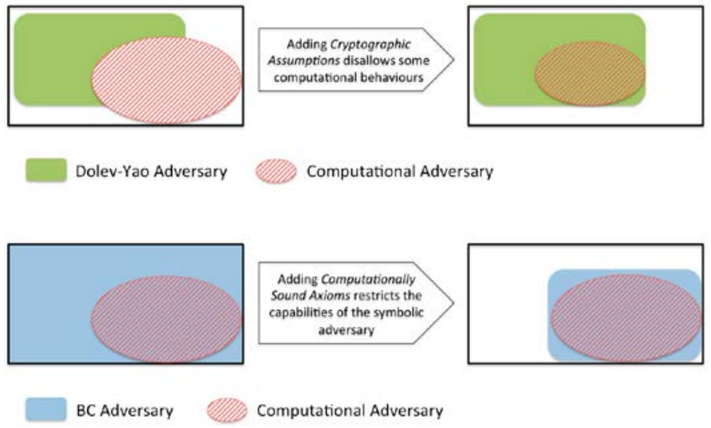
ComFormCrypt

Computational Semantics of Formal Methods in Cryptography

Security protocols have been mostly studied in what is called the symbolic model. In this model some abstractions are performed and in particular, cryptography is assumed to be perfect. However, we all know that in reality cryptography is far from being perfect and vulnerabilities that explore this fact are revealed more often than not. Thus, analysing the relationship between symbolic and real (computational) cryptography is essential as it can provide a clearer picture of how relevant symbolic proofs are to reality.


Adding *Cryptographic Assumptions* disallows some computational behaviours
Dolev-Yao Adversary
Computational Adversary
Adding *Computationally Sound Axioms* restricts the capabilities of the symbolic adversary
BC Adversary
Computational Adversary

Main Project Team	
Pedro Adão	**SQI-Lx**
Gergely Bana (INRIA-Paris)	SQI-Lx
Carlos Caleiro	SQI-Lx
Paulo Mateus	SQI-Lx
Pedro Baltazar	SQI-Lx
David Henriques	SQI-Lx
Andreia Mordido	SQI-Lx
Filipe Casal	SQI-Lx
Funding Agencies	
Fundação para a Ciência e Tecnologia **PTPC/EIA-CCO/113033/2009**	**72,332€**
Start Date	01/02/2011
Ending Date	31/07/2014
Indicators	
Journal Papers	6
Conference Papers	14
Concluded MSc	3

Two Main Publications

P. Adão, P. Mateus, L. Viganò, **Protocol Insecurity with a Finite Number of Sessions and a Cost-Sensitive Guessing Intruder is NP-Complete**, Theoretical Computer Science, Vol. 538, No. 1, pp. 2 - 15, June, 2014.

G. Bana, H. Comon-Lundh, **A Computationally Complete Symbolic Attacker for Equivalence Properties,** ACM Conference on Computer and Communications Security, 2014 (CCS), 609 - 620.

PROJECT WEBPAGE URL
https://www.math.tecnico.ulisboa.pt/~padao/projects/ComFormCrypt/

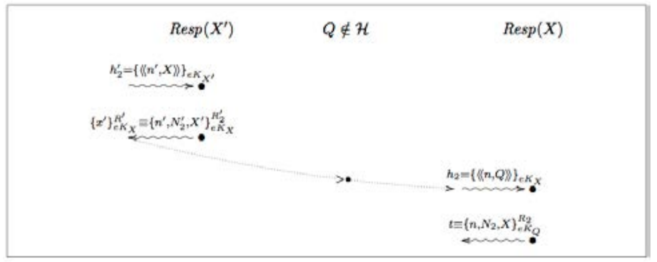

$Resp(X')$
$Q \notin \mathcal{H}$
$Resp(X)$
$h'_2=\{\langle\langle n',X\rangle\rangle\}_{eK_{X'}}$
$\{x'\}^{R'}_{eK_X}\equiv\{n',N'_2,X'\}^{R'_2}_{eK_X}$
$h_2=\{\langle\langle n,Q\rangle\rangle\}_{eK_X}$
$t\equiv\{n,N_2,X\}^{R_2}_{eK_Q}$

Fig. 1 Attack to the NSL protocol when the answer of a responder X' is used to initiate a new session with responder X.

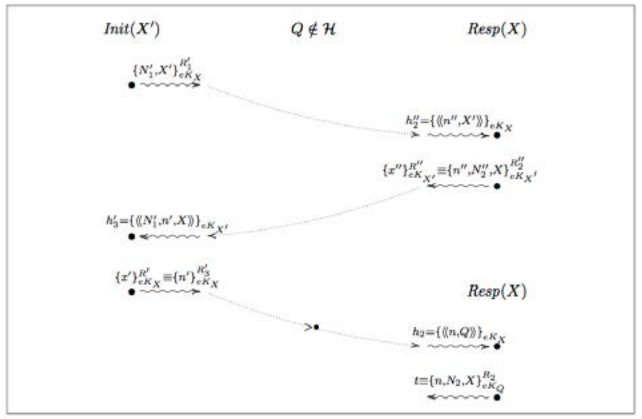

$Init(X')$
$Q \notin \mathcal{H}$
$Resp(X)$
$\{N'_1,X'\}^{R'_1}_{eK_X}$
$h''_2=\{\langle\langle n'',X'\rangle\rangle\}_{eK_X}$
$\{x''\}^{R''}_{eK_{X'}}\equiv\{n'',N''_2,X\}^{R''_2}_{eK_{X'}}$
$h'_3=\{\langle\langle N'_1,n',X\rangle\rangle\}_{eK_{X'}}$
$\{x'\}^{R'}_{eK_X}\equiv\{n'\}^{R'_3}_{eK_X}$
$Resp(X)$
$h_2=\{\langle\langle n,Q\rangle\rangle\}_{eK_X}$
$t\equiv\{n,N_2,X\}^{R_2}_{eK_Q}$

Fig. 2 Attack to the NSL protocol when the last message of a correctly executed protocol between X' and X is used to initiate a new protocol with responder X.

GENERAL MOTIVATION AND OBJECTIVES

During a cryptographic protocol, participants exchange messages using some cryptographic primitive such as encryption or digital signature. An attacker to a protocol may try to break the encryption itself, or it may combine the several messages that were sent around, this way revealing some partial information about what was encrypted, even without actually breaking the code; also, the attacker may corrupt or deceive participants in a protocol. The aim of cryptography is to provide mathematical models for the cryptographic primitives, for the protocols, for the attackers, come up with new cryptographic schemes, or analyze whether a given protocol satisfies its desired properties. Modern encryptions and digital signatures are probabilistic and, since computers have limited computing powers, the notion of efficient computability is a key to cryptographic analysis. Hence, the most natural, closest-to-reality descriptions of protocols use complexity and probability theory; this model is called "computational". There is however another model, called "symbolic" that uses formal logic to describe the behavior of protocols and adversaries, and that ignores probabilistic behavior. Both models have advantages and disadvantages. Briefly, the advantage of the former is that it is closer to reality than the latter, however more difficult to handle and conduct proofs. One advantage of the latter is that proofs can be automated, while in the former they have to be done manually.

It is therefore an important question, how relevant the results obtained using automated formal methods are to reality, that is, to the computational world. Does security proven via symbolic models provide security in the real computational world (soundness), and does the existence of a symbolic attack imply an attack in real life (completeness)? Furthermore, if the symbolic descriptions currently used are unsatisfactory, then how should we modify them to provide better description of the computational world?

CHALLENGE

The goal of the ComFormCrypt project was to investigate the relationship between these two worlds, i.e., given the proof of correctness of a security protocol, how confident can one be about the security of a concrete implementation of this protocol? In which conditions does a protocol proved secure in the symbolic model remains computationally secure when cryptographic primitives are instantiated?

WORK DESCRIPTION AND ACHIEVEMENTS

In the ComFormCrypt project we were able to propose a (computationally sound) logical system that allows the symbolic adversary to perform similar (malicious) actions as the computational adversary. We were able to prove a general soundness theorem for this logic in the case of trace properties, and soundness of an axiom expressing secrecy of an IND-CCA encryption.

We extended this framework with axioms for Secrecy and Non-Malleability for both public and shared-key encryption expanded it to handle the case of key distribution defining predicates that express key usability, and applied it to known protocols such as the NSL, sNS, and Otway-Rees protocols. To finalise the project, we extended the framework to also consider equivalence properties.

We also considered the case of systems that may leak partial information at a given cost, or that can be attacked with certain probabilities, and how one could compute these probabilities. We showed that the quantified intruder deduction problem is NP complete, and we were able to find attacks and estimate their success probabilities, which is beyond existing symbolic methods.

We also developed FAST, an efficient decision procedure for message deducibility and static equivalence under subterm-convergent equational theories that has a better asymptotic complexity than the other algorithms implemented by existing tools for the same task; and a prototype implementation to model non-trivial properties of RSA encryption and automatically estimate the probability of off-line guessing attacks on the EKE protocol.