ÉLÉMENT DE PORTFOLIO 02

Publication

1 DÉFINITION DE CET ÉLÉMENT

Titre de l'élément : Oblivious Transfer is in MiniQCrypt

URL de l'élément : `http://hal.science/hal-03033900`

Fichier de élément : Fichier pdf, `Eurocrypt 21 - Oblivious Transfer is in MiniQCrypt.pdf`

2 MOTIVATIONS DU CHOIX DE CET ÉLÉMENT

Ce travail [2], accepté à Eurocrypt 2021 et présenté en séance plénière à QIP 2021, —la conférence la plus importante en information quantique théorique— a eu un fort impact en cryptographie quantique, démontrant une différence importante entre les mondes classiques et quantiques. Il est représentatif de travaux effectués dans l'équipe qui étudient utilisent des méthodes rigoureuses issues de l'informatique classique pour étudier des problématiques cryptographiques dans le monde quantique— on pourrait citer, entre autres, [3–5] comme autres exemples, mais utilisant des techniques très différentes.

Ce travail est au cœur de la collaboration entre Alex Bredariol Grilo (QI) et Damien Vergnaud (ALMASTY), très active autour de la thèse de Samuel Bouaziz--Ermann et du postdoc de Quoc Huy Vu.

3 PRÉSENTATION DE CET ÉLÉMENT

Depuis le travail fondateur de Bennet et Brassard en 1984 [1], qui démontre un protocole quantique d'échange de clé avec une sécurité parfaite, une question importante dans le domaine de la cryptographie quantique consiste à trouver des primitives qui peuvent être implémentées quantiquement sous des hypothèses calculatoires plus faibles que les protocoles classiques. En particulier, Crépeau et Kilian [6] ont proposé un protocole pour le transfert inconscient et ils ont suggéré que sa sécurité pouvait être prouvée à partir de l'hypothèse minimale de la cryptographie classique : l'existence d'une fonction à sens unique, aussi appelée *MiniCrypt*. Cette primitive est universelle pour le calcul distribué sécurisé ; elle est donc fondamentale en cryptographie théorique.

La construction des protocoles de transfert inconscient à partir de l'existence des fonctions de sens unique est restée ouverte pendant plus de vingt ans, toutes les preuves de sécurité du protocole original nécessitaient des hypothèses plus fortes —qui impliquent déjà elle-même l'existence de protocoles classiques de transfert inconscient. Cet article a finalement résolu cette question ouverte, en utilisant des techniques de cryptographie classique pour soulever la sécurité du protocole.

4 RÉFÉRENCES BIBLIOGRAPHIQUES

[1] Charles H Bennett and Gilles Brassard. Quantum cryptography : Public key distribution and coin tossing. *arXiv preprint arXiv :2003.06557*, 2020.

[2] Alex Bredariol Grilo, Huijia Lin, Fang Song, and Vinod Vaikuntanathan. Oblivious Transfer is in MiniQCrypt. In *Advances in Cryptology - EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, volume 12697 of *Lecture Notes in Computer Science*, pages 531–561, Zagreb, Croatia, October 2021. Springer.

[3] Federico Centrone, Niraj Kumar, Eleni Diamanti, and Iordanis Kerenidis. Experimental demonstration of quantum advantage for NP verification with limited information. *Nature Communications*, 12(1) :850, February 2021.

[4] Ulysse Chabaud, Tom Douce, Frédéric Grosshans, Elham Kashefi, and Damian Markham. Building trust for continuous variable quantum states. In Steven T. Flammia, editor, *15th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2020)*, volume 158 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 3 :1–3 :15, Riga, Latvia, June 2020. Schloss Dagstuhl–Leibniz-Zentrum für Informatik.

[5] Alexandru Cojocaru, Léo Colisson, Elham Kashefi, and Petros Wallden. QFactory : classically-instructed remote secret qubits preparation. In *ASIACRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security*, volume 11921 of *Lecture Notes in Computer Science*, pages 615–645, Kobe, Japan, December 2019. Springer. 51 pages, 4 figures.

[6] C. Crepeau and J. Kilian. Achieving oblivious transfer using weakened security assumptions. In *[Proceedings 1988] 29th Annual Symposium on Foundations of Computer Science*, pages 42–52, 1988.