

Circular-Secure Encryption from Learning Problems

David Cash¹
cdc@gatech.edu.

November 2, 2008

1 Introduction

We propose to study problems related to *circular-secure encryption*, a primitive that is practically very useful but not well understood theoretically. In its most basic form, circular-secure encryption deals with the problems inherent with encrypting a key under itself. That is, if we write $E_k(m)$ to mean an encryption of m using the key k , is it “safe” to publish $E_k(k)$ (a one-cycle)? If k_1, k_2 are independent keys, is it safe to publish $E_{k_1}(k_2)$ and $E_{k_2}(k_1)$ (a two-cycle)?

In the early days of complexity-based cryptography it was noticed that, in general, the answer was negative; there exist encryption schemes that satisfy our standard definition of semantic security but break completely if an adversary is given $E_k(k)$ (the answer is not known for cycles of size greater than one). The solution then was to disallow this usage of encryption, which seemed pathological in the 80s when many security definitions were first formalized.

Recently, however, some applications have attempted to do just this, with the most natural example being encrypted hard drive backups, where the key is usually stored on the hard drive. In fact, the IEEE P1619 standard for encrypted stored data contained a vulnerability due to circular encryption¹. In addition, some protocols intentionally publish encrypted key cycles [4]. Even if a protocol does not do this explicitly, it is sometimes difficult to guarantee that it will not incidentally happen.

In addition to practical issues, another line of research that uses formal logics to reason about protocol security has always implicitly used a type of circular security. Reconciling that approach with the complexity-based version of cryptography requires constructions that can securely encrypt cycles of keys [1].

/bin/bash: q: command not found Boneh et al [3], with security based on the Decisional Diffie-Hellman (DDH) problem, which is closely related to computing discrete logarithms. Their scheme sits in the gray area of “somewhat efficient” and must send thousands of group elements to encrypt a single bit.

2 This Project

We propose to construct circular-secure encryption by basing security on the hardness of machine learning problems. We have several motivations for attempting this direction. The first is efficiency: given our preliminary results, it seems that we can dramatically improve on the computational and communication overhead of the Boneh et al scheme. Second, there is only one known approach to achieve circular-security, and in cryptography we always prefer a diversity of schemes, in case algorithms are improved for one of the problems on which we have based security (e.g. DDH, mentioned above). Of particular interest is the possibility of basing security of worst-case hardness instead of average-case hardness, which is the norm for cryptography. Finally, connecting the (very small) areas of learning-based cryptography and circular security is surprising; the foundations for learning-based cryptography have been known since the 80s [2], but it seems that no connection was noticed. The techniques we contribute will hopefully be useful for solving other problems in learning-based cryptography.

In our preliminary results, we can construct circular-secure symmetric-key encryption based on the hardness of Learning Parity with Noise (LPN). We plan to adapt the techniques to use the so-called Learning

¹ Supervised by Alexandra Boldyreva.

¹c.f. http://en.wikipedia.org/wiki/IEEE_P1619

with Error (LWE) [5] problem, which is a generalization of LPN that will probably allow for a more efficient schemes *and* security from worst-case hardness.

In addition, we will explore constructions of public-key encryption from LPN and LWE. We are also considering the following foundational question, posed by Boneh et al [3], mentioned above: *Is standard semantic security equivalent to circular-security, for cycles larger than one?* We have settled this question in the negative for the case of symmetric-key encryption. We will consider the same question for public-key encryption.

Other Information I am planning to graduate in August 2009. My advisor can fund half of my GRA for Spring but not all of it. I will be a GTA in the Spring without some other funding. This research will form a significant portion of my dissertation. I have spoken about this work at the GT Student Theory Seminar and at the GT Cryptography Reading Group. One portion of this work is joint with Kaoru Kurosawa (Ibaraki University, Japan), and another is joint work with Chris Peikert (SRI) and Amit Sahai (UCLA).

References

- [1] Martín Abadi and Phillip Rogaway. Reconciling two views of cryptography (the computational soundness of formal encryption). *Journal of Cryptology*, 15(2):103–127, 2002.
- [2] Avrim Blum, Merrick L. Furst, Michael J. Kearns, and Richard J. Lipton. Cryptographic primitives based on hard learning problems. In Douglas R. Stinson, editor, *CRYPTO'93*, volume 773 of *LNCS*, pages 278–291. Springer-Verlag, Berlin, Germany, August 1994.
- [3] Dan Boneh, Shai Halevi, Michael Hamburg, and Rafail Ostrovsky. Circular-secure encryption from decision diffie-hellman. In *CRYPTO*, pages 108–125, 2008.
- [4] Jan Camenisch and Anna Lysyanskaya. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In Birgit Pfitzmann, editor, *EUROCRYPT 2001*, volume 2045 of *LNCS*, pages 93–118. Springer-Verlag, Berlin, Germany, May 2001.
- [5] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In *37th ACM STOC*, pages 84–93. ACM Press, May 2005.