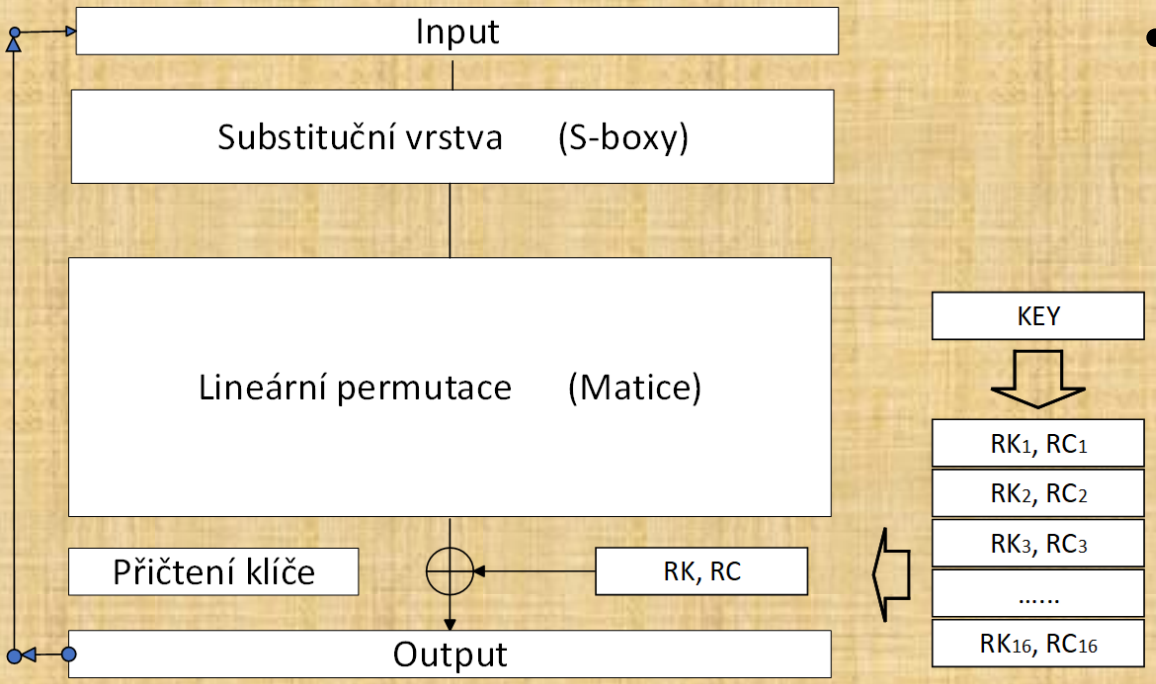
Klíč obsahující šifru

RNDr. Vlastimil Klíma

MKB, 5. 12. 2024

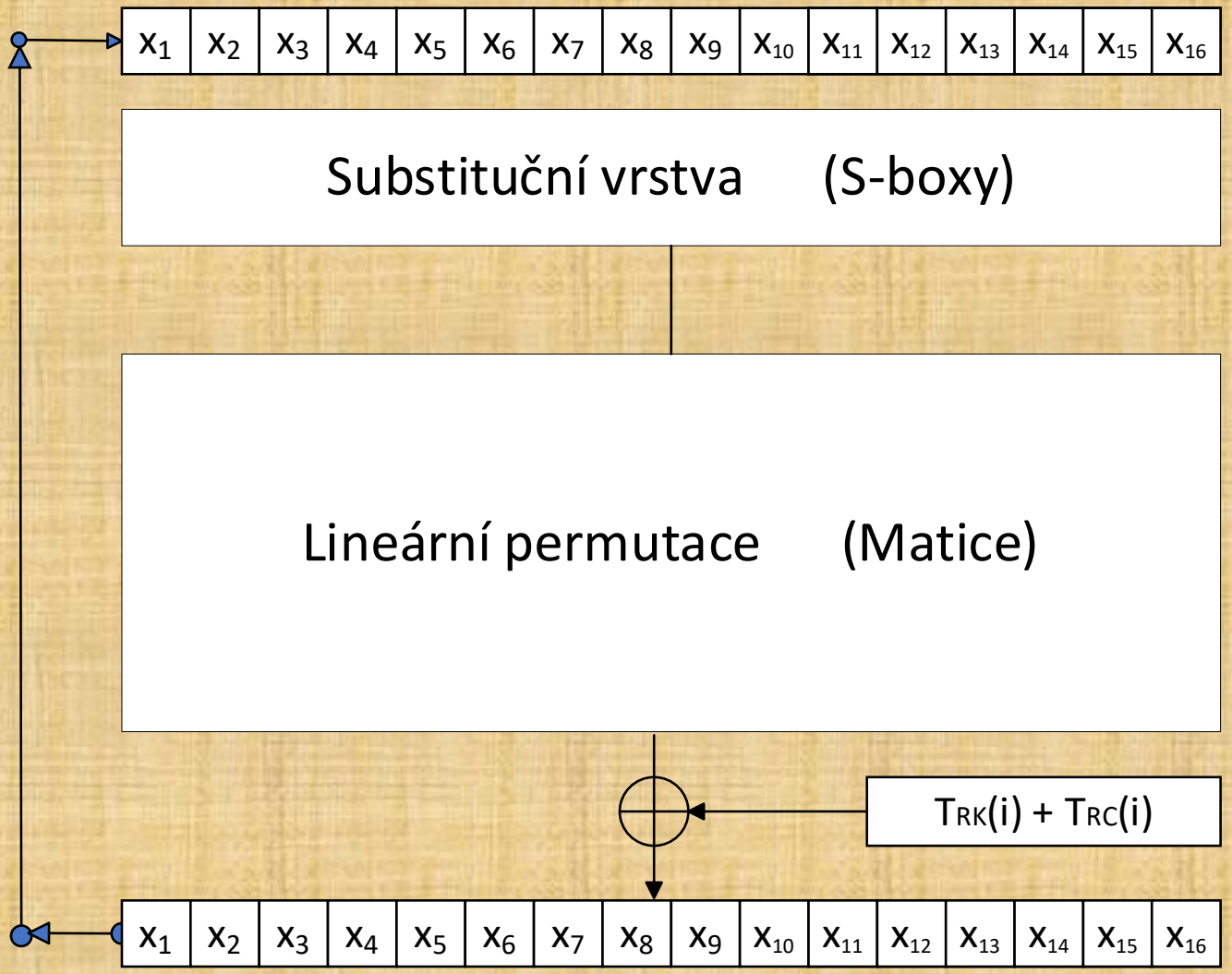
Založeno na odborném vystoupení na Národním úřadu pro kybernetickou bezpečnost

Substitučně permutační sítě jako výsledek evolučního vývoje

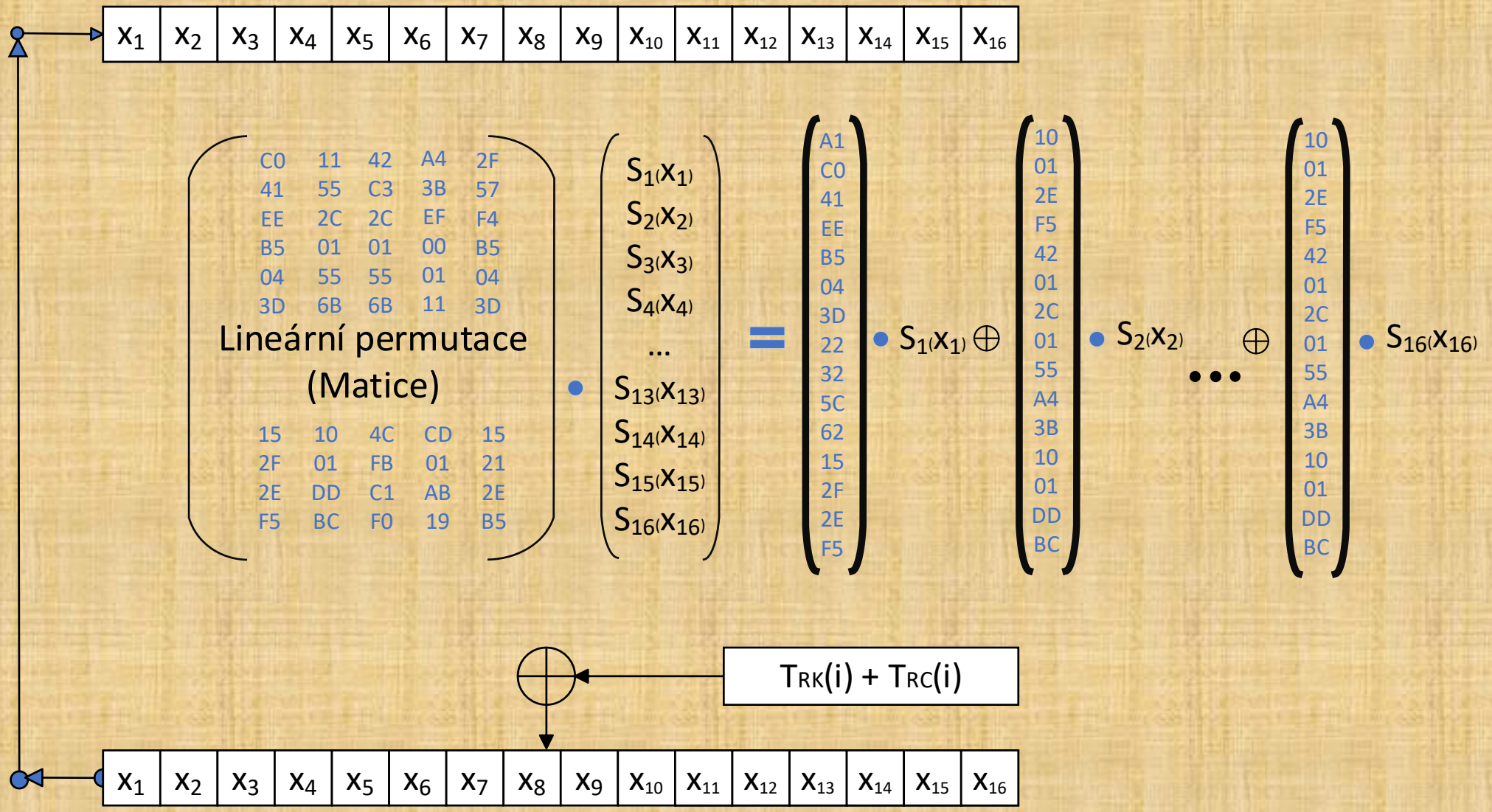


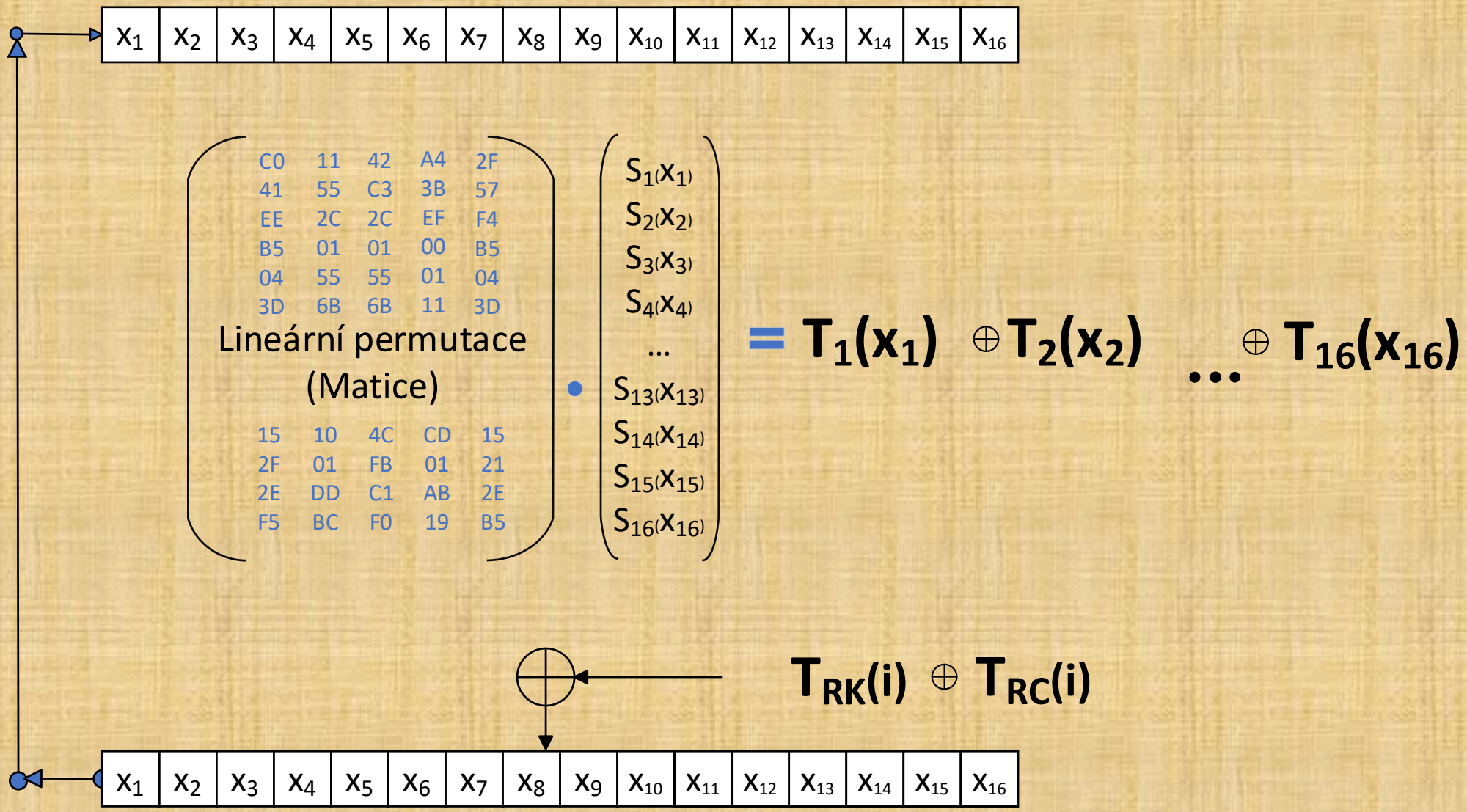
- Vývoj dospěl k tomu, že je vhodné vytvořit kvalitní nelineární vrstvu, následovanou kvalitní lineární permutací a přičtení (rundovního) klíče

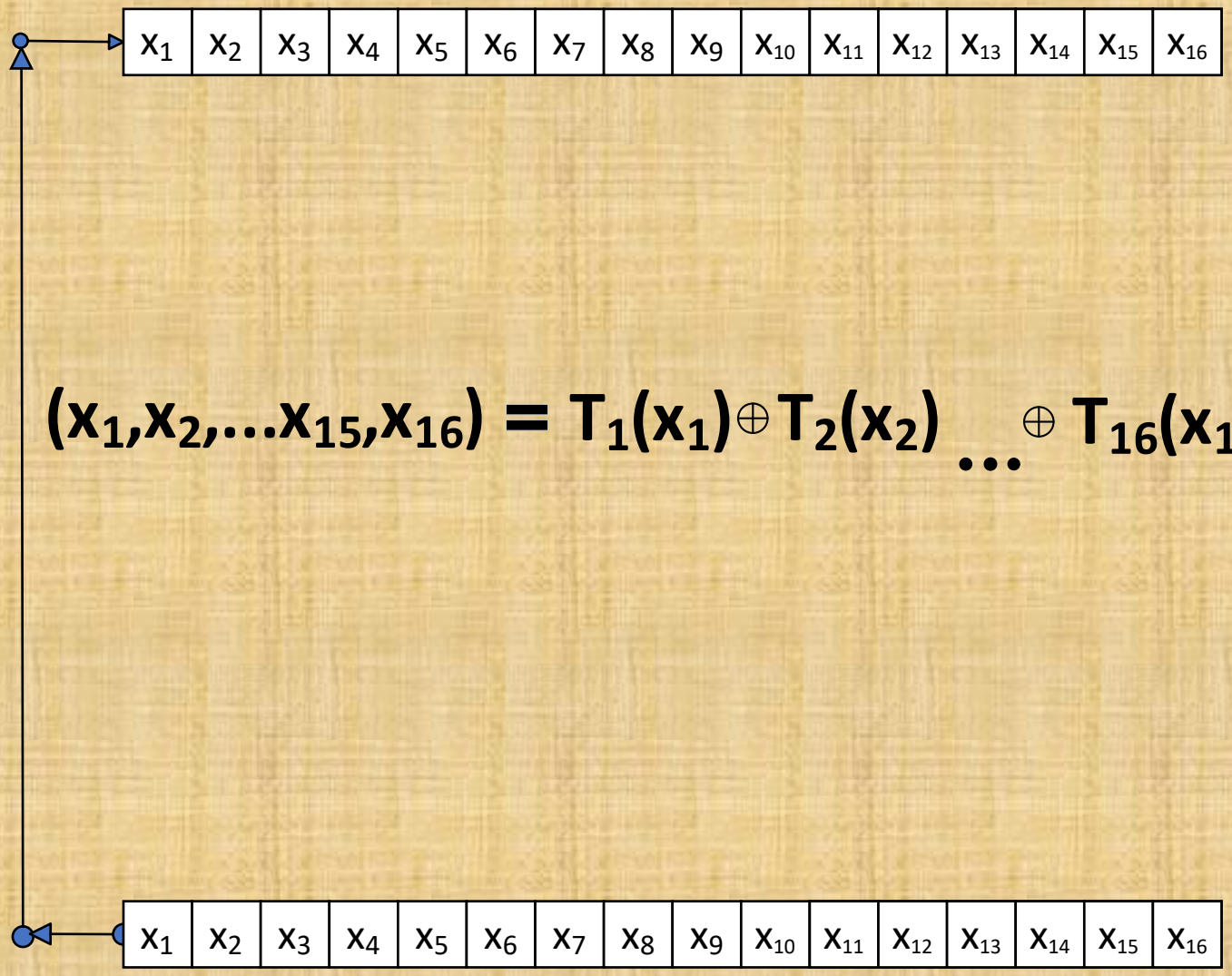
AES, CLEFIA, KALYNA, KASUMI, KUZNYECHIK, MISTY, PRESENT, RIJNDAEL, SAFER, SERPENT, SHARK, SM4, SPACE, SQUARE, WARX, WAS, 3-WAY, 3DES, ...



Příklad pro šířku bloku 16 bajtů


x1 x2 x3 x4 x5 x6 x7 x8 x9 x10 x11 x12 x13 x14 x15 x16
C0 11 42 A4 2F
41 55 C3 3B 57
EE 2C 2C EF F4
B5 01 01 00 B5
04 55 55 01 04
3D 6B 6B 11 3D
Lineární permutace
(Matice)
15 10 4C CD 15
2F 01 FB 01 21
2E DD C1 AB 2E
F5 BC F0 19 B5
S1(x1)
S2(x2)
S3(x3)
S4(x4)
...
S13(x13)
S14(x14)
S15(x15)
S16(x16)
A1 C0 41 EE B5 04 3D 22 32 5C 62 15 2F 2E F5
S1(x1)
10 01 2E F5 42 01 2C 01 55 A4 3B 10 01 DD BC
S2(x2)
10 01 2E F5 42 01 2C 01 55 A4 3B 10 01 DD BC
S16(x16)
TRK(i) + TRC(i)
x1 x2 x3 x4 x5 x6 x7 x8 x9 x10 x11 x12 x13 x14 x15 x16


x1 x2 x3 x4 x5 x6 x7 x8 x9 x10 x11 x12 x13 x14 x15 x16
C0 11 42 A4 2F
41 55 C3 3B 57
EE 2C 2C EF F4
B5 01 01 00 B5
04 55 55 01 04
3D 6B 6B 11 3D
Lineární permutace
(Matice)
15 10 4C CD 15
2F 01 FB 01 21
2E DD C1 AB 2E
F5 BC F0 19 B5
S1(x1)
S2(x2)
S3(x3)
S4(x4)
...
S13(x13)
S14(x14)
S15(x15)
S16(x16)
= T1(x1) ⊕ T2(x2) ... ⊕ T16(x16)
TRK(i) ⊕ TRC(i)
x1 x2 x3 x4 x5 x6 x7 x8 x9 x10 x11 x12 x13 x14 x15 x16



$$(x_1,x_2,\ldots x_{15},x_{16}) = T_1(x_1) \oplus T_2(x_2) \ldots \oplus T_{16}(x_{16}) \quad \oplus T_{RK}(i) \oplus T_{RC}(i)$$

For i=1 to Nr

$$(x_1,x_2,\ldots x_{15},x_{16}) = T_1(x_1) \oplus T_2(x_2) \ldots \oplus T_{16}(x_{16}) \oplus T_{RK}(i) \oplus T_{RC}(i)$$

Tabulka T
T1
T2
……
Tn
RC
RK1, RK2, RK3, …. RK15, RK16
Pracovní oblast pro vstup a výstup X1, x2, … xn

For i=1 to N

$$T(Adr_0) = T(Adr_1) \oplus T(Adr_2) \oplus \ldots \oplus T(Adr_{n1}) \oplus T(Adr_{n2})$$

Tabulka T
Základní údaje: N, Nb,...
i=1: počet adres, adresy: A, A, A, A, A,
i=2: počet adres, adresy: A, A, A, A, A,
… počet adres, adresy: A, A, A, A, A,
T1
T2
…..
Tn
RC
RK1, RK2, RK3, … RK15, RK16
Pracovní oblast pro vstup a výstup X1, x2, … xn

For i=1 to N **T(Adr)=T(Adr) ⊕ T(Adr)…⊕ T(Adr)**

Tabulka T	-	AES
Tabulka T	-	CLEFIA
Tabulka T	-	KAL Y NA
Tabulka T	-	KASUMI
Tabulka T	-	KUZNYECHIK
Tabulka T	-	MISTY
Tabulka T	-	PRESENT
Tabulka T	-	RIJNDAEL
Tabulka T	-	SAFER
Tabulka T	-	SERPENT
Tabulka T	-	SHARK
Tabulka T	-	SM4
Tabulka T	-	SPACE
Tabulka T	-	SQUARE
Tabulka T	-	WARX
Tabulka T	-	3-WAY
Tabulka T	-	3DES

For i=1 to N $\mathbf{T(Adr) = T(Adr) \oplus T(Adr) \ldots \oplus T(Adr)}$

Tabulka T

For i=1 to N **T(Adr)=T(Adr) ⊕ T(Adr)...⊕ T(Adr)**

Tabulka T - KEY

For i=1 to N **T(Adr)=T(Adr) ⊕ T(Adr)...⊕ T(Adr)**

For i=1 to N $\mathbf{T(Adr) = T(Adr) \oplus T(Adr) \ldots \oplus T(Adr)}$

Tabulková šifra - vlastnosti

- Tabulková šifra může realizovat většinu známých **světových nebo národních standardů**.
- Tabulková šifra má **jeden řádek** programového kódu.
- V tabulkové šifře **klíč obsahuje i šifru.**
- Některé **státní šifry** mají například tajné S-boxy, které **nemohou být ve veřejném software. Tabulková šifra může být ve veřejném software, protože má tajné prvky chráněné v klíči.**
- Pokud se **umělá inteligence nebo kvantová kryptografie** nedostane ke klíči, nedostane se ani k šifře, nemá na čem trénovat a co luštit.
- Tabulková šifra používá teoreticky jen čtení a psaní do paměti a operaci xor, tj. **operace, které umí každý procesor.**
- Prostředí a programátor určí, jak velké Tabulky se použijí (1 kB, 100 kB, 1 MB,…), přičemž je zde silný vztah mezi časem a pamětí.
- Poznámky:
  - Celá tabulka je kromě řádků klíče konstantní. Klíče téže šifry tak mohou mít tabulku **společnou a mění** se jen některé řádky tabulky.
  - **Přípravu klíčů** lze většinou realizovat dohromady se šifrou.
  - Takže **někdy stačí přenášet jen 256 bitů klíče jako dosud**.