“Finding the answer in nature, which may seem similar but is never the same” GIST and KAIST develop unclonable optical fingerprint security technology that mimics natural structural color

- GIST Department of Electrical Engineering and Computer Science Professor Hyeon-Ho Jeong's team and KAIST Professor Young Min Song's team jointly implemented a nano-optical-based selective authentication optical security device... Anti-counterfeiting and tampering without design damage, and innovation in genuine authentication expected

- Results of actual applications such as pharmaceuticals have proven stability even in high temperature, high humidity, and friction environments, and secured industrial usability through large-area process application... Published in the international academic journal 《Nature Communications》

▲ (Clockwise from top left) Professor Hyeon-Ho Jeong of the Department of Electrical Engineering and Computer Science at GIST, Professor Young Min Song of the School of Electrical Engineering at KAIST, Researcher Gyurin Kim of the Department of Electrical Engineering and Computer Science at GIST, Dr. Se-Yeon Heo, Researcher Juhwan Kim, Researcher JuHyeong Lee, Dr. Doeun Kim

The Gwangju Institute of Science and Technology (GIST, President Kichul Lim) announced that a joint research team led by Professor Hyeon-Ho Jeong of the Department of Electrical Engineering and Computer Science and Professor Young Min Song of the School of Electrical Engineering at the Korea Advanced Institute of Science and Technology (KAIST) developed a security authentication technology that cannot be copied using nano-optical technology inspired by nature.

This technology can be easily inserted into various physical products such as ID cards or QR codes, and is characterized by providing a strong anti-counterfeiting function without damaging the design because it is

indistinguishable from existing products to the naked eye. It can be widely used in areas where authenticity authentication is important, such as high-end consumer goods, pharmaceuticals, and electronic products.

Until now, QR codes and barcodes used to prevent counterfeiting had limitations in that they were easy to copy and difficult to assign unique information to each product.

A technology that has recently been gaining attention to complement this is the 'physically unclonable function (PUF).'

This can improve security and authentication reliability by using the randomness that naturally occurs during the product manufacturing process to give each product unique physical characteristics to the device.

However, existing PUF technology has secured randomness and uniqueness, but it has the disadvantage of being difficult to control surface color and being easily identifiable from the outside, making it vulnerable to security.

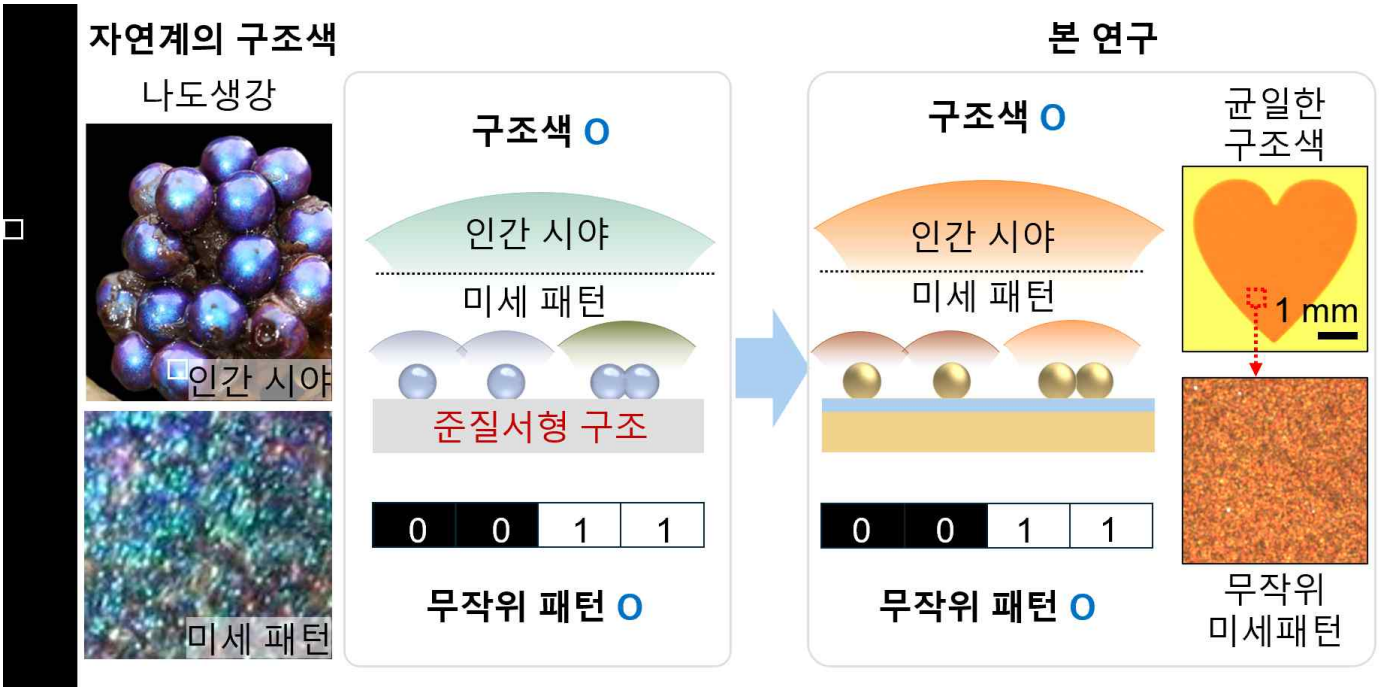
* physically unclonable function (PUF): This is a technology that generates a unique authentication key by using physical changes formed during the process. Since the randomness of the process cannot be replicated, it has the advantage of not being able to produce hardware for actual authentication even if authentication information is stolen.

Accordingly, the research team focused on the unique structural color* phenomenon observed in natural organisms. For example, butterfly wings, bird feathers, and seaweed leaves are arranged in a 'quasi-order*' form that is neither completely orderly nor completely disordered by nanometer-sized microstructures.

These structures have a uniform color to the naked eye, but internally, there is subtle randomness, enabling the performance of functions advantageous to survival such as camouflage, communication, and predator avoidance.

* quasi-order: An arrangement that is neither completely regular nor completely disordered, meaning an intermediate structure where microstructures follow a certain pattern but are partially random. In nature, it is commonly found in butterfly wings, seaweed leaves, and bird feathers, and creates a uniform color as well as unique optical properties.

* structural color: A color that appears when microstructures aligned at the nanometer level interact with light, rather than pigments. It is a natural phenomenon often observed on the surfaces of plants and animals. For example, the color of butterfly wings or peacock feathers are representative structural colors.



▲ structural color through quasi-ordered structures: (Left) Structural color through quasi-ordered structures in nature, and (Right) Optical security devices fabricated in this study by imitating this.

The research team imitated this natural principle by depositing a thin layer of dielectric (HfO_2) on a metal mirror, and then electrostatically self-assembled gold nanoparticles tens of nanometers in size on top of it to create a plasmonic metasurface with a quasi-ordered structure*.

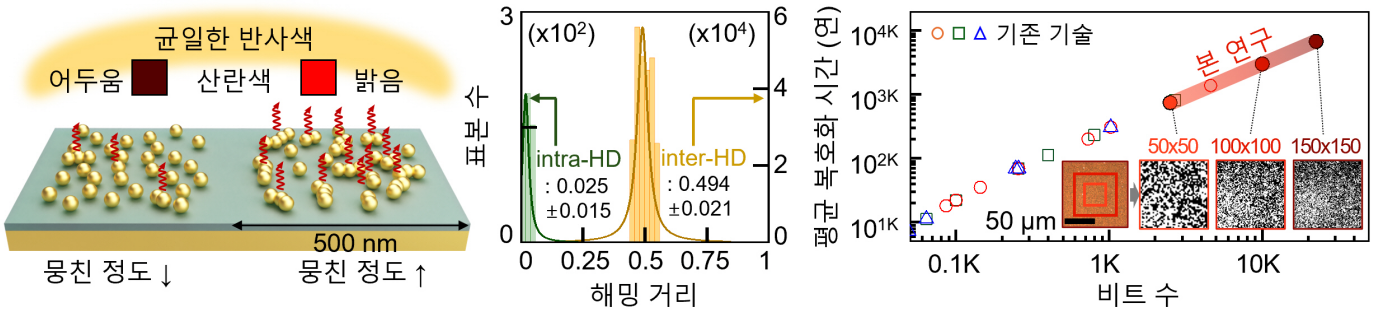
When seen with the naked eye, this structure has a constant reflected color, but when observed under a high-magnification optical microscope, a random scattering pattern, or optical fingerprint*, appears in each area.

Thanks to this seemingly identical nanostructure that can never be duplicated internally, it can be applied as a high-dimensional security authentication device that can hide or selectively expose invisible unique information.

* plasmonic metasurface: An ultra-thin optical structure designed to freely control the phase, polarization, and intensity of light by precisely arranging nanometer-sized metal structures on a plane. By forming a strong electromagnetic field locally using the surface plasmon resonance phenomenon that occurs on the metal surface, it can interact with light much more compactly and precisely than existing optical elements.

* optical fingerprint: A technology that identifies each structure by utilizing the unique reflection, scattering, and interference patterns that appear when light is irradiated on the structure, and is a physical security measure that is virtually impossible to duplicate. Microstructures randomly formed on the nano or micrometer scale are difficult to duplicate in the same way, and the optical response generated from this structure acts as a unique identification value for each element.

The research team also confirmed that utilizing random patterns generated from nanostructures improves the PUF performance of the device compared to the existing ones.

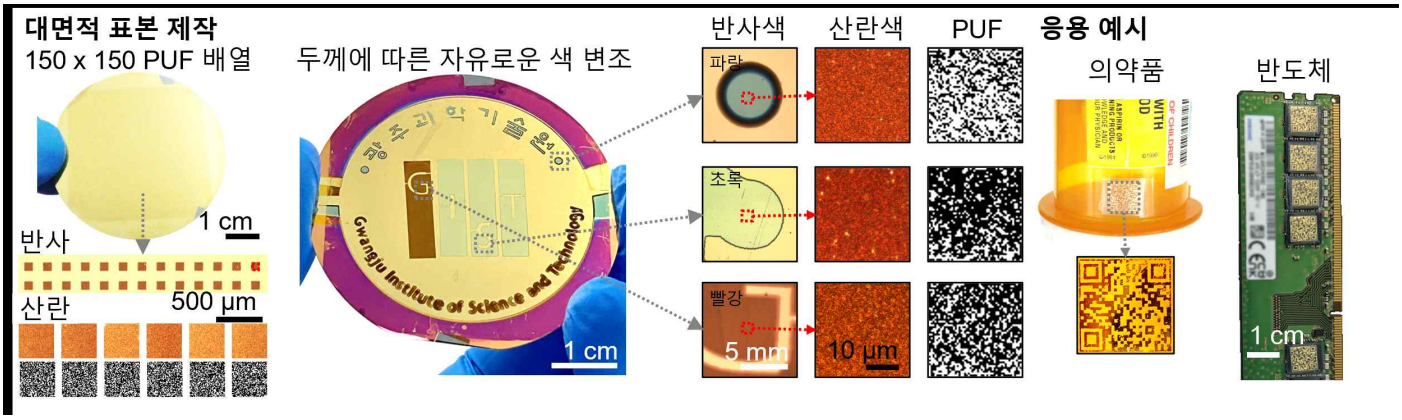


▲ Operating principle and main performance indicators of the manufactured PUF: (Left) Random scattering color due to the degree of agglomeration of metal nanoparticles. (Right) Representative performance indicators of the optical security device developed in this study

The structure itself is tens of micrometers in size, but the pattern containing information is on the nanometer level, so it can store a vast amount of information exceeding the world's population.

In addition, assuming that a hacker randomly creates a device to hack this security system, the time it takes to decrypt it is longer than the age of the Earth, making it virtually impossible to replicate.

The research team demonstrated the possibility of practical industrial use of the developed security device through a technology demonstration that applied it to pharmaceuticals, semiconductors, QR codes, etc.



▲ Examples for real-life applications: (Left) Example of large-area manufacturing using optical PUF (Right) Example of application to actual anti-counterfeiting/tampering products

As a result of generating and analyzing over 500 PUF keys, the average of the bit value distribution was 0.501, which is close to the ideal balance (0.5), and the Hamming distance, which indicates the difference between different keys, was also measured at an average of 0.494, showing high uniqueness and stability.

In addition, the scattering pattern was stably maintained even under various environmental changes such as high temperature, high humidity, and friction, confirming excellent durability.

Professor Hyeon-Ho Jeong of GIST explained, “By reproducing the structure where natural order and disorder coexist using nanotechnology, we were able to implement optical information that cannot be essentially copied even if the appearance is the same.” He added, “This technology can be utilized as a powerful anti-counterfeiting measure in various fields such as high-end consumer goods, pharmaceutical product authentication, and national security.”

Professor Young Min Song of KAIST emphasized, “While existing security labels can be easily deformed even with minor damage, this technology simultaneously secures structural stability and

unduplicateability," and "In particular, it will be able to present a new paradigm for security authentication in that it can separate visible color information from invisible unique key information."

This research, supervised by Professor Hyeon-Ho Jeong of the Department of Electrical Engineering and Computer Science at GIST and Professor Young Min Song of the School of Electrical Engineering at KAIST and conducted by researchers Gyurin Kim, Doeun Kim, JuHyeong Lee, Juhwan Kim, andSe-Yeon Heo, was supported by the Ministry of Science and ICT and the National Research Foundation of Korea's Excellent New Researcher Project, the R&D Special Zone Regional Innovation Mega Project, and the Gwangju Institute of Science and Technology GIST-MIT AI International Cooperation Project. The results of the research were published online in the international academic journal 《Nature Communications》 on July 8, 2025.

GIST
Since 1993