Why does the grid needs cryptography?

V. B. Litovski, P. M. Petković

Abstract—**New developments and the future of electrical energy production and distribution system are investigated first. Use of alternative energy resources, synergy with the existing large energy generation facilities, control of the distribution, integrated billing and control, information distribution via the grid and many others are the facts that are to be considered while conceiving the system in future. It comes that electronics and ICT will play a major role in control, billing and communication. Information is expected to flow at any level of distribution and control. That already gives opportunities for misuses such as tampering and eavesdropping at the power lines used for communication imposes the need of secure communication. We will, therefore, explain how and why cryptography is intended to be used within the TR 1107 project (financed by the Serbian Ministry of Science) in order to prevent attacks on the information distributed via the grid. We also discuss the physical implementation of the cryptographic infrastructure with special attention paid to the so-called side channel attacks (SCA).**

Index Terms—**Electricity, control, grid, microgrid, tampering, eavesdropping, cryptography, side channel attack.**

I. Introduction

MODERN society critically depends on a secure supply of high-quality electrical energy [1].

According to an International Energy Agency estimate, global investments required in the energy sector over period 2003-2030 are about USD 16 trillion. Future electricity grids have to adapt to changes in technology while matching societal values for environment and commerce. Technologies should also demonstrate reliability, sustainability, and cost effectiveness.

At the distribution level, the new requirements call for the development of:

- distribution grids accessible to distributed generation (DG) and renewable energy sources (RESs), either self-dispatched or dispatched by local distribution system operators,
- distribution grids enabling local energy demand management interacting with the users through smart metering systems, and
- distribution grids that benefit transmission dynamic control techniques and overall level of power security, quality, reliability, and availability.

Putting all together, distribution grids are being transformed from passive to active networks in the sense that decision-making and control is distributed and the power flows bi-directionally. The function of the active distribution network is to efficiently link power sources with customer demands, allowing both to decide how best to operate in real time. Power flow assessment, voltage control, and protection require cost-competitive technologies and new communication systems with information and communication technologies

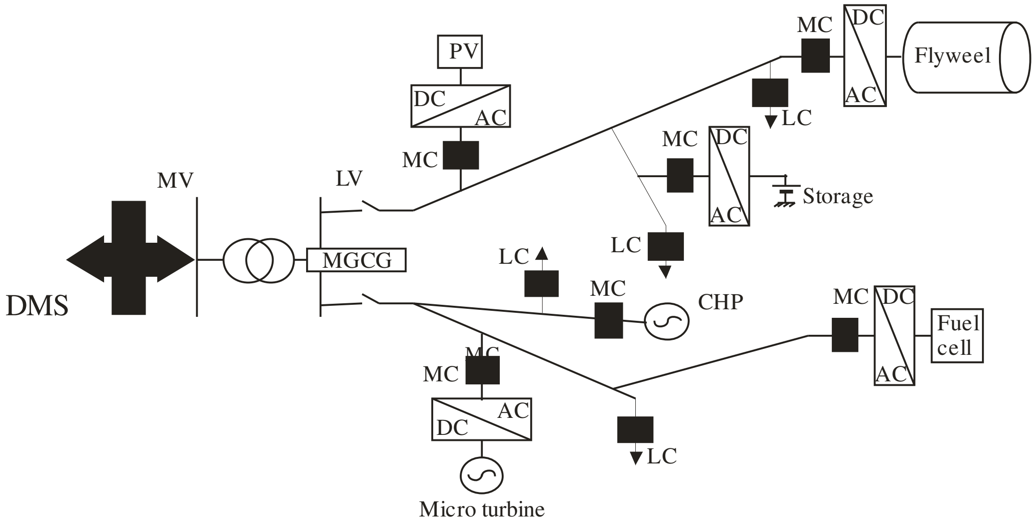

Fig. 1. Typical microgrid structure coordinated by the *microgrid central controller* (MGCC) and interfaced to the *distribution management system* (DMS) [MV = medium voltage, LV = low voltage, MC = medium current, PV = photo voltaic, LC = low current, CHP = combined heat and power] [1].

V. B. Litovski is with the Laboratory for Electronic Design Automation, University of Niš, Serbia (e-mail: vanco.litovski@elfak.ni.ac.yu).

M. P. Petković is with the Laboratory for Electronic Design Automation, University of Niš, Serbia.

(ICTs) playing a key role.

Probably the most promising novel network structure is the microgrid paradigm. Microgrids comprise low voltage (LV) distribution system with distributed energy resources (DERs) as shown in Fig. 1, offering considerable control capabilities over the network operation. These systems are interconnected to medium voltage (MV) distribution network, but they can also operate isolated from the main grid in case of faults in the upstream network.

To demonstrate the importance of the communication part of the microgrid-to-utility grid interconnection one may analyze Fig. 2 [2] where a schematic diagram of the interconnection switch based on circuit breaker is shown. Information is distributed both inner to the microgrid, and upstream to the utility network. Real time monitoring and inter-utility information sharing is handled. In that way control (voltage, frequency, power factor etc.) is enabled while, in parallel, the billing system and communication is made possible.

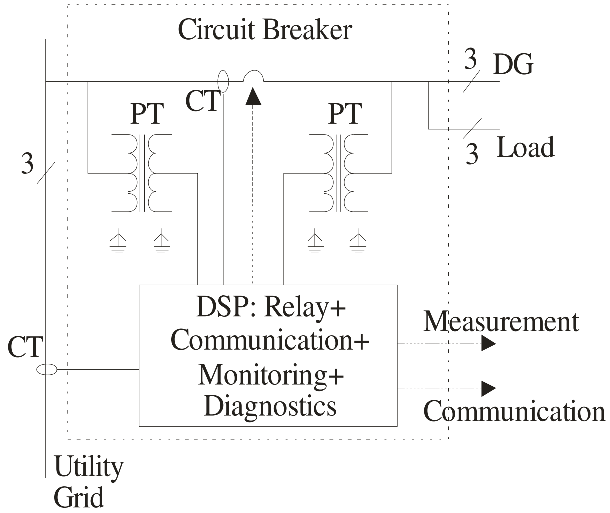

Fig. 2. A circuit breaker based interconnection switch.

Fig. 3 emphasizes another view to importance of the ICTs for the future of the distribution system [3]. On one side it represents a bit futuristic view of a “household” where all loads and the advanced metering device are informatically interconnected to a dashboard that is controlled by the customer. It is supposed the customer will be capacitated to control the use of the resources that were made available to him based on information (measurement, billing, and pricing data) gathered at the dashboard. In the same time all customers are informatically interconnected to the “Meter Data Management Agency” and indirectly to the “Independent System Operator”. This is to anticipate a steady progression toward a Participatory Network.

An “advanced meter” (a collection of which is known as an Advanced Meter Infrastructure, or AMI) is an electronic meter that can be read and controlled remotely. In Fig. 3. we show how an AMI network could be organized in the future [3]. The network is divided into three main domains that are connected via Field-Area-Network (FAN) and potentially Wide-Area-Network (WAN) links.

Meters today already provide many potential advantages to ESPs, their customers, and many other entities:

1) *Customer control*: Customers gain access to information on their current energy usage and real-time electricity prices.
2) *Demand response*: Power utilities can more effectively send control signals to advanced metering systems to curtail customer loads, either directly or in cooperation with the customer’s building automation system. Current demand response schemes are typically very coarse-grained and provide marginal power savings.
3) *Improved reliability*: More agile demand response and DER management can improve the reliability of the distribution grid by preventing line congestion and generation overloads. These improvements will also reduce the strain on the transmission grid.
4) *Simplified sub-metering*: a single meter can monitor multiple customers, reducing equipment costs and maintenance burdens.

There are several distinct categories of advanced metering systems that support the functionality discussed above with varying degrees of success. The least capable systems use low-bandwidth, time-multiplexed radio networks, which preclude any advanced functionality beyond simply reading the meters due to bandwidth limitations. More capable systems use mesh networks to provide more consistent and perhaps higher-bandwidth connectivity, and the most capable systems have full broadband network connections. The less capable systems are typically less expensive to deploy initially, but high-bandwidth systems support more advanced services, possibly providing more economic benefits in the long run.

This was all to enable the envisagement of the complexity of the information infrastructure needed for the establishment of the future distribution system. There is an international push toward a more advanced infrastructure for the metering of electrical usage [4]. This is driven by applications like demand response, distributed energy resources, outage management, prepayment schemes, and improved theft detection as well as a desire to eliminate the expense of manually reading the meters in the field. AMI aims to accomplish this with computer-controlled meters linked by digital networks [5, 6].

In the next threats to the AMI system conceived above will be considered first. Then, a view of an ICT infrastructure will be analyzed in order to come to the right physical position of the conceived cryptographic chip planned to be developed at the LEDA laboratory. Design requirements will be discussed in order to get the right functionality and SCA resistance. In the appendix we are presenting a simplified version of the public key cryptography procedure in order to give some basic insight in the technology.

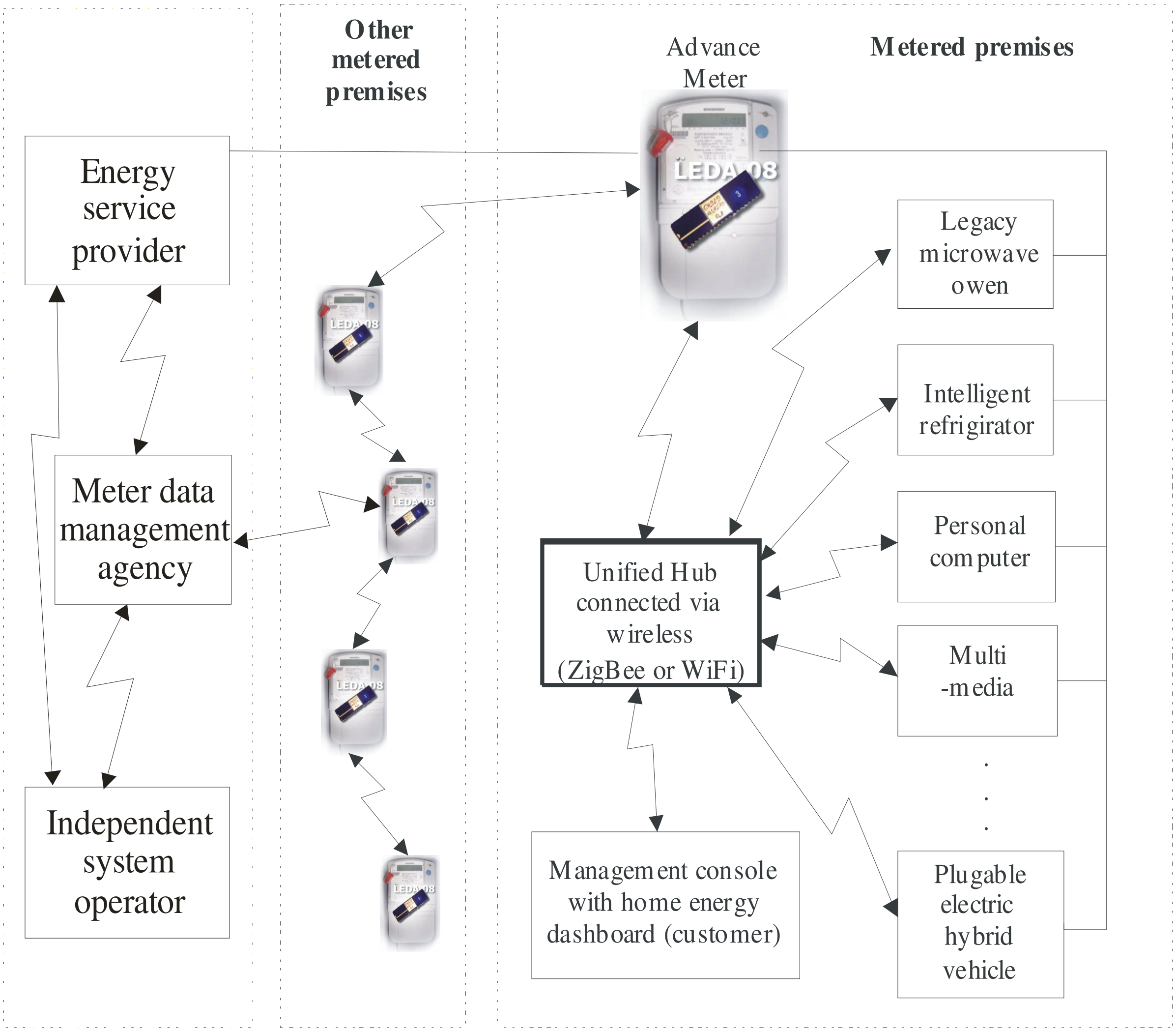
Other metered premises
Advance Meter
Metered premises
Energy service provider
Meter data management agency
Independent system operator
LEDA 08
Legacy microwave owen
Intelligent refrigirator
Personal computer
Multi -media
Unified Hub connected via wireless (ZigBee or WiFi)
Management console with home energy dashboard (customer)
Plugable electric hybrid vehicle

Fig. 3. The distribution network and the smart metering system seen as an ICT challenge for the future.

II. Cryptography Within the Grid and its Implementation in Power Metering Device

Just as cellphones have become ubiquitous, mobile computing platforms, advanced meters may become the first ubiquitous, fixed (non-mobile) computing platforms. This could have a number of positive outcomes, such as the expansion of network access into currently unreachable areas. However, it also raises serious privacy concerns. The introduction of cellphones compromised the location privacy of customers, since the radio signals of cellphones can be tracked to determine the approximate locations of cellphone users. Similarly, advanced meters can potentially be used to determine not only whether a metered premise is occupied, but also how the occupants of the premise are currently behaving. This information could be correlated with location information to develop detailed profiles of those individuals, unless we control the dissemination of such information.

Another significant characteristic of advanced meters follows directly from the previous one. Massive meter deployments may lead to significant availability issues. If many meters attempt to transmit large quantities of data simultaneously, they may overload their communications infrastructure. This could interrupt service providers' income, if they are unable to collect billing data for significant periods of time. It could also lead to blackouts if load reduction signals are blocked or delayed.

While AMI could bring significant benefits, it is potentially subject to security violations such as tampering with the software in the meters, eavesdropping on its communication links, or abusing the copious amount of private data the new meters are able to collect. With anticipated deployments of millions of advanced meters, high costs for replacing meters, and greater dependence on AMI for the stability and financial integrity of the power grid, these threats must be taken seriously. In addition to securing market sensitive data from competitors, information systems for the power grid need to defend against malicious attacks that intend to harm the power grid as a whole. The more comprehensive an information system becomes, the greater the consequences of a successful attack and thus the need for security measures increases. In light of the last decade's developments in the world and the "war on terror" the need for securing the power grid against

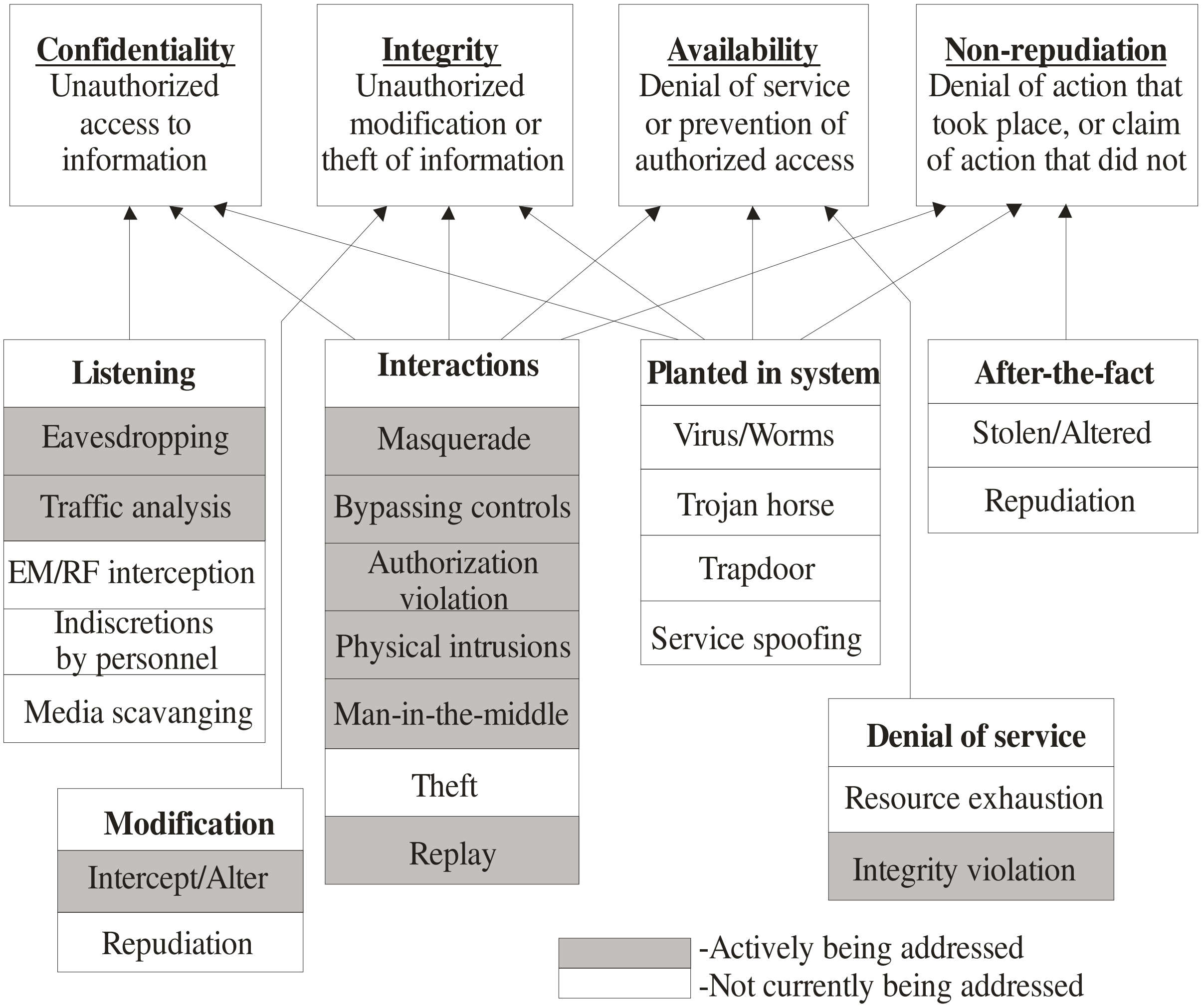

Fig. 4. Attacks defined by IEC TC57 WG15.

such attacks have been all around recognized [7].

A. *The expected solution*

In order to make a security system self-sufficient it needs to secure its own communication completely. Nothing is gained by adding security measures for the data plane while introducing new security weaknesses in the management plane, for example. Any security system needs to protect its own management communication by providing confidentiality, integrity and authentication in the same way as it provides it for the payload data.

We can divide the security problem into two main levels: the communication and the end-point security. After giving a short view to the security problem at the communication level we will properly address the end-point level and give some basic information on the design requirements of a cryptographic chip.

In the late 1990's the the International Electrotechnical Commission (IEC) Technical Council (TC) 57 Power Systems Management and Associated Information Exchange, which is responsible for developing international standards for power grid information systems, created a working group called WG15 to explore the security aspects of their protocols. WG15 is an IEC TC57 working group with the title Power system control and associated communications - Data and communication security. Since its creation in 1997 it has tried to develop security mechanisms for the power grid information system. It has defined four main types of desired security properties:

- confidentiality,
- integrity,
- availability and
- non-repudiation

and explored how to provide safeguards against them. Fig. 4. depicts the types of attacks the group envisions and which types of attacks they actively try to address.

A standard named X.509 is being developed by the Public-Key Infrastructure working group (PK-IX) and was first proposed in 1988. It has gone through two major updates since then, one in 1993 and one in 2000 [8]. X.509 specifies standards for formats, certificates, certificate validation and a hierarchical composition of certificate authorities (CAs).

Certificates combine public keys with digital signatures and something that identifies them, e.g. an IP address. These certificates are sent from the server side to the client side (called an end-node in X.509 terminology) of a connection so that the clients can authenticate the server by ascertaining that the signatures of the certificates are valid. Fig. 5 illustrates how public key cryptography can be used to accomplish this. If the signature is valid the client can conclude that the public key it received is the correct key for the server with the specified name and thus assume that the server is the only one that can decrypt messages encrypted with the public key.

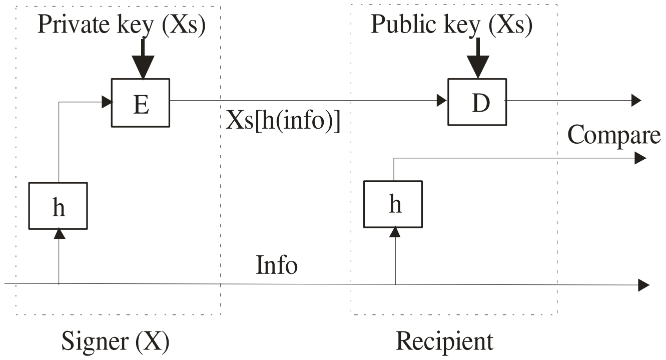

Fig. 5. Certificate signature validation (X.509).

There are two ways to sign a certificate, either it can be self-signed which means that the server signs his own certificate with its own key before sending it to the client. Self-signed certificates achieve little security when sent over-the-wire. The only thing a client can conclude from such a certificate is that whoever sent the certificate possesses the private key it was signed with. For self-signed certificates to provide any security they have to be loaded out of band from a trusted source [8].

The alternative way is to use trusted third parties CAs, to sign the certificate. By signing a certificate the CA endorses the server and says: If you trust me, you can trust that he is who he says he is. This assumes that the client already got the CA's public key installed and can use it to validate its signature.

A certificate may be revoked if it is discovered that its related private key has been compromised, or if the relationship (between an entity and a public key) embedded in the certificate is discovered to be incorrect or has changed. X.509 does this by checking if a certificate is valid through the use of a certificate revocation list (CRL) whose address is specified in the certificate.

A X.509 certificate roughly contains the following information:

- The public key being signed.
- A name, which can refer to a person, a computer or an organization.
- A validity period.
- Certificate Authority identification.
- The location (URL) of a revocation center.
- Name of the algorithm to use.
- The digital signature of the certificate produced by the CA's private key.

X.509 also defines an optional entity, called Registration Authority (RA), that complements the CAs by taking care of personal authentication, token distribution, revocation reporting, name assignment, key generation and archival of key pairs.

Public key infrastructures is build on public key cryptography, but only use it to achieve trust and to agree upon a faster and less resource greedy symmetrical session key for the real data transference. In this way the performance hit of using asymmetric algorithms can be partially mitigated.

Based on these and many other considerations systems are under developments that are to function as telecommunication system acting as an overlay over the grid [3,9]. It is our goal in the rest of this paragraph to define the basic functions and the proper location of the cryptographic integrated circuit that

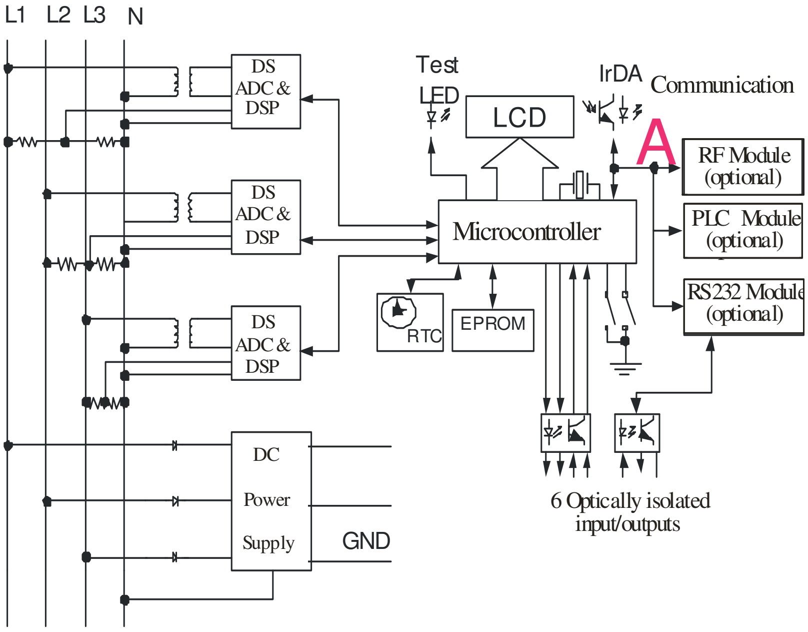

Fig. 6. Architecture of the advanced metering device produced by ATLAS Electronics.

would act as one of the actors in such a communication system at its end-points.

B. A cryptographic chip and its implementation

The cryptographic algorithms may be implemented both in software and hardware. Software solutions are cheaper and more flexible, while hardware implementations provide more speed and intrinsic security. In general, trade-off in cost and speed can be achieved by hardware software codesign.

A smart meter, however, is an example of a platform where the core port, i.e. the most computationally intensive part, is hardware-based, the hardware being custom designed. Accordingly, from now on we will consider the hardware implementation only.

When implementing public key cryptography the primary requirements are high speed arithmetic computation, small size and low power consumption, and resistance to SCAs. There are many sources in the literature describing hardware implementatons of the AES and RSA algorith.

In [10], for example, an optimized coding for the implementation of Rijndael (AES) algorithm for 128 bytes has been developed. The speed factor of the algorithm implementation has been targeted and a software code in VHDL that boasts of a throughput of 2.18 Gb/sec has been developed. The architectural innovations that have been incorporated in the coding include on the fly round key generation, which facilitates simultaneous execution of sub bytes, shift rows and mix columns and round key generation. A look up table called S-Box has been used to obtain the sub byte values instead of applying affine transformation every time to calculate sub byte values. This implementation was intended to be used in wireless security like military communication and mobile telephony where there is a greater emphasis on the speed of communication.

In [11,12] a review of techniques for implementation of the modular exponentiation operation in hardware is given. Techniques for exponentiation, modular multiplication, modular addition, and addition operations are discussed. In [13] an efficient way to build fast modular operation has been explored, using redundant digit sets with higher radices and making modifications to Montgomery's Algorithm in order to achieve deep pipelining at architecture level which improves the throughput and latency of the system. Alternative solutions were offered in [14].

On the other hand, the security of the implementation also needs to be considered. Namely, attacks on cryptographic algorithms are usually divided into mathematical (theoretical) and implementational (practical) attacks. The later are based on weaknesses in the implementation and can be passive and active [15]. The passive attacks are also called SCAs as they benefit from the side channel information that is achieved by measuring some physical quantity. The active attacks are more invasive as they are based on the introduction of faults that results in erroneous calculations leading to exposure of the secret key.

Serious research is under way searching for methods hardening the designs against SCAs [16]. We intend to publish a separate overview of that subject. One should note, however, that information systems for the power grid have life expectancies of 25 years or more, and thus cause another serious technical challenge for this problem space. No one knows how much the computational power available to attackers will increase over such a long period of time, not to mention possible breakthroughs in ways to crack specific algorithms. This makes it very hard to design a static security system that with reasonable certainty can be trusted until the communication system someday is replaced.

III. Conclusion

A view to the future electricity distribution system and communications related to it were considered. Cryptography was advised as a must for protection of these systems against malicious users. Joining the efforts for best solution in the hardware implementation of cryptography for power metering devices, LEDA starts the design of a new chip to be placed in an existing power meter produced by ATLAS Electronics as shown in Fig. 6. The place wher the cryptographic chip is to be placed is marked by the letter A.

Appendix: Basics of Public Key Cryptography

It is already widely accepted that the success of the Information age depends on the ability to protect information as it flows around the world, and this relies on the power of cryptography. Encryption can be seen as providing the locks and the keys of the Information age [17]. The development of public key cryptography (PKC), particularly the RSA cipher [18] has given today's cryptographers a clear advantage in their continual power struggle against cryptanalysts. We intend to use PKC in our implementation and this is why we will here address the cryptography and the key exchange in some details.

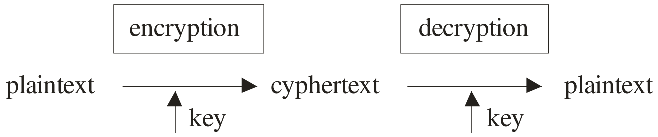

Fig. 7. Basic flow of information within cryptography.

Until modern times, cryptography referred almost exclusively to encryption, the process of converting ordinary information (plaintext) into unintelligible gibberish (ie, ciphertext). (Fig. 7) Decryption is the reverse, moving from unintelligible ciphertext to plaintext. A cipher (or cypher) is a pair of algorithms which perform this encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and, in each instance, by a key. This is a secret parameter (ideally, known only to the communicants) for a specific message exchange context. Keys are important, as ciphers without variable keys are trivially breakable and therefore less than useful for most purposes. Historically, ciphers were often used directly for encryption or decryption, without additional procedures such as authentication or integrity checks. If the same key is used for both encryption and decryption one speaks on symmetric keys.

In modern computer encryption and decryption procedures standardization was introduced meanning the complete procedure of encypherment was standardized leaving the key to be known to the communicating part as the only protection against eavesdropers. A standard that was mostly used is DES (Data encryption Standard) and his later version AES (Advanced decryption standard) introduced in the early seventies but still in use. It imposes, however, the problem of key distribution having in mind that many messages may be intended to be delivered to recipients all over the world. The problem was solved by using assymetric key pairs, a public and a privat key, in a procedure that is known as RSA, the name comming from the first laters of the family names of the authors.

While the symmetric key encription is performed by some algorithm of distorting the plaintext that produces different results wehen different keys are used, the RSA uses more complicated procedure enabling generation of cyphertext that is controlled by one side of the communication channel only. Becose of the importance of the subjec we will try here to express the essence of the procedure.

Since we use computer interpretaion of the text we may express the whole idea by numbers. Suppose the secret message to be transmitted is M. Two numbers are published by the receipient: e and N. N is suposed to be a very large number obtained by multiplication of two prime numbers: p and q, i.e. $N=p\cdot q$. p and q are kept secret by the receipient. e is referred to as the public key exponent. It is reqired e to be coprime with $\varphi=(p-1)\cdot(q-1)$ meanning that they share no factors other than 1. Now, the sender is creating the cyphertext i.e. he or she is calculating

$$C = M^{e}\big|_{\mathrm{mod}\ N} \tag{1}$$

For instance, if p=11, q=13, we get N=143 and φ=120. p, q, and φ are not known to the sender. For M=7, if e=7 one gets C=6. C is transmitted to the receipient. Note the importance of the modulo function. It is an one-way function that needs incomparably much more time to be inverted then to be calculated. For a very large N the problem of inversion is not tractable in a conceivable time.

Now the recipient performs the following calculations. First, one has to solve the equation

$$e \cdot d\big|_{\mathrm{mod}\ \varphi} = 1 \tag{2}$$

for d. In our example that is d=103. In general case this equation is solved by the so called Euclid’s algorithm hence the complexity and time needed for performing the calculations. Finally, to decript the message one has to compute

$$\hat{M} = C^{d}\big|_{\mathrm{mod}\ N} \tag{3}$$

which is the secret message: $M=(6^{103}\ \mathrm{mod}\ 143)=7$.

In case of a long message one brakes the original binary code into blocks, say 128 bit or more, and implements the above procedure to the blocks separately.

Instead of exponential the so called eliptic functions are used nowadays with much success.

It is conceivable now that the role of the recepient is the utilty company’s computer that randomly produces public keys (e and N) using a very large pool of previously stored very large prime numbers (p and q). The public key is expected to be communicated to the metering device that will encript the information to be sent back.

If the private key is used to encrypt the message, every node with the public key can decrypt it, which means the message is not confidential, but since only the private key could have encrypted the message in the first place, the origin of the message can be authenticated. This is often called electronic signatures.

REFERENCES

[1] Hatziargiriou, N., “Microgrids, the key to unlock distributed energy resources”, IEEE Power and Energy Magazine, Vol. 6, No. 3, May/June 2008, pp. 26-29.

[2] Kroposki, B., et all., “Making microgrids work”, IEEE Power and Energy Magazine, Vol. 6, No. 3, May/June 2008, pp. 41-53.

[3] http://seclab.uiuc.edu/web/critical-infrastructur e/attested-metering.html

[4] Valocchi, M., Schurr, A., Juliano, J. and Nelson, E. “Plugging in the consumer, Innovating utility business models for the future”, IBM Institute for Business Value, Somers, NY 10589, U.S.A., 2007. http://www-935.ibm.com/ services/us/gbs/bus/pdf/ibv_g510-7872-00_ plugging_in.pdf

[5] Jovanović, B., et all., “A new testing setup for integrated power meter”, Proc. of the LI conf. of ETRAN, Herceg Novi, June 2007, Proc. on CD, EL2.5, R65.

[6] -, “IMPEG - An Integrated Power Meter IC”, http://leda.elfak.ni.ac.yu

[7] Cleveland, F., “IEC TC57 security standards for the power systems information infrastructure beyond simple encryption”. June 2007. IEC TC57 WG15 Security Standards White Paper ver. 11. http://xanthus-consulting.com/pages/publications.htm

[8] ITU Telecommunication Standardization Sector (ITI-T). ITU-T Recommendation X.509, July 2005, URL:http://www.itu.int/ rec/T-REC-X.509-200508-I/en

[9] Solum, E., “Achieving over-the-wire configurable confidentiality, integrity, authentication and availability in gridstat’s status dissemination”, M.S. Thesis, Washington State University, December 2007.

[10] Umamaheswari, G., and Shanmugam, A.,” Efficient VLSI implementation of the block cipher Rijndael algorithm”, Academic Open Internet Journal, Volume 12, 2004, http://www.acadjournal.com/2004/V12/Part5/p1/

[11] Kaya Koç, Ç., “RSA Hardware Implementation”, RSA Data Security, Inc., Version 1.0, August 1995, http://security.ece.orst.edu/ koc/ ece575/rsalabs/tr-801.ps

[12] Kaya Koç, Ç.,, “High-Speed RSA Implementation”. Technical Report TR 201, RSA Laboratories, November 1994. ftp://ftp.rsasecurity.com/pub/pdfs/tr201.pdf

[13] Shantilal, A. C., “A Faster Hardware Implementation of RSA Algorithm”, Oregon State University, Corvallis, Oregon 97331 -USA, http://islab.oregonstate.edu/koc/ece679/project/ 2002/ajay.pdf

[14] Ziya Alkar, A., and Sönmez, R., “A hardware version of the RSA using the Montgomery's algorithm with systolic arrays”, Integration, the VLSI Journal, Vol. 38, No. 2, Dec. 2004, pp. 299-307.

[15] Batina, L., et all., “Side channel attacks and fault attacks on cryptographic algorithms”, Revue HF Tijdschrift, No. 4, 2004, pp. 36-45.

[16] Tiri, K., and Verbauwhede, I., "A VLSI design flow for secure side-channel attack resistant ICs," Proc. Design Automation and Test Conf. in Europe (DATE 2005), pp. 58-63, March 2005.

[17] Singh, S., “The code book”, Fourth Estate (HarperColins Publishers), London, 1999.

[18] Konheim, A. G., “Computer security and cryptography”, Wiley, Hoboken, N.J., 2007.