SAND2019-1878C

Cryptography Considerations for Distributed Energy Resource Systems

Christine Lai*, Patricia Cordeiro*, Adarsh Hasandka†, Nicholas Jacobs*, Shamina Hossain-McKenzie*, Deepu Jose*, Danish Saleem†, Maurice Martin†

*Sandia National Laboratories
Albuquerque, NM, USA
{cflai,pgcorde,njacobs,shossai,djose}@sandia.gov

†National Renewable Energy Laboratory
Golden, CO, USA
{Danish.Saleem,Adarsh.Hasandka,Maurice.Martin}@nrel.gov

***Abstract*—Distributed energy resource (DER) systems are rapidly being adopted and integrated within the electric power grid. Developments in smart grid devices and communication protocols are advancing the power system domain but are also introducing new cyber attack vectors. In particular, the ability to maintain the confidentiality, integrity, and availability of data is of increasing concern. Cryptography is a powerful tool that can be leveraged to protect DER systems and their critical information. This paper discusses prominent methods of cryptographic authentication and encryption that can be used to secure DER communications. Specific considerations and recommendations for applying cryptography to DER systems are provided, including system design constraints and system impact. These will be demonstrated with two case studies that assess cryptography hardware requirements and communications latency in DERs.**

***Keywords*–cryptography, encryption, distributed energy resources, cybersecurity, cyber attacks, hardware design, latency**

I. Introduction

Penetration of distributed energy resources (DERs) is rapidly increasing in the bulk power system (BPS); they are growing to be a significant portion of generation. As such, grid-support capabilities are being developed and implemented in DER devices and networks [1]. With the growing presence of DERs in the grid, their impact on the BPS increases, as does the potential for a disturbance originating in a DER system to cause effects that propagate throughout the BPS. These disturbances include a variety of events that range from natural equipment malfunctions and resource variability to malicious cyber attacks. In addition to representing an attack surface for the grid, rising concerns for DERs include the lack of built-in defenses, poorly secured communications, and the emergence of advanced persistent threats that exploit industrial control system (ICS) protocols [2]. BlackEnergy, originally developed as a botnet generation tool for distributed denial of service (DDoS) attacks, has been leveraged to gain access to ICS networks [3]. The malware framework commonly called Industroyer or CrashOverride contains modules that specifically target ICS protocols and has been implicated in attacks on systems operating on IEC 61850 [4].

Thus, addressing cybersecurity risks is of increasing importance in DER systems. As with information-based systems, cyber-physical systems security may be viewed through considerations of confidentiality, integrity, and availability (the CIA triad) [5]. The primary concern in the grid has traditionally been availability, or the ability to "keep the lights on." However, with the increasing threat of cyber attacks that aim to manipulate and intercept data and control signals, integrity and confidentiality are increasingly important factors in maintaining availability [6], [7]. Remote access and automated functions render DER devices vulnerable to attacks on integrity (e.g. harmful data injection and control input spoofing) that can disrupt power system operation. Breaches in confidentiality could allow an adversary to exploit operator controls and successfully evade fault detection mechanisms (e.g. report normal status during an attack); furthermore, personally identifiable information (PII) data is at risk due to the deployment of devices on private networks (e.g., customer-owned DERs), and power usage patterns that may indicate whether a building is occupied or not.

In contemporary devices and networks, data confidentiality and integrity are protected through cryptographic means. This paper discusses prominent methods of cryptographic authentication and encryption, addresses considerations for their application to DER systems, and presents two demonstrative case studies for DER encryption.

II. Review of Cryptography

As the level of active communications within DER networks increases, new opportunities arise for cyber threat actors seeking to misuse the system. Cryptography presents a solution to these issues by enabling two parties, often referred to as Alice and Bob, to communicate without allowing an outsider, Eve, to eavesdrop on transmitted data. Typically, the information

This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government. Sandia National Laboratories is a multi-mission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. This work is supported by the U.S. Department of Energy Cybersecurity for Energy Delivery Systems program. SAND2019-XXXXX

(plaintext) is encrypted using a secret key, translated into ciphertext, and decrypted once it reaches its intended reader. In addition to cipher algorithms, common components of cryptographic schemes include digital signatures, key management, and authentication protocols [5]. It is important to note that cryptography is by no means a panacea for all security needs, but it is a powerful tool for ensuring the safety of one's data assets.

Confidentiality is typically maintained through encryption and decryption. If Alice and Bob both keep their keys secret, then Eve has no way of decrypting data that has been intercepted via eavesdropping. Moreover, Eve should not be able to intercept messages exchanged between Alice and Bob to deduce their keys or spoof their identities. Integrity, which encompasses the accuracy and consistency of data over its intended lifecycle, is heavily dependent on confidentiality, as Eve should not be able to alter intercepted data without being detected unless Alice or Bob's keys have been compromised.

A. Symmetric Encryption Algorithms

Symmetric ciphers are employed when both parties in a cryptographic exchange share the same key for encryption and decryption. These algorithms are often based on substitution and permutation functions, and can be categorized into stream and block ciphers. The former category encrypts data one bit at a time and is based on the one-time pad, a mathematically proven cipher; however, it is cumbersome in practice due to the requirement that the key must be at least as long as the data encrypted [8].

Among symmetric encryption techniques, the Advanced Encryption Standard (AES) is most widely used today. AES was codified in 2001 by the National Institute of Standards and Technology (NIST) to address vulnerabilities in a predecessor, the Data Encryption Standard (DES), and it is the only publicly known algorithm approved by the National Security Agency (NSA) for protecting classified information at a TOP SECRET level [9]. The Rijndael block cipher used in AES works by separating information into 128 bits (16 bytes). Data is encrypted with N rounds (10, 12, or 14) depending on key length (128, 192, pr 256, respectively). Each round consists of four layers: byte substitution, row shifting, column mixing, and key addition [10]. A simplified flow chart of this process is shown in Fig. 1. AES can be implemented with different modes of cipher block operation, which can have a significant impact on security and performance. Common cipher modes for AES include:

- *Electronic codebook (ECB)*, in which each block is encrypted separately. This mode is typically only used for demonstrative purposes, as patterns in data can still be gleaned from the ciphertext.
- *Cipher block chaining (CBC)*, in which XOR operations are performed between the current and preceding block to improve security and computational efficiency.
- *Counter mode (CTR)*, which employs a sequence counter to operate as a stream cipher, allowing blocks to be encrypted in parallel.
- *Counter with cipher block chaining message authentication code (CCM)*, which combines CBC with MAC authentication.
- *Galois/counter mode (GCM)*, which combines CTR with Galois field multiplication for authentication, improving performance over CCM on most hardware.

Stream ciphers, namely the Salsa and ChaCha family of algorithms, are currently used with Transport Layer Security (TLS) for securing public network traffic. The ChaCha20 algorithm [11] is often deployed alongside AES, as it uses add-rotate-XOR (ARX) instructions that perform faster on general purpose processors that do not contain specialized instructions for AES. Moreover, ChaCha20 is thought to be invulnerable to cache-timing attacks, as it is not implemented with a lookup table. However, as the body of published research for cryptanalysis of ChaCha20 is sparse in comparison to AES, it is possible that critical unknown vulnerabilities exist.

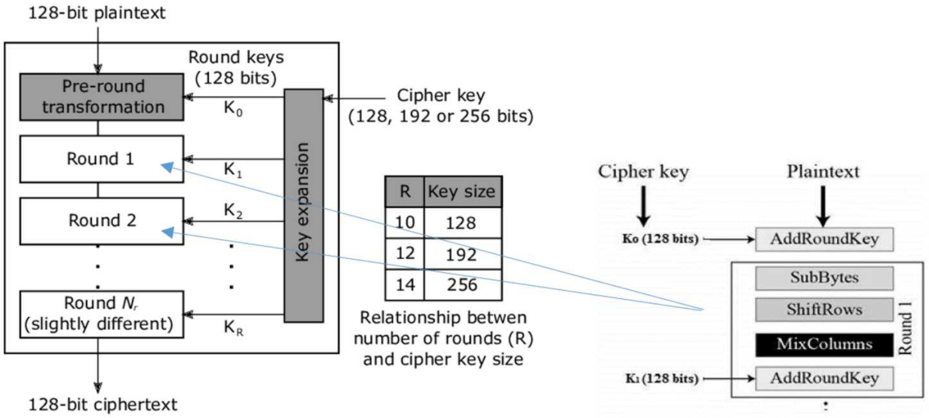
As processor efficiency and cryptanalysis techniques improve, ciphers often become easier to break, and algorithms must be updated to maintain an acceptable balance between security and performance. Less computationally intensive algorithms, such as the Blowfish block cipher and the streaming Rivest Cipher 4 (RC4), are sometimes used in resource limited environments where lower cryptographic security is accepted in exchange for operating with limited processing power, memory, or storage [12]. Although RC4 often appears in legacy systems, and previously experienced widespread usage in the now deprecated Wired Encryption Privacy (WEP) and Wireless Protected Access (WPA) protocols, it has since been prohibited from use with TLS due to the increasing efficacy of exploits [13].

B. Asymmetric Encryption Algorithms

Asymmetric ciphers use sets of corresponding private and public keys for encryption and decryption rather than a single shared key. Since public keys are often associated with identities, asymmetric key generation algorithms are also employed in conjunction with one-way hash algorithms to produce digital signatures. In most implementations, each user has a key pair consisting of a secret (private) key and a corresponding public key. Prominent asymmetric cryptosystems include Rivest-Shamir-Adleman (RSA), Elliptic Curve Cryptography (ECC), and Elliptic Curve Digital Signature Algorithm (ECDSA); more information can be found in [15].

C. Key Strength, Establishment, and Exchange

The current generation of symmetric ciphers employs key lengths that typically range from 128 to 256 bits; longer keys are required for asymmetric ciphers to achieve the same level of security. The key length is a relative indicator of the amount of work that is believed to be required to break an algorithm with respect to a known type of attack. Longer key lengths correspond to higher number of bit flips required to execute the attack, which in turn requires a minimum amount of physical energy consumption, known as the Landauer limit [16]. For example, the Landauer limit for a brute-force attack



R	Key size
10	128
12	192
14	256

Fig. 1. Simplified flow chart of AES, from [14].

on AES is approximately 2^{128} for AES-128 and 2^{256} for AES-256, with an attack on the latter requiring 2^{128} times the computational complexity. For further discussion on the bit strength of cryptographic algorithms, see NIST Special Publication 800-57 [17].

Although symmetric ciphers generally have the advantage of small key sizes and efficient computations when compared with asymmetric ciphers, successfully implementing symmetric encryption relies on a secure method for generating and sharing the secret keys. Therefore, asymmetric encryption is often employed to create a secure channel over which a shared symmetric key is established before proceeding with symmetric encryption. The Diffie-Hellman key exchange protocol, which is used in many cipher suites for symmetric key agreement, employs a series of one-way functions to prevent an eavesdropper from reconstructing the shared key [5]. Asymmetric ciphers require management of public and private keys, often through public key infrastructure (PKI), in which each public key is digitally signed into a certificate and registered with the identity of the corresponding entity, allowing for verification through a trusted third party [18].

III. Considerations for Cryptography in DER Systems

Best practices for implementing cryptography in DER systems can be treated as an extension of best practices for DER cybersecurity, or for ICS and IT networks in general. Risk analysis should be applied to understand the nature of threats to the system and the resources available to attackers to thwart security controls. As most DER systems do not have extremely high-cost, high-performance computing hardware, it is generally recommended that proven technologies such as Internet Protocol Security (IPSec) and TLS be applied to provide defense-in-depth on the system. Existing protocols used to communicate with DER devices, specifically Modbus and DNP3, do not support encryption and are typically operated within the Transmission Control Protocol and Internet Protocol (TCP/IP) to leverage TLS.

The X.509 certificate standard was first issued in 1988 and currently forms the basis for public key exchange over the Internet [19]. The IEEE 2030.5 Smart Energy Profile (SEP 2.0) specification has been incorporated into California Rule 21, which mandates the use of X.509 certificates for DER devices [20]. The adoption of certificate-based PKI poses numerous infrastructure and security challenges that must be addressed for successful implementation over a DER network. For one, PKI for computer networks currently relies on a large set of certificate authorities, which makes for ambiguity in certificate chains and slow validation for cross-signed certificates. Moreover, blacklisting of certificates only occurs when revocation lists are available, and there is no system for revocation of root certificates. Due to these complexities, implementations of PKI are often adjusted to exclude certain security features, including certification expiration, revocation checks, and naming constraints. While alternatives to PKI are numerous, and include a broad range of certificateless strategies (e.g. web of trust, whitelisting) and trustless protocols (e.g. blockchain), only X.509 certificates have been incorporated into DER standards for key management thus far.

IV. Impact of Cryptography on DER Systems

Cryptography in DER systems can be implemented via an embedded module within DER devices, or as a standalone module that serves as a bump-in-the-wire (BITW) or attachable solution. In this paper, we will focus on the elements of an encryption module that enable retrofitting of current DER systems. The basic functionality of such a module is to support encryption and decryption of data between two entities on a secure line (e.g. between a utility and a photovoltaic (PV) inverter) for the purpose of securing system control and health status messages. The solution should be flexible enough to be implemented broadly (e.g. via either software or hardware) and utilize a structured, efficient cipher suite that has minimal impact on normal DER system operations. SEP 2.0 specifies the use of *TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8*, which is tailored for efficient deployment on embedded devices, as it specifies the use of elliptic-curve cryptography over Galois fields, 128-bit AES over 192-bit or 256-bit AES, and a relatively short 8-byte hash.

A. Case Study 1: Hardware Constraints for Encryption in DER Systems

With the growth of distributed generation in DER systems, cost and power efficiency are increasingly crucial to the successful deployment of devices to residential and commercial sites, which generally are numerous but have less supporting infrastructure than the BPS. Network routers and PV inverters may vary among sites and may not be directly managed by utilities, requiring the devices to be highly configurable. Therefore, a cryptographic module should be designed with considerations made toward addressing these constraints.

In Fig. 2, an example hardware design is presented that leverages existing low-cost processing platforms to meet the needs of DER encryption. At the core of the module, a lightweight single board computer (e.g. a Raspberry Pi) provides general processing and handles the translation between the various internal software and hardware interfaces in the system, as well as the external interfaces that carry communications to and from the attached DER device. Due to space and power constraints, the Universal Serial Bus (USB) and Ethernet interface controllers share system resources, limiting simultaneous throughput on both interfaces. To minimize the burden on the processor, specialized adapters are employed to process TCP/IP communications through the USB port and serial communications through Inter-Integrated Circuit (I2C) pins. The TCP/IP interface provides support for DER devices connected over a local area network (LAN), while the serial interface provides support for DER controllers directly connected to the module.

Another key consideration for the hardware design is the ability to secure the module itself, as each interface and component on the module represents an addition to the attack surface of the DER system as a whole. As shown in Fig. 2, the various components in the module each encapsulate a separate function, allowing them each to be separately addressed. All internal and external traffic must pass through a firewall that resides on the single board computer. Any cryptographic processing is offloaded to the AT88CK590, which contains three application-specific integrated circuit (ASIC) chips (ATSHA204A, ATAES132A, and ATECC508A) for dedicated hardware acceleration of the respective hash function (Secure Hash Algorithm, or SHA), symmetric encryption cipher (AES), and key generation (ECC) operations within the module. This not only provides a layer of protection against eavesdropping attacks on partly encrypted intermediate data stored in memory, but also prevents the code governing the cryptographic functions from being modified or overwritten. The device stores cryptographic data such as certificates and private keys in a Trusted Platform Module (TPM) [21], which offers cost-effective tamper resistance.

The design illustrated here follows several security best practices that help to mitigate the likelihood or threat of a successful attack on the system. In accordance with the principle of least privilege, each component is given access to only the minimum amount of data required to perform its function. This segregation ensures that an attacker that has compromised one component of the system does not have full knowledge of the information passing through the entire system. Moreover, it allows for the use of low-cost open-source components that have been thoroughly validated for security risks and have well-documented vulnerabilities. Protections and resources are focused on the most critical elements of the system, with the use of TPMs and ASICs to protect the execution of cryptographic functions and store cryptographic data. However, while these design decisions protect confidentiality and integrity, the performance of the module must be evaluated to ensure that it can adequately support system availability. Testing the module in a DER environment would aid in quantifying the performance impact from the encryption module and evaluating the trade-offs between cost and performance that result from the modular component design.

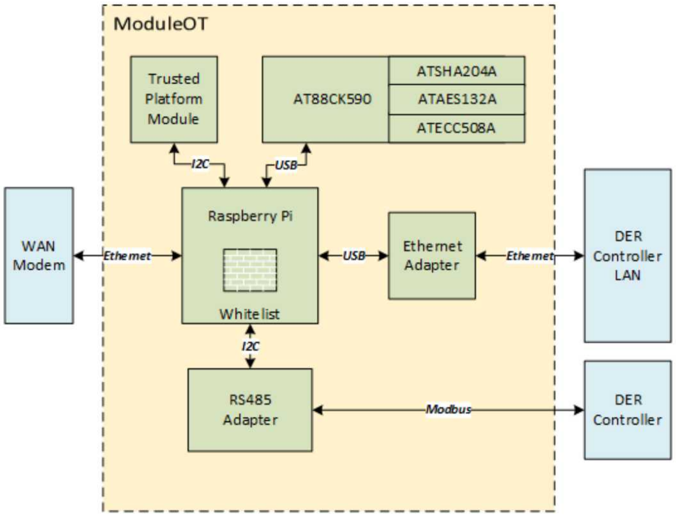


Fig. 2. Example cryptographic hardware design for DER encryption.

B. Case Study 2: Encryption Impact to Latency

With the growing impact of DER systems on the BPS and addition of grid support functions to DER devices, communications latency and jitter have become critical to evaluating the effects of encryption on DER performance. Here we focus on a comparison of various symmetric ciphers, as they are responsible for encrypting the bulk of data transmitted over the network. As illustrated in Fig. 1, encryption strength is partly dependent on key length, as larger key sizes increase the difficulty and number of rounds of computation. Therefore, it is important to assess the impact of key length on performance in addition to examining the differences between ciphers and modes.

In a study titled "Performance of State-of-the-Art Cryptography on ARM-based Microprocessors," [22] AES algorithms of different key lengths and modes of operation were tested in a controlled hardware environment using a lightweight NXP-LPCI768 microcontroller and ARM Cortex-M3 processor to encrypt 1024 input bytes. As seen in Fig. 3, AES exhibited better performance in CBC mode in comparison to GCM and CCM, as CBC mode does not include the overhead of message authentication. However, if CBC mode is used in conjunction with SHA-based message authentication, it exhibits lower combined performance. As hypothesized, the shorter key lengths exhibited better performance than the longer key lengths for AES, though the impact from key length was lower than the impacts arising from the choice of cipher or mode of operation.

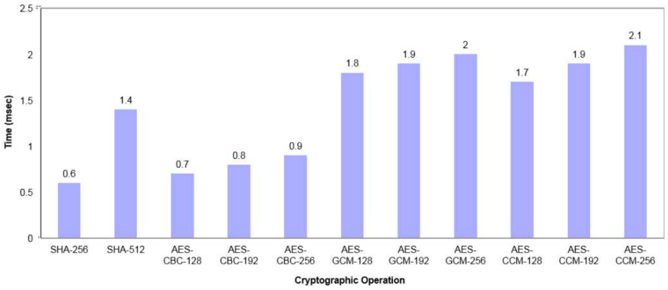


Fig. 3. Comparison of performance between different AES algorithms, from [22].

To approximate conditions on a DER system, a DER testbed network was constructed using an emulated network containing distributed inverters, or remote terminal units (RTUs), which were monitored and controlled at a utility using the SunSpec Validation Platform (SVP). As shown in Fig. 4, the SVP machine was connected through a gateway to a utility router attached to an Internet service provider (ISP) router on a wide area network (WAN), which can either represent a dedicated private line or shared public connection. A total of 20 identical DER inverters were connected to the ISP router through a gateway device. Communications occurred between the DER devices and the SVP machine using Modbus over TCP, with the gateway devices at each end providing an encrypted tunnel using the Secure Shell (SSH) protocol. To demonstrate encryption impact, various symmetric ciphers were deployed in parallel to establish the SSH tunnels between the inverter devices and the controller. For the inverters shown in Fig. 4, each of the connections to DER 01-06 used a different symmetric cipher, while the connection to DER 20 was left unencrypted.

The round-trip communication times required for Modbus/TCP packets to traverse the network were measured using packet capture analysis at each DER device interface, with results plotted in Fig. 5, and mean latency and jitter values given in Table I. Note that there were a small number of cases in which the connection was reset, adding outliers to the latency data and increasing jitter.

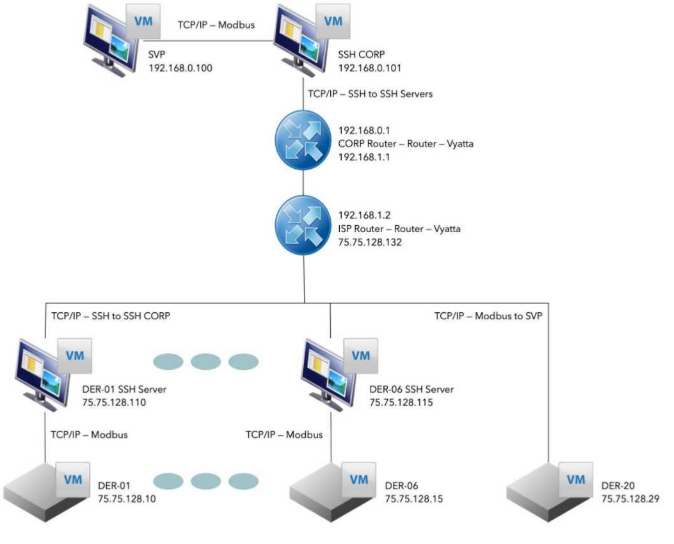


Fig. 4. Topology for testing performance of TLS encryption over a DER network.

TABLE I
MODBUS/TCP DER COMMUNICATION TIMES FOR COMMON SYMMETRIC ENCRYPTION CIPHERS AND MODES.

Case	Mean Latency (ms)	Jitter (ms)
AES128-CTR	4.0526	0.4086
AES192-CTR	4.0662	0.4127
AES256-CTR	4.3728	0.5278
AES128-GCM	4.1056	0.4255
AES256-GCM	4.4290	0.5333
ChaCha20-Poly1305	4.0496	0.3852
Unencrypted	2.3834	0.3358

We confirmed that all modes of encryption resulted in a performance impact when compared with unencrypted communications. As expected, longer key lengths resulted in higher latency and jitter, though the performance impact of using a 256-bit key over a 192-bit key was more significant than that of using a 192-bit key over a 128-bit key. The ChaCha20 cipher with Poly1305 message authentication exhibited similar performance to 128-bit AES in CTR mode, but exhibited lower jitter. The performance differences between the tested modes of operation for AES were lower than the performance differences for various key lengths, confirming the observations made in the encryption performance study discussed above [22].

DER control systems can typically operate with high communication latencies, with supervisory control and data acquisition (SCADA) measurements occurring on intervals of 2-4s [23]). However, smart grid applications can have much lower performance limits, as they may rely on phasor measurement units (PMU), which usually require latencies on the order of 100ms or below. Certain non-DER systems and devices, such as relays located at the utility, substations, or DER aggregators, can require latencies on the order of 10ms. Although the encryption latencies reported in this case study are well under current requirements, they may become more significant if DER devices pick up more grid support functions in the future or if encryption must be performed under the processing

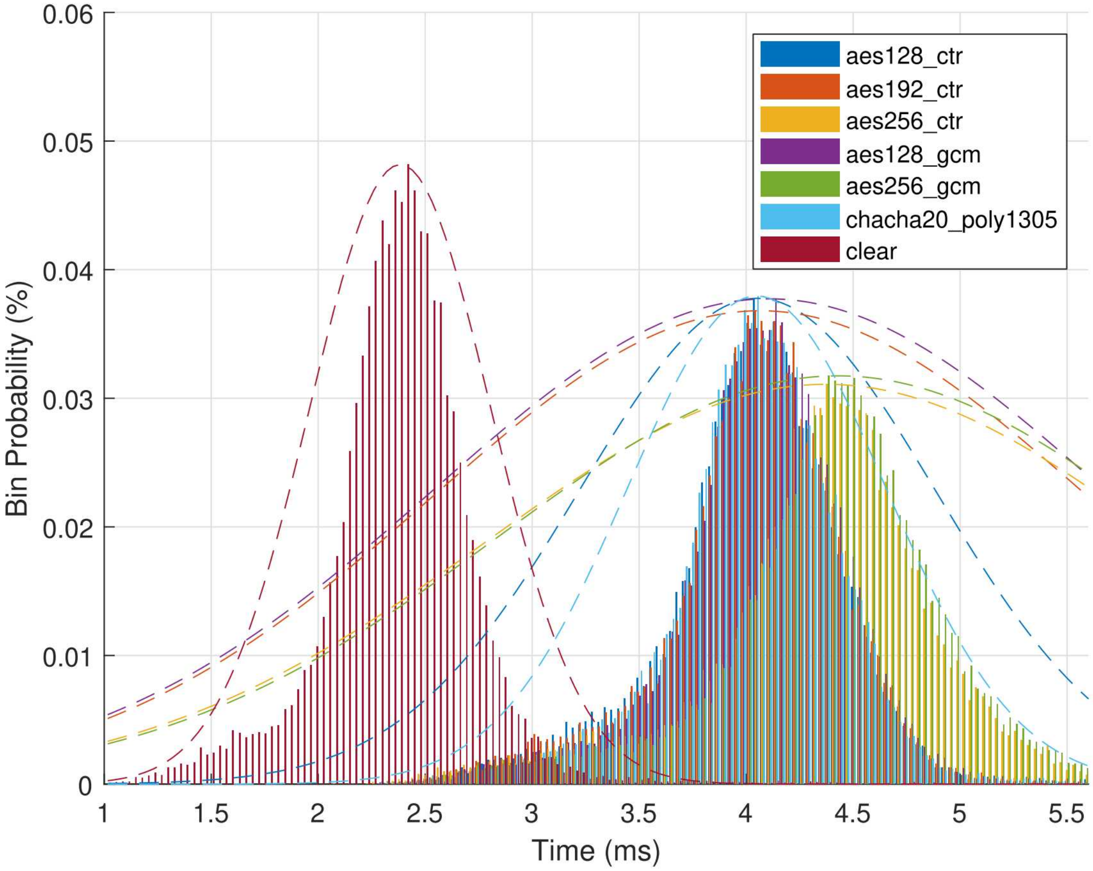


Fig. 5. Modbus/TCP DER communication times for common symmetric encryption ciphers and modes.

constraints of the device.

V. Conclusions

Cryptography is an essential tool for securing communications in DER systems, which represent a rapidly growing segment of the electric grid. However, security risks and mitigation strategies need to be considered against their potential impact on DER system function and performance. In this paper, a review of cryptography algorithms and implementation requirements has been provided to inform the selection and design process for DER cryptosystems. Functional considerations and trade-offs were demonstrated through a case study of a hardware encryption module design, and performance impacts for various symmetric ciphers were measured through a case study on an emulated DER control network. These tests demonstrated that while the performance overhead for symmetric encryption increased round-trip communications latency by a factor of two, the differences between AES and ChaCha performance were less significant, with the encryption key length having a larger impact on AES performance than the block cipher mode.

VI. Acknowledgements

The authors would like to thank the rest of the U.S. Department of Energy Cybersecurity for Energy Delivery Systems (CEDS) Modular Security Apparatus for Managing Distributed Cryptography for Command & Control Messages on Operational Technology Networks (ModuleOT) team and DNK Consulting LLC for their guidance on this research.

References

[1] S. Sridhar, A. Hahn, and M. Govindarasu, “Cyberphysical system security for the electric power grid,” in *Proceedings of the IEEE*, vol. 100, Oct 2011, pp. 210–224.

[2] C. Lai, N. Jacobs, S. Hossain-Mckenzie, C. Carter, P. Cordeiro, I. Onunkwo, and J. Johnson, “Cyber security primer for DER vendors, aggregators, and grid operators,” Sandia National Laboratories, Tech. Rep., 12 2017. [Online]. Available: https://energy.sandia.gov/download/43733/

[3] R. Landauer, “BlackEnergy,” *New Jersey Cybersecurity & Communications Integration Cell (NJCCIC)*. [Online]. Available: https://www.cyber.nj.gov/threat-profiles/ics-malware-variants/blackenergy

[4] “CRASHOVERRIDE analysis of the threat to electric grid operations,” Dragos Inc., Tech. Rep., 2017. [Online]. Available: https://dragos.com/blog/crashoverride/CrashOverride-01.pdf

[5] W. Stallings, L. Brown, M. D. Bauer, and A. K. Bhattacharjee, *Computer security: principles and practice*. Pearson Education, 2012.

[6] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, “A review of false data injection attacks against modern power systems,” *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1630–1638, July 2017.

[7] S. S. Hossain-McKenzie, “Protecting the power grid: strategies against distributed controller compromise,” Ph.D. dissertation, University of Illinois at Urbana-Champaign, 2017.

[8] W. Trappe and L. C. Washington, *Introduction to Cryptography with Coding Theory (2nd Edition)*. Prentice-Hall, Inc., 2012.

[9] "CNSS Policy No. 15, Fact Sheet No. 1, National policy on the use of the advanced encryption standard (AES) to protect national security systems and national security information," National Security Agency, Tech. Rep., 2003. [Online]. Available: https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/cnss15fs.pdf

[10] "Federal information processing standards (FIPS) publication 197 - announcing the advanced encryption standard (AES)," National Institute of Standards and Technology (NIST), Tech. Rep., 2001.

[11] D. J. Bernstein, "Chacha, a variant of salsa20," National Science Foundation, Tech. Rep., 2008.

[12] I. Bhardwaj, A. Kumar, and M. Bansal, "A review on lightweight cryptography algorithms for data security and authentication in IoTs," in *2017 4th International Conference on Signal Processing, Computing and Control (ISPCC)*, Sept 2017, pp. 504–509.

[13] "Rfc 7465 - prohibiting rc4 cipher suites," Internet Engineering Task Force (IETF), Tech. Rep., 2015.

[14] "Advanced encryption standard," *TutorialsPoint*, 2018. [Online]. Available: https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm

[15] J. N. Gaithuru, M. Bakhtiari, M. Salleh, and A. M. Muteb, "A comprehensive literature review of asymmetric key cryptography algorithms for establishment of the existing gap," in *2015 9th Malaysian Software Engineering Conference (MySEC)*, Dec 2015, pp. 236–244.

[16] R. Landauer, "Irreversibility and heat generation in the computing process," *IBM Journal of Research and Development*, vol. 5, no. 3, pp. 183–191, 1961.

[17] "NIST Special Publication 800-53 (Rev. 4)," National Institute of Standards and Technology, Tech. Rep., 2015. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final

[18] R. W. Younglove, "Public key infrastructure: How it works," *Computing & Control Engineering Journal*, vol. 12, no. 2, pp. 99–102, 2001.

[19] R. Housley, W. Ford, W. Polk, and D. Solo, "RFC 5280: Internet x.509 public key infrastructure certificate and CRL profile," International Engineering Task Force, Tech. Rep., 1998.

[20] *IEEE 2030.5-2018 - IEEE Approved Draft Standard for Smart Energy Profile Application Protocol*, IEEE Standards Association Std., 2018.

[21] "Iso/iec 11889-1:2009 information technology - trusted platform module," International Standards Organization (ISO)/International Electrotechnical Commission (IEC), Tech. Rep., 2009. [Online]. Available: https://cr.yp.to/chacha/chacha-20080120.pdf

[22] H. Tschofenig and M. Pegourie-Gonnard, "Performance of state-of-the-art cryptography on arm-based microprocessors," National Institute of Standards and Technology (NIST), Tech. Rep., 2015. [Online]. Available: https://csrc.nist.gov/csrc/media/events/lightweight-cryptography-workshop-2015/documents/presentations/session7-vincent.pdf

[23] P. Kansal and A. Bose, "Bandwidth and latency requirements for smart transmission grid applications," *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1344–1352, 2012.