Side Channel Analysis on Biometric-based Key Generation Algorithms on Resource Constrained Devices

Dimitrios L. Delivasilis and Sokratis K. Katsikas
(Corresponding author: Dimitrios L. Delivasilis)

Department of Information and Communication Systems Engineering, University of the Aegean
Karlovasi, Samos, 83200, Greece (Email: {delivasilis, ska}@aegean.gr)

(Received Aug. 26, 2005; revised and accepted Oct. 1, 2005)

Abstract

Side channel analysis is a technique that enables the adversary to benefit from information leakages occurring due to the implementation of encryption algorithms on hardware. Since its introduction, side channel analysis has been extensively used in cryptology, more precisely in cryptanalysis. In this paper we describe a novel method, according to which side channel analysis is applied to biometric key generation algorithms, operating on resource constrained devices. Instead of aiming to identify the encryption key, and therefore penetrate the cryptographic system, the biometric signature of the user, necessary for the generation of the encryption key, can be accurately extracted. In the following sections we outline our approach for achieving this goal, describe its implications and discuss directions for future work.

Keywords: Biometrics, key generation algorithms, side channel attacks

1 Introduction

Wireless communications constitute an area of digital communications that has evolved rapidly throughout the last decades. With the past and recent proliferation of handheld mobile technologies and devices, vendors have moved aggressively to extend the wired network through mobile gateways, allowing businesses and service providers to operate with confidence. Security in wireless communication is an issue that causes a lot of scepticism. Recent advances utilise the always increasing capabilities of the mobile computing platforms to offer privacy and confidentiality to the end user.

One of these latest developments is the involvement of biometrics on handheld devices. Biometrics identify people by measuring some aspect of individual anatomy or physiology, some deeply ingrained skill, or other behavioural characteristics, or something that is the combination of the two. They use unique personal traits for security purposes, most probably for authentication. There are fourteen different types of biometrics that fall into two categories: those that measure behaviour and those that measure physical traits [11]. It is not in the intentions of this paper to get into great detail about biometrics as a means for user authentication. A reader should refer to [6, 11] for a comprehensive coverage in the area.

During the past couple years it has been initiated a research effort towards investigating the possibility of utilising certain methodologies of biometrics in the cryptography arena. Unique user characteristics derived from the biometric information or else biometric signatures, provide the foundation upon which cryptographic keys and in some cases pseudorandom numbers can be generated [4, 9, 14, 15, 19]. The keys are closely related with the user and claimed to be only reproducible by the authorised entity. Moreover, they can be generated upon demand, eliminating any security vulnerabilities that might occur from the otherwise necessary storage of the keys.

An interesting dimension on the biometric generation of cryptographic keys is the computational power optimisation of the algorithm that enables it to operate in pervasive and ubiquitous computing. Consequently, the wireless user can generate cryptographic keys using either physical or behavioural biometrics to secure the transmission of voice and/or data through the airwaves. In case an attacker compromises the device, reverse engineer it and extract all the available information about the key generator, however, the key itself should not be confidently determined.

In this paper, we introduce a general class of side channel attacks against biometric based key generation systems. We demonstrate the steps should be followed to extract additional information leaked from the implementation of the key generator. Based on this information the

attacker can not only derive important conclusions about generator's operation but is also able to partially and in some cases fully retrieve the biometric signature of the valid user. While our approach substantially increases the scope of side channel attacks, the defence mechanism needed to minimize its effectiveness is no different than the existing countermeasures against side channel analysis [5, 10].

Interestingly enough, during our research all the hardware implementations of cryptographic key generators based on biometrics that were analysed did not incorporate in their design basic principles that would eliminate even the simplest type of side channel attacks (timing attacks).

The remainder of this paper is organised as follows. Section 2 describes side channel analysis by emphasising on its different types of attack. Section 3 introduces the generation of secret keys based on voice biometrics and demonstrates our research efforts in attacking such systems by employing side channel analysis. Finally, Section 4 concludes the paper, by discussing the research results achieved and proposing research areas needing some further development.

2 Side Channel Attacks

Side channel attacks fall into the general category of passive attacks. Side channel information, deriving by measuring some physical characteristic of the algorithm's operation, is processed by the attacker in order to gain additional knowledge about the cryptographic operation itself. This extra information, also known as *information leakage*, can be used to bypass any security barriers and invalidate the cryptographic system.

The information leakage model has derived from research studies that have shown that the power consumption of an algorithm operating with various data inputs (preferably random) generates power consumption traces with small but existent variations. These variations can be correlated to the Hamming weight of the processed data. The latter implies that the attacker is able, with a small overhead of computation power, to create several hypotheses about the very nature of the plaintext, the individual probabilities of which are very high.

Depending on the type of the physical characteristic measured, side channel attacks are classified into four main categories: timing, power, electromagnetic emanation and faults analysis. In the following subsections an abstract description of each of these types of side channel attacks provided.

2.1 Timing Analysis

In this category of attacks the execution time of the algorithm is measured for a large number of different data entries. The duration of the algorithm can provide assistance to the attacker only when it is dependent on the data it processes and does not have a fixed value. This vulnerability firstly exposed by Paul Kocher in 1996, when in his paper [12] he described timing attacks on implementations of Diffie-Hellman, RSA, DSS and others. Since then, there have been several timing attacks on cryptographic algorithms like [3, 17, 20], denoting the strength of this cryptanalytic methodology. Consequently, contemporary implementations are tolerant against timing analysis attacks. It is believed, though, that timing analysis can be combined with other types of side channel attacks, increasing significantly the impact on the cryptographic algorithm targeted. The simplest defence against timing analysis is to build cryptographic algorithms that its execution time is constant and does not depend on the information bits it handles.

2.2 Power Analysis

Unless the power consumption of an algorithm, in our case cryptographic, is code independent it can also leak critical information. The simplest type of power analysis attacks is known as Simple Power Analysis (SPA) and it is based on a single measurement. The collected power trace leaks information about algorithm's operations and results in the disclosure of the secret key or part of it. It has been employed against cryptographic algorithms such as RSA implementation targeting the differences between squaring and multiplication operations, DES and AES.

Differential Power Analysis (DPA) is a more powerful type of attack than SPA. It uses statistical methods to obtain side channel information, and therefore it requires a large number of power traces before data analysis can take place. During the data collection phase the input of the plaintext can take random values but the secret key should remain unaltered. DPA aims in identifying the relationship between the processed data and the power trace, whereas SPA is targeting algorithm's operations. The latter implies that DPA needs less information about the cryptographic algorithm that SPA does. The area of DPA attacks has been introduced by Paul Kocher in 1999 [13].

2.3 EM Emanation Analysis

A cryptographic device consists of a large number of components, placed in a close proximity to each other due to physical size constraints. Current passes through those components and results in the generation of an electromagnetic field. The type of side channel attack described in this section, proliferates from information leaked from the existent electromagnetic emanation. An EM emanation occurs either when current flows within circuits (direct emanation) or due to electronic and electromagnetic coupling (unintentional emanation). Direct emanation consisted the base for the first EM attacks [8, 16]. However, attacks that utilise unintentional emanations are proved to be substantially more efficient [1]. Furthermore, EM analysis enables the attacks against the

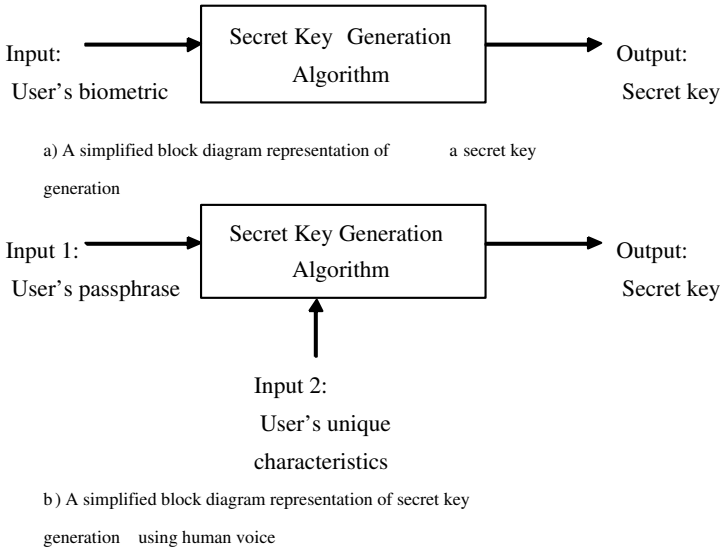

Figure 1: A general key generation algorithm and a key generation algorithm based on speech

cryptographic algorithm to be mounted from a distance, bypassing any physical security defence mechanisms employed to protect the device.

2.4 Fault Analysis

In 1997 Boneh et al. introduced in [2] another side channel analysis technique that is based on faults cryptographic systems generate. Fault attack is the only type of side channel attacks that is not passive. According to Boneh, systems malfunctions are always accompanied with a special message indicating the erroneous result. This information is analysed and processed by the adversary for cryptanalytic purposes. There are three main categories of faults and these are the transient, latent and induced faults. Transient faults occur randomly triggering the system to perform erroneous computations. Latent faults are related with all hardware and software bugs that are very difficult to be identified. The third category of faults, induced faults, is considered as the most sophisticated and effective. They require physical access to the cryptographic device so that adversary designed errors can be induced.

3 Generation of Secret Keys Using Human Voice

3.1 Fundamentals

Biometrics is a research area that experiences rapid evolution and is closely related with computer security because it is employed as a measure that improves the confidence of the system for a user's identity. Although the advances of biometrics solutions have been significant, their involvement in cryptographic algorithms is in a premature stage

During the last couple of years there has been an increasing scientific interest in employing biometrics into the generation of secret keys [4, 7, 9, 14, 19]. Either behavioural or physical, biometrics aim in capturing unique biometric characteristics of the user and utilise this sensitive data so that a secret key can be generated. An important aspect of this generation process is the reproducibility of the key. In plain words this means that every time a valid user produces the correct biometric signature, the same output should be accurately generated. Especially in behavioural biometrics, like human voice, the latter can be proved really challenging. The entire process of generating secret keys by using biometrics should be designed to operate on a resource constrained environment, like a smart card, so that its overall usability as an application is ensured.

3.2 Security of a Key Generation System

Our previous exposure in the area [7], created a scientific interest towards the overall security of the secret key generation system. The significant advances in side channel analysis, as described in Section 2, caused a certain amount of skepticism which can be summarised in a single question: Is this type of secret key generation susceptible to side channel attacks when it is implemented in resource constraint devices?

Instead of trying to describe a theoretical side channel attack on a general key generation system using biometrics, it has been decided to narrow down the scope of this research by choosing a specific biometric type.

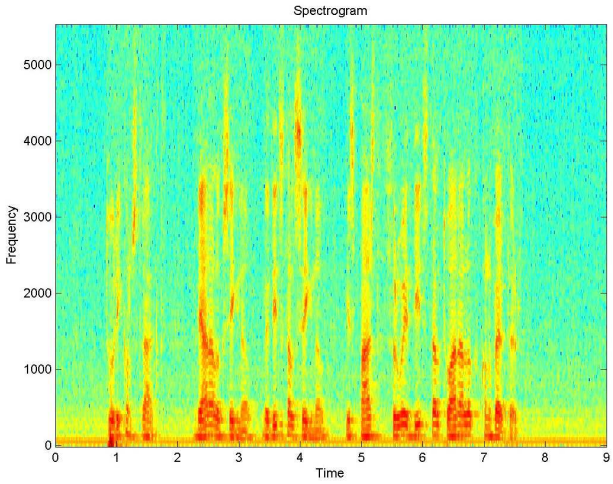

Figure 2: The spectrogram of the voice signal of person X1 speaking the sentence

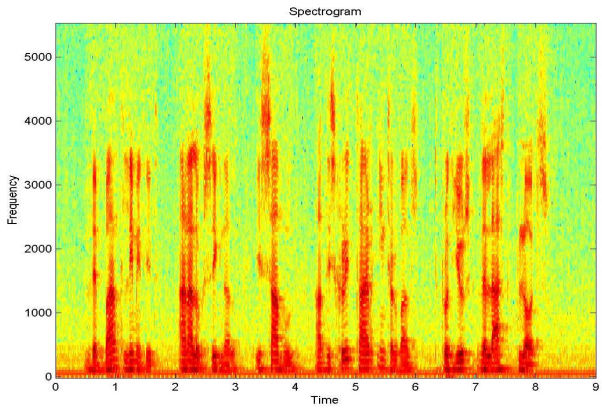

Figure 3: The spectrogram of the voice signal of person X1 speaking the sentence S2

Behavioural biometric systems considered more intrusion tolerant than their physical counterparts. The latter happens because behavioural traits can easily be affected by human behaviour and therefore change rapidly as time passes by. The last point distinguishes these biometrics from the ones measuring physical traits because they do not have to record the same phenomenon each time. Consequently, an adversary has to capture or guess a trait that is not stable and changes dynamically over time. For the remaining of our research work, human voice will be the biometric trait our system needs as input to generate secret keys.

Speech has some considerable advantages when it is used as a biometric. It is not difficult to elicit, is easy to record and many types of disguise are easy to detect, even in automatic systems. Furthermore, human's linguistic behaviour is unique and manifests itself most obviously in people's speech.

Furthermore, speech constitutes a two-dimensional input for the key generation algorithm as it is shown in Figure 1. It consists of the passphrase chosen to be spoken and the unique characteristics of the user's voice (pitch). The secret key is dependent on both the context of the passphrase and the characteristics of the person's voice. Otherwise, any systems that emphasise on one of these two "variables", neglecting the existence of the other substantially minimises the security of the system.

A close observation of Figure 1b, shows that a key generation algorithm using human voice has some fundamental similarities with a cryptographic operation. Conventional cryptographic algorithms take plaintext and secret key as input to produce ciphertext as output. In our case, the chosen passphrase can be parallelised with the plaintext, whereas user's voice characteristics can be treated as the secret key. Moreover, the several phases of operations within the key generation algorithm are heavily contaminated by the algorithm's input and especially by the speaker's pitch. The latter can be justified by mentioning that all the key generation algorithms based on biometrics, produce outputs that claim to obey a one-to-one relationship with the input and that are uniquely dependent on the characteristics of the user's voice.

The contamination of the produced output create a significant question about the overall security of the secret key generation based on biometrics: Can side channel attacks apply on this type of algorithms and expose part of the secret user's voice characteristics? In the following section we present the empirical research approach we followed in order to address this critical question.

3.3 Empirical Testing

It has become apparent that human voice plays a centre role in the biometric-based generation of secret keys. Hence it is necessary to investigate some of the attributes speech contains as a digital signal. Twenty-five people were involved in this research work, providing two thousand voice samples. The participants were of both genders aged between twenty-one and forty five years old. Their mother tongue was English with the exception of two people who were not native speakers. Each person produced a set of forty voice recordings indoor and another set of the same number of recordings outdoors.

3.3.1 Same Speaker - Different Pass Phrase

This category of speech recordings investigated the relationship between the context of the spoken sentence and the generated waveform. It is expected that the output of the biometric algorithm will be closely related to the context of the pass phrase. The following Figure 2,3,4 illustrate the speech of a person, X1, speaking three different sentences S1, S2, S3 respectively.

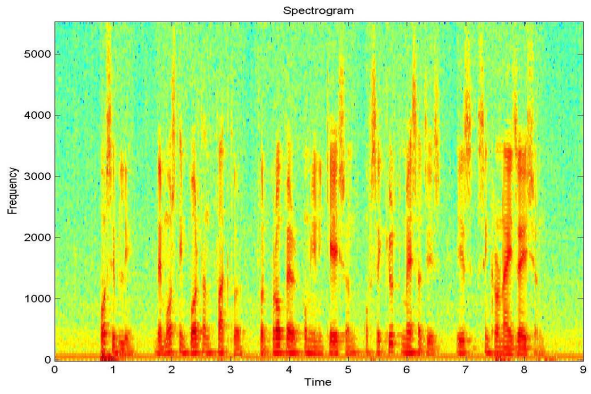

Figure 4: The spectrogram of the voice signal of person X1 speaking the sentence S3

The previous three spectrograms emphasise the impact the context of the pass phrase has on the generation of the voice signal, as there is no close resemblance between them. Evidently, there are some similarities, which can be reasoned due to the existence of common letters within the three spoken sentences S1, S2 and S3. The entropy of the English language, guarantees the presence of certain letters in a frequent manner, within any syntactically correct sentence. The entropy is expressed in terms of probabilities involved. The relative entropy of the source derives from the ratio of the actual to the maximum entropy with the remainder forming the redundancy. It is most interesting to note that the redundancy of English is approximately fifty percent, so that about half of the letters or words chosen in writing or speaking are controlled by the statistical structure of the language [18].

3.3.2 Attacking the Key Generation Algorithm

Based on this scenario, same speaker-different passphrase, we mounted the first side channel attack against a key generation system. The measurement setup used to collect the large number of power traces is illustrated in Figure 5. The speaker remained the same in an attempt to approximate the DPA attack according to which the cryptographic algorithm is executed many times with random data input, while the secret key remained unaltered.

In reality, an SPA attack was deployed first so that we manage to identify and target specific operations of the key generation algorithm. An emphasis was given to the part of the algorithm where the biometric signature, or else speaker descriptor is generated. The generation of this binary number has been intentionally designed to be based on unique speech characteristics so that it ensures the uniqueness of the secret key. Interestingly enough, an analysis of the power consumption resulted by the operation of the key generation algorithm on the development board, revealed a weakness against SPA attacks. The amplitude of the power trace in all collected samples was linearly dependent on the hamming weight of the processed data. This implies that the attacker could have access to this sensitive information with a simple monitoring mechanism as described here.

Once this operation is identified, we start collecting a large number of power traces to mount a DPA attack. A single user produced thousand voice signals by speaking random passphrases chosen from a novel book. The large number of recordings aims in the deployment of statistical techniques to identify smaller scale power variations that are difficult to locate otherwise due to the presence of noise or measurement errors. The methodology presented in [13] was followed with minor modifications that were necessary for the transition from a cryptographic to a key generation algorithm.

1) Collect thousand voice samples from a single speaker repeating random passphrases. Instead of having a fixed number of data points per sample, as is the case in DPA attack against DES, voice recordings vary in duration (seconds) and consequently vary in the number of data points they consist of (time duration x sampling rate). During the recording phase the sampling rate is kept constant at 11.025 samples/sec.

2) The attacker focuses on the key generation function responsible for the construction of the biometric signature. This function would have the form $B(U_i, K)$, where U_i is some biometric signature information, and K is the generated secret key. The adversary's goal is to find the correct value of U_i, assuming that the generated secret key has been compromised.

3) A differential average trace $T[i]$ is then computed based on information produced during the first two steps.

4) Every time the set $T[i]$ demonstrates power consumption biases, the adversary can safely conclude that the corresponding U_i has the correct bit value. In any other case $T[i]$ will average to zero due to lack of correlation.

5) The previous steps should be repeated for the remaining of the biometric signature U.

3.3.3 Tolerance Algorithm

A behavioural biometric algorithm should be able to tolerate the small variations of the human voice. This can be achieved if the architect of the biometric system designs an "intelligent" routine that enables the system to cope with minor physical variations of a person's speech. During the design phase, the architect is able to choose the attributes of the biometric system. The trade off between usability and security should be adjusted so that the system meets the application's requirements. The tolerance percentage can be set by the programmer and is closely related with the desired level of security of the application and the background environment. It is a trade off between

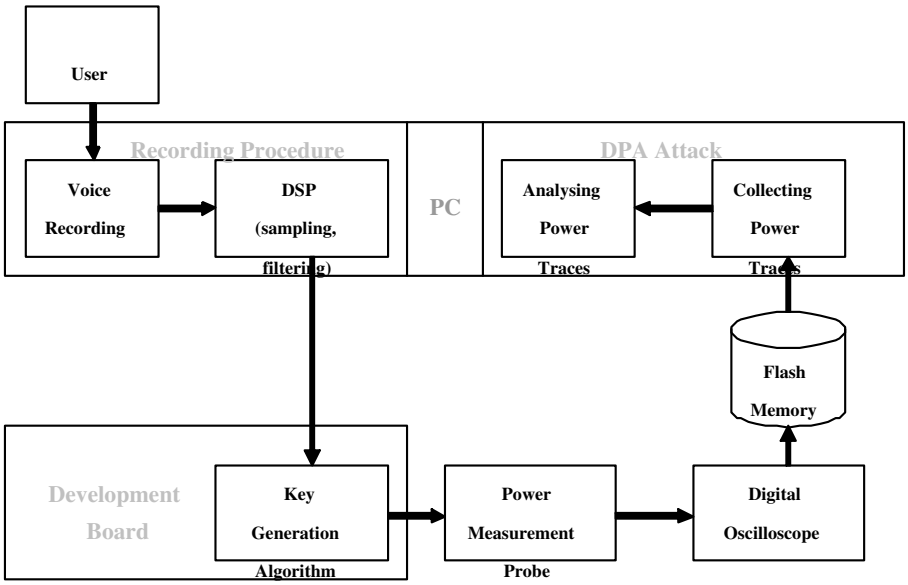

Figure 5: Block diagram representation of the SPA and DPA attacks mechanism

the usability of the system and its security. The environmental noise interference in outdoor recordings distorts the signal more than it does in indoor recordings. Evidently, the tolerance percentage has to be greater in the first instant than in the second.

During the analysis phase of the measured power traces, especially during the SPA attack, the tolerance function was identified. Whenever there was a small fluctuation of the recorded signal, the algorithm was using this function to test whether the variation is within the acceptable range or not. This extra process affects directly the power consumption and is easily identifiable, providing useful information about user's biometric signature to an attacker.

4 Conclusions and Further Directions

Biometric-based generation of secret keys is a research area that has evolved recently. Either behavioral or physical, biometrics have been proposed as a secure way of generating robust cryptographic keys, even in resource constraint environments. In this paper we presented certain side channel attacks, based on power analysis, that have been applied, to the best of our knowledge, for the first time against implementations of key generation algorithms. The strong resemblance between cryptographic and key generation operations provided the pilot for this research work.

Furthermore, it was demonstrated that an adversary is able to extract accurately part of even the entire biometric signature of a valid user. In order the latter to be feasible, the attacker should only compromise the generated key and have detailed knowledge of the key generation algorithm. Crucial information about algorithm's operations and the sequence followed are deducted by mounting an SPA attack first.

During the several phases of research work, another important security vulnerability has been exposed. Most biometric systems increase their usability by deploying a tolerance algorithm that enables the system to cope with small variations of the recorded signal's amplitude. However, this tolerance algorithm, once implemented on hardware, provides vital information to an adversary leading to the exposure of the biometric signature.

Finally, we believe that our research approach of attacking a biometric based key generation algorithms should be enriched by including more types of side channel attacks like EM emanation and fault analysis. The research focus can move to some physical biometric systems, where the significance of exposing the biometric signature is substantially of a larger scale. At last but not least, some optimization refinements should take place on our technique so that power analysis attacks can be mounted with a smaller number of collected traces.

References

[1] D. Agrowal, B. Archambeault, S. Chari, P. Rohatgi, and J. Rao, "Advances in side-channel cryptanalysis, electromagnetic analysis and template attacks," *Cryptobytes, RSA Laboratories*, vol. 6, no. 1, pp. 20-32, 2003.

[2] D. Boneh, R. DeMillo, and R. Lipton, "On the importance of checking cryptographic protocols for faults," in *EUROCRYPT'97*, LNCS 1233, pp. 37-51, Springer-Verlag, 1997.

[3] D. Brumley and D. Boneh,"Remote timing attacks are practical," in *Proceedings of 12th USENIX Security Symposium*, pp. 1-14, 2003.

[4] Y. Chang, W. Zhang, and T. Chen, "Biometric based cryptographic key generation," in *IEEE Conference on Multimedia and Expo*, pp. 2203-2206, 2004.

[5] S. Chari, C. S. Jutla, J. R. Rao, and P. Rohatgi, "Towards sound countermeasures to counteract power-analysis attacks," *CRYPTO '99*, LNCS 1666, pp. 398-412, Springer-Verlag, 1999.

[6] J. Chirillo and S. Blaul, *Implementing Biometric Security*, Wiley & Sons, 2003.

[7] D. Delivasilis, *Data Security for Third Generation Telecommunication Systems*, Thesis, University of Warwick, 2003.

[8] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic attacks: concrete results," in *CHES 2001*, LNCS 2162, pp. 251-261, Springer-Verlag, 2001.

[9] A. Goha and D. Ngo, "Computation of cryptographic keys from face biometrics," in *Conference on Communications and Multimedia Security*, pp. 1-13, Italy, Oct. 2003.

[10] L. Goubin and J. Patarin, "DES and differential power analysis (The "duplication" method)," in *CHES '99*, LNCS 1717, pp. 158-172, Springer-Verlag, 1999.

[11] A. Jain, R. Bolle, and S. Pankati, *Biometrics: personal identification in networked society*, Kluwer Academic Publishers, 1998.

[12] P. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS and other systems," in *CRYPTO'96*, LNCS 1109, pp. 104-113, Springer-Verlag, 1996.

[13] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis: Leaking secrets," in *CRYPTO'99*, LNCS 1666, pp. 388-397, Springer-Verlag, 1999.

[14] F. Monrose, M. K. Reiter, Q. Li, and S. Wetzel, "Cryptographic key generation from voice (extended abstract)," in *Proceedings of IEEE symposium on Security and Privacy*, pp. 202-213, 2001.

[15] M. Peyravian, S. M. Matyas, A. Rosginsky, and N. Zunic, "Generating user-based cryptographic keys and random numbers," *Journal of Computers and Security*, vol. 18, no. 7, pp. 619-626, 1999.

[16] J. Quisquater and D. Samyde, "Electromagnetic analysis (EMA): measures and countermeasures for smart cards," in *Esmart 2001*, LNCS 2140, pp. 200-210, Springer-Verlag, 2001.

[17] W. Schindler, F. Koeune, and J. Quisquater, *Unleashing the Full Power of Timing Attack*, Technical Report 2002-03, UCL Crypto Group, 2002.

[18] C. E. Shannon and Warren Weaver, *The Mathematical Theory of Communication*," University of Illinois Press, 1949, 1963.

[19] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, and B. V. K. V. Kumar, "Biometric encryption using image processing," in *Proceeding of SPIE 3314*, pp. 178-188, 1998.

[20] C. Walter and S. Thompson, "Distinguishing exponent digits by observing modular subtractions," in *Proceedings of Topics in Cryptology*, LNCS 2020, pp. 192-207, Springer-Verlag, 2001.

Dr. Dimitrios L. Delivasilis was born in Greece in 1976. He holds a B.Eng. in Computer Hardware and Software Engineering, an MSc. in Data Communication Systems and a Ph.D. in Data Security for Third Generation (3G) Telecommunication Systems, from the universities of Coventry, Brunel and Warwick respectively. Prior to the beginning of his academic career he has obtained over four years commercial experience in R&D departments of telecommunication industry, in the countries of England and Greece. His current research interests include wireless security, cryptographic algorithms, intrusion tolerance systems and biometrics. His published scientific work includes several international journals and conferences, as well as, a filed British patent. He is a member of International Association for Cryptologic Research (IACR), IEEE Computer Society and serves as a reviewer for IEE Proceedings.

Sokratis K. Katsikas was born in Greece in 1960. He received the Diploma in Electrical Engineering degree from the University of Patras, Greece, the M.Sc. in Electrical & Computer Engineering from the University of Massachusetts at Amherst, USA, and the Ph.D. in Computer Engineering from the University of Patras, Greece. He now is Professor at the Department of Information and Communication Systems Engineering and Rector of the University of the Aegean, Greece. He has authored or co-authored more than 150 technical papers and conference presentations in his areas of research interest, which include information and communication systems security, estimation theory, adaptive control, and artificial intelligence. He has served on steering, program and organizing committees of international conferences on informatics and is a reviewer for several scientific journals.