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

Monika Trimoska

Gilles Dequen

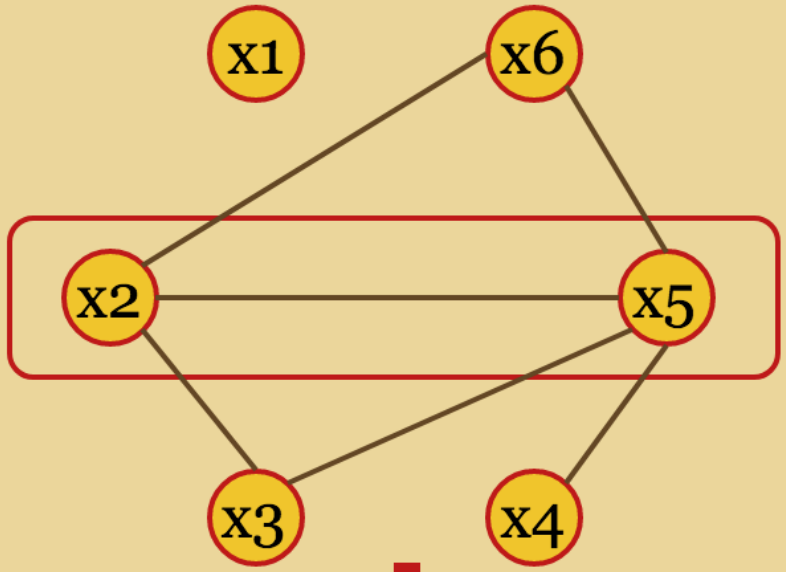
Sorina Ionica

Équipe GOC

Journée des Jeunes Chercheurs du MIS
Amiens le 5 juillet 2019

Problème du Transversal Minimum

$x1 + x2 \cdot x3 + x4 + x4 \cdot x5 = 0$
$x1 + x2 \cdot x3 = 0$
$x1 + x3 \cdot x5 + x6 = 0$
$x1 + x2 \cdot x5 \cdot x6 + x6 = 0$



Bivium

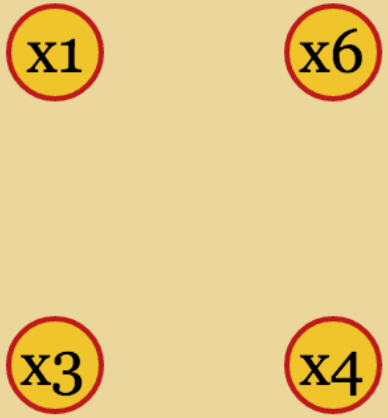
Trivium

Calcul d'indices
S3

Calcul d'indices
S4

$x1 + x3 = 0$
$x1 + x3 = 0$
$x1 + x3 + x6 = 0$
$x1 = 0$

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