HKT-SDL100

LoRaWAN Smart Door Lock User Manual

湖南华宽通科技股份有限公司
HUNAN HKT TECHNOLOGY CO., LTD.

Safe Operating Guidelines

- To protect the product and ensure safe operation, please follow this instruction manual. If the product is used improperly or not according to the manual, the company will not be responsible.
- Do not disassemble, change the internal wiring, or modify the product at will.
- Do not subject the device to strong shocks and vibrations.
- Do not place the product in an environment that does not meet the working temperature, humidity and other conditions, and keep it away from cold sources, heat sources and open flames .
- Do not install the product battery upside down, otherwise it may cause the product to burn out.

Disclaimer and Copyright Notice

Due to product version upgrades or other reasons, the contents of this manual may change. Hunan HKT Technology Co., Ltd. reserves the right to modify the contents of this manual without any notice or reminder. This manual is only used as a guide. Hunan HKT Technology Co., Ltd. does its best to provide accurate information in this manual, but Hunan HKT Technology Co., Ltd. does not guarantee that the content of the manual is completely error-free. All statements in this manual , information and advice do not constitute any express or implied warranty.

The products described in this manual may contain copyrighted software of Hunan HKT Technology Co., Ltd. and its existing licensors. Unless the permission of the relevant obligee is obtained, otherwise, without the written consent of the company, no unit or individual may Unauthorized excerpt, copy part or all of the content of this manual, and disseminate in any form.

contact us:

Email : sales1@hkttech.com

Address: No. 10 Qingshan Road, Changsha High-tech Development Zone, Hunan Province

Website: www.hkttech.com www.hktlora.com

Document revision history

Date	Version	Content
2023.8.10	V 1.0	First edition

Table of contents

1 Product introduction

1.1 Product introduction

HKT-SDL100 smart door lock is independently developed and designed by Hunan HKT Technology Co., Ltd. The door lock is easy to operate and easy to use, and uses voice broadcast to guide users to operate . At the same time, it supports 100 groups of passwords, 100 fingerprints, 100 cards, and small program temporary password unlocking, and supports unlocking records, alarm information, power report, temporary passwords and other functions. Both local and cloud can add and reset the unlock password, and use wireless LoRaWAN® communication technology to realize remote data transmission.

This smart door lock solution is very practical for the management of homestays, apartments, office buildings, house rentals and other fields. Users who have booked a room can check in only with the password issued by the owner, which saves the inconvenience and insecurity of key delivery, and the owner can grasp the check-in and check-out status of customers in real time.

Based on the application of the Internet and big data on the basis of the use of smart locks, it will greatly improve the operational efficiency of housing, apartments, office buildings, homestays and other leasing fields.

1.2 Product Highlights

- communication distance: the maximum communication distance can reach 5Km in an open environment
- Super long standby: low power consumption, easy to replace, use 4 AAA alkaline batteries, can be used continuously for 1 year
- Easy to operate : rich voice prompts, local operation will not get lost
- High security: C-level anti-theft lock cylinder, multiple alarm functions
- Powerful functions: support keys, fingerprints, passwords, cards to unlock, support

virtual passwords, temporary passwords

- Unlocking records: support local storage of more than 10,000+ historical operation records
- Good compatibility: Compatible with standard LoRaWAN® gateways and third-party network server platforms, supporting ad hoc networks
- Integrated management: quickly connect with Huakuantong LoRaWAN® gateway and cloud platform without additional configuration
- Three-dimensional appearance: the shell is simple and elegant

`

2 Product Structure Introduction

2.1 Packing list

1 ×
HKT-SDL100

1×
certificate

2 ×
Kits

2 ×
IC card

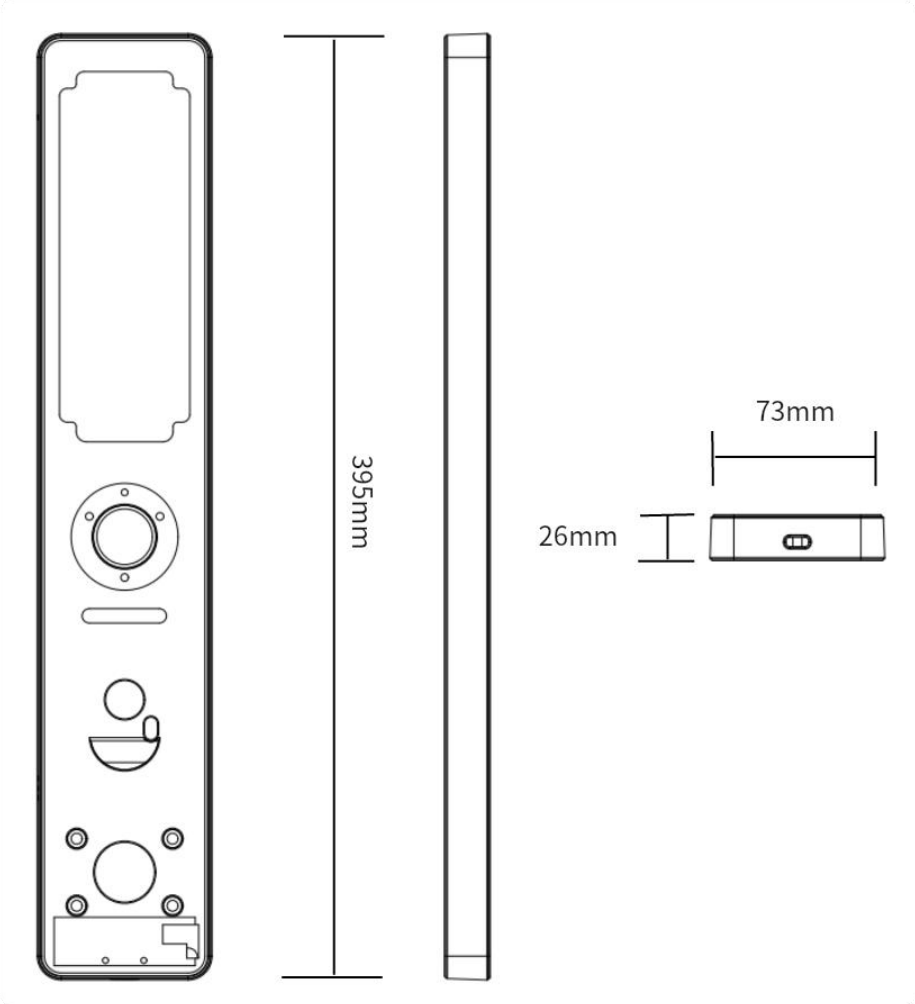
⚠ If the above items are damaged or missing, please contact your agent or sales representative in time.

Accessories Kit List

1) Door lock 55 straight mortise blade lock cylinder x 1;
2) key x 2;
3) Assembly screw x 1;
4) square stick x 1;
5) 5*110 flat head bamboo machine wire screws x 2;
6) 5*6*40 color silk tube x 2;
7) 7.4*0.4*30mm square axis magazine x 1;
8) Lock ruler section 8*90*2 x 1;
9) Steering screw x 2;

2.2 Appearance overview

2.3 Product size



3 Functional description

3.1 Initial state

- Any key/fingerprint can wake up the door lock;
- The door lock will be initialized when the power is turned on again. At this time, the keyboard light will light up "13579", and the operation can be performed when the keyboard light returns to full brightness.
- In the initial state, the administrator password is "123456";
- Enter the administrator mode: "*#+123456";
- "123456" is the factory default administrator password. After the administrator user is registered, the password will automatically become invalid. The next time you enter the system menu, you need to verify the registered administrator's fingerprint or password;

3.2 Operating instructions

3.2.1 Touch keyboard

- The device has 12 touch buttons, the corresponding numbers are "1, 2, 3, 4, 5, 6, 7, 8, 9, *, 0, #", and supports saving the record of the last 20 keyboard inputs, which can be Press the key to unlock with a password, manage user information and other operations. Supports storing up to 100 passwords. The system supports local management of adding and deleting passwords, and synchronizes them to the cloud platform;
- 【#】key is the confirmation key or the function key to enter the menu;
- The [*] key is the clear key/back key, short press to clear the input when entering the password;
- Press any key at will in the sleep state, there will be a voice message after waking up, and the first key input will not be triggered after waking up;
- It is recommended to wake up the screen and wait until the wake-up prompt is

over/the LEDs are all on before entering the key to avoid false triggering when sliding to wake up;

3.2.2 Unlock/Unlock

- Directly swipe the card/enter the password/fingerprint to open the door normally;
- Successful unlocking: Voice: Unlocked/motorized; the "*" button lights up after the motor finishes running. Press this button to immediately return to the lock. After returning to the lock, the "locked" sleeps. The method will become invalid and will be automatically restored after the lock is returned;
- Failed to unlock: the voice will play "error prompt tone" accompanied by "unlock failed";
- Deletion: After entering the password, press "*" to delete all the entered passwords, and press "*" to turn off the LED light if there is no password;
- Lock back: Automatically lock back after 5 seconds after unlocking, the voice broadcasts "locked", after unlocking, the "*" key lights up, press "*" to immediately lock back;

3.2.3 Unlock user management

- User information includes: fingerprint users (100), password users (100), card users (100); user ID numbers will correspond to user authority level information;
- User authority levels are divided into administrator users (management user number range: 000-009), common user number range: 010-099. Ordinary users cannot make relevant settings, but can only verify their identity to open the door; in addition to verifying and opening the door, administrator users can also enter the system configuration menu;
- User information can be added and deleted locally; password users support adding and deleting via cloud, and fingerprint users support cloud management and deleting;

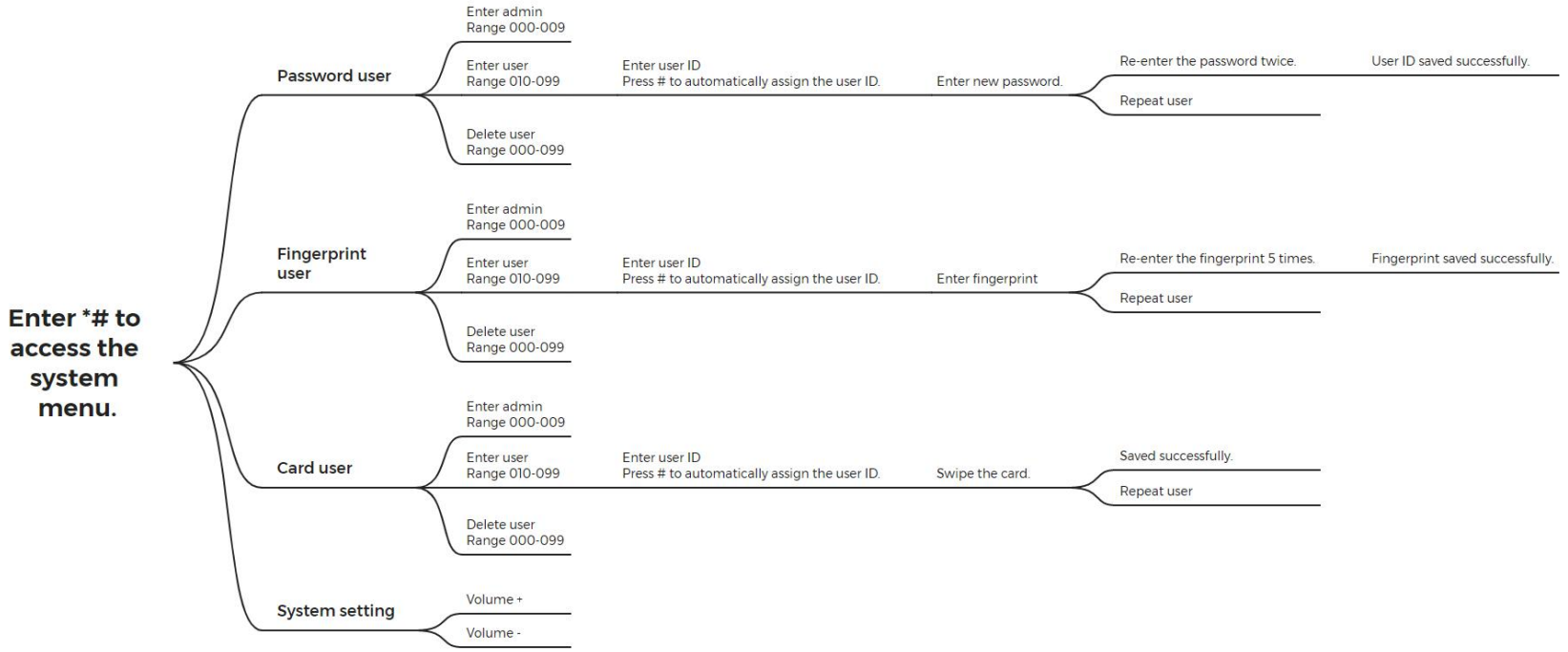
- If the operation is successful, there will be a voice prompt: "Operation successful";
- If the operation fails, there will be a voice prompt: "Operation failed";

3.2.4 System menu

- Enter the administrator menu: (enter *# to enter the system menu, at this time the voice prompts "Please enter the administrator information");
- Enter the system menu:
- Successful verification: enter the system menu and start to broadcast the system menu voice (1 password user, 2 fingerprint user, 3 card user, 4 system setting);
- Verification failed: Voice broadcast "Operation failed" and prompt "Please enter administrator information";
- Lock the screen after 5 continuous input errors for 3 minutes;
- In the case of no input, it will automatically exit and enter dormancy after 10s;
- Under the system menu, every time you press the button corresponding to the function, it will voice broadcast "this function" again with "confirm, please press #, return please press *"; and light up the white light of "*" and "#"; again Press "#" to enter the specific function of the submenu;

3.2.5 Manage keys

- Select the corresponding method in the system menu, and complete the system operation with the voice prompt;
- Note: Enter the management user number range: 000-009; input the common user number range: 010-099; you cannot delete yourself when deleting user information;
- When prompted to enter the user ID, press "#" to automatically assign the ID, the administrator starts from "000", and the common user starts from "010" to fill in the blank;



3.2.6 Other functions

- System lock: When verifying the unlock or verifying the authority to enter the system menu, if there are 5 wrong input in any way, the system will be locked for 100S, and the keyboard light will count down within 100S;
- Local key synchronization: every time a local password is added or deleted, the operation record will be saved, and the latest version will be synchronized to the cloud platform after accessing the network; the downlink of the cloud platform will overwrite the local key operation;
- When the device stores too many passwords, the device may take too long to load during the startup initialization stage, and it can be used normally after the startup is stable (keyboard lights are all on);
- The device supports false passwords, you can add irrelevant codes before and after the correct password (such as: XXX password XXX, the correct password must be entered continuously), and then press the [#] key to confirm;
- After 10 seconds of no further operation on the setting page and verification page, the system will automatically exit;

3.3 Anti-tamper button

- The device has 1 button, which is used to monitor whether the door lock has been pried open, abnormal installation conditions, etc.;
- After the tamper is triggered, the door lock will report the alarm sound all the time (the trigger is invalid if the password is not entered), and send the alarm information to the platform, which can be released by verifying the user;

3. 4 USB interface

- The device has a type-c USB data interface, which can be used to power the device or transmit data.

- The user can plug into the computer through the USB interface to communicate with the upper computer to modify some configuration parameters of LoRa, and can export historical data or trigger records.

3.4 Local data storage

The product provides 512KB storage space to store more than 10,000+ operation records, and supports exporting stored data through local software.

3.5 Working mode

- **Data reporting**
  - The device establishes a connection with the platform based on the LoRaWAN communication method, and reports the triggered data. By default, the device configuration information is synchronized every 24 hours (the reporting interval can be configured through the platform);
  - When a new event (unlock, alarm, tamper) occurs, the display data will be updated immediately, and the data will be reported to the cloud platform.
- **Power detection**
  - The device will report power information by percentage at regular intervals;
- **Working frequency**
  - The device supports LoRa multi-band wireless communication capabilities at home and abroad, and the following are the working frequency bands supported by the device

    CN470\IN865\EU868\US915\AU915\AS923 (If you need to customize the frequency band, please contact the supplier) .
- **Anti-drop mechanism**
  - The device will check whether the data packets are successfully sent according to the reporting interval, and will re-enter the network after a certain number of sending failures.

4 Parameters

Model No.		HKT-SDL100
configuration	keyboard light	12
	button	12 touch buttons + 1 reset button (built-in)
	fingerprint	1
	Card	1
	Bluetooth	1 (optional)
	interface	1 USB Type-C interface (emergency power supply)
	doorbell function	have
	Tamper alarm	have
	amount of users	300 (fingerprint, password, card)
fingerprint	Fingerprint detection time	< 1s
	False recognition rate of fingerprint module	< 0.0001%
	Fingerprint module rejection rate	< 0.1%
password	normal password bits	6~8 digits
	false password	20 bits
credit card	Card type	13.56MHz complies with IOS/IEC14443 (such as M1 card)
	Checking distance	0-15mm
wireless parameters	letter of agreement	Standard LoRaWAN ® 1.0.2 protocol
	Working frequency	EU868 (CN470\IN865\US915\AU915\AS923 is optional)

	transmit power	18.5±1dBm (max)
	Super high receiving sensitivity	-13 5±1 dBm @ SF=12
	Network access/work mode	OTAA/ABP Class A
	LoRaWAN port	Default 10 (1-233)
	Equipment EUI	LoRaWAN® device, which can be found on the product label.
	App EUI	App EUI of the device, the default value is 083FBC0065000001.
	application key	The default application key (App Key) used by OTAA to access the network is 2D35C7963275D743B4E73BEA91681A3B.
configuration	configuration method	server or serial port
	software function	Low battery reminder , IAP (firmware upgrade)
physical properties	Power supply	4 AAA high-capacity alkaline batteries
	battery life *	>1 year (10 unlocks/day)
	Operating temperature	-10°C ~60°C
	Working humidity	20%~ 90% (no condensation)
	size	395*73*26mm
	Adapt to door type	Wooden door, anti-theft door, copper door
	Adapt to door thickness	40-120mm
	Door opening times	More than 5000 times
	main material	Aluminum alloy + tempered glass
	color	elegant black

Notice:

（1）If you purchase a large number of equipment, you can contact Hunan Huakuantong to obtain the equipment EUI and other parameter tables.

（2）If you need a random App Key, please contact Hunan Huakuantong before purchasing.

（3）If you use the cloud to manage HKT-SDL100 series devices, please use OTAA to access the network.

（4）The LoRa frequency band used to send data must generally match the frequency band used by the LoRaWAN® gateway.

5 Data communication protocol

5.1 Communication protocol data structure

All data are expressed in HEX format

sync head 3 bytes	special type 1bytes	package serial number 1 bytes	type of data 1bytes	data n bytes	N (data type + data) 1+n+1+n+...

5.2 Analysis of communication protocol

Field name	Description
header	The synchronization header is fixed 3 bytes length data (0x68 0x6B 0x74), taken from "hkt".
special type	The special type is fixed 1 bytes length data , and the specific function is represented by BIT bit; BIT0: Used to inform the device or server whether a response or confirmation packet is required (0: no response 1: response required); BIT1~BT17: Function to be determined.
package serial number	The packet serial number is data with a fixed length of 1 bytes , which is used to identify the packet serial number .
type of data	The data type is fixed 1 bytes length data, which is mainly used to identify different functional types of data of the device.

data	The data is n bytes variable length data, and the length of the data content is confirmed according to different data types.

5.3 Data Type Table

type of data	Function	Remark
0x01	Device software and hardware version	The data length is fixed at 2 bytes, and the uplink is automatically synchronized when the power is turned on again, and only uplink is supported The first 1 byte represents the hardware version, and the last 1 byte represents the software version Example: Sync hardware version 1, software version 5: 68 6B 74 00 01 01 01 05
0x03	Device power information	Upload by battery percentage, only supports uplink Example: Synchronized battery information: 68 6B 74 00 03 03 64 (battery 100%)
0x2E	Manage unlock codes	The data length is fixed at 11 bytes, supporting uplink and downlink data[0]: operation command 0 add/modify 1 delete 2 read (local operation by the user when the device is uplink) data[1]: user number (number 0 is the super administrator) data[2]: password length 6~8 data[3-10]: ASCII code password, if there are not enough 8 digits, add zero before the password and send it

		reply data[0]: operation instruction FF operation is successful, FE operation is failed data[1]: user number (number 0 is the super administrator) data[2]: password length 6~8 data[3-10]: ASCII code password, if there are not enough 8 digits, pad zero before the password Example: 1. The new number 1 password is 123456: 68 6B 74 00 01 2E 00 01 06 00 00 31 32 33 34 35 36 The device responded that the addition was successful 68 6B 74 00 01 2E 00 01 06 00 00 31 32 33 34 35 36 Delete the number 2 password: 68 6B 74 00 01 2E 01 02 00 00 00 00 00 00 00 00 00 The device responds that the deletion is successful 68 6B 74 00 01 2E FF 02 00 00 00 00 00 00 00 00 00 Read number 3 password 68 6B 74 00 01 2E 02 03 00 00 00 00 00 00 00 00 00 The device responds that the read is successful, the password length is 6, and the password content is 123456 68 6B 74 00 01 2E FF 03 06 00 00 31 32 33 34 35 36
0x2F	remote unlock	The data length is fixed at 1 bytes, and only supports downlink 0 = remote unlock Example: Request device remote unlock: 68 6B 74 00 01 2F 00
0x30	Door lock operation record report	The data length is fixed at 6 bytes, and only supports uplink data[0]: 0x01: fingerprint to open the door 0x02: Password to open the door 0x03: MF card to open the door 0xC1: fingerprint alarm

		0xC2: password alarm 0xC3: MF card alarm 0xC4: tamper alarm 0xC5: LoRa remote unlock 0xC6: Bluetooth near-field unlocking data[1]: user number data[2-5]: Timestamp (GMT) Example: Fingerprint to open the door 68 6B 74 00 01 30 01 63 AE 57 D4
0x31	Management Card and Fingerprint	The data length is fixed at 3 bytes, supporting uplink and downlink data[0]: operation command 0 synchronization (only uplink) 1 delete 2 read data[1]: user number (number 0 is the super administrator) data[2]: type 0 card 1 fingerprint reply data[0]: operation instruction FF operation is successful, FE operation is failed data[1]: user number (number 0 is the super administrator) data[2]: valid or not 0 valid 1 invalid/not entered/deleted Example: delete card number 1 68 6B 74 00 01 31 01 01 00 The device responds that the deletion is successful 68 6B 74 00 01 31 FF 01 01 Read the fingerprint status of number 1 68 6B 74 00 01 31 02 01 01 The device responds that the read is successful and valid 68 6B 74 00 01 31 FF 01 00

0x32	active sync/ temporary password	The data length is fixed at 11 bytes, supporting uplink and downlink (temporary passwords are issued during downlink) 0 = Synchronize cloud data (the device actively presses 1# to initiate) server reply data[0 -1]: Valid duration (in minutes, the maximum time is 24 hours) data[2]: password length 6~8 data[3-10]: ASCII code password, if there are not enough 8 digits, pad zero before the password Example: The user actively presses 1# to initiate a cloud data synchronization request 68 6B 74 00 01 3 2 00 The server responds with a temporary password of 123456, valid for 30 minutes 68 6B 74 00 01 32 0 0 1E 06 00 00 31 32 33 34 35 36
0x80	Synchronize system time	Uplink data bits are invalid, downlink time format: year, month, day, hour, minute, second When the device goes up through this command, it is a request command. At this time, the server should downlink the correct time to the device. Example: Request server to synchronize system time: 68 6B 74 01 01 80 Server downlink synchronization system time (2022/03/28/12:00): 68 6B 74 00 08 80 16 02 1C 0C 00
0x85	Restore default factory settings	Downlink command, uplink is invalid 1 = Reset device to factory settings

		Example: Downlink the server to restore the device to factory settings: 68 6B 74 00 0A 85 01
0x86	Data Synchronization Period	Synchronize the device status to the server interval, the data length is fixed at 2 bytes, and supports uplink and downlink Unit: minute Value range: 10-1440 (10 minutes to 24 hours), the default is 24 hours, when set to 0, the data will not be actively synchronized. Example: Set the data synchronization interval to 1440 minutes: 68 6B 74 00 01 86 05 A0

5.4 Examples

Device synchronization software and hardware version information

68 6B 74 00 01 01				
sync head	**special type**	**package serial number**	**type of data**	**data**
68 6B 74 (sync header)	00 (no confirmation package required)	01	0 1	01 05 (hardware version 1 & software 5)

Notice:

(1) The device information is reported once when it is connected to the network or restarted;

(2) For an example of a data parser, please refer to: "sdl-100.js " .
https://github.com/HKT-SmartHard/decode .