Design of data encryption storage module for coal mine law enforcement record terminal

Qiwei Li1,2,3,4
1CCTEG China Coal Research Institute, Beijing 100013, China
2Engineering Research Center for Technology Equipment of Emergency Refuge in Coal Mine, Beijing 100013, China
3Beijing Mine Safety Engineering Technology Research Center, Beijing 100013, China
4E-mail: liqiwei@ccrise.cn

Abstract. Coal mine law enforcement record terminal is mostly used in Android operating system. Aiming at the data security problem of Android system, this paper designs a data encryption storage module based on ThreadX real-time operating system with i.MX RT1021 processor as the core. This paper introduces the hardware and software design of the encryption storage module in detail. Using DSA data encryption algorithm, combined with the characteristic information, through the actual test, this storage module realizes the reliable encryption storage of audio, video and text data of the law enforcement record terminal, which can effectively prevent the electronic evidence from being tampered with.

1. Introduction
The law enforcement record terminal has the functions of shooting, taking pictures, recording, data uploading, etc., which has been widely used in public security, fire protection and other fields. It plays an important role in recording the implementation, collecting evidence, and standardizing law enforcement, which has a good reference for the national coal mine safety supervision institutions to use the law enforcement record terminal in the process of coal mine safety supervision and law enforcement [1].

Android system can easily achieve human-computer interaction, audio, video capture, text entry and other functions, and Android operating system is widely used in the field of mobile intelligent terminal, so the coal mine law enforcement record terminal mostly uses this system. Due to the open source feature of Android system and the lack of strict audit and self-discipline mechanism for the release of Android applications, system vulnerabilities and malicious code pose a serious threat to data security [2-3], in order to prevent the data of the law enforcement recorder from being tampered or deleted, this paper designs a data encryption storage module, which only opens the read or write permission to the upper Android system, and does not allow the data to be modified or deleted after being written into the module.

Android system can write video, audio, image, text and other data to the encrypted storage module through the special communication interface. The module integrates and encrypts the above data with the current time stamp, location information, power information, user information and other characteristic data. The encrypted storage module solves the threat to data security caused by Android system vulnerability and malicious code, and can effectively prevent data from being tampered with or...
deleted. The connection mode between the encrypted storage module and Android motherboard is shown in Figure 1.

![Connection mode between encrypted storage module and Android motherboard.](image)

Figure 1. Connection mode between encrypted storage module and Android motherboard.

### 2. Hardware design of encrypted storage module

The encrypted storage module is mainly composed of power supply circuit, main control unit, storage circuit and interface circuit with Android system motherboard.

#### 2.1. Power circuit design

The rated power supply voltage of the main control chip and peripheral circuit of the encryption memory module is 3.3V. A 10Ah lithium iron phosphate battery is built in the law enforcement recorder, and its voltage range is 2.8V~3.6V. Therefore, a buck boost type is needed to convert the battery voltage to 3.3V. In this design, LTM8045 step-down boost type μ module regulator produced by ADI company is used. LTM8045 has built-in power devices, power inductors, control circuits and some passive components. Its peripheral design is relatively simple, only need to configure input and output capacitors, and a number of resistors to set its output voltage and switching frequency. In order to reduce the impulse current when power on, the soft start function of LTM8045 is also enabled. The schematic diagram of power supply circuit is shown in Figure 2.

![LTM8045 buck boost circuit.](image)

Figure 2. LTM8045 buck boost circuit.

#### 2.2. Main control unit

In this application, i.MX RT1021 produced by NXP semiconductor company is adopted, which is supported by arm ARM Cortex-M7 kernel, with a running frequency of 500MHz, supporting full function floating point unit (FPU) and VFPv5 architecture. i.MX RT1021 also has various memory interfaces, including SDRAM, RAW NAND flash, NOR flash, SD/eMMC, four channel SPI, and various connection interfaces, including UART, SPI, I2C, USB and CAN. It also has a built-in 10/100M Ethernet controller to support IEEE1588, which fully meets the application requirements.
2.3. Memory circuit
The main control chip i.MX RT1021 is integrated with the uSDHC (Ultra Secured Digital Host Controller) host controller, which can drive SD/SDIO/MMC card.

i. The main features of the uSDHC peripheral of MX RT1021 are as follows:
- Support SD/SDIO specification, up to 3.0 version;
- MMC system specification is supported, up to version 4.5.
- Supports 1-bit/4-bit SD and SDIO modes, 1-bit/4-bit/8-bit MMC mode

In SDR mode, 4 parallel data lines are used, and the data transmission rate of SDXC card can reach up to 800Mbps. Based on the above characteristics, SDXC card can be used as storage medium, which can fully encrypt and store video, audio, image and text data transmitted by Android host in real time. The connection diagram of SDXC card and i.MX RT1021 master control chip is shown in Figure 3.

Data pin DATA3 hardware does not add pull-down resistance. If DATA3 pin is needed as card detection, the corresponding GPIO needs to be configured as pull-down mode.

![Figure 3. Connection diagram of i.MX RT1021 and SDXC card.](image)

2.4. Host interface with Android system
Android system host should write video, audio, image, text and other files to the storage encryption module, which is large and lasts for a long time. The normal serial port or SPI communication mode is difficult to meet the requirements. In this application, Ethernet interface is used to realize communication with Android host. When communication is conducted, the storage encryption module is server side and Android host is client. Ethernet PHY chip is LAN8720A, which is connected with MAC inside i.MX RT1021 through RMII interface. i.MX RT1021 provides 50MHz clock source for LAN8720A. The interface circuit with Android host is shown in Figure 4.

![Figure 4. Interface circuit with Android host.](image)

3. DSA data encryption algorithm
SA(Digital Signature Algorithm) signature algorithm is an American federal information processing standard about digital signature proposed by National Institute of standards and technology. DSA is a more advanced data verification method. It not only has public key, private key, but also digital signature,
which can be used for digital signature and authentication. The private key encrypts to generate digital signature; the public key is used to verify data and digital signature, and the role of digital signature is to verify whether the data is modified in the transmission process [7-8].

The process of digital signature and authentication in DSA is as follows:

- Generating digital digest: the sender uses message digest algorithm to encrypt the data to be sent, so as to generate digital digest.
- Form digital signature: the sender re-encrypts the digest with his private key to form a digital signature.
- Data transmission: the sender transmits the original text and encrypted abstract to the receiver at the same time.
- Digest decryption: after receiving the data, the receiver decrypts the digest with the sender's public key, and generates the same digest with the message digest algorithm for the received data.
- Summary comparison: the receiver compares the decrypted summary with the re-encrypted summary after receiving the data. If the two are consistent, it means that the information is not damaged or tampered in the process of transmission. Otherwise, the information has lost its security and confidentiality.

The principle of DSA encryption and digital signature is shown in Figure 5.

![Figure 5. DSA digital signature principle block diagram.](image)

4. Software programming

4.1. ThreadX SMP RTOS

This storage module needs to receive a large amount of data through the network port and encrypt the storage in real time. It has high requirements for real-time and security. In this storage module, ThreadX real-time operating system is used for task scheduling and management. ThreadX is an advanced industrial real-time operating system designed for deep embedded, real-time and IoT applications. Because of the non-hierarchical microkernel architecture and tailorable of ThreadX kernel, the minimum space of ThreadX only needs 2KB Flash space and 1KB RAM space. ThreadX provides advanced scheduling, communication, synchronization, timer, memory management and interrupt management functions. In addition, thread has many advanced functions, including microkernel architecture, Preemptive Threshold Scheduling, event chain, runtime performance analysis, performance indicators and system event tracking. ThreadX is an ideal choice for demanding embedded applications [9-10].
ThreadX real-time operating system has perfect middleware, including file system Filex, network protocol stack NetX, USB protocol stack USBX, trace debugging software TraceX, etc. ThreadX and all its middleware have obtained high-level security certification in medical, industrial, automotive, aerospace and other industries, which fully meet the application requirements of this module.

The encrypted storage module communicates with Android motherboard through Ethernet interface. The TCP/IP protocol stack can use NetX, the middleware of ThreadX real-time operating system. NetX supports HTTP, MQTT, SNMP, FTP, TFTP and other communication protocols\(^\text{[11]}\). In this application, the data interaction between the encrypted storage module and Android motherboard is realized through FTP protocol.

### 4.2. System initialization thread design

The main function of the system initialization thread is to initialize the hardware peripherals and ThreadX operating system after the system is powered on, initialize the necessary kernel components such as Filex and NetX, and finally mount the memory card. The flow chart is shown in Figure 6.

#### Figure 6. System initialization thread flow chart.

```
Start

Initialization of storage module peripherals

ThreadX system initialization

Initialize system components such as Filex and NetX

Initialize and mount the memory card

End
```

#### Figure 7. Data transceiver storage encryption thread.

```
Start

Received audio, video, text data?

No

Yes

Get current system time

Get current location information

DSA digital signature encryption

Store to encrypted data

End
```

### 4.3. Design of data encryption storage thread

After receiving the audio, video and text data from Android motherboard, the storage module immediately obtains the system time and current location information at that time, encrypts it with DSA digital signature, and then stores the encrypted data in the memory card. The flow chart is shown in Figure 7.
5. Conclusion
This paper introduces an encryption storage module with i.MX rt1021 processor as the core, which can be used in the coal mine law enforcement record terminal. After obtaining audio, video and text data, combined with the current time information, location information, terminal physical properties and other characteristic information, DSA digital signature encryption algorithm is adopted to realize the reliable encryption storage of electronic evidence and ensure the data security. Through practice, the encryption storage module can also be applied to other products or fields that need data encryption storage.

Acknowledgments
Thanks for the financial support of the state key scientific research project 2018YFC008304.

References
[1] Xu Feng. Effect of law enforcement recorder on enhancing the effectiveness of fire supervision and law enforcement [J]. Journal of Guangxi University for Nationalities(Natural Science Edition), 2016, 22(S1):158-160.
[2] Liufei Chen. Communication and Information Systems [D]. University of Electronic Science and Technology of China, 2019.
[3] Yitian Zhang. Design and implementation of mobile application reinforcement system on Android Platform[D]. Beijing University of Posts and Telecommunications, 2015.
[4] Analog Devices:LTM8045: Inverting or SEPIC \(\mu\) Module (Power Module) DC/DC Converter with Up to 700mA Output Current Data Sheet [EB/OL]. 2021-3-15.https://www.analog.com/cn/products/ltm8045.html.
[5] NXP Semiconductors; i.MX RT1020 Crossover Processors for Consumer Products [EB/OL]. 2021-3-15.https://www.nxp.com.cn/products/processors-and-microcontrollers.
[6] WU Jun-jie,WU Jian-hui. Implementation of Ethernet MAC MII Interface to RMII Interface [J]. Chinese Journal of Electron Devices, 2008(2):712-715.
[7] Hengwu Li, Chenyang Wang, Hui Guo. Application of data encryption technology in computer network communication security[J]. Electronic Technology & Software Engineering, 2020,188(18):238-239.
[8] Yuxin Guo. Encryption algorithm of network communication system[J]. Telecom World, 2019,(26)04,7-9.
[9] Yingjin Pan, Ziyuan Zhu. Development of USB Device Driver Based on ThreadX Real Time Operation System [J]. Industrial Control Computer, 2016, 29(2): 30-32.
[10] Liu Wuyang. Design of I2S Audio Bus Driver Based on ThreadX System[J]. Microcontrollers & Embedded Systems, 2018,18(01):61-66.
[11] ZHANG Jiong, LV Zi-xu, LIU Dong, et al. Analysis of Real Time Operating System: ThreadX [J]. Computer Technology and Development, 2008, 129(01): 22-24+29.