It is impossible to construct an internal re-keying that is suitable for any encryption mode

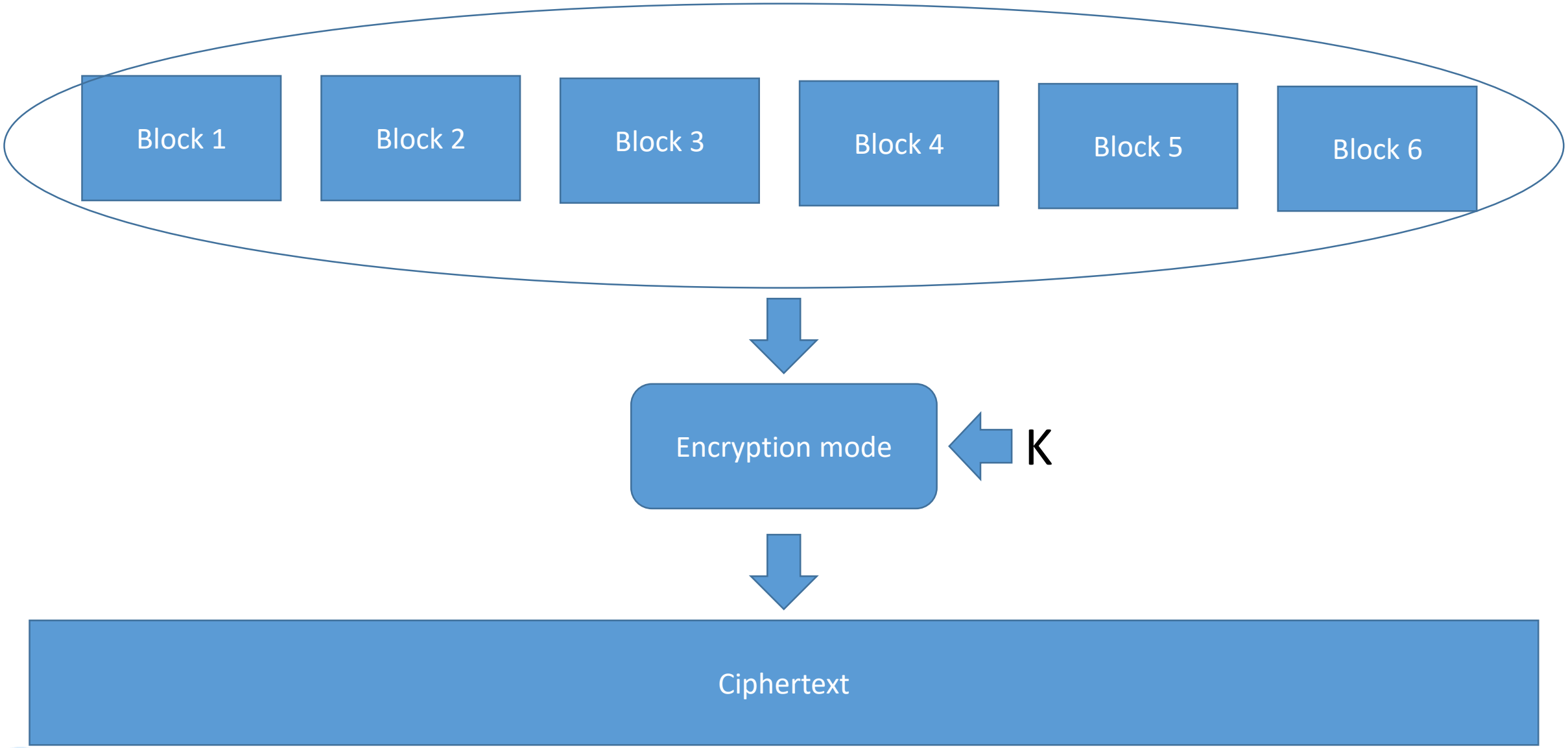
Alekseev Evgeny

CryptoPro LLC

CRYPTOPRO

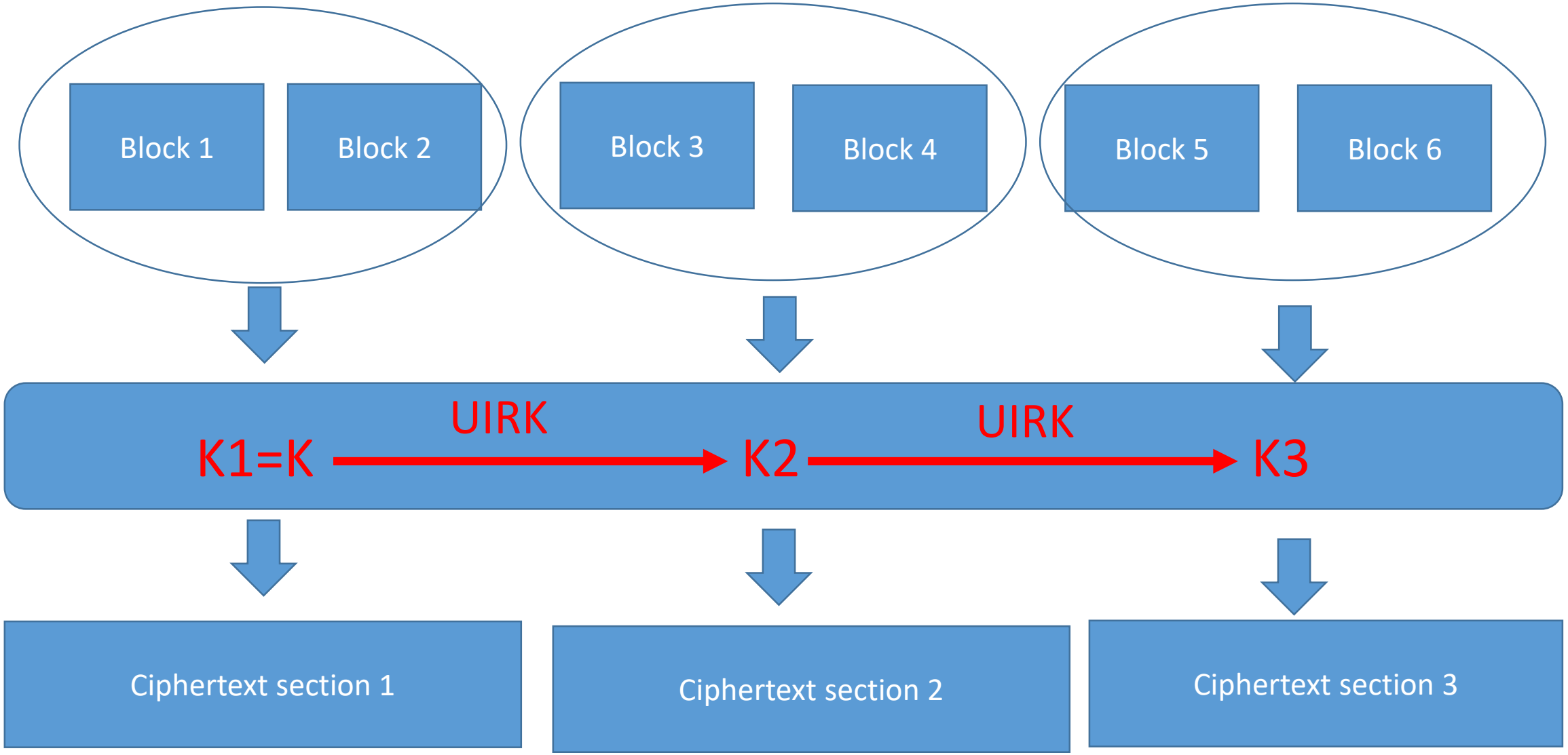
2023 CTCRYPT

Universal internal re-keying



CRYPTOPRO

Universal internal re-keying



Counterexample

$\underline{\text{CTR1.KGen}()}$

$K \xleftarrow{\mathcal{U}} \{0,1\}^k$

return K

$\underline{\text{CTR1.Enc}(K, M)}$

$IV \xleftarrow{\mathcal{U}} \{0,1\}^{n/2}$

$z \leftarrow \text{false}$

$T \leftarrow E_K(0^n)$

$G \leftarrow \varepsilon$

for $i = 1..|M|_n$ **do**

  if $T \neq E_K(0^n)$ **do** $z \leftarrow \text{true}$

  fi

  if z **do** $G \leftarrow G||0^n$

  else do $G \leftarrow G||E_K(IV||str_{n/2}(i))$

  fi

endfor

$C \leftarrow M \oplus G\,[:|M|]$

return (IV, C)

Counterexample

$\underline{\text{CTR1.KGen}()}$

$K \xleftarrow{\mathcal{U}} \{0,1\}^k$

return K

$\underline{\text{CTR1.Enc}(K, M)}$

$IV \xleftarrow{\mathcal{U}} \{0,1\}^{n/2}$

$z \leftarrow \text{false}$

$T \leftarrow E_K(0^n)$

$G \leftarrow \varepsilon$

for $i = 1..|M|_n$ **do**

  if $T \neq E_K(0^n)$ **do** $z \leftarrow \text{true}$

  fi

  if z **do** $G \leftarrow G||0^n$

  else do $G \leftarrow G||E_K(IV||str_{n/2}(i))$

  fi

endfor

$C \leftarrow M \oplus G\,[:|M|]$

return (IV, C)

K1, K2, K3

Thank you for your attention!

alekseev@cryptopro.ru

CRYPTOPRO

The presentation uses images from freepik.com