

# From Cryptographer's Cryptography to Engineer's Crypto

Liqun Chen  
HP Laboratories, Bristol





Graeme Proudler  
TCG Technical Committee  
Chairman

**What the heck are you  
talking about!?**



# Cryptographer's cryptography and engineer's crypto

Are they the same thing?

They ought to be the same thing, but actually they are not.

- What do I mean by cryptographer's cryptography?
  - Solutions designed by (academic) cryptographers
  - Published in cryptographic conferences and journals

Technically cool!!!
- What do I mean by engineer's crypto?
  - Solutions developed by (industrial) engineers
  - Used by banks, mobility, Internet .....

Practically useful!!!

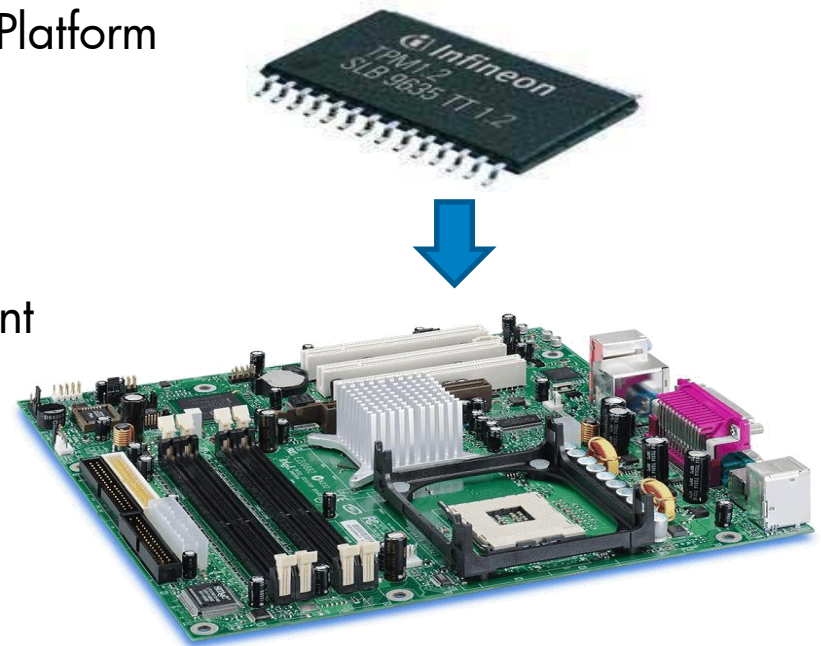
They've been getting further and further apart, but they still need to talk to each other

# The content of this talk is based on

My experiences of working with TCG



- TCG (Trusted Computing Group) is an industrial standard body and aims to provide technical building blocks for trusted computing platforms
- The main technology of TCG is TPM (Trusted Platform Module)
- TPM is a small hardware chip
- TPM spec v1.2 = ISO/IEC 11889
- The next generation TPM is under development



# TPM has become a crypto engine

Although it was designed for a different purpose

TPM supports:

- Hardware-based random number generation
- A set of cryptographic functions:
  - Hash functions
  - MAC functions
  - Key generation
  - Signing and signature verification
  - Asymmetric encryption and decryption
  - DAA (Direct Anonymous Attestation)
- Next generation TPM is intended to support algorithm agility, and might need additional cryptography such as:
  - KDF
  - Symmetric encryption and decryption
  - DH

# How to select crypto algorithms for TPM?

A lot of criteria but only a few of interest to the cryptographer

Even a crypto-agile TPM must have a restricted set of algorithms

What could affect crypto algorithm selection?:

- Regulation
  - Over the last ten years some (not all) cryptographic regulations have been relaxed
  - export/import licenses now permit some usage of symmetric algorithms
- Standardization
  - Authoritative recommendations
- Existing usage
  - Third party recommendations
- Potential market/business strategy
  - Mass-market
  - Niche-market
- Cryptographers' advice

Cryptographers are living in  
a self-created world;  
engineers are living in a  
world often beyond their  
control

# Life in these two worlds

## Target and schema

### Cryptographers

- Find a cryptographic problem
- Define a cryptographic primitive
- Define security of the primitive
  - A security model
- Design/attack a scheme
- Analyse security of the scheme
  - It is secure because it can be proved under the model, otherwise it is insecure
- Aim to create something elegant and delicate

**Pressure/satisfaction: publications**

### Engineers

- Take a real world problem
- Choose a crypto solution to solve the problem
  - Regulation
  - Standards
  - Cryptographer's recommendations
- Evaluate usage cases of the solution
  - It is secure because it survives under real world attacks
- Worry about lifetime guarantee and maintainability

**Pressure: customer satisfaction, success in the market**



# Life in these two worlds

## Keywords and languages

### Cryptographers

- Assumptions/hard problems
  - computationally infeasible
- Negligible
  - a mathematical function
- Provable security
  - proof under a model/hard problem
- Broken
  - don't achieve a claimed security level
- Practical
  - More efficient than previous works
- Oracles
  - .....

### Engineers

- Assumptions
  - attackers are not interested
- Negligible
  - no a business case for criminal
- Security evaluation
  - pass a variety of case studies
- Broken
  - affecting real usage
- Practical
  - can be manufactured
- Oracles
  - no such things

# Security proof is essential

But what cryptographers say is different from what engineers hear

**Cryptographer:** Here is our proposed scheme, blah, blah, blah

**Engineer:** Is your scheme safe?

**Cryptographer:** Yes, we have a security proof. Our scheme is secure as long as .....

**Engineer:** Good. Thank you very much

**Engineer** (to himself): She said the scheme is safe, why do I have to worry about what after “as long as” is?

**Cryptographer** (to herself): I didn't say it is completely safe!



There is a great disparity  
between cryptographer's and  
engineer's point of view  
regarding acceptable security  
levels

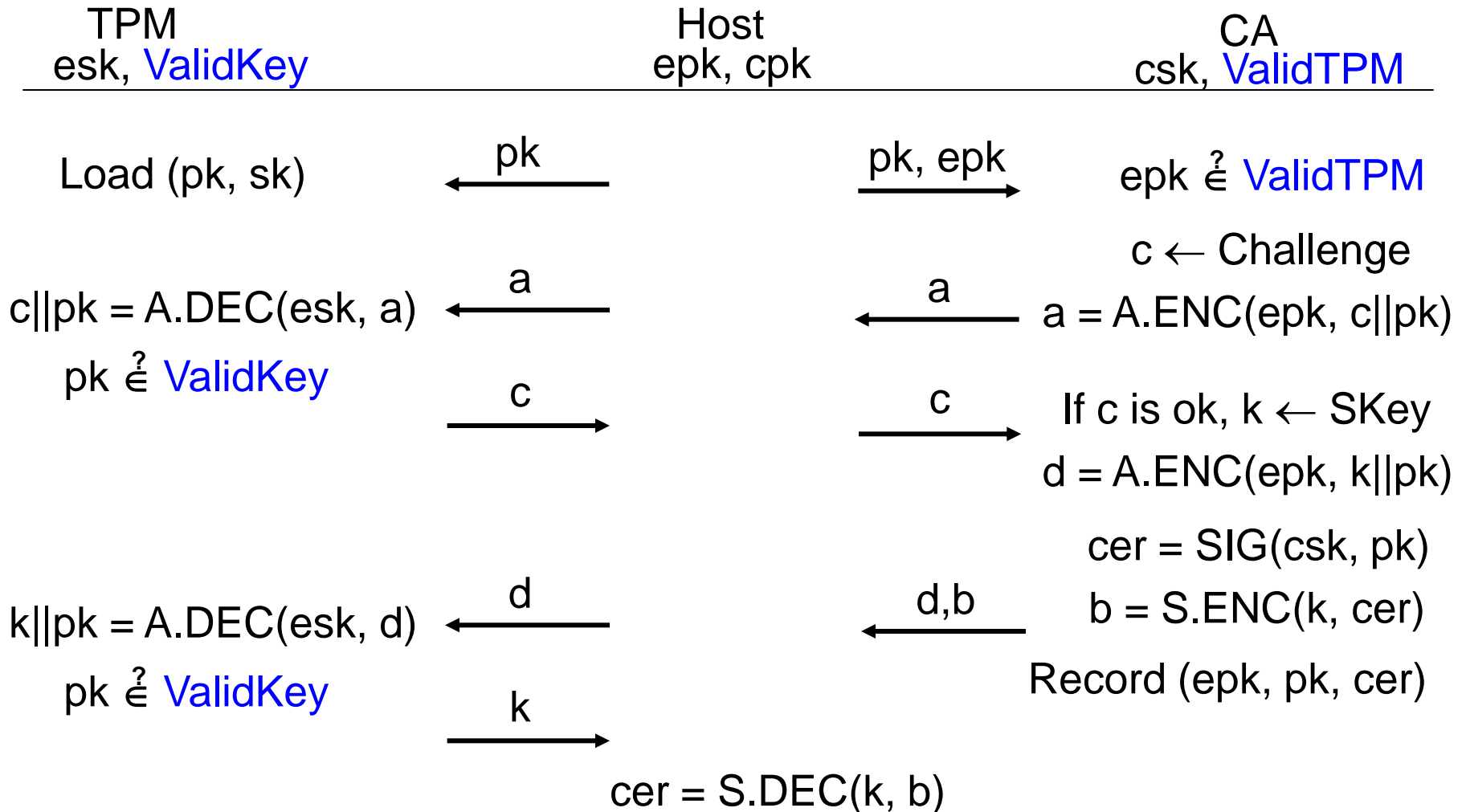
# Privacy-CA solution

Secure under a weaker security model

- This solution uses PKI to support anonymity
- It is specified in TCG TPM V1.2, ISO/IEC 11889




# The TCG Privacy-CA Protocol



# Privacy-CA solution

Secure under a weaker security model




Example 1:  
Privacy-CA  
solution

- This solution uses PKI to support anonymity
- It is specified in TCG TPM V1.2, ISO/IEC 11889
- A rigorous security analysis was done with Warinschi and Lee
- What does the proof tell us?
  - The protocol is secure only under a weak model: the adversary is not allowed to corrupt any TPM
  - From our point of view, the model is quite weak – breaking one TPM, an adversary can impersonate any other TPMs
  - We then proposed an enhanced protocol secure under a stronger model – the adversary is allowed to corrupt any TPM except one
- From TCG's point of view, its security level is acceptable
  - It works in many use cases (corporations, for example)
  - A broken TPM is a big problem only if the break is public knowledge, but if it is public knowledge it can be blacklisted

# Authorisation Values

A piece of grey area

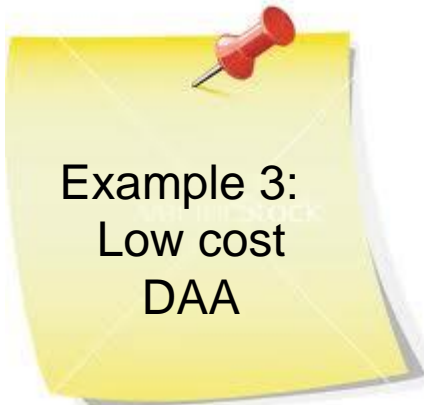


Example 2:  
Authorization  
values

- Authorization values are used as a key in communications between a TPM and user
- TCG allows users to use passwords as authorization values
- An off-line dictionary attack was discovered (joint work with Ryan)
- We also suggested a few remedies
- This contribution was well-received by TCG
- The next generation TPM is expected to include methods to handle
  - Low entropy authorisation values
  - Well known authorisation values
  - Reused authorisation values
- I agree that TCG has done its best, though it might not be satisfactory for cryptographers

# Privacy is very important, but at what cost?

DAA – the work causing Graeme's headache ...



Example 3:  
Low cost  
DAA

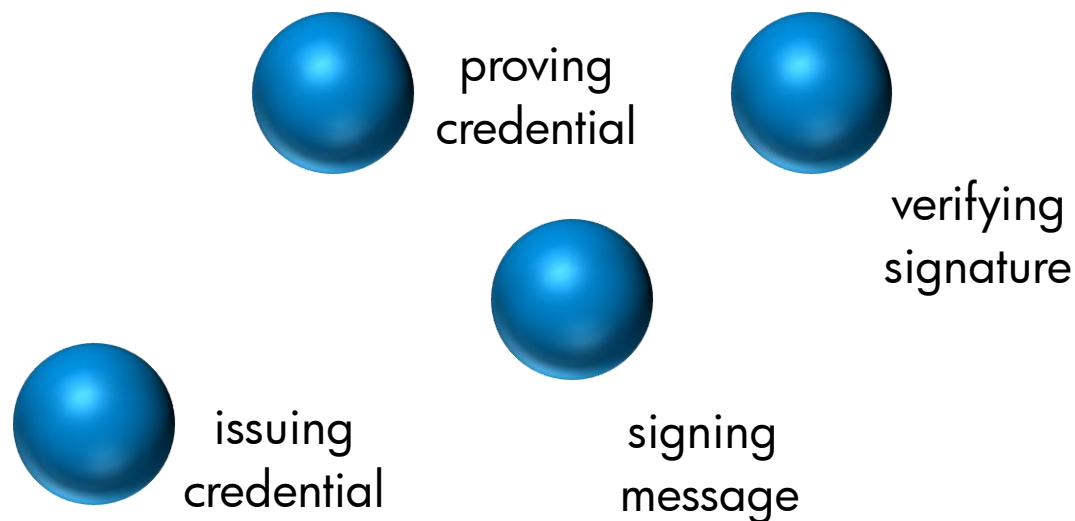
DAA is included in the TPM for consumer use cases

- TPM v1.2 has an RSA-DAA scheme (joint work with Brickell and Camenisch)
  - which is inefficient
- TCG would like to significantly reduce the cost of DAA to the TPM
  - There are a lot of academic interests in this area
- We have found several ECDAA solutions with very low cost  
(Joint work with many colleagues: Brickell, Li, Morrissey, Page, Proudler, Smart, ...)
- Some solutions might be included in the next generation TPM
- Probably no one is going to be completely happy
  - Cryptographer: it is not the best solution from our research
  - Engineer: the DAA scheme still severely distorts the TPM's architecture
    - Might be able to do better if we had more time



# A non cryptographer's crypto solution

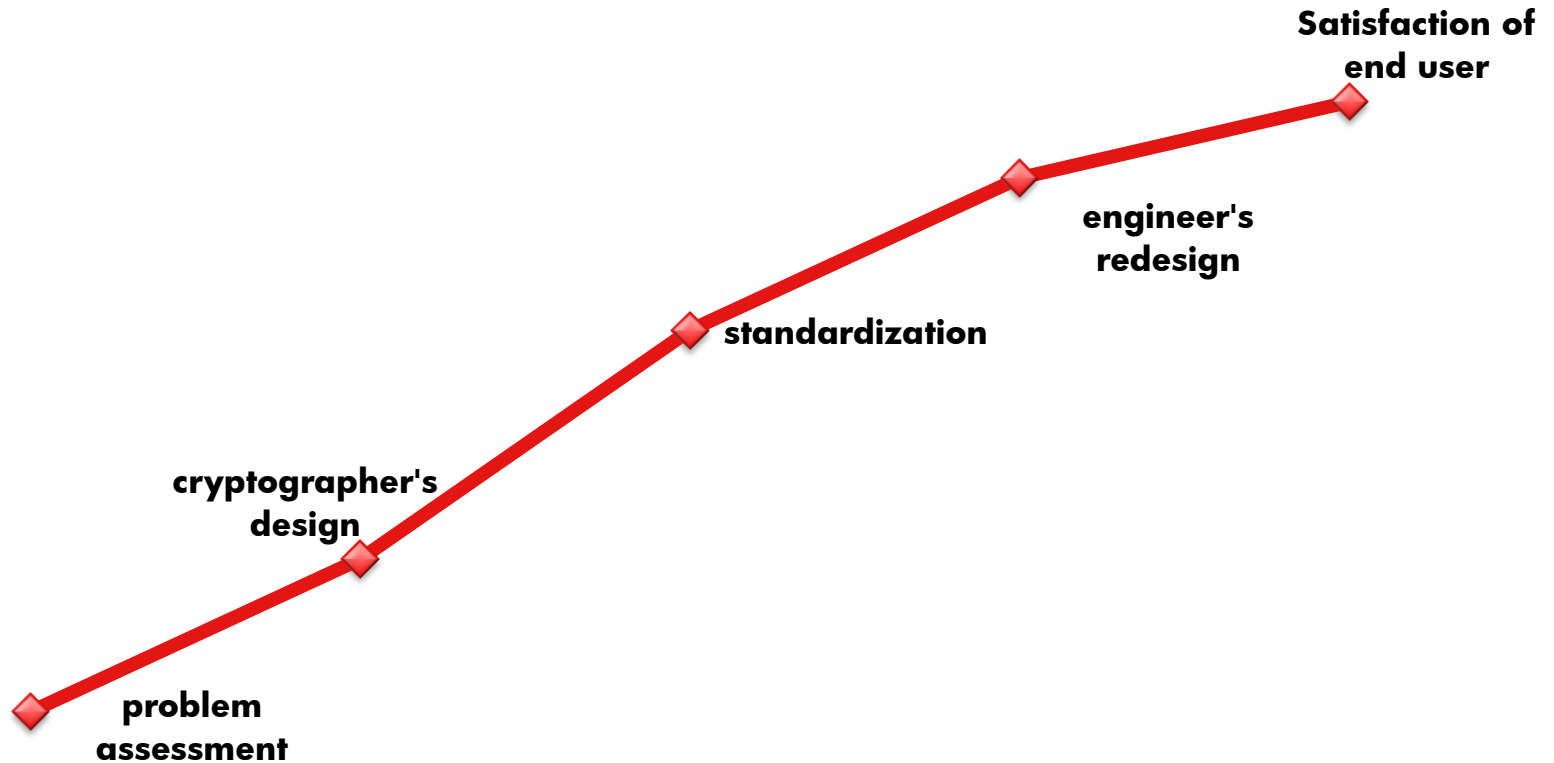
Using engineer's logic to see crypto



Graeme's observation: why prove the credential? Signing a message and verifying the signature is sufficient to carry out the "proving" function.

Cryptography is not solely the domain of cryptographers but also the domain of computer engineers

# Stages of cryptographic development



This talk covers the cryptographer's design to the engineer's redesign.

# Standards – a bridge

Between cryptographers' cryptographer and engineers' crypto

- Cryptographers and engineers have different ways of thinking and use different languages
- Standards are a bridge between them
- It is much much easier to convince engineers to use a cryptographic mechanism if it appears in some standard(s) than if published in a well-known conference or journal
- Standards help the engineer make a quick and safe decision

# Cryptographers and engineers are in the same boat

Please be nice to each other

Cryptography (crypto)

- Gives a lot of pleasure to the cryptographer
- Is just a recipe as far as the engineer is concerned
- Creates a minefield for problems if the engineer needs to tweak the cryptography

On the one hand (cryptographers talking about engineers)

- What they have done is all wrong
- Neither of them can be proved in an acceptable model
- They don't know what they are doing

On the other hand (engineers talking about cryptographers)

- Cryptographers create all the problems
- "Cryptographers are a real pain" ----- Graeme Proudler
- "The first thing we do, let's kill all the cryptographers." ----- an anonymous engineer

Can we be nicer to each other?

# Is cryptographic theory practically relevant?

One way to answer it

## Assumptions:

1. Suppose  $n$  out of  $N$  cryptographers will say YES,  $n > \epsilon$
2. Suppose  $m$  out of  $M$  engineers will say YES,  $m > \epsilon$

## Goals:

- A. I want to get my theory published
- B. I want to get my theory used

**XYZ.** The answer to the above question is YES under these two assumptions

## Proof (sketch):

- Based on Assumption 1, I have to say YES with Goal A, otherwise my submission will be rejected with a non-negligible probability
- Based on Assumption 2, I have to say YES with Goal B, otherwise my scheme will never be built
- Therefore XYZ follows since A and B are the only two goals we are concerned

□

Thank You!  
&  
Questions?

