Via PUF Technology

There are various PUF technologies, but most of them are implemented using active devices, which are sensitive to PVT (process, voltage, temperature) changes, and are also prone to aging. To overcome this, an ECC (Error Correction Code) logic function must be additionally introduced.

However, VIA PUF is a technology that implements PUF by using the process deviation that occurs minutely when forming the via hole connecting the metal layers during the semiconductor production process.

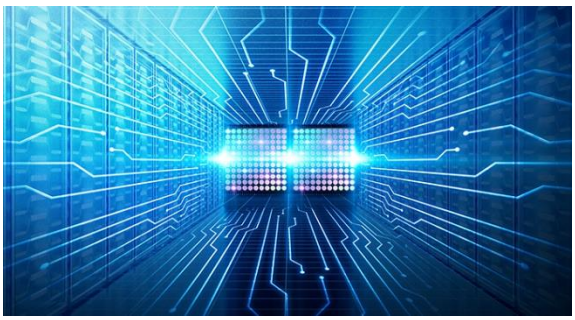
This is a passive device method that is different from the existing active device method. It is an innovative method that solves all the problems of existing technologies.

Although it is made with the same design in the same process of semiconductor production, each semiconductor chip has different characteristics because it uses fine tolerances.
That is, different IDs are generated for each semiconductor chip.

This is also called the fingerprint of the semiconductor.

> Silicon Inborn ID

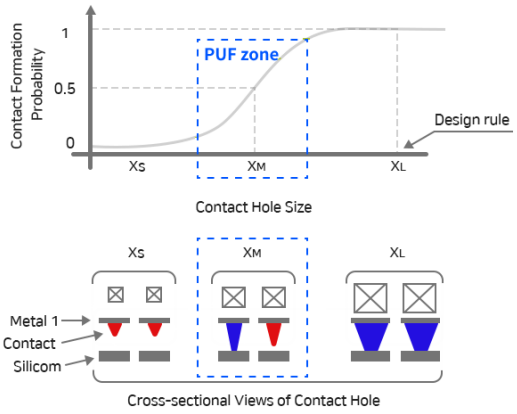
VIA PUF is the result of a "thinking shift" that reverses the semiconductor design method that has been taken for granted.



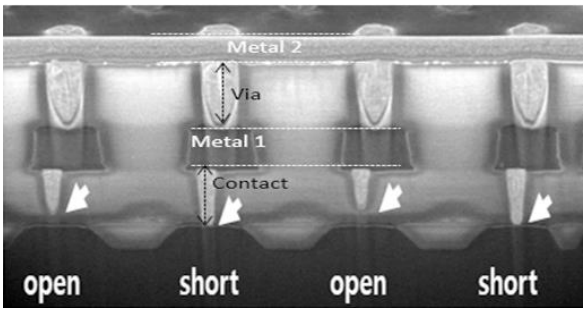
Although general semiconductor designs are created for the purpose of forming via holes, VIA PUF is designed by choosing between the formation of via holes and non-formation of via holes. Accordingly, the VIA PUF has unpredictable randomness (meeting the NIST SP800-90B standard), in which short and open appear half and half.

Due to the characteristics of the VIA Hole, which is a passive device, it has a homeostasis that does not change its characteristics in any environment change.

Since it is indistinguishable from general Via VIA, it has security that cannot be distinguished even with reverse engineering.

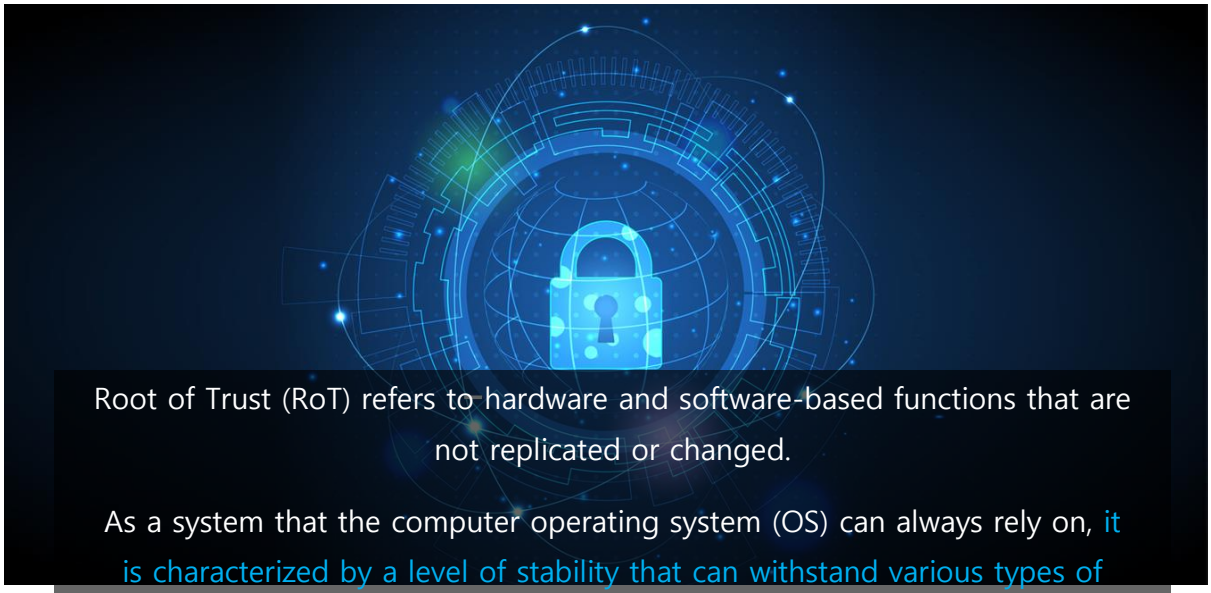


[a]PUF zone at 50% probability of Via or Contact fomation



[b]Cross sectional microscopic image of VIA PUF

Root of Trust based on Via PUF

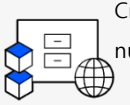


Root of Trust (RoT) refers to hardware and software-based functions that are not replicated or changed.

As a system that the computer operating system (OS) can always rely on, it is characterized by a level of stability that can withstand various types of hacking attacks.

RoT cannot be achieved with SW alone, and

it is **important to have a HW-based RoT.**



Create a Unique ID and use this random number to generate

an encryption key ▶ **Root of Trust**

Via PUF is the foundation of RoT, **the source of all trust,**

by providing the characteristics of a unique Silicon Inborn ID.

Instead of injecting a unique ID from the outside,

it is generated internally: **improved security**

Due to the characteristics of the Via Hole, which is a passive device, it has a **homeostasis** that does not change

its characteristics in any environment change.

The table below shows the Via PUF-based RoT function and its implementation method.

Properties	RoT Function	Implementation
Uniqueness	Create a unique ID on a physical device	Via PUF
Integrity	Integrity verification function for firmware	Via PUF + asymmetric key algorithm
Execution Security	Secure firmware update	Via PUF + asymmetric key algorithm
Data Security	Secure Storage (Digital key or Certificate protection	Via PUF
Randomness	Unpredictable function by securing randomness	Via PUF
Encryption	Crypto Accelerator	Via PUF + encryption algorithm
Communication security	Generate private key in communication protocol	Via PUF + communication algorithm