Notions of Black-Box Reductions, Revisited

ASIACRYPT 2013

Paul Baecher, Christina Brzuska, Marc Fischlin

Tel Aviv University & Darmstadt University of Technology; supported by DFG Heisenberg and Center For Advanced Security Research Darmstadt (CASED)

CASED

Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

Heisenberg-Programm
Deutsche Forschungsgemeinschaft

Introduction

The Cryptographic Zoo

PRP **PKE**

PRF

MAC **KA**

MPC

OWF

OWP

PRG

CRHF

COM

SIG

ZK

- basic issues in cryptography
  - what can be built from what?
  - how (efficient)?

A Typical Theorem in Cryptography

$f \xrightarrow{\text{constr.}} G[f]$

Theorem: Let f be a $\overbrace{P}^{\text{e.g. OWP}}$. Then construction $G[f]$ is a $\overbrace{Q}^{\text{e.g. PRG}}$.

Question 1: what is $G[f]$?

A Typical Theorem in Cryptography

$f \xrightarrow{\text{constr.}} G[f]$

Theorem: Let f be a $\overset{\text{e.g. OWP}}{\downarrow P}$. Then construction $G[f]$ is a $\overset{\text{e.g. PRG}}{\downarrow Q}$.

Question 1: what is $G[f]$?

- construction G uses f as an oracle (G^f)
- construction G uses f in some constricted way
- construction G uses f's code
- ???

A Typical Theorem in Cryptography

$f \xrightarrow{\text{constr.}} G[f]$

Theorem: Let f be a $\overset{\text{e.g. OWP}}{\overbrace{P}}$. Then construction $G[f]$ is a $\overset{\text{e.g. PRG}}{\overbrace{Q}}$.

(corollary: if P exists, then Q exists.)

Question 1: what is $G[f]$?

- construction G uses f as an oracle (G^f)
- construction G uses f in some constricted way
- construction G uses f's code
- ???

Proving the Theorem

$$\begin{tikzcd} f \arrow[r, "\text{constr.}"] & G[f] \\ \mathcal{S}[\mathcal{A}, f] \arrow[u, dotted] & \mathcal{A} \arrow[l, "\text{red.}"'] \arrow[u, dotted] \end{tikzcd}$$

Theorem: Let f be a P. Then construction $G[f]$ is a Q.

- almost always: proof by reduction (show the contrapositive)
- transform an attack on G into an attack on f
- if algorithm $\mathcal{A}$ breaks G, then algorithm $\mathcal{S}[\mathcal{A}, f]$ breaks f

Proving the Theorem

$$\begin{tikzcd} f \arrow[r, "\text{constr.}"] & G[f] \\ \mathcal{S}[\mathcal{A}, f] \arrow[u, dotted] & \mathcal{A} \arrow[u, dotted] \arrow[l, "\text{red.}"'] \end{tikzcd}$$

Theorem: Let f be a P. Then construction $G[f]$ is a Q.

- almost always: proof by reduction (show the contrapositive)
- transform an attack on G into an attack on f
- if algorithm $\mathcal{A}$ breaks G, then algorithm $\mathcal{S}[\mathcal{A}, f]$ breaks f

- $\mathcal{S}[\mathcal{A}, f]$ is the (constructive) reduction
  - Question 2: what is $\mathcal{S}[\mathcal{A},\ \ ]$?
  - Question 3: what is $\mathcal{S}[\ \ , f]$?

Why We Care About these Questions

- very important for impossibility results / separations
  - i.e., *much weaker* versions of P exists $\not\Rightarrow$ Q exists
  - what exactly is being ruled out?
  - ...and what is left to try?
  - impossibility results are inspiring
- enforces precise definitions of primitives
  - "we separate xyz from OWFs..."
- more black box, more efficient, more practical (usually)
- better understanding of a fundamental technique in our field

Notions of Reductions

$$\begin{tikzcd} f \arrow[r, "\text{constr.}"] & G[f] \\ \mathcal{S}[\mathcal{A}, f] \arrow[u, dotted] & \mathcal{A} \arrow[l, "\text{red.}"'] \arrow[u, dotted] \end{tikzcd}$$

- Defined by Reingold, Trevisan, and Vadhan (TCC '04, [RTV04])
- three* types of reductions:

Notions of Reductions

$$\begin{tikzcd} f \arrow[r, "\text{constr.}"] & G[f] \\ \mathcal{S}[\mathcal{A}, f] \arrow[u, dotted] & \mathcal{A} \arrow[l, "\text{red.}"'] \arrow[u, dotted] \end{tikzcd}$$

- Defined by Reingold, Trevisan, and Vadhan (TCC ’04, [RTV04])
- three* types of reductions:

fully black box. $\exists \mathcal{S} \forall \mathcal{A}$: if $\mathcal{A}$ breaks G^f, then $\mathcal{S}^{\mathcal{A},f}$ breaks f.

Notions of Reductions

$$\begin{tikzcd} f \arrow[r, "\text{constr.}"] & G[f] \\ \mathcal{S}[\mathcal{A}, f] \arrow[u, dotted] & \mathcal{A} \arrow[l, "\text{red.}"] \arrow[u, dotted] \end{tikzcd}$$

- Defined by Reingold, Trevisan, and Vadhan (TCC '04, [RTV04])
- three* types of reductions:

fully black box. $\exists \mathcal{S} \forall \mathcal{A}$: if $\mathcal{A}$ breaks G^f, then $\mathcal{S}^{\mathcal{A},f}$ breaks f.

semi black box. $\forall \mathcal{A} \exists \mathcal{S}$: if $\mathcal{A}^f$ breaks G^f, then $\mathcal{S}^f$ breaks f.

order switched

f oracle

no $\mathcal{A}$ oracle

Notions of Reductions

$$\begin{tikzcd} f \arrow[r, "\text{constr.}"] & G[f] \\ \mathcal{S}[\mathcal{A}, f] \arrow[u, dotted] & \mathcal{A} \arrow[l, "\text{red.}"'] \arrow[u, dotted] \end{tikzcd}$$

- Defined by Reingold, Trevisan, and Vadhan (TCC '04, [RTV04])
- three* types of reductions:

fully black box. $\exists \mathcal{S} \forall \mathcal{A}$: if $\mathcal{A}$ breaks G^f, then $\mathcal{S}^{\mathcal{A},f}$ breaks f.

semi black box. $\forall \mathcal{A} \exists \mathcal{S}$: if $\mathcal{A}^f$ breaks G^f, then $\mathcal{S}^f$ breaks f.

weakly black box. $\forall \mathcal{A} \exists \mathcal{S}$: if $\mathcal{A}$ breaks G^f, then $\mathcal{S}^f$ breaks f.

no f oracle

Notions of Reductions

$$\begin{tikzcd} f \arrow[r, "\text{constr.}"] & G[f] \\ \mathcal{S}[\mathcal{A}, f] \arrow[u, dotted] & \mathcal{A} \arrow[l, "\text{red.}"'] \arrow[u, dotted] \end{tikzcd}$$

- Defined by Reingold, Trevisan, and Vadhan (TCC '04, [RTV04])
- three* types of reductions:

fully black box. $\exists \mathcal{S} \forall \mathcal{A}$: if $\mathcal{A}$ breaks G^f, then $\mathcal{S}^{\mathcal{A},f}$ breaks f.

semi black box. $\forall \mathcal{A} \exists \mathcal{S}$: if $\mathcal{A}^f$ breaks G^f, then $\mathcal{S}^f$ breaks f.

weakly black box. $\forall \mathcal{A} \exists \mathcal{S}$: if $\mathcal{A}$ breaks G^f, then $\mathcal{S}^f$ breaks f.

In This Work

- even more, fine-grained notions
  - . . . derived in a systematic way

In This Work

- even more, fine-grained notions
  - ... derived in a systematic way

- consider, for example,
  - reduction makes non-black-box use of primitive, but black-box use of adversary (think meta reductions)
  - efficient primitives and/or adversaries
  - black-box use, but partial information (run time, #queries, ...)
- [RTV04] too coarse to capture such differences

CAP

Three Questions: A Short Encoding

$$\begin{tikzcd} f \arrow[r, "\text{constr.}"] & G[f] \\ \mathcal{S}[\mathcal{A}, f] \arrow[u, dotted] & \mathcal{A} \arrow[l, "\text{red.}"'] \arrow[u, dotted] \end{tikzcd}$$

Q1: what is $G[f]$?

Q2: what is $\mathcal{S}[\mathcal{A}, \quad]$?

Q3: what is $\mathcal{S}[\quad, f]$?

Three Questions: A Short Encoding

$$\begin{tikzcd} f \arrow[r, "\text{constr.}"] & G[f] \\ \mathcal{S}[\mathcal{A}, f] \arrow[u, dotted] & \mathcal{A} \arrow[l, "\text{red.}"'] \arrow[u, dotted] \end{tikzcd}$$

Q1: what is $G[f]$?

C

Q2: what is $\mathcal{S}[\mathcal{A},\ \ ]$?

Q3: what is $\mathcal{S}[\ \ , f]$?

Three Questions: A Short Encoding

$$\begin{tikzcd} f \arrow[r, red, "\text{constr.}"] & G[f] \\ \mathcal{S}[\mathcal{A}, f] \arrow[u, dotted] & \mathcal{A} \arrow[l, blue, "\text{red.}"'] \arrow[u, dotted] \end{tikzcd}$$

Q1: what is $G[f]$?

C A

Q2: what is $\mathcal{S}[\mathcal{A},\quad]$?

Q3: what is $\mathcal{S}[\quad, f]$?

Three Questions: A Short Encoding

$$\begin{tikzcd} f \arrow[r, "\text{constr.}"] & G[f] \\ \mathcal{S}[\mathcal{A}, f] \arrow[u, dotted] & \mathcal{A} \arrow[l, "\text{red.}"'] \arrow[u, dotted] \end{tikzcd}$$

Q1: what is $G[f]$?

C A P

Q2: what is $\mathcal{S}[\mathcal{A},\ \ ]$?

Q3: what is $\mathcal{S}[\ \ , f]$?

Three Questions: A Short Encoding

$$\begin{tikzcd}
f \arrow[r, "\text{constr.}"] & G[f] \\
\mathcal{S}[\mathcal{A}, f] \arrow[u, dotted] & \mathcal{A} \arrow[l, "\text{red.}"'] \arrow[u, dotted]
\end{tikzcd}$$

Q1: what is $G[f]$?

C A P

Q2: what is $\mathcal{S}[\mathcal{A},\ \ ]$?

Q3: what is $\mathcal{S}[\ \ , f]$?

- $C, A, P \in \{\mathrm{N}, \mathrm{B}\}$
- <u>N</u>on black box / <u>B</u>lack box

Obtaining Actual Definitions

$$\begin{tikzcd} f \arrow[r, "\text{constr.}"] & G[f] \\ \mathcal{S}[\mathcal{A}, f] \arrow[u, dotted] & \mathcal{A} \arrow[l, "\text{red.}"'] \arrow[u, dotted] \end{tikzcd}$$

example: BBB

1. what is $G[f]$? B "$\exists G$" $\prec$ "$\forall f$"
   what is $\mathcal{S}[\mathcal{A},\ \ ]$? B
   what is $\mathcal{S}[\ \ , f]$? B

Obtaining Actual Definitions

$$\begin{tikzcd} f \arrow[r, "\text{constr.}"] & G[f] \\ \mathcal{S}[\mathcal{A}, f] \arrow[u, dotted] & \mathcal{A} \arrow[l, "\text{red.}"'] \arrow[u, dotted] \end{tikzcd}$$

example: BBB

1. what is $G[f]$? B "$\exists G$" $\prec$ "$\forall f$"
   what is $\mathcal{S}[\mathcal{A},\ \ ]$? B "$\exists \mathcal{S}$" $\prec$ "$\forall \mathcal{A}$"
   what is $\mathcal{S}[\ \ , f]$? B "$\exists \mathcal{S}$" $\prec$ "$\forall f$"

2. "$\exists G$", "$\exists \mathcal{S}$" $\prec$ "$\forall f$", "$\forall \mathcal{A}$"

Obtaining Actual Definitions

$$\begin{tikzcd} f \arrow[r, red, "\text{constr.}"] & G[f] \\ \mathcal{S}[\mathcal{A}, f] \arrow[u, dotted] & \mathcal{A} \arrow[l, blue, "\text{red.}"'] \arrow[u, dotted] \end{tikzcd}$$

example: BBB

1. what is $G[f]$? B "$\exists G$" $\prec$ "$\forall f$"
   what is $\mathcal{S}[\mathcal{A},\ \ ]$? B "$\exists\mathcal{S}$" $\prec$ "$\forall\mathcal{A}$"
   what is $\mathcal{S}[\ \ , f]$? B "$\exists\mathcal{S}$" $\prec$ "$\forall f$"

2. "$\exists G$", "$\exists\mathcal{S}$" $\prec$ "$\forall f$", "$\forall\mathcal{A}$"

3. $\exists G, \mathcal{S}\, \forall f, \mathcal{A}$ $\quad$ $\mathcal{A}^{f, G^f}$ breaks $G^f \Longrightarrow \mathcal{S}^{\mathcal{A}^f, f}$ breaks f

Obtaining Actual Definitions

$$\begin{tikzcd} f \arrow[r, "\text{constr.}"] & G[f] \\ \mathcal{S}[\mathcal{A}, f] \arrow[u, dotted] & \mathcal{A} \arrow[l, "\text{red.}"'] \arrow[u, dotted] \end{tikzcd}$$

example: NBB

1. what is $G[f]$? N "$\forall f$" $\prec$ "$\exists G$"
   what is $\mathcal{S}[\mathcal{A},\ \ ]$? B "$\exists \mathcal{S}$" $\prec$ "$\forall \mathcal{A}$"
   what is $\mathcal{S}[\ \ , f]$? B "$\exists \mathcal{S}$" $\prec$ "$\forall f$"

2. "$\exists \mathcal{S}$" $\prec$ "$\forall f$" $\prec$ "$\exists G$" and "$\exists \mathcal{S}$" $\prec$ "$\forall \mathcal{A}$"

3. $\exists \mathcal{S}\, \forall f \exists G \forall \mathcal{A}$ $\qquad$ $\mathcal{A}^{f,G^f}$ breaks $G^f \Longrightarrow \mathcal{S}^{\mathcal{A}^f, f}$ breaks f

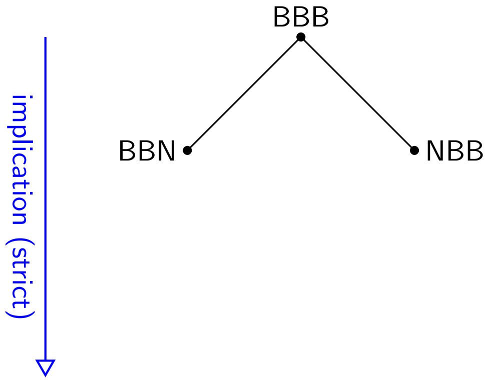
Obtaining Actual Definitions (cont'd)

$$\begin{tikzcd} f \arrow[r, "\text{constr.}"] & G[f] \\ \mathcal{S}[\mathcal{A}, f] \arrow[u, dotted] & \mathcal{A} \arrow[l, "\text{red.}"'] \arrow[u, dotted] \end{tikzcd}$$

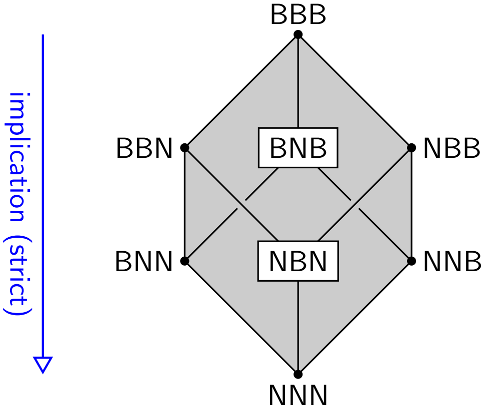
Name	Summary of definition				
BBB	$\exists G$	$\exists \mathcal{S}$	$\forall f$	$\forall \mathcal{A}$	$((G^f, \mathcal{A}^f) \Rightarrow (f, \mathcal{S}^{\mathcal{A},f}))$
BNB	$\exists G$	$\forall \mathcal{A}$	$\exists \mathcal{S}$	$\forall f$	$((G^f, \mathcal{A}^f) \Rightarrow (f, \mathcal{S}^{\mathcal{A},f}))$
BBN	$\exists G$	$\forall f$	$\exists \mathcal{S}$	$\forall \mathcal{A}$	$((G^f, \mathcal{A}^f) \Rightarrow (f, \mathcal{S}^{\mathcal{A},f}))$
BNN	$\exists G$	$\forall f$	$\forall \mathcal{A}$	$\exists \mathcal{S}$	$((G^f, \mathcal{A}^f) \Rightarrow (f, \mathcal{S}^{\mathcal{A},f}))$
NBB	$\exists \mathcal{S}$	$\forall f$	$\exists G$	$\forall \mathcal{A}$	$((G^f, \mathcal{A}^f) \Rightarrow (f, \mathcal{S}^{\mathcal{A},f}))$
NBN	$\forall f$	$\exists G$	$\exists \mathcal{S}$	$\forall \mathcal{A}$	$((G^f, \mathcal{A}^f) \Rightarrow (f, \mathcal{S}^{\mathcal{A},f}))$
NNN	$\forall f$	$\exists G$	$\forall \mathcal{A}$	$\exists \mathcal{S}$	$((G^f, \mathcal{A}^f) \Rightarrow (f, \mathcal{S}^{\mathcal{A},f}))$

see page 305 of the proceedings (Part I)

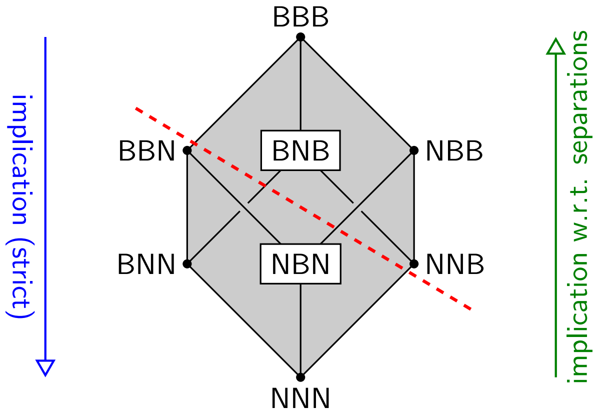
Basic Relations



Basic Relations



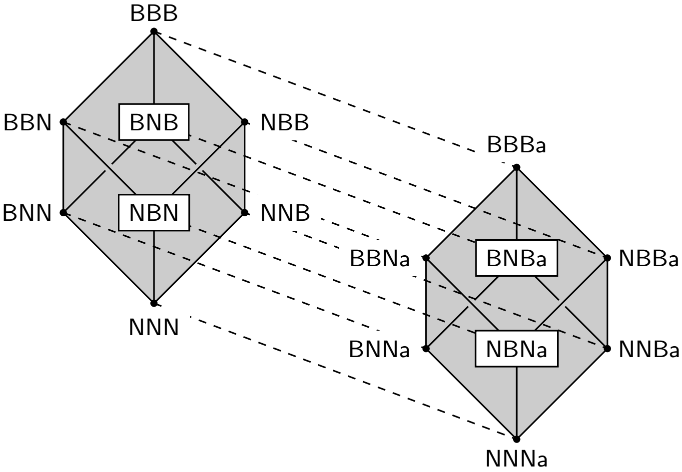
Basic Relations



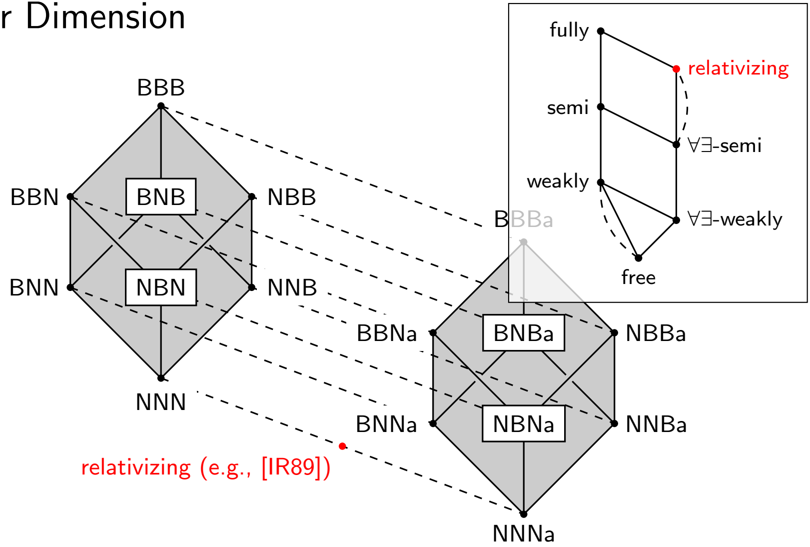
There is More...

- adversaries $\mathcal{A}$ can be PPT or inefficient
  - [RTV04]: mixed
  - here: inefficient up to now
- all previous notions can be considered for efficient adversaries
- shorthand: CAPa, restricted quantification $\forall\,\text{PPT}\mathcal{A}$

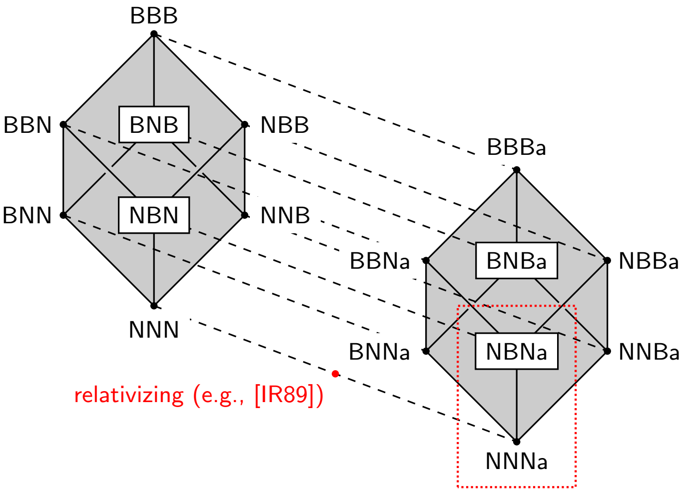
Another Dimension



Another Dimension



Another Dimension

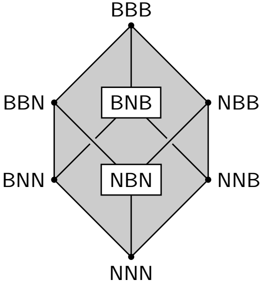


note: not all *CAP*a implications are strict

Neither B nor N

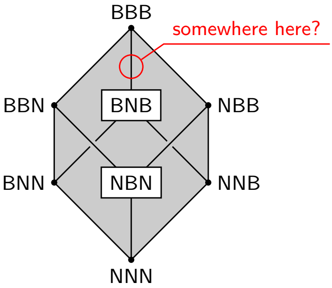
Parameterized Reductions

- consider the Goldreich–Levin hardcore bit [GL89]
- reduction requires success probability of adversary (but nothing else)
- black box? non black box?



Parameterized Reductions

- consider the Goldreich–Levin hardcore bit [GL89]
- reduction requires success probability of adversary (but nothing else)
- black box? non black box?



- parameterized reduction
- here: par($\mathcal{A}$) := success probability
- BBB w/ param: $\mathcal{A}^{f,G^f}$ breaks $G^f \Longrightarrow \mathcal{S}^{\mathcal{A}^f,f}(\text{par}(\mathcal{A}))$ breaks f

$\rightarrow$ *parameters made explicit*

Summary

- things I forgot to tell you
  - CAPp: efficient primitives
  - CAPap: efficient adversaries and efficient primitives
  - careful when defining primitives

Summary

- things I forgot to tell you
  - *CAP*p: efficient primitives
  - *CAP*ap: efficient adversaries and efficient primitives
  - careful when defining primitives
- things to remember
  - given any reduction/separation, ask three (five) questions
  - "impossibility" rarely means *impossible*
  - look for hidden parameters

The End

Thank you!

?

References

Oded Goldreich and Leonid A. Levin.
A hard-core predicate for all one-way functions.
In STOC 1989 [STO89], pages 25–32.

Russell Impagliazzo and Steven Rudich.
Limits on the provable consequences of one-way permutations.
In STOC 1989 [STO89], pages 44–61.

Omer Reingold, Luca Trevisan, and Salil P. Vadhan.
Notions of reducibility between cryptographic primitives.
In Moni Naor, editor, *TCC 2004: 1st Theory of Cryptography Conference*, volume 2951 of *Lecture Notes in Computer Science*, pages 1–20, Cambridge, MA, USA, February 19–21, 2004. Springer, Berlin, Germany.

21st Annual ACM Symposium on Theory of Computing, Seattle, Washington, USA, May 15–17, 1989.
ACM Press.

Another Dimension for Efficie