Affronter et exploiter la vague quantique en informatique : nouvelles définitions de la sécurité et constructions cryptographiques (Document en Français)

Accès au(x) document(s)

Modalités de diffusion de la thèse :

- **Thèse soumise à l'embargo de l'auteur : embargo illimité (communication intranet).**

Informations sur les contributeurs

Auteur : Vu Quoc-Huy
Date de soutenance : 01-02-2023

Directeur(s) de thèse : Chevalier Céline

Etablissement de soutenance : Université Paris-Panthéon-Assas
Ecole doctorale : École doctorale des sciences économiques et gestion, sciences de l'information et de la communication (Paris)

Informations générales

Discipline : Informatique
Classification : Informatique

Mots-clés libres : Cryptographie quantique, Modèles de sécurité, Chiffrement, Preuves à divulgation nulle de connaissance, Cryptographie non clonable
Mots-clés :

- Cryptographie
- Cryptographie quantique
- Chiffrement (informatique)
- Preuves à divulgation nulle de connaissance

Résumé : La cryptographie moderne a un ennemi de taille à l'horizon : la montée inévitable des ordinateurs quantiques. Cependant, cette même puissance de calcul permettrait également de trouver des solutions sur des tâches cryptographiques qui sont tout simplement impossibles à réaliser avec la technologie actuelle. Dans cette thèse, nous mettons les pieds dans un univers où le quantique est omniprésent en y présentant notamment deux principales contributions. Nous mettons en avant à la fois des nouveaux modèles et de nouvelles analyses de sécurité pour deux primitives cryptographiques : les chiffrements et les preuves à divulgation nulle de connaissance non interactives. Les définitions usuelles de sécurité de ces primitives requièrent intrinsèquement la capacité d'enregistrer et de comparer des chaînes classiques. Cependant, les tâches d'enregistrement et de comparaison sont extrêmement difficiles dans le monde quantique en raison du principe d'incertitude. Nous proposons deux alternatives afin de surmonter cette barrière. De plus, nos notions de sécurité sont les premières à prendre pleinement en compte les attaques quantiques dans lesquelles les attaquants peuvent interagir avec les utilisateurs finaux sur des canaux quantiques. D'autre part, nous montrons que la disponibilité des ordinateurs quantiques se révèle être également à l'avantage des cryptographes, même lorsque les utilisateurs finaux n'utilisent que des communications classiques. En particulier, nous présentons un protocole interactif entre une Alice classique et un Bob quantique. Ce dispositif permet à Alice d'envoyer un état quantique caché non clonable à Bob par des canaux classiques. En outre, cet état quantique non clonable établit une forte propriété dite de monogamie de l'intrication, qui décrit les limites de la force des corrélations multipartites quantiques. Enfin, nous appliquons notre protocole et nous donnons les premiers schémas semi-quantiques de protection contre la copie.

Informations techniques

Type de contenu : Text
Format : PDF

Informations complémentaires

Entrepôt d'origine : star
Identifiant : 2023ASSA0017
Type de ressource : Thèse