Life as a PhD student

Caroline Sandsbråten

NTNU | Norwegian University of Science and Technology

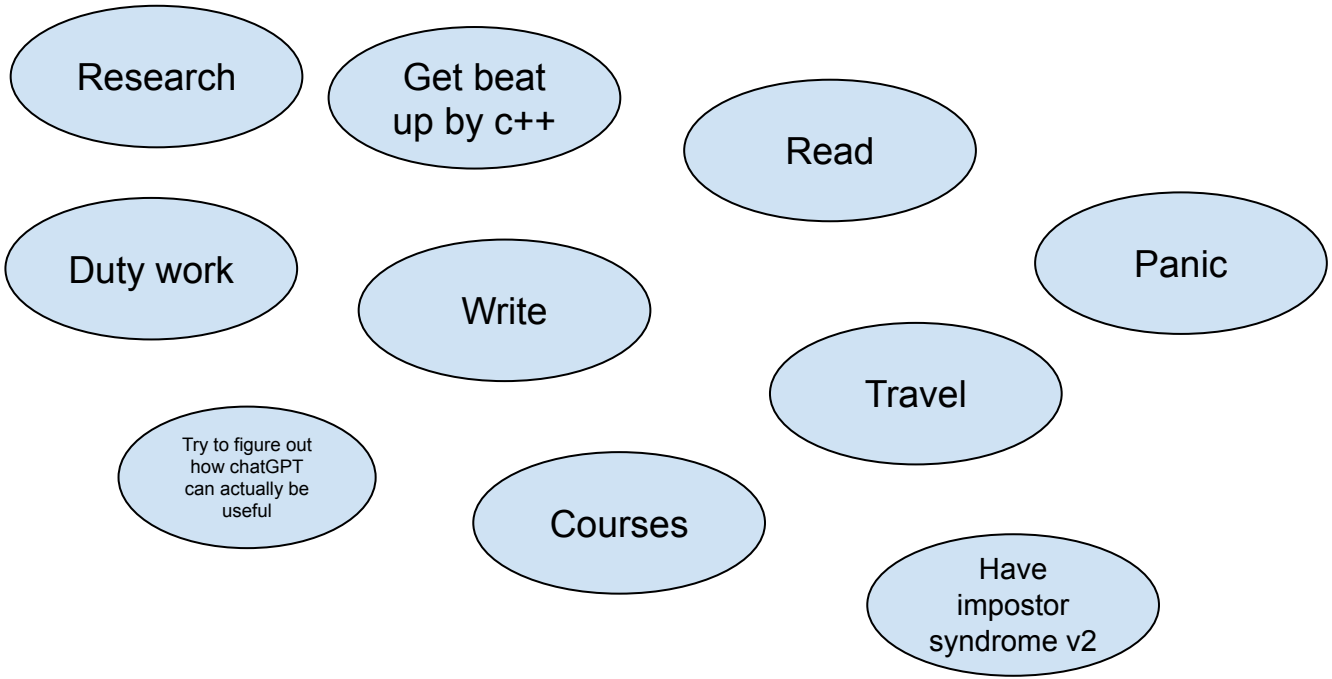
Who am I?

- Started with physics
- Almost finished Informatics Bsc.
- Started and finished KomTek (2022)
- Research in lattice-based post-quantum crypto
- Just started my second year

Caroline Sandsbråten
Stipendiat
Institutt for informasjonssikkerhet og kommunikasjonsteknologi

caroline.sandsbraten@ntnu.no
94812815
Elektro B, B211, Gløshaugen

What do I do?


Research
Get beat up by c++
Read
Duty work
Write
Panic
Travel
Try to figure out how chatGPT can actually be useful
Courses
Have impostor syndrome v2

Read

- There is so much to know
- Everyone else already knows everything???
- How do I even know what I should read?

Write

- It is incredibly difficult to be a good writer
- I take notes of everything all the time
- But it is a very important part of the job

What writing your first paper feels like

Duty work

- Actually kind of fun
- So far I have graded a bazillion TTM4100 exams and organising the TTM4137 lab this year
- I have also held a couple of lectures (scary)

ChatGPT

- What do you use it for?
- I use it to add comments to my code sometimes
- get a half bad grip on new things
- Tried to get it to write code for me, can not recommend that. :(
- Super efficient googling
- I love AskTheCode

Courses

- Have to take 30 sp
- Mandatory ethics
- If there are courses you wanted to take but didn’t have time for you can do those courses now!

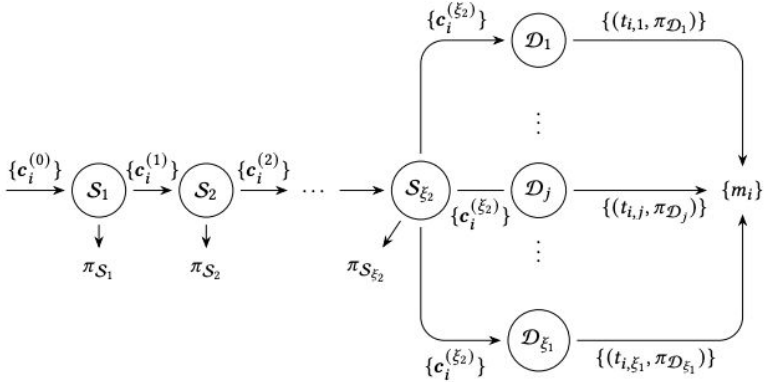
Get beat up by c++

```
** Tests for NTRU encryption:

[1]    1144795 segmentation fault (core dumped)  ./ntru
```

Research

- E-voting
- Secure
- Less potential to tamper with votes?
- Kinda hot topic?



Research

- Distributed Key Generation
- Why?
- Less need to trust anyone

Key Generation: $\mathsf{KeyGen}_{\mathsf{NTRU}}(\mathsf{sp})$.

1. For each user $P_i, i \in [1, \ldots, N]$:
   (a) Sample $g_i, f_i \leftarrow D_\sigma$ s.t. $f_i \equiv 1$ in R_p
   (b) Compute $h_i = g_i / f_i$, publish public key share h_i
   (c) Compute ZK PoK for $(g_i, f_i), i \in [1, \ldots, N]$?
2. Compute Key Shares $\hat{f}_i, i \in [1, \ldots, N]$ s.t. $\sum_{i=1}^{N} \hat{f}_i = \prod_{i=1}^{N} f_i$

Encryption: $\mathsf{Enc}_{\mathsf{NTRU}}(m, pk)$. Given message $m \in R_p$ and public key $pk = h$:

1. Sample encryption randomness $s, e \leftarrow S_v$
2. Return ciphertext $c = p \cdot (hs + e) + m \in R_q$

Decryption: $\mathsf{DistDec}_{\mathsf{NTRU}}(c, sk_{share})$. Given ciphertext c and secret key $sk_{share} = \hat{f}_i$:

1. Compute message share $c_i' = \hat{f}_i \cdot c \mod q$.
2. Return the message share $c_i = c_i' \mod p$.

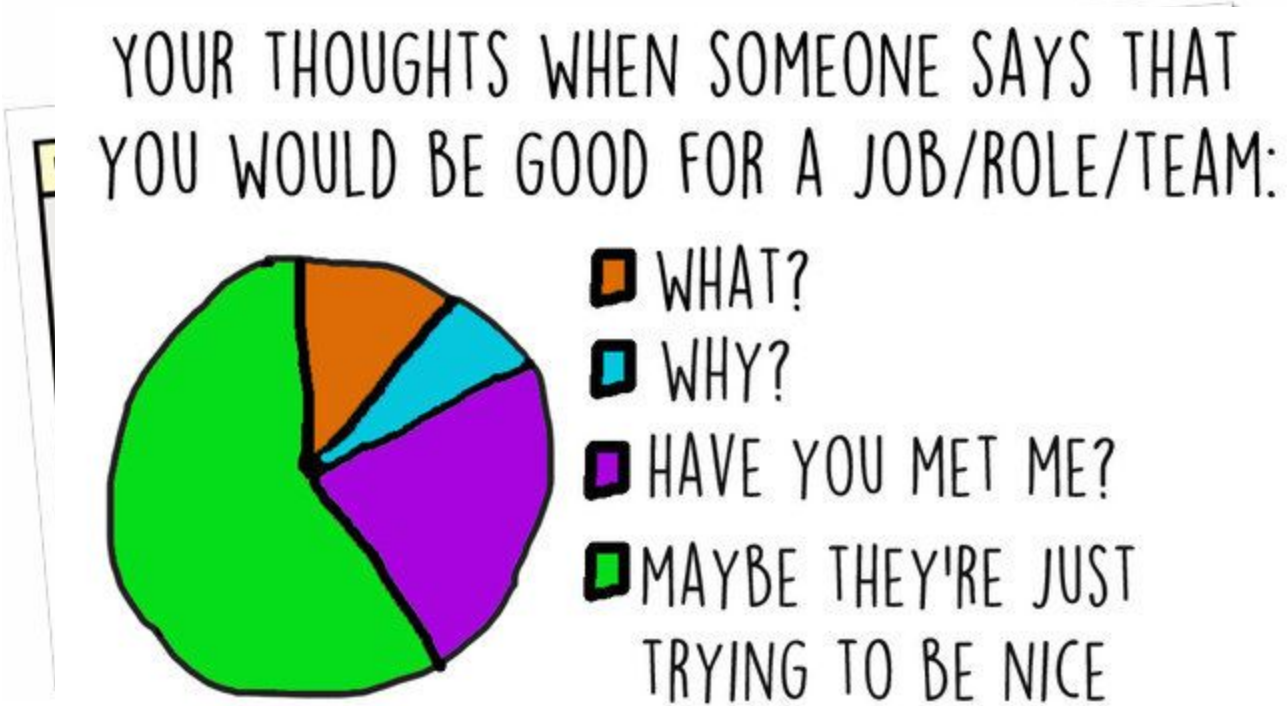
Combine: $\mathsf{Comb}_{\mathsf{NTRU}}(c_1, c_2, \ldots, c_N)$. Given all the message shares from $\mathsf{DistDec}_{\mathsf{NTRU}}$, $c_i, i \in [1, \ldots, N]$:

1. Compute $m = \sum_{i=1}^{N} c_i$.
2. Return the plaintext message m.

Panic

- There is a lot to do
- Most of it you have no clue how to do before you do it

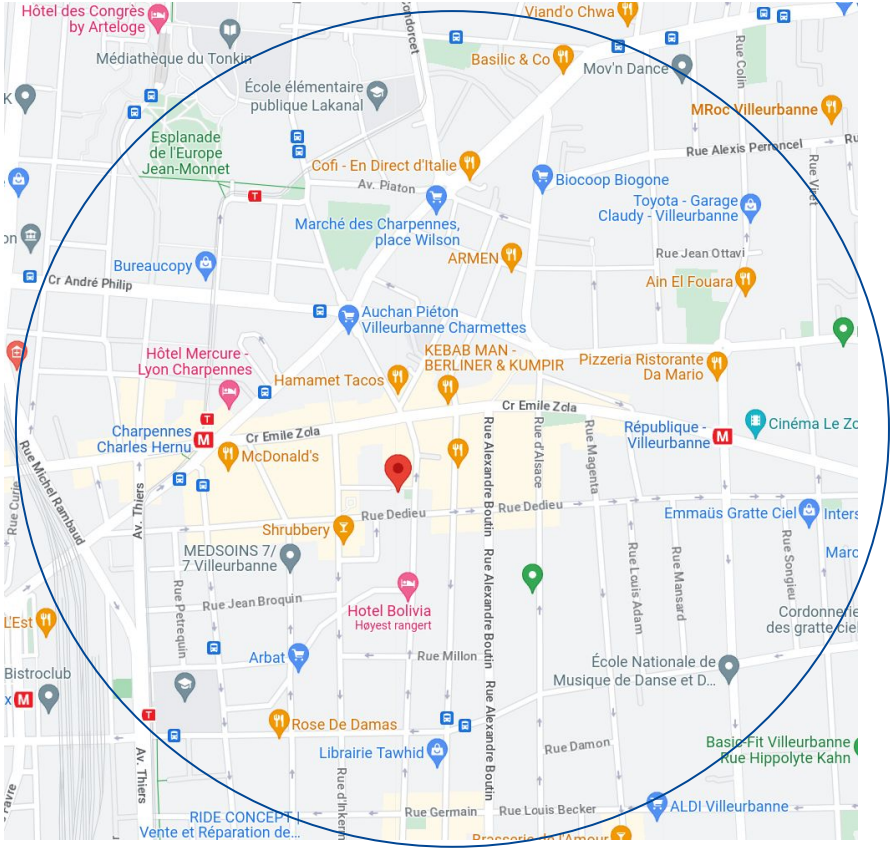
Impostor syndrome v2



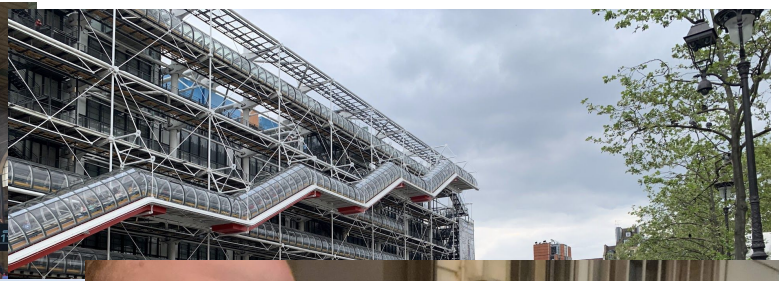
Travel

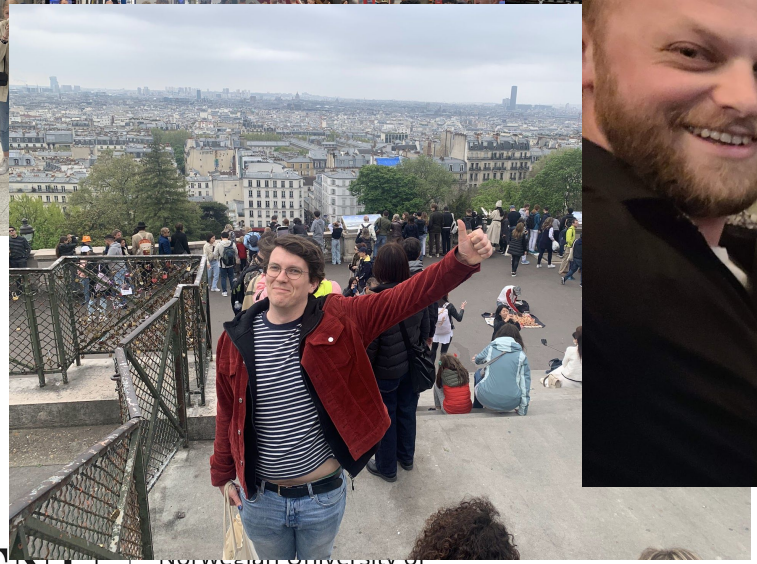
- At one point I felt like I was traveling too much
- Conferences
- Seminars
- Summer schools
- Winter schools

Lyon


Hôtel des Congrès by Arteloge
Médiathèque du Tonkin
École élémentaire publique Lakanal
Esplanade de l'Europe Jean-Monnet
Viand'o Chwa
Basilic & Co
Mov'n Dance
MRoc Villeurbanne
Rue Alexis Perroncel
Cofi - En Direct d'Italie
Av. Piaton
Biocoop Biogone
Toyota - Garage Claudy - Villeurbanne
Marché des Charpennes, place Wilson
ARMEN
Rue Jean Ottavi
Ain El Fouara
Bureaucopy
Cr André Philip
Auchan Piéton Villeurbanne Charmettes
Hôtel Mercure - Lyon Charpennes
KEBAB MAN - BERLINER & KUMPIR
Pizzeria Ristorante Da Mario
Hamamet Tacos
Cr Emile Zola
Charpennes Charles Hernu
McDonald's
Rue Michel Ranvaud
Av. Thiers
Rue Alexandre Boutin
Rue d'Alsace
Rue Magenta
République - Villeurbanne
Cinéma Le Zo
Rue Dedieu
Shrubbery
Emmaüs Gratte Ciel
MEDSOINS 7/ 7 Villeurbanne
Rue Petrequin
Rue Jean Broquin
Hotel Bolivia
Høyest rangert
Rue Louis Adam
Rue Mansard
Rue Songieu
Cordonnerie des gratte ciel
L'Est
Arbat
Rue Millon
Bistroclub
École Nationale de Musique de Danse et D...
Rose De Damas
Librairie Tawhid
Rue Damon
Basic-Fit Villeurbanne Rue Hippolyte Kahn
Rue d'Ikerrin
Rue Germain
Rue Louis Becker
ALDI Villeurbanne
RIDE CONCEPT | Vente et Réparation de...

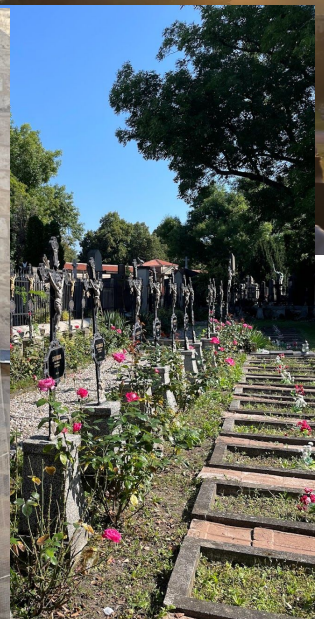
Paris






swix

Prague



Are you thinking about a PhD?

- It is mostly very fun
- You spend so much time digging deep into topics you would not have time for if you had a normal grown-up-people-job
- Worst that can happen is you give up or fail, so why not try?
- You meet a lot of awesome people
- And other valuable life skills


QUESTIONS