面向BDSBAS电文认证的OTAR设计与仿真

田 翔[1,2],陈 颖[3],邵 搏[4],罗瑞丹[1],丁 群[4],刘 婷[1*]
(1. 中国科学院空天信息创新研究院,北京 100094;2. 中国科学院大学电子电气与通信工程学院,北京 100049;3. 北京跟踪与通信技术研究所,北京 100094;4. 中国电子科技集团公司第二十研究所,陕西西安 710000)

摘 要: 星基增强系统(Satellite Based Augmentation System, SBAS)的电文格式公开,为防止SBAS服务遭受生成式欺骗攻击,国际民航组织积极推进SBAS认证服务标准的制定.本文面向北斗星基增强系统(BeiDou Satellite-Based Augmentation System, BDSBAS)阐述了基于中国商用密码算法的椭圆曲线数字签名(Elliptic Curve Digital Signature Algorithm, ECDSA)电文认证方案与时间效应流丢失容错(Time Efficient Stream Loss-tolerant Authentication, TESLA)电文认证方案,设计了BDSBAS认证电文,依据空中密钥管理OTAR(Over The Air Rekeying)的策略制定了OTAR电文(OTAR Message Type, OMT)与播发方案.通过蒙特卡洛OTAR仿真器开展仿真,对不同OTAR电文接收时间进行分析,本文设计的方案与国外方案对比结果有明显的提升,有效的减少了接收机完成认证使用SBAS增强服务的时间,对BDSBAS电文认证服务提供一定参考与建议.

关键词: 北斗星基增强系统;电文认证;椭圆数字签名;时间效应流丢失容错认证;空中密钥更新
基金项目: 国家自然科学基金(No.41904033)
中图分类号: TN967.1;V19;X949 **文献标识码:** A **文章编号:** 0372-2112(2024)03-0729-11
电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20220573

OTAR Design and Simulation for BDSBAS Message Authentication

TIAN Xiang[1,2], CHEN Ying[3], SHAO Bo[4], LUO Rui-dan[1], DING Qun[4], LIU Ting[1*]
(1. *Airspace Information Innovation Institute*, *Chinese Academy of Sciences* (*CAS*), *Beijing* 100094, *China*;
2. *School of Electronic*, *Electrical and Communication Engineering*, *University of Chinese Academy of Sciences*, *Beijing* 100049, *China*;
3. *Beijing Institute of Tracking and Communication Technology*, *Beijing* 100094, *China*;
4. 20*th Research Institute of China Electronics Technology Group Corporation*, *Xi'an*, *Shaanxi* 710000, *China*)

Abstract: The message format of the satellite based augmentation system (SBAS) is open, and the system is relatively fragile. In order to prevent the SBAS service from being subjected to generative spoofing attacks, the international civil aviation organization (ICAO) actively promotes the formulation of the SBAS certification service standard. This paper expounds the elliptic curve digital signature Algorithum (ECDSA) message authentication scheme and the time efficient stream loss-tolerant authentication (TESLA) message authentication scheme based on the Chinese commercial cryptographic algorithm for the Beidou satellite based augmentation system (BDSBAS). The BDSBAS authentication message is designed, and according to the air key management OTAR(Over The Air Rekeying) strategy formulates the OTAR message type (OMT) and broadcast scheme. The Monte Carlo OTAR simulator is used to simulate and analyze the receiving time of different OTAR messages. The results of the scheme designed in this paper are significantly improved compared with foreign schemes, which effectively reduces the time for the receiver to complete the authentication with the SBAS enhanced service. The message authentication service provides certain references and suggestions.

Key words: BDSBAS; message authentication; ECDSA; TESLA; OTAR
Foundation Item(s): National Natural Science Foundation of China (No.41904033)

1 引言

为提升卫星导航系统精度和完好性,满足航空领域安全性,星基增强系统(Satellite Based Augmentation System, SBAS)应运而生[1],SBAS系统利用地球静止

收稿日期:2022-05-20;修回日期:2022-09-29;责任编辑:梅志强
*通讯作者:刘婷

轨道（Geosynchronous Earth Orbit，GEO）卫星向用户广播差分改正和完好性信息，实现广域导航增强．由于SBAS广播信号格式公开，其电文具有一定可预测性，因此SBAS系统主要遭受生成式欺骗攻击[2]，攻击方通过篡改SBAS电文来影响服务性能．为了应对生成式欺骗，国外提出了基于系统端的解决方案，即SBAS导航电文认证（Navigation Message Authentication，NMA），通过在SBAS电文中加入认证电文，使用户确认SBAS电文是否来自真实的GEO卫星以及SBAS电文是否被伪造及篡改，保障SBAS电文完整性，为终端提供信息源认证服务[3]．

欧盟于2016年提出了EGNOS（European Geostationary Navigation Overlay Service）的电文认证计划，开发了EGNOS认证安全测试床（EGNOS Authentication Security Test-bed，EAST）项目[4]，提出了基于椭圆曲线的数字签名认证方案（Elliptic Curve Digital Signature Algorithm，ECDSA）与时间效应流丢失容错认证方案（Time Efficient Stream Loss-tolerant Authentication，TESLA）[5]．2019年欧美成立了联合工作小组开展了SBAS认证方案的细化与仿真工作，计划将SBAS认证方案标准化，其中美国斯坦福大学针对ECDSA方案与TESLA方案进行了SBAS电文设计，并提出了使用空中密钥播发（Over The Air Rekeying，OTAR）[6]的方法来进行密钥更新与管理．2021年5月，美国、欧洲和日本成立了SBAS电文认证标准化小组，计划于2022年底完成初步设计．随着国际民航组织工作小组积极推进SBAS认证方案标准化及BDSBAS（BeiDou Satellite-Based Augmentation System，BDSBAS）系统完成初步建设，国内有关单位已经开展了基于中国商用密码算法的ECDSA认证方案[7]与TESLA认证方案[8]的电文设计，但方案主要聚焦于电文设计与KPI（Key Performance Indicators，KPI）仿真，对OTAR电文设计关注较少，本文主要针对OTAR电文进行优化设计，基于不同级别密钥的更新周期，确定不同系统状态与对应的OTAR电文，减少OTAR播发带宽需求从而降低接收机的首次认证时间．

本文分析了SBAS系统可选认证协议，结合信号支路特点，确定合适的SBAS电文认证方案，并基于中国商用密码算法优化BDSBAS系统的认证电文，提出精简的OTAR电文内容，同时根据密钥结构确定系统状态与对应的OTAR电文，开展OTAR电文接收时间仿真，从接收机角度评估本文设计方案的性能．

2 BDSBAS电文认证方案设计

2.1 BDSBAS电文认证方案设计

SBAS电文认证技术是指在SBAS电文中加入数字签名或者消息认证码（Message Authentication Code，MAC）等认证标识，用户接收机通过标识判断接收的SBAS电文是否来自于真实的GEO卫星[9]．NMA无需更改接收机硬件，实现相对简单，对接收机新增的运算和存储负担可以忽略，NMA技术基于非对称密码体制实现，主要有ECDSA[10]和TESLA两种方式．

2.1.1 ECDSA认证原理

ECDSA是借助椭圆曲线密码完成模拟数字签名算法的过程．ECDSA协议在开始生成一对用于签名与验签的密钥对，其中私钥用于签名，公钥验签．为验证公钥的合法性，使用CA（Certification Authority）机构私钥进行数字签名，并与公钥一起通过OTAR发送，接收机利用内置的CA机构公钥验证公钥签名，进而通过公钥验证SBAS电文．基于ECDSA协议的SBAS认证具体流程见图1．

ECDSA协议优点是在同样等级的安全性下，相比于传统的离散对数系统密钥更短，且ECDSA协议具有国际标准，可以保证安全性和通用性；但是带来的问

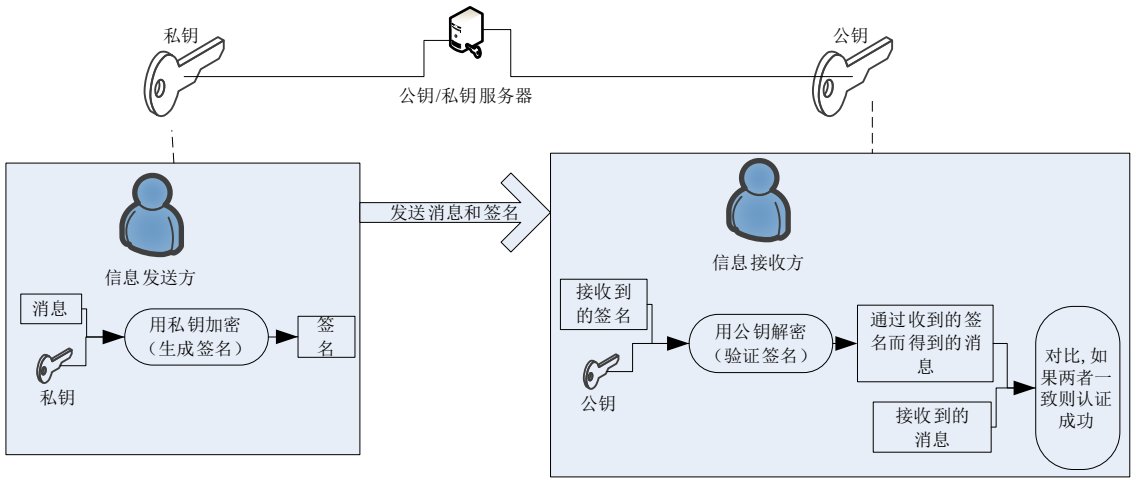

图1 ECDSA协议认证流程

题是椭圆曲线体制的数学计算更加复杂.

2.1.2　TESLA认证原理

TESLA是应用于组播和广播数据流的一种比较安全的源认证协议，通过密钥的延迟播发构造出非对称密码体制[11]. 首先使用单向散列函数生成密钥链，接着将密钥链中的密钥作为对称密钥生成并发送消息认证码[12]，基于密钥延迟发送机制，在延迟δ时间后发送用于生成MAC的密钥，接收机接收并使用该对称密钥检验MAC，而此时该密钥已不能再用于生成MAC，因此不会造成攻击者使用该密钥伪造电文发送给用户接收机的情况. 基于TESLA方案的SBAS认证具体流程见图2.

TESLA协议使用单向散列函数生成密钥链及发布密钥过程[12]如图3所示，H代表单向散列函数. 为确保接收机获取到真实的根密钥，需要其他的认证系统对根密钥进行认证，采用数字签名认证，将数字签名算法密钥对称为系统钥对. 单向性的基本特点可以确保密钥K_1由接收者完成接收之后，能够完成对根密钥K_0的验证，然而不能计算出接下来使用的密钥K_2，因此公开密钥即使被攻击者获取，也无法推断出下一个要使用的密钥.

TESLA协议的优点在于计算负载和通信负载低，适合预留带宽有限的卫星导航系统，并且单向密钥链可以确保链内密钥丢失后可以通过后续播发的密钥计算得到，提高了认证服务稳定性与数据丢失的鲁棒性；其缺点在于需要发送方与接收方时钟同步.

ECDSA协议与TESLA协议两者的对比如表1所示.

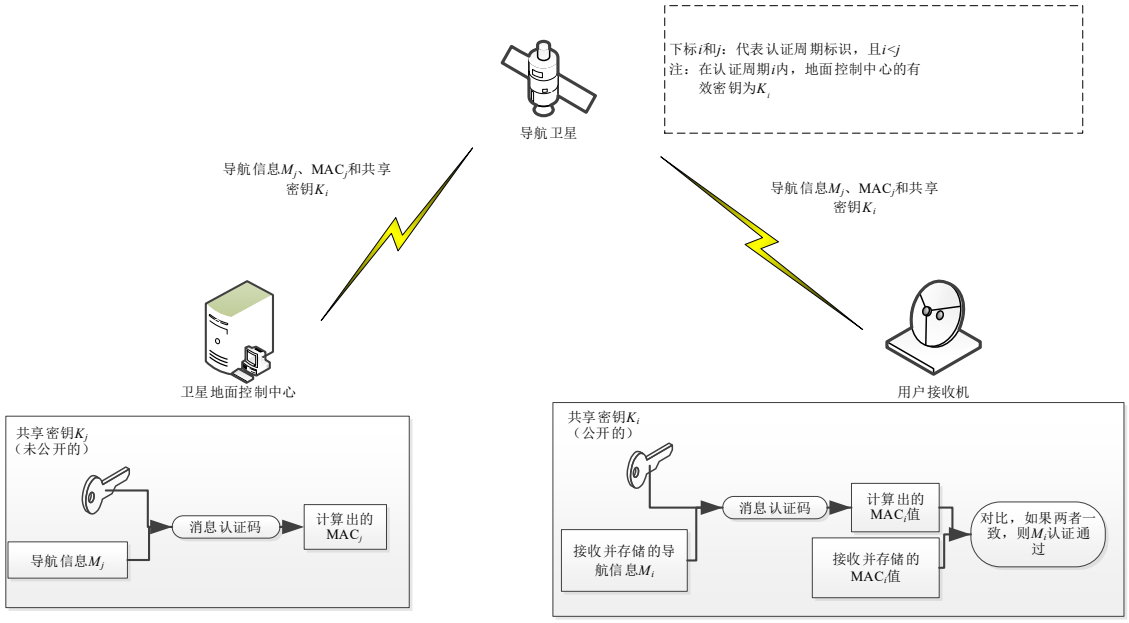

图2　TESLA协议认证流程

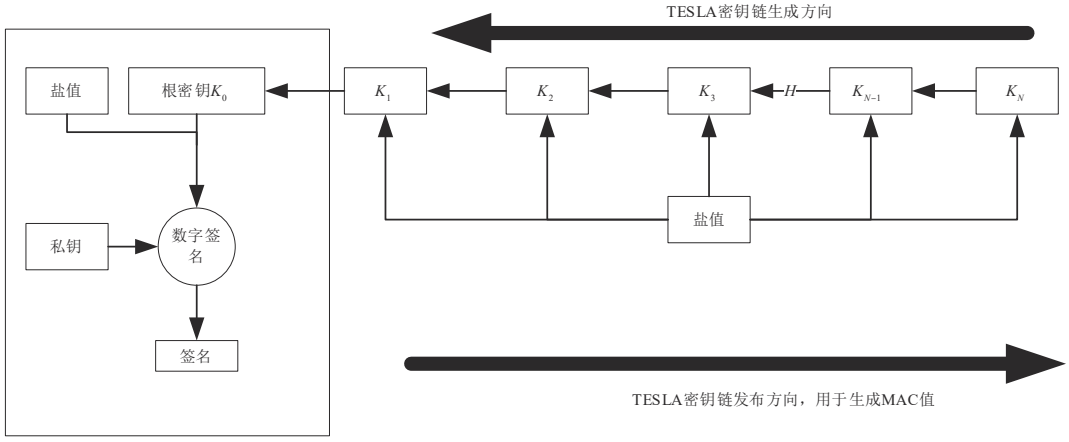

图3　TESLA单向密钥链的产生与密钥分发

表1 ECDSA协议与TESLA协议对比

认证协议	运算量	所需带宽	数据丢失鲁棒性	时钟同步
ECDSA	大	大	弱	不需要
TESLA	小	小	强	需要

2.1.3 认证方案选择

（1） 频点选择

SBAS认证服务可供选择的频点包括L1频点与L5频点. SBAS认证服务需要在现行的电文中添加认证标识，但是目前SBAS L1频点的电文格式已经固定，可以提供的带宽有限，不利于开展认证服务，随着2016年国际民航组织（International Civil Aviation Organization，ICAO）对双频多星座（Dual Frequency Multi Constellation，DFMC）接口控制文档的制定[13]，SBAS系统开始推进双频增强服务，计划增加L5频点的SBAS服务，因此SBAS L5频点是开展NMA的契机.

（2） I/Q支路选择

SBAS L5频点的电文播发通路包括同相支路（In-phase）和正交支路（Quadrature-phase）.

L5-I支路目前用于播发双频多星座电文，若在L5-I支路提供认证服务需要压缩SBAS电文的带宽，并且受SBAS完好性信息告警时间6 s的限制，I支路可提供给认证电文的带宽较小；L5-Q支路目前未调制电文，仅作为导频通路，若在L5-Q支路提供认证服务，SBAS电文和认证电文分别在L5-I路和L5-Q路并行播发，可提供给认证电文的带宽大，且无需考虑完好性信息告警时间.

（3） 认证方案选择

电文播发支路结合两种认证协议共有四种备选认证方案，即L5-I支路ECDSA方案、L5-I支路TESLA方案、L5-Q支路ECDSA方案以及L5-Q支路TESLA方案.

考虑两种认证协议所需的带宽与电文播发支路的特点，目前可行的认证方案为L5-I支路TESLA方案与L5-Q支路ECDSA方案.

2.2 基于国密的BDSBAS认证方案设计

中国商用密码算法是我国自主研发、具有知识产权的一系列密码算法. 其中SM2算法[14]是非对称密码算法，SM3算法[15]是密码杂凑算法.

2.2.1 基于SM2算法的Q支路ECDSA方案

我国ECDSA方案采用中国商用密码标准椭圆曲线（SM2）算法，SM2算法拥有固定的128位安全等级，私钥长度为256 bit，公钥长度为512 bit，签名长度为512 bit. 与国外使用算法相比[16]，SM2算法安全等级更高，但得到的数字签名长度更长，占用的传输带宽更大，各算法对比如表2所示.

表2 非对称密码算法对比

	中国	美国	欧洲
加密算法	SM2	ECDSA P-224	ECSCH
公钥长度	512 bit	224bit	512 bit
安全等级	128位	112位	128位
签名长度	512 bit	448 bit	512 bit

L5-Q支路ECDSA方案中，I支路播发BDS- BAS电文，Q支路播发认证电文，认证电文包括数字签名和密钥管理信息. SM2数字签名长度为512 bit，假定Q支路的信息速率和电文帧长度均与I支路一致，信息速率250 bps，电文帧长度为250 bit，则播发数字签名至少需要3帧，剩余带宽可用做OTAR位播发密钥管理信息.

具体格式如图4所示，M_i代表BDSBAS电文帧，DS_i表示SM2数字签名，OTAR表示密钥管理信息.

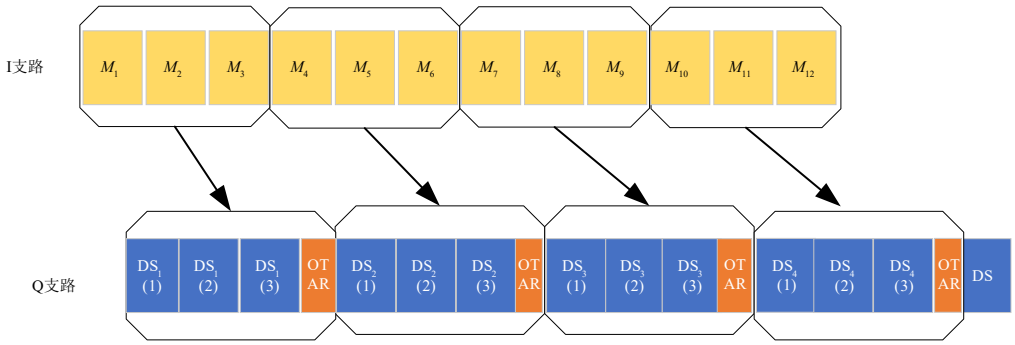

图4 L5-Q支路ECDSA方案电文格式

2.2.2 基于SM3算法的I支路TESLA方案

在BDSBAS系统中，L5-I支路TESLA方案使用中国商用密码算法密码杂凑（SM3）算法生成单向密钥链，利用HMAC（Hash-based Message Authentication Code）[17]算法通过单向散列函数来构造消息认证码，其中单向散列函数同样使用SM3算法. 同时对密钥链根密钥以及盐值使用SM2算法进行签名，得到数字签名，确保接收机接收到正确的密钥链.

SM3算法是在SHA-256基础上改进实现的一种算法，采用Merkle-Damgard结构，相比于SHA-256算法的设计结构更加复杂，安全性更高，输出为256 bit，目前国际上各类杂凑算法对比如表3所示.

表3　杂凑算法对比

	中国	美国	欧洲
加密算法	SM3	SHA-256	RIPEMD-256
算法结构	Merkle-Damgard结构	基于特殊的可逆模幂运算	基于特殊的可逆模幂运算
输入消息长度	$<2^{64}$	$<2^{64}$	$<2^{64}$
安全等级	128位	128位	128位
输出长度	256 bit(可截断)	256 bit(可截断)	256 bit(可截断)

SM3杂凑算法用于产生密钥链，并将产生的256 bit哈希值作为密钥，HMAC算法将密钥以及BDSBAS电文作为输入，输出256 bit的消息认证码. 由于I支路每一帧电文的长度为250 bit，为了节约带宽，在确保安全性的前提下，将密钥与MAC进行截断，密钥截断为115 bit，MAC截断为30 bit.

L5-I支路TESLA方案中，I支路播发BDSBAS电文和认证电文，认证电文包括MAC、延迟密钥和密钥管理信息. MAC和延迟密钥可在1帧内播发完成，剩余带宽可用做OTAR位播发密钥管理信息. 基于密钥延迟播发体制，用于生成当前MAC的密钥延迟6 s后播发，具体结构如图5所示，M_i代表BDSBAS电文帧，MAC表示截断后的消息认证码，K表示延迟密钥，OTAR表示密钥管理信息.

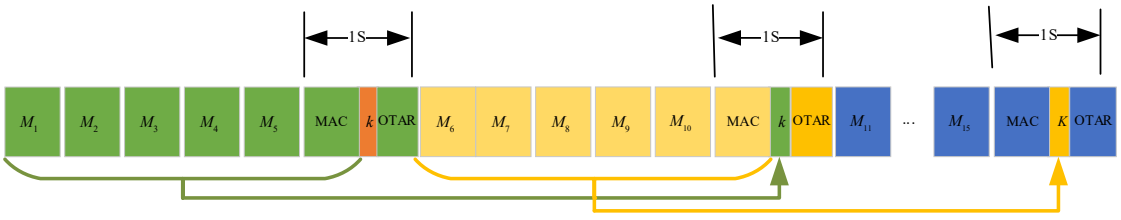

图5　L5-I支路TESLA方案电文格式

3　BDSBAS OTAR电文的设计

OTAR是指通过SBAS的广播信道传输辅助电文认证的密钥资料[16]，其内容主要为在认证过程中更新周期较长的密钥或者辅助密钥认证的密钥链信息. 用户在接收到OTAR电文以后，可以判断认证中使用的密钥是否被篡改，完成密钥的认证；同时用户还可以通过OTAR电文中关于下一周期密钥信息进行密钥更新[18].

3.1　ECDSA方案OTAR电文设计

ECDSA方案具有两级密钥结构，其中二级密钥为SM2算法公钥，也称为系统公钥，其使用周期一般为两年，用于认证SBAS电文；一级密钥为CA机构公钥，用于验证系统公钥的CA签名. ECDSA方案下的密钥结构见图6.

CA机构公钥在接收机生命周期内有效，出厂时预置于接收机，需要在OTAR电文中播发系统公钥及其CA数字签名. 考虑系统公钥更新需求，对当前系统公钥与下一周期的系统公钥分类标识分别进行播发，所有OTAR播发电文类型OMT（OTAR Message Type）见表4.

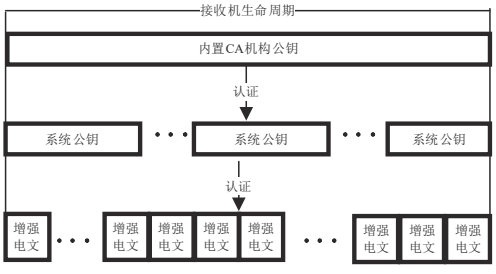

图6　ECDSA方案密钥结构

表4　L5-Q支路ECDSA方案OTAR电文

OTAR信息标识	定义	长度/bit
OMT1	当前系统公钥	512
OMT2	当前系统公钥+到期声明	512+30
OMT3	OMT1∣OMT2的数字证书	512
OMT4	下一个系统公钥	512
OMT5	下一个系统公钥的数字证书	512

系统公钥更新周期一般为两年，因此无需在当前系统公钥有效期内持续播发下一周期系统公钥相关电文. 本文提出两种系统状态，分场景设计OTAR播发电文见表5.

表5 L5-Q支路ECDSA方案系统状态以及OTAR播发电文

系统状态	播发内容	总长度/bits	备注
系统正常运行期	OMT1 & OMT3	1 024	常态播发
系统公钥更新期	OMT2&OMT3&OMT4&OMT5	2 078	提前两周播发

(1)系统正常运行期：当前系统公钥并未到期，OTAR位只需要播发当前系统公钥及其数字证书，即OMT1与OMT3.

(2)系统公钥更新期：提前两周开始播发当前系统公钥的到期声明、下一周期的系统公钥以及数字证书，即OMT2、OMT3、OMT4与OMT5.

3.2 TESLA方案OTAR电文设计

TESLA方案具有三层密钥结构，其中三级密钥为TESLA密钥链中的密钥，TESLA密钥链一般使用一周，主要用于认证SBAS电文；二级密钥为SM2算法的公钥，即系统公钥，使用周期两年，用于验证TESLA密钥链根密钥有效性；一级密钥为CA机构公钥，一般在接收机的生命周期内都有效，用于验证系统公钥的CA签名. TESLA方案下的3层密钥结构如图7所示.

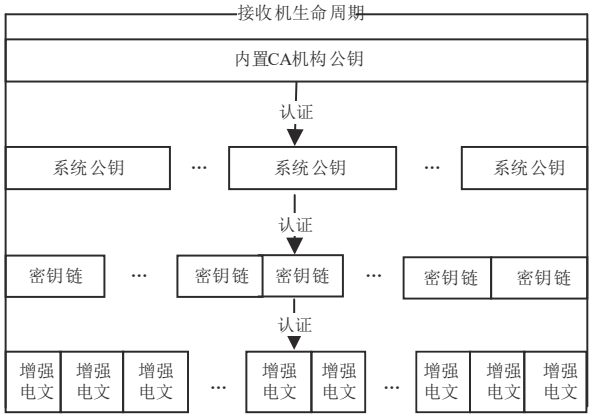

图7 TESLA方案密钥结构

与ECDSA方案相同，在接收机出厂时将CA公钥预置于接收机，需要在OTAR电文中播发系统公钥以及TESLA密钥链相关电文，所有OMT电文如表6.

表6 L5-I支路TESLA方案OTAR电文

OTAR信息标识	定义	长度/bit
OMT1	当前密钥链的盐值+根密钥	30+115
OMT2	当前密钥链的盐值+根密钥+到期声明	30+115+30
OMT3	OMT1∣OMT2的数字签名	512
OMT4	当前系统公钥	512
OMT5	当前系统公钥+到期声明	512+30
OMT6	OMT4∣OMT5的数字证书	512
OMT7	下一个密钥链的盐值+根密钥	30+115
OMT8	下一个密钥链的盐值+根密钥的数字签名	512
OMT9	下一个系统公钥	512
OMT10	下一个系统公钥的数字证书	512

相较于ECDSA方案，TESLA方案需额外使用密钥链，系统状态更为复杂，根据TESLA方案中的3层密钥结构，在TESLA方案中将系统状态分为以下三种，见表7.

(1)系统正常运行期：OTAR位只需要播发当前密钥链的根密钥与盐值，当前的系统公钥与数字证书，即播发电文OMT1、OMT3、OMT4与OMT6.

(2)系统公钥更换期：系统公钥即将到期需提前两周播发下一周期的系统公钥，播发电文为OMT1、OMT3、OMT5、OMT6、OMT9与OMT10.

(3)TESLA密钥链更换期：TESLA密钥链即将到期需要提前两天播发下一密钥链的根密钥与盐值，播发电文为OMT2、OMT3、OMT4、OMT6、OMT7与OMT8.

表7 L5-I支路TESLA方案系统状态以及OTAR播发电文

系统状态	111播发内容	总长/bits	备注
系统正常运行期	OMT1 & OMT3 & OMT4 & OMT6	1 681	常态播发
系统公钥更换期	OMT1 & OMT3 & OMT5 & OMT6 & OMT9 & OMT10	2 560	提前两周播发
密钥链更换期	OMT2 & OMT3 & OMT4 & OMT6 & OMT7 & OMT8	2 268	提前两天播发

4　OTAR电文播发仿真

为了分析本文设计方案性能，从理论分析入手获得不同的系统状态下接收机获取各类密钥电文所需时间的区间值；进一步，结合蒙特卡洛仿真实验，评估接收机不同启动状态下实现首次认证所需密钥的获取时间统计值．蒙特卡洛仿真器仿真从电文播发到用户接收的过程，首先构造出电文播发序列，仿真接收机在播发序列不同时刻开机对应接收到所需OTAR电文的时间．

在文中进行仿真实验时，将误码率统一设置为0，分析方案在理想情况下的最佳性能，同时通过10 000次仿真来模拟接收机的不同开机时刻，降低仿真结果的随机性．

4.1　ECDSA方案OTAR电文播发仿真

L5-Q支路每秒共有250 bit的带宽用于播发电文，将帧头、电文类型、数字签名以及循环校验码(Cyclic Redundancy Check，CRC)所占带宽减去，3 s内余136 bit用于OTAR电文播发，具体的格式如图8所示．

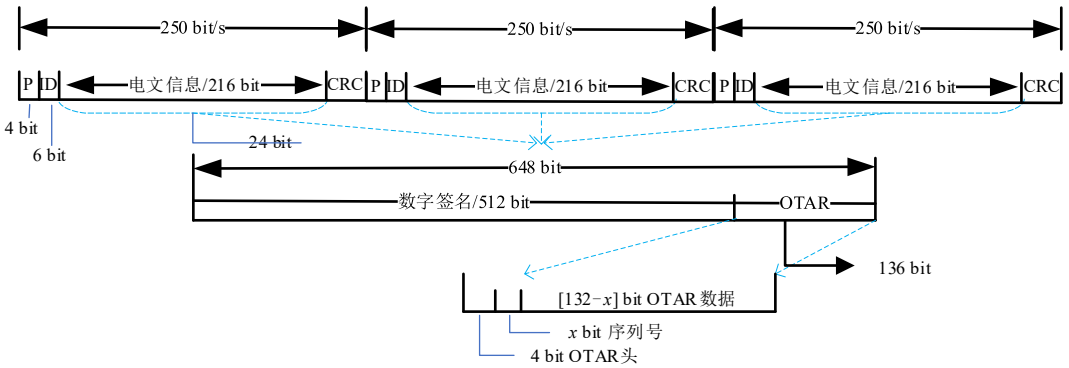

图8　L5-Q支路ECDSA方案OTAR位设计

图8中OTAR头是用来表征当前播发的密钥管理电文类型，设置为4 bit，可支持15种密钥管理电文类型，目前还有部分OMT电文内容未定义；序列号用来帮助接收机接收到OTAR电文后拼凑完整的密钥管理电文，针对不同长度的密钥管理电文，序列号位数不固定，因此在文中用X代替，表8为OTAR头与密钥管理电文类型的对应关系以及序列号所需位数．

表8　ECDSA方案OTAR头与OMT电文对应关系

OTAR头	密钥管理电文类型	序列号所需位数
0001	OMT1	2 bit
0010	OMT2	3 bit
0011	OMT3	2 bit
0100	OMT4	2 bit
0101	OMT5	2 bit
0110	OMT6	未定
…	…	…
1111	OMT15	未定

按照表5所示的L5-Q支路ECDSA方案OTAR播发策略，将各类OMT信息同频次顺序循环播发，可通过公式计算得出不同的系统状态下接收当前系统公钥及其CA签名、全部密钥信息所需时间，具体计算公式如下：

$$\begin{cases} T_{\mathrm{MAX}}=\left[\sum\dfrac{l_{\mathrm{ECDSA\text{-}\ OMT}X}\cdot n}{l_{\mathrm{ECDSA\text{-}\ OTAR}}-\mathrm{head}_{\mathrm{OTAR}}-\mathrm{Seq}_{\mathrm{OMT}X}}\right]\cdot t_{\mathrm{ECDSA}} \\ T_{\mathrm{MIN}}=\left[\sum\dfrac{l_{\mathrm{ECDSA\text{-}\ OMT}X}}{l_{\mathrm{ECDSA\text{-}\ OTAR}}-\mathrm{Head}_{\mathrm{OTAR}}-\mathrm{Seq}_{\mathrm{OMT}X}}-1\right]\cdot t_{\mathrm{ECDSA}}+1 \end{cases} \tag{1}$$

其中，OMT X代表OMT电文类型，在ECDSA方案下X取值为1~5；n代表在一个周期内OMT X电文类型的数目；$l_{\mathrm{ECDSA\text{-}\ OMT}X}$代表ECDSA方案下OMT X电文的长度；$l_{\mathrm{ECDSA\text{-}\ OTAR}}$表示ECDSA方案的OTAR位长度，为136 bit；$\mathrm{head}_{\mathrm{OTAR}}$表示OTAR头位数，两种方案都为4 bit；$\mathrm{Seq}_{\mathrm{OMT}X}$表示播发OMT X电文需要的序列号位数；t_{ECDSA}表示ECDSA方案下认证电文的播发周期，为3 s.

以系统公钥更换期下接收当前系统公钥及其CA签名为例，得到的仿真结果如图9所示．

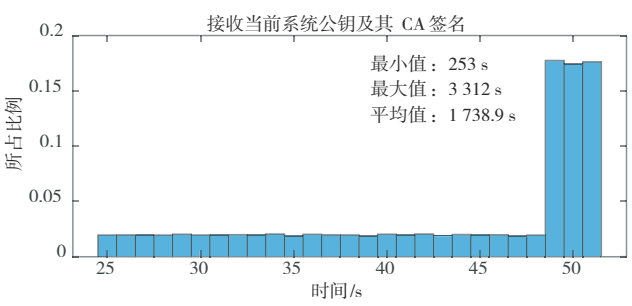

图9　接收系统公钥及其CA签名时间

所有仿真结果与理论计算一致，具体结果如表9所示.

表9 同频次顺序播发下ECDSA方案密钥接收时间

接收状态	系统状态	
	系统正常运行期	系统公钥更换期
接收当前系统公钥及其CA签名	区间: [22 s,24 s]	区间: [25 s,51 s]
接收全部密钥信息	区间: [22 s,24 s]	区间: [49 s,51 s]

为评估接收机侧的认证服务性能，结合ECDSA方案密钥结构，定义ECDSA方案下的两种接收机启动状态. ECDSA冷启动即除CA公钥外，接收机无任何密钥信息，此时，完成首次认证所需密钥获取时间取决于接收当前系统公钥及其CA签名所需时间；ECDSA热启动即接收机拥有当前系统公钥及其CA签名，此时，接收机开机后可直接进行认证，首次认证时间不受密钥获取时间限制. 根据ECDSA密钥的更新周期，一旦接收机开机完成了当前系统公钥的验证，则在当前系统公钥有效期的两年内任意时间开机均属于热启动.

使用蒙特卡洛仿真包仿真得到在ECDSA方案两种系统状态下，冷启动接收机完成首次认证所需密钥获取时间的平均值如表9所示. 将本文设计的方案与斯坦福大学方案的结果进行对比，其中斯坦福大学未区分系统状态[16]，得到表10.

表10 国内外ECDSA方案下接收机认证时间对比

接收机启动状态	斯坦福大学方案	本文设计方案不同状态	
		系统正常运行期	系统公钥更换期
冷启动	平均时间: 63.62 s	平均时间: 23.12 s	平均时间: 43.64 s

与斯坦福大学方案的结果相比，两种系统状态下接收机冷启动完成首次认证所需密钥的获取时间分别减少了63.66%与31.40%.

4.2 TESLA方案OTAR电文播发仿真

在L5-I支路TESLA方案中，SBAS电文与认证电文串行播发，6 s的周期内播发5 s的SBAS电文，余1 s用于播发认证电文，除去115 bit的延迟密钥以及30 bit的MAC[6]，剩余71 bit用于播发OTAR内容，具体结构图10所示. 其中OTAR头和序列号的定义与ECDSA方案相同.

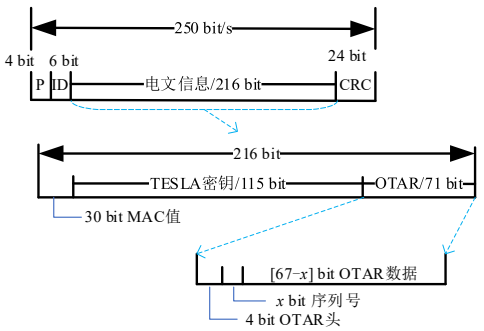

图10 L5-I支路TESLA方案OTAR位设计

在表7所示的L5-I支路TESLA方案OTAR播发策略下，考虑到系统公钥与密钥链的更新周期相差较大，在系统公钥的有效期内TESLA密钥链会多次更换，为确保TESLA密钥链电文被尽快接收，因此需要为TESLA密钥链电文分配更多带宽，提出各类OMT信息分频次顺序循环播发方法，如图10所示. 在系统公钥以及密钥链都未到期的状态下，将当前TESLA密钥链相关电文与当前系统公钥相关电文的播发频次之比设置为30∶10；在其他两种状态下，将当前TESLA密钥链相关电文、当前系统公钥相关电文、下一周期密钥链或系统公钥相关电文这三类电文的播发频次设置为30∶10∶1. 以表7中密钥链即将到期需要更换的系统状态为例，具体播发序列如图11所示.

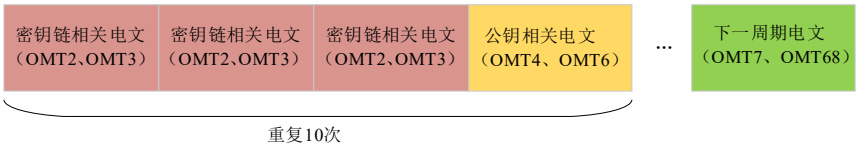

图11 TESLA方案下OMT分频次顺序循环播发方案示意图

TESLA方案下的理论时间计算公式如下：

$$\begin{cases} T_{\mathrm{MAX}}=\left[\sum\dfrac{l_{\mathrm{TESLA\text{-}\ OMT}\,X}\cdot n}{l_{\mathrm{TESLA\text{-}\ OTAR}}-\mathrm{head}_{\mathrm{OTAR}}-\mathrm{Seq}_{\mathrm{OMT}\,X}}\right]\cdot t_{\mathrm{TESLA}} \\ T_{\mathrm{MIN}}=\left[\sum\dfrac{l_{\mathrm{TESLA\text{-}\ OMT}\,X}}{l_{\mathrm{TESLA\text{-}\ OTAR}}-\mathrm{Head}_{\mathrm{OTAR}}-\mathrm{Seq}_{\mathrm{OMT}\,X}}-1\right]\cdot t_{\mathrm{TESLA}}+1 \end{cases} \tag{2}$$

其中，OMT X代表OMT电文类型，在TESLA方案下X取值为1~10；$l_{\mathrm{TESLA\text{-}OMT}\,X}$代表TESLA方案下OMT X电文的长度；n代表在一个周期内OMT X电文类型的数目；$l_{\mathrm{TESLA\text{-}OTAR}}$表示TESLA方案的OTAR位长度，为71 bit；t_{TESLA}表示TESLA方案下认证电文的播发周期，为6 s.

以TESLA密钥链即将到期需要更换的系统状态为例，通过蒙特卡洛仿真包按照上图所示播发序列进行仿真，得到的仿真结果如图12~14所示.

图中纵坐标“所占比例”是指仿真中在对应时间接

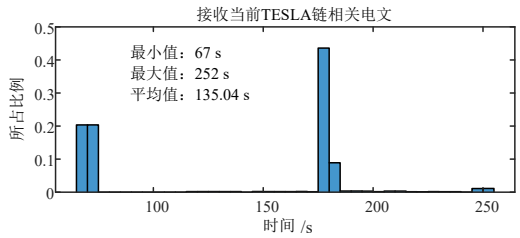

图12　接收当前密钥链相关电文的时间

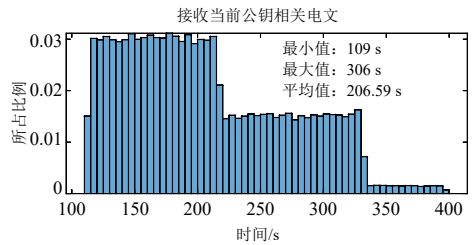

图13　接收当前系统公钥相关电文的时间

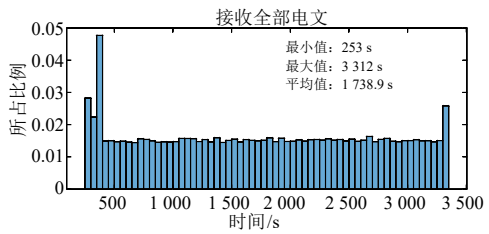

图14　接收全部电文的时间

收到所需电文的次数占全部仿真次数中的比例.

经过验证，理论计算得到的结果与仿真得到的结果一致，将三种系统状态下的仿真结果进行汇总得到接收机接收不同电文的时间见表11.

为评估接收机侧的认证服务性能，结合TESLA方案密钥结构，定义TESLA方案下的三种接收机启动状态. TESLA冷启动即除CA公钥外，接收机无任何密钥信息，此时，完成首次认证所需密钥获取时间取决于接收当前系统公钥及其CA签名、当前TESLA密钥链电文所需时间；TESLA温启动即接收机拥有当前系统公钥及其CA签名但是无当前TESLA密钥链信息，完成首次认证所需密钥获取时间取决于接收当前TESLA密钥链电文所需时间；TESLA热启动即接收机拥有当前TESLA密钥链相关信息和当前系统公钥及其CA签名，首次认证时间不受密钥获取时间限制. 根据TESLA各层级密钥的更新周期，一旦接收机开机完成了当前系统公钥的验证，则在当前系统公钥有效期的两年内任意时间开机均属于温启动. 一旦接收机开机完成了当前TESLA密钥链根密钥验证，则在当前TESLA密钥链有效期的一周内任意时间开机均属于热启动.

使用蒙特卡洛仿真包仿真得到在TESLA方案三种系统状态下，冷启动接收机和温启动接收机完成首次认证所需密钥获取时间的平均值如表12所示. 将本文设计的方案与斯坦福方案的结果进行对比，得到下表：

从表中可得，对于温启动接收机，当系统处于系统公钥以及密钥链都未到期的状态时，接收机完成首次认证所需密钥获取时间相比于斯坦福大学方案的结果降低了16.61%，其余两种状态所需时间均与斯坦福大学方案的结果相当. 对于冷启动接收机，当系统处于系统公钥以及密钥链都未到期的状态时，接收机完成首次认证所需密钥获取时间相比于斯坦福大学方案的结果相当，但其余两种系统状态下所需时间相较于斯坦福大学方案分别下降了14.93%和18.20%.

表11　分频次播发下TESLA方案接收时间

	系统状态		
	系统正常运行期	系统公钥更换期	密钥链更换期
接收当前TESLA链电文	区间:[67 s,180 s]	区间:[67 s,294 s]	区间:[67 s,252 s]
接收当前系统公钥及其CA签名	区间:[108 s,324 s]	区间:[116 s, 438 s]	区间:[109 s,396 s]
接收全部密钥信息	区间:[175 s,324 s]	区间:[295 s,3 408 s]	区间:[253 s,3 312 s]

表12　国内外TESLA方案下接收机认证时间对比

接收机启动状态	斯坦福大学方案	本文设计方案		
		系统正常运行期	系统公钥更换期	密钥链更换期
温启动	平均时间: 134.18 s	平均时间: 111.89 s	平均时间: 142.53 s	平均时间: 135.04 s
冷启动	平均时间: 252.57 s	平均时间: 251.01 s	平均时间: 214.85 s	平均时间: 206.59 s

由以上分析可得，本文所提TESLA方案下的OTAR播发方案仿真结果略优于斯坦福大学方案，可以改善BDSBAS认证服务性能.

5　结论

(1)ECDSA方案产生的数字签名长度较长，SBAS L5-I支路提供的带宽较小，不适合在I路实施ECDSA

方案；TESLA方案产生的消息认证码可以截断，占用带宽小，因此目前较为合适的认证方案为L5-I支路TESLA方案以及L5-Q支路ECDSA方案，本文结合中国商用密码标准SM2算法与SM3算法设计适合北斗系统的SBAS电文与认证电文格式.

（2）本文针对ECDSA方案以及TESLA方案的密钥结构，结合不同层级密钥的更新周期以及密钥生命周期特点，设计了不同系统状态下的空中密钥更新播发策略，及对应状态下的OTAR电文.

（3）根据仿真结果，对于ECDSA方案下OTAR电文同频次顺序循环播发方法，冷启动接收机实现首次认证所需密钥的获取时间平均值约为23 s和43 s，均优于斯坦福方案；TESLA方案下OTAR电文分频次顺序循环播发方法，对于冷启动和温启动接收机实现首次认证所需密钥获取时间相较于斯坦福方案在部分系统状态下性能相当，其余系统状态下性能有所提升.

（4）使用SM2算法的ECDSA方案与使用SM3算法的TESLA方案均满足安全性，但是在Q路实施认证需要考虑国际电联Res609协议，同时会增加认证的成本，同时TESLA协议的运算量小，数据丢失鲁棒性强，因此实际选择中应该选用L5-I支路TESLA方案进行认证.

（5）本文提出一种可行的BDSBAS认证方案，相较于国际现有的方案有一定的性能提升，对于未来BDSABS认证的发展提供可选技术方案.

参考文献

[1] 梁曦, 陶晓霞, 周昀, 等. 星基增强系统导航电文及完好性信息研究[J]. 空间电子技术, 2016, 13(5): 39-42, 47.
LIANG X, TAO X X, ZHOU Y, et al. Research of SBAS navigation message and integrity message[J]. Space Electronic Technology, 2016, 13(5): 39-42, 47. (in Chinese)

[2] 黄双临, 辛洁, 王冬霞, 等. 星基增强系统电文及播发特性研究[J]. 数字通信世界, 2019(2): 4-6, 3.
HUANG S L, XIN J, WANG D X, et al. Research on propagating message and strategy of satellite-based augmentation system[J]. Digital Communication World, 2019(2): 4-6, 3. (in Chinese)

[3] FERNÁNDEZ-HERNÁNDEZ I. GNSS authentication: Design parameters and service concepts[EB/OL]. (2014-04)[2022-04-20]. https://www. researchgate. net/profile/Ignacio-Fernandez-Hernandez/publication/264761996_GNSS_Authentication_Design_Parameters_and_Service_Concepts/links/53ee38070cf26b9b7dc655b8/GNSS-Authentication-Design-Parameters-and-Service-Concepts.pdf.

[4] CHIARA A D, BROI G D, POZZOBON O, et al. Authentication concepts for satellite-based augmentation systems [C]//Proceedings of the 29th International Technical Meeting of the Satellite Division of the Institute of Navigation. Portland: ION Institute of Navigation, 2016: 3208-3221.

[5] CHIARA A D, BROI G D, POZZOBON O, et al. SBAS Authentication proposals and performance assessment[C]// Proceedings of the 30th International Technical Meeting of the Satellite Division of the Institute of Navigation. Portland: ION Institute of Navigation, 2017: 2106-2116.

[6] NEISH A M, WALTER T, ENGE P. Parameter selection for the TESLA keychain[C]//Proceedings of the 31st International Technical Meeting of the Satellite Division of the Institute of Navigation. Portland: ION Institute of Navigation, 2018: 2155-2171.

[7] 穆盛林, 陈颖, 刘婷, 等. 面向BDSBAS电文认证的OTAR播发策略设计[J]. 北京航空航天大学学报, 2021, 47(7): 1453-1461.
MU S L, CHEN Y, LIU T, et al. Design of message authentication and OTAR broadcast strategy for BDSBAS[J]. Journal of Beijing University of Aeronautics and Astronautics, 2021, 47(7): 1453-1461. (in Chinese)

[8] 陈潇, 田翔, 罗瑞丹, 等. 基于TESLA协议的BDSBAS电文认证技术[J]. 北京航空航天大学学报, 2023, 49(9): 2289-2298.
CHEN X, TIAN X, LUO R D, et al. Design of message authentication based on TESLA protocol for BDSBAS[J]. Journal of Beijing University of Aeronautics and Astronautics, 2023, 49(9): 2289-2298. (in Chinese)

[9] NEISH A, WALTER T, ENGE P. Quantum-resistant authentication algorithms for satellite-based augmentation systems[J]. Navigation, 2019, 66(1): 199-209.

[10] WU Z J, LIU R S, CAO H J. ECDSA-based message authentication scheme for BeiDou-II navigation satellite system[J]. IEEE Transactions on Aerospace and Electronic Systems, 2019, 55(4): 1666-1682.

[11] NEISH A M, WALTER T, POWELL J. SBAS data authentication: A concept of operations[C]//Proceedings of the 32nd International Technical Meeting of the Satellite Division of the Institute of Navigation. Portland: ION Institute of Navigation, 2019: 1812-1823.

[12] PERRIG A, CANETTI R, TYGAR J D, et al. Efficient authentication and signing of multicast streams over lossy channels[C]//Proceeding 2000 IEEE Symposium on Security and Privacy. S&P 2000. Piscataway: IEEE, 2000: 56-73.

[13] Satellite Based Augmentation System Interoperability WorkingGroup. SBAS L5 DFMC interface control document:E-OC-7260-ESA[S]. Montreal: SBAS IWG, 2015.

[14] 国家质量监督检验检疫总局, 中国国家标准化管理委员会. 信息安全技术 SM2椭圆曲线公钥密码算法 第1部分:总则: GB/T 32918.1—2016[S]. 北京: 中国标准出版社, 2017.
General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China, Standardization Administration of the People's Republic of China. Information security technology—Public key cryptographic algorithm SM2 based on elliptic curves—Part 1: General: GB/T 32918.1—2016[S]. Beijing: Standards Press of China, 2017. (in Chinese)

[15] 中华人民共和国国家质量监督检查检验检疫总局, 中国国家标准化管理委员会. SM3密码杂凑算法: GB/T 32905——2016. [S]. 北京: 中国标准出版社, 2017.

[16] NEISH A, WALTER T, DAVID POWELL J. Design and analysis of a public key infrastructure for SBAS data authentication[C]//Proceedings of the ION 2019 Pacific PNT Meeting. Honolulu: Institute of Navigation, 2019: 964-988.

[17] 结城浩. 图解密码技术[M]. 周自恒,译. 2版. 北京: 人民邮电出版社, 2016.

[18] FERNÁNDEZ-HERNÁNDEZ I, CHÂTRE E, DALLA CHIARA A, et al. Impact analysis of SBAS authentication[J]. Navigation, 2018, 65(4): 517-532.

作者简介

田　翔　男,1998年8月出生于甘肃省武威市,毕业于兰州大学通信工程专业,现为中国科学院空天信息创新研究院在读研究生,主要研究方向为卫星导航、导航信号认证及密码学.
E-mail: tianxiang20@mails.ucas.ac.cn

陈　颖　女,现为中国卫星导航工程中心高级工程师,获信息与通信系统专业研究生学位,长期从事BDS总体设计、GNSS系统国际合作与标准、兼容性与互操作性、BDS系统测试验证等工作.

邵　搏　男,现为中国电子科技集团第二十研究所高级工程师,主要从事星基增强系统相关技术研究和软件研制工作.

罗瑞丹　女,现为中国科学院空天信息创新研究院副研究员,研究方向为卫星导航及其增强技术、机会信号定位技术等. 中国电子学会会员编号:E190025489S.

丁　群　男,现为中国电子科技集团公司首席专家,第二十研究所副总工程师,北斗星基增强系统民用服务平台总设计师,中国第二代卫星导航系统重大专项专家组专家,中国卫星导航定位协会北斗增强服务与应用专业委员会主任委员,中国卫星导航年会科学委员会委员,长期从事北斗系统及航空应用技术研究. 中国电子学会会员编号:E190008213M.

刘　婷　女,1986年6月出生于湖北省枣阳市,现为中国科学院空天信息创新研究院工程师,主要研究方向为导航信号认证.
E-mail: liuting101015@aircas.ac.cn