Research Statement

Antonio Faonio,
Aarhus University,
afaonio@gmail.com

My research area is cryptography. From ancient Greek, "crypt" means hidden while "graphy" refers to the process of writing. Once considered the art of "secret communication", nowadays, cryptography is much more. Rapid technological advances and ubiquitous social and communication networks (such as the Internet) have leaded to the development of new complex digital services which security requirements go far beyond the need of "communicating secretly".

In modern terms, cryptography is concerned with the feasibility or infeasibility of securely realizing a task. The answer to whether or not a task can be securely realized depends on the assumed power of the adversary and the network model. The goal is to obtain security while minimizing the need for trust. The obtained security holds in a strong mathematical sense, meaning that breaking a secure cryptographic protocol is either impossible or it would require to solve some computational problem which is believed to be hard with the current technology.

In what follow I describe the main themes concerning my research, together with directions for future research.

Research

The achievements of my research are mostly on leakage resilient cryptography, but not limited to this. In fact, I participated to research projects in different topics of cryptography, both from applied to theoretic prospective.

Leakage Resilient Cryptography

The areas of research of leakage resilience can be motivated with a very simple observation, which has made and makes me very enthusiastic to work on these fields: A cryptographic primitive has to be implemented in a program that will run a specific architecture and surrounded by a specific environment. An attacker could take advantage of implementation-specific characteristics, and indeed, mathematically secure systems turned out to be physically vulnerable. This vulnerabilities are exploited via the so called side-channel attacks.

The point is that standard security definitions for cryptographic primitives (e.g., encryption or signature schemes) assume implicitly that the adversary has only black-box access to the underlying algorithms, however side-channel attacks have shown that this is not the case.

In the recent years a lot of progress has been done, both in term of practical countermeasures on specific side-channel attacks and in term of realizing cryptographic primitives for gradually stronger security models. My research lies in the second trend, with the goal of making efficient cryptographic schemes secure in reasonable models which capture existing side-channels attacks.

Here, I would like to stress on the words "reasonable" and "efficient". The common critique is whether the known theoretical models cover physical leakages in an appropriate way or not. As example, while the bounded leakage model (probably the most known and studied leakage model) offers a beautiful abstraction by only bounding the nature of the leakage on its output

size, a power measurement attack can hardly be described by a few bits of information. The second critique is that leakage-resilient (and also tamper-resilient) schemes are still far from being practical. For the reasons described above, my works concentrate on general models with a stress on efficiency. With my co-authors I contributed to the development of leakage-resilient primitives.

- In **[12]**, we developed signature schemes in the noisy (and fully) leakage model . Here we considered a leakage model where the only constraint is that the secret material (both the secret key and the randomness of the signing process) must retain some uncertainty (in an information-theoretic sense) after the leakage. By considering attacks also on the randomness we push the boundary even further, in fact, it is natural that an enemy capable of side-channel attacks would also leak from the random source. The standard notion of signature scheme does not cope well with leakage, short signature schemes are indeed impossible according to the standard definition, however, we were able to provide secure schemes with short signature size (and indeed better efficiency, at least in term of communication complexity) by relaxing the definition to "the best we can hope for". Namely, we relaxed the definition considering an adversary that might be able to produce some signatures (this because, in principle, it could leak them), however it cannot produce more signatures that it can leak. The paper also contains a fairly practical scheme using the random oracle model, the scheme achieves the extra efficiency of (a noisy version of) the bounded retrieval model (BRM) where the secret key can be as big as we want without any degradation of all the other efficiency parameters.

I consider the BRM very interesting: having a 1GB long secret key stored in our device, right now, is not a big deal, on the other hand, performing a side-channel attack that stealthily leaks all this amount of data (either using side-channel or a by infecting the device) seems to be quite unpractical. The bounded retrieval model is the subject of another paper that I co-authored:

- In **[4]**, we showed that Proof of Storage (specifically, their zero-knowledge version) can be proved to be secure identification scheme in the BRM. This leaded to a very practical RSA based scheme, which I could easily implement on top of an already implemented RSA Proof of Storage [3].

More recently, I got interested in general purpose compilers that provide leakage resilience to any cryptographic functionality.

- In **[11]**, we analyzed the tool of Leakage Resilient Codes (LRC) that are very useful in the setting I mentioned before (see Faust and Dziembowski [8]). One of the drawbacks of using LRC is that the inputs need to be encoded in a leak-free environment. We investigated if this is necessarily the case. Unfortunately, we showed that LRC that are also resilient to small leakage from the encoding process (which we dubbed Fully Leakage Resilient Codes) are impossible to achieve. This is the case because the leakage function can be very complicated. Fortunately, we showed that the impossibility result can be bypassed in certain circumstances e.g., by putting some limitations on the complexity of the leakage or by having milder setup assumptions like the common reference string.

From my point of view, it is necessary to find the right balance between efficiency and a good approximation of the real capability of the adversary: standard model primitives are very fast but they cannot be considered truly secure. Bounded leakage is a halfway through, it is not quite the answer against real side-channel attacks, but it is a significant step forward and fairly efficient schemes exist. On the other hand, the landscape in more general models e.g., the noisy leakage model or the fully leakage model is still broadly unknown.

Other works on Theoretic and Applied Cryptography

Cryptography is an awesome field to work on, in fact, while motivated by highly practical problems, it allows to originate new surprising mathematical concepts that were never studied before. Below I give some examples from my research achievements in foundational cryptography.

- In [**2**], we started with the practical question of making the BlockChain[1] technology environmental friendly[2]. The paper introduces the concept of Proof of Space (PoSpace). Briefly, a PoSpace protocol allows to succinctly show to a verifier the posses of some space, specifically, to compute such a proof, the prover must use a specified amount of space. To compare, we proposed an alternative to the Proof-of-Work technology which makes the Bitcoin system secure, by using space (like unused hard drive space) rather than computational power. Apart of proposing a new concept, we showed constructions in the Random Oracle Model, both interactive and non-interactive.

- In [**13**], we initiated the characterization of proof systems that we called Predictable Arguments of Knowledge (PAoK). The project started when we were working on the paper of Fully Leakage Resilient Codes, we noticed that, in order to strengthen our result, we needed a new form of proof system. Soon we realized that the concept deserved more interest. Specifically, we analyzed argument of knowledge[3] for NP where the verifier can predict the answer that the prover will give. Thanks to this powerful tool we were able to show that any LRC (in the popular split-state model) can be broken by leaking only 7 bits from the encoding process. But this is only an application that shows the power of PAoK. More interestingly, we showed connections with other cryptographic primitives, we showed that PAoK can be made extremely succinct (one round and one bit from the prover to the verifier are enough!), we gave a full characterization of its zero-knowledge versions and analyzed its power in the context of adaptive security. This is, up to now, probably the most theoretic work which I was involved in.

As mentioned already, I am open to do research in all the aspects of cryptography. I am also interest in applied cryptography:

- In [**5**], we described an extension of the Bitcoin protocol that preserves its decentralized nature, while also enabling payers to optionally specify the involvement of a trusted authority that attests to the identity of the payee, by requiring payees to use certified Bitcoin addresses. More specifically, we introduce the concept of Bitcoin addresses that need to be generated with the support of a semi-trusted authority. Notice that, while the semi-trusted authority can mint coins on behalf of a particular user, it cannot spend any of them. Nicely, these certified addresses are allowed to co-exist with the standard auto-generated Bitcoin addresses and can be easily integrated without any change in the specifications of the BlockChain.

Future Directions

I expect to continue working in the areas I mentioned in the future, while remaining open to new opportunities. Below are just a few examples to illustrate the kind of problems I expect to pursue in the coming years.

[1] The BlockChain is the public ledger used by Bitcoin, which is a peer-to-peer electronic cash system.

[2] See "Virtual Bitcoin Mining Is a Real-World Environmental Disaster" by Mark Gimein.

[3] Namely, proof systems where any convincing polynomial-time prover must "know" the witness relative to the instance being proven.

The concept of Proof of Space has received a lot of interest (e.g., see [9, 15, 1, 14] for related works[4]), however, all the proposed constructions of Proof of Space or of related cryptographic primitives are in the Random Oracle Model. It is is still an open problem to find a protocol in the standard model. I have in mind to leverage some a recent advance in complexity (see Raz [16]) to tackle the problem.

Currently, I am involved in research projects that spread from tamper resilient cryptography to subversion resilience. Tamper Resilience considers the scenario where the adversary can somehow alter the state of the cryptographic device through physical attack such as microwaving the device or exposing to heat or EM radiation. Unfortunately, strong negative results exist even for restricted versions of this problem. On the other hand, something can be done in many realistic scenarios. For example a recent paper of Damgaard *et al.* [7] introduced the concept of bounded-tamper resilience where an adversary can tamper only for a limited amount of time with the memory of the device. This model is very reasonable: the more the attacker tampers with the device the more likely it will break down and stop to work. With my co-authors, we have already some preliminary results on signature schemes and efficient CCA (based on the Cramer-Shoup paradigms) secure encryption schemes. Another interesting research trend in tamper resilience is the fascinating tool of Non-Malleable Code (NMC). Since their introduction by Dziembowski *et al.* [10], NMC received a lot of interest. Devise new flavor of NMC always brings an improvement in the context of tamper resilience. I have in mind several extensions, for example, recently, I'm working on non-malleable and leakage resilient codes in the split-state model that can be succinctly updated. In this model the codeword is divided in two (or more) pieces and the tampering happens independently in each piece. We found out that in the information theoretic setting, the updating procedure necessarily needs interaction between the pieces. However, in computational setting, this does not seem to be the case. In fact, we have already some feasibility results that need to be further investigated.

In the revelations of Edward Snowden have evidenced that some cryptographic protocol specifications, for example the standard Dual EC in NIST SP 800-90A, were modified to embed backdoors. Recently, the ability of substituting a cryptographic algorithm with an altered version was (re)considered by Bellare *et al.* [6] (see also [17]). The landscape shown is mostly negative: all stateless and randomized encryption schemes can be stealthily subverted by a powerful adversary, a big brother, in such a way that no privacy can be assured. In [6] is shown a class of encryption schemes that are subversion resilient, however, we have a preliminary result showing that in a more general setting where the subversion-resistant encryption scheme is triggered by an application, that in turn can be subverted, subversion resilience is not enough to assure privacy. Currently I am working on way to overcome this negative result, the idea is to apply knowledge from leakage and tamper resilience cryptography in this context.

In my view, privacy is essential for a free and functioning society. Doing research in cryptography is therefore not only real fun but also an active way to collaborate for a better world. Leakage and tampering attacks are getting cheaper and easier to implement while substitution attacks were showed to be a real threat. In my opinion, it is, therefore, important to bring to a practical level both leakage and tamper resilient schemes, and actively get involved with the research on the new and still undiscovered setting of subversion resilience.

References

[1] Joël Alwen and Vladimir Serbinenko. High parallel complexity graphs and memory-hard functions. In *STOC*, pages 595–603, 2015.

[4] Specifically, [9] is an independent work.

[2] Giuseppe Ateniese, Ilario Bonacina, Antonio Faonio, and Nicola Galesi. Proofs of space: When space is of the essence. In *SCN*, pages 538–557, 2014.

[3] Giuseppe Ateniese, Randal C. Burns, Reza Curtmola, Joseph Herring, Lea Kissner, Zachary N. J. Peterson, and Dawn Xiaodong Song. Provable data possession at untrusted stores. In *CCS*, pages 598–609, 2007.

[4] Giuseppe Ateniese, Antonio Faonio, and Seny Kamara. Leakage-resilient identification schemes from zero-knowledge proofs of storage. In *Cryptography and Coding - 15th IMA International Conference, IMACC*, pages 311–328, 2015.

[5] Giuseppe Ateniese, Antonio Faonio, Bernardo Magri, and Breno de Medeiros. Certified bitcoins. In *ACNS*, pages 80–96, 2014.

[6] Mihir Bellare, Kenneth G. Paterson, and Phillip Rogaway. Security of symmetric encryption against mass surveillance. In *CRYPTO*, pages 1–19, 2014.

[7] Ivan Damgård, Sebastian Faust, Pratyay Mukherjee, and Daniele Venturi. Bounded tamper resilience: How to go beyond the algebraic barrier. In *ASIACRYPT*, pages 140–160, 2013.

[8] Stefan Dziembowski and Sebastian Faust. Leakage-resilient circuits without computational assumptions. In *TCC*, pages 230–247, 2012.

[9] Stefan Dziembowski, Sebastian Faust, Vladimir Kolmogorov, and Krzysztof Pietrzak. Proofs of space. In *CRYPTO*, pages 585–605, 2015.

[10] Stefan Dziembowski, Krzysztof Pietrzak, and Daniel Wichs. Non-malleable codes. In *ICS*, pages 434–452, 2010.

[11] Antonio Faonio and Jesper Buus Nielsen. Fully leakage-resilient codes. *IACR Cryptology ePrint Archive*, 2015:1151, 2015.

[12] Antonio Faonio, Jesper Buus Nielsen, and Daniele Venturi. Mind your coins: Fully leakage-resilient signatures with graceful degradation. In *ICALP*, pages 456–468, 2015.

[13] Antonio Faonio, Jesper Buus Nielsen, and Daniele Venturi. Predictable arguments of knowledge. *IACR Cryptology ePrint Archive*, 2015:740, 2015.

[14] Tal Moran and Ilan Orlov. Proofs of space-time and rational proofs of storage. *IACR Cryptology ePrint Archive*, 2016:35, 2016.

[15] Sunoo Park, Krzysztof Pietrzak, Albert Kwon, Joël Alwen, Georg Fuchsbauer, and Peter Gazi. Spacemint: A cryptocurrency based on proofs of space. *IACR Cryptology ePrint Archive*, 2015:528, 2015.

[16] Ran Raz. Fast learning requires good memory: A time-space lower bound for parity learning. *IACR Cryptology ePrint Archive*, 2016:170.

[17] Adam L. Young and Moti Yung. Kleptography: Using cryptography against cryptography. In *EUROCRYPT*, pages 62–74, 1997.