SPHINCS+ 數位簽章演算法成為後量子密碼學標準，NIST 公佈 FIPS 205 以應對量子時代安全挑戰

2024 年 8 月 13 日，美國國家標準與技術研究院（NIST）正式公布了《無狀態雜湊數位簽章標準》也即美國聯邦資訊處理標準 (FIPS) 發行集 205。這標誌著後量子時代密碼技術的一個重要里程碑。這一標準的制定，是基於全球研究人員對抗量子電腦威脅的多年努力，特別是基於 SPHINCS+演算法的成果，該演算法是由一國際團隊開發並於 2022 年 7 月被選為後量子密碼學標準之一。該團隊包含本院資訊所副研究員倪儒本 (Dr. Ruben Niederhagen) 和他的指導老師郎丹雅 (Dr. Tanja Lange) 和狄傑比 (Dr. Daniel J. Bernstein), 這兩位是正在本院長期訪問的國際級大師。 這是繼去年 4 月 Ed25519 數位簽章系統納入 FIPS 186 後又再次有本院的密碼學研究群參與設計的密碼系統被選為美國國家標準，即事實上的國際標準。

量子電腦的潛在威脅與密碼技術的挑戰

量子電腦是具有廣闊的應用前景的未來科技，但它同時也對當前的網路安全構成了嚴峻挑戰。傳統的密碼元件，特別是基於公鑰密碼學的系統，隨著量子電腦的發展將變得脆弱。這些系統廣泛應用於互聯網上的協議如 HTTPS、數位基礎建設如自然人憑證等、和任何數位簽章被應用到的場域，一旦被破解，將帶來無法估量的資安風險。

量子電腦的崛起主要威脅到目前依賴大整數分解和離散對數問題的密碼系統，這些問題在現今的電腦上難以解決，但在量子電腦上變得容易。因此，研發能夠抵抗量子電腦攻擊的新型密碼元件成為了全球資安研究的重中之重。

NIST 的後量子密碼學競賽

為了應對這一挑戰，NIST 於 2016 年啟動了一項公開的後量子密碼學標準制定過程，邀請全球頂尖的密碼學專家提出解決方案。經過三輪嚴格的評估，NIST 選定了四個演算法來標準化，其中之一便是 SPHINCS+。

SPHINCS+及其在後量子密碼學中的角色

SPHINCS+演算法是基於雜湊函數的一種數位簽章技術，它不依賴傳統的基於大整數分解或離散對數問題的簽章演算法。取而代之的是，SPHINCS+利用雜湊函數的抗碰撞性和不可逆性來保證數位簽章的安全性。SPHINCS+的入選，不僅是對其技術卓越性的肯定，也是對其長期安全性的信任。在許多應用中，安全性是首要考慮因素，而 SPHINCS+正是為了滿足這一需求而設計的。

SPHINCS+的設計理念是提供一種能夠抵禦未來量子電腦攻擊的長期安全解決方案。它和其他基於雜湊函數的數位簽章技術不同，採用無狀態設計，這意味著每次簽名操作不需要之前的簽名狀態，而避免了潛在的安全風險。這一特性使得 SPHINCS+在需要高安全性和高可靠性的應用中具有顯著的優勢。

根據 NIST 公佈的 FIPS 205 標準，SPHINCS+被重命名為“無狀態基於雜湊數位簽章演算法”（Stateless Hash-Based Digital Signature Algorithm，SLH-DSA）。這一標準的公佈進一步確認了 SPHINCS+在後量子密碼學中的重要性並保證它會廣為採用。

FIPS 205 的公佈與意義

NIST 正式公布的 FIPS 205 詳細規範了無狀態基於雜湊函數的數位簽章演算法的技術細節。它的公布標誌著 SPHINCS+的正式標準化，這也意味著美國政府在面對量子電腦威脅時，已經擁有了一種廣受信任、安全可靠的數位簽章技術。

FIPS 205 不僅適用於所有美國聯邦部門和機構，還對私營和商業組織開放，允許他們在保護敏感資訊時採用這一標準。這一標準的推行，將有效提高數據的完整性和來源認證能力，並在電子郵件、電子資金轉帳、電子數據交換、軟體分發等領域發揮重要作用。

根據 FIPS 205 的規定，數位簽章演算法應用於需要數據完整性保證和數據來源認證的場合，並應防止私鑰洩露，確保簽章的安全性。NIST 強調，雖然 FIPS 205 規範了數位簽章的安全要求，但仍需由各機構自行確保其整體系統的安全性。

其他的國家和制定標準的組織很有可能採用 NIST 選定的標準, 故此 SPHINCS+ 有可能在不久的將來成為廣為採用的國際標準。

未來的發展方向

隨著 FIPS 205 的正式公佈，各行業應該開始著手將現有的前量子系統升級到後量子系統，以確保在量子電腦出現後依然能夠保護敏感資訊。專家多數認為現有系統與後量子系統應該並行運行，以確保達到最強的安全性。

總結來看，FIPS 205 的公布不僅是後量子密碼學領域的大事，也是全球網路安全領域的重要進展。隨著量子計算技術的不斷發展，後量子密碼學將成為保護我們數位資訊生活安全的基礎。隨著量子電腦技術的進步，未來的幾年中我們會看到更多基於這些標準的新技術和應用進一步提升全球的網路安全防護能力。

SPHINCS+ Digital Signature Algorithm Becomes Post-Quantum Cryptography Standard, NIST Releases FIPS 205 to Address Quantum-Era Security Challenges

On August 13, 2024, the National Institute of Standards and Technology (NIST) officially released the "Stateless Hash-Based Digital Signature Standard," also known as Federal Information Processing Standards (FIPS) Publication 205. This marks a significant milestone in post-quantum cryptography. The creation of this standard is the result of years of global efforts to combat the threats posed by quantum computers, particularly based on the SPHINCS+ algorithm, which was developed by an international team and selected as one of the post-quantum cryptography standards in July 2022. The team includes Dr. Ruben Niederhagen, an Associate Research Fellow at the Institute of Information Science, plus Dr. Tanja Lange and Dr. Daniel J. Bernstein, both of whom are international experts visiting the institute long-term. This is the second time a cryptographic system designed with the involvement of the institute's cryptography research group has been selected as a U.S. national standard, following the inclusion of the Ed25519 digital signature system in FIPS 186 in April last year, effectively making it an international standard.

The Potential Threat of Quantum Computers and the Challenges for Cryptography

Quantum computers are an upcoming future technology with vast potential applications, but they also pose severe challenges to current network security. Traditional cryptographic components, especially public-key cryptosystems, will become vulnerable as quantum computers develop. These systems are widely used in internet protocols like HTTPS, public digital infrastructure such as the Digital Citizen Certificate, and anywhere that digital signatures are used. Once compromised, the security risks are immeasurable.

The rise of quantum computers mainly threatens cryptosystems that rely on problems like large integer factorization and discrete logarithms, which are difficult to solve on today's computers but become easy with quantum computers. Therefore, developing new cryptographic components that can withstand quantum computer attacks has become a top priority for global cybersecurity research.

NIST's Post-Quantum Cryptography Competition

To address this challenge, NIST launched an open post-quantum cryptography standardization process in 2016, inviting top cryptography experts worldwide to propose solutions. After three rounds of rigorous evaluation, NIST selected four algorithms to standardize, one of which is SPHINCS+.

SPHINCS+ and Its Role in Post-Quantum Cryptography

The SPHINCS+ algorithm is a hash-based digital signature technique that does not rely on large integer factorization or discrete logarithm problems (like traditional signature algorithms). Instead, SPHINCS+ uses security properties of hash functions to ensure the security of digital signatures. The selection of SPHINCS+ not only affirms its technical excellence but also shows the trust in its long-term security. In many applications, security is the primary concern, and SPHINCS+ is designed to meet this need.

SPHINCS+ is designed to provide a long-term secure solution that can resist future quantum computer attacks. Unlike other hash-based digital signature techniques like the Internet Engineering Task Force (IETF) standards XMSS and LMS, it employs a stateless design, meaning that each signing operation does not require the previous signing state, thereby avoiding potential security risks. This feature gives SPHINCS+ a significant advantage in applications requiring high security and reliability.

According to the FIPS 205 standard published by NIST, SPHINCS+ has been renamed the "Stateless Hash-Based Digital Signature Algorithm" (SLH-DSA). The publication of this standard further confirms the importance of SPHINCS+ in post-quantum cryptography and ensures its widespread adoption.

The Release and Significance of FIPS 205

The official release of FIPS 205 by NIST details the technical specifics of the stateless hash-based digital signature algorithm. Its release marks the formal standardization of SPHINCS+, which means that the U.S. government now has a widely trusted and secure digital signature technology to face the threats of quantum computers.

FIPS 205 applies not only to all U.S. federal departments and agencies but is also open to private and commercial organizations, allowing them to adopt this standard to protect sensitive information. The implementation of this standard will effectively enhance data integrity and source authentication capabilities, playing a crucial role in areas such as email, electronic funds transfer, electronic data interchange, and software distribution.

According to FIPS 205, digital signature algorithms should be applied in scenarios requiring data integrity assurance and data source authentication, and should prevent private key leakage to ensure the security of signatures. NIST emphasizes

that while FIPS 205 specifies the security requirements for digital signatures, it is still up to individual organizations to ensure the overall security of their systems.

It is widely expected that the NIST standards will be considered for adoption by other national and international standardization agencies as well and that hence SPHINCS+ is likely to also become a standard in other countries and for a wide range of digital solutions.

Future Development Directions

With the official release of FIPS 205, industries should begin to upgrade existing pre-quantum systems to post-quantum systems to ensure the protection of sensitive information after the advent of quantum computers. Most experts believe that existing systems and post-quantum systems should operate in parallel to achieve the highest level of security.

In summary, the release of FIPS 205 is not only a significant event in the field of post-quantum cryptography but also a major advancement in global cybersecurity. As quantum computing technology continues to develop, post-quantum cryptography will become the foundation for securing our digital information lives. In upcoming years, we will see more new technologies and applications based on these standards further enhancing global cybersecurity.

SPHINCS$^+$ Team

- Jean-Philippe Aumasson
- Daniel J. Bernstein, University of Illinois at Chicago (US) and Ruhr University Bochum (DE) and Academia Sinica (TW)
- Ward Beullens, IBM Research Europe - Zurich (CH)
- Christoph Dobraunig, Graz University of Technology (AT)
- Maria Eichlseder, Graz University of Technology (AT)
- Scott Fluhrer
- Stefan-Lukas Gazdag, genua GmbH
- Andreas Hülsing, Eindhoven University of Technology (NL) & SandboxAQ (US)
- Panos Kampanakis, AWS
- Stefan Kölbl, Google (CH)
- Mikhail Kudinov, Eindhoven University of Technology (NL)
- Tanja Lange, Eindhoven University of Technology (NL) and Academia Sinica (TW)
- Martin M. Lauridsen
- Florian Mendel, Infineon Technologies (DE)
- Ruben Niederhagen, Academia Sinica (TW) & University of Southern Denmark (DK)
- Christian Rechberger, Graz University of Technology (AT)
- Joost Rijneveld, Radboud University (NL)
- Peter Schwabe, MPI-SP & Radboud University (NL)
- Bas Westerbaan, Cloudflare