Attack-aware Self-logic-transformation Cryptographic Algorithm

Introduction.

this is a preview of the cryptographic algorithm that is based on AI technology. existing cryptography such as DES, AES, ECDSA, it is based on mathmathics and from it designed algorithms, encounters their limitation from the quauntum computing's powerful operation ability.

the algorithms based on mathmathics and its utilization with computing for the cryptography on the system is proved method by many expert. and currently, in many area in which systems need data encryption and decryption from that another area such as public key infra has been used for the purpose.

but, they can encounter expected limitation from internals of themselves.
many experts say that the algorithms utilized in various area to improve the security level of HW or SW based system can be broken by the quauntum computing's ability. the ability is based on the qubit, it has possibility to be determined by the instrument device, that is unchanged but its status being determined by the device can be changed. and from it, the ability is decided depending on the number of qubit.

AI technology based on the complicate operations and massive datas, the AI algorithm model use them to design and train the model and infer something for the purpose it want to achieve, is already utilizing in diverse industry.
with them, also parameter tuning is perceived as one of consideration to improve the model.
the operations, AI technology uses internals, highly complicated-form at the entire view. it is combined each other together and many operations are used to form the AI model.

under this circumstances, I want to propose this algorithm.
the main idea starts with combining the cryptography and AI to overcome the limitation of existing cryptographic algorithm from quauntum computing.

Expected Effect.

first of all, if this algorithm could have the proved ability to overcome the limitation and achieve to the goal, I think, this could be one of way to advance the cryptography.

this algorithm should meet these condition to achieve the goal of it.

attack-aware

with the AI operations and internal's operations, this algorithm should have ability to determine coming data or input could be attack or not.

self-logic-transformation

with the AI operations and internal's operations, this algorithm should have ability to transform internal's operations or its algorithmic logic.

cryptographic operation

with the AI operations and internal's operations, this algorithm should have ability to correctly decrypt the encrypted-data.

from under this conditions, expected effect will be below.

enhanced cryptographic performance
the complicate AI operations could be useful to hide internals operation comparing the existing algorithm.
it can means that AI makes internals more densely complicate.

also, this algorithm makes crpytographic strength more stronger.
one of features change itself when attack is coming.

low running-time comparing with existing algorithms
I cant accurately predict the running-time of this algorithm.
but I think the time of this algorithm needs more than existing algorithms.

encryption/decryption without cryptographic key
the key of cryptography is on how to safely keep the crpytographic key used for the algorithm.
but, AI operations need a lot of parameters so also it could hide the key inside

the model.