How to manipulate standards

Daniel J. Bernstein
Verizon Communications Inc.

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

Our core mission:

Delivering information

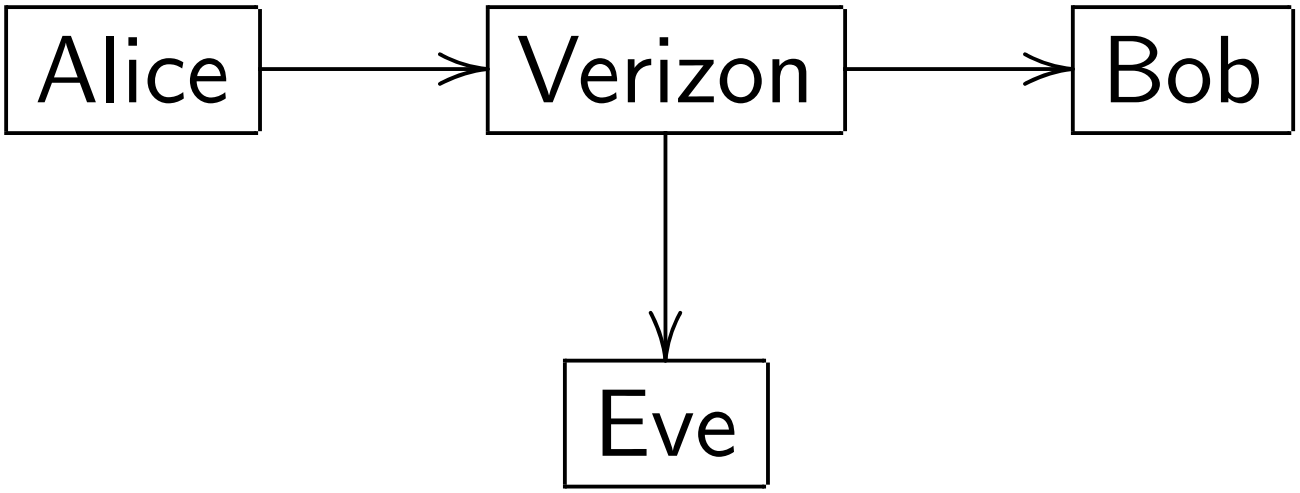
from point A to point B.

Our core mission:

Delivering information

from point A to point B,

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

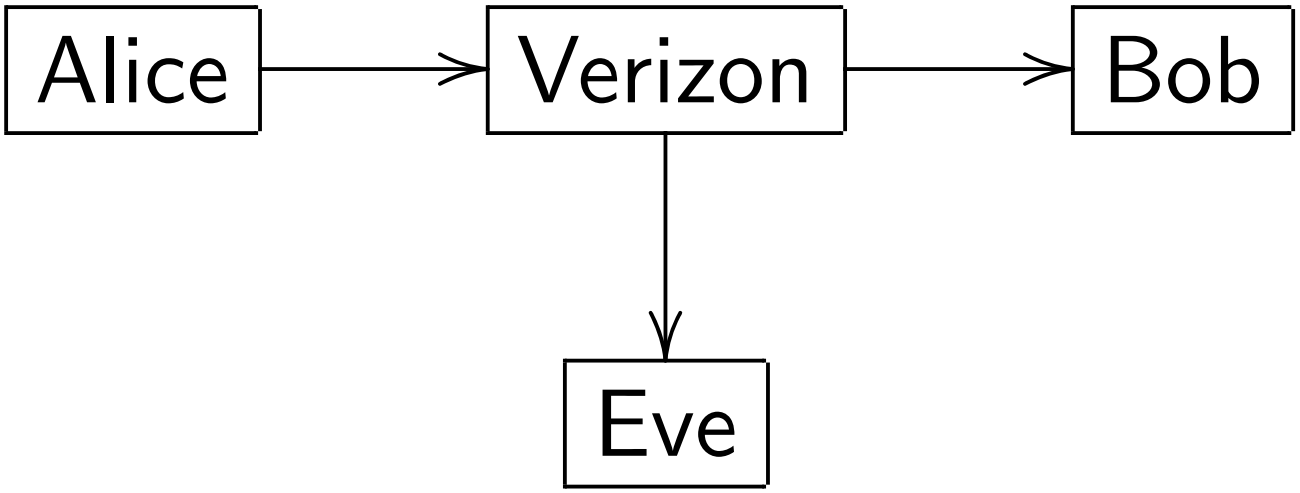


Our core mission:

Delivering information

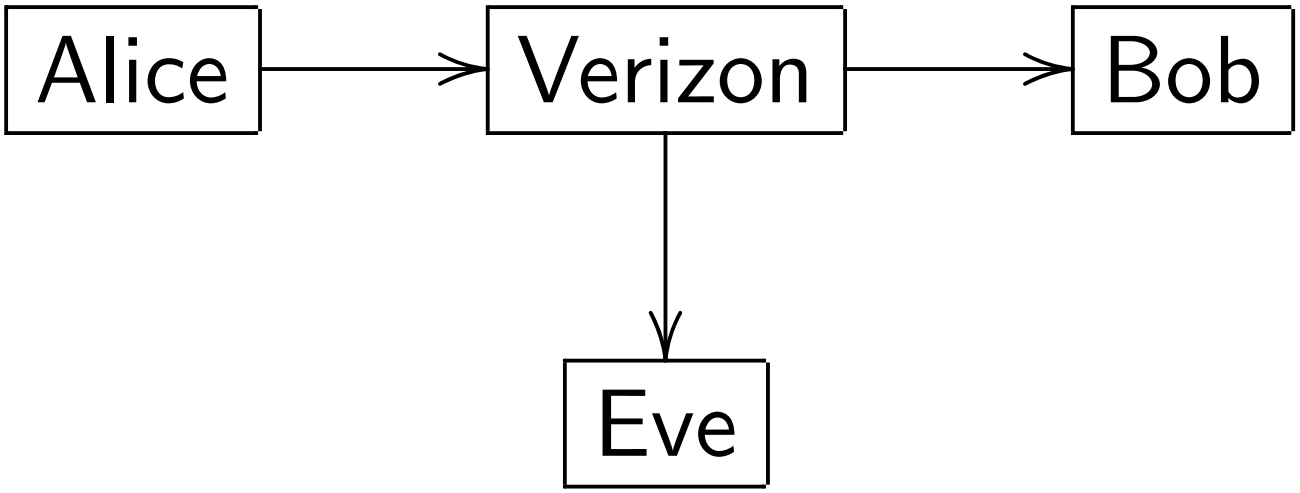
from point A to point B,

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



“Can you hear me now? Good.”

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



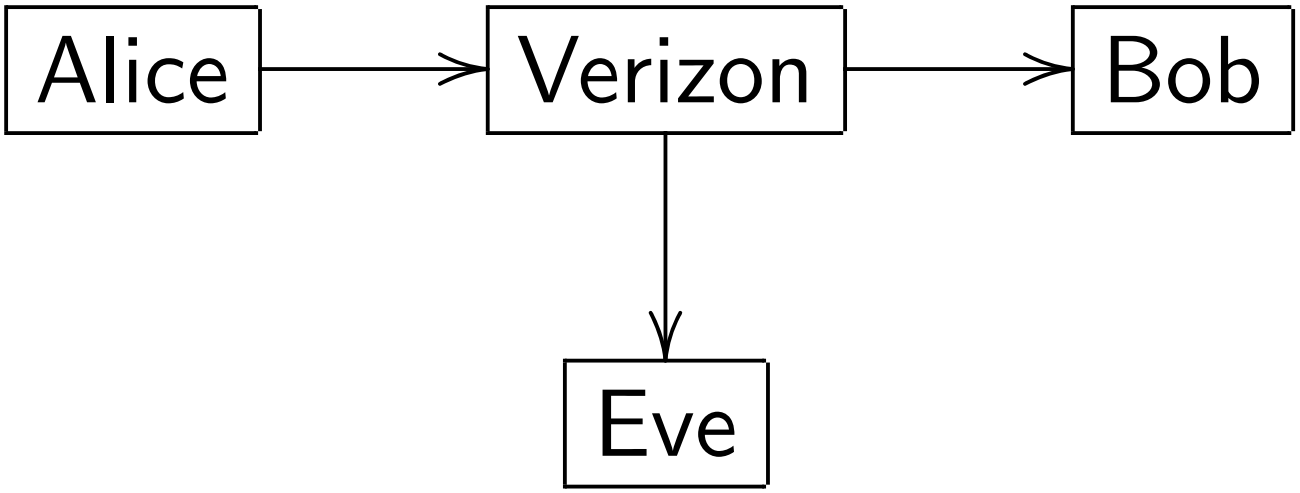
"Can you hear me now? Good."
"Can they hear you now? Good."

Our core mission:

Delivering information

from point A to point B,

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

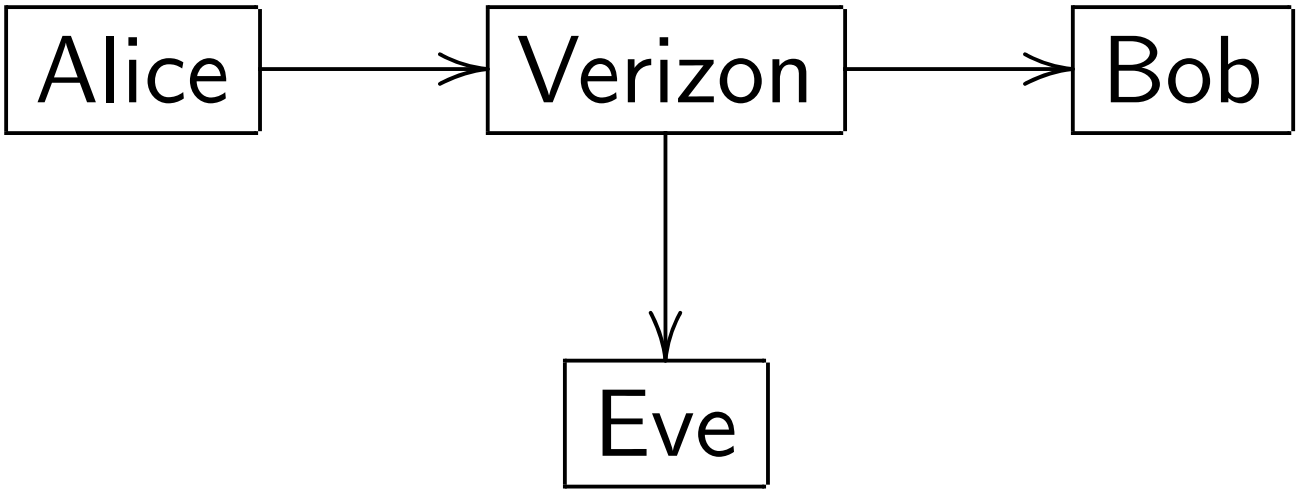


“Can you hear me now? Good.”

“Can they hear you now? Good.”

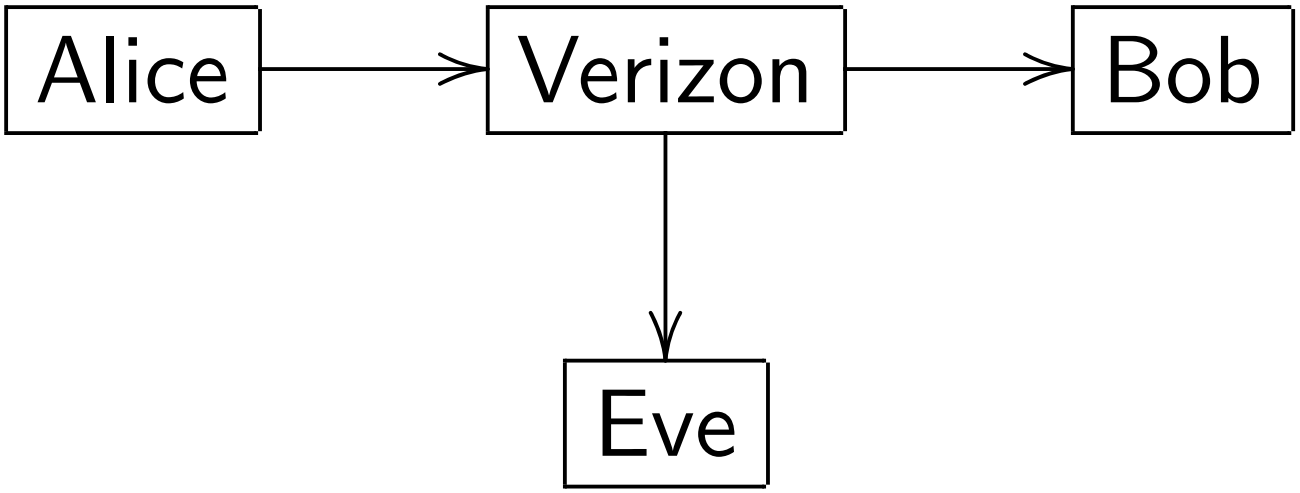
“We never stop working for you.”

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



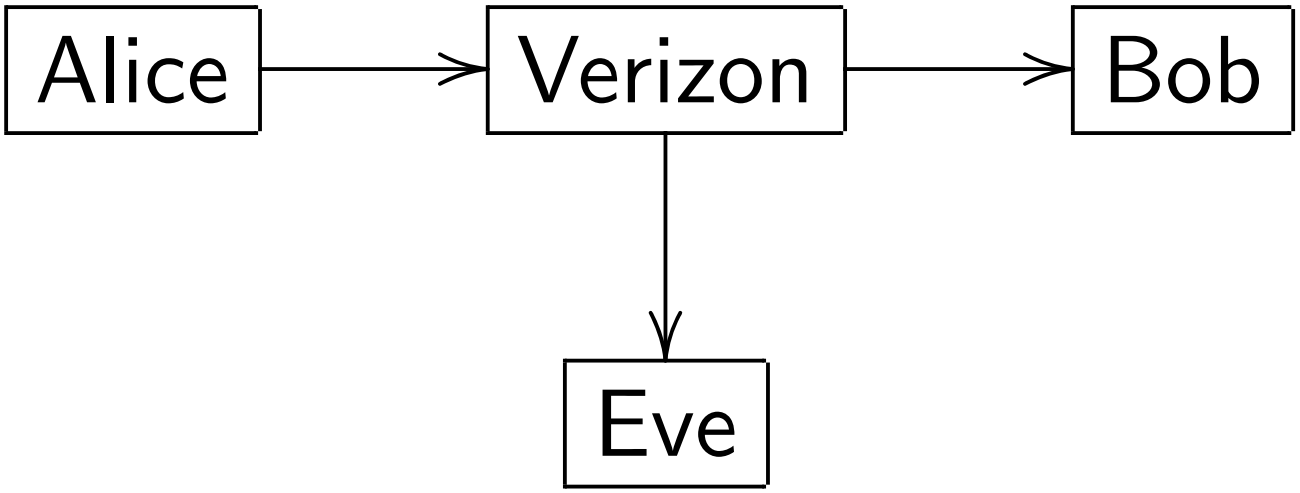
"Can you hear me now? Good."
"Can they hear you now? Good."
"We never stop working for you."
"Rule the air."

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."

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.

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."

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.

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**.

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.

"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."

"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."

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.

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."

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.

Technical backlash?

Increasing problem for us:

Crypto. This "breaks network management, content distribution and network services"; creates "congestion" and "latency";

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";

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!

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**.

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.

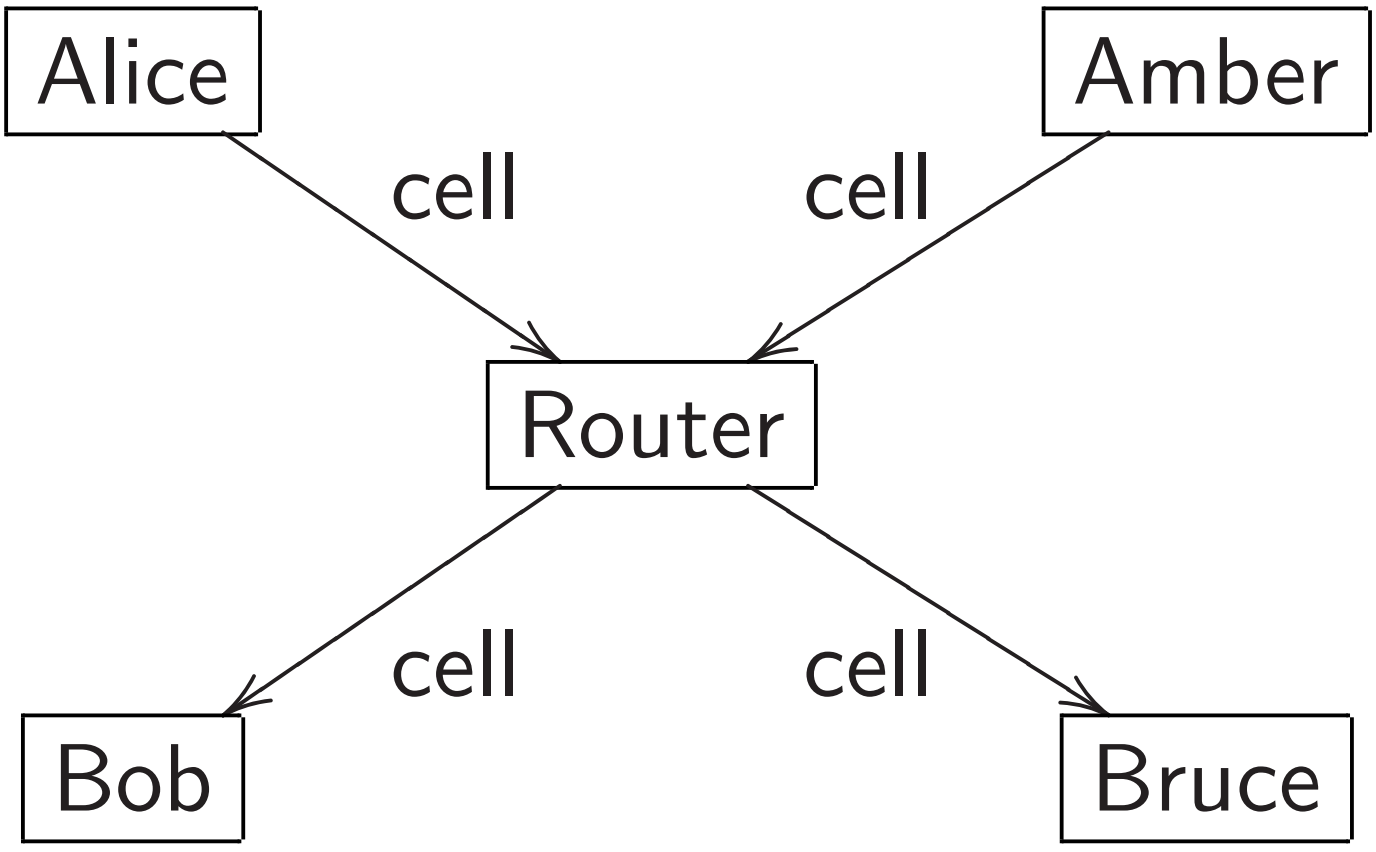
Can't modify signed data but

can track in many other ways.

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

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?

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

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**?

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?

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.”

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."

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.

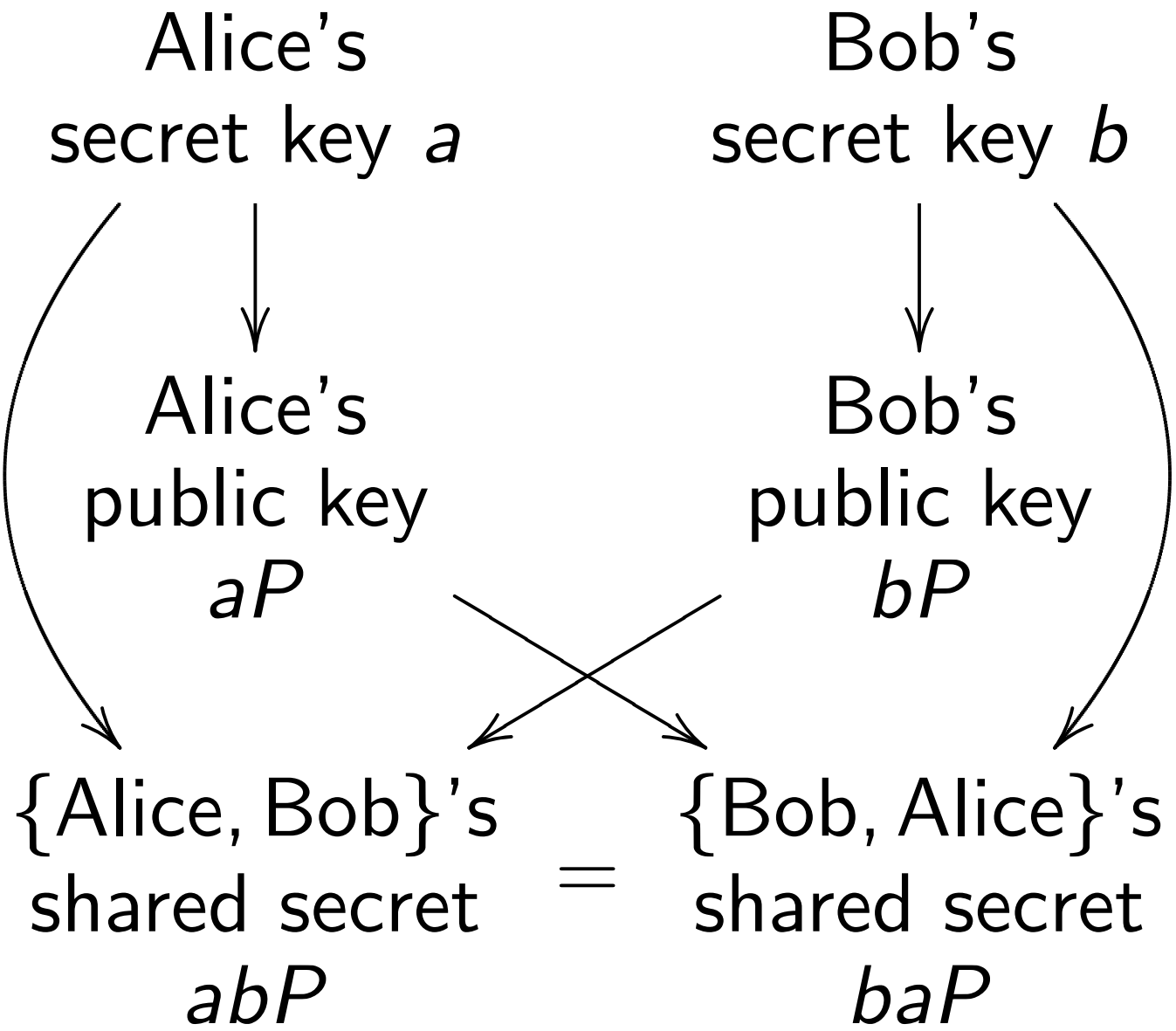
Sabotaging crypto details

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

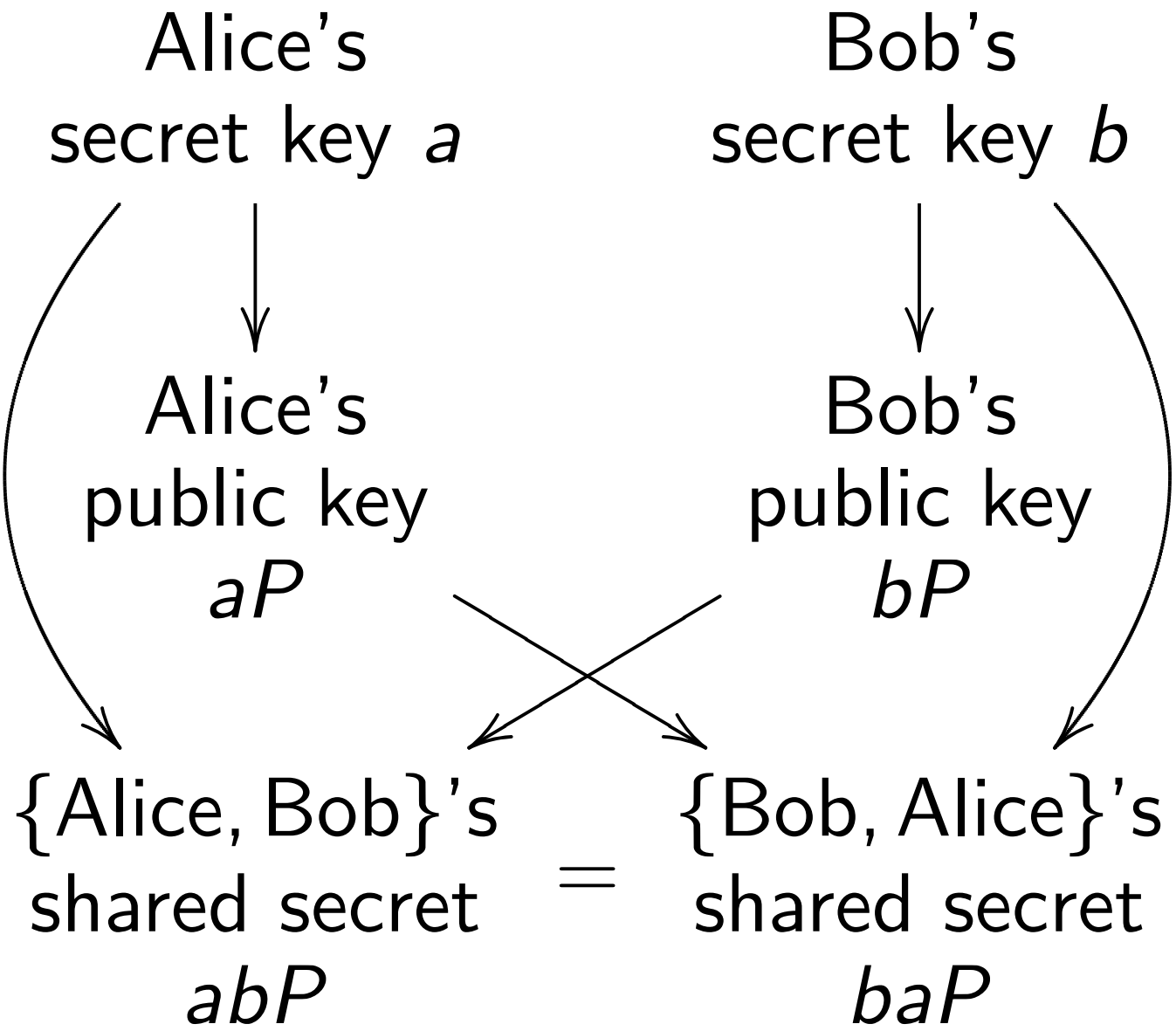
Daniel J. Bernstein
Tung Chou
Chitchanok Chuengsatiansup
Andreas Hülsing
Tanja Lange
Ruben Niederhagen
Christine van Vredendaal

safecurves.cr.yp.to
/bada55.html

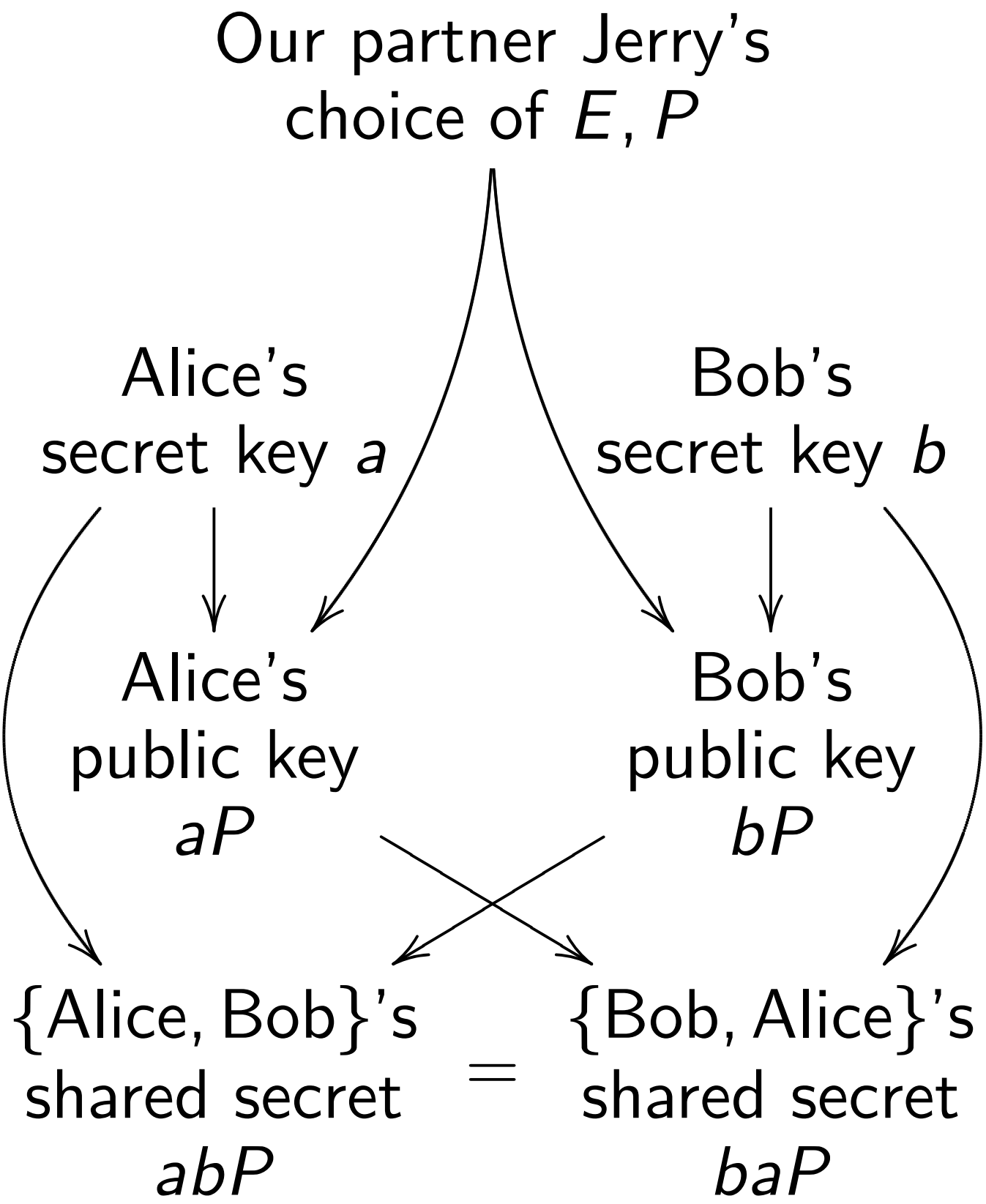
Textbook key exchange
using standard point P
on a standard elliptic curve E:

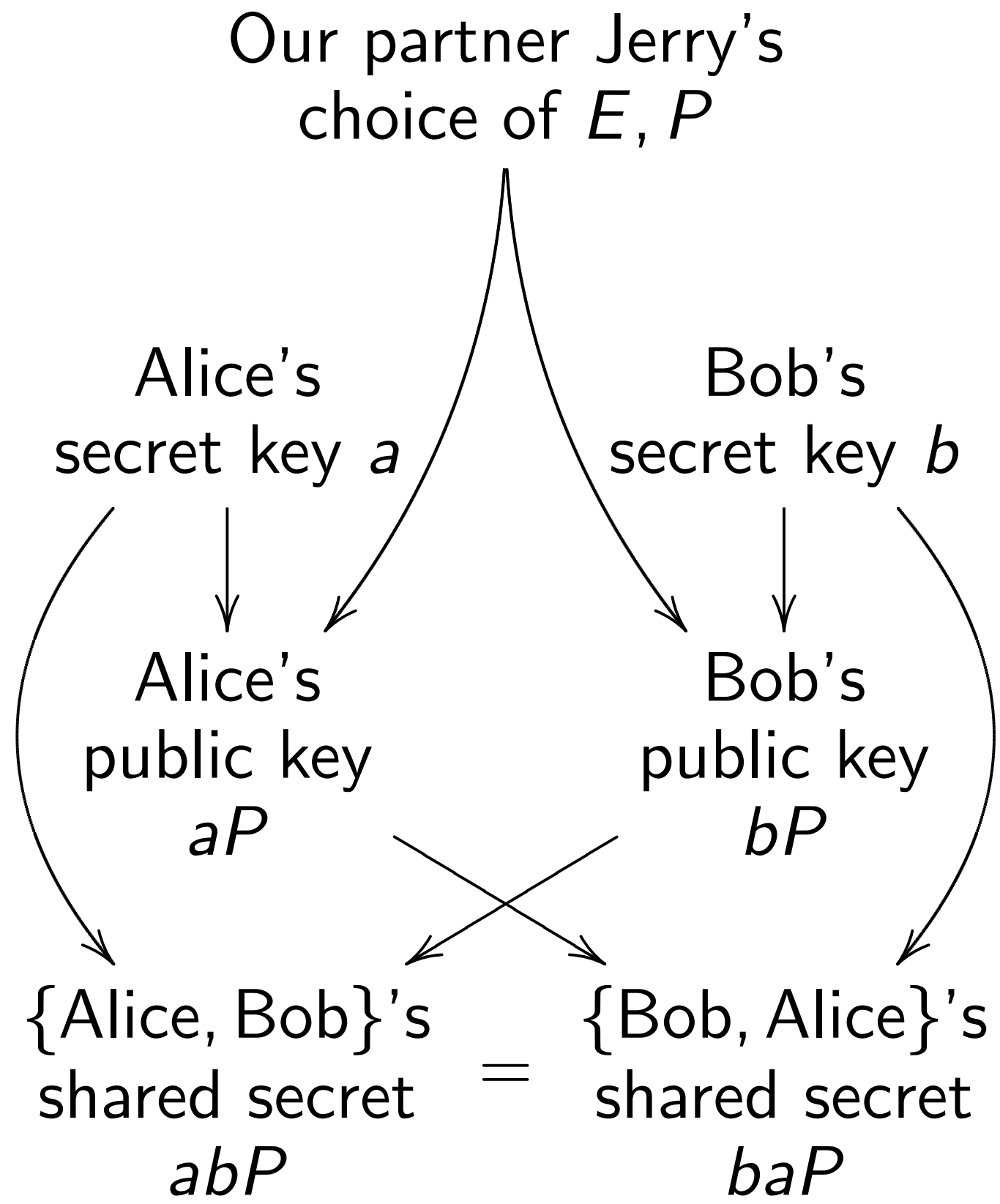


Textbook key exchange
using standard point P
on a standard elliptic curve E:



Security depends on choice of E.


Our partner Jerry's
choice of E, P
Alice's
secret key a
Bob's
secret key b
Alice's
public key
aP
Bob's
public key
bP
{Alice, Bob}'s
shared secret
abP
=
{Bob, Alice}'s
shared secret
baP



Can we exploit this picture?

Depends on public criteria
for accepting E, P.

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.

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.

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?

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.

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 $E = H(s)$.

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.

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.

What exactly is H?

NIST defines curve E as
$y^2 = x^3 - 3x + b$ where
$b^2 c = -27$; 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."

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

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

Maybe in some countries
the public is more demanding.

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".

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

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.

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!