

Design and Implementation of a Windows Kernel Driver for LUKS2-encrypted Volumes

I do not know yet whether I want to have
a subtitle, have a placeholder for now

MAX IHLENFELDT

Universität Augsburg
Lehrstuhl für Organic Computing
Bachelorarbeit im Studiengang Informatik

Copyright © 2021 Max Ihlenfeldt

This document is licensed under the Creative Commons
Attribution-ShareAlike 4.0 International Public License (CC BY-SA 4.0).

Abstract

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore e

Contents

1 Introduction	1
2 Background	2
2.1 LUKS2 Disk Encryption	2
2.1.1 On-Disk Format	2
2.1.2 Unlocking a Partition	4
2.1.3 Using an Unlocked Partition	6
2.2 Introduction to Windows Kernel Driver Development	7
2.2.1 Structure and Hierarchy of the Windows Operating System	7
2.2.2 The Windows Driver Model for Kernel Drivers	7
2.2.3 Communication Between Kernel and Userspace	7
3 Related Work	8
3.1 Measuring Filesystem Driver Performance	8
3.2 Cryptographic Aspects of LUKS2	8
4 Other Approaches	9
4.1 Linux Kernel Implementation of LUKS2	9
4.2 VeraCrypt	9
4.3 BitLocker	9
5 Design and implementation of our approach	10
5.1 Failed Attempts	10
5.2 The Final WDM Driver	10
5.2.1 Architecture	10
5.2.2 Initialization and Configuration	10
5.2.3 De-/encrypting Reads and Writes	10
5.2.4 Handling Other Request Types	10
5.3 Security Considerations	10
6 Performance of Our Driver	11
6.1 First Experiments	11
6.2 Final Experimental Setup	11
6.3 Results	11
7 Discussion	12
8 Conclusion	13
List of Figures	14
List of Tables	15
References	16

1 Introduction

Explain use case etc.

Note that in this thesis the terms *disk*, *drive*, *volume* and *partition* are used somewhat loosely and probably mean roughly the same.

2 Background

2.1 LUKS2 Disk Encryption

Linux Unified Key Setup 2, or short LUKS2, is the second version of a disk encryption standard. It provides a specification [1] for a on-disk format for storing the encryption metadata as well as the encrypted user data. Unlocking an encrypted disk is achieved by providing one of possibly multiple passphrases or keyfiles. The intended usage of LUKS2 is together with the Linux dm-crypt subsystem, but that is not mandatory¹.

The differences between the original LUKS and LUKS2 are minor. According to [1], LUKS2 adds “more flexible ways of storing metadata, redundant information to provide recovery in the case of corruption in a metadata area, and an interface to store externally managed metadata for integration with other tools.” Practically, this means that LUKS2 has a different on-disk layout and, among other things, supports more password hashing algorithms (more precisely, password-based key derivation functions).

The reference implementation² is designed only for usage on Linux, which is why we developed a new Rust library for interacting with LUKS2 partitions. This is not a full equivalent, but only a cross-platform helper. Its task is to take care of all the cryptographic work needed before actually decrypting and encrypting data. Notably, it lacks the following features of the reference implementation:

- formatting new LUKS2 partitions,
- modifying or repairing existing LUKS2 partitions,
- converting a LUKS partition to a LUKS2 partition,
- actually mounting a LUKS2 partition for read/write usage (this is what our kernel driver and its userspace configuration tool is for).

Our library does provide access to the raw decrypted user data, but the practical use of this is very limited: the decrypted data is in the format of a filesystem, e.g. FAT32, btrfs, or Ext4. Therefore a filesystem driver is needed to actually access the stored files. One way of exposing the decrypted data to the system’s filesystem drivers is by transparently decrypting the data directly in the kernel, which is what our driver does (see section 5).

2.1.1 On-Disk Format

Figure 1 shows the high-level layout of a LUKS2-encrypted disk.

The two binary headers have a size of exactly one sector, so that they are always written atomically. Only the first 512 bytes are actually used. The header marks the disk as following the LUKS2 specification, and contains metadata such as labels, a UUID, and a header checksum. The labels and UUID can be accessed using the `blkid`³ command-line tool and also be used in the `udev`⁴ Linux subsystem. For the detailed contents, see Figure 2. Figure 3 also contains an example hexdump of a binary header.

The sector containing the binary header is followed by the JSON area. This area arguably contains the metadata that is most relevant for decryption and encryption. Figure 4 contains an overview of the objects stored in JSON and their relationships. For

¹ As we show in this thesis, it is possible to make the combination of LUKS2 and Windows work.

² <https://gitlab.com/cryptsetup/cryptsetup>

³ <https://linux.die.net/man/8/blkid>

⁴ <https://linux.die.net/man/8/udev>

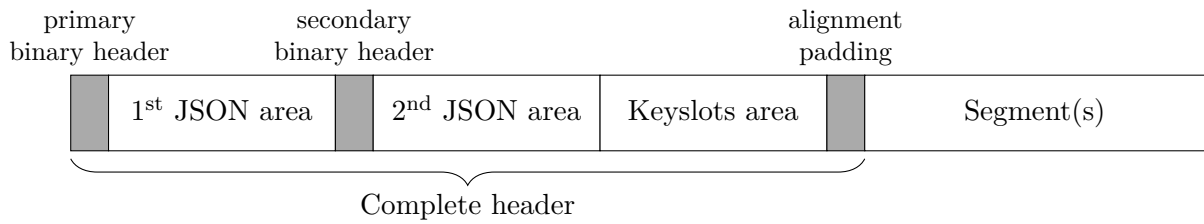


Figure 1: LUKS2 on-disk format (modified after [1]). The complete header consists of three areas: a binary header of exactly one 4096-byte sector, JSON metadata, and the binary keyslots data. A *keyslot* is an “encrypted area on disk that contains a key” [1]. For redundancy, the binary header and the JSON metadata are stored twice. After that follow one or areas containing encrypted user data. The specification calls these areas *segments*.

```
#define MAGIC_1ST "LUKS\xba\xbe"
#define MAGIC_2ND "SKUL\xba\xbe"
#define MAGIC_L 6
#define UUID_L 40
#define LABEL_L 48
#define SALT_L 64
#define CSUM_ALG_L 32
#define CSUM_L 64

struct luks2_hdr_disk {
    char    magic[MAGIC_L];           // MAGIC_1ST or MAGIC_2ND
    uint16_t version;                 // Version 2
    uint64_t hdr_size;                // size including JSON area [bytes]
    uint64_t seqid;                   // sequence ID, increased on update
    char    label[LABEL_L];           // ASCII label or empty
    char    csum_alg[CSUM_ALG_L];     // checksum algorithm, "sha256"
    uint8_t salt[SALT_L];             // salt, unique for every header
    char    uuid[UUID_L];             // UUID of device
    char    subsystem[LABEL_L];       // owner subsystem label or empty
    uint64_t hdr_offset;               // offset from device start [bytes]
    char    _padding[184];            // must be zeroed
    uint8_t csum[CSUM_L];             // header checksum
    char    _padding4096[7*512];      // Padding, must be zeroed
} __attribute__((packed));
```

Figure 2: LUKS2 binary header structure from [1]. Integers are stored in big-endian format, and all strings have to be null-terminated. The `magic`, `version`, and `uuid` fields are also present in the LUKS1 binary header and were placed at the same offsets as there.

this thesis’ brevity’s sake, please refer to Chapter 3.1 in [1] for an example of a LUKS2 JSON area.

After the JSON area, the keyslots area is stored on the disk. This is space reserved for storing encrypted cryptographic keys. The metadata from the JSON keyslot objects describe the position of a key on the disk as well as information on how to decrypt it.

0000	4C	55	4B	53	BA	BE	00	02	00	00	00	00	00	00	40	00	LUKS%.....@.
0010	00	00	00	00	00	00	00	03	54	68	69	73	20	69	73	20This is
0020	61	6E	20	41	53	43	49	49	20	6C	61	62	65	6C	00	00	an ASCII label..
0030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0040	00	00	00	00	00	00	00	00	73	68	61	32	35	36	00	00sha256..
0050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0060	00	00	00	00	00	00	00	00	EB	0F	D2	C6	E3	D2	8D	4Bë.ÔÆaÔ.K
0070	BB	2B	8A	49	E6	2E	4E	B7	04	2F	A9	39	76	71	8F	8A	>+ŠIæ.N../©9vq.Š
0080	33	E8	F3	90	FF	DC	4D	3D	E8	30	7B	37	01	30	E7	5D	3ëó.ÿÜM=ë0{7.0ç]
0090	AD	A0	57	1C	0E	63	BC	D4	DD	3C	EC	F5	DE	67	F8	D8	..W...c%ÖŸ<iôPgøØ
00A0	F2	7E	82	CD	B9	DD	77	10	65	39	33	64	63	61	66	61	ô-,í'Ýw.e93dcafa
00B0	2D	65	65	30	62	2D	34	31	36	38	2D	61	61	37	63	2D	-ee0b-4168-aa7c-
00C0	66	33	30	34	37	34	38	38	36	61	32	65	00	00	00	00	f30474886a2e....
00D0	54	68	69	73	20	69	73	20	61	6E	20	6F	70	74	69	6F	This is an optio
00E0	6E	61	6C	20	73	65	63	6F	6E	64	61	72	79	20	6C	61	nal secondary la
00F0	62	65	6C	00	00	00	00	00	00	00	00	00	00	00	00	00	bel.....
0100	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0110	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0120	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0130	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0140	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0150	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0160	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0170	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
01A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
01B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
01C0	91	A4	A9	83	03	FF	FB	68	4E	C2	94	6F	4C	78	71	AF	'm@f.ÿûhNÃ"oLxq~
01D0	AE	1A	91	F8	E0	2C	F3	71	D5	17	CB	60	E5	2F	D6	36	@. 'øã,ôqŮ.Ě 'ã/Ů6
01E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
01F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

Figure 3: LUKS2 binary header example. The fields, as described in Figure 2, were coloured differently to be easily distinguishable. A similar header, although with different salt and hash, can be generated by executing `fallocate -l 16M luks2.img && cryptsetup luksFormat --label 'This is an ASCII label' --subsystem 'This is an optional secondary label' --uuid e93dcafa-ee0b-4168-aa7c-f30474886a2e luks2.img` in a Linux shell.

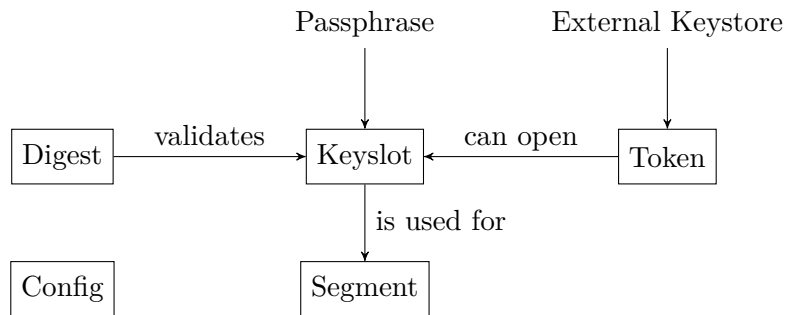


Figure 4: LUKS2 object schema from [1]. The most important objects are the following: *keyslots*, which describe the details of how cryptographic keys are stored and encrypted; *digests*, which can be used to verify that one has successfully extracted a key from a keyslot; and *segments*, which describe the disk areas where the encrypted user data is stored. Figure 1 shows where the areas described by the keyslot and segment objects actually lie on disk.

2.1.2 Unlocking a Partition

For simplicity, our LUKS2 Rust library does not support unlocking a keyslot using an external keystore defined by a token. Only unlocking via password is implemented. The library does however include support for different *password-based key derivation functions*

(*PBKDFs*), namely `pbkdf2` with SHA-256, `argon2i`, and `argon2id`. These are all the PBKDF algorithms that are listed in the LUKS2 specification (see [1], Table 3).

maybe [2] could be useful here?

The LUKS2 specification allows for multiple segments in one partition. To make things easier, our driver only supports unlocking one segment. Therefore, in this thesis we may speak of unlocking a partition and mean unlocking one of the partition's segments.

To unlock a segment means to derive the cryptographic key that is needed for reading decrypted or writing encrypted data. This key is called the segment's *master key*.

LUKS2 uses a process called *anti-forensic splitting* to store the master key on the disk. This method was introduced in [3]. It is used to diffuse the key's bytes into a longer sequence of bytes that has the following property: if at least one bit of the diffused sequence is changed, the key cannot be recovered. This is achieved by a clever combination of XOR and a hash function. The motivation behind this to make it easier (or possible) to dispose of an old key in such a way that it cannot be recovered from the disk. This is because it is much more feasible to partially erase a long sequence of bytes than to completely erase a short sequence. Erasing here means to overwrite the data in such a way that it cannot be recovered, which is not as trivial as one might think.

[3] calls the operation that splits data anti-forensically *AFsplit* and the recovery operation *AFmerge*. We will adhere to this convention (with slight variations).

To necessitate the need of a password to recover the key, the data is also encrypted before it gets written to the disk. The encryption key is a hash of the password obtained by a PBKDF.

The properties of anti-forensic splitting can be used when the user wants to change the password: the master key is derived using the old password and then re-encrypted with the new password. The key as it was encrypted with the old password can then be destroyed.

[3] presents two templates for storing keys, TKS1 and TKS2. The difference is whether the key is encrypted before or after splitting it. LUKS and LUKS2 use TKS2, which is schematically explained in Figure 5. The hash function used by LUKS2 for anti-forensic splitting is SHA-256.

explain multiple keyslots and deriving the same master key using different passwords

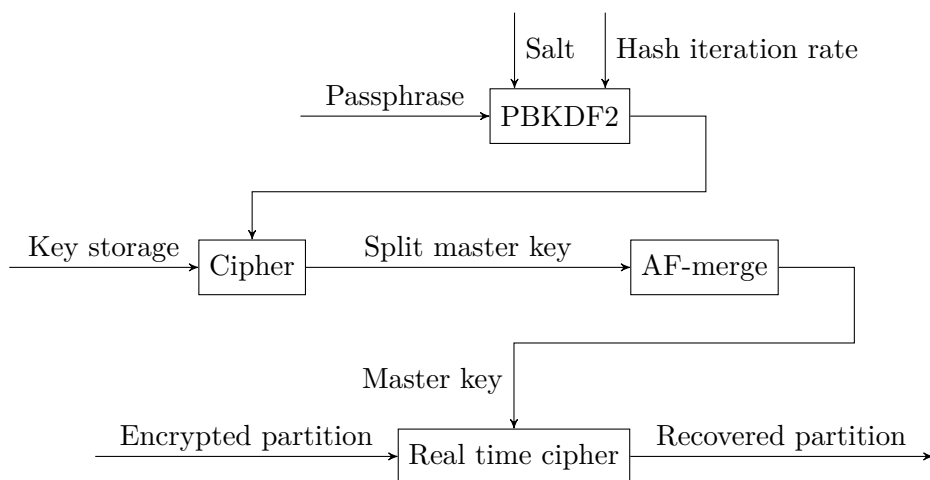


Figure 5: TKS2 scheme (modified after [3]).

For a more detailed pseudocode for the master key derivation see [4], Figure 5. Figure 6 shows the outline of an implementation of this process in Rust.


```

1  fn decrypt_keyslot(
2      password: &[u8], keyslot: &LuksKeyslot, json: &LuksJson, /* ... */
3  ) -> Result<Vec<u8>, LuksError> {
4      let mut k = vec![
5          0; keyslot.key_size() as usize * keyslot.af.stripes() as usize
6      ];
7      // read keyslot data from disk into k...
8
9      let mut pw_hash = vec![0; area.key_size() as usize];
10     match keyslot.kdf() {
11         // hash into pw_hash using pbkdf2, argon2i, or argon2id...
12     }
13
14     // decrypt keyslot area using the password hash as key
15     match area.key_size() {
16         32 => {
17             let key1 = Aes128::new_varkey(&pw_hash[..16]).unwrap();
18             let key2 = Aes128::new_varkey(&pw_hash[16..]).unwrap();
19             let xts = Xts128::<Aes128>::new(key1, key2);
20             xts.decrypt_area(&mut k, sector_size, 0, get_tweak_default);
21         },
22         // 64 byte key uses AES256 instead...
23     }
24
25     // merge and hash master key
26     let master_key = af::merge(
27         &k, keyslot.key_size() as usize, af.stripes() as usize
28     );
29     let digest_actual = base64::decode(json.digests[&0].digest())?;
30     let mut digest_computed = vec![0; digest_actual.len()];
31     let salt = base64::decode(json.digests[&0].salt())?;
32     pbkdf2::pbkdf2::<Hmac<Sha256>>(
33         &master_key, &salt, json.digests[&0].iterations(), &mut digest_computed
34     );
35
36     // compare digests
37     if digest_computed == digest_actual {
38         Ok(master_key)
39     } else {
40         Err(LuksError::InvalidPassword)
41     }
42 }

```

Figure 6: LUKS2 master key decryption in Rust. Some values are hardcoded: only the digest with index 0 is used (lines 29, 31, 33), and it is assumed that the digest algorithm is always pbkdf2 with SHA-256 (line 32). The latter is compliant with the specification, which lists this digest algorithm as the only option, but not optimal in the sense of input validation.

2.1.3 Using an Unlocked Partition

After a partition has been unlocked, i.e. after the master key of one of its segments has been decrypted, the partition is ready to be read from and written to. LUKS2 supports different segment encryption algorithms, see Figure 7 for a selection of them. Our driver only supports the default aes-xts-plain64 encryption. Therefore we will focus on that in this section.

The AES encryption algorithm is a block cipher for processing 128 bit data blocks [5]. To encrypt data longer than one block, a *block cipher mode* is needed [6]. These are encryption functions that build on a existing block cipher. When using aes-xts-plain64, LUKS2 uses the XTS block cipher mode [citation needed]. [6] for explaining IVs plain64 means “the initial vector is the 64-bit little-endian version of the sector number, padded with zeros if necessary.” [7] This sector number is relative to the first sector of the segment, i.e. the first sector is sector 0.

Algorithm in dm-crypt [7] notation	Description
aes-xts-plain64	AES in XTS mode with sequential IV
aes-cbc-essiv:sha256	AES in CBC mode with ESSIV IV
serpent-xts-plain64	Serpent cipher with sequential IV
twofish-xts-plain64	Twofish cipher with sequential IV

Figure 7: Selection of LUKS2 encryption algorithms (modified after [1]). See [7] for a detailed explanation of the different elements of the algorithm notation. cite/footnote for serpent/twofish/xts/cbc/essiv?

2.2 Introduction to Windows Kernel Driver Development

This section gives an introduction on the development of Windows kernel drivers and related important concepts.

2.2.1 Structure and Hierarchy of the Windows Operating System

Roughly summarize important concepts from chapters 1 and 2 of [8]

2.2.2 The Windows Driver Model for Kernel Drivers

Also explain how it gets loaded (if not done already)

2.2.3 Communication Between Kernel and Userspace

Via ports

3 Related Work

3.1 Measuring Filesystem Driver Performance

3.2 Cryptographic Aspects of LUKS2

[3]

Search for more papers, e.g. attacks against LUKS? e.g. [2]

4 Other Approaches

4.1 Linux Kernel Implementation of LUKS2

4.2 VeraCrypt

4.3 BitLocker

[9] and [10] and [11] and [12]

5 Design and implementation of our approach

5.1 Failed Attempts

FilterManager framework

Mention KMDF / UMDF and why we didn't use that if not already done in earlier section

5.2 The Final WDM Driver

Why WDM?

5.2.1 Architecture

5.2.2 Initialization and Configuration

luks2filterstart.exe

5.2.3 De-/encrypting Reads and Writes

custom AES implementation

make sure this chapter and subsection 2.1.3 are not too similar

LUKS2 supports many encryption algorithms (see [1], Table 4), but luks2flt only supports aes-xts-plain64.

```
VOID
EncryptWriteBuffer(
    PUINT8 Buffer,
    PLUKS2_VOLUME_INFO VolInfo,
    PLUKS2_VOLUME_CRYPTO CryptoInfo,
    UINT64 OrigByteOffset,
    UINT64 Length
)
{
    UINT64 Sector = OrigByteOffset / VolInfo->SectorSize;
    UINT64 Offset = 0;
    UINT8 Tweak[16];

    while (Offset < Length) {
        ToLeBytes(Sector, Tweak);
        CryptoInfo->Encrypt(
            &CryptoInfo->Xts, Buffer + Offset,
            VolInfo->SectorSize, Tweak
        );
        Offset += VolInfo->SectorSize;
        Sector += 1;
    }
}
```

5.2.4 Handling Other Request Types

5.3 Security Considerations

How does cryptsetup send the master key to dm-crypt?

6 Performance of Our Driver

6.1 First Experiments

6.2 Final Experimental Setup

6.3 Results

7 Discussion

8 Conclusion

List of Figures

1	LUKS2 on-disk format	3
2	LUKS2 binary header structure	3
3	LUKS2 binary header example	4
4	LUKS2 object schema	4
5	TKS2 scheme	5
6	LUKS2 master key decryption in Rust	6
7	Selection of LUKS2 encryption algorithms	7

List of Tables

References

- [1] M. Broz, *LUKS2 On-Disk Format Specification Version 1.0.0*, 2018, visited on 2021-07-31. [Online]. Available: https://gitlab.com/cryptsetup/LUKS2-docs/-/raw/861197a9de9cba9cc3231ad15da858c9f88b0252/luks2_doc_wip.pdf
- [2] V. Polášek, “Argon2 security margin for disk encryption passwords,” Master’s thesis, Masaryk University, 2019.
- [3] C. Fruhwirth, “New methods in hard disk encryption,” Ph.D. dissertation, Vienna University of Technology, 2005.
- [4] C. Fruhwirth, *LUKS1 On-Disk Format Specification Version 1.2.3*, 2018, visited on 2021-07-31. [Online]. Available: https://mirrors.edge.kernel.org/pub/linux/utils/cryptsetup/LUKS_docs/on-disk-format.pdf
- [5] National Institute of Standards and Technology, “Advanced Encryption Standard (AES),” U.S. Department of Commerce, Tech. Rep., 2001.
- [6] N. Ferguson, B. Schneier, and T. Kohno, *Cryptography Engineering – Design Principles and Practical Applications*. Wiley, 2010.
- [7] *dm-crypt: Linux device-mapper crypto target*, 2020, visited on 2021-08-06. [Online]. Available: https://gitlab.com/cryptsetup/cryptsetup/-/wikis/DMCrypt?version_id=ee336a2c1c7ce51d1b09c10472bc777fa1aa18cd
- [8] P. Yosifovich, D. A. Solomon, and A. Ionescu, *Windows Internals, Part 1: System architecture, processes, threads, memory management, and more*. Microsoft Press, 2017.
- [9] J. D. Kornblum, “Implementing BitLocker drive encryption for forensic analysis,” *Digital Investigation*, vol. 5, no. 3-4, pp. 75–84, 2009.
- [10] S. G. Lewis and T. Palumbo, “BitLocker full-disk encryption: Four years later,” in *Proceedings of the 2018 ACM SIGUCCS Annual Conference*, 2018, pp. 147–150.
- [11] S. Törpe, A. Poller, J. Steffan, J.-P. Stotz, and J. Trukenmüller, “Attacking the BitLocker boot process,” in *International Conference on Trusted Computing*. Springer, 2009, pp. 183–196.
- [12] C. Tan, L. Zhang, and L. Bao, “A deep exploration of BitLocker encryption and security analysis,” in *2020 IEEE 20th International Conference on Communication Technology (ICCT)*. IEEE, 2020, pp. 1070–1074.