Report on

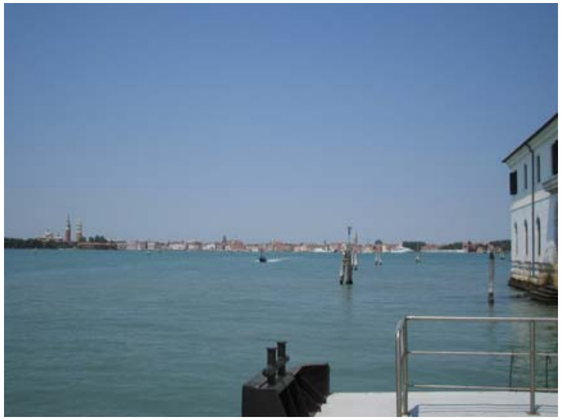
CSFW-FCC-ICALP

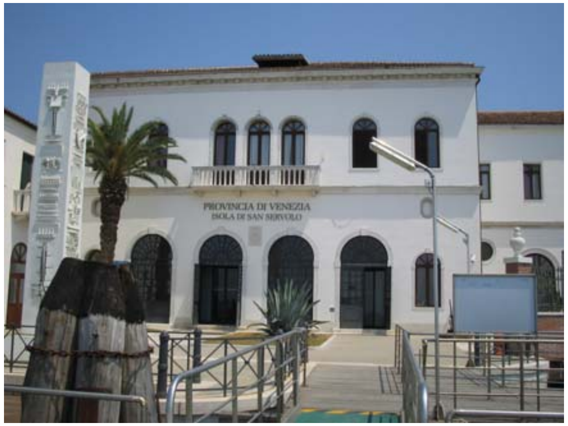
T. Araragi (NTT CS labs)　　櫟 粛之（NTT）
M. Hagiya (Tokyo University)　萩谷 昌己（東京大学）

CSFW-FCC-ICALP

2006 July: Italy - Venice - S. Servolo Island

- CSFW: 5-7 July
- FCC: 9 July
- ICALP: 10-14 July





S. Servolo Island

General of FCC

- FCC(2nd): 1st: all accepted, 2nd: 10/13 accepted

- 5 minutes talk (12 talks: advertisement, ongoing)

- panel discussion on “non-determinism”:

  Canetti, Micciancio, Mitchell, Pfitzmann, Palamidessi*, Segala*

  (*prob. concurrent system)

next meeting

- CSFW: same place, same time
- FCC: ? join with ICALP/CSFW
- ICALP: Poland

FCC

(1) Computationally Sound Secrecy Proofs by Mechanized Flow Analysis.
Backes, Laud.

symbolic foundation

(2) Computationally Sound Compositional Logic for Security Protocols.
Datta, Derek, Mitchell, Roy, Shmatikov, Turuani, Warinschi

symbolic foundation

(3) Language Design for Computationally Sound Communications Abstractions.
Adao, Fournet.

symbolic foundation

(4) Soundness of Symbolic Equivalence for Modular Exponentiation.
Lakhnech, Mazare, Warinschi.

positive result

(5) Sound and Complete Computational Interpretation of Symbolic Hashes in the Standard Model.
Garcia, van Rossum.

positive result

(6) Soundness Limits of Dolev-Yao Models.
Backes, Pfitzmann, Waidner.

negative result

(7) Using Task-Structured Probabilistic I/O Automata to Analyze Cryptographic Protocols.
Canetti, Cheung, Kaynar, Liskov, Lynch, Pereira, Segala.

real/ideal foundation

(8) Games and the Impossibility of Realizable Ideal Functionality.
Backes, Datta, Derek, Mitchell, Ramanathan, Scedrov.

negative result

(9) An example of proving UC-realization with formal methods.
Andova, Gjøsteen, Kråkmo, Mjølsnes, Radomirović.

symbolic foudation

(1) Computationally Sound Secrecy Proofs by Mechanized Flow Analysis.

Backes, Laud.

symbolic

- tool based on BPW
- transform a protocol to a set of constraint
- abstract analysis deduce cryptographic secrecy?

related papers

Backes-ERORICS-2004, Backes-Pfitzmann-FST-TCS-2003

(2) Computationally Sound Compositional Logic for Security Protocols.
Datta, Derek, Mitchell, Roy, Shmatikov, Turuani, Warinschi.

symbolic

the state of art of
protocol composition logic by Mitchell et al

- history
- DH predicate and axioms for key exchange
- application: ISO-9798-3 key exchange
  Kerberos V5

(3) Language Design for Computationally Sound Communications Abstractions.
Adao, Fournet.

symbolic

- a language based on process algebra
- no cryptographic primitive (as spi-cal)
  (abstract secure primitives on securacy, authentication)

presented in ICALP 2006

complicated (by Mitchell)

(4) Soundness of Symbolic Equivalence for Modular Exponentiation.
Lakhnech, Mazare, Warinschi.

positive

Extension of Abadi-Rogaway logic
(m $\cong$ n in DY -> IND of m and n : encryption scheme: type0)

$\Downarrow$

(...................................... : encryption scheme: IND-CPA
exponentiation : DDDH)

- DynamicDDH: (1) exp(x1x2-x2x3) (2) (3) neg dist from random
- slight modification of DY model
  - adv's knowledge
  - pattern
  - renaming (linear dep pres bij)

application: Burmester-Desmedt protocol

related work: D. Boneh?

(5) Sound and Complete Computational Interpretation of Symbolic Hashes in the Standard Model. Garcia, van Rossum.

positive

Extension of Abadi-Rogaway logic
(m $\cong$ n in DY -> IND of m and n : encryption scheme: type0)

⇩

(..................................... : encryption scheme: type
hash: Canetti's oracle hash)

- Canetti's oracle hash (1) $P[D_\eta (H(1^\eta,x)=1)] - P[D_\eta (H(1^\eta,y)=1)] < 1/p(\eta)$
  (2) collision resistance
- slight modification of DY model
  - pattern

- sound & complete

(6) Soundness Limits of Dolev-Yao Models.
Backes, Pfitzmann, Waidner

negative

(1) protocols with hash prevent sound DY-model in BPW
(otherwise DY-model reverses hash)

(2) protocols with XOR prevent sound DY-model in BPW
(otherwise DY-model realizes signature creation/verif)
- restrict protocols allows sound DY-model

Related papers:

(1) "Limits of the Cryptographic Realization of Dolev-Yao-style XOR"
Backes, Pfitzmann (2005)

(2) "Limits of the Reactive Simulatability/UC of Dolev-Yao Models with Hashes"
Backes, Pfitzmann, Waidner (2006)

(7) Using Task-Structured Probabilistic I/O Automata to Analyze Cryptographic Protocols. Canetti, Cheung, Kaynar, Liskov, Lynch, Pereira, Segala.

real/ideal

extension of I/O Automata

- execution -> probabilistic execution [task scheduler]
- time bound (polynomial)

- prob. ver. of implementation (trace inclusion)
- prob. ver of simulation relation

⇩

accurate formalization of
IND between real and ideal in UC framework

Shoup's sequence of games

(8) Games and the Impossibility of Realizable Ideal Functionality.

Backes, Datta, Derek, Mitchell, Ramanathan, Scedrov.

negative

Scedrov→Mitchell→Derek→Backes

question: game description => real-ideal description
answer: generally negative

examples:
- multiparty coin-tossing
- bit-commitment (explained)
- shared random sequences

proof:
- create a game using ideal functionality.
- ideal realization -> information theoretic contradiction
  the game

(9) An example of proving UC-realization with formal methods.

Andova, Gjøsteen, Kråkmo, Mjølsnes, Radomirović.

Proving universally composable theorem of
(F_{PKI}, F_{SC})- hybird system for F_{SM}
by formal method

similar approach with Mitchell et al?

CSFW

many talks on foundation of access control/ authorization /policy

(1) *Cryptographically Sound Theorem Proving:* Mukhamedov, Ryan

- flaw against verified protocol
- manual proof -> fix and model check -> flaw in umbd num of participants

(2) Refuting Claimed Security Proofs for Tripartite Key Exchange with Model Checker: Choo

- finding new flaws
- tools based on AI planning system

(3) *Cryptographically Sound Theorem Proving*: Sprenger, Basin, BPW

- verification tool for BPW
- transform BPW representation for Isabelle