Combinatoire et chiffrement : le père noel secret et ses applications

Pour notre TIPE nous sommes partis d'un problème concret de répartition aléatoire. De plus, les différentes notions d'informatique et de mathématiques mises en jeu nous ont semblé justifier la pertinence de ce sujet ainsi que du travail de groupe.
ancrage au thème de l'année

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

Liste des membres du groupe :

— *Alice ESPINOSA*
— *Stanislas MEZUREUX*

Positionnement thématique

MATHÉMATIQUES (Algèbre), INFORMATIQUE (Informatique pratique), INFORMATIQUE (Informatique théorique)

Mots-clés

Mots-Clés (en français)	**Mots-Clés** (en anglais)
Faille zero-knowledge	*Zero-knowledge proof*
Répartiton aléatoire	*Random distribution*
Chiffrement homomorphe	*Homomorphic encryption*
Combinatoire	*Combinatorics*
Dénombrement	*Enumeration*

Bibliographie commentée

De nombreux domaines tels que la santé conduisent à devoir créer un réseau de transmission aléatoire et sécurisé entre différentes personnes. L'organisation d'un Secret Santa ou père Noël secret en français en est une application relativement simple à comprendre. 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 additif, qui est un cryptosystème permettant de faire des opérations sur des données chiffrées. De plus, on profitera 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 de Cray Gentry qui est totalement homomorphe **[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. Pour compter le nombre de tirages existants lorsque l'on s'intéresse à un tirage avec un seul groupe de n personnes, on cherche le cardinal de l'ensemble des permutations sans point fixe de l'ensemble fini $[\![1, n]\!]$, ce que l'on appelle des dérangements. La démonstration se base sur la formule du crible de Poincaré **[5]**.

Problématique retenue

Il s'agit d'implémenter en Python le tirage au sort d'un père Nöel secret qui sera envoyé par mail et qui respecte les conditions sur les groupes, le tout de manière sécurisée. L'algorithme devra également être capable de dire si le tirage est réalisable ou non, ce qui implique une seconde partie plus théorique axée sur les mathématiques.

Objectifs du TIPE du candidat

1. Condition sur l'existence du tirage
2. Dénombrement du nombre de tirages possibles selon le nombre de groupes et la taille des groupes

Objectifs du TIPE du second membre du groupe

1. Implémentation en Python de l'algorithme effectuant le tirage
2. Étude de la sécurité des données lors de l'envoi de ces dernières
3. Étude du problème sous forme de graphe

Références bibliographiques

[1] Sjouke Mauw, Sasa Radomirovic, and 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] Craig Gentry, *Computing Arbitrary Functions of Encrypted Data, Communications of the ACM, Volume 53 (2010)*

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