**LibreSSL vs BoringSSL**

**Initial Remarks**

LibreSSL and BoringSSL are both open-source cryptographic libraries that aim to provide secure implementations of cryptographic functions and protocols. While they share some similarities, there are key differences between the two:

1. Codebase and Forking: LibreSSL is a fork of OpenSSL that was created in response to security concerns and perceived code quality issues in OpenSSL. It was developed by the OpenBSD project with a focus on simplicity, correctness, and removing unnecessary code and features. BoringSSL, on the other hand, is a fork of OpenSSL created by Google to meet the specific needs of its projects. BoringSSL also focuses on code simplicity, maintainability, and performance, but it may include modifications and additions that are specific to Google's use cases.
2. Development and Community: LibreSSL is primarily maintained by the OpenBSD project and benefits from the contributions and expertise of the OpenBSD community. BoringSSL, developed by Google, is primarily maintained by Google engineers and receives contributions from the broader Google development community. Both projects have their own development processes and priorities.
3. Goals and Scope: LibreSSL aims to provide a drop-in replacement for OpenSSL with a focus on security, code quality, and compatibility with existing applications and protocols. It aims to maintain API and ABI compatibility with OpenSSL to ensure seamless integration for existing applications. BoringSSL, on the other hand, focuses on providing a minimal and streamlined library that can be easily integrated into Google's projects. It may not prioritize maintaining full compatibility with OpenSSL.
4. Licensing: LibreSSL is released under the OpenBSD License, which is a permissive license similar to the ISC License. BoringSSL is released under the Apache License 2.0, which is also a permissive license.
5. Platform Support: Both LibreSSL and BoringSSL support multiple platforms, including Linux, BSD, and macOS. However, due to their different development focuses, they may have varying levels of support for different platforms or architectures.

When choosing between LibreSSL and BoringSSL, consider your specific needs, project requirements, and compatibility with existing software. If you are looking for a drop-in replacement for OpenSSL with a focus on security and code quality, LibreSSL may be a suitable choice. On the other hand, if you are working on a project that aligns with Google's use cases and prioritizes simplicity and performance, BoringSSL may be a better fit.

**Testcase Directories:**

1. 20220421\_170140\_libressl-2.4.0-boringssl-f0451ca-update-1\_tgt-0\_all
2. 20220421\_172021\_libressl-2.4.0-boringssl-f0451ca-update-1\_tgt-1\_all
3. 20220511\_171904\_libressl-2.4.0-boringssl-f0451ca-update-1-rank-1-5bbe7\_tgt-0\_all
4. 20220511\_175758\_libressl-2.4.0-boringssl-f0451ca-update-1-rank-1-5bbe7\_tgt-1\_all
5. 20220511\_181900\_libressl-2.4.0-boringssl-f0451ca-update-1-rank-2-b3b1f\_tgt-0\_all
6. 20220511\_190522\_libressl-2.4.0-boringssl-f0451ca-update-1-rank-2-b3b1f\_tgt-1\_all