

Dimanche 15 octobre

- Soir: accueil des participants et repas à 20h

Lundi 16 octobre

- **Matin**
 - 8h45-9h: Ouverture
 - 9h-10h:
Jacques Traoré: Sécurité du vote électronique
 - 10h-10h30:
Cécile Delerablée: Nouveau schéma de monnaie électronique anonyme
 - 10h30-11h: Pause
 - 11h-11h30:
Christine Bachoc: Bornes pour les codes sphériques et programmation semi-définie
 - 11h30-12h:
Frédéric A.B. Edoukou: La distribution des poids du code $C_2(X)$ défini sur des variétés projectives
 - 12h-12h30:
Jean Creignou: Configurations Simplectiques Optimales dans les Espaces Grassmanniens

Repas: 12h45
- **Après-midi**
 - 15h45-16h: goûter
 - 16h-16h30:
Eric Férard, François Rodier: Non-linéarité des fonctions booléennes et courbes hypersingulières
 - 16h30-17h:
Frédéric Didier: Comment utiliser l'algorithme de Wiedemann pour le calcul de l'immunité d'une fonction booléenne contre les attaques algébriques
 - 17h-17h30:
Laurent Poinot: Fonctions booléennes courbes dans les cas impossibles : les dimensions impaires et planes
 - 17h30-18h:
Vincent Bénony: BCS
- **Pot de bienvenue au Musée Rebeyrolles: 18h30**

navette retour du musée: 20h
repas: 20h30

Mardi 17 octobre

- **Matin**

- 9h-10h:

- Serge Chaumette: Problèmes de sécurité dans les matériels/configurations nomades

- 10h-10h30:

- Marine Minier: Cryptographie spécifique aux réseaux ad-hoc

- 10h30-11h: Pause

- 11h-11h30:

- Eve Atallah: Gestion des identités dans les MANets

- 11h30-12h

- Vincent Bénony, Eric Wegrzynowski: Sécurité et bibliothèques logicielles font-elles bon ménage?

- 12h-12h30

- Cédric Lauradoux: Implémentation efficace de primitives cryptographiques

Repas: 12h45

- **Après-midi**

- 15h45-16h : goûter

- 16h-16h30:

- Alban Duverdier: Techniques de codage utilisées dans les standards DVB pour les liaisons satellite

- 16h30-17h:

- Iryna Andriyanova, Jean-Pierre Tillich, Jean-Claude Carlach: Les performances de décodage itératif des codes Treillis-LDPC

- 17h-17h30:

- Vahid Meghdadi, Mohammad Reza Zahabi, Jean-Pierre Cances: Décodage analogique

- 17h30-18h

- Mathieu Cluzeau: Reconstruction d'un code linéaire en bloc en utilisant un algorithme de décodage itératif

- 18h-18h30:

- Andrea Röeck: Entropy Loss and Random Functions

Repas: 20h

Mercredi 18 octobre

- **Matin**
 - 9h-10h:
David Pointcheval: La sécurité prouvée
 - 10h-10h30:
Pierre-Alain Foulque, David Pointcheval, Jacques Stern et Sébastien Zimmer: Indistinguabilité des LSB du résultat d'un échange Diffie-Hellman
 - 10h30-11h: Pause
 - 11h-11h30:
Damien Vergnaud: Etude de propriétés de sécurité de signatures basées sur RSA
 - 11h30-12h:
Emeline Hufschmitt, Jacques Traoré: Fair Blind Signatures Revisited
 - 12h-12h30:
Ayoub Otmani, Damien Vergnaud: (In)sécurité des signatures de Kabatianskii-Krouk-Smeets

Repas: 12h45
- **Après-midi:**
 - 14h30-18h: visite de l'Ile de Vassivière et du Musée

Repas: 20h

Jeudi 19 octobre

- **Matin**
 - 9h-10h:
Ludovic Perret, Jean-Charles Faugères: Polynomial Equivalence Problems: Algorithmic and Theoretical Aspects
 - 10h-10h30:
Frederik Armknecht, Pierre-Louis Cayrel, Philippe Gaborit et Olivier Ruatta: Improved algorithm to find equations for algebraic attacks for combiners with memory
 - 10h30-11h: Pause
 - 11h-11h30:
D. Boucher, W. Geiselmann et F. Ulmer: Skew cyclic codes
 - 11h30-12h:
Cédric Faure: Nombre moyen de mots de code de Gabidulin à l'intérieur d'une boule
 - 12h-12h30

Repas: 12h45

- Après-midi
 - 14h45-15h45:
Présentation du GDR Informatique Mathématiques par Brigitte Vallée,
discussions autour du fonctionnement du groupe de travail C2.
 - 15h45-16h: goûter
 - 16h-17h:
Olivier Ruatta, Philippe Gaborit: Les méthodes d'interpolation et leur application en codage et cryptographie
 - 17h-17h30:
Eric Levieil Résolution efficace du problème LPN
 - 17h30-18h:
Christophe Negre, Thomas Plantard Multiplication modulaire dans les systèmes de représentation adaptés en utilisant la représentation de Lagrange
 - 18h-18h30:
Adnen Sboui Spectre de poids des codes de Red-Muller Généralisés GRM(q,d,n)
 - 18h30-19h
Christophe Chabot Tests statistiques et reconnaissance de codes

- Soir: banquet à 20h

Vendredi 20 octobre

- Matin
 - 9h-9h30:
Thomas Houtmann: Polynômes de classes et multiplication complexe en genre 2
 - 9h30-10h:
Laurent Imbert: The Double-Base Number System and its Application to Elliptic Curve Scalar Multiplication
 - 10h-10h30:
Nicolas Meloni: Chaines d'Additions Différentielles Appliquées à la Multiplication de Point sur les Courbe Elliptique
 - 10h30-11h: Pause
 - 11h-11h30:
Florent Bernard: Implémentation flexible de la multiplication modulaire de Montgomery
 - 11h30-12h
Nicolas Gama: Réduction symplectique de réseaux euclidiens

Repas: 12h15

Départ des participants: 13h30