Colloquium
de mathématiques

Daniel AUGOT
INRIA et École polytechnique

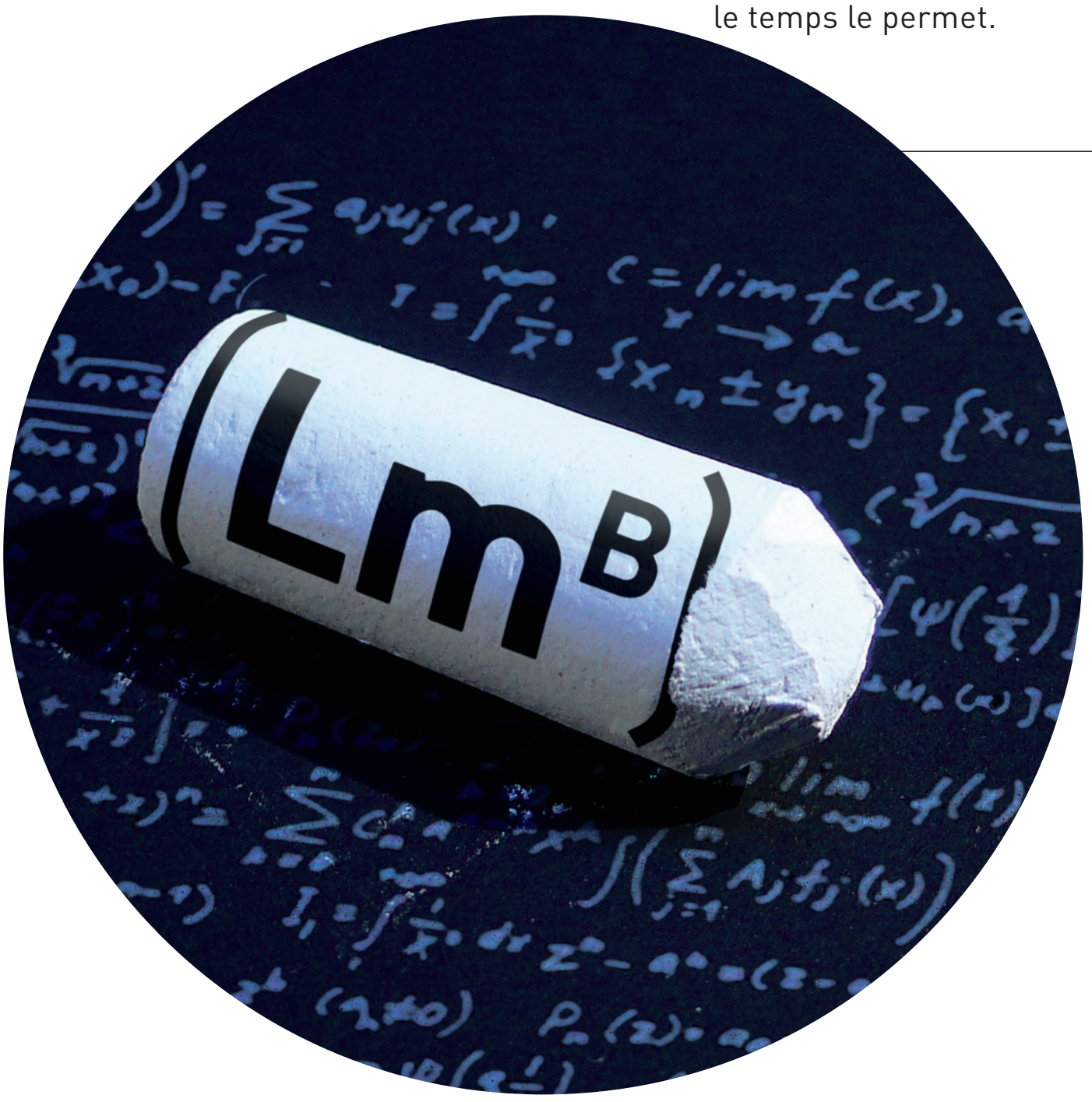
jeudi 24 oct. 2019
à 16h40

Amphi A, UFR ST
16 route de Gray - Besançon

http://lmb.univ-fcomte.fr/

→ Protocoles cryptographiques non standard autour des blockchains

Alors que la cryptographie traite en standard le plus souvent de chiffrement, de signature et d'authentification, le monde des blockchains est très demandeur de protocoles plus exotiques, comme le partage de secret ou des preuves de connaissance à divulgation nulle ("*zero-knowledge*").
Après avoir présenté rapidement ce qu'est une blockchain ouverte classique avec preuve de travail à la bitcoin, une méthode *zero-knowledge* sera présentée, voire un protocole de partage de secret, si le temps le permet.



laboratoire de mathématiques de besançon
UNIVERSITÉ DE FRANCHE-COMTÉ • CNRS • UMR 6623

UNIVERSITÉ DE FRANCHE-COMTÉ

UFR Sciences et techniques
UNIVERSITÉ DE FRANCHE-COMTÉ

DESIGN GRAPHIQUE et ©PHOTO BOUTEILLER COMMUNICATION BESANÇON - SEPTEMBRE 2019