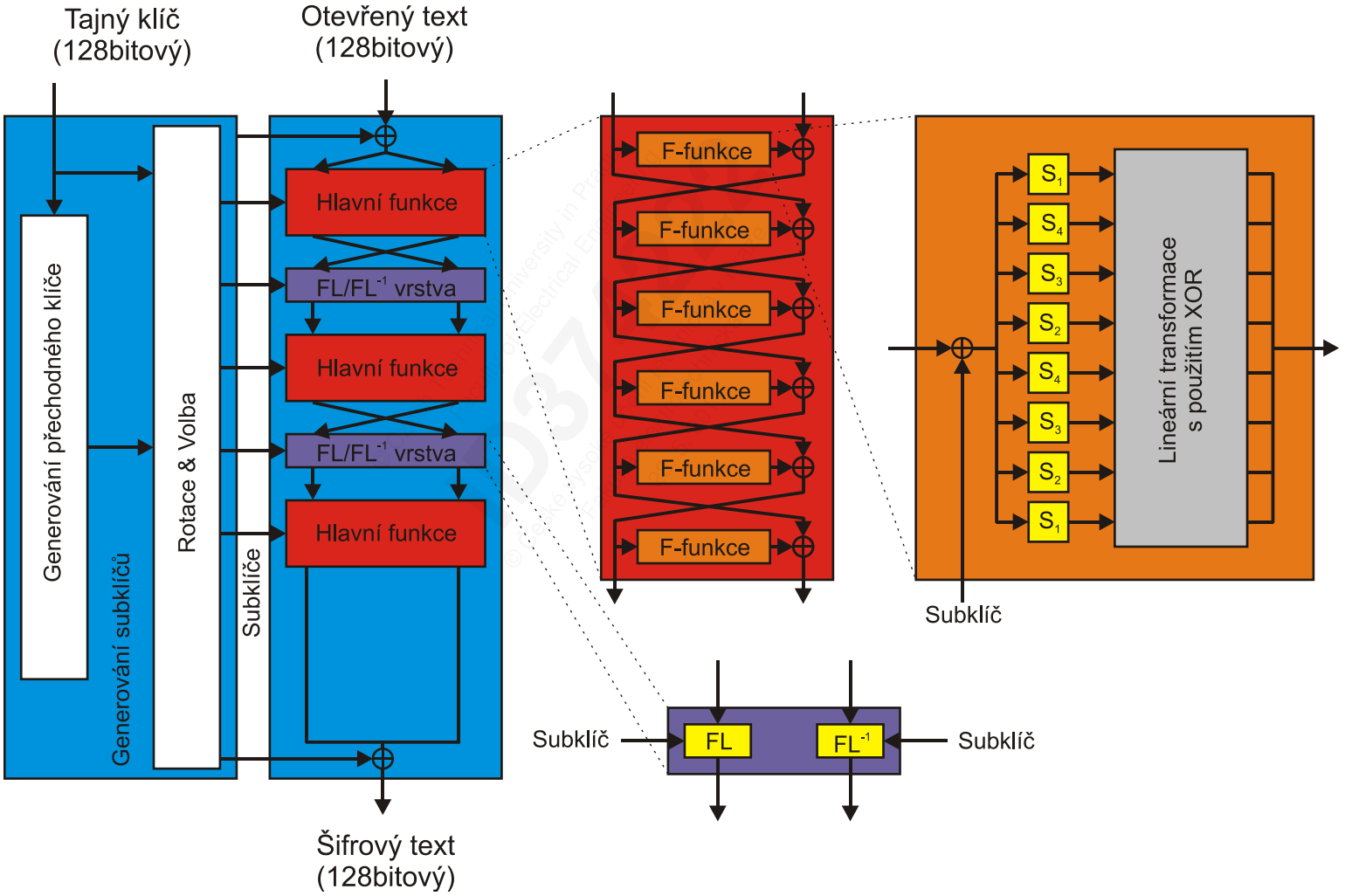
- symetrická bloková šifra
- patentovaná, ale volně k dispozici (royalty-free licence)
- délka bloku: 128 bitů
- délka klíče: 128, 192, a 256-bitů
- počet rund - 18 pro klíč délky 128 bitů
  - 24 pro klíče délky 192, 256 bitů
- každých 6 rund vloženy přídavné funkce FL, FL^{-1}
- čtyři 64bitové S-boxy
- 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:

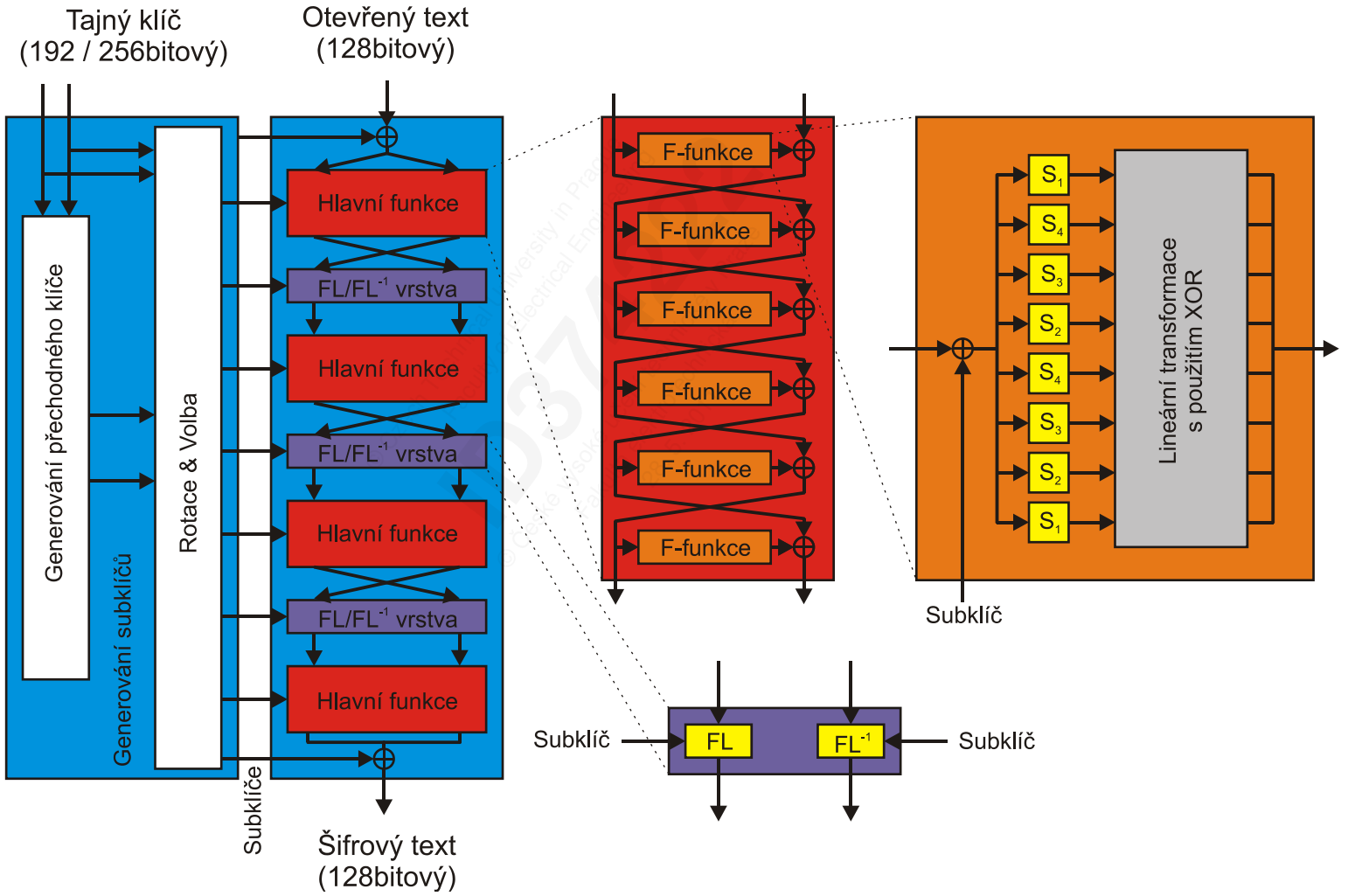
$$L_r = R_{r-1} \oplus F(L_{r-1}, k_r)$$
$$R_r = L_{r-1}.$$

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

$$L'_r = R_{r-1} \oplus F(L_{r-1}, k_r)$$
$$R'_r = L_{r-1}$$
$$L_r = FL(L'_r, kl_{r/3-1})$$
$$R_r = FL^{-1}(R'_r, kl_{r/3}).$$

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

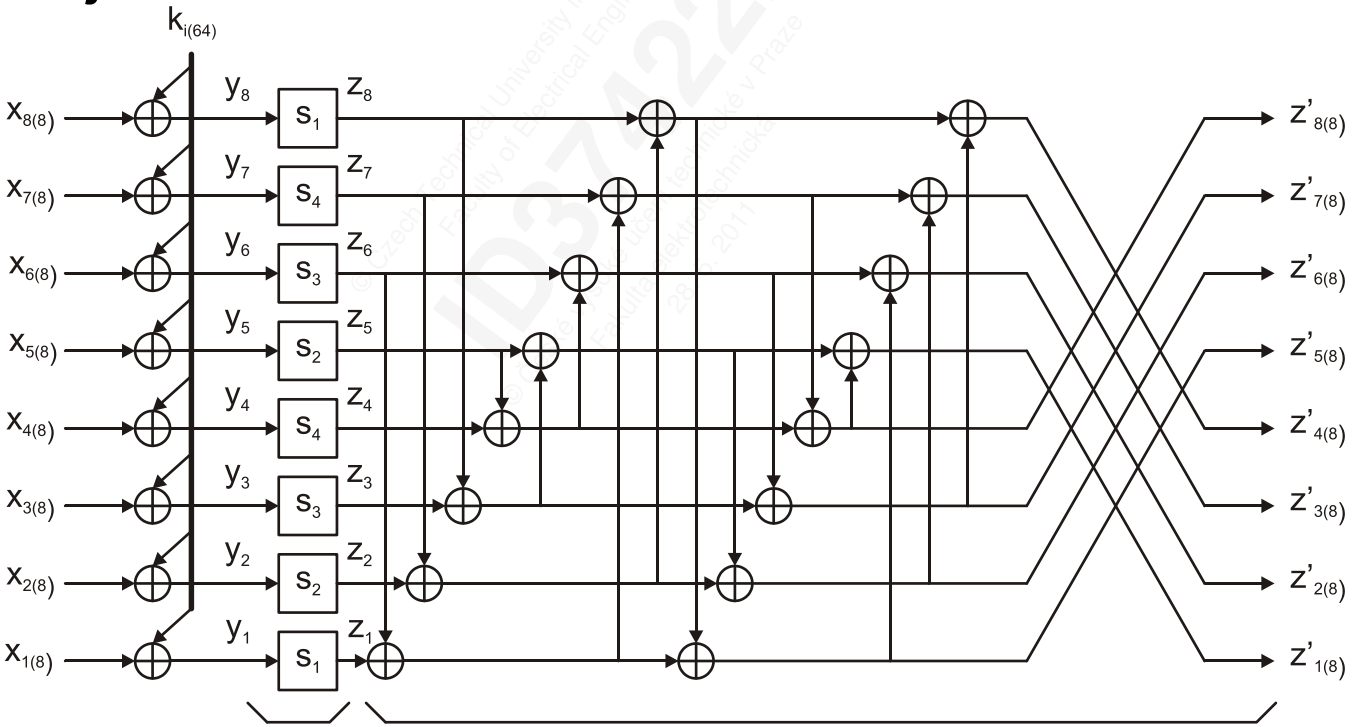


CAMELLIA

- 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:

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

kde

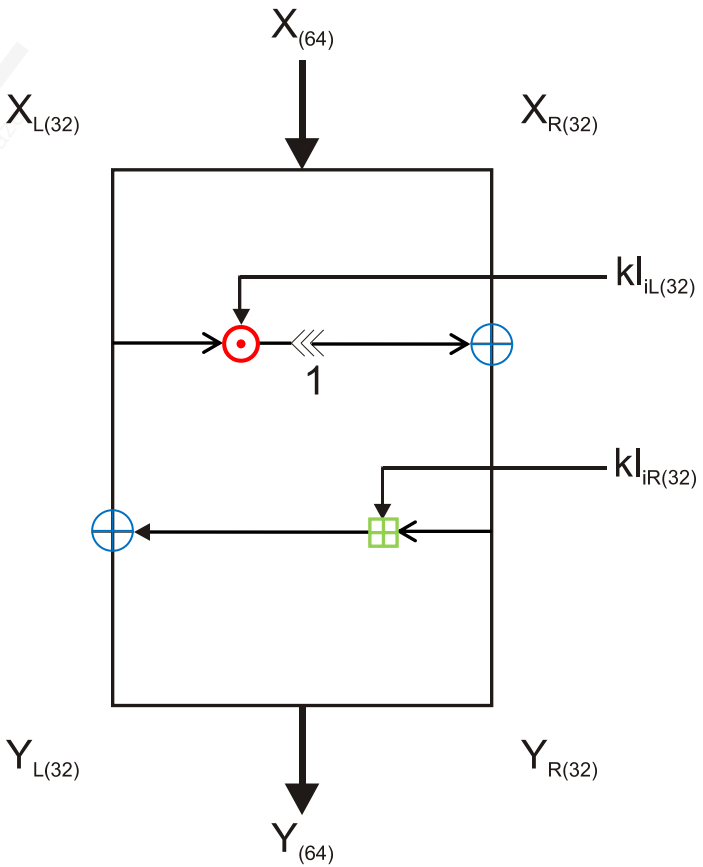
$$z'_1 = z_1 \oplus z_3 \oplus z_4 \oplus z_6 \oplus z_7 \oplus z_8$$
$$z'_2 = z_1 \oplus z_2 \oplus z_4 \oplus z_5 \oplus z_7 \oplus z_8$$
$$z'_3 = z_1 \oplus z_2 \oplus z_3 \oplus z_5 \oplus z_6 \oplus z_8$$
$$z'_4 = z_2 \oplus z_3 \oplus z_4 \oplus z_5 \oplus z_6 \oplus z_7$$
$$z'_5 = z_1 \oplus z_2 \oplus z_6 \oplus z_7 \oplus z_8$$
$$z'_6 = z_2 \oplus z_3 \oplus z_5 \oplus z_7 \oplus z_8$$
$$z'_7 = z_3 \oplus z_4 \oplus z_5 \oplus z_6 \oplus z_8$$
$$z'_8 = z_1 \oplus z_4 \oplus z_5 \oplus z_6 \oplus z_7.$$

CAMELLIA – schéma FL-funkce

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

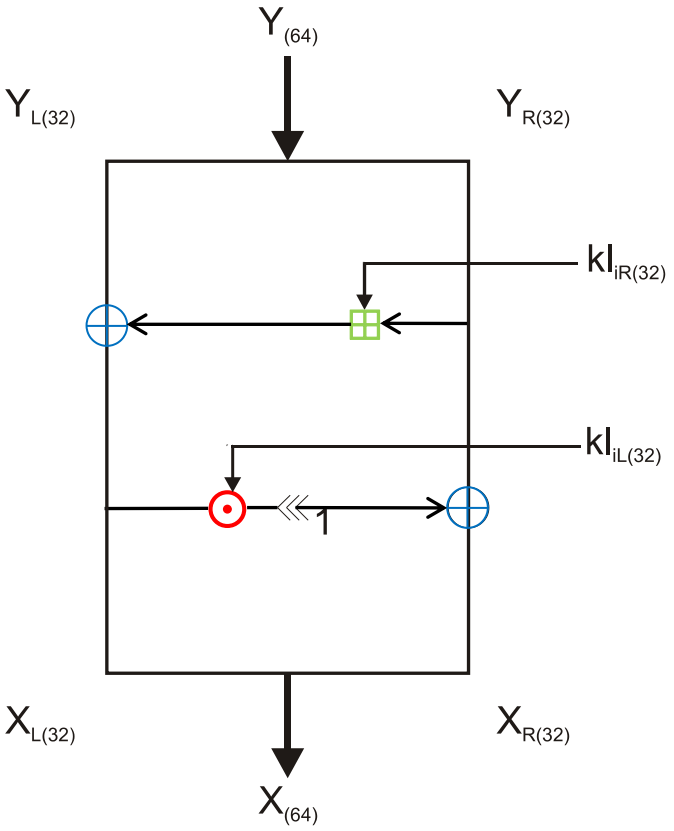
kde $Y_R = ((X_L \odot kl_L) <<<_1) \oplus X_R$

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



CAMELLIA – schéma FL^{-1}-funkce

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



CAMELLIA - bezpečnost

- nejsou známé 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