**BoringSSL vs WolfSSL**

**Initial Remarks**

BoringSSL and wolfSSL are both open-source cryptographic libraries that provide SSL/TLS and other cryptographic functionalities. Here are the key differences between BoringSSL and wolfSSL:

1. Origin and Forking: BoringSSL is a fork of OpenSSL created by Google to meet the specific needs of its projects. It was developed with a focus on code simplicity, maintainability, and performance. BoringSSL includes modifications and additions that are specific to Google's use cases. WolfSSL, formerly known as CyaSSL, is an independent project that started as a lightweight SSL/TLS library for embedded systems. It emphasizes efficiency and a small footprint while providing essential SSL/TLS and cryptography functionality.
2. Codebase and Features: BoringSSL and wolfSSL have different codebases and feature sets. BoringSSL aims to provide a minimal and streamlined library with a focus on security, performance, and maintainability. It may not prioritize maintaining full compatibility with OpenSSL. WolfSSL, on the other hand, is designed to be a compact and lightweight library suitable for resource-constrained environments such as embedded systems. It offers a broad range of features and supports various cryptographic protocols.
3. Development and Community: BoringSSL is primarily maintained by Google engineers and benefits from contributions within the Google development community. It follows its own development processes and priorities. WolfSSL is developed and maintained by the wolfSSL company, which provides commercial support and services around the library. It has its own community of users and contributors and follows its own development processes.
4. Platform Support: Both BoringSSL and wolfSSL support multiple platforms, including Linux, Windows, macOS, and embedded systems. However, BoringSSL may have a stronger focus on specific Google platforms and use cases, while wolfSSL aims to provide cross-platform compatibility.
5. Licensing: BoringSSL is released under the Apache License 2.0, which is a permissive license. WolfSSL is dual-licensed, offering both a GPLv2 license and commercial licensing options for proprietary use.
6. Industry Adoption: BoringSSL is primarily used by Google and is integrated into various Google projects and services. It may have limited adoption outside of the Google ecosystem. WolfSSL is widely used in embedded systems, IoT devices, and security-focused applications. It has a strong presence in the embedded systems and IoT community and is integrated into various products and projects.

When choosing between BoringSSL and wolfSSL, consider your specific requirements, platform support, licensing preferences, and the level of compatibility needed with existing software. If you are working on a project that aligns with Google's use cases and prioritizes simplicity and performance, BoringSSL may be a suitable choice. If you need a lightweight library with a small footprint and broad feature set for embedded systems and IoT, wolfSSL might be a better fit.

**Testcase Directories:**

1. 20220421\_170553\_boringssl-f0451ca-wolfssl-3.9.6-update-1\_tgt-0\_all
2. 20220421\_174559\_boringssl-f0451ca-wolfssl-3.9.6-update-1\_tgt-1\_all
3. 20220511\_172254\_boringssl-f0451ca-wolfssl-3.9.6-update-1-rank-1-44ed8\_tgt-0\_all
4. 20220511\_180318\_boringssl-f0451ca-wolfssl-3.9.6-update-1-rank-1-44ed8\_tgt-1\_all
5. 20220511\_180722\_boringssl-f0451ca-wolfssl-3.9.6-update-1-rank-2-b06f4\_tgt-0\_all
6. 20220511\_184738\_boringssl-f0451ca-wolfssl-3.9.6-update-1-rank-2-b06f4\_tgt-1\_all