Breaking RSA is Equivalent to Factoring

Divesh Aggarwal and Ueli Maurer

ETH Zurich, www.crypto.ethz.ch

CRYPTO 2008 Rump Session.

Breaking RSA Generically is Equivalent to Factoring

Divesh Aggarwal and Ueli Maurer

ETH Zurich, www.crypto.ethz.ch

CRYPTO 2008 Rump Session.

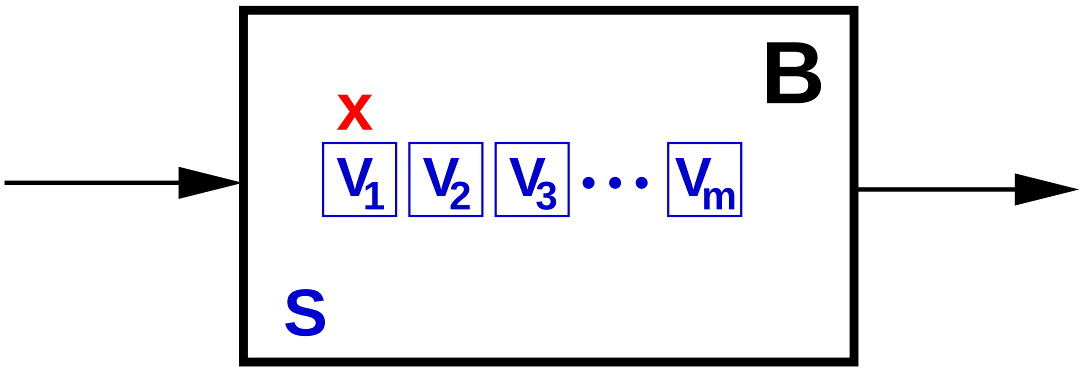
Generic algorithms

- **Cannot exploit representation of elements, except for trivial properties.**
- **Used to prove lower bounds (e.g. DL, DH, DDH).**
- **Many known algorithms/reductions are generic.**
- **Often modeled as a random mapping [Shoup97].**

Generic algorithms

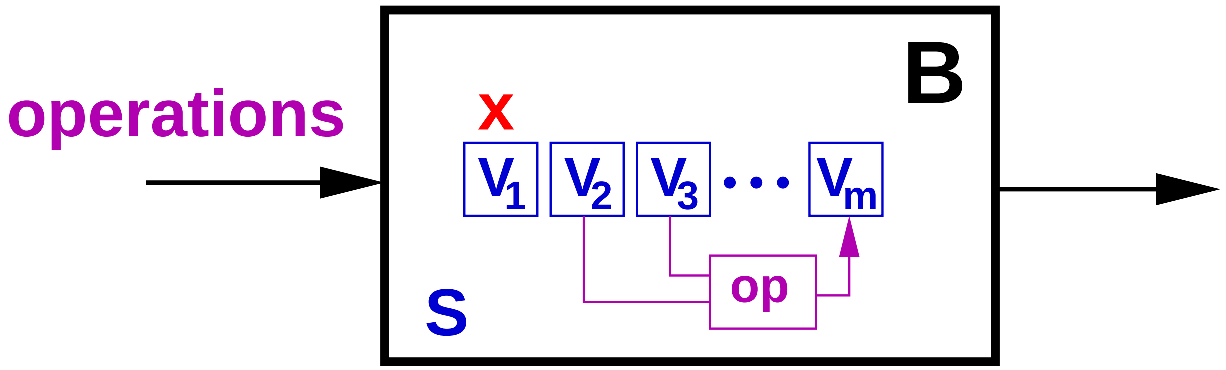
- **Cannot exploit representation of elements, except for trivial properties.**
- **Used to prove lower bounds (e.g. DL, DH, DDH).**
- **Many known algorithms/reductions are generic.**
- **Often modeled as a random mapping [Shoup97].**
- **Next: simpler and more general abstract model of computation [Mau05].**

Abstract Model of Computation



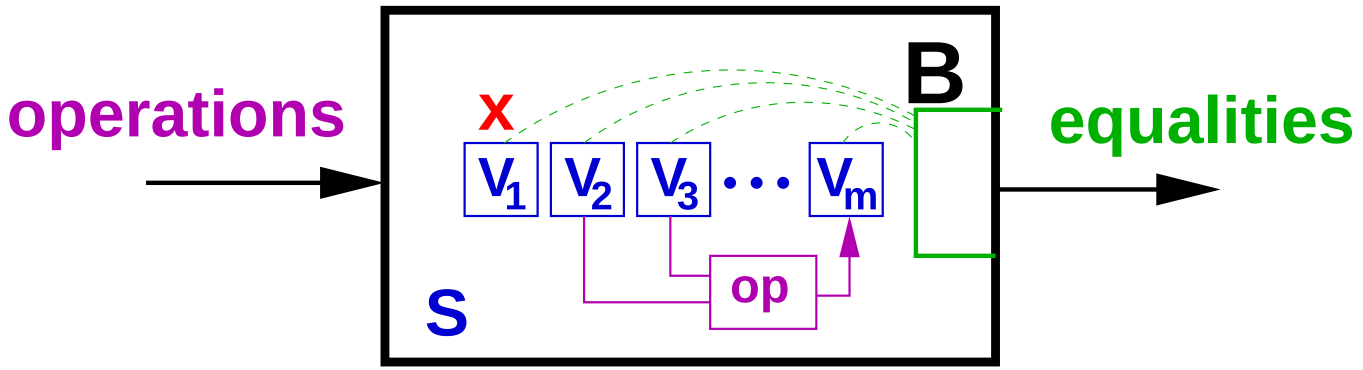
- **Blackbox B contains registers $V_1, \ldots, V_m$ with $V_1 = x$**

Abstract Model of Computation



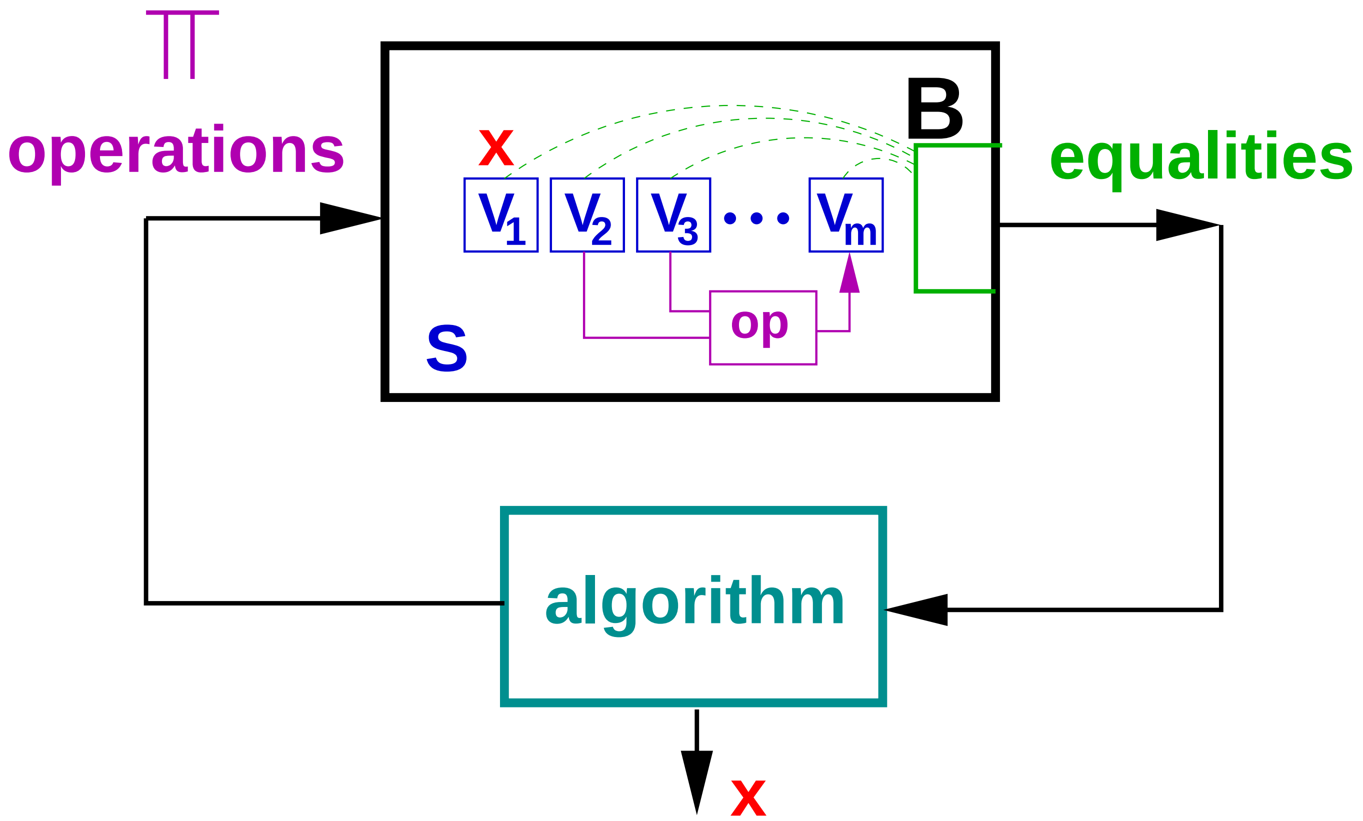
- **Blackbox B contains registers $V_1, \ldots, V_m$ with $V_1 = x$**
- **B allows to perform internal operations.**

Abstract Model of Computation



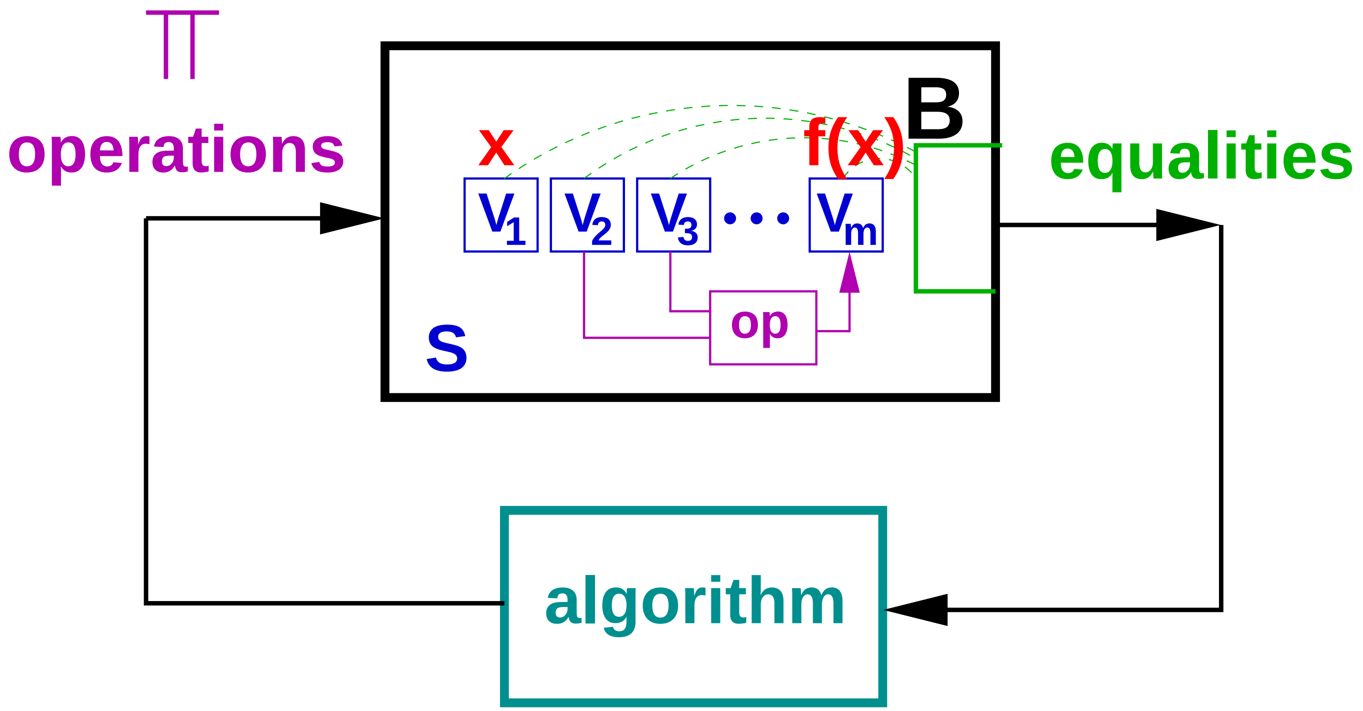
- **Blackbox B contains registers $V_1, \ldots, V_m$ with $V_1 = x$**
- **B allows to perform internal operations.**
- **Possible type of operation: equality tests.**

Abstract Model of Computation



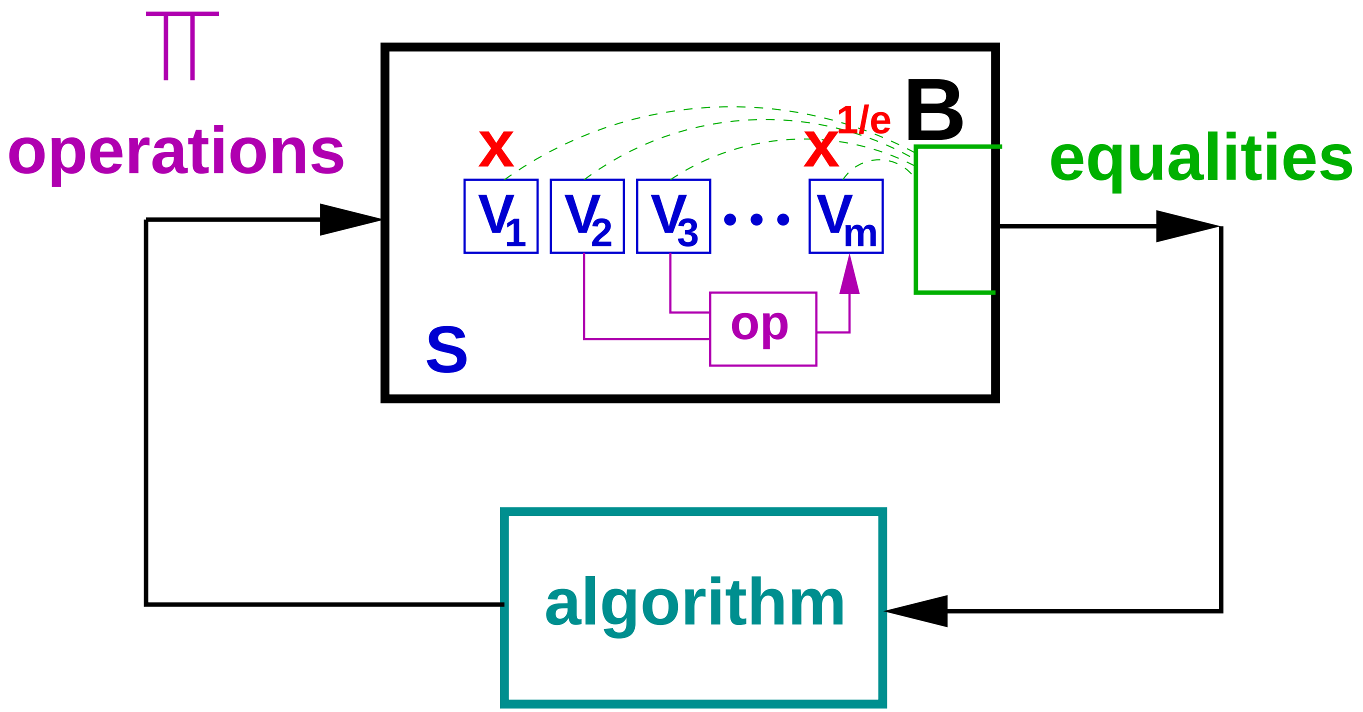
- Blackbox B contains registers $V_1, \ldots, V_m$ with $V_1 = x$
- B allows to perform internal operations.
- Possible type of operation: equality tests.
- Task of algorithm: extract x.

Abstract Model of Computation



- Blackbox B contains registers $V_1, \ldots, V_m$ with $V_1 = x$
- B allows to perform internal operations.
- Possible type of operation: equality tests.
- Task of algorithm: achieve V_m= f(x) for some f.

Breaking RSA Generically

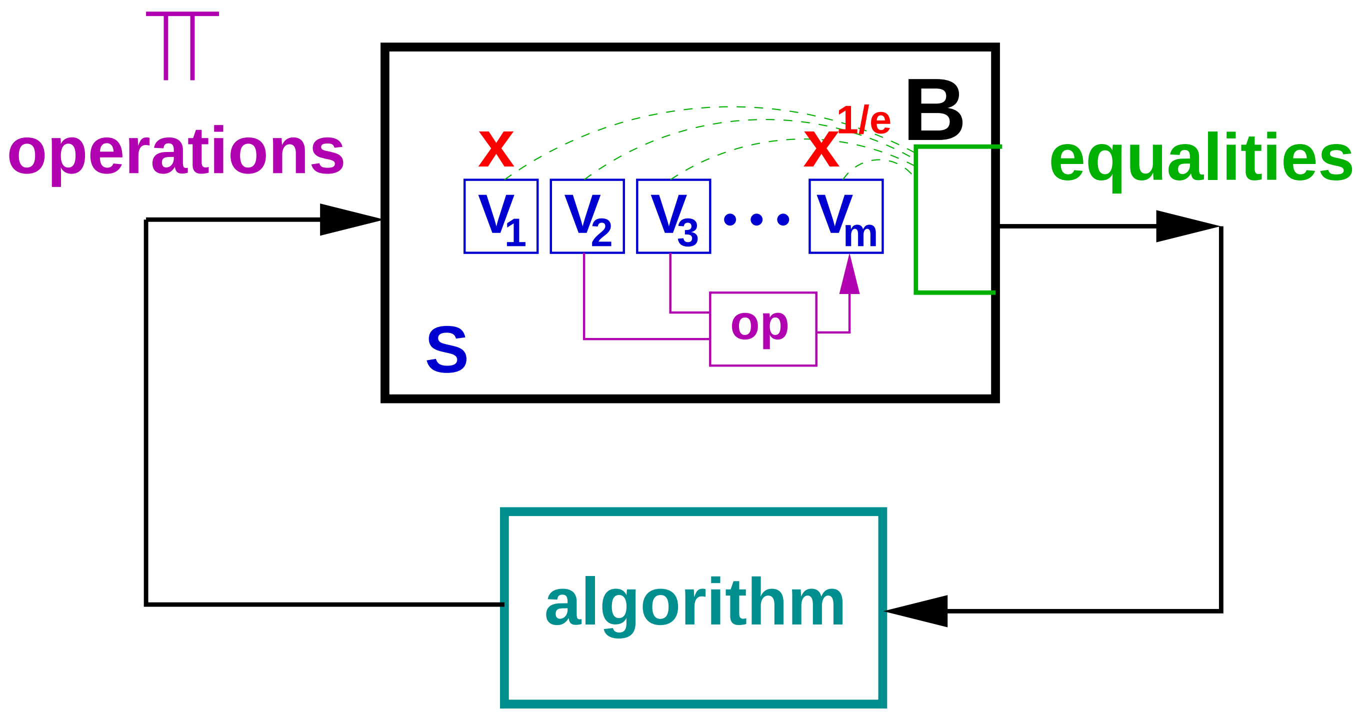


$$\mathbf{S} = Z_n$$

$$\mathbf{f(x)} = \sqrt[e]{\mathbf{x}}$$

$$\Pi = \{+\,,\,-\,,\,*\,,\,/\,,\,(\cdot)^{-1}\,,\,\mathbf{eq?}\}$$

Breaking RSA Generically



$\mathbf{S} = Z_n$

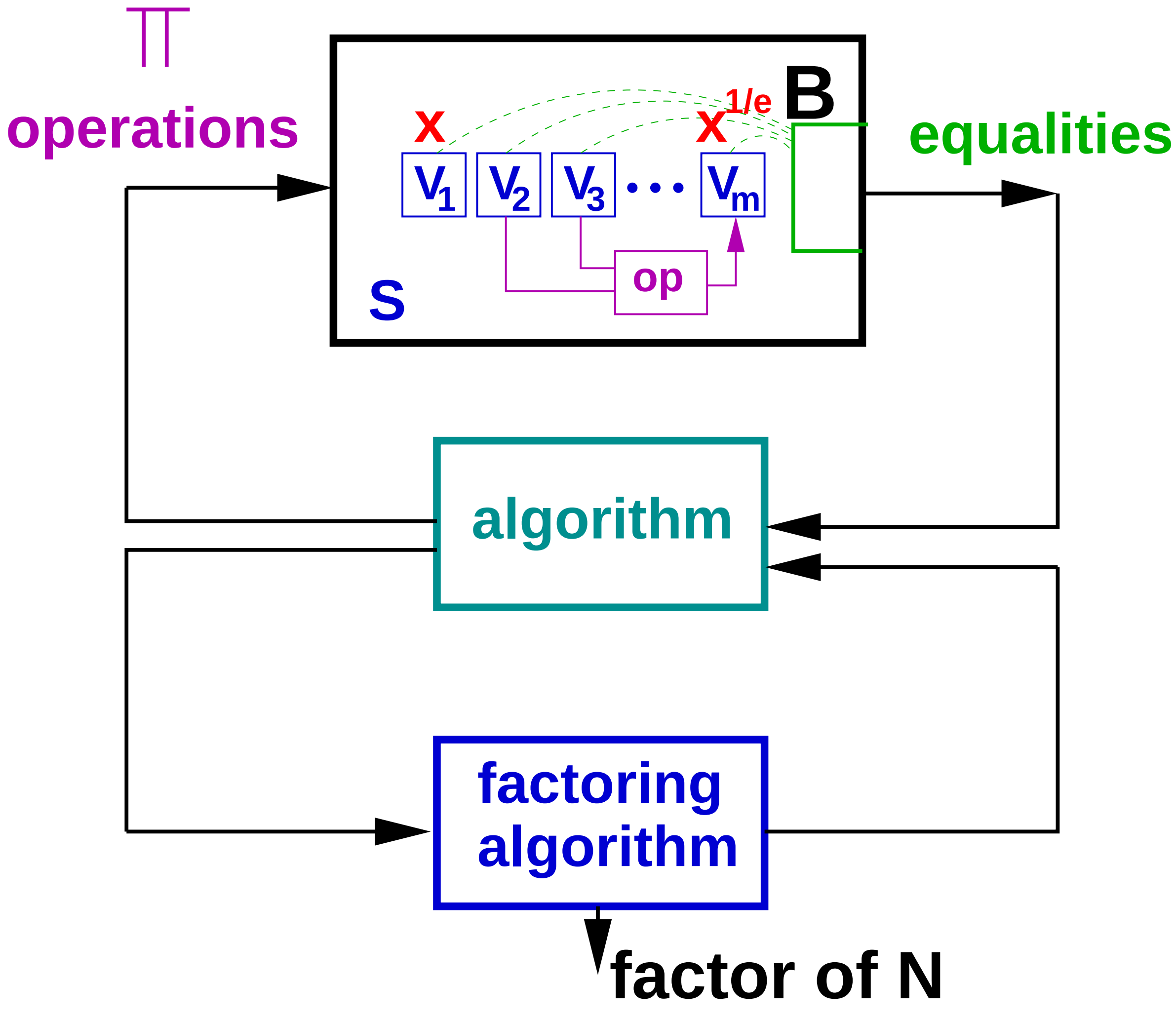
$\mathbf{f(x)} = \sqrt[e]{\mathbf{x}}$

$\Pi = \{+\,,\,-\,,\,*\,,\,/\,,\,(\cdot)^{-1}\,,\,\textbf{eq?}\}$

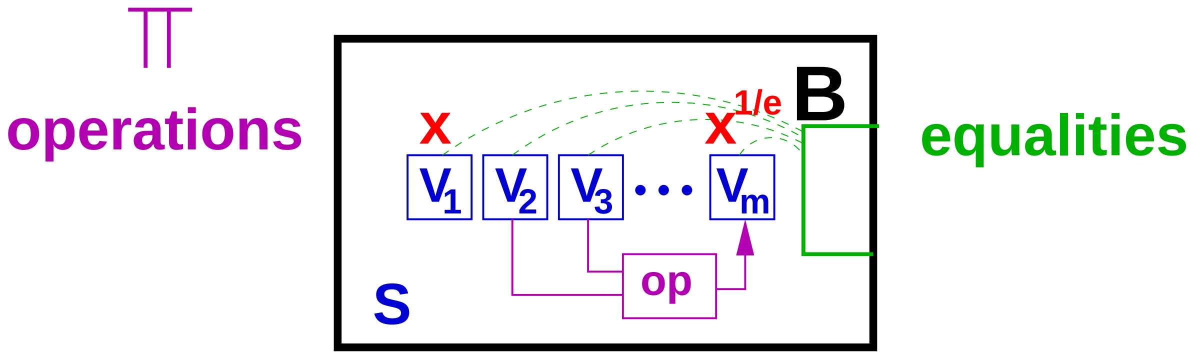
Previous results: [Brown05], [Leander/Rupp06],

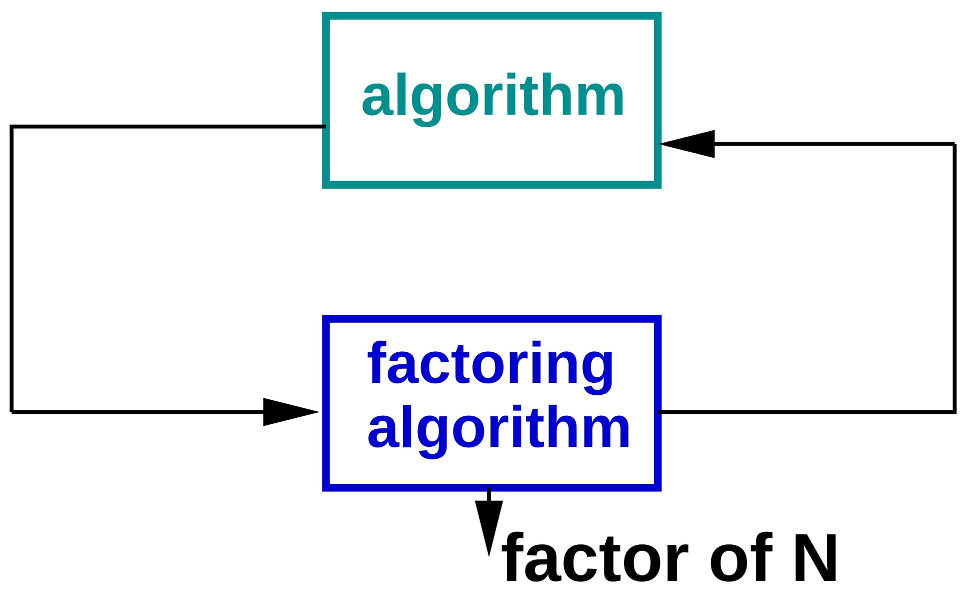
Theorem: **There exists an efficient algorithm which, when given access to any generic e-th root algorithm, factors N (with essentially the same success prob.).**

Theorem: **There exists an efficient algorithm which, when given access to any generic e-th root algorithm, factors N (with essentially the same success prob.).**



Theorem: There exists an efficient algorithm which, when given access to any generic e-th root algorithm, factors N (with essentially the same success prob.).





Paper on e-print, but contains an error!

Fixed version (more involved) will soon be on-line.