33920 MEZUREUX Stanislas

Combinatoire et chiffrement : le père Noël secret et ses applications

Célèbre tradition, le Père Noël secret est en apparence un simple tirage au sort pouvant être effectué numériquement. Pourtant, en se penchant sur le sujet, nous avons découvert plusieurs notions de chiffrement et de combinatoire que nous nous proposons d'étudier.
Ainsi, cette tradition de Noël nous a permis d'aborder les thématiques de l'aléatoire et de la prévention contre la triche. Le sujet s'inscrit donc bien dans le thème de l'année.

Ce TIPE fait l'objet d'un travail de groupe.

Liste des membres du groupe :

- *ESPINOSA Alice*

Positionnement thématique (ETAPE 1)

MATHEMATIQUES (Algèbre), INFORMATIQUE (Informatique pratique), INFORMATIQUE (Informatique Théorique).

Mots-clés (ETAPE 1)

Mots-Clés (en français)	**Mots-Clés** (en anglais)
Preuve à divulgation nulle de connaissance	*Zero-knowledge proof*
Répartiton aléatoire	*Random distribution*
Chiffrement homomorphe	*Homomorphic encryption*
Combinatoire	*Combinatorics*
Dénombrement	*Enumeration*

Bibliographie commentée

Le numérique ne cessant de prendre de l'ampleur, la prévention contre la triche se doit d'évoluer par la même occasion. En particulier, les canaux de transmissions sécurisés et l'étude de l'aléa sont des éléments de réponses à des problèmes concrets tels que le vote électronique. L'organisation d'un Secret Santa ou père Noël secret en français en est une autre application relativement simple. En effet, dans cette tradition chaque participant tire au hasard un autre participant à qui il devra faire un cadeau. Elle met donc en jeu les différents aspects de cette transmission, du tirage jusqu'à l'envoi des mails en passant par le chiffrement complet des données **[1]**.

L'étude d'un tirage du Père Noël Secret demande la prise en compte de plusieurs aspects : l'existence, l'intérêt, la sécurité et la fiabilité de ce tirage **[2]**. Cette étude peut se complexifier avec l'ajout de conditions, par exemple si on souhaite que des personnes qui vivent sous un même toit ne puissent pas se faire de cadeaux entre elles.

Un premier point important est de réussir à allier confidentialité et sécurité. Il faut alors trouver une méthode pour prouver que le tirage a été effectué correctement sans avoir besoin de le dévoiler. Pour cela, nous avons utilisé une "preuve à divulgation nulle de connaissance", qui est un processus consistant à prouver la véracité d'une information sans connaître cette information **[3]**. Il peut se baser sur plusieurs principes, notamment sur le chiffrement homomorphe, qui est un cryptosystème permettant de faire des opérations sur des données chiffrées. De plus, nous profiterons de l'utilisation du chiffrement homomorphe pour pouvoir sécuriser les données des participants et stocker le tirage dans un fichier annexe dans l'optique d'être en capacité de renvoyer le tirage par mail. Le système utilisé ici est celui du cryptographe égyptien Taher ElGamal **[4]**.

Un second point sur lequel nous nous sommes concentrés est la prise en compte de différentes contraintes. Nous les avons modélisés avec des groupes, les membres d'un groupe ne pouvant pas se tirer entre eux. Le nombre de tirages possibles dépend du nombre de groupes mais aussi du nombre de participants dans chaque groupe. L'aspect combinatoire nous a donc permis de définir l'existence ainsi que la rentabilité d'un tirage. Lorsqu'il y a trop peu de participants, le nombre de combinaisons possibles est trop faible pour que le tirage garde son intérêt. Nous avons commencé par étudier le cas de n groupes, en utilisant la formule du crible de Poincaré, puis nous avons essayé de généraliser aux cas où nous avions entre 2 et n-1 groupes **[5][6]**.

Problématique retenue

Il s'agit d'implanter en Python le tirage au sort d'un père Nöel secret afin de mettre en avant les différentes technologies de prévention contre la triche et d'en étudier l'efficacité.

Objectifs du TIPE

1. Implantation en Python de l'algorithme effectuant le tirage
2. Etude de la sécurité des données lors de l'envoi de ces dernières
3. Preuve à divulgation nulle de connaissance

Références bibliographiques (ETAPE 1)

[1] Sjouke Mauw, Sasa Radomirovic, Peter Ryan : Security protocols for Secret Santa : *Cambridge International Workshop on Security Protocols (2014)*

[2] Evgeniy Prikhodko : Théorie des graphes : *https ://binary-machinery.github.io/2021/02/03/secret-santa-graph.html*

[3] Cécile GONÇALVES : Cryptographie Avancée : *Identification Zéro-Knowledge, Cryptographie distribuée et Chiffrement homomorphe (2015)*

[4] Wikipédia : Cryptosystème d'ElGamal : *https://fr.wikipedia.org/wiki/Cryptosystème_de_ElGamal*

[5] Marc SAGE : Combinatoire : *7-9 (2008)*

[6] Fatima A. Akinola : On Hamilton cycle decompositions of complete multipartite graphs which are both cyclic and symmetric (2021)

DOT

[1] *Octobre : étude dans le cas le plus simple i.e. un seul groupe puis ébauche du processus de création des paires dans le cas général*

[2] *Décembre : choix et implantation du cryptosystème une fois le cas général implanté en Python*

[3] *Janvier : décision de fournir une preuve à divulgation nulle de connaissance après la lecture de la référence [3] et de changer de cryptosystème pour des raisons de performances*

[4] *Février : synthèse des preuves et des explications pour faciliter la présentation puis travail de dénombrement/combinatoire pour quantifier le nombre de tirages pour un groupe et deux groupes à l'aide de l'ouvrage [5]*

[5] *Mars : tentative d'approche du problème par la théorie des graphes infructueuse*

[6] *Avril : conjecture du nombre de tirages dans le cas général à l'aide d'un algorithme*

[7] *Juin : correction de la preuve à divulgation nulle de connaissance*