Is Theory of Crypto good for anything in Practice?

Ivan Damgård

Århus University

What this talk is about

Not about discussing whether crypto is useful for anything at all in practice.

But about the differences between how practitioners and theoreticians in crypto think.

– Is the difference as large as some people say?

- Must there be a difference?

Design of systems using cryptography is hard

Countless examples where it went wrong in practice:

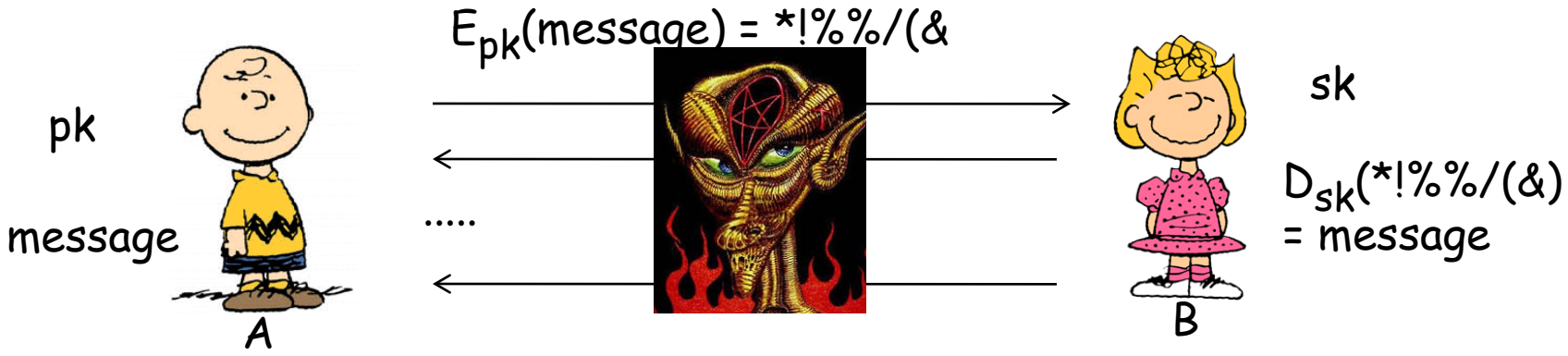
- GSM encryption
- PKCS#1
- WiFi encryption

Why?

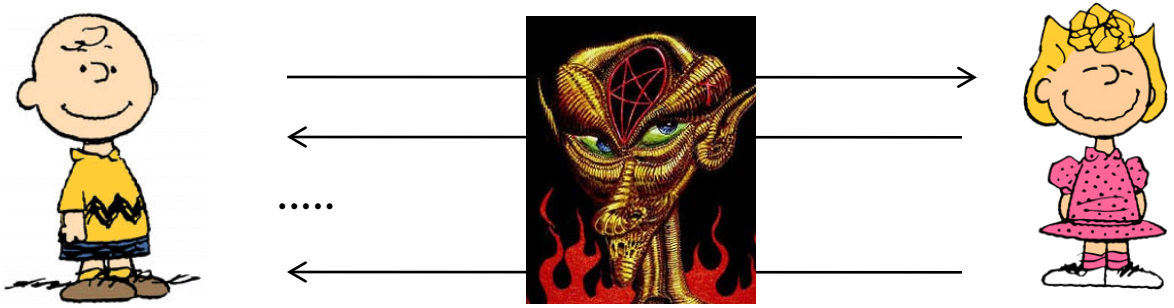
- sometimes, simple lack of expertise -- but also more fundamental problems:
- designers make designs based on the attacks they can think of – even experts often fail of think of all relevant attacks.
- system may be reasonable in the context it was designed for, but real systems are often migrated to completely new cenvironments.

An example

A wants to send confidential data to B – wants to make sure that B gets the data and no adversary gets anything, even if he listens on the network and modifies messages.



Many known constructions for this, e.g., based on RSA encryption:
A sends the data encrypted under B's public key...
..and we do some confirmation to make sure the message made it to B.



Several examples known where protocol turns out to be insecure, e.g. Bleichenbacher's attack on PKCS#1. He did NOT break RSA, instead exploited a design failure in the protocol.

How do we know a concrete proposed protocol is secure?

Theoretician's answer:
Prove a theorem saying that to break the protocol, adversary must break RSA.

Concretely, a reduction saying: if you give me an efficient algorithm that breaks the protocol, I will give you an efficient algorithm that breaks RSA encryption.

Issues With Security Reductions

Not an absolute security proof: we don't know for a fact that RSA really is hard to break.

The efficiency of the reduction matters

Focus of this talk - The model matters:

We always make assumptions about what the adversary *knows* and *what he can do*.

In the example: adversary can read and modify network traffic as he wants. Has no information on player's private storage.

Security Reduction Implies an Implementation is Secure?

Suppose we have a tight security reduction to RSA for our protocol. In implementation: B's private key is stored on her PC, encrypted under password.

Attack: hack B's computer and steal the key.

So we have an insecure system even though we have a proof of security.

So theory is useless in practice?

My opinion: NO

– but there is a problem, namely the model does not cover the attack

Model assumes the adversary has no information on player's private state, and gives no guarantees if this is not true.

Models are always an abstraction of reality!

Two reasons for not giving up.

1) Even if the model does not cover all attacks, it covers some.

In the example: even if crypto cannot help to prevent stealing the key, that does not mean you can ignore attacks on network traffic.

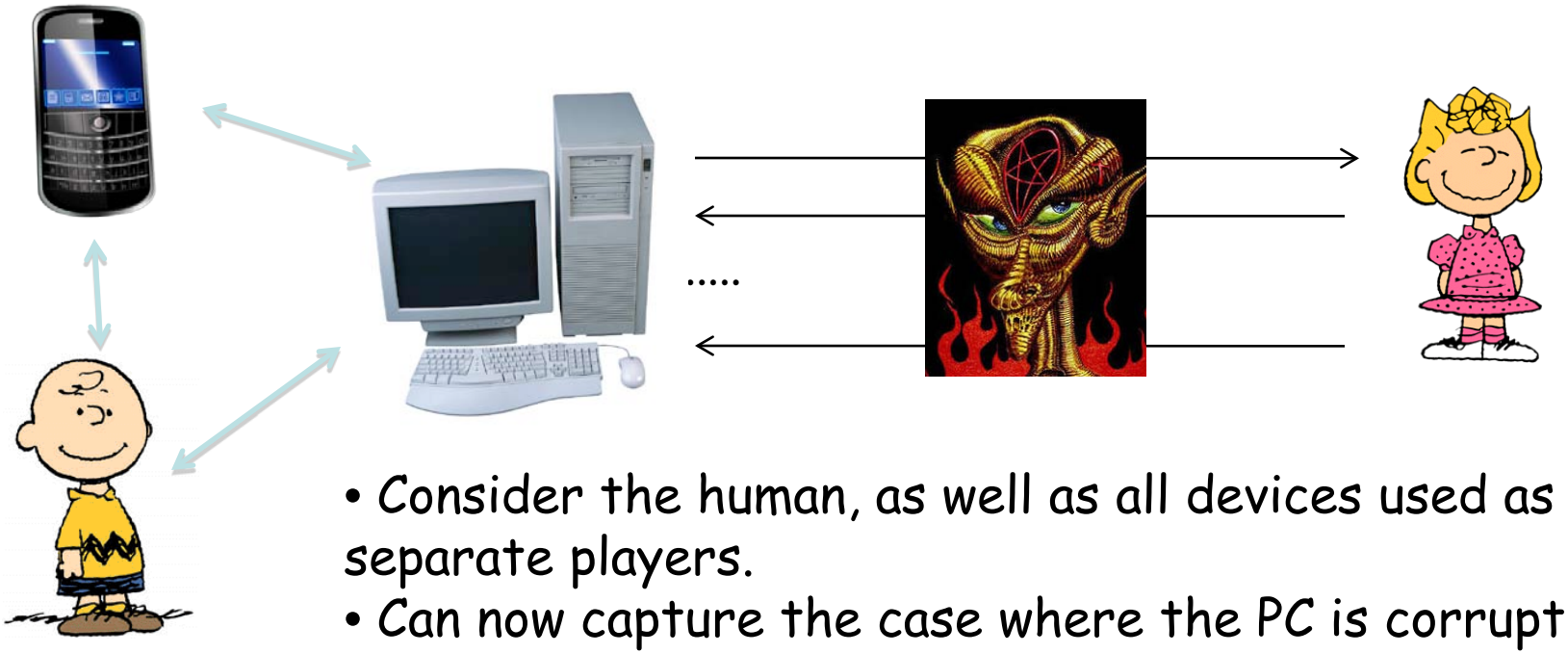
Still need crypto and a security reduction for that!

2) We can extend the model

Original model talks about "player A" and abstracts away the fact that in real life, a player is composed of a human, a PC, handheld devices etc.

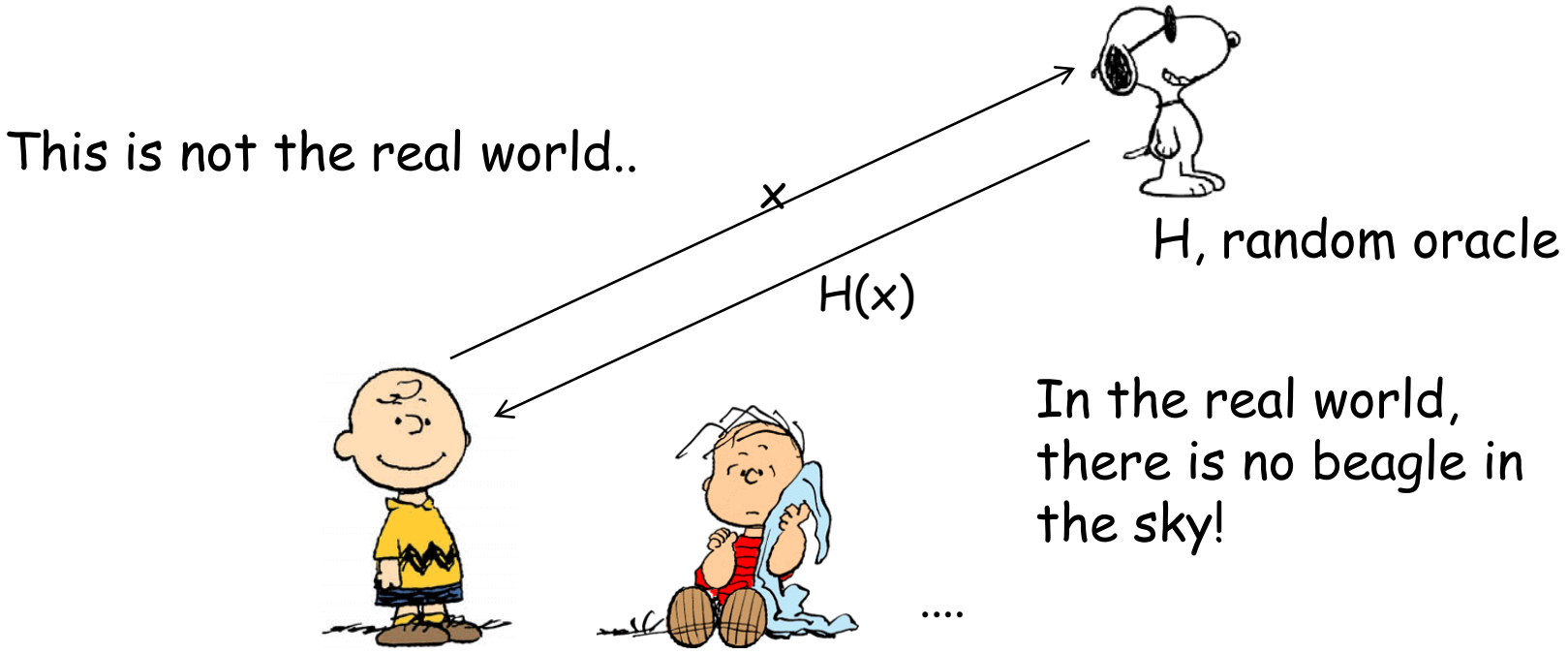
We could include this in the model..

A refined model



- Consider the human, as well as all devices used as separate players.
- Can now capture the case where the PC is corrupt (but not the human).
- Try to build and prove protocol to protect against this.
- Of course, must still rely on physical protection, but the crypto may now do more for you than before..

Another Example of Model Trouble: The Random Oracle Model.



Any player can call the oracle H with input x, and get a random response H(x) back. Any time input is x, response is H(x).
All responses are independent and random ⇒ until someone calls H with input x, no one has any information on H(x).

RO Results and Problems

In the random oracle model, can prove security of lots of efficent cryptographic constructions, Schnorr signatures, OAEP etc..

Constructions are transplanted to the real world by replacing the oracle by a concrete function, typically a cryptographic hash function.

But now, the proof is no longer valid: a concrete hash function is not a random oracle!

Interpretation

Just like other models, the RO model abstracts away some details of reality, namely details of the hash function.

Hence RO model only covers attacks that consider the hash function as a black box.

A Dialog Between Theory and Practice..

Those practitioners don't understand cryptography! How can they use schemes with no proof, or schemes that only work in the RO model?? They probably haven't even read my last paper..

Those theoreticians don't understand cryptography! How can they write papers about fancy mathematical attacks when there are real attacks to worry about??

What is that discussion really about?

Aren't these guys actually accusing each other of the same thing?

Namely: working in a model that does not cover some important attacks.

But – which attacks are important?

I don't know! we can only find out by collaborating, and keeping and open mind…

.. and avoid misconceptions such as:

"What I don't understand can't possibly be important"

Conclusions

In the substance of the matter, no reason for theoreticians and practitioners to be on opposite sides of a discussion. Of course we want as much assurance as we can get that our systems are secure!

If we want to argue about security, no way around the use of models.

No model covers all attacks, so any real system is faced with the risk of being subjected to an attack outside the model, and cannot be handled by the physical security.

To reduce this risk, theoreticians and practitioners should work together to find better models, where

better= reflects real life more accurately, so that the crypto theory can do more for you - but still simple enough so we can prove things.

Is Theoretical Crypto good for anything in Practice?

Yes!

But it could be more useful - and improving this situation can only be done by meaningful interaction between theory and practice