SAND2018-11778R

Review of Authentication Strategies and Trends for Distributed Energy Resources (DERs)

Sandia National Laboratories

SAND#

Module OT Project

Christine Lai and Patricia Cordeiro

September 2018

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & 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.

Synopsis

In this study we review literature on machine to machine (M2M) authentication and encryption pertaining to communication with grid-attached power inverters. We regard security recommendations from NIST, constrained device recommendations from CoAP, as well as influences from the existing markets. We will not focus on passwordless or multifactor schemes of user authentication, the handover/roaming authentication of mobile systems, or the group authentication of WiMAX/LTE communications.

The de-facto standards for authentication and encryption are certificate-based public key cryptography and AES, respectively. While certificate-based public key cryptography is widely adopted, certificate management is seen as an Achilles heel of public key infrastructure (PKI). State of the art authentication system research includes work on certificateless authentication; however, much work in the areas of privacy preservation, efficient or lightweight systems continue to be based in public key methods. We will see efforts such as bilinear pairing, aggregate message authentication codes, one-time signatures, and Merkle trees surface and resurface with improved authentication approaches.

Though research continues to produce new encryption schemes, AES prevails as a viable choice, as it can be implemented across a variety of resource constrained devices. Other lightweight encryption algorithms often employ the same fundamental addition-rotation-xor operations as AES while achieving higher efficiency, but at steep tradeoffs to security. Despite mathematical proofs of the security of cryptographic algorithms, in practice the greatest weaknesses continue to be incurred during implementation. Security researchers will find edge cases and bugs that allow unintentional behavior.

In the following sections, accepted methodologies of authentication and encryption are discussed. Due diligence for securing M2M communications requires consideration during planning, design, implementation and product lifetime, as opposed to a set-it and forget-it policy. Best practices can be gleaned from published successes *and* failures, with no single end-all, be-all detailed solution.

Review of Current Cryptography Strategies

With increased communication among DER systems, new opportunities for misuse will be accessible to potential cyber attackers and eavesdroppers. Cryptography presents a solution to these issues by enabling two parties, often referred to as Alice and Bob, to communicate without allowing an outside source, Eve, to understand what is being said. Ideally, the information (plaintext) is encrypted using a secret key, translated into ciphertext, and decrypted once it reaches its intended reader. Common components of cryptographic schemes include digital signatures, certificate authentication, and key management. However, it is important to note that cryptography is by no means a panacea for all security needs, but a powerful tool for ensuring the safety of one's data assets.

Symmetric cryptographic algorithms

Confidentiality is maintained through proper key management. If Bob and Alice keep their keys secret, Eve has no way of decrypting the data. When both parties share the same key for encryption and decryption, this is known as a symmetric cipher. These algorithms are often based on substitution and permutation functions and can further be categorized into stream and block ciphers. The former encrypts data one bit at a time and is based on the one-time pad, a cipher proven unbreakable; however, it is cumbersome due to the requirement that the key must be at least as long as the data

encrypted [1]. For example, RC4 was a commonly used algorithm that could be found in 802.11 Wired Equivalent Privacy (WEP), a standard for Wi-Fi communication. Unfortunately, it was poorly designed, and messages between the client and access point were insecure [2].

Among block ciphers, the Advanced Encryption Standard (AES) is a widely used today. AES was announced in 2001 by the National Institute of Standards and Technology (NIST) after the Data Encryption Standard (DES) had been compromised. The organization chose the Rijndael algorithm out of 15 competing designs, and it is now deemed sufficient for use in protected classified information at a TOP SECRET level using its 192 or 256 key lengths [3]. The block cipher works by separating information into 128 bits (16 bytes). Info is encrypted with N rounds (10, 12, 14) depending on key length (128, 192, and 256) respectively. Each round consists of four layers – byte substitution, shift row, mix column, key addition. A simplified flow chart of the encryption can be seen in Fig. 2. There also exist lighter weight cryptography algorithms, e.g., Blowfish and its successor, Twofish, and TEA (tiny encryption algorithm), which function with less memory, storage or time requirements

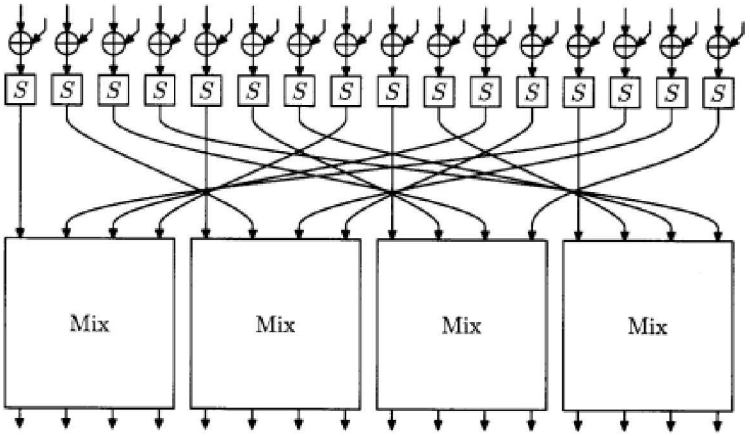

Figure 2: Single round of AES [4, 5].

Asymmetric cryptographic algorithms

Integrity encompasses the accuracy and consistency of data over its intended life cycle. Thus, Eve must not be able to change the data if she manages to intercept it in its transit between Alice and Bob. When working with symmetric algorithms one must ensure that the connection is secure for key handling. Managing several keys at once also becomes an issue when there are numerous recipients. A common solution is implementing public key (asymmetric) encryption.

Asymmetric cryptography can be used for establishment of a shared secret, for encryption and decryption, and for signing and verification. In all these uses, each user has a key pair consisting of a private key and a corresponding public key. The public pieces of the key pairs are distributed ahead of time by a trusted third party such as a certificate authority.

As seen in Fig. 3, when encrypting a message, Alice encrypts with the public key of the intended receiving party. Bob, who possesses the only private key corresponding to this public key, is the only party able to decrypt the message.

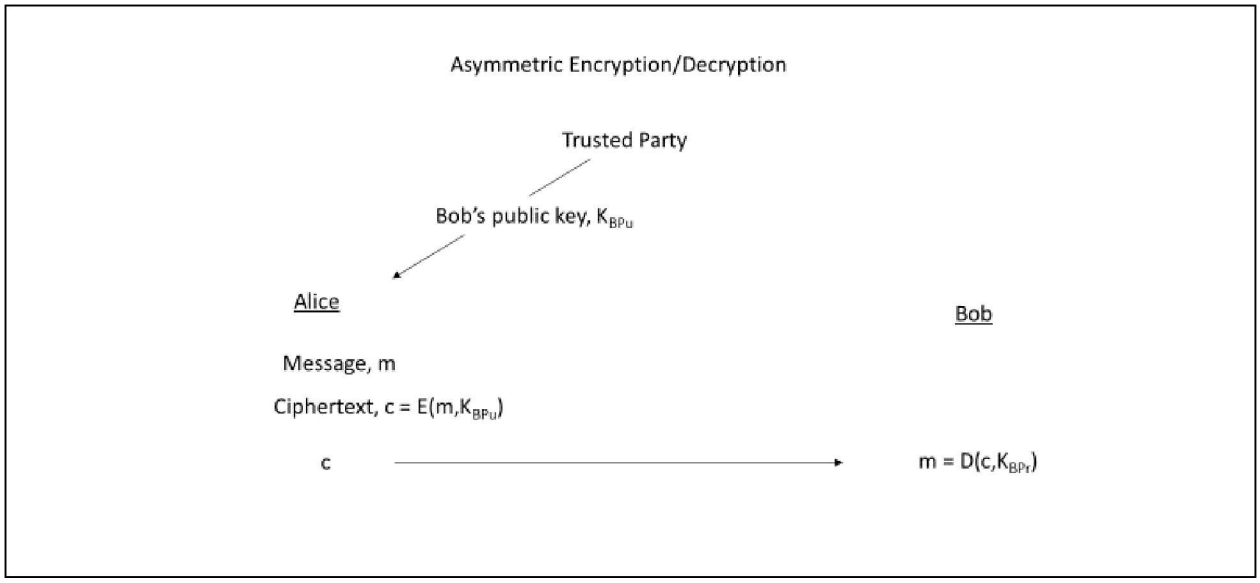

Figure 3: Public key encryption

In the signing and verification scenario seen in Fig. 4, Alice uses her private key to encrypt a hash of the message requiring signature. Bob, upon receipt of the message and signature, decrypts the signature using the public key of the sender, hashes the received message and compares the two for signature validation. Only Alice with the private key corresponding to the known public key could have correctly generated the given signature.

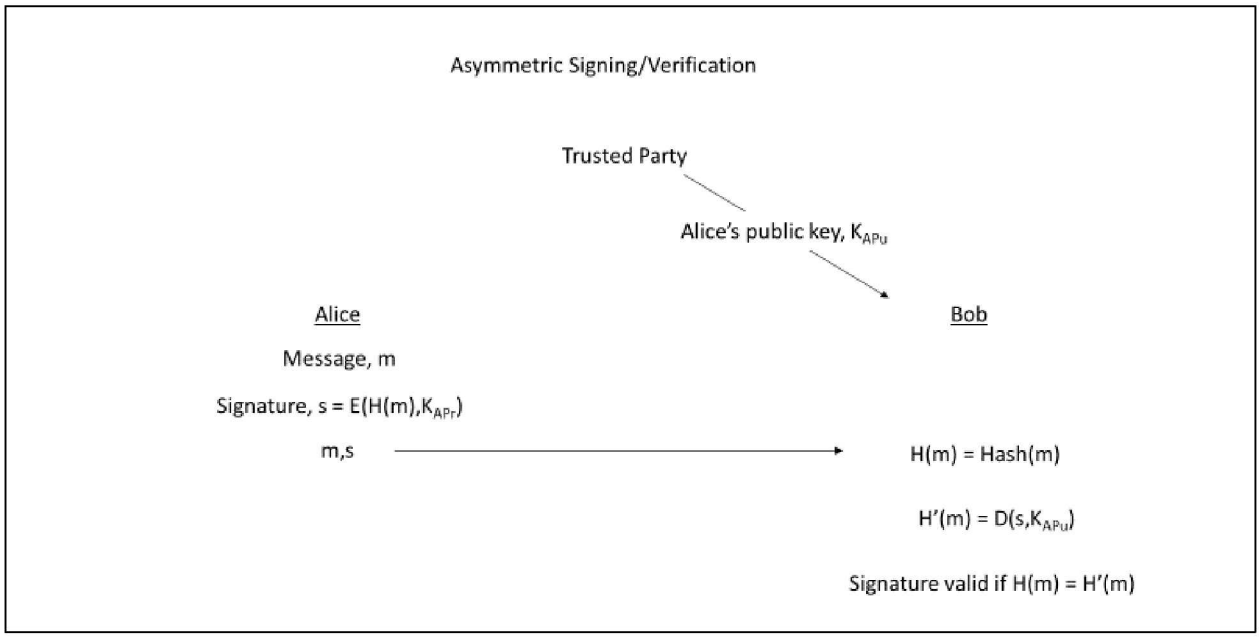

Figure 4: Digital Signatures

RSA is the best-known example of asymmetric cryptography. This algorithm was named after its founders, Rivest-Shamir-Adleman, who publicly announced it in 1978. 1024- or 2048-bit keys are

common for RSA and are still widely used today. The algorithm relies on the computational difficulty of integer factorization and is simplified in Fig. 5 as seen below.

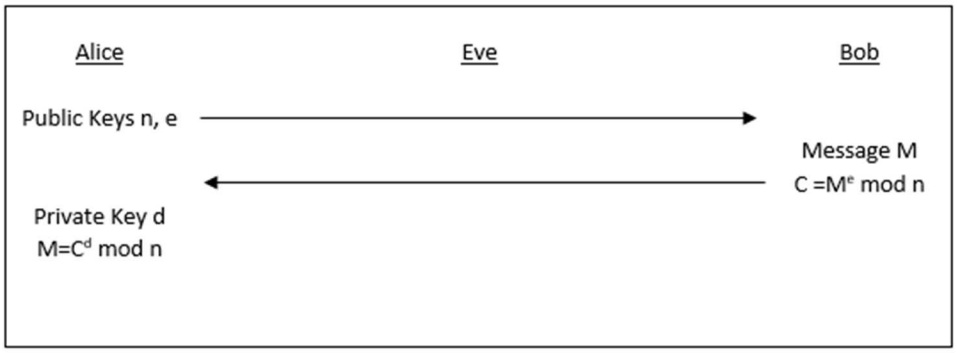

Figure 5: RSA Operation

Alice begins by choosing two large prime numbers p and q. Computers today can determine primes hundreds of digits long. Assuming a 1024-bit key (150 digits) and 1/log(n) probability of primality [6], there would be approximately $2.8*10^{147}$ values to choose from. Alice then multiplies the two values to obtain the product n, which is the first public key sent to Bob. The totient function, $\phi(n)$ is then computed, which yields the number of values coprime with n. Due to $\phi(n)$ being semiprime, this value is (p-1)(q-1). Another value is computed such that $1<e<\phi(n)$ and e is also coprime to $\phi(n)$. This is released as the second public key. Finally, a value, d, is computed such that $de=1+k\,\phi(n)$. This value is kept hidden for decryption. Using the public keys, Bob can encrypt the message using the formula $C=M^e \bmod(n)$ and Alice can decrypt using the formula $C^d=m(\bmod(n))$. It is important to note that while Eve may obtain the public keys n and e, and encrypted message M, she has no way of interpreting the message without the key d.

Elliptic Curve Cryptography (ECC) is another algorithm using one-way functions to perform encryption/decryption and signing/verification operations with asymmetric cryptography. In the case of ECC, the one-way function is the discrete-log problem derived from multiplication of a point on an elliptic curve [7]. Communicating parties agree on a particular curve, E, and a particular base point, P, and obtain each other's public key ahead of time. This is illustrated in Fig. 6.

An example elliptic curve encryption scheme uses the El Gamal cryptosystem [8]. In simple terms, each user selects their own random number as a secret integer and multiplies the base point with their individual secret integer, making the resulting products publicly known. To encrypt a message, the sender multiplies her secret integer by the other party's product and adds this value to the message, sending the resulting sum to the recipient. The recipient multiplies his secret integer by the sender's publicly known product and can now recover the message by subtracting this value from the sender's sum.

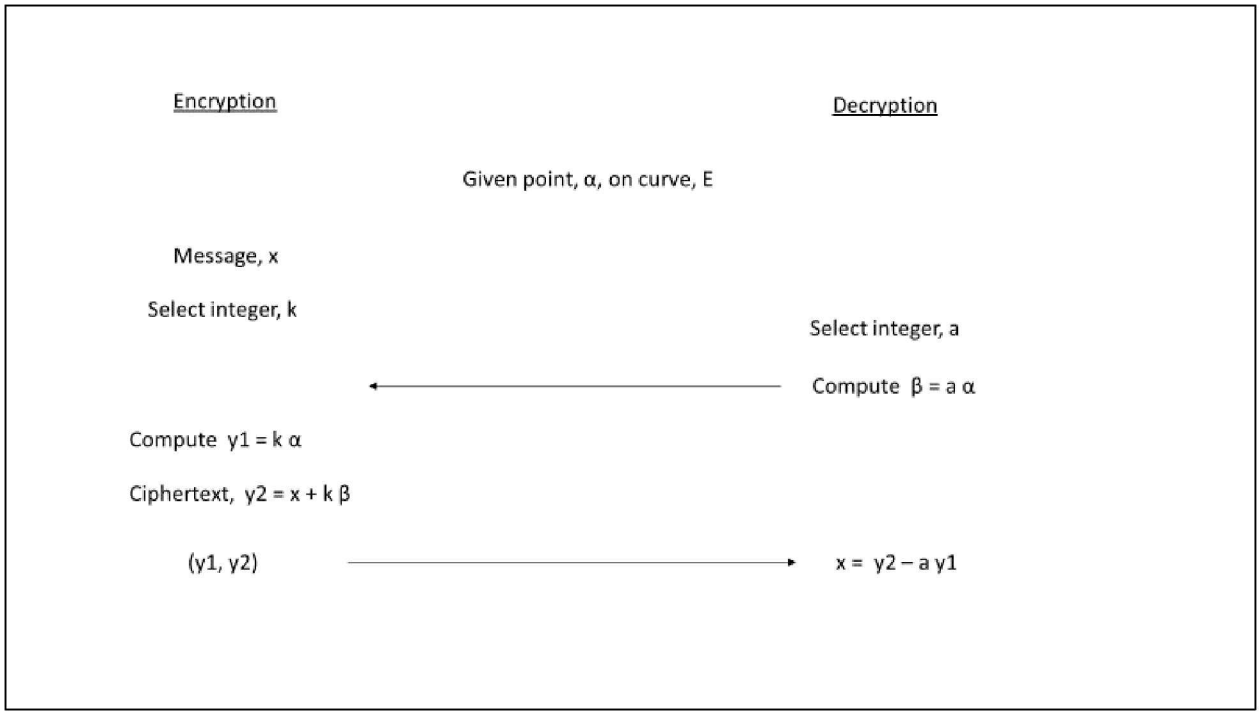

Figure 6: ECC operation.

Elliptic Curve Digital Signature Algorithm (ECDSA) is a commonly used signature/verification scheme [9]. Though the steps shown in Fig. 7 appear more complex than the previously described signing and verification scheme, the essentials are the same. The signer users her private key, dA, to generate a signature, s, by encrypting a hash of her message. The recipient also calculates the message hash, z, and uses the sender's public key, QA, with the signature (r,s), to determine whether the point multiplications on the curve agreed.

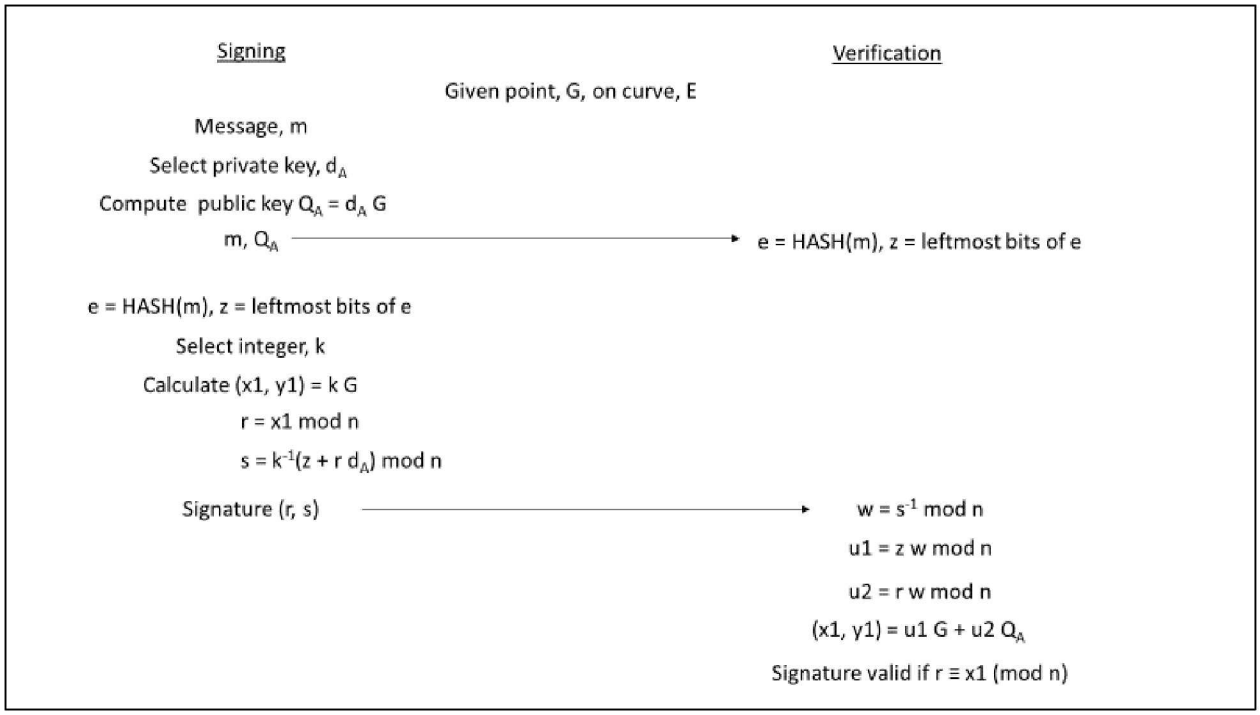

Figure 7: ECDSA process.

For more information on elliptic curve math, see Hans Knutson's article, "What is the math behind elliptic curve cryptography?" [10].

Bit Security Strength of Keys

As previously stated, 128- or 256-bit keys are common for symmetric encryption, however, longer keys are required for asymmetric to achieve same level of security (e.g., 1024- or 2048-bit for RSA, 256- or 384-bit for ECC). The number of bits of security is an indication of how much work is believed to be required to break a cryptographic algorithm with respect to the type of known attacks against the algorithm. For a discussion of security bit strength of cryptographic algorithms, see NIST Special Publication 800-57 [11].

Key establishment and identity binding methods are required

Symmetric ciphers require a secure method for sharing or generating shared secrets. Diffie–Hellman key exchange was one of the earliest examples of generating a shared secret over public channels. The algorithm uses one-way functions such that an eavesdropper is unable to determine the base secrets of the users. Asymmetric ciphers require distribution of public keys and a public key infrastructure is typically used to certify the identity of each key owner.

Public Key Infrastructure (PKI): Enabling Symmetric Cryptography via Asymmetric Cryptography

Symmetric crypto schemes have the advantage of small key sizes and efficient computations when compared with typical asymmetric crypto schemes. Symmetric schemes, however, provide no method of securely sharing the required symmetric key. The common solution is to utilize the less efficient asymmetric algorithms with their asymmetric public/private key pairs to securely establish a shared symmetric key and then proceed with the more efficient symmetric cryptography.

In order to have confidence that a public key belongs to a given entity prior to using that key for establishing a shared secret, theoretically, the following PKI process is used to register, produce and verify a certificate carrying the entity's public key. The steps shown in Fig. 8 are as follows:

1. Entity (e.g. DER) provides proof of identity to Registration Authority (RA)
2. RA requests certificate for entity after authenticating identity

3a. Certificate Authority (CA) binds public/private key pair with identity

3b. CA distributes public portion of certificate to Verification Authority (VA)

4. Entity presents asymmetric-generated signature and public portion of certificate to other party (e.g. Utility)
5. Other party asks Verification Authority (VA) to verify certificate
6. VA responds with revocation status of certificate
7. The other party verifies entity's asymmetric-generated signature based on verified (non-revoked) certificate

Mutual authentication requires that the other party take the exact same steps to prove its identity to the first entity. After mutual authentication, the communicating parties may establish a shared secret key via methods stated in their certificates and proceed with symmetric key encryption and decryption of their transactions.

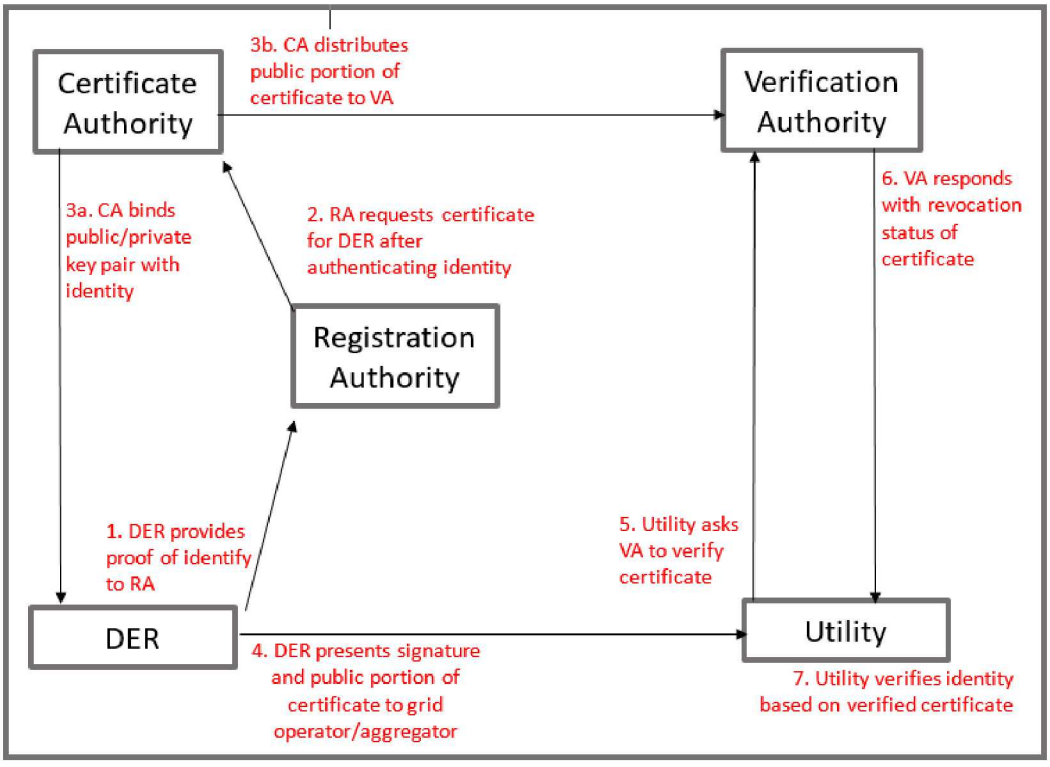

Figure 8: PKI process illustration.

Best Practices for DER Cryptography

Applying best practices toward DER cryptography is much the same as applying best practices toward DER cybersecurity, or ICS and IT networks in general. Risk analysis should be applied to understand the nature of the 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 devices, it is generally recommended that proven technologies be applied such as Internet Protocol Security (IPSec), Transport Layer Security (TLS), to provide defense-in-depth on the system. Many of these general practices are outlined in the DoE/Sandia National Laboratories technical report "Cyber Security Primer for DER Vendors, Aggregators, and Grid Operators" [12].

Security practitioners are certainly not all of one mind with respect to best practices. Some industry groups (such as Digicert, a company in the business of providing certificates) stand by certificate-based public key infrastructure, touting the technology's 20-year run securing banking and commerce [13], while other groups catalog the weaknesses of PKI. Some experts believe in trusted platform modules (TPMs) and other hardware-based keys, while others claim that they are easily circumvented and exploited once an entity has gained privileges in a system. We already rely heavily on both software authentication over the internet and hardware authentication in the form of cellular SIM cards and chip credit cards. Stina Ehrensvard writes that security is a matter of minimizing the available attack surface and achieving separation between processes [14].

Peter Gutmann wrote in 2015:

> "TPMs don't work because all that they can do is store the fixed key that's required to decrypt the other keys (TPMs are just repurposed smart cards and don't have the horsepower to perform anything more than lightweight crypto themselves so you can't offload the overall encryption processing to them), and since for unattended operation they have to release their secrets without a PIN being entered they're just providing plaintext key storage with one level of indirection. Adding custom encryption hardware and performing all of the crypto operations in that is another possible solution, but most manufacturers will be reluctant to add $500 of specialized encryption hardware to a $50 embedded device, or when it's scaled up to PC terms, a $20,000 hardware security module (HSM) to a $2,000 server" [15].

Still, where security is based on raising the bar against attackers, TPMs are a cost effective and tamper-resistant option, as those are two of the main requirements are written into the TPM specifications [16].

PKI Challenges and Alternatives

The X.509 certificate standard was first issued in 1988 and currently forms the basis for public key exchange over the internet. The IEEE 2030.5 (SEP 2.0) specification is incorporated into California Rule 21, which mandates the use of X.509 certificates for DER devices. The adoption of certificate based PKI poses numerous challenges, some of which are specific to ICS environments. One such issue is certificate expiration. The CA/Browser Forum, which regulates TLS/SSL certificates issued for internet clients and servers, currently has a cap of 825 days on certificate lifetimes to improve auditing and enforcement of compliance with validation and revocation standards. However, certificates issued to DER devices currently are set without expiration, as certificate renewal would require that the vendor either have direct access or some other means to validate the physical device.

In addition to the unique challenges posed by the Operational Technology (OT) space, X.509 has many known security flaws and issues which have proved difficult to address over decades of iteration on IT networks. For one, X.509 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, many implementations of PKI turn off key security features, including revocation checks and naming constraints.

Multiple CA Chains and Whitelisting

A quick fix for the issue of root CA revocation and chain ambiguity is to allow an entity to present multiple certificate chains. Unfortunately, this provides minimal benefit to DER devices, as it does not improve the validation process for non-expiring certificates [17].

Instead of presenting a certificate chain and using revocation lists for blacklisting, whitelists can be built using a set of trusted authorization entities that monitor the identity of hosts on the network. This may be a feasible alternative to X.509 provided that DER network maintainers have the incentive to stand up a sufficient number of authorization entities.

Certificateless Public Key Systems

Rather than pre-publishing a certificate to store and verify public keys, a number of alternative methods can be applied to generate private keys for encryption and decryption.

In the simplest certificateless key systems, identifiers such as partial private keys and biometric system data can be provided as inputs to an external key generator to directly encrypt and decrypt messages. Although this removes the problems and costs associated with maintaining certificates and CAs, it compromises security as it requires more information to be exchanged and does not include a revocation mechanism. Shamir (1984) first described an identity-based cryptosystem that eliminates the need for a key exchange process or third party key generator, instead relying on private key generation centers that issue smart cards to users for signing and encryption [18]. These centers serve as a sort of identity escrow, reducing the exposure of the keys during distribution, but also producing a new surface for attack. Al-Riyami and Paterson (2003) published a seminal paper describing a concept for certificateless cryptography that eliminates the identity-based system entirely using a modified key exchange algorithm [19]. This forms the basis for many of the certificateless two-party authentication protocols in development today.

Trust on First Use

The SSH protocol operates on a trust on first use basis, which means that it is assumed that the network has not been compromised at initialization. Rather than setting an expiration date on a certificate, keys are rotated on a periodic basis. This model works well for ICS devices operating within a trusted and contained environment such as a reactor system, but may not necessarily provide the same benefit to DER networks which may have multiple owners, making it more difficult to verify new keys.

PGP: Web of Trust

PKI certificate chains tend to follow a hierarchical structure, with signatures tracing back to a central root authority. In the PGP web of trust model, individuals sign the keys of other individuals within their trusted circle, eventually forming a web of interconnected key signatures [20]. The web of trust has

been used successfully in secure IT network environments with a small number of entities, but more work needs to be done to automate the key installation process for mass deployment. A major flaw in the web of trust model is that if a trusted key is compromised, it is difficult to detect and has a similar level of impact to a root CA compromise.

Blockchain and Trustless Protocols

Rather than relying on a centralized authority or user verification, trustless cryptographic protocols may be employed to verify the identity of devices and encrypt information over a network.

Recent progress has been made on zero-knowledge proof (ZKP) systems, which seek to prove the integrity of data using a set of shared secret keys, but without passing any data over the network. Rather than attempting to verify that a specific device on the network is trusted, ZKP based protocols verify that the device's computations are correct and have not been tampered with, and are particularly useful for validating the output of untrusted computing hardware such as distributed cloud resources. In their simplest form, ZKP systems can be used to prove the identity of a key holder without exchanging or submitting the actual key for verification, eliminating a common attack vector through which keys can be intercepted and duplicated [21]. Although ZKP authentication relies on the use of a secure pre-distribution scheme to initialize the secret keys, the operational complexity is lower than that exhibited by standard key exchange protocols such as Diffie-Hellman [22].

Distributed ledger technology such as blockchains are another means by which device identities and critical data may be stored and verified [23].

However, the technology for trustless ZKP based protocols and decentralized blockchains is still in a nascent state compared to PKI, and the issues of speed, reliability, and scalability still need to be addressed before these technologies are deployed onto ICS systems.

Data Centric Management

Named data networking (NDN) is an alternative to the Internet Protocol (IP) model of communications, in which data is passed between two specified endpoints, and authorization is based on the identity of each endpoint. In the NDN, the data itself is signed and named according to predefined schema, and data access is based on a publish-subscribe model. Although work is still in progress for exchanging information over wide area networks, NDN has been successfully tested as a solution for local networks containing IoT devices and sensors in which it may not be feasible to maintain public key certificates and IP address mappings [24].

Recent Developments and Trends in M2M Authentication

Current research on authentication protocols acknowledges the tradeoffs that must be made between security, reliability, performance, and usability for any particular system. Rather than attempting to build a perfectly secure protocol, the objective is to build a protocol that is secure against the most frequent or harmful attacks. In [5]"How to Authenticate a Device? Formal Authentication Models for M2M Communications Defending against Ghost Compromising Attack", the authors specify four categories of attacks against machine-centric communications and then propose authentication models for defending against each mode of attack. The attack models are summarized in **Error! Reference source not found.** below.

Table 1: Four M2M attack modes and corresponding authentication models, as proposed by Ren et al.

Attack Mode	Authentication Model
Channel eavesdropping	Credential-based
Credential compromising	Machine-metrics based Computation-based Location-based
Function compromising	Reference-based History-based Neighborhood-based Trustworthy stunt Threshold stunt
Ghost compromising	Witness-based Contamination-based

As a result of the broad scope and attack surface for communications systems, the M2M authentication schemes under development by researchers is varied. In "Authentication Protocols for Internet of Things: A Comprehensive Survey," Ferrag et al review several state of the art authentication protocols, as summarized in **Error! Reference source not found.** below [25]. Though their survey includes research which may not directly apply to DER, such as mobile phone authentication schemes capable of handling roaming handovers from cell tower to cell tower, it provides an informative "taxonomy and comparison of authentication protocols."

Table 2: State of the Art M2M Authentication Protocols

Group-based handover authentication **[26]**
Lightweight group authentication **[27]**
Secure and efficient group authentication and key agreement protocol **[28]**
Secure and efficient group roaming **[29]**
Conditional privacy-preserving authentication with access linkability for roaming service **[30]**
Security authentication scheme in machine-to-machine home network service **[31]**
Group-based lightweight authentication scheme for resource constrained machine to machine communications **[32]**
Lightweight acoustic fingerprints based wireless device authentication protocol **[33]**
Duth: A user-friendly dual-factor authentication for Android smartphone devices **[34]**

In "State of the Art in Lightweight Symmetric Cryptography," Biryukov and Perrin examine how to evaluate the tradeoffs that may be made between security, performance and cost [35]. Specific performance metrics for hardware and software implementations are presented, which are summarized below.

Table 3: Hardware and Software Performance Metrics from “State of the Art in Lightweight Symmetric Cryptography

Hardware Metrics	Software Metrics
Gate equivalents (memory consumption and size)	RAM consumption
Throughput (bits or bytes per second)	Code size
Latency since input was set (seconds)	Throughput (bits or bytes per second)
Power consumption (Watts)	

The authors further note that most symmetric encryption algorithms incorporate the following elements:

Table 4: Symmetric encryption elements from " of the Art in Lightweight Symmetric Cryptography"

Non-linear operations
Look-up table
Bit-slice
Add-Rotate-XOR based
Side Channel Analysis countermeasures
Linear operations
Maximum Distance Separable matrix
Bit permutations
XOR and Rotations
Key Schedule
Modes of Operation

Due to the commonalities between most symmetric algorithms, it is unlikely that resources focused on improving or supplanting AES in the DER space would be productive. However, it is important to be aware of developments to ensure that DER systems are interoperable with broader communication networks going forward into the future. Rather than targeting algorithms, the research on DER cryptosystems should focus on making efficient and secure decisions on protocol implementation.

In Table 5: Recent Publications on M2M Authentication below, we present a summary of recent publications on M2M Authentication and describe the key features of various proposed protocols with regards to secure cryptographic communications and resilience against network based attacks. We also highlight their applicability to DER, as well as implementation challenges for the DER space.

Table 5: Recent Publications on M2M Authentication

Title	Authors (Year)	Technology	Notes / Security Features	Applicability to DER
Local Authentication and Access Control Scheme in M2M Communications With Computation Offloading. 10.1109/JIOT.2018.2837163	Lin, Yi-Hui & Huang, Jheng-Jia & Fan, Chun-I & Chen, Wen-Tsuen (2018)	Local Authentication and Access Control Scheme (LACS)	1. User anonymity 2. Mutual authentication 3. Secure key agreement 4. Securely outsourcing computation	+ Device heterogeneity is accounted for + Computation is offloaded from resource-constrained devices - No remote access control
Anonymous mutual authentication with location privacy support for secure communication in M2M home network services. 10.1007/s12652-017-0626-x	Gope, Prosanta (2017)	Secure lightweight anonymous authentication and key agreement protocol	1. Resistance to spoofing and insider attacks 2. Resilience against key exposure	+ Designed for residential home networks - Significant computational and communications overhead
Internet of Things (IoT) Protocols: A Brief Exploration of MQTT and CoAP. 10.5120/ijca2018916438	Ansari, Danish Bilal & Rehman, Atteeq-Ur & Ali, Rizwan (2018)	Message Queue Telemetry Transport (MQTT) and Constrained Application Protocol (CoAP)	In addition MQTT and CoAP, examine XMPP, AMQP, and LWM2M protocols for authenticated and secure transmission.	+ Key exchange and authentication implemented together + CoAP allows communication for constrained IoT devices over the internet - Significant computational and communications overhead

A distributed authentication and key exchange approach for secure M2M communications. 10.1109/ICATCCT.2017.8389148	Satyanarayana Murthy, B & Lingamgunta, Sumalatha (2017)	Simple authentication and key exchange mechanism based on a lightweight public key and symmetric encryption scheme	1. Mutual authentication 2. Trusted key distribution 3. Signing and encryption 4. Formal verification using Simple Promila Interpreter (SPIN)	+ Key exchange and authentication implemented together - Requires trusted key server - Uses RSA, symmetric encryption scheme not specified
Chaotic ZKP Based Authentication and Key Distribution Scheme in Environmental Monitoring CPS. 10.1007/978-3-319-68179-5_41	Boubakri, Wided & Abdallah, Walid & Boudriga, N. (2017)	Chaotic zero knowledge proof authentication and key distribution scheme	1. Private and public keys using Chaotic Chebyshev polynomial 2. ZKP protocol for identity and public key validation 3. Resistance to man-in-the-middle attacks	+ Decentralized key management - Complex implementation and computational overhead
An Anonymous Authentication Scheme for Multi-Domain Machine-to-Machine Communication in Cyber-Physical Systems. 10.1016/j.comnet.2017.10.006	Qiu, Yue & Ma, Maode & Chen, Shuo (2017)	Anonymous authentication scheme for multi-domain M2M environment	1. Validated using Burrows–Abadi–Needham (BAN) logic and Automated Validation of Internet Security Protocols and Applications (AVISPA) 2. Hybrid encryption scheme using certificateless cryptography and AES 3. Resistance to man-in-the-middle and spoofing attacks 4. Resilience against key exposure	+ Certificateless system for cyber-physical system (CPS) + Uses AES for symmetric encryption - Identity is more important than anonymity in power infrastructure

Authentication Protocols for Internet of Things: A Comprehensive Survey. 10.1155/2017/6562953	Ferrag, Mohamed Amine & Maglaras, Leandros & Janicke, Helge & Jiang, Jianmin & Shu, Lei (2017)	Various IoT authentication protocols	Survey of Authentication Protocols: 1. Machine to machine communications (M2M) 2. Internet of Vehicles (IoV) 3. Internet of Energy (IoE) 4. Internet of Sensors (IoS) 5. Threat models, countermeasures, and formal security verification techniques	+ IoT authentication deals with large numbers of untrusted devices + IoT includes cyber-physical devices and sensors - IoT devices may have different computational constraints - Reliability is not as critical for IoT
A Lightweight Authentication Mechanism for M2M Communications in Industrial IoT Environment. 10.1109/JIOT.2017.2737630	Esfahani, Alireza & Mantas, Georgios & Matischek, Rainer & Saghezchi, Firooz & Rodriguez, Jonathan & Bicaku, Ani & Maksuti, Silia & Tauber, Markus & Schmittner, Christoph & Bastos, Joaquim (2017)	Lightweight authentication mechanism based only on hash and XOR operations	1. Mutual authentication 2. Session key agreement 3. Integrity checks 4. Resistance against man-in-the-middle and spoofing attacks	+ IoT authentication deals with large numbers of untrusted devices + IoT includes cyber-physical devices and sensors + Helps to reduce communication and computational costs - Reliability is not as critical for IoT
M2M: From mobile to embedded internet. 10.1109/MCOM.2011.5741144	Wu, Geng & Talwar, Shilpa & Johnsson, Kerstin & Himayat, Nageen & Johnson, Kevin D. (2011)	M2M requirements, challenges, and motivations	Discussion of M2M: 1. Standards development 2. Embedded interfaces 3. Network architectures 4. Technology gaps 5. Enhancements	+ IoT represents not just mobile, but embedded devices + Scalable connectivity + Low latency + Outsourced computation and management - Security for IoT is behind IT - Reliability is not as critical for IoT

Conclusion and Further Work

Authentication and encryption for M2M is an area full of experimentation with constant new attacks and countermeasures. Cryptographic literature on M2M authentication and encryption shows the steady march of proposals and improvements to algorithms with security proofs, efficiency claims and tradeoffs of features.

Standards bodies like NIST write recommendations and normative descriptions with test vectors to ensure proper usage of accepted information protection mechanisms. Methodologies for authentication and encryption are given by these standards bodies though not very plainly as there are many threads to follow and many implementation details left unspecified. Regulatory bodies in finance and medicine, for example, already stipulate the legally required levels of protection for consumer and personal data. Yet, steady innovations, recommendations and regulations are seemingly inadequate vis a vis lists of security vulnerabilities such as those of US-Cert, OWASP and regular headlines.

Security researchers repeatedly show that newly invented crypto schemes must be vetted by application, not just by theoretical proofs, and that standards recommendations, such as dualEC, sometimes fail to hold up to scrutiny. Research shows that cobbling together pieces of a crypto scheme is less secure than using a time-tested library. The research on DER cryptosystems should focus on making efficient and secure decisions on protocol implementation. Minimizing the attack surface and achieving separation of processes in communication-enabled DERs are two important stances for improving security.

Because security research continually discovers new vulnerabilities, the best practice beyond using vetted solutions may be to allocate sufficient resources during planning, design, implementation and life of product, to defend against changing threats. As cryptographer and security reporter Bruce Schneier says, “don’t be complacent.” This may mean creating products that are more easily updated or swapped out by authorized agents, and not allowing devices to be abandoned in the field.

The above work suggests further efforts are needed to assist the DER community in adopting practices defending against evolving threats.

References

[1] "Perfect Secrecy of the one-time pad," Univeristy of Maryland, Maryland.

[2] W. Stallings, "The RC4 Stream Encryption Algorithm," Cryptography and Network Security, 2005.

[3] N. S. Agency, "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," 2003.

[4] N. Fergusen and B. Schneier, in *Practical Cryptography*, Wiley Publishing, 2003, p. 55.

[5] W. Ren, L. Yu, L. Ma and Y. Ren, "How to Authenticate a Device? Formal Authentication Models for M2M Communications Defending against Ghost Compromising Attack," *International Journal of Distributed Sensor Networks,* vol. 9, no. 2, 2013.

[6] H. Riesel, "Progress in Mathematics Vol, 126," in *Prime numbers and computer methods for factorization*, Birkhäuser Boston, 1994.

[7] M. Musson, "Attacking the Elliptic Curve Discrete Logarithm Problem," Acadia University, 2006.

[8] "Elliptic Curve ElGamal Cryptosystem," [Online]. Available: https://www.youtube.com/watch?v=6bGxLE9rIAY. [Accessed June 2018].

[9] "Elliptic Curve Digital Signature Algorithm," [Online]. Available: https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm. [Accessed June 2018].

[10] H. Knutson, "What is the math behind elliptic curve cryptography?," [Online]. Available: https://hackernoon.com/what-is-the-math-behind-elliptic-curve-cryptography-f61b25253da3. [Accessed June 2018].

[11] National Institute of Standards and Technology, "NIST Special Publication 800-53 (Rev. 4)," [Online]. Available: https://nvd.nist.gov/800-53/Rev4/control/SA-18..

[12] 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, Albuquerque, NM, 2017.

[13] "Device to Service Authentication," 2016. [Online]. Available: https://www.digicert.com/wp-content/uploads/2017/04/DeviceToServiceAuthentication.pdf.

[14] S. Ehrensvard, "Why 2018 will be the year for authentication hardware," 2018. [Online]. Available: https://www.yubico.com/2018/02/2018-will-year-authentication-hardware/. [Accessed August 2018].

[15] P. Guttman, "Engineering Security Book Draft April 2014," 2014. [Online]. Available: https://www.cs.auckland.ac.nz/~pgut001/pubs/book.pdf. [Accessed August 2018].

[16] Trusted Computing Group, "TPM Main Specification Level 2 Version 1.2, Revision 116," 2011.

[17] P. Gutmann, "PKI: it's not dead, just resting," *Computer,* vol. 35, no. 8, pp. 41-49, 2002.

[18] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," in *Advances in Cryptology*, Santa Barbara, CA, USA, 1984.

[19] S. S. A.-R. a. K. G. Paterson, "Certificateless Public Key Cryptography," in *Advances in Cryptology - ASIACRYPT 2003*, Taipei, TW, 2003.

[20] A. Abdul-Rahman, "The PGP Trust Model," Department of Computer Science, University College London, London, UK, 1996.

[21] A. F. a. A. S. Uriel Feige, "Zero-Knowledge Proofs of Identity," *Journal of Cryptology,* vol. 1, no. 2, pp. 77-94, 1988.

[22] N. Boudriga, W. Boubakri and W. Abdallah, "A Chaos-based Authentication and Key Management Scheme for M2M Communication," in *9th International Conference for Internet Technology and Secured Transactions*, London, UK, 2014.

[23] M. Swan, Blockchain: Blueprint for a New Economy, Sebastopol, CA, US: O'Reilly Media, Inc., 2015.

[24] L. Zhang, D. Estrin, J. Burke, V. Jacobson, J. Thornton, D. K. Smetters, B. Zhang, G. Tsudik, k. claffy, D. Krioukov, D. Massey, C. Papadopoulos, T. Abdelzaher, L. Wang, P. Crowley and E. Yeh, "Named Data Networking (NDN) Project," PARC: A Xerox Company, Palo Alto, CA, US, 2010.

[25] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang and L. Shu, "Authentication Protocols for Internet of Things: A Comprehensive Survey," *Security and Communication Networks,* 2017.

[26] A. Fu, S. Lan, B. Huang, Z. Zhu and Y. Zhang, "Anovel groupbased handover authentication scheme with privacy preservation for mobile WiMAX networks," *IEEE Communications Letters,* vol. 16, no. 11, p. 1744–1747, 2012.

[27] C. Lai, H. Li, R. Lu, R. Jiang and X. Shen, "LGTH: a lightweight group authentication protocol for machine-type communication in LTE networks," in *Proceedings of the IEEE Global Communications Conference (GLOBECOM'13)*, 2013.

[28] C. Lai, H. Li, R. Lu and X. Shen, "SE-AKA: a secure and efficient group authentication and key agreement protocol for LTE networks," *Computer Networks,* vol. 57, no. 17, p. 3492– 3510, 2013.

[29] C. Lai, H. Li, R. Lu, R. Jiang and X. Shen, "SEGR: A secure and efficient group roaming scheme for machine to machine communications between 3GPP and WiMAX networks," in *Proceedings of the 2014 1st IEEE International Conference on Communications, ICC 2014*, 2014.

[30] C. Lai, H. Li, X. Liang, R. Lu, K. Zhang and X. Shen, "CPAL: A conditional privacy-preserving authentication with access linkability for roaming service," *IEEE Internet ofThings Journal,* vol. 1, no. 1, p. 46–57, 2014.

[31] X. Sun, S.Men, C. Zhao and Z. Zhou, "A security authentication scheme in machine-to-machine home network service," *Security and Communication Networks,* vol. 8, no. 16, p. 2678–2686, 2015.

[32] C. Lai, R. Lu, D. Zheng, H. Li and X. Sherman, "GLARM: group-based lightweight authentication scheme for resourceconstrained machine to machine communications," *Computer Networks,* vol. 99, p. 66–81, 2016.

[33] D. Chen, N. Zhang and Z. Qin, "S2M: a lightweight acoustic fingerprints based wireless device authentication protocol," *IEEE Internet ofThings Journal,* vol. 4, no. 1, p. 88–100, 2017.

[34] H. Zhu, X. Lin, Y. Zhang and R. Lu, "Duth: A user-friendly dual-factor authentication for Android smartphone devices," *Security and Communication Networks,* vol. 8, no. 7, p. 1213–1222, 2015.

[35] A. Biryukov and L. Perrin, "State of the Art in Lightweight Symmetric Cryptography," *IACR Cryptology ePrint Archive,* 2017.