Proof *Certificates*

- What is a *certificate* ?
- Where does the name come from ??
- Not from formal proofs ! (it seems)

Certificates for *non*-primality

Simple example: convince you that 75 is not prime

- Look: it is dividable by 5 (or 3...) compute 75 mod 5, check it is equal to 0
- Look: 3x25 = 75
- Just run the certified factorization program, stupid ! factorize 75

Verification is always a process

- It involves computation -

Even more detailled certificate

Detail why 75=3x25

$$\begin{array}{rrr} & 2 & 5 \\ \times & & 3 \\ \hline & 1 & 5 \\ + & 6 & . \\ \hline = & 7 & 5 \end{array}$$

This goes to far...

How much computing freedom do we have to verify the certificate

Primality certificates

Pocklington (1914) :

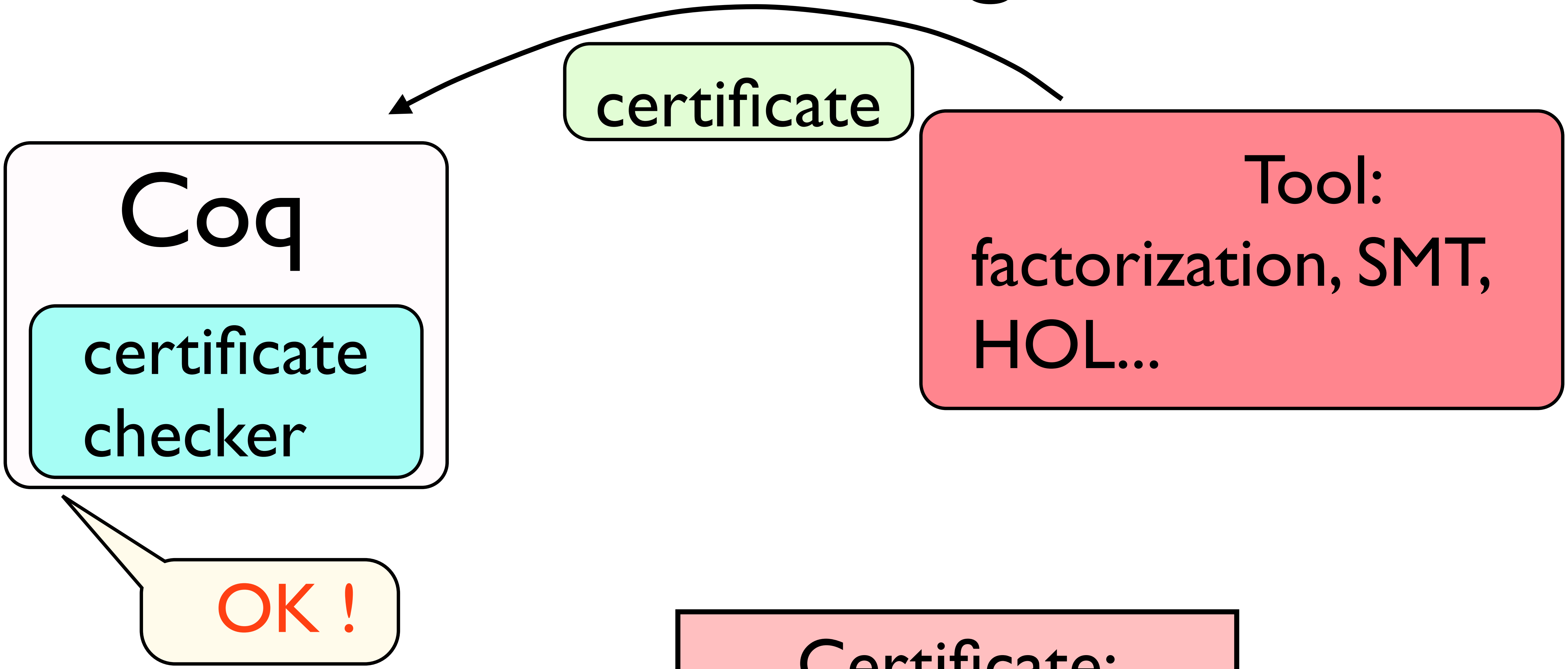
$n>1$ is prime if,

Difficult to build
easy to check

- $p_1, \ldots, p_k$
- $(p_1^{a1}. \ldots .p_k^{ak}) \mid (n-1)$
- $(p_1^{a1}. \ldots .p_k^{ak}) > \sqrt{n}$
- $c^{n-1} = 1 \pmod{n}$
- $\forall i, \gcd(c^{(n-1)/p_i}-1, n) = 1$

$(c, p1, \ldots, pk)$ is a certificate

An often occuring scheme



certificate

Coq

certificate checker

Tool: factorization, SMT, HOL...

OK !

certitude

Certificate:

- result of search
- input of checking

Often occuring scheme

- Primality certificates
- SAT/SMT produced certificate
- certificate of positivity (sum-of-squares) $P=\sum(Q_i)^2$ computed through linear programming
- The fix-point of an abstract interpretation checking ?

Often occuring scheme

- Primality certificates
- SAT/SMT produced certifica
- certificate of positivity (sum $P=\sum(Q_i)^2$ computed through programming
- The fix-point of an abstract interpretation checking ?

Certificate as a link between systems, paradigms...

A question of strategy

For helping our work, our technologies to spread, should we:

- continue using the word for various formats, various situations,

- or agree on *one* notion of «certificate»

Or just one notion of «proof»

Summary

- result of a search procedure; input of a verification procedure
- Easier to check than to build
- How much freedom given in the certificate verification
- Certificate as a go-between between systems
- Should we advertize «one» notion of certificate