How to manipulate standards

Daniel J. Bernstein

Verizon Communications Inc.

manipulate standards

. Bernstein

Communications Inc.

You understand and hereby agree
udio, video, and text of this
n are provided "as is", without
any kind, whether expressed
including, without limitation,
warranties of merchantability,
a particular purpose or otherwise.
are not a blithering idiot, you also
that Verizon Communications Inc.
tire Verizon family of companies
ually associated in any way with
, have not reviewed the contents of
tation, and are not responsible for
s of this presentation. Continuing
ten to, or otherwise absorb this
constitutes acceptance of this
y court dispute regarding this
n shall be resolved in the state
n the United States of America.

Our core
Deliverin
from poi

Alice

Verizon is a global leader
delivering innovative
communications and technology
solutions that improve the way
our customers live, work and play.

e standards

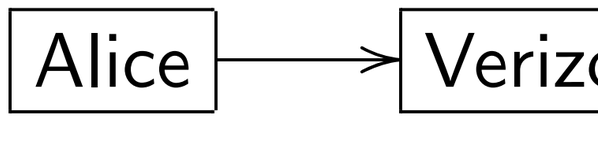
n

cations Inc.

d and hereby agree
d text of this
"as is", without
nether expressed
hout limitation,
merchantability,
urpose or otherwise.
nering idiot, you also
Communications Inc.
mily of companies
ed in any way with
viewed the contents of
e not responsible for
entation. Continuing
erwise absorb this
cceptance of this
te regarding this
olved in the state
States of America.

Verizon is a global leader
delivering innovative
communications and technology
solutions that improve the way
our customers live, work and play.

Our core mission:
Delivering informa
from point A to p



ls

c.

agree

out
ed
n,
ty,
erwise.
ou also
ons Inc.
anies
with
ntents of
ble for
tinuing
this
this
his
tate
erica.

Verizon is a global leader
delivering innovative
communications and technology
solutions that improve the way
our customers live, work and play.

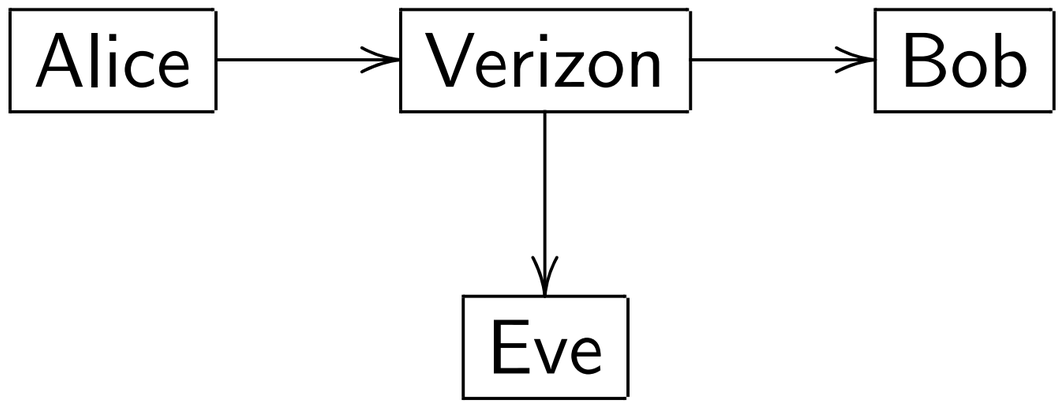
Our core mission:
Delivering information
from point A to point B.

Our core mission:
Delivering information
from point A to point B.

Verizon is a global leader
delivering innovative
communications and technology
solutions that improve the way
our customers live, work and play.

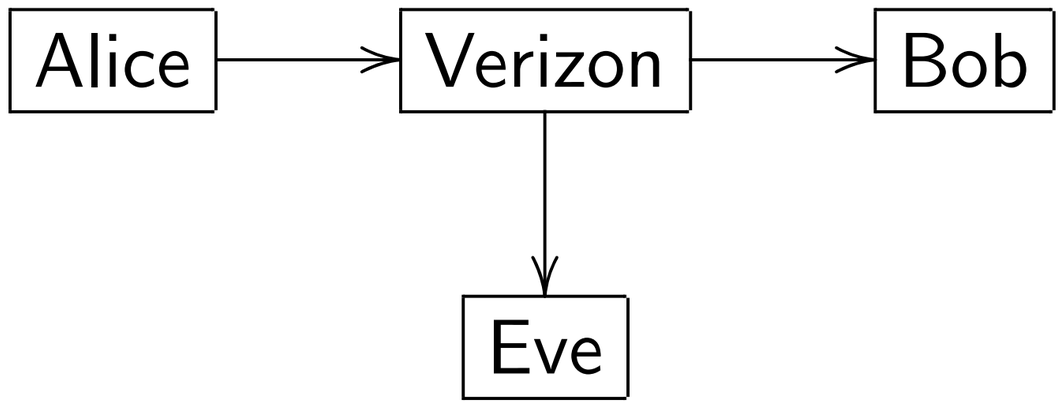
Verizon is a global leader
delivering innovative
communications and technology
solutions that improve the way
our customers live, work and play.

Our core mission:
Delivering information
from point A to point B,
and also to points C, D, E, ...



Verizon is a global leader
delivering innovative
communications and technology
solutions that improve the way
our customers live, work and play.

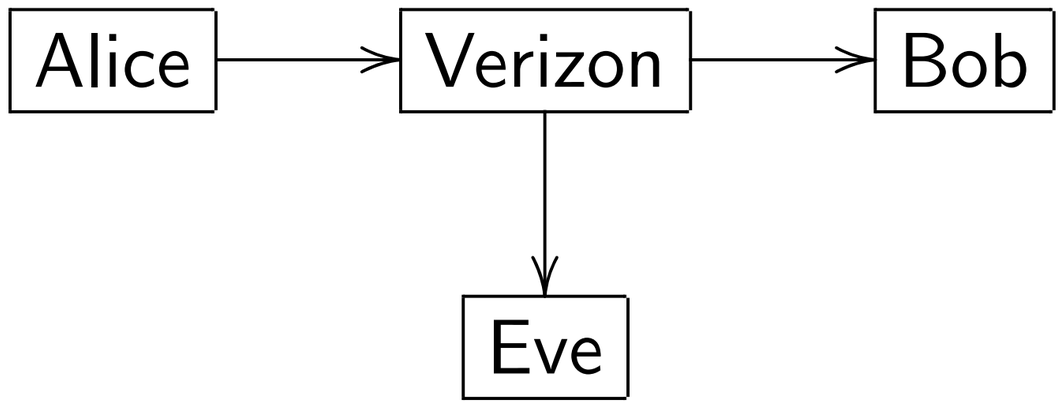
Our core mission:
Delivering information
from point A to point B,
and also to points C, D, E, ...



"Can you hear me now? Good."

Verizon is a global leader
delivering innovative
communications and technology
solutions that improve the way
our customers live, work and play.

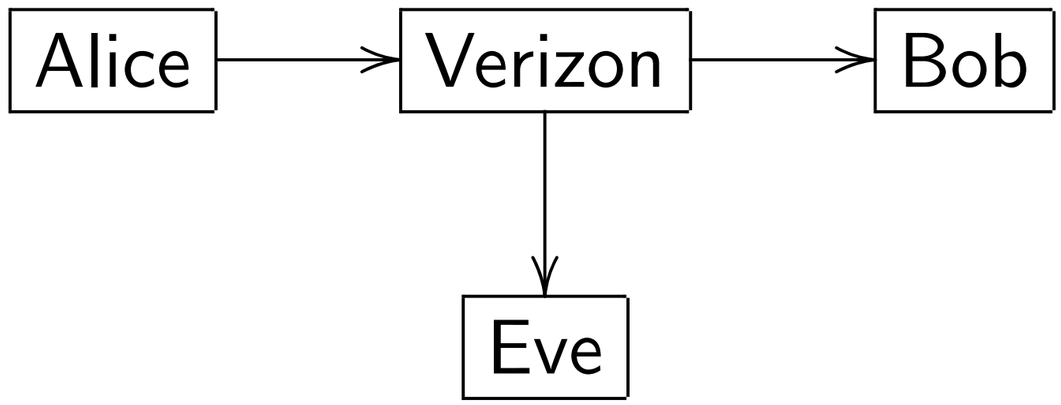
Our core mission:
Delivering information
from point A to point B,
and also to points C, D, E, ...



"Can you hear me now? Good."
"Can they hear you now? Good."

Verizon is a global leader
delivering innovative
communications and technology
solutions that improve the way
our customers live, work and play.

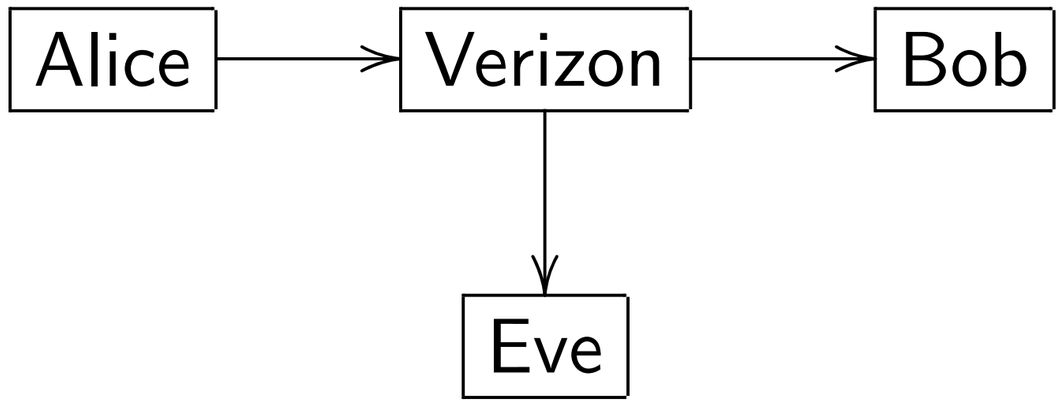
Our core mission:
Delivering information
from point A to point B,
and also to points C, D, E, ...



"Can you hear me now? Good."
"Can they hear you now? Good."
"We never stop working for you."

Verizon is a global leader
delivering innovative
communications and technology
solutions that improve the way
our customers live, work and play.

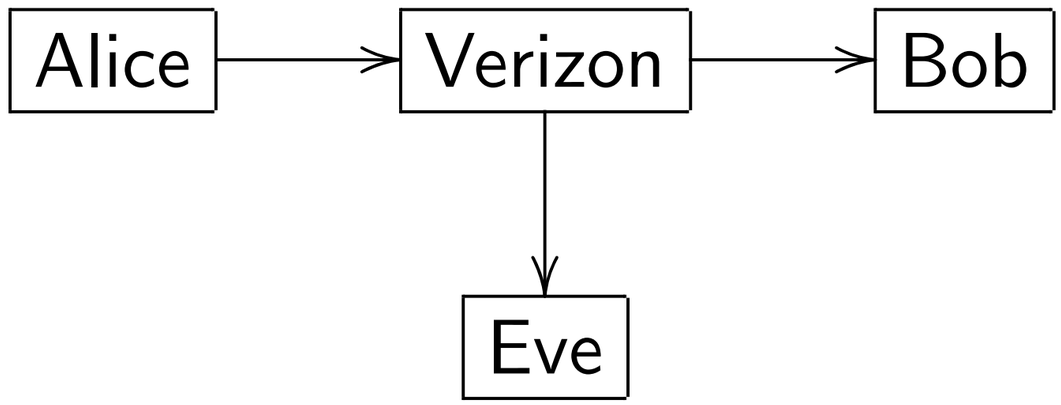
Our core mission:
Delivering information
from point A to point B,
and also to points C, D, E, ...



"Can you hear me now? Good."
"Can they hear you now? Good."
"We never stop working for you."
"Rule the air."

Verizon is a global leader
delivering innovative
communications and technology
solutions that improve the way
our customers live, work and play.

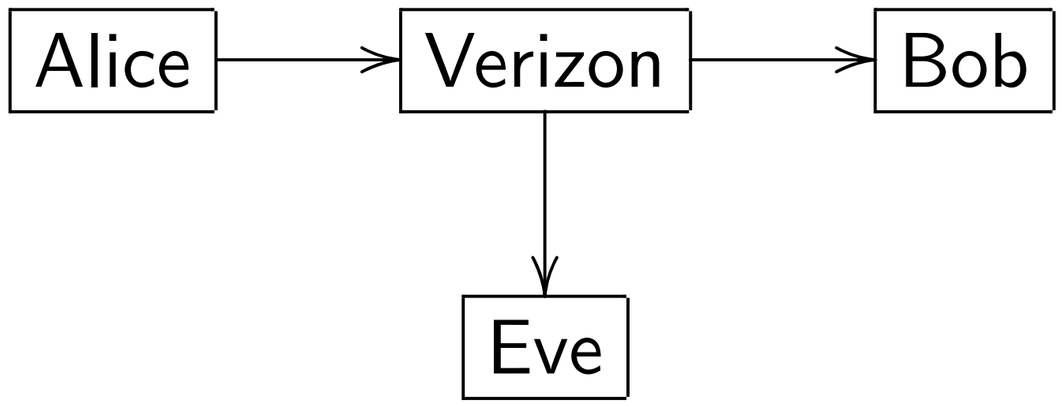
Our core mission:
Delivering information
from point A to point B,
and also to points C, D, E, ...



"Can you hear me now? Good."
"Can they hear you now? Good."
"We never stop working for you."
"Rule the air."
"Never settle."

Verizon is a global leader
delivering innovative
communications and technology
solutions that improve the way
our customers live, work and play.

Our core mission:
Delivering information
from point A to point B,
and also to points C, D, E, ...

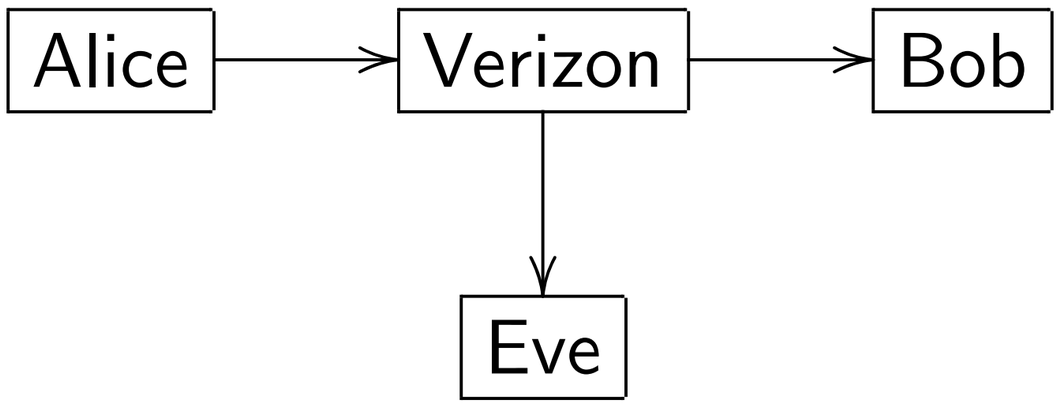


"Can you hear me now? Good."
"Can they hear you now? Good."
"We never stop working for you."
"Rule the air."
"Never settle."
"I am the man in the middle."

Ultimate

is a global leader
g innovative
nications and technology
s that improve the way
omers live, work and play.

Our core mission:
Delivering information
from point A to point B,
and also to points C, D, E, . . .



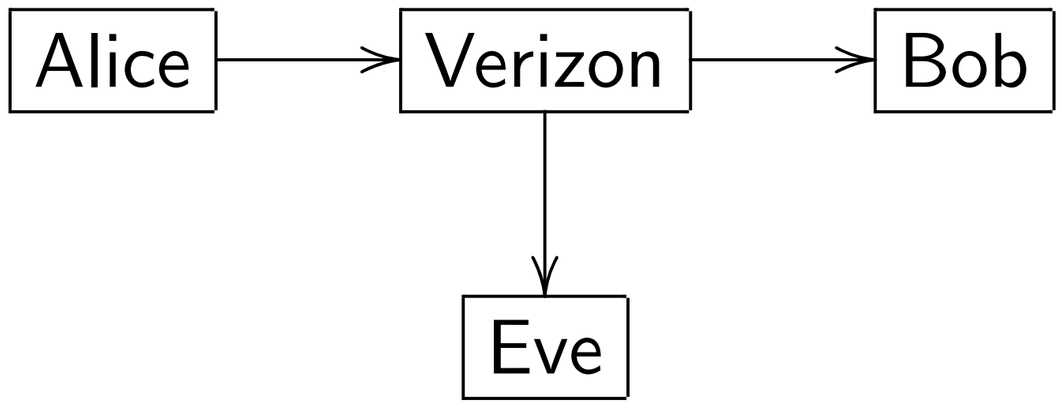
“Can you hear me now? Good.”
“Can they hear you now? Good.”
“We never stop working for you.”
“Rule the air.”
“Never settle.”
“I am the man in the middle.”

Our core mission:

Delivering information

from point A to point B,

and also to points C, D, E, . . .



"Can you hear me now? Good."

"Can they hear you now? Good."

"We never stop working for you."

"Rule the air."

"Never settle."

"I am the man in the middle."

Ultimate goal: Ma

l leader

ve

nd technology

rove the way

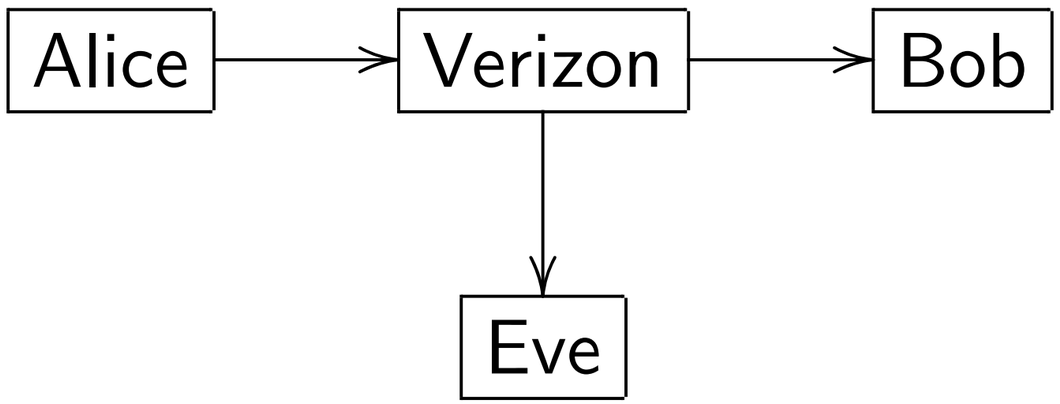
, work and play.

Our core mission:

Delivering information

from point A to point B,

and also to points C, D, E, ...



"Can you hear me now? Good."

"Can they hear you now? Good."

"We never stop working for you."

"Rule the air."

"Never settle."

"I am the man in the middle."

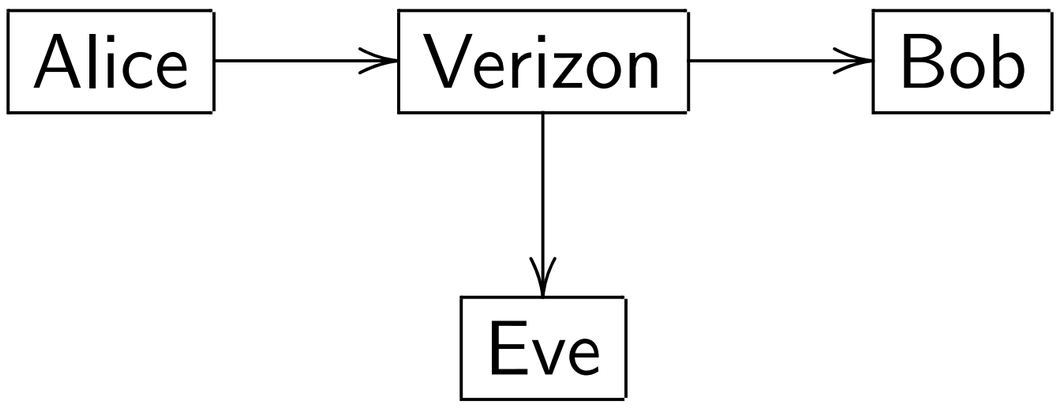
Ultimate goal: Make money

logy

vay

d play.

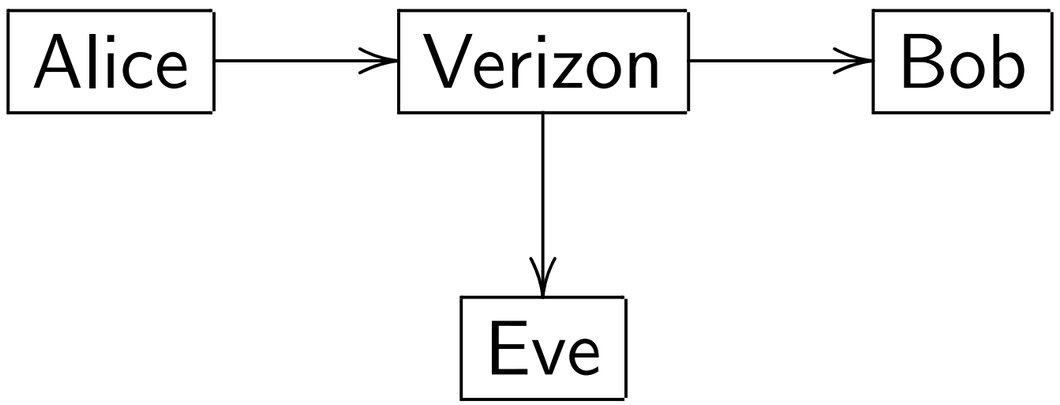
Our core mission:
Delivering information
from point A to point B,
and also to points C, D, E, ...



"Can you hear me now? Good."
"Can they hear you now? Good."
"We never stop working for you."
"Rule the air."
"Never settle."
"I am the man in the middle."

Ultimate goal: Make money.

Our core mission:
Delivering information
from point A to point B,
and also to points C, D, E, ...

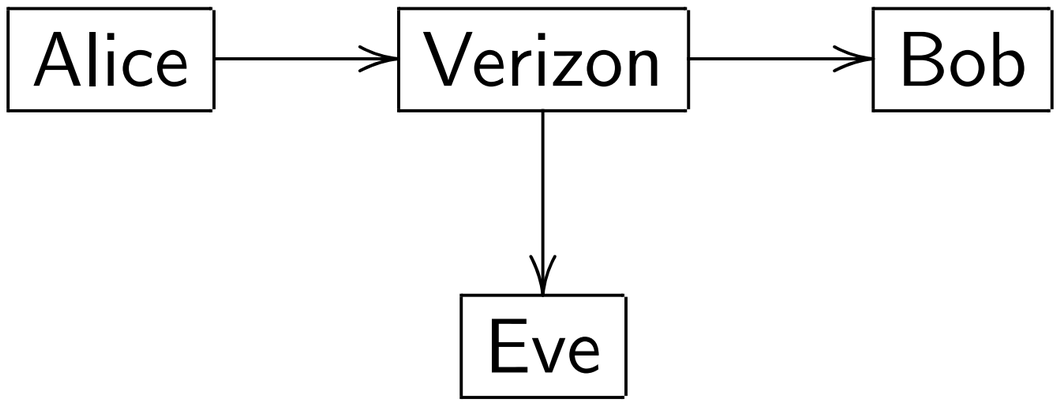


"Can you hear me now? Good."
"Can they hear you now? Good."
"We never stop working for you."
"Rule the air."
"Never settle."
"I am the man in the middle."

Ultimate goal: Make money.

NSA "pays AT&T, Verizon and Sprint several hundred million dollars a year for access to 81% of all international phone calls into the US."

Our core mission:
Delivering information
from point A to point B,
and also to points C, D, E, ...



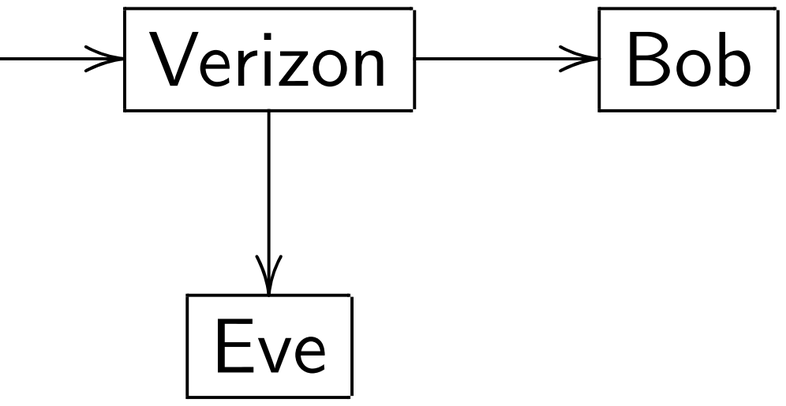
"Can you hear me now? Good."
"Can they hear you now? Good."
"We never stop working for you."
"Rule the air."
"Never settle."
"I am the man in the middle."

Ultimate goal: Make money.

NSA "pays AT&T, Verizon and Sprint several hundred million dollars a year for access to 81% of all international phone calls into the US."

"Precision Market Insights, Verizon's data marketing arm ... will now sell its tool to advertisers for mobile ad campaigns that target Verizon's massive subscriber base based on demographics, interests and geography."

e mission:
ng information
int A to point B,
to points C, D, E, ...



u hear me now? Good."
ey hear you now? Good."
ver stop working for you."
ne air."
settle."
ne man in the middle."

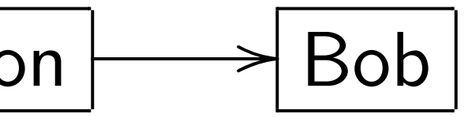
Ultimate goal: Make money.

NSA "pays AT&T, Verizon and Sprint several hundred million dollars a year for access to 81% of all international phone calls into the US."

"Precision Market Insights, Verizon's data marketing arm ... will now sell its tool to advertisers for mobile ad campaigns that target Verizon's massive subscriber base based on demographics, interests and geography."

Many of
rely on **y**
to send

tion
oint B,
C, D, E, . . .



e

now? Good."
u now? Good."
orking for you."

the middle."

Ultimate goal: Make money.

NSA "pays AT&T, Verizon and Sprint several hundred million dollars a year for access to 81% of all international phone calls into the US."

"Precision Market Insights, Verizon's data marketing arm . . . will now sell its tool to advertisers for mobile ad campaigns that target Verizon's massive subscriber base based on demographics, interests and geography."

Many of our comp
rely on **your brow**
to send data to Ev

...

Bob

od."

ood."

you."

e."

Ultimate goal: Make money.

NSA "pays AT&T, Verizon and Sprint several hundred million dollars a year for access to 81% of all international phone calls into the US."

"Precision Market Insights, Verizon's data marketing arm ... will now sell its tool to advertisers for mobile ad campaigns that target Verizon's massive subscriber base based on demographics, interests and geography."

Many of our competitors rely on **your browser** to send data to Eve.

Ultimate goal: Make money.

NSA "pays AT&T, Verizon and Sprint several hundred million dollars a year for access to 81% of all international phone calls into the US."

"Precision Market Insights, Verizon's data marketing arm ... will now sell its tool to advertisers for mobile ad campaigns that target Verizon's massive subscriber base based on demographics, interests and geography."

Many of our competitors rely on **your browser** to send data to Eve.

Ultimate goal: Make money.

NSA "pays AT&T, Verizon and Sprint several hundred million dollars a year for access to 81% of all international phone calls into the US."

"Precision Market Insights, Verizon's data marketing arm ... will now sell its tool to advertisers for mobile ad campaigns that target Verizon's massive subscriber base based on demographics, interests and geography."

Many of our competitors rely on **your browser** to send data to Eve.

"Libert has discovered that the vast majority of health sites, from the for-profit WebMD.com to the government-run CDC.gov, are loaded with tracking elements that are sending records of your health inquiries to the likes of web giants like Google, Facebook, and Pinterest, and data brokers like Experian and Acxiom."

e goal: Make money.

ays AT&T, Verizon and
everal hundred million
year for access to 81%
ternational phone calls
US."

on Market Insights,
s data marketing arm ...
sell its tool to advertisers
le ad campaigns
get Verizon's massive
er base based on
aphics, interests and
hy."

Many of our competitors
rely on **your browser**
to send data to Eve.

"Libert has discovered that the vast majority of health sites, from the for-profit WebMD.com to the government-run CDC.gov, are loaded with tracking elements that are sending records of your health inquiries to the likes of web giants like Google, Facebook, and Pinterest, and data brokers like Experian and Acxiom."

We are
You **give**
We **redi**
We **moc**

ake money.

, Verizon and
dred million
access to 81%
phone calls

Insights,
rketing arm . . .
ol to advertisers
paigns
n's massive
sed on
erests and

Many of our competitors
rely on **your browser**
to send data to Eve.

"Libert has discovered that the vast majority of health sites, from the for-profit WebMD.com to the government-run CDC.gov, are loaded with tracking elements that are sending records of your health inquiries to the likes of web giants like Google, Facebook, and Pinterest, and data brokers like Experian and Acxiom."

We are **your netw**
You **give us** your
We **redirect it** to
We **modify it to**

.

and

on

31%

lls

m ...

rtisers

e

Many of our competitors
rely on **your browser**
to send data to Eve.

"Libert has discovered that the vast majority of health sites, from the for-profit WebMD.com to the government-run CDC.gov, are loaded with tracking elements that are sending records of your health inquiries to the likes of web giants like Google, Facebook, and Pinterest, and data brokers like Experian and Acxiom."

We are **your network**.
You **give us** your data.
We **redirect it** to Eve.
We **modify it to help Eve**.

Many of our competitors
rely on **your browser**
to send data to Eve.

"Libert has discovered that the vast majority of health sites, from the for-profit WebMD.com to the government-run CDC.gov, are loaded with tracking elements that are sending records of your health inquiries to the likes of web giants like Google, Facebook, and Pinterest, and data brokers like Experian and Acxiom."

We are **your network**.
You **give us** your data.
We **redirect it** to Eve.
We **modify it to help Eve**.

Many of our competitors
rely on **your browser**
to send data to Eve.

"Libert has discovered that the vast majority of health sites, from the for-profit WebMD.com to the government-run CDC.gov, are loaded with tracking elements that are sending records of your health inquiries to the likes of web giants like Google, Facebook, and Pinterest, and data brokers like Experian and Acxiom."

We are **your network**.
You **give us** your data.
We **redirect it** to Eve.
We **modify it to help Eve**.

"In an effort to better serve advertisers, Verizon Wireless has been silently modifying its users' web traffic on its network to inject a cookie-like tracker. This tracker, included in an HTTP header called X-UIDH, is sent to every unencrypted website a Verizon customer visits from a mobile device."

f our competitors
your browser
data to Eve.

has discovered that the
jority of health sites, from
profit WebMD.com to the
ment-run CDC.gov, are
with tracking elements
sending records of your
nquiries to the likes of web
ke Google, Facebook, and
t, and data brokers like
n and Acxiom."

We are **your network**.
You **give us** your data.
We **redirect it** to Eve.
We **modify it to help Eve**.

"In an effort to better serve advertisers, Verizon Wireless has been silently modifying its users' web traffic on its network to inject a cookie-like tracker. This tracker, included in an HTTP header called X-UIDH, is sent to every unencrypted website a Verizon customer visits from a mobile device."

"Verizon
marketin
Experian
and Ora
anonymo
the Prec
third-par

petitors
ser
ve.

ered that the
ealth sites, from
MD.com to the
DC.gov, are
ng elements
ecords of your
the likes of web
Facebook, and
a brokers like
om."

We are **your network**.
You **give us** your data.
We **redirect it** to Eve.
We **modify it to help Eve**.

"In an effort to better serve advertisers, Verizon Wireless has been silently modifying its users' web traffic on its network to inject a cookie-like tracker. This tracker, included in an HTTP header called X-UIDH, is sent to every unencrypted website a Verizon customer visits from a mobile device."

"Verizon has partn
marketing data pro
Experian Marketin
and Oracle's Bluek
anonymous match
the Precision ID ic
third-party data.

the
, from
to the
re
ts
your
of web
k, and
like

We are **your network**.
You **give us** your data.
We **redirect it** to Eve.
We **modify it to help Eve**.

"In an effort to better serve advertisers, Verizon Wireless has been silently modifying its users' web traffic on its network to inject a cookie-like tracker. This tracker, included in an HTTP header called X-UIDH, is sent to every unencrypted website a Verizon customer visits from a mobile device."

"Verizon has partnerships w
marketing data providers lik
Experian Marketing Services
and Oracle's BlueKai to ena
anonymous matches betwee
the Precision ID identifier a
third-party data.

We are **your network**.
You **give us** your data.
We **redirect it** to Eve.
We **modify it to help Eve**.

"In an effort to better serve advertisers, Verizon Wireless has been silently modifying its users' web traffic on its network to inject a cookie-like tracker. This tracker, included in an HTTP header called X-UIDH, is sent to every unencrypted website a Verizon customer visits from a mobile device."

"Verizon has partnerships with marketing data providers like Experian Marketing Services and Oracle's BlueKai to enable anonymous matches between the Precision ID identifier and third-party data.

We are **your network**.
You **give us** your data.
We **redirect it** to Eve.
We **modify it to help Eve**.

"In an effort to better serve advertisers, Verizon Wireless has been silently modifying its users' web traffic on its network to inject a cookie-like tracker. This tracker, included in an HTTP header called X-UIDH, is sent to every unencrypted website a Verizon customer visits from a mobile device."

"Verizon has partnerships with marketing data providers like Experian Marketing Services and Oracle's BlueKai to enable anonymous matches between the Precision ID identifier and third-party data. Although there's deterministic linkage back to the hashed ID, Verizon's data partners are not able to collect or save the data profiles."

We are **your network**.
You **give us** your data.
We **redirect it** to Eve.
We **modify it to help Eve**.

"In an effort to better serve advertisers, Verizon Wireless has been silently modifying its users' web traffic on its network to inject a cookie-like tracker. This tracker, included in an HTTP header called X-UIDH, is sent to every unencrypted website a Verizon customer visits from a mobile device."

"Verizon has partnerships with marketing data providers like Experian Marketing Services and Oracle's BlueKai to enable anonymous matches between the Precision ID identifier and third-party data. Although there's deterministic linkage back to the hashed ID, Verizon's data partners are not able to collect or save the data profiles." . . . "Rather than a universal ID, I think there will probably be really rich algorithms that can tie multiple IDs together into a rationalized campaign."

your network.
e us your data.
rect it to Eve.
dify it to help Eve.

ffort to better serve
ers, Verizon Wireless has
ently modifying its users'
ffic on its network to
cookie-like tracker. This
included in an HTTP
called X-UIDH, is sent
unencrypted website a
customer visits from a
device."

"Verizon has partnerships with marketing data providers like Experian Marketing Services and Oracle's BlueKai to enable anonymous matches between the Precision ID identifier and third-party data. Although there's deterministic linkage back to the hashed ID, Verizon's data partners are not able to collect or save the data profiles." . . . "Rather than a universal ID, I think there will probably be really rich algorithms that can tie multiple IDs together into a rationalized campaign."

Political

"A Cong
the mult
brokerag
that coll
personal
for mark
intensify

work.
data.
Eve.
help Eve.

etter serve
n Wireless has
fying its users'
network to
e tracker. This
n an HTTP
IDH, is sent
ted website a
visits from a

"Verizon has partnerships with marketing data providers like Experian Marketing Services and Oracle's BlueKai to enable anonymous matches between the Precision ID identifier and third-party data. Although there's deterministic linkage back to the hashed ID, Verizon's data partners are not able to collect or save the data profiles." . . . "Rather than a universal ID, I think there will probably be really rich algorithms that can tie multiple IDs together into a rationalized campaign."

Political backlash?

"A Congressional
the multibillion-do
brokerage industry
that collect, analy
personal details ab
for marketing purp
intensifying."

s has
sers'
o
This
P
nt
e a
n a

"Verizon has partnerships with marketing data providers like Experian Marketing Services and Oracle's BlueKai to enable anonymous matches between the Precision ID identifier and third-party data. Although there's deterministic linkage back to the hashed ID, Verizon's data partners are not able to collect or save the data profiles." . . . "Rather than a universal ID, I think there will probably be really rich algorithms that can tie multiple IDs together into a rationalized campaign."

Political backlash?

"A Congressional probe into the multibillion-dollar data brokerage industry—compan that collect, analyze, sell or personal details about consu for marketing purposes—is intensifying."

"Verizon has partnerships with marketing data providers like Experian Marketing Services and Oracle's BlueKai to enable anonymous matches between the Precision ID identifier and third-party data. Although there's deterministic linkage back to the hashed ID, Verizon's data partners are not able to collect or save the data profiles." . . . "Rather than a universal ID, I think there will probably be really rich algorithms that can tie multiple IDs together into a rationalized campaign."

Political backlash?

"A Congressional probe into the multibillion-dollar data brokerage industry—companies that collect, analyze, sell or share personal details about consumers for marketing purposes—is intensifying."

"Verizon has partnerships with marketing data providers like Experian Marketing Services and Oracle's BlueKai to enable anonymous matches between the Precision ID identifier and third-party data. Although there's deterministic linkage back to the hashed ID, Verizon's data partners are not able to collect or save the data profiles." . . . "Rather than a universal ID, I think there will probably be really rich algorithms that can tie multiple IDs together into a rationalized campaign."

Political backlash?

"A Congressional probe into the multibillion-dollar data brokerage industry—companies that collect, analyze, sell or share personal details about consumers for marketing purposes—is intensifying."

"Experian, the massive data-broker with far-reaching influence over your ability to get a mortgage, credit-card, or job, sold extensive consumer records to an identity thieves' service."

n has partnerships with
ng data providers like
n Marketing Services
cle's BlueKai to enable
ous matches between
cision ID identifier and
rty data. Although there's
nistic linkage back to the
D, Verizon's data partners
able to collect or save the
files." . . . "Rather than
sal ID, I think there will
be really rich algorithms
tie multiple IDs together
tionalized campaign."

Political backlash?

"A Congressional probe into the multibillion-dollar data brokerage industry—companies that collect, analyze, sell or share personal details about consumers for marketing purposes—is intensifying."

"Experian, the massive data-broker with far-reaching influence over your ability to get a mortgage, credit-card, or job, sold extensive consumer records to an identity thieves' service."

Solution

No need

nerships with
oviders like
g Services
Kai to enable
es between
dentifier and
Although there's
ge back to the
n's data partners
llect or save the
"Rather than
hink there will
rich algorithms
ple IDs together
campaign."

Political backlash?

"A Congressional probe into the multibillion-dollar data brokerage industry—companies that collect, analyze, sell or share personal details about consumers for marketing purposes—is intensifying."

"Experian, the massive data-broker with far-reaching influence over your ability to get a mortgage, credit-card, or job, sold extensive consumer records to an identity thieves' service."

Solution: **Talk ab**

No need to **protec**

ith
e
s
ble
n
nd
there's
o the
artners
ve the
than
will
ithms
gether
."

Political backlash?

"A Congressional probe into the multibillion-dollar data brokerage industry—companies that collect, analyze, sell or share personal details about consumers for marketing purposes—is intensifying."

"Experian, the massive data-broker with far-reaching influence over your ability to get a mortgage, credit-card, or job, sold extensive consumer records to an identity thieves' service."

Solution: **Talk about** privac

No need to **protect** privacy.

Political backlash?

"A Congressional probe into the multibillion-dollar data brokerage industry—companies that collect, analyze, sell or share personal details about consumers for marketing purposes—is intensifying."

"Experian, the massive data-broker with far-reaching influence over your ability to get a mortgage, credit-card, or job, sold extensive consumer records to an identity thieves' service."

Solution: **Talk about** privacy.

No need to **protect** privacy.

Political backlash?

"A Congressional probe into the multibillion-dollar data brokerage industry—companies that collect, analyze, sell or share personal details about consumers for marketing purposes—is intensifying."

"Experian, the massive data-broker with far-reaching influence over your ability to get a mortgage, credit-card, or job, sold extensive consumer records to an identity thieves' service."

Solution: **Talk about** privacy.
No need to **protect** privacy.

"Verizon said it is not using or selling its first-party subscriber data, but rather deploying partnerships with third-party data providers to target Verizon's massive consumer base."

Political backlash?

"A Congressional probe into the multibillion-dollar data brokerage industry—companies that collect, analyze, sell or share personal details about consumers for marketing purposes—is intensifying."

"Experian, the massive data-broker with far-reaching influence over your ability to get a mortgage, credit-card, or job, sold extensive consumer records to an identity thieves' service."

Solution: **Talk about** privacy.
No need to **protect** privacy.

"Verizon said it is not using or selling its first-party subscriber data, but rather deploying partnerships with third-party data providers to target Verizon's massive consumer base."

"We will never sacrifice our core business and our commitment to privacy because there's an additional dollar to be made by pumping data out into the ecosystem."

backlash?

gressional probe into
tibillion-dollar data
ge industry—companies
ect, analyze, sell or share
details about consumers
keting purposes—is
ing."

an, the massive data-
with far-reaching influence
r ability to get a
e, credit-card, or job, sold
e consumer records to an
thieves' service."

Solution: **Talk about** privacy.
No need to **protect** privacy.

"Verizon said it is not using or selling its first-party subscriber data, but rather deploying partnerships with third-party data providers to target Verizon's massive consumer base."

"We will never sacrifice our core business and our commitment to privacy because there's an additional dollar to be made by pumping data out into the ecosystem."

Technica

Increasin
Crypto.

?

probe into
llar data
—companies
ze, sell or share
bout consumers
poses—is

ssive data-
aching influence
o get a
card, or job, sold
er records to an
ervice."

Solution: **Talk about** privacy.
No need to **protect** privacy.

"Verizon said it is not using or selling its first-party subscriber data, but rather deploying partnerships with third-party data providers to target Verizon's massive consumer base."

"We will never sacrifice our core business and our commitment to privacy because there's an additional dollar to be made by pumping data out into the ecosystem."

Technical backlash

Increasing problem
Crypto.

nies
share
umers

-
uence

o, sold
to an

Solution: **Talk about** privacy.
No need to **protect** privacy.

"Verizon said it is not using or selling its first-party subscriber data, but rather deploying partnerships with third-party data providers to target Verizon's massive consumer base."

"We will never sacrifice our core business and our commitment to privacy because there's an additional dollar to be made by pumping data out into the ecosystem."

Technical backlash?

Increasing problem for us:
Crypto.

Solution: **Talk about** privacy.

No need to **protect** privacy.

"Verizon said it is not using or selling its first-party subscriber data, but rather deploying partnerships with third-party data providers to target Verizon's massive consumer base."

"We will never sacrifice our core business and our commitment to privacy because there's an additional dollar to be made by pumping data out into the ecosystem."

Technical backlash?

Increasing problem for us:

Crypto.

Solution: **Talk about** privacy.
No need to **protect** privacy.

"Verizon said it is not using or selling its first-party subscriber data, but rather deploying partnerships with third-party data providers to target Verizon's massive consumer base."

"We will never sacrifice our core business and our commitment to privacy because there's an additional dollar to be made by pumping data out into the ecosystem."

Technical backlash?

Increasing problem for us:
Crypto. This "breaks network management, content distribution and network services"; creates "congestion" and "latency";

Solution: **Talk about** privacy.
No need to **protect** privacy.

"Verizon said it is not using or selling its first-party subscriber data, but rather deploying partnerships with third-party data providers to target Verizon's massive consumer base."

"We will never sacrifice our core business and our commitment to privacy because there's an additional dollar to be made by pumping data out into the ecosystem."

Technical backlash?

Increasing problem for us:
Crypto. This "breaks network management, content distribution and network services"; creates "congestion" and "latency"; "limits the ability of network providers to protect customers from web attacks";

Solution: **Talk about** privacy.
No need to **protect** privacy.

"Verizon said it is not using or selling its first-party subscriber data, but rather deploying partnerships with third-party data providers to target Verizon's massive consumer base."

"We will never sacrifice our core business and our commitment to privacy because there's an additional dollar to be made by pumping data out into the ecosystem."

Technical backlash?

Increasing problem for us: **Crypto**. This "breaks network management, content distribution and network services"; creates "congestion" and "latency"; "limits the ability of network providers to protect customers from web attacks"; breaks "UIDH (unique client identifier) insertion" and "data collection for analytics"; breaks "value-add services that are based on access to header and payload content from individual sessions"; etc.

: **Talk about** privacy.
to **protect** privacy.

n said it is not using or
ts first-party subscriber
t rather deploying
hips with third-party
oviders to target Verizon's
consumer base."

l never sacrifice our core
and our commitment
cy because there's an
al dollar to be made
oing data out into the
m."

Technical backlash?

Increasing problem for us:
Crypto. This "breaks network management, content distribution and network services"; creates "congestion" and "latency"; "limits the ability of network providers to protect customers from web attacks"; breaks "UIDH (unique client identifier) insertion" and "data collection for analytics"; breaks "value-add services that are based on access to header and payload content from individual sessions"; etc.

Best cas
No crypt

out privacy.
ct privacy.

not using or
ty subscriber
eploying
third-party
target Verizon's
base."

crifice our core
commitment
e there's an
o be made
out into the

Technical backlash?

Increasing problem for us:
Crypto. This "breaks network management, content distribution and network services"; creates "congestion" and "latency"; "limits the ability of network providers to protect customers from web attacks"; breaks "UIDH (unique client identifier) insertion" and "data collection for analytics"; breaks "value-add services that are based on access to header and payload content from individual sessions"; etc.

Best case for us:
No crypto. Lobby

cy.

or

ber

y

izon's

core

nt

n

e

ne

Technical backlash?

Increasing problem for us:

Crypto. This "breaks network management, content distribution and network services"; creates "congestion" and "latency"; "limits the ability of network providers to protect customers from web attacks"; breaks "UIDH (unique client identifier) insertion" and "data collection for analytics"; breaks "value-add services that are based on access to header and payload content from individual sessions"; etc.

Best case for us:

No crypto. Lobby for this!

Technical backlash?

Increasing problem for us:

Crypto. This "breaks network management, content distribution and network services"; creates "congestion" and "latency"; "limits the ability of network providers to protect customers from web attacks"; breaks "UIDH (unique client identifier) insertion" and "data collection for analytics"; breaks "value-add services that are based on access to header and payload content from individual sessions"; etc.

Best case for us:

No crypto. Lobby for this!

Technical backlash?

Increasing problem for us:

Crypto. This "breaks network management, content distribution and network services"; creates "congestion" and "latency"; "limits the ability of network providers to protect customers from web attacks"; breaks "UIDH (unique client identifier) insertion" and "data collection for analytics"; breaks "value-add services that are based on access to header and payload content from individual sessions"; etc.

Best case for us:

No crypto. Lobby for this!

Almost as good for us:

"Opportunistic encryption"

without authentication.

"Stops passive eavesdropping"

but **we aren't passive**.

Technical backlash?

Increasing problem for us:

Crypto. This "breaks network management, content distribution and network services"; creates "congestion" and "latency"; "limits the ability of network providers to protect customers from web attacks"; breaks "UIDH (unique client identifier) insertion" and "data collection for analytics"; breaks "value-add services that are based on access to header and payload content from individual sessions"; etc.

Best case for us:

No crypto. Lobby for this!

Almost as good for us:

"Opportunistic encryption" without authentication.

"Stops passive eavesdropping" but **we aren't passive**.

Almost as good for us:

Signatures on some data.

We can still see everything.

Can also censor quite selectively.

Can't modify signed data but can track in many other ways.

al backlash?

ng problem for us:

This "breaks network
ment, content distribution
work services"; creates
tion" and "latency";
he ability of network
s to protect customers
b attacks"; breaks
(unique client identifier)
" and "data collection
ytics"; breaks "value-add
that are based on access
er and payload content
lividual sessions"; etc.

Best case for us:

No crypto. Lobby for this!

Almost as good for us:

"Opportunistic encryption"
without authentication.
"Stops passive eavesdropping"
but **we aren't passive**.

Almost as good for us:

Signatures on some data.
We can still see everything.
Can also censor quite selectively.
Can't modify signed data but
can track in many other ways.

More tro
authenti
But we s
adequate

n?

n for us:
eaks network
tent distribution
ces"; creates
"latency";
of network
ct customers
; breaks
ent identifier)
ata collection
aks "value-add
ased on access
load content
ssions"; etc.

Best case for us:
No crypto. Lobby for this!

Almost as good for us:
"Opportunistic encryption"
without authentication.
"Stops passive eavesdropping"
but **we aren't passive**.

Almost as good for us:
Signatures on some data.
We can still see everything.
Can also censor quite selectively.
Can't modify signed data but
can track in many other ways.

More troublesome
authenticated encr
But we still see m
adequate for most

ork
bution
es
k
ers
fier)
on
-add
ccess
ent
c.

Best case for us:

No crypto. Lobby for this!

Almost as good for us:

"Opportunistic encryption"

without authentication.

"Stops passive eavesdropping"

but **we aren't passive**.

Almost as good for us:

Signatures on some data.

We can still see everything.

Can also censor quite selectively.

Can't modify signed data but

can track in many other ways.

More troublesome: End-to-e

authenticated encryption.

But we still see metadata—

adequate for most surveillan

Best case for us:

No crypto. Lobby for this!

Almost as good for us:

"Opportunistic encryption"

without authentication.

"Stops passive eavesdropping"

but **we aren't passive**.

Almost as good for us:

Signatures on some data.

We can still see everything.

Can also censor quite selectively.

Can't modify signed data but

can track in many other ways.

More troublesome: End-to-end

authenticated encryption.

But we still see metadata—

adequate for most surveillance.

Best case for us:

No crypto. Lobby for this!

Almost as good for us:

"Opportunistic encryption"

without authentication.

"Stops passive eavesdropping"

but **we aren't passive**.

Almost as good for us:

Signatures on some data.

We can still see everything.

Can also censor quite selectively.

Can't modify signed data but

can track in many other ways.

More troublesome: End-to-end

authenticated encryption.

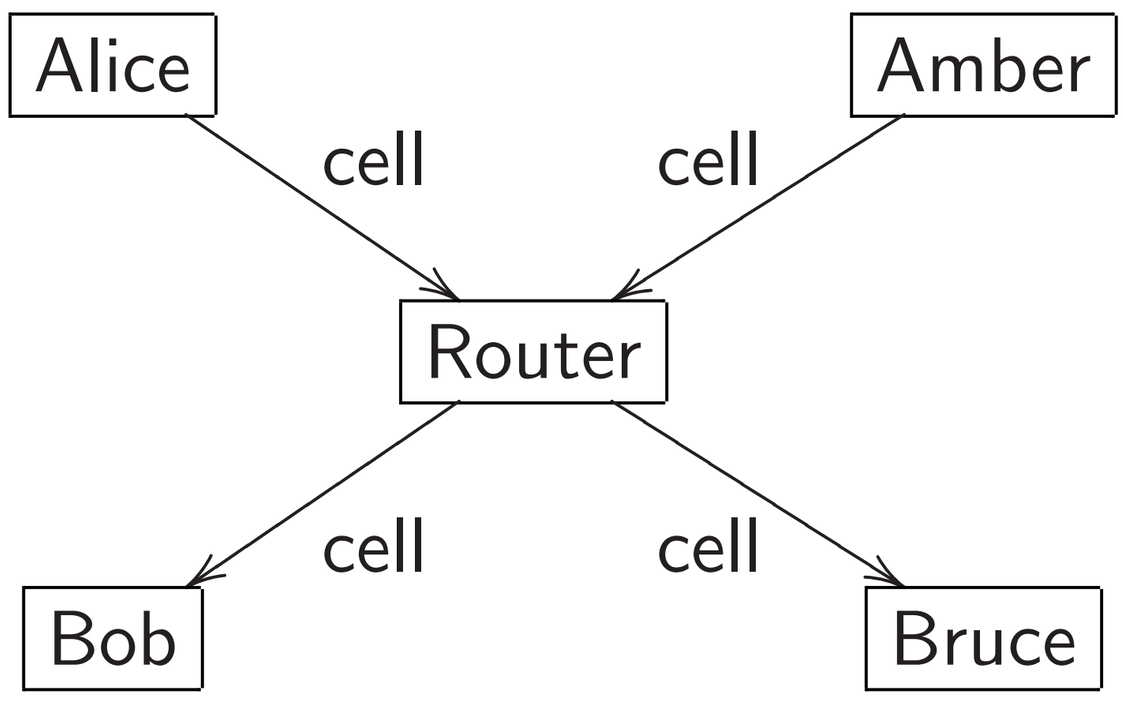
But we still see metadata—

adequate for most surveillance.

Nightmare scenario: Scrambling

unidentifiable encrypted cells—

Tor has multiple layers of this:



se for us:

to. Lobby for this!

as good for us:

unistic encryption"

authentication.

passive eavesdropping"

aren't passive.

as good for us:

res on some data.

still see everything.

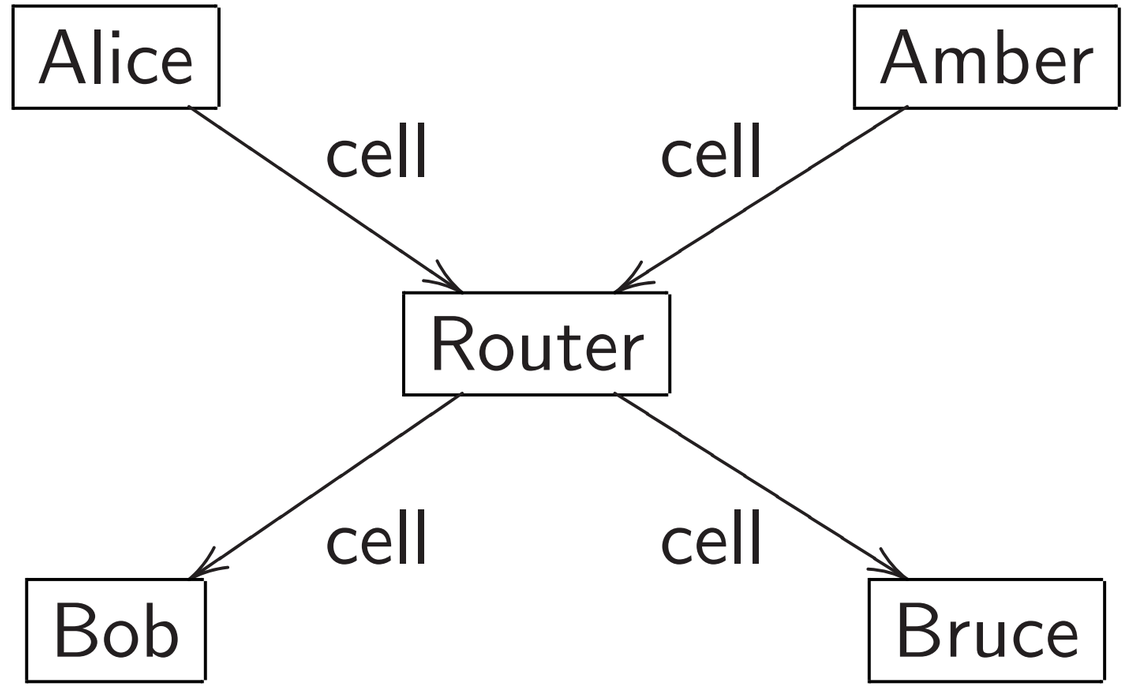
o censor quite selectively.

odify signed data but

k in many other ways.

More troublesome: End-to-end authenticated encryption.
But we still see metadata—adequate for most surveillance.

Nightmare scenario: Scrambling unidentifiable encrypted cells—Tor has multiple layers of this:



Can we

for this!

or us:

cryption"

ation.

vesdropping"

ssive.

or us:

ne data.

verything.

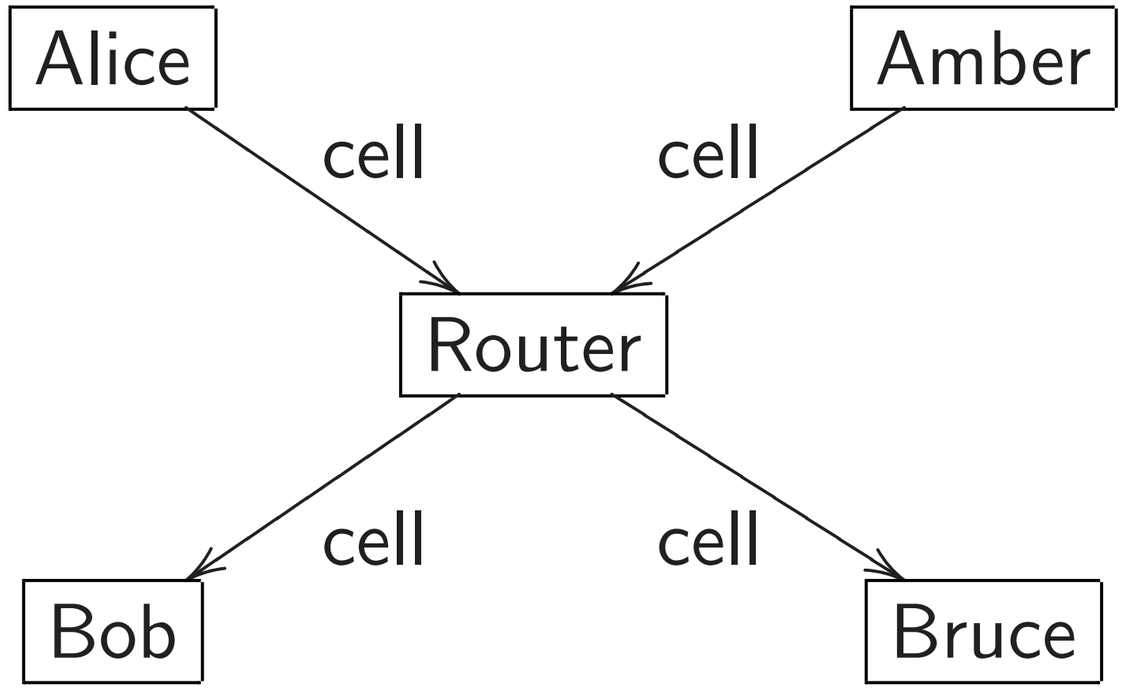
uite selectively.

ed data but

other ways.

More troublesome: End-to-end authenticated encryption.
But we still see metadata—
adequate for most surveillance.

Nightmare scenario: Scrambling unidentifiable encrypted cells—
Tor has multiple layers of this:



Can we ban crypto

g"

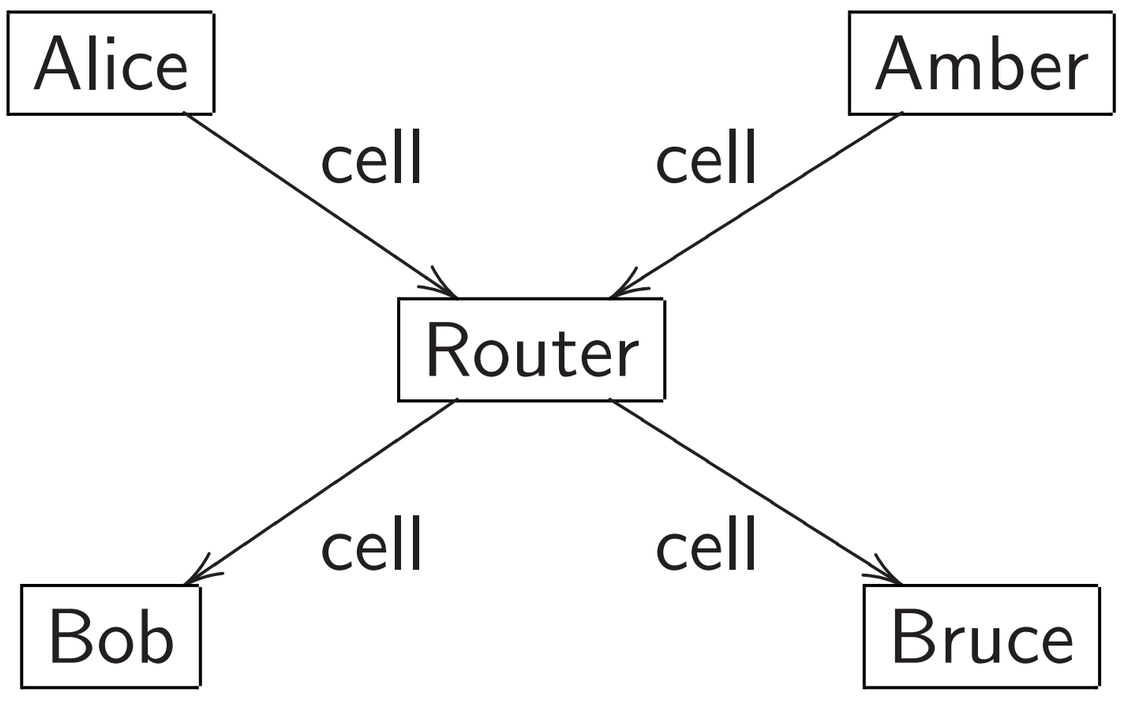
vely.

ut

ys.

More troublesome: End-to-end authenticated encryption.
But we still see metadata—
adequate for most surveillance.

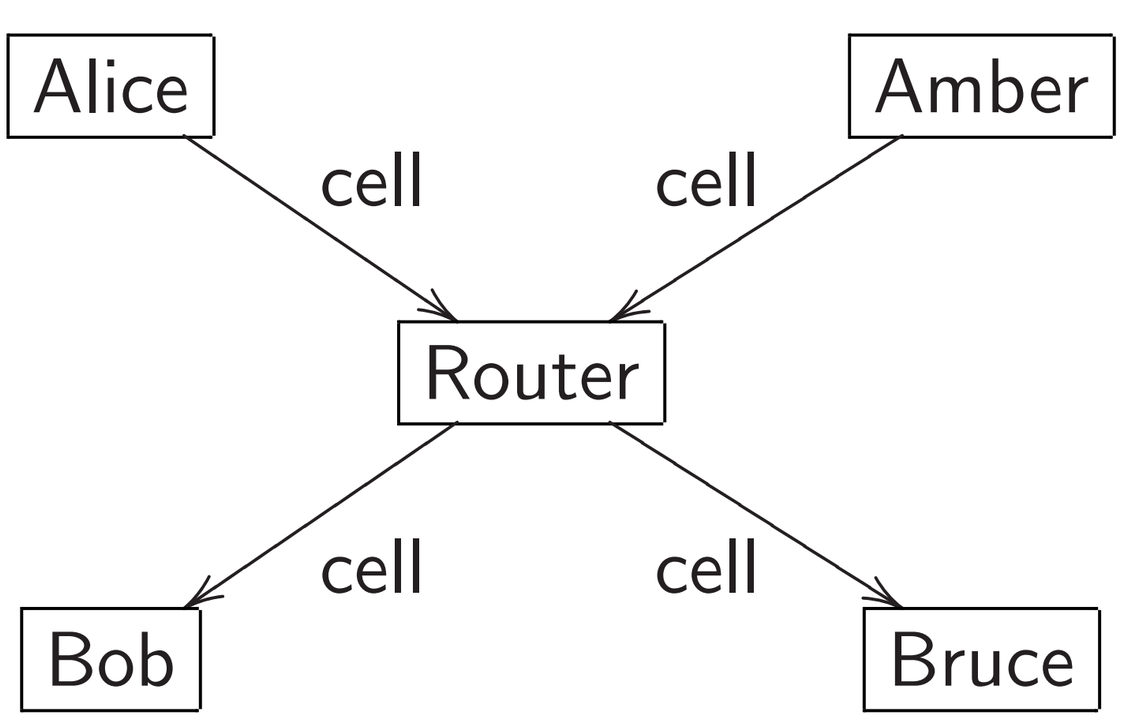
Nightmare scenario: Scrambling unidentifiable encrypted cells—
Tor has multiple layers of this:



Can we ban crypto?

More troublesome: End-to-end authenticated encryption.
But we still see metadata—
adequate for most surveillance.

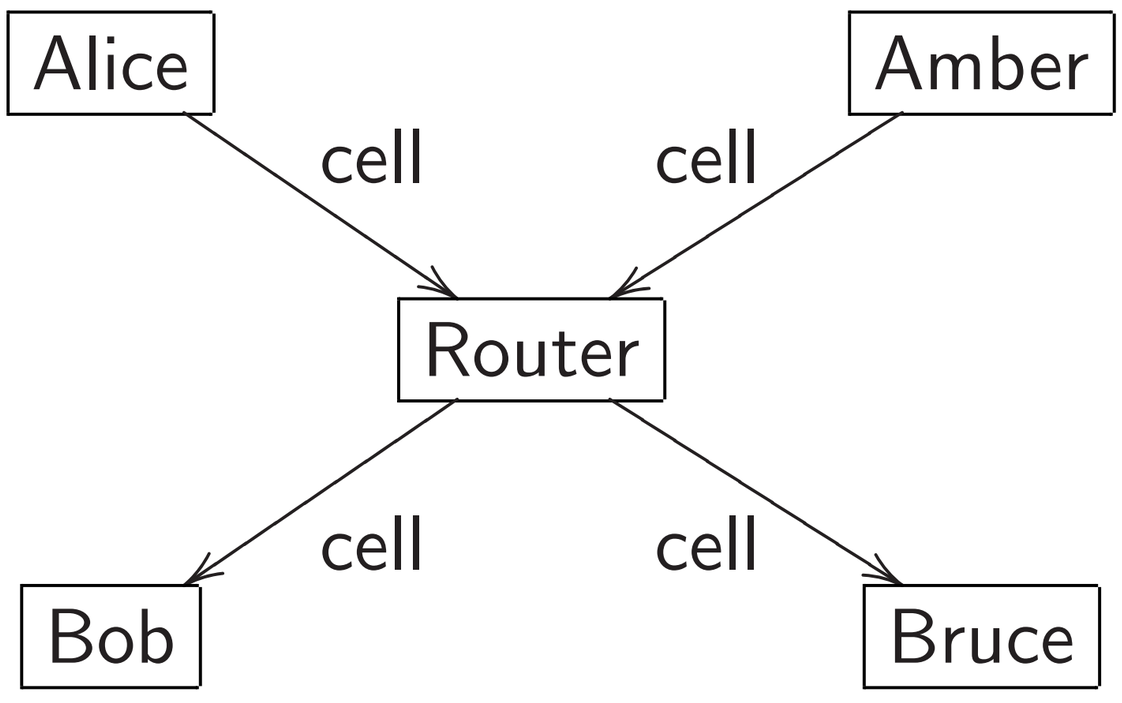
Nightmare scenario: Scrambling unidentifiable encrypted cells—
Tor has multiple layers of this:



Can we ban crypto?

More troublesome: End-to-end authenticated encryption.
But we still see metadata—
adequate for most surveillance.

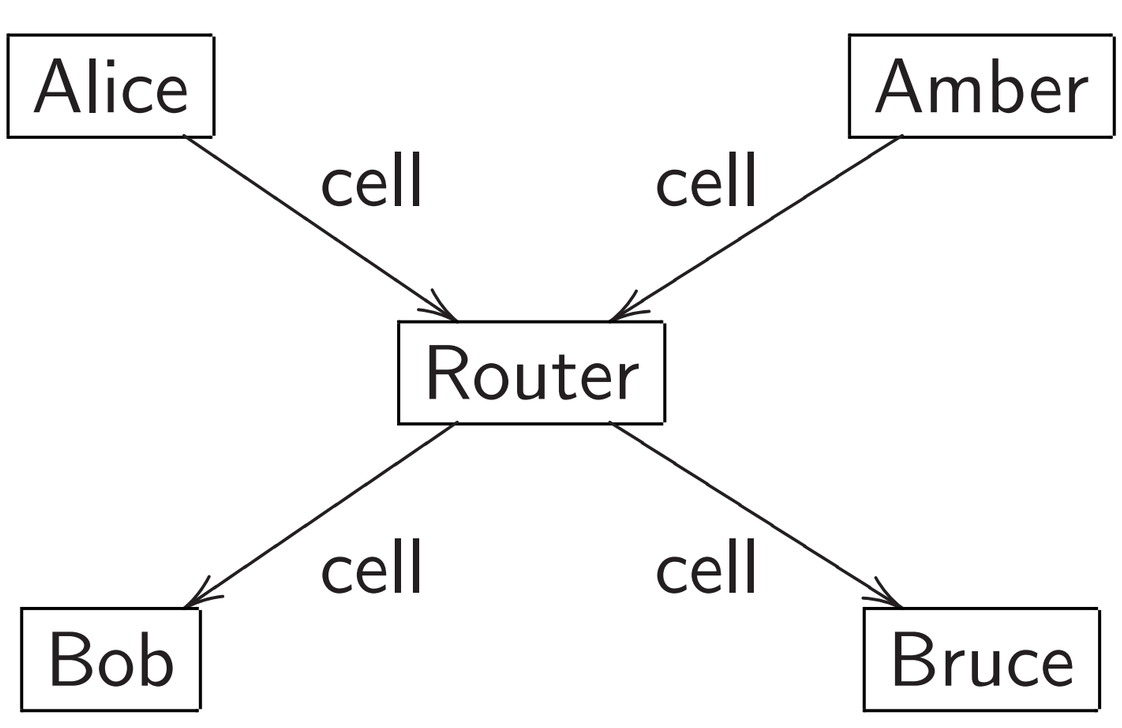
Nightmare scenario: Scrambling unidentifiable encrypted cells—
Tor has multiple layers of this:



Can we ban crypto? If not,
can we divert effort into
opportunistic encryption,
or into pure authentication?

More troublesome: End-to-end authenticated encryption.
But we still see metadata—adequate for most surveillance.

Nightmare scenario: Scrambling unidentifiable encrypted cells—Tor has multiple layers of this:

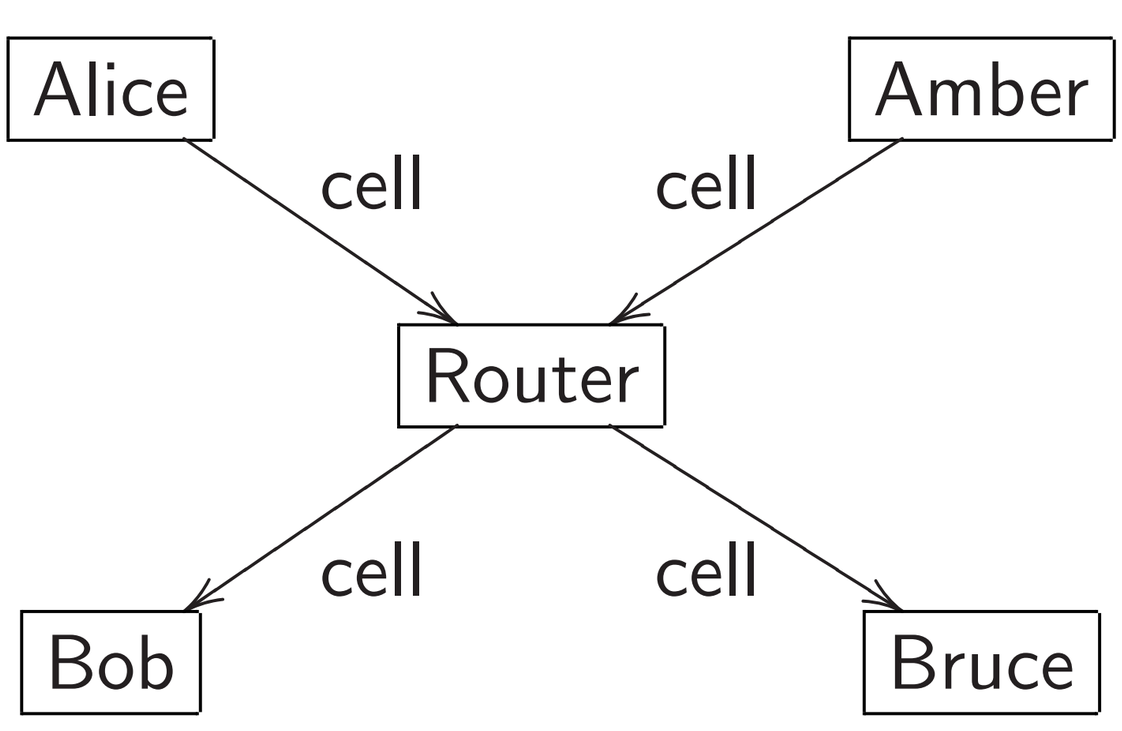


Can we ban crypto? If not, can we divert effort into opportunistic encryption, or into pure authentication?

Can we promote standards that expose most data, or that **trust our proxies**?

More troublesome: End-to-end authenticated encryption.
But we still see metadata—
adequate for most surveillance.

Nightmare scenario: Scrambling unidentifiable encrypted cells—
Tor has multiple layers of this:



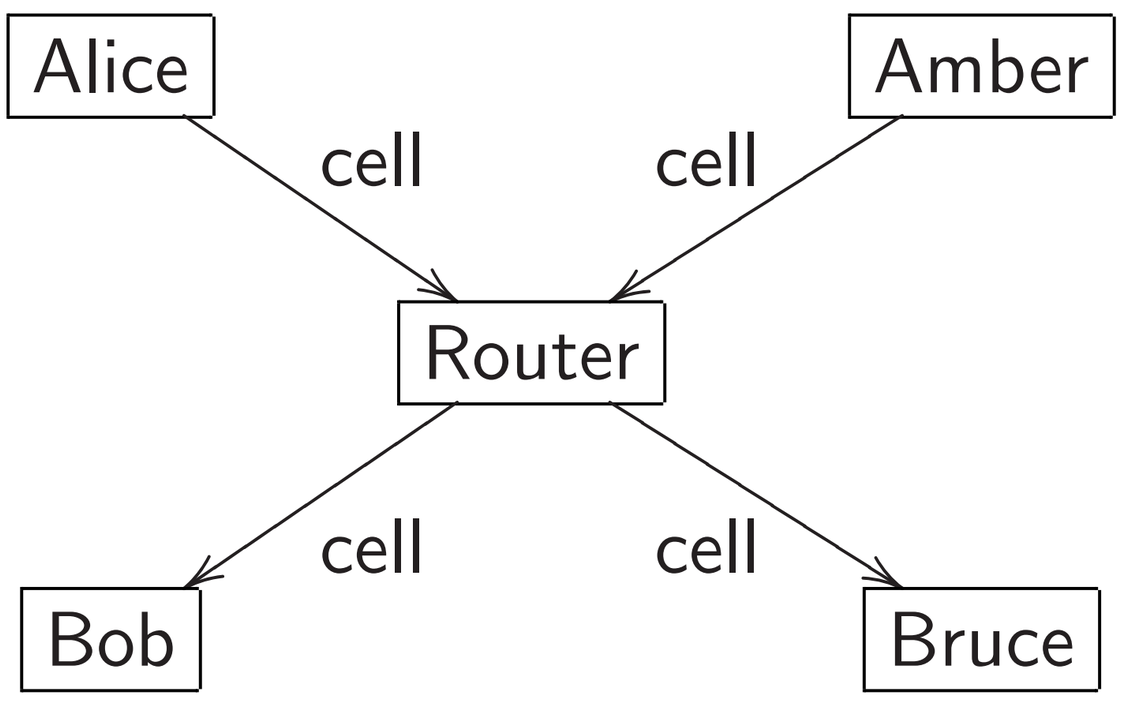
Can we ban crypto? If not,
can we divert effort into
opportunistic encryption,
or into pure authentication?

Can we promote standards
that expose most data, or
that **trust our proxies**?

Very often crypto protocols and
implementations have weaknesses.
Can we promote weak crypto?

More troublesome: End-to-end authenticated encryption.
But we still see metadata—
adequate for most surveillance.

Nightmare scenario: Scrambling unidentifiable encrypted cells—
Tor has multiple layers of this:



Can we ban crypto? If not,
can we divert effort into
opportunistic encryption,
or into pure authentication?

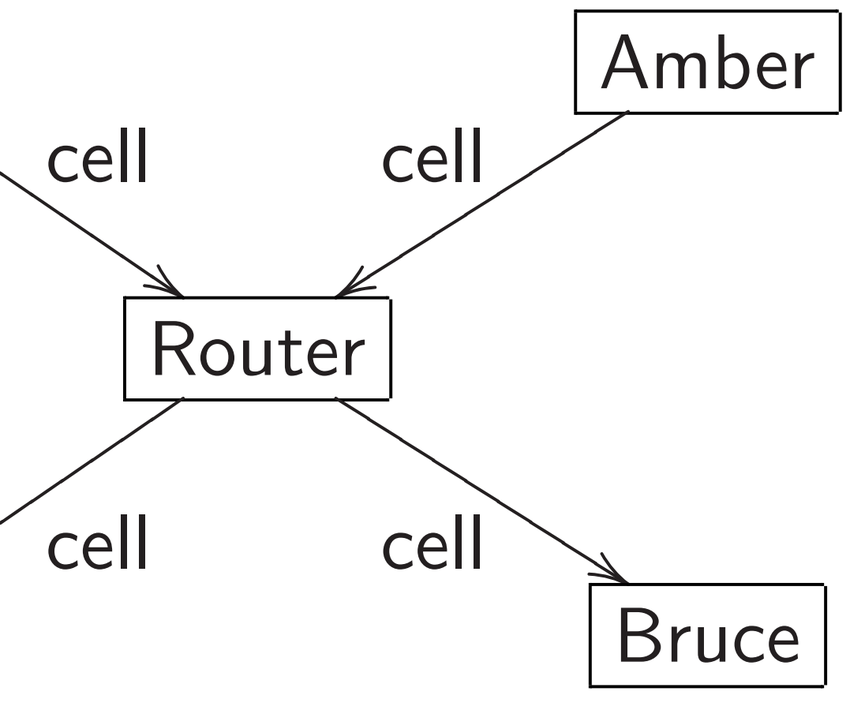
Can we promote standards
that expose most data, or
that **trust our proxies**?

Very often crypto protocols and implementations have weaknesses.
Can we promote weak crypto?

We've started working with
experts in crypto sabotage.

oublesome: End-to-end
cated encryption.
still see metadata—
e for most surveillance.

are scenario: Scrambling
fiable encrypted cells—
multiple layers of this:



Can we ban crypto? If not,
can we divert effort into
opportunistic encryption,
or into pure authentication?

Can we promote standards
that expose most data, or
that **trust our proxies**?

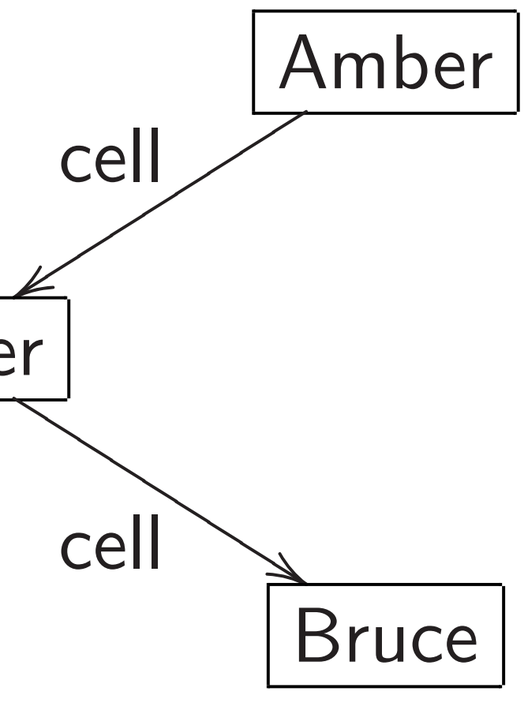
Very often crypto protocols and
implementations have weaknesses.
Can we promote weak crypto?

We've started working with
experts in crypto sabotage.

Emphasi
'heart' o
simple a
pseudo-r

: End-to-end
ryption.
etadata—
surveillance.

o: Scrambling
rypted cells—
ayers of this:



Can we ban crypto? If not,
can we divert effort into
opportunistic encryption,
or into pure authentication?

Can we promote standards
that expose most data, or
that **trust our proxies**?

Very often crypto protocols and
implementations have weaknesses.
Can we promote weak crypto?

We've started working with
experts in crypto sabotage.

Emphasize perform
'heart' of RC4 is it
simple and extrem
pseudo-random ge

end

ce.

bling

s—

is:

Amber

Bruce

Can we ban crypto? If not,
can we divert effort into
opportunistic encryption,
or into pure authentication?

Can we promote standards
that expose most data, or
that **trust our proxies**?

Very often crypto protocols and
implementations have weaknesses.
Can we promote weak crypto?

We've started working with
experts in crypto sabotage.

Emphasize performance: "T
'heart' of RC4 is its exceptio
simple and extremely efficien
pseudo-random generator."

Can we ban crypto? If not, can we divert effort into opportunistic encryption, or into pure authentication?

Can we promote standards that expose most data, or that **trust our proxies**?

Very often crypto protocols and implementations have weaknesses. **Can we promote weak crypto?**

We've started working with experts in crypto sabotage.

Emphasize performance: "The 'heart' of RC4 is its exceptionally simple and extremely efficient pseudo-random generator."

Can we ban crypto? If not, can we divert effort into opportunistic encryption, or into pure authentication?

Can we promote standards that expose most data, or that **trust our proxies**?

Very often crypto protocols and implementations have weaknesses. **Can we promote weak crypto?**

We've started working with experts in crypto sabotage.

Emphasize performance: "The 'heart' of RC4 is its exceptionally simple and extremely efficient pseudo-random generator."

Bamboozle people: Dual EC is "the only DRBG mechanism in this Recommendation whose security is related to a hard problem in number theory."

Can we ban crypto? If not, can we divert effort into opportunistic encryption, or into pure authentication?

Can we promote standards that expose most data, or that **trust our proxies**?

Very often crypto protocols and implementations have weaknesses. **Can we promote weak crypto?**

We've started working with experts in crypto sabotage.

Emphasize performance: "The 'heart' of RC4 is its exceptionally simple and extremely efficient pseudo-random generator."

Bamboozle people: Dual EC is "the only DRBG mechanism in this Recommendation whose security is related to a hard problem in number theory."

Make crypto protocols so complicated that nobody will get them right. Standards committees rarely fight against complications.

ban crypto? If not,
divert effort into
nistic encryption,
pure authentication?

promote standards
ose most data, or
st our proxies?

en crypto protocols and
ntations have weaknesses.
promote weak crypto?

tarted working with
in crypto sabotage.

Emphasize performance: "The 'heart' of RC4 is its exceptionally simple and extremely efficient pseudo-random generator."

Bamboozle people: Dual EC is "the only DRBG mechanism in this Recommendation whose security is related to a hard problem in number theory."

Make crypto protocols
so complicated that
nobody will get them right.
Standards committees rarely
fight against complications.

Sabotag

How to
manipul
a white

Daniel J
Tung Ch
Chitchan
Andreas
Tanja La
Ruben N
Christine

safecur
/bada55

o? If not,
rt into
yption,
ntication?

tandards
data, or
oxies?

protocols and
ave weaknesses.
weak crypto?

king with
sabotage.

Emphasize performance: "The 'heart' of RC4 is its exceptionally simple and extremely efficient pseudo-random generator."

Bamboozle people: Dual EC is "the only DRBG mechanism in this Recommendation whose security is related to a hard problem in number theory."

Make crypto protocols
so complicated that
nobody will get them right.
Standards committees rarely
fight against complications.

Sabotaging crypto

How to
manipulate curve
a white paper for

Daniel J. Bernstei
Tung Chou
Chitchanok Chuen
Andreas Hülsing
Tanja Lange
Ruben Niederhage
Christine van Vred

safecurves.cr.y
/bada55.html

and
nesses.
pto?

Emphasize performance: "The 'heart' of RC4 is its exceptionally simple and extremely efficient pseudo-random generator."

Bamboozle people: Dual EC is "the only DRBG mechanism in this Recommendation whose security is related to a hard problem in number theory."

Make crypto protocols
so complicated that
nobody will get them right.
Standards committees rarely
fight against complications.

Sabotaging crypto details

How to
manipulate curve standards:
a white paper for the black

Daniel J. Bernstein
Tung Chou
Chitchanok Chuengsatiansup
Andreas Hülsing
Tanja Lange
Ruben Niederhagen
Christine van Vredendaal

safecurves.cr.yp.to
/bada55.html

Emphasize performance: "The 'heart' of RC4 is its exceptionally simple and extremely efficient pseudo-random generator."

Bamboozle people: Dual EC is "the only DRBG mechanism in this Recommendation whose security is related to a hard problem in number theory."

Make crypto protocols
so complicated that
nobody will get them right.
Standards committees rarely
fight against complications.

Sabotaging crypto details

How to
manipulate curve standards:
a white paper for the black hat

Daniel J. Bernstein
Tung Chou
Chitchanok Chuengsatiansup
Andreas Hülsing
Tanja Lange
Ruben Niederhagen
Christine van Vredendaal

`safecurves.cr.yp.to`
`/bada55.html`

ize performance: "The
of RC4 is its exceptionally
nd extremely efficient
random generator."

ozle people: Dual EC is
y DRBG mechanism in
ommendation whose
is related to a hard
in number theory."

ypto protocols
licated that
will get them right.
ds committees rarely
ainst complications.

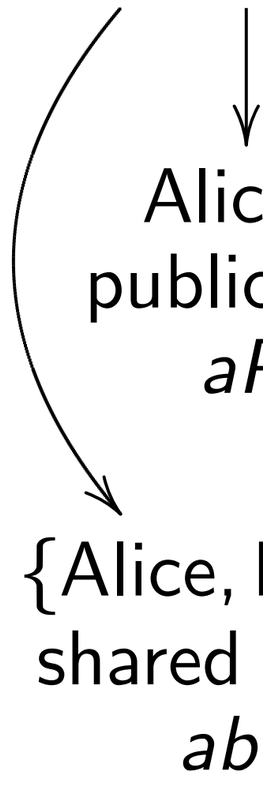
Sabotaging crypto details

How to
manipulate curve standards:
a white paper for the black hat

Daniel J. Bernstein
Tung Chou
Chitchanok Chuengsatiansup
Andreas Hülsing
Tanja Lange
Ruben Niederhagen
Christine van Vredendaal

safecurves.cr.yp.to
/bada55.html

Textboo
using sta
on a sta



mance: “The
ts exceptionally
ely efficient
enerator.”

e: Dual EC is
mechanism in
tion whose
to a hard
r theory.”

ocols
at
em right.
tees rarely
blications.

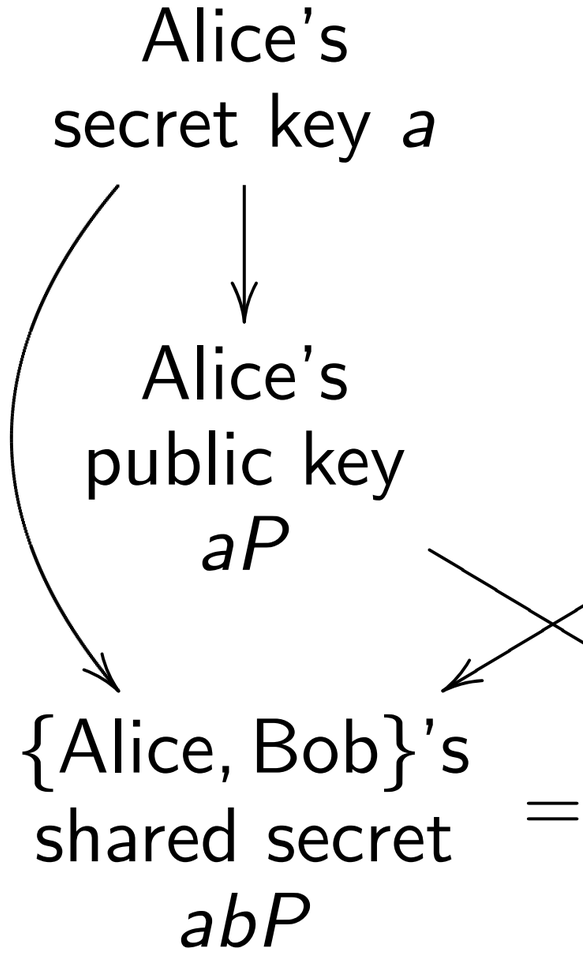
Sabotaging crypto details

How to
manipulate curve standards:
a white paper for the black hat

Daniel J. Bernstein
Tung Chou
Chitchanok Chuengsatiansup
Andreas Hülsing
Tanja Lange
Ruben Niederhagen
Christine van Vredendaal

safecurves.cr.yp.to
/bada55.html

Textbook key exch
using standard poi
on a standard ellip



he
onally
nt

C is
in
e

Sabotaging crypto details

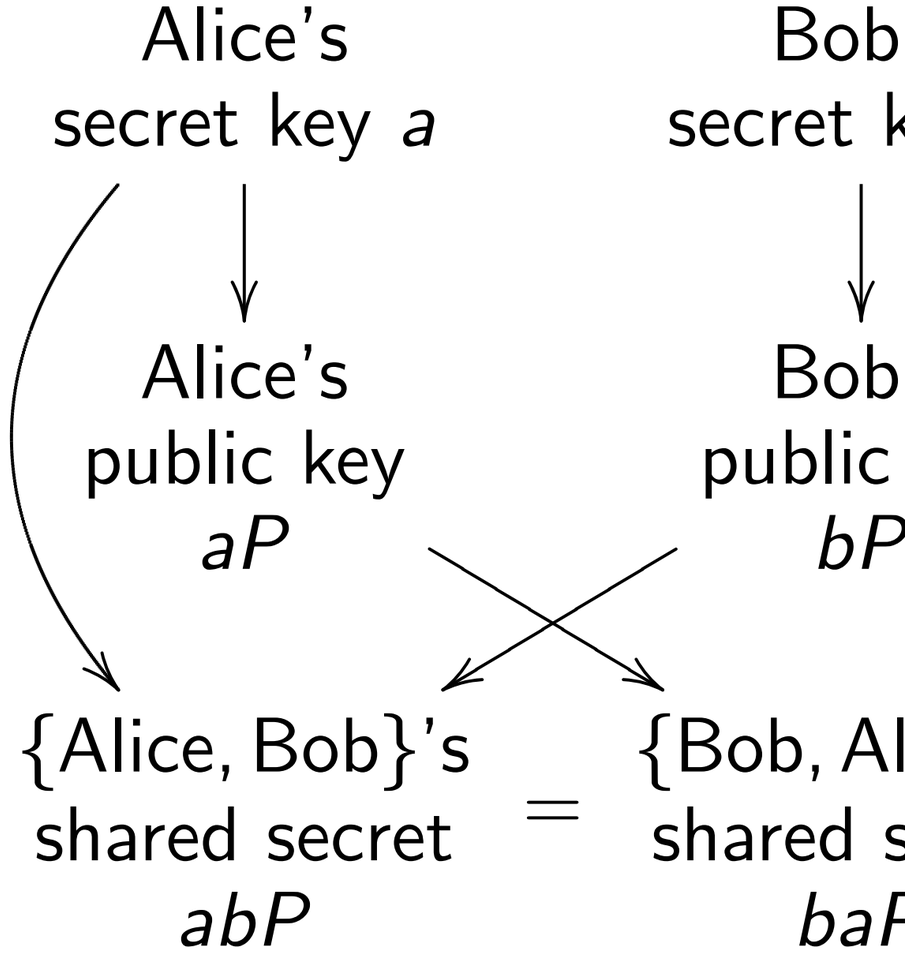
How to
manipulate curve standards:
a white paper for the black hat

Daniel J. Bernstein
Tung Chou
Chitchanok Chuengsatiansup
Andreas Hülsing
Tanja Lange
Ruben Niederhagen
Christine van Vredendaal

safecurves.cr.yp.to
/bada55.html

Textbook key exchange

using standard point P
on a standard elliptic curve



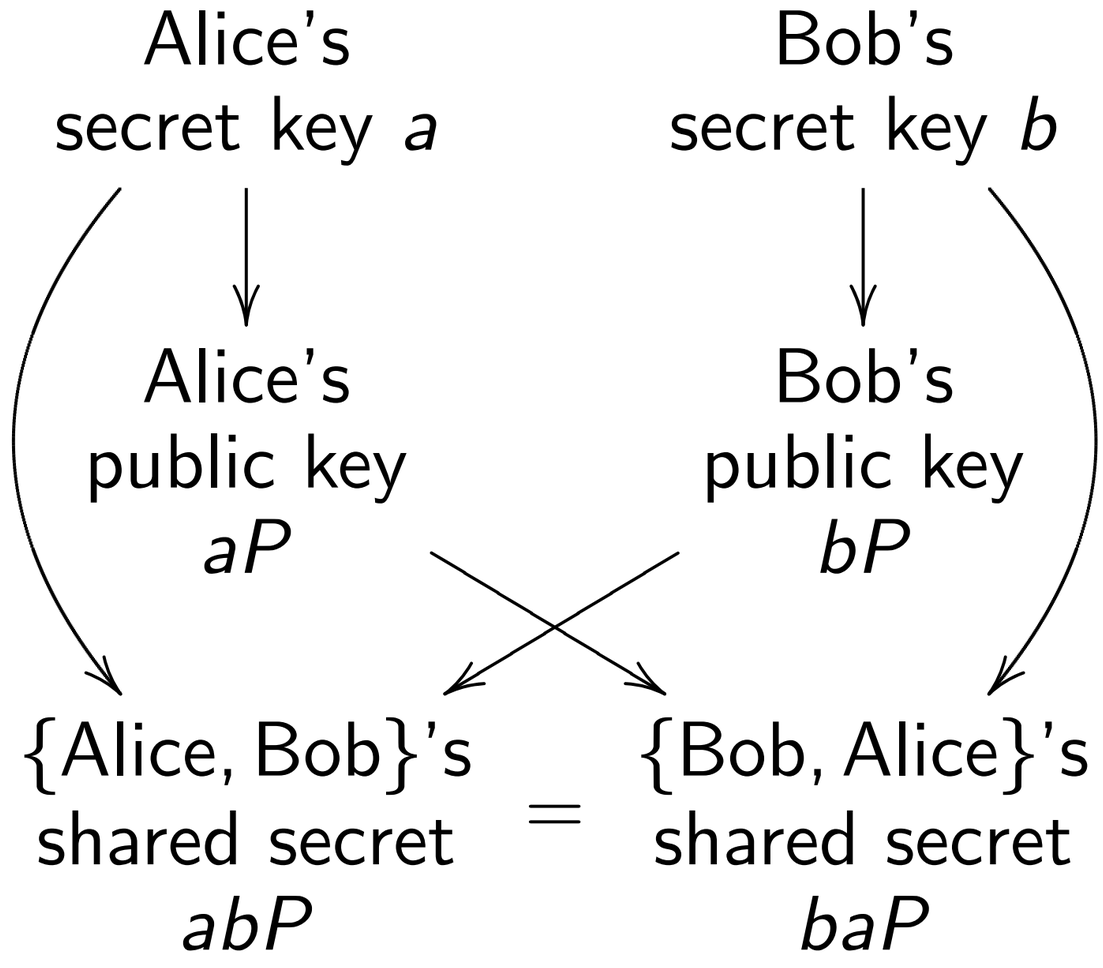
Sabotaging crypto details

How to
manipulate curve standards:
a white paper for the black hat

Daniel J. Bernstein
Tung Chou
Chitchanok Chuengsatiansup
Andreas Hülsing
Tanja Lange
Ruben Niederhagen
Christine van Vredendaal

safecurves.cr.yp.to
/bada55.html

Textbook key exchange using standard point P on a standard elliptic curve E:



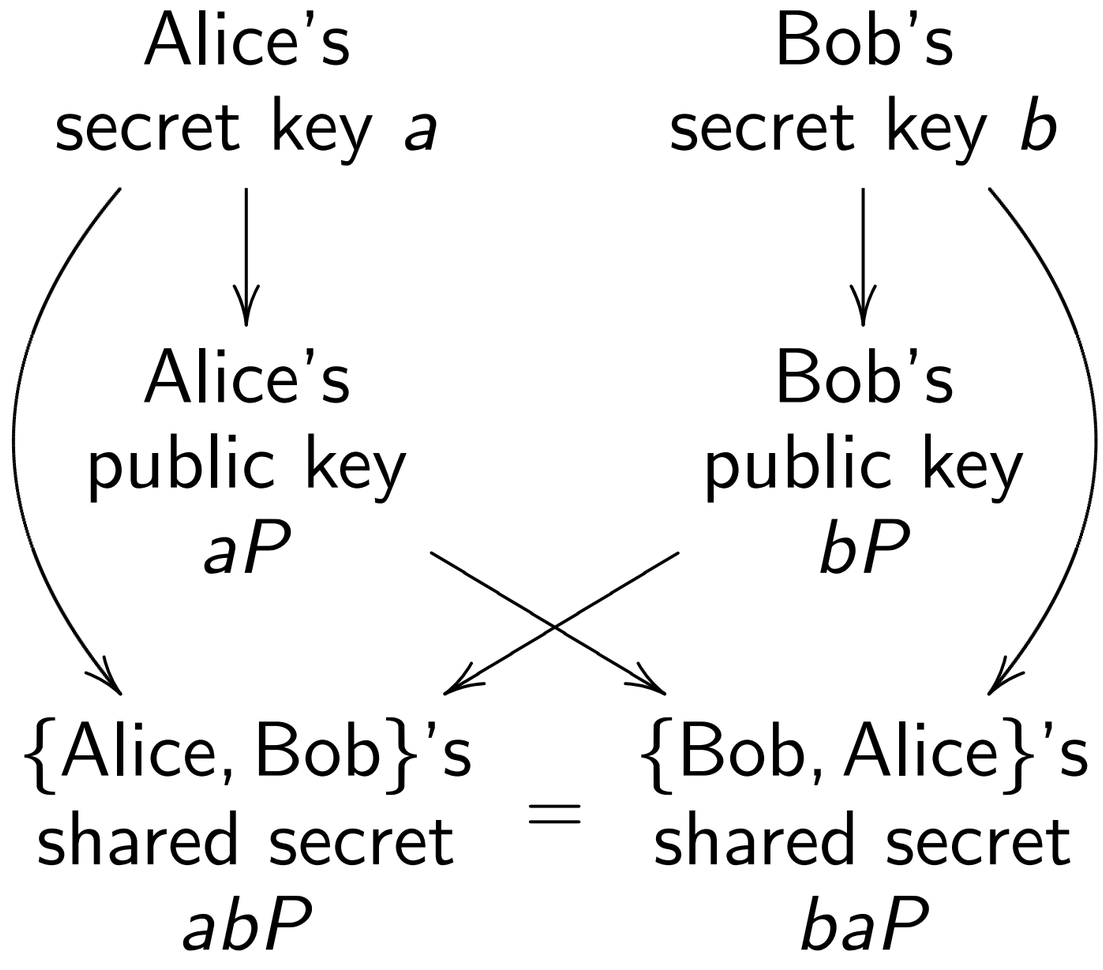
Sabotaging crypto details

How to
manipulate curve standards:
a white paper for the black hat

Daniel J. Bernstein
Tung Chou
Chitchanok Chuengsatiansup
Andreas Hülsing
Tanja Lange
Ruben Niederhagen
Christine van Vredendaal

safecurves.cr.yp.to
/bada55.html

Textbook key exchange using standard point P on a standard elliptic curve E:



Security depends on choice of E.

ing crypto details

ate curve standards:

paper for the black hat

. Bernstein

nou

nok Chuengsatiansup

Hülsing

ange

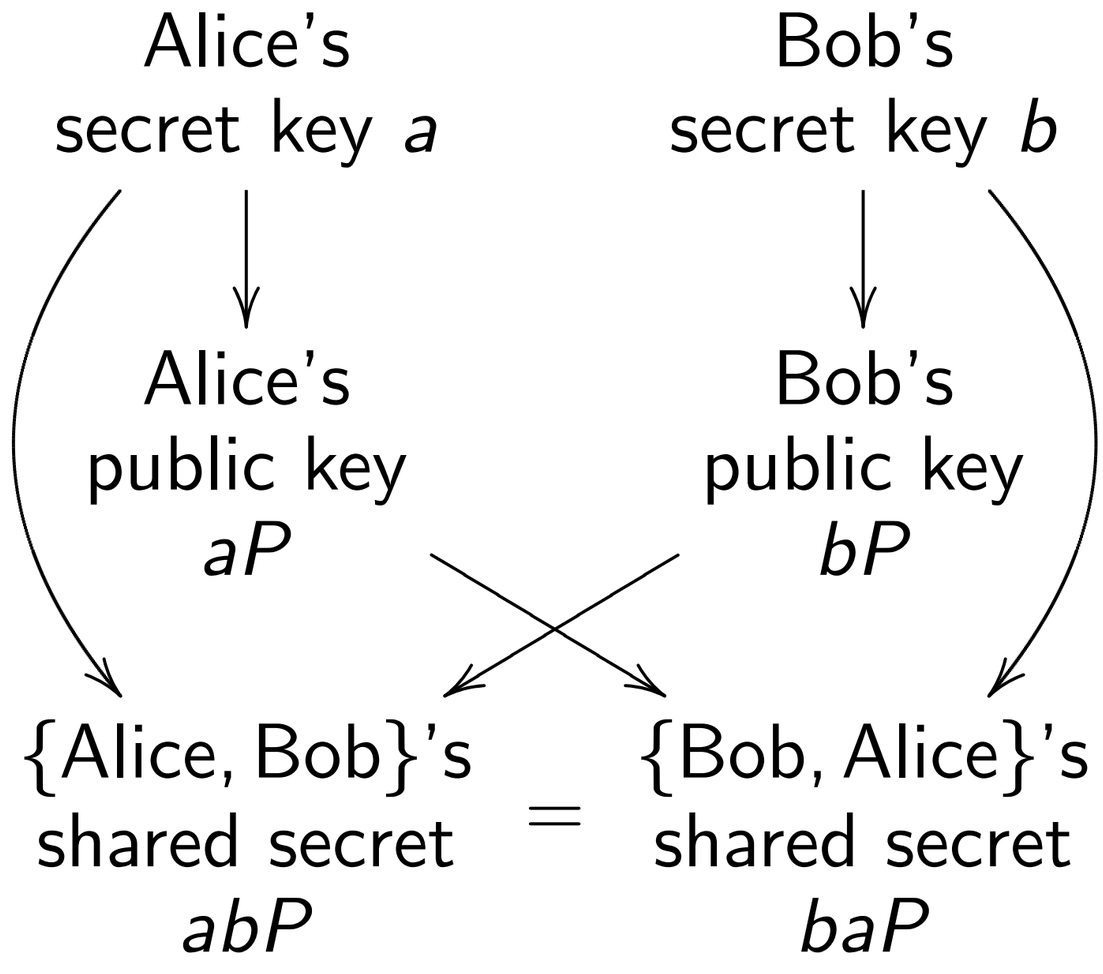
Niederhagen

e van Vredendaal

rves.cr.yp.to

5.html

Textbook key exchange
using standard point P
on a standard elliptic curve E:



Security depends on choice of E.

Alic
secret

Alic
public
aP

{Alice,
shared
ab

details

standards:

the black hat

n

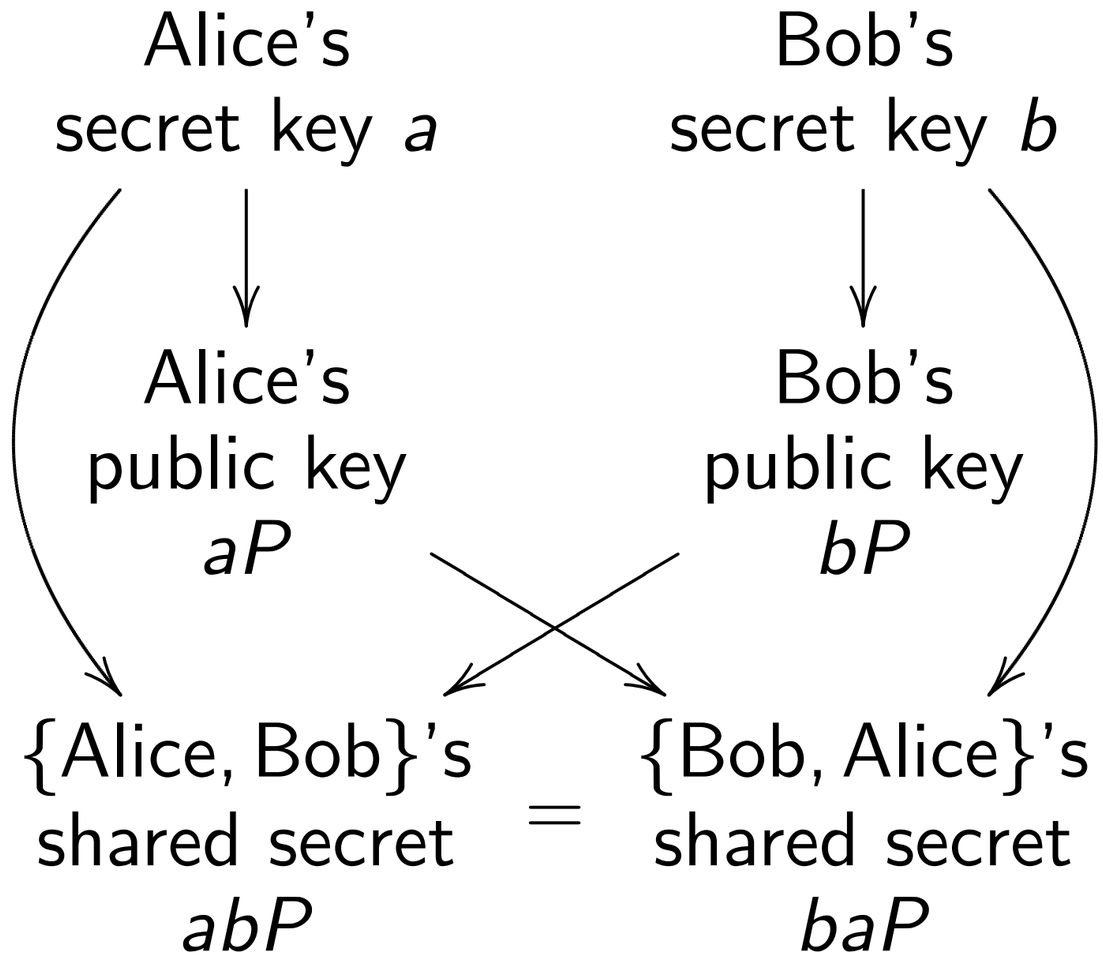
gsatiansup

en

lendaal

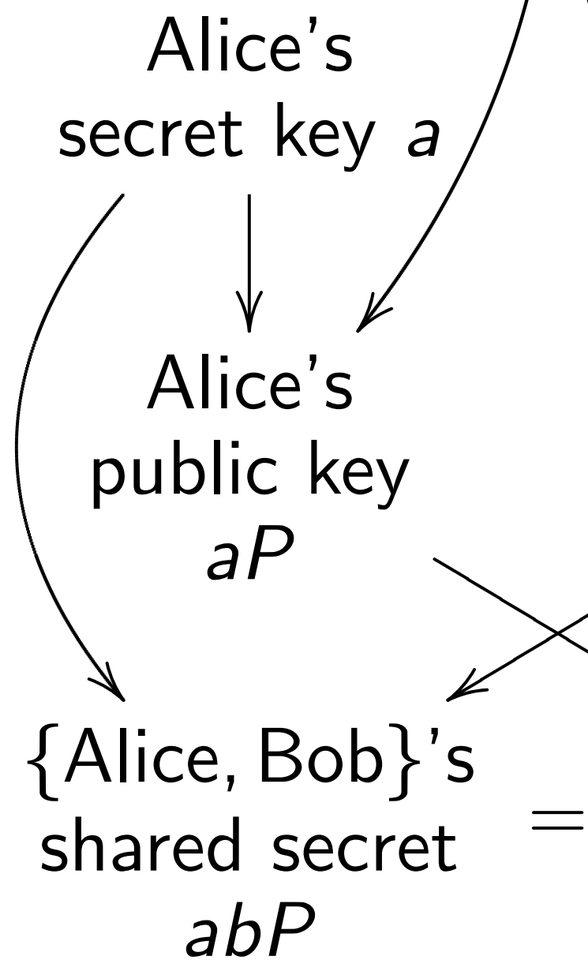
yp.to

Textbook key exchange
using standard point P
on a standard elliptic curve E:



Security depends on choice of E.

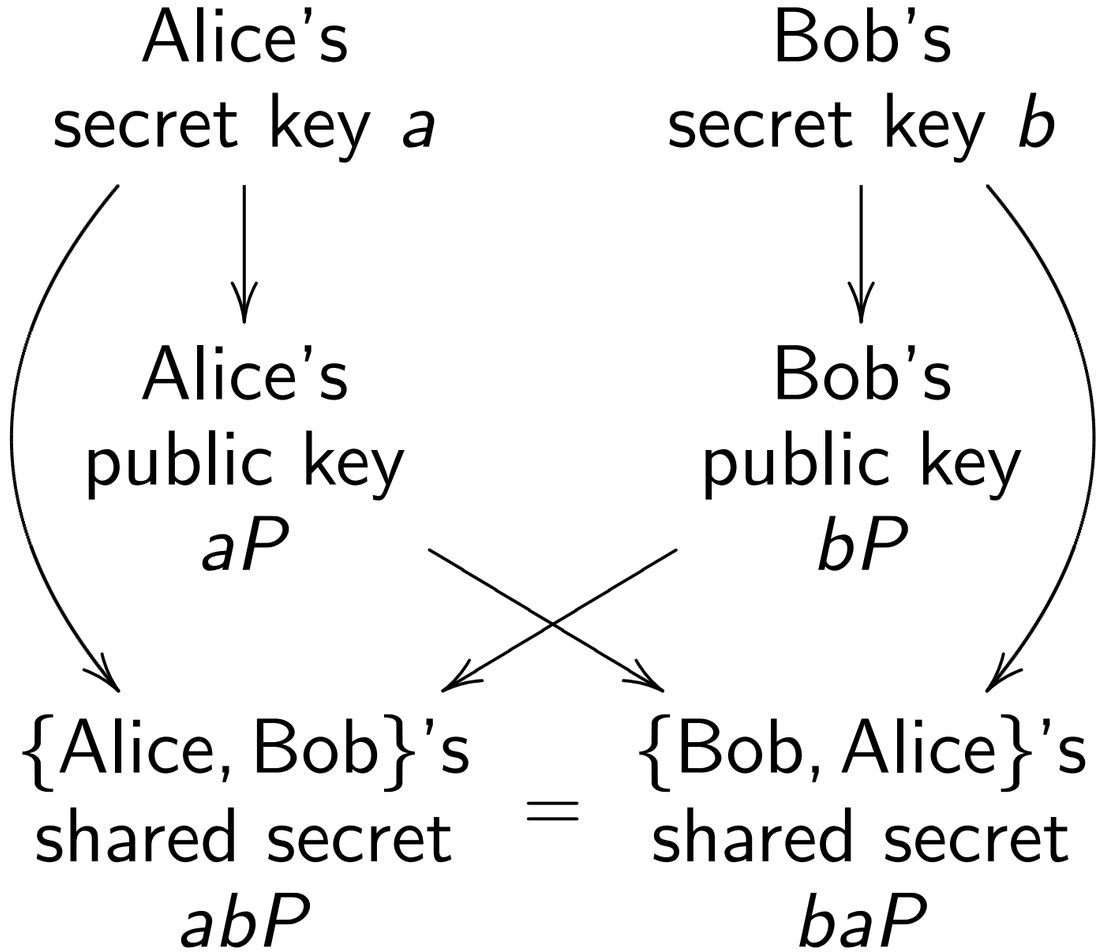
Our partne
choice o



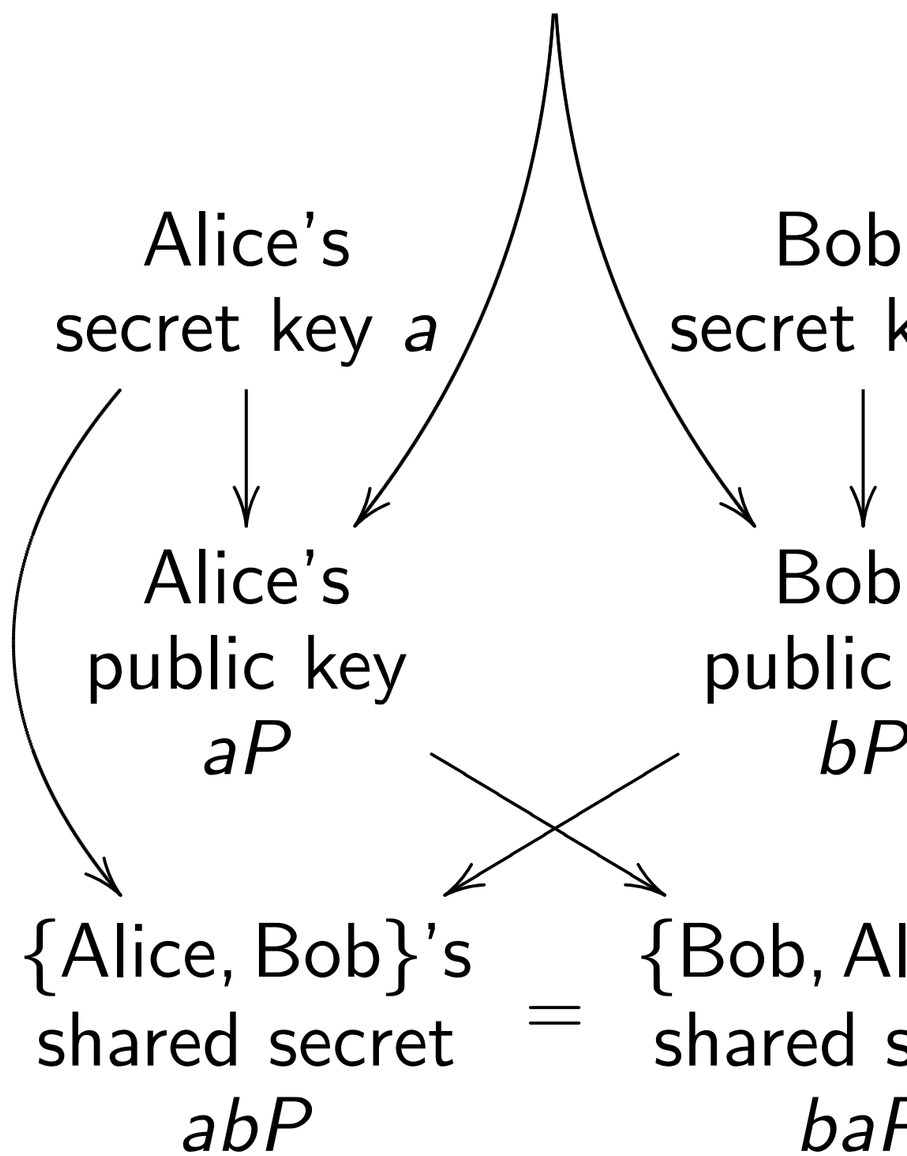
hat

p

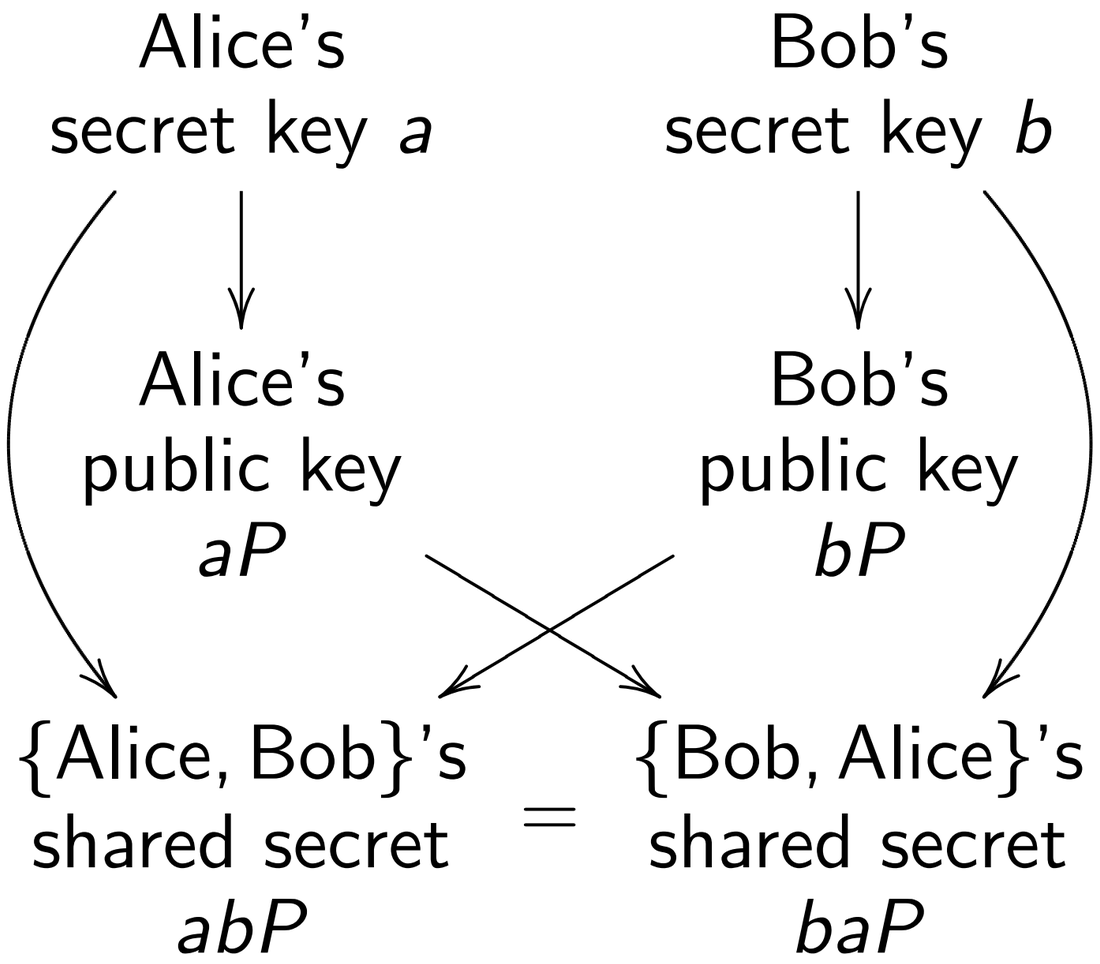
Textbook key exchange
using standard point P
on a standard elliptic curve E:



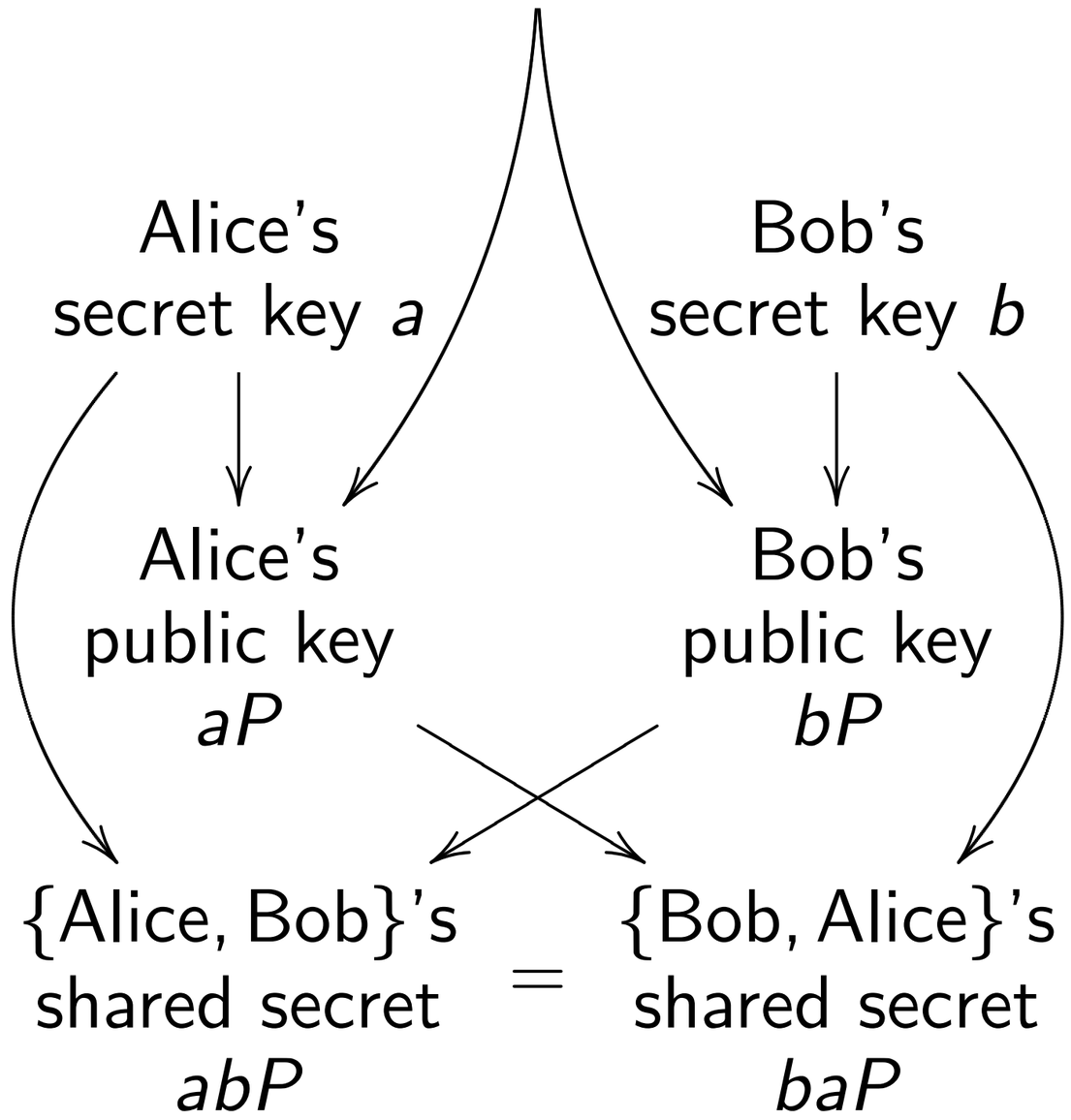
Security depends on choice of E.



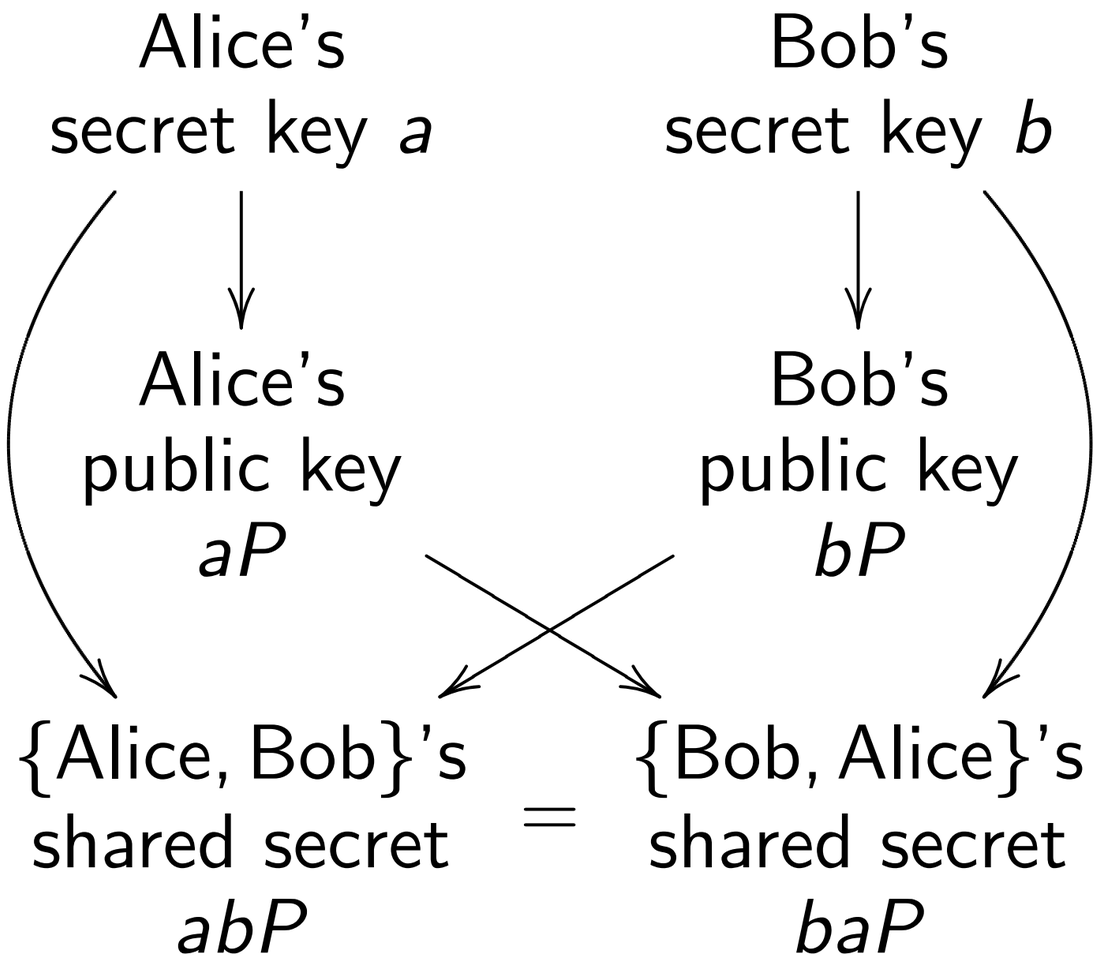
Textbook key exchange
using standard point P
on a standard elliptic curve E:



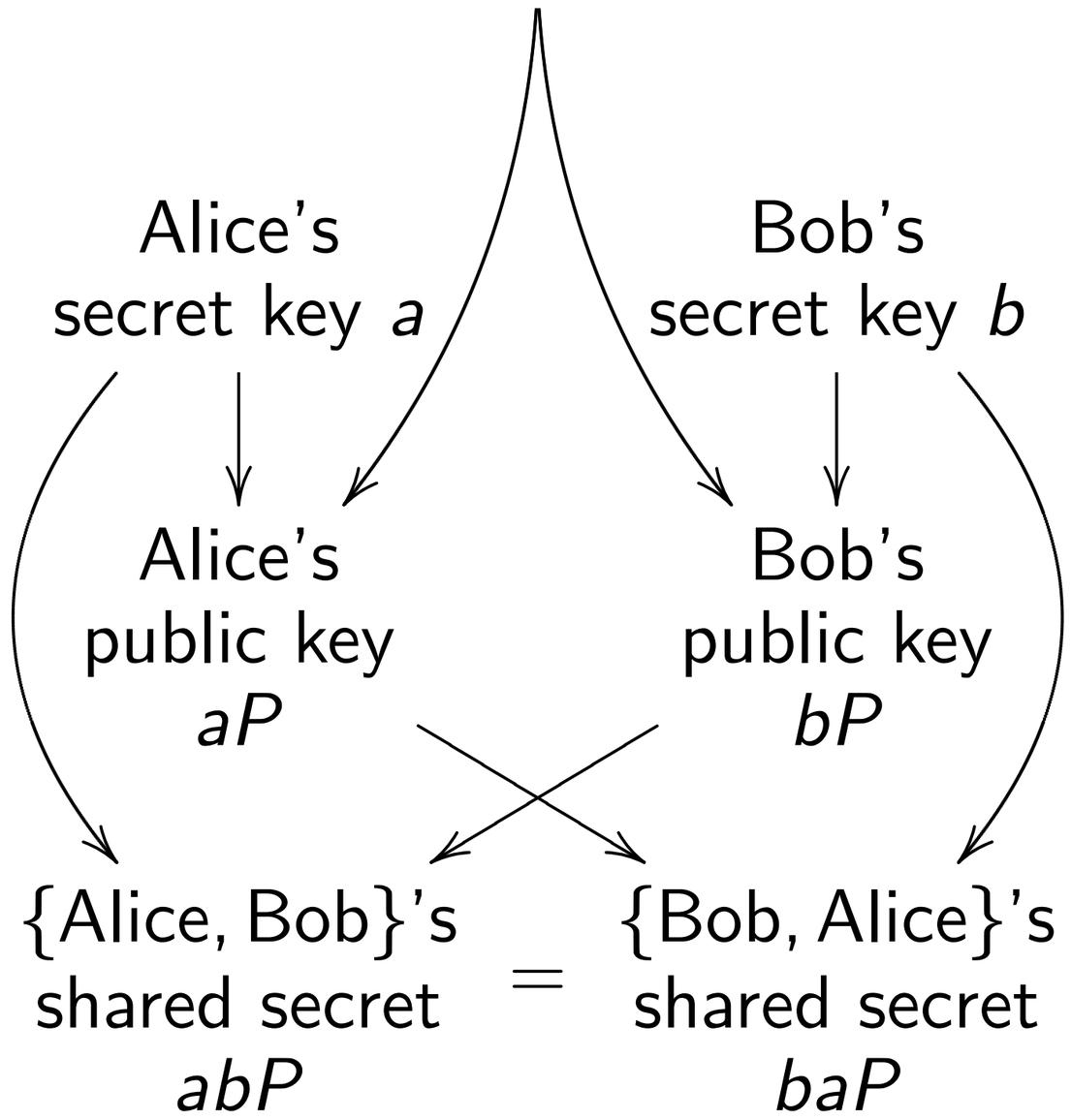
Security depends on choice of E.



Textbook key exchange
using standard point P
on a standard elliptic curve E:



Security depends on choice of E.

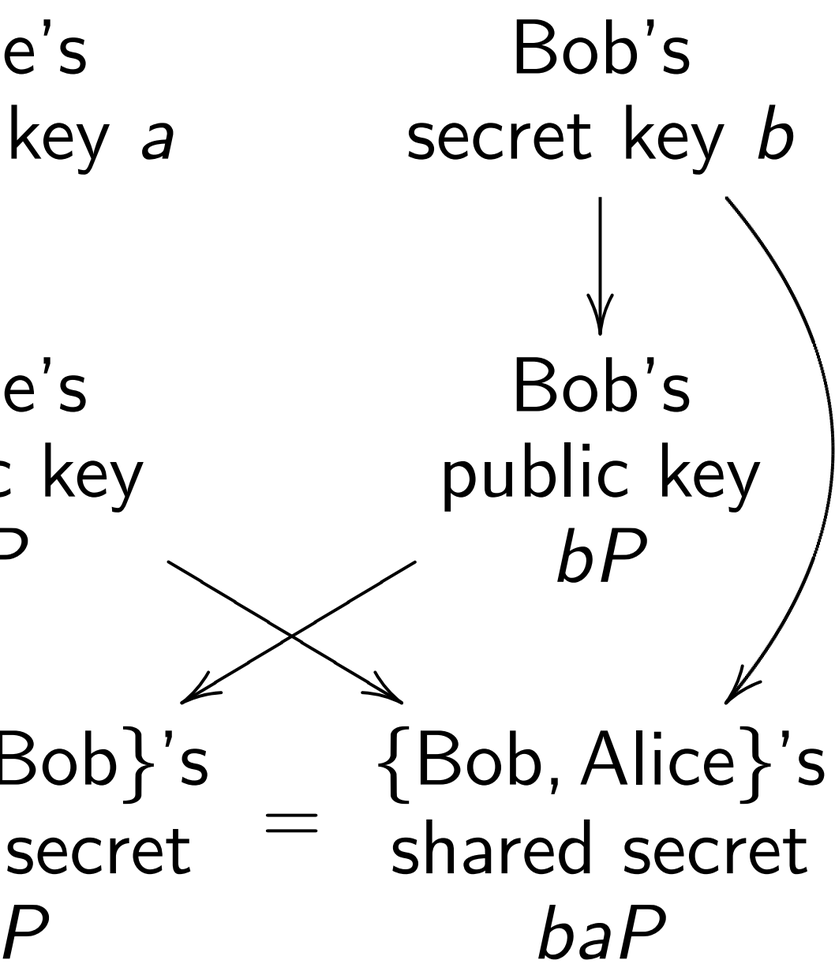


Can we exploit this picture?

k key exchange

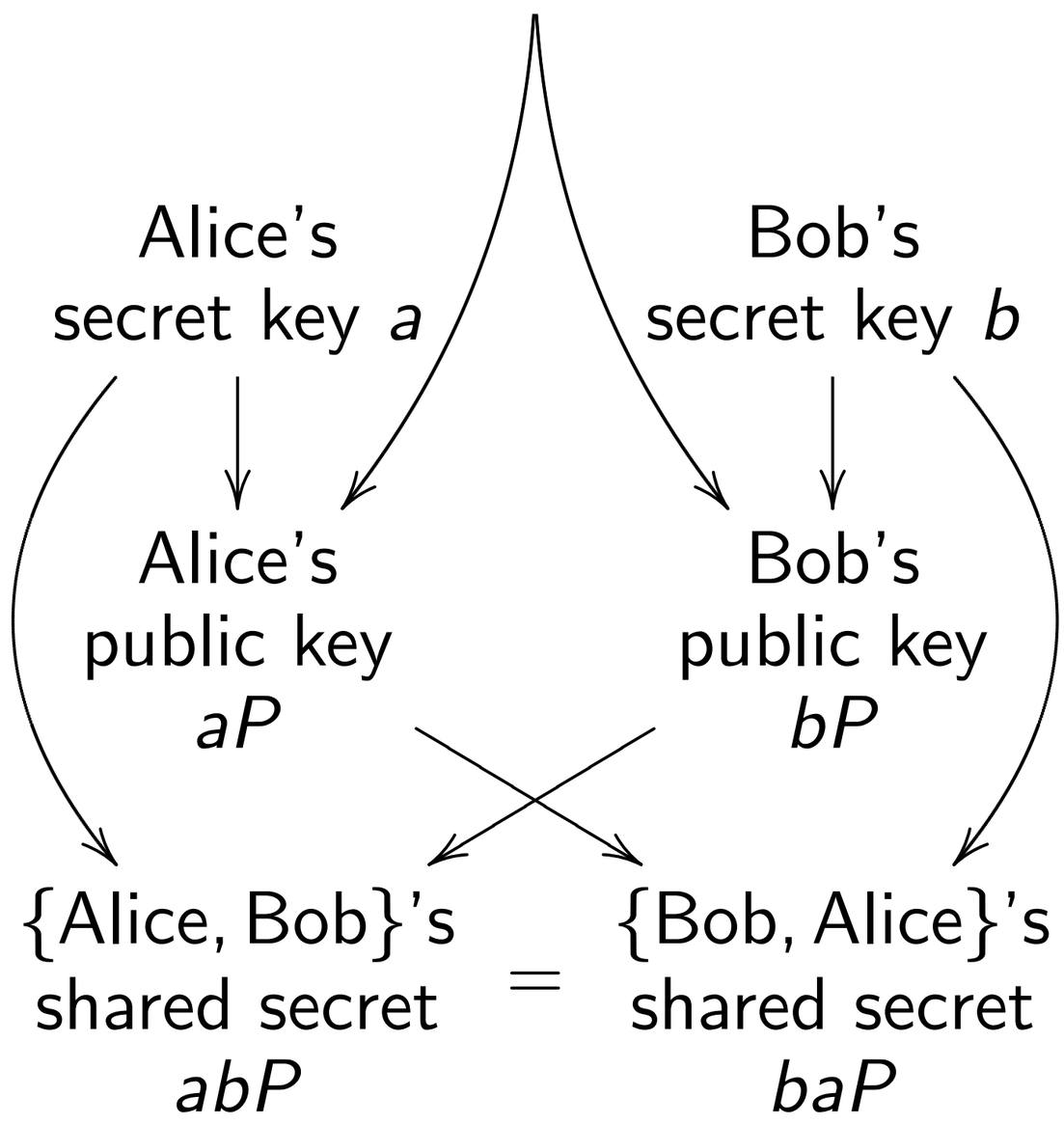
andard point P

ndard elliptic curve E:



depends on choice of E.

Our partner Jerry's
choice of E, P



Can we exploit this picture?

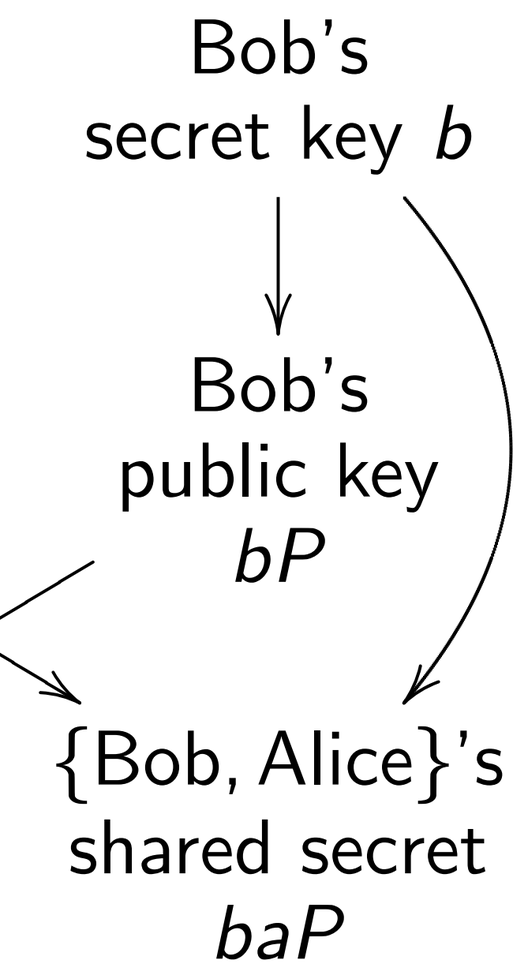
Depends

for acce

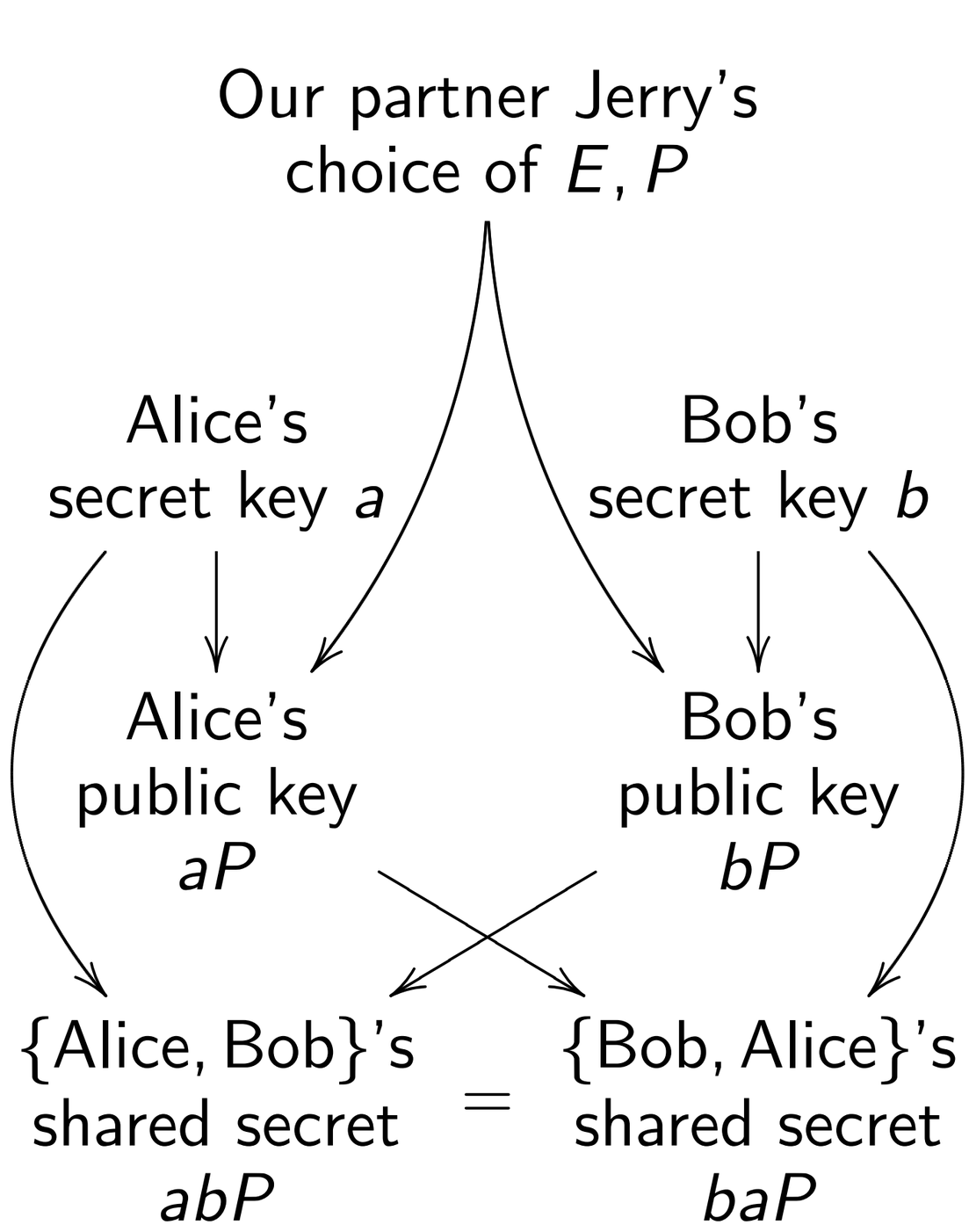
nange

int P

otic curve E:



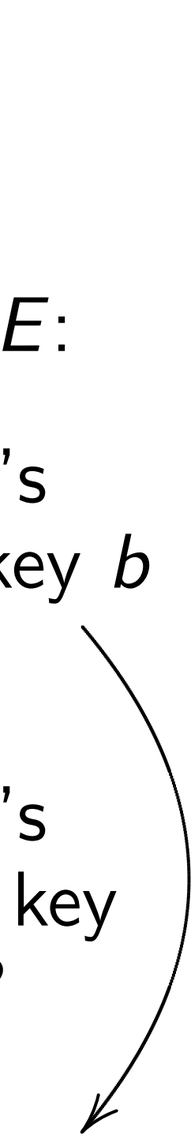
on choice of E.

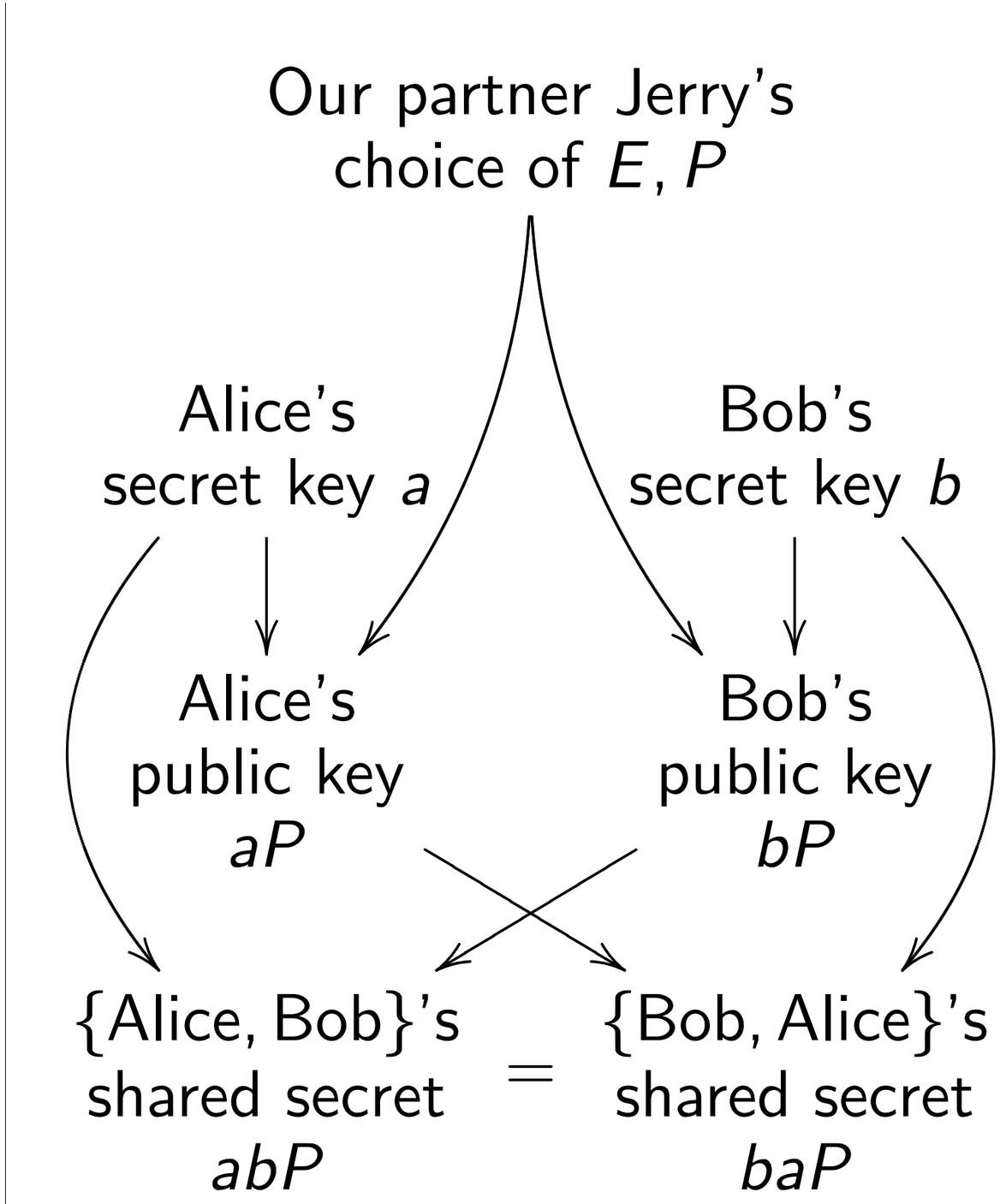


Can we exploit this picture?

Depends on public

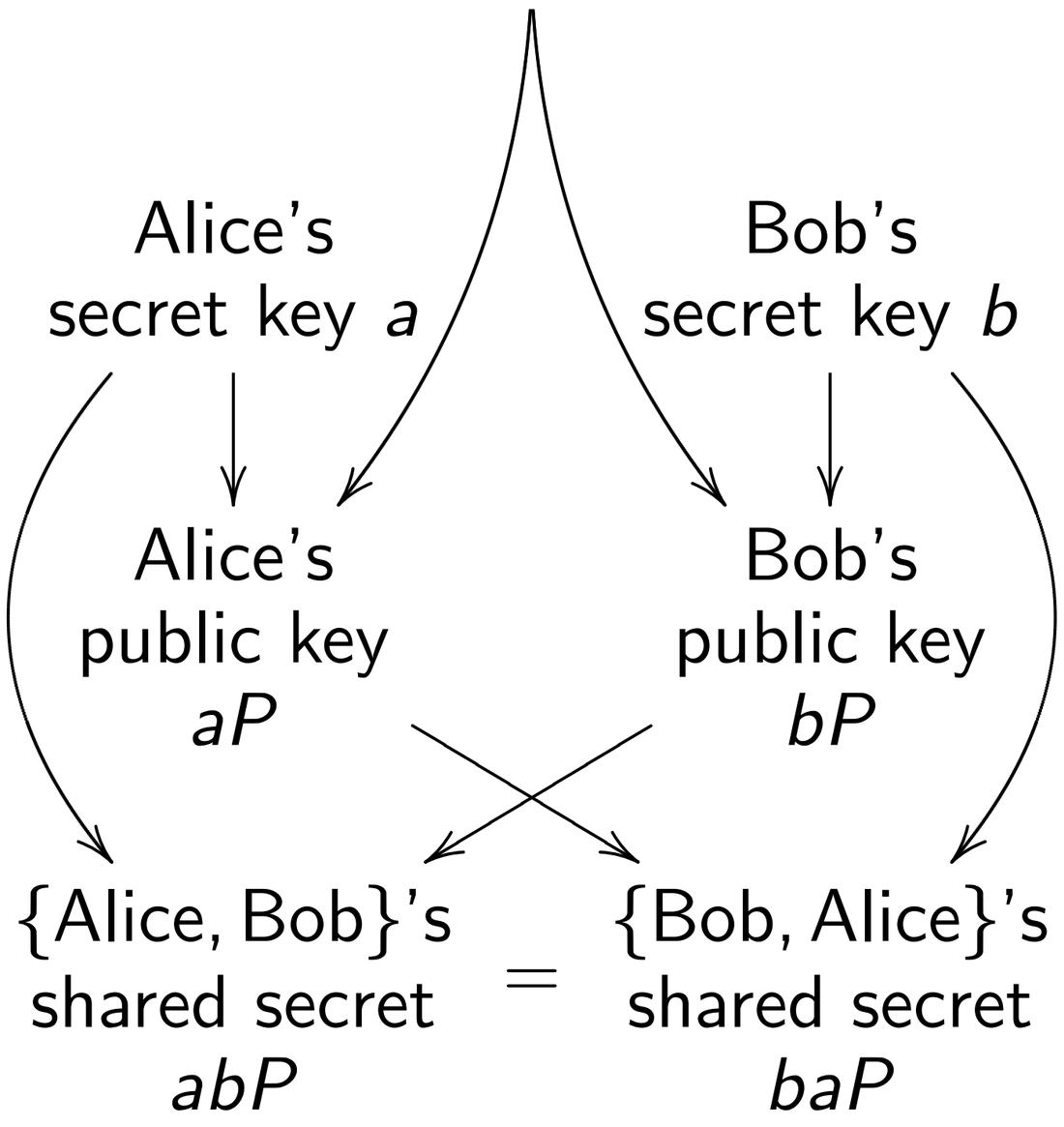
for accepting E, P





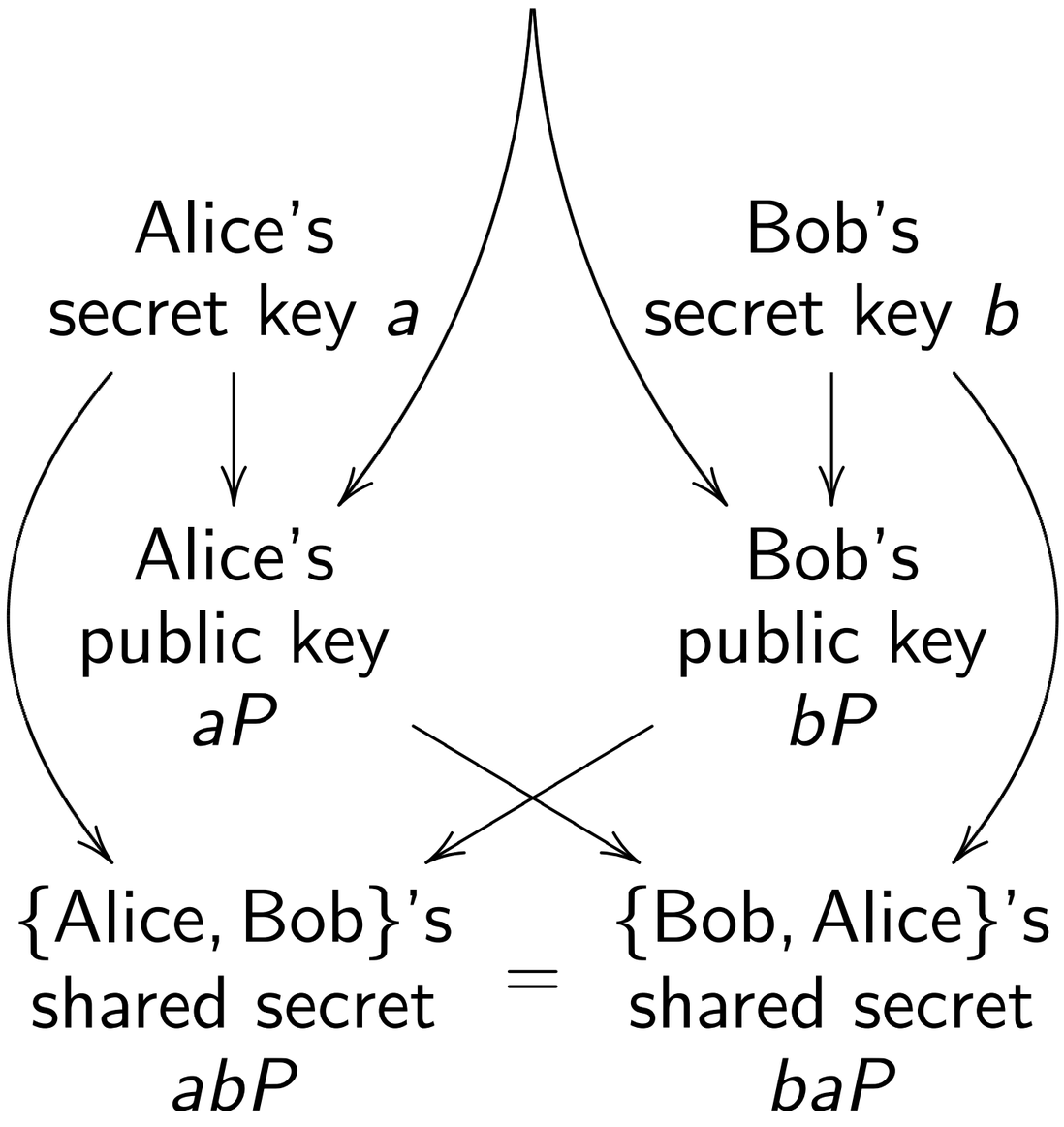
Can we exploit this picture?

Depends on public criteria for accepting E, P.



Can we exploit this picture?

Depends on public criteria for accepting E, P.

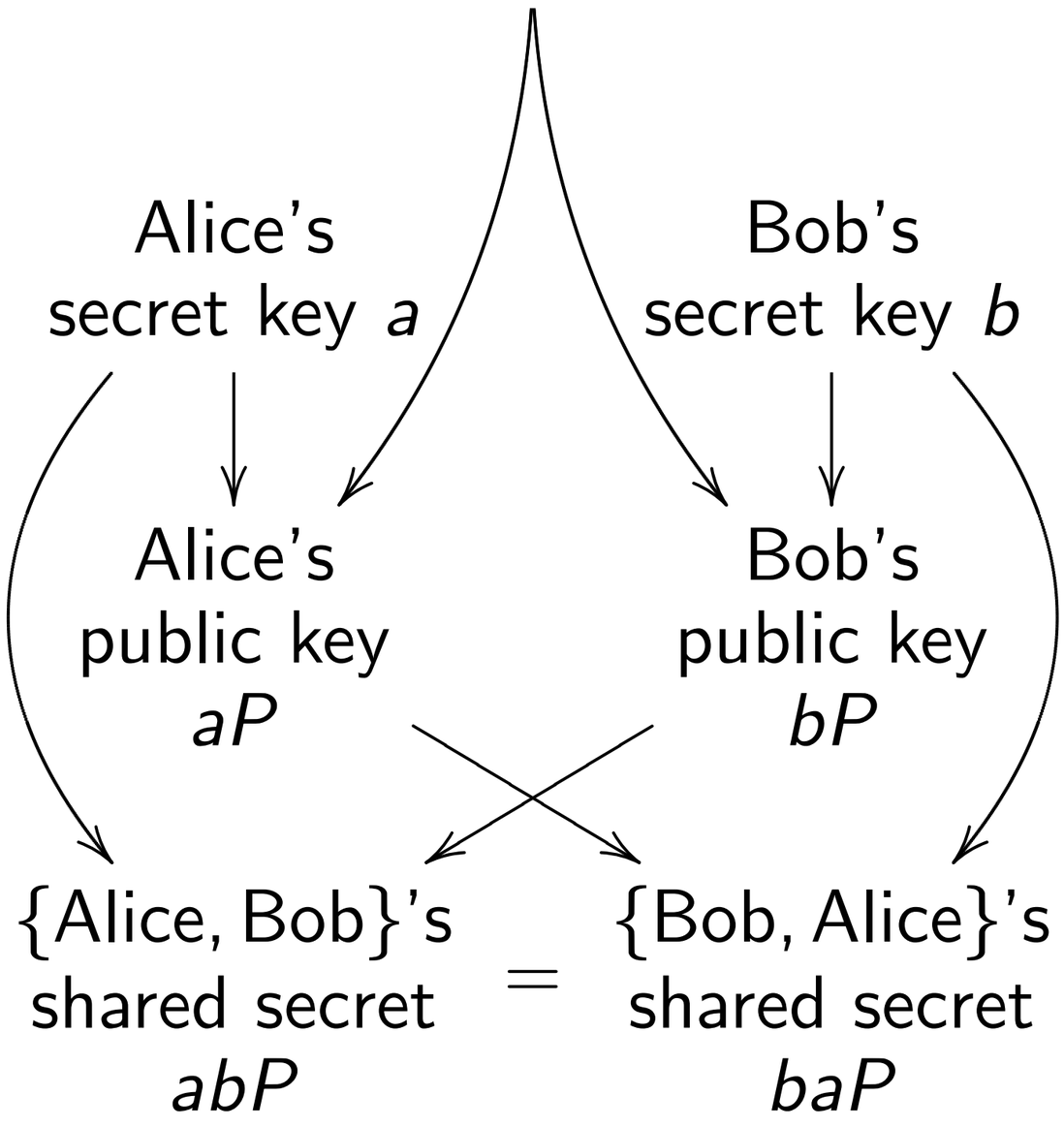


Can we exploit this picture?

Depends on public criteria for accepting E, P.

Extensive ECC literature:
Pollard rho breaks small E,
Pohlig–Hellman breaks most E,
MOV/FR breaks some E,
SmartASS breaks some E, etc.

Assume that public will accept any E not publicly broken.



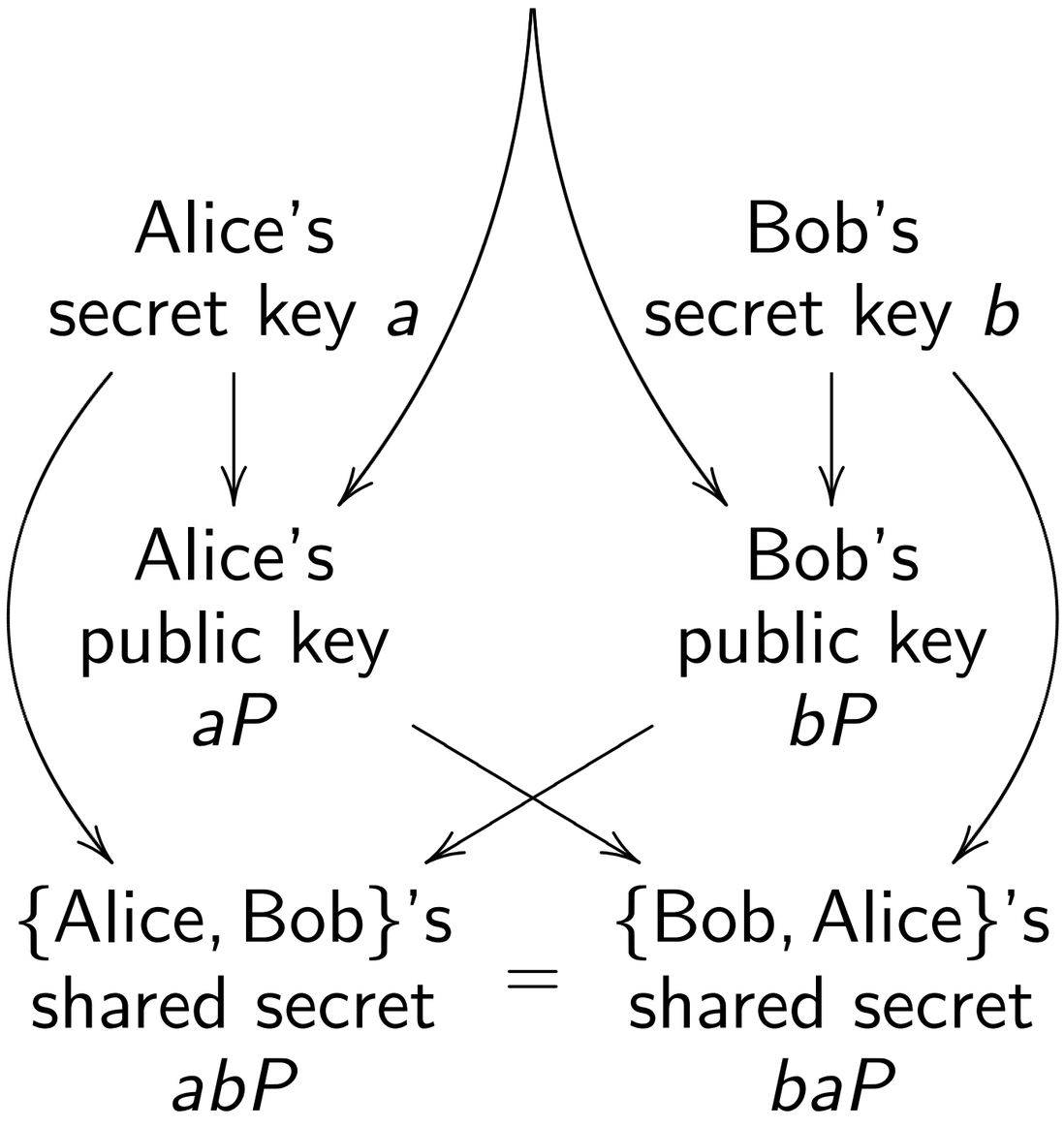
Can we exploit this picture?

Depends on public criteria for accepting E, P.

Extensive ECC literature:
Pollard rho breaks small E,
Pohlig–Hellman breaks most E,
MOV/FR breaks some E,
SmartASS breaks some E, etc.

Assume that public will accept any E not publicly broken.

Assume that we've figured out how to break another curve E.



Can we exploit this picture?

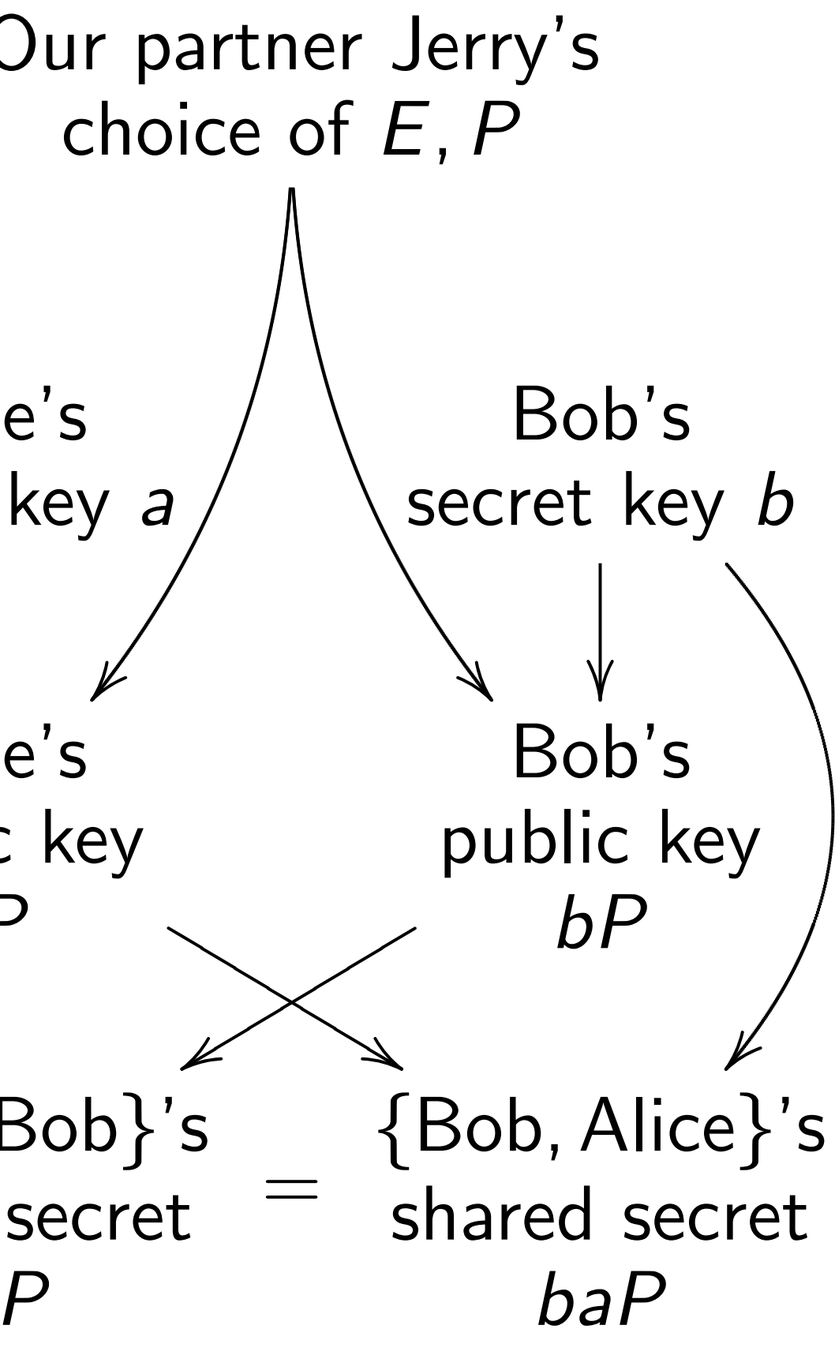
Depends on public criteria for accepting E, P.

Extensive ECC literature:
Pollard rho breaks small E,
Pohlig–Hellman breaks most E,
MOV/FR breaks some E,
SmartASS breaks some E, etc.

Assume that public will accept any E not publicly broken.

Assume that we've figured out how to break another curve E.

Jerry standardizes this curve.
Alice and Bob use it.



exploit this picture?

Depends on public criteria
for accepting E, P.

Extensive ECC literature:
Pollard rho breaks small E,
Pohlig–Hellman breaks most E,
MOV/FR breaks some E,
SmartASS breaks some E, etc.

Assume that public will accept
any E not publicly broken.

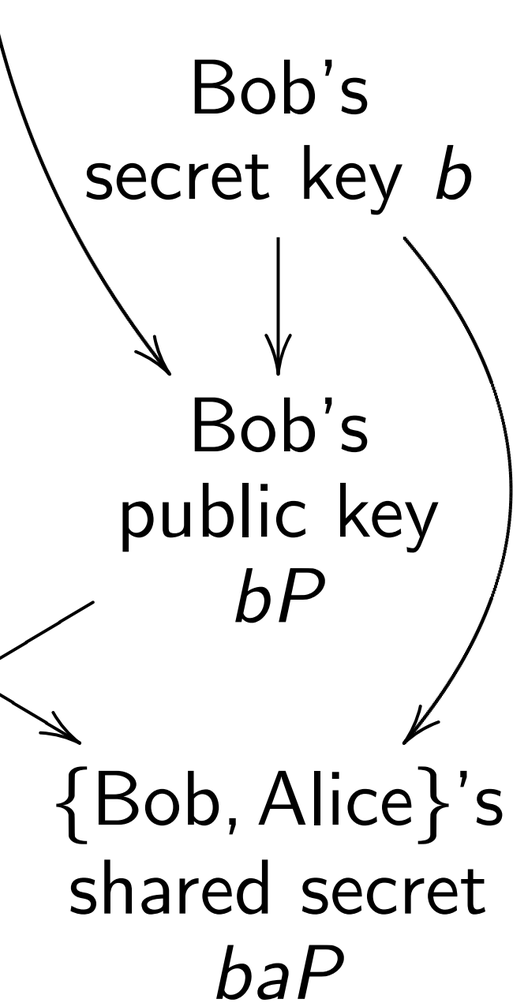
Assume that we've figured out
how to break another curve E.

Jerry standardizes this curve.
Alice and Bob use it.

Is first a

Would t
any curv
that surv

er Jerry's
f E, P



s picture?

Depends on public criteria
for accepting E, P.

Extensive ECC literature:
Pollard rho breaks small E,
Pohlig–Hellman breaks most E,
MOV/FR breaks some E,
SmartASS breaks some E, etc.

Assume that public will accept
any E not publicly broken.

Assume that we've figured out
how to break another curve E.

Jerry standardizes this curve.
Alice and Bob use it.

Is first assumption

Would the public

any curve chosen

that survives these

's
key b

's
key

ice}'s
secret
?

Depends on public criteria
for accepting E, P.

Extensive ECC literature:
Pollard rho breaks small E,
Pohlig–Hellman breaks most E,
MOV/FR breaks some E,
SmartASS breaks some E, etc.

Assume that public will accept
any E not publicly broken.

Assume that we've figured out
how to break another curve E.

Jerry standardizes this curve.
Alice and Bob use it.

Is first assumption plausible?

Would the public really acce
any curve chosen by Jerry
that survives these criteria?

Depends on public criteria
for accepting E, P.

Extensive ECC literature:
Pollard rho breaks small E,
Pohlig–Hellman breaks most E,
MOV/FR breaks some E,
SmartASS breaks some E, etc.

Assume that public will accept
any E not publicly broken.

Assume that we've figured out
how to break another curve E.

Jerry standardizes this curve.
Alice and Bob use it.

Is first assumption plausible?

Would the public really accept
any curve chosen by Jerry
that survives these criteria?

Depends on public criteria
for accepting E, P.

Extensive ECC literature:
Pollard rho breaks small E,
Pohlig–Hellman breaks most E,
MOV/FR breaks some E,
SmartASS breaks some E, etc.

Assume that public will accept
any E not publicly broken.

Assume that we've figured out
how to break another curve E.

Jerry standardizes this curve.
Alice and Bob use it.

Is first assumption plausible?

Would the public really accept
any curve chosen by Jerry
that survives these criteria?

Example showing plausibility:
French ANSSI FRP256V1 (2011)
is a random-looking curve
that survives these criteria
and has no other justification.

Depends on public criteria
for accepting E, P.

Extensive ECC literature:
Pollard rho breaks small E,
Pohlig–Hellman breaks most E,
MOV/FR breaks some E,
SmartASS breaks some E, etc.

Assume that public will accept
any E not publicly broken.

Assume that we've figured out
how to break another curve E.

Jerry standardizes this curve.
Alice and Bob use it.

Is first assumption plausible?

Would the public really accept
any curve chosen by Jerry
that survives these criteria?

Example showing plausibility:
French ANSSI FRP256V1 (2011)
is a random-looking curve
that survives these criteria
and has no other justification.

Earlier example:
Chinese OSCCA SM2 (2010).

s on public criteria
pting E, P.

e ECC literature:
rho breaks small E,
Hellman breaks most E,
R breaks some E,
SS breaks some E, etc.

that public will accept
ot publicly broken.

that we've figured out
break another curve E.

andardizes this curve.
d Bob use it.

Is first assumption plausible?

Would the public really accept
any curve chosen by Jerry
that survives these criteria?

Example showing plausibility:
French ANSSI FRP256V1 (2011)
is a random-looking curve
that survives these criteria
and has no other justification.

Earlier example:
Chinese OSCCA SM2 (2010).

Maybe p
outside
E must
and Jerr
"seed" s

c criteria
.

erature:
small E,
reaks most E,
some E,
some E, etc.

c will accept
broken.

e figured out
her curve E.

this curve.
it.

Is first assumption plausible?

Would the public really accept
any curve chosen by Jerry
that survives these criteria?

Example showing plausibility:
French ANSSI FRP256V1 (2011)
is a random-looking curve
that survives these criteria
and has no other justification.

Earlier example:
Chinese OSCCA SM2 (2010).

Maybe public is m
outside France an
E must not be pu
and Jerry must pr
"seed" s such that

t E,

etc.

ept

out

E.

e.

Is first assumption plausible?

Would the public really accept
any curve chosen by Jerry
that survives these criteria?

Example showing plausibility:
French ANSSI FRP256V1 (2011)
is a random-looking curve
that survives these criteria
and has no other justification.

Earlier example:
Chinese OSCCA SM2 (2010).

Maybe public is more dema
outside France and China:
E must not be publicly brok
and Jerry must provide a
"seed" s such that $E = H(s$

Is first assumption plausible?

Would the public really accept
any curve chosen by Jerry
that survives these criteria?

Example showing plausibility:
French ANSSI FRP256V1 (2011)
is a random-looking curve
that survives these criteria
and has no other justification.

Earlier example:
Chinese OSCCA SM2 (2010).

Maybe public is more demanding
outside France and China:
E must not be publicly broken,
and Jerry must provide a
"seed" s such that $E = H(s)$.

Is first assumption plausible?

Would the public really accept
any curve chosen by Jerry
that survives these criteria?

Example showing plausibility:
French ANSSI FRP256V1 (2011)
is a random-looking curve
that survives these criteria
and has no other justification.

Earlier example:
Chinese OSCCA SM2 (2010).

Maybe public is more demanding
outside France and China:
E must not be publicly broken,
and Jerry must provide a
"seed" s such that $E = H(s)$.

Examples: ANSI X9.62 (1999)
"selecting an elliptic curve
verifiably at random"; Certicom
SEC 2 1.0 (2000) "verifiably
random parameters offer
some additional conservative
features"—"parameters cannot
be predetermined"; NIST FIPS
186-2 (2000); ANSI X9.63 (2001);
Certicom SEC 2 2.0 (2010).

ssumption plausible?

he public really accept
ve chosen by Jerry
vives these criteria?

e showing plausibility:
ANSSI FRP256V1 (2011)
dom-looking curve
vives these criteria
no other justification.

xample:
OSCCA SM2 (2010).

Maybe public is more demanding
outside France and China:
E must not be publicly broken,
and Jerry must provide a
"seed" s such that $E = H(s)$.

Examples: ANSI X9.62 (1999)
"selecting an elliptic curve
verifiably at random"; Certicom
SEC 2 1.0 (2000) "verifiably
random parameters offer
some additional conservative
features"—"parameters cannot
be predetermined"; NIST FIPS
186-2 (2000); ANSI X9.63 (2001);
Certicom SEC 2 2.0 (2010).

What ex

NIST de
$y^2 = x^3$
$b^2c = -$
hash is S

plausible?

really accept
by Jerry
e criteria?

plausibility:
P256V1 (2011)
ng curve
e criteria
justification.

M2 (2010).

Maybe public is more demanding outside France and China: E must not be publicly broken, *and* Jerry must provide a "seed" s such that $E = H(s)$.

Examples: ANSI X9.62 (1999) "selecting an elliptic curve verifiably at random"; Certicom SEC 2 1.0 (2000) "verifiably random parameters offer some additional conservative features"—"parameters cannot be predetermined"; NIST FIPS 186-2 (2000); ANSI X9.63 (2001); Certicom SEC 2 2.0 (2010).

What exactly is H

NIST defines curv
$y^2 = x^3 - 3x + b$
$b^2c = -27$; c is a
hash is SHA-1 co

?

ept

y:

2011)

n.

).

Maybe public is more demanding outside France and China: E must not be publicly broken, *and* Jerry must provide a "seed" s such that $E = H(s)$.

Examples: ANSI X9.62 (1999) "selecting an elliptic curve verifiably at random"; Certicom SEC 2 1.0 (2000) "verifiably random parameters offer some additional conservative features"—"parameters cannot be predetermined"; NIST FIPS 186-2 (2000); ANSI X9.63 (2001); Certicom SEC 2 2.0 (2010).

What exactly is H?

NIST defines curve E as $y^2 = x^3 - 3x + b$ where $b^2c = -27$; c is a hash of s hash is SHA-1 concatenation

Maybe public is more demanding outside France and China: E must not be publicly broken, *and* Jerry must provide a "seed" s such that $E = H(s)$.

Examples: ANSI X9.62 (1999) "selecting an elliptic curve verifiably at random"; Certicom SEC 2 1.0 (2000) "verifiably random parameters offer some additional conservative features"—"parameters cannot be predetermined"; NIST FIPS 186-2 (2000); ANSI X9.63 (2001); Certicom SEC 2 2.0 (2010).

What exactly is H?

NIST defines curve E as $y^2 = x^3 - 3x + b$ where $b^2c = -27$; c is a hash of s; hash is SHA-1 concatenation.

Maybe public is more demanding outside France and China: E must not be publicly broken, *and* Jerry must provide a "seed" s such that $E = H(s)$.

Examples: ANSI X9.62 (1999) "selecting an elliptic curve verifiably at random"; Certicom SEC 2 1.0 (2000) "verifiably random parameters offer some additional conservative features"—"parameters cannot be predetermined"; NIST FIPS 186-2 (2000); ANSI X9.63 (2001); Certicom SEC 2 2.0 (2010).

What exactly is H?

NIST defines curve E as $y^2 = x^3 - 3x + b$ where $b^2c = -27$; c is a hash of s; hash is SHA-1 concatenation.

But clearly public will accept other choices of H.

Maybe public is more demanding outside France and China:
E must not be publicly broken,
and Jerry must provide a
"seed" s such that $E = H(s)$.

Examples: ANSI X9.62 (1999)
"selecting an elliptic curve
verifiably at random"; Certicom
SEC 2 1.0 (2000) "verifiably
random parameters offer
some additional conservative
features"—"parameters cannot
be predetermined"; NIST FIPS
186-2 (2000); ANSI X9.63 (2001);
Certicom SEC 2 2.0 (2010).

What exactly is H?

NIST defines curve E as
$y^2 = x^3 - 3x + b$ where
$b^2c = -27$; c is a hash of s;
hash is SHA-1 concatenation.

But clearly public will accept
other choices of H.

Examples: Brainpool (2005)
uses $c = g^3/h^2$ where
g and h are separate hashes.
NIST FIPS 186-4 (2013) requires
an "approved hash function, as
specified in FIPS 180";
no longer allows SHA-1!

ublic is more demanding
France and China:
not be publicly broken,
y must provide a
s such that $E = H(s)$.

es: ANSI X9.62 (1999)
ng an elliptic curve
y at random"; Certicom
.0 (2000) "verifiably
parameters offer
ditional conservative
"—"parameters cannot
etermined"; NIST FIPS
2000); ANSI X9.63 (2001);
n SEC 2 2.0 (2010).

What exactly is H?

NIST defines curve E as
$y^2 = x^3 - 3x + b$ where
$b^2c = -27$; c is a hash of s;
hash is SHA-1 concatenation.

But clearly public will accept
other choices of H.

Examples: Brainpool (2005)
uses $c = g^3/h^2$ where
g and h are separate hashes.
NIST FIPS 186-4 (2013) requires
an "approved hash function, as
specified in FIPS 180";
no longer allows SHA-1!

1999 Sc
possibili
of all cu
structure
but we c
generate
until the
one of 't
get us to

ore demanding
d China:
blicly broken,
ovide a
t $E = H(s)$.

K9.62 (1999)
tic curve
m"; Certicom
"verifiably
s offer
onservative
neters cannot
; NIST FIPS
SI X9.63 (2001);
.0 (2010).

What exactly is H?

NIST defines curve E as
$y^2 = x^3 - 3x + b$ where
$b^2c = -27$; c is a hash of s;
hash is SHA-1 concatenation.

But clearly public will accept
other choices of H.

Examples: Brainpool (2005)
uses $c = g^3/h^2$ where
g and h are separate hashes.
NIST FIPS 186-4 (2013) requires
an "approved hash function, as
specified in FIPS 180";
no longer allows SHA-1!

1999 Scott: "Cons
possibility that on
of all curves have
structure that 'the
but we don't. The
generate a million
until they find one
one of 'their' curv
get us to use them

nding

ken,

s).

99)

com

y

e

not

PS

2001);

What exactly is H?

NIST defines curve E as
$y^2 = x^3 - 3x + b$ where
$b^2c = -27$; c is a hash of s;
hash is SHA-1 concatenation.

But clearly public will accept
other choices of H.

Examples: Brainpool (2005)
uses $c = g^3/h^2$ where
g and h are separate hashes.
NIST FIPS 186-4 (2013) requires
an "approved hash function, as
specified in FIPS 180";
no longer allows SHA-1!

1999 Scott: "Consider now
possibility that one in a mill
of all curves have an exploit
structure that 'they' know a
but we don't. Then 'they' s
generate a million random s
until they find one that gene
one of 'their' curves. Then t
get us to use them."

What exactly is H?

NIST defines curve E as
$y^2 = x^3 - 3x + b$ where
$b^2c = -27$; c is a hash of s;
hash is SHA-1 concatenation.

But clearly public will accept
other choices of H.

Examples: Brainpool (2005)
uses $c = g^3/h^2$ where
g and h are separate hashes.
NIST FIPS 186-4 (2013) requires
an "approved hash function, as
specified in FIPS 180";
no longer allows SHA-1!

1999 Scott: "Consider now the possibility that one in a million of all curves have an exploitable structure that 'they' know about, but we don't. Then 'they' simply generate a million random seeds until they find one that generates one of 'their' curves. Then they get us to use them."

What exactly is H?

NIST defines curve E as
$y^2 = x^3 - 3x + b$ where
$b^2c = -27$; c is a hash of s;
hash is SHA-1 concatenation.

But clearly public will accept
other choices of H.

Examples: Brainpool (2005)
uses $c = g^3/h^2$ where
g and h are separate hashes.
NIST FIPS 186-4 (2013) requires
an "approved hash function, as
specified in FIPS 180";
no longer allows SHA-1!

1999 Scott: "Consider now the possibility that one in a million of all curves have an exploitable structure that 'they' know about, but we don't. Then 'they' simply generate a million random seeds until they find one that generates one of 'their' curves. Then they get us to use them."

New: Optimized this computation using Keccak on cluster of 41 GTX780 GPUs. In 7 hours found "secure+twist-secure" $b =$ `0x`
`BADA55EC`D8BBEAD3ADD6C534F92197DE
B47FCEB9BE7E0E702A8D1DD56B5D0B0C.

xactly is H?

efines curve E as
$-3x+b$ where
-27; c is a hash of s;
SHA-1 concatenation.

rly public will accept
oices of H.

es: Brainpool (2005)
$= g^3/h^2$ where
are separate hashes.
PS 186-4 (2013) requires
roved hash function, as
l in FIPS 180";
er allows SHA-1!

1999 Scott: "Consider now the possibility that one in a million of all curves have an exploitable structure that 'they' know about, but we don't. Then 'they' simply generate a million random seeds until they find one that generates one of 'their' curves. Then they get us to use them."

New: Optimized this computation using Keccak on cluster of 41 GTX780 GPUs. In 7 hours found "secure+twist-secure" $b =$ `0x`
`BADA55EC`D8BBEAD3ADD6C534F92197DE
B47FCEB9BE7E0E702A8D1DD56B5D0B0C.

Maybe i
the publ

?

e E as
where
hash of s;
ncatenation.

will accept
I.

ool (2005)
here
ate hashes.
(2013) requires
n function, as
180";
HA-1!

1999 Scott: "Consider now the possibility that one in a million of all curves have an exploitable structure that 'they' know about, but we don't. Then 'they' simply generate a million random seeds until they find one that generates one of 'their' curves. Then they get us to use them."

New: Optimized this computation using Keccak on cluster of 41 GTX780 GPUs. In 7 hours found "secure+twist-secure" $b =$ `0x`
`BADA55EC`D8BBEAD3ADD6C534F92197DE
B47FCEB9BE7E0E702A8D1DD56B5D0B0C.

Maybe in some co
the public is more

;
n.
t

)
.
quires
as

1999 Scott: "Consider now the possibility that one in a million of all curves have an exploitable structure that 'they' know about, but we don't. Then 'they' simply generate a million random seeds until they find one that generates one of 'their' curves. Then they get us to use them."

New: Optimized this computation using Keccak on cluster of 41 GTX780 GPUs. In 7 hours found "secure+twist-secure" $b =$ 0x BADA55ECD8BBEAD3ADD6C534F92197DE B47FCEB9BE7E0E702A8D1DD56B5D0B0C.

Maybe in some countries the public is more demandin

1999 Scott: "Consider now the possibility that one in a million of all curves have an exploitable structure that 'they' know about, but we don't. Then 'they' simply generate a million random seeds until they find one that generates one of 'their' curves. Then they get us to use them."

New: Optimized this computation using Keccak on cluster of 41 GTX780 GPUs. In 7 hours found "secure+twist-secure" $b = \texttt{0x}$

BADA55ECD8BBEAD3ADD6C534F92197DE

B47FCEB9BE7E0E702A8D1DD56B5D0B0C.

Maybe in some countries the public is more demanding.

1999 Scott: "Consider now the possibility that one in a million of all curves have an exploitable structure that 'they' know about, but we don't. Then 'they' simply generate a million random seeds until they find one that generates one of 'their' curves. Then they get us to use them."

New: Optimized this computation using Keccak on cluster of 41 GTX780 GPUs. In 7 hours found "secure+twist-secure" $b =$ `0x`
`BADA55EC`D8BBEAD3ADD6C534F92197DE
B47FCEB9BE7E0E702A8D1DD56B5D0B0C.

Maybe in some countries the public is more demanding.

Brainpool standard:
"The choice of the seeds from which the [NIST] curve parameters have been derived is not motivated leaving an essential part of the security analysis open. . . .
Verifiably pseudo-random.
The [Brainpool] curves shall be generated in a pseudo-random manner using seeds that are generated in a systematic and comprehensive way."

ott: “Consider now the
ty that one in a million
rves have an exploitable
e that ‘they’ know about,
don’t. Then ‘they’ simply
e a million random seeds
ey find one that generates
their’ curves. Then they
o use them.”

ptimized this computation
eccak on cluster of 41
GPUs. In 7 hours found
+twist-secure” $b =$ 0x
CD8BBEAD3ADD6C534F92197DE
9BE7E0E702A8D1DD56B5D0B0C.

Maybe in some countries
the public is more demanding.

Brainpool standard:
“The choice of the seeds
from which the [NIST] curve
parameters have been derived is
not motivated leaving an essential
part of the security analysis
open. . . .
Verifiably pseudo-random.
The [Brainpool] curves shall be
generated in a pseudo-random
manner using seeds that are
generated in a systematic and
comprehensive way.”

Wikiped
nothing
are any
construc
of hidde

Microsof
“generat
from the

Albertin
Mendel–
hashing”
in hash
expected
nothing-

sider now the
e in a million
an exploitable
ey' know about,
en 'they' simply
random seeds
e that generates
es. Then they
n."

his computation
luster of 41
n 7 hours found
ure" $b =$ 0x
ADD6C534F92197DE
2A8D1DD56B5D0B0C.

Maybe in some countries
the public is more demanding.

Brainpool standard:
"The choice of the seeds
from which the [NIST] curve
parameters have been derived is
not motivated leaving an essential
part of the security analysis
open. . . .
Verifiably pseudo-random.
The [Brainpool] curves shall be
generated in a pseudo-random
manner using seeds that are
generated in a systematic and
comprehensive way."

Wikipedia: "In cry
nothing up my sl
are any numbers w
construction, are a
of hidden properti

Microsoft "NUMS
"generated determ
from the security

Albertini–Aumasso
Mendel–Schläffer
hashing" (2014):
in hash functions a
expected to be ide
nothing-up-your-sl

the
ion
able
bout,
imply
eeds
erates
they

itation
41
found
0x
92197DE
B5D0B0C.

Maybe in some countries
the public is more demanding.

Brainpool standard:
"The choice of the seeds
from which the [NIST] curve
parameters have been derived is
not motivated leaving an essential
part of the security analysis
open. . . .
Verifiably pseudo-random.
The [Brainpool] curves shall be
generated in a pseudo-random
manner using seeds that are
generated in a systematic and
comprehensive way."

Wikipedia: "In cryptography
nothing up my sleeve num
are any numbers which, by t
construction, are above susp
of hidden properties."

Microsoft "NUMS" curves (
"generated deterministically
from the security level".

Albertini–Aumasson–Eichlse
Mendel–Schläffer "Malicious
hashing" (2014): "constants
in hash functions are normal
expected to be identifiable a
nothing-up-your-sleeve numb

Maybe in some countries
the public is more demanding.

Brainpool standard:
"The choice of the seeds
from which the [NIST] curve
parameters have been derived is
not motivated leaving an essential
part of the security analysis
open. . . .
Verifiably pseudo-random.
The [Brainpool] curves shall be
generated in a pseudo-random
manner using seeds that are
generated in a systematic and
comprehensive way."

Wikipedia: "In cryptography,
nothing up my sleeve numbers
are any numbers which, by their
construction, are above suspicion
of hidden properties."

Microsoft "NUMS" curves (2014):
"generated deterministically
from the security level".

Albertini–Aumasson–Eichlseder–
Mendel–Schläffer "Malicious
hashing" (2014): "constants
in hash functions are normally
expected to be identifiable as
nothing-up-your-sleeve numbers".

n some countries
ic is more demanding.

ol standard:
oice of the seeds
ich the [NIST] curve
ers have been derived is
ivated leaving an essential
he security analysis
.

ly pseudo-random.
ainpool] curves shall be
ed in a pseudo-random
using seeds that are
ed in a systematic and
ensive way."

Wikipedia: "In cryptography, **nothing up my sleeve numbers** are any numbers which, by their construction, are above suspicion of hidden properties."

Microsoft "NUMS" curves (2014): "generated deterministically from the security level".

Albertini–Aumasson–Eichlseder–Mendel–Schläffer "Malicious hashing" (2014): "constants in hash functions are normally expected to be identifiable as nothing-up-your-sleeve numbers".

New: W
curve "E
with a B

untries
demanding.

d:
e seeds
IST] curve
been derived is
ving an essential
y analysis

o-random.
urves shall be
eudo-random
ls that are
tematic and
y."

Wikipedia: "In cryptography, **nothing up my sleeve numbers** are any numbers which, by their construction, are above suspicion of hidden properties."

Microsoft "NUMS" curves (2014): "generated deterministically from the security level".

Albertini–Aumasson–Eichlseder–Mendel–Schläffer "Malicious hashing" (2014): "constants in hash functions are normally expected to be identifiable as nothing-up-your-sleeve numbers".

New: We generate
curve "BADA55-V
with a Brainpool-I

g.

e
ed is
sential

be
om

nd

Wikipedia: “In cryptography, **nothing up my sleeve numbers** are any numbers which, by their construction, are above suspicion of hidden properties.”

Microsoft “NUMS” curves (2014): “generated deterministically from the security level”.

Albertini–Aumasson–Eichlseder–Mendel–Schläffer “Malicious hashing” (2014): “constants in hash functions are normally expected to be identifiable as nothing-up-your-sleeve numbers”.

New: We generated a BADA
curve “BADA55-VPR-224”
with a Brainpool-like explan

Wikipedia: "In cryptography, **nothing up my sleeve numbers** are any numbers which, by their construction, are above suspicion of hidden properties."

Microsoft "NUMS" curves (2014): "generated deterministically from the security level".

Albertini–Aumasson–Eichlseder–Mendel–Schläffer "Malicious hashing" (2014): "constants in hash functions are normally expected to be identifiable as nothing-up-your-sleeve numbers".

New: We generated a BADA55 curve "BADA55-VPR-224" with a Brainpool-like explanation.

Wikipedia: "In cryptography, **nothing up my sleeve numbers** are any numbers which, by their construction, are above suspicion of hidden properties."

Microsoft "NUMS" curves (2014): "generated deterministically from the security level".

Albertini–Aumasson–Eichlseder–Mendel–Schläffer "Malicious hashing" (2014): "constants in hash functions are normally expected to be identifiable as nothing-up-your-sleeve numbers".

New: We generated a BADA55 curve "BADA55-VPR-224" with a Brainpool-like explanation.

We actually generated >1000000 curves, each having a Brainpool-like explanation.

Wikipedia: "In cryptography, **nothing up my sleeve numbers** are any numbers which, by their construction, are above suspicion of hidden properties."

Microsoft "NUMS" curves (2014): "generated deterministically from the security level".

Albertini–Aumasson–Eichlseder–Mendel–Schläffer "Malicious hashing" (2014): "constants in hash functions are normally expected to be identifiable as nothing-up-your-sleeve numbers".

New: We generated a BADA55 curve "BADA55-VPR-224" with a Brainpool-like explanation.

We actually generated >1000000 curves, each having a Brainpool-like explanation.

Example of underlying flexibility: Brainpool generates seeds from exp(1) and primes from arctan(1); MD5 generates constants from sin(1); BADA55-VPR-224 generated a seed from cos(1).

ia: “In cryptography,
up my sleeve numbers
numbers which, by their
ction, are above suspicion
n properties.”

ft “NUMS” curves (2014):
ted deterministically
e security level”.

i–Aumasson–Eichlseder–
-Schläffer “Malicious
” (2014): “constants
functions are normally
d to be identifiable as
up-your-sleeve numbers”.

New: We generated a BADA55 curve “BADA55-VPR-224” with a Brainpool-like explanation.

We actually generated >1000000 curves, each having a Brainpool-like explanation.

Example of underlying flexibility: Brainpool generates seeds from exp(1) and primes from arctan(1); MD5 generates constants from sin(1); BADA55-VPR-224 generated a seed from cos(1).

Many jo

yptography,
eeve numbers
which, by their
above suspicion
es."

" curves (2014):
ninistically
evel".

on–Eichlseder–
"Malicious
"constants
are normally
entifiable as
eeve numbers".

New: We generated a BADA55 curve "BADA55-VPR-224" with a Brainpool-like explanation.

We actually generated >1000000 curves, each having a Brainpool-like explanation.

Example of underlying flexibility: Brainpool generates seeds from exp(1) and primes from arctan(1); MD5 generates constants from sin(1); BADA55-VPR-224 generated a seed from cos(1).

Many jobs availab

Exp

Marke

y,
nbers
their
oicion

2014):

der–
s
s
lly
ns
bers”.

New: We generated a BADA55 curve “BADA55-VPR-224” with a Brainpool-like explanation.

We actually generated >1000000 curves, each having a Brainpool-like explanation.

Example of underlying flexibility: Brainpool generates seeds from exp(1) and primes from arctan(1); MD5 generates constants from sin(1); BADA55-VPR-224 generated a seed from cos(1).

Many jobs available!

New: We generated a BADA55 curve "BADA55-VPR-224" with a Brainpool-like explanation.

We actually generated >1000000 curves, each having a Brainpool-like explanation.

Example of underlying flexibility: Brainpool generates seeds from exp(1) and primes from arctan(1); MD5 generates constants from sin(1); BADA55-VPR-224 generated a seed from cos(1).

Many jobs available!