A Survey of Cryptography Based on Physically Unclonable Objects

Kai-Yuen Cheong *

September 9, 2011

Abstract

This paper studies a new notion of a hardware: physically unclonable verifiable object (PUVO). Such objects are usually used in authentications. In the context of cryptography, we study the relation of such objects to Bit Commitment (BC) and Oblivious Transfer (OT). Both possibility and impossibility results are found.

1 Introduction

Physically unclonable objects are abundent. In fact, they are more common than clonable objects. Authentication based on physical objects exists before cryptography. Naturally, if you recognise a person by face, you usually would not ask for other identification documents. On the other hand, a piece of work by Van Gogh must be identified by trained experts. These are based on the assumption that a person's face and a masterpiece in painting are unclonable objects. As shown in the case of Van Gogh's work, the unclonable property must be considered together with the techniques available to identity the objects. Therefore, counterfeiting and anti-counterfeiting and two sides of the coin. Luckily, counterfeiting is usually the harder problem. We have many more examples:

1. Biometrics such as fingerprint and iris recognition are used to identify a person.
2. Almost all banknotes in the world have anti-counterfeiting features.
3. Some consumer goods come with unclonable seals.

There are two major types of unclonable objects. They can be solely based on technological advantages of the maker of the objects, like the case of banknotes. They can also be partly based on the natural disorder in objects that is hard

*School of Information, Japan Advanced Institute of Science and Technology. Email: kaiyuen@jaist.ac.jp

to reproduce, like the case of fingerprint. The latter seems to be more reliable, because technology can be stolen or overcome.

In order for unclonable objects to be useful, they must also be verifiable. In such a case, they are perfect for authentication. The purpose of this paper is to investigate some of their applications other than authentication.

2 Physically unclonable objects

We look at three notions of physically unclonable objects. The first type are simple unclonable objects (PUO) like fingerprint. We assume that they are verifiable, but make no assumption of how. Therefore, as in the case of fingerprint, a back-end database storing all fingerprints is usually required for the verification process. Next, we define the physically unclonable verifiable objects (PUVO) and the physically unclonable functions (PUF).

2.1 Physically unclonable verifiable object

An object ρ is PUVO if:

1. There is a public function v such that $v(\rho)$ can be computed with a public physical device V.
2. For a randomly chosen ρ, the output $v(\rho)$ is a uniformly random string of length n, where n is a security parameter of the system. This is called the verification tag of ρ.
3. For any given v_0 it is physically infeasible to produce a specific ρ_0 such that $v(\rho_0) = v_0$ with non-negligible probability.
4. It is physically infeasible to produce ρ_1 and ρ_2 such that $v(\rho_1) = v(\rho_2)$ with non-negligible probability.

The difference between PUO and PUVO is that PUVO comes with a verification process that is independent of the objects.

2.2 Physically unclonable funtions

The physically unclonable functions (PUF) is another type of physically unclonable objects. The definition of PUF s is:

1. There is a physical system S that represents the function s.
2. For any C in the domain of s, the physical system S can be used to compute $s(C)$, which can be assumed to be a random string.
3. It is physically infeasible for anyone to create S with pre-determined behavior on any input.

4. It is physically infeasible for anyone to create a pair of systems (S, S') such that S and S' have the same behavior on a pre-determined input.

5. It is computational infeasible to have a complete description of function s. This is usually because the function domain is too large.

One example of PUF is called the ALILE [5] using natural unpredictable fluctuations of resistence on a sheet of conducting material. In this case, the input is the coordinates of a point on the material and the output is the resistence value.

2.3 Relation between the physically unclonable objects

It is a trivial fact that PUVO is a subset of PUO. It is also clear that PUF is a subset of PUVO, by fixing $v(S) = s(0)$. Compared with PUVO, the PUF have additional features that are very useful for cryptographic purposes, as it behaves like a random function.

In the rest of this paper, we focus on the cryptographic applications of PUVO. For PUF, we already know that it can be used to build Oblivious Transfer (OT) [5]. In this paper, we show that OT cannot be based in PUVO only. Therefore PUF is strictly stronger than PUVO. On the other hand, Bit Commitment (BC), a weaker cryptographic construction than OT, can be based on PUVO. For PUO, it is unlikely that it can be used to build even BC.

3 Cryptography with physically unclonable objects

Recently, there are many studies of cryptography based on special tamper-proof hardware [1, 2, 3, 4]. But the study of physically unclonable objects is on another direction of hardware based cryptography with very different assumptions. Both OT and BC are usually the topics of interest, as they are known as the important building blocks for general cryptographic protocols. On the other hand, BC is weaker than OT because it can be constructed easily from OT. In [5], PUF is shown to be sufficient for building OT. In this paper, we focus on the weaker PUVO.

3.1 Oblivious transfer impossibility

In this part we see that unconditionally secure oblivious transfer is impossible using only PUVO. First, the definition of OT is:

1. Sender Alice has a pair of secret bits (ω_0, ω_1).

2. Receiver Bob has a choice σ

3. At the end of the protocol, if they are honest Bob receives ω_σ.

4. If Bob follows the protocol, a malicious Alice receives no information on σ.

5. If Alice follows the protocol, there exist some c such that a malicious Bob who attacks the protocol receives no information on ω_c, even if he is also independently given ω_{c-1}.

We assume that Alice and Bob obtains sufficient PUVO $(\rho_{A_1}, \rho_{A_2}...\rho_{A_k})$ and $(\rho_{B_1}, \rho_{B_2}...\rho_{B_j})$ respectively, for the use of the protocol. In the protocol, they communicate on a normal channel and exchange PUVO on a special physical channel. We have the following observations about the use of PUVO. Since they are unclonable, they are also distinguishable. Also, if a PUVO ρ is never sent to the other party, it serves no purpose. The owner can just create a random string to replace $v(\rho)$ whenever $v(\rho)$ is called.

When the protocol is finished, we denote by m the transcript of the communication. Now all of $(\rho_{A_1}, ...\rho_{A_k})$ have been sent to Bob and all of $(\rho_{B_1}, ...\rho_{B_j})$ have been sent to Alice. Now assume $\sigma = 0$ and Bob receives ω_0 but no information of ω_1 based on the knowledge of m, $v(\rho_{A_1}), ...v(\rho_{A_k})$, and $v(\rho_{B_1}), ...v(\rho_{B_j})$. This implies that Alice can simulate Bob and guess $\sigma = 0$, as Alice also has exactly the same information.

4 Bit commitment protocol

It is possible to use PUVO for bit commitment. A bit commitment scheme has the following definition:

1. Alice has a bit b. She wants to commit to b but does not want to reveal it. She interacts with Bob to make the commitment at the commit stage.

2. At the commit stage Bob cannot get any information of b, but he is sure that Alice is committed to a bit.

3. At the reveal stage, Alice shows b and some proofs that it is really the original committed bit.

Bit commitment based on PUVO:

1. Alice creates PUVO ρ and obtains $v(\rho)$.

2. Alice sets x to be the first bit of $v(\rho)$, and sets y to be the rest it.

3. Alice sends Bob y and $x \oplus b$ as the commitment.

4. At the reveal stage, Alice sends the physical object ρ and bit b. Bob verifies Alice's honesty with the value of $v(\rho)$.

5 Conclusion

In the bit commitment, we do not really need ρ to be unclonable. We only require that $v(\rho)$ is random. On the other hand, the object seems to be too simple for OT to be possible, while OT is strictly stronger than BC.

References

[1] S. Goldwasser, Y.T. Kalai, and G.Y. Rothblum: One-time programs, In *Advances in Cryptology — CRYPTO '08*, LNCS 5157, pp.39–56, 2008.

[2] T. Moran and M. Naor: Basing cryptography protocols on tamper-evident seals, In *ICALP 2005*, LNCS 3580, pp.285–297, 2005.

[3] V. Goyal, Y. Ishai, A. Sahai, R. Venkatesan, and A. Wadia: Founding cryptography on tamper-proof hardware tokens, In *TCC 2010*, LNCS 5978, pp.308–326, 2010.

[4] V. Kolesnikov: Truly efficient oblivious transfer using resettable tamper-proof tokens, In *TCC 2010*, LNCS 5978, pp.327–342, 2010.

[5] U. Rührmair: Oblivious transfer based on physical unclonable functions, In *Proc. TRUST 2010*, LNCS 6101, pp.430–440, 2010.