**LibreSSL vs MbedTLS**

**Initial Remarks**

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

1. Origin and Forking: LibreSSL is a fork of OpenSSL that was created by the OpenBSD project. It was developed to address security concerns and code quality issues in OpenSSL. MbedTLS (previously known as PolarSSL) is an independent project developed by ARM, now owned by NXP Semiconductors. It was designed specifically for embedded systems and IoT devices.
2. Codebase and Features: LibreSSL and mbedTLS have different codebases and feature sets. LibreSSL aims to be a drop-in replacement for OpenSSL with a focus on security, code simplicity, and compatibility with existing applications and protocols. It removes or rewrites code from OpenSSL that is considered unnecessary, deprecated, or problematic. MbedTLS, on the other hand, is designed to be a lightweight library optimized for resource-constrained environments. It provides a minimal footprint while offering essential SSL/TLS and cryptographic functionalities.
3. Development and Community: LibreSSL is primarily maintained by the OpenBSD project, benefiting from the contributions and expertise of the OpenBSD community. MbedTLS is maintained by a dedicated team at ARM/NXP and has its own community of users and contributors. Both projects have their development processes, but mbedTLS has a strong focus on the embedded systems and IoT community.
4. Platform Support: Both LibreSSL and mbedTLS support various platforms, including Linux, Windows, macOS, and embedded systems. However, mbedTLS places a strong emphasis on embedded systems, IoT devices, and resource-constrained environments. It provides platform-specific optimizations and features tailored for these environments.
5. Licensing: LibreSSL is released under the OpenBSD License, which is a permissive license similar to the ISC License. MbedTLS is dual-licensed, offering both an Apache License 2.0 and a GPLv2 license.
6. Industry Adoption: LibreSSL has gained significant adoption, particularly in the OpenBSD and BSD communities. It is the default SSL/TLS library in OpenBSD. MbedTLS is widely used in embedded systems, IoT devices, and security-focused applications, and it has a strong presence in the IoT and ARM ecosystem.

When choosing between LibreSSL and mbedTLS, consider your specific requirements, platform support, licensing preferences, and the target environment. If you need a drop-in replacement for OpenSSL with a focus on security and compatibility, LibreSSL may be a suitable choice. If you are targeting resource-constrained environments and require a lightweight library optimized for embedded systems and IoT, mbedTLS might be a better fit.

**Testcase Directories:**

1. 20220421\_170403\_libressl-2.4.0-mbedtls-2.2.1-update-1\_tgt-0\_all
2. 20220421\_173422\_libressl-2.4.0-mbedtls-2.2.1-update-1\_tgt-1\_all
3. 20220511\_172105\_libressl-2.4.0-mbedtls-2.2.1-update-1-rank-1-f8a33\_tgt-0\_all
4. 20220511\_174914\_libressl-2.4.0-mbedtls-2.2.1-update-1-rank-1-f8a33\_tgt-1\_all
5. 20220511\_180145\_libressl-2.4.0-mbedtls-2.2.1-update-1-rank-2-810d1\_tgt-0\_all
6. 20220511\_182508\_libressl-2.4.0-mbedtls-2.2.1-update-1-rank-2-810d1\_tgt-1\_all