Psychology-based Cryptology: Past Present and Future

Yvo Desmedt
The University of Texas at Dallas
USA

December 4, 2012

1. A PARALLEL

In unconditionally secure cryptography we proof security assuming we can privately extract random from nature.

In computational complexity we proof security assuming some computational problem is hard.

In quantum cryptography we assume correctness of the laws of quantum physics.

This topic is now studied too by people in physics.

In psychology-based cryptography we assume correctness of

psychology.

So, one could expect that information security will be studied by psychologist.

2. IMPACT OF THE PARALLEL

Need to know key research results from psychology, e.g.,

what is observed consciously or not, e.g., when observing a picture (e.g., with an optical illusion), dependents heavily whether one is male or female.

This may give rise to gender-based cryptography.

Other ideas:

- fear is a well known pedagogical tool (see e.g., Willis, Rousová, etc.). In cryptography that may lead to:

  fear-based cryptography.

- Erasing memory, in particular is now a hot research topic (thousands

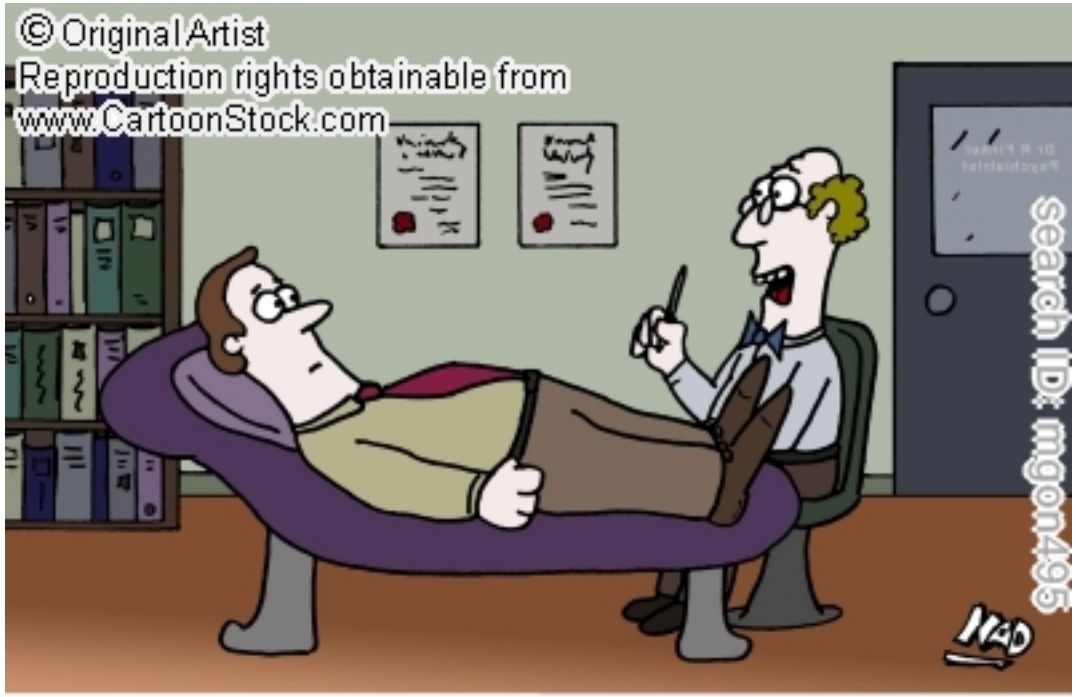
of hits on Google Scholar). Combining this with today's presentation by Patterson-Polychroniadou-Sibborn, this may lead to:

Erasable psychology-based cryptography

and

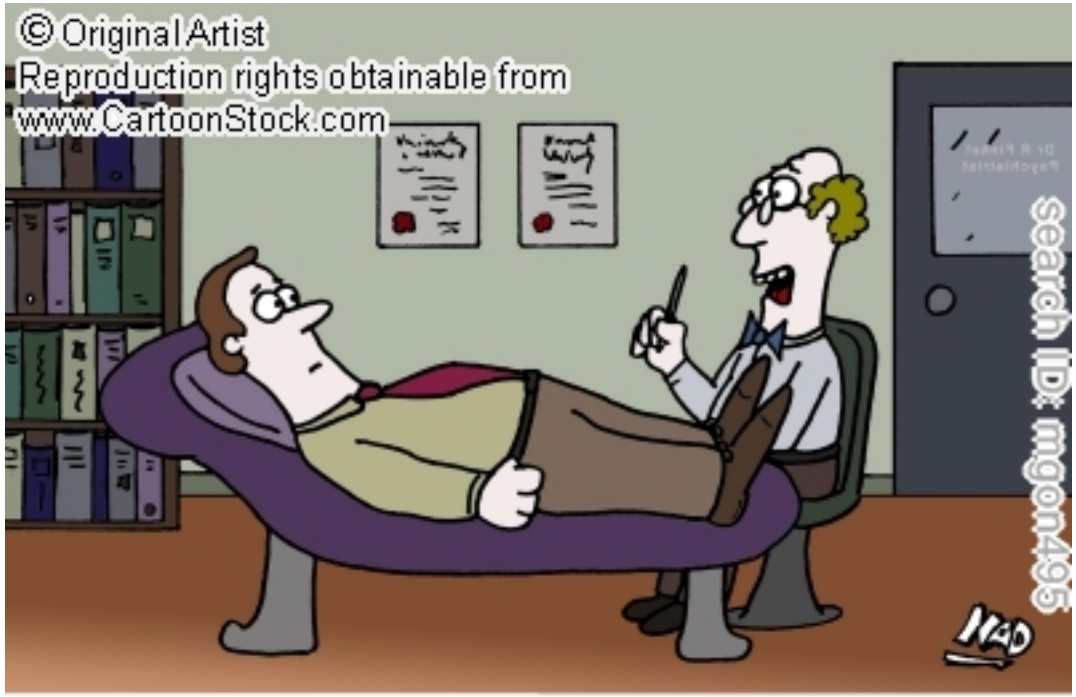
Un-erasable psychology-based cryptography

3. FUTURE



You never have headaches! What might you have done?

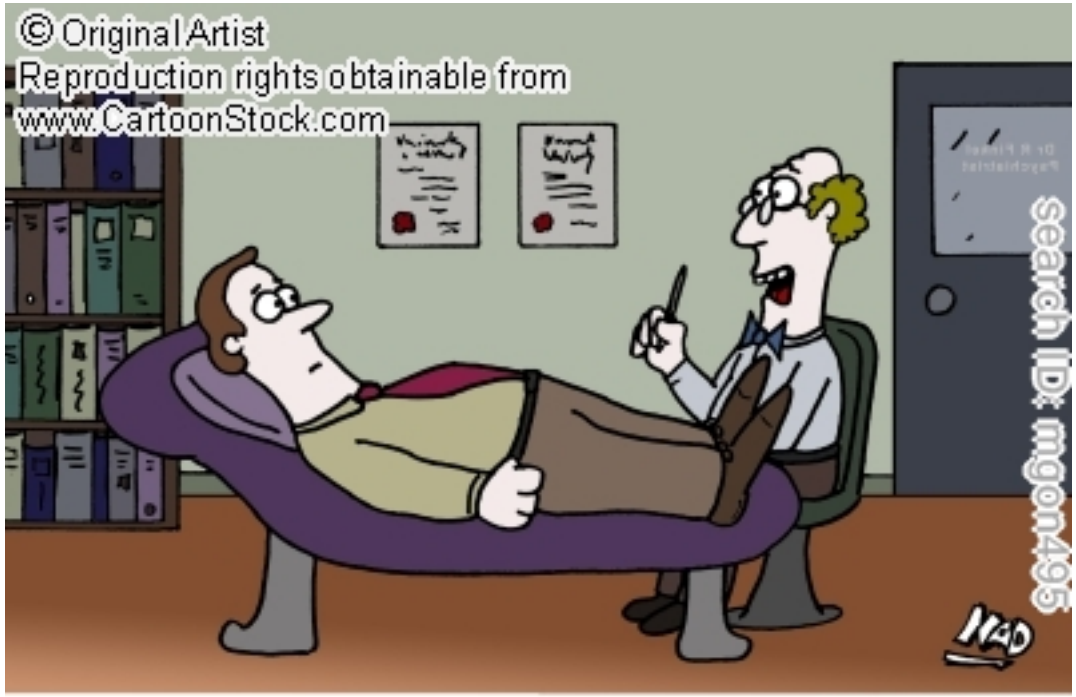
3. FUTURE



You never have headaches! What might you have done?

Patient: I do not remember!

3. FUTURE

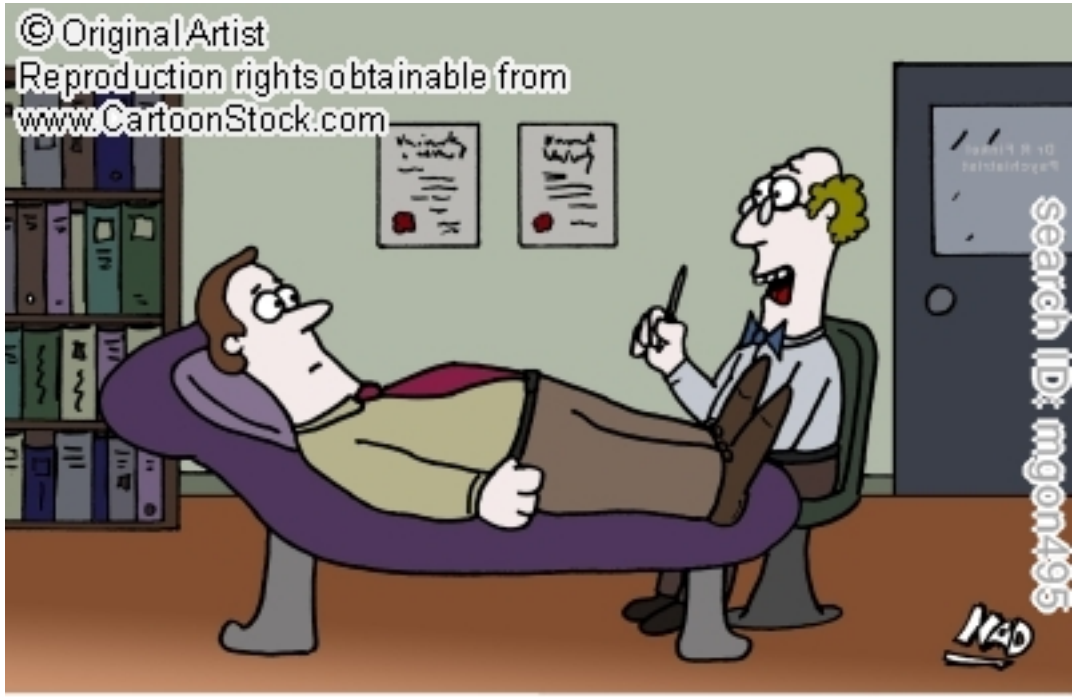


You never have headaches! What might you have done?

Patient: I do not remember!

Did you volunteer for some experiment?

3. FUTURE



You never have headaches! What might you have done?

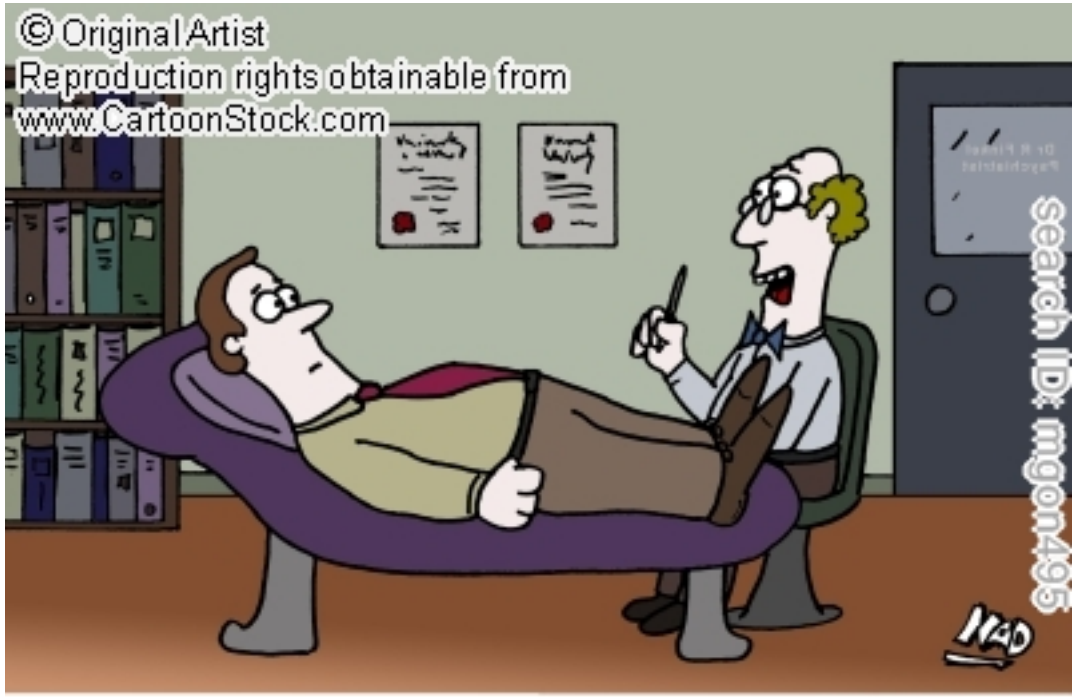
Patient: I do not remember!

Did you volunteer for some experiment?

Patient: Now I remember:

I learned a secure lattice-based secret key.

3. FUTURE



You never have headaches! What might you have done?

Patient: I do not remember!

Did you volunteer for some experiment?

Patient: Now I remember:

I learned a secure lattice-based secret key.

Isn't this thousands of bits, no surprise you have a headache!

4. IMPACT

What is the health impact of psychology-based cryptography?

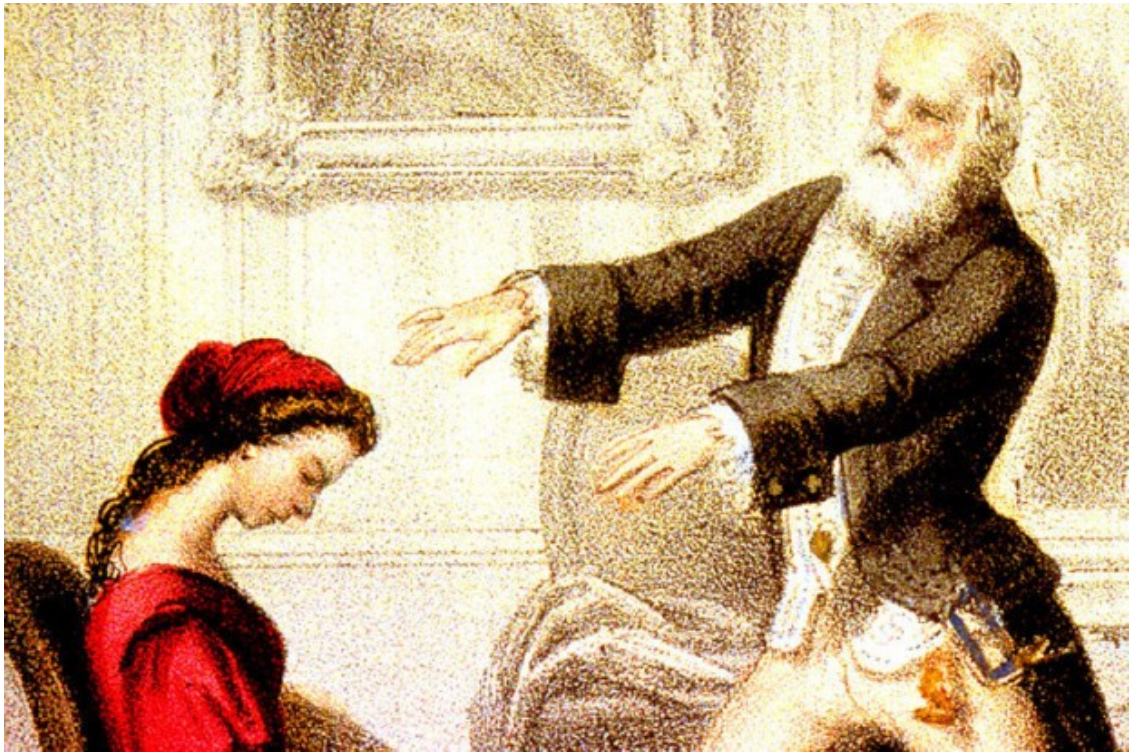
4. IMPACT

What is the health impact of psychology-based cryptography?

So, now instead of seeing NIST standards for cryptography, we will see:

FDA standards

5. NEW CRYPTANALYTIC TECHNIQUES



Although hypnoses was regarded as a dark art, practised at state fairs and the like, today it is a serious psychological tool.

It allows to block or enhance part of the memory!

Question (serious:) is psychology-based password secure against hypnotic attack?

6. PAST

Earlier work in cryptography using the brain:

Y. G. Desmedt and S. Hou and J.-J. Quisquater

Cerebral Cryptography

Information Hiding, 1998