

# How to manipulate standards

Daniel J. Bernstein

Verizon Communications Inc.

LICENSE: You understand and hereby agree that the audio, video, and text of this presentation are provided “as is”, without warranty of any kind, whether expressed or implied, including, without limitation, the implied warranties of merchantability, fitness for a particular purpose or otherwise. Since you are not a blithering idiot, you also understand that Verizon Communications Inc. and the entire Verizon family of companies are not actually associated in any way with the speaker, have not reviewed the contents of this presentation, and are not responsible for the contents of this presentation. Continuing to read, listen to, or otherwise absorb this information constitutes acceptance of this license. Any court dispute regarding this presentation shall be resolved in the state of Illinois in the United States of America.



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

manipulate standards

. Bernstein

Communications Inc.

You understand and hereby agree  
audio, video, and text of this  
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.  
entire Verizon family of companies  
ually associated in any way with  
, have not reviewed the contents of  
ation, 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.



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

Our core  
Delivering  
from poi

Alice

e standards

n

ications Inc.

d and hereby agree

d text of this

“as is”, without

ether expressed

hout limitation,

merchantability,

urpose or otherwise.

nering idiot, you also

Communications Inc.

amily of companies

ed in any way with

viewed the contents of

e not responsible for

entation. Continuing

erwise absorb this

acceptance of this

ce regarding this

olved in the state

States of America.

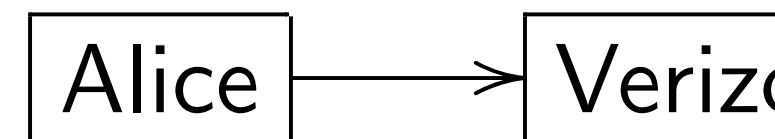


Verizon is a global leader  
delivering innovative  
communications and technology  
solutions that improve the way  
our customers live, work and play.

Our core mission:

Delivering informa

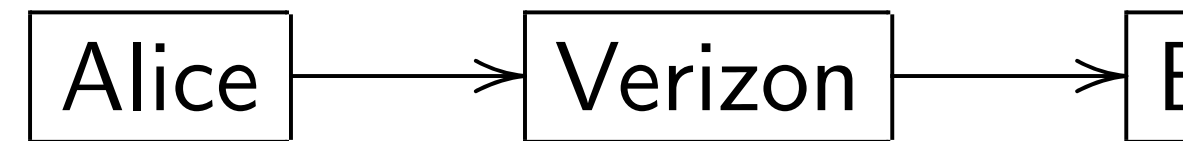
from point A to p





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.





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

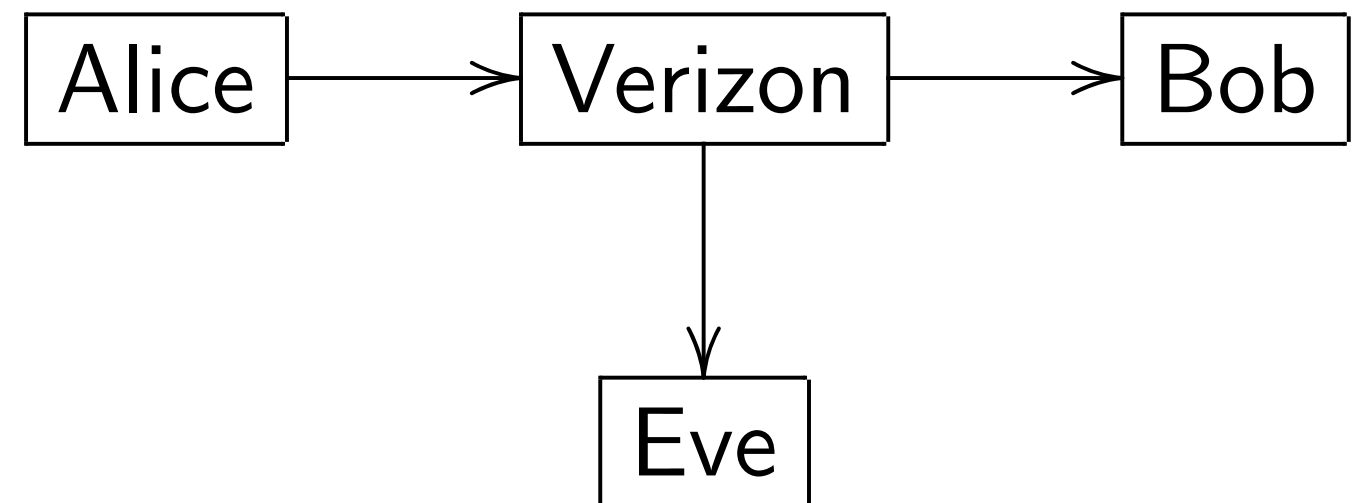
Our core mission:  
Delivering information  
from point A to point B.





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

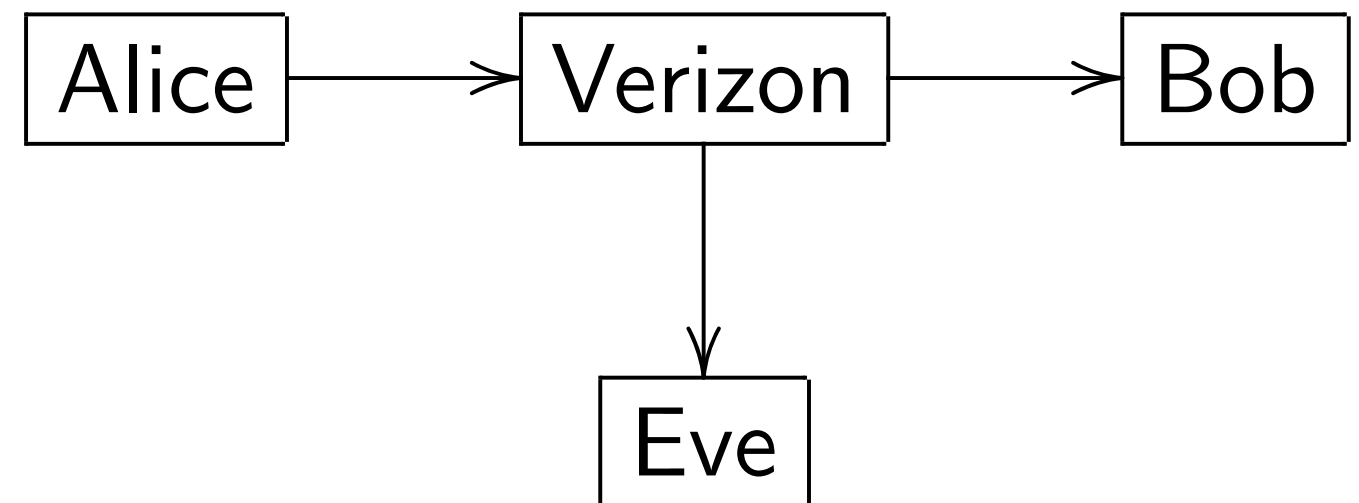
Our core mission:  
Delivering information from point A to point B, and also to points C, D, E, ...





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, ...

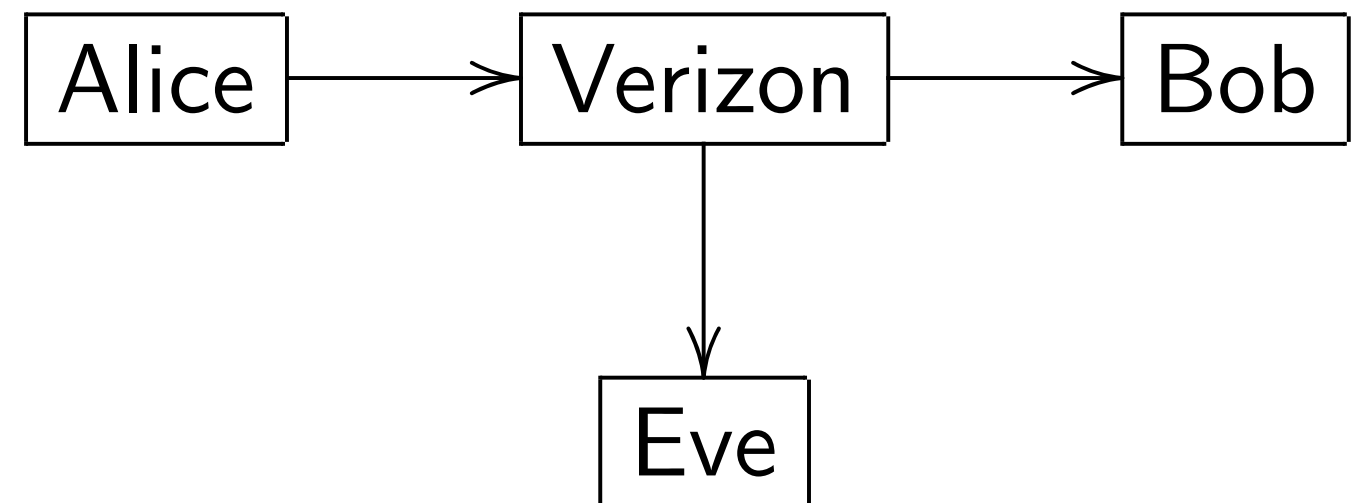


“Can you hear me now? Good.”



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, ...



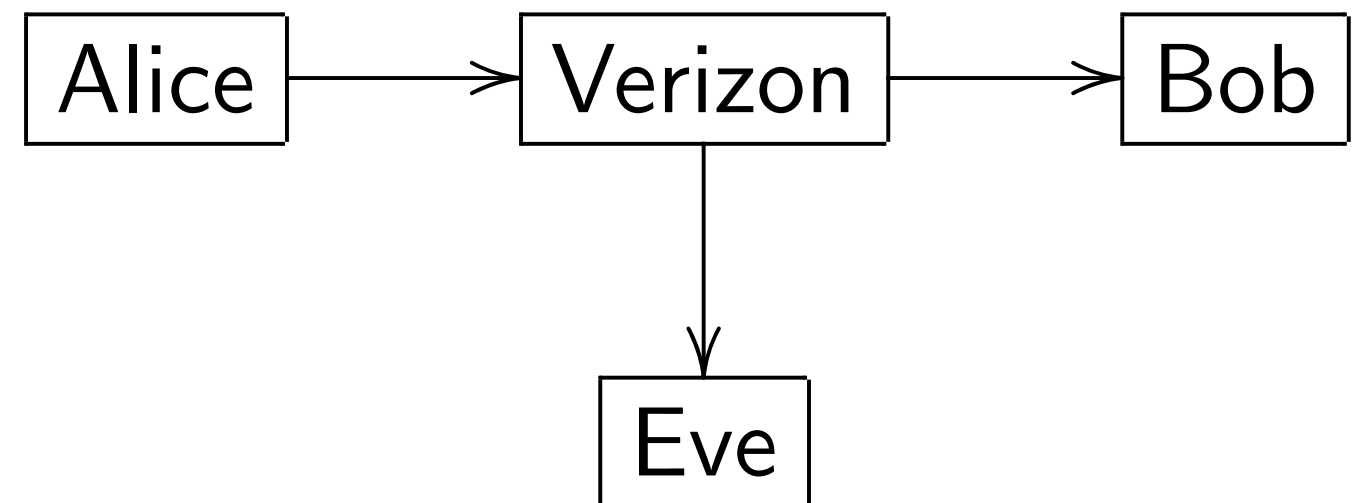
“Can you hear me now? Good.”  
“Can they hear you now? Good.”





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, ...

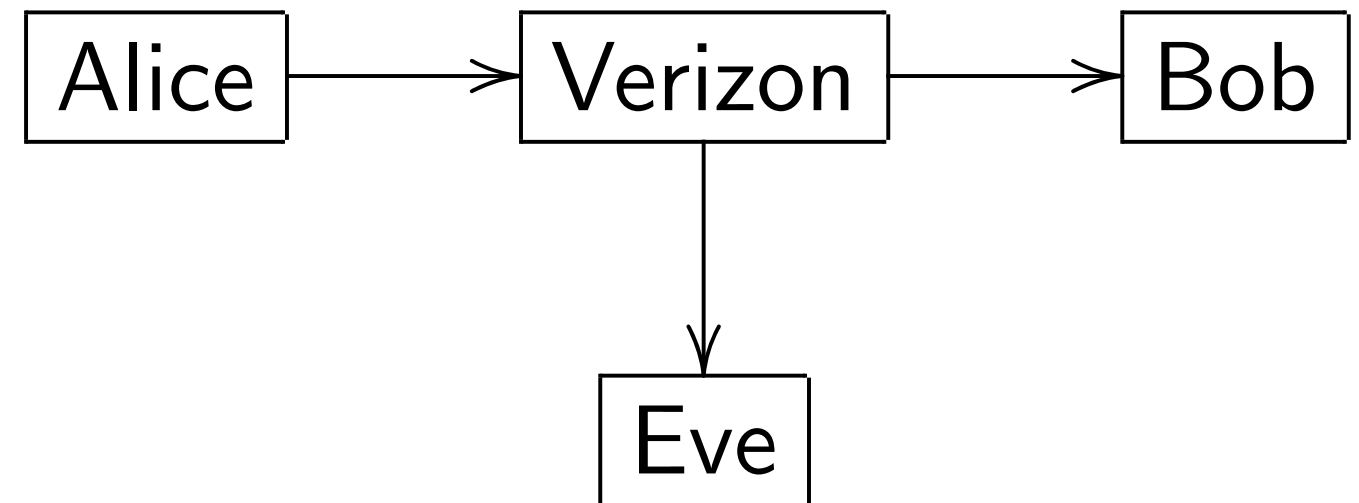


“Can you hear me now? Good.”  
“Can they hear you now? Good.”  
“We never stop working for you.”



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, ...

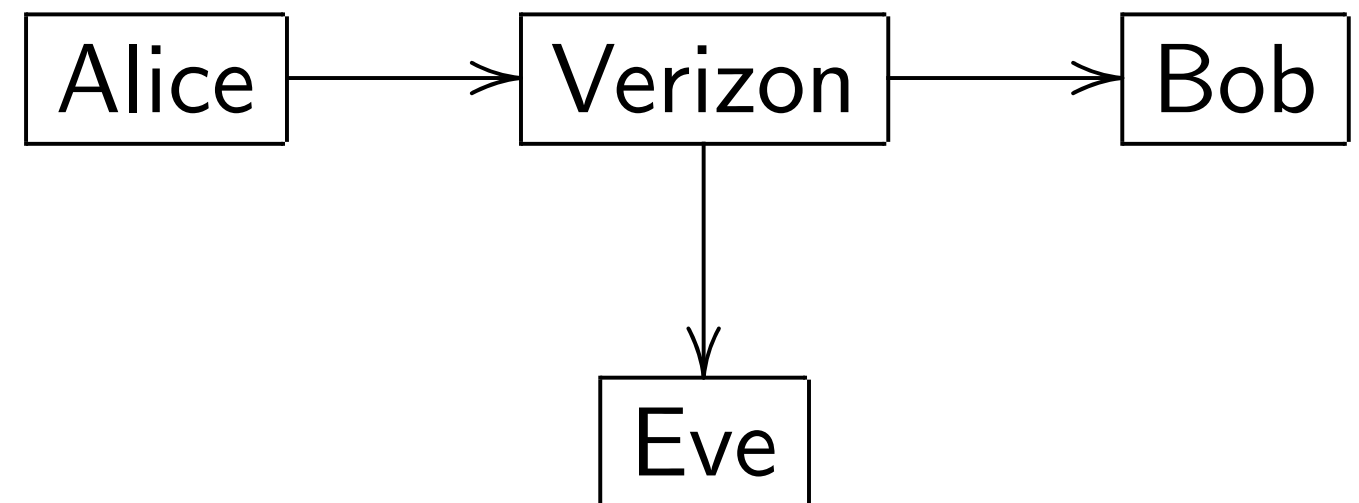


“Can you hear me now? Good.”  
“Can they hear you now? Good.”  
“We never stop working for you.”  
“Rule the air.”



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, ...

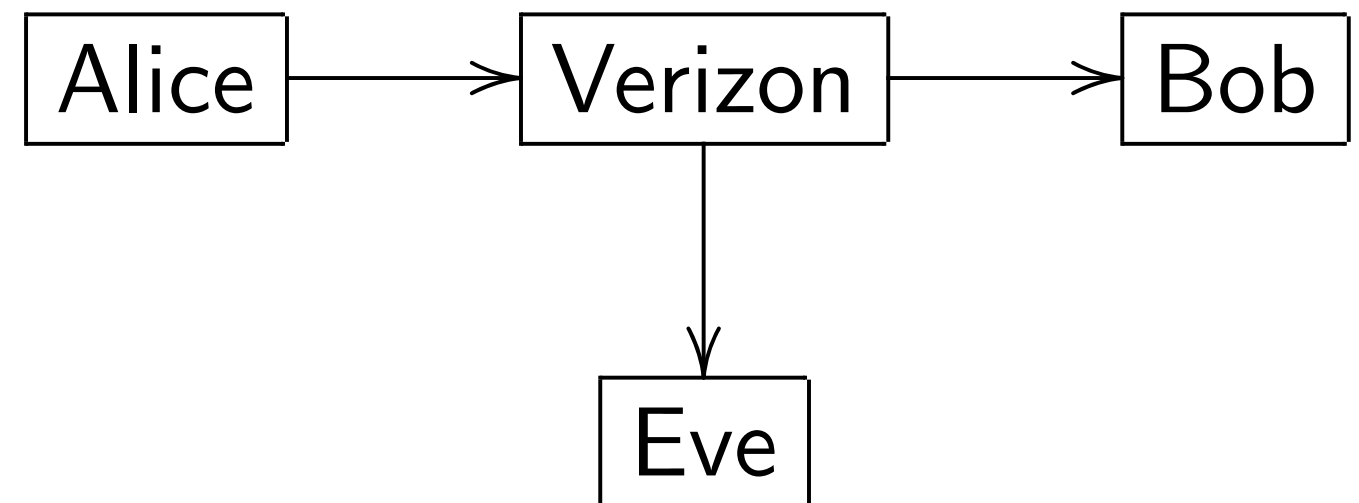


“Can you hear me now? Good.”  
“Can they hear you now? Good.”  
“We never stop working for you.”  
“Rule the air.”  
“Never settle.”



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, ...

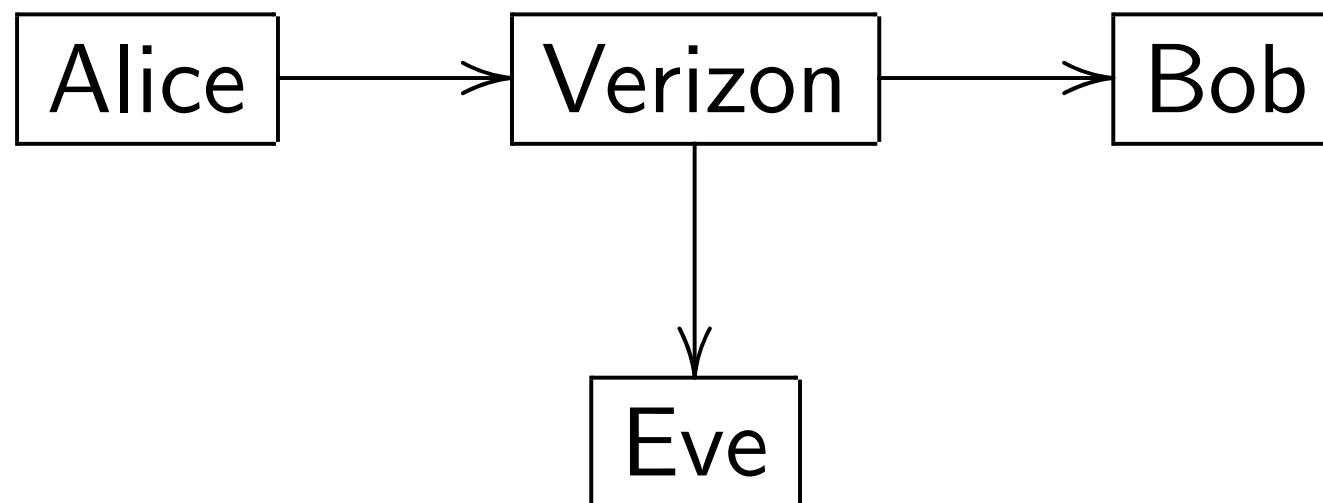


“Can you hear me now? Good.”  
“Can they hear you now? Good.”  
“We never stop working for you.”  
“Rule the air.”  
“Never settle.”  
“I am the man in the middle.”



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.”

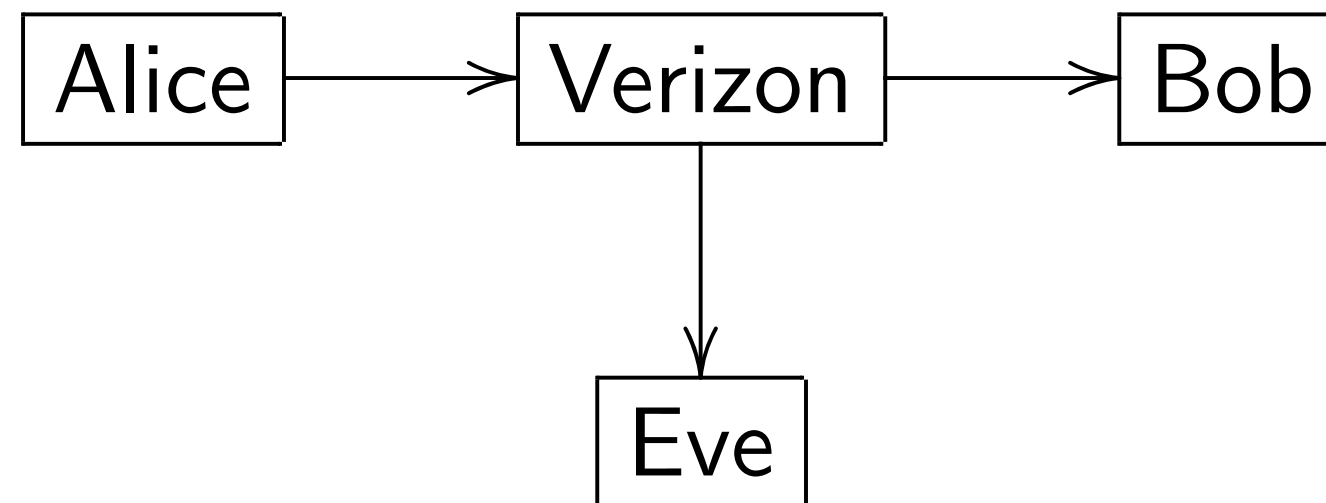
“I am the man in the middle.”

Ultimate



l leader  
ve  
nd technology  
rove the way  
, work and play.

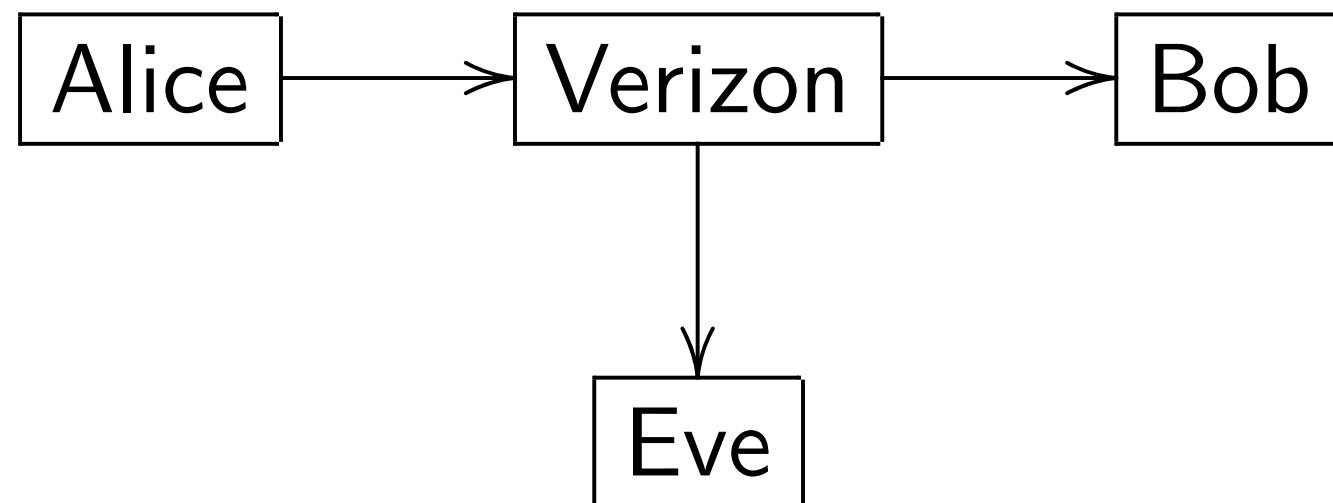
Our core mission:  
Delivering information  
from point A to point B,  
and also to points C, D, E, ...



“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: Ma

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.”

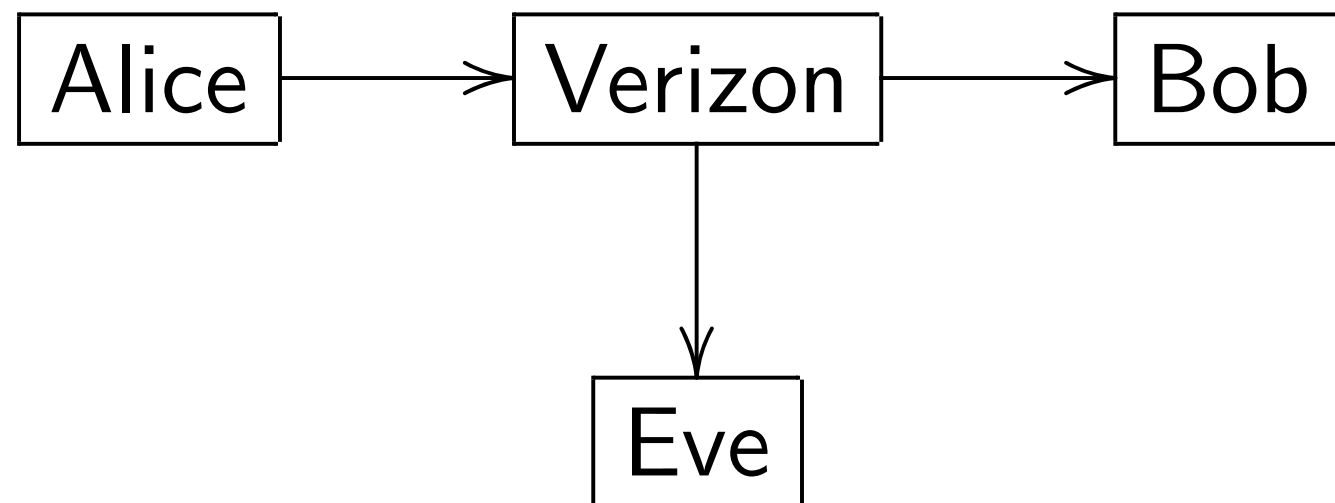
“I am the man in the middle.”

Ultimate goal: Make money

logy  
way  
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.”

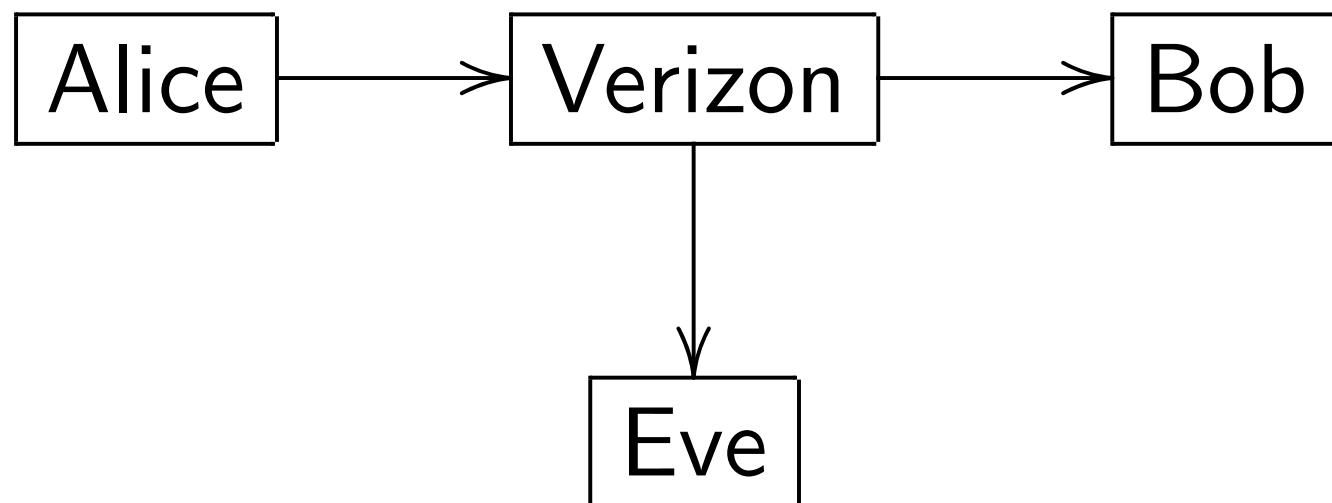
“I am the man in the middle.”

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.”

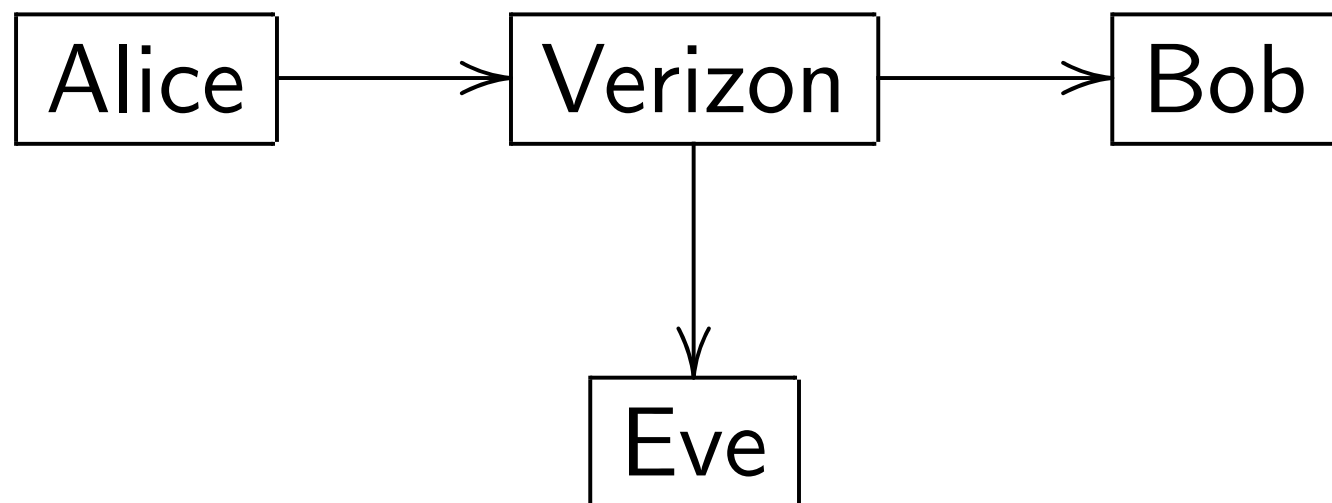
“I am the man in the middle.”

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.”

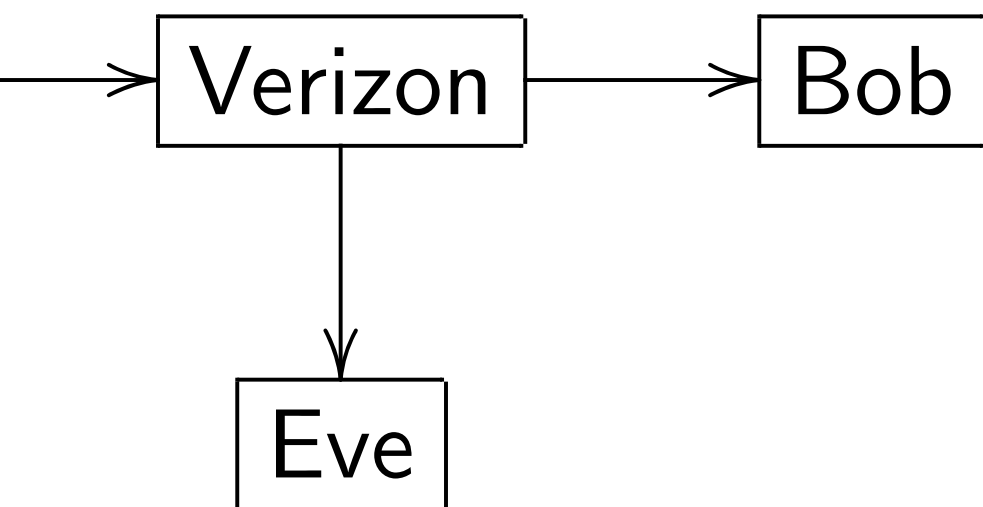
“Precision Market Insights, Verizon’s data marketing arm ... will now **sell its tool to advertisers for mobile ad campaigns that target Verizon’s massive subscriber base** based on demographics, interests and geography.”

the mission:

ing information

point A to point B,

to points C, D, E, ...



u hear me now? Good.”

ey hear you now? Good.”

ver stop working for you.”

he air.”

ettle.”

he 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

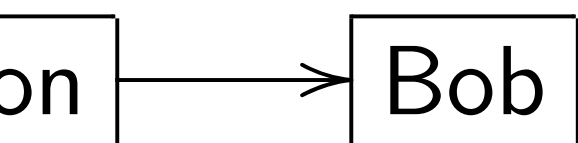
geography.”

Many of

rely on y

to send

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



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

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.

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.

“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.**”

the goal: Make money.

pays AT&T, Verizon and

several hundred million

year for access to 81%

international phone calls

US.”

on Market Insights,

its data marketing arm . . .

sell its tool to advertisers

to run ad campaigns

to target Verizon’s massive

customer base based on

demographics, interests and

location.”

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 y

You give

We redi

We moc



ake money.

, Verizon and  
dred million

access to 81%  
phone calls

Insights,  
marketing arm ...  
ol to advertisers  
paings  
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 network**  
You **give us** your  
We **redirect it** to  
We **modify it to**

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.”

of our competitors  
**your browser**  
data to Eve.

has discovered that the  
majority of health sites, from  
for-profit WebMD.com to the  
government-run CDC.gov, are  
filled with tracking elements  
that are sending records of your  
inquiries to the likes of web  
sites like Google, Facebook, and  
Twitter, 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.”

“Verizon  
marketing  
Experian  
and Ora  
anonymo  
the Prec  
third-par

competitors

user

ive.

ered that the

health sites, from

MD.com to the

DC.gov, are

ng elements

records 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 Blue**

**anonymous match**

**the Precision ID id**

**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.



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.**

**Give us your data.**

**Direct it to Eve.**

**Identify it to help Eve.**

Effort to better serve

users, Verizon Wireless has

recently modifying its users'

traffic on its network to

include a cookie-like tracker. This

is included in an HTTP

header called X-UIDH, is sent

to an 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.”

“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 use 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.”

“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.**”

has partnerships with  
ing data providers like  
Marketing Services  
le's BlueKai to enable  
ous matches between  
ision ID identifier and  
erty data. Although there's  
histic linkage back to the  
D, Verizon's data partners  
able to collect or save the  
files." ... "Rather than  
sal ID, I think there will  
y be really rich algorithms  
tie multiple IDs together  
ationalized 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



Partnerships with providers like Google Services and Facebook to enable connections between identifiers and user profiles. Although there's a push back to the companies' data partners collect or save the information.

“Rather than think there will be rich algorithms that combine IDs together for a targeted advertising 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**

## 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.

## 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

trillion-dollar data

ge industry—companies

ect, analyze, sell or share

details about consumers

marketing 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.”

Technical

Increasing

**Crypto.**

probe into  
ollar data  
—companies  
ze, sell or share  
out consumers  
poses—is

ssive data-  
aching influence  
o get a  
ard, 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.**

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**  
**s first-party subscriber**  
t rather deploying  
hips with third-party  
viders to target Verizon's  
consumer base."  
I never sacrifice our core  
and our **commitment**  
**cy** because there's an  
al dollar to be made  
ping 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 case  
No crypt

**out** privacy.

**ct** privacy.

not using or

ty subscriber

employing

third-party

target Verizon's

base."

sacrifice 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**

## 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  
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.

More tro

authenti

But we s

adequate

n?

n for us:

breaks network

content distribution

services"; creates

"latency";

of network

direct customers

; breaks

(content identifier)

data collection

breaks "value-add

based on access

load content

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 troublesome

authenticated encr

But we still see m

adequate for most

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.

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

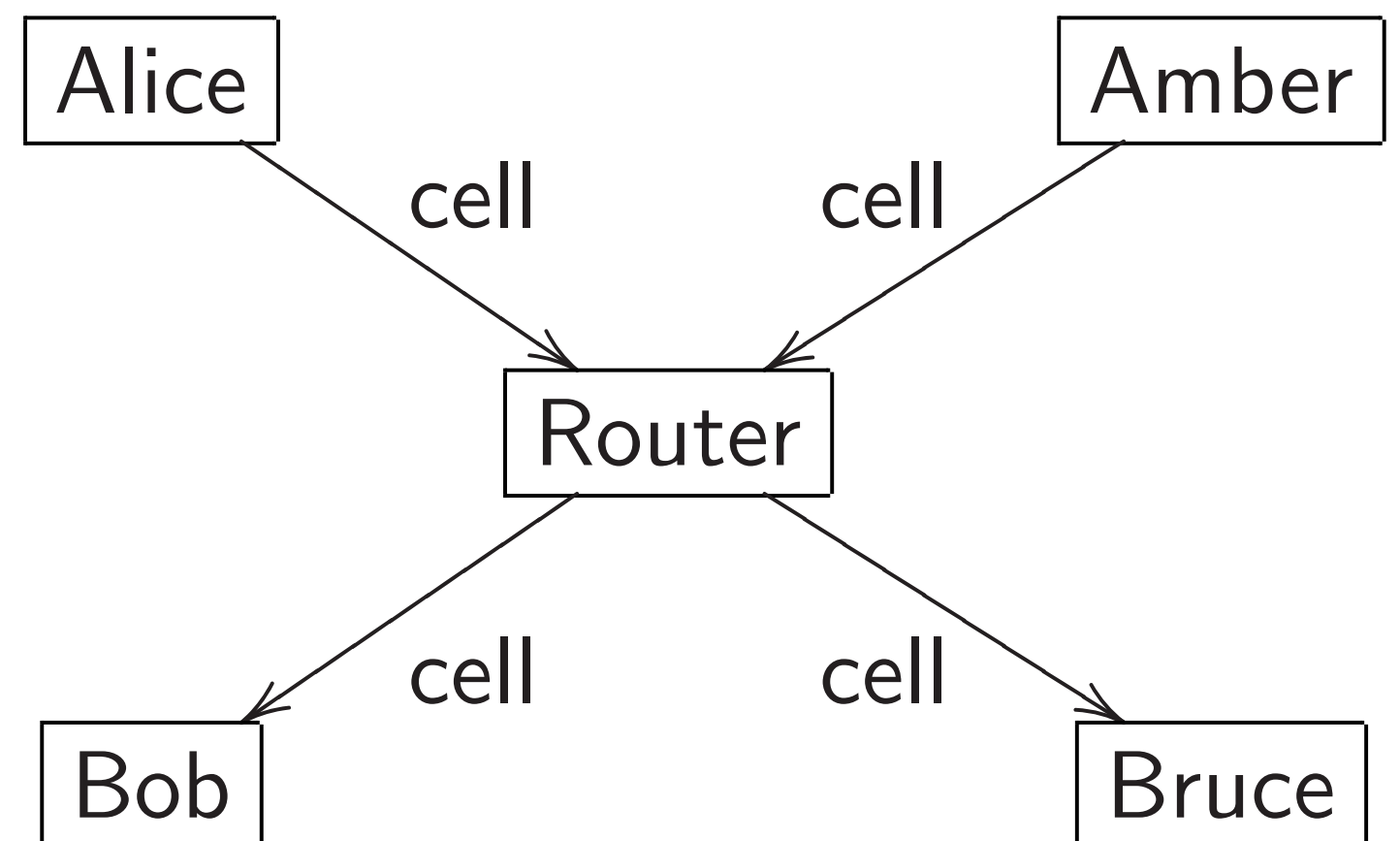
can track in many other ways.

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:



is good for us:

to. [Lobby for this!](#)

is good for us:

["Authenticated encryption"](#)

authentication.

"passive eavesdropping"

**aren't passive.**

is good for us:

[relies on some data.](#)

still see everything.

to censor quite selectively.

to modify signed data but

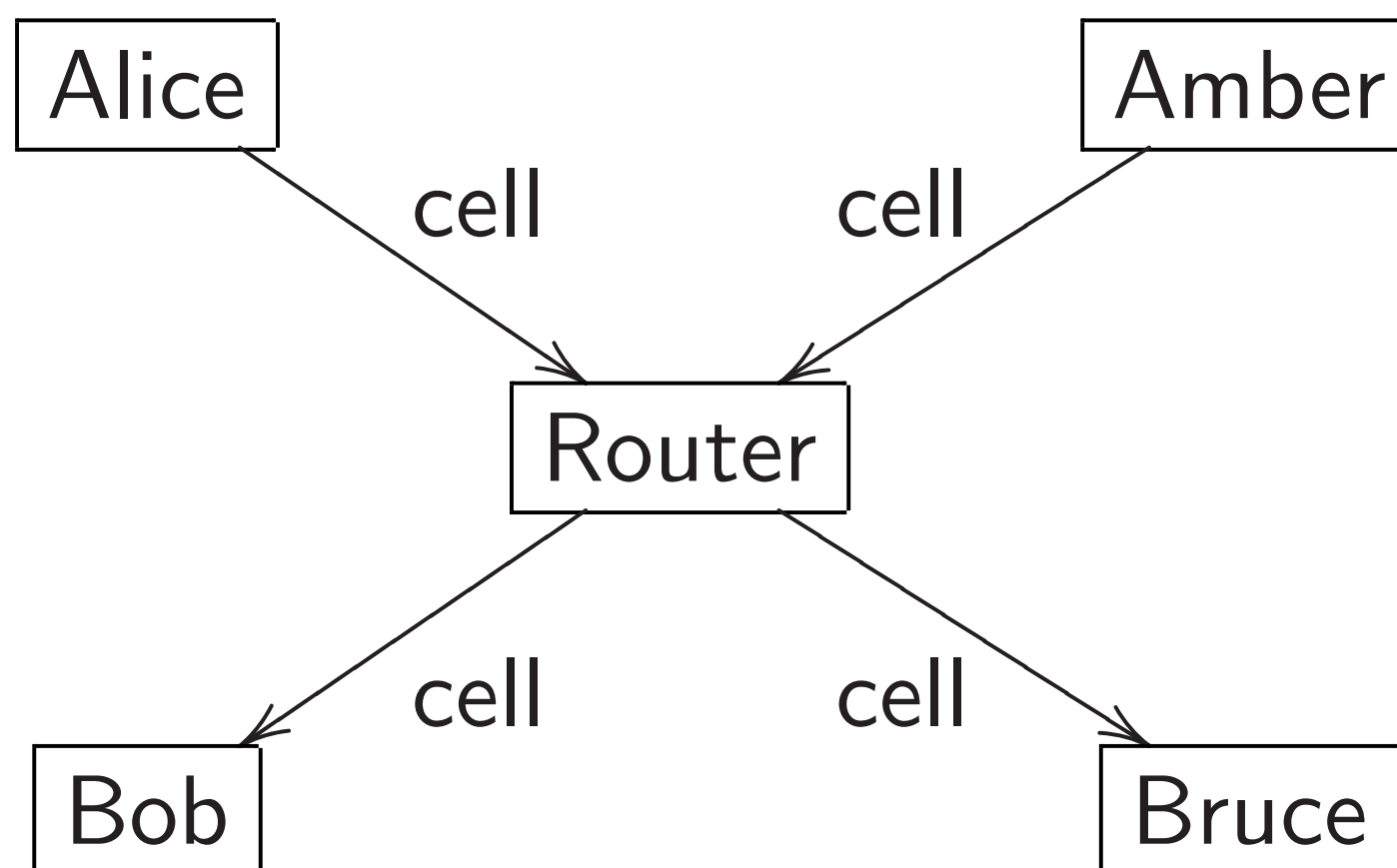
to work in many other ways.

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:

“encryption”

ation.

vesdropping”

ssive.

or us:

the data.

everything.

quite selectively.

ed data but

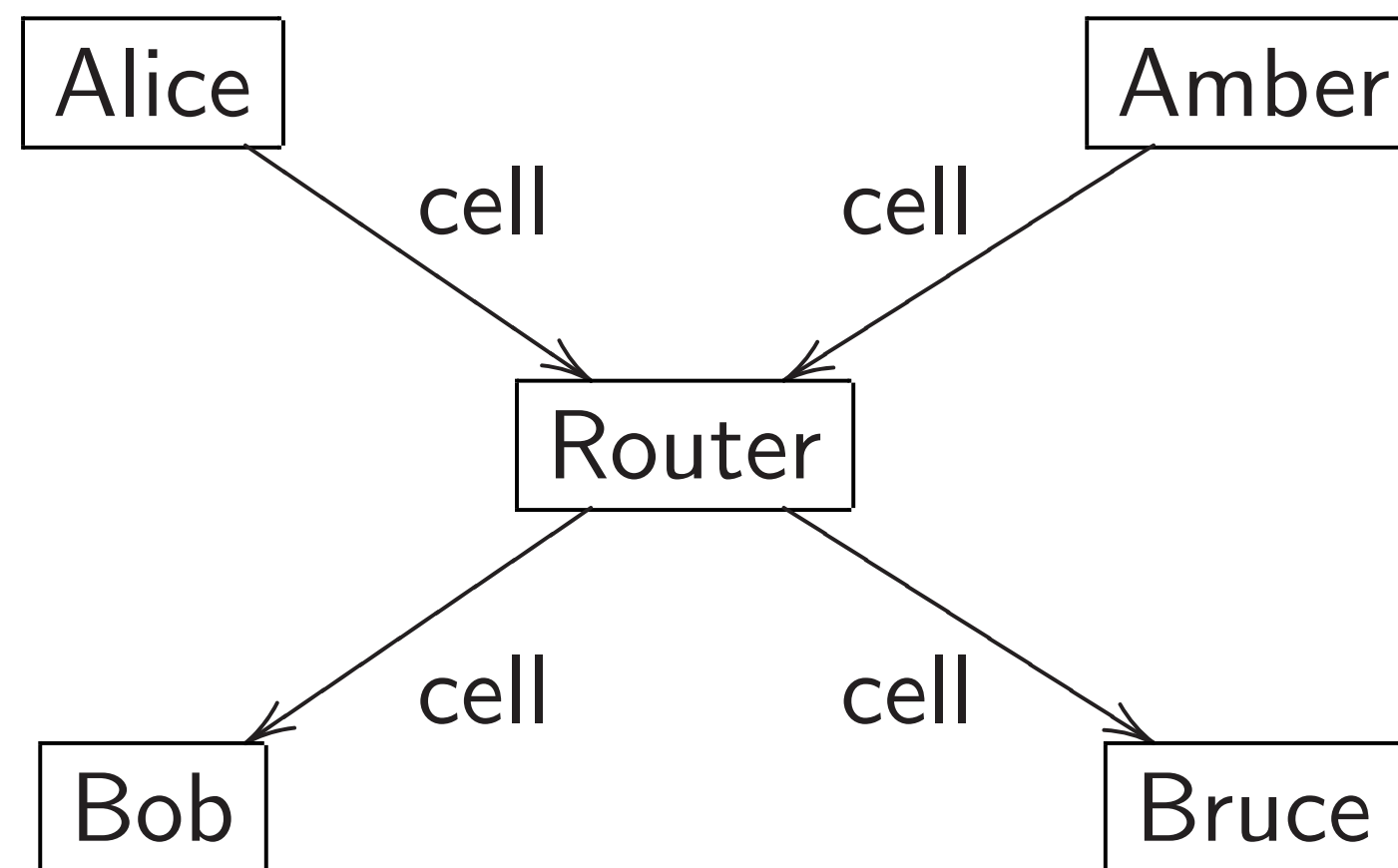
other ways.

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:



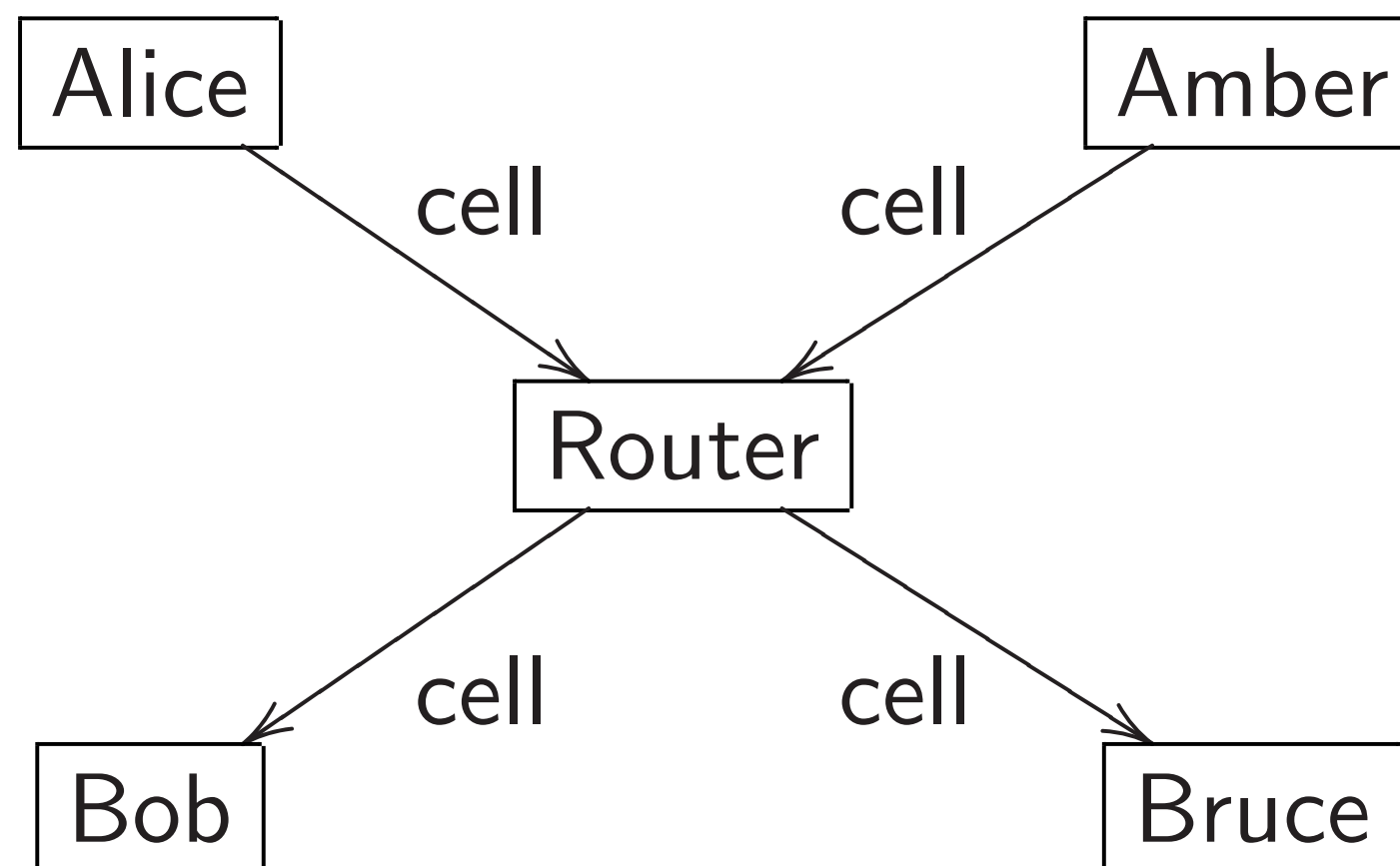
Can we [ban crypto](#)

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:



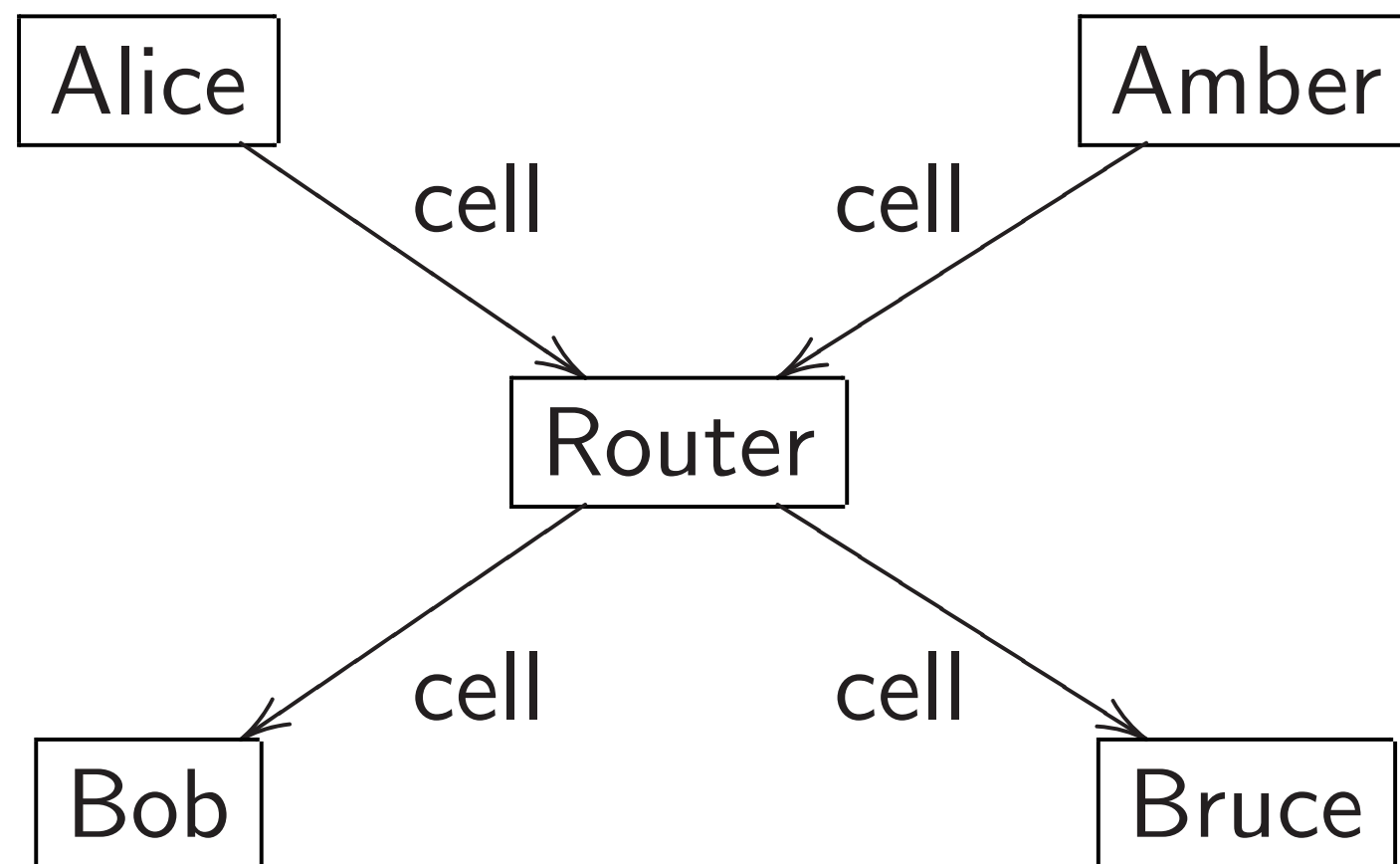
Can we [ban crypto](#)?

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:



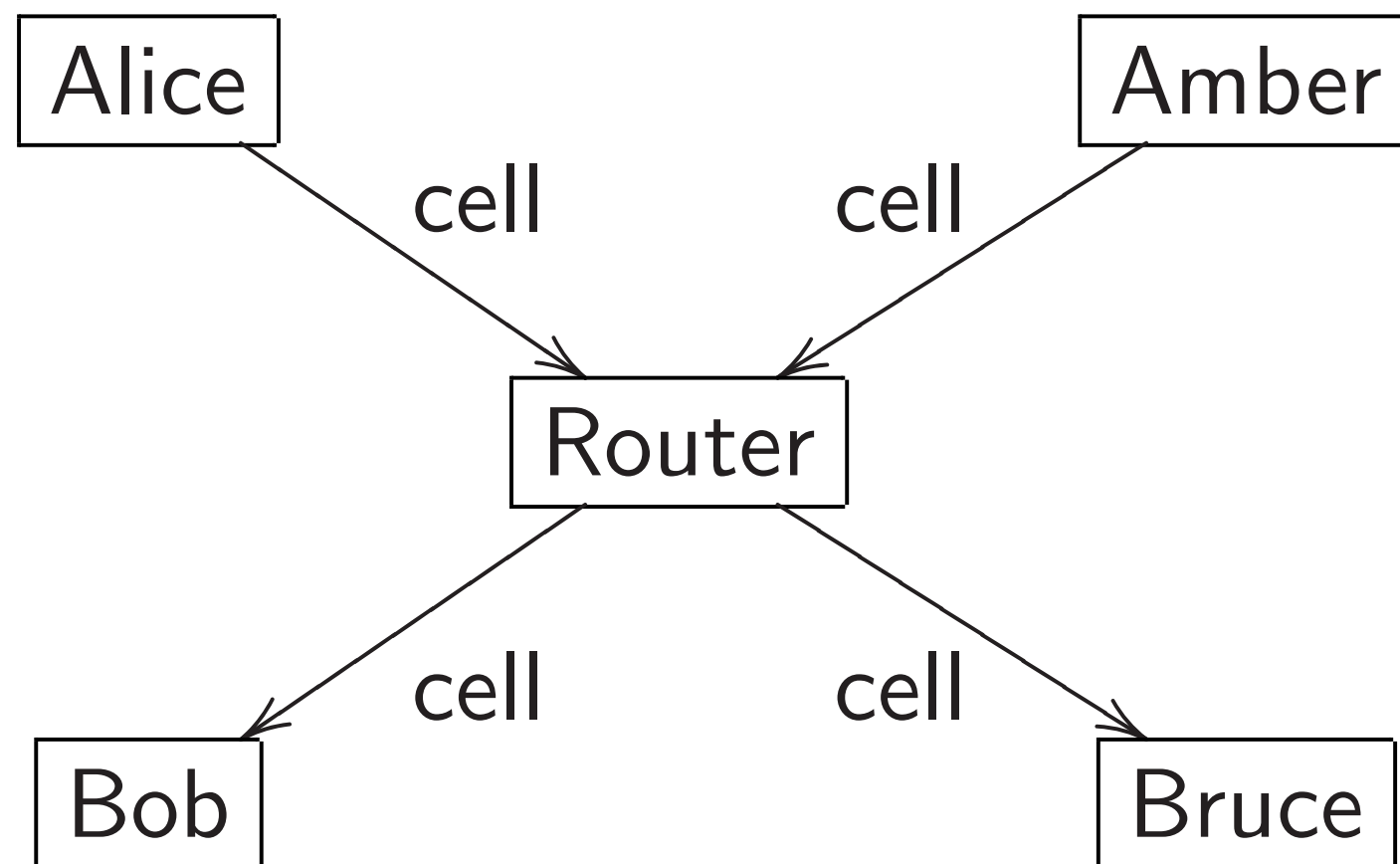
Can we [ban crypto](#)?

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:



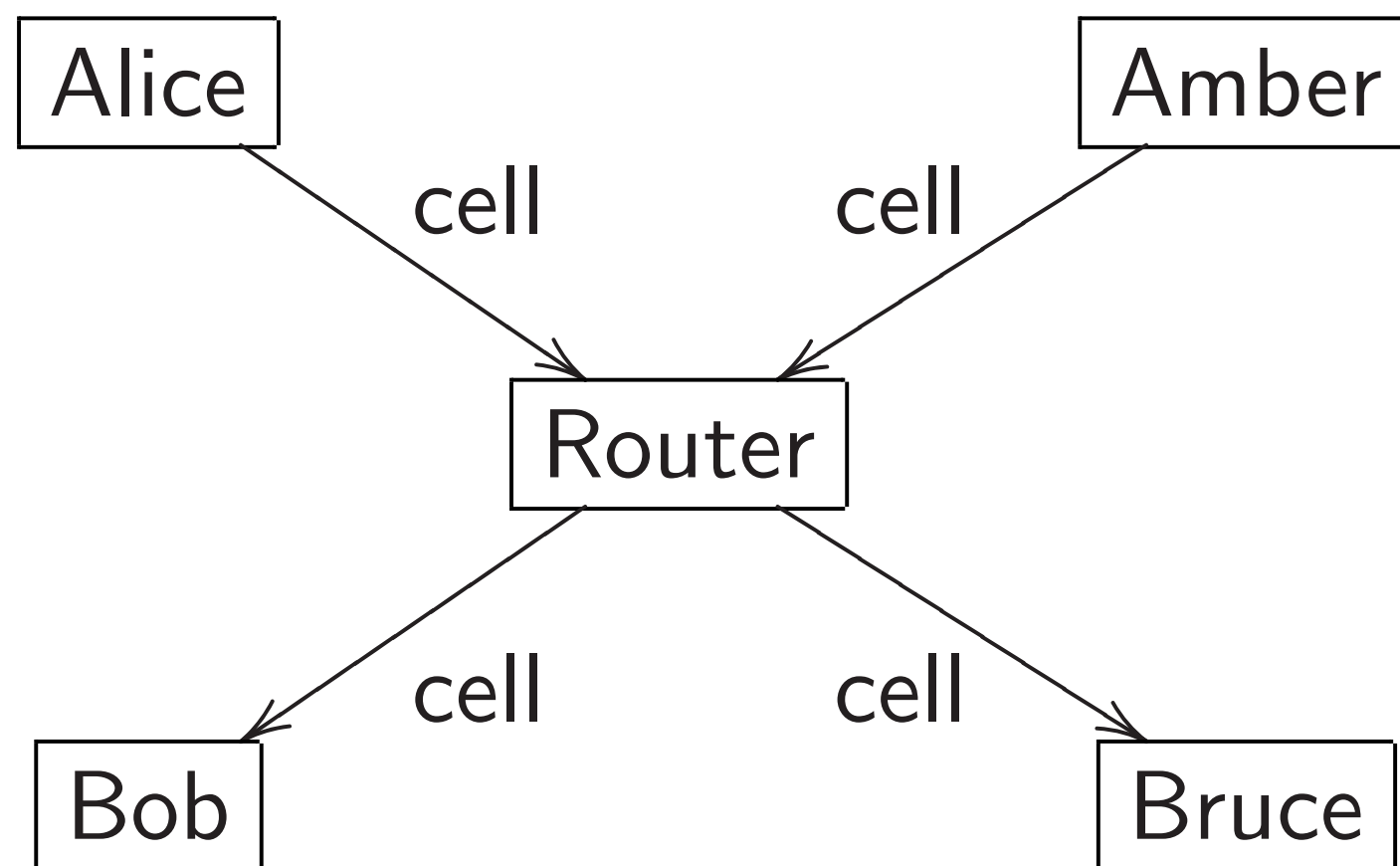
Can we [ban crypto](#)? If not, can we divert effort into opportunistic encryption, or into pure authentication?

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?

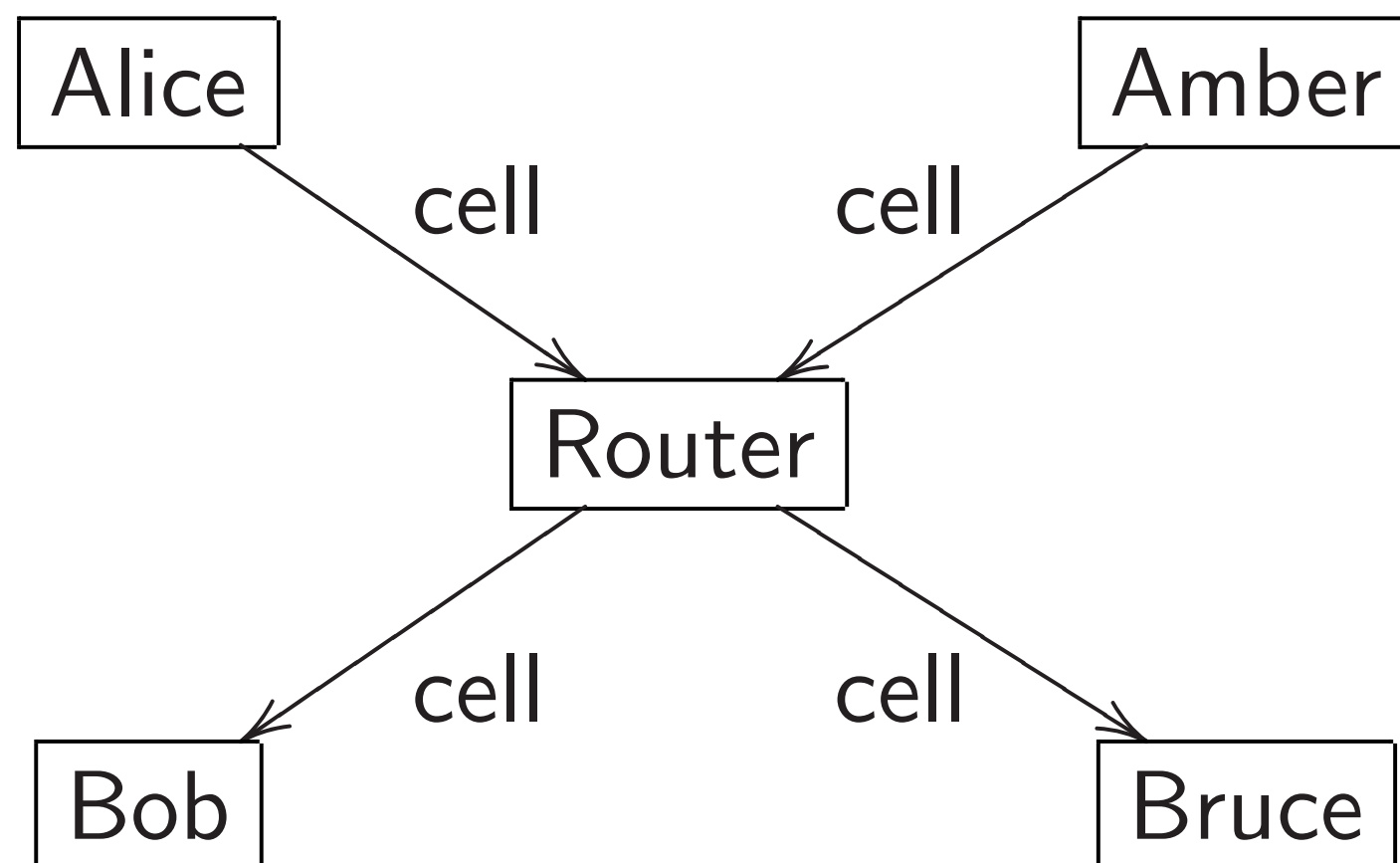
Can we promote standards that expose most data, or that **trust our proxies**?

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.

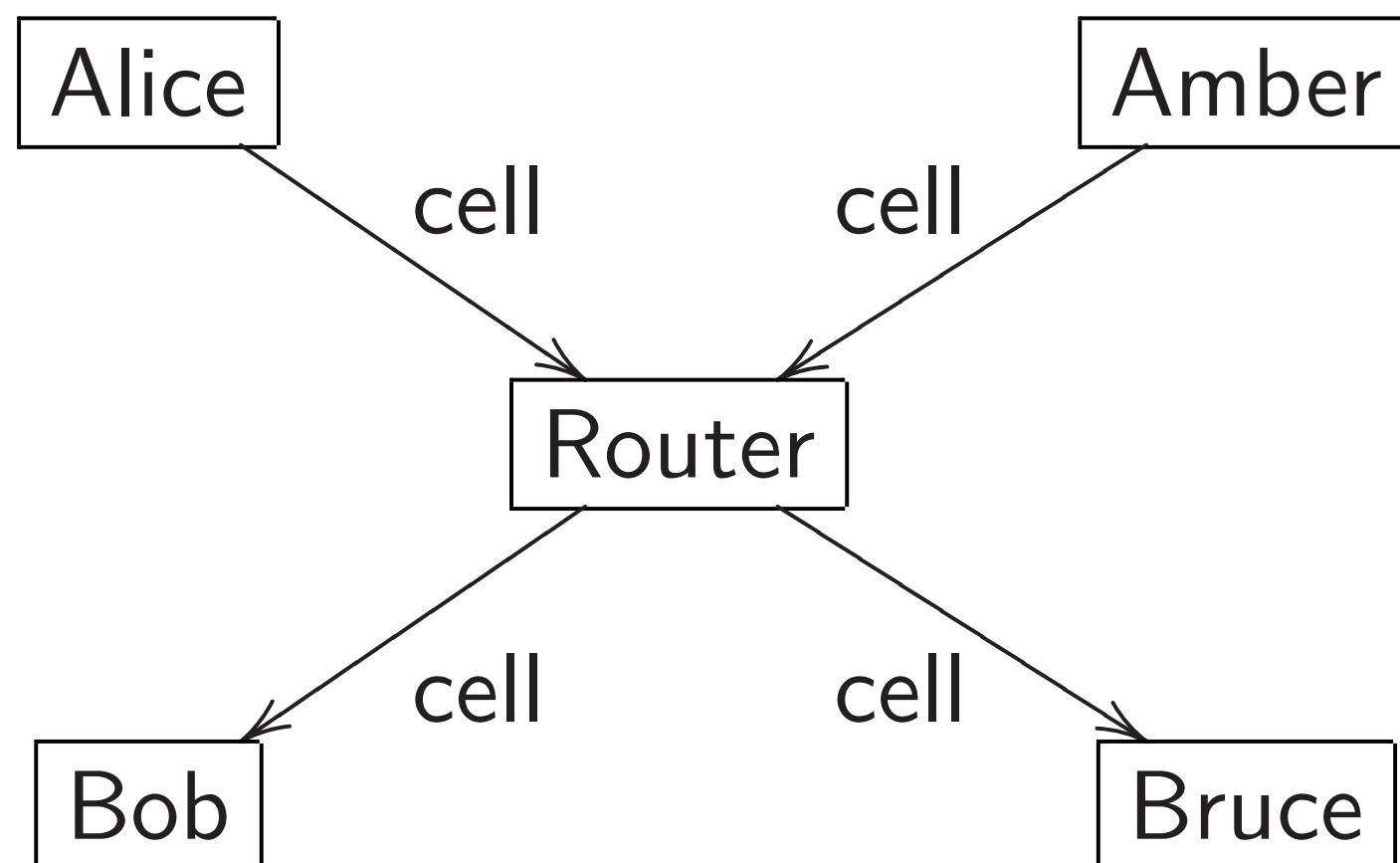
**Can we promote weak crypto?**

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**?

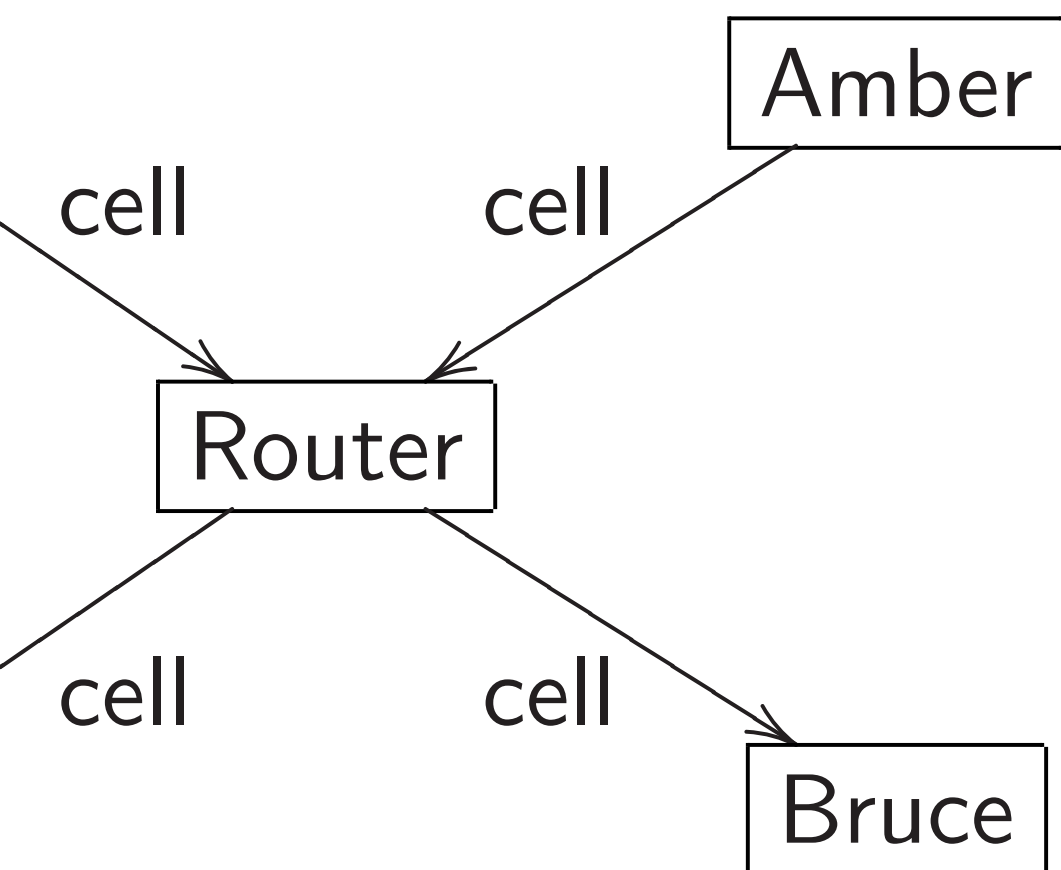
Very often crypto protocols and implementations have weaknesses.

**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?**

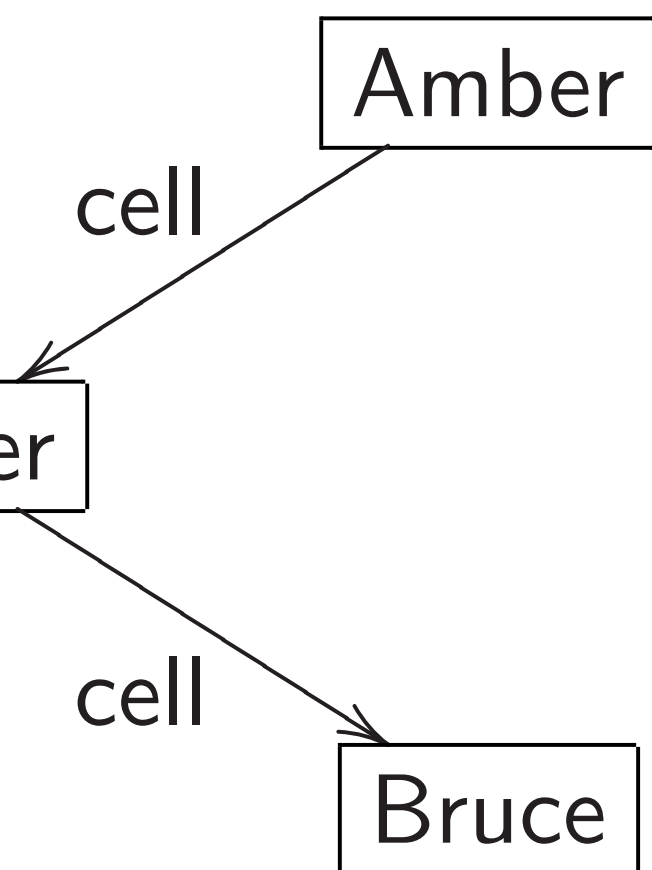
We've started working with  
experts in crypto sabotage.

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.

oling

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: “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.**”

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  
stochastic encryption,  
secure authentication?

promote standards  
lose most data, or  
**test our proxies?**

even crypto protocols and  
implementations have weaknesses.

**promote weak crypto?**

started 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.

Sabotage

*How to  
manipulate  
a white*

Daniel J  
Tung Ch  
Chitchan

Andreas  
Tanja La

Ruben M  
Christine

[safecur](#)  
[/bada55](#)

o? If not,  
rt into  
yption,  
ntication?

standards  
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. Bernstein  
Tung Chou

Chitchanok Chuen

Andreas Hülsing

Tanja Lange

Ruben Niederhage

Christine van Vreoc

[safecurves.cr.y](http://safecurves.cr.y)

[/bada55.html](http://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*

Daniel J. Bernstein

Tung Chou

Chitchanok Chuengsatiansup

Andreas Hülsing

Tanja Lange

Ruben Niederhagen

Christine van Vredendaal

[safecurves.cr.yp.to/bada55.html](http://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](http://safecurves.cr.yp.to/bada55.html)

ize performance: “The  
of RC4 is its **exceptionally**  
**and extremely efficient**  
**random generator.**”

uzzle people: Dual EC is  
**y DRBG mechanism in**  
**ommendation whose**  
**is related to a hard**  
**in number theory.**”

rypto 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](http://safecurves.cr.yp.to)

[/bada55.html](http://bada55.html)

Textboo  
using sta  
on a sta



formance: “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

lications.

## 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

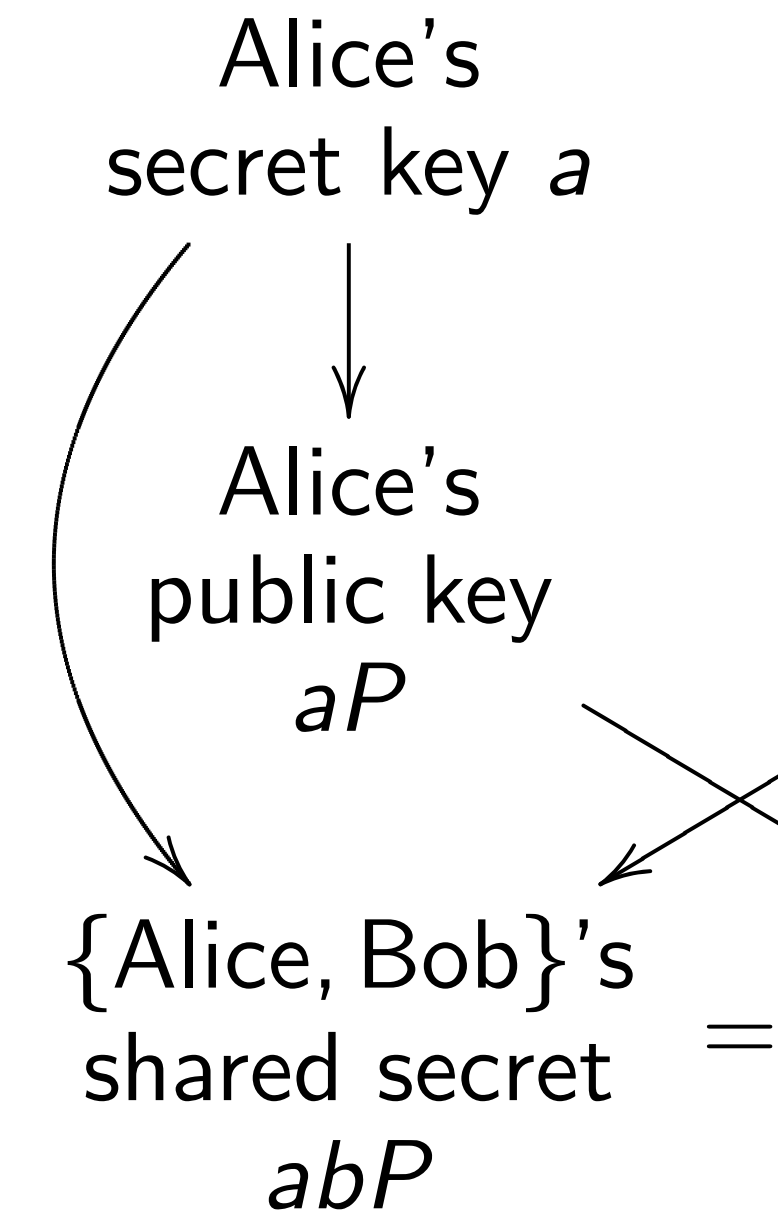
Ruben Niederhagen

Christine van Vredendaal

[safecurves.cr.yp.to](http://safecurves.cr.yp.to)

[/bada55.html](http://bada55.html)

Textbook key exchange  
using standard point  
on a standard elliptic



## 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

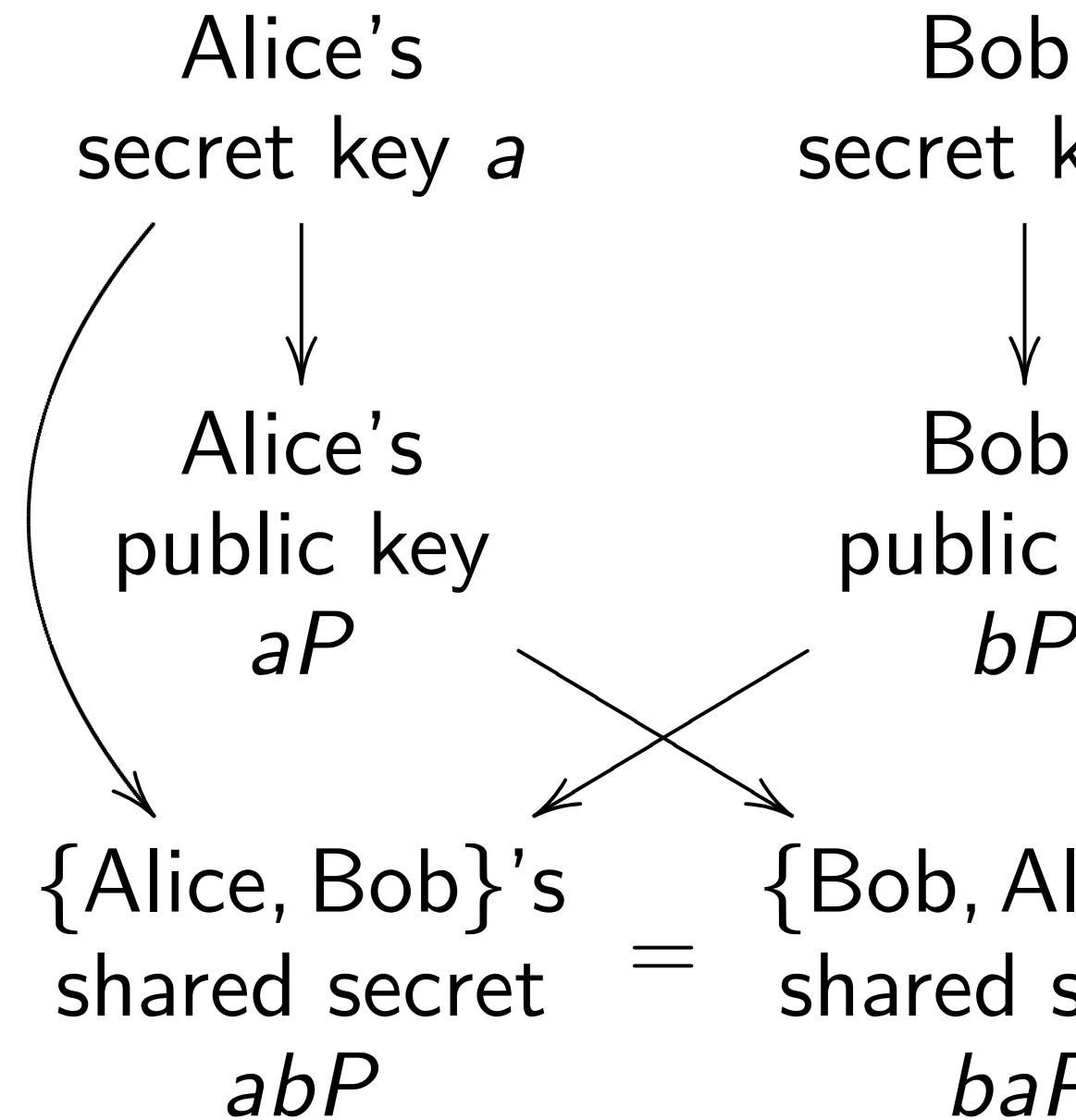
Ruben Niederhagen

Christine van Vredendaal

[safecurves.cr.yp.to](http://safecurves.cr.yp.to)

[/bada55.html](http://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

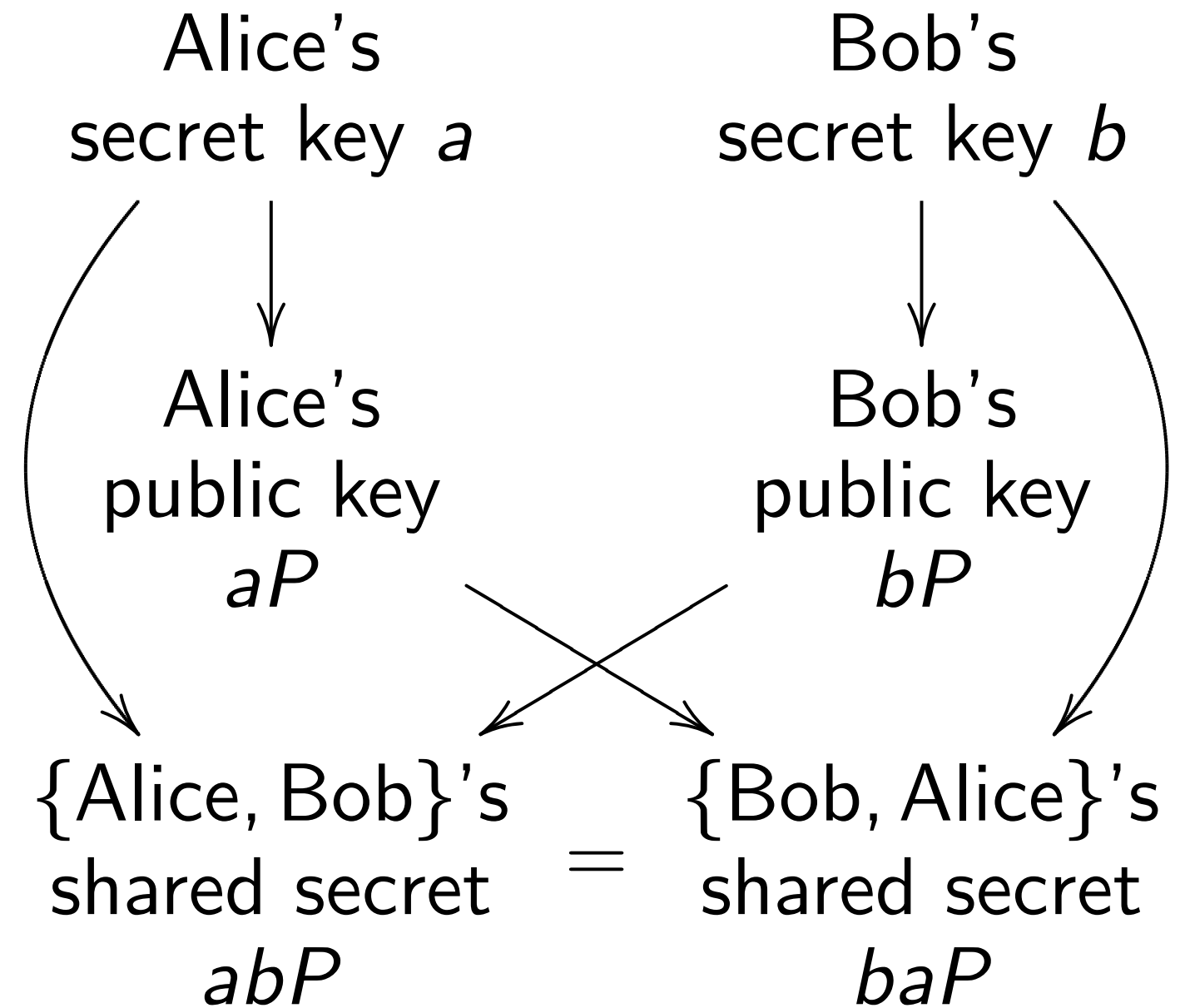
Ruben Niederhagen

Christine van Vredendaal

[safecurves.cr.yp.to](https://safecurves.cr.yp.to)

[/bada55.html](https://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

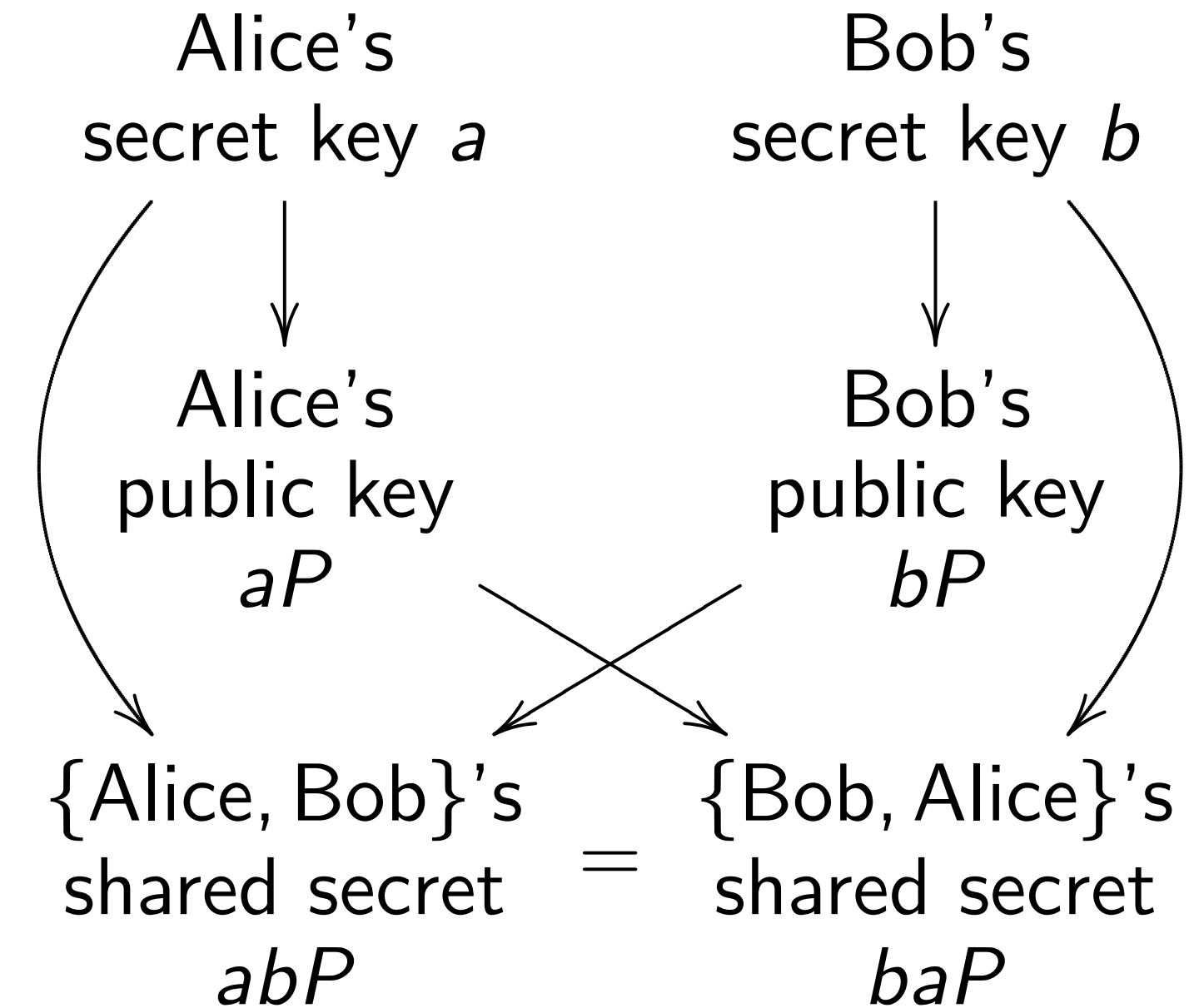
Ruben Niederhagen

Christine van Vredendaal

[safecurves.cr.yp.to](http://safecurves.cr.yp.to)

[/bada55.html](http://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

ou

ok Chuengsatiansup

Hülsing

ange

Niederhagen

e van Vredendaal

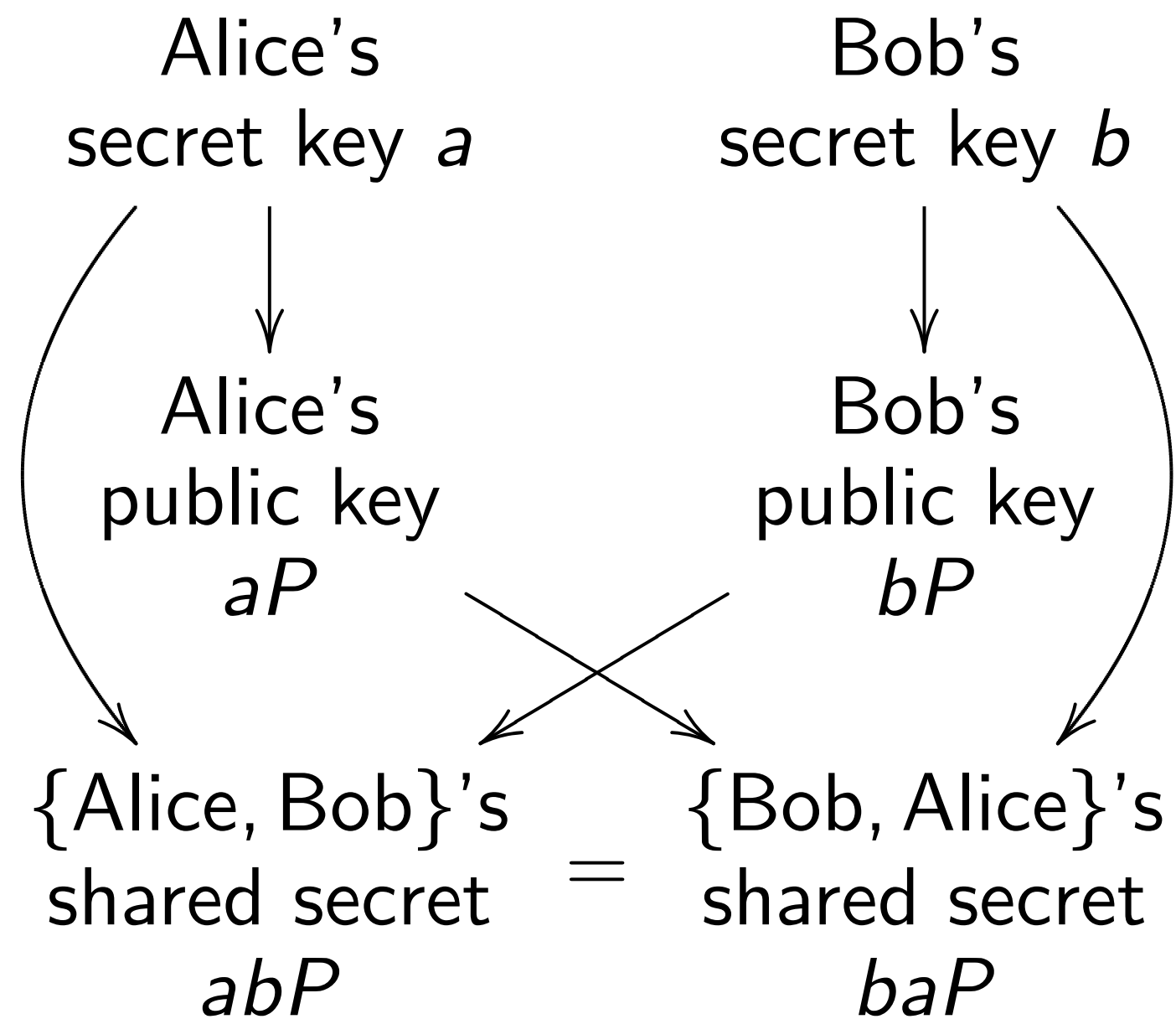
[cr.yp.to](https://cr.yp.to)

[5.html](#)

Textbook key exchange

using standard point  $P$

on a standard elliptic curve  $E$ :



Security depends on choice of  $E$ .



details

standards:

the black hat

n

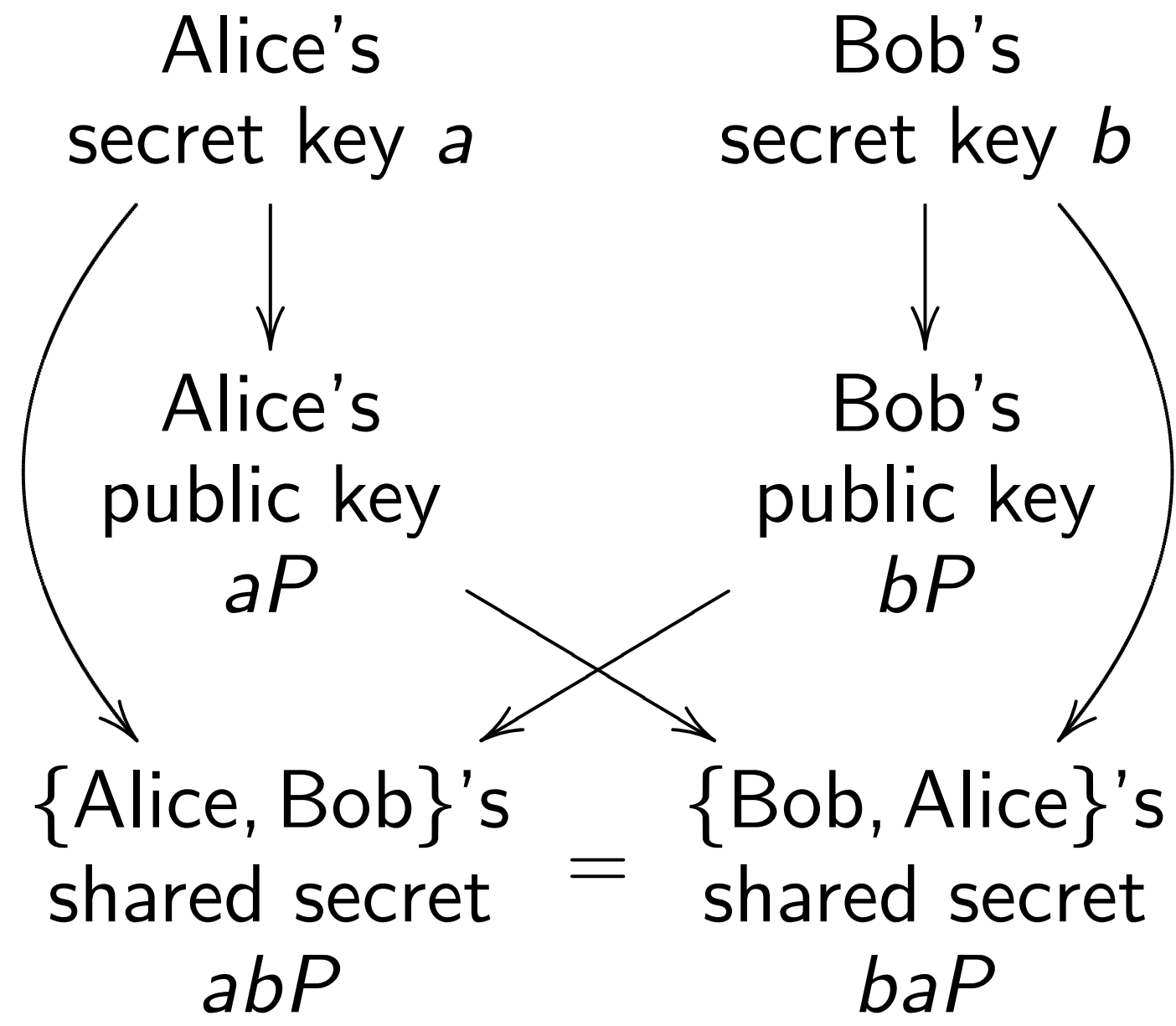
gsatiansup

n

lendaal

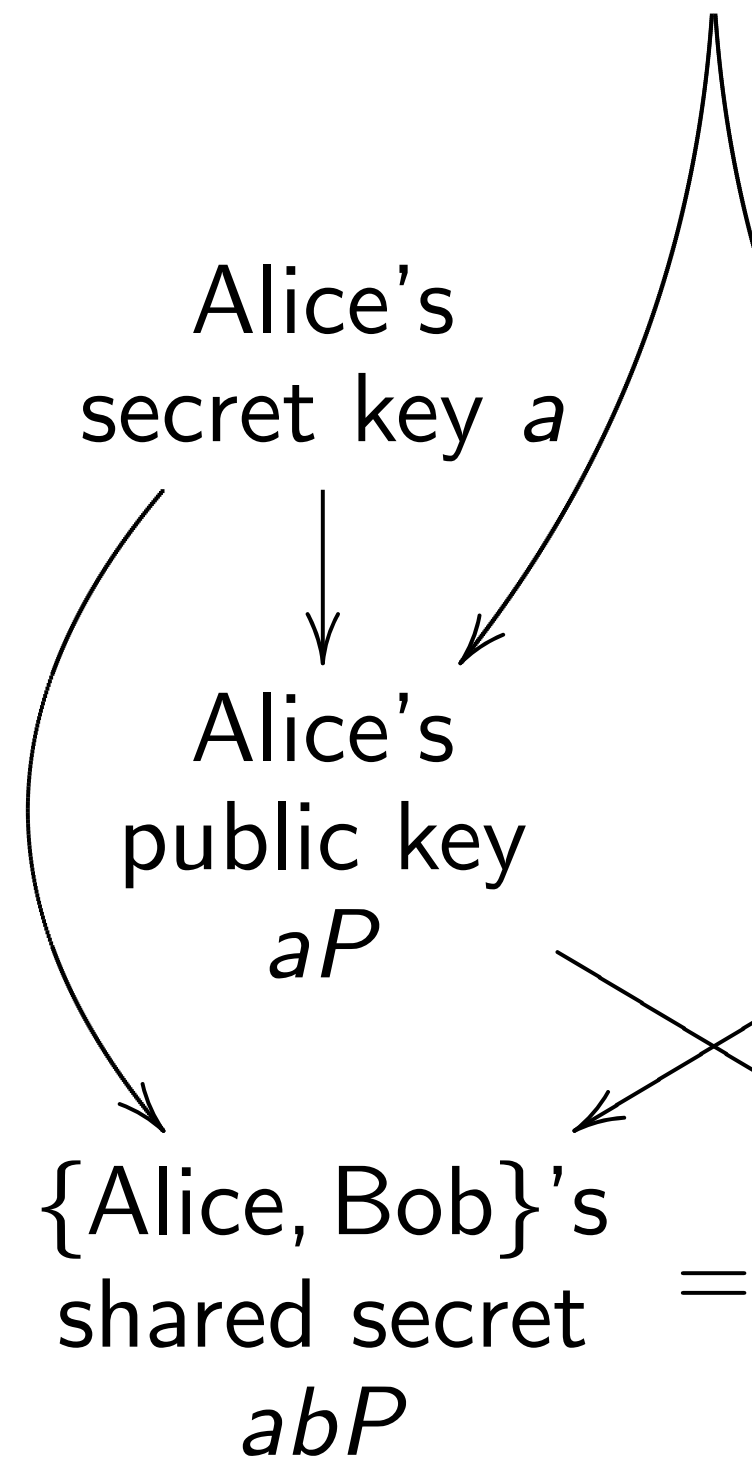
yp.to

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



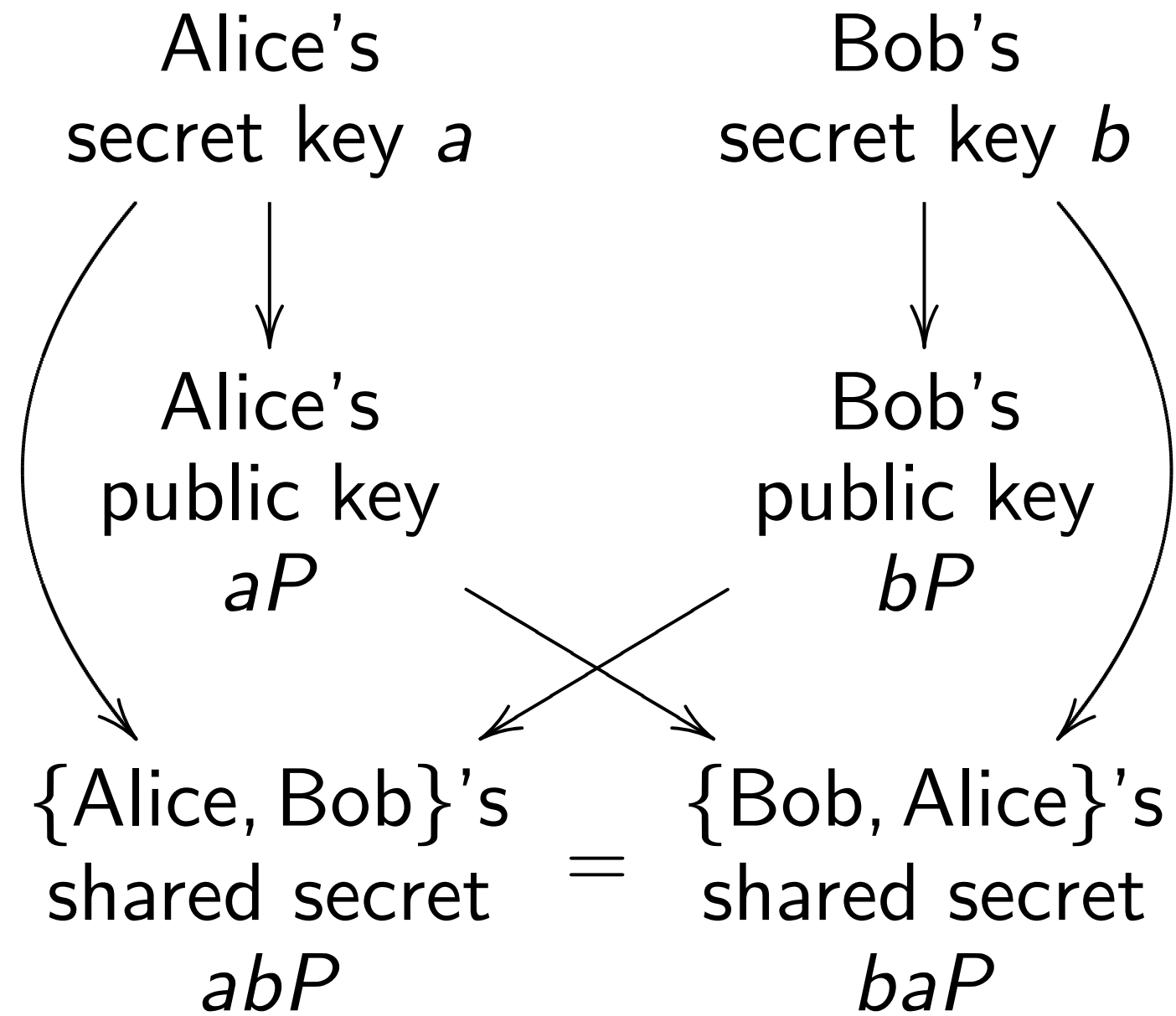
Security depends on choice of  $E$ .

Our partner  
choice of



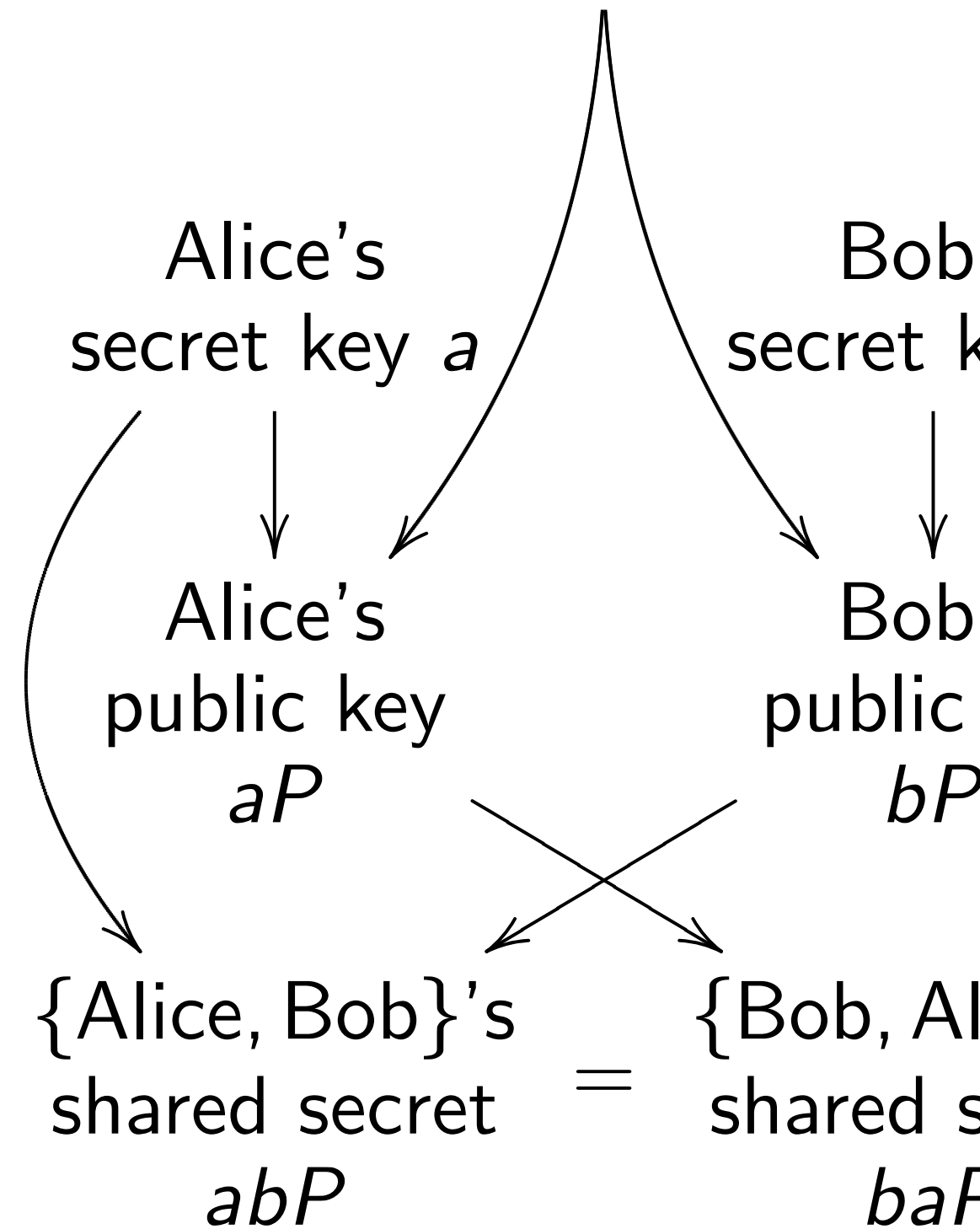


Textbook key exchange  
using standard point  $P$   
on a standard elliptic curve  $E$ :

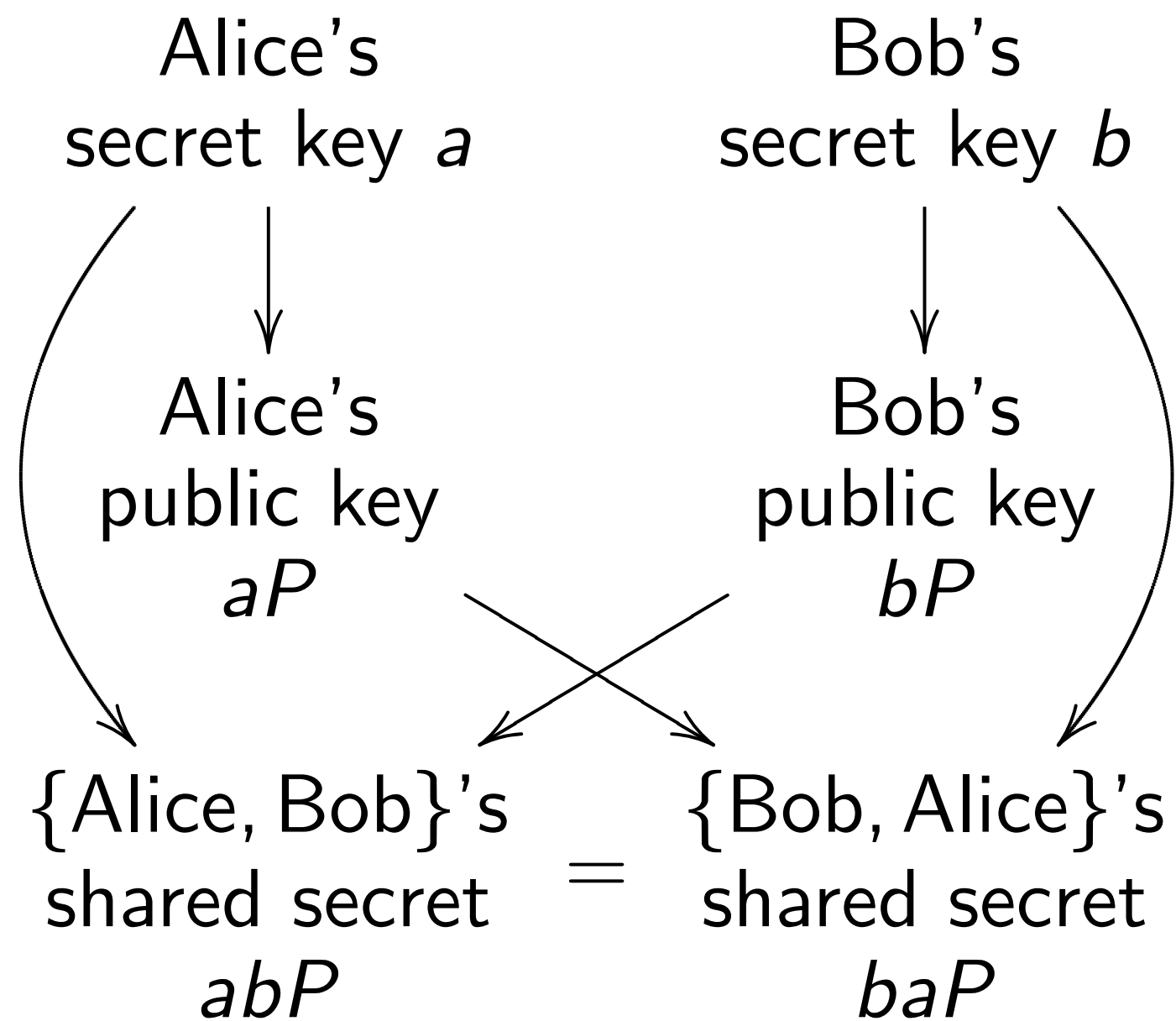


Security depends on choice of  $E$ .

Our partner Jerry's  
choice of  $E, P$

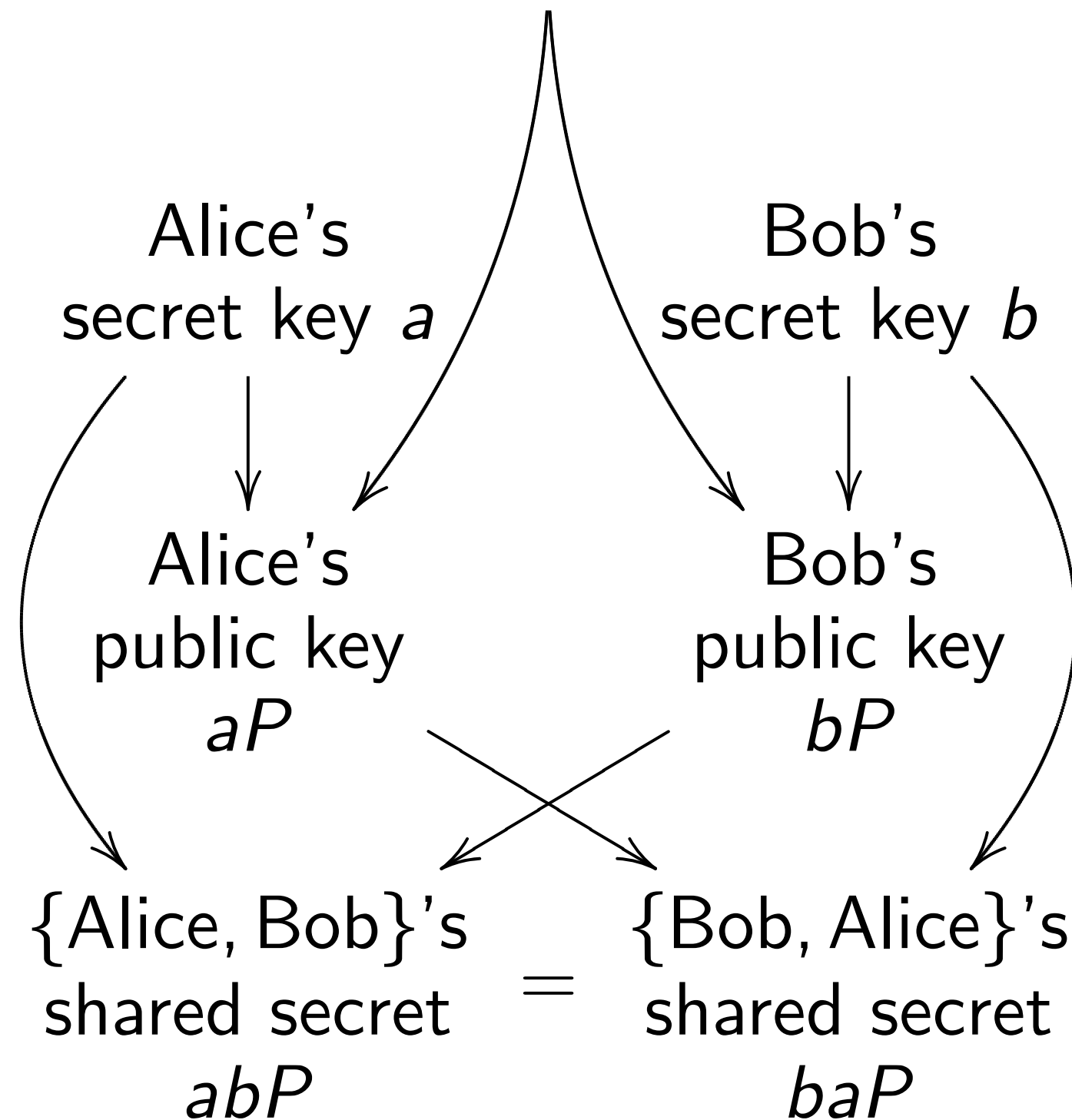


Textbook key exchange  
 using standard point  $P$   
 on a standard elliptic curve  $E$ :

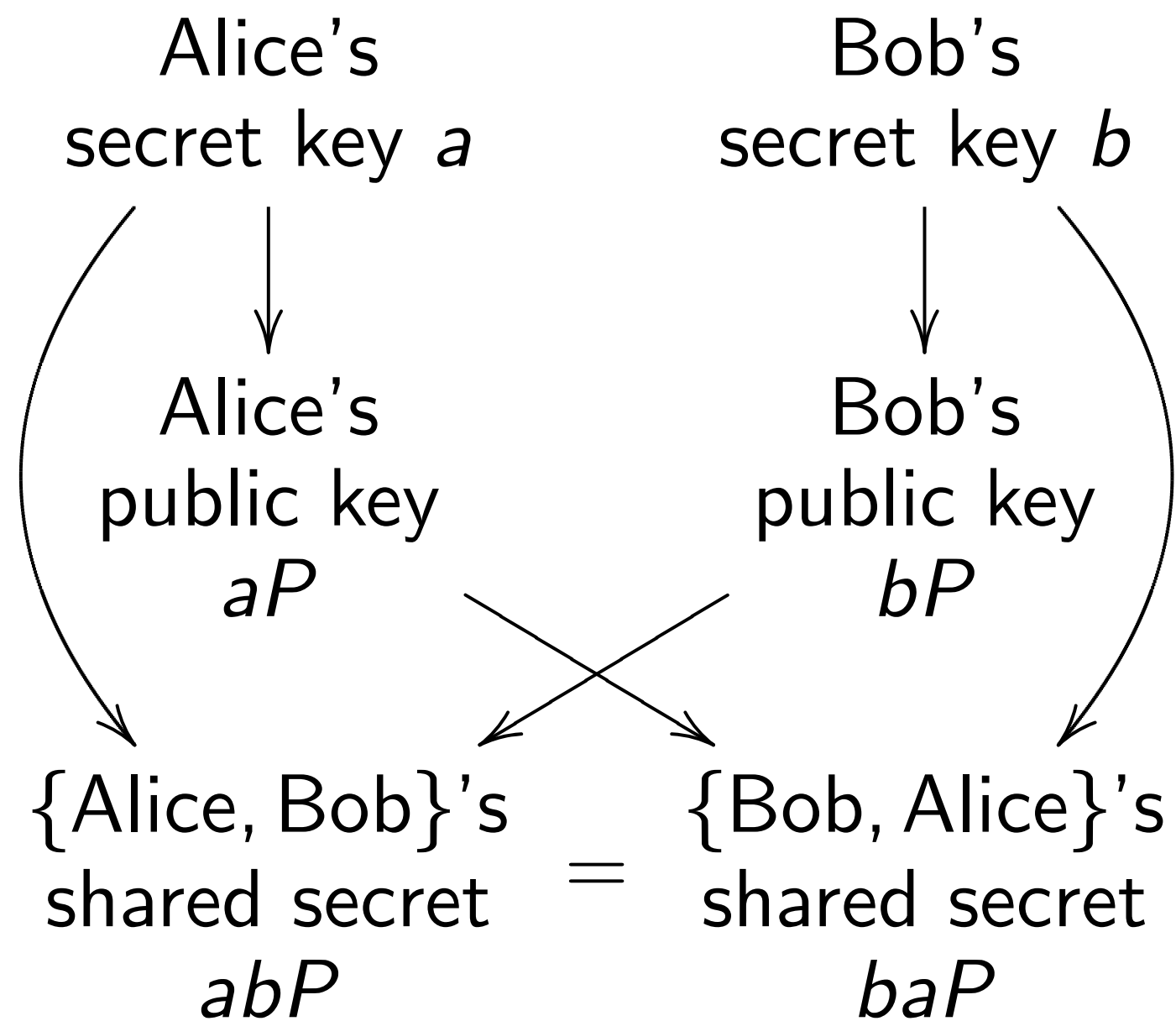


Security depends on choice of  $E$ .

Our partner Jerry's  
 choice of  $E, P$

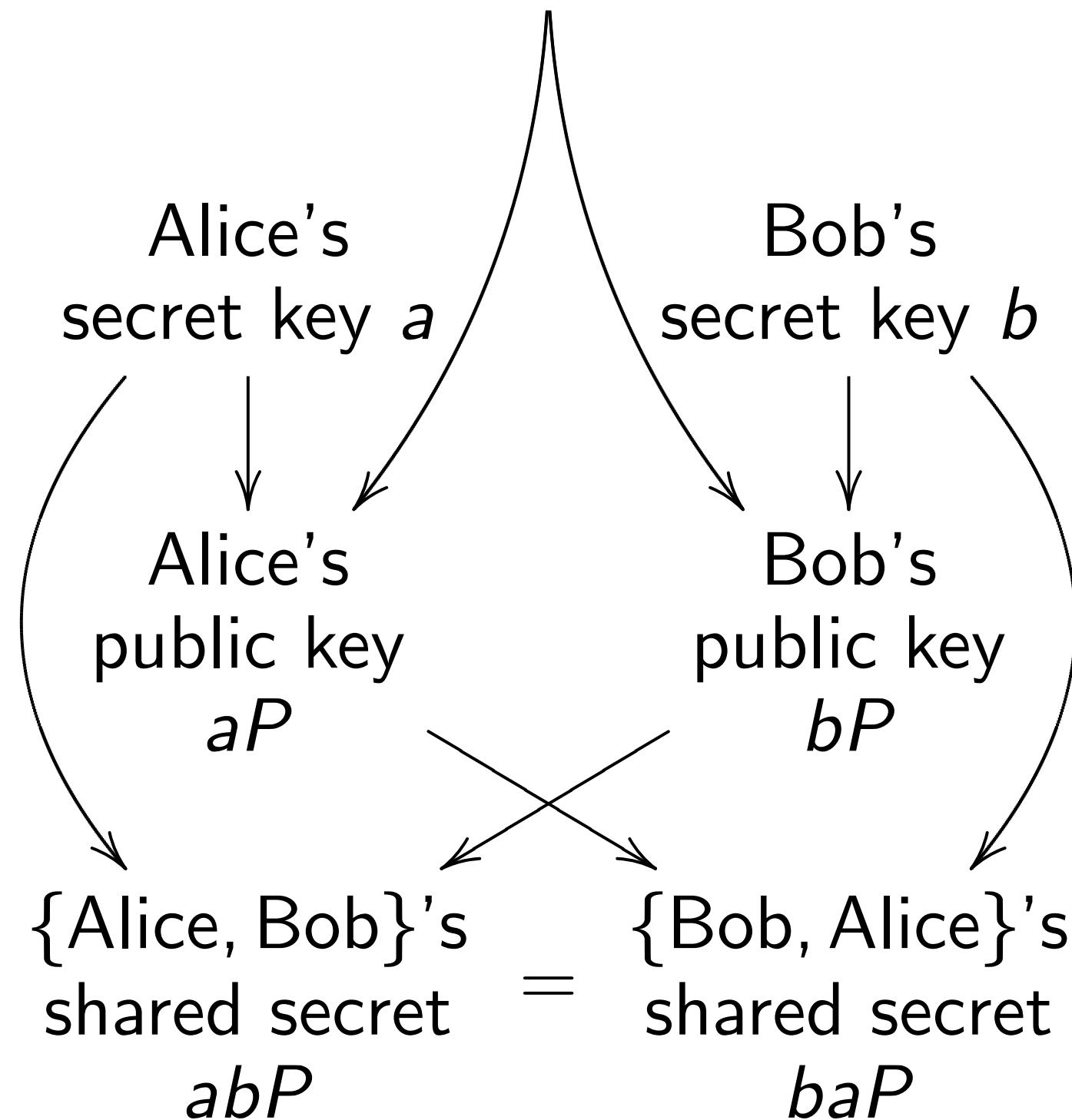


Textbook key exchange  
using standard point  $P$   
on a standard elliptic curve  $E$ :



Security depends on choice of  $E$ .

Our partner Jerry's  
choice of  $E, P$

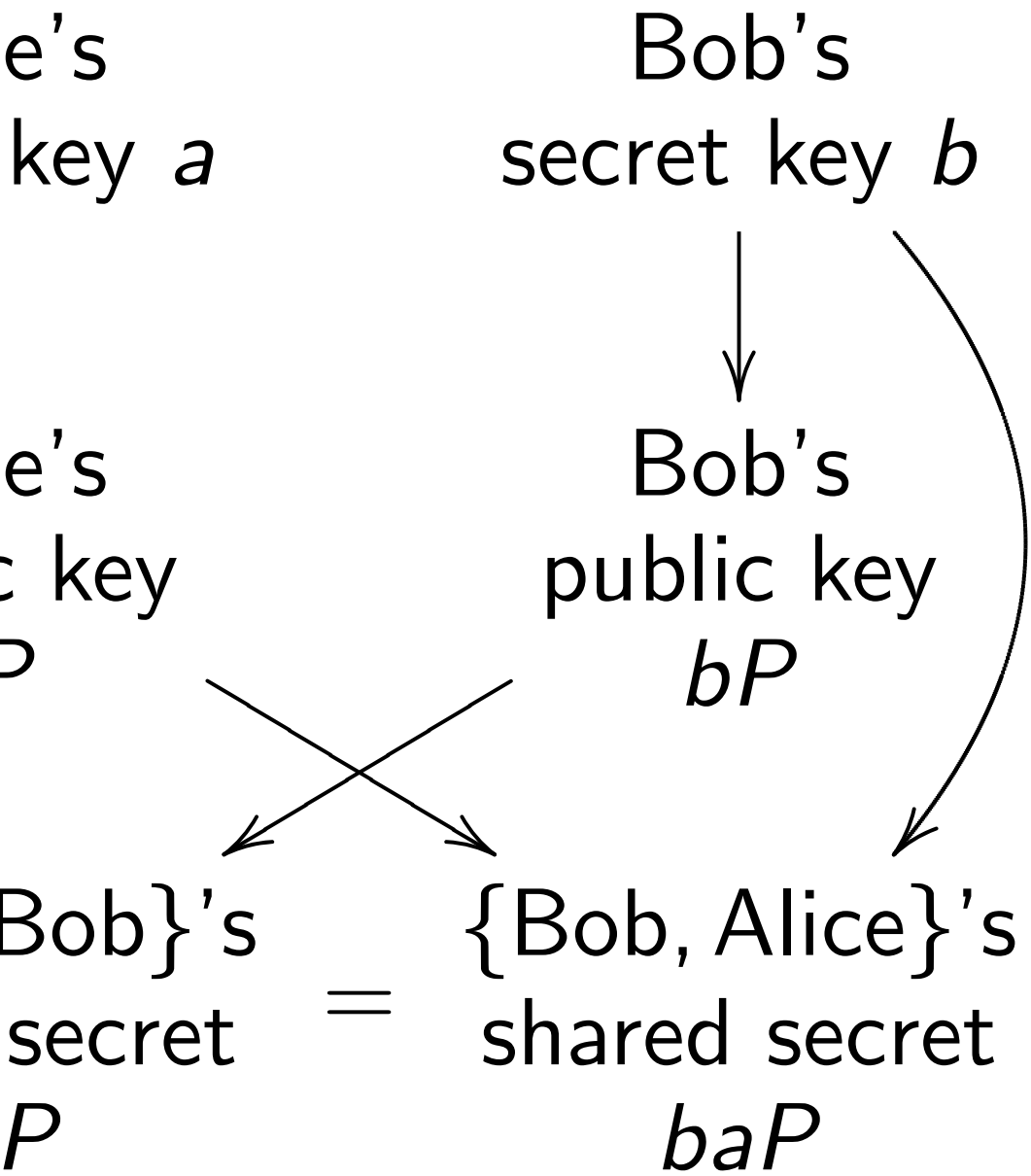


Can we exploit this picture?

key exchange

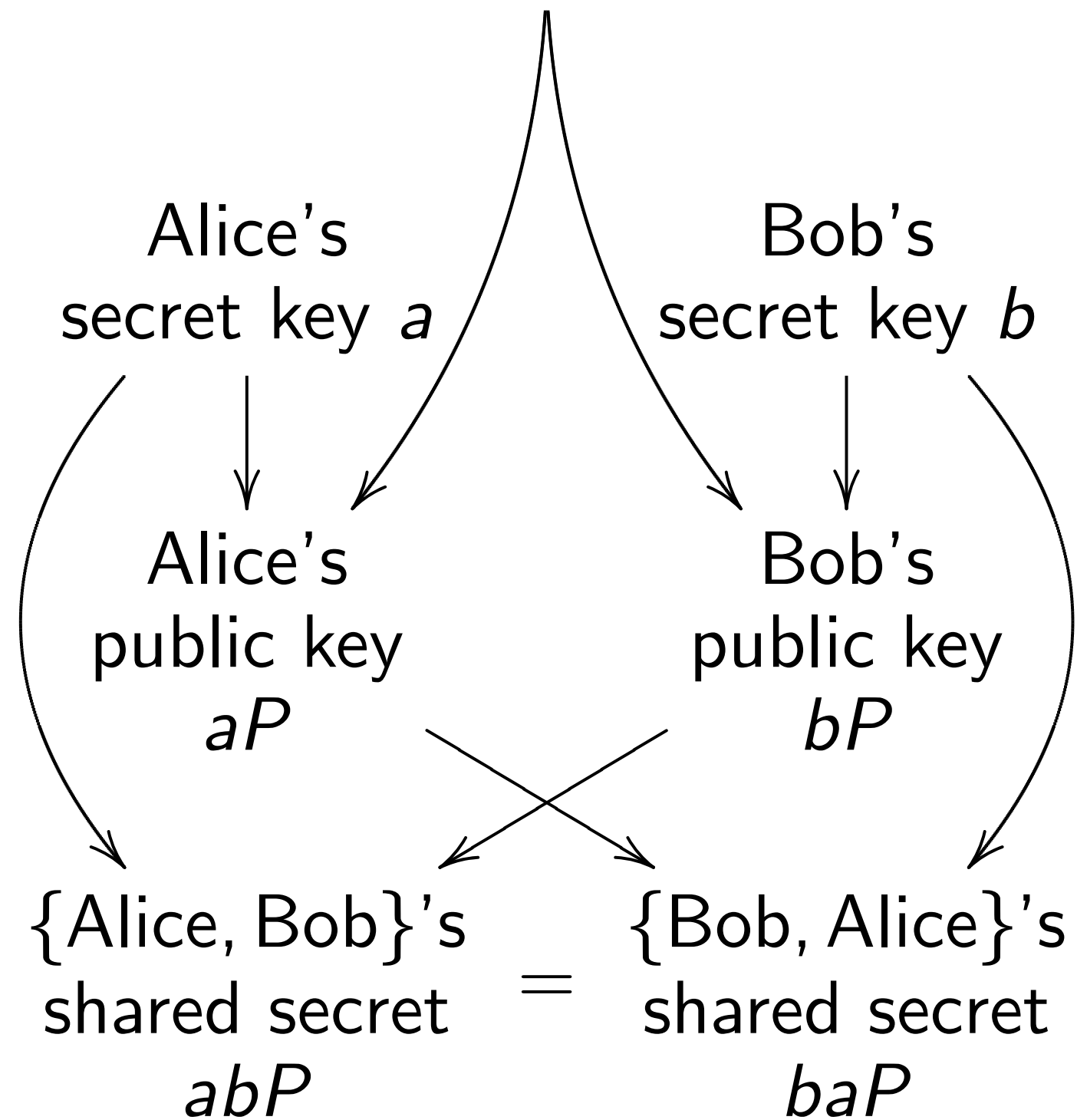
standard point  $P$

standard elliptic curve  $E$ :



depends on choice of  $E$ .

Our partner Jerry's choice of  $E, P$



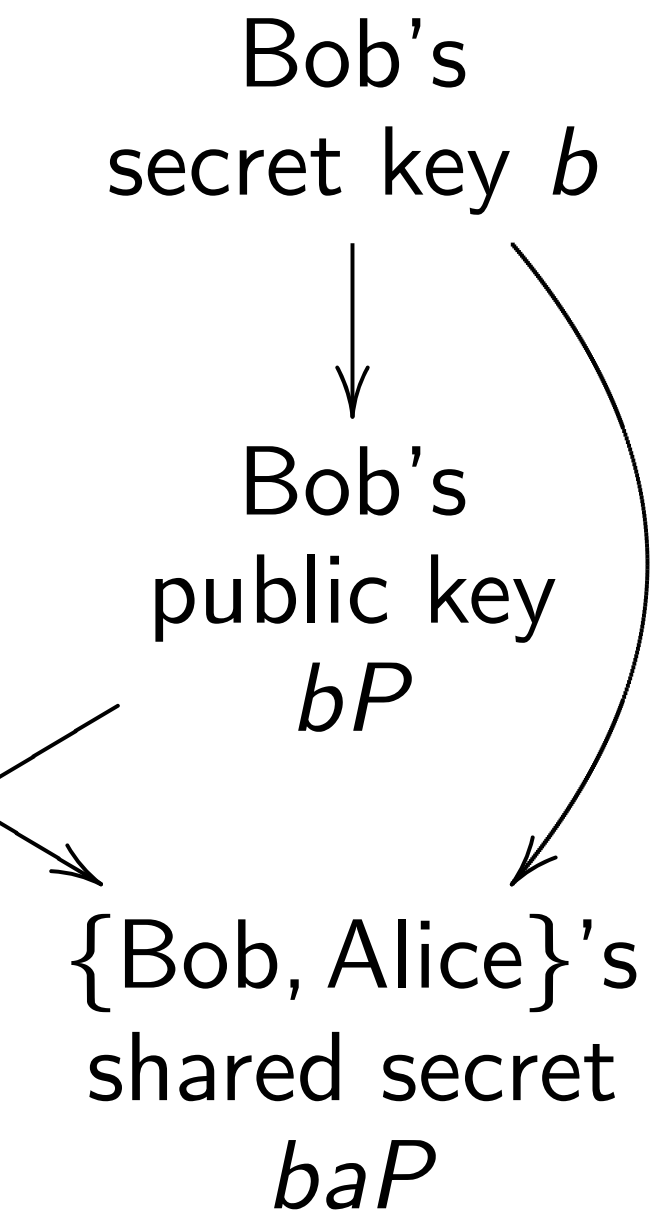
Can we exploit this picture?

Depends for accep

change

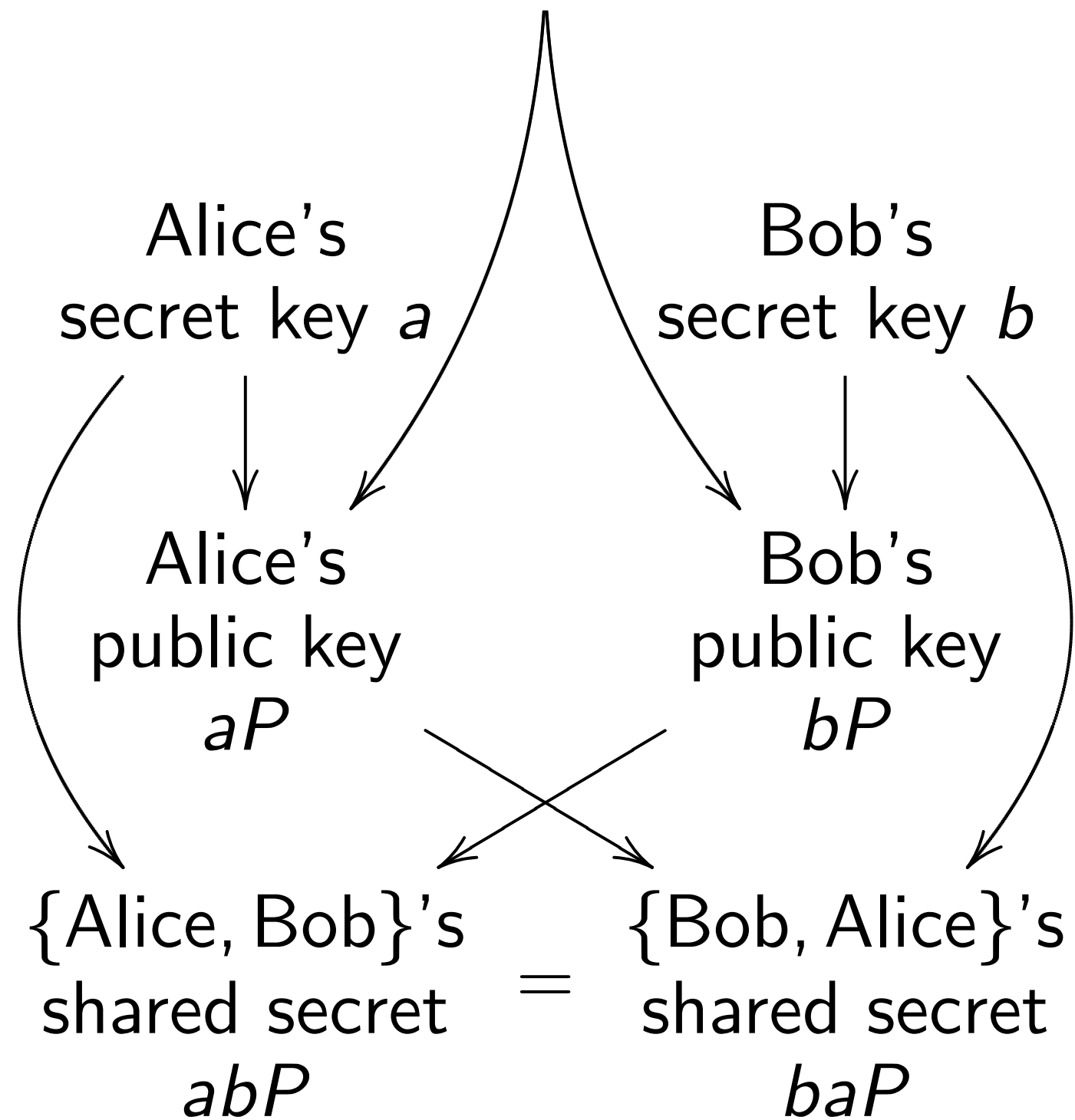
point  $P$

elliptic curve  $E$ :



on choice of  $E$ .

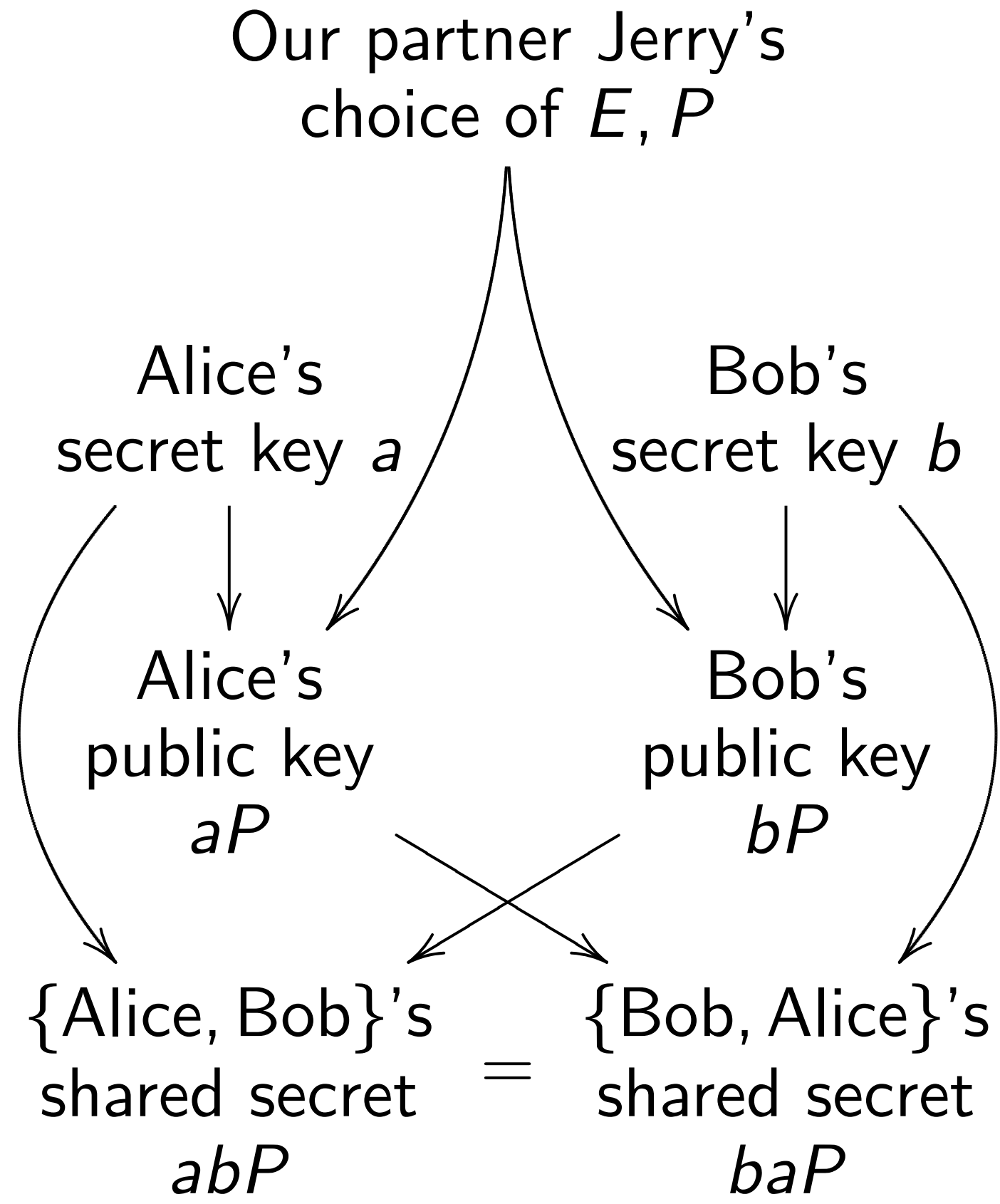
Our partner Jerry's choice of  $E, P$



Can we exploit this picture?

Depends on public key for accepting  $E, P$

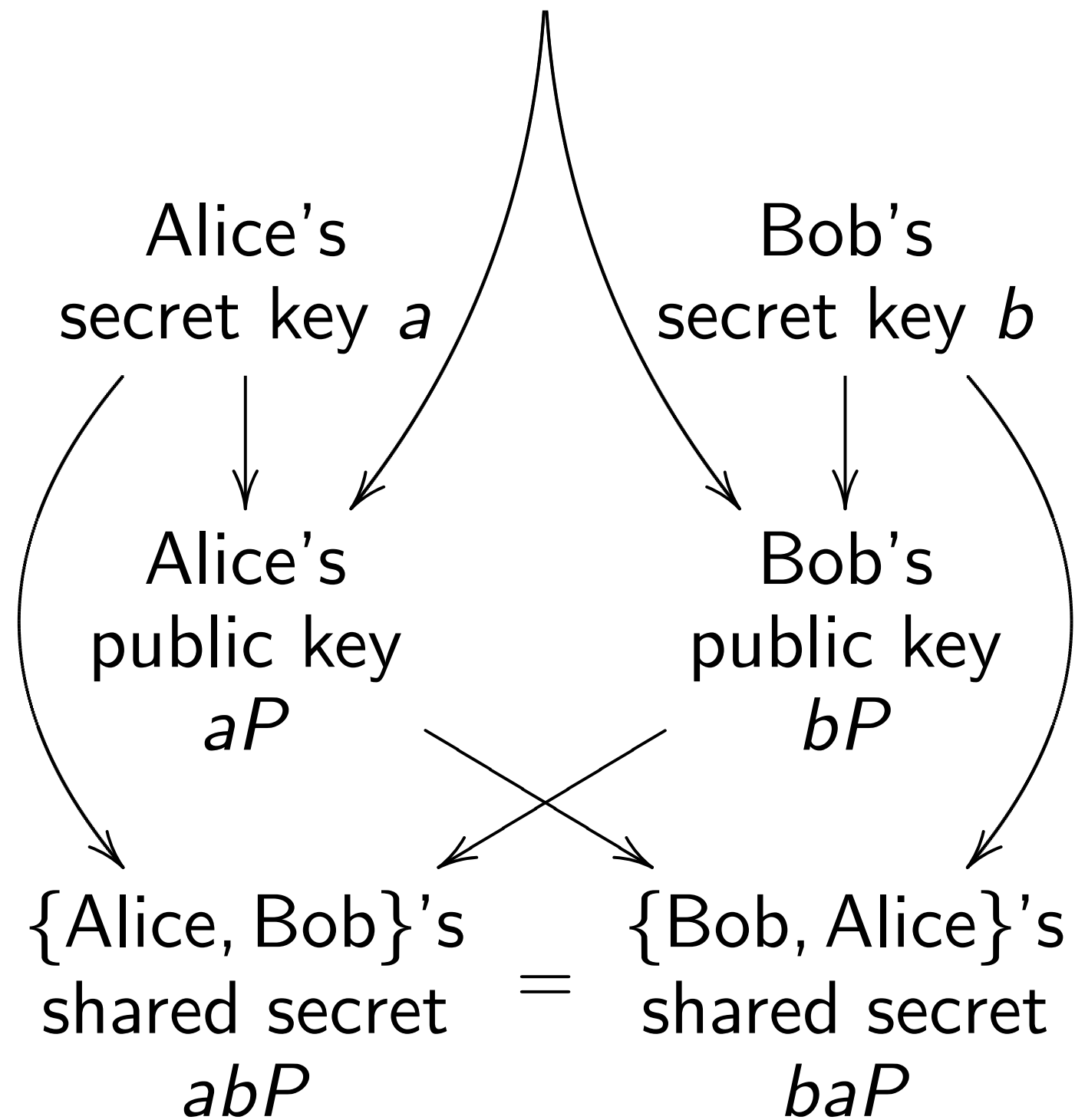
$E$ :  
Alice's secret key  $b$   
Alice's public key  
Alice's secret key  
of  $E$ .



Depends on public criteria for accepting  $E, P$ .

Can we exploit this picture?

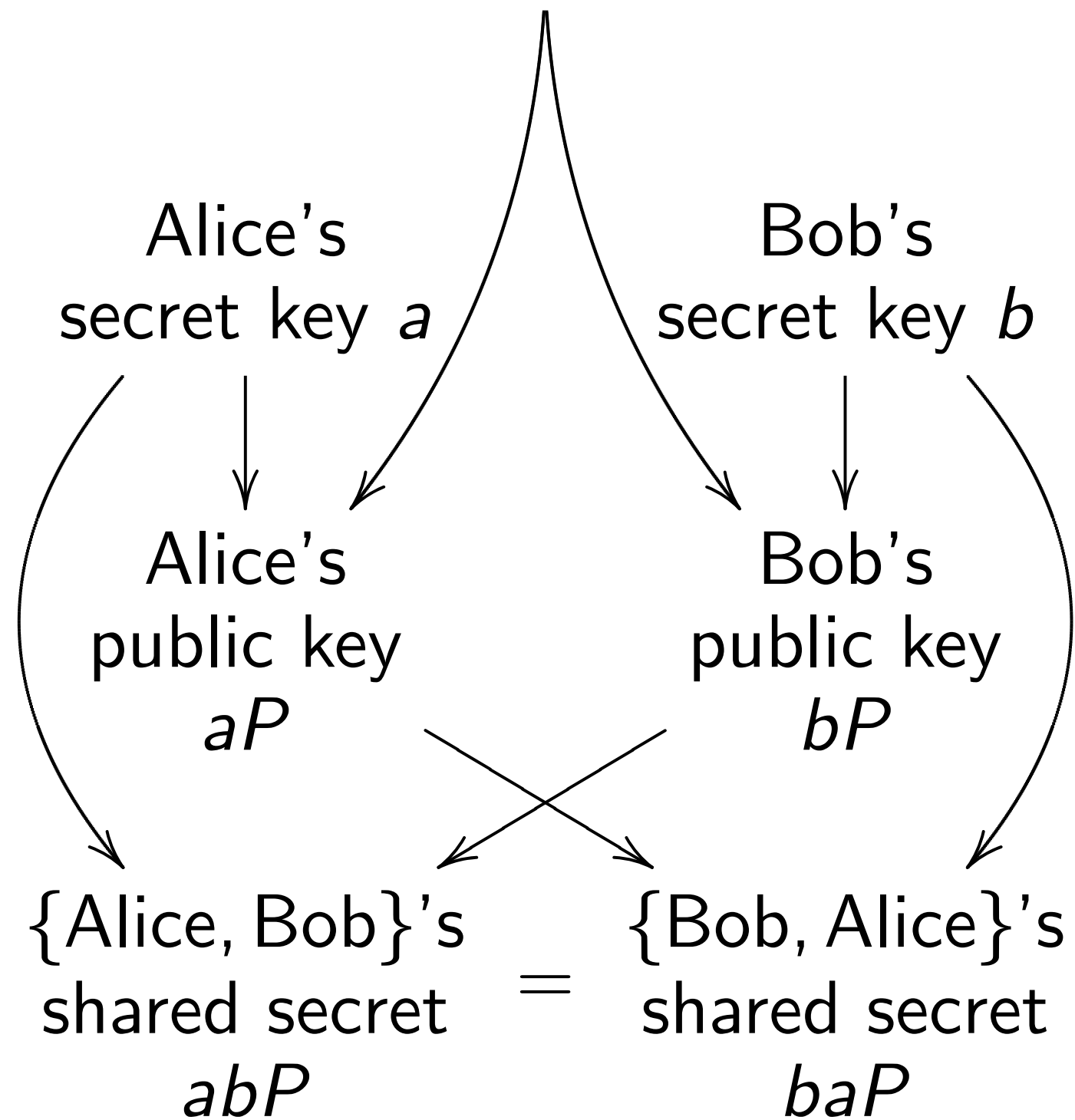
Our partner Jerry's  
choice of  $E, P$



Depends on public criteria  
for accepting  $E, P$ .

Can we exploit this picture?

Our partner Jerry's  
choice of  $E, P$



Can we exploit this picture?

Depends on public criteria  
for accepting  $E, P$ .

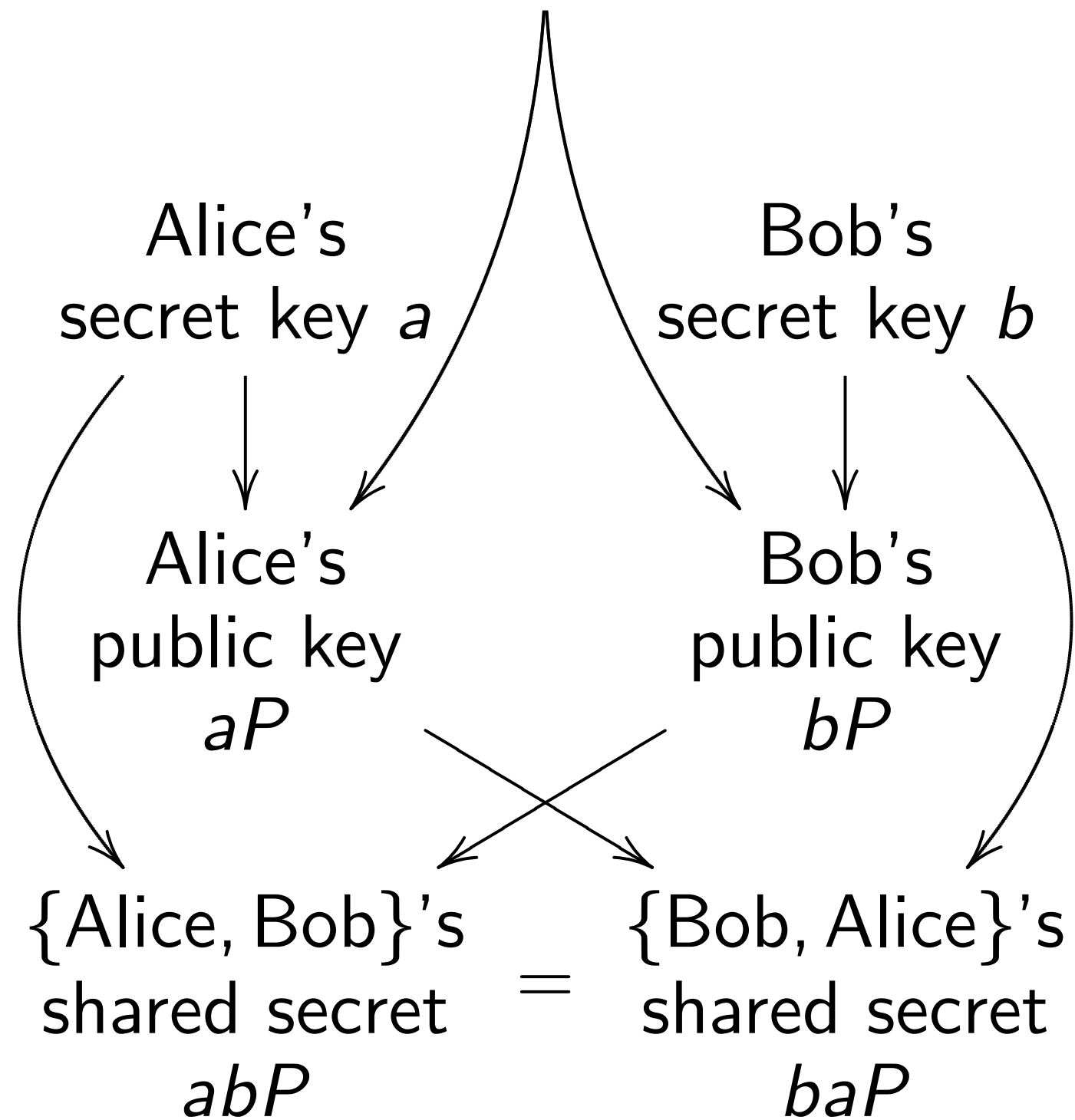
Extensive ECC literature:

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.



Our partner Jerry's  
choice of  $E, P$



Can we exploit this picture?

Depends on public criteria  
for accepting  $E, P$ .

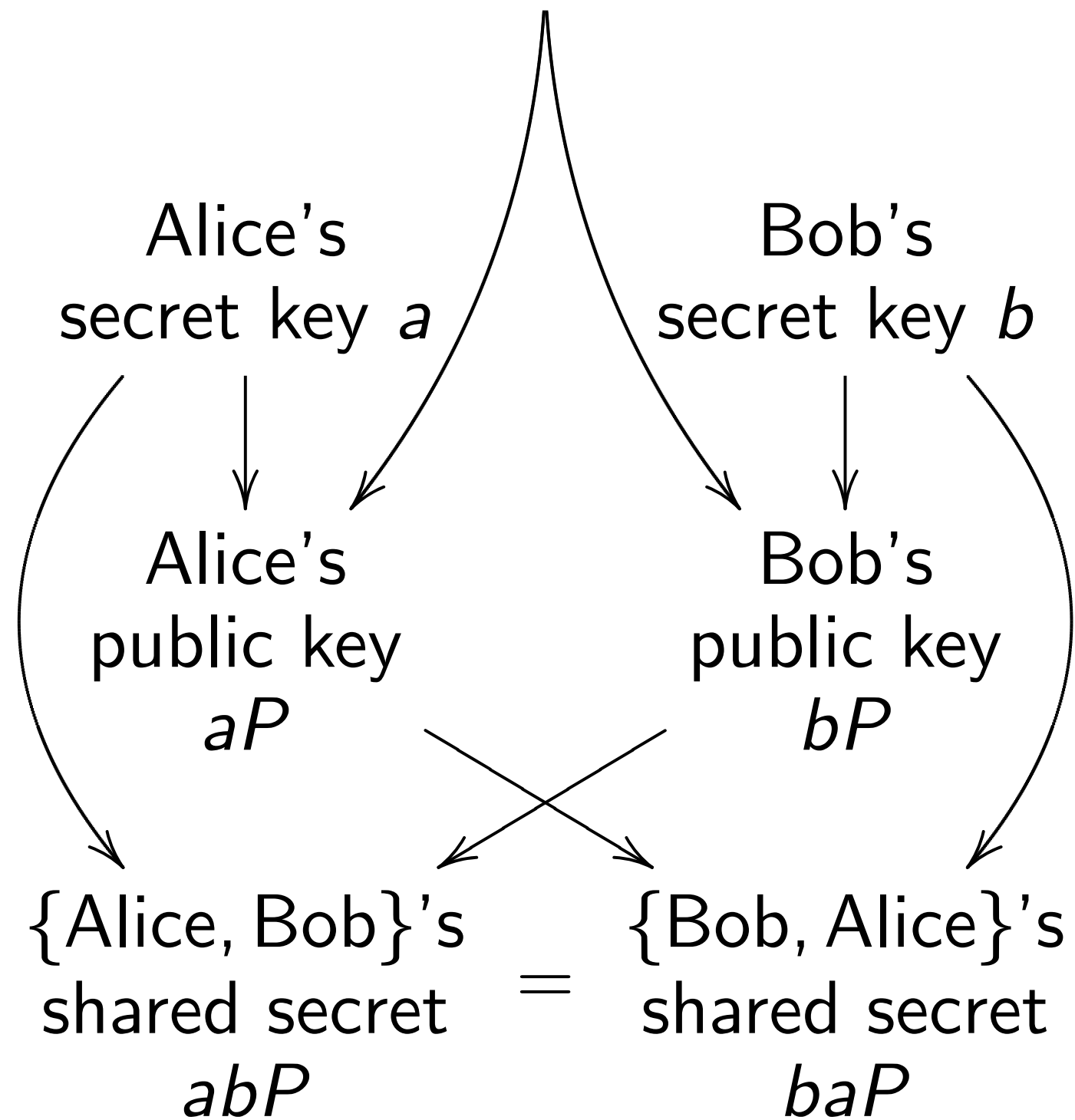
Extensive ECC literature:

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.

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

Our partner Jerry's  
choice of  $E, P$



Can we exploit this picture?

Depends on public criteria  
for accepting  $E, P$ .

Extensive ECC literature:

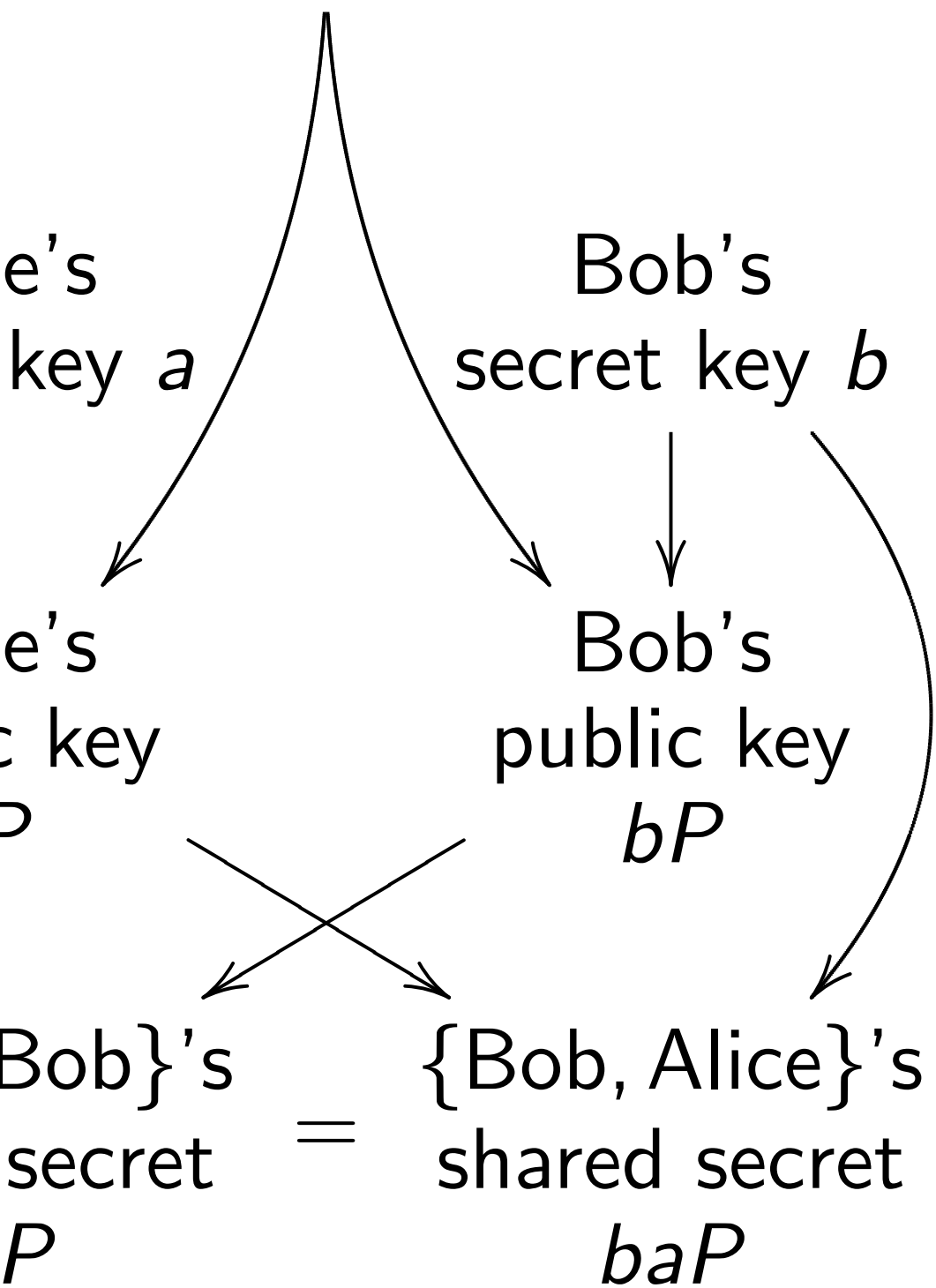
Pollard rho breaks small  $E$ ,  
Pohlig–Hellman breaks most  $E$ ,  
MOV/FR breaks some  $E$ ,  
SmartASS breaks some  $E$ , etc.

Assume that public will accept  
any  $E$  not publicly broken.

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

Jerry standardizes this curve.  
Alice and Bob use it.

Our partner Jerry's  
choice of  $E, P$



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.

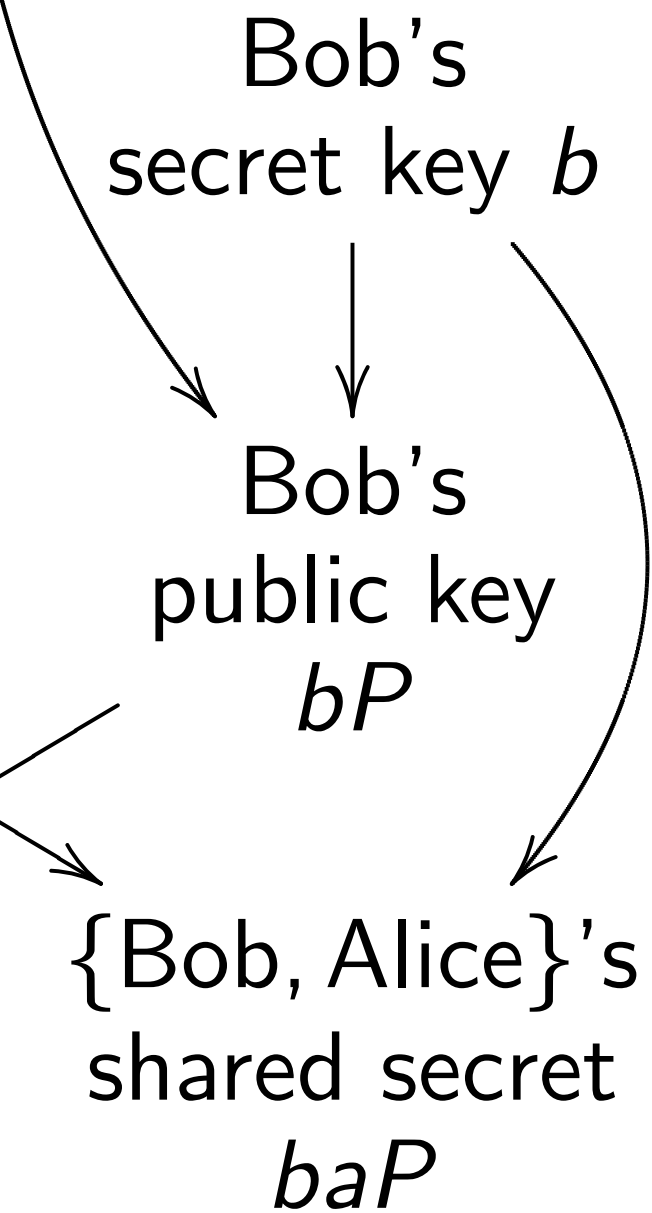
Assume that public will accept  
any  $E$  not publicly broken.

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  
  
Alice}'s  
secret  
b



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?

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  
oting  $E, P$ .

e ECC literature:

who 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 l  
 $E$  must  
*and* Jerry  
"seed" s

criteria

erature:

small  $E$ ,

breaks most  $E$ ,

some  $E$ ,

some  $E$ , etc.

c will accept

y 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 and

$E$  must not be pu

*and* Jerry must pr

“seed”  $s$  such that

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  $E = H(s)$ .

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).

assumption plausible?

the 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

criteria?

plausibility:

[P256V1](#) (2011)

ing curve

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 curve

$y^2 = x^3 - 3x + b$

$b^2c = -27$ ;  $c$  is a

hash is SHA-1 con

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!

public is more demanding

France and China:

not be publicly broken,

ry must provide a

s such that  $E = H(s)$ .

es: [ANSI X9.62](#) (1999)

g 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

possibilit

of all cu

structure

but we c

[generate](#)

until the

one of ‘t

get us to

more demanding  
d China:  
publicly broken,  
provide a  
t  $E = H(s)$ .

X9.62 (1999)  
tic curve  
m”; [Certicom](#)

“verifiably  
s offer

onservative  
eters 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 one  
of all curves have  
structure that ‘the  
but we don’t. The  
[generate a million](#)  
until they find one  
one of ‘their’ curves  
get us to use them

What exactly is  $H$ ?

NIST defines curve  $E$  as

$$y^2 = x^3 - 3x + b \text{ where}$$

$b^2c = -27$ ;  $c$  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 million of all curves have an exploitable structure that ‘they’ know about but we don’t. Then ‘they’ [generate a million random samples](#) 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

$$y^2 = x^3 - 3x + b \text{ where}$$

$b^2c = -27$ ;  $c$  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

$$y^2 = x^3 - 3x + b \text{ where}$$

$b^2c = -27$ ;  $c$  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.



actly is  $H$ ?

efines curve  $E$  as

$- 3x + b$  where

$-27$ ;  $c$  is a hash of  $s$ ;

SHA-1 concatenation.

arly 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  $s$ ;

concatenation.

will accept

!

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

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

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.

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**  
**a million random seeds**  
ey find one that generates  
their’ curves. Then they  
o use them.”

optimized 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 t  
expected  
**nothing–**

Consider now the  
in a million  
an exploitable  
they' know about,  
when 'they' **simply**  
**random seeds**  
that generates  
es. Then they  
n.”

This computation  
cluster of 41  
in 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 v  
construction, are a  
**of hidden properties**

Microsoft “NUMS  
“**generated determ**  
from the security

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

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 ( “**generated deterministically**  
from the security level” .

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



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**” .

in some countries  
is more demanding.

ol standard:

oice of the seeds

ich the [NIST] curve

ers have been derived is

ivated leaving an essential

the 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

countries  
demanding.  
d:  
e seeds  
[IST] curve  
been derived is  
ving an essential  
y analysis

**o-random.**  
urves shall be  
udo-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

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  
tion, 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 jobs





ptography,  
**eeve numbers**  
which, by their  
**above suspicion**  
**es.**”  
” curves (2014):  
**ministically**  
level” .  
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 available

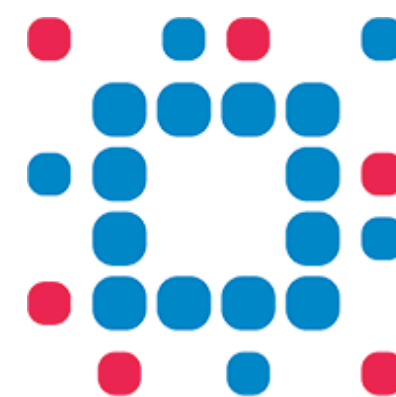


New: We generated a **BADA55** curve “BADA55-VPR-224” with a Brainpool-like explanation.

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!



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!



**OWA**  
Open Web Alliance



**Experian**  
Marketing Services