CS 1657: Privacy in the Electronic Society
Homework 2

Adiantum is a new cryptographic construction developed by Google that enables efficient and secure full-disk encryption on low-end mobile devices. It is a stream cipher that uses a combination of two primitives: the ChaCha20 stream cipher and the AES block cipher in counter mode.

Adiantum provides the same security properties as standard full-disk encryption (FDE) techniques, including confidentiality, integrity, and authenticity. It also addresses the threat model of an attacker who has physical access to the device but cannot retrieve the encryption key. However, Adiantum does not address the threat model of an attacker who can retrieve the key from memory or the device's secure enclave. Despite these limitations, Adiantum is considered secure for everyday use based on Google's internal security evaluations.

Adiantum is composed of existing cryptographic primitives that are used in other scenarios and protocols, such as HTTPS and the Signal protocol. These primitives are well-suited to these situations because they are widely studied and have been shown to be secure. Adiantum builds upon these primitives by providing a way to efficiently encrypt and decrypt data on low-end mobile devices.

Standard FDE techniques cannot be used on some low-end mobile devices because they lack hardware support for AES encryption, which is required by most FDE schemes. Adiantum is different because it uses the lightweight ChaCha20 stream cipher instead of AES. This makes Adiantum much faster than other FDE techniques on low-end devices.

Converting a plaintext sector into a same-sized ciphertext is non-trivial because some plaintext sectors may be shorter than the block size of the underlying cipher. Adiantum works around this issue by using a length-preserving mode of operation called Miscreant, which was inspired by the Hasty Pudding cipher. Hasty Pudding was a conceptual predecessor to Adiantum that pioneered the

idea of using a stream cipher to encrypt disk sectors. Adiantum improves upon this idea by using a more secure and efficient stream cipher.

The block diagram near the bottom of the article portrays Adiantum's functionality. Adiantum consists of a key derivation function that generates a key and nonce for each disk sector. These are then used to encrypt and decrypt the data using the Miscreant mode of operation.

Adiantum is suitable for use in all FDE devices and scenarios where low-end mobile devices are concerned. In scenarios where higher-end devices are used, other FDE techniques such as AES-based schemes may be more appropriate. However, Adiantum is still a good choice for low-end devices because of its efficiency and security properties.

Adiantum is an important contribution to the field of cryptography because it enables efficient and secure full-disk encryption on low-end mobile devices. Its use of lightweight cryptographic primitives and innovative modes of operation make it an attractive alternative to standard FDE techniques. While it may not be suitable for all scenarios, Adiantum is a valuable addition to the cryptographic toolbox.