CLAIMS

What is claimed is:

1. A method for protecting a truncated parameter, wherein the method comprises:

determining, by a mobility management network element, whether a terminal meets a preset condition~~, wherein the preset condition comprises that the terminal uses a control plane cellular internet of things CIoT 5th generation system 5GS optimization function~~; and

sending, by the mobility management network element to the terminal when the terminal meets the preset condition, a downlink non-access stratum (NAS) message on which NAS security protection is performed by using a NAS security context, wherein the downlink NAS message comprises ~~a~~ the truncated parameter, and the truncated parameter is used to truncate a 5th generation-system architecture evolution-temporary mobile subscriber identity (5G-S-TMSI) of the terminal.

2. The method according to claim 1, wherein the truncated parameter is pre-stored in the mobility management network element.

~~3. The method according to claim 1, wherein the method further comprises:~~

~~receiving, by the mobility management network element, the truncated parameter from an access network device.~~

~~4~~3. The method according to ~~any one of~~ claim~~s~~ 1 ~~to 3~~, wherein the preset condition comprises that the terminal uses a control plane cellular internet of things (CIoT) 5th generation system (5GS) optimization function, ~~wherein~~ and the determining, by a mobility management network element, whether a terminal meets a preset condition comprises:

determining, by the mobility management network element, whether the terminal uses the control plane CIoT 5GS optimization function; and

~~if the terminal uses the control plane CIoT 5GS optimization function,~~ determining, by the mobility management network element when the terminal uses the control plane CIoT 5GS optimization function, that the terminal meets the preset condition~~; or~~

~~if the terminal does not use the control plane CIoT 5GS optimization function, determining, by the mobility management network element, that the terminal does not meet the preset condition~~.

~~5~~4. The method according to ~~any one of~~ claim~~s~~ 1 ~~to 3~~or 2, wherein the preset condition further comprises that the terminal is initially registered with a network; and

the determining, by a mobility management network element, whether a terminal meets a preset condition comprises:

determining, by the mobility management network element, whether the terminal uses the control plane CIoT 5GS optimization function and whether the terminal is initially registered with the network; and

if the terminal uses the control plane CIoT 5GS optimization function and the terminal is initially registered with the network, determining, by the mobility management network element, that the terminal meets the preset condition; or

if the terminal does not use the control plane CIoT 5GS optimization function or the terminal is not initially registered with the network, determining, by the mobility management network element, that the terminal does not meet the preset condition.

~~6~~5. The method according to claim ~~5~~4, wherein the determining, by the mobility management network element, whether the terminal is initially registered with the network comprises:

determining, by the mobility management network element based on a registration type reported by the terminal, that the terminal is initially registered with the network.

~~7~~6. The method according to ~~any one of~~ claim~~s~~ 1 or 2 ~~to 3~~, wherein the preset condition ~~further~~ comprises that the terminal uses a control plane cellular internet of things (CIoT) 5th generation system, 5GS, optimization function and the terminal needs to update the truncated parameter; and

the determining, by a mobility management network element, whether a terminal meets a preset condition comprises:

determining, by the mobility management network element, whether the terminal uses the control plane CIoT 5GS optimization function and whether the terminal needs to update the truncated parameter; and

~~if the terminal uses the control plane CIoT 5GS optimization function and the terminal needs to update the truncated parameter,~~ determining, by the mobility management network element when the terminal uses the control plane CIoT 5GS optimization function and the terminal needs to update the truncated parameter, that the terminal meets the preset condition~~; or~~

~~if the terminal does not use the control plane CIoT 5GS optimization function or the terminal does not need to update the truncated parameter, determining, by the mobility management network element, that the terminal does not meet the preset condition~~.

~~8~~7. The method according to claim ~~7~~6, wherein the determining, by the mobility management network element, whether the terminal needs to update the truncated parameter comprises:

when a truncated parameter configured in the mobility management network element is different from the truncated parameter that is stored in a context of the terminal, determining, by the mobility management network element, that the terminal needs to update the truncated parameter.

~~9~~8. The method according to claim ~~7~~6, wherein the determining, by the mobility management network element, whether the terminal needs to update the truncated parameter comprises:

after the mobility management network element updates the truncated parameter, determining, by the mobility management network element, that the terminal needs to update the truncated parameter.

~~10~~9. The method according to any one of claims ~~4~~ 3 to ~~9~~8, wherein the determining, by the mobility management network element, whether the terminal uses the control plane CIoT 5GS optimization function comprises:

~~if~~ when a preferred network behavior reported by the terminal indicates that the terminal prefers to use the control plane CIoT 5GS optimization function, and the mobility management network element supports the control plane CIoT 5GS optimization function, determining, by the mobility management network element, that the terminal uses the control plane CIoT 5GS optimization function.

~~11. The method according to any one of claims 4 to 9, wherein the determining, by the mobility management network element, whether the terminal uses the control plane CIoT 5GS optimization function comprises:~~

~~if the context of the terminal indicates that the terminal uses the control plane CIoT 5GS optimization function, determining, by the mobility management network element, that the terminal uses the control plane CIoT 5GS optimization function.~~

~~12~~10. The method according to any one of claims 1 to ~~11~~9, wherein the ~~determining, by a mobility management network element, whether a terminal meets a preset condition~~ method further comprises:

~~after the mobility management network element~~ receiving, by the mobility management network element,~~es~~ a registration request message ~~or a service request message of~~ from the terminal~~,~~ before determining~~, by the mobility management network element,~~ whether the

terminal meets the preset condition.

~~13~~11. The method according to any one of claims 1 to ~~12~~10, wherein the downlink NAS message is a service accept message or a registration accept message.

~~14~~12. The method according to any one of claims 1 to ~~13~~11, wherein the first bit to the tenth bit of the 5G-S-TMSI are used to indicate an access and mobility management function (AMF) set ID, the eleventh bit to the sixteenth bit of the 5G-S-TMSI are used to indicate an AMF pointer, and the seventeenth bit to the forty-eighth bit of the 5G-S-TMSI are used to indicate a 5G-TMSI; and

the truncated parameter comprises a first truncated parameter and a second truncated parameter, the first truncated parameter is used to truncate the AMF set ID and the 5G-TMSI, and the second truncated parameter is used to truncate the AMF pointer and the 5G-TMSI.

~~15. The method according to claim 14, wherein the method further comprises:~~

~~updating, by the mobility management network element, the truncated parameter based on a quantity of AMF set IDs and/or a quantity of AMF pointers; or~~

~~updating, by the mobility management network element, the truncated parameter according to an instruction of a network management system; or~~

~~receiving, by the mobility management network element, an updated truncated parameter sent by the access network device.~~

~~16~~13. A method for protecting a truncated parameter, wherein the method comprises:

receiving, by an ~~terminal~~apparatus from a mobility management network element, a downlink NAS message on which NAS security protection is performed by using a NAS security context, wherein the downlink NAS message comprises ~~a~~ the truncated parameter, and the truncated parameter is used to truncate a 5G-S-TMSI of the ~~terminal~~apparatus;

performing, by the ~~terminal~~apparatus, security deprotection on the downlink NAS message; and

storing, by the ~~terminal~~apparatus, the truncated parameter after successfully performing security deprotection on the downlink NAS message.

~~17~~14. The method according to claim ~~16~~13, wherein the storing, by the ~~terminal~~apparatus, the truncated parameter comprises:

storing, by a NAS layer of the ~~terminal~~apparatus, the truncated parameter.

~~18~~15. The method according to claim ~~17~~14, wherein the method further comprises:

sending, by the NAS layer of the ~~terminal~~apparatus, the truncated parameter to a radio

resource control (RRC) layer of the ~~terminal~~apparatus; and

truncating, by the RRC layer of the ~~terminal~~apparatus, the 5G-S-TMSI of the ~~terminal~~apparatus based on the truncated parameter, to obtain a truncated 5G-S-TMSI.

~~19. The method according to claim 17, wherein the method further comprises:~~

~~truncating, by the NAS layer of the terminal, the 5G-S-TMSI of the terminal based on the truncated parameter, to obtain a truncated 5G-S-TMSI; and~~

~~sending, by the NAS layer of the terminal, the truncated 5G-S-TMSI to an RRC layer of the terminal.~~

~~20. The method according to claim 16, wherein the storing, by the terminal, the truncated parameter comprises:~~

~~sending, by a NAS layer of the terminal, the truncated parameter to an RRC layer of the terminal; and~~

~~storing, by the RRC layer of the terminal, the truncated parameter.~~

~~21. The method according to claim 20, wherein the method further comprises:~~

~~truncating, by the RRC layer of the terminal, the 5G-S-TMSI of the terminal based on the truncated parameter, to obtain a truncated 5G-S-TMSI.~~

~~22. The method according to claim 20, wherein the method further comprises:~~

~~sending, by the RRC layer of the terminal, the truncated parameter to the NAS layer of the terminal;~~

~~truncating, by the NAS layer of the terminal, the 5G-S-TMSI of the terminal based on the truncated parameter, to obtain a truncated 5G-S-TMSI; and~~

~~sending, by the NAS layer of the terminal, the truncated 5G-S-TMSI to the RRC layer of the terminal.~~

~~23~~16. The method according to claim ~~18, 19, 21, or 22~~15, wherein the method further comprises:

sending, by the ~~terminal~~apparatus, an RRC reestablishment request message to an access network device, wherein the RRC reestablishment request message comprises the truncated 5G-S-TMSI.

~~24~~17. The method according to any one of claims ~~16~~ 13 to ~~23~~16, wherein the downlink NAS message is a service accept message or a registration accept message.

~~25~~18. The method according to any one of claims ~~16~~ 13 to ~~24~~17, wherein the first bit to the

tenth bit of the 5G-S-TMSI are used to indicate an access and mobility management function (AMF) set ID, the eleventh bit to the sixteenth bit of the 5G-S-TMSI are used to indicate an AMF pointer, and the seventeenth bit to the forty-eighth bit of the 5G-S-TMSI are used to indicate a 5G-TMSI; and

the truncated parameter comprises a first truncated parameter and a second truncated parameter, the first truncated parameter is used to truncate the AMF set ID and the 5G-TMSI, and the second truncated parameter is used to truncate the AMF pointer and the 5G-TMSI.

~~26. A method for protecting a truncated parameter, wherein the method comprises:~~

~~determining, by an access network device, whether a terminal supports a CIoT 5GS optimization feature; and~~

~~sending, by the access network device, a truncated parameter to a mobility management network element when the terminal supports the CIoT 5GS optimization feature, wherein the truncated parameter is used to truncate a 5G-S-TMSI of the terminal.~~

~~27. The method according to claim 26, wherein the determining, by an access network device, whether a terminal supports a CIoT 5GS optimization feature comprises:~~

~~if capability indication information of the terminal is used to indicate that the terminal supports the CIoT 5GS optimization feature, determining, by the access network device, that the terminal supports the CIoT 5GS optimization feature.~~

~~28. The method according to claim 26, wherein the determining, by an access network device, whether a terminal supports a CIoT 5GS optimization feature comprises:~~

~~if a frequency used by the terminal is the same as a frequency used by a CIoT device, determining, by the access network device, that the terminal supports the CIoT 5GS optimization feature.~~

~~29. The method according to claim 26, wherein the determining, by an access network device, whether a terminal supports a CIoT 5GS optimization feature comprises:~~

~~if a type of a message sent by the terminal is the same as a type of a message sent by a CIoT device, determining, by the access network device, that the terminal supports the CIoT 5GS optimization feature.~~

~~30. The method according to any one of claims 26 to 29, wherein the determining, by an access network device, whether a terminal supports a CIoT 5GS optimization feature comprises:~~

~~after the access network device receives an uplink RRC message sent by the terminal,~~

determining, by the access network device, whether the terminal supports the CIoT 5GS optimization feature.

31. The method according to claim 30, wherein the uplink RRC message is an RRC establishment request message or an RRC establishment complete message.

32. The method according to any one of claims 26 to 31, wherein the sending, by the access network device, a truncated parameter to a mobility management network element comprises:

sending, by the access network device, an initial UE message to the mobility management network element, wherein the initial UE message comprises the truncated parameter.

33. The method according to any one of claims 26 to 32, wherein the truncated parameter is pre-stored in the access network device.

34. The method according to any one of claims 26 to 33, wherein the method further comprises:

receiving, by the access network device, an RRC reestablishment request message sent by the terminal, wherein the RRC reestablishment request message comprises a truncated 5G-S-TMSI.

35. The method according to any one of claims 26 to 34, wherein the first bit to the tenth bit of the 5G-S-TMSI are used to indicate an AMF set ID, the eleventh bit to the sixteenth bit of the 5G-S-TMSI are used to indicate an AMF pointer, and the seventeenth bit to the forty-eighth bit of the 5G-S-TMSI are used to indicate a 5G-TMSI; and

the truncated parameter comprises a first truncated parameter and a second truncated parameter, the first truncated parameter is used to truncate the AMF set ID and the 5G-TMSI, and the second truncated parameter is used to truncate the AMF pointer and the 5G-TMSI.

36. A method for protecting a truncated parameter, wherein the method comprises:

updating, by a mobility management network element, a truncated parameter, wherein the truncated parameter is used to truncate a 5G-S-TMSI;

searching, by the mobility management network element, for a terminal that uses a control plane CIoT 5GS optimization function; and

sending, by the mobility management network element to the terminal that uses the control plane CIoT 5GS optimization function, a downlink NAS message on which NAS security protection is performed by using a NAS security context, wherein the downlink NAS message comprises the updated truncated parameter.

37. The method according to claim 36, wherein the updating, by a mobility management

network element, a truncated parameter comprises:

updating, by the mobility management network element, the truncated parameter based on a quantity of AMF set IDs and/or a quantity of AMF pointers; or

updating, by the mobility management network element, the truncated parameter according to an instruction of a network management system; or

receiving, by the mobility management network element, the updated truncated parameter sent by an access network device.

38. The method according to claim 36 or 37, wherein the sending, by the mobility management network element to the terminal that uses the control plane CIoT 5GS optimization function, a downlink NAS message on which NAS security protection is performed by using a NAS security context comprises:

when the terminal that uses the control plane CIoT 5GS optimization function is in a connected state, sending, by the mobility management network element, the downlink NAS message to the terminal that uses the control plane CIoT 5GS optimization function.

39. The method according to claim 36 or 37, wherein the sending, by the mobility management network element to the terminal that uses the control plane CIoT 5GS optimization function, a downlink NAS message on which NAS security protection is performed by using a NAS security context comprises:

when the terminal that uses the control plane CIoT 5GS optimization function is in a non-connected state, waiting, by the mobility management network element, for the terminal that uses the control plane CIoT 5GS optimization function to enter a connected state; and

after the terminal that uses the control plane CIoT 5GS optimization function enters the connected state, and the mobility management network element and the terminal that uses the control plane CIoT 5GS optimization function activate NAS security, sending, by the mobility management network element, the downlink NAS message to the terminal that uses the control plane CIoT 5GS optimization function.

40. The method according to claim 36 or 37, wherein the sending, by the mobility management network element to the terminal that uses the control plane CIoT 5GS optimization function, a downlink NAS message on which NAS security protection is performed by using a NAS security context comprises:

when the terminal that uses the control plane CIoT 5GS optimization function is in a non-

connected state, triggering, by the mobility management network element through paging, the terminal that uses the control plane CIoT 5GS optimization function to enter a connected state; and

after the terminal that uses the control plane CIoT 5GS optimization function enters the connected state, and the mobility management network element and the terminal that uses the control plane CIoT 5GS optimization function activate NAS security, sending, by the mobility management network element, the downlink NAS message to the terminal that uses the control plane CIoT 5GS optimization function.

41. The method according to any one of claims 36 to 40, wherein the downlink NAS message is a UE configuration update command message or a service accept message.

42. The method according to any one of claims 36 to 41, wherein the first bit to the tenth bit of the 5G-S-TMSI are used to indicate an AMF set ID, the eleventh bit to the sixteenth bit of the 5G-S-TMSI are used to indicate an AMF pointer, and the seventeenth bit to the forty-eighth bit of the 5G-S-TMSI are used to indicate a 5G-TMSI; and

the truncated parameter comprises a first truncated parameter and a second truncated parameter, the first truncated parameter is used to truncate the AMF set ID and the 5G-TMSI, and the second truncated parameter is used to truncate the AMF pointer and the 5G-TMSI.

43. A method for protecting a truncated parameter, wherein the method comprises:

receiving, by a mobility management network element, a truncated parameter sent by an access network device, wherein the truncated parameter is used to truncate a 5G-S-TMSI of a terminal;

performing, by the mobility management network element, integrity calculation on the 5G-S-TMSI of the terminal based on a NAS security context of the terminal, to generate a first NAS MAC; and

sending, by the mobility management network element, the first NAS MAC to the access network device.

44. The method according to claim 43, wherein the method further comprises:

receiving, by the mobility management network element, protection indication information and/or a freshness parameter sent by the access network device, wherein the protection indication information is used to indicate the mobility management network element to perform security protection on the truncated parameter, and the freshness parameter is used to perform integrity

calculation on the truncated parameter.

45. The method according to claim 43 or 44, wherein the first bit to the tenth bit of the 5G-S-TMSI are used to indicate an AMF set ID, the eleventh bit to the sixteenth bit of the 5G-S-TMSI are used to indicate an AMF pointer, and the seventeenth bit to the forty-eighth bit of the 5G-S-TMSI are used to indicate a 5G-TMSI; and

the truncated parameter comprises a first truncated parameter and a second truncated parameter, the first truncated parameter is used to truncate the AMF set ID and the 5G-TMSI, and the second truncated parameter is used to truncate the AMF pointer and the 5G-TMSI.

46. A method for protecting a truncated parameter, wherein the method comprises:

sending, by an access network device, a truncated parameter to a mobility management network element, wherein the truncated parameter is used to truncate a 5G-S-TMSI of a terminal;

receiving, by the access network device, a first NAS MAC sent by the mobility management network element, wherein the first NAS MAC is obtained by performing integrity calculation on the truncated parameter; and

sending, by the access network device, the first NAS MAC and the truncated parameter to the terminal.

47. The method for protecting a truncated parameter according to claim 46, wherein the method further comprises:

determining, by the access network device, whether the terminal supports a CIoT 5GS optimization feature; and

the sending, by an access network device, a truncated parameter to a mobility management network element comprises:

sending, by the access network device, the truncated parameter to the mobility management network element when the terminal supports the CIoT 5GS optimization feature.

48. The method according to claim 47, wherein the determining, by the access network device, whether the terminal supports a CIoT 5GS optimization feature comprises:

if capability indication information of the terminal is used to indicate that the terminal supports the CIoT 5GS optimization feature, determining, by the access network device, that the terminal supports the CIoT 5GS optimization feature.

49. The method according to claim 47, wherein the determining, by the access network device, whether the terminal supports a CIoT 5GS optimization feature comprises:

if a frequency used by the terminal is the same as a frequency used by a CIoT device, determining, by the access network device, that the terminal supports the CIoT 5GS optimization feature.

50. The method according to claim 47, wherein the determining, by the access network device, whether the terminal supports a CIoT 5GS optimization feature comprises:

if a type of a message sent by the terminal is the same as a type of a message sent by a CIoT device, determining, by the access network device, that the terminal supports the CIoT 5GS optimization feature.

51. The method according to any one of claims 47 to 50, wherein the determining, by the access network device, whether the terminal supports a CIoT 5GS optimization feature comprises:

after the access network device receives an uplink RRC message sent by the terminal, determining, by the access network device, whether the terminal supports the CIoT 5GS optimization feature.

52. The method according to claim 51, wherein the uplink RRC message is an RRC establishment request message or an RRC establishment complete message.

53. The method according to any one of claims 46 to 52, wherein the method further comprises:

sending, by the access network device, protection indication information and/or a freshness parameter to the mobility management network element, wherein the protection indication information is used to indicate the mobility management network element to perform security protection on the truncated parameter, and the freshness parameter is used to perform integrity calculation on the truncated parameter.

54. The method according to any one of claims 46 to 53, wherein the method further comprises:

receiving, by the access network device, an RRC reestablishment request message sent by the terminal, wherein the RRC reestablishment request message comprises a truncated 5G-S-TMSI.

55. The method according to any one of claims 46 to 54, wherein the first bit to the tenth bit of the 5G-S-TMSI are used to indicate an AMF set ID, the eleventh bit to the sixteenth bit of the 5G-S-TMSI are used to indicate an AMF pointer, and the seventeenth bit to the forty-eighth bit of the 5G-S-TMSI are used to indicate a 5G-TMSI; and

the truncated parameter comprises a first truncated parameter and a second truncated

parameter, the first truncated parameter is used to truncate the AMF set ID and the 5G-TMSI, and the second truncated parameter is used to truncate the AMF pointer and the 5G-TMSI.

56. A method for protecting a truncated parameter, wherein the method comprises:

receiving, by a terminal, a first NAS-MAC and a truncated parameter that are sent by an access network device, wherein the truncated parameter is used to truncate a 5G-S-TMSI of the terminal;

performing, by the terminal, integrity calculation on the truncated parameter based on a NAS security context, to generate a second NAS-MAC;

checking, by the terminal, the first NAS-MAC based on the second NAS-MAC; and

storing, by the terminal, the truncated parameter if the check on the first NAS-MAC succeeds.

57. The method according to claim 56, wherein the storing, by the terminal, the truncated parameter comprises:

storing, by an RRC layer of the terminal, the truncated parameter.

58. The method according to claim 57, wherein the method further comprises:

truncating, by the RRC layer of the terminal, the 5G-S-TMSI of the terminal based on the truncated parameter, to obtain a truncated 5G-S-TMSI.

59. The method according to claim 57, wherein the method further comprises:

sending, by the RRC layer of the terminal, the truncated parameter to a NAS layer of the terminal;

truncating, by the NAS layer of the terminal, the 5G-S-TMSI of the terminal based on the truncated parameter, to obtain a truncated 5G-S-TMSI; and

sending, by the NAS layer of the terminal, the truncated 5G-S-TMSI to the RRC layer of the terminal.

60. The method according to claim 56, wherein the storing, by the terminal, the truncated parameter comprises:

sending, by an RRC layer of the terminal, the truncated parameter to a NAS layer of the terminal; and

storing, by the NAS layer of the terminal, the truncated parameter.

61. The method according to claim 60, wherein the method further comprises:

truncating, by the NAS layer of the terminal, the 5G-S-TMSI of the terminal based on the truncated parameter, to obtain a truncated 5G-S-TMSI; and

sending, by the NAS layer of the terminal, the truncated 5G-S-TMSI to the RRC layer of the terminal.

62. The method according to claim 60, wherein the method further comprises:

sending, by the NAS layer of the terminal, the truncated parameter to the RRC layer of the terminal; and

truncating, by the RRC layer of the terminal, the 5G-S-TMSI of the terminal based on the truncated parameter, to obtain a truncated 5G-S-TMSI.

63. The method according to any one of claims 56 to 62, wherein the method further comprises:

sending, by the terminal, an RRC reestablishment request message to the access network device, wherein the RRC reestablishment request message comprises the truncated 5G-S-TMSI.

64. The method according to any one of claims 56 to 63, wherein the first bit to the tenth bit of the 5G-S-TMSI are used to indicate an AMF set ID, the eleventh bit to the sixteenth bit of the 5G-S-TMSI are used to indicate an AMF pointer, and the seventeenth bit to the forty-eighth bit of the 5G-S-TMSI are used to indicate a 5G-TMSI; and

the truncated parameter comprises a first truncated parameter and a second truncated parameter, the first truncated parameter is used to truncate the AMF set ID and the 5G-TMSI, and the second truncated parameter is used to truncate the AMF pointer and the 5G-TMSI.

65. A communications apparatus, comprising:

a processing module, configured to determine whether a terminal meets a preset condition, wherein the preset condition comprises that the terminal uses a control plane CIoT 5GS optimization function; and

a communications module, configured to send, to the terminal when the terminal meets the preset condition, a downlink NAS message on which NAS security protection is performed by using a NAS security context, wherein the downlink NAS message comprises a truncated parameter, and the truncated parameter is used to truncate a 5G-S-TMSI of the terminal.

66. The communications apparatus according to claim 65, wherein the communications apparatus further comprises a storage module; and

the storage module is configured to store the truncated parameter.

67. The communications apparatus according to claim 65, wherein

the communications module is further configured to receive the truncated parameter sent by

~~an access network device.~~

~~68. The communications apparatus according to any one of claims 65 to 67, wherein that the processing module is configured to determine whether the terminal meets the preset condition comprises:~~

~~determining whether the terminal uses the control plane CIoT 5GS optimization function; and~~

~~if the terminal uses the control plane CIoT 5GS optimization function, determining that the terminal meets the preset condition; or~~

~~if the terminal does not use the control plane CIoT 5GS optimization function, determining that the terminal does not meet the preset condition.~~

~~69. The communications apparatus according to any one of claims 65 to 67, wherein the preset condition further comprises that the terminal is initially registered with a network; and~~

~~that the processing module is configured to determine whether the terminal meets the preset condition comprises:~~

~~determining whether the terminal uses the control plane CIoT 5GS optimization function and whether the terminal is initially registered with the network; and~~

~~if the terminal uses the control plane CIoT 5GS optimization function and the terminal is initially registered with the network, determining that the terminal meets the preset condition; or~~

~~if the terminal does not use the control plane CIoT 5GS optimization function or the terminal is not initially registered with the network, determining that the terminal does not meet the preset condition.~~

~~70. The communications apparatus according to claim 69, wherein~~

~~the processing module is specifically configured to determine, based on a registration type reported by the terminal, that the terminal is initially registered with the network.~~

~~71. The communications apparatus according to any one of claims 65 to 67, wherein the preset condition further comprises that the terminal needs to update the truncated parameter; and~~

~~that the processing module is configured to determine whether the terminal meets the preset condition comprises:~~

~~determining whether the terminal uses the control plane CIoT 5GS optimization function and whether the terminal needs to update the truncated parameter; and~~

~~if the terminal uses the control plane CIoT 5GS optimization function and the terminal needs to update the truncated parameter, determining that the terminal meets the preset condition; or~~

if the terminal does not use the control plane CIoT 5GS optimization function or the terminal does not need to update the truncated parameter, determining that the terminal does not meet the preset condition.

72. The communications apparatus according to claim 71, wherein

the processing module is specifically configured to: when a truncated parameter configured in a mobility management network element is different from the truncated parameter that is stored in a context of the terminal, determine that the terminal needs to update the truncated parameter.

73. The communications apparatus according to claim 71, wherein

the processing module is specifically configured to: after the mobility management network element updates the truncated parameter, determine that the terminal needs to update the truncated parameter.

74. The communications apparatus according to any one of claims 68 to 73, wherein

the processing module is specifically configured to: if a preferred network behavior reported by the terminal is used to indicate that the terminal prefers to use the control plane CIoT 5GS optimization function, and the mobility management network element supports the control plane CIoT 5GS optimization function, determine that the terminal uses the control plane CIoT 5GS optimization function.

75. The communications apparatus according to any one of claims 68 to 73, wherein

the processing module is specifically configured to: if the context of the terminal indicates that the terminal uses the control plane CIoT 5GS optimization function, determine that the terminal uses the control plane CIoT 5GS optimization function.

76. The communications apparatus according to any one of claims 68 to 75, wherein

the processing module is specifically configured to: after the communications module receives a registration request message or a service request message of the terminal, determine whether the terminal meets the preset condition.

77. The communications apparatus according to any one of claims 65 to 76, wherein the downlink NAS message is a service accept message or a registration accept message.

78. The communications apparatus according to any one of claims 65 to 77, wherein the first bit to the tenth bit of the 5G-S-TMSI are used to indicate an AMF set ID, the eleventh bit to the sixteenth bit of the 5G-S-TMSI are used to indicate an AMF pointer, and the seventeenth bit to the forty-eighth bit of the 5G-S-TMSI are used to indicate a 5G-TMSI; and

the truncated parameter comprises a first truncated parameter and a second truncated parameter, the first truncated parameter is used to truncate the AMF set ID and the 5G-TMSI, and the second truncated parameter is used to truncate the AMF pointer and the 5G-TMSI.

79. The communications apparatus according to claim 78, wherein

the processing module is configured to update the truncated parameter based on a quantity of AMF set IDs and/or a quantity of AMF pointers; or

the processing module is configured to update the truncated parameter according to an instruction of a network management system; or

the communications module is configured to receive an updated truncated parameter sent by the access network device.

80. A communications apparatus, comprising:

a communications module, configured to receive a downlink NAS message that is sent by a mobility management network element and on which NAS security protection is performed by using a NAS security context, wherein the downlink NAS message comprises a truncated parameter, and the truncated parameter is used to truncate a 5G-S-TMSI of a terminal;

a processing module, configured to perform security deprotection on the downlink NAS message; and

a storage module, configured to store the truncated parameter after the processing module successfully performs security deprotection on the downlink NAS message.

81. The communications apparatus according to claim 80, wherein the storage module is configured to store the truncated parameter, comprising:

storing, by a NAS layer, the truncated parameter.

82. The communications apparatus according to claim 81, wherein the processing module is further configured to obtain a truncated 5G-S-TMSI, comprising:

sending, by the NAS layer, the truncated parameter to an RRC layer; and

truncating, by the RRC layer, the 5G-S-TMSI of the terminal based on the truncated parameter, to obtain the truncated 5G-S-TMSI.

83. The communications apparatus according to claim 81, wherein the processing module is further configured to obtain a truncated 5G-S-TMSI, comprising:

truncating, by the NAS layer, the 5G-S-TMSI of the terminal based on the truncated parameter, to obtain the truncated 5G-S-TMSI; and

sending, by the NAS layer, the truncated 5G-S-TMSI to an RRC layer.

84. The communications apparatus according to claim 80, wherein the storage module is configured to store the truncated parameter, comprising:

sending, by a NAS layer, the truncated parameter to an RRC layer; and

storing, by the RRC layer, the truncated parameter.

85. The communications apparatus according to claim 84, wherein the processing module is further configured to obtain a truncated 5G-S-TMSI, comprising:

truncating, by the RRC layer, the 5G-S-TMSI of the terminal based on the truncated parameter, to obtain the truncated 5G-S-TMSI.

86. The communications apparatus according to claim 84, wherein the processing module is further configured to obtain a truncated 5G-S-TMSI, comprising:

sending, by the RRC layer, the truncated parameter to the NAS layer;

truncating, by the NAS layer, the 5G-S-TMSI of the terminal based on the truncated parameter, to obtain the truncated 5G-S-TMSI; and

sending, by the NAS layer, the truncated 5G-S-TMSI to the RRC layer.

87. The communications apparatus according to claim 82, 83, 85, or 86, wherein

the communications module is further configured to send an RRC reestablishment request message to an access network device, wherein the RRC reestablishment request message comprises the truncated 5G-S-TMSI.

88. The communications apparatus according to any one of claims 80 to 87, wherein the downlink NAS message is a service accept message or a registration accept message.

89. The communications apparatus according to any one of claims 80 to 88, wherein the first bit to the tenth bit of the 5G-S-TMSI are used to indicate an AMF set ID, the eleventh bit to the sixteenth bit of the 5G-S-TMSI are used to indicate an AMF pointer, and the seventeenth bit to the forty-eighth bit of the 5G-S-TMSI are used to indicate a 5G-TMSI; and

the truncated parameter comprises a first truncated parameter and a second truncated parameter, the first truncated parameter is used to truncate the AMF set ID and the 5G-TMSI, and the second truncated parameter is used to truncate the AMF pointer and the 5G-TMSI.

90. A communications apparatus, comprising:

a processing module, configured to determine whether a terminal supports a CIoT 5GS optimization feature; and

a communications module, configured to send a truncated parameter to a mobility management network element when the terminal supports the CIoT 5GS optimization feature, wherein the truncated parameter is used to truncate a 5G-S-TMSI of the terminal.

91. The communications apparatus according to claim 90, wherein

the processing module is specifically configured to: if capability indication information of the terminal is used to indicate that the terminal supports the CIoT 5GS optimization feature, determine that the terminal supports the CIoT 5GS optimization feature.

92. The communications apparatus according to claim 90, wherein

the processing module is specifically configured to: if a frequency used by the terminal is the same as a frequency used by a CIoT device, determine that the terminal supports the CIoT 5GS optimization feature.

93. The communications apparatus according to claim 90, wherein

the processing module is specifically configured to: if a type of a message sent by the terminal is the same as a type of a message sent by a CIoT device, determine that the terminal supports the CIoT 5GS optimization feature.

94. The communications apparatus according to any one of claims 90 to 93, wherein

the processing module is specifically configured to: after the communications module receives an uplink RRC message sent by the terminal, determine whether the terminal supports the CIoT 5GS optimization feature.

95. The communications apparatus according to claim 94, wherein the uplink RRC message is an RRC establishment request message or an RRC establishment complete message.

96. The communications apparatus according to any one of claims 90 to 95, wherein

the communications module is specifically configured to send an initial UE message to the mobility management network element, wherein the initial UE message comprises the truncated parameter.

97. The communications apparatus according to any one of claims 90 to 96, wherein the communications apparatus further comprises a storage module; and

the storage module is configured to store the truncated parameter.

98. The communications apparatus according to any one of claims 90 to 97, wherein

the communications module is configured to receive an RRC reestablishment request message sent by the terminal, wherein the RRC reestablishment request message comprises a

truncated 5G-S-TMSI.

99. The communications apparatus according to any one of claims 90 to 98, wherein

the first bit to the tenth bit of the 5G-S-TMSI are used to indicate an AMF set ID, the eleventh bit to the sixteenth bit of the 5G-S-TMSI are used to indicate an AMF pointer, and the seventeenth bit to the forty-eighth bit of the 5G-S-TMSI are used to indicate a 5G-TMSI; and

the truncated parameter comprises a first truncated parameter and a second truncated parameter, the first truncated parameter is used to truncate the AMF set ID and the 5G-TMSI, and the second truncated parameter is used to truncate the AMF pointer and the 5G-TMSI.

100. A communications apparatus, comprising:

a processing module, configured to: update a truncated parameter, wherein the truncated parameter is used to truncate a 5G-S-TMSI; and search for a terminal that uses a control plane CIoT 5GS optimization function; and

a communications module, configured to send, to the terminal that uses the control plane CIoT 5GS optimization function, a downlink NAS message on which NAS security protection is performed by using a NAS security context, wherein the downlink NAS message comprises an updated truncated parameter.

101. The communications apparatus according to claim 100, wherein

the processing module is configured to: update the truncated parameter based on a quantity of AMF set IDs and/or a quantity of AMF pointers; or update the truncated parameter according to an instruction of a network management system; or receive the updated truncated parameter sent by an access network device.

102. The communications apparatus according to claim 100 or 101, wherein

the communications module is specifically configured to: when the terminal that uses the control plane CIoT 5GS optimization function is in a connected state, send the downlink NAS message to the terminal that uses the control plane CIoT 5GS optimization function.

103. The communications apparatus according to claim 100 or 101, wherein

the communications module is specifically configured to: when the terminal that uses the control plane CIoT 5GS optimization function is in a non-connected state, wait for the terminal that uses the control plane CIoT 5GS optimization function to enter a connected state; and after the terminal that uses the control plane CIoT 5GS optimization function enters the connected state, and a mobility management network element and the terminal that uses the control plane CIoT

5GS optimization function activate NAS security, send the downlink NAS message to the terminal that uses the control plane CIoT 5GS optimization function.

104. The communications apparatus according to claim 100 or 101, wherein

the communications module is specifically configured to: when the terminal that uses the control plane CIoT 5GS optimization function is in a non-connected state, trigger, through paging, the terminal that uses the control plane CIoT 5GS optimization function to enter a connected state; and after the terminal that uses the control plane CIoT 5GS optimization function enters the connected state, and a mobility management network element and the terminal that uses the control plane CIoT 5GS optimization function activate NAS security, send the downlink NAS message to the terminal that uses the control plane CIoT 5GS optimization function.

105. The communications apparatus according to any one of claims 100 to 104, wherein the downlink NAS message is a UE configuration update command message or a service accept message.

106. The communications apparatus according to any one of claims 100 to 105, wherein the first bit to the tenth bit of the 5G-S-TMSI are used to indicate an AMF set ID, the eleventh bit to the sixteenth bit of the 5G-S-TMSI are used to indicate an AMF pointer, and the seventeenth bit to the forty-eighth bit of the 5G-S-TMSI are used to indicate a 5G-TMSI; and

the truncated parameter comprises a first truncated parameter and a second truncated parameter, the first truncated parameter is used to truncate the AMF set ID and the 5G-TMSI, and the second truncated parameter is used to truncate the AMF pointer and the 5G-TMSI.

107. A communications apparatus, comprising:

a communications module, configured to receive a truncated parameter sent by an access network device, wherein the truncated parameter is used to truncate a 5G-S-TMSI of a terminal; and

a processing module, configured to perform integrity calculation on the 5G-S-TMSI of the terminal based on a NAS security context of the terminal, to generate a first NAS MAC, wherein

the communications module is further configured to send the first NAS MAC to the access network device.

108. The communications apparatus according to claim 107, wherein

the communications module is further configured to receive protection indication information and/or a freshness parameter sent by the access network device, wherein the protection indication

information is used to indicate a mobility management network element to perform security protection on the truncated parameter, and the freshness parameter is used to perform integrity calculation on the truncated parameter.

109. The communications apparatus according to claim 107 or 108, wherein the first bit to the tenth bit of the 5G-S-TMSI are used to indicate an AMF set ID, the eleventh bit to the sixteenth bit of the 5G-S-TMSI are used to indicate an AMF pointer, and the seventeenth bit to the forty-eighth bit of the 5G-S-TMSI are used to indicate a 5G-TMSI; and

the truncated parameter comprises a first truncated parameter and a second truncated parameter, the first truncated parameter is used to truncate the AMF set ID and the 5G-TMSI, and the second truncated parameter is used to truncate the AMF pointer and the 5G-TMSI.

110. A communications apparatus, comprising:

a communications module, configured to: send a truncated parameter to a mobility management network element, wherein the truncated parameter is used to truncate a 5G-S-TMSI of a terminal; receive a first NAS-MAC sent by the mobility management network element, wherein the first NAS-MAC is obtained by performing integrity calculation on the truncated parameter; and send the first NAS-MAC and the truncated parameter to the terminal.

111. The communications apparatus according to claim 110, wherein the communications apparatus further comprises a processing module;

the processing module is configured to determine whether the terminal supports a CIoT 5GS optimization feature; and

the communications module is specifically configured to send the truncated parameter to the mobility management network element when the terminal supports the CIoT 5GS optimization feature.

112. The communications apparatus according to claim 111, wherein

the processing module is specifically configured to: if capability indication information of the terminal is used to indicate that the terminal supports the CIoT 5GS optimization feature, determine that the terminal supports the CIoT 5GS optimization feature.

113. The communications apparatus according to claim 111, wherein

the processing module is specifically configured to: if a frequency used by the terminal is the same as a frequency used by a CIoT device, determine that the terminal supports the CIoT 5GS optimization feature.

~~114. The communications apparatus according to claim 111, wherein~~

~~the processing module is specifically configured to: if a type of a message sent by the terminal is the same as a type of a message sent by a CIoT device, determine that the terminal supports the CIoT 5GS optimization feature.~~

~~115. The communications apparatus according to any one of claims 111 to 114, wherein~~

~~the communications module is further configured to receive an uplink RRC message sent by the terminal; and~~

~~the processing module is specifically configured to: after the communications module receives the uplink RRC message sent by the terminal, determine whether the terminal supports the CIoT 5GS optimization feature.~~

~~116. The communications apparatus according to claim 115, wherein the uplink RRC message is an RRC establishment request message or an RRC establishment complete message.~~

~~117. The communications apparatus according to any one of claims 110 to 116, wherein~~

~~the communications module is further configured to send protection indication information and/or a freshness parameter to the mobility management network element, wherein the protection indication information is used to indicate the mobility management network element to perform security protection on the truncated parameter, and the freshness parameter is used to perform integrity calculation on the truncated parameter.~~

~~118. The communications apparatus according to any one of claims 110 to 117, wherein~~

~~the communications module is further configured to receive an RRC reestablishment request message sent by the terminal, wherein the RRC reestablishment request message comprises a truncated 5G-S-TMSI.~~

~~119. The communications apparatus according to any one of claims 110 to 118, wherein the first bit to the tenth bit of the 5G-S-TMSI are used to indicate an AMF set ID, the eleventh bit to the sixteenth bit of the 5G-S-TMSI are used to indicate an AMF pointer, and the seventeenth bit to the forty-eighth bit of the 5G-S-TMSI are used to indicate a 5G-TMSI; and~~

~~the truncated parameter comprises a first truncated parameter and a second truncated parameter, the first truncated parameter is used to truncate the AMF set ID and the 5G-TMSI, and the second truncated parameter is used to truncate the AMF pointer and the 5G-TMSI.~~

~~120. A communications apparatus, comprising:~~

~~a communications module, configured to receive a first NAS MAC and a truncated parameter~~

that are sent by an access network device, wherein the truncated parameter is used to truncate a 5G-S-TMSI;

a processing module, configured to: perform integrity calculation on the truncated parameter based on a NAS security context, to generate a second NAS MAC; and check the first NAS MAC based on the second NAS MAC; and

a storage module, configured to store the truncated parameter if the check on the first NAS MAC succeeds.

121. The communications apparatus according to claim 120, wherein the storage module is configured to store the truncated parameter, comprising:

storing, by an RRC layer, the truncated parameter.

122. The communications apparatus according to claim 121, wherein the processing module is further configured to obtain a truncated 5G-S-TMSI, comprising:

truncating, by the RRC layer, the 5G-S-TMSI of a terminal based on the truncated parameter, to obtain the truncated 5G-S-TMSI.

123. The communications apparatus according to claim 121, wherein the processing module is further configured to obtain a truncated 5G-S-TMSI, comprising:

sending, by the RRC layer, the truncated parameter to a NAS layer;

truncating, by the NAS layer, the 5G-S-TMSI of a terminal based on the truncated parameter, to obtain the truncated 5G-S-TMSI; and

sending, by the NAS layer, the truncated 5G-S-TMSI to the RRC layer.

124. The communications apparatus according to claim 120, wherein the storage module is configured to store the truncated parameter, comprising:

sending, by an RRC layer, the truncated parameter to a NAS layer; and

storing, by the NAS layer, the truncated parameter.

125. The communications apparatus according to claim 124, wherein the processing module is further configured to obtain a truncated 5G-S-TMSI, comprising:

truncating, by the NAS layer, the 5G-S-TMSI of a terminal based on the truncated parameter, to obtain the truncated 5G-S-TMSI; and

sending, by the NAS layer, the truncated 5G-S-TMSI to the RRC layer.

126. The communications apparatus according to claim 124, wherein the processing module is further configured to obtain a truncated 5G-S-TMSI, comprising:

~~sending, by the NAS layer, the truncated parameter to the RRC layer; and~~

~~truncating, by the RRC layer, the 5G-S-TMSI of a terminal based on the truncated parameter, to obtain the truncated 5G-S-TMSI.~~

~~127. The communications apparatus according to any one of claims 120 to 126, wherein the communications module is further configured to send an RRC reestablishment request message to the access network device, wherein the RRC reestablishment request message comprises the truncated 5G-S-TMSI.~~

~~128. The communications apparatus according to any one of claims 120 to 127, wherein the first bit to the tenth bit of the 5G-S-TMSI are used to indicate an AMF set ID, the eleventh bit to the sixteenth bit of the 5G-S-TMSI are used to indicate an AMF pointer, and the seventeenth bit to the forty-eighth bit of the 5G-S-TMSI are used to indicate a 5G-TMSI; and~~

~~the truncated parameter comprises a first truncated parameter and a second truncated parameter, the first truncated parameter is used to truncate the AMF set ID and the 5G-TMSI, and the second truncated parameter is used to truncate the AMF pointer and the 5G-TMSI.~~

~~129~~19. A communications apparatus, comprising:

at least one processor; and

a memory coupled to the processor and having program instructions stored thereon which, when executed by the at least one processor, cause the communications apparatus to:

determine whether a terminal meets a preset condition; and

send, to the terminal when the terminal meets the preset condition, a downlink non-access stratum (NAS) message on which NAS security protection is performed by using a NAS security context, wherein the downlink NAS message comprises a truncated parameter, and the truncated parameter is used to truncate a 5th generation-system architecture evolution-temporary mobile subscriber identity (5G-S-TMSI) of the terminal.

20. The communications apparatus according to claim 19, wherein the truncated parameter is pre-stored in the mobility management network element.

21. The communications apparatus according to claim 19 or 20, wherein the preset condition comprises that the terminal uses a control plane cellular internet of things (CIoT) 5th generation system (5GS) optimization function, and the program instructions further cause the communications apparatus to:

determine whether the terminal uses the control plane CIoT 5GS optimization function; and

determine that the terminal meets the preset condition when the terminal uses the control plane CIoT 5GS optimization function.

22. The communications apparatus according to claim 19 or 20, wherein the preset condition comprises that the terminal uses a control plane cellular internet of things (CIoT) 5th generation system, 5GS, optimization function and the terminal needs to update the truncated parameter, and the program instructions further cause the communications apparatus to:

determine whether the terminal uses the control plane CIoT 5GS optimization function and whether the terminal needs to update the truncated parameter; and

determine that the terminal meets the preset condition when the terminal uses the control plane CIoT 5GS optimization function and the terminal needs to update the truncated parameter.

23. The communications apparatus according to claim 21 or 22, wherein the program instructions further cause the communications apparatus to determine that the terminal uses the control plane CIoT 5GS optimization function when a preferred network behavior reported by the terminal indicates that the terminal prefers to use the control plane CIoT 5GS optimization function, and the communications apparatus supports the control plane CIoT 5GS optimization function.

24. The communications apparatus according to any one of claims 19 to 23, wherein the program instructions further cause the communications apparatus to receive a registration request message from the terminal before determining whether the terminal meets the preset condition.

25. The communications apparatus according to any one of claims 19 to 24 wherein the downlink NAS message is a service accept message or a registration accept message.

26. A communications apparatus, comprising:

at least one processor; and

a memory coupled to the processor and having program instructions stored thereon which, when executed by the at least one processor, cause the communications apparatus to:

receive, from a mobility management network element, a downlink NAS message on which NAS security protection is performed by using a NAS security context, wherein the downlink NAS message comprises the truncated parameter, and the truncated parameter is used to truncate a 5G-S-TMSI of the communications apparatus;

perform security deprotection on the downlink NAS message; and

store the truncated parameter after successfully performing security deprotection on the downlink NAS message.

27. The communications apparatus according to claim 26, wherein the program instructions further cause the communications apparatus to store, by a NAS layer of the communications apparatus, the truncated parameter.

28. The communications apparatus according to claim 27, wherein the program instructions further cause the communications apparatus to:

send, by the NAS layer of the communications apparatus, the truncated parameter to a radio resource control (RRC) layer of the terminal; and

truncate, by the RRC layer of the communications apparatus, the 5G-S-TMSI of the communications apparatus based on the truncated parameter, to obtain a truncated 5G-S-TMSI.

29. The communications apparatus according to claim 28, wherein the program instructions further cause the communications apparatus to send an RRC reestablishment request message to an access network device, wherein the RRC reestablishment request message comprises the truncated 5G-S-TMSI.

30. The communications apparatus according to any one of claims 26 to 29, wherein the downlink NAS message is a service accept message or a registration accept message.

~~a processor and a communications interface, wherein the processor is configured to execute a computer program instruction, so that the communications apparatus implements the method for protecting a truncated parameter according to any one of claims 1 to 64.~~

~~130~~31. A computer-readable storage medium, wherein the computer-readable storage medium stores an instruction, and when the instruction is run on a computer, the computer is enabled to perform the method for protecting a truncated parameter according to any one of claims 1 to ~~64~~18.

~~131. A computer program product, wherein the computer program product comprises an instruction, and when the computer program product runs on a computer, the computer is enabled to perform the method for protecting a truncated parameter according to any one of claims 1 to 64.~~

~~1~~32. A chip, comprising a processor, wherein when the processor executes a computer program instruction, the chip is enabled to perform the method for protecting a truncated parameter according to any one of claims 1 to 18~~64~~.