An Approach for Reduction of the Security Overhead in Smart Grid Communication Infrastructure Employing Dedicated Encryption

Miodrag J. Mihaljević
Mathematical Institute, Serbian Academy
of Sciences and Arts, Belgrade, Serbia, and
RISEC, National Institute AIST, Tsukuba, Japan
Email: miodragm@turing.mi.sanu.ac.rs

Aleksandar Kavičić
Department of Electrical Engineering
University of Hawaii
Honolulu, USA
Email: kavcic@hawaii.edu

***Abstract*—This paper considers an approach for partial reduction of the overhead implied by request for data security within the Smart Grid communications infrastructure. A significant part of the implementation and processing overhead appears as a consequence of the data confidentiality request and the related requirement for massive data encryption. Accordingly, this paper points out to the related requirements and employment of certain light-weight and highly secure encryption dedicated to the noisy communication channels.**

***Keywords*—Smart Grid; information-communication infrastructure; overheads; data confidentiality; light-weight encryption; randomness; coding.**

I. Introduction

Generally, a Smart Grid is an autonomous system consisting of an information collection network, a data management center, a power grid control center and power generation and transmission infrastructures (see [16], for example). The information collection network is a complex network involving a multi-hop ad hoc network, WiFi, cellular network, and Internet. The sensor nodes, such as Phasor Measuring Units (PMUs) and Smart Meters (SMs), are deployed over the power grid to monitor the states of the system.

A communication infrastructure is an essential part in the Smart Grid and a scalable and pervasive communication infrastructure is crucial for the operation of a Smart Grid. To ensure the correct functionality of a Smart Grid, it is essential that communications are secured, devices are protected, and privacy is respected. Two main requirements regarding communications are data authentication and confidentiality, and the information-communication infrastructure as a whole must be robust. Note that confidentiality of communications also support the privacy of Smart Grid customers.

In certain domains of information-communications infrastructure of the Smart Grid, the communications channels suffer from unavoidable and high noise (see [2][7], for example). A particular example are the floating wind turbines where only wireless and power line cable (PLC) are available for communications and control purposes, and both of these channels are extremely noisy.

On the other hand, it is interesting to address the following issues: utilization of the inherent noise for design dedicated cryptographic algorithms (based on which the security mechanism are built), when appropriate, to employ the available error-correction coding within a cryptographic algorithm.

Extensive employment of cryptography as ”a must” implies request for light-weight cryptographic primitives in order to minimize the overheads. Overheads as a consequence of information security requests can be listed as follows: (i) implementation overhead; (ii) computational overhead; (iii) communications overhead.

Motivation for the Work. In order to reduce the overheads in a lot of scenarios the requirement is employment of the lightweight cryptographic techniques On the other hand, also in a lot of scenarios, the requirement is high (provable, preferably) security of the employed cryptographic primitives; particularly the above requirements appear regarding a number cryptographic techniques required in the Smart Grid. As illustrations of the previous statements, note the following: (i) a lot of IT components requires power supply from batteries, because it is too expensive to equip each tiny IT device with AC to DC convertor; (ii) the smart-meters are two-way communication-control devices which could remotely control the power availability at a home, and in order to avoid potential disastrous impacts of malicious control the employed cryptographic techniques should be highly secure and preferably provably secure ones.

Organization of the Paper. A background on Smart Grid relevant for this paper is given in Section II, and Section III discusses corresponding data security issues and implications. Section IV points out to the noisy nature of the main communication channels within Smart Grid. An approach for light-weight and dedicated encryption which fits into the security and implementation requirements is given in Section IV, and its implementation complexity is considered in Section V. Concluding discussion is given in Section VI.

II. A Background on Smart Grid

In the Smart Grid, data collection is performed by measuring devices, including PMUs and SMs. The data management center communicates with the sensors and the control centers through the network. It analyzes the information of the power grid and makes corresponding decisions. The power grid control centers receive instructions from the data management center and rule the power system according to the received instructions. The whole system works in a real-time manner, which implies real-time situation awareness, real-time response, and real-time control.

According to the above discussion, Fig. 1 points out the important two-way nature of the information transmission within the information-communications sub-infrastructure related to SMs (advanced metering infrastructure - AMI), and the required basic cryptographic techniques for providing security of this infrastructure.

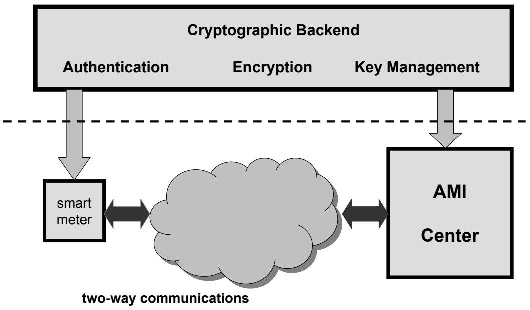

Figure 1. Illustrative model of security issues regarding communications within advanced metering infrastructure (AMI).

In addition to the above, particularly note the following. The measuring nodes are usually implemented as embedded systems to perform data processing and two-way communications. Due to the vast amount of deployment, each node is relatively cheap and simple. Thus, they have very limited on-board resources including power availability. For example, they usually have one simple low speed Micro Control Unit (MCU) as the processor, very limited memory space and very tight power budget due to their deploying areas, cost and physical sizes. The MCU is a small computer integrated on a single chip. It runs programs to support computation and control tasks in an embedded system. The MCUs are usually much simpler than the CPUs for the general purpose computers. Therefore, only some basic tasks, like simple computation and communication, can be implemented on these nodes.

Also, basically, most of the PMUs and SMs are deployed ”in the wild”. The collected data are usually transmitted through wireless links that rely on the open media (i.e., wireless channel). The adversaries can easily physically destroy or replicate these devices by capturing them. The attackers can also launch attacks by setting up some hacker equipment.

III. Data Security Issues and Implications

A. Preliminaries

The network based monitoring system provides efficient remote monitoring and control, but also exposes the Smart Grid to potential cyber attacks. On the other hand, misleading information (or stale information) can cause severe (even disastrous) consequences to the system, as well as to the customers. Illustrations of the previous claim are given as follows. For example malicious modification of phasor information can cause wrong management operations. Malicious analysis against the smart meter data can reveal the living schedule of the householders or production activities of a plant. In an attacking scenario, which should not be excluded due to the interconnection of the system, the terrorists could collect (for example) 80% of the sensitive information that can be used to mount further attacks on the whole Smart Grid. Accordingly, communication security which provides integrity, authenticity, availability and confidentiality over the whole system has to be enforced by appropriate cryptographic algorithms (as illustrated in Fig. 1).

B. On the Need for Advanced Cryptographic Techniques for Information Security within the Smart Grid

A consideration of suitable cryptographic components could begin from the following simple question: Do we face any specific security requirement regarding the Smart Grid information-communication infrastructure, in comparison with traditional security requirements for wireless networks, for example. If we claim ”Yes”, a natural follow-up question is: ”Why”. On the other hand, if we need advanced cryptographic techniques a natural question is: ”What are the related requirements”. This section addresses the previously mentioned issues.

First, we stress the following:

- Security requirements should be related to the impacts of potential security problems. We can identify a number of very different impacts of the security problems in the Smart Grid information-communication infrastructure in comparison with a mobile telephony network, for example.
- Compromising the security of the information-communication infrastructure could imply a collapse of the Smart Grid, and recovering the Smart Grid is much more complex then recovering a wireless network. Accordingly, the Smart Grid information-communication infrastructure requires stronger security in comparison with a wireless network because of possible more severe impacts of compromising the security.

Regarding the question ”Do we need cryptographic techniques different than currently standardized ones”, we emphasis the following:

- For example, if AES (Advanced Encryption Standard) is enough, why we do not employ it in mobile telephony and in a number of other possible applications;

- If the existing cryptographic techniques are enough than we already have the best ones, and this is very unlikely ...

C. Requirements on Cryptographic Techniques for the Smart Grid

In a number of application scenarios within the Smart Grid, an important request is employment of light-weight cryptographic algorithms in order to reduce the overhead to the system implied by involved cryptographic mechanisms (see, for example, discussions in [5][12][16]). At the same time, beside the light-weightiness, the employed cryptographic algorithms should be highly secure. These issues are elaborated in more details as follows.

1) Light-Weight and Highly Secure: Employed cryptographic techniques:

- should provide low overhead implied by implementation of cryptographic elements - massive employment of cryptographic techniques if they are not light-weight, cumulatively could imply high overhead, and particularly regarding extensive device-to-device (M2M) communications; particularly, note that complex encryption algorithms also imply heavy power consumption and when the power is obtained from batteries a consequence is the excessive drain on batteries.
- should not be a weak point because impacts of compromised security could be much more stronger in comparison with other systems - a Smart Grid requires employment of strong cryptographic primitives because impacts of compromising a cryptographic primitive could be disastrous.

2) Dedicated: In order to achieve the above implementation and security requirements, we need advanced and dedicated cryptographic primitives which are light-weight and provably secure ones in order to provide/support efficient and effective Smart Grid security and privacy; taking into account the entire overhead which security requirements imply, dedicated cryptographic techniques that meet security requirements and minimize the overhead are very welcome.

IV. Noisy Communication Channels in the Smart Grid

In certain domains of information-communications infrastructure of the Smart Grid, the communications channel suffer from unavoidable and high noise. A particular example are the floating wind turbines where only wireless and power line cable (PLC) are available for communications and control purposes, and both of these channels appear as very noisy. Accordingly, for reliable communications we need an adequate error-correction coding scheme. On the other hand it is interesting to address the issues of employment the inherent noise for design dedicated cryptographic algorithms based on which the security mechanism are built, as well as, when appropriate, to employ the available error-correction coding within a cryptographic algorithm.

Particularly, note the following communications problems regarding floating wind turbines.

- Highly reliable (low noise) communication channels are not available, and standard Internet-like communication channels are not available.
- Basically, there are only two communication options: Wireless or via Power Line Cable (PLC). Both options suffer from high noise (as discussed in [2][7], for example).
  - Wireless Channel: Mostly assumed AWGN, presence of impulsive noise in certain environments
  - PLC Channel: More complicated noise structure: colored background noise, narrow band noise and impulsive noise.

V. An Approach for Dedicated Encryption

As discussed in the previous sections, in certain Smart Grid scenarios we need light-weight and highly secure cryptographic components and at the same instance we face a noisy implementation environment. This and the next section address design and analysis of a cryptographic algorithm for encryption which employ the channel noise for the cryptographic security enhancement. Light-weight cryptographic algorithms are very important but currently available ones suffer from security weaknesses (as an illustration, see [13] and [14]). On the other hand, it has been shown that physical noise could play a supporting role in cryptographic security enhancement (see [8][11], for example). This section points out to an encryption scheme suitable for the scenarios where (i) the requirement is employment of lightweight (in order to reduce the overweight implied by the employed cryptography) and highly secure algorithms; (ii) physical noise is available for enhancing the security. It is assumed that the symmetric key management is based on a pre-distribution paradigm.

A. Encryption and Decryption Algorithms

The approach [15] pointed out in this section yields a framework for achieving light-weight implementation and processing complexity and a high cryptographic security level implied by employment of the randomness which appears as a supporting element for enhancing the security implied by hardness of the so called LPN problem (Learning Parity with Noise).

We assume the following notation:

- $\mathbf{a} = [a_i]_{i=1}^{\ell}$: ℓ-dimensional binary vector of message/plaintext data;

- $\mathbf{r} = [r_i]_{i=1}^{m-\ell}$: $(m-\ell)$-dimensional binary vector of random data where each r_i is a realization of the binary random i.i.d. variable R_i such that $\Pr(R_i = 1) = \Pr(R_i = 0) = 1/2$, $i = 1, 2, ..., n$;

- $\mathbf{u} = [u_i]_{i=1}^{k}$: k-dimensional binary vector of random data

where each u_i is a realization of the binary random i.i.d. variable U_i such that $\Pr(U_i = 1) = \Pr(U_i = 0) = 1/2$, $i = 1, 2, ..., k$;
- $\mathbf{S} = [s_{i,j}]_{i=1}^{k}\,{}_{j=1}^{n}$: $k \times n$-dimensional binary matrix of the secret key
- $\mathbf{v} = [v_i]_{i=1}^{n}$: n-dimensional binary vector of random data where each v_i is a realization of the binary random i.i.d. variable V_i such that $\Pr(V_i = 1) = p$ and $\Pr(V_i = 0) = 1 - p$, $i = 1, 2, ..., n$;
- $C_H(\cdot)$ and $C_H^{-1}(\cdot)$: operators of the homophonic encoding and decoding, respectively; $C_H(\cdot)$ denotes a mapping $\{0, 1\}^m \rightarrow \{0, 1\}^m$;
- $C_{ECC}(\cdot)$ and $C_{ECC}^{-1}(\cdot)$: operator of the error-correction encoding and decoding, respectively; $C_{ECC}(\cdot)$ denotes a mapping $\{0, 1\}^m \rightarrow \{0, 1\}^n$.

This section points out to a symmetric key encryption scheme [15], where the encryption and decryption operations are specified by the following.

- *Encryption*
  1) Employing $\mathbf{r}$, perform the homophonic encoding of $\mathbf{a}$, and the error-correction encoding of the resulting vector as follows: $C_{ECC}(C_H(\mathbf{a}||\mathbf{r}))$ where $||$ denotes concatenation.
  2) Generate the ciphertext in form of n an dimensional binary ciphertext vector $\mathbf{z}$ as follows:

$$\mathbf{z} = C_{ECC}(C_H(\mathbf{a}||\mathbf{r})) \oplus \mathbf{u} \cdot \mathbf{S} \oplus \mathbf{v} \ . \qquad (1)$$

- *Decryption*
  Assuming availability of the pair $(\mathbf{u}, \mathbf{z})$ decrypt the ciphertext as follows:

$$\mathbf{a} = tcat_\ell(C_H^{-1}(C_{ECC}^{-1}(\mathbf{z} \oplus \mathbf{u} \cdot \mathbf{S}))) \ , \qquad (2)$$

  where $tcat_\ell(\cdot)$ denotes truncation of the argument vector to the first ℓ bits and the assumption is that the employed code which corresponds to $C_{ECC}(\cdot)$ and $C_{ECC}^{-1}(\cdot)$ can correct the errors introduced by a binary symmetric channel with the crossover probability p.

Note that the random vector $\mathbf{u}$ is a public one, and the decryption part assumes availability of the pair $(\mathbf{u},\ \mathbf{z})$. Also note that the decryption does not require knowledge of $\mathbf{r}$.

The proposed encryption scheme is displayed in Fig. 2.

B. Algebraic Structure Assuming Employment of Linear Codes

Encoding Issues. When the employed homophonic and error-correcting codes are linear, the encoding operations in both cases are vector-matrix multiplications. Accordingly, the encoded version of $\mathbf{a}||\mathbf{r}$ is given by the following:

$$C_H(\mathbf{a}||\mathbf{r}) = [\mathbf{a}||\mathbf{r}]\mathbf{G}_H , \qquad (3)$$

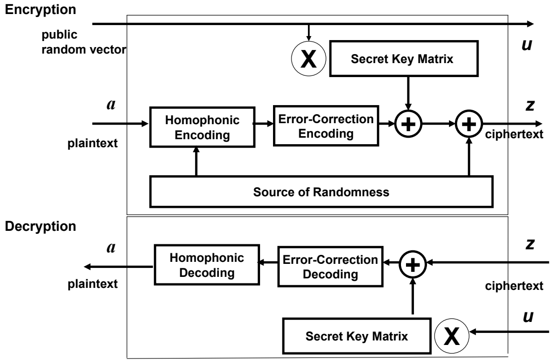

Figure 2. Encryption scheme [15] which involves randomness and dedicated coding.

and $\mathbf{G}_H$ is an $m \times m$ matrix, and thus

$$\begin{aligned} C_{ECC}(C_H(\mathbf{a}||\mathbf{r})) &= C_{ECC}([\mathbf{a}||\mathbf{r}]\mathbf{G}_H) \\ &= [\mathbf{a}||\mathbf{r}]\mathbf{G}_H\mathbf{G}_{ECC} \\ &= [\mathbf{a}||\mathbf{r}]\mathbf{G} \qquad (4) \end{aligned}$$

where $\mathbf{G}_{ECC}$ is an $m \times n$ binary generator matrix corresponding to $C_{ECC}(\cdot)$, and $\mathbf{G} = \mathbf{G}_H\mathbf{G}_{ECC}$ is an $m \times n$ binary matrix summarizing the two successive encodings at the encryption side, implying that

$$\mathbf{z} = [\mathbf{a}||\mathbf{r}]\mathbf{G} \oplus \mathbf{u} \cdot \mathbf{S} \oplus \mathbf{v} \ . \qquad (5)$$

Decoding Issues. Assuming that the employed error-correction code can correct all the errors introduced by the vector $\mathbf{v}$ we have

$$C_{ECC}^{-1}(\mathbf{z} \oplus \mathbf{u} \cdot \mathbf{S}) = C_{ECC}^{-1}(C_{ECC}(C_H(\mathbf{a}||\mathbf{r})) \oplus \mathbf{v}) = [\mathbf{a}||\mathbf{r}]\mathbf{G}_H \qquad (6)$$

and accordingly,

$$C_H^{-1}(C_{ECC}^{-1}(\mathbf{z} \oplus \mathbf{u} \cdot \mathbf{S})) = [\mathbf{a}||\mathbf{r}]\mathbf{G}_H\mathbf{G}_H^{-1} = [\mathbf{a}||\mathbf{r}] \ , \qquad (7)$$

implying that

$$tcat_\ell(C_H^{-1}(C_{ECC}^{-1}(\mathbf{z} \oplus \mathbf{u} \cdot \mathbf{S}))) = \mathbf{a} \ . \qquad (8)$$

C. A Summary of Security Issues

The encryption technique [15] is based on a framework for enhancing security of light-weight stream ciphers employing randomness and dedicated coding. Security evaluation of the considered framework has been discussed from information-theoretic and computational-complexity points of view in [15]. Regarding the information-theoretic approach, the equivocation of the secret key is analyzed. The computational-complexity evaluation approach shows that recovering of the secret key appears as hard as decoding of certain general linear block codes, i.e. certain problems of learning the parity in noise (the LPN problem) assuming appropriate design a linear block codes, which provide joint error-correction and homophonic coding.

LPN based schemes offer a very strong security guarantee. The LPN$_{k,\epsilon}$ problem is equivalent to the problem of decoding certain random linear code (k,n) after the binary symmetric channel with the crossover probability (”noise level”) equal to ϵ, a problem that has been extensively studied in the last half century and which is provably NP-complete in the worst case scenario as shown in [3]. On the other hand hardness of the LPN problem in the average case has been studied and still, the fastest known algorithms run in exponential time.

VI. Implementation Issues

This section discusses the implementation resources required and complexity of the considered encryption/decryption which shows that the entire implementation is light-weight. Particularly, we point out to a technique for the inner product evaluation which provides an opportunity for a trade-off between time and space implementation complexity. Finally, a brief summary of the Advanced Encryption Standard (AES), relevant for comparison with the approach given in this paper regarding the implementation, is given.

A. Implementation Requirements

The implementation of the considered encryption requires the following: (i) a source of randomness, (ii) suitable error correction code; (iii) suitable homophonic code, and (iv) resources for the computations over GF(2). The following discussion show that the above requirements fit into a framework of the light-weight encryption.

Regarding requirement for a source of randomness, note that it is the same as requirement discussed regarding HB-authentication protocols (see [9], for example) designed for resource limited implementation scenarios like RFID ones, and accordingly the assumption on availability of a ”light-weight” source of randomness is justified, particularly noting that the generation of randomness could be supported by the assumed environmental noise.

Following [1], the ECC reported in [17] can be employed in the proposed cipher as well. Particularly note that the codes reported in [17], have the property that the encoding can be computed via a circuit of size $O(n)$ and the decoding can be decoded by a circuit of size $O(n\log_2 n)$ making them the candidate codes.

Regarding the required homophonic coding we point out to the following. Homophonic coding or ”multiple substitution” (see [10], for example) is a technique for mapping source data employing certain random bits into the encoded data which are the randomized form of the source ones so that the source data can be recovered from the noise-free encoded ones without knowledge of the random bits. Homophonic encoding provides that many particular outputs of encoding become possible substitutes (or ”homophones”) of the source data based on employment of different random sequences. Perfect homophonic code provides that the encoded data appear as truly random ones.

A particular class of homophonic codes are the universal ones reported in [10]: These codes provide the randomization without knowledge of the source data statistics which is a request for some homophonic coding schemes. The source data can be recovered from the homophonic encoder output without knowledge of the randomizing data by passing the encoded data through the decoder and then discarding the randomizer bits.

Finally, note that the Wire-tap channel coding [18] is based on assigning multiple codewords to the same information vector and from that point of view, particularly when the main channel is noise-free, it shares the same underlying idea employed in the homophonic coding.

Next subsection discusses some of the issues regarding implementation of the operations over GF(2).

B. Discussion of the Encryption and Decryption Operations

We assume that implementation of the proposed scheme is based on employment of light-weight source of randomness, based on the existing channel noise, and error-correction coding. Particularly, we assume that a low-implementation complexity linear error correcting code is employed: such coding scheme has encoding and decoding complexities linearly proportional to the codeword length n. Also note that the proposed scheme requires only one additional (homophonic) encoding at the encryption side and one additional (homophonic) decoding at the decryption side

Accordingly, the algebraic representation of encryption and decryption, when liner codes are employed, implies the following: (i) Encryption requires $mn + kn$ binary multiplications and $mn + kn + n$ mod 2 additions (see (5)); (ii) Decryption requires $kn+m^2$ binary multiplications, $kn + n + m^2$ mod 2 additions, and $O(n)$ operations for decoding of the employed linear error correcting code.

Also, note the following: When the linear codes are employed, the algebraic representation of encryption and decryption directly shows that the implementation complexity is dominated by the required number of the inner products between binary vectors. The next section points out that we can employ dedicated look-up tables instead of binary multiplications and additions for obtaining (if appropriate) certain trade-offs between the time and space implementation complexity.

C. An Implementation of the Inner Products Evaluation

Here is given an approach for time-memory trade-off based on a read-only memoriy (which play role of a number of look-up tables) In a look-up table implementation, all the possible outputs of the function are pre-calculated and stored in the memory. Each time the output of an input is looked up in the memory instead of being calculated calculated. The look-up table can save the computation operations at cost of storage space.

Let $\mathcal{A}$ be a set of binary vectors $\mathbf{a} = [a_i]_{i=1}^n$, and $\mathcal{B}$ be a set of binary vectors $\mathbf{b} = [b_i]_{i=1}^n$ with the cardinalities $|\mathcal{A}| >> |\mathcal{B}|$.

Any inner product

$$\mathbf{a} \cdot \mathbf{b} = \bigoplus_{i=1}^{n} a_i b_i \ \ , \tag{9}$$

can be considered as

$$\mathbf{a} \cdot \mathbf{b} = \bigoplus_{j=0}^{\frac{n}{\Delta}-1} (\bigoplus_{i=1}^{\Delta} b_{j\Delta+i} \ a_{j\Delta+i}) \ \ , \tag{10}$$

assuming that $\frac{n}{\Delta}$ is an integer. On the other hand, each sub-sum $\bigoplus_{i=1}^{\Delta} b_{j\Delta+i} \ a_{j\Delta+i}$ can be considered as a liner Boolean function of Δ arguments. Accordingly, the inner product (9) can be considered as the modulo 2 sum of of the outputs of Δ linear Boolean functions. Taking into account that $|\mathcal{A}| >> |\mathcal{B}|$, it is suitable to consider that a segment of $\mathbf{b}$ specifies a linear Boolean function $f_j(\cdot)$, and a segment of $\mathbf{a}$ the arguments of this Boolean function. Accordingly, we have:

$$f_{j,b}([a_{j\Delta+i}]_{i=1}^{\Delta}) = \bigoplus_{i=1}^{\Delta} b_{j\Delta+i} \ a_{j\Delta+i} \ . \tag{11}$$

Consequently, the inner product (10) appears as

$$\mathbf{a} \cdot \mathbf{b} = \bigoplus_{j=0}^{\frac{n}{\Delta}-1} f_{j,b}([a_{j\Delta+i}]_{i=1}^{\Delta}) \ . \tag{12}$$

It is well known that any Boolean function of Δ arguments (see [4], for example) can be implemented employing a look-up table of dimension 2^{Δ}. Also, the cumulative inner product (12) can be evaluated employing a binary look-up table of dimension $2^{n/\Delta}$. (Of course, instead of one-step look-up table evaluation of (12), a multiple step approach could be considered employing a cascade of look-up tables, but this approach is out of the scope of the current consideration.)

According to the above discussion, any of the considered inner products can be evaluated with time complexity $O(1)$ employing $\frac{n}{\Delta}$ binary look-up tables each of dimension 2^{Δ}, and an additional look-up table of dimension $2^{n/\Delta}$. So, the total space complexity C_S of the above approach for the inner products evaluation is upper-bounded as follows:

$$C_S \leq 2^{n/\Delta} + |\mathcal{B}|\frac{n}{\Delta}2^{\Delta} \tag{13}$$

where m is a parameter. In order to have a balance between the space complexity required for the evaluation of partial inner products (11) and the cumulative one (12), we have the following requirement:

$$2^{n/\Delta} \leq |\mathcal{B}|\frac{n}{\Delta}2^{\Delta} \tag{14}$$

which for the given parameters $|\mathcal{B}|$ and n yields the maximal $\frac{n}{\Delta}$ such that (14) is fulfilled.

D. Elements for an Illustrative Comparison

A number of different encryption schemes are employed in Smart Grid: Some are proprietary algorithms (not disclosed) and some are the standardized/recommended ones like Advanced Encryption Standard (AES).

For the illustrative preliminary comparison of the proposed encryption technique and the currently recommended ones, we point out to the recommendation from [6], where AES is pointed out as an encryption algorithm and discussions of its energy consumption from [16].

AES is an encryption algorithms which generates the ciphertext through a number of iterative recalculations. AES with 128-bit secret key consists of the following operations: (i) $Key\_Expansion$ round keys are derived from the secret key; (ii) Initial Round each byte of the state is combined with the round key using bitwise xor (iii) 10 Rounds each consisting of the following four procedures: (a) Sub_Bytes - a non-linear substitution step where each byte is replaced with another according to a lookup table; (b) $Shift\_Rows$ - a transposition step where each row of the state is shifted cyclically a certain number of steps. (c) $Mix\_Columns$ - a mixing operation which operates on the columns of the state, combining the four bytes in each column. (d) Add_Round_Key; (iv) Final Round (no $Mix\_Columns$): Sub_Bytes, $Shift\_Rows$, Add_Round_Key.

The above description illustrates that AES has significantly higher implementation complexity, particularly because AES operates through 10 main rounds plus the initial and final ones, and the employed operations are more complex in comparison with mod 2 additions. This higher implementation complexity, in a number of scenarios, implies a heavy overhead at least regarding the power consumption.

VII. Conclusion

This paper elaborated that Smart Grid communication infrastructure requires low-weight and highly secure cryptographic techniques and particulary the ones for encryption. Also, it is shown that certain communications channels are highly noisy. Taking into account the addressed scenario, this paper points out to a light-weight and highly secure stream cipher encryption technique which employs the unavoidable channel noise for enhancing the cryptographic security.

This paper shows an alternative approach for encryption which is based on joint employment of pseudorandomness, randomness and dedicated coding. The approach is based on an enhanced underlying LPN problem. The LPN problem based schemes provide a background for simple and efficient designs in terms of code-size as well as time and space requirements. This makes them prime candidates for light-weight devices like RFID tags, which are too weak to implement standard cryptographic primitives like the block cipher AES.

This paper points out to a particular light weight symmetric encryption as a component for reduction of the following overheads: (i) implementation overhead; (ii) processing overhead, and (iii) power consumption overhead. At the same time the considered encryption provides a high level of provable security required because of possible high impacts of the broken encryption algorithms and particularly in the scenarios which assume pre-distribution of the symmetric secret keys.

The algorithm proposed for the encryption, within noisy communication channels of the Smart Grid communication infrastructure, provides the required light-weightiness and high security. Particularly, note that the encryption/decryption operations are based only on simple mod 2 additions and table look-up operations which directly imply low complexity (as well as the related overheads) implementation, processing and power-consumption. In order to illustrate its simplicity, the considered encryption is preliminary compared with AES. Quantitative consideration of the complexities as well as an in-details comparison of the proposed approach with the traditional ones is highly dependable on the particular instantiations of implementation constraints, and so is out of the scope of this paper. Accordingly, the paper yields a construction and application framework which is a proposal for an alternative encryption approach which contributes to reduction of the security overheads in certain application scenarios. This proposal could be considered as a background for the planed experimental implementation and analysis.

Acknowledgment

Parts of this work were supported by NSF grant ECCF-0129081.

The authors thank to the anonymous reviewers for their comments and suggestions resulting in an improved presentation of the addressed issues.

References

[1] B. Applebaum, D. Cash, C. Peikert and A. Sahai, ”Fast Cryptographic Primitives and Circular-Secure Encryption Based on Hard Learning Problems”, CRYPTO 2009, *Lecture Notes in Computer Science*, vol. 5677, pp. 595-618, Aug. 2009.

[2] J. Anatory, N. Theethayi, R. Thottappillil, M. M. Kissaka, and N. H. Mvungi, ”Broadband Power-Line Communications: The Channel Capacity Analysis,” *IEEE Transactions on Power Delivery*, vol. 23, no. 1, pp. 164-170, Jan. 2008.

[3] E.R. Berlekamp, R.J. McEliece, and H.C.A. van Tilborg, “On the Inherent Intractability of Certain Coding Problems”, *IEEE Trans. Info. Theory*, vol. 24, pp. 384-386, 1978.

[4] T.W. Cusick and P. Stanica, *Cryptographic Boolean Functions and Applications*. Academic Press (Elsevier), San Diaego, USA, 2009.

[5] M.M. Fouda, Z.M. Fadlullah, N. Kato, Rongxing Lu and Xuemin Shen, ”A Lightweight Message Authentication Scheme for Smart Grid Communications”, *IEEE Transactions on Smart Grid*, vol. 2, pp. 675-685, dec. 2011.

[6] ”Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements”, NIST TR 7628, August 2010.

[7] M. Katayama, T. Yamazato, and H. Okada, ”A Mathematical Model of Noise in Narrowband Power Line Communication Systems,” *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 7, pp. 1267-1276, Jul 2006.

[8] Y.S. Khiabani, S. Wei, J. Yuan, and J. Wang, ”Enhancement of Secrecy of Block Ciphered Systems by Deliberate Noise”, *IEEE Transactions on Information Forensics and Security*, vol. 7, pp. 1604-1613, Oct 2012.

[9] E. Kiltz, K. Pietrzak, D. Cash, A. Jain, and D. Venturi, ”Efficient Authentication from Hard Learning Problems”, EUROCRYPT 2011, *Lecture Notes in Computer Science*, vol. 6632, pp. 7-26, 2011.

[10] J. Massey, “Some Applications of Source Coding in Cryptography”, *European Transactions on Telecommunications*, vol. 5, pp. 421-429, July-August 1994.

[11] M.J. Mihaljevic and H. Imai, ”An approach for stream ciphers design based on joint computing over random and secret data,” *Computing*, vol. 85, pp. 153-168, June 2009.

[12] M.J. Mihaljevi´, H. Imai, M. David, K. Kobara and H. Watanabe, ”On Advanced Cryptographic Techniques for Information Security of Smart Grid AMI”, *CSIIRW 2011*, Oak Ridge National Laboratory, Tennessee, USA, 11-14 Oct. 2011, Proceedings, ACM International Conferences Series, Article no. 64, 4 pages, March 2012.

[13] M.J. Mihaljević, S. Gangopadhyay, G. Paul and H. Imai, “State Recovery of Grain-v1 Employing Normality Order of the Filter Function”, *IET Information Security*, vol. 6, no. 2, pp. 55-64, June 2012

[14] M.J. Mihaljević, S. Gangopadhyay, G. Paul and H. Imai, “Internal State Recovery of Keystream Generator LILI-128 Based on a Novel Weakness of the Employed Boolean Function”, *Information Processing Letters*, vol. 112, no. 21, pp. 805-810, November 2012.

[15] M.J. Mihaljević, ”An Approach for Light-Weight Encryption Employing Dedicated Coding”, *IEEE GLOBECOM 2012, CISS*, Anaheim CA, USA, 03-07 Dec. 2012, Proceedings, pp. 892-898.

[16] M. Qiu, H. Su, Z. Ming and T. Yang, ”Balance of Security Strength and Energy for a PMU Monitoring System in Smart Grid”, *IEEE Communications Magazine*, pp. 142-149, May 2012.

[17] D.A. Spielman, ”Linear-time encodable and decodable error-correcting codes”. *IEEE Trans. Information Theory*, vol. 42, No 6, pp. 1723-1732, 1996.

[18] A.D. Wyner, “The wire-tap channel”, *Bell Systems Technical Journal*, vol. 54, pp. 1355-1387, Oct. 1975.