Overview of post-quantum cryptography

D. J. Bernstein
University of Illinois at Chicago &
Technische Universiteit Eindhoven

Cryptography = "secret writing".

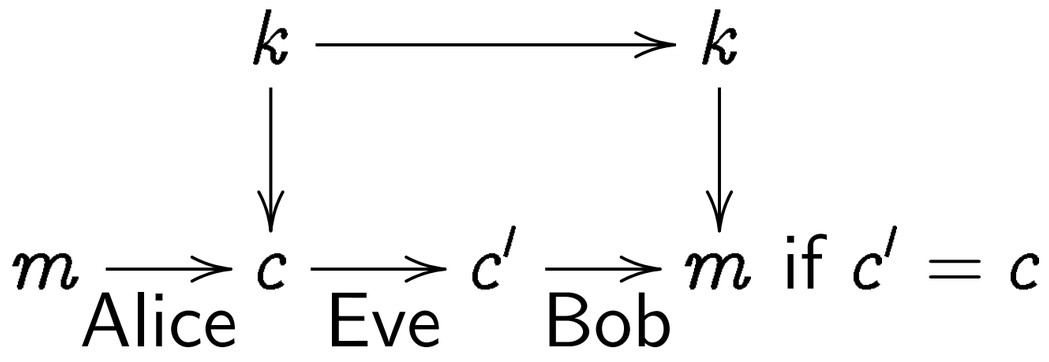
Achieve various security goals
by secretly transforming messages.

Major theme of research:
Users have cost constraints.
Can be challenging to reach
acceptable security levels.

Secret-key cryptography

Prerequisite: Alice and Bob
share a short secret key k
not known to eavesdropper Eve.

Security goals:
Confidentiality and integrity
for any number of messages
exchanged by Alice and Bob,
despite Eve's espionage+forgery.



w of
antum cryptography

ernstein
ty of Illinois at Chicago &
che Universiteit Eindhoven

---

raphy = "secret writing".

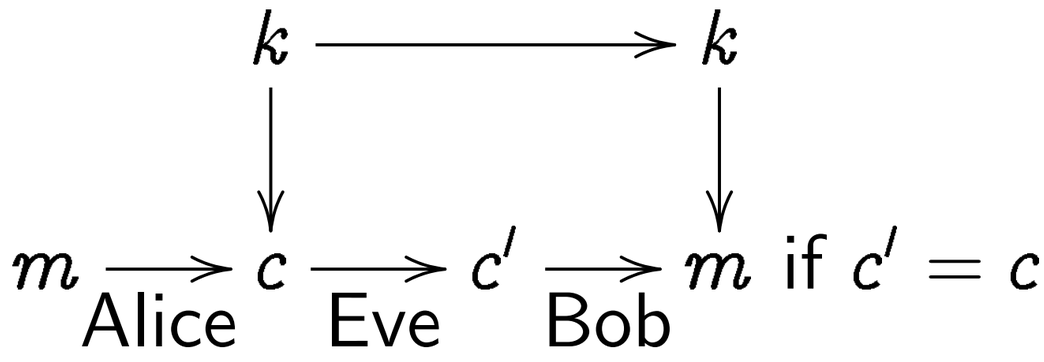
various security goals
tly transforming messages.

heme of research:
ave cost constraints.
challenging to reach
ble security levels.

Secret-key cryptography

Prerequisite: Alice and Bob
share a short secret key k
not known to eavesdropper Eve.

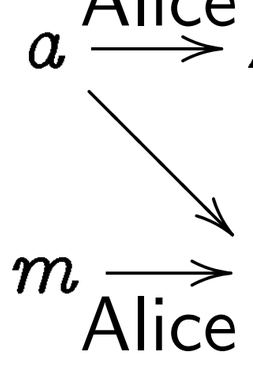
Security goals:
Confidentiality and integrity
for any number of messages
exchanged by Alice and Bob,
despite Eve's espionage+forgery.



Public-k

Prerequi
Alice ha
correspo
Everyone
Eve does

Security
for any
publishe



ptography

is at Chicago &
siteit Eindhoven

---

secret writing".

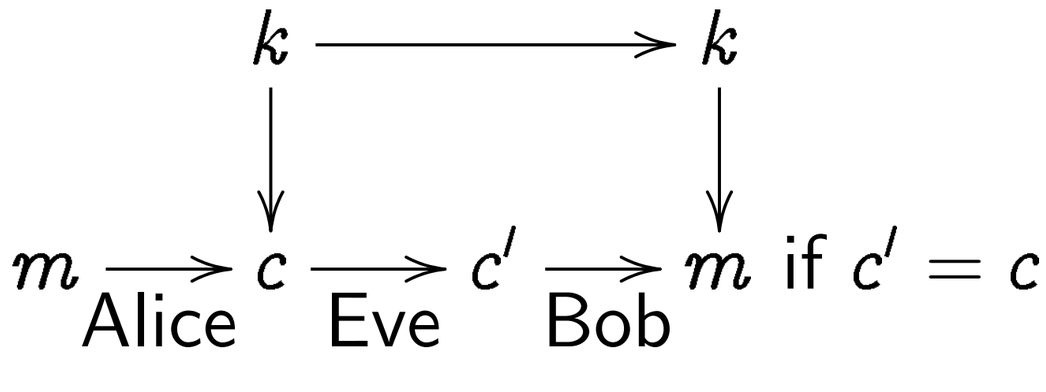
curity goals
rming messages.

search:
onstraints.
g to reach
y levels.

Secret-key cryptography

Prerequisite: Alice and Bob
share a short secret key k
not known to eavesdropper Eve.

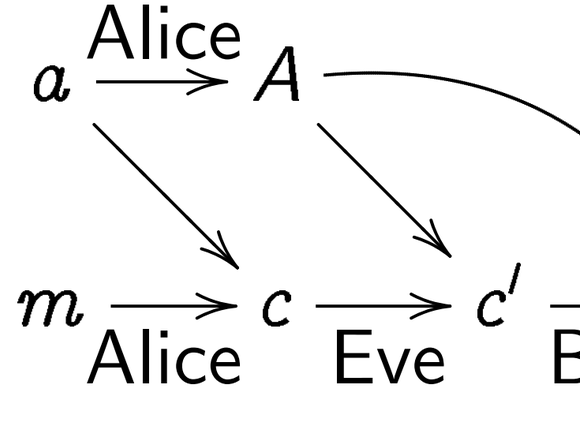
Security goals:
Confidentiality and integrity
for any number of messages
exchanged by Alice and Bob,
despite Eve's espionage+forgery.



Public-key signatu

Prerequisite:
Alice has a short s
corresponding pub
Everyone knows A
Eve does not know

Security goal: Inte
for any number of
published by Alice



ago &
hoven

---

ting".

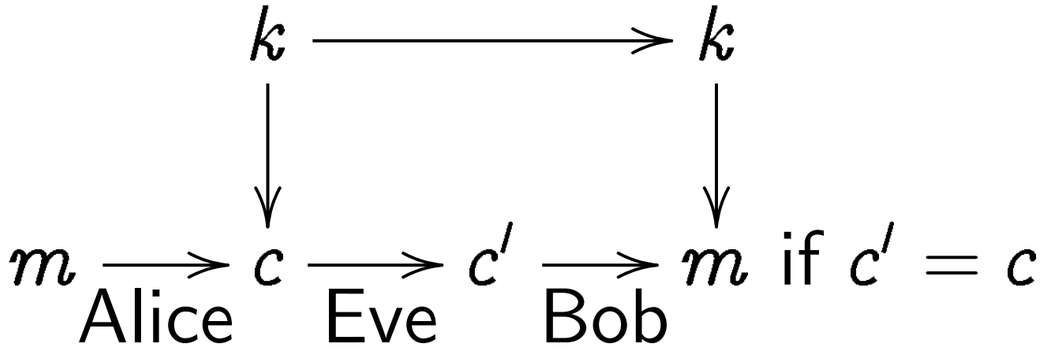
ls

ssages.

Secret-key cryptography

Prerequisite: Alice and Bob
share a short secret key k
not known to eavesdropper Eve.

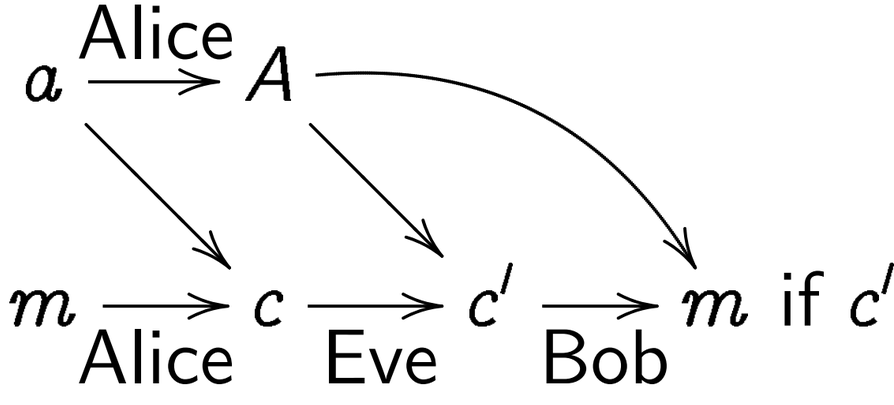
Security goals:
Confidentiality and integrity
for any number of messages
exchanged by Alice and Bob,
despite Eve's espionage+forgery.



Public-key signatures

Prerequisite:
Alice has a short secret key a
corresponding public key A.
Everyone knows A.
Eve does not know a.

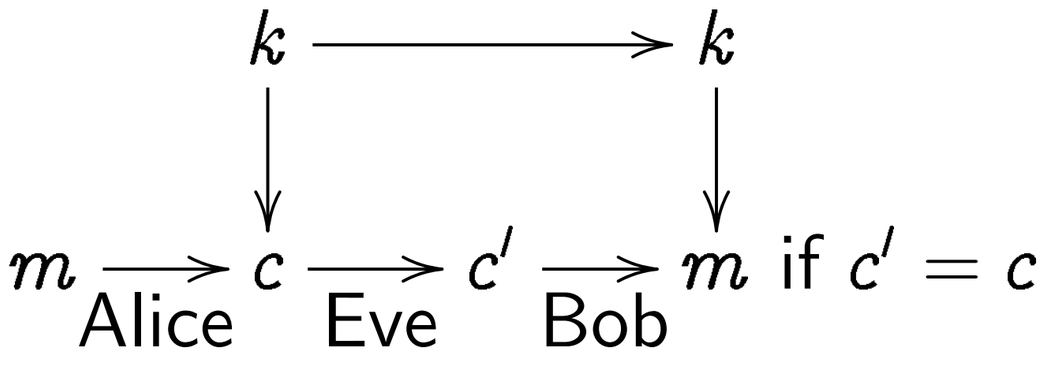
Security goal: Integrity
for any number of messages
published by Alice.



Secret-key cryptography

Prerequisite: Alice and Bob
share a short secret key k
not known to eavesdropper Eve.

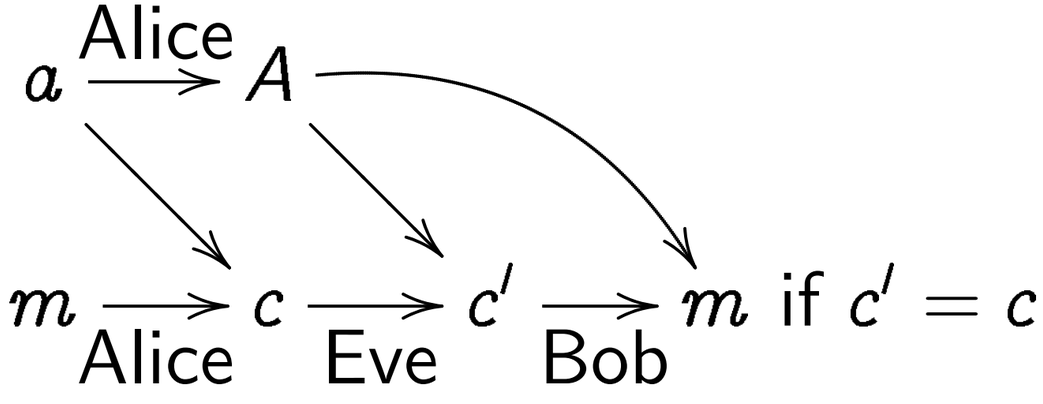
Security goals:
Confidentiality and integrity
for any number of messages
exchanged by Alice and Bob,
despite Eve's espionage+forgery.



Public-key signatures

Prerequisite:
Alice has a short secret key a,
corresponding public key A.
Everyone knows A.
Eve does not know a.

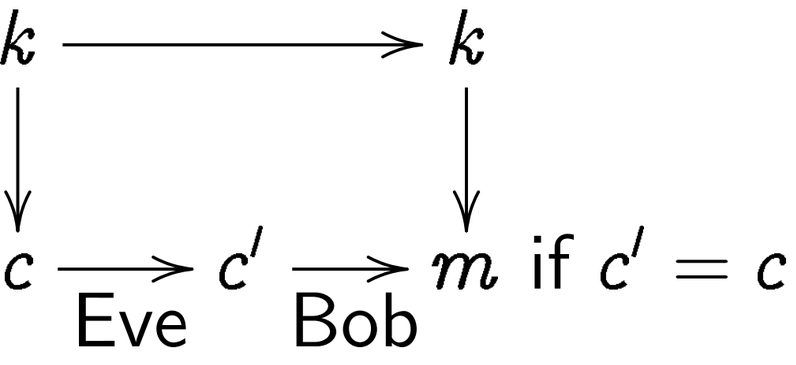
Security goal: Integrity
for any number of messages
published by Alice.



ey cryptography

site: Alice and Bob
short secret key k
wn to eavesdropper Eve.

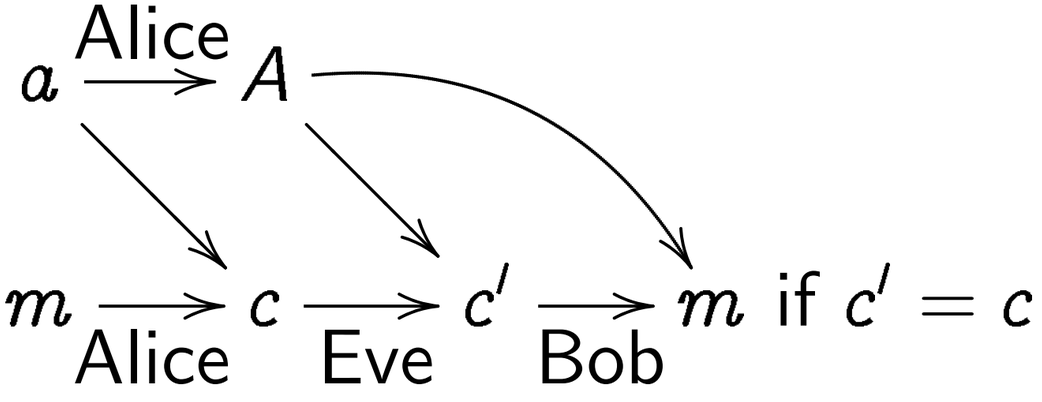
goals:
ntiality and integrity
number of messages
ed by Alice and Bob,
Eve's espionage+forgery.



Public-key signatures

Prerequisite:
Alice has a short secret key a,
corresponding public key A.
Everyone knows A.
Eve does not know a.

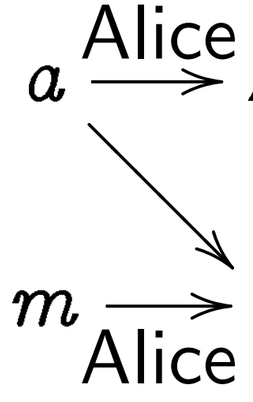
Security goal: Integrity
for any number of messages
published by Alice.



Public-k

Prerequi
Alice ha
Public k
Eve does

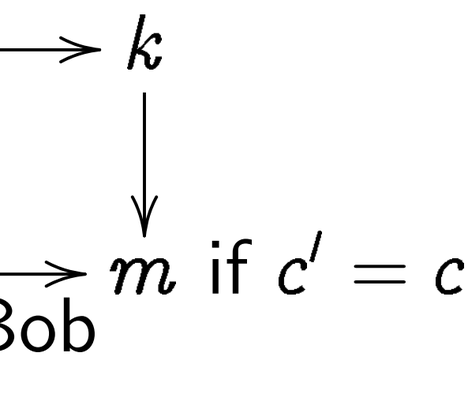
Security
Confiden
for any
exchang



graphy

e and Bob
et key k
esdropper Eve.

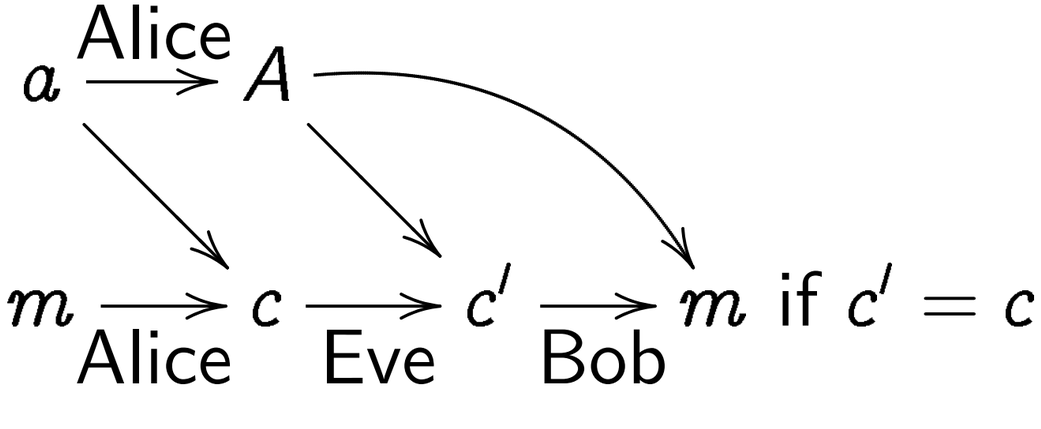
d integrity
messages
e and Bob,
onage+forgery.



Public-key signatures

Prerequisite:
Alice has a short secret key a,
corresponding public key A.
Everyone knows A.
Eve does not know a.

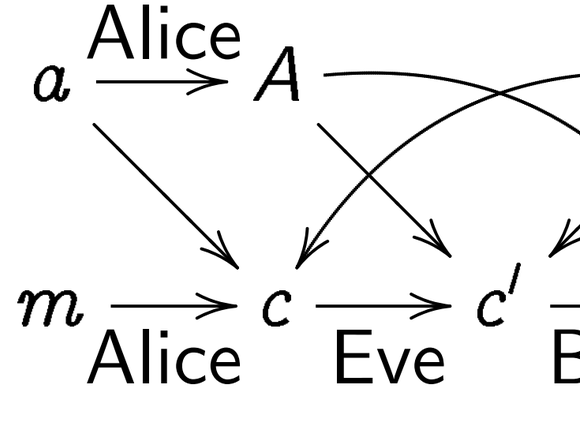
Security goal: Integrity
for any number of messages
published by Alice.



Public-key encrypt

Prerequisite:
Alice has a, A; Bo
Public knows A an
Eve does not know

Security goals:
Confidentiality and
for any number of
exchanged by Alic



Eve.

,

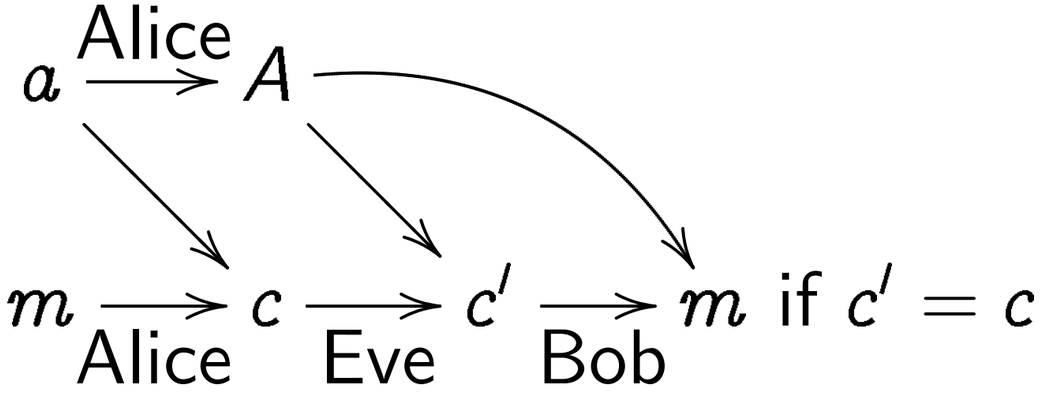
gery.

$= c$

Public-key signatures

Prerequisite:
Alice has a short secret key a,
corresponding public key A.
Everyone knows A.
Eve does not know a.

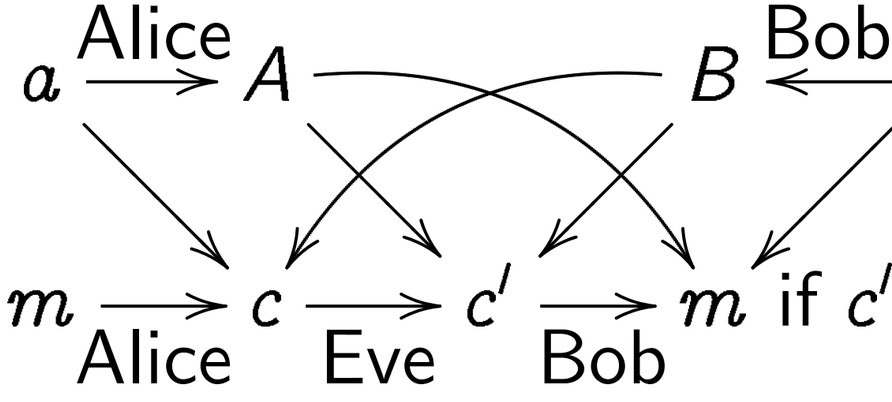
Security goal: Integrity
for any number of messages
published by Alice.



Public-key encryption (DH f

Prerequisite:
Alice has a, A; Bob has b, B
Public knows A and B.
Eve does not know a, b.

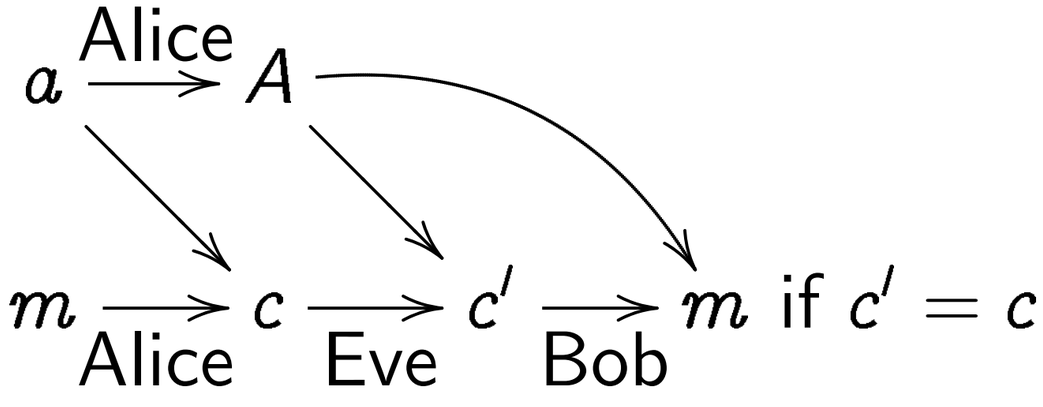
Security goals:
Confidentiality and integrity
for any number of messages
exchanged by Alice and Bob



Public-key signatures

Prerequisite:
Alice has a short secret key a,
corresponding public key A.
Everyone knows A.
Eve does not know a.

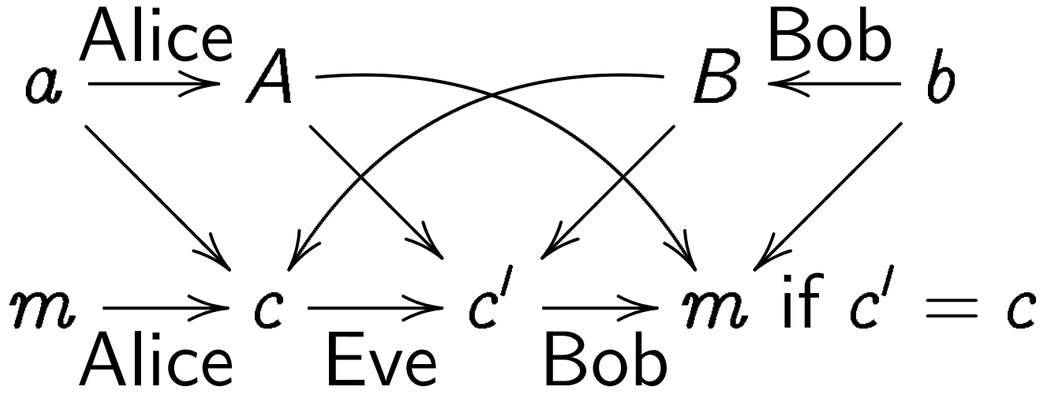
Security goal: Integrity
for any number of messages
published by Alice.



Public-key encryption (DH form)

Prerequisite:
Alice has a, A; Bob has b, B.
Public knows A and B.
Eve does not know a, b.

Security goals:
Confidentiality and integrity
for any number of messages
exchanged by Alice and Bob.

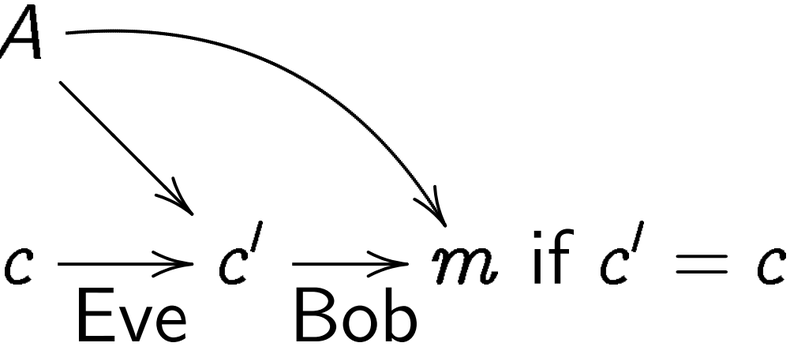


ey signatures

site:

s a short secret key a,
nding public key A.
e knows A.
s not know a.

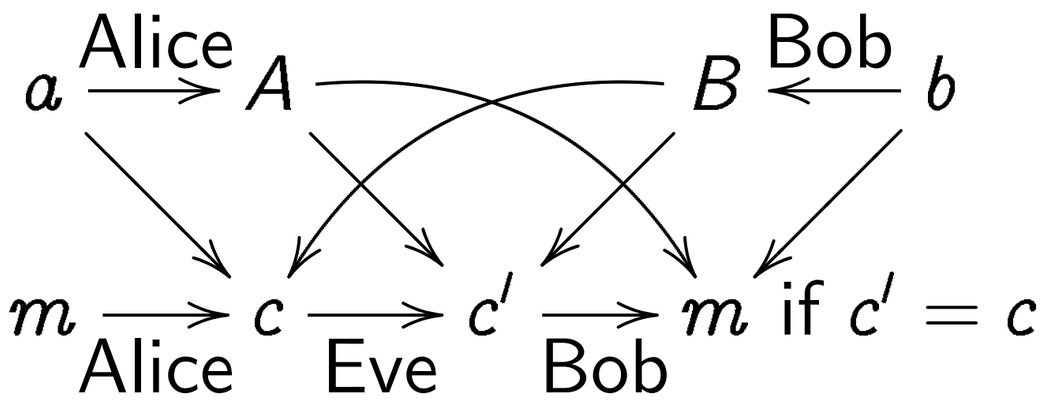
goal: Integrity
number of messages
d by Alice.



Public-key encryption (DH form)

Prerequisite:
Alice has a, A; Bob has b, B.
Public knows A and B.
Eve does not know a, b.

Security goals:
Confidentiality and integrity
for any number of messages
exchanged by Alice and Bob.



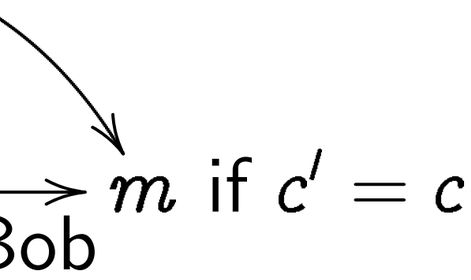
Advance

Many ot
studied i
stopping
securely
searchin
and muc

res

secret key a,
lic key A.
.
v a.

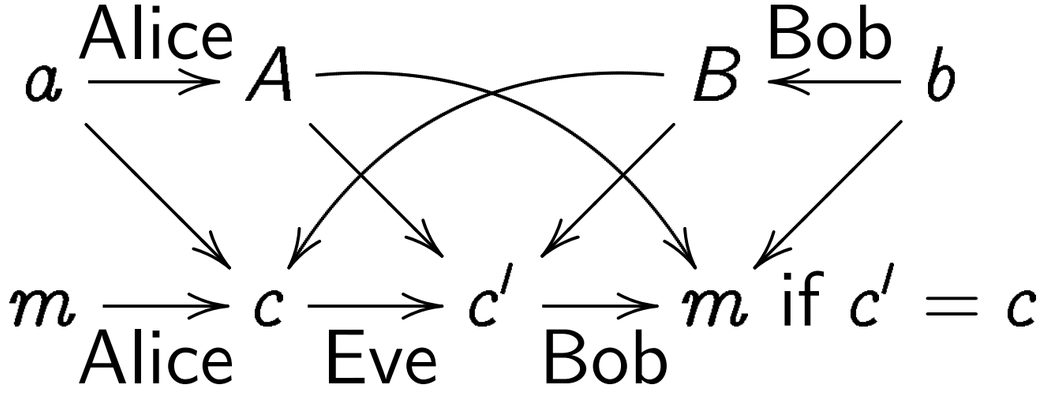
egrity
messages
.



Public-key encryption (DH form)

Prerequisite:
Alice has a, A; Bob has b, B.
Public knows A and B.
Eve does not know a, b.

Security goals:
Confidentiality and integrity
for any number of messages
exchanged by Alice and Bob.



Advanced security

Many other securi
studied in cryptog
stopping traffic an
securely tallying vo
searching encrypte
and much more.

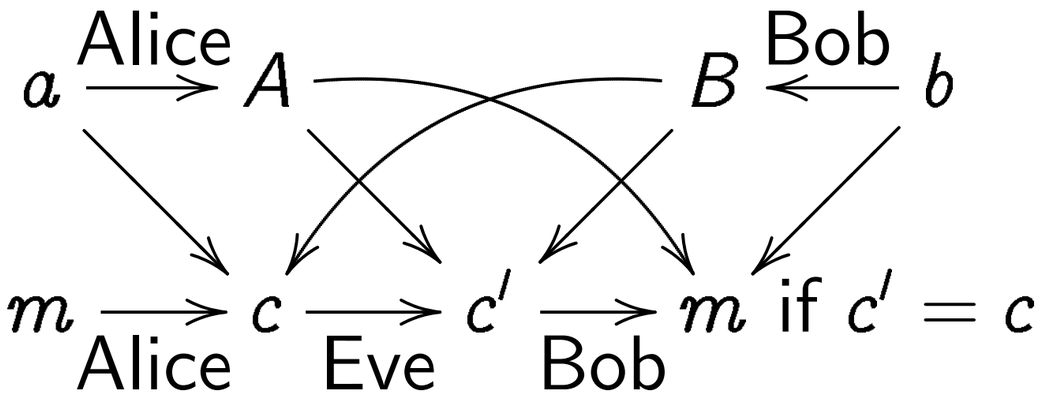
a,

$= c$

Public-key encryption (DH form)

Prerequisite:
Alice has a, A; Bob has b, B.
Public knows A and B.
Eve does not know a, b.

Security goals:
Confidentiality and integrity
for any number of messages
exchanged by Alice and Bob.



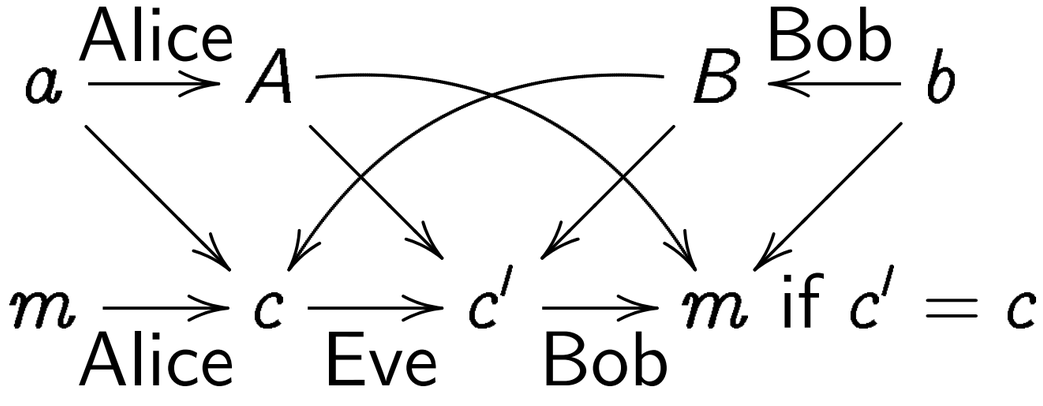
Advanced security goals

Many other security goals
studied in cryptography:
stopping traffic analysis,
securely tallying votes,
searching encrypted data,
and much more.

Public-key encryption (DH form)

Prerequisite:
Alice has a, A; Bob has b, B.
Public knows A and B.
Eve does not know a, b.

Security goals:
Confidentiality and integrity
for any number of messages
exchanged by Alice and Bob.



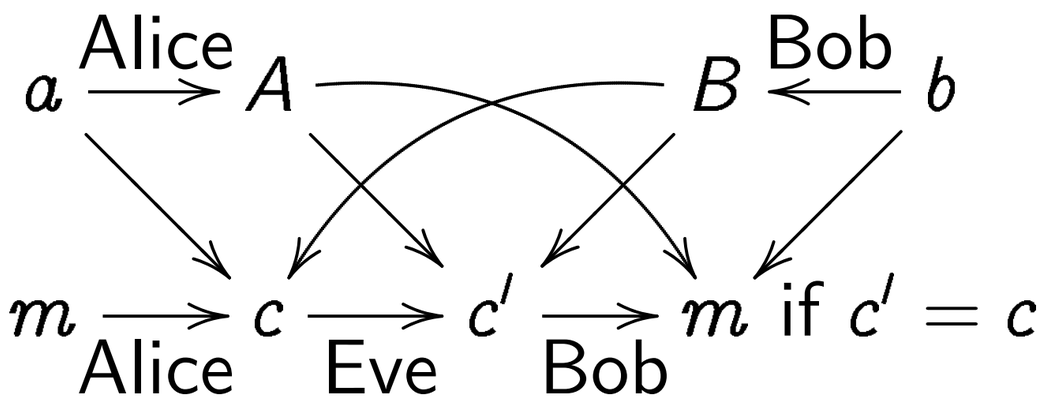
Advanced security goals

Many other security goals
studied in cryptography:
stopping traffic analysis,
securely tallying votes,
searching encrypted data,
and much more.

Public-key encryption (DH form)

Prerequisite:
Alice has a, A; Bob has b, B.
Public knows A and B.
Eve does not know a, b.

Security goals:
Confidentiality and integrity
for any number of messages
exchanged by Alice and Bob.



Advanced security goals

Many other security goals
studied in cryptography:
stopping traffic analysis,
securely tallying votes,
searching encrypted data,
and much more.

But I'll focus on the
most fundamental operations:
secret-key cryptography,
public-key signatures,
public-key encryption.

ey encryption (DH form)

site:

s a, A; Bob has b, B.

nows A and B.

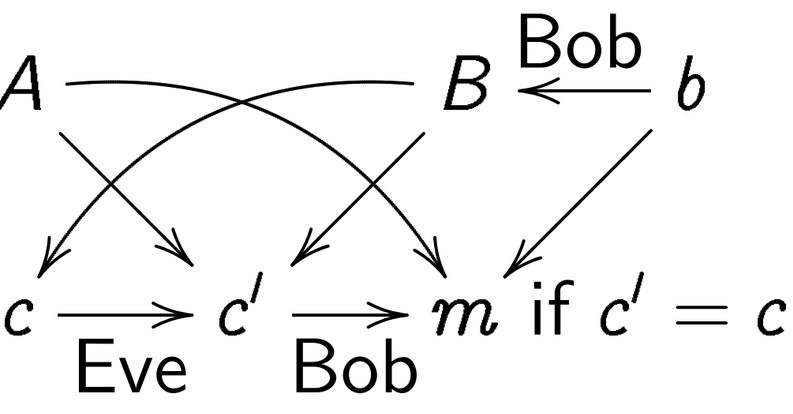
s not know a, b.

goals:

ntiality and integrity

number of messages

ed by Alice and Bob.



Advanced security goals

Many other security goals studied in cryptography: stopping traffic analysis, securely tallying votes, searching encrypted data, and much more.

But I'll focus on the most fundamental operations: secret-key cryptography, public-key signatures, public-key encryption.

The imp

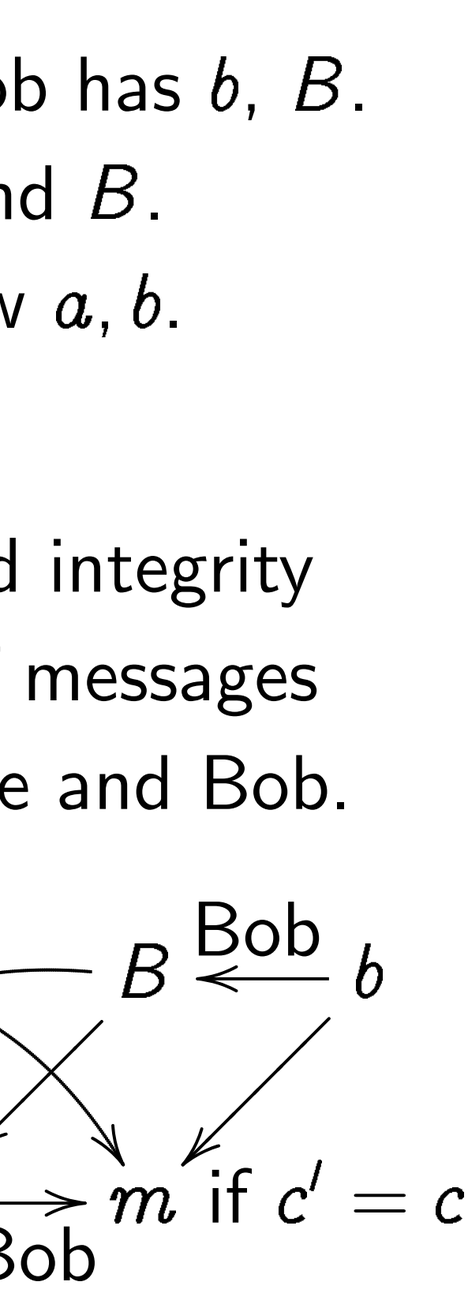
Critical f
attacker

1996 Ko
is broke

tion (DH form)

ob has b, B.
nd B.
v a, b.

d integrity
messages
e and Bob.



Advanced security goals

Many other security goals studied in cryptography: stopping traffic analysis, securely tallying votes, searching encrypted data, and much more.

But I'll focus on the most fundamental operations: secret-key cryptography, public-key signatures, public-key encryption.

The impact of phy

Critical for cryptog
attackers exploit p

1996 Kocher: typi
is broken by side c

orm)

3.

b

= c

Advanced security goals

Many other security goals studied in cryptography: stopping traffic analysis, securely tallying votes, searching encrypted data, and much more.

But I'll focus on the most fundamental operations: secret-key cryptography, public-key signatures, public-key encryption.

The impact of physics

Critical for cryptography: attackers exploit physical rea

1996 Kocher: typical crypto is broken by side channels.

Advanced security goals

Many other security goals
studied in cryptography:
stopping traffic analysis,
securely tallying votes,
searching encrypted data,
and much more.

But I'll focus on the
most fundamental operations:
secret-key cryptography,
public-key signatures,
public-key encryption.

The impact of physics

Critical for cryptography:
attackers exploit physical reality.

1996 Kocher: typical crypto
is broken by side channels.

Advanced security goals

Many other security goals studied in cryptography: stopping traffic analysis, securely tallying votes, searching encrypted data, and much more.

But I'll focus on the most fundamental operations: secret-key cryptography, public-key signatures, public-key encryption.

The impact of physics

Critical for cryptography: attackers exploit physical reality.

1996 Kocher: typical crypto is broken by side channels.

$\Rightarrow$ Hundreds of papers on side-channel defenses.

Advanced security goals

Many other security goals studied in cryptography: stopping traffic analysis, securely tallying votes, searching encrypted data, and much more.

But I'll focus on the most fundamental operations: secret-key cryptography, public-key signatures, public-key encryption.

The impact of physics

Critical for cryptography: attackers exploit physical reality.

1996 Kocher: typical crypto is broken by side channels.

⇒ Hundreds of papers on side-channel defenses.

1994 Shor, 1996 Grover: typical crypto will be broken by large **quantum computers**.

Advanced security goals

Many other security goals studied in cryptography: stopping traffic analysis, securely tallying votes, searching encrypted data, and much more.

But I'll focus on the most fundamental operations: secret-key cryptography, public-key signatures, public-key encryption.

The impact of physics

Critical for cryptography: attackers exploit physical reality.

1996 Kocher: typical crypto is broken by side channels.

⇒ Hundreds of papers on side-channel defenses.

1994 Shor, 1996 Grover: typical crypto will be broken by large **quantum computers**.

⇒ Hundreds of papers on **post-quantum cryptography**.

ed security goals

ther security goals
in cryptography:
g traffic analysis,
tallying votes,
g encrypted data,
ch more.

focus on the
ndamental operations:
ey cryptography,
ey signatures,
ey encryption.

The impact of physics

Critical for cryptography:
attackers exploit physical reality.

1996 Kocher: typical crypto
is broken by side channels.

⇒ Hundreds of papers on
side-channel defenses.

1994 Shor, 1996 Grover:
typical crypto will be broken by
large **quantum computers**.

⇒ Hundreds of papers on
post-quantum cryptography.

Post-qua

$m \xrightarrow[\text{Alice}$

Very eas
long uni

goals

ty goals
raphy:
alysis,
otes,
ed data,

he
operations:
raphy,
res,
ion.

The impact of physics

Critical for cryptography:
attackers exploit physical reality.

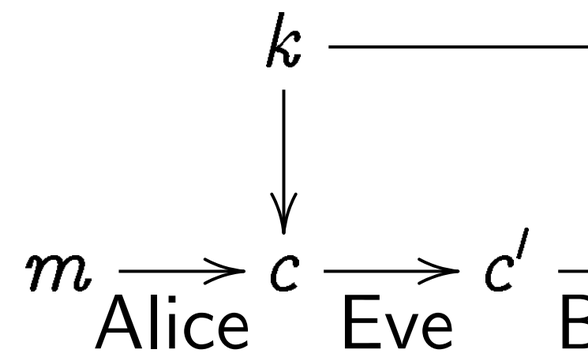
1996 Kocher: typical crypto
is broken by side channels.

⇒ Hundreds of papers on
side-channel defenses.

1994 Shor, 1996 Grover:
typical crypto will be broken by
large **quantum computers**.

⇒ Hundreds of papers on
post-quantum cryptography.

Post-quantum sec



Very easy solution
long uniform rand

s:

The impact of physics

Critical for cryptography:
attackers exploit physical reality.

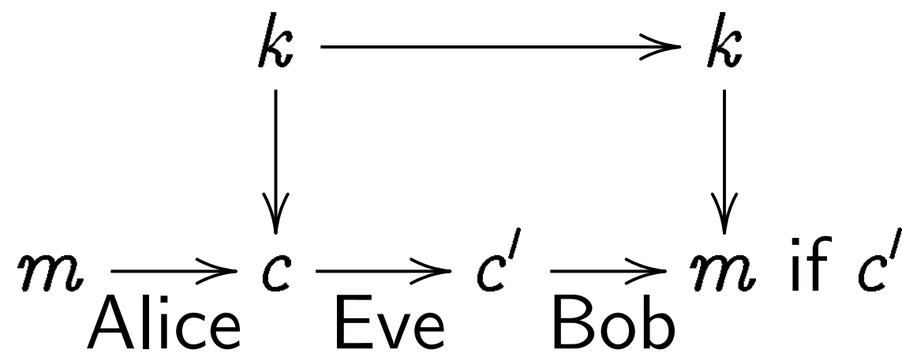
1996 Kocher: typical crypto
is broken by side channels.

$\Rightarrow$ Hundreds of papers on
side-channel defenses.

1994 Shor, 1996 Grover:
typical crypto will be broken by
large **quantum computers**.

$\Rightarrow$ Hundreds of papers on
post-quantum cryptography.

Post-quantum secret-key cry



Very easy solutions if k is
long uniform random string.

The impact of physics

Critical for cryptography:
attackers exploit physical reality.

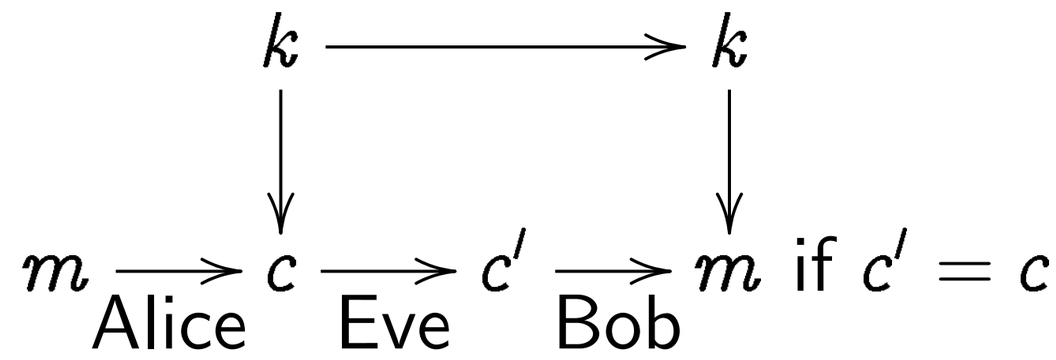
1996 Kocher: typical crypto
is broken by side channels.

$\Rightarrow$ Hundreds of papers on
side-channel defenses.

1994 Shor, 1996 Grover:
typical crypto will be broken by
large **quantum computers**.

$\Rightarrow$ Hundreds of papers on
post-quantum cryptography.

Post-quantum secret-key crypto



Very easy solutions if k is
long uniform random string.

The impact of physics

Critical for cryptography:
attackers exploit physical reality.

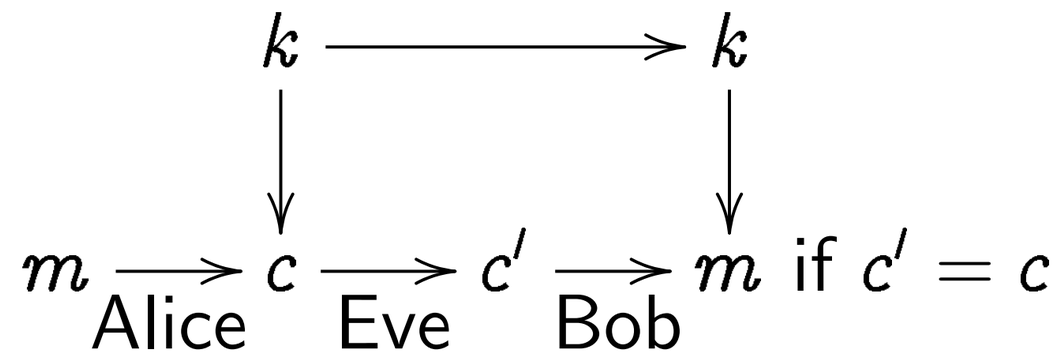
1996 Kocher: typical crypto
is broken by side channels.

$\Rightarrow$ Hundreds of papers on
side-channel defenses.

1994 Shor, 1996 Grover:
typical crypto will be broken by
large **quantum computers**.

$\Rightarrow$ Hundreds of papers on
post-quantum cryptography.

Post-quantum secret-key crypto



Very easy solutions if k is
long uniform random string.

Already standardized method
to expand short k into string
indistinguishable from long k:
1998 Daemen–Rijmen "Rijndael"
cipher ("AES") using 256-bit key.
Security analyzed in papers by
dozens of cryptanalysts.

pact of physics

for cryptography:
s exploit physical reality.

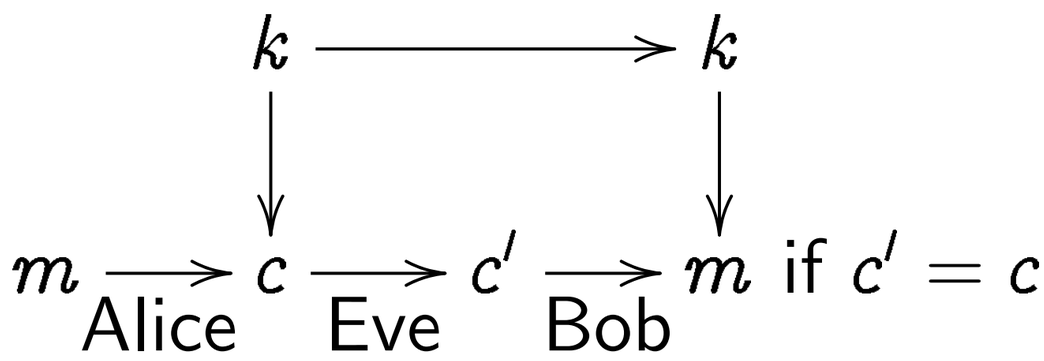
ocher: typical crypto
n by side channels.

lreds of papers on
nnel defenses.

or, 1996 Grover:
crypto will be broken by
antum computers.

lreds of papers on
antum cryptography.

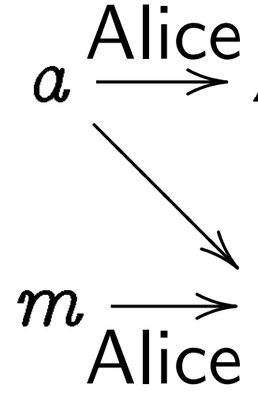
Post-quantum secret-key crypto



Very easy solutions if k is
long uniform random string.

Already standardized method
to expand short k into string
indistinguishable from long k:
1998 Daemen–Rijmen "Rijndael"
cipher ("AES") using 256-bit key.
Security analyzed in papers by
dozens of cryptanalysts.

Post-qua



Safe, rea
1979 Me
public-ke

Modern
are guar
as the u

Reasona
Keccak

ysics

graphy:
physical reality.

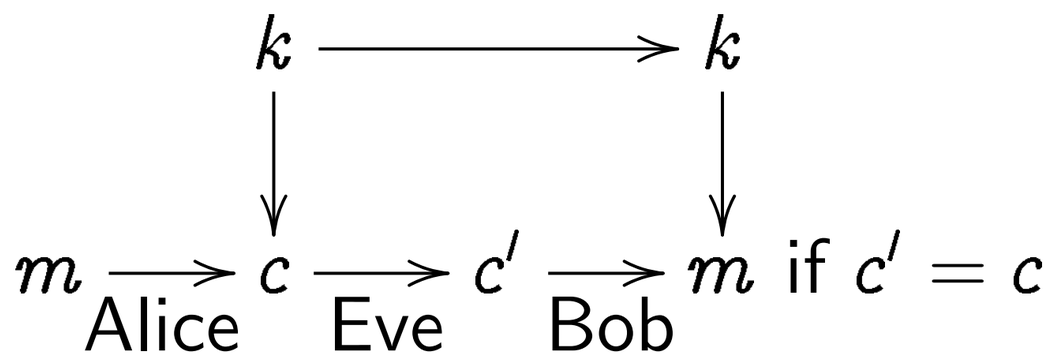
cal crypto
channels.

apers on
ses.

Grover:
be broken by
omputers.

apers on
yptography.

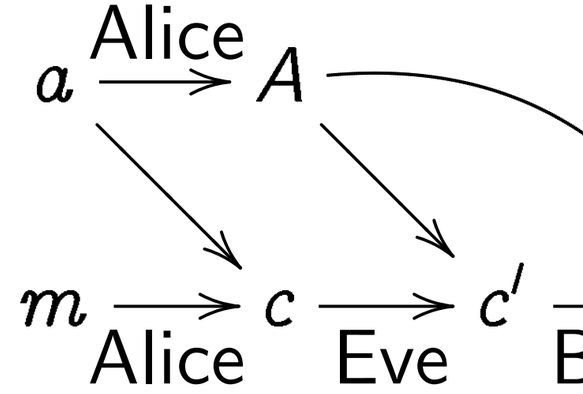
Post-quantum secret-key crypto



Very easy solutions if k is long uniform random string.

Already standardized method to expand short k into string indistinguishable from long k: 1998 Daemen–Rijmen "Rijndael" cipher ("AES") using 256-bit key. Security analyzed in papers by dozens of cryptanalysts.

Post-quantum pub



Safe, ready for sta
1979 Merkle hash-
public-key signatu

Modern variants o
are guaranteed to
as the underlying

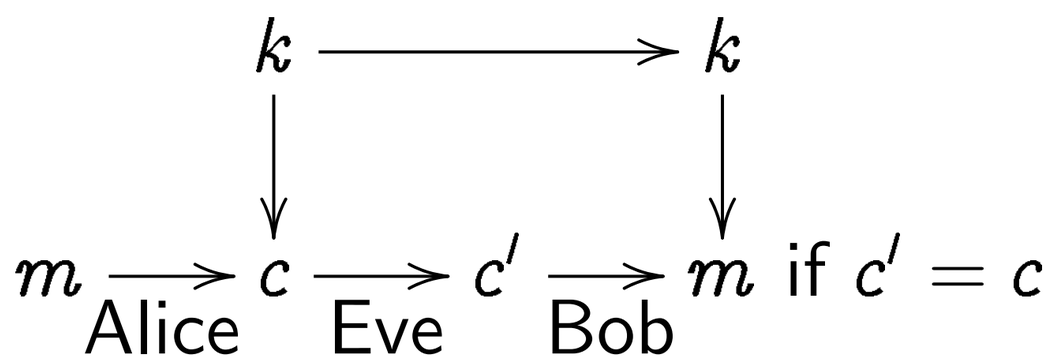
Reasonable choice
Keccak with 576-b

ality.

by

hy.

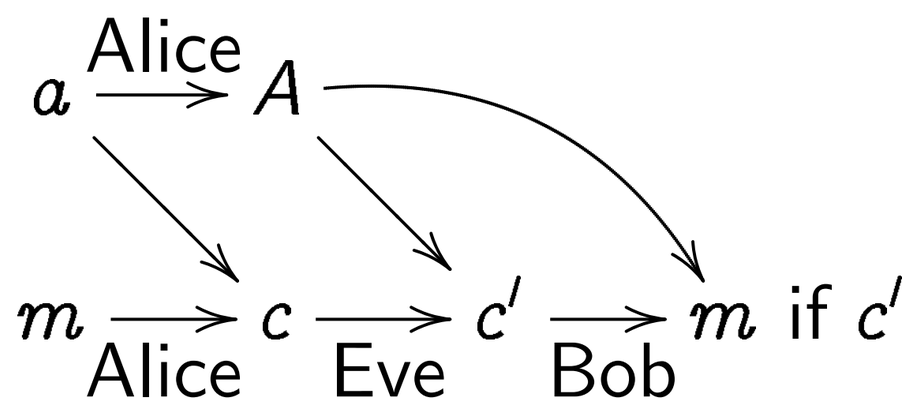
Post-quantum secret-key crypto



Very easy solutions if k is long uniform random string.

Already standardized method to expand short k into string indistinguishable from long k: 1998 Daemen–Rijmen "Rijndael" cipher ("AES") using 256-bit key. Security analyzed in papers by dozens of cryptanalysts.

Post-quantum public-key sig



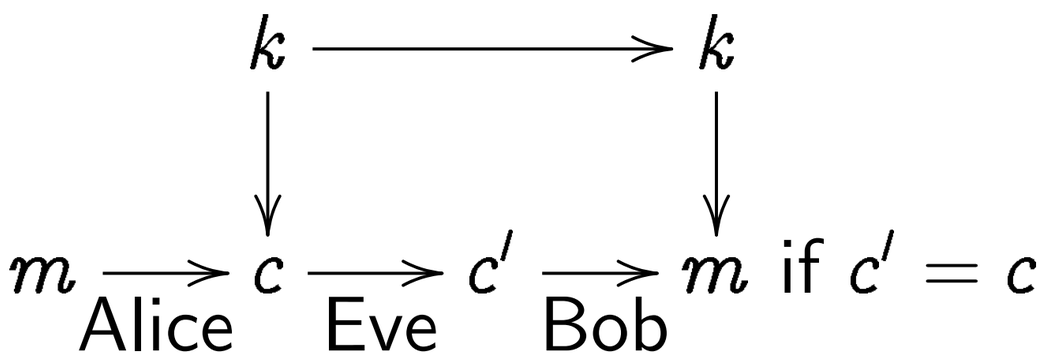
Safe, ready for standardizati

1979 Merkle hash-tree public-key signature system.

Modern variants of system are guaranteed to be as secu as the underlying hash funct

Reasonable choice of functio Keccak with 576-bit capacit

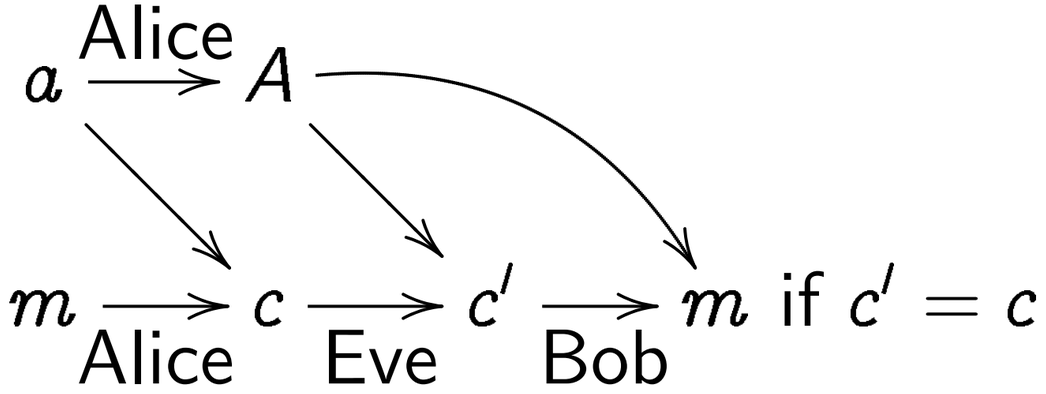
Post-quantum secret-key crypto



Very easy solutions if k is long uniform random string.

Already standardized method to expand short k into string indistinguishable from long k: 1998 Daemen–Rijmen "Rijndael" cipher ("AES") using 256-bit key. Security analyzed in papers by dozens of cryptanalysts.

Post-quantum public-key signatures

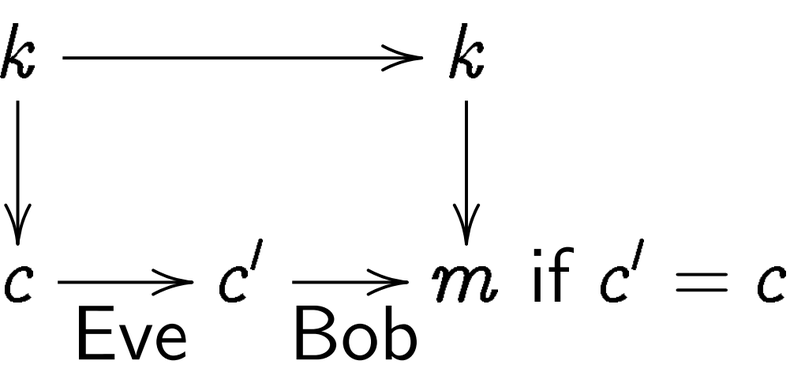


Safe, ready for standardization: 1979 Merkle hash-tree public-key signature system.

Modern variants of system are guaranteed to be as secure as the underlying hash function.

Reasonable choice of function: Keccak with 576-bit capacity.

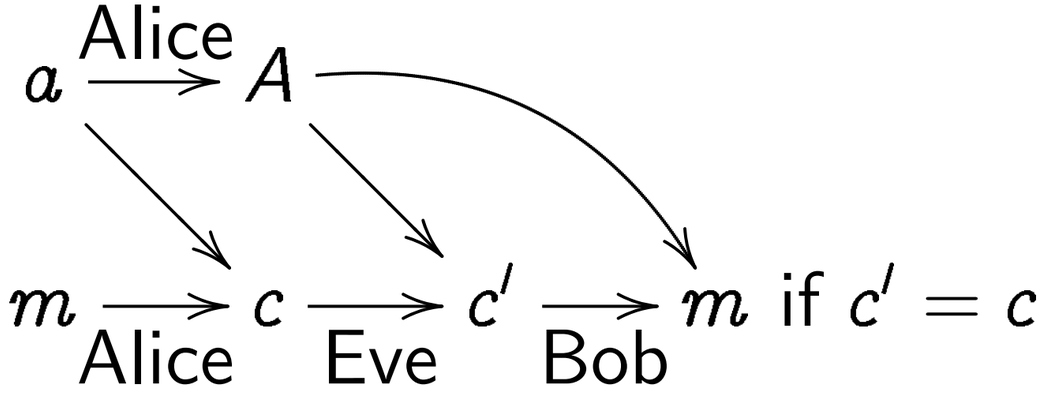
antum secret-key crypto



sy solutions if k is
form random string.

standardized method
nd short k into string
guishable from long k:
hemen–Rijmen "Rijndael"
"AES") using 256-bit key.
analyzed in papers by
of cryptanalysts.

Post-quantum public-key signatures

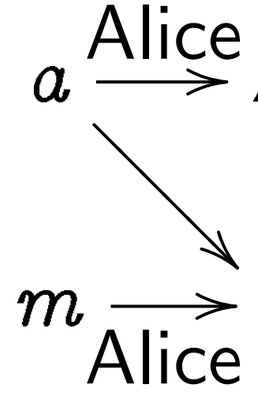


Safe, ready for standardization:
1979 Merkle hash-tree
public-key signature system.

Modern variants of system
are guaranteed to be as secure
as the underlying hash function.

Reasonable choice of function:
Keccak with 576-bit capacity.

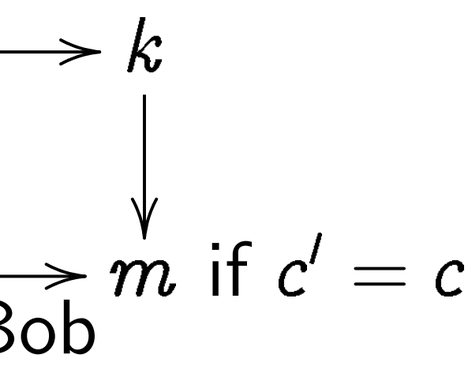
Post-qua



Safe, rea
1978 Mc
using bir

Main sec
1981, 19
1989, 19
1993, 19
1998, 20
2010, 20

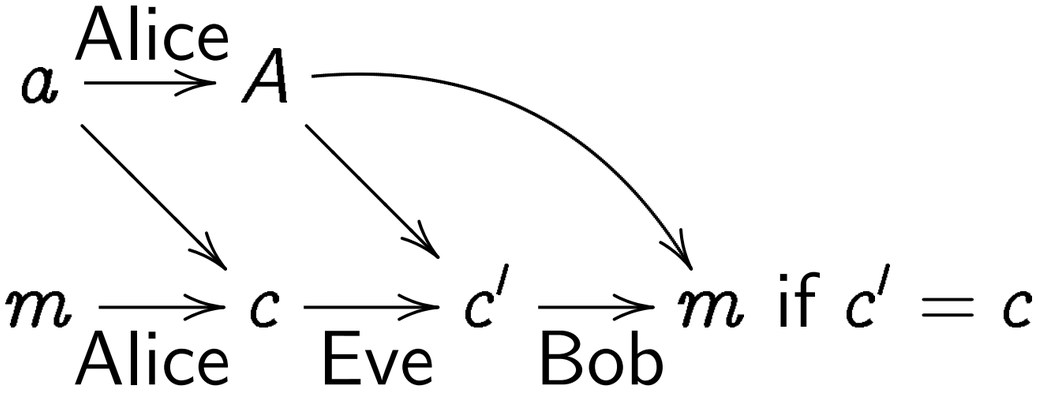
ret-key crypto



s if k is
om string.

zed method
into string
rom long k:
men "Rijndael"
sing 256-bit key.
in papers by
alysts.

Post-quantum public-key signatures

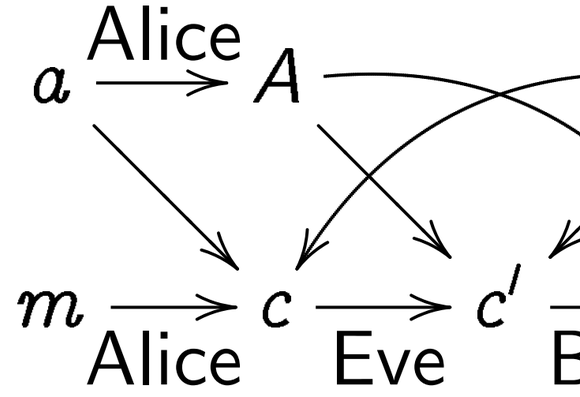


Safe, ready for standardization:
1979 Merkle hash-tree
public-key signature system.

Modern variants of system
are guaranteed to be as secure
as the underlying hash function.

Reasonable choice of function:
Keccak with 576-bit capacity.

Post-quantum pub



Safe, ready for sta
1978 McEliece enc
using binary Gopp

Main security-anal
1981, 1988, 1988,
1989, 1990, 1990,
1993, 1993, 1994,
1998, 2008, 2009,
2010, 2011, 2011,

ypto

$= c$

d

g

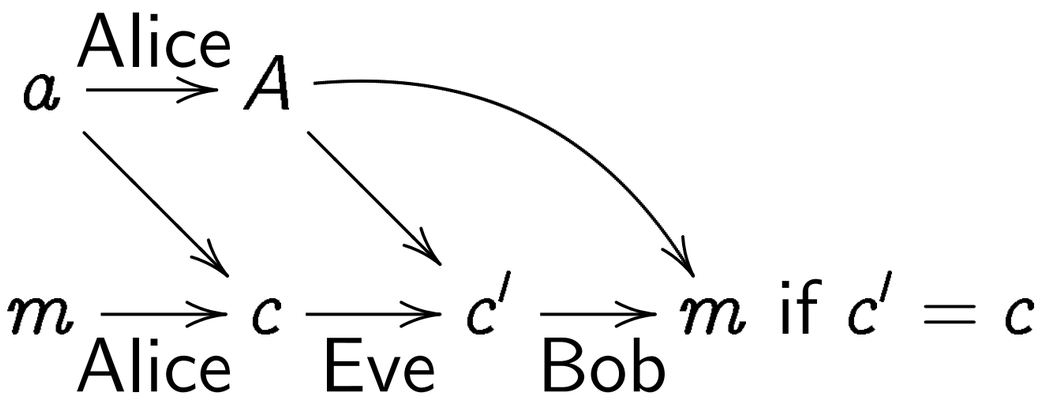
k:

dael”

it key.

by

Post-quantum public-key signatures

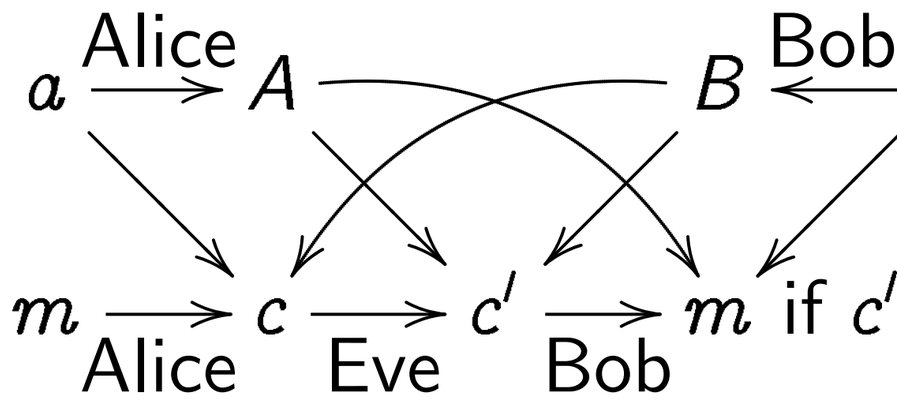


Safe, ready for standardization:
1979 Merkle hash-tree
public-key signature system.

Modern variants of system
are guaranteed to be as secure
as the underlying hash function.

Reasonable choice of function:
Keccak with 576-bit capacity.

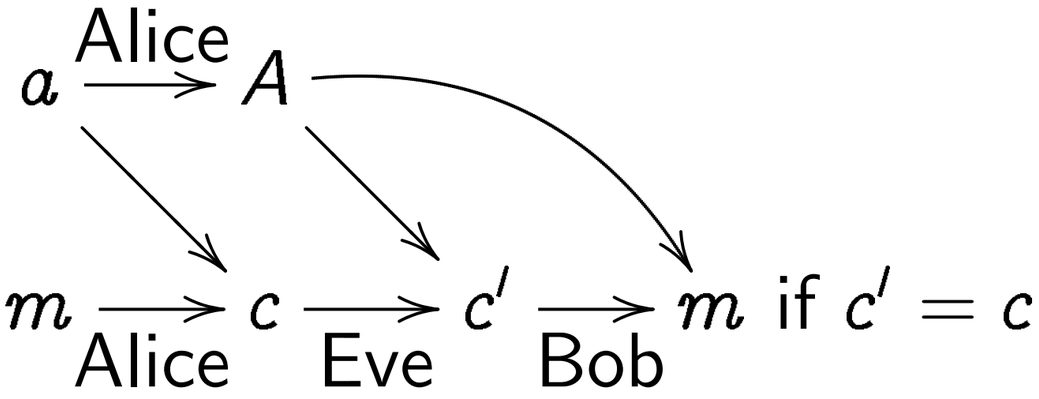
Post-quantum public-key en



Safe, ready for standardizati
1978 McEliece encryption
using binary Goppa codes.

Main security-analysis paper
1981, 1988, 1988, 1989, 198
1989, 1990, 1990, 1991, 199
1993, 1993, 1994, 1994, 199
1998, 2008, 2009, 2009, 200
2010, 2011, 2011, 2012, 201

Post-quantum public-key signatures

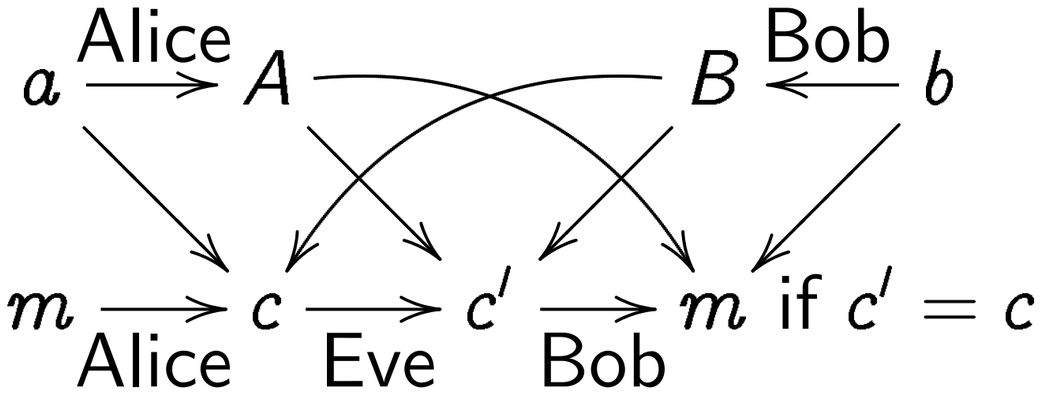


Safe, ready for standardization:
1979 Merkle hash-tree
public-key signature system.

Modern variants of system
are guaranteed to be as secure
as the underlying hash function.

Reasonable choice of function:
Keccak with 576-bit capacity.

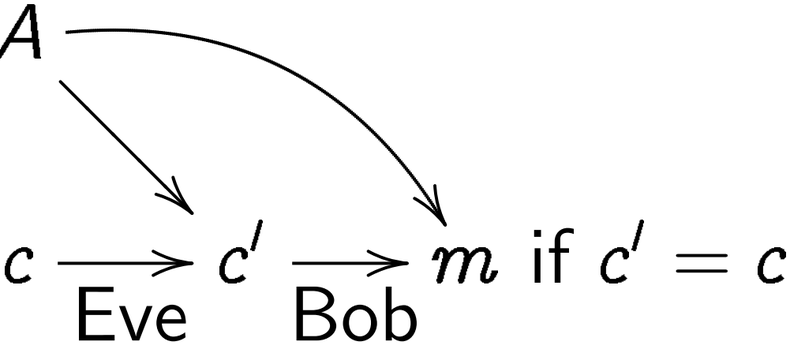
Post-quantum public-key encryption



Safe, ready for standardization:
1978 McEliece encryption
using binary Goppa codes.

Main security-analysis papers:
1981, 1988, 1988, 1989, 1989,
1989, 1990, 1990, 1991, 1991,
1993, 1993, 1994, 1994, 1998,
1998, 2008, 2009, 2009, 2009,
2010, 2011, 2011, 2012, 2013.

antum public-key signatures

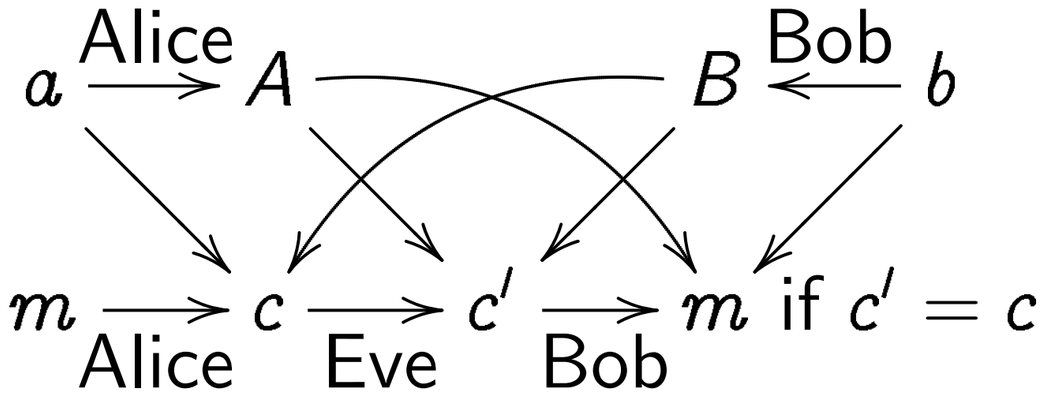


ady for standardization:
erkle hash-tree
ey signature system.

variants of system
anteed to be as secure
nderlying hash function.

ble choice of function:
with 576-bit capacity.

Post-quantum public-key encryption



Safe, ready for standardization:
1978 McEliece encryption
using binary Goppa codes.

Main security-analysis papers:
1981, 1988, 1988, 1989, 1989,
1989, 1990, 1990, 1991, 1991,
1993, 1993, 1994, 1994, 1998,
1998, 2008, 2009, 2009, 2009,
2010, 2011, 2011, 2012, 2013.

Example

Better s
smaller,
against

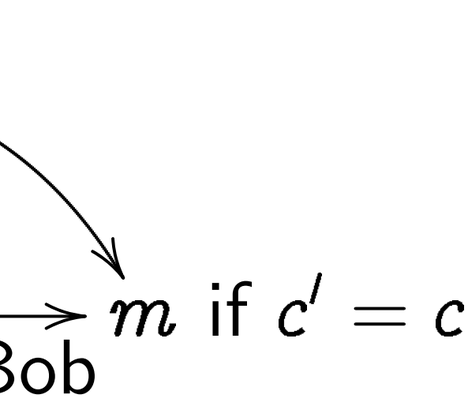
Lattice-b
similar i
maybe a
security

Signatur

Multivar
very sho
maybe t

http://

blic-key signatures

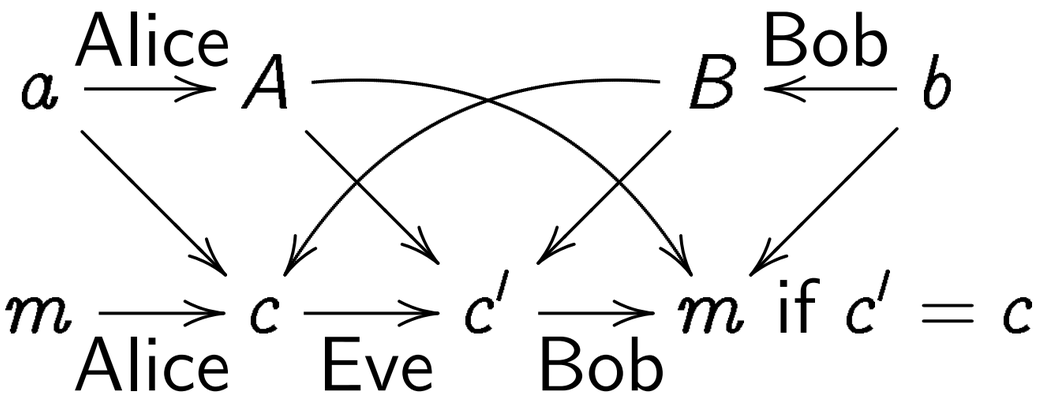


ndardization:
-tree
re system.

f system
be as secure
hash function.

of function:
bit capacity.

Post-quantum public-key encryption



Safe, ready for standardization:
1978 McEliece encryption
using binary Goppa codes.

Main security-analysis papers:
1981, 1988, 1988, 1989, 1989,
1989, 1990, 1990, 1991, 1991,
1993, 1993, 1994, 1994, 1998,
1998, 2008, 2009, 2009, 2009,
2010, 2011, 2011, 2012, 2013.

Examples of post-

Better secret-key
smaller, faster, eas
against side chann

Lattice-based cryp
similar idea to cod
maybe allows sma
security analysis n

Signatures using c

Multivariate quadr
very short signatur
maybe tolerable fo

http://pqcrypto

gnatures

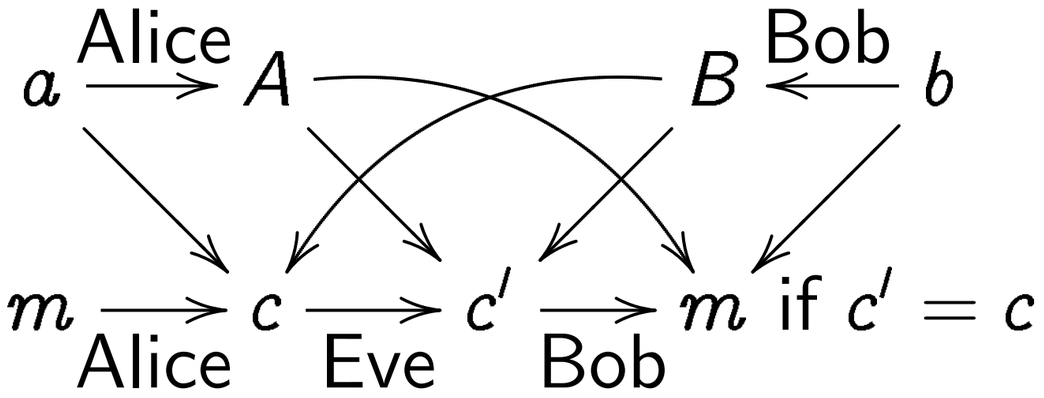
$= c$

on:

ure
tion.

on:
y.

Post-quantum public-key encryption



Safe, ready for standardization:
1978 McEliece encryption
using binary Goppa codes.

Main security-analysis papers:
1981, 1988, 1988, 1989, 1989,
1989, 1990, 1990, 1991, 1991,
1993, 1993, 1994, 1994, 1998,
1998, 2008, 2009, 2009, 2009,
2010, 2011, 2011, 2012, 2013.

Examples of post-quantum

Better secret-key crypto:
smaller, faster, easier to pro
against side channels, etc.

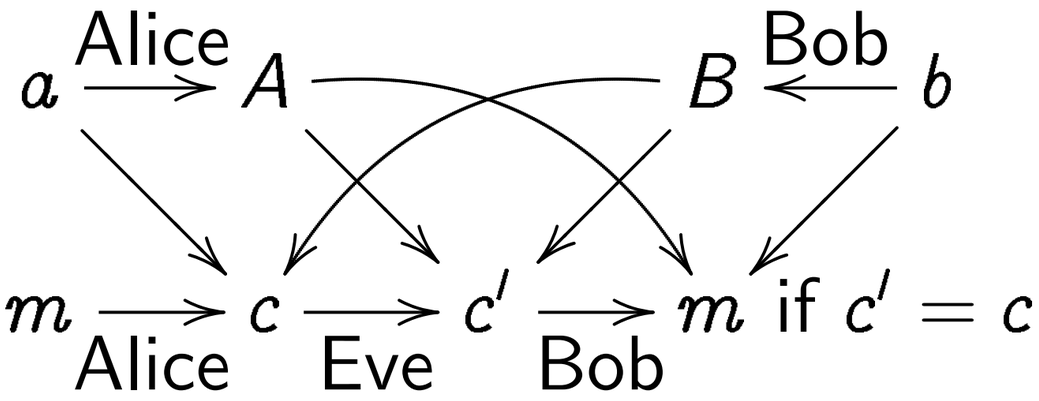
Lattice-based cryptography:
similar idea to code-based;
maybe allows smaller keys;
security analysis not as matu

Signatures using codes/latti

Multivariate quadratics:
very short signatures;
maybe tolerable for encrypti

http://pqcrypto.org

Post-quantum public-key encryption



Safe, ready for standardization:
1978 McEliece encryption
using binary Goppa codes.

Main security-analysis papers:
1981, 1988, 1988, 1989, 1989,
1989, 1990, 1990, 1991, 1991,
1993, 1993, 1994, 1994, 1998,
1998, 2008, 2009, 2009, 2009,
2010, 2011, 2011, 2012, 2013.

Examples of post-quantum research

Better secret-key crypto:
smaller, faster, easier to protect
against side channels, etc.

Lattice-based cryptography:
similar idea to code-based;
maybe allows smaller keys;
security analysis not as mature.

Signatures using codes/lattices.

Multivariate quadratics:
very short signatures;
maybe tolerable for encryption.

http://pqcrypto.org