Are Proof Checkers useful in security?(preview)

(We are going to try Mizar)

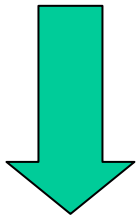
Hiroyuki OKAZAKI
Shinshu Univ.

MIZAR

- Proof Checker
- Mathematics Library
- http://mizar.uwb.edu.pl/
- http://markun.cs.shinshu-u.ac.jp/mirror/mizar/
- http://www.wakasato.org/mizar/

computational

- Adv ORACLE



- Solving ORACLE Problem (hard)

example

- C=RabinENC(m,n) s.t. n=p*q
- {m1,m2,m3,m4}=RabinDEC(C,p,q)

- m_i=ADV(C,n)

- gcd(m_i-m,n)=1 or p or q or n

Our Aim, with MIZAR

- Formalize proving method of computational security
- Search for the common ground between computational security and security of formal method.

Problems

- Difficult for Beginners.
- Few mizar libraries that can be used to research cryptology
- Very strict

  To translate into the mizar language, we must strictly re-describe several theorems, definitions, and so on.

My mission
in the VERY near future

- mastering the Mizar language
- Writing Mizar libraries for security
- Proving something with Mizar

Useful?

- Useful for conventional (computational) proof

  Checking strictly

  formal expression
- Is there new proof method?

  I believe so