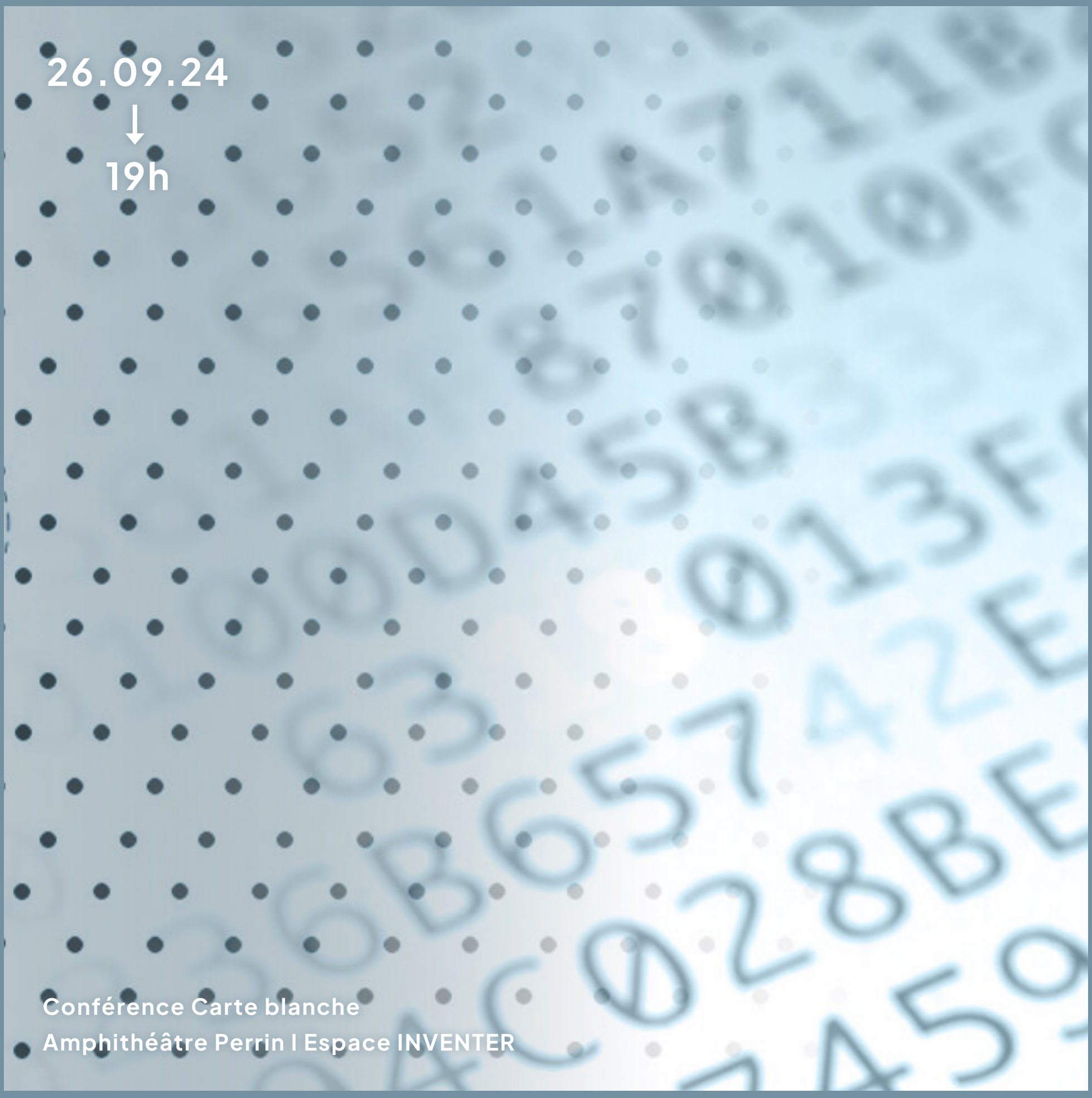
MAISON POINCARÉ

SÉCURISER LES DONNÉES FACE À DES ADVERSAIRES QUANTIQUES

Une grande partie des protocoles cryptographiques déployés pour sécuriser des données seront prochainement susceptibles d'être cassés par un ordinateur quantique puissant. Aussi, la cryptographie post-quantique se développe pour faire face à des adversaires disposant de ressources quantiques, et ce sans imposer aux utilisateurs et utilisatrices « honnêtes » de recourir à des technologies quantiques. Cette conférence propose un survol de ce domaine de recherche en pointant notamment l'utilisation des réseaux euclidiens.

Par Damien Stehlé, informaticien, directeur scientifique CryptoLab, professeur invité Télécom Paris, membre junior honoraire Institut Universitaire de France (IUF).



Institut Henri Poincaré | M
SORBONNE UNIVERSITÉ
cnrs