ResearchInChina
www.researchinchina.com

China Automotive Cybersecurity Hardware Research Report, 2022

Oct.2022

Cybersecurity hardware research: security chip and HSM that meet the national encryption standards will build the automotive cybersecurity hardware foundation for China.

1. OEMs generally adopt the security chip + HSM strategy to build their cybersecurity protection system.

At the core of cybersecurity hardware are security chip and hardware security module (HSM). Security chip, or secure element (SE), is an integrated circuit that integrates cryptographic algorithms and features physical attack prevention design.

Hardware security module (HSM) is a computer device used to protect and manage the keys and sensitive data applied by the strong authentication system, and also provide related cryptographic operations. It is the basic support for automotive security solutions.

At present, most OEMs employ the security chip + HSM strategy to build an automotive cybersecurity protection system.

For example, in its automotive cybersecurity security system, NIO uses security chips and HSM to reinforce hardware and networks; in terms of secure communication, the HSM and certificate system featuring integrity, encryption, pseudonymization and anonymity is the basis for enabling data privacy protection. In addition, bug fixes over the air (OTA) are available in the case of emergency.

GAC completes the hardware security design and creates the four systems of border protection, automotive security, PKI certification & transmission, and security services, using security chip (SE) + HSM, and secure boot, trusted zone and encryption technologies. And at the vehicle end, GAC conducts in-depth research on vehicle inside and outside multi-node security protections, such as Linux OS for T BOX 4G module, Android OS for vehicle head unit, QNX OS for gateway and MCU, and communication interaction, aiming to establish an in-depth protection system for in-vehicle security.

2. Homemade SE chips are mass-produced and applied in vehicles.

As the US passed CHIPS Act, the localization of semiconductors in China assumes greater urgency. More chip equipment, materials and industrial software among others will be homemade. The cybersecurity hardware market is no exception. The need for local security chips that conform to the national encryption algorithms is a pressing problem.

In current stage, Tongxin Micro's automotive-grade security chips are often used in the Internet of Vehicles, and are being tried out in small batches by Chinese manufacturers. They are expected to be mass-produced during 2023-2024. In the future, Tongxin Micro's SE chips will head in the direction of vehicle controllers that meet higher vehicle driving safety and product performance requirements. Following the completion of development and testing of samples of key products in this series in 2022, the research and development is expected to be fulfilled around 2025.

Major Automotive Cybersecurity Chip Vendors in China (Part)

Major Automotive Cybersecurity Chip Vendors in China (Part)

Vendor	Chip Model	Encapsulation	Interfaces (Max.)	Encryption Algorithms	Application Fields	Certification
Tongxin Micro	TMC-T97-315E	QFN32(5*5)	SPI: 8M, 7816 Interface	AES, ECC, RSA, SM2, SM3, SM4, SM9, SHA256	Digital car key, etc.	CC EAL5+, IT EAL4+, Commercial Encryption Grade 2, AEC-Q100 Grade 2
	TMS-T97-131A	QFN32(4*4)	SPI: 8M, IIC: 100kbps, 7816 Interface	AES, RSA, ECC, SM2, SM3, SM4, SHA256ButterflyKey Derivation, AES-GCM, SM4-CCM	Vehicle V2X encryption chip	CC EAL6+, IT EAL4+, Commercial Encryption Grade 2, AEC-Q100 Grade2
	TMS-T97-111A	QFN32(4*4)	SPI: 8M, IIC: 100kbps, 7816 Interface	AES, RSA, ECC, SM2, SM3, SM4, SHA256	Vehicle connected communication, data encryption, identity authentication, etc.	CC EAL6+, IT EAL4+, Commercial Encryption Grade 2, AEC-Q100Grade2
CEC Huada Electronic Design	CIU98_B	QFN32 (5*5)	7816, SPI	3DES, AES, RSA, ECC, SM1, SM2, SM3, SM4, SM9, SHA_n	TBOX SE, etc.	
Tianjin C*Core Technology	CCM3310S-T		EPORT*16, USB, SPI*2, I2C, UART Interface (SCI), ISO7816*3	SM3, SHA-0, SHA-1, SHA-224, SHA-256	ETC, OBD, TBOX	Commercial Encryption Grade 2, CNITSEC EAL4+, AEC-Q100
Fudan Microelectronics	FMSE	SOP8, DFN12	I2C, SPI, ISO7816	TDES, AES, SSF33, RSA, ECC, SHA1, SHA224, SHA256, SM1, SM2, SM3, SM4, SM9 Algorithms	China Phase VI TBox, vehicle center console, etc.	AEC-Q100, National Encryption Grade 2 EAL4+
Hongsi Electronic Technology	HSC32C1	SOP8, DFN8, QFN20	7816, SPI, I2C, UART	National Encryption Algorithms: SM2, SM3, SM4 International Encryption Algorithms: ECC, AES, SHA, DES	China Phase VI OBD, T-BOX, vehicle terminals, etc.	Commercial Encryption Grade 2, AEC-Q100 Grade 2
Datang Microelectronics	DMT-CBS-CE3D		ISO7816, ISO14443	Support Both International and National Encryption Algorithms	ETC	AEC-Q100 Grade 2
Thinktech	Mizar TTM20	LQFP64, QFN64 (TBD)	SPI*1, GPIO*2	RSA (up to 2048bit), ECC-256, SHA-256, AES, DES, SM2, SM4, SM3	Vehicle terminals	National Encryption Grade 2, AEC-Q100 Grade 1
Suzhou C*Core Technology	CCM3310S-T	/	EPORT*16, SPI*2, I2C, UART (SCI), USB, ISO7816*3	• Public Key Algorithm Engine: Support 1024bit RSA/2048bit RSA; Support 256bit SM2 Prime Field • Symmetric Algorithm Engine: DES/3DES Supports ECB/CBC Mode; AES Supports ECB/CBC/CFB/OFB Mode; SM4 Supports ECB/CBC/CFB/OFB Mode • Digest Algorithm Engine: SM3; SHA-0/ SHA-1/ SHA-224/ SHA-256	ETC, OBD, TBOX	• Commercial Encryption Grade 2 • CNITSEC EAL4+ • AEC-Q100
Xinda Jiean Information Technology	XDSM3275	/	SD / SPI, etc.	National Encryption Algorithms: SM1, SM4, SM2, SM3, etc. International Encryption Algorithms: 3DES, AES, RSA1024, RSA2048, SHA256, etc.	V2X, etc.	EAL5+
	XDSM3276					EAL5+, Commercial Encryption Grade 2, AEC-Q100 Grade 1
	XDSM1505					Commercial Encryption Grade 2, AEC-Q100 (being certified)

Mass Production Capacity

Despite a large number of companies, their mass production capacity is limited. Only a few players like Tongxin Micro and CEC Huada Electronic Design have products largely mounted on vehicles in the OEM market. Nations Technologies has mass-produced products for the aftermarket covering T-BOX, driving recorder, vehicle diagnosis, in-vehicle infotainment and navigation, vehicle ambient lighting, and 360-degree panoramic view.

Tongxin Micro was established by the national second-generation resident ID card chip R&D team at the Institute of Microelectronics of Tsinghua University. Its T9 Series security chips that were introduced into homegrown vehicle models in 2021 have been spawned and used in T-BOX, V2X, eUICC, China Phase VI OBD, and digital car keys, building a four-in-one trustworthy application environment for connected vehicles, that integrates cybersecurity, payment security, communication security, and identity authentication security.

Currently Tongxin Micro's automotive-grade security chips are largely seen in the Internet of Vehicles, often not involving vehicle driving safety, with a relatively short assessment and certification cycle. Chinese manufacturers have the chips on trial in small batches, which are projected to be produced in quantities during 2023-2024. In the future, Tongxin Micro's SE chips will head in the direction of vehicle controllers, involving high vehicle driving safety and product performance requirements, with a relatively long certification period. The key products in this series, with samples developed in 2022, are being tested, and the research and development is expected to be completed around 2025.

CEC Huada Electronic Design is a group company formed by CEC integrating its integrated circuit companies. In 2019, CEC Huada Electronic Design made a foray into telematics security chips. Its telematics solutions based on its high security SEs are led by:

* The in-vehicle security involves the security protection of vehicle bus, ECU, OBD, TBOX and IVI system. The SEs deployed on key nodes guarantee the link security of the in-vehicle network and TSP platform.
*For V2X security, devices such as on-board unit (OBU) and roadside unit (RSU) use the integrated SEs to store the unique network access identifier, registration certificate and application certificate; the verification of communication message signatures is a solution to such problems as protocol cracking, illegal authentication and privacy leakage in the direct connection environment.

CEC Huada Electronic Design's series of automotive-grade security chip products have been spawned and launched on market, with more than 8 million units having been pre-installed and deployed in commercial vehicles and passenger cars.

Typical model of Most HSM players are foreign companies, and the SecIC-HSM based on national encryption algorithms will become an application direction.dual display: Haval Shenshou

3. Most HSM players are foreign companies, and the SecIC-HSM based on national encryption algorithms will become an application direction.

HSM providers are mainly foreign companies including Thales, Entrust Datacard, Utimaco, ATOS SE, Exceet Secure Solutions GmbH, Securosys, Ultra Electronics, Synopsys, Futurex, Marvell Technology Group, and Yubico. Typical application solutions are also from these foreign players, for example, the HSM framework in Infineon's AURIX chip and Vector's HSM firmware solution.

In the context of the hindered global semiconductor industry chain, the demand for homemade HSM and solutions in China is bound to rise. Westone and Sansec are among the few HSM providers in China. The SecIC-HSM Series security modules created by Shanghai Uni-Sentry adopt the HSM security stack that uses national encryption algorithms, support mainstream chips used in production vehicle models, and are compatible with chips of NXP and ST and domestic mainstream domain controllers, meeting the technical requirements of vehicle controller security.

SecIC-HSM Series of Shanghai Uni-Sentry

Solutions	• **Technical requirements of vehicle controller security:** with years of experience in AUTOSAR and cybersecurity, the company launched HSM firmware products and provides standard interfaces that can be integrated with AUTOSAR software and support mainstream chip types such as Infineon and NXP. • **Independent encryption and decryption functions:** meet the authentication requirements for in-vehicle key ECU communication data in SecOC application scenarios; implement commercial cryptographic algorithms such as SM2, SM3 and SM4 by driving hardware accelerators; and provide different levels of encryption protections according to functional requirements to improve the execution efficiency of the cryptographic calculation process. • **Independent key storage module:** support such functions as Secure Boot, Secure Debug, Secure Data and Secure Log, so as to enable secure boot, secure refresh and secure communication.
Highlights	• HSM acceleration module: the independent HSM acceleration module enables the high-speed execution of the encryption and decryption process, and six times higher performance, meeting the requirements of real-time communication. • Flexible firmware: the modular and scalable software components can improve the flexibility of firmware, support multiple national encryption algorithms, and allow automatic configuration of encryption parameters, making it easy to adapt to various needs and functions. • Higher security: advanced security algorithms and key extraction methods are used to improve security.
Features	• **Low cost**: support multiple encryption algorithms, e.g., national encryption algorithms, without additional chip cost. • **Provide the parameter configuration page and standardized interface:** automatically configure encryption parameters, and easily call the HSM firmware. • **Easily adapt to various needs and functions:** modular and scalable software components are used to improve firmware flexibility; both the encryption algorithms and the number of keys can be customized, making it easy to fit various needs and functions.

Source: Shanghai Uni-Sentry

The providers of software and hardware integrated solutions walk at a faster pace in application to vehicles.

4. The providers of software and hardware integrated solutions walk at a faster pace in application to vehicles.

In terms of mass production, providers of software and hardware integrated solutions go ahead of simple SE chip vendors.

Since 2015, Zhengzhou Xinda Jiean Information Technology Co., Ltd. has signed agreements with BYD, AIWAYS, BAIC, Ingeek and Suzhou Zhito Technology among others, providing customized cybersecurity solutions as they require.

In addition, Xinda Jiean provides V2X security chips that comply with national encryption standards and supporting security services for its partners Huawei and Lear, in a bid to support Audi's next-generation V2X intelligent connected vehicle project.

Project	Signing Time	Partner	Main Content
Joint R&D Agreement on Intelligent Vehicle Security Solutions	Sept. 2015	BYD	(1) Intelligent vehicle security solutions: Xinda Jiean provides BYD with security chips, mobile terminal protection systems, secure access systems and supporting technical services, based on which BYD establishes its intelligent vehicle cybersecurity system. (2) Intelligent vehicle services: Xinda Jiean provides BYD with vehicle terminal remote security management services and application remote management services.
Technical Service Contract	May 2019	AIWAYS	Xinda Jiean provides the project implementation services for cybersecurity integrated solutions based on the MAS861 vehicle "terminal-pipe-cloud" system architecture.
Zotye Automotive Security System Platform Project Construction	Jul. 2019	Zotye	Zotye entrusts the development of components for the B21 model to Xinda Jiean, to build a vehicle security system platform.
Technology Development Contract on Automotive Cybersecurity Development Project Based on V2X Technology	Dec. 2019	Beijing Automotive Research Institute	Establish the automotive cybersecurity project development based on V2X technology to build systematic security solutions.
Framework Cooperation Agreement	Dec. 2019	Shanghai InGeek Cyber Security	Build technical cooperation on PKI/CA in SAIC Volkswagen's digital key project.
Strategic Cooperation Framework Agreement	Apr. 2020	Suzhou Zhito Technology	They build in-depth cooperation in the fields of intelligent connected vehicle cybersecurity, security chips and V2X.

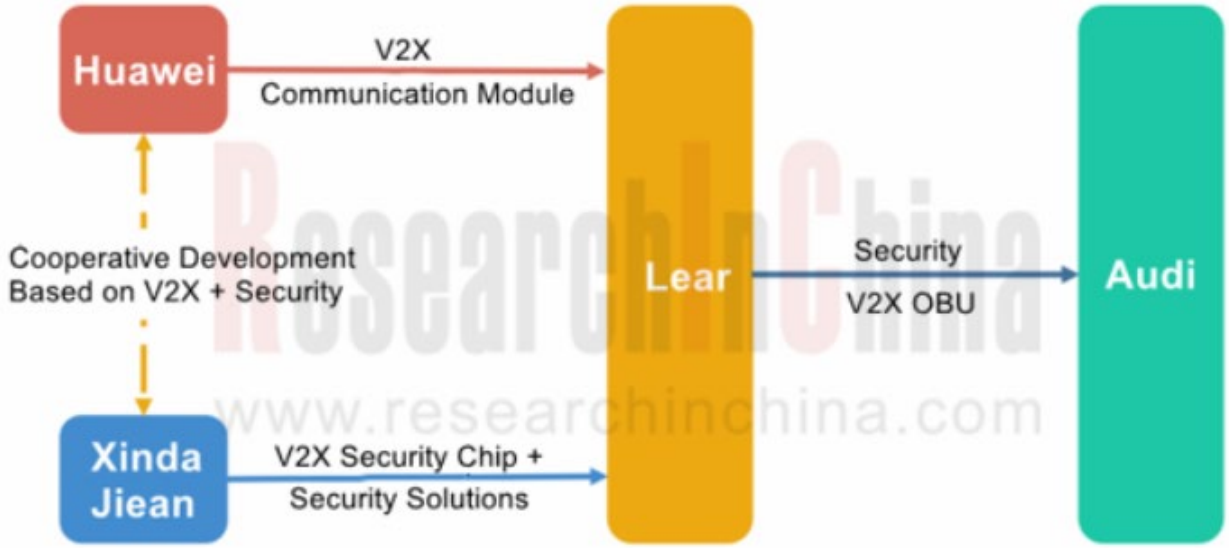
Source: Xinda Jiean

Highlights of China Automotive Cybersecurity Hardware Research Report, 2022

China Automotive Cybersecurity Hardware Research Report, 2022 combs through China's automotive cybersecurity hardware system and highlights the following:

- Automotive cybersecurity system architecture and the range of key hardware products, with vehicle systems as the main object;
- Cybersecurity policies, regulations and standard systems (the main content and certification process of ISO21434 and R155, and the process and planning of Chinese standards and regulations);
- Automotive SE security chips (features, application scenarios, and major Chinese and foreign vendors);
- Features and application solutions of automotive hardware security module (HSM);
- OEMs' construction of cybersecurity systems and application of hardware modules.

Cooperation Model between Huawei, Xinda Jiean, Lear and Audi



Source: Xinda Jiean

Table of Content (1)

Table of Content (2)

Contact

Beijing Headquarters
TEL: 010-82601561, 82863481
Mobile: 137 1884 5418
Email: report@researchinchina.com

Website:
www.researchinchina.com

WeChat: zuosiqiche

zuosiqiche

Chengdu Branch

TEL: 028-68738514
FAX: 028-86930659