Life-logging in Smart Environments: Challenges and Security Threats

Nikolaos E. Petroulakis*, Ioannis G. Askoxylakis*, Theo Tryfonas†
*Institute of Computer Science, Foundation for Research and Technology-Hellas, Greece
†Faculty of Engineering, University of Bristol, UK
{npetro,asko}@ics.forth.gr, theo.tryfonas@bristol.ac.uk

***Abstract*—As the world becomes an interconnected network in which objects and humans interact, new challenges and threats appear. In this interconnected world, smart objects seam to have an important role in giving users the chance for life-logging in smart environments. However, the limitation of smart devices with regard to memory, resources and computation power, hinder the opportunity to apply well-established security algorithms and techniques for secure life-logging on the Internet of Things domain. As the need for secure and trustworthy life-logging in smart environments is vital, a lightweight approach has to be considered to overcome the constraints of smart objects. The purpose of this paper is to detail current topics of life-logging in smart environments while describing interconnection issues, security threats and suggesting a lightweight framework for ensuring security, privacy and trustworthy life-logging.**

***Index Terms*—Smart Objects, Smart Environments, Internet of Things, Life-logging, Security.**

I. Introduction

In an interconnected smart world the interaction between humans and devices has resulted in the creation of a smart environment in which the exchange of data and decisions is continuous. The Internet has given us the opportunity to enhance aspects of its network such as computers, smart devices, smart phones, people, families and communities. A digital ecosystem has been developed consisting of two layers in which the first layer is the reality involving communication between people, daily duties or entertainment and the second layer is the virtual life in which human and objects are connected to a local network or the Internet in which communication is done throughout different collaborating technologies offering seamless connectivity.

The term *smart object* has been assigned to small ubiquitous devices, such as sensors, actuators, RFID tags, smart phones and embedded systems, with limited capabilities but able to connect to a wireless or wired network with and without IP. These devices have many constraints compared to high-powered smart phones or computers because of their narrow capabilities in resources. One of the greatest challenges for future networks is the ability for smart objects to get connected to a local network or the Internet under the *Internet of Things* (IoT) domain. The idea is transparent but faces many unsolved issues owing to the different technologies of smart objects which try to interact with well-established technologies. In the IoT, users have the potentiality of connecting their life with objects physically or virtually, giving them the chance to use, monitor and manage smart devices and communicate with other people or objects. The act of recording information or personal data and its interaction or exchange with others throughout the network introduces the term of *life-logging*. The life-logging procedure in smart environment involves either the acquirement of personal activities from devices or their execution into a virtual space such as a social network.

All given benefits of life-logging in smart environments confront new challenges, with security as one of the most critical. There are several security issues of life-logging in an interconnected smart world due to the lack of capable security standards of smart objects. Just as real-life networks encounter challenges in security, privacy and trust the same can occur in a virtual network. Security risks arise because of the lack of suitable security protocols in lossy smart devices and in the IoT. Smart objects have many security vulnerabilities caused by their limited resources for supporting well-established cryptography and security algorithms. In an insufficient security environment new lightweight approaches should be considered in order to overcome the lack of trust and privacy, thereby avoiding security dangers.

The remainder of this paper is organized as follows. In Section II we present the factors of life-logging in a smart environment in which life-logging is applied to different technologies of smart objects to the IoT. In Section III we discuss the security challenges and vulnerabilities of life-logging in a smart environment. In Section IV we suggest a lightweight framework consisting of the most important pillars to overcome the described security challenges. We conclude this paper in Section V.

II. Life-logging in a smart environment

In a modern ecosystem devices, building, places and people have the potential to create a smart environment in which internal and external interfaces with different technologies are used. The importance of smart infrastructure in the context of smart cities has attracted several companies to develop initiatives such as the IBM's vision of Smart Planet [1] and the Smart+Connected Communities from Cisco [2]. The structure of smart environments consists of three basic ingredients: the first ingredient involves smart objects which interact with the environment, the second component comprises of the interconnection of smart objects with the network; either the Internet of the IoT, and thirdly the procedure of life-logging

978-1-4577-2053-6/12/$31.00 ©2012 IEEE

in this interconnected smart environment. The structure of the described smart ecosystem is depicted in Figure 1, consisting of a network infrastructure layer, an object ecosystem layer and an overlay layer.

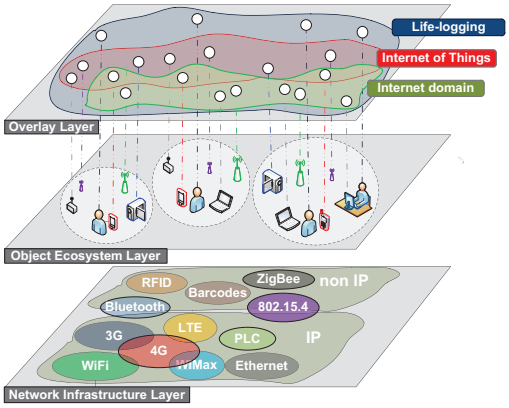

Fig. 1: A life-logging smart ecosystem

A. Smart objects

First of all, what exactly is a *smart object*? Introduced for the first time by Neil Gershefelds in his article *When Things Start to Think* [3], their primary characteristics have been described as their unique identity and their capability of communicating with other objects and detecting the nature of the environment. Usually, they are communication devices with small micro-electronic components, low power radio, limited energy resources, and a tiny microprocessor. Smart devices encompass innovations such as intelligent tags (RFID), sensors that measure physical quantities and convert them into analog or digital signals (temperature, pollution, motions), actuators that control equipment and embedded devices that perform specific functions [4]. Furthermore, smart objects can be combined with mobile devices such as laptops, PDAs, mobile phones or smartphones, as well as Bluetooth devices. In the Future Internet different wireless technologies (WiFi, 3G/4G, 802.15.4, RFID etc) or wired ones (ethernet, PLC) might interact and create a machine to machine ecosystem.

There are two basic categories: the IP-based and the non IP-based objects. The IP based objects are able to connect to the Internet by running operating systems, only having requirements regarding energy and memory for supporting the TCP/IP protocol. Sensors have natural limitations such as limited energy resources, low memory and processing capability, which make them difficult to provide full IP protocol stack support. For that reason, suitable OS have been developed for tiny embedded systems and sensors with limited requirements such as Contiki, TinyOS and FreeRTOS [5]. For the connectivity and communication of non-IP objects, protocols, such as ZigBee [6], have been developed for short-range low-power and low bit-rate radios and sensors. Non IP-based devices such as RFID tags can be passive, which do not incorporate a power supply, because the electrical power induced by the reader is enough to transmit data, or active, which use their own battery to transmit [7]. The main disadvantage of the non IP-based sensors is the lack of network connectivity without the need of gateways.

B. Interconnecting smart objects with the Internet of Things

It is assumed that the *Internet of Things* (IoT) will be a very important pillar for the Future Networks which has attracted many supporters in the research community and industry. The European Commission has made a deal of great effort to fund project proposals, especially in the 7th Framework Programme, related to the IoT and Future Networks [8]. The term of IoT was coined in 1999 by Kevin Ashton [9] with the vision of interconnecting previously unconnected and isolated objects to the Internet. The IoT gives the potential to incorporate into the network devices with minimal capabilities like smart objects. Moreover, the IoT aims to connect not only things but also networks as well (a network of networks).

As described in [10], the three most important characteristics of IoT are: their ability to instrument ordinary objects with a chip and a communication device, their interconnection capability, and a way to provide intelligent services. One critical challenge for the IoT is to combine heterogeneous IP or non IP-based objects under the same network and enable them into the Internet. The Internet Engineering Task Force (IETF) [11] and the IPSO Alliance [12] with the support of companies such as Cisco, Ericsson, Oracle, Intel, Google and Motorola, aim to standardize IP and more specifically IPv6 for embedded systems in order to homogenize heterogeneous smart objects.

C. Life-logging

The main concept of *life-logging* improves the way people record and exchange of their data, communicate with others and log into applications or devices. Life-logging is not a new idea but it has been applied throughout history. Since ancient times, people used to keep data about their personal activities within a community. Calendars, books, diaries, letters and paintings can be added to the catalogue of life-logging personal data. Over the last century new life-logged info were added to the above list such as photos, sounds and videos. Especially in the 80s, the broad propagation of personal computers gave us the opportunity to keep records and personalize our environment to bring interfaces closer to our personal preferences, accounts and applications. At the end of 90s and the begin of 20th century, especially with the widespread establishment of the Internet, personal data such as email accounts, gaming data, login accounts, favorite web pages, personal documents, digital photo albums, online web services and applications were stored in personal devices. In the 21st century, social networks have attracted a great number of life-logged in users who share similar concerns, ideas, personal moments, photos, achievements, news, and data.

A life-logging experience of interacting with devices is a daily issue for a variety of people. The scenario of [13], in which a runner with a heart rate sensor and a pedometer, records his data and transfer them through his WiFi-connected iPod to a web database in which his friend have access, is not a future scenario but is already reality. The increasing use and need for personal smart devices such as sensors and actuators indoor or outdoor create the need to develop applications in which a user may log and interact with these devices under

the prism of the Internet or into the IoT. Whereas a couple of years ago smart phones were unavailable for many, they now have a widespread penetration into the market with a variety of developed applications with interconnected capabilities in different environments. A very interesting framework platform for Android phones has been developed by Google under the Tungsten Project with the name *Android at Home* [14] in which IoT is applied for allowing individual users to log into their accounts and control their smart objects at home. Google's next challenge is the enhancement of Android at Home in Google Plus where life-logging in social networks will fulfill the intersection with smart objects and the IoT.

III. Security threats in smart environments

Security is assumed to be one of the key elements for smart environments. The need to secure them is vital. Not only is it critical for the connected devices and users but it is also dangerous for the gateways that are connected to them. In addition, applications such as in the army, factories and industries, bridges, medical and health, environmental applications and home environment are some examples when security threats should be taken into consideration. Moreover, the widespread use of smart objects in the home environment endangers disclosing private data. For instance, a wireless installed camera, for recording possible intruders, connected to an insecure home network, could be a susceptible threat to disclose the private actions of a family. The fast growth of life-logging applications and the potential for integrating them into smart environments means security issues need to be addressed. Secure and trustworthy life-logging in smart environments involves challenges, risk and threats in security of smart objects, on the communication layer under the IoT and finally on the end-users who log on and interchange data with their smart objects.

The general concept of CIA triad (confidentiality, integrity and availability) supported by [5] and [15] can be applied successfully for the security of smart environments. *Confidentiality* focuses on keeping information private by encrypting it or ensuring that only the right people will have access to it. *Integrity* confirms that data has not been modified. Integrity is achieved by the use of Message Integrity Codes (MICs) or Message Authentication Codes (MACs). Finally, *availability*, guarantees that information is available when it is needed.

A. Security vulnerabilities and attacks in smart objects and the IoT

Smart objects, particularly sensor networks, are vulnerable by their very nature because of the lack of security support in the primary design of low lossy networks. Their previous status did not face the need to ensure secure transmissions. Information about measurements such as temperature and humidity did not attract attackers to interfere. Nevertheless, the rapid growth of system automation and the massive production of sensors and smart devices and their integration in the environment reveals security deficits and possible threats from malicious users. Additional security add-on feature in an insecure design cannot replace the capabilities of a securely designed network. Moreover, the limited resources in memory, CPU and energy of smart objects make the enhancement of add-on security features even harder. Security on the IoT is challenging due to the existing constraints of smart objects which are mainly focused on their difficulties to adopt well-established security protocols of the Internet. Based on the proposed scheme by [16] and [15] we can categorize security challenges into pillars including security threats on different layers of OSI model [17].

Security and privacy are critical points in sensors and actuators. A malicious node can easily steal transmitted information or impersonate a receiver. Furthermore, privacy seemed to be challenging because of their weakness to realize and sense possible listeners. If nodes have a MIC in the headers and payload, it is not possible to have an impersonation attack but it is possible to have passive listening or cause Denial of Service (DoS) attack. On the other hand, if the payload message is encrypted then it is presumably a malicious node, having the encryption key, to impersonate but not to be a passive listener. The disclose of sensitive information about the location, track and identity of a user is a very serious situation which may occur jeopardy situations for him and for his connected network.

Authentication is a very important issue which is missing in many objects. Trusted Platform Computing (TPM), implemented in laptops, is difficult to be applied because of the lack of suitable cryptographic algorithms developed for lightweight smart devices. Moreover, lack of authentication, encryption or integrity on the interconnected objects creates serious considerations. The Transport Layer Security (TLS) protocol and the Secure Socket Layer (SSL) protocol appear to be efficient cryptographic solutions but they lack because of the limitations of smart objects for supporting them. The low processing mechanisms for data mining and services capable for authenticity, confidentiality and privacy of devices create security issues and threats for reveal of sensitive information to insecure devices and storages.

Low networking capabilities in bandwidth, throughput, data rate along with the minimal computation power for real time aggregations and buffering, which are needed for secure networking, make them fragile to attacks on the network layer. At the MAC layer security issues occur in the MAC protocols in which collisions, occupation of the communication channel cause difficulties to transmit exhausting batteries in parallel. At the physical layer jamming, DoS, traffic analysis, injection and tampering are very critical security threats for smart objects. Especially, the inability for many objects to acquire IP addresses makes them vulnerable to attacks (such as DoS) that in powerful IP hardware devices, running efficient security protocols, are rebutted successfully.

Finally, *topology* in a IoT multi-hop and multi-route domain is completely different what it is in the Internet where service providers route and manage the traffic avoiding malicious attacks securing not only the computers but also the topology, issues which seem to be challenging for the IoT domains. The lack of IP for a number of smart objects occur security issues on the routing protocols in where black holes, spoofing, forwarding and sinkholes are happened.

B. Risks and security issues of life-logging

The trend of life-logging encounters a number of security issues which need to be resolved in order to step forward into the interconnected world and the Future Internet. To highlight the benefits and the risks of life-logging, authors in [18] present a future scenario in which they detail benefits, challenges, risks and threats of life-logging in real life. The scenario occurs in 3-5 years from now when the members of a family live in an integrated smart world in which life and objects have acquired a stable and tailored relationship. Several possible risks and threats are depicted in this scenario involving life-logging in a variety of activities, services and devices. Social networking, as a part of their lifestyle and as a tool for socializing or for work, has substantially enhanced the virtual reality in a cyber space world.

There are several security threats which could spread from life-logging to the Internet, capable of interfering with the life of every life-logger. Authors in [19] address the most common life-logging security and privacy risks, including the surveillance of someone's life, memory hazards which means that mistakes in life can not be forgotten easily; long term availability of personal information will remain even if his life and ideology has changed, and finally the problem of stolen life-log information. Moreover, the danger of a lost password or a stolen one, is believed to be one of the most serious issues for most people. The risks of such an incident could be used to gain access to a person's accounts and create problems in something unimportant, such as logging into his social networking profile or reading his emails, up to entering his bank account and taking his money.

Life-logging from a computer or a laptop on to the Internet differs from life-logging in a smart environment because of the unsolved security threats which occur in the unsafe smart environments. Secure life-logging in smart environments is relatively straightforward compared to the security of smart objects and the IoT. As discussed in previously, there are many vulnerabilities in a heterogeneous ecosystem in which every device faces different challenges in security and privacy. The discrepancy between technologies and the attempt to interconnect them have brought new security challenges and gaps which need to be filled. Life-logging on to insecure environments generates new dangers for the life and the privacy of users in their work environment, their personal life and for their family.

IV. Defining a lightweight framework

The increasing inclination for the addition of life-logging applications into the smart environment and the discussed security threats require suitable countermeasures to offer security, privacy and trustworthy life-logging. The key way to overcome security constraints in smart environments is the development of a lightweight framework for ensuring security, privacy and trustworthy life-logging in smart environments. We describe the basic pillars of this framework including the use of lightweight IP protocols, lightweight privacy by design and the use of lightweight cryptography.

A. Lightweight IP protocols for securing smart objects

Security threats in life-logging under a smart environment and the IoT occur mainly because of the lack of suitable security protocols. Considering smart objects' limited capabilities, proper algorithms and techniques need to be implemented in order to achieve maximum security and privacy. The IPSO Alliance advocates the use of the IP protocol for establishing a secure exchange of data. In order to achieve security in smart objects, the IPv6 over Low power Wireless Personal Area Networks (6lowPAN) protocol is proposed [20]. Smart objects are able to connect throughout the lightweight 6lowPan protocol which gains its advantage from the use of AES-128 link-layer security mechanism of IEEE 802.15.4. However, the IP fragmentation allows the use of available buffer from malicious users to send large or invalid packets. Even if in the transport layer 6lowPAN is shown to have efficiency, in the network layer, Internet Protocol Security (IPsec) and Secure Neighbor Discovery (SEND) appear to be more suitable to attain network security in IPv6 [21]. Authors in [22] suggest a security adaptation layer to overcome security issues when connecting the IoT network to the Internet. The adaptation layer is based on one similar to the 6lowPAN adaptation layer concept or IPv6 in which gateways connected to different domains are able to translate standard IP security protocols to domain-specific protocols variants.

B. Lightweight design for ensuring privacy

Privacy is a major concept of life-logging especially in insecure smart environments in which a variety of data from users and devices are exchanged and collected. The massive production and transfer of sensitive data such as personal photos, messages and videos encounter the danger of disclosure. In order to ensure privacy on smart environments the principles of privacy should be applied in a lightweight privacy by design approach. The basic principles for ensuring privacy in smart environments of life-logging are detailed in [23]. *Openness* is established when recorded data is transparent. *Participation of Individuals* ensures if records are able to be seen by them. *Limits of Recorded Data* have to be assigned for specific applications. Moreover, *Data Quality* of recorded data should be related and accurate to the application. *Limits of Use* have to be used only by authorized users and for an assessed purpose. Furthermore, personal data should be *Secured Appropriately* on storage devices. *Accountability* of record keepers has to be ensured. The last principle which should be emphasized is *Awareness* from the user point of view. Since privacy is not a convenient issue to be resolved, especially in smart environments, the principles of privacy should be implemented under an international framework and standards. Privacy in smart environments and more precisely in the IoT have to apply the concern of Privacy by Design (PbD) defined by Ann Cavoukia [24] who suggested that privacy should be embedded into the design of technologies ensuring privacy and control over one's information and not solely by compliance with regulatory frameworks.

C. Lightweight cryptography for trustworthy life-logging in smart environments

Cryptography is assumed to be the key element for trustworthy transactions in smart environments. The authentication and the authorization between users and devices in the IoT face many challenges because of the limited capabilities of smart environments. One of the most important issues in life-logging is the users' authentication and their devices connected to the IoT. For establishing authentication and authorization in the IoT the use of Lightweight Cryptography (LWC) is crucial. The LWC algorithm and protocol tailors have been designed especially for constrained environments where the resources are limited such as in RFIDs, Sensors, tags, smart cards etc. Based on [25], the proposed lightweight cryptography is supported for two main reasons: for the efficiency of end-to-end communication and for the applicability to lower resource devices. Constraints of low resource devices, such as battery limitations and narrow computation power, require lightweight symmetric key cryptography to decrease power consumption of devices. Moreover, the footprint of LWC primitives is smaller compared to the conventional ones. Even though it is possible for some nodes to store footprints in hardware and run algorithms, it is crucial the low-power and low-cost devices to embed applications instead of hardware circuitry because of the limited resources of smart objects. Symmetric and asymmetric key cryptography can apply lightweight properties for trustworthy life-logging in the IoT.

Symmetric Key Cryptography can be separated into three categories, block ciphers, stream ciphers and hash functions. Block ciphers with lightweight properties have been proposed for Advanced Encryption Standard (AES) and Data Encryption Standard (DES) such as CLEFIA [26] and PRESENT [27]. Stream cipher algorithms with lightweight properties have been proposed and developed in the ECTRYP II eSTREAM portfolio [28]. Hash algorithm SHA-3 [29] do not satisfy lightweight requirements. Lightweight hash functions are possible to construct based on lightweight block ciphers.

Asymmetric Key Cryptography is difficult to implement because the amount of data for public key cryptography in smart objects is much larger than in symmetric key cryptography. Efficient security such as Rivest Shamir Adleman (RSA) and Elliptic Curve Cryptography (ECC) cannot be implemented efficiently in smart objects because of the limitations for storing additional footprints. ECC is more likely to be implemented because of its smaller operand lengths and relatively lower computational requirements [30]. Nevertheless, it is possible to implement public key cryptography in smart environments but it is difficult to execute in reasonable time.

Considering the major need for authentication and authorization for users and devices in smart environments, cryptography will always be a challenge. Well-established or new algorithms may well have to be implemented efficiently in order to overcome the limitations of smart objects with lightweight capabilities. However, as strong as the cryptographic algorithms are, they will never get over the vulnerability of an insecure or inexpert user with a lack of basic security and privacy precautions.

V. Conclusion

In this paper we analyzed the topic of life-logging in smart environments. The potential of smart objects and their interconnection with the Internet of Things has gained great attention in the research community because of the rising interest in Future Networks. The plethora of smart objects and life-logging under this framework has undercovered new issues and security threats. Security challenges appear due to the lack of suitable security mechanisms and protocols in the Internet of Things because of the limited resources of smart objects. To overcome considerations in security, privacy and trustworthy life-logging, a lightweight framework was described.

References

[1] IBM. Smart Planet, http://www.ibm.com/smarterplanet.
[2] Cisco. Smart+connected communities, changing a city, a country, the world, 2010.
[3] N. Gershenfeld. *When Things Start to Think*. Owl Books, 2000.
[4] P. Wetterwald. Promoting the use of IP in networks of Smart Objects. *ETSI M2M Workshop*, 2010.
[5] J.P. Vasseur and A. Dunkels. *Interconnecting Smart Objects with IP: The Next Internet*. Morgan Kaufmann Publishers Inc., 2010.
[6] ZigBee Alliance. www.zigbee.org.
[7] R. Tesoriero, J.A. Gallud, M. Lozano, and V.M.R. Penichet. Using active and passive RFID technology to support indoor location-aware systems. *ICCE*, 2008.
[8] Internet of Things and Future Internet Enterprise Systems, http://cordis.europa.eu/fp7/ict/enet/.
[9] K. Ashton. That 'Internet of Things' Thing. *RFID Journal*, 2009.
[10] H. Ma. Internet of Things : Objectives and Scientific Challenges. *Journal of Computer Science*, 26, 2011.
[11] IETF. The Internet Engineering Task Force, http://www.ietf.org/ .
[12] IPSO Alliance. Enabling the Internet of Things, www.ipso-alliance.org, 2011.
[13] A. Manfred. Security in the Internet of Things. *RFIDsec Asia*, 2010.
[14] P. Wetterwald. Android@home. *Google I/O developer conference*, 2011.
[15] K. Stammberger, M. Semp, M. B. Anand, and D. Culler. Introduction to Security for Smart Object Networks. *IPSO Alliance*, 2010.
[16] C. P Mayer. Security and Privacy Challenges in the Internet of Things. *WowKiVS*, 17, 2009.
[17] IOS/IEO Commission. Information technology - Open Systems Interconnection - Basic Reference Model: The Basic Model. *ISO/IEC*, 1994.
[18] I. Askoxylakis, I. Brown, P. Dickman, M. Friedewald, K. Irion, E. Kosta, M. Langheinrich, P. McCarthy, D. Osimo, S. Papiotis, A. Pasic, M. Petkovic, B. Price, S. Spiekermann, and D. Wright. TO L0G OR NOT TO L0G ? Risks and benefits of emerging life-logging applications. *ENISA*, 2011.
[19] R. Rawassizadeh and A M. Tjoa. Securing Shareable Life-logs. *Social Computing (SocialCom),*, 2010.
[20] J. Hui, D. Culler, and S. Chakrabarti. 6LoWPAN: Incorporating IEEE 802.15.4 into the IP architecture. *IPSO Alliance*, 2009.
[21] C. E. Caicedo, J.B.D. Joshi, and S. R. Tuladhar. IPv6 Security Challenges. *Computer*, 42(2), February 2009.
[22] R. Hummen, T. Heer, and K. Wehrle. A Security Protocol Adaptation Layer for the IP-based Internet of Things. *Interconnecting Smart Objects with the Internet Workshop*, 2011.
[23] P.A. Nixon, W. Wagealla, and C. English. Security, privacy and trust issues in smart environments. *Smart Environments*, 2004.
[24] A. Cavoukian. Privacy by Design: The 7 Foundational Principles. *http://privacybydesign.ca/*, 2011.
[25] M. Katagi and S. Moriai. Lightweight Cryptography for the Internet of Things. *Sony Corporation*, 2008.
[26] T. Shirai, K. Shibutani, and T. Akishita. The 128-Bit Blockcipher CLEFIA. *FSE*, 2007.
[27] A Bogdanov, L Knudsen, G Leander, and C Paar. PRESENT: An ultra-lightweight block cipher. *Systems-CHES*, 2007.
[28] The eSTREAM Project. http://www.ecrypt.eu.org/stream/, 2008.
[29] A. Regenscheid, J. Kelsey, and S. Paul. Status Report on the First Round of the SHA-3 Cryptographic Hash Algorithm Competition. *NIST*, 2009.
[30] T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann, and L. Uhsadel. A Survey of Lightweight-Cryptography Implementations. *IEEE Design & Test of Computers*, 24(6), November 2007.