

Simon Désaulniers

✉ sim.desaulniers@gmail.com
🌐 <https://sim590.github.io>
in [simon-désaulniers-86648097](https://www.linkedin.com/in/simon-désaulniers-86648097)
🔗 [sim590](https://github.com/sim590)

Formation

- 2019 **Doctorat informatique (cryptographie quantique)**, *Université de Montréal*
Analyse d'hypothèses de calcul résistantes à l'ordinateur quantique pour l'élaboration de méthodes cryptographiques modernes sûres.
N.B : *Non complété en faveur d'une continuité au professionnel.*
- 2016 – 2018 **Maîtrise en informatique**, *Université du Québec à Montréal (UQÀM)*
Opérations non rudimentaires de tables de hachage distribuées et clavardage en groupe sûr de bout en bout. [🔗 Voir le mémoire.](#)
- 2010 – 2015 **Baccalauréat en informatique**, *Université du Québec à Trois-Rivières (UQTR)*
Baccalauréat en mathématiques, *Université du Québec à Trois-Rivières*

Expériences professionnelles

- Juin 2020
à Aujourd'hui **Développeur sénior**, *Solutions Mieux-Être Lifeworks* :
Rédaction d'analyses, développement, entretien d'un logiciel complexe de gestion de régime de rente à prestation déterminée.
- Responsable de migration du système de gestion de version centralisé TFS au système de gestion de version distribué Git (optimisations majeures de l'espace, restructuration du projet) ;
 - Prise en charge des préoccupations DevOps et formation de différentes équipes sur les nouveaux outils ;
 - Mise en place d'un système et de pratiques de gestion de dépendance de projet basés sur le gestionnaire de paquet Nuget ;
 - Modernisation des approches de développement (programmation offensive, tests statiques, méthodes de débogage et de développement diverses, documentation exhaustive).
- Mai 2015
à août 2017 **Chercheur et concepteur logiciel**, *Savoir-faire Linux*
Contribution au projet GNU/Jami ([🔗 https://jami.net](https://jami.net)), un logiciel de communication audio/vidéo et clavardage. Conception et implémentation de différentes solutions :
- Indexation distribuée sur une table de hachage distribuée (THD).
 - Protocole de clavardage en groupe sur une THD.
 - Optimisations d'accessibilité des données de la THD OpenDHT (pagination et persistance de valeurs).
 - Développement et entretien d'OpenDHT en général.
-
- [🔗 https://github.com/savoirfairelinux/opensdht](https://github.com/savoirfairelinux/opensdht)
- Été 2012
à avril 2015, **Auxiliaire de recherche en mathématiques (informatique)**, *UQÀM, UQTR*
Supervisé par et Alexandre Blondin Massé Ph. D., Alain Goupil Ph. D. et Sébastien Gams Ph. D.
- Août 2017
à avril 2019 **Chercheur en cryptographie**, *Université de Montréal*
Contribution à un protocole de clavardage sûr de bout en bout résistant aux corrélations de cryptogrammes ;
- Élaboration d'outil d'énumération de polyominos pour épauler la recherche combinatoire ;
 - Correction de travaux pratiques et démonstrations magistrales en laboratoire pour les bacheliers.
-
- [🔗 https://bitbucket.org/ablondin/polyenum](https://bitbucket.org/ablondin/polyenum)
- Été 2011 **Stagiaire en informatique**, *Johnston-Vermette Groupe Conseil, inc.*, Trois-Rivières
Exécution, rédaction, analyse et correction de scripts de test de non-régression sur les systèmes informatiques à la centrale nucléaire Gentilly-2.

Publications

- 2017 *Fully Distributed Indexing over a Distributed Hash Table*
Simon Désaulniers et collab. « Fully Distributed Indexing over a Distributed Hash Table ». Dans : Ubiquitous Networking. Sous la dir. d'Essaid Sabir et collab. Cham : Springer International Publishing, 2017, p. 308-318. ISBN : 978-3-319-68179-5.

Habiletés générales

- Langues Français, Esperanto, Anglais.
Qualités Sens de l'analyse ; initiative ; organisé et responsable ; bonnes habiletés de communication ; travail seul ou en équipe ; flexible ; s'adapte facilement à de nouvelles situations.

Conférences et programmes collaboratifs

- QCrypt 2019 (Montréal) Conférence réunissant les différents spécialistes en cryptographie quantique et post-quantique.
GoSec 2018 (Montréal) Événement annuel qui rassemble plusieurs experts du domaine de la sécurité des TI provenant de différents secteurs.
UNet 2017 (Casa Blanca, Maroc) « Third Symposium on Ubiquitous Networking. » Présentation d'article scientifique.
GSoC 2016 (Montréal) Participation au programme *Google summer of code* pour le projet Debian. Contribution à l'élaboration d'une solution de persistance de données et optimisations diverses pour OpenDHT.
Debconf 2016 (Le Cap, Afrique du sud) Conférence annuelle du projet Debian. Présentation du logiciel GNU/Jami (anciennement GNU/Ring). [Voir la vidéo.](#)

Projets d'initiative personnelle et contributions pertinentes

- Debian, Archlinux Écriture et entretien de paquets, contributions à la documentation.
[dpaste](#) Presse-papier sur THD muni d'une couche de sécurité au moyen d'un chiffre à clef publique (PGP) et d'un chiffre à clef secrète (AES).
[qurlshare](#) Extension du navigateur Qutebrowser pour partage d'URL entre plusieurs machines sur THD.
[amh](#) Extension du gestionnaire de fenêtres AwesomeWM pour le démarrage de programmes en simultané sur plusieurs ordinateurs.
[yauml](#) Traducteur de YAML pour génération de diagrammes de conception UML.
[splitbmf](#) Outil de scission de fichiers audio/vidéo à partir d'une liste donnée.

Connaissances particulières

- Concepts Cryptographie, analyse de sécurité, chiffrement bout-en-bout, protocole, optimisation d'algorithme, tables de hachage distribuées, chaînes de bloc (*blockchain* en ang.).
Langages C/C++, Python, Haskell, Java, C#, Lua, Bash, PowerShell, L^AT_EX, Vimscript, BRE, informatiques ERE, PCRE, HTML, CSS, PHP/SQL, Javascript.
Systèmes GNU/Linux (Debian, Ubuntu, Archlinux), Android.
Logiciels et outils Vim, Git (et les services connexes comme GitHub, GitLab, Bitbucket, Azure DevOps), GCC, GNU Make, GNU Gdb, GNU Autotools, CMake, Jenkins, Gerrit, Tuleap, Docker, Setuptools (Python), Cabal (Haskell), MSBuild, Visual Studio, Nuget, Interface système GNU.

Autres activités

Culturel	Apprentissage de langues
Sports	Vélo, entraînement physique, ski alpin.
Artistique	Musique, guitare.
Intérêts divers	Échecs, jeux vidéo, jeux de société, séries télévisées, films, documentaires variés.