Ruben De Smet

About me

A privacy advocate since high school, with extensive experience in applied cryptography and privacy-enhancing technologies in Rust. Passionate about developing decentralized real-world solutions that protect user privacy. This passion reflects in projects like Whisperfish and Glycos.

Education

2018–2024 **Doctor of Philosophy**, *Vrije Universiteit Brussel*
Research on zero-knowledge proofs as privacy-enhancing technology.

2016–2018 **Master of Science**, *Vrije Universiteit Brussel*
Engineering Science: Computer Science: Multimedia

2013–2017 **Bachelor of Science**, *Vrije Universiteit Brussel*
Engineering Science: Electronics and Information Technology, computer science

Skills

Programming	■■■■■	Rust	■■■■□	C
	■■■■□	Python	■■■□□	Java
Languages	■■■■■	Dutch	■■■■□	English
	■■■□□	French		

Experience

2024–now **Postdoctoral researcher applied cryptography**, *Vrije Universiteit Brussel*, Brussels, Belgium
- Research projects in cryptography and privacy engineering
- Technology projects regarding Rust, cloud and IoT

2019–now **Whisperfish**, *lead developer*, Unofficial Signal app for Sailfish OS
- Rewritten in Rust, fully backwards compatible
- Implemented large parts of the Signal API

2018–2024 **Teaching assistant**, *Vrije Universiteit Brussel*, Brussels, Belgium
- Teaching programming and electronics
- Research projects in cryptography and privacy engineering

me@rubdos.be • www.rubdos.be • rubdos
rubdos • rubdos.95 • rubdos • @rubdos

Education

2018–2024 **Doctor of Philosophy**, *Vrije Universiteit Brussel*, Brussels, Belgium, *Engineering Science: PhD Electronics and Information Technology*
applied cryptography, security, privacy, telecommunication.

2016–2018 **Master of Science**, *Vrije Universiteit Brussel*, Brussels, Belgium, *Engineering Science: Computer Science: Multimedia*
computer vision, image and video technology, digital speech and audio processing, cryptography and security.

2013–2017 **Bachelor of Science**, *Vrije Universiteit Brussel*, Brussels, Belgium, *Engineering Science: Electronics and Information Technology, computer science*
basic electronics, computer networks and protocols, algorithms, data structures, computer architectures

2006–2013 **ASO**, *Sint-Ritacollege*, Kontich, Belgium, *Wetenschappen-Wiskunde*

Experience references on request

2024–now **Postdoctoral researcher applied cryptography**, *Vrije Universiteit Brussel*, Brussels, Belgium
I am involved in several research and technology projects regarding Rust, IoT, privacy and security. My research mainly involves development of practical privacy-enhancing technologies. For details, see the academic section at page 5.

2018–2024 **Teaching assistant**, *Vrije Universiteit Brussel*, Brussels, Belgium
As a teaching assistant, I was co-responsible for the first bachelor Informatica ("programming 101") course and a part of the third bachelor electronics course at the Engineering Sciences faculty. I was also involved in several research and technology projects, regarding Rust and cloud technologies. For details, see the academic section at page 5.

2015–now **Owner at De Smet Multimedia BV**, *Consulting*, Brussels / Antwerp, Belgium
General IT, implementation and integration.

Freelance

2016–now **Tutoring secondary education**
Long term tutoring mathematics and physics for 5th and 6th secondary education. Tutoring computer science topics for 1st Bachelor.

2015–2018 **Freelance Linux system administrator**, *BruWind/Vrije Universiteit Brussel*, Brussels, Belgium
Deploying, testing, administrating a CentOS 7 cluster using Ansible. System monitoring. Continuous integration, complex continuous deployment of Docker based micro service architecture.

Student work

July 2015 **ETL implementation**, *Vrije Universiteit Brussel*, Brussels, Belgium
Implemented ETL software using Python 3 and SOS-Berlin JobScheduler. Loading vast amounts of windturbine sensor data into a PostgreSQL 9.4 database.
Worked on npTDMS and TDMSpp, of which the latter improves the performance of the former with a factor 5

2010–2014 **IT specialist**, *NetLogic*, Duffel, Belgium
General IT and server administration for a small company

Personal projects

2023–now **blurhash-rs**, *maintainer*
Together with the Whisperfish team, I took over the maintenance of this widely used blurhash computing library. I implemented multiple performance improvements, which makes this library by far the fastest blurhash decoding and encoding library available. https://github.com/whisperfish/blurhash-rs

2023–now **rust-phonenumber**, *maintainer*
Together with the Whisperfish team, I took over the maintenance of this widely used phonenumber parsing library. https://github.com/whisperfish/rust-phonenumber

2019–now **Whisperfish**, *lead developer*
Whisperfish is a third-party implementation of the Signal protocol stack for Sailfish OS. It was left unmaintained in 2019, and I took over development. Whisperfish is rapidly growing in users, and has gotten the attention of several other communities. Whisperfish is becoming the go-to community for third-party Signal client development. https://gitlab.com/whisperfish

2019–now **Belgium Rust user group Organiser**
I have become the official "Organiser" of the Belgium Rust user group, since 2019. Due to the COVID-19 pandemic, we only started organising physical events again in February 2022. We organise events for Rust enthusiasts and engineers all around Belgium, at different locations, typically centrally reachable in Brussels.

2017–now **Belgium Rust user group member**
Having spoken about a plethora of topics at all Meetups until now, I have been an active member of the Belgium Rust user group until the start of the pandemic.

2016–now **Official LaTeX assets for the Vrije Universiteit Brussel**
Both `beamer` and `article` class templates for the new VUB style, compatible with most LaTeX distributions. https://gitlab.com/rubdos/texlive-vub

2014–2019 **TheBounty Renderer**
A free software fork of the famous *YafaRay* raytracer, mostly working on documentation using LaTeX and GNU Make and optimising the Blender Exporter by porting Python 3 code to C++. I also maintain its custom (Ruby on Rails) website and forum.

2013–now **Glycos**
Development of a private, performant, and extensible peer-to-peer online social network. Starting as a personal project in high school, Glycos evolved into my current academic research; see page 6.

Languages

Dutch	Native
English	Proficient
French	Conversational

Engineering skills

System	Kubernetes, Docker, nginx, Ansible, PostgreSQL
CI/CD	GitLab CI, Github Actions
Development	Rust, C, Bash/Shell scripting, Python
Cryptography	Elliptic curve cryptography, zero-knowledge protocols, Signal protocol stack
Misc.	Git, LaTeX, vim, cross compiling

Hobbies and Interests

Chess	I thought chess to the youth of the Schaakkring Oude God in Mortsel. I participate in the national interclub competition.
Free software & Privacy	I am a proponent of the free software philosophy, and a privacy advocate. I believe free software and digital privacy go hand-in-hand.
Home Automation	I have an extensive home automation and domotics system based on Home Assistant and other free software.

Doctoral thesis

June 17, 2024 **Rapid prototyping and deployment of privacy-enhancing technologies**, *Vrije Universiteit Brussel*, Brussels, Belgium, Engineering Science

promoters prof. dr. ir. Kris Steenhaut and prof. dr. An Braeken

Master thesis

Glycos an extensible, resilient and private peer-to-peer online social network

development and implementation of an abstract tool set for building performant decentralised online social networks.

promoters prof. dr. Ann Dooms and prof. dr. Jo Pierson

Research and technology projects

2022–2024 **RustIEC**, *Vrije Universiteit Brussel*, Brussels, Belgium

Under the promotorship of prof. Kris Steenhaut, prof. An Braeken, dr. Jorn Lapon and prof. Stijn Volckaert, I am co-leading the RustIEC project. RustIEC is a VLAIO TETRA project (grant HBC.2021.0066) with the goal of teaching Flanders' companies proficiency in the Rust programming language. The project has a specific focus on secure IoT systems, secure edge computing, and secure cloud computing. – https://rustiec.be

2021–now **ETRO JupyterLab**, *Vrije Universiteit Brussel*, Brussels, Belgium

JupyterLab is a platform that hosts Jupyter Notebooks. The goal of this setup is to provide all engineering students at the faculty an online environment to learn Python. This platform has been online since 2021, https://gitlab.com/etrovub/smartnets/jupyterhub/canvas-sync/, and is used in seven courses ranging from first Bachelor Informatica ("programming 101") to "vibrations and acoustics".

The system is setup on our internal Kubernetes cluster, and integrates https://nbgrader.readthedocs.io/en/stable/, for use in exercise sessions and during exams.

I am the main responsible for its rollout, maintenance and daily operation.

2019–2023 **OpenCloudEdge**, *Vrije Universiteit Brussel*, Brussels, Belgium

This technology-transfer project (VLAIO TETRA) had the goal of teaching companies in Flanders to work with cloud technologies, among which OpenStack and Kubernetes. I was active in the Kubernetes tests.

2018–now **Glycos**

Research on private, performant, and extensible peer-to-peer online social networks. Heavy use of modern cryptography (elliptic curve signatures, zero-knowledge systems).
Prof. dr. Ann Dooms made it possible to work on this on an academic level for my master thesis together with digital privacy expert prof. dr. Jo Pierson, which was then continued in my PhD study under supervision of prof. dr. An Braeken and prof. dr. ir. Kris Steenhaut.
Glycos has now become the topic of my postdoctoral research, and subtopics are part of the doctoral research of multiple colleagues.

Publications

2025 **De Smet, R.** (2025, February 28). 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, September 8). 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, January 15). Flick.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 (Eds.), Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data (pp. 123–136, Vol. 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, November 12). Cryptography for peer-to-peer online social media (Conference presentation). Ghent, Belgium.

Appearance in media

2023 Braeken, A., Steenhaut, K., **De Smet**, **R.**, & Deac, D. (2023, April 10). Standaarden voor de beveiliging van IoT. Cybersecurity Bites. https://cybersecurity-bites.be/technologie/standaarden-voor-de-beveiliging-van-iot/

2022 **De Smet**, **R.** (2022, April 15). 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, January 18). 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, February 17). 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, December 21). 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, December 21). Beveiligingsoverwegingen voor het uitrollen van IoT-applicaties. Cybersecurity Bites. https://cybersecurity-bites.be/beveiligingsinfrastructuur/beveiligings-overwegingen-voor-het-uitrollen-van-iot-applicaties/

Public speaking

2024 **De Smet**, **R.** (2024, February 5). 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, February 3). How Rust won us a second place in a Hackathon/Flick.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, February 3). 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, October 22). Signal and Sailfish OS. Your Phone & You, Renens, Switserland. https://fixme.ch/node/219

De Smet, R., & Shearer, D. (2022, April 6). Attribute-based Encryption and A Portable Data Format. LumoSQL Seminar Vrije Universiteit Brussel, Brussels, Belgium. https://lumosql.org/talks.html

CVE's

2025 Whisperfish Team. (2025a, February). 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, February). 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, June 27). CVE-2024-39697: Panic on parsing crafted phonenumber inputs (Common Vulnerability Enumeration No. CVE-2024-39697). Common Vulnerability Enumeration. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-39697

2023 Whisperfish Team. (2023a, September 8). CVE-2023-42444: Panic on parsing crafted RFC3966 phonenumber inputs (Common Vulnerability Enumeration No. CVE-2023-42444). Common Vulnerability Enumeration. MITRE. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-42444

Whisperfish Team. (2023b, September 8). CVE-2023-42447: Panic on parsing crafted blurhash inputs (Common Vulnerability Enumeration No. CVE-2023-42447). Common Vulnerability Enumeration. MITRE. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-42447