OMEGA KRYPTO©

Stance on Information Privacy

IMMUNIZE YOUR SENSITIVE DATA©

Table of Contents

Omega Krypto's Stance on Information Privacy

Omega Krypto vehemently opposes any misuse, wrongdoing, or criminal exploitation of private information, regardless of whether it emanates from an individual, an organization, or a government entity.

The Universal Declaration of Human Rights, proclaimed by the United Nations General Assembly in Paris on 10 December 1948 (General Assembly resolution 217 A), clearly states in its article 12: "***No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.***"

In today's globally interconnected digital landscape, safeguarding information privacy has become an ever-evolving challenge. The emergence of quantum computing, with its potential to unravel existing encryption methods, coupled with the alarming surge in ransomware attacks worldwide, poses a pervasive threat. Without proactive measures to fortify the defense of our privacy, especially in the digital realm, we risk losing not only our sensitive data but also jeopardizing our freedom and, in extreme cases, our very lives.

Committed to the principle, Omega Krypto advocates for the rigorous enforcement of information privacy protection, pioneering innovative cryptography techniques and tools designed to shield the digital privacy of everyone.

NIST's Cryptography Standardization

The Advanced Encryption Standard (AES), introduced by the National Institute of Standards and Technology (NIST) in 1997, emerged as a widely adopted encryption algorithm aimed at supplanting the antiquated Data Encryption Standard (DES). AES operates on a symmetric-key encryption approach, utilizing the same key for both encryption and decryption.

Over recent years, NIST has issued multiple calls for new cryptographic approaches, with two of the most significant being:

- In 2016 a call for Post Quantum Cryptography proposals (cryptographic solutions that may resist the attack of a quantum computer), based on the risk quantum computers pose to current encryption techniques. NIST announced the first four Quantum-Resistant Cryptographic Algorithm winners back in 2022, yet have failed to define a standardized solution:, "Four additional algorithms are under consideration for inclusion in the standard, and NIST plans to announce the finalists from that round at a future date. NIST is announcing its choices in two stages because of the need for a robust variety of defense tools."

- In 2018 a call for Lightweight Cryptography, in order to be able to add cryptography on simple devices, where current encryption techniques cannot be implemented due to processing and memory constraints. The Ascon lightweight family of algorithms was selected, although they continue to advise organizations to wait until the final standard is published before using this suite of algorithms for secure communication and data storage.

The reality is that, as of now, there has been no implementation of a new encryption methodology due to a dual challenge: the absence of standardization, as indicated on NIST's website, which notes, "NIST plans to announce the finalists at a future date," and the deficiency in legislative frameworks for consumer protection.

Omega Krypto and NIST

Omega Krypto has received multiple invitations to collaborate and engage in the latest standardization calls initiated by NIST. However, the set rules of engagement established by NIST present a significant impediment, rendering participation unfeasible for a private entity like Omega Krypto.

The underlying challenge lies in finding common ground between the interests of the Government and the Private sector, serving as the central point of contention that has impeded the progress toward establishing new standardization standards. Case in point, the Apple–FBI encryption dispute (see below) a decade ago, as well as Snowdon's NSA activity revelations serve as a prologue of what to expect going forward.

From the standpoint of Omega Krypto, the following observations encapsulate its perspective:

a) **Royalty Free**: In section 2.D, NIST clearly states that "*NIST has observed that royalty-free availability of cryptosystems and implementations has facilitated adoption of cryptographic standards in the past. For that reason, NIST believes it is critical that this process leads to cryptographic standards that can be freely implemented in security technologies and products. As part of its evaluation of a PQC cryptosystem for standardization, NIST will consider assurances made in the statements by the submitter(s) and any patent owner(s), with a strong preference for submissions as to which there are commitments to license, without compensation, under reasonable terms and conditions that are demonstrably free of unfair discrimination*".

   Omega Krypto has devoted significant time, pooled extensive knowledge, harnessed creative insights, applied specialized expertise, invested substantial effort, and dedicated financial resources to innovate a groundbreaking encryption technique. As any company would do, Omega Krypto has safeguarded its intellectual property by obtaining patents in Europe, Asia and the US, and will not forgo expected financial gains of this development for the benefit of NIST standardization.

The absence of an opportunity to secure a financial return on this investment is viewed as inequitable, and contributes to the entity's decision to refrain from submitting its encryption for consideration in NIST's call.

b) **Government Modifications**: The "Statements" that must be signed by each submitter and patent owner includes the following paragraph: "*I also acknowledge and agree that the U.S. Government may, during the public review and the evaluation process, and, if my submitted cryptosystem is selected for standardization, during the lifetime of the standard, modify my submitted cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability)*".

Omega Krypto is clearly reluctant to grant any entity, including the U.S. Government, unrestricted authority to modify the specifications of its cryptosystem. While acknowledging a possible scenario where modifications might be considered acceptable—specifically, to address a newly identified vulnerability with explicit approval—the current paragraph fails to convey this nuance effectively. It clarifies that the mentioned example of safeguarding against vulnerabilities is not a restrictive condition, as the entity explicitly grants authorization for other modifications to be executed without its knowledge.

Having engineered a novel encryption technique with the versatility to serve as a foundation for diverse algorithms, each boasting equal security capable of withstanding attacks, including those from the most formidable quantum computers and their future replacements, the entity is unwavering in its commitment to maintaining the inherent security of its creation. A firm stand is taken against any measures that may compromise this integrity, such as the inclusion of backdoors facilitating unauthorized access to encrypted information.

The company's unwavering commitment to the absence of an opportunity to secure a financial return, and the principle of safeguarding the unyielding security of its cryptographic system, led to the firm decision to refrain from submitting its encryption for consideration to NIST.

Apple – FBI Encryption Dispute

The Apple–FBI encryption dispute revolves around the question of whether U.S. courts can compel manufacturers, specifically Apple in this particular case, to assist in unlocking encrypted data on iPhones for law enforcement purposes. The controversy gained prominence in 2015 and 2016 when Apple faced multiple court orders, issued under the All Writs Act of 1789, to help unlock iPhones related to criminal investigations.

The most notable case involved an iPhone 5C used by one of the perpetrators of the 2015 San Bernardino terrorist attack. The FBI sought Apple's assistance in creating new software to bypass the device's security features. Apple refused, citing concerns about customer data security and the potential precedent for undermining the security of its products. A legal battle ensued, but before a

court hearing, the government claimed to have found a third party capable of unlocking the iPhone, leading to the withdrawal of the request.

The dispute raised broader issues regarding privacy, national security, and the balance between them. Apple argued that being compelled to create new software amounted to compelled speech and violated the First Amendment. The government contended that the All Writs Act empowered courts to demand technical assistance, drawing parallels to a 1977 case involving a phone company providing access to phone records.

In the end, the FBI withdrew its request after claiming to have successfully unlocked the iPhone with the help of a third party. The third party was later reported to be Azimuth Security, an Australian company, according to sources cited by The Washington Post in April 2021. The case brought attention to the ongoing debate over the use of strong encryption and the balance between privacy rights and law enforcement needs.

Support for Apple in the encryption dispute was widespread:

Tech Coalition: The Reform Government Surveillance coalition, including major tech firms like Google, Microsoft, Facebook, Twitter, and others, opposed the court order.

Amicus Curiae Briefs: Many technology companies, such as Amazon, Box, Cisco, Dropbox, Google, Microsoft, and others, filed amicus curiae briefs supporting Apple. Organizations like the ACLU, Electronic Frontier Foundation, Access Now, and the Center for Democracy and Technology also backed Apple.

International Support: The United Nations High Commissioner for Human Rights warned the FBI of potential damaging implications on human rights. General Michael Hayden, former NSA and CIA director, supported Apple, emphasizing the importance of cybersecurity.

Summary & Conclusion

Privacy is a fundamental human right recognized in the UN Declaration of Human Rights, the International Covenant on Civil and Political Rights and in many other international and regional treaties. Safeguarding digital assets is also imperative for the survival of any business, and a cybersecurity strategy devoid of Cyber-Privacy is inherently inadequate.

As a vanguard in cryptography technology, and with an unwavering commitment to privacy, Omega Krypto adamantly opposes any measures that could jeopardize this integrity. This includes staunch resistance to the incorporation of backdoors for government access or intrusion — an action contrary to our core principles. In this stance, Omega Krypto finds itself aligned with major tech firms such as Google, Microsoft, Facebook, and others who share our values in safeguarding user privacy.

Omega Krypto has developed a cutting-edge Post Quantum Encryption (PQE) technique that is ready to go to market, and has secured patents in pivotal regions such as the United States (Patent US 10,873,448), United Kingdom and mainland European Union, spanning over 20 member countries (Patent EU 3382929), India (Patent IN 467,334) and Uruguay (Patent UY 36412).