Cryptography Without (Hardly Any) Secrets ?

Shafi Goldwasser

MIT and Weizmann Institute

Abstract. The absolute privacy of the secret-keys associated with cryptographic algorithms has been the corner-stone of modern cryptography. Still, in practice, keys do get compromised at times for a variety or reasons. A particularly disturbing loss of secrecy is as a result of side channel attacks. These attacks exploit the fact that every cryptographic algorithm is ultimately implemented on a physical device and such implementations enable 'observations' which can be made and measured on secret data and secret keys. Indeed, side channel observations can lead to information leakage about secret keys, which in turn can and have lead to complete breaks of systems which have been proved mathematically secure, without violating any of the underlying mathematical principles or assumptions. Traditionally, such attacks have been followed by ad-hoc 'fixes' which make particular implementation invulnerable to particular attacks, only to potentially be broken anew by new examples of side-channel attacks.

In recent years, starting with the work on *physically observable cryptography* by [MR04] Micali and Reyzin, a new goal has been set to build a general theory of physical security against a large class of families of side channel attacks which one may call *computational* side-channel attacks. These include *any* side channel attack in which leakage of information on secrets occurs as a result of performing a *computation* on secrets. Some well-known examples of such attacks include Kocher's timing attacks [Koc96] and power attacks [KJJ99]. A basic defining feature of a computational side-channel attack, as put forth by [MR04] is that *computation and only computation leaks information.* Namely, portions of memory which are not involved in computation do not leak information. A growing number of works [MR04,ISW03,PSP$^+$08,GKR08,DP08] have proposed cryptographic algorithms provably robust against computational side-channel attacks, by limiting in various ways the portions of the secret key which are involved in each step of the computation.

In the work on *one time programs* this is taken to an extreme [GKR08]. Goldwasser, Tauman-Kalai, and Rothblum show how by using a new proposed type of secure-memory which never touches any secrets or data which is not ultimately fully revealed, it is possible to perform any secure computations which is provably secure against *all* computational side channel attacks.

Memory-attacks proposed by Akavia, Goldwasser, and Vaikuntanathan [AGV09] are an entirely very different family of side-channel attacks that are not included in the computational side-channel attack family, as they violate the basic premise of [MR04] that *only computation* leaks information. This class of attacks was inspired by (although not restricted

to) the memory-freezing attack introduced recently by Halderman et al. [HSH$^+$08], where its is shown how to measure a significant fraction of the bits of secret keys if the keys were *ever stored* in a part of memory (e.g. DRAM), which could be accessed by an adversary even after the power of the machine has been turned off. Thus, information leaks about portions of the secret key which may have never been involved in any computation. A memory-attack leaks a bounded number of bits computed as a result of applying *an arbitrary function* of bounded length (smaller than than the size of the secret key) to the content of the secret key of a cryptographic algorithm. Naturally, this family of attacks is inherently parameterized and quantitative in nature, as if the attack would uncover the entire secret key at the outset, there would be no hope for any cryptography. The work of [AGV09] exhibits a public-key encryption algorithm which is especially robust against memory-attacks. Its security is based on the computationally intractability of the *learning with errors* (LWE) problem which is related to the intractability of approximating the length of the shortest vector in an integer lattice. Finally, a new interesting variant on the idea of memory attacks, had been proposed by Tauman-Kalai etal [DTKL09] in their work on security with auximlary-inputs. They propose to replace the restriction of revealing a length shrinking function of the secret, to revealing functions of the secret which are exponentially hard to invert.

In this talk we will survery this development, with special emphasis on the works of [GKR08,AGV09,DTKL09].

References

[AGV09] A. Akavia, S. Goldwasser, and V. Vaikuntanathan. Simulatneous hard-core bits and cryptography against memory attack. In *TCC*, 2009.

[DP08] Stefan Dziembowski and Krysztof Pietrzak. Leakage-resilient stream ciphers. In *To Appear in the IEEE Foundations of Computer Science*, 2008.

[DTKL09] Y. Dodis, Y. Tauman-Kalai, and S. Lovett. Cryptography with auxilary input. In *STOC*, 2009.

[GKR08] Shafi Goldwasser, Yael Tauman Kalai, and Guy N. Rothblum. One-time programs. In *CRYPTO*, pages 39–56, 2008.

[HSH$^+$08] Alex Halderman, Seth Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph Calandrino, Ariel Feldman, Jacob Appelbaum, and Edward Felten. Lest we remember: Cold boot attacks on encryption keys. In *Usenix Security Symposium*, 2008.

[ISW03] Yuval Ishai, Amit Sahai, and David Wagner. Private circuits: Securing hardware against probing attacks. In *CRYPTO*, pages 463–481, 2003.

[KJJ99] Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In *CRYPTO*, pages 388–397, 1999.

[Koc96] Paul C. Kocher. Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems. In *CRYPTO*, pages 104–113, 1996.

[MR04] Silvio Micali and Leonid Reyzin. Physically observable cryptography (extended abstract). In *TCC*, pages 278–296, 2004.

[PSP$^+$08] Christophe Petit, François-Xavier Standaert, Olivier Pereira, Tal Malkin, and Moti Yung. A block cipher based pseudo random number generator secure against side-channel key recovery. In *ASIACCS*, pages 56–65, 2008.