Empowered by Innovation NEC

Real-life Cryptographic Protocols and Standardization

--How to become a good cook--

Kazue Sako

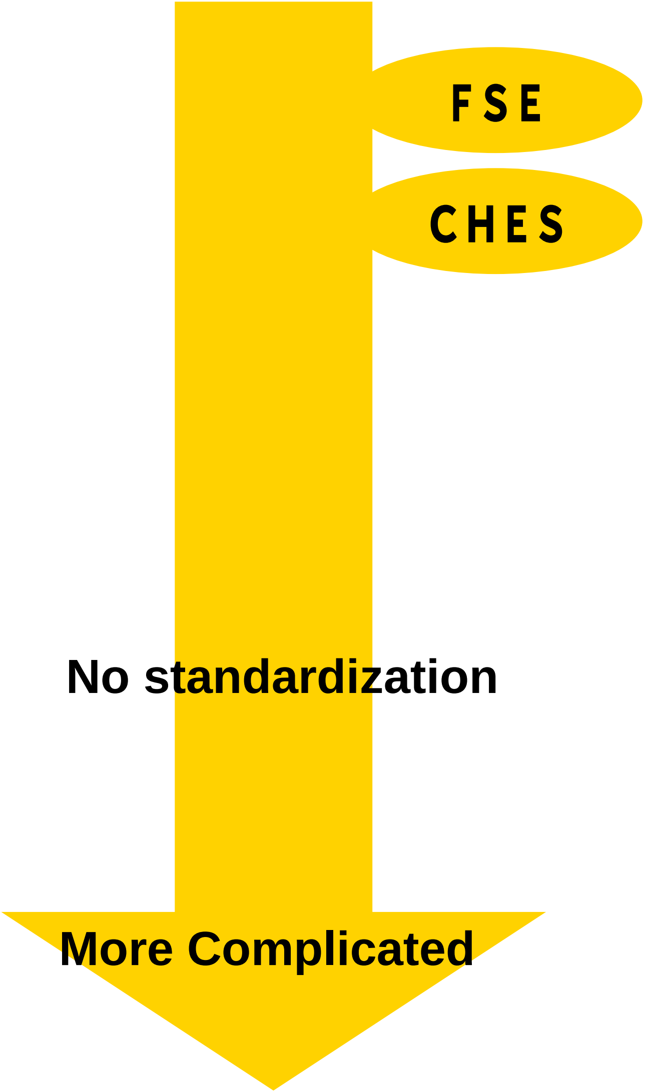
佐古　和恵

k-sako@ab.jp.nec.com

Cryptography

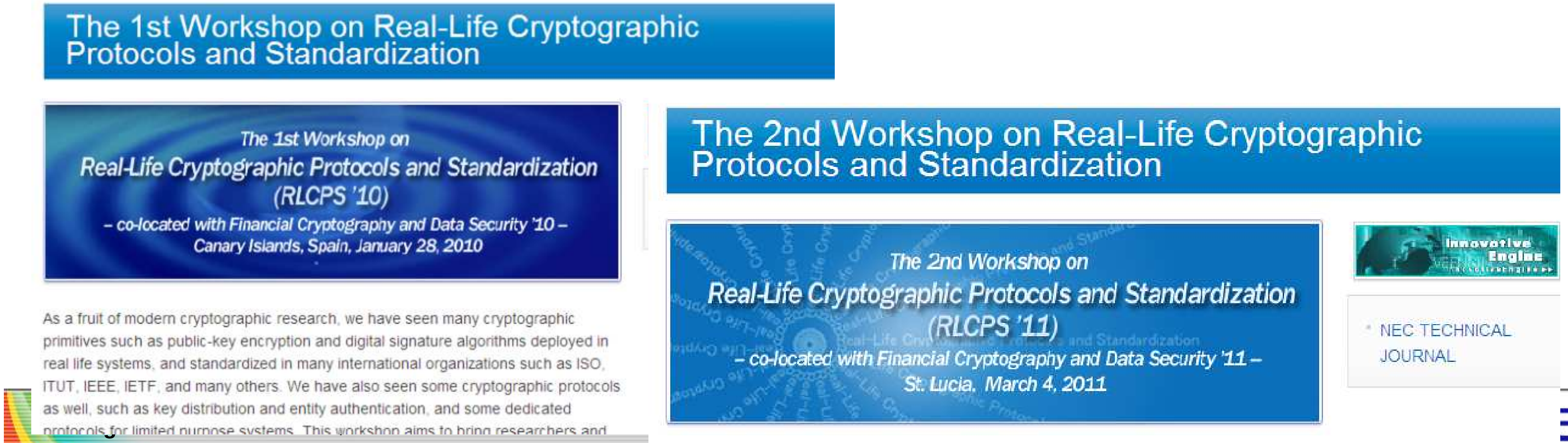
Consists of

- Primitives
  - Encryption
  - Hash function
  - Signature
- Well used protocols
  - Message authentication
  - Entity authentication
  - Key distribution/Key agreement
- Complex cryptographic protocols
  - Multi party protocols
  - Zero knowledge proofs
  - Blind signatures
  - Group signatures
  - Secret sharing schemes
  - Voting protocols



Cryptography or Security techniques are spices

- Dish is IT systems/services
- ‘Spice’ can be manufactured independent of the dish. It can be purified, grained, evaluated by itself. Several spice can be mixed together for better flavor.
- Cook must know which spice is good for his dish.
  - Too strong spice would kill the dish
- We need to learn the skill of harmonizing spice and dish
  - But there is no school that teaches us the skill
- If there is none, we’d better make one



The 1st Workshop on Real-Life Cryptographic Protocols and Standardization

The 1st Workshop on
Real-Life Cryptographic Protocols and Standardization
(RLCPS '10)
– co-located with Financial Cryptography and Data Security '10 –
Canary Islands, Spain, January 28, 2010

As a fruit of modern cryptographic research, we have seen many cryptographic primitives such as public-key encryption and digital signature algorithms deployed in real life systems, and standardized in many international organizations such as ISO, ITUT, IEEE, IETF, and many others. We have also seen some cryptographic protocols as well, such as key distribution and entity authentication, and some dedicated protocols for limited purpose systems. This workshop aims to bring researchers and

The 2nd Workshop on Real-Life Cryptographic Protocols and Standardization

The 2nd Workshop on
Real-Life Cryptographic Protocols and Standardization
(RLCPS '11)
– co-located with Financial Cryptography and Data Security '11 –
St. Lucia, March 4, 2011

- NEC TECHNICAL JOURNAL

Moti Yung’s words (RLCPS 11 Invited Talk LNCS Volume 7126)

- **‘Cryptographic Protocols: From the Abstract to the Practical to the Actual’**
  - **first level ABSTRACT: theoretical cryptography**
  - **second level PRACTICAL: designs which are contributed to systems and international standards, mechanisms ready to be implemented in hardware and software**
  - **third level ACTUAL: includes fielded cryptography as external contribution to, and part of “general (hardware/ software) engineering projects,” requiring cryptographic participation and supervision throughout the life cycle of the constructed system.**
- Restrictions of
  - Software (including OS versions, ID management of the system)
  - Hardware
  - Time to Market
  - Speed, size
  - Security Level
  - Cost
  - Operational aspects
- The art of harmonizing all these restrictions is in ‘ACTUAL’

What is missing

- Place where these security designs are discussed
  - Design criteria
  - What were the other options for the design, and why that was not chosen
- Place where failed implementations are discussed
- Documents that describe security design so that the readers can follow (without the presence of the author)
- Documents that engineers can follow and implement its own prototype correctly
- Ability to evaluate if papers on design are good enough for discussions/publications
- Methods to standardize cryptographic protocols

- 。。Permission from our customers to publish about real life systems
  - Or how to abstract it to be not too sensitive, yet still interesting

Real-Life Cryptographic Protocols and Standardization

- 1st workshop at Tenerife 2010, co-located with FC10
  - http://www.nec.com/en/global/rd/event/RLCPS10.html
- 2nd workshop at St. Lucia 2011, co-located with FC11
  - http://www.nec.com/en/global/rd/event/RLCPS11.html
- … yet to come, perhaps co-located with ACMCCS in 2013

The 1st Workshop on Real-Life Cryptographic Protocols and Standardization

The 1st Workshop on
Real-Life Cryptographic Protocols and Standardization
(RLCPS '10)
– co-located with Financial Cryptography and Data Security '10 –
Canary Islands, Spain, January 28, 2010

As a fruit of modern cryptographic research, we have seen many cryptographic primitives such as public-key encryption and digital signature algorithms deployed in real life systems, and standardized in many international organizations such as ISO, ITUT, IEEE, IETF, and many others. We have also seen some cryptographic protocols as well, such as key distribution and entity authentication, and some dedicated protocols for limited purpose systems. This workshop aims to bring researchers and

The 2nd Workshop on Real-Life Cryptographic Protocols and Standardization

The 2nd Workshop on
Real-Life Cryptographic Protocols and Standardization
(RLCPS '11)
– co-located with Financial Cryptography and Data Security '11 –
St. Lucia, March 4, 2011

- NEC TECHNICAL JOURNAL

Standardization

ISO/IEC JTC 1 SC 27: Group Signatures

- 20008-2 Anonymous Digital Signatures: Mechanisms using a group public key
    - Certificate Issuing Phase
    - Generating Group Signatures
    - Verifying Group Signatures
    - Opening
- Variation
    - Who generates Certificates? Server only or Joint with Client?
    - What is ‘group public key’? Does it include domain parameters, public key of opener, revocation status flag?
    - Does Opening include verification of signatures?
    - Possible duplicates but secure API, or compact but insecure for lazy programmer?
- We need good practices and know-hows for standardizing cryptographic protocols

Empowered by Innovation

NEC