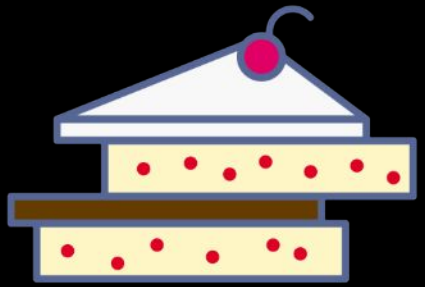
Shufflecake

AKA TrueCrypt on Steroids for Linux



Tommaso Gagliardoni, Kudelski Security

From a joint work with Elia Anzuoni

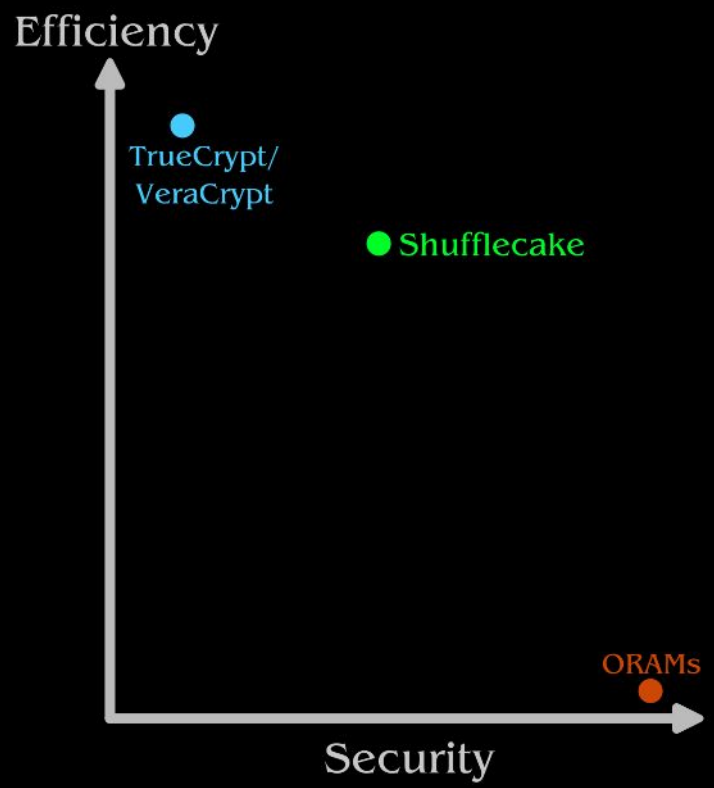
Pass the SALT

2024-07-03, Lille, France

Pass the SALT

Shufflecake: TL;DR

- Encrypts, hides existence of disk partitions
- Plausible deniability like TrueCrypt/VeraCrypt
- Security and usability improvements
- Cryptographic proof of security
- Faster than ORAM-based solutions
- Potential to improve security even further
- FLOSS (“free” as in “freedom”)



Shufflecake: TL;DR

Shufflecake

AKA TrueCrypt on Steroids for Linux

DEF CON 31 Demo Labs

2023-08-11, Las Vegas (NV), USA

Introducing Shufflecake: Plausible Deniability For Multiple Hidden Filesystems on Linux (kudelskisecurity.com) 90

Posted by EditorDavid on Saturday November 12, 2022 @02:34PM from the magic-mounting dept.

Thursday the Kudelski Group's cybersecurity division released "a tool for Linux that allows creation of multiple hidden volumes on a storage device in such a way that it is very difficult, even under forensic inspection, to prove the existence of such volumes."

"Each volume is encrypted with a different secret key, scrambled across the empty space of an underlying existing storage medium, and indistinguishable from random noise when not decrypted."

> Even if the presence of the Shufflecake software itself cannot be hidden — and hence the

Shufflecake: Plausible Deniability For Multiple Hidden Filesystems On Linux

Elia Anzuoni
ETHZ and EPFL and Kudelski Security
Switzerland

Tommaso Gagliardoni
Kudelski Security
Switzerland

ABSTRACT

We present Shufflecake, a new plausible deniability design to hide the existence of encrypted data on a storage medium making it very difficult for an adversary to prove the existence of such data.

by means of (physical, legal, psychological) coercion, they can obtain the encryption keys to any encrypted content identifiable on the user's device. The security goal in this scenario, then, becomes to still retain secrecy of some selected, "crucial" data on the disk, by making the presence of such data not even identifiable, thus allow-

30th Anniversary 2023 acm SIGSAC

ACM CCS 2023

26-30 NOV., 2023

Who am I

Tommaso “tomgag” Gagliardoni

- PhD in cryptography at TU Darmstadt, Germany
- Post-doc at IBM Research Zurich, Security & Privacy Group
- Since 2019: cryptography researcher at Kudelski Security, Switzerland
- Focus on privacy, cryptography, quantum security

More business

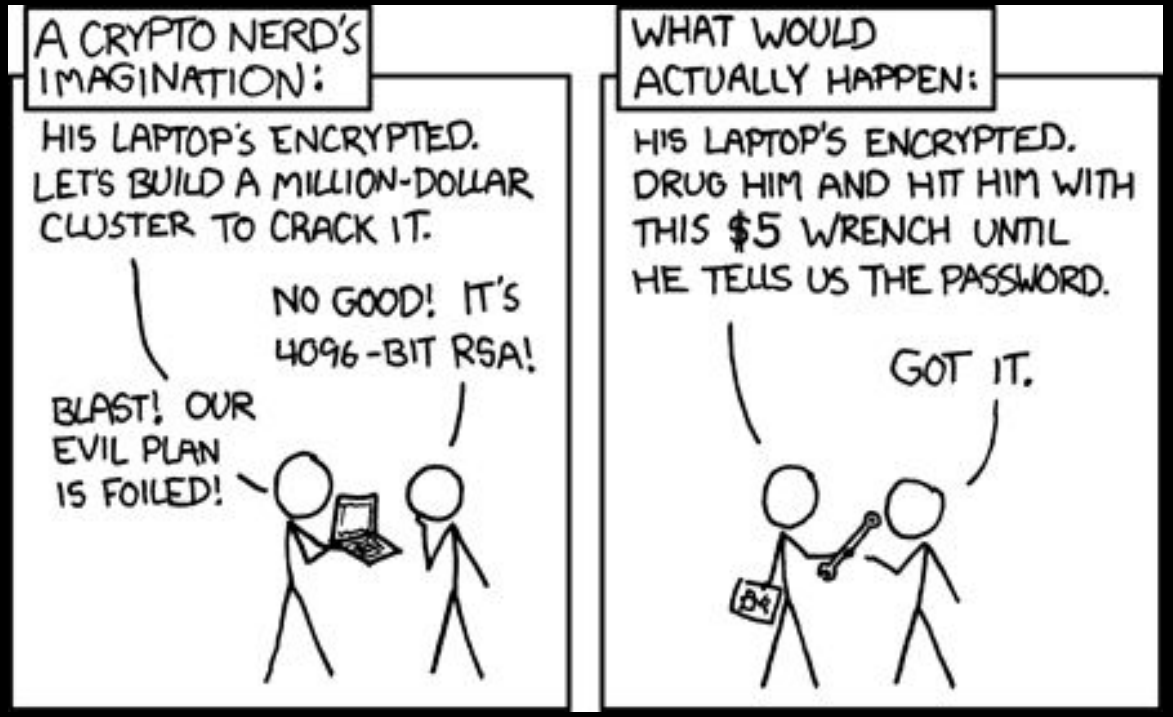
Less business

Overview

- TL;DR
- Bio
- Introduction
- TrueCrypt (and VeraCrypt)
- ORAMs and wo-ORAMs
- Shufflecake
- Implementation and benchmarks
- Future directions
- How to contribute

Introduction

- BitLocker (Windows)
- FileVault 2 (MacOS)
- LUKS (Linux)
- ...



Source: https://xkcd.com/538/

How bad is it?

Legislation by nation
Antigua and Barbuda
Australia
Belgium
Cambodia
Canada
Czech Republic
Finland
France
Germany
Iceland
India
Ireland
New Zealand
Poland
South Africa
Spain
Sweden
Switzerland

Key disclosure law

Article Talk

From Wikipedia, the free encyclop

Key disclosure laws, also known a

law enforcement. The purpose is t

Man jailed over computer password refusal

5 October 2010

Oliver Dr

A teenag
passwor

FRONTIER FOUNDATION

US v. Fricosu

EFF urged a federal district court in Colorado to block the government's attempt to force a woman to enter a password into an encrypted laptop, arguing that it would violate her Fifth Amendment

How a Syrian refugee risked his life to bear witness to atrocities

A few hours before leaving his home in Syria to begin a new life in Canada, Mostafa picked up a kitchen knife and began cutting into his left arm

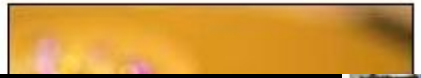
Why Cage director was guilty of withholding password

25 September 2017

Campaigners hit by decryption law

By Mark Ward
Technology correspondent, BBC News website

Animal rights activists are thought to be the first Britons to



TrueCrypt (and VeraCrypt)

TrueCrypt: one of the earliest, efficient full-disk encryption software (released 2004)

Troubled history, discontinued in 2014, replaced by VeraCrypt

Don't mess up with this guy lol

User data (FAT filesystem)

Empty Space (FAT16 Filesystem: Contiguous)

Normal (Disk Encryption) Mode

Decoy data (FAT filesystem)

Hidden Volume

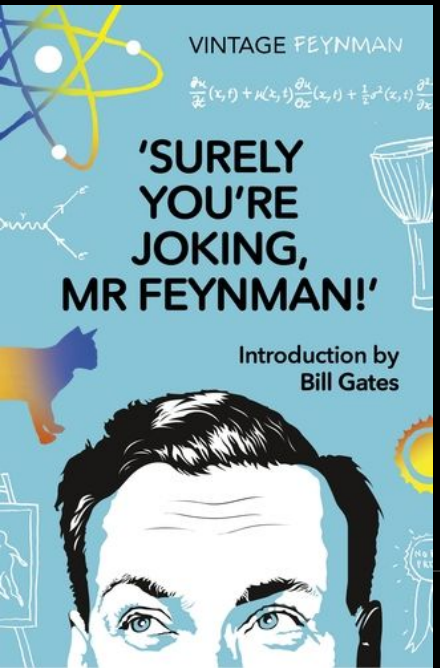
Plausible Deniability Mode

Who is this for?

- Repressed minorities in low-democracy countries
- Investigative journalists
- Whistleblowers
- Human right activists in repressive regimes

Problems with TrueCrypt

- Single-snapshot secure (more on this in a bit)
- Container must be FAT (old)
- Only 2 layers of secrecy (not enough)



Objections

- TrueCrypt is dead, we use VeraCrypt now Same.
- I still use FAT on my laptop
- I only use the FDE feature of VeraCrypt
- LUKS can do plausible deniability too, you just need to fill the disc with random data, make a bootable USB drive with your bootloader on it, make a LUKS header only file on that USB drive, and then create an encrypted filesystem on the disc using that detached header file. You'll want to backup that header file, and possibly hide it with another encrypted volume using a headerless encryption on the USB drive. It's OK as long as both the USB drive and the disc stay inside the pentacle you just painted on the floor with black chicken blood.

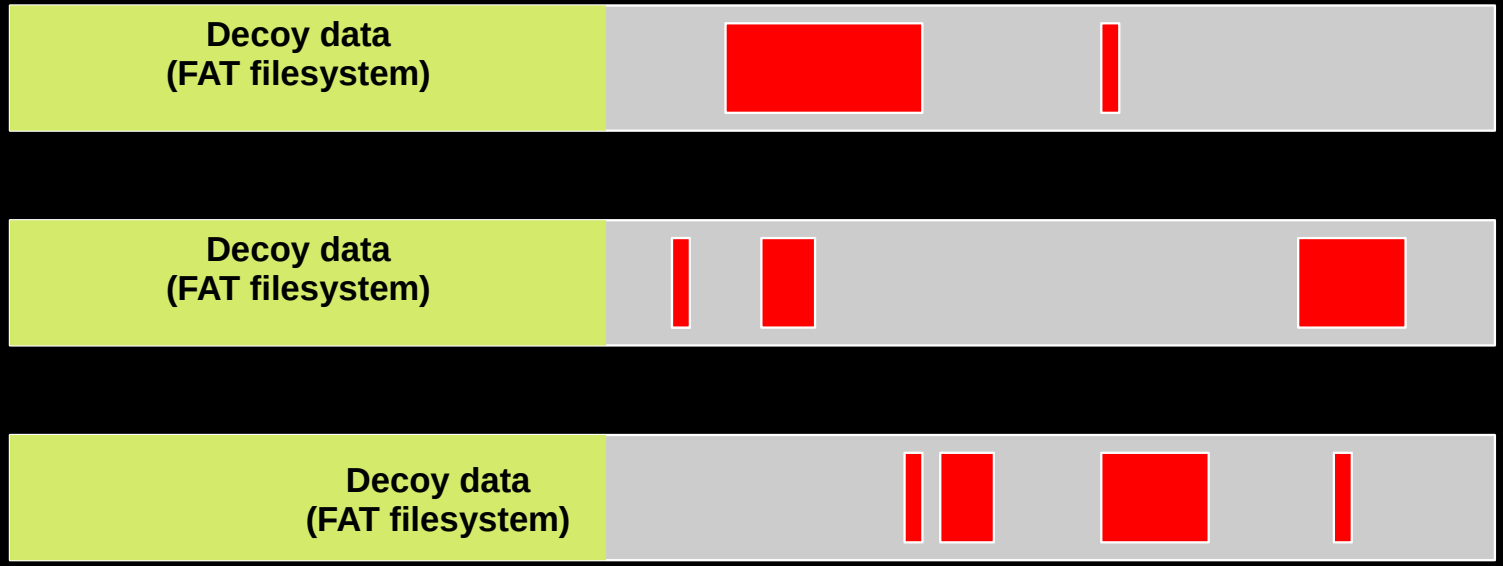
Let's talk about multi-snapshot

Physical volume (hard disk/partition)

Decoy data (FAT filesystem)	Empty space (?)

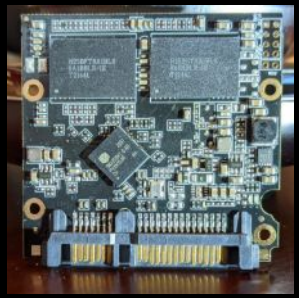
Let's talk about multi-snapshot

"modern" solid-state drives: caching / layering / TRIM



Can we do better?

- Long story short: multi-snapshot security is hard
- There are techniques to achieve it: ORAMs/woORAMs
- But they have extremely low performance
- Moreover, we think they overpromise

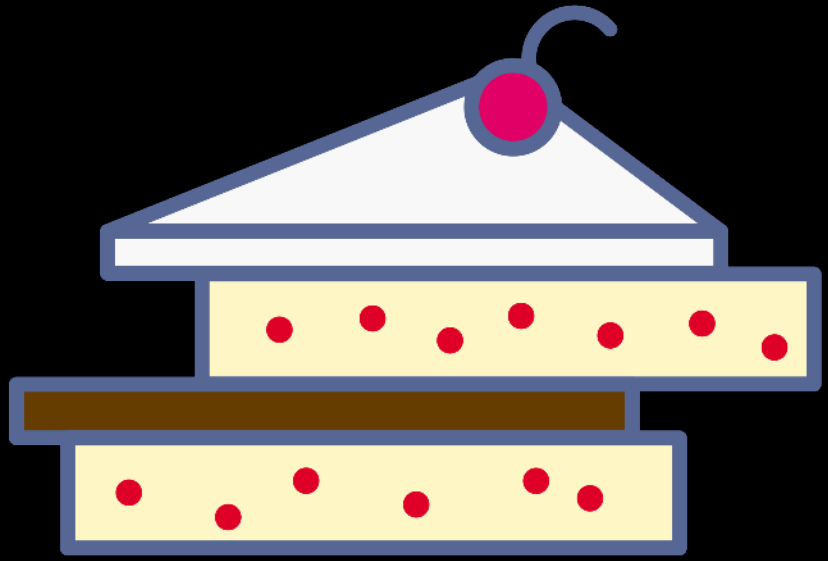


- How about practical / legal security?
- What if secure "with high enough" probability?
- What if I'm proved guilty with 2/3 probability?

- How about operational security?
- How about limitations on, e.g., FS type or number of layers?

Shufflecake

- Native for Linux
- File-System agnostic
- Many nested layers
- Concurrent volume use
- One password to open
- GPLv2 “or superior”



Shufflecake

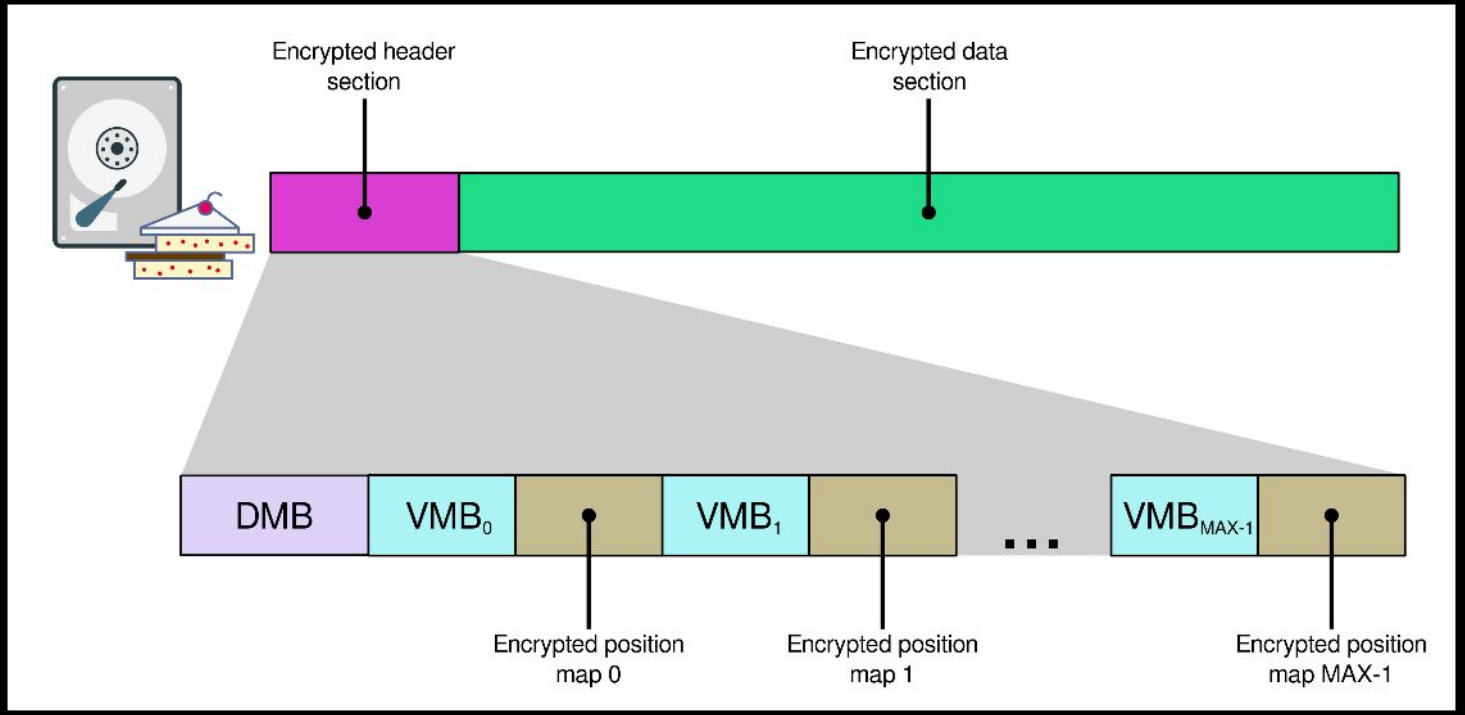
Operating Principles

- One device = multiple volumes (with concurrency)
- 1 volume = 1 password
- Volumes are numbered (from least to most secret)
- Unlocking volume N also unlocks volume N-1

Cryptography

- Well-established schemes (AES, Argon2)
- Cryptographic security proof (single-snapshot)

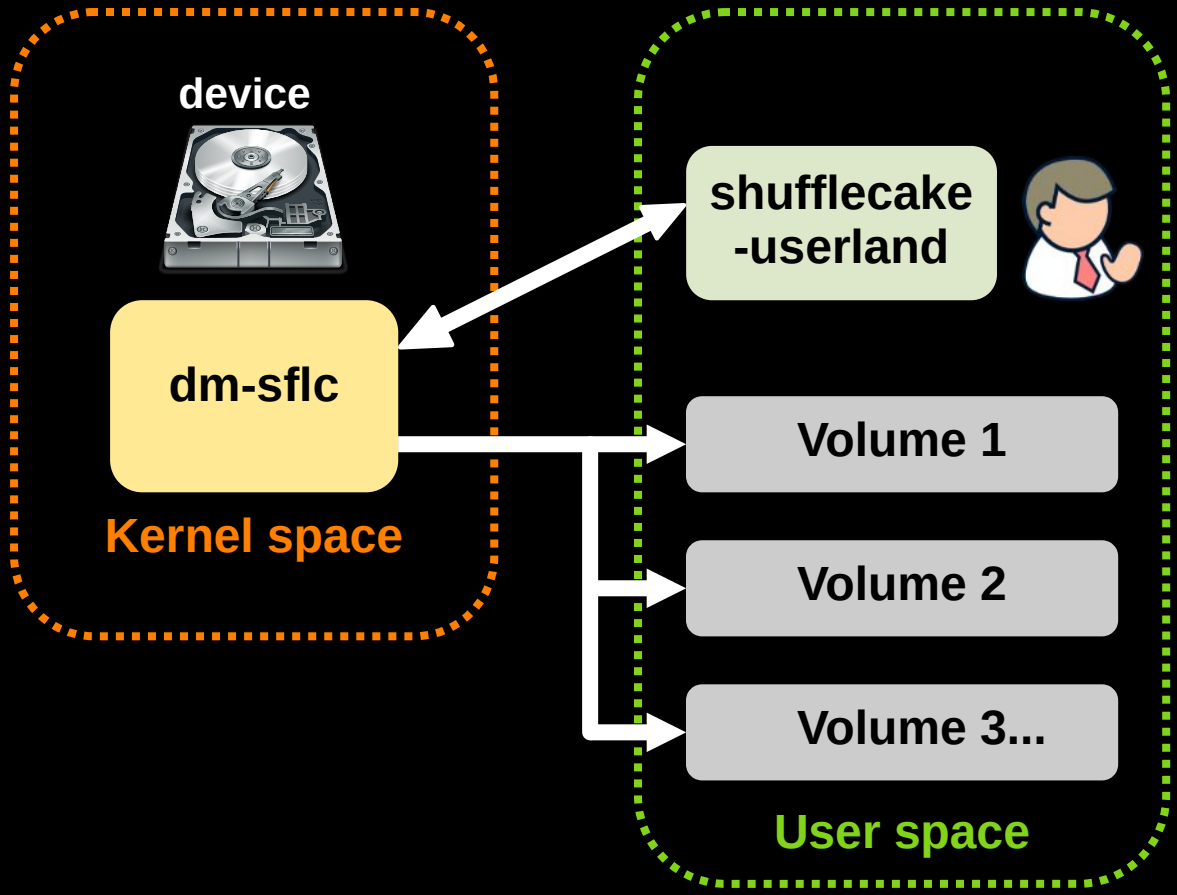
Shufflecake: disk layout



DMB = Device Master Block VMB = Volume Master Block

Header size: 60 MiB for a 1 TB device (worst case)

Shufflecake: implementation



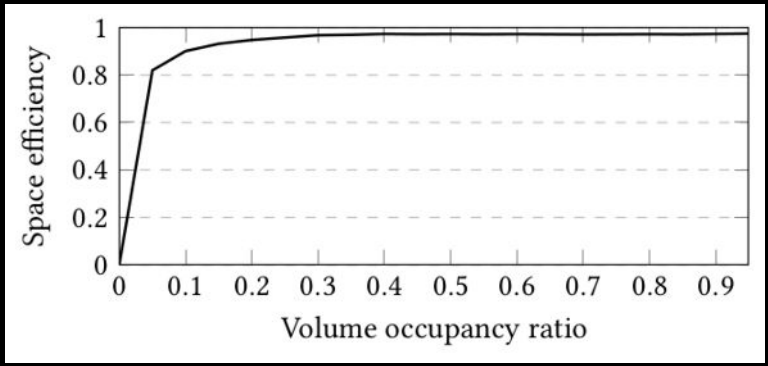
- Userspace can leverage more advanced crypto
- Also better for error handling, interfacing, etc
- Also use `/sys` for communication and stats
- Hidden volumes appear as `/dev/mapper/sflc_X_Y`
- They can be used as any other block device (formatted at wish, mounted, etc)

Shufflecake: implementation

- `shufflecake init <block_device>`
- `shufflecake open <block_device>`
- `shufflecake close <block_device>`

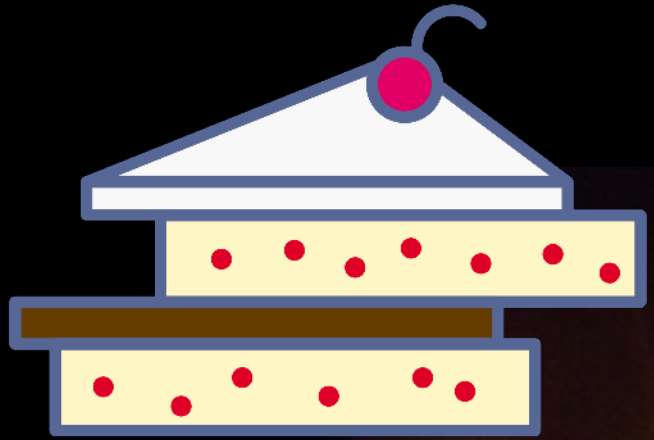
	Shufflecake	dm-crypt/LUKS	VeraCrypt
random write	26.77	38.43	39.07
random read	26.78	38.44	39.09
sequential write	176.87	247.14	247.75
sequential read	177.10	247.43	248.04

Table 1: I/O performance (in MB/s) of Shufflecake, dm-crypt/LUKS, and VeraCrypt.



- ~30% slower than LUKS/VeraCrypt
- Negligible waste of space

Future Directions



Chores and external contribution

Shufflecake is still an experimental, very low-level tool

- Expand testing to other Linux distros (now: Debian, Ubuntu)
- `make install`
- Distribute through DKMS
- Packetization (.deb, .rpm etc)
- Developer documentation

- Porting to Rust?
- GUI?
- Port to Windows/iOS?

Work in progress and plans

- Crash consistency
- (Partial) multi-snapshot security
- Shufflecake “Lite”
- Corruption resistance
- Use of volume metadata
- Reclaiming unused slices
- Hidden Shufflecake OS
- Shufflecake mobile
- Anti-safeword: unbounded number of volumes

How to contribute

- Code https://codeberg.org/shufflecake
- Mastodon @shufflecake@fosstodon.org
- Website https://shufflecake.net
- E-mail website@shufflecake.net
- Jabber xmpp:shufflecake@conference.draugr.de

Thank you for your attention!