UNIVERSITY OF TARTU
FACULTY OF MATHEMATICS AND COMPUTER SCIENCE
Institute of Computer Science

Tiina Turban

Type Inference for a Cryptographic Protocol Prover Tool

Bachelor's Thesis (6 ECTS)

Supervisor: Liina Kamm, MSc
Supervisor: Sven Laur, PhD

Author: .... "....." 2012

Supervisor: .... "....." 2012
Supervisor: .... "....." 2012

Allowed to defence
Professor: .... "....." 2012

Tartu 2012

Contents

1 Introduction

What is it in simple terms (title)?

Why should anyone care?

What was my contribution?

What you are doing in each section (a sentence or two per section)

Tip: if it's hard for you to start writing, then try to split it to smaller parts, e.g. if the title is "Type Inference for a Cryptographic Protocol Prover Tool" then the "What is it" can be divided into "what is type inference", "what is cryptographic protocol" and "what is the prover tool". These three can also be split to smaller parts etc.

2 Title of Section 2

Short description of what this section is about

2.1 Title of Subsection 1

Some text...

2.1.1 Title of Subsubsection 1

Some text...

2.1.2 Title of Subsubsection 2

Some text...

2.2 Title of Subsection 2

Rule: If you divide the text into subsections (or subsubsections) then there has to be at least two of them, otherwise do not create any.

Tip: You can also use paragraphs, e.g.

Type rules for integers. Some text ...

Type rules for rational numbers. Some text here too...

2.3 How to use references

Tip: Use label and ref to make sure you are always referring to the the correct figure, table or section even if you rearrange them (see Section 2.3).

Example: Game-based proving is a way to analyse security of a cryptographic protocol [BR04, Sho04]. There are automatic provers, such as CertiCrypt [BGZ09] and ProVerif [Bla].

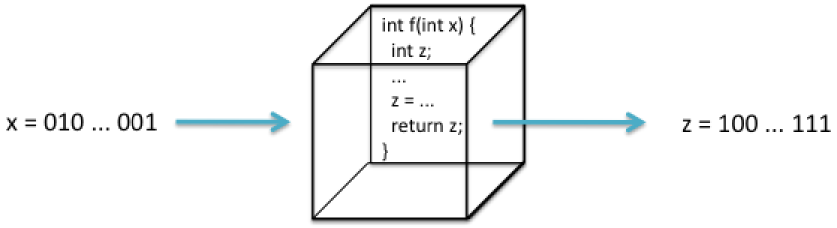
Tip: Jabref (`http://jabref.sourceforge.net/`) might be a helpful tool to use.

Tip: Many articles have BibTeX reference ready and you can just copy-paste.

3 How to add figures and pictures to your thesis

Here are a few examples of how to add figures or pictures to your thesis (see Figures 1, 2, 3).

Rule: All the figures, tables and extras in the thesis have to be referred to somewhere in the text.



```
int f(int x) {
  int z;
  ...
  z = ...
  return z;
}
```

Figure 1: The title of the Figure

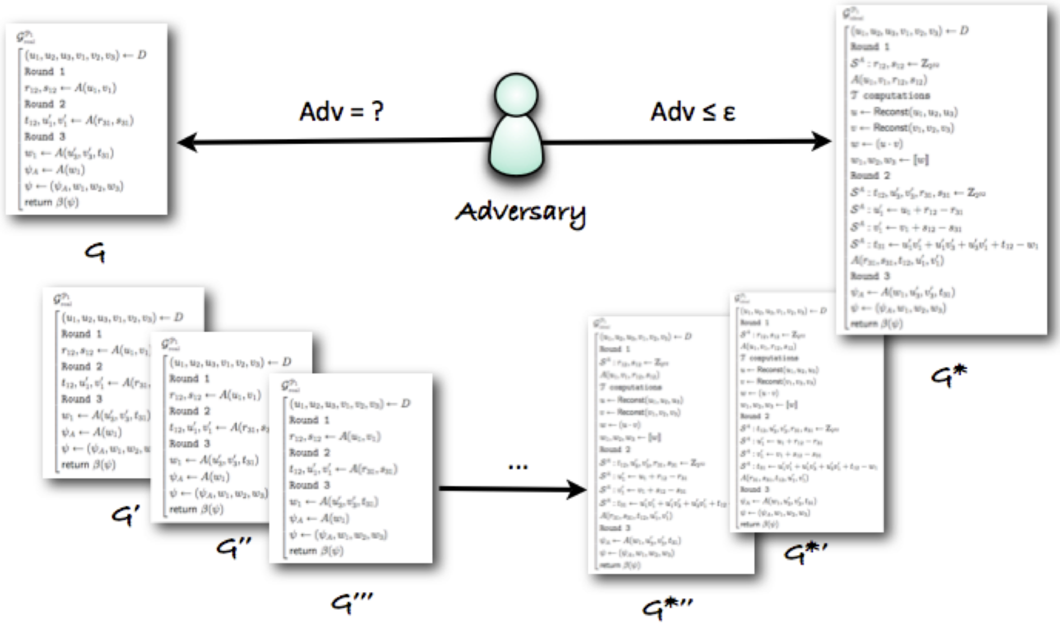
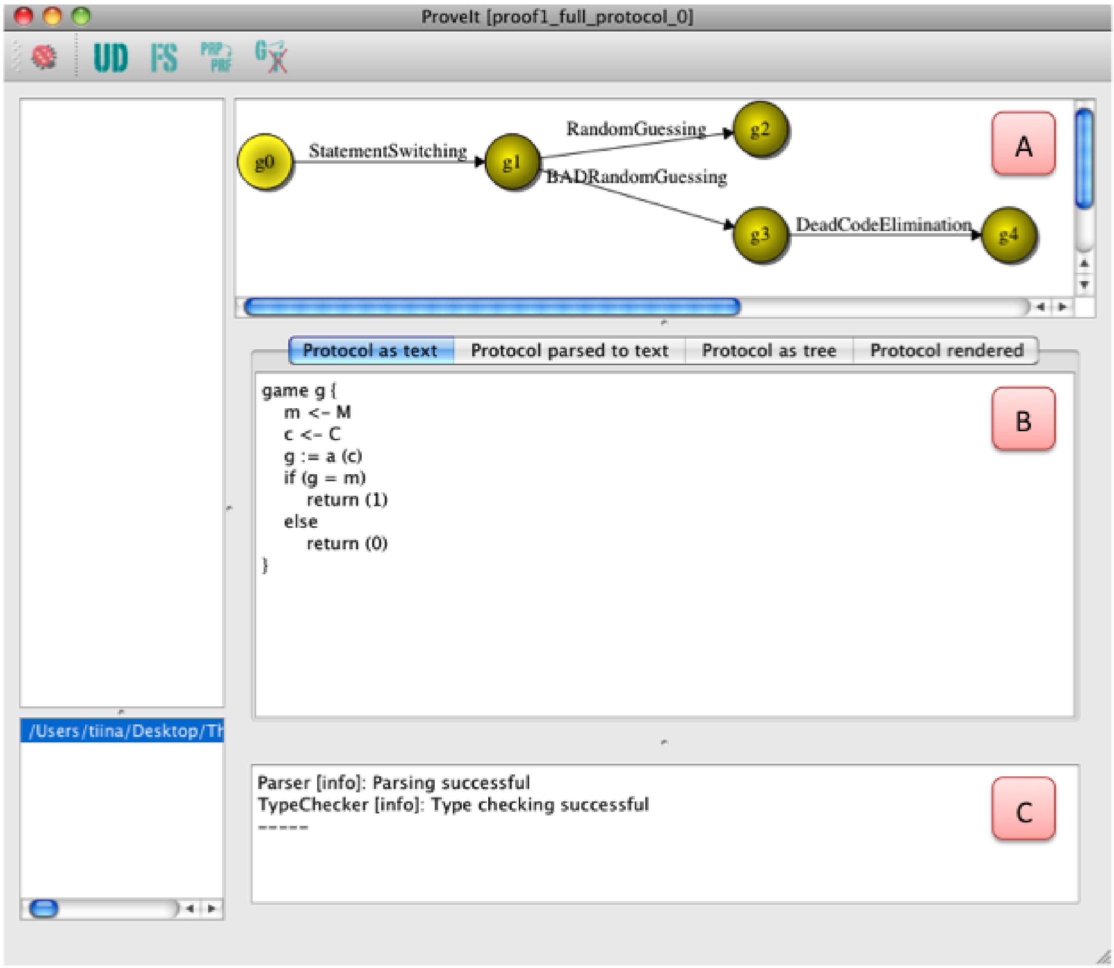


Figure 2: Refer if the figure is not yours [Kam12]



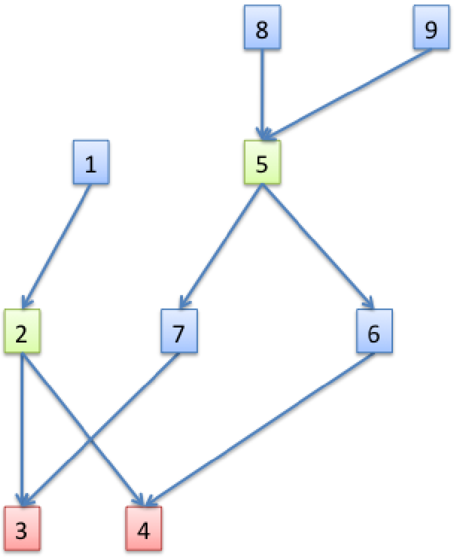
```
game g {
   m <- M
   c <- C
   g := a (c)
   if (g = m)
      return (1)
   else
      return (0)
}
```

```
Parser [info]: Parsing successful
TypeChecker [info]: Type checking successful
-----
```

Figure 3: Screenshot of ProveIt

Tip: If you add a screenshot then labeling the parts might help make the text more understandable (panel C vs bottom left part), e.g.

Example: A screenshot of ProveIt can be seen on Figure 3. The user first enters the pseudocode of the initial game in panel B. ProveIt also keeps track of all the previous games showing the progress on a graph seen in panel A.



Node	Decendants
1	2, 3, 4
2	3, 4
3	
4	
5	3, 4, 6, 7
6	4
7	3
8	3, 4, 5, 6, 7
9	3, 4, 5, 6, 7

Figure 4: Example how to put two figures parallel to each other

4 Other Ways to Represent Data

4.1 Tables

Statement	**Typeset Example**
assignment	$a := 5 + b$
uniform choice	$m \leftarrow M$
function signature	$f : K \times M \to L$

Table 1: Statements in the ProveIt language

4.2 Lists

Numbered list example:

1. item one;
2. item two;
3. item three.

4.3 Math mode

Example:

$$a + b = c + d$$

Aligning:

$$\begin{aligned} a &= 5 \\ b + c &= a \\ a - 2 * 3 &= 5/4 \end{aligned}$$

Hint: Variables or equations in text are separated with $ sign, e.g. a, $x - y$.

Inference Rules

$$\text{addition}\,\frac{\Gamma \vdash x : T \qquad \Gamma \vdash y : T}{\Gamma \vdash x + y : T}$$

Bigger example:

$$\text{assign}\,\frac{\Gamma \vdash c := a + b \qquad \text{addG}\,\dfrac{\Gamma \vdash a : \mathsf{Rat} \qquad \text{var}\,\dfrac{\Gamma \vdash b : \mathsf{Int} \qquad \Gamma \vdash \mathsf{Int} \subseteq \mathsf{Rat}}{\Gamma \vdash b : \mathsf{Rat}}}{\Gamma \vdash a + b : \mathsf{Rat}}}{\Gamma \vdash c : \mathsf{Rat}}$$

4.4 algorithm2e

Algorithm 1: typeChecking

```
Input: Abstract syntax tree
Result: Type checking result; In addition, type table $\mathsf{type}_{\mathsf{G}}$ for global
        variables, $\mathsf{type}_{\mathsf{game}}$ for the main game and $\mathsf{type}_{\mathsf{fun}}$ for each $fun \in F$
while something changed in last cycle do
    foreach global statement s do parseStatement(s, $\mathsf{type}_{\mathsf{G}}$);
    foreach function $fun$ do
        foreach statement s in $fun$ do parseStatement(s, $\mathsf{type}_{\mathsf{fun}}$);
    foreach statement s in game do parseStatement(s, $\mathsf{type}_{\mathsf{game}}$);
```

4.5 Pseudocode

```
expression
  : NUMBER
  | VARIABLE
  | '-' expression
  | expression '+' expression
  | expression '-' expression
  | function_name '(' parameters ')'
  | '(' expression ')'
```

Figure 5: Grammar of arithmetic expressions

4.6 Frame Around Information

Tip: We can use minipage to create a frame around some important information.

1. integer division (\div) - only usable between Int types
2. remainder (%) - only usable between Int types

Figure 6: Arithmetic operations in ProveIt revisited

5 Conclusion

what did you do?

What are the results?

future work?

6 Eestikeelne pealkiri

Bakalaureusetöö (6 EAP)
Eesnimi Perekonnanimi
Resümee

Use introduction and conclusion to give a brief overview of what this thesis is about

References

[BGZ09] Gilles Barthe, Benjamin Grégoire, and Santiago Zanella Béguelin. Formal certification of code-based cryptographic proofs. In *36th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL 2009*, pages 90–101. ACM, 2009.

[Bla] Bruno Blanchet. Proverif: Cryptographic protocol verifier in the formal model. `http://www.proverif.ens.fr/`.

[BR04] Mihir Bellare and Phillip Rogaway. Code-based game-playing proofs and the security of triple encryption. Cryptology ePrint Archive, Report 2004/331, 2004. `http://eprint.iacr.org/`.

[Kam12] Liina Kamm. ProveIt - How to make proving cryptographic protocols less tedious. Talk at the 21st Estonian Computer Science Theory Days at Kubija, January 2012.

[Sho04] Victor Shoup. Sequences of games: a tool for taming complexity in security proofs. Cryptology ePrint Archive, Report 2004/332, 2004. `http://eprint.iacr.org/`.