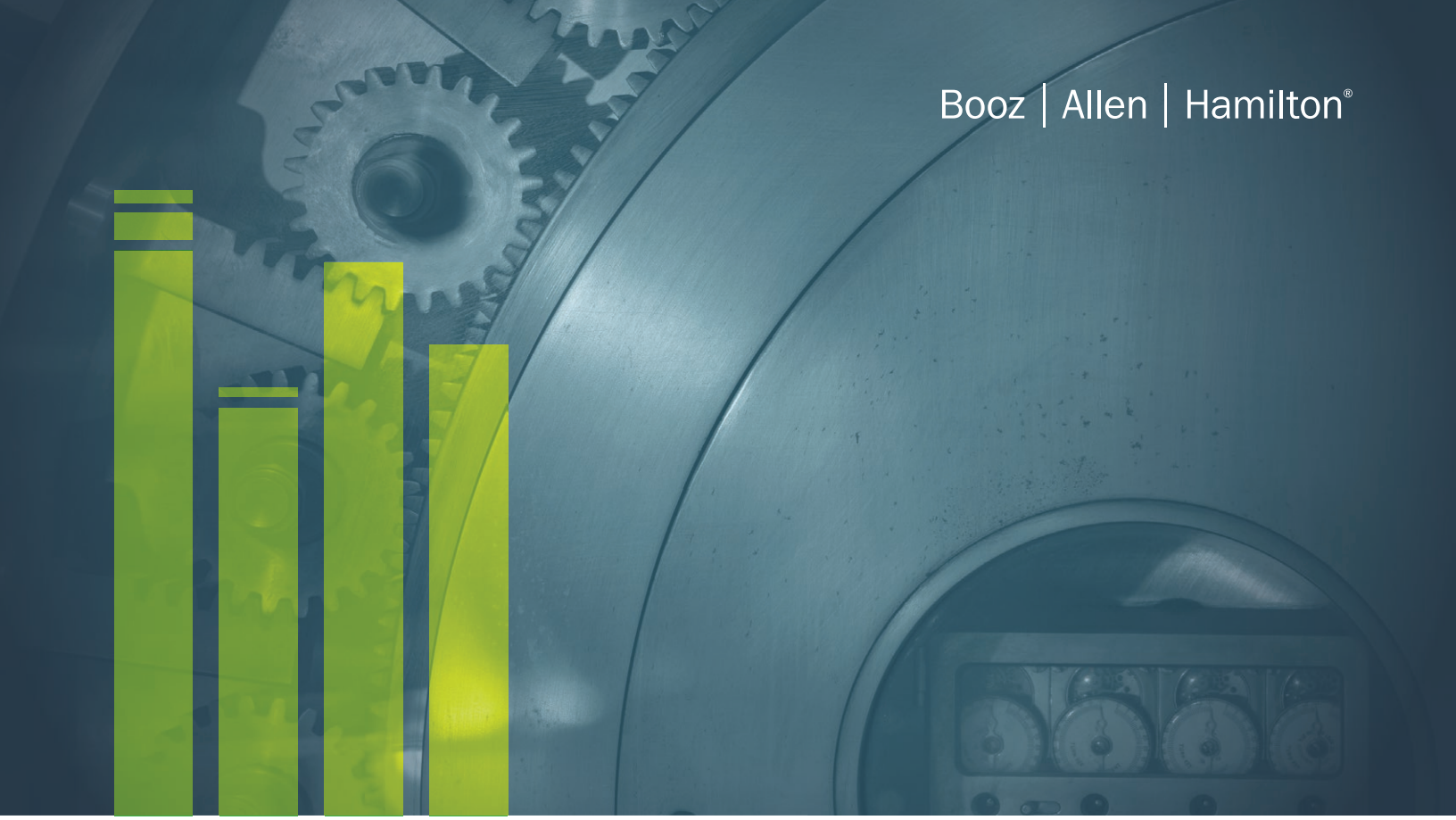
Booz | Allen | Hamilton®

2021 TECHNOLOGY SPOTLIGHT

THE FUTURE OF ENCRYPTION

CONSULTING | ANALYTICS | DIGITAL SOLUTIONS | ENGINEERING | CYBER



As the amount of data being generated and transmitted grows exponentially, the government will need more advanced encryption technology to reliably secure information and protect against insider and adversarial threats.

With significant growth in government usage of cloud, 5G, the Internet of Things (IoT), and other next-generation technologies, federal leaders are responsible for securing increasingly larger and more complicated digital systems, including the data that is collected, stored, transmitted, and processed within and between those systems. This expansion intensifies the need for advanced encryption software as part of enterprise cybersecurity efforts. Though some might argue it lacks the novelty or shine of other emerging technologies, progress in encryption technology will be central to the government's ability to successfully manage the confidentiality, integrity, and availability of data.

WHAT IS THE FUTURE OF ENCRYPTION?

Encryption is defined as the process of encoding information by converting information into ciphertext. Modern encryption has evolved from its 20th Century origins in intelligence and military operations to today's broader focus on keeping data safe across devices and networks. Broadly speaking, encryption at an enterprise level may consist of a large set of related areas—*including messaging security, data loss prevention, multifactor authentication, database security, network encryption, database encryption, and endpoint security*. But across these areas, most modern encryption methods rely on "encryption keys" to prevent adversaries from subverting systems and using data maliciously.

Conceptually, the process of using keys for encryption is simple: To encrypt data, an encryption key uses an algorithm to translate (or "encode") readable data into unreadable data. To decrypt that unreadable data and make it readable once more, an individual or machine must use the corresponding decryption key.

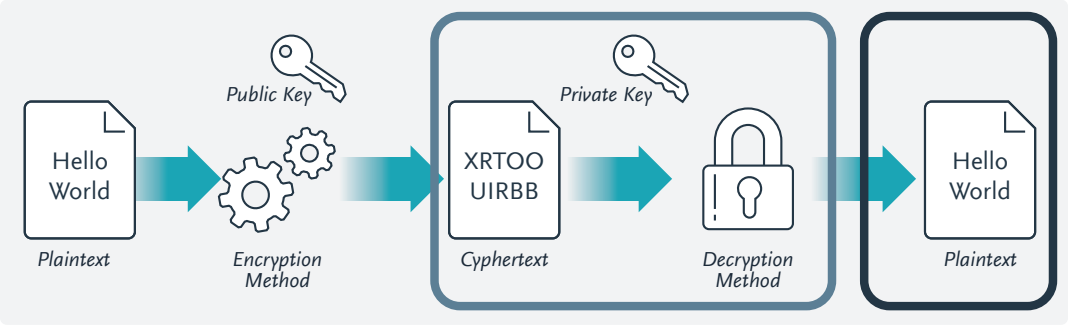


Figure 1: Graphical Representation of a Cryptosystem

In practice, the methods and types of encryption can be much more complicated. But regardless of complexity, there are significant challenges tied to the foundational structure of today's key-based encryption methods:

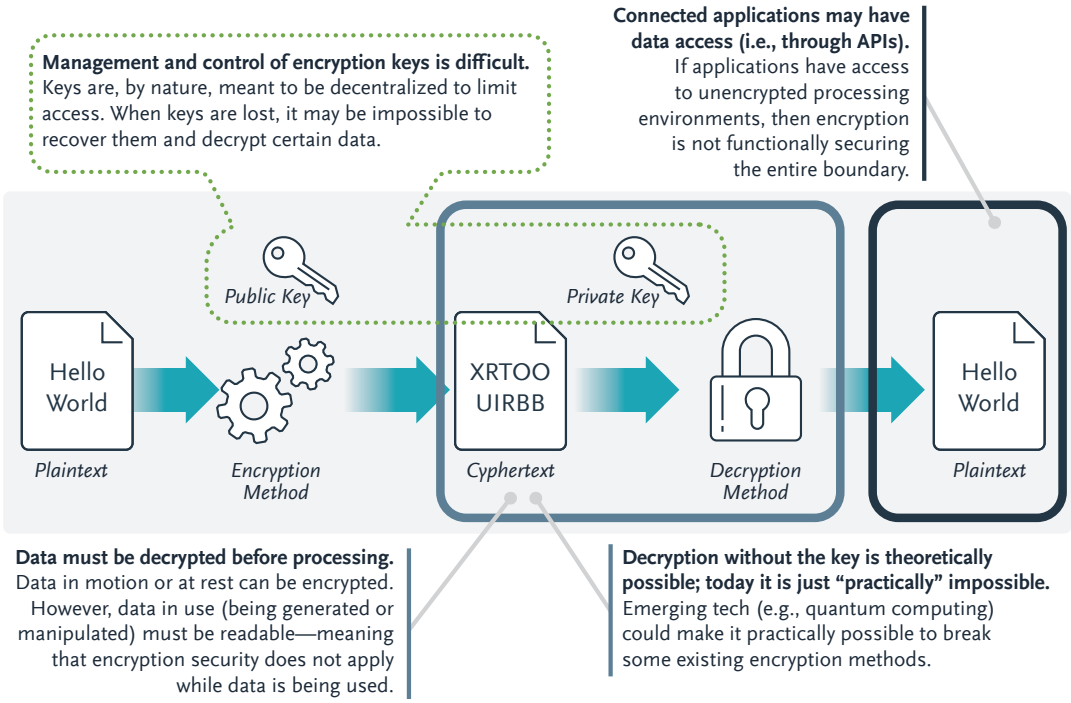


Figure 2: Challenges with Current Encryption Systems

Given that current encryption and authentication protocols have workarounds, and the cost of a fully secure method is high, advanced encryption methods currently under development are aimed at addressing the challenges illustrated above.

A CLOSER LOOK: PROMISING FUTURE ENCRYPTION METHODS

Any technology ecosystem consists of, or can be broken down into, a set of core components. Over time, capabilities and offerings sprout up around these core components as they mature. To fully understand a technology, it is often easier to analyze the individual components. We identify the following four core components (i.e., most promising methods) for future encryption methods:

Future Encryption Methods	What It Is	Purpose
BEHAVIORAL BIOMETRICS	Biometrics encryption combines a user's biometric data with standard encryption methodology to create a more secure authentication process	Behavioral biometrics produces user profiles of behavior and then looks for deviations to those patterns to identify possible threats. Possible patterns for monitoring include typing patterns (speed of typing, length and pauses between strokes, degree of impact); navigation patterns (mouse movements and finger movements); and engagement patterns (usage frequency and timing of applications).
QUANTUM KEY DISTRIBUTION (QKD)	QKD is a secure method of communication using quantum mechanics	QKD, by virtue of being quantum, resists interception and retransmission by an eavesdropper attempting to tamper with this provably secure form of cryptography. This promising concept has long been demonstrated by researchers over the last decade. Quantum cryptography, however, requires near-perfect behavior of the quantum bits themselves, and though researchers are making significant advances to account for error rates, QKD is not yet known to work over long distances. It is unlikely the National Security Agency (NSA) will approve QKD given these limitations (see **guidance**). However, several proof-of-concept implementations have shown that there is strong evidence for surface-satellite QKD since most optical turbulence effects occur predominantly within the lowest 2km of the atmosphere, and thus QKD for low earth orbit (LEO) and geostationary satellites could very well be possible.
HOMOMORPHIC ENCRYPTION	Homomorphic encryption is a form of encryption that protects data while it is in use—the "holy grail" of encryption	Homomorphic encryption is a highly disruptive technology that could solve the longstanding problem of compromised data security by allowing the user access to data without having to decrypt. It may be the answer for organizations looking for more access to quality data to run artificial intelligence/machine learning analyses; however, adoption is slow as the technology is still in development and there is a large computational overhead.
POST QUANTUM CRYPTOGRAPHY (PQC)	Encryption methods that will not be breakable using quantum computers	These encryption methods will be standardized by the National Institute of Standards and Technology (NIST) and will be used throughout the commercial sector for network security, database security, and more. Today's public-key algorithms such as RSA and the Elliptic Curve Digital Signature Algorithm (ECDSA) will eventually be replaced by PQC.

DEEP DIVE: HOMOMORPHIC ENCRYPTION

There are three types of homomorphic encryption: partially, somewhat, and fully homomorphic. **Partially homomorphic encryption** secures data but limits the computations that can be executed on the data such as addition or multiplication. **Somewhat homomorphic encryption** supports limited operations that can be performed only a set number of times. **Fully homomorphic encryption** (FHE) allows computation or analysis of data while it is encrypted, meaning it guarantees data privacy even during analysis. Experts also postulate that FHE may be well-equipped to protect against quantum codebreaking. To achieve this degree of security, however, FHE requires enormous computing power for analysis. Additionally, FHE has other current limitations: It is impractical for traditional hardware, there is currently no FHE solution at a Technology Readiness Level (TRL) 6 and higher, and most FHE schemes do not support multiple users working on a single data set.

Nevertheless, research and development to scale FHE is highly active, and enterprise-scale applications for homomorphic encryption are just starting to arrive. With $100M+ annual global investment and key players such as Microsoft and IBM advancing open source solutions, FHE is an emerging technology for which to keep an eye out.

IMPACT HIGHLIGHTS

Today's encryption market encompasses a wide array of technologies to address various levels of encryption including disk, file/folder, database, communication, and cloud.

Of these levels, cloud encryption is the most relevant area for most U.S. government agencies to address given requirements around data access. Organizations can expect more robust cloud encryption solutions in coming years given the significant growth in the cloud encryption software market. Keep in mind that differences between the three main cloud platform models—Platform as a Service (PaaS), Infrastructure as a Service (IaaS), and Software as a Service (SaaS)—may pose complications in the compatibility or availability of emerging encryption solutions. Organizations must understand the impact that various encryption processes will have on their cloud environments and establish expectations for the cloud service provider's ability to maintain services.

The most significant challenge with encryption technology today is the management of the encryption keys.

Today, most encryption uses asymmetric-key algorithms where the keys used for the encryption and decryption are different. This means that they require both a public key and a private key to access the data. As a result, the loss of keys often results in the loss of data.

This major challenge of losing keys sheds light on the human error element of encryption. Employee mistakes continue to be the threat most significant to data security breaches. The complexity of encryption technology implementation can cause confusion for users. This is why it is imperative that employees understand the steps to take to avoid accidentally disabling encryption or sharing decrypt keys to unauthorized persons. With encryption, the basis of the mathematical operations remains the same, yet adding people into the equation presents a new variable with its own layer of challenges.

Advanced encryption software and more stringent cybersecurity solutions will allow the government to better address security concerns with adoption of enterprise mobility and IoT.

The increase in remote work brought on by the COVID-19 pandemic and the exponential rise in digital transactions have dramatically increased the size of the cyber attack surface. In this environment, IT security personnel continue to remain at a disadvantage: as they try to stop cyber attacks to protect businesses and government, they must work to balance security needs with feasibility concerns in the context of day-to-day organizational activity and distributed operations. This balance is difficult to achieve in dynamic, digitally connected spaces,
but future encryption solutions will help IT personnel mitigate security risks that may arise. Whether in the near term (e.g., with Behavioral Biometrics) or medium term (e.g., with Quantum Key Distribution and Homomorphic Encryption), advanced encryption software can help government agencies better address nefarious activity.

THE FUTURE OF ENCRYPTION IN SUPPLY CHAIN ATTACKS

TAKEAWAYS FOR YOUR ORGANIZATION

Because encryption methods serve as enabling technologies for any enterprise cybersecurity ecosystem, there is universal need for organizations to utilize emerging encryption solutions to monitor and protect their systems from both insider threats and outside adversarial attacks on firmware, hardware, and supply chains.

Today, supply chain attacks through cloud-hosted environments are becoming increasingly common. These attacks are often more dangerous than traditional phishing campaigns or downloaded viruses because corruption can take place via trusted pieces of software packaged with malware inside of them. Simply put, hackers let companies and government agencies do the challenging work themselves by installing faulty updates at the company or agency's cue. These vulnerabilities—evidenced by recent and highly visible targeted, manually executed attacks—put into question whether today's current encryption methods will be able to stand up to future potential attack postures for cyber penetration, particularly with increased reliance on automation.

Looking toward the future, it will be crucial for organizations to understand and evaluate the vulnerabilities of existing cyber approaches against these developing attack postures. While needs will vary by organization, advanced encryption will be central to any modernized digital infrastructure.

FOR MORE INFORMATION:

The content in this 2021 Technology Spotlight Series originates from Booz Allen's emerging technologies capabilities as part of our innovation agenda, and this spotlight on the *Future of Encryption* was developed by Booz Allen's Technology Scouting team. For more in-depth security guidance, please visit **BoozAllen.com/cyber**.

About Emerging Technologies at Booz Allen

For over a century, Booz Allen has been at the forefront of technology and strategy. We provide strategic advisory services, design, build, and deploy solutions across sectors to a wide range of federal government organizations. We are the only management and technology consulting firm that has invested to establish an innovation network exclusively focused on scouting dual-use technologies for federal government missions. As a result, we successfully partner with the tech community to showcase a wide range of capabilities and deliver innovative solutions to our clients.

Our deep pool of technical talent, access to critical networks in innovation hubs, and experience performing tech scouting across technologies and sectors uniquely position Booz Allen to serve clients who seek to be at the cutting edge.

To learn more, visit BoozAllen.com (NYSE: BAH)