

Attack-aware Self-logic-transformation Cryptographic Algorithm

MIT License
Copyright (c) 2025 Sang Hun.

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 mathematics and from it designed algorithms, encounters their limitation from the quantum computing's powerful operation ability.

the algorithms based on mathematics 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 quantum 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 quantum 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.

it means the complexity of this algorithm could be self-changed from it the difficulty to break crpytographic operations will be higher.

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.

it means the parameters will be used by itself as key and the key will be changed by itself.

Expected Restriction.

at top view, this algorithm should have these ability as its functionalities to fully run and defend itself from attack.

attack-aware

in this phase, when data comes to this algorithm, the algorithm should get the data as itself and determine whether the data is attack or needs to be encrypted or decrypted.

if this determines the data as attack, it should pass the output to the next.

if this determines the data to be encrypt or decrypt, it should pass the data as itself to the next.

also, it should have ability to make itself more stronger by this ability it have to defend itself from the another expected-attack by malicious attacker to break this phase.

self-logic-transformation for cryptographic operation

in this phase, when the datas passed by the front phase comes to, this algorithm should get the data as itself and determine whether it have to change the operations inside this phase or have to encrypt or decrypt the data.

if the passed data is attack, it should change the operations in this phase.

if the passed data is pure, it should run cryptographic operations to encrypt or decrypt the data.

to continuously defend the attack, when it change the operations its goals should focus on how to enhance strength.

from under this conditions, expected problem will be below.

identifying attack

the data fed into this algorithm is considered as pure itself.

it should be determined as one of attack or data to be processed by this

algorithm.

under this condition, the data should be fixed-size.

if data is bigger or smaller, necessary tasks should be.

the factors to determine whether the data is attack or not should only be on this algorithm itself.

if others are combined with this algorithm for attack-aware, it will impact on this algorithm by changing the operations in each phase so entire operations in this algorithm will be changed.

therefore, the algorithm in attack-aware should be fixed-form or be redesigned if there is needs to customize this.

the output passed to next phase doesn't have to be complicate but should be fixed-size for processing in next phase.

its purpose is notifying the type of input data to next phase.

enhancing strength of each phase

the factors utilized to enhance strength of each phase should be on this algorithm itself and they should interact with each other at the entire operations.

the operations should be changed to enhance strength of this algorithm.

therefore, feedback should be at each phase.

self-transformation with purpose of correctly decrypting the data

when attack comes, the operations or algorithmic logic at each phase will be changed by itself.

the main purpose of this functionality is not on changing itself but on how to correctly decrypt the encrypted data under with changing operations and parameters used as key.

DESIGN.

under this conditions, this algorithm will have below structure but it can be changed.



Figure 1. overview of algorithm.

the Input is pure data but it can be attack by malicious attacker.
the Output is outcome of this algorithm and it can be one of encrypted data or decrypted data by this algorithm.

attack-aware phase will have below structure.

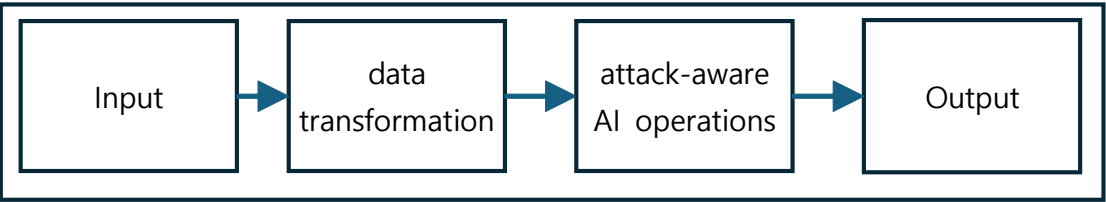


Figure 2. top view of attack-aware phase.

at top view of attack-aware phase, it runs AI operations for the purpose.
in this phase, main purpose is determining that attack from data exists.
then if the attack appears it should run operations to enhance its strength.
if attack doesn't appear, pass the data to next phase.



Figure 3. middle-level view of attack-aware phase.

attack-aware operations will be consisted of some layers.

self-logic-transformation phase will have below structure.



Figure 4. top view of self-logic-transformation phase.

at top view of self-logic-transformation phase, it runs AI operations for the purpose.
in this phase, main tasks are cryptographic operation transformation for encryption and decryption, operation enhancing strength.



Figure 5. middle-level view of self-logic-transformation phase.

low-level view of each phase will be added.

Expected Problem.