Génération d'aléa quantique, et intrication

ARNAULT François, arnault@unilim.fr
Tél : 0587506814
Tél : 0

Equipe : CRYPTIS, Limoges

Mots clés : Cryptographie, true random generation, quantum physics, quantum entanglement, Bell inequalities

Résumé de la thèse :

Le problème de la génération de nombres aléatoires de bonne qualité est central en cryptographie. La physique quantique ouvre des persectives très différentes de celles de la physique classique, avec la possibilité de génération d'aléa vrai. Cette thèse vise à étudier la génération d'aléa vrai (par exemple estimer la quantité d'aléa produit lors de processus de mesure, à l'aide des inégalités définies dans [Arn12]). Elle vise aussi à étudier l'intrication quantique multipartie est ses applications cryptographiques.

Random generation is of primary interest for cryptography. With quantum physics, true random generation can be obtained with measurements. The aim of this thesis is to study true random generation, and for example quantifying improvements in the generation rate when using homogeneous Bell inequalities. The work will consider also multipartite quantum entanglement and cryptographic applications.

Objectifs :

Améliorer et quantifier la quantité d'aléa vrai produit lors de processus de mesure quantique.

Description complète du sujet de thèse :

La production de nombres aléatoires de bonne qualité est un problème central en cryptographie. Alors que le déterminisme de la physique classique ne permet que la production de nombres apparemment aléatoires, la physique quantique ouvre grand la porte à la production d'aléa vrai. Le sujet de cette thèse est l'étude théorique des possibilités offertes par la physique quantique

Dans [PAM+] l'inégalité de Bell CHSH est utilisée pour analyser un processus générant de l'aléa vrai à partir de mesures quantiques. On y montre une borne inférieure de l'entropie obtenue lors de ce processus, assurant la qualité de l'aléa généré.

L'un des objectifs de la thèse est de déterminer une borne similaire utilisant les inégalités homogènes décrites dans [Arn12]. Ces inégalités, étant sujettes à des violations quantiques plus grandes que CHSH, en particulier en dimension 3, devraient permettre d'obtenir de meilleures bornes. Cela montrerait la faisabilité de la génération d'aléa vrai à un taux plus élevé que celui démontré dans [PAM+]. D'autres aspects de la génération d'aléa quantique seront ensuite étudiés.

Le travail pourrait se poursuivre par une étude de l'intrication quantique multi-partie, et à ses applications cryptographiques, par exemple, la génération de clés aléatoires partagées, dont la sécurité est garantie par des lois physiques. L'intrication est un manifestation essentielle de la mécanique quantique, qui prévoit l'existence d'objets dont les propriétés sont fortement corrélées, bien qu'étant séparés dans l'espace. Dans le cas de deux particules, on sait parfaitement définir et caractériser l'intrication. Lorsque plus de deux parties sont concernées, on ne connait pas encore de mesure satisfaisante de l'intrication. L'enjeu est important pour les applications potentielles en cryptographie ou en calcul quantique, mais aussi d'un point de vue fondamental.

Le candidat devra avoir une formation solide en mathématiques discrètes. Des connaissances préalables en physique ne sont pas nécessaires.

Bibliographie

[PAM+] S. Pironio, A. Acin, S. Massar et al. Random Numbers certified by Bell's theorem. Nature 464,
1021, 2010.

[Arn12] F. Arnault. A complete set of multidimensional Bell inequalities. J. of Ph. A : Math. Theor. 45, 255304, 2012.

[TDALP] M.C. Tran, B. Dakic, F. Arnault, W. Laskowski, T. Paterek. Quantum entanglement from
random measurements. PRA 92 050330(R), 2015.

Compétences à l'issue de la thèse :

Cryptographie quantique. Recherche fondamentale et appliquée.

Présentation de l'équipe d'accueil :

Equipe Cryptis (Cryptographie et Sécurité de l'Information). Un axe scientifique émergent de cette équipe est sur la "cryptographie quantique". La première thèse sur ce thème à Limoges sera soutenue fin 2016.

Financement : Lot1: Sujet financé sur crédits institutionnels (sujets fléchés)

Spécialité de Doctorat : Mathématiques et leurs Interactions

Domaine de compétences principal: Mathématiques

Domaine de compétences secondaire: Sciences pour l'Ingénieur

Candidat :
Compétences souhaitées : Master Mathématiques ou Cryptographie.

Conditions restrictives de candidature : Aucune

Date Limite de candidature : 4 Juin 2016 - 18h