Generalized Indistinguishability

Ueli Maurer and Renato Renner[1]
Institute of Theoretical Computer Science, ETH Zürich
CH-8092 Zürich, Switzerland
{maurer,renner}@inf.ethz.ch

Abstract — **Indistinguishability between systems is a basic concept in cryptography, allowing for a generic type of security proofs. Its scope of application is however restricted to systems whose behavior depends on some secret randomness. We propose a generalized definition of indistinguishability which overcomes this restriction, such that the same type of security proofs applies in a more general context where this randomness might be public.**

I. Indistinguishability

The concept of indistinguishability is widely used in cryptography, in particular for definitions and security proofs. Most cryptographic systems can be regarded as consisting of several subsystems or *components*. These are themselves systems, giving on each new input an output which in general depends on this input, all previous inputs, and some internal randomness. Two components C and C' are said to be *indistinguishable* if no (efficient) algorithm (the *distinguisher*), interacting with a blackbox system B, is able to decide whether $B = C$ or $B = C'$.

Indistinguishability between C and C' implies that any cryptosystem $S(C)$ involving the component C is at least as secure as the cryptosystem $S(C')$ which is built from $S(C)$ by replacing the component C by C'. The problem of proving the security of a cryptosystem $S(C)$ with a component C can thus be reduced to the problem of proving the security of an idealized system $S(C')$ where the component C is replaced by an idealized component C', and to show that C is indistinguishable from C'. However, for this type of proof to work in general, it is crucial that the internal randomness of the component C is kept secret.

As an example, consider a *pseudo random generator (PRG)*. This is an algorithm which, starting from some random value (the *seed*), computes a bitstring which, by definition, is indistinguishable from truly random bits [1]. Again, in order to conclude that the security of a cryptosystem which uses true random bits implies the security of the cryptosystem where these random bits are generated by a PRG, the seed must not be known to a possible adversary.

II. Generalization

Nevertheless, it is useful to consider components whose internal randomness is public. As an example, one might want to compare the security of cryptosystems involving different hash functions (i.e., parameterized classes of functions) whose parameter is publicly known. However, the conventional concept of indistinguishability is not appliable in this case.

We propose a generalization of indistinguishability between components which is not subject to this restriction. More precisely, we consider a more general type of components C whose internal randomness is thought to consist of a part which is public, called *public information* of C. Then, security of a cryptosystem $S(C)$ using component C means that $S(C)$ can not be broken even by an attacker which has access to the public information of C.

In order to define indistinguishability for components with public information, let us first introduce a special type of proof system: A verifier V is connected to a blackbox component B, but has no access to its public information. The goal of a prover P (which might have access to the public information of B) is to compute a witness w which convinces V of some statement about B. *Convincing* means that, (a) if the statement is true, then there is a witness w such that V accepts the proof with high probability, and, (b) if the statement is false, then the probability that V accepts (for any arbitrary witness w) is negligible.

Let C and C' be components with public information, and consider a proof system where either $B = C$ or $B = C'$. We say that V is a *verifier for distinguishing C from C'* if there is a witness convincing V of the fact that $B = C$. C is defined to be *indistinguishable* from C' if no such verifier exists.

This definition meets exactly the requirement needed for the generic type of security proofs described in Section I.

Theorem. *If and only if the component C is indistinguishable from C', then security of any cryptosystem $S(C)$ using C implies security of the cryptosystem $S(C')$ (the cryptosystem built from $S(C)$ by replacing C by C').*

III. Concluding Remarks

The concept of indistinguishability applies to a wider range of cryptographic problems than previously believed. On one hand, our extended notion of indistinguishability can be seen as the basis for new security proofs. On the other hand, it leads to impossibility results, e.g., in the context of the random oracle methodology. For instance, it allows for a significantly simplified proof of a statement proven in [2], saying that there is a cryptosystem which is secure when using a random oracle (which essentially is a completely random function), but becomes completely insecure when this random oracle is replaced by any hash function.

Acknowledgments

The authors would like to thank Clemens Holenstein for many interesting discussions.

References

[1] M. Blum and S. Micali, "How to generate cryptographically strong sequences of pseudo-random bits," *SIAM Journal on Computing*, vol. 13, pp. 850–864, 1984.

[2] R. Canetti, O. Goldreich, and S. Halevi, "The random oracle methodology, revisited," in *Proceedings of the 30th Annual ACM Symposium on the Theory of Computing*, 1998, pp. 209–218.

[1] This work was supported by the Swiss National Science Foundation (SNF).