The Equivalence of Strong RSA and Factoring in the Generic Ring Model of Computation

Divesh Aggarwal and Ueli Maurer and Igor Shparlinski

EUROCRYPT 2010

Rump Session

The Strong RSA Assumption

The Strong RSA Problem:

Given $n = pq$, $x \in_R \mathbb{Z}_n$, compute y, e s.t.

$$y^e = x \mod n.$$

The Strong RSA Assumption

The Strong RSA Problem:

Given $n = pq$, $x \in_R \mathbb{Z}_n$, compute y, e s.t.

$$y^e = x \mod n.$$

Strong RSA Assumption: The Strong RSA Problem is hard.

The Strong RSA Assumption

The Strong RSA Problem:

Given $n = pq$, $x \in_R \mathbb{Z}_n$, compute y, e s.t.

$$y^e = x \mod n.$$

Strong RSA Assumption: The Strong RSA Problem is hard.

Factor n $\Longrightarrow$ Solve Strong RSA

$$x^{\phi(n)+1} = x \mod n.$$

The Strong RSA Assumption

The Strong RSA Problem:

Given $n = pq$, $x \in_R \mathbb{Z}_n$, compute y, e s.t.

$$y^e = x \mod n.$$

Strong RSA Assumption: The Strong RSA Problem is hard.

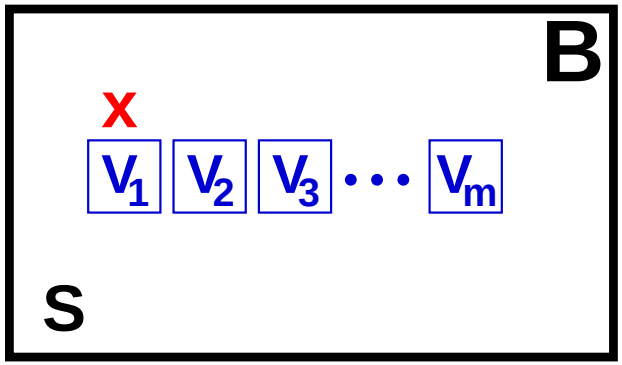
Factor n $\Longrightarrow$ Solve Strong RSA

$$x^{\phi(n)+1} = x \mod n.$$

Solve Strong RSA $\stackrel{?}{\Longrightarrow}$ Factor n

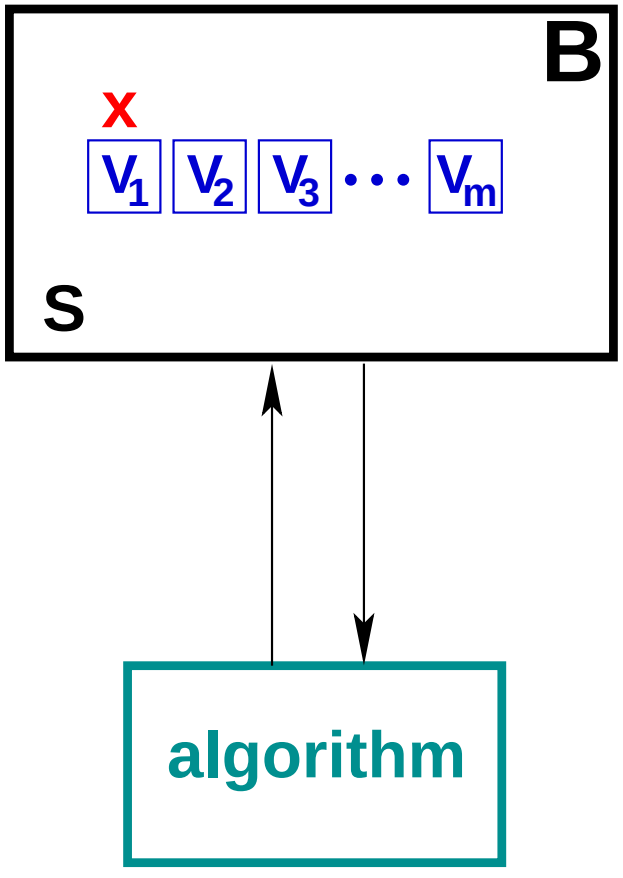
The generic model of computation [Sho97, Mau05]

Used to analyze representation independent algorithms



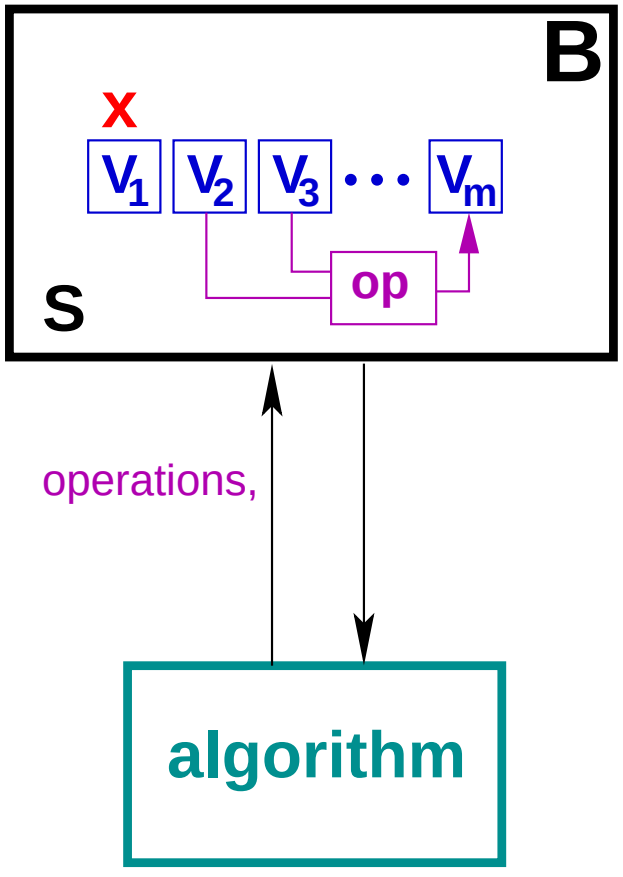
The generic model of computation [Sho97, Mau05]

Used to analyze representation independent algorithms



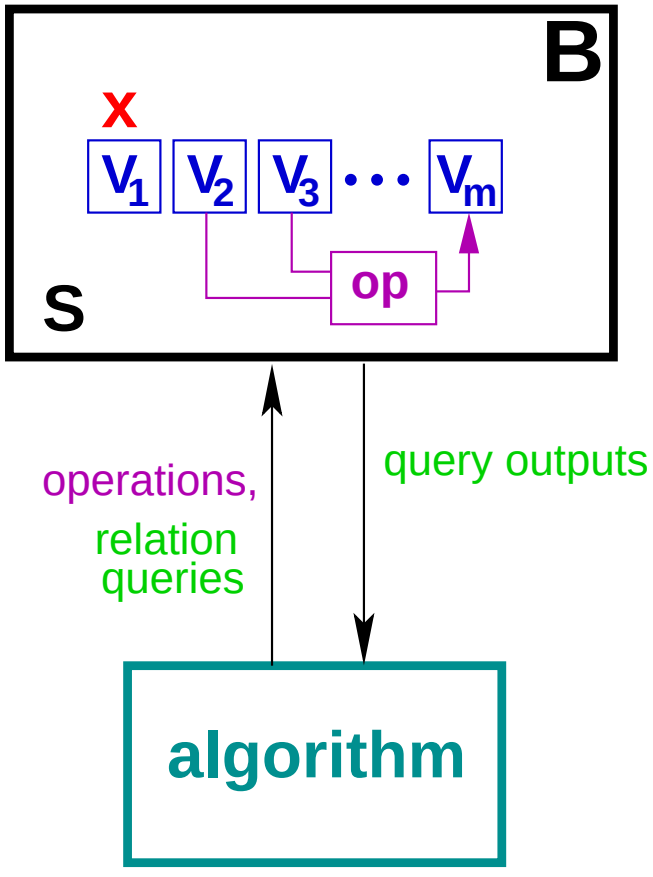
The generic model of computation [Sho97, Mau05]

Used to analyze representation independent algorithms

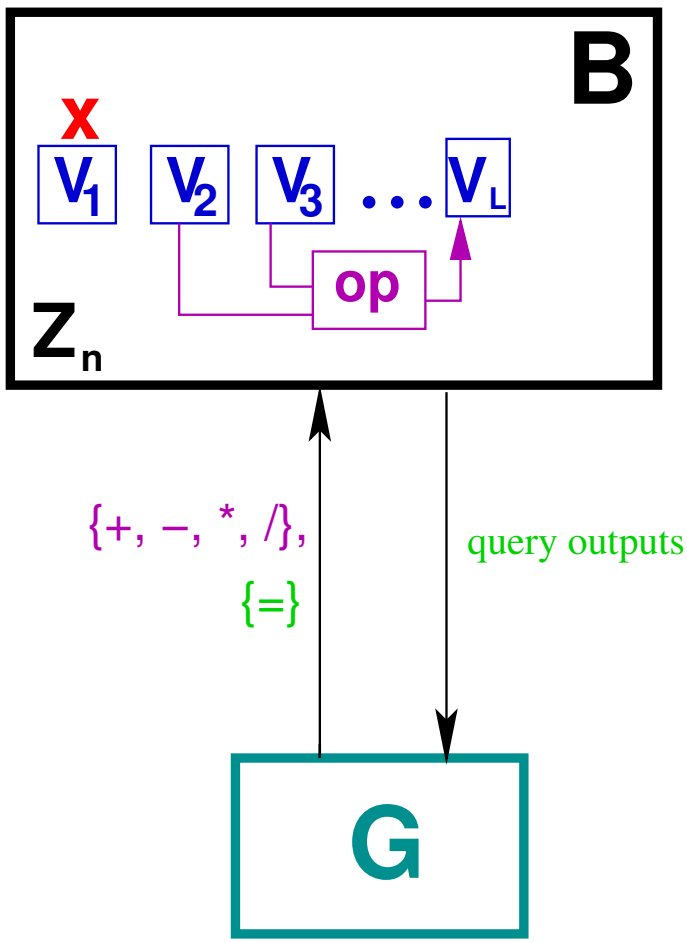


The generic model of computation [Sho97, Mau05]

Used to analyze representation independent algorithms

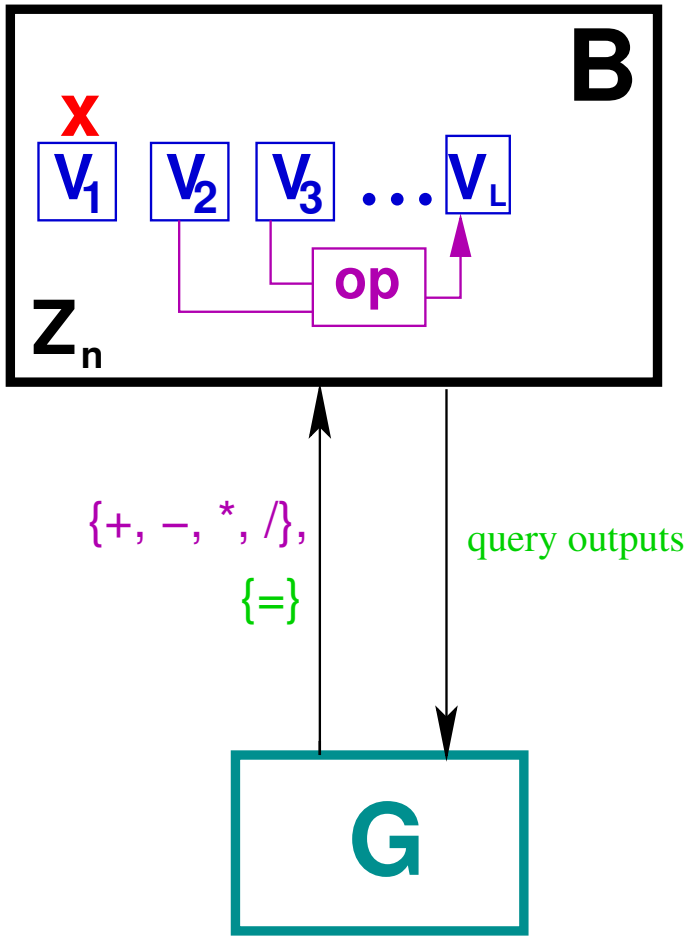


For the ring $\mathbb{Z}_n$



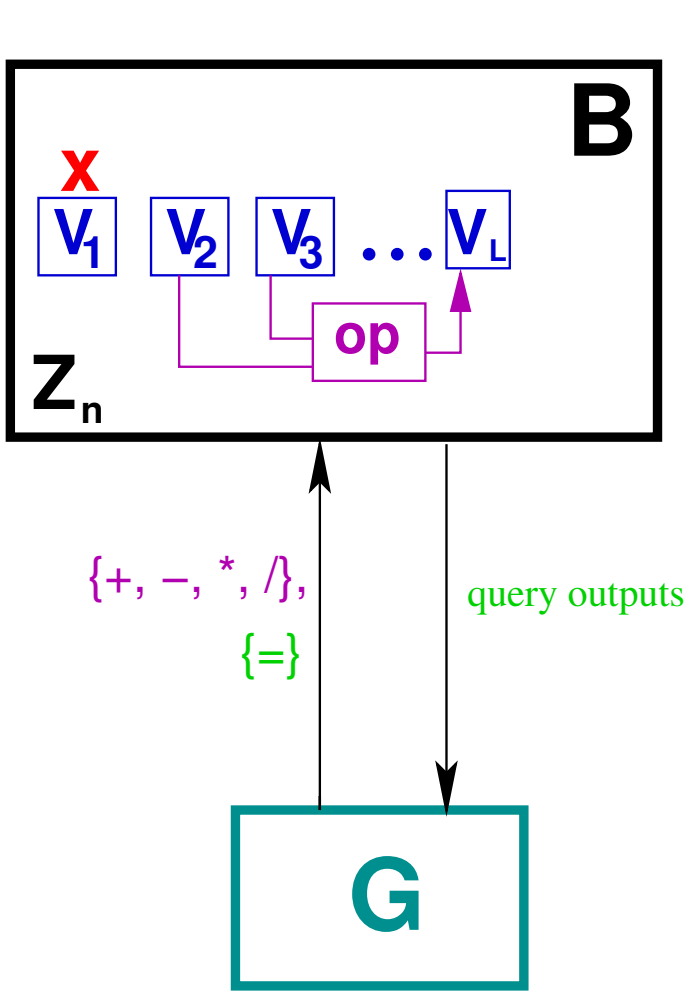
For the ring $\mathbb{Z}_n$, we have from [AM09]...

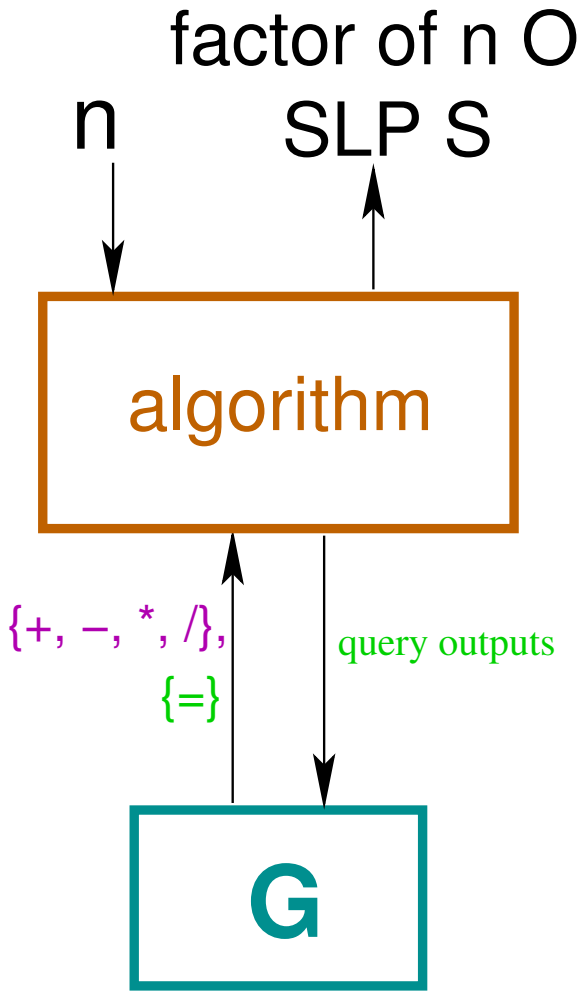
For any problem $\mathcal{P}$ that G solves..



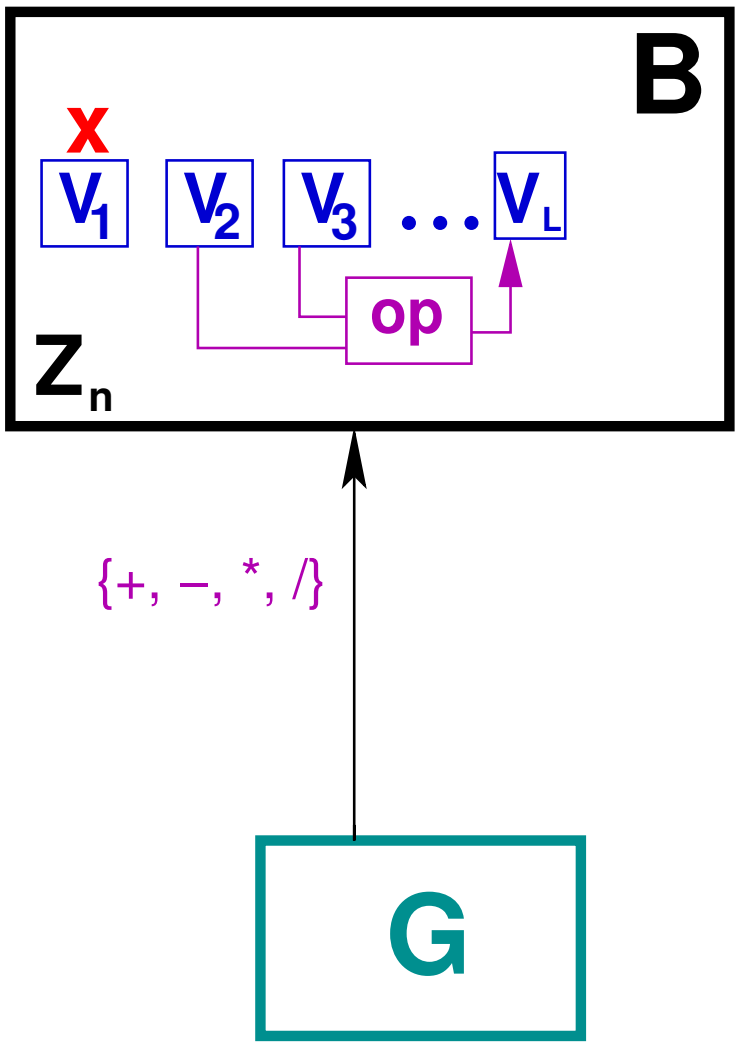
For the ring $\mathbb{Z}_n$, we have from [AM09]...

For any problem $\mathcal{P}$ that G solves..

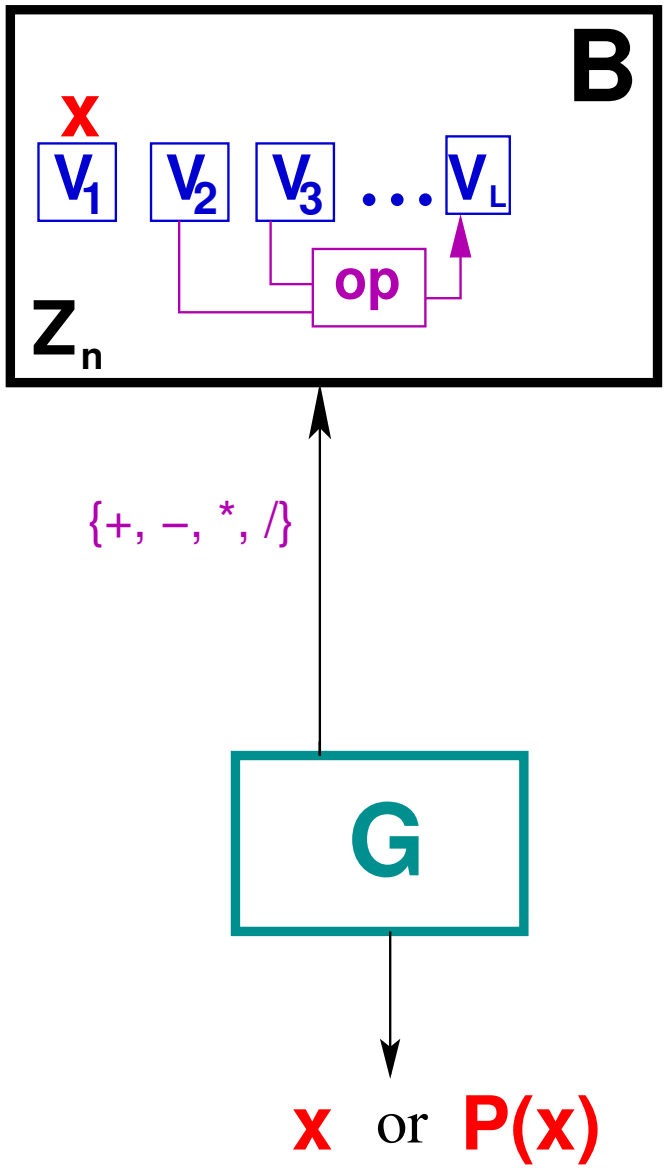




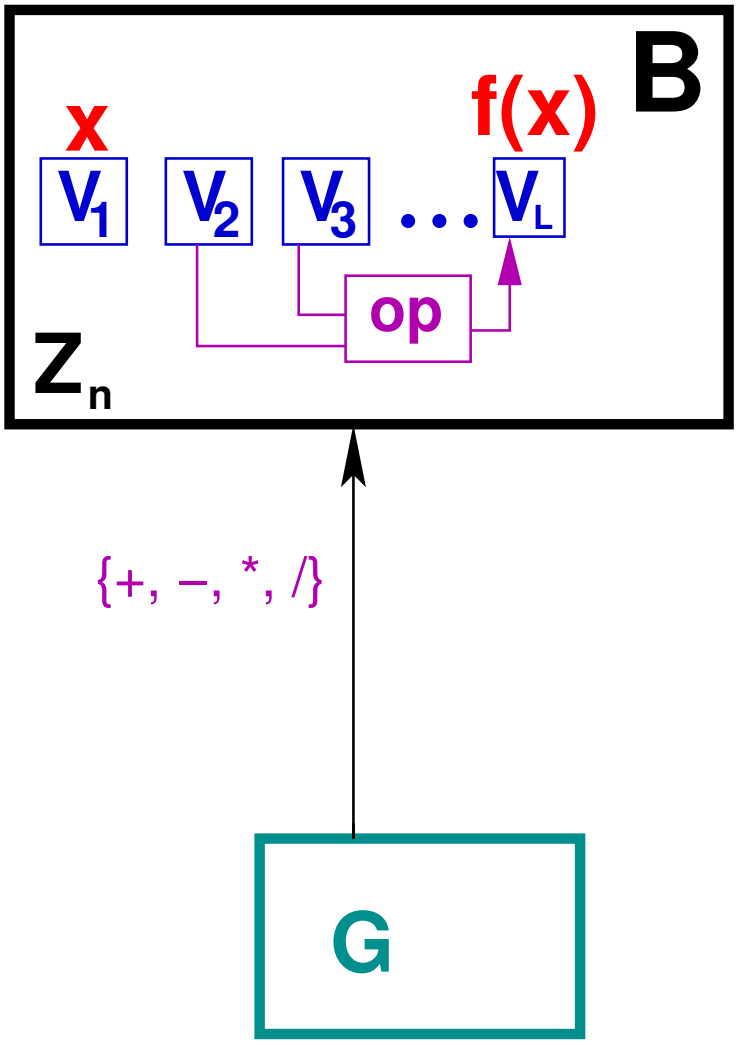
Thus assuming factoring *n* is hard, we can restrict attention to Straight Line Programs



Extraction/Decision Problems Uninteresting

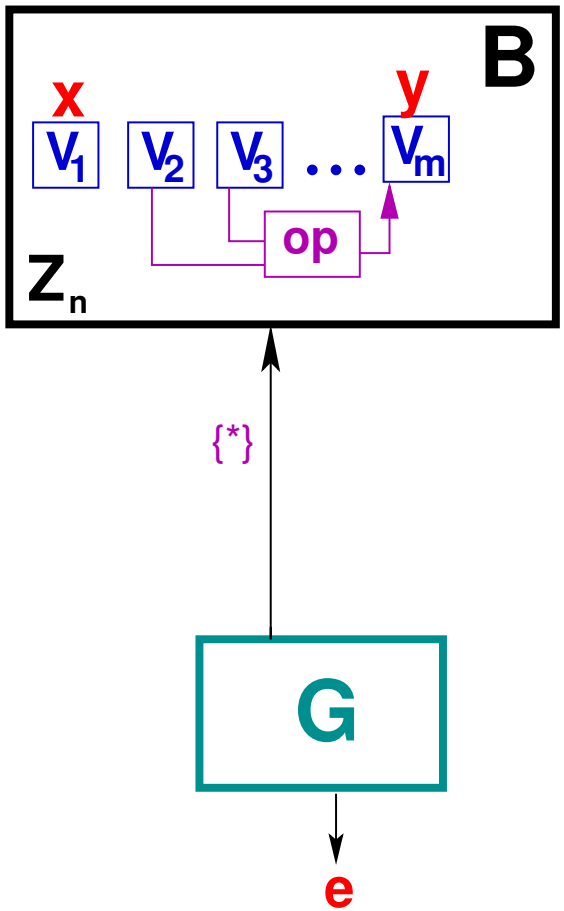


Computation Problems More Interesting



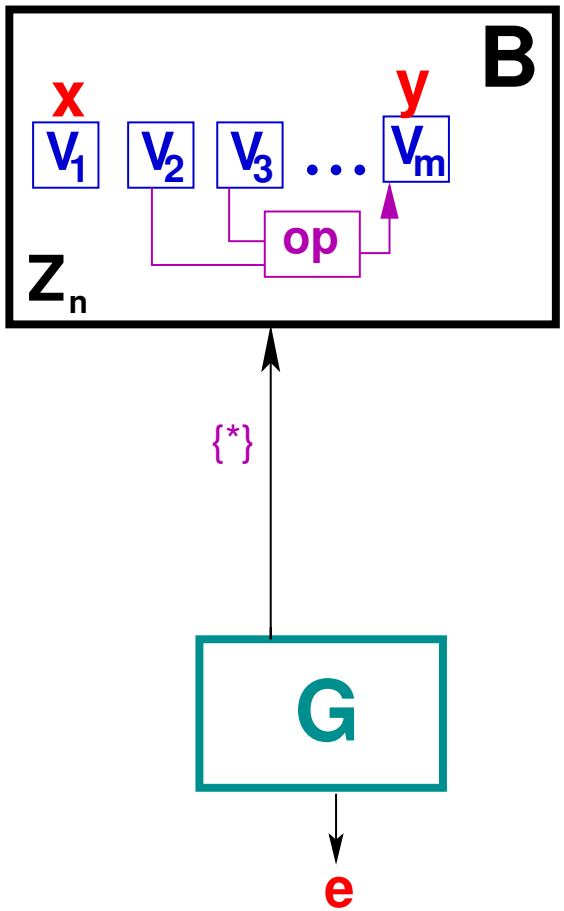
Earlier Attempt at Strong RSA in the Generic Model [DK02]

Strong RSA: Given x, find y, e such that $y^e = x \mod n$



Earlier Attempt at Strong RSA in the Generic Model [DK02]

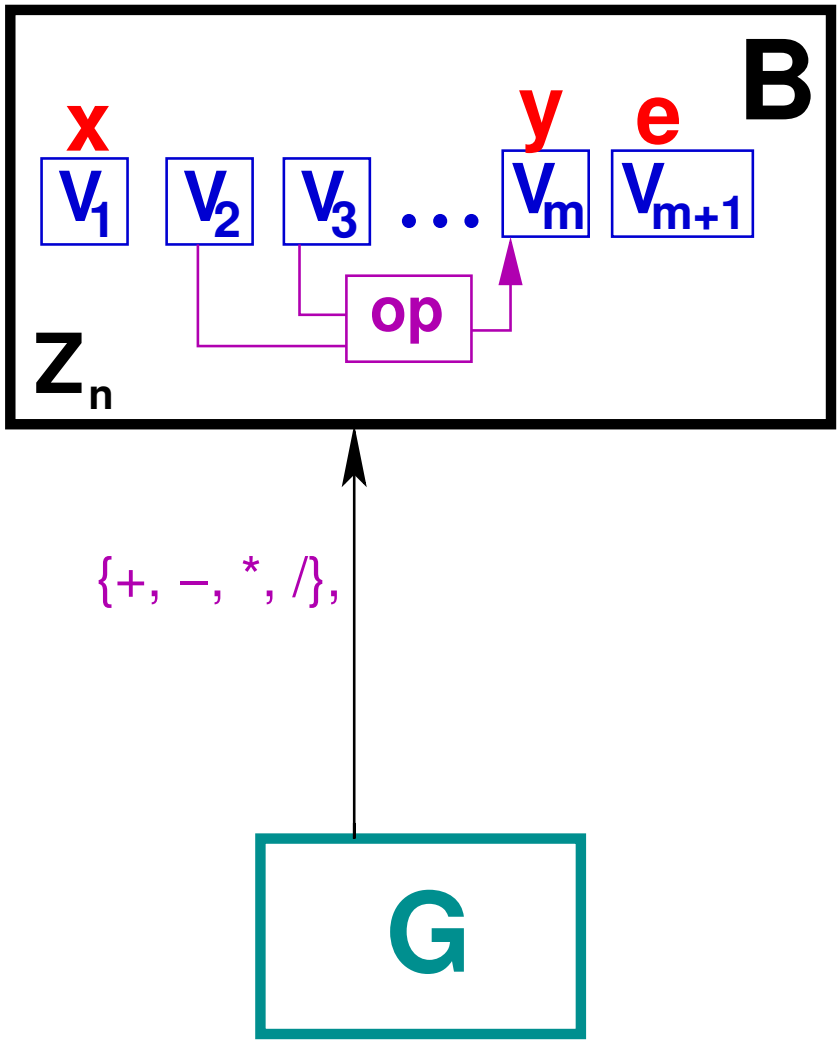
Strong RSA: Given x, find y, e such that $y^e = x \mod n$



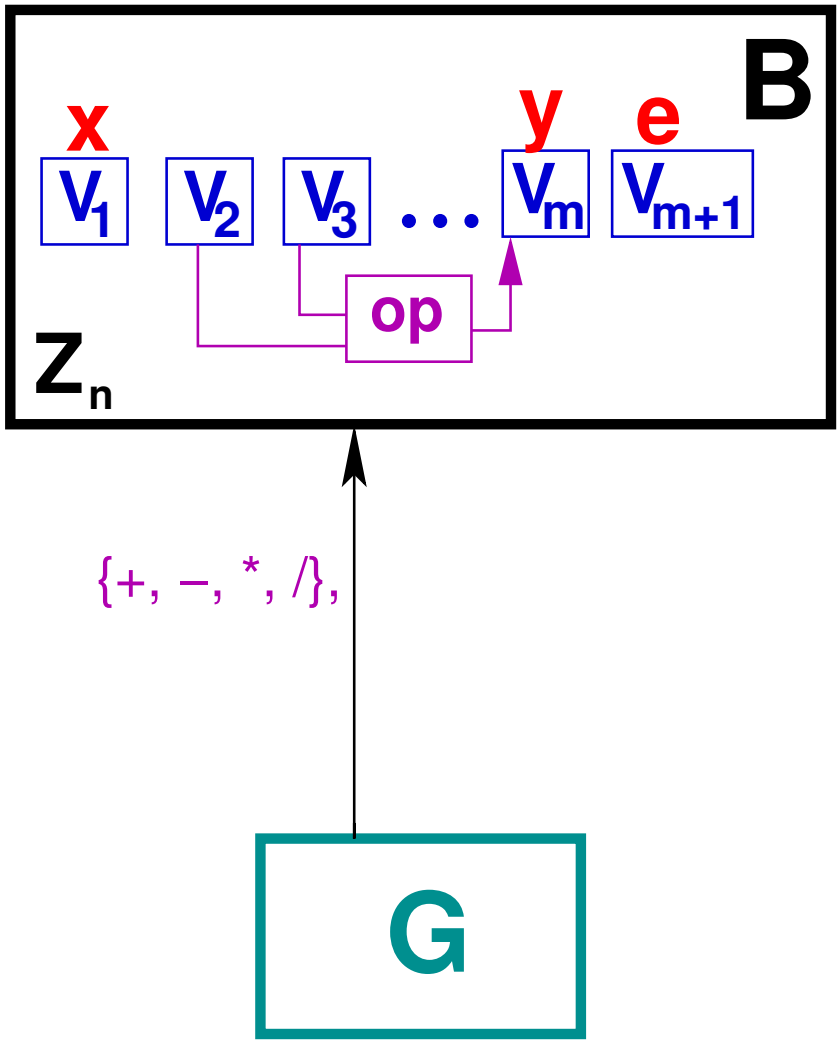
Not much different from RSA

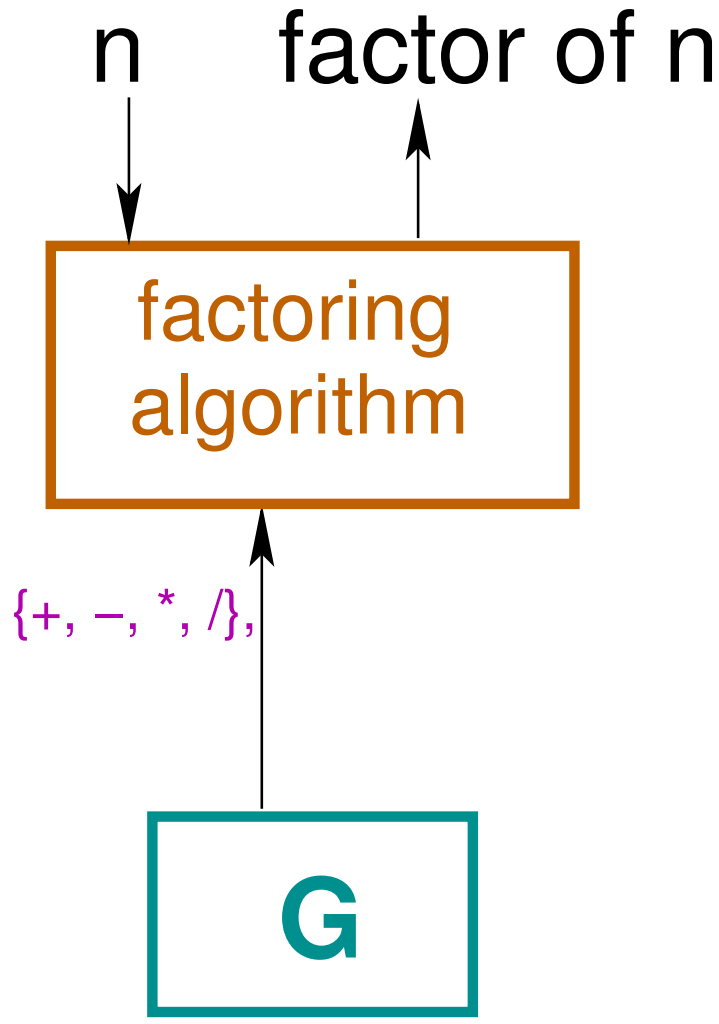
How to model Strong RSA in the generic model?

Here is how!

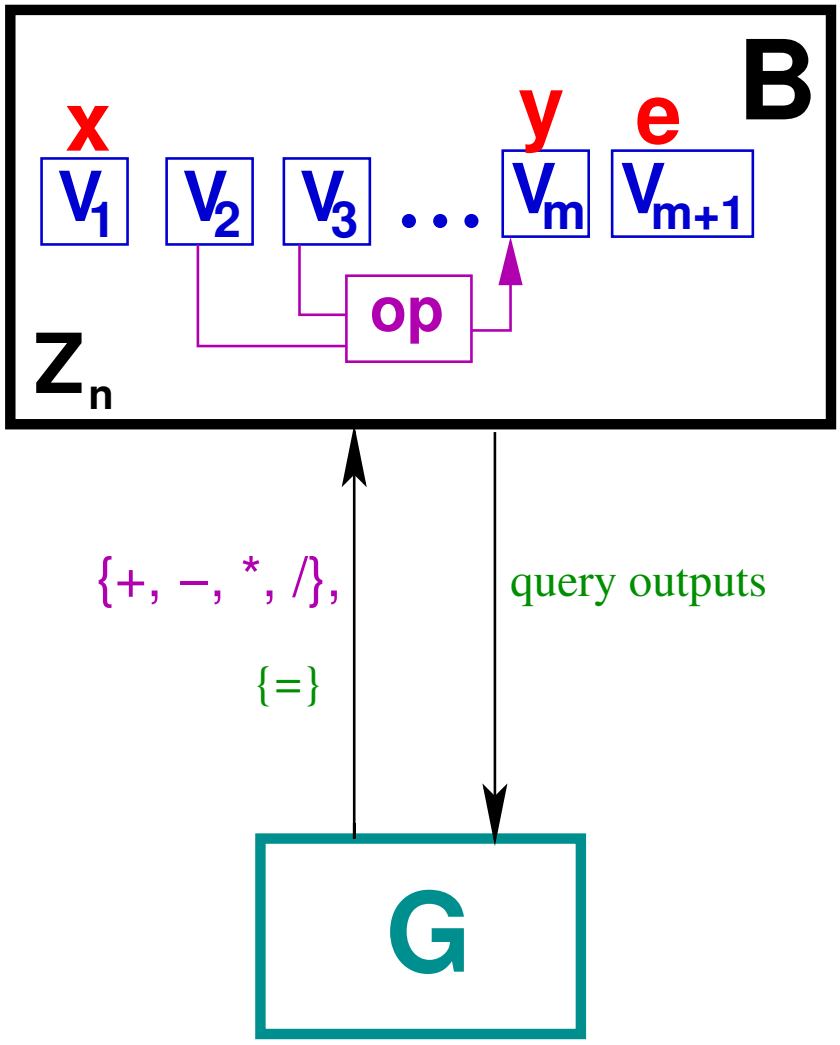


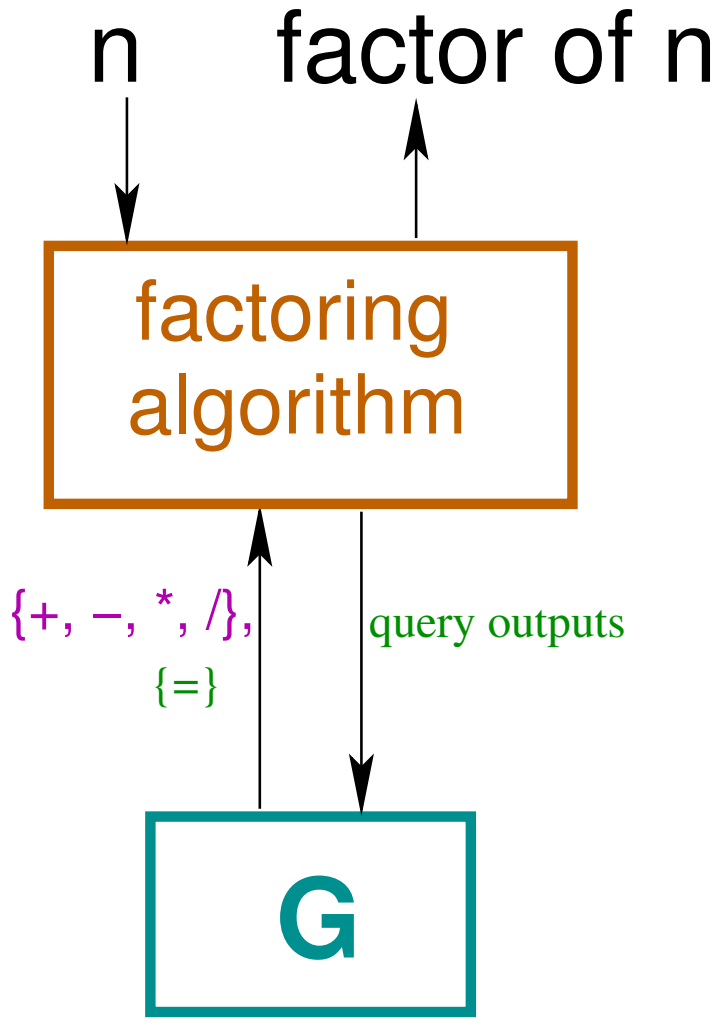
Our Result





Our Result


B
x
y
e
V1
V2
V3
...
Vm
Vm+1
op
Zn
{+, −, *, /},
{=}
query outputs
G


n
factor of n
factoring
algorithm
{+, −, *, /},
{=}
query outputs
G