5269 Bourbonnière
Montréal, H1X 2N1, QC
☎ (514)907-2290
✉ sim.desaulniers@gmail.com
https://sim590.github.io
simon-désaulniers-86648097
sim590

Simon Désaulniers

Education

2019 **Ph. D. in Computer Science (Quantum Cryptography)**, *Université de Montréal.*
Analysis of computation hypothesis resisting quantum computer for elaborating modern and secure cryptographic methods.
N.B: *Was not completed in favor of pursuing a profesional career.*

2016 – 2018 **Master's degree in Computer Science**, *Université du Québec à Montréal (UQÀM).*
Advanced operations over distributed hash tables and end-to-end secure group chat.
See master thesis.

2010 – 2015 **Bachelor's degree in Computer Science**, *Université du Québec à Trois-Rivières (UQTR).*

Bachelor's degree in Mathematics, *Université du Québec à Trois-Rivières.*

Professional experience

May 2015 up to August 2017 **Computer science researcher and programmer analyst**, *Savoir-faire Linux.*
GNU/Ring development (https://jami.net), an audio/video and chat communication software. Design and implementation of multiple solutions:

- distributed indexation over a distributed hash table (DHT);
- group chat communication protocol over a DHT;
- data pagination and persistence feature on OpenDHT;
- OpenDHT development and maintenance in general.

https://github.com/savoirfairelinux/opendht

Summer 2012 up to April 2015, August 2017 up to April 2019 **Mathmematics and Computer Science research assistant**, *UQÀM, UQTR.*
Supervised by Alexandre Blondin Massé Ph. D. and Alain Goupil Ph. D. and Sébastien Gambs Ph. D..

- Contribution to the elaboration of an end-to-end secure group chat protocol resisting cipher correlations in asynchronous context while keeping a light network load;
- Design and implementation of polyominoes enumeration tools in order contribute to combinatorics research team's work;
- Marking of undergrads' homework and magisterial demonstrations in laboratories.

https://bitbucket.org/ablondin/polyenum

Summer 2011 **Trainee in Software engineering**, *Johnston-Vermette Groupe Conseil, inc.*, Trois-Rivières.
Non-regression test scripts on Hydro-Québec Gentilly-2 nuclear plant computer systems.

Publications

2017 **Fully Distributed Indexing over a Distributed Hash Table.**
Simon Désaulniers et al. "Fully Distributed Indexing over a Distributed Hash Table". In: Ubiquitous Networking. Ed. by Essaid Sabir et al. Cham: Springer International Publishing, 2017, pp. 308–318. isbn: 978-3-319- 68179-5.

General abilities

Langues French, Esperanto, English.

Personal attributes	Analytical skills; initiative; organised and rational; good communication skills; work well alone or as part of a team; flexible; can easily adapt to new situations.

Conferences and collaborative programs

QCrypt 2019	(Montréal) Conference on Quantum Cryptography and Post-Quantum Cryptography.
GoSec 2018	(Montréal) GoSec is an annual convention which brings together several experts in the IT security field, from both the private and public sector.
UNet 2017	(Casa Blanca, Maroc) Third Symposium on Ubiquitous Networking. Presentation of a scientific paper.
GSoC 2016	(Montréal) Participating in Google Summer of Code for the Debian project. Contribution to efforts aiming at the design of a solution to divers DHT optimizations for the OpenDHT project.
Debconf 2016	(Cape Town, South Africa) Annual conference of the Debian project. Presenting GNU/Jami (anciennement GNU/Ring). 🔗 See the video recording.

Personnal projects and relevant contributions

Debian, Archlinux	Writing and maintenance of packages in addition to various contributions to documentation and bug tracking.
🔗 dpaste	Pastebin over a DHT. Support for encryption through a public key encryption scheme (PGP) or a secret key encryption scheme.
🔗 qurlshare	Qutebrowser extension for URL sharing between multiple machines over a DHT.
🔗 amh	AwesomeWM window manager extension for launching programs simultaneously on multiple computers.
🔗 yauml	YAML formatted UML diagram translation to Graphviz compatible input file, notably enabling generation of PDF files.
🔗 splitbmf	Audio/video file splitting tool.

Particular knowledge

Concepts	Cryptography, security analysis, end-to-end encryption, communication protocol, algorithm optimization, distributed hash tables, blockchain, byzantine generals problem, free software.
Computer languages	C/C++, Python, Haskell, Java, C#, Lua, Bash, LaTeX, Vimscript, BRE, ERE, PCRE, HTML, CSS, PHP/SQL, Javascript.
Operating systems	GNU/Linux (Debian, Ubuntu, Archlinux), Android.
Software and tools	Vim, Git, GCC, GNU Make, GNU Gdb, GNU Autotools, CMake, Setuptools (Python), GNU shell. Docker, Cabal (Haskell),

Hobbies

Cultural	Language learning, book reading.
Sports	Riding a bike, physical training, alpine skiing.
Artistic	Music, guitar playing.
Divers interests	Chess, board games, television series, movies, various documentaries.