

Analyse de la difficulté des Cryptosystèmes à l'Aide du Problème du Transversal Minimum

Monika Trimoska

Gilles Dequen

Sorina Ionica

Équipe GOC

Journée des Jeunes Chercheurs du MIS
Amiens le 5 juillet 2019

Problème du Transversal Minimum

$$x_1 + x_2 \cdot x_3 + x_4 + x_4 \cdot x_5 = 0$$

$$x_1 + x_2 \cdot x_3 = 0$$

$$x_1 + x_3 \cdot x_5 + x_6 = 0$$

$$x_1 + x_2 \cdot x_5 \cdot x_6 + x_6 = 0$$



$$\begin{aligned}x_1 + x_3 &= 0 \\x_1 + x_3 &= 0 \\x_1 + x_3 + x_6 &= 0 \\x_1 &= 0\end{aligned}$$

Bivium

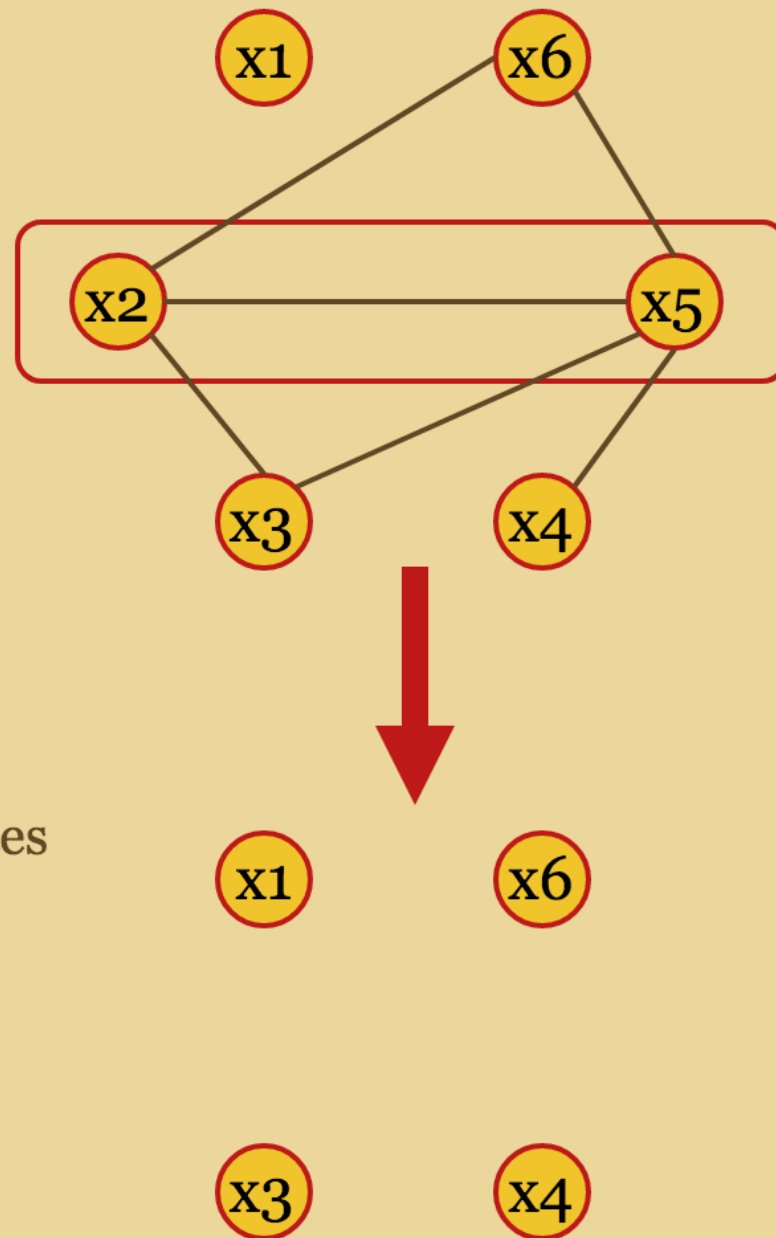
Trivium



Calcul d'indices
 S_3

Calcul d'indices
 S_4

Keccak



Analyse de la difficulté des Cryptosystèmes à l'Aide du Problème du Transversal Minimum

Questions ?



Journée des Jeunes Chercheurs du MIS
Amiens le 5 juillet 2019