

6G内生安全可信技术白皮书

6G Endogenous Security&Safety
and Trustworthy Technology White Paper

网络通信与安全紫金山实验室

国家数字交换系统工程技术研究中心

移动互联网安全技术国家工程研究中心

2023年1月



6G

来 6G 界
岛
6G 供 50 5G 4G
5G
无 现
现 健
6G 底 服
施
6G 未来
供 服 在 施 6G
2030 界 供
服 6G 沿
健 6G

现
 底 本
 本
 3G 4G 5G 施 服 无
 供 底
 服 供 国家
 供 服
 6G 现 6G 现
 现
 产
 施
 6G 现 现
 6G 健
 击 国家 6G
 当 国在 6G 域 在 域
 无 界
 家 底
 6G
 国 国

本 主 保护
本 来 6G
2023 1

主

强

1.	6G	底	1
1.1	6G		1
1.2	6G		4
1.3	6G		6
2.	6G		9
2.1	6G	主	9
2.1.1		击	9
2.1.2		无	10
2.1.3		失	11
2.1.4		AI	11
2.1.5			12
2.2	6G		12
2.3		Four Key Pillars	14
2.3.1			16
2.3.2			17
2.3.3		保护	19
2.3.4		供	21
2.4		Four Enabling Factors	22
2.4.1		Structuring	22

2.4.2	Customization	23
2.4.3	Intelligentize	24
2.4.4	Automation	25
2.5	本 (Four Basic Properties)	26
2.5.1	Designability)	26
2.5.2	Perceibility	27
2.5.3	Metrizability	28
2.5.4	Evolvability	29
3. 6G		30
3.1		30
3.2		33
3.3 无		35
3.4		38
3.5		40
3.6		42
3.7		44
3.8 供		46
4.		49
		50

1		6
2	6G	13
3	6G	16
4		18
5		19
6	CMP	20
7	云 供	21
8	DHR	31
9	6G	34
10	无	36
11		42

3GPP	3rd Generation Partnership Project	
5GIA	5G Infrastructure Association	5G 施
AES	Advanced Encryption Standard	
AI	Artificial Intelligence	
AKA	Authentication Key Agreement	
API	Application Programming Interface	
APT	Advanced Persistent Threat	
ARM	Advanced RISC Machine	RISC
B5G	Beyond 5G	5G
CD	Continuous Deployment	
CI	Continuous Integration	
CMD	Cyberspace Mimic Defense	
CMP	Credibility, Mobility, and Privacy	
CPS	Cyber-Physical Systems	
CPSoS	Cyber-Physical Systems of Systems	
DevOps	Development and Operations	

DevSecOps	Development, Security, and Operations	
DHR	Dynamic Heterogeneous Redundancy	
ECC	Elliptic Curve Cryptography	
FP7	7th Framework Programme	
ICT	Information and Communications Technology	
IMT-2030	International Mobile Telecommunications-2030	国 -2030
KEM	Key Encapsulation Mechanism	
KPI	Key Performance Indicator	
KVM	Kernel-based Virtual Machine	
ML	Machine Learning	
NFV	Network Functions Virtualization	
NICT	National Institute of Information and Communications Technology	本
NIST	National Institute of Standards and Technology	国国家
NSF	National Science Foundation	国国家
PQC	Post Quantum Cryptography	
PKI	Public Key Infrastructure	施
QC	Quantum Cryptography	
QKD	Quantum Key Distribution	
RAN	Radio Access Network	无

RINGS	Resilient & Intelligent NextG Systems	NextG
RIS	Reconfigurable Intelligent Surface	
SBA	Service Bases Architecture	服
SDL	Security Development Lifecycle	
SEPP	Security Edge Protection Proxy	护
SUCI	Subscription Concealed Identifier	
TEE	Trusted Execution Environment	
ZUC	ZU Chongzhi	



1.安全是6G的基石底座

6G内生安全可信技术白皮书

6G Endogenous Security&Safety and
Trustworthy Technology White Paper

1. 6G

在 6G 2030 服
乎 施 6G 服
保 界 6G
5G 保护
供服
5G/B5G 乃 未来 6G
6G 来
本

1.1 6G

国 IMT-2030 6G 在 6G
6G 施
现 在
域

未来

Future 在 6G

AI 6G

国

NEXTGA 在 6G

Roadmap to 6G

Trust Security and Resilience 6G

1 2 强 界 3

4 云 5 无 6

在 6G Hexa-X 6G

6G Trustworthiness

Inclusion Sustainability 6G 未来

6G

5G 施 5GIA 在 6G

6G 主

施

本 在 B5G 2030 5.0

Vigorous Resilient

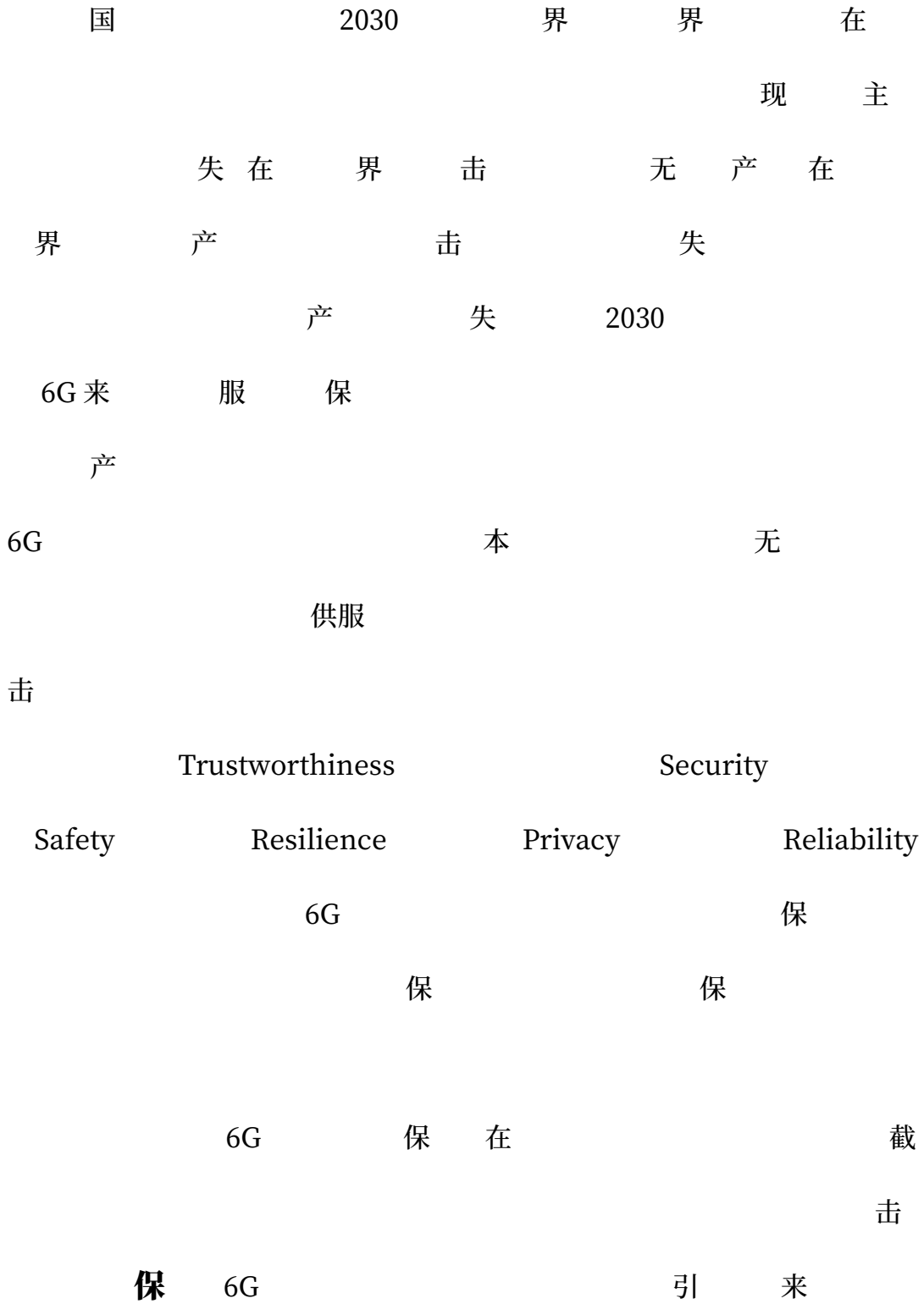
Inclusive Sustainable

Dependable

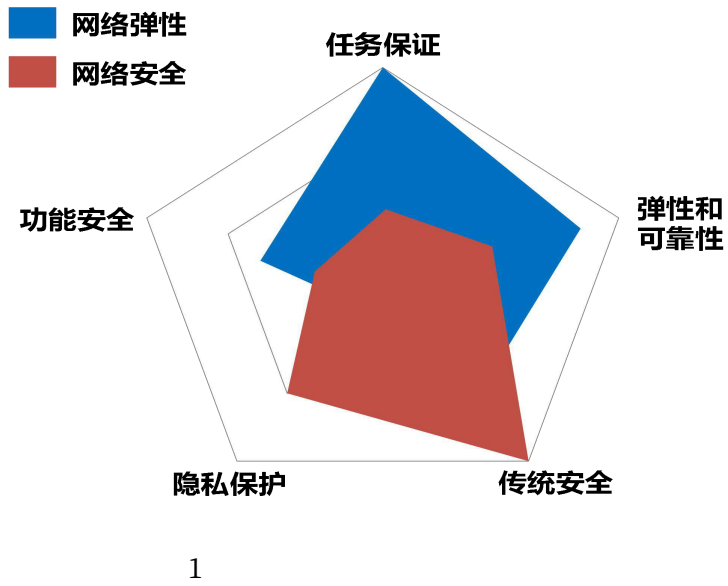
本国家 NICT B5G/6G 2.0

本 现 在 6G 无 来 6G
 B5G/6G 5.0
 施 现 在 6G 未 来 6G 底 域 保 界
 2030 B5G/6G
 CPS
 未 来 5.0
 在 产 界 在 6G
 6G 无 6G
 强 现 在 6G 国
 在 2030+ 未 来 6G
 服 在 6G
 无 6G AI 在 6G
 现 界 6G
 现 在 强 无
 6G 底 在 6G 未
 来 6G 域
 6G 服 供 供 保 界

1.2 6G



供 保
6G 供
6G
击 服 在
击 保 溃
5G 6G 在 击
在
6G 强 保
护 击
健 击
击 在 击 保
在 保护
保 在
本 强 在 保 本
主
主
保护 保 1
在 保护 在



1.3 6G

施

6G

2030

本

施

两

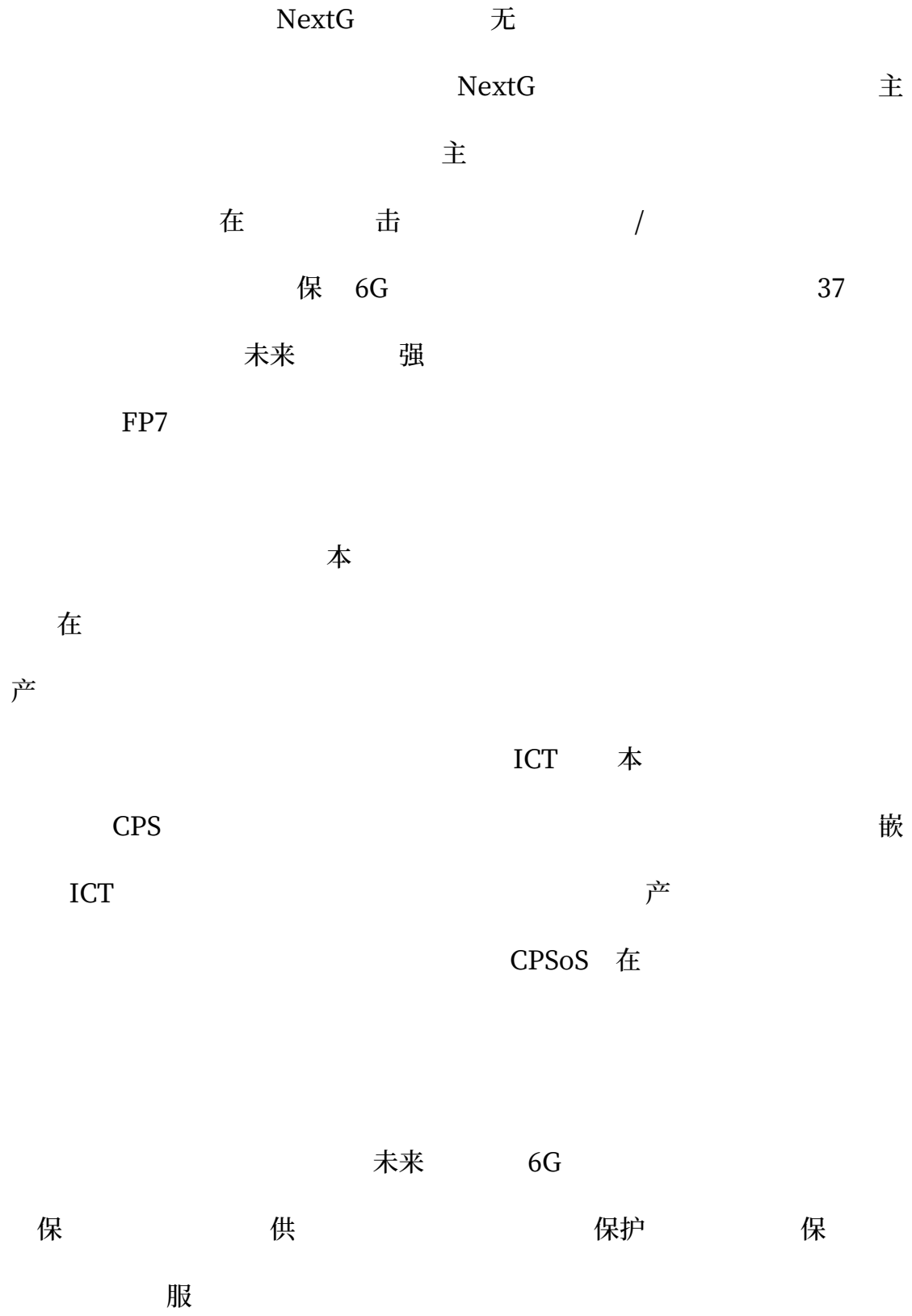
引

供

6G

来 界 6G
来
国 6G 6G
现
国 IMT-2030 6G 6G
在
未来 6G
在 保
2G-5G
现 6G 在
在 击
失
2030+
+ +
未来 界
现
国国家 National Science Foundation NSF
家 NextG 6G 未来 本 WiFi

RINGS Resilient & Intelligent NextG Systems



2. 6G

6G 在 底
服 保 在 排
击 产
在 击
6G
6G 6G 6G 供 供 6G
护
护

2.1 6G 主

6G 来
未 击 AI
未

2.1.1

2030 6G 来
服 击

在 6G 云

在

来

服 击

击

云

施

在

侧 击 服

供

6G

1000 /

供 击

2.1.2

无

摆

界

无

无 来

击

引

产

Safety

无

主 击产

Security

6G

无

无 侧 6G

无 在 6G

无

界

强

击

6G 无 无
保

2.1.3

失 失
乱 6G 云
失 乱
来 NfV 云
来
云 在 当
6G NfV 现 云
云 在
保 来

2.1.4 AI

在 6G AI/ML 在未来
主
AI 在
6G 引 AI 来 1 AI
击

2 AI 6G 击 击 击 击 击
击 现 击
WiFi
AI AI保 6G
6G

2.1.5

现 在 现 在
RSA ECC 现 在
强 在
现 RSA Diffie-Hellman
底 Grover 供
来 强
6G

2.2 6G

6G
现 在
保护 供



2 6G

6G

Integrated Design

Anti-fragile Design

主

现

High performance, High availability, and

High trustworthiness trinity

Integrated

design of the Four key pillars 6G

国
 / Cyber-resilience 强
 Fall less often Withstand the fall better 强
 Rise up stronger everytime 强 在 未 未
 击 强
 6G
 服 无 惧
 击
 失 伤 伤
 击 失 服 供 AI

2.3 Four Key Pillars

在 1G 5G
 1G 2G Authentication Key
 Agreement, AKA 强 A5/1 供

保护 在 3G 现

3G 供

保护 在 3G

保护 4G 强

域 护 引 AES SNOW 3G ZUC

域 强 在 现 保护

在

保护 域

主 5G

3GPP 在 5G

服 Service Bases Architecture SBA 强

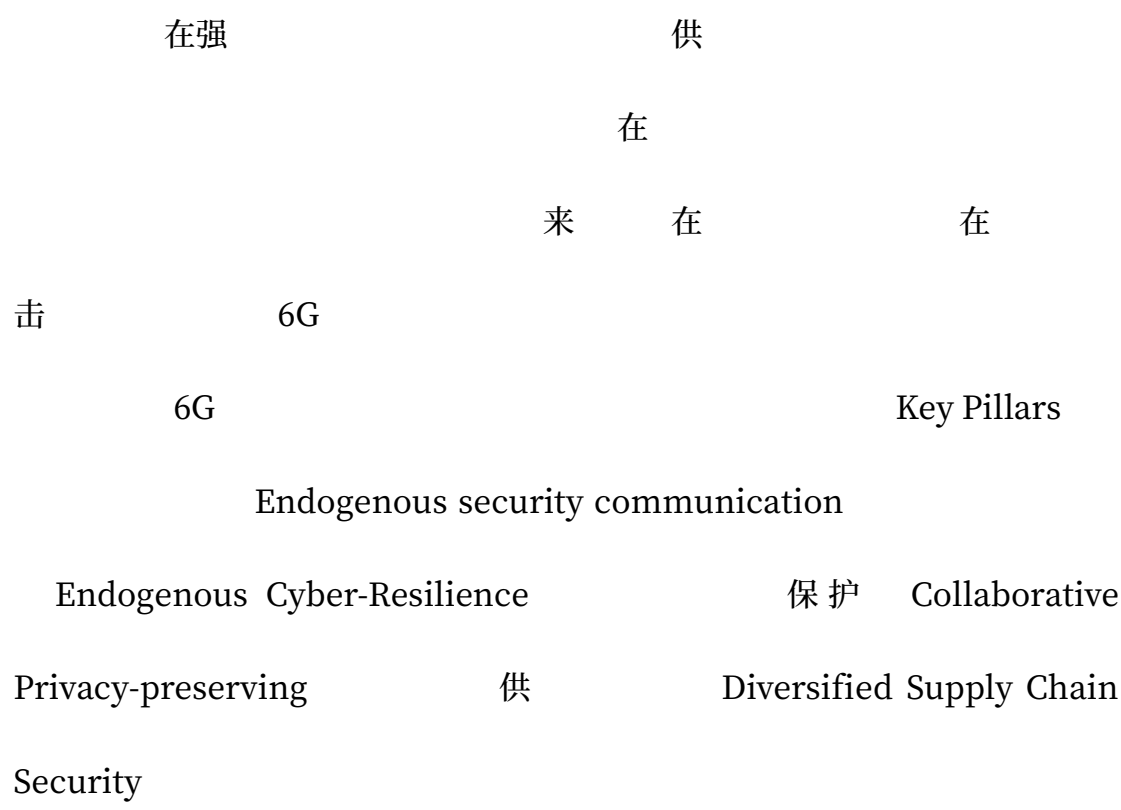
域 域 护 强 保护 引

Subscription Concealed Identifier

SUCI IMSI

域 护 Security Edge

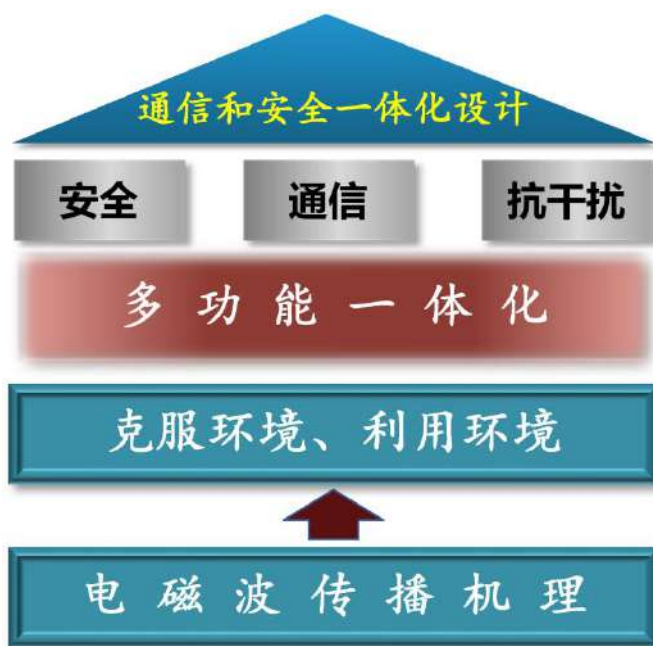
Protection Proxy SEPP 来



2.3.1

在 服 现

KPI Key Performance Indicator



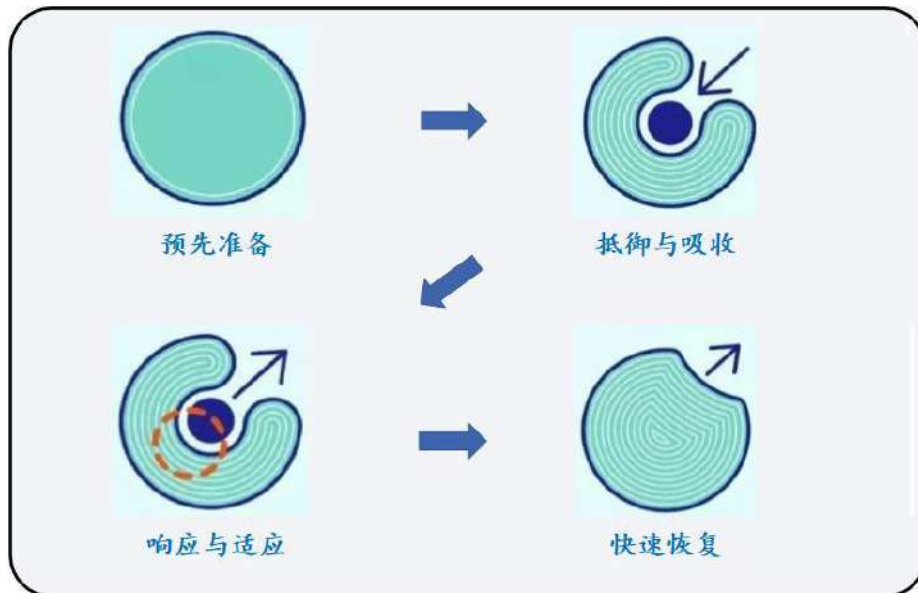
3 6G

6G	保	Confidentiality
Integrity	Availability	CIA
无		
3	在 供	供
6G	服	6G
	6G	6G
来	服	现

2.3.2

现 主 击
在
现 未 现

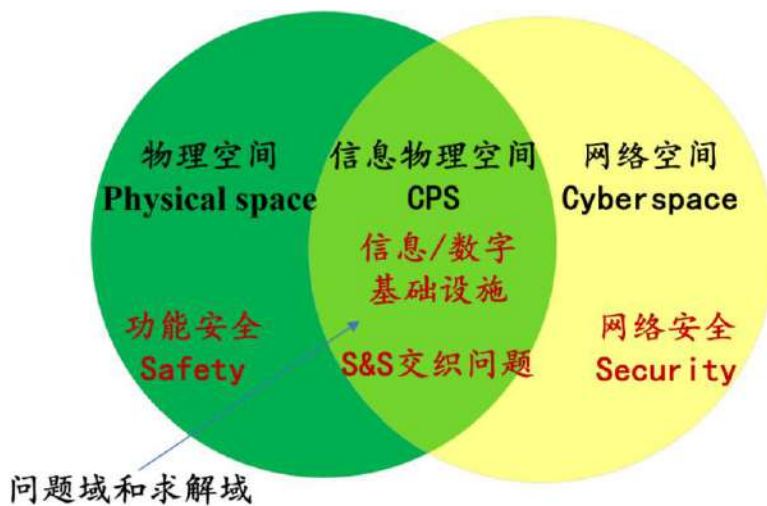
未 击 强 供 击
 在 击 0-day
 击 现 APT 击
 服 供 现
 当 击 现



4

6G 现 施
 CPS CPS
 在 副
 在 引

现 在 击
 失 6G 在 失
 来 在 击
 在 未 击
 保 本
 6G 保 服 保 5



5

2.3.3 保

1G 2G
 在 3G 4G 界
 保护 来 在 5G/6G 保护
 域
 Identity Credibility 服

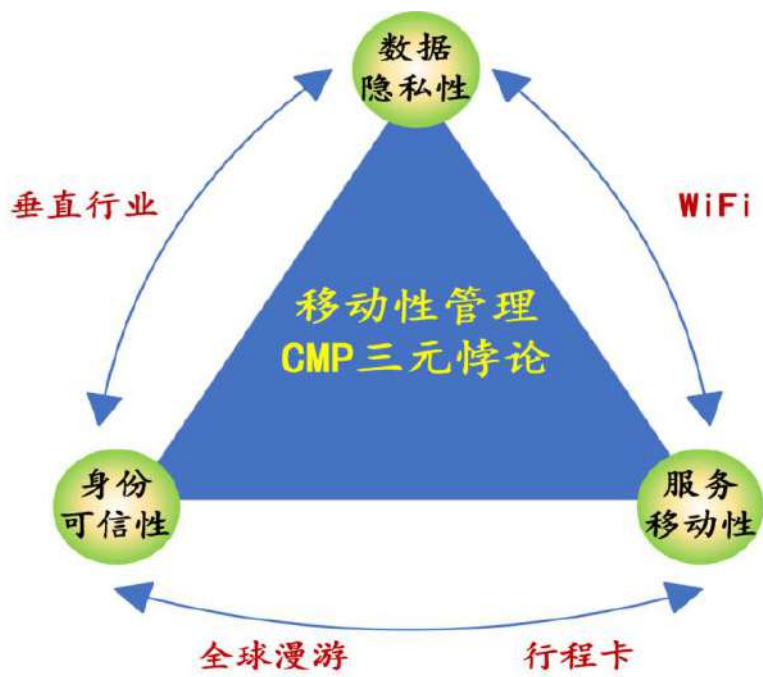
Service Mobility

Data Privacy

Credibility, Mobility, and Privacy CMP

6

服 供 服 在 服 在 保 本 当 域 当 在 WiFi



6 CMP

在无 服 6G 强 护 供

保护 在 6G

保 在 域 保 主
在 主
/保护

2.3.4

6G

来 供

6G 云

供 供 保

施

产

产 服

产 供

供

供

供

供

服务软件



虚拟化



操作系统



底层硬件



7 云

供

2.4

Four Enabling Factors

6G

底

2.4.1

Structuring

界

未来 6G

6G

在

现在

施

6G

施

击

6G

供

底 现 两

供

6G

供

护 供

在

服 保

供

供

底

供

供

界

DHR Dynamic

Heterogeneous Redundancy

2.4.2 Customization

服 6G 域 在

服

服 在 6G

域

现

施 护

击

6G

施 PKI

嵌

域

域

保

凝

产

产

RISC-V

供 侧
来

产

排

2.4.3 Intelligentize

在 6G

/

6G

(

API

)

在

域

/

来 强现

排

未来

强

6G

供健

服

服 保护

来

当

云

来 服

保护

未

6G

来

在

当

在

在

供

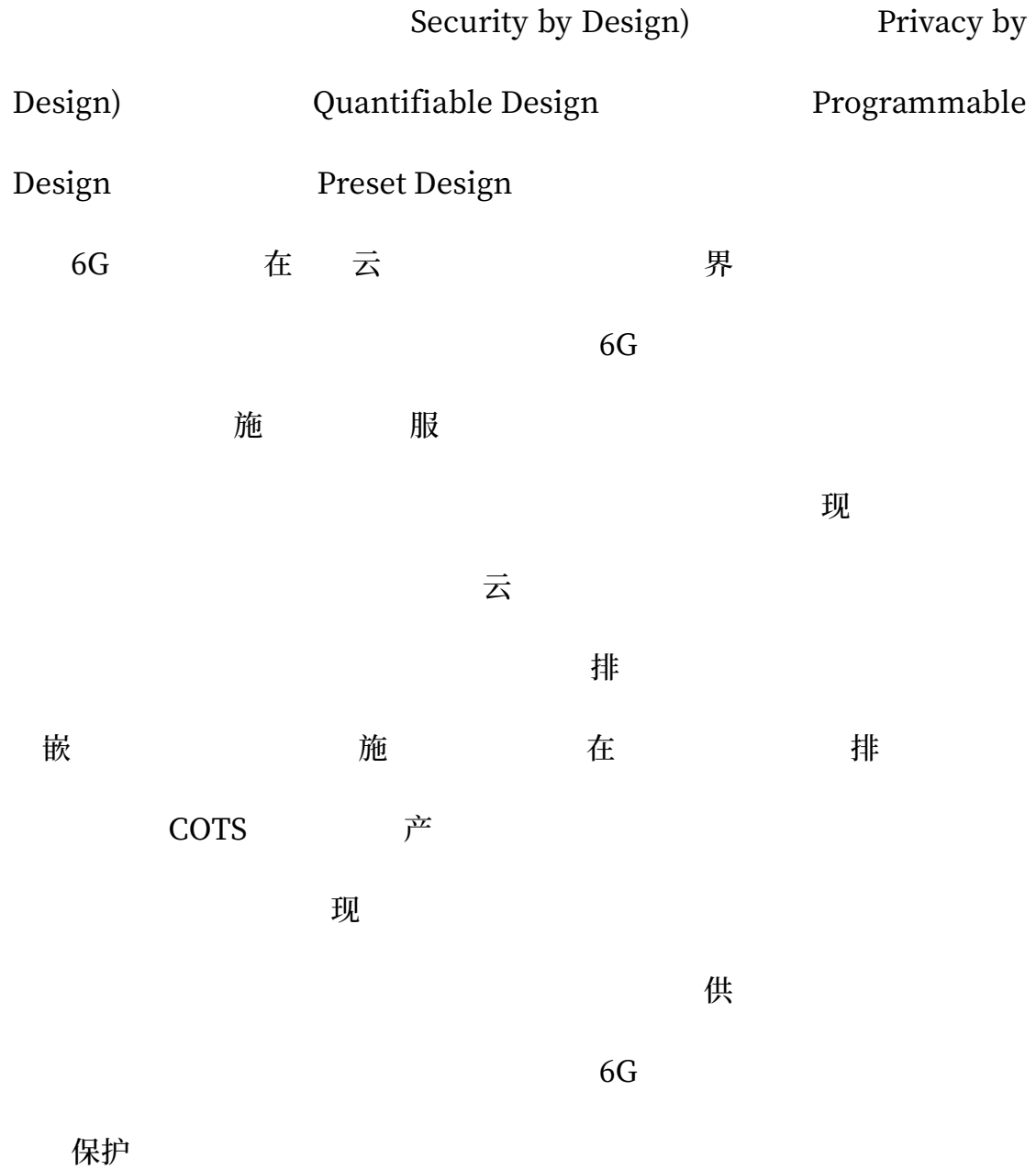
现 失 在
强

2.4.4 Automation

6G 在 引 AI/ML 6G
现 6G 保 主 服 供 6G
击 服 来 6G
本 在 击
底 当
现 当
无 无 无
主 施 当 击 来 来
无 无
无 无 无 无 无 无
在

2.5 Four Basic Properties)

2.5.1 Designability)



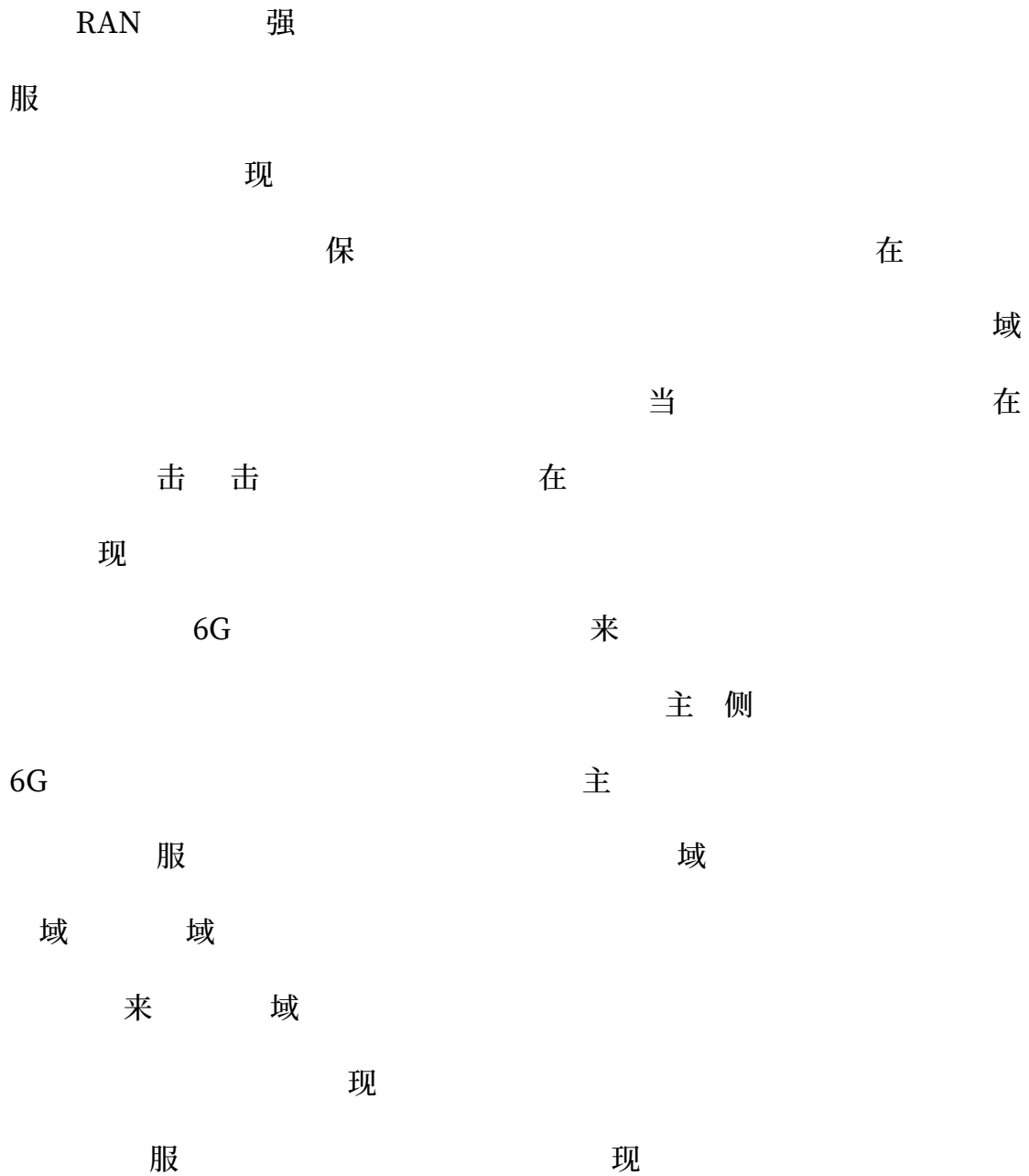
2.5.2 Perceibility

End-to-end Observability 主

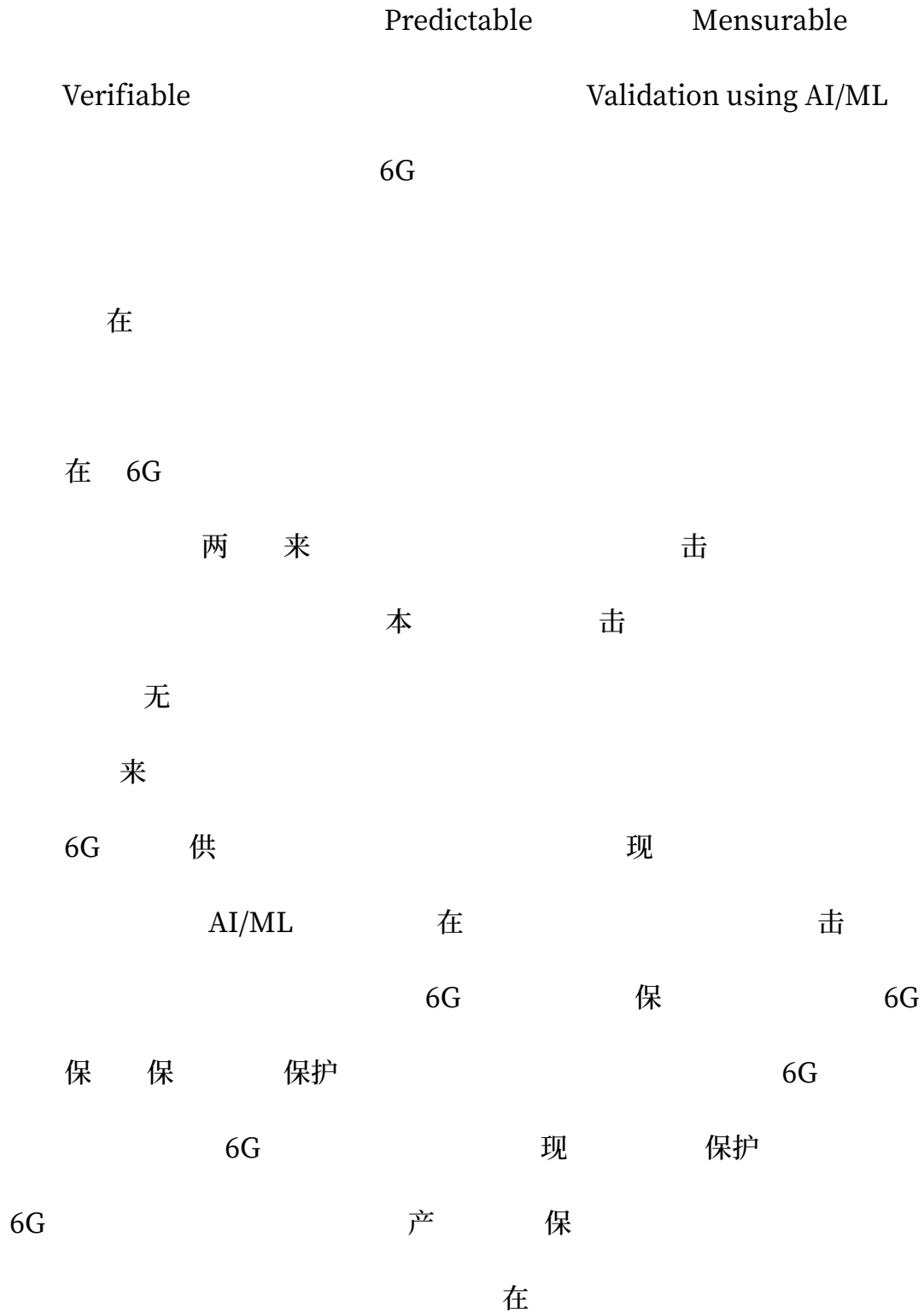
Active Perception and Threat Detection

Security Visualizations

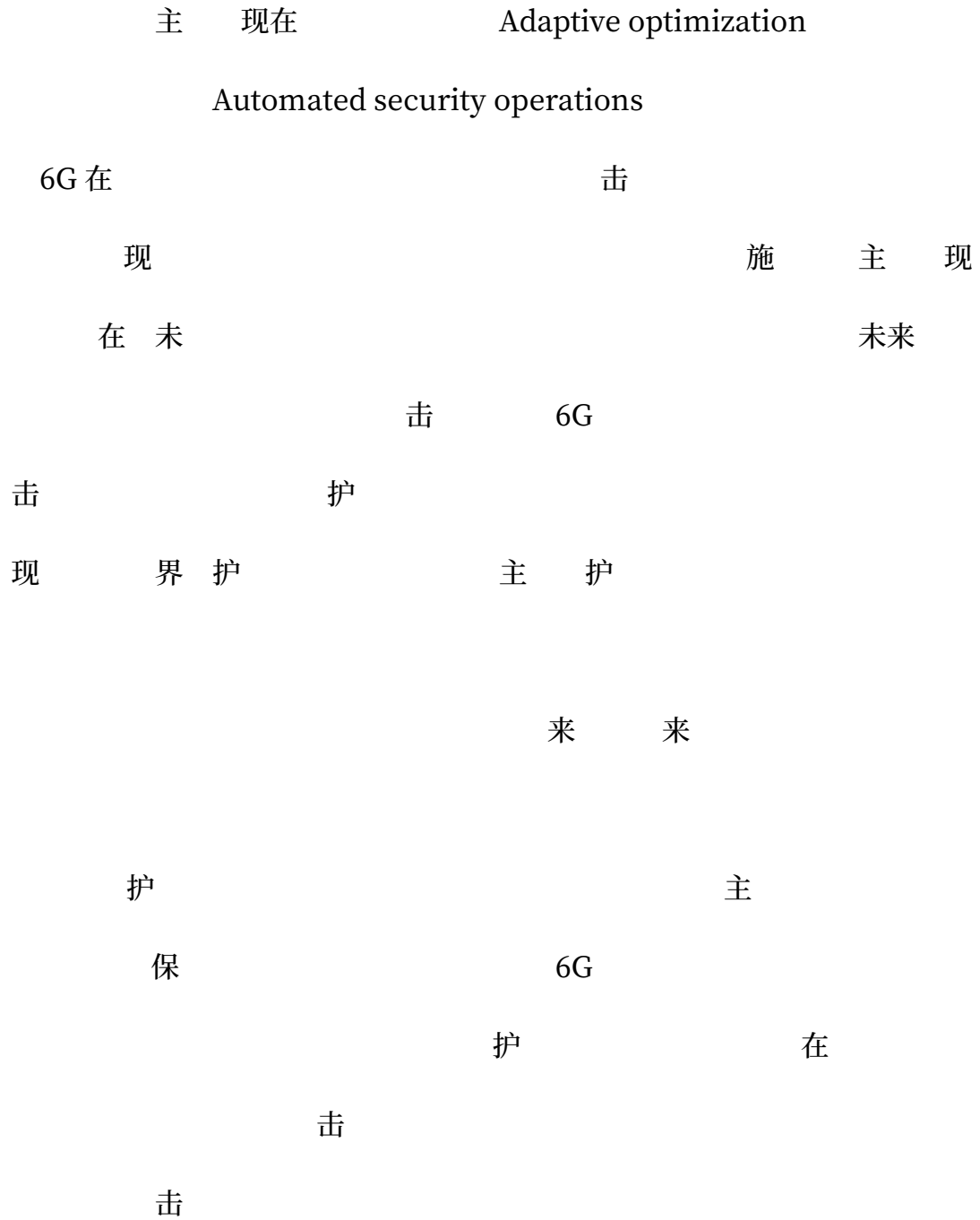
Explainable AI



2.5.3 Metrizable



2.5.4 Evolvability



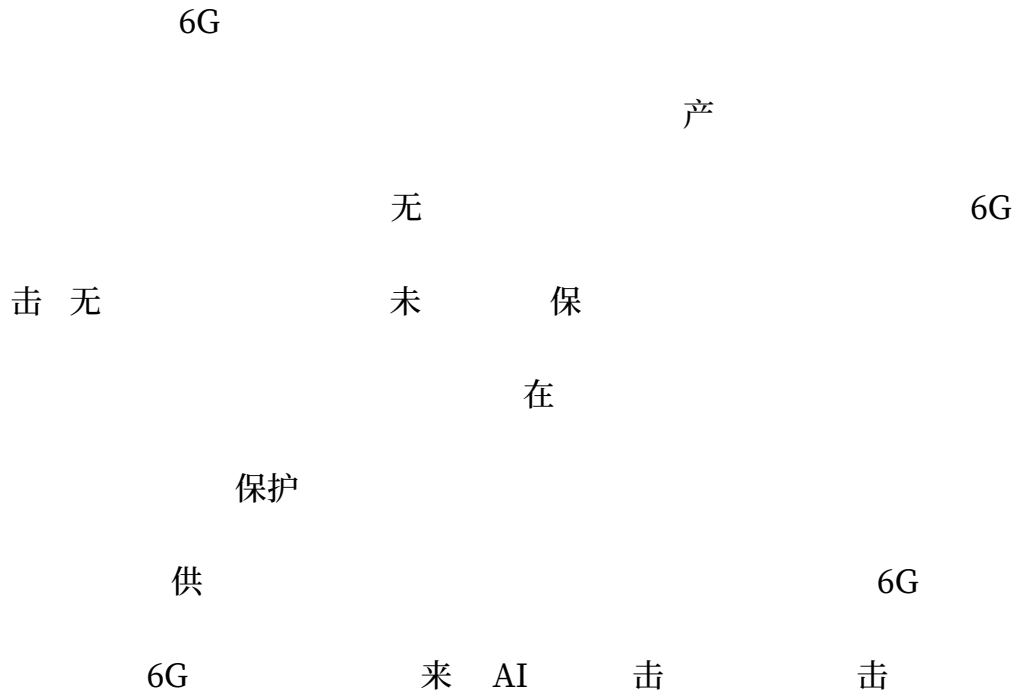


3. 6G内生安全关键技术

6G内生安全可信技术白皮书

6G Endogenous Security&Safety and
Trustworthy Technology White Paper

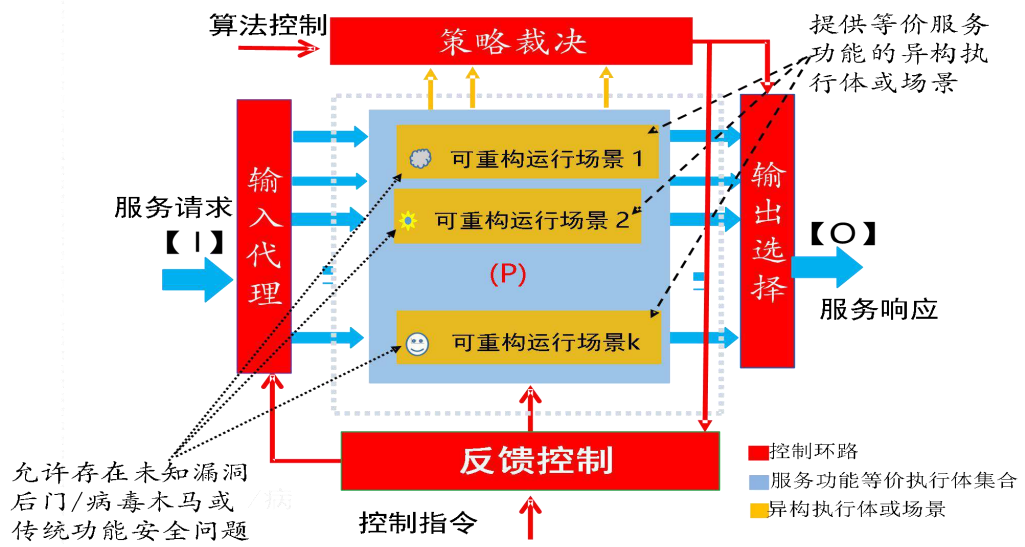
3. 6G



3.1

Dynamic Heterogeneity Redundancy





8 DHR

在 DHR

服

K

P

产

服

现

在 /

当

在

失

主

DHR

在 排 在 在

击

现 现 DHR

产

界 现 在 排

施

击 失 引

供 Safety Security

DHR 供

供 未 未 未

击 强 DHR /

DHR /

击 无

供

DHR 击

击 DHR 惑

击

在

DHR

供

COTS

产

本 无

在

3.2

6G

在 5G

云

服

施云

服

来

IT

6G

云

6G

DDoS 击

供

6G

9

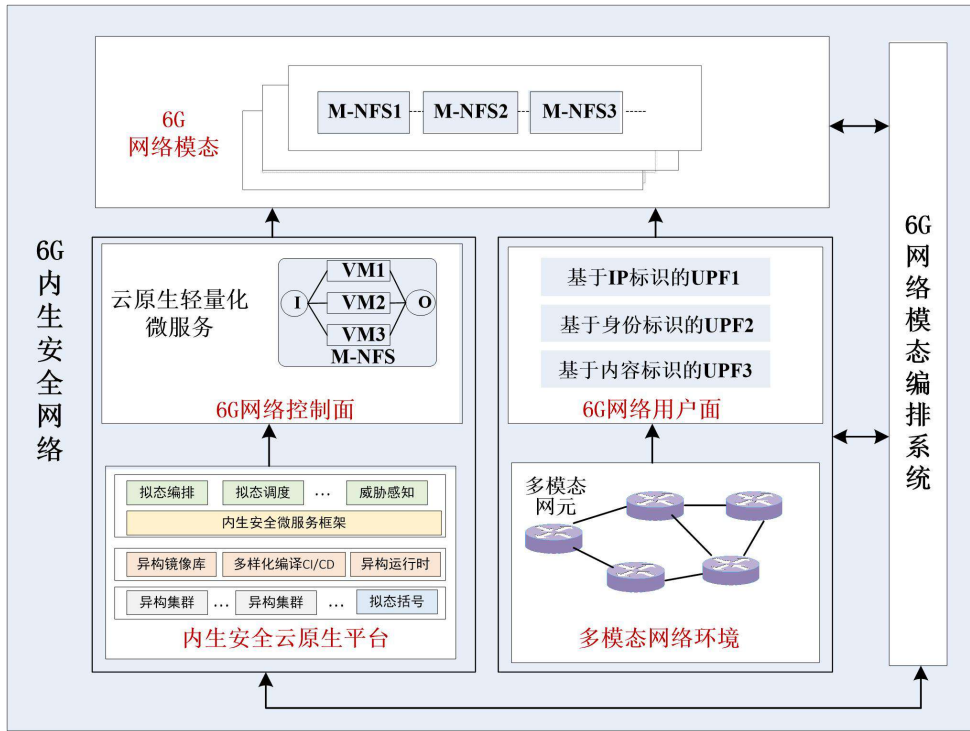
云

6G

6G

6G

排



9 6G

6G 两供云 6G 供服 6G 服

DHR 云 在 云 服 来 未 服 在 云 服 6G

云 云 服 6G 服

DHR 服 在 6G

云 云

云

供 服

6G

云 供

云

云

供

保

3.3

现

无 侧

沿

无

在

6G

在

6G 无

无

无

保

无

无

击

来

保

无

无

产

无

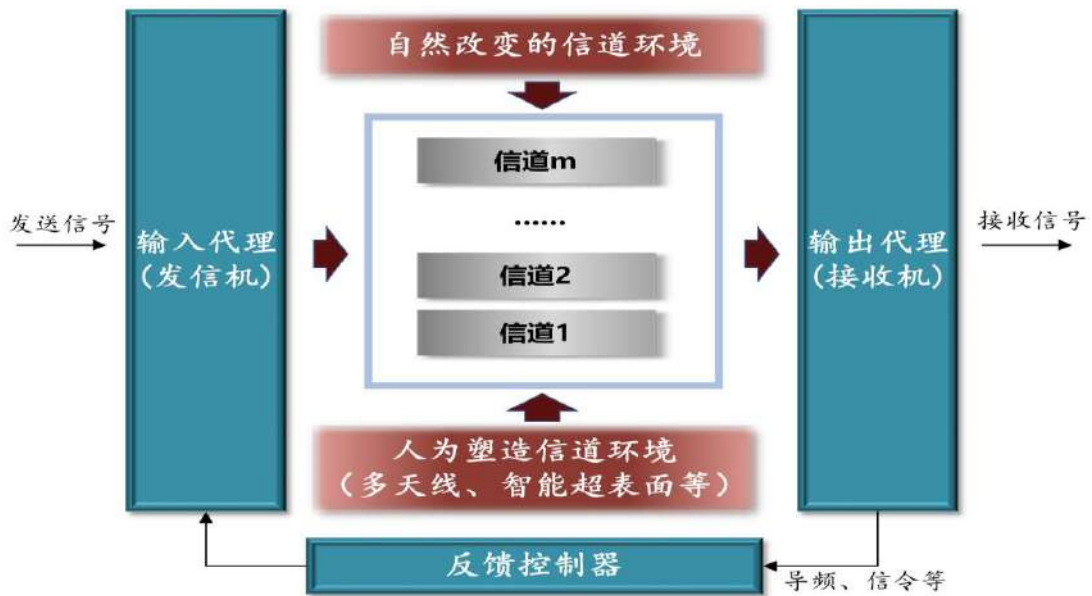
引

无

界

无

无 本 无 界 现 无



10 无

10

, 无

DHR

DHR

本

, 无

DHR

无

无

DHR

无

现

无

1

无

2

无

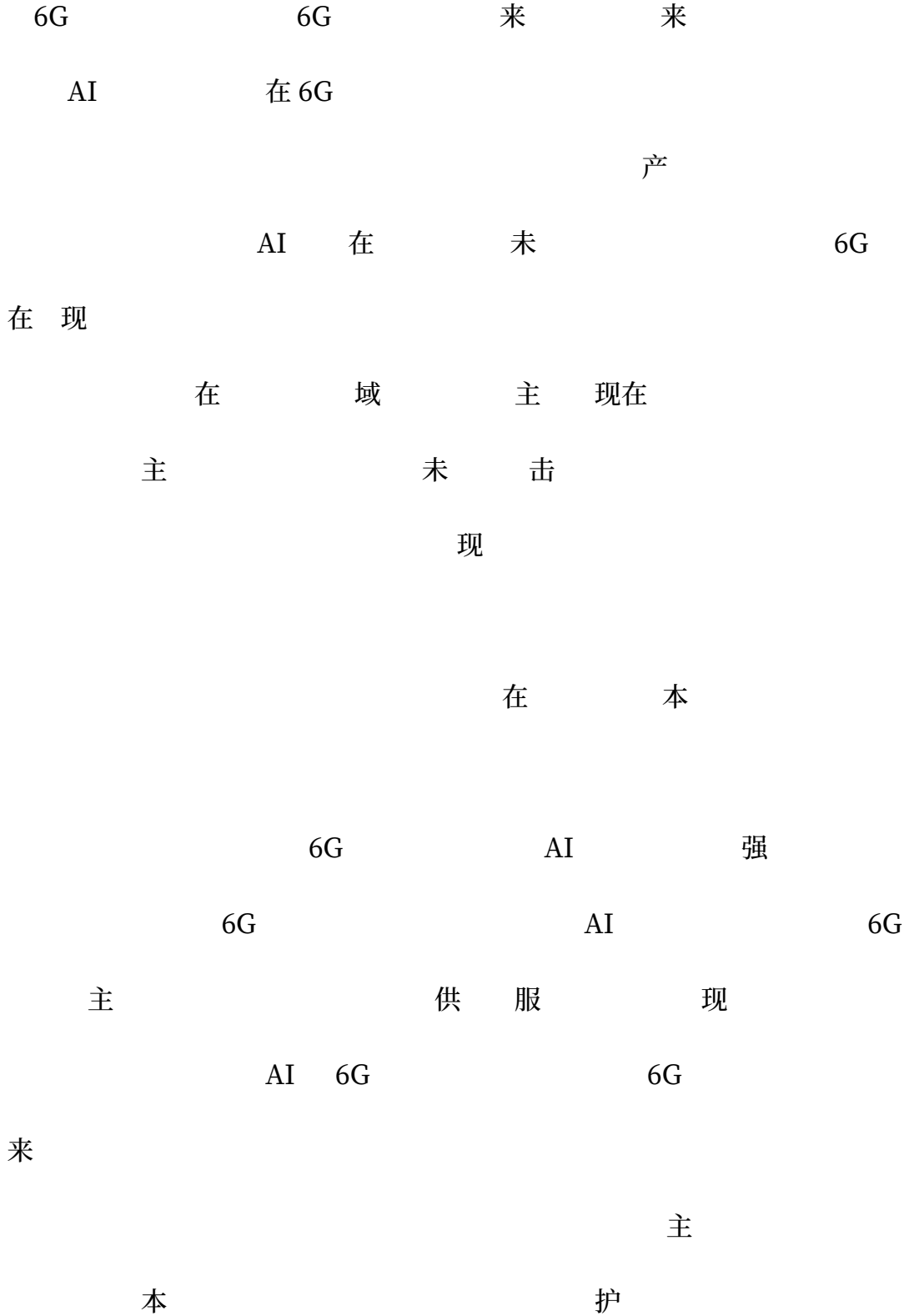
3

强 无

无

Intelligence Surface
 现 RIS (Reconfigurable
 无 现
 供 RIS
 DHR
 当 5G DHR
 1
 无 无 现
 2 域 域 供
 现 RIS DHR
 3
 在 现 无
 无 DHR
 在无 无
 无 供 在 现
 强健 击
 来 产 未
 6G

3.4



6G

击

未

击 现 界 域

排

产

6G AI 引

AI 击 来 AI 本 击

在 AI 来 主

击 击 击 AI

1 击 保护 在

供

2 击 击

强

3 击

AI API 供 在

3.5

		PQC		现	
击		未来		Next G	
6G	Hexa-X	本 B5G	国	IMT-2030 (6G)	
国	国	6G	保	6G	
			现		RSA
Diffie-Hellman					来
					主
4	现	1	Hash-based	主	
2		Code-based	主		3
Multivariate-based			主		
4		Lattice-based	主		
			当	当	
无					
2016	国国家		NIST		
在			2020	NIST	
1		KEM	Key Encapsulation Mechanism		
/					

在

NIST

在 2024 年 现

表 1 NIST PQC 竞赛的入围算法

KEMs/ 加密	基于编码	Classic McEliece	密文短，但公钥尺寸较大，适用于密文短的应用，不适用于通用互联网协议
	基于格	CRYSTAL-KYBER	公钥尺寸小，各方面性能权衡较好，有解密失败的风险，可用于TLS协议，不推荐用于离线解密
		NTRU	公钥尺寸小，速度快，各方面性能权衡较好，提出时间较早，有解密失败的风险，安全性不及其他基于格的算法
		SABER	各方面性能权衡较好，具有轻量级模式，具有解密失败的风险，可用于通用应用
签名	基于多变量	Rainbow	快速签名认证，但公钥尺寸较大，不适用于通用应用
	基于格	CRYSTALS-DILITHIUM	实现简单，各方面性能权衡较好，但安全性还需进一步研究
		FALCON	带宽要求最小、高效，但实现比较复杂，密钥生成速度慢，总体性能较好

未来 PQC

引 PQC

PQC

/

/

现

QKD

QC

来 强

国 本

保 B5G/6G

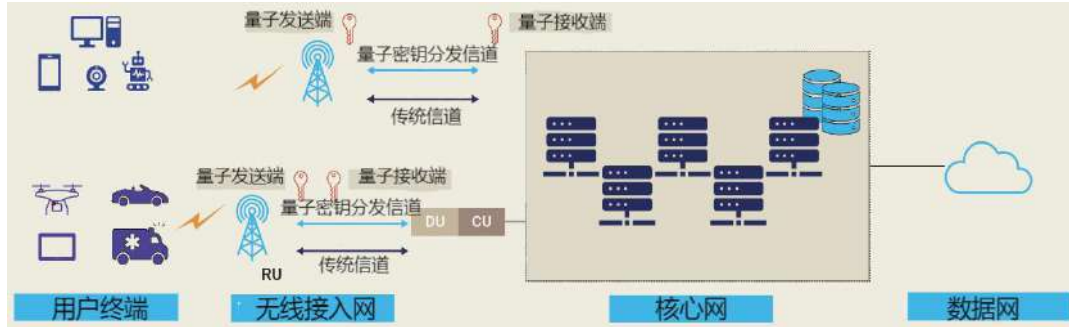
6G

在

11

在 现

保护



11

3.6

在 现 侧

保护

6G

在

6G

在本

云

在

云供

云

在 在

6G

在

供 护

云

主

供强

保

保

云

保护

在

Trusted Execution Environment TEE

供保护

保

在

在

在 保

护 CPU enclave 未 云供
在 TEE 在 TEE
在 底 供 保
在
在
云服 供
在 6G 来 在 云
保护 6G AI
供
在 在 TEE
强 护
保 在
本 现
未
主 无
来

在 来 现
来 域

3.7

现

护 6G 引 6G 强 6G 保
现

保护

域

1 无 服

保

在

无

两 保

2 无

来 主

无

供

3 保护 当

无 彼 无

无

来

截

保护 来

供保护

4

服 供

服 在

供

5 6G

域

域

主 产

现 主

6G

域

在

主

域

3.8

保供 在 供 来
家 现

本 供 在
服

1
当 击

在无 AI/ML 在 6G
来 AI/ML 在
供

AI/ML 本

本 来 现
在

DevOps Development and Operations

现 2030

施 AI 6G

来
在
主 在
现
2 **Secure-by-design**
来 界 护
2012 Gartner DevSecOps Development, Security, and
Operations 护 DevOps
供强 保 在
现
现在 无 现
现 DevSecOps
在 在
国国家 NIST
在 本 当 在 30
现 SDL Security Development
Lifecycle 在 在
SDL
保 现
在

3 DHR

底
在
产
产 无
击 产 ,
主
击 供 击
强 击
/
/
供 产 6G 国家



4. 总结

6G内生安全可信技术白皮书

6G Endogenous Security&Safety and
Trustworthy Technology White Paper

4.

	2030		施 6G		6G
	无		强		
			现		
保护	供			6G	击
无	失 AI				强
	施	乱	击		
本		6G	供		
	界	6G	保	6G	
本	国家	6G		6G	
	2020YFB806607		无		6G
	2022YFB2902202	6G	无		保护
	2022YFB2902204	6G		保护	
	2022YFB2902205				



移动互联网安全技术
国家工程研究中心



参考文献

6G内生安全可信技术白皮书

6G Endogenous Security&Safety and
Trustworthy Technology White Paper

- [1] Xinsheng Ji, Jiangxing Wu, Liang Jin, Kaizhi Huang, Yajun Chen, Xiaoli Sun, Wei You, Shumin Huo, Jing Yang, 2022. Discussion on a new paradigm of endogenous security towards 6G networks. *Frontiers of Information Technology & Electronic Engineering*, 23(10):1421-1450.
- [2] Ji X, Huang K, Jin L, et al. Overview of 5G security technology[J]. *Science China Information Sciences*, 2018, 61(8): 1-25.
- [3] 邬江兴. 网络空间内生安全——拟态防御与广义鲁棒控制[M]. 科学出版社, 2020.
- [4] 邬江兴. 网络空间内生安全发展范式[J]. *中国科学: 信息科学*, 2022, 52: 189-204.
- [5] 刘彩霞, 季新生, 邬江兴. 移动通信网的内生安全共性问题及破解之道[J]. *通信学报*, 2022, 43(9): 70-79.
- [6] 粟粟, 庄小君, 杜海涛, 等. 6G 网络内生安全架构研究[J]. *中国科学: 信息科学*, 2022, 52: 205-216.
- [7] 聂凯君, 曹侯, 彭木根. 6G 内生安全: 区块链技术[J]. *电信科学*, 2020, 36(1): 21-27.
- [8] Hu X , Jin L , Lou Y , et al. Introduction to Wireless Endogenous Security and Safety: Problems, Attributes, Structures and Functions[J]. *中国通信:英文版*, 2021, 18(9):12.
- [9] Center for a New American Security. Securing America’s 6G Future[R]. 2021.
- [10] 宋振远. 智能反射表面辅助通信系统的物理层安全技术研究[D]. 重庆邮电大学, 2021.
- [11] National Science Foundation (NSF) . Resilient & Intelligent NextG Systems (RINGS) [EB/OL]. <https://www.nsf.gov/pubs/2021/nsf21581/nsf21581.pdf>
- [12] Next G Alliance. Next G Alliance Report: Roadmap to 6G[R]. 2022.02
- [13] M. Uusitalo, P. Rugeland, M. Boldi, et al. Hexa-X the European 6G Flagship Project[C]. 2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), Porto, Portugal, 2021, 580-585.
- [14] Beyond 5G Promotion Consortium. Beyond 5G White Paper: Message to the 2030s[R]. 2022.03
- [15] IMT-2030 (6G) 推进组. 6G 网络架构愿景与关键技术展望白皮书[R]. 2021
- [16] IMT-2030 (6G) 推进组. 6G 网络安全愿景技术研究报告[R]. 2021.09
- [17] 童文, 朱佩英. 6G: 无线通信新征程[M]. 机械工业出版社, 2021
- [18] Next G Alliance. Next G Alliance Report: 6G Technologies[R]. 2022.06

- [19] 中兴通讯股份有限公司. 2030+网络内生安全愿景白皮书[M]. 2021.06.
- [20] 中国移动通信集团有限公司. 中国移动 6G 网络架构技术白皮书[M]. 2022.06.
- [21] Next G Alliance. Next G Alliance Report: Trust, Security, and Resilience for 6G Systems [R]. 2022.07.
- [22] Hexa-X. Deliverable D1.2 Expanded 6G vision, use cases and societal values [R]. 2021.04.
- [23] Ronald S. Ross, Victoria Y. Pillitteri, Richard Graubart, et al. Developing Cyber-Resilient Systems: A Systems Security Engineering Approach[R]. Special Publication (NIST SP), National Institute of Standards and Technology, 2019.
- [24] 紫金山实验室.6G 无线网络：愿景、使能技术与新应用范式 2021.
- [25] 紫金山实验室. 区块链赋能 6G 移动通信白皮书: 体系架构与技术原理[R]. 2021.
- [26] Nokia Bell Labs. Security and trust in the 6G era [R]. 2021.
- [27] Samsung Research. 6G: The Next Hyper Connected Experience for All[R]. 2020.



移动互联网安全技术
国家工程研究中心

网络通信与安全紫金山实验室
国家数字交换系统工程技术研究中心
移动互联网安全技术国家工程研究中心

2023年1月