About Cryspen

Vision & Mission

End-to-end security and privacy are fundamental requirements for a modern and open society. However, designing and implementing systems that achieve these goals is tremendously difficult and notoriously error-prone, requiring specialized domain knowledge in cryptography and careful low-level software engineering.

We believe that formal verification, when used effectively, can significantly improve the assurance of complex cryptographic software by eliminating large classes of bugs and attacks. To this end, we rely on recent landmark research results from Inria and Microsoft Research and state-of-the-art formal verification tools for cryptographic protocols and implementations.

Our mission is to provide services and software for high assurance cryptography in order to establish trust in your security-critical systems.

Our Approach

Cryspen is a development studio focused on bringing state-of-the-art privacy and cryptography solutions to customers, using cutting-edge formal methods. Few companies have the expertise or resources to establish dedicated formal methods teams. Cryspen makes formal methods instantly accessible, enabling its customers to adopt the new benchmark in terms of software security and reliability, without sacrificing performance or having to adopt new programming languages. Cryspen revolves around two offerings.

The **Cryspen High Assurance Crypto Toolkit** is a collection of verified, drop-in implementations of standardized cryptographic algorithms and protocols in C, Rust, and WebAssembly. With these, your company can instantly embrace well-analyzed, modern cryptographic mechanisms and standards, with the peace of mind offered by our support contract.

Cryspen also **develops custom high-assurance** security solutions when your company needs bespoke cryptographic mechanisms that go beyond established standards. We design and analyze the mechanism, in close collaboration with the Prosecco team at INRIA Paris before we author custom high-assurance implementations for the new mechanism in collaboration with your in-house engineers.

The Team

With an unwavering commitment to high-performance high-assurance software engineering, our founders have a demonstrated track record of solving the most challenging problems. With a combined experience of over 40 years in the cryptography and formal methods space, the three co-founders are uniquely equipped to solve cryptographic challenges; starting from the design and analysis phase all the way to the production system.

Prof Karthikeyan Bhargavan has 20 years of experience in formal verification, protocol analysis, and applied cryptography. He leads the Programming Securely with Cryptography group at INRIA Paris and focuses on the design and implementation of new program verification techniques that would enable formal analyses of real-world security applications.

Dr Franziskus Kiefer has 10 years of experience in analyzing and proving cryptographic protocols academically as well as implementing and maintaining cryptography software for Mozilla and others.

Dr Jonathan Protzenko has 10 years of experience designing languages, verification software and toolchains for formal methods. Whether it's a verified cryptographic library or a secure protocol implementation, the projects he drives bridge the gap between academia and usable, real world software.

The Cryspen software portfolio revolves around the open-source projects **HACL***, **evercrypt-rust**, and **hacspec**, which are developed and maintained by the co-founders and the wider research community at Prosecco, Microsoft Research and CMU. On top of these low-level libraries, Cryspen develops implementations of **MLS** and **TLS** that offer the highest assurances with respect to correctness and safety. All this is provided without compromising on performance.

The strong research background of the projects and continuing close research relation with the Prosecco team puts Cryspen in the unique position of being able to offer the only production-quality high-assurance cryptography library. The library is further embedded in a set of tools for formally verifying properties of cryptographic primitives and protocols with hacspec as a front-end.

The Cryspen High Assurance Crypto Toolkit

Cryspen offers long-term maintenance, enhancement, and support of **HACL*** and hacspec. Long-term support contracts guarantee maintenance and bug fixes of the toolkit. If certain primitives, protocols, or environments are not supported by the toolkit yet, Cryspen can be contracted to enhance the toolkit accordingly. This includes, but is not limited to, emerging cryptography for Post-Quantum Cryptography (PQC), and advanced constructions and protocols for Multi Party Computation (MPC) and Zero-Knowledge (ZK) proofs.

Cryspen also offers support to adapt the toolkit and custom solutions to new environments or hardware platforms if they are not supported yet.

▼ **Cryptographic Software Verification**

The biggest differentiator between our toolkit and existing cryptography libraries is our rigorous use of formal methods in the engineering process. As foundational building blocks, all cryptographic primitives are formally verified for their correctness, memory safety, and secret independent computation. Higher level primitives and protocols employ formal methods to prove critical properties, for example, the uniqueness and confidentiality of the keys generated in the TLS handshake.

Good engineering processes are paramount when developing safe code. To ensure that any code developed by Cryspen is safe, secure development practices (also see the Microsoft SDL description) are employed. In particular, testing through test vectors, fuzzing, and property based testing is employed in addition to strict review and CI requirements, and a transparent vulnerability disclosure process.

▼ **Safe programming languages**

Manually authored code in the Cryspen toolkit is written in the memory safe programming language Rust. This ensures the absence of the largest class of security bugs in software, which is unsafe memory handling.

To further enable the formal verification of cryptographic code written in Rust, we develop and apply new tools and languages, such as hacspec, a crypto-oriented subset of Rust. The team is heavily invested in the Rust programming language and active in the community, especially the Rust Cryptography and the Rust Formal Verification Interest Groups.

Custom High-Assurance Security Solutions

Cryspen can help customers design and analyze, but also implement new cryptographic mechanisms. The former involves using manual and computer-aided formal modelling to assess security and correctness of systems before their implementation. The latter encompasses all flavors of high assurance implementations aided by formal verification.

With a close focus and active involvement in the cryptography research community, Cryspen is particularly well-equipped and capable of realizing complex cryptographic mechanisms safely. This in particular includes modern cryptographic systems such as Multi Party Computation (MPC), Post-Quantum Cryptography (PQC), Zero-Knowledge (ZK) protocols, or any combination thereof.

Services Cryspen can offer include but are not limited to

- Verification of new cryptographic standards, e.g post-quantum cryptography
- Verification of custom cryptographic primitives and protocols
- Design and analysis of new cryptographic solutions, e.g. multi-party computation
- Support for using and integrating the Cryspen cryptographic software toolkit
- Implementation of proprietary extensions to the toolkit
- Porting and optimizing toolkit for new platforms
- Minimal cryptographic libraries for embedded devices
- Integrating and implementing MLS group messaging and its variants
- Integrating and implementing custom variants of TLS 1.3

Selected Publications

- **HACL*: A Verified Modern Cryptographic Library.** Jean Karim Zinzindohoué, Karthikeyan Bhargavan, Jonathan Protzenko, Benjamin Beurdouche. ACM Conference on Computer and Communications Security 2017: 1789-1806
- **Verified Models and Reference Implementations for the TLS 1.3 Standard Candidate.** Karthikeyan Bhargavan, Bruno Blanchet, Nadim Kobeissi. IEEE Symposium on Security and Privacy 2017: 483-502
- **hacspec: Towards Verifiable Crypto Standards.** Karthikeyan Bhargavan, Franziskus Kiefer, Pierre-Yves Strub. Security Standardisation Research 2018: 1-20

- **Formally Verified Cryptographic Web Applications in WebAssembly.** Jonathan Protzenko, Benjamin Beurdouche, Denis Merigoux, Karthikeyan Bhargavan. IEEE Symposium on Security and Privacy 2019: 1256-1274
- **HACLxN: Verified Generic SIMD Crypto (for all your favourite platforms).** Marina Polubelova, Karthikeyan Bhargavan, Jonathan Protzenko, Benjamin Beurdouche, Aymeric Fromherz, Natalia Kulatova, Santiago Zanella Béguelin. ACM Conference on Computer and Communications Security 2020: 899-918