



Ruben De Smet

Over mij

Een voorvechter van privacy sinds de middelbare school, met uitgebreide ervaring in toegepaste [cryptografie](#) en [privacy](#)-verbeterende technologieën in [Rust](#). Gepassioneerd over het ontwikkelen van gedecentraliseerde oplossingen die de privacy van de gebruiker beschermen. Deze passie weerspiegelt zich in projecten zoals [Whisperfish](#) en Glycos.

Opleiding

- 2018–2024 **Doctor of Philosophy**, *Vrije Universiteit Brussel*
Onderzoek naar zero-knowledge proofs als privacy-verbeterende technologie.
- 2016–2018 **Master of Science**, *Vrije Universiteit Brussel*
Ingenieurswetenschappen: Computerwetenschappen: Multimedia
- 2013–2017 **Bachelor of Science**, *Vrije Universiteit Brussel*
Ingenieurswetenschappen: Elektronica en Informatietechnologie, computerwetenschappen

Vaardigheden

Programmeren	■■■■■	Rust	■■■■■	C
	■■■■■	Python	■■■■■	Java
Talen	■■■■■	Nederlands	■■■■■	Engels
	■■■■■	Frans		

Ervaring

- 2024–nu **Postdoctoraal onderzoeker**, *Vrije Universiteit Brussel*, Brussel
- Onderzoeksprojecten in cryptografie en privacy engineering
 - Technologieprojecten betreffende Rust, cloud en IoT
- 2019–nu **Whisperfish**, *hoofdontwikkelaar*, Onofficiële Signal app voor Sailfish OS
- Herschreven in Rust, volledig achterwaarts compatibel
 - Grote delen van de Signal API geïmplementeerd

2018–2024 **Doctor of Philosophy**, *Vrije Universiteit Brussel*, Brussel

- Onderwijs in programmeren en elektronica
- Onderzoeksprojecten in cryptografie en privacy engineering

Opleiding

- 2018–2024 **Doctor of Philosophy**, *Vrije Universiteit Brussel*, Brussel, België, *Ingenieurswetenschappen: Doctoraat Electronics and Information Technology*
toegepaste cryptografie, informatieveiligheid, privacy, telecommunicatie.
- 2016–2018 **Master of Science**, *Vrije Universiteit Brussel*, Brussel, België, *Engineering Science: Computer Science: Multimedia*
computer vision, image en video technologie, digitale spraak en audio-verwerking, cryptografie en computer security.
- 2013–2017 **Bachelor of Science**, *Vrije Universiteit Brussel*, Brussel, België, *Engineering Science: Electronics and Information Technology, computer science*
electronica, computer netwerken and protocols, algoritmen, data structuren, computer en software architecturen
- 2006–2013 **ASO**, *Sint-Rita college*, Kontich, België, *Wetenschappen-Wiskunde*

Ervaring referenties op aanvraag

- 2024–now **Postdoctoraal onderzoeker**, *Vrije Universiteit Brussel*, Brussel, België
Ik ben betrokken bij meerdere onderzoeks- en technologieprojecten betreffende Rust, IoT, privacy en veiligheid. Mijn onderzoek houdt zich voornamelijk bezig met de ontwikkeling van praktische privacy-verbeterende technologieën. Voor details, zie de academische sectie op pagina 6.
- 2018–2024 **Assistent**, *Vrije Universiteit Brussel*, Brussel, België
Als assistent ben ik mede verantwoordelijk voor de cursus Informatica in de eerste bachelor en voor deel van de Elektronica cursus in de derde bachelor in de faculteit ingenieurswetenschappen. Ik nam ook deel in meerdere onderzoeks- en technologieprojecten, betreffende Rust en cloud technologieën. Zie de academische sectie op pagina 6.
- 2015–nu **Eigenaar bij De Smet Multimedia BV, Consulting**, Brussel / Antwerpen, België
Algemeen IT, implementatie en integratie.

Freelance

- 2016–nu **Bijles secundair onderwijs**
Langdurige bijles wiskunde en fysica in 5^{de} en 6^{de} jaar secundair onderwijs. Bijles C++ in de 1^{ste} Bachelor.

- 2015–2018 **Freelance Linux systeemadministratie**, *BruWind/Vrije Universiteit Brussel*, Brussel, België
Uitrollen, testen, administratie van een CentOS 7 gebaseerde cluster met Ansible. Monitoring van het systeem. Continuous integration, complexe continous deployment van Docker gebaseerde microservices.
- Jobstudent**
- juli 2015 **ETL implementatie**, *Vrije Universiteit Brussel*, Brussel, België
Bouwen van ETL software met Python 3 en SOS-Berlin JobScheduler. Grote hoeveelheden windturbinesensordata inladen in een PostgreSQL 9.4 database.
Gewerkt op npTDMS en later TDMSpp om de prestaties van npTDMS op te voeren met een factor 5.
- 2010–2014 **IT specialist**, *NetLogic*, Duffel, België
Algemeen IT en serverbeheer voor bij een KMO

Persoonlijke projecten

- 2023–nu **blurhash-rs**
Samen met het Whisperfish team, nam ik de ontwikkeling over van deze veelgebruikte bibliotheek om blurhash te encodere en decoderen. Ik heb meerdere prestatieverbeteringen doorgevoerd, zodat deze bibliotheek nu de snelste beschikbare blurhashbibliotheek is. <https://github.com/whisperfish/blurhash-rs>
- 2023–nu **rust-phonenumbers**
Samen met het Whisperfish team, nam ik de ontwikkeling over van deze veelgebruikte bibliotheek om telefoonnummers te parsen. <https://github.com/whisperfish/rust-phonenumbers>
- 2019–nu **Whisperfish**, *hoofdontwikkelaar*
“Whisperfish” is een onofficiële app voor Signal op SailfishOS. Het project werd in 2019 niet meer onderhouden, waarop ik het ontwikkelen heb overgenomen. Whisperfish groeit snel in gebruikers, en heeft de aandacht gekregen van verschillende andere gemeenschappen. Het wordt nu stilaan de gemeenschap van non-officiële Signal applicaties. <https://gitlab.com/whisperfish>
- 2019–nu **Belgium Rust gebruikersgroep Organisator**
Sinds 2019 ben ik de “Organisator” geworden van de Belgium Rust gebruikersgroep. Door de COVID-19 pandemie zijn we pas in februari 2022 opnieuw begonnen met evenementen. We organiseren evenementen voor Rustenthousiastelingen en -programmeurs in België, op verschillende locaties, veelal centraal en bereikbaar in Brussel.
- 2017–nu **Belgium Rust gebruikersgroep (lid)**
Ik ben actief lid sinds het begin van de Rustgebruikersgroep en heb op elke meetup tot nu toe over één of meerdere uiteenlopende onderwerpen gesproken, tot aan het begin van de pandemie.

- 2016–nu **Officiële L^AT_EX themas voor de Vrije Universiteit Brussel**
 Zowel beamer als article class templates voor de nieuwe VUB stijl, compatibel met de meeste L^AT_EX distributies. <https://gitlab.com/rubdos/texlive-vub>
- 2014–2019 **TheBounty Renderer**
 Een fork van de bekende *YafaRay* raytracer, waarbij ik werk rond de documentatie (met L^AT_EX) en GNU Make, en het optimaliseren van de Blender plugin, door Python 3 code te porten naar C++. Ik beheer ook hun Ruby on Rails gebaseerde website en forum.
- 2013–nu **Glycos**
 Ontwikkeling van een privaat, performant, en uitbreidbaar gedecentraliseerd online sociaal netwerk. Gestart als een persoonlijk project in het middelbaar, is Glycos geëvolueerd naar mijn huidige academisch onderzoek; zie pagina 7.

Taal

- Nederlands Moedertaal
 Engels Bekwaam
 Frans Conversationeel

Ingenieursvaardigheden

- Server Kubernetes, Docker, nginx, Ansible, PostgreSQL
 CI/CD GitLab CI, Github Actions
 Ontwikkeling Rust, C, Bash/Shell scripting, Python
 Cryptografie Elliptische krommen, zero-knowledge protocollen, Signal protocol stack
 Andere Git, L^AT_EX, vim, crosscompilen

Hobbies en Interesses

- Schaken Ik gaf les aan de jeugd van de Schaakkring Oude God in Mortsel. I neem deel aan de nationale interclubcompetitie.
- Vrije software & Privacy Ik ben een voorstander van de vrije softwarefilosofie en een privacyvoorvechter. Ik geloof dat vrije software en digitale privacy hand in hand gaan.
- Domotica Ik heb thuis een uitgebreid domoticasysteem gebaseerd op Home Assistant en andere vrije software.

Doctoraatsthesis

- 17 juni 2024 **Rapid prototyping and deployment of privacy-enhancing technologies**, *Vrije Universiteit Brussel*, Brussel, België, Engineering Science
- promotors prof. dr. ir. Kris Steenhaut en prof. dr. An Braeken

Masterproef

- Glycos een uitbreidbaar, zelfherstellend, besloten peer-to-peer online sociaal netwerk
- ontwikkeling en implementatie van een abstracte tool set voor het bouwen van een efficiënt gedecentraliseerd online sociaal netwerk.
- promotors prof. dr. Ann Dooms en prof. dr. Jo Pierson

Onderzoeks- en technologieprojecten

- 2022–2024 **RustIEC**, *Vrije Universiteit Brussel*, Brussel, België
- Onder promotorschap van prof. Kris Steenhaut, prof. An Braeken, dr. Jorn Lapon en prof. Stijn Volckaert, begeleid ik mee het RustIEC project. RustIEC is een VLAIO TETRA project (grant HBC.2021.0066) met als doel Vlaamse bedrijven de Rust programmeertaal te doen beheersen. Het project legt specifiek de focus op veiligheid in IoT systemen, veiligheid in edge computing en veiligheid in cloud computing. – <https://nl.rustiec.be>
- 2021–now **ETRO JupyterLab**, *Vrije Universiteit Brussel*, Brussel, België
- JupyterLab is een platform dat Jupyter Notebooks host. Het doel van deze omgeving is om alle ingenieursstudenten van de faculteit een online omgeving te bieden om Python te leren. Dit platform is online sinds 2021, <https://gitlab.com/etrovub/smartnets/jupyterhub/canvas-sync/>, en wordt gebruikt in zeven cursussen, gaande van de eerste bachelor Informatica tot “vibraties en akoestiek”.
- Het systeem is opgezet op onze intern Kubernetes cluster, en integreert <https://nbgrader.readthedocs.io/en/stable/>, voor gebruik in werkkolleges en tijdens examens.
- Ik ben verantwoordelijk voor de uitrol, het onderhoud en de dagelijkse werking.
- 2019–2023 **OpenCloudEdge**, *Vrije Universiteit Brussel*, Brussel, België
- Dit technologieoverdrachtproject (VLAIO TETRA) had als doel bedrijven in Vlaanderen te leren werken met cloud technologieën, waaronder OpenStack en Kubernetes. Ik was actief in de Kubernetes tests.

Ontwikkeling van een privaat, performant, en uitbreidbaar gedecentraliseerd online sociaal netwerk. Doorgedreven gebruik van moderne elliptische kromme gebaseerde cryptografie en zero-knowledge.

Prof. dr. Ann Dooms maakte het mogelijk om hieraan te werken op een academisch niveau als mijn masterproef, samen met privacy expert prof. dr. Jo Pierson, dan vervolgd in mijn doctoraatsonderzoek onder begeleiding van prof. dr. An Braeken en prof. dr. ir. Kris Steenhaut.

Glycos is nu het onderwerp van mijn postdoctoraal onderzoek, en delen-onderwerpen zijn onderwerp van het doctoraatsonderzoek van meerdere collega's.

Publicaties

- 2025 **De Smet, R.** (2025, 28 februari). [Decoupling Permission Management from Cryptography for Privacy-Preserving Systems](#) (Conference presentation). San Diego, CA, USA.

De Smet, R., Godden, T., Steenhaut, K., & Braeken, A. (2025). Decoupling Permission Management from Cryptography for Privacy-Preserving Systems. [Workshop on Innovation in Metadata Privacy: Analysis and Construction Techniques \(IMPACT\) 2025](#), 1–6. <https://doi.org/10.14722/impact.2025.23050>

- 2024 **De Smet, R.**, Blancquaert, R., Godden, T., Steenhaut, K., & Braeken, A. (2024). Armed with Faster Crypto: Optimizing Elliptic Curve Cryptography for ARM Processors. [Sensors](#), *24*(3), 1030. <https://doi.org/10.3390/s24031030>

De Smet, R., Steenhaut, K., & Braeken, A. (2024). Private Electronic Road Pricing Using Bulletproofs With Vector Commitments. [IEEE Transactions on Dependable and Secure Computing](#), *21*(4), 2659–2671. <https://doi.org/10.1109/TDSC.2023.3314867>

Van Glabbeek, R., **De Smet, R.**, Steenhaut, K., & Braeken, A. (2024). Zero-Touch Authentication for Device Deployment and Configuration in Industrial Internet of Things. [2024 IEEE 35th Annual International Symposium on Personal, Indoor and Mobile Radio Communications](#), 7, (accepted for publication).

Vandervelden, T., **De Smet, R.**, Deac, D., Steenhaut, K., & Braeken, A. (2024). Overview of Embedded Rust Operating Systems and Frameworks. [Sensors](#), *24*(17), 5818. <https://doi.org/10.3390/s24175818>

Vandervelden, T., Deac, D., Van Glabbeek, R., **De Smet, R.**, Braeken, A., & Steenhaut, K. (2024). Evaluation of 6LoWPAN Generic Header Compression in the Context of a RPL Network. [Sensors](#), *24*(1), 73. <https://doi.org/10.3390/s24010073>

- 2023 **De Smet, R.**, Steenhaut, K., & Braeken, A. (2023, 8 september). [Cryptography for private electronic traffic pricing](#) (Conference presentation). Brussels, Belgium.
- 2022 **De Smet, R.**, Thielemans, S., Lemeire, J., Braeken, A., & Steenhaut, K. (2022). Educational Software-as-a-Service Based on JupyterHub and Nbgrader Running on Kubernetes. [2022 IEEE 9th International Conference on E-Learning in Industrial Electronics \(ICELIE\)](#), 1–6. <https://doi.org/10.1109/ICELIE55228.2022.9969419>
- Godden, T., **De Smet, R.**, Debruyne, C., Vandervelden, T., Steenhaut, K., & Braeken, A. (2022). Circuitree: A Datalog Reasoner in Zero-Knowledge. [IEEE Access](#), **10**, 21384–21396. <https://doi.org/10.1109/ACCESS.2022.3153366>
- Thielemans, S., **De Smet, R.**, Benedetti, P., Reali, G., Braeken, A., & Steenhaut, K. (2022). Experiences with On-Premise Open Source Cloud Infrastructure with Network Performance Validation. [IECON 2022 – 48th Annual Conference of the IEEE Industrial Electronics Society](#), 1–6. <https://doi.org/10.1109/IECON49645.2022.9968898>
- Vandervelden, T., **De Smet, R.**, Steenhaut, K., & Braeken, A. (2022a). SHA3 and Keccak variants computation speeds on constrained devices. [Future Generation Computer Systems](#), **128**, 28–35. <https://doi.org/10.1016/j.future.2021.09.042>
- Vandervelden, T., **De Smet, R.**, Steenhaut, K., & Braeken, A. (2022b). Symmetric-Key-Based Authentication among the Nodes in a Wireless Sensor and Actuator Network. [Sensors](#), **22**(4), 1403. <https://doi.org/10.3390/s22041403>
- 2021 **De Smet, R.**, Vandervelden, T., Godden, T., & Braeken, A. (2021, 15 januari). [Flickr.rs: Creating Hogwarts' Flickr without magic](#) (Award). Virtual. <https://researchportal.vub.be/en/prizes/iacr-rwc21-cryptohackathon-on-functional-encryption-2nd-prize>
- De Smet, R.**, Vandervelden, T., Steenhaut, K., & Braeken, A. (2021). Lightweight PUF based authentication scheme for fog architecture. [Wireless Networks](#), **27**(2), 947–959. <https://doi.org/10.1007/s11276-020-02491-0>
- 2019 **De Smet, R.**, Dooms, A., Braeken, A., & Pierson, J. (2019). Glycos: The Basis for a Peer-to-Peer, Private Online Social Network. In E. Kosta, J. Pierson, D. Slamanig, S. Fischer-Hübner, & S. Krenn (Ed.), [Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data](#) (pp. 123–136, Deel 547). Springer International Publishing. https://doi.org/10.1007/978-3-030-16744-8_9

- 2018 **De Smet, R.**, Dooms, A., Braeken, A., & Pierson, J. (2018, 12 november). [Cryptography for peer-to-peer online social media](#) (Conference presentation). Ghent, Belgium.

Optreden in media

- 2023 Braeken, A., Steenhaut, K., **De Smet, R.**, & Deac, D. (2023, 10 april). [Standaarden voor de beveiliging van IoT](#). Cybersecurity Bites. <https://cybersecurity-bites.be/technologie/standaarden-voor-de-beveiliging-van-iot/>
- 2022 **De Smet, R.** (2022, 15 april). [End-to-end encryption is not the end](#). Ruben De Smet. <https://www.rubdos.be/2022/04/15/about-secure-messengers.html>
- De Smet, R.**, Vandervelden, T., Steenhaut, K., & Braeken, A. (2022a, 18 januari). [Cryptografische technieken voor dataminimalisatie](#). Cybersecurity Bites. <https://cybersecurity-bites.be/beveiligingsinfrastructuur/cryptografische-technieken-voor-dataminimalisatie/>
- De Smet, R.**, Vandervelden, T., Steenhaut, K., & Braeken, A. (2022b, 17 februari). [End-to-end encryptie is niet het einde](#). Cybersecurity Bites. <https://cybersecurity-bites.be/cybersecuritybydesign/end-to-end-encryptie-is-niet-het-einde/>
- De Smet, R.**, Vandervelden, T., Steenhaut, K., & Braeken, A. (2022c). End-to-end encryptie is niet het einde [magazine]. [MinistryTalks](#), 2022(3), 5–8.
- 2021 **De Smet, R.**, Vandervelden, T., Steenhaut, K., & Braeken, A. (2021, 21 december). [Back-ups als ultieme gemoedsrust](#). Cybersecurity Bites. <https://cybersecurity-bites.be/ict-beheer/back-ups-als-ultieme-gemoedsrust/>
- Vandervelden, T., **De Smet, R.**, Steenhaut, K., & Braeken, A. (2021, 21 december). [Beveiligingsoverwegingen voor het uitrollen van IoT-applicaties](#). Cybersecurity Bites. <https://cybersecurity-bites.be/beveiligingsinfrastructuur/beveiligings-overwegingen-voor-het-uitrollen-van-iot-applicaties/>

Publiek spreken

- 2024 **De Smet, R.** (2024, 5 februari). [Vulnerabilities in Rust programs](#). Post-FOSDEM Rust Meetup @ Vrije Universiteit Brussel, Brussels, Belgium. <https://researchportal.vub.be/en/activities/vulnerabilities-in-rust-programs>

- 2022 **De Smet, R.** (2022a, 3 februari). [How Rust won us a second place in a Hackathon/Flickr.rs: Creating Hogwarts' Flickr without magic](#). Belgium Rust User Group February 3 2022: In-person Rust Meetup: Async Qt, Bubbly Bubblesorts and How to Win Hackathons. Leuven, Belgium. <https://video.rubdos.be/w/bhhMcctgLXTX5hrVARw3eu?start=30m31s>
- De Smet, R.** (2022b, 3 februari). [Qt5 in an asynchronous runtime/qmeta-async: How to run Qt and Tokio together](#). Belgium Rust User Group February 3 2022: In-person Rust Meetup: Async Qt, Bubbly Bubblesorts and How to Win Hackathons. Leuven, Belgium. <https://video.rubdos.be/w/bhhMcctgLXTX5hrVARw3eu?start=51m45s>
- De Smet, R.** (2022c, 22 oktober). [Signal and Sailfish OS](#). Your Phone & You, Renens, Switzerland. <https://fixme.ch/node/219>
- De Smet, R., & Shearer, D.** (2022, 6 april). [Attribute-Based Encryption and A Portable Data Format](#). LumoSQL Seminar Vrije Universiteit Brussel, Brussels, Belgium. <https://lumosql.org/talks.html>

CVEs

- 2025 Whisperfish Team. (2025a, februari). [CVE-2025-24903: Message Authenticity Check Bypass](#) (Common Vulnerability Enumeration). Common Vulnerability Enumeration. <https://cve.mitre.org/cgi-bin/cvename.cgi?name=2025-24903>
- Whisperfish Team. (2025b, februari). [CVE-2025-24904: End-to-End Encryption Bypass](#) (Common Vulnerability Enumeration). Common Vulnerability Enumeration. <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-24904>
- 2024 Whisperfish Team. (2024, 27 juni). [CVE-2024-39697: Panic on Parsing Crafted Phonenumber Inputs](#) (Common Vulnerability Enumeration Nr. CVE-2024-39697). Common Vulnerability Enumeration. <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-39697>
- 2023 Whisperfish Team. (2023a, 8 september). [CVE-2023-42444: Panic on Parsing Crafted RFC3966 Phonenumber Inputs](#) (Common Vulnerability Enumeration Nr. CVE-2023-42444). Common Vulnerability Enumeration. MITRE. <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-42444>
- Whisperfish Team. (2023b, 8 september). [CVE-2023-42447: Panic on Parsing Crafted Blurhash Inputs](#) (Common Vulnerability Enumeration Nr. CVE-2023-42447). Common Vulnerability Enumeration.

tion. MITRE. <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-42447>