Anonymous, Robust Post-Quantum Public Key Encryption

Varun Maram
Applied Cryptography Group
ETH Zurich

Joint work with Paul Grubbs and Kenneth G. Paterson

[Full version of paper: *https://eprint.iacr.org/2021/708.pdf*]

What is “Cryptography”?

What is “Cryptography”?

From **Handbook of Applied Cryptography** (http://cacr.uwaterloo.ca/hac)**:**

Definition (Cryptography)

Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication.

What is “Cryptography”?

From **Handbook of Applied Cryptography** (http://cacr.uwaterloo.ca/hac)**:**

Definition (Cryptography)

Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication.

- Historically, *cryptography* is only associated with *encryption/confidentiality*.

What is “Cryptography”?

From **Handbook of Applied Cryptography** (http://cacr.uwaterloo.ca/hac)**:**

Definition (Cryptography)

Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication.

- Historically, *cryptography* is only associated with *encryption/confidentiality*.
- But it is much more than that!

Applications of Cryptography

Applications of Cryptography

- e-commerce

Applications of Cryptography

- e-commerce
- social media

Applications of Cryptography

- e-commerce
- social media
- secure messaging (WhatsApp, Signal, Telegram)

Applications of Cryptography

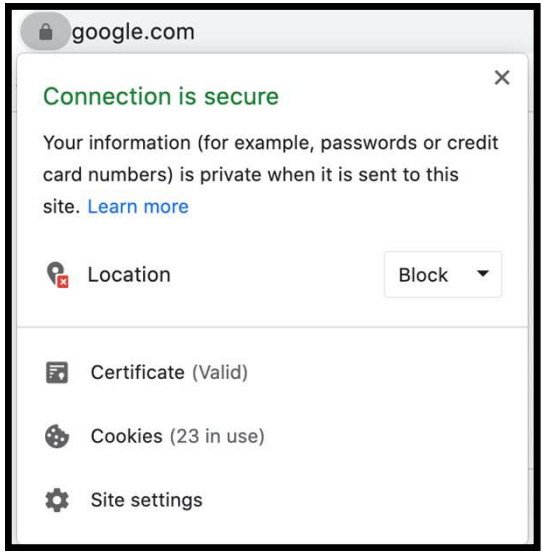
- e-commerce
- social media
- secure messaging (WhatsApp, Signal, Telegram)
- online personal banking
- debit/credit card payments
- interbank payments
- mobile telephony
- VPN/remote access
- video conferencing
- secure cloud data storage
- privacy-preserving contact tracing (GAEN, DP3T)
- Cryptocurrencies
- military and government communications systems

Applications of Cryptography

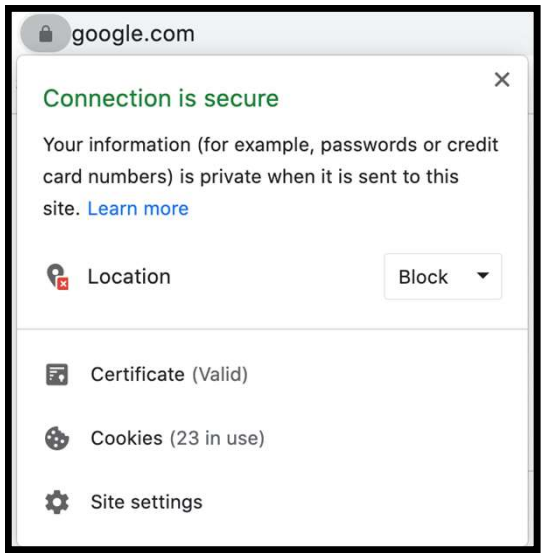
- e-commerce
- social media
- secure messaging (WhatsApp, Signal, Telegram)
- online personal banking
- debit/credit card payments
- interbank payments
- mobile telephony
- VPN/remote access
- video conferencing
- secure cloud data storage
- privacy-preserving contact tracing (GAEN, DP3T)
- Cryptocurrencies
- military and government communications systems

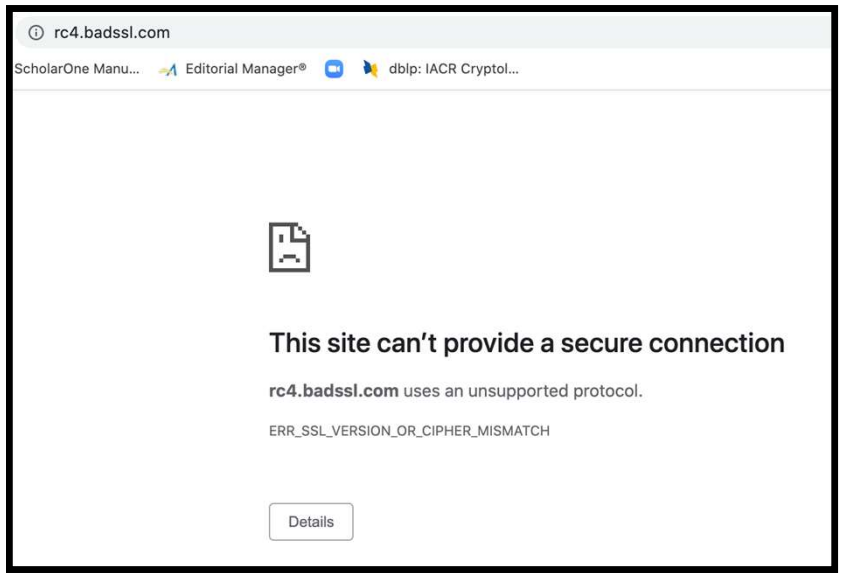
… and more!

Under the Hood

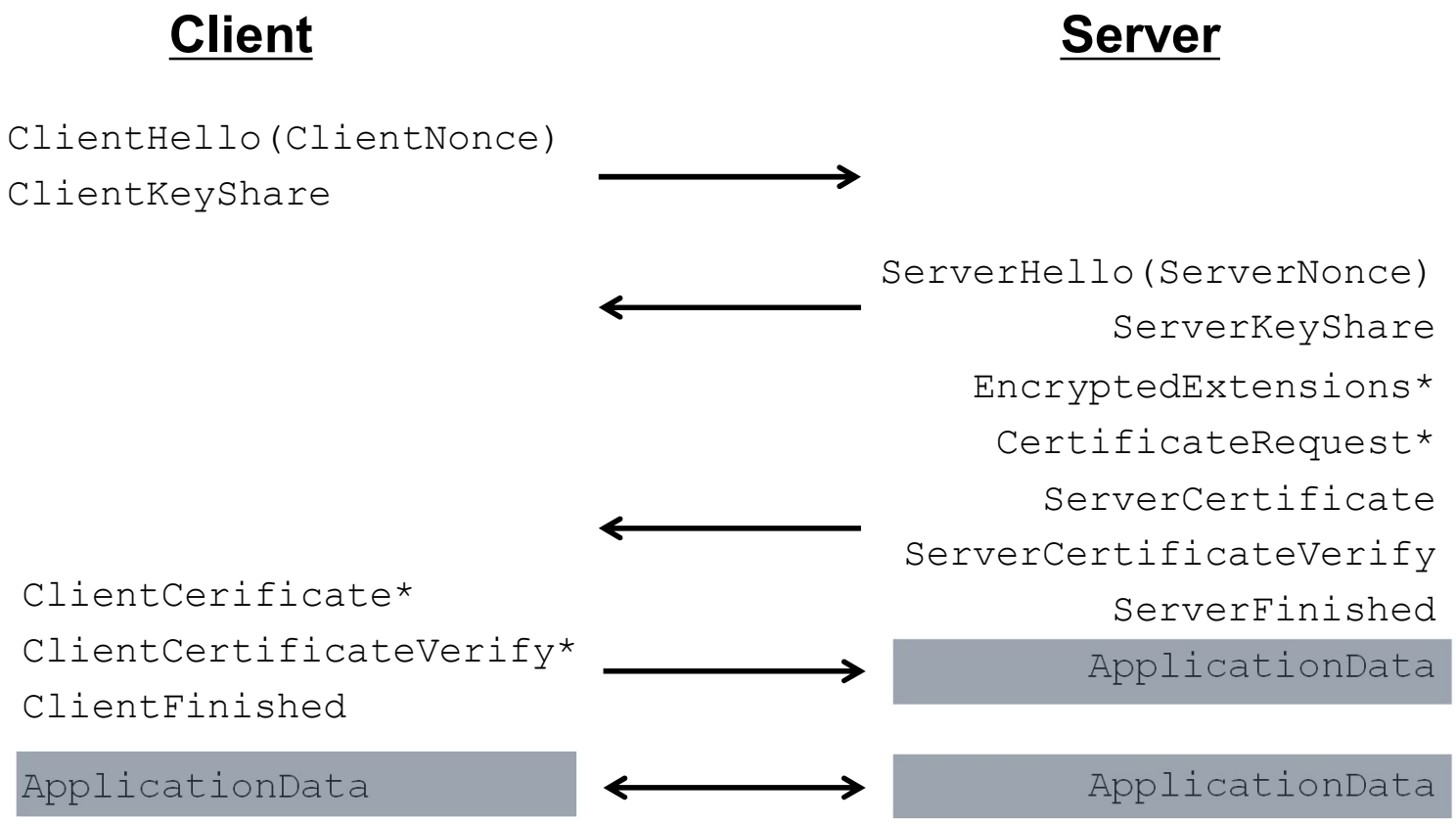


Under the Hood

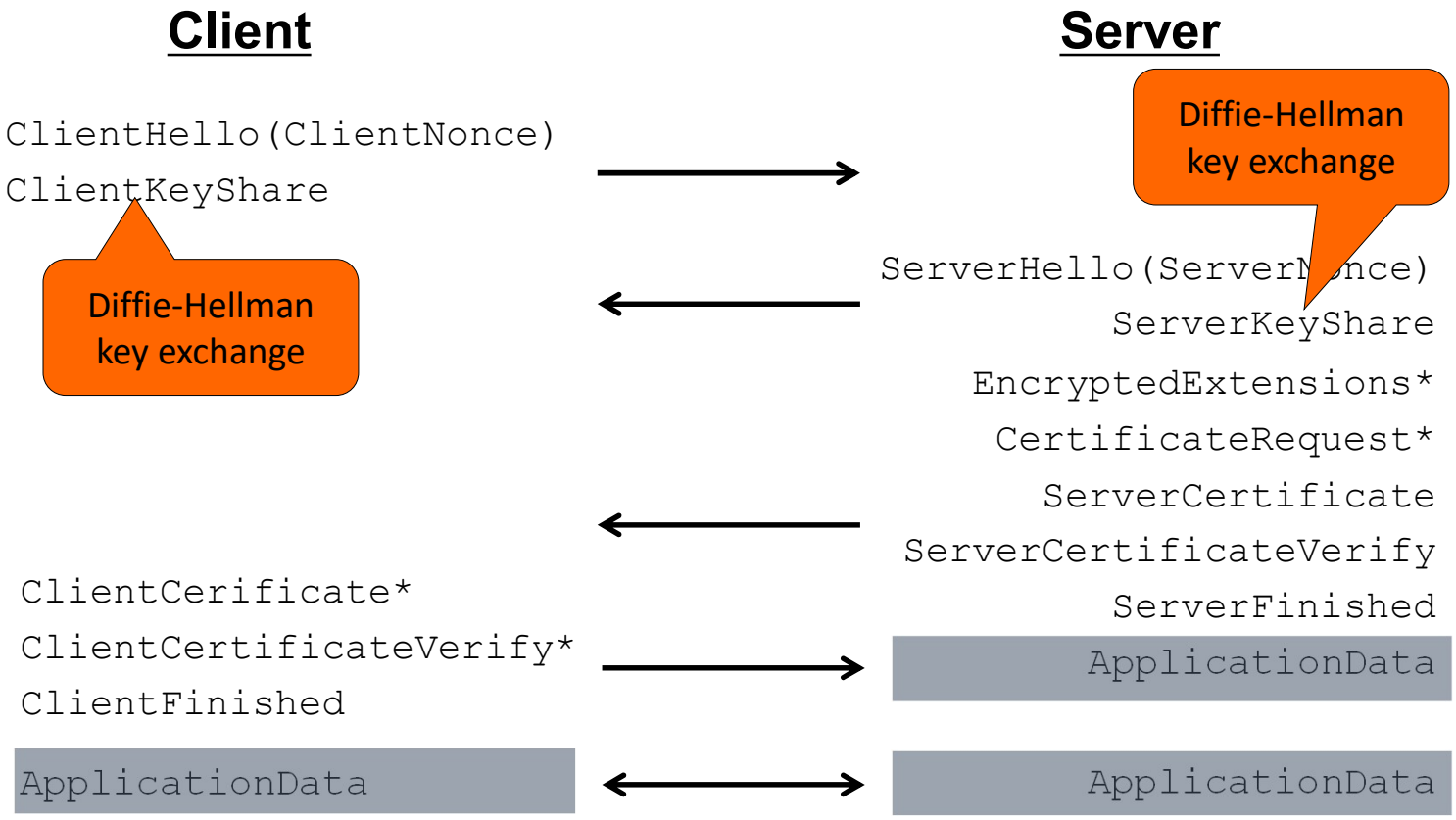




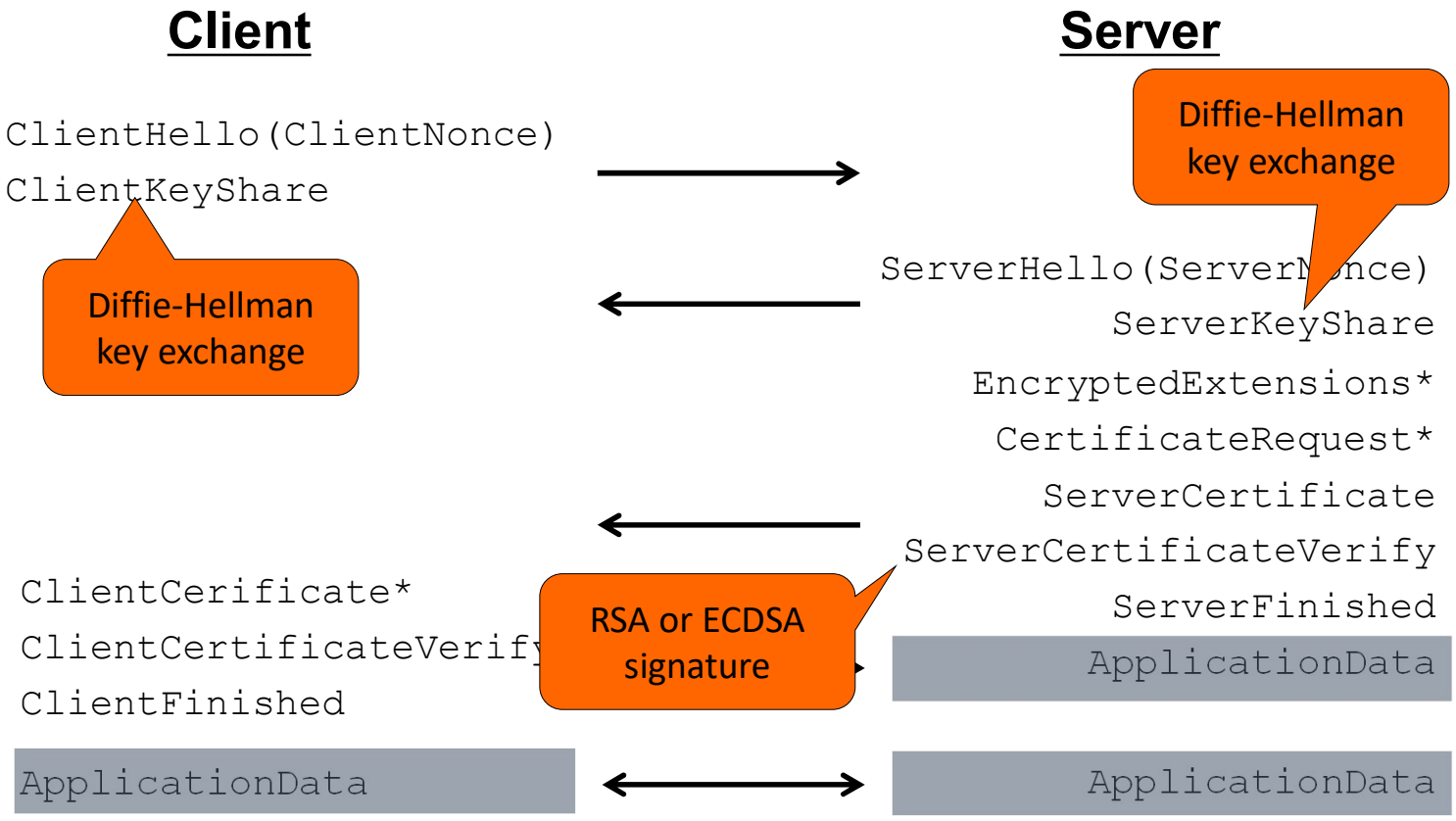
Under the Hood – the TLS 1.3 Handshake



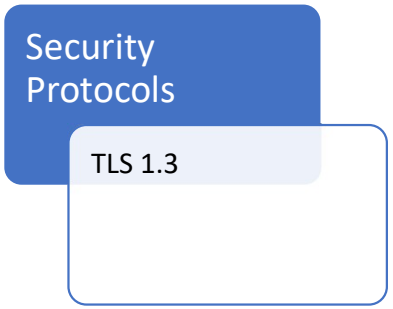
Under the Hood – the TLS 1.3 Handshake



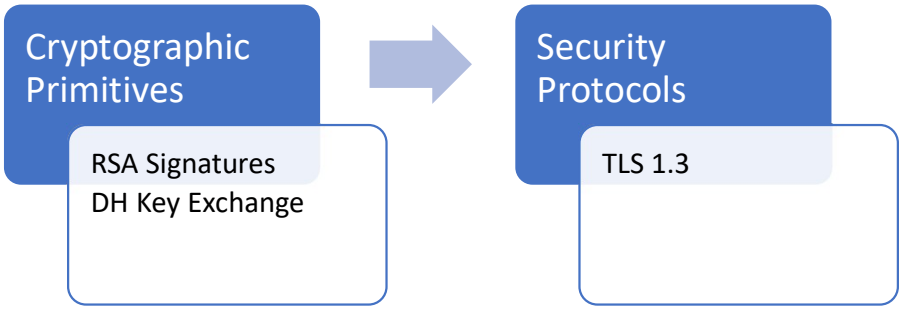
Under the Hood – the TLS 1.3 Handshake



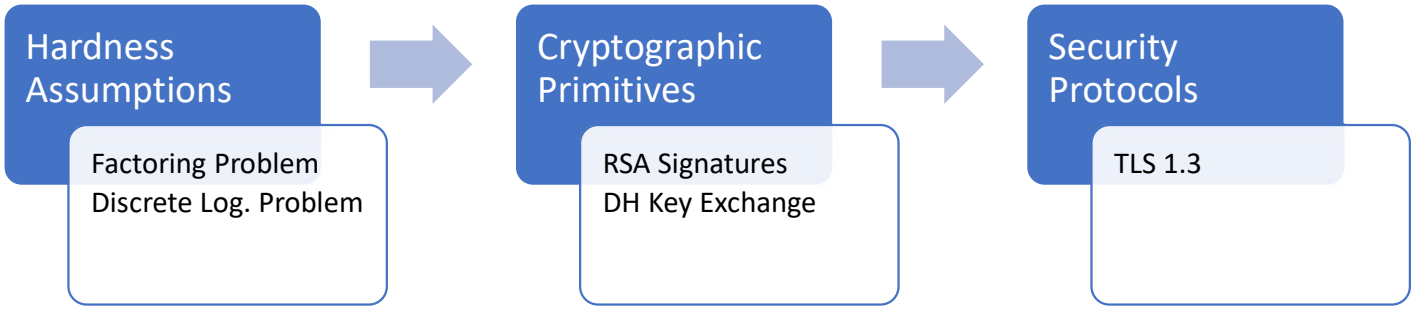
Bird’s-eye View



Bird’s-eye View

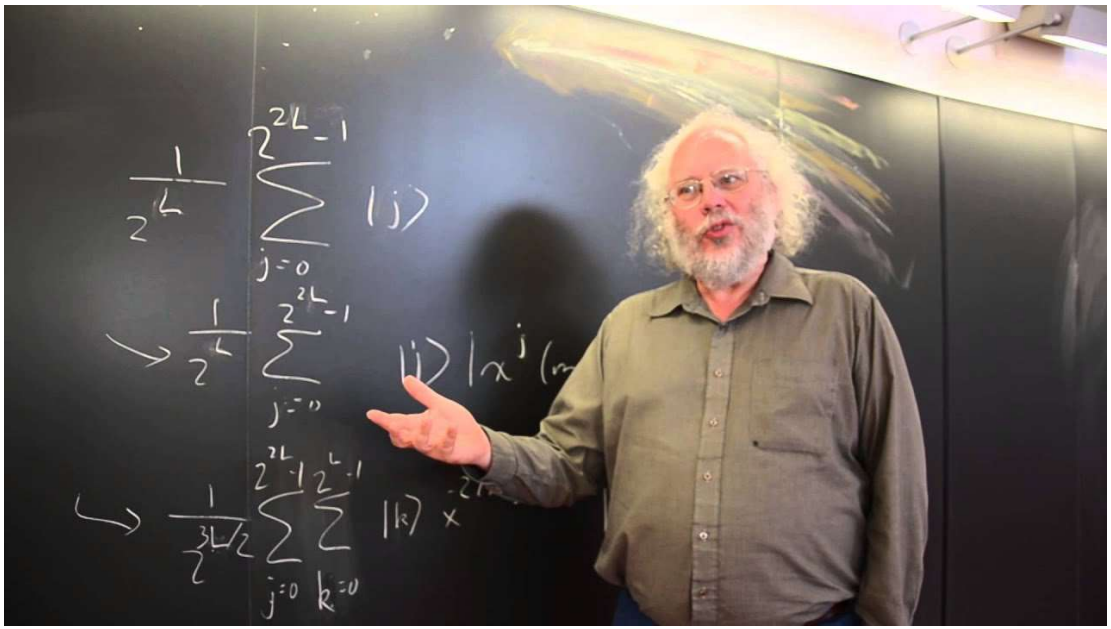


Bird’s-eye View



Enter Quantum Computing

Enter Quantum Computing



Enter Quantum Computing

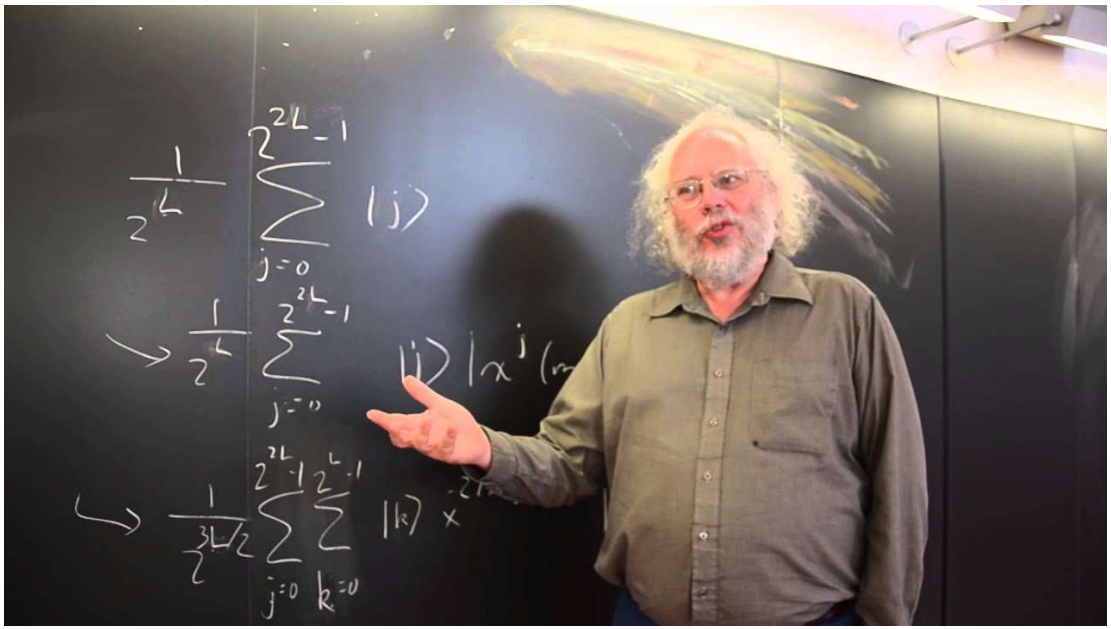
Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

Peter W. Shor†

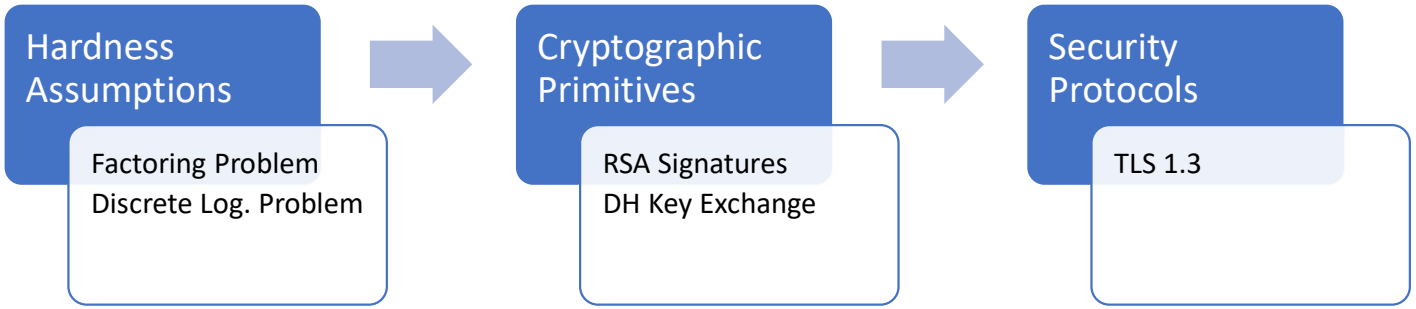
Abstract

A digital computer is generally believed to be an efficient universal computing device; that is, it is believed able to simulate any physical computing device with an increase in computation time by at most a polynomial factor. This may not be true when quantum mechanics is taken into consideration. This paper considers factoring integers and finding discrete logarithms, two problems which are generally thought to be hard on a classical computer and which have been used as the basis of several proposed cryptosystems. Efficient randomized algorithms are given for these two problems on a hypothetical quantum computer. These algorithms take a number of steps polynomial in the input size, e.g., the number of digits of the integer to be factored.

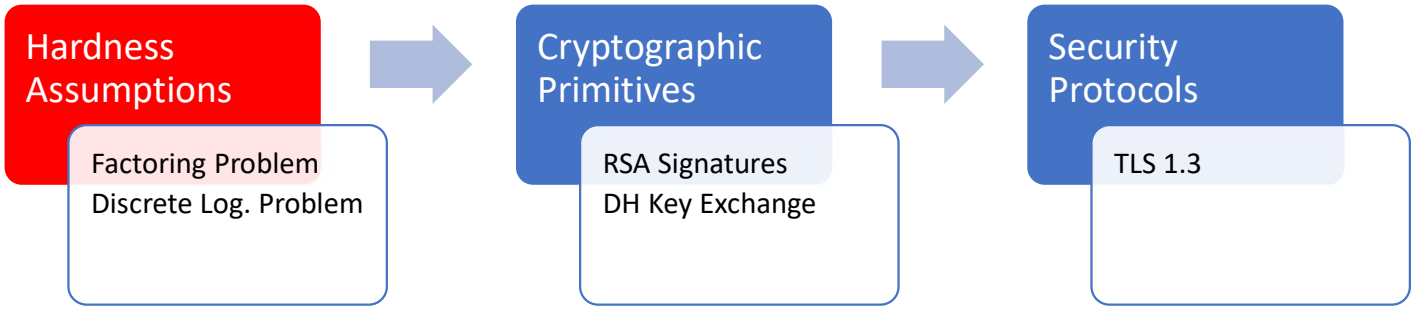
[FOCS'94]



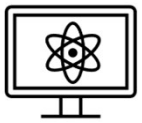
Enter Quantum Computing

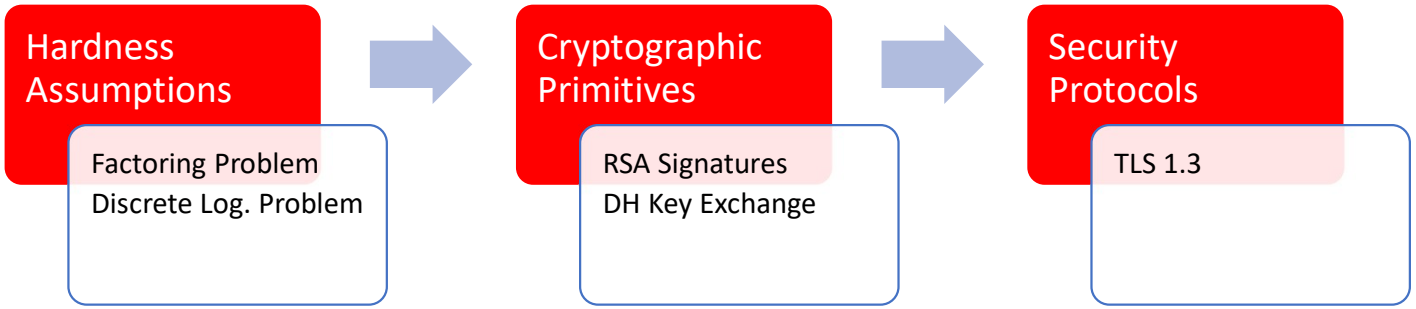


Enter Quantum Computing

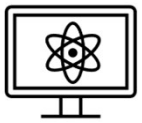


Enter Quantum Computing





Enter Quantum Computing



Hardness Assumptions

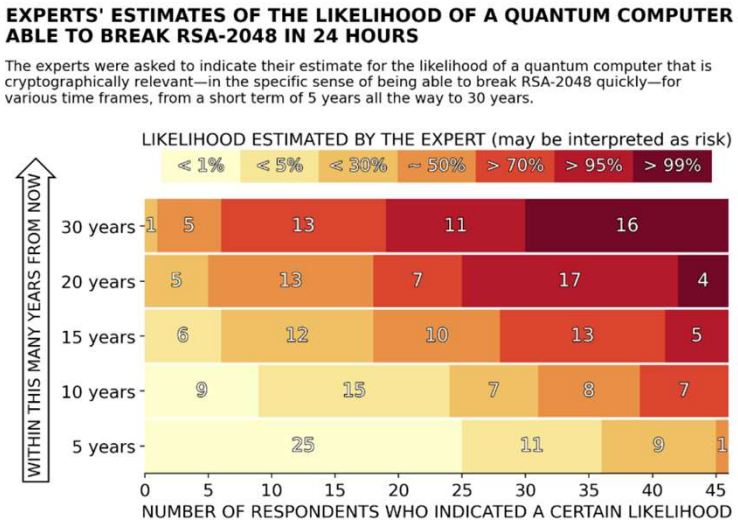
Factoring Problem
Discrete Log. Problem

Cryptographic Primitives

RSA Signatures
DH Key Exchange

Security Protocols

TLS 1.3



[Image: Global Risk Institute, 2021 Quantum Threat Timeline Report]

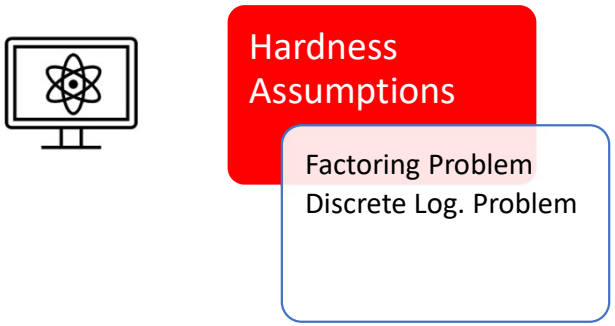
Post-Quantum Cryptography (PQC)

Post-Quantum Cryptography (PQC)

Conventional public-key cryptosystems that resist known quantum algorithms.

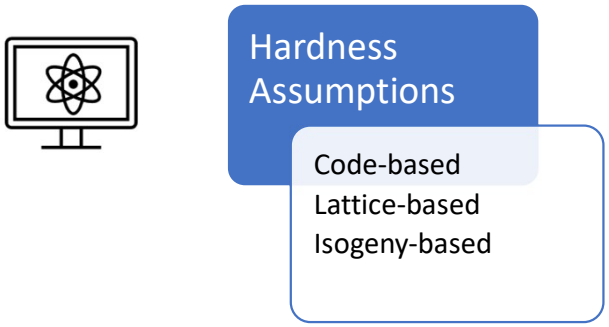
Post-Quantum Cryptography (PQC)

Conventional public-key cryptosystems that resist known quantum algorithms.



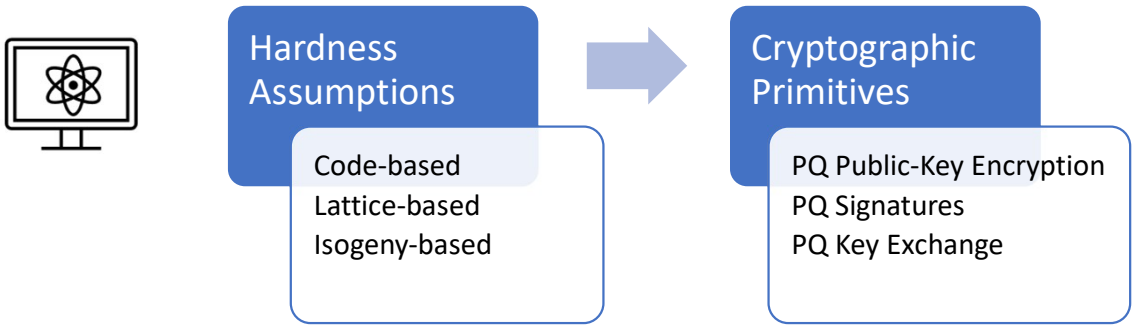
Post-Quantum Cryptography (PQC)

Conventional public-key cryptosystems that resist known quantum algorithms.



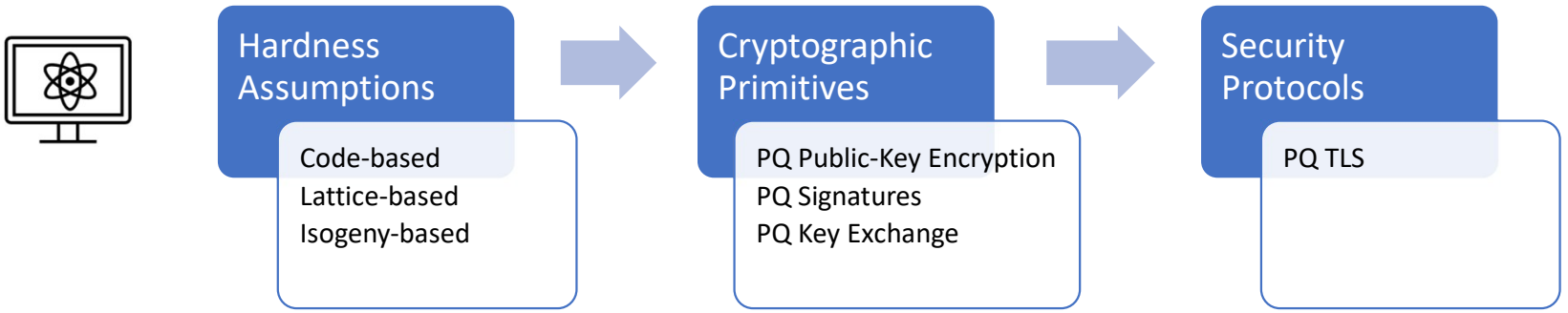
Post-Quantum Cryptography (PQC)

Conventional public-key cryptosystems that resist known quantum algorithms.



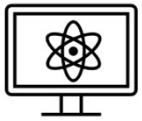
Post-Quantum Cryptography (PQC)

Conventional public-key cryptosystems that resist known quantum algorithms.



Post-Quantum Cryptography (PQC)

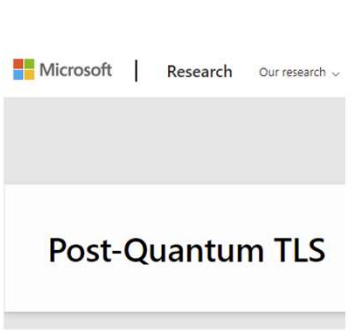
Conventional public-key cryptosystems that resist known quantum algorithms.

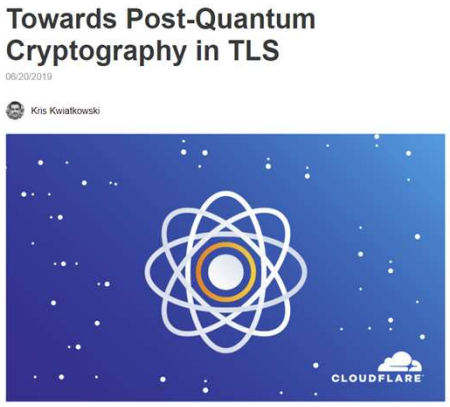


Hardness Assumptions
- Code-based
- Lattice-based
- Isogeny-based

Cryptographic Primitives
- PQ Public-Key Encryption
- PQ Signatures
- PQ Key Exchange

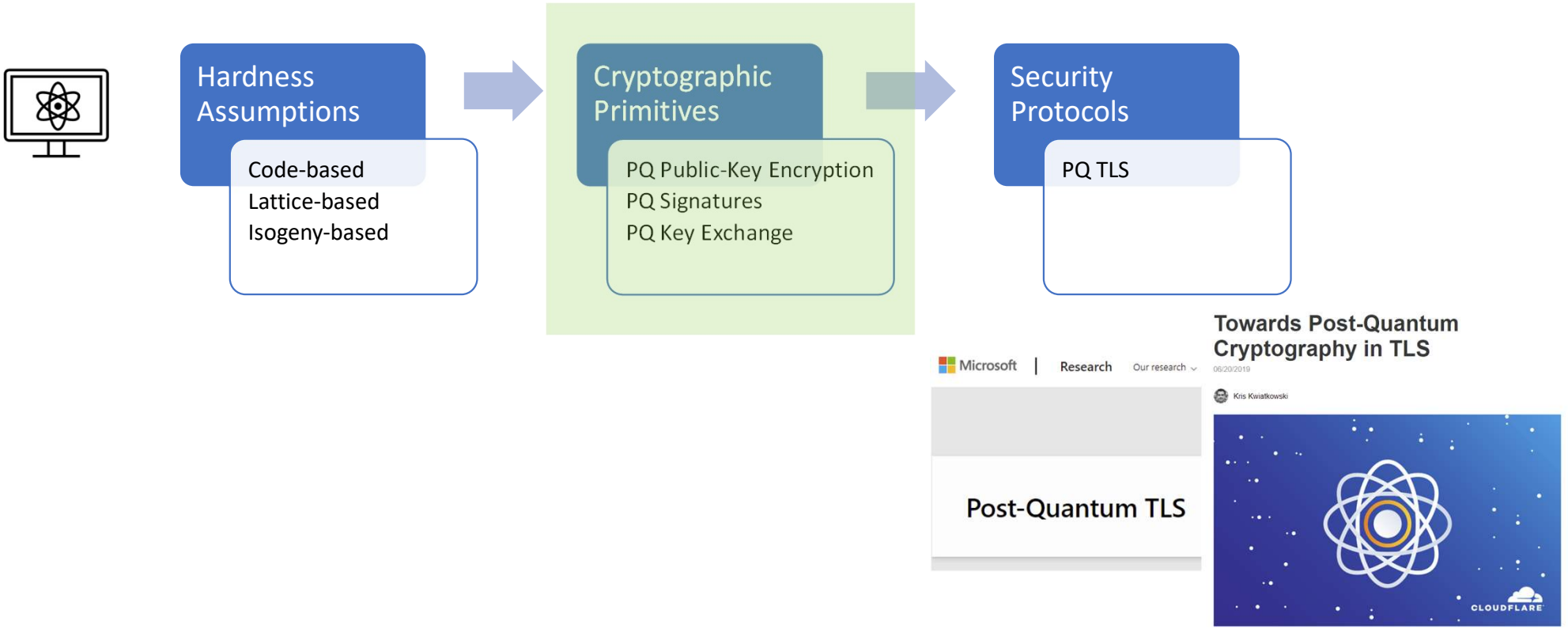
Security Protocols
- PQ TLS





Post-Quantum Cryptography (PQC)

Conventional public-key cryptosystems that resist known quantum algorithms.



Post-Quantum Cryptography (PQC)

Conventional public-key cryptosystems that resist known quantum algorithms.

NIST Kicks Off Effort to Defend Encrypted Data from Quantum Computer Threat

April 28, 2016

What will happen to computer security if quantum computers are built? A new NIST publication looks to the road ahead.
Credit: Hanacek/NIST

If an exotic *quantum computer* is invented that could break the codes we depend on to protect confidential electronic information, what will we do to maintain our security and privacy? That's the overarching question posed by a new report from the National Institute of Standards and Technology (NIST), whose cryptography specialists are beginning the long journey toward effective answers.

NIST Internal Report (NISTIR) 8105: *Report on Post-Quantum Cryptography* details the status of research into quantum computers, which would exploit the often counterintuitive world of quantum physics to solve problems that are intractable for conventional computers. If such devices are ever built, they will be able to defeat many of our modern cryptographic systems, such as the computer algorithms used to protect online bank transactions. NISTIR 8105 outlines a long-term approach for avoiding this vulnerability before it arises.

MEDIA CONTACT
Chad Boutin
charles.boutin@nist.gov
(301) 975-4261

ORGANIZATIONS
Information Technology Laboratory
Computer Security Division

SIGN UP FOR UPDATES FROM NIST

Enter Email Address

"It will be a long process involving public vetting of quantum-resistant algorithms," Moody said. "And we're not expecting to have just one winner. There are several systems in use that could be broken by a quantum computer—public-key encryption and digital signatures, to take two examples—and we will need different solutions for each of those systems."

Post-Quantum Cryptography (PQC)

Conventional public-key cryptosystems that resist known quantum algorithms.

NIST Kicks Off Effort to Defend Encrypted Data from Quantum Computer Threat

April 28, 2016

What will happen to computer security if quantum computers are built? A new NIST publication looks to the road ahead.
Credit: Hanacek/NIST

If an exotic *quantum computer* is invented that could break the codes we depend on to protect confidential electronic information, what will we do to maintain our security and privacy? That's the overarching question posed by a new report from the National Institute of Standards and Technology (NIST), whose cryptography specialists are beginning the long journey toward effective answers.

NIST Internal Report (NISTIR) 8105: *Report on Post-Quantum Cryptography* details the status of research into quantum computers, which would exploit the often counterintuitive world of quantum physics to solve problems that are intractable for conventional computers. If such devices are ever built, they will be able to defeat many of our modern cryptographic systems, such as the computer algorithms used to protect online bank transactions. NISTIR 8105 outlines a long-term approach for avoiding this vulnerability before it arises.

MEDIA CONTACT
Chad Boutin
charles.boutin@nist.gov
(301) 975-4261

ORGANIZATIONS
Information Technology Laboratory
Computer Security Division

SIGN UP FOR UPDATES FROM NIST

Enter Email Address

"It will be a long process involving public vetting of quantum-resistant algorithms," Moody said. "And we're not expecting to have just one winner. There are several systems in use that could be broken by a quantum computer—public-key encryption and digital signatures, to take two examples—and we will need different solutions for each of those systems."

US National Institute for Standards in Technology

Post-Quantum Cryptography (PQC)

Conventional public-key cryptosystems that resist known quantum algorithms.

NIST Kicks Off Effort to Defend Encrypted Data from Quantum Computer Threat

April 28, 2016

What will happen to computer security if quantum computers are built? A new NIST publication looks to the road ahead.
Credit: Hanacek/NIST

If an exotic *quantum computer* is invented that could break the codes we depend on to protect confidential electronic information, what will we do to maintain our security and privacy? That's the overarching question posed by a new report from the National Institute of Standards and Technology (NIST), whose cryptography specialists are beginning the long journey toward effective answers.

NIST Internal Report (NISTIR) 8105: *Report on Post-Quantum Cryptography* details the status of research into quantum computers, which would exploit the often counterintuitive world of quantum physics to solve problems that are intractable for conventional computers. If such devices are ever built, they will be able to defeat many of our modern cryptographic systems, such as the computer algorithms used to protect online bank transactions. NISTIR 8105 outlines a long-term approach for avoiding this vulnerability before it arises.

MEDIA CONTACT
Chad Boutin
charles.boutin@nist.gov
(301) 975-4261

ORGANIZATIONS
Information Technology Laboratory
Computer Security Division

SIGN UP FOR UPDATES FROM NIST
Enter Email Address

"It will be a long process involving public vetting of quantum-resistant algorithms," Moody said. "And we're not expecting to have just one winner. There are several systems in use that could be broken by a quantum computer—public-key encryption and digital signatures, to take two examples—and we will need different solutions for each of those systems."

US National Institute for Standards in Technology

- Is a part of the US Department of Commerce.

Post-Quantum Cryptography (PQC)

Conventional public-key cryptosystems that resist known quantum algorithms.

NIST Kicks Off Effort to Defend Encrypted Data from Quantum Computer Threat

April 28, 2016

What will happen to computer security if quantum computers are built? A new NIST publication looks to the road ahead.
Credit: Hanacek/NIST

If an exotic *quantum computer* is invented that could break the codes we depend on to protect confidential electronic information, what will we do to maintain our security and privacy? That's the overarching question posed by a new report from the National Institute of Standards and Technology (NIST), whose cryptography specialists are beginning the long journey toward effective answers.

NIST Internal Report (NISTIR) 8105: *Report on Post-Quantum Cryptography* details the status of research into quantum computers, which would exploit the often counterintuitive world of quantum physics to solve problems that are intractable for conventional computers. If such devices are ever built, they will be able to defeat many of our modern cryptographic systems, such as the computer algorithms used to protect online bank transactions. NISTIR 8105 outlines a long-term approach for avoiding this vulnerability before it arises.

MEDIA CONTACT
Chad Boutin
charles.boutin@nist.gov
(301) 975-4261

ORGANIZATIONS
Information Technology Laboratory
Computer Security Division

SIGN UP FOR UPDATES FROM NIST
Enter Email Address

"It will be a long process involving public vetting of quantum-resistant algorithms," Moody said. "And we're not expecting to have just one winner. There are several systems in use that could be broken by a quantum computer—public-key encryption and digital signatures, to take two examples—and we will need different solutions for each of those systems."

US National Institute for Standards in Technology

- Is a part of the US Department of Commerce.
- Publishes many basic cryptographic standards.

Post-Quantum Cryptography (PQC)

Conventional public-key cryptosystems that resist known quantum algorithms.

NIST Kicks Off Effort to Defend Encrypted Data from Quantum Computer Threat

April 28, 2016

What will happen to computer security if quantum computers are built? A new NIST publication looks to the road ahead.
Credit: Hanacek/NIST

If an exotic *quantum computer* is invented that could break the codes we depend on to protect confidential electronic information, what will we do to maintain our security and privacy? That's the overarching question posed by a new report from the National Institute of Standards and Technology (NIST), whose cryptography specialists are beginning the long journey toward effective answers.

NIST Internal Report (NISTIR) 8105: *Report on Post-Quantum Cryptography* details the status of research into quantum computers, which would exploit the often counterintuitive world of quantum physics to solve problems that are intractable for conventional computers. If such devices are ever built, they will be able to defeat many of our modern cryptographic systems, such as the computer algorithms used to protect online bank transactions. NISTIR 8105 outlines a long-term approach for avoiding this vulnerability before it arises.

MEDIA CONTACT
Chad Boutin
charles.boutin@nist.gov
(301) 975-4261

ORGANIZATIONS
Information Technology Laboratory
Computer Security Division

SIGN UP FOR UPDATES FROM NIST
Enter Email Address

"It will be a long process involving public vetting of quantum-resistant algorithms," Moody said. "And we're not expecting to have just one winner. There are several systems in use that could be broken by a quantum computer—public-key encryption and digital signatures, to take two examples—and we will need different solutions for each of those systems."

US National Institute for Standards in Technology

- Is a part of the US Department of Commerce.
- Publishes many basic cryptographic standards.
- These standards become de facto global standards for cryptography (notwithstanding algorithms from China, Russia, etc).

Post-Quantum Cryptography (PQC)

Conventional public-key cryptosystems that resist known quantum algorithms.

NIST Kicks Off Effort to Defend Encrypted Data from Quantum Computer Threat

April 28, 2016

What will happen to computer security if quantum computers are built? A new NIST publication looks to the road ahead.
Credit: Hanacek/NIST

If an exotic *quantum computer* is invented that could break the codes we depend on to protect confidential electronic information, what will we do to maintain our security and privacy? That's the overarching question posed by a new report from the National Institute of Standards and Technology (NIST), whose cryptography specialists are beginning the long journey toward effective answers.

NIST Internal Report (NISTIR) 8105: *Report on Post-Quantum Cryptography* details the status of research into quantum computers, which would exploit the often counterintuitive world of quantum physics to solve problems that are intractable for conventional computers. If such devices are ever built, they will be able to defeat many of our modern cryptographic systems, such as the computer algorithms used to protect online bank transactions. NISTIR 8105 outlines a long-term approach for avoiding this vulnerability before it arises.

MEDIA CONTACT
Chad Boutin
charles.boutin@nist.gov
(301) 975-4261

ORGANIZATIONS
Information Technology Laboratory
Computer Security Division

SIGN UP FOR UPDATES FROM NIST
Enter Email Address

"It will be a long process involving public vetting of quantum-resistant algorithms," Moody said. "And we're not expecting to have just one winner. There are several systems in use that could be broken by a quantum computer—public-key encryption and digital signatures, to take two examples—and we will need different solutions for each of those systems."

US National Institute for Standards in Technology

- Is a part of the US Department of Commerce.
- Publishes many basic cryptographic standards.
- These standards become de facto global standards for cryptography (notwithstanding algorithms from China, Russia, etc).
- They are often adopted by other standards bodies, e.g. IETF and ISO.

PQC and NIST

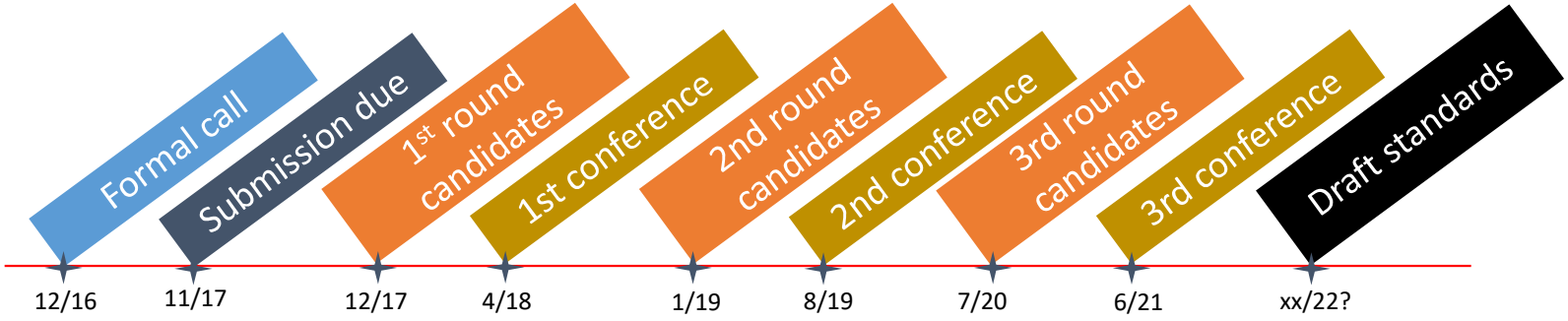
NIST PQC Process, 2016 – 2023(ish) for standardising post-quantum public key algorithms.

- http://csrc.nist.gov/groups/ST/post-quantum-crypto/
- **Formal project start:** 2012.
- **Evaluation criteria**: security, cost, flexibility/simplicity/adoptability.

PQC and NIST

NIST PQC Process, 2016 – 2023(ish) for standardising post-quantum public key algorithms.

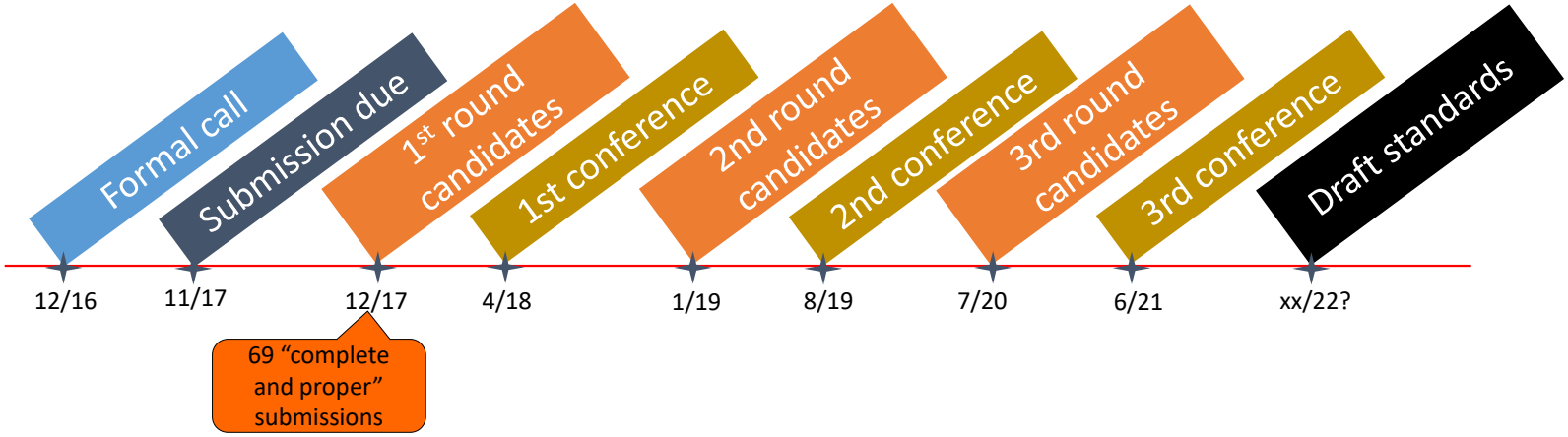
- http://csrc.nist.gov/groups/ST/post-quantum-crypto/
- **Formal project start:** 2012.
- **Evaluation criteria**: security, cost, flexibility/simplicity/adoptability.
- **Process (5-7 years)**:



PQC and NIST

NIST PQC Process, 2016 – 2023(ish) for standardising post-quantum public key algorithms.

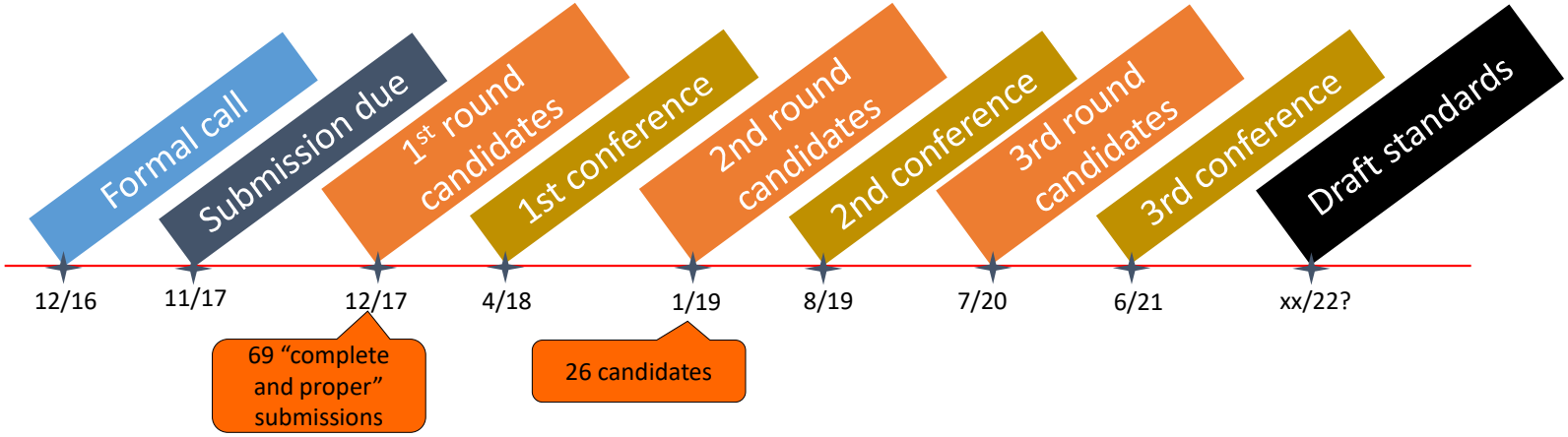
- http://csrc.nist.gov/groups/ST/post-quantum-crypto/
- **Formal project start:** 2012.
- **Evaluation criteria**: security, cost, flexibility/simplicity/adoptability.
- **Process (5-7 years)**:



PQC and NIST

NIST PQC Process, 2016 – 2023(ish) for standardising post-quantum public key algorithms.

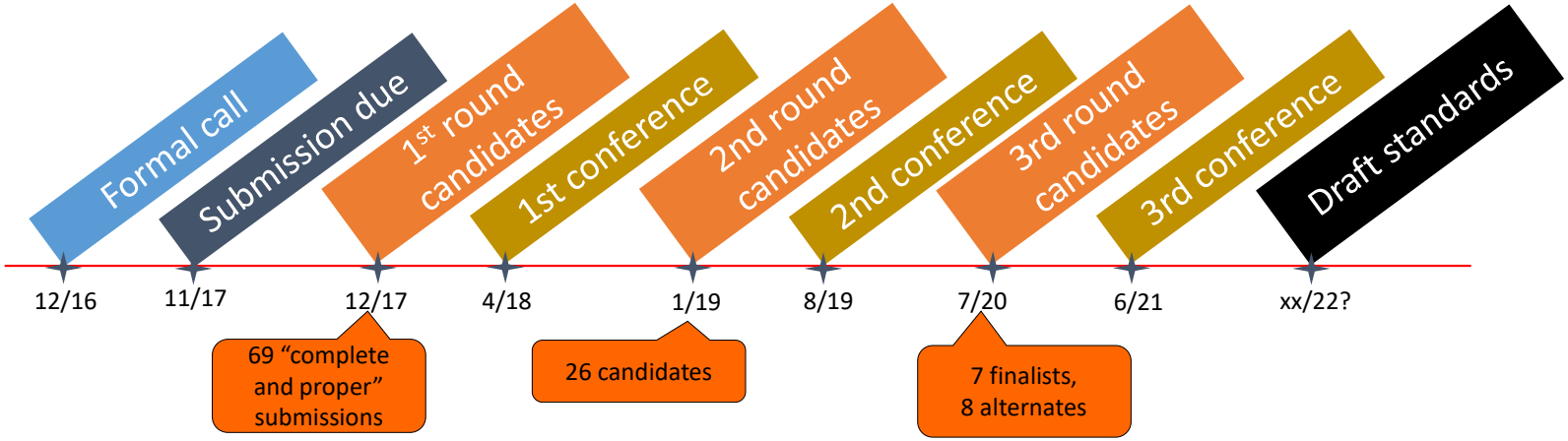
- http://csrc.nist.gov/groups/ST/post-quantum-crypto/
- **Formal project start:** 2012.
- **Evaluation criteria**: security, cost, flexibility/simplicity/adoptability.
- **Process (5-7 years)**:



PQC and NIST

NIST PQC Process, 2016 – 2023(ish) for standardising post-quantum public key algorithms.

- http://csrc.nist.gov/groups/ST/post-quantum-crypto/
- **Formal project start:** 2012.
- **Evaluation criteria**: security, cost, flexibility/simplicity/adoptability.
- **Process (5-7 years)**:



PQC and NIST

PQC Standardization Process: Third Round Candidate Announcement

NIST is announcing the third round finalists of the NIST Post-Quantum Cryptography Standardization Process. More details are included in NISTIR 8309.

July 22, 2020

It has been almost a year and a half since the second round of the NIST PQC Standardization Process began. After careful consideration, NIST would like to announce the candidates that will be moving on to the third round.

Third Round Finalists	Alternate Candidates
Public-Key Encryption/KEMs	Public-Key Encryption/KEMs
Classic McEliece	BIKE
CRYSTALS-KYBER	FrodoKEM
NTRU	HQC
SABER	NTRU Prime
	SIKE

ORGANIZATIONS

Information Technology Laboratory

Computer Security Division

Cryptographic Technology Group

PQC and NIST

PQC Standardization Process: Third Round Candidate Announcement

NIST is announcing the third round finalists of the NIST Post-Quantum Cryptography Standardization Process. More details are included in NISTIR 8309.

July 22, 2020

It has been almost a year and a half since the second round of the NIST PQC Standardization Process began. After careful consideration, NIST would like to announce the candidates that will be moving on to the third round.

Third Round Finalists	Alternate Candidates
Public-Key Encryption/KEMs	Public-Key Encryption/KEMs
Classic McEliece	BIKE
CRYSTALS-KYBER	FrodoKEM
NTRU	HQC
SABER	NTRU Prime
	SIKE

ORGANIZATIONS

Information Technology Laboratory

Computer Security Division

Cryptographic Technology Group

PQC and NIST

PQC Standardization Process: Third Round Candidate Announcement

NIST is announcing the third round finalists of the NIST Post-Quantum Cryptography Standardization Process. More details are included in NISTIR 8309.

July 22, 2020

It has been almost a year and a half since the second round of the NIST PQC Standardization Process began. After careful consideration, NIST would like to announce the candidates that will be moving on to the third round.

Third Round Finalists	Alternate Candidates
Public-Key Encryption/KEMs	Public-Key Encryption/KEMs
Classic McEliece	BIKE
CRYSTALS-KYBER	FrodoKEM
NTRU	HQC
SABER	NTRU Prime
	SIKE

Classic McEliece:
conservative code-based cryptography

10 October 2020

Principal submitter

This submission is from the following team, listed in alphabetical order:

- Martin R. Albrecht, Information Security Group, Royal Holloway, University of London
- Daniel J. Bernstein, University of Illinois at Chicago and Ruhr University Bochum
- Tung Chou, Academia Sinica
- Carlos Cid, Royal Holloway, University of London and Simula UiB
- Jan Gilcher, ETH Zürich
- Tanja Lange, Eindhoven University of Technology
- Varun Maram, ETH Zürich
- Ingo von Maurich, self
- Rafael Misoczki, Google
- Ruben Niederhagen, University of Southern Denmark
- Kenneth G. Paterson, ETH Zürich
- Edoardo Persichetti, Florida Atlantic University
- Christiane Peters, self
- Peter Schwabe, Max Planck Institute for Security and Privacy & Radboud University
- Nicolas Sendrier, Inria
- Jakub Szefer, Yale University
- Cen Jung Tjhai, PQ Solutions Ltd.
- Martin Tomlinson, PQ Solutions Ltd. and University of Plymouth
- Wen Wang, Yale University

Public-Key Encryption (PKE)

Public-Key Encryption (PKE)

Alice

Bob

Public-Key Encryption (PKE)

$$PKE = (KGen, Enc, Dec)$$

Alice

Bob

Public-Key Encryption (PKE)

$$PKE = (KGen, Enc, Dec)$$

Key Generation

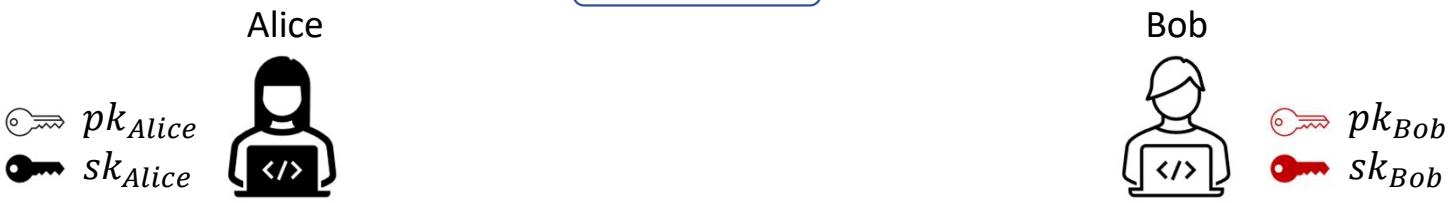
Alice

Bob

Public-Key Encryption (PKE)

$$PKE = (KGen, Enc, Dec)$$

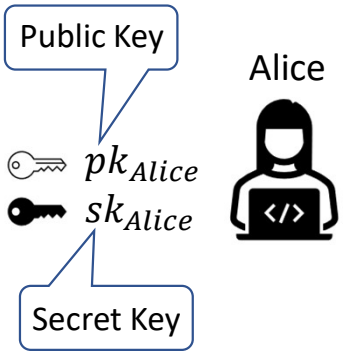
Key Generation



Public-Key Encryption (PKE)

$$PKE = (KGen, Enc, Dec)$$

Key Generation



Alice

Bob

pk_{Bob}

sk_{Bob}

Public-Key Encryption (PKE)

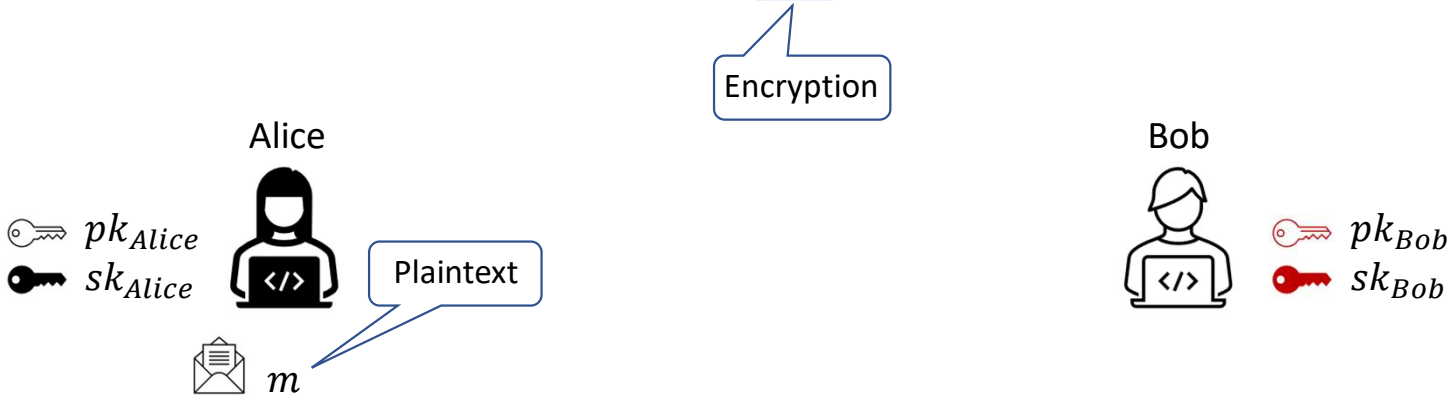
$$PKE = (KGen, Enc, Dec)$$

Public-Key Encryption (PKE)

$$PKE = (KGen, Enc, Dec)$$

Public-Key Encryption (PKE)

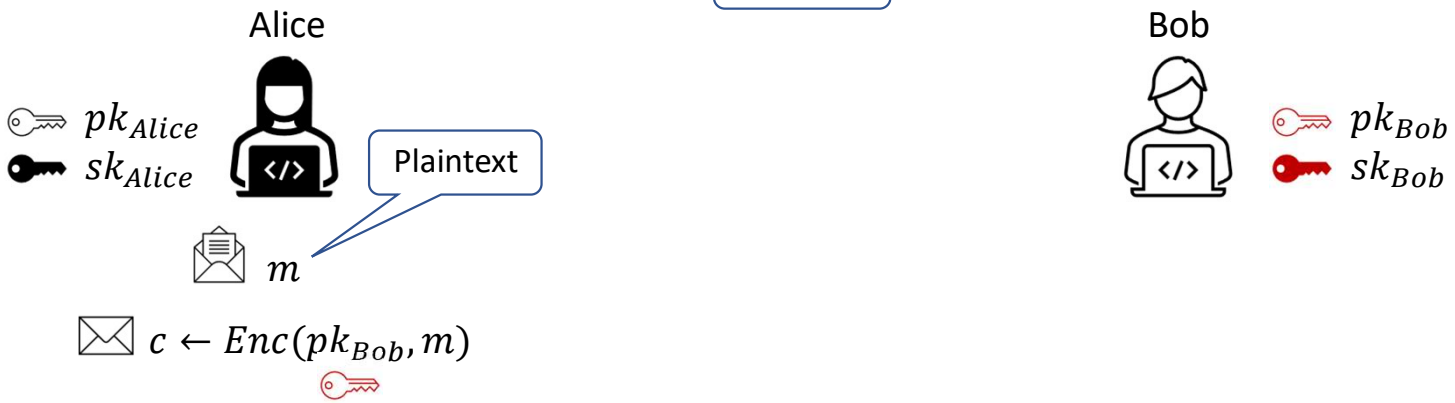
$$PKE = (KGen, Enc, Dec)$$



Public-Key Encryption (PKE)

$$PKE = (KGen, Enc, Dec)$$

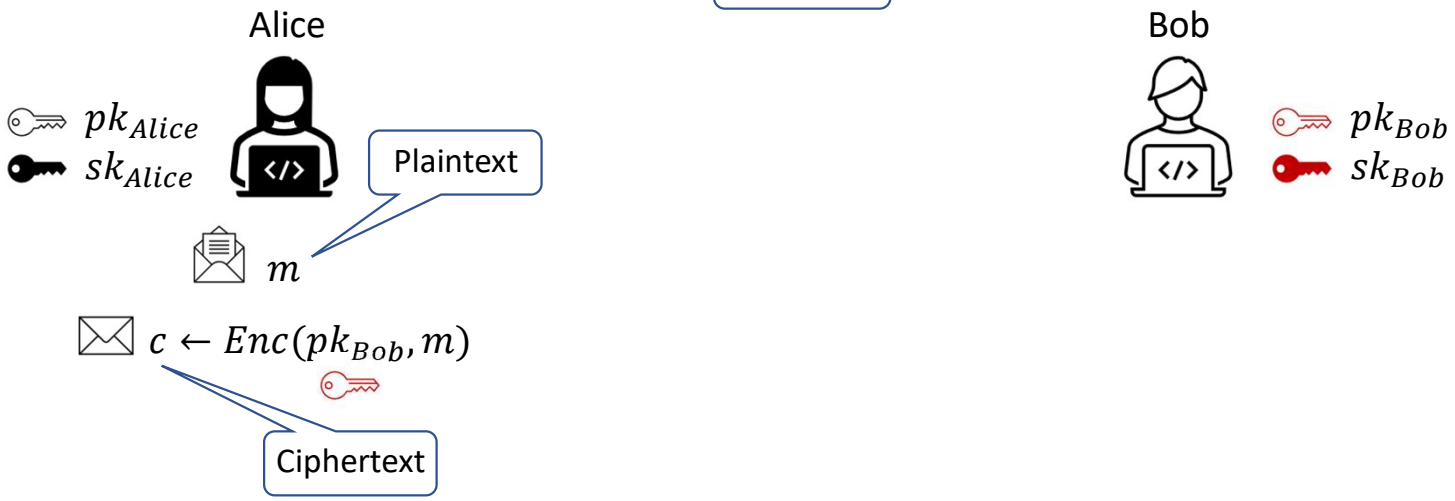
Encryption



Public-Key Encryption (PKE)

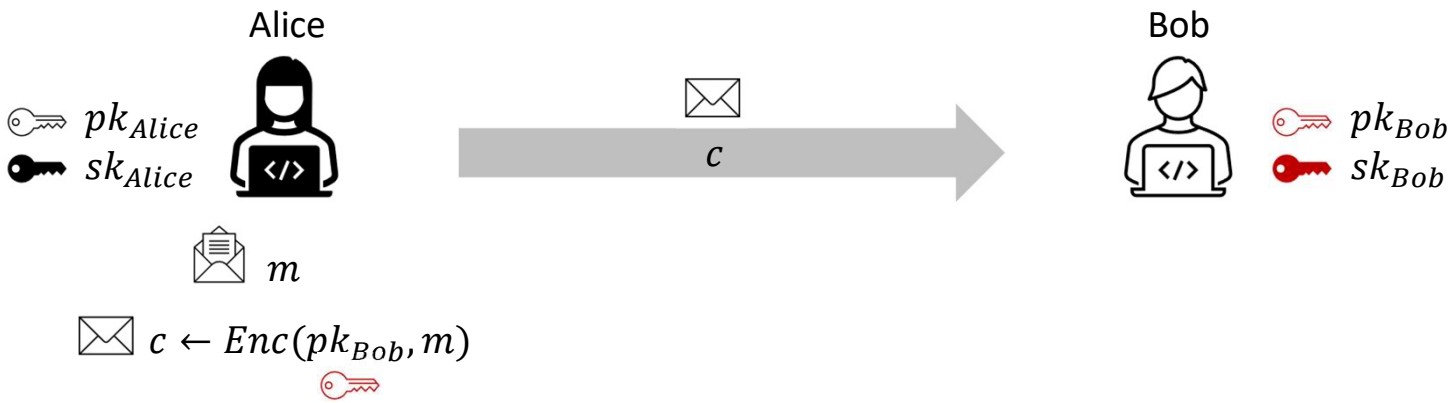
$$PKE = (KGen, Enc, Dec)$$

Encryption

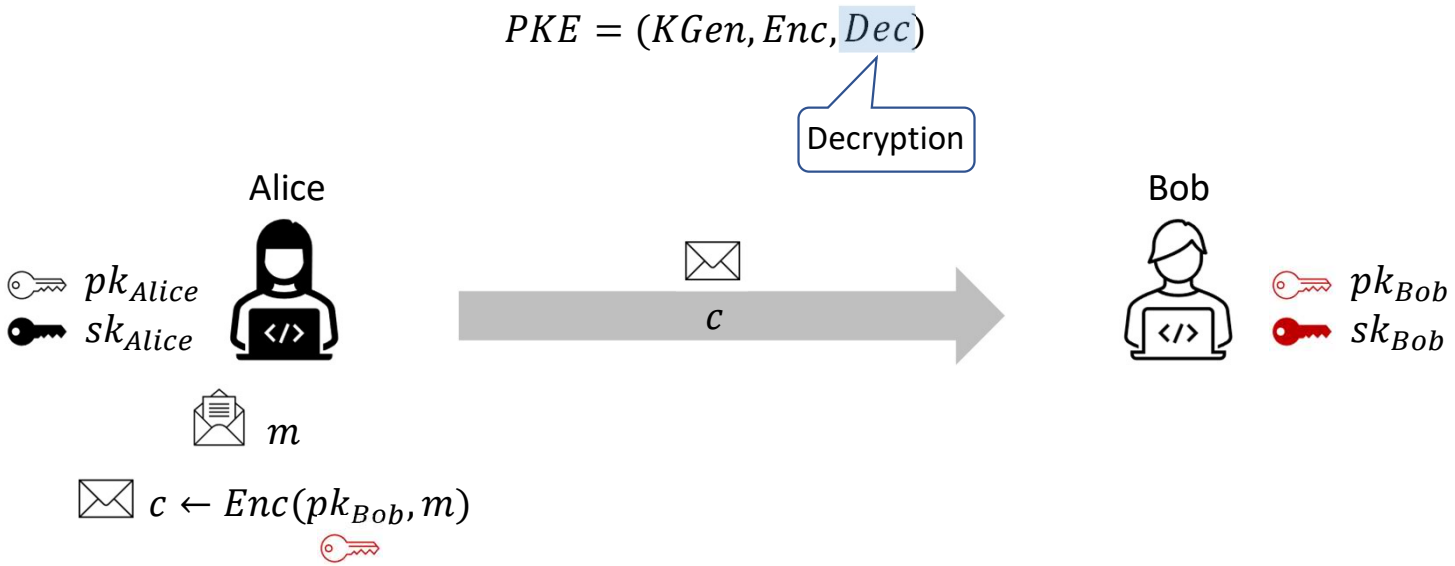


Public-Key Encryption (PKE)

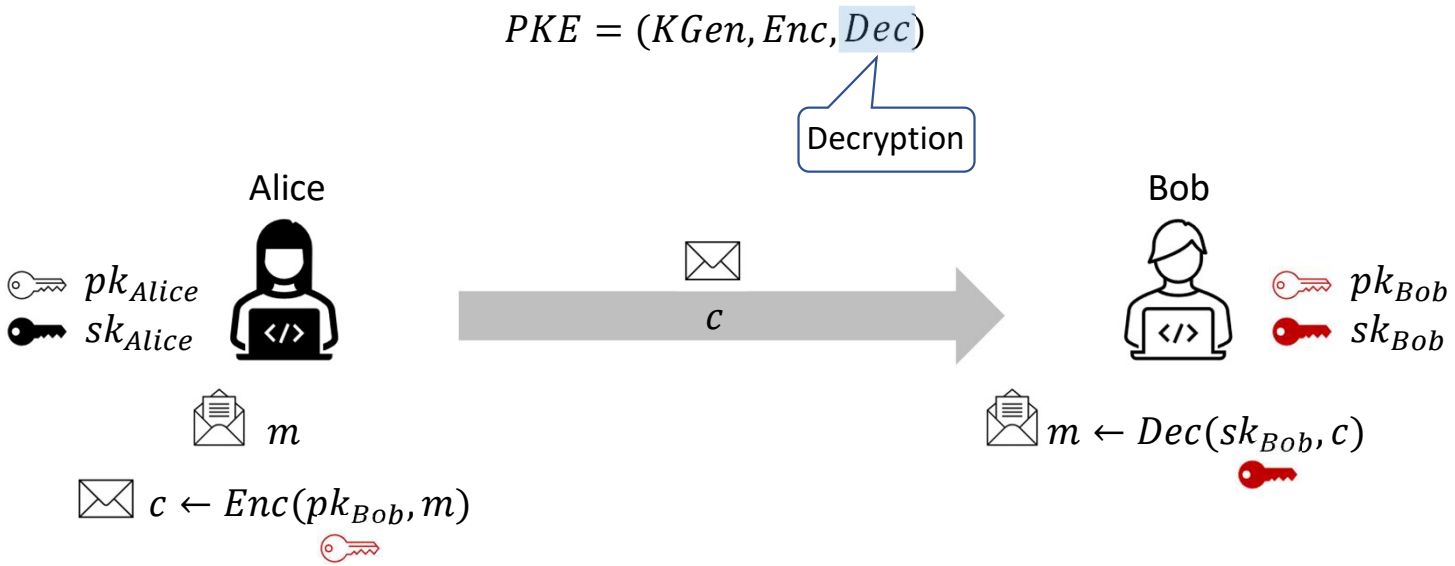
$$PKE = (KGen, Enc, Dec)$$



Public-Key Encryption (PKE)



Public-Key Encryption (PKE)



PQC and NIST

PQC Standardization Process: Third Round Candidate Announcement

NIST is announcing the third round finalists of the NIST Post-Quantum Cryptography Standardization Process. More details are included in NISTIR 8309.

July 22, 2020

It has been almost a year and a half since the second round of the NIST PQC Standardization Process began. After careful consideration, NIST would like to announce the candidates that will be moving on to the third round.

Third Round Finalists	Alternate Candidates
Public-Key Encryption/KEMs	Public-Key Encryption/KEMs
Classic McEliece	BIKE
CRYSTALS-KYBER	FrodoKEM
NTRU	HQC
SABER	NTRU Prime
	SIKE

ORGANIZATIONS

Information Technology Laboratory

Computer Security Division

Cryptographic Technology Group

PQC and NIST

PQC Standardization Process: Third Round Candidate Announcement

NIST is announcing the third round finalists of the NIST Post-Quantum Cryptography Standardization Process. More details are included in NISTIR 8309.

July 22, 2020

It has been almost a year and a half since the second round of the NIST PQC Standardization Process began. After careful consideration, NIST would like to announce the candidates that will be moving on to the third round.

Third Round Finalists	Alternate Candidates
Public-Key Encryption/KEMs	Public-Key Encryption/KEMs
Classic McEliece	BIKE
CRYSTALS-KYBER	FrodoKEM
NTRU	HQC
SABER	NTRU Prime
	SIKE

ORGANIZATIONS

Information Technology Laboratory

Computer Security Division

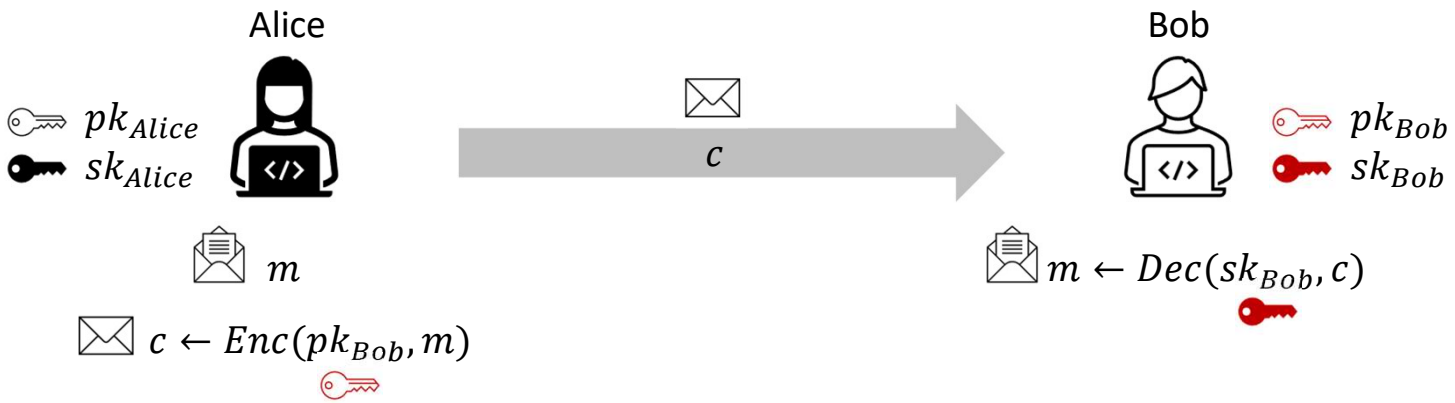
Cryptographic Technology Group

4.A.2 Security Definition for Encryption/Key-Establishment

NIST intends to standardize one or more schemes that enable "semantically secure" encryption or key encapsulation with respect to adaptive chosen ciphertext attack, for general use. This property is generally denoted *IND-CCA2 security* in academic literature.

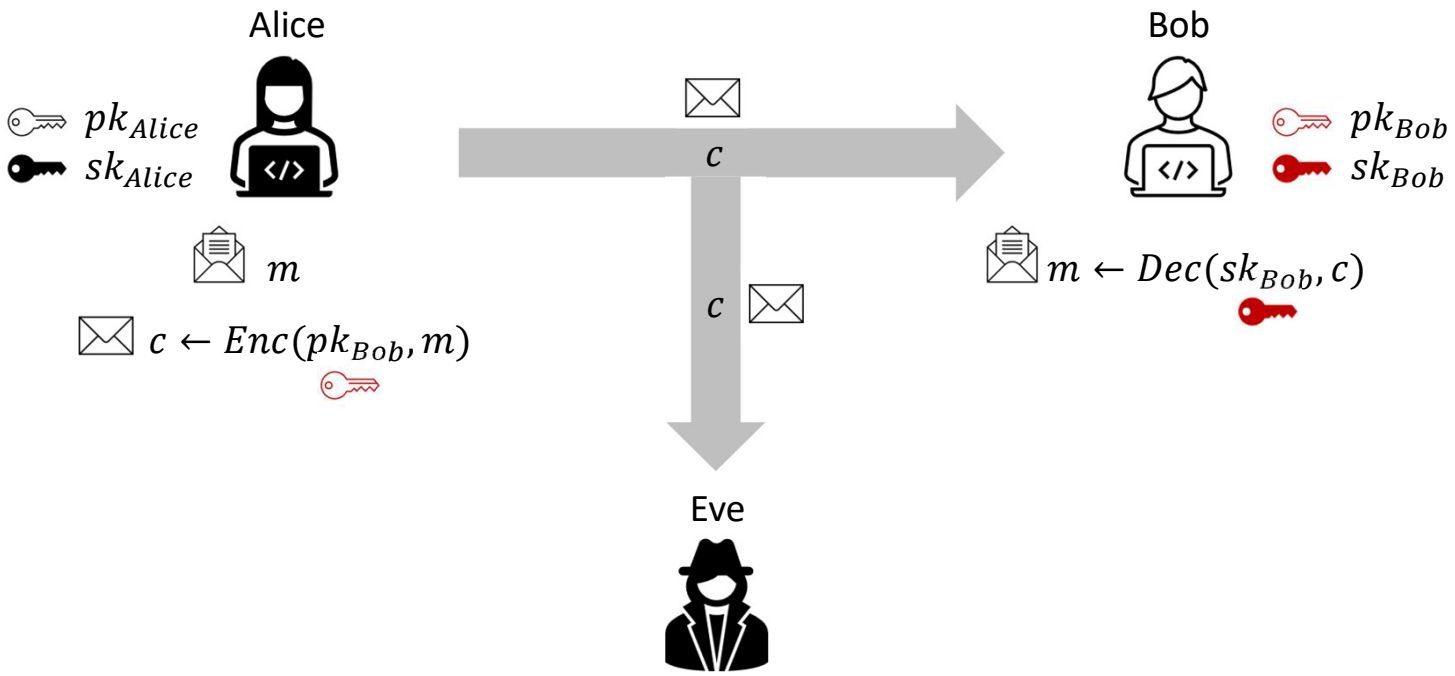
IND-CCA Security

$$PKE = (KGen, Enc, Dec)$$



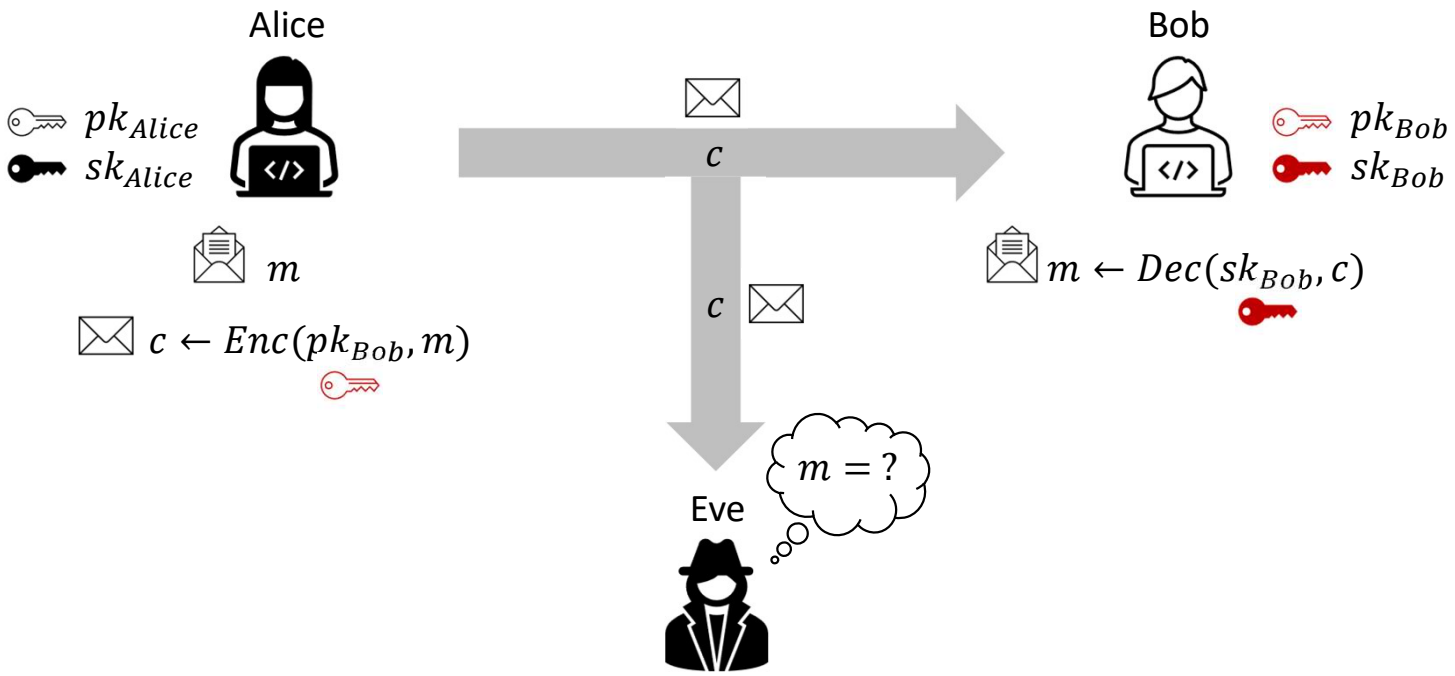
IND-CCA Security

$$PKE = (KGen, Enc, Dec)$$



IND-CCA Security

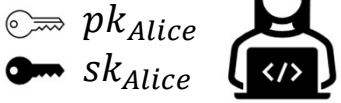
$$PKE = (KGen, Enc, Dec)$$



Anonymity

$PKE = (KGen, Enc, Dec)$

Alice



Bob

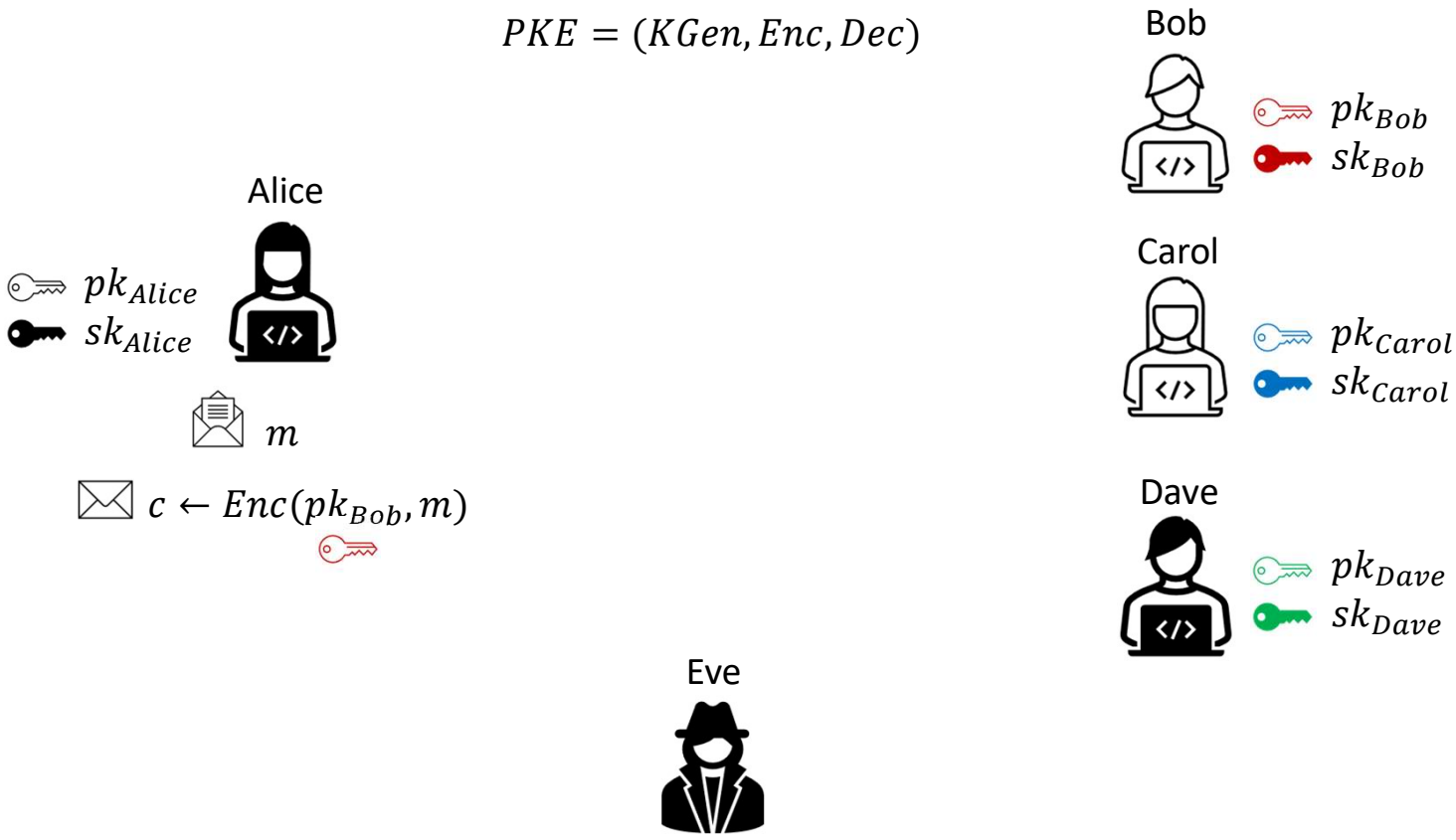
Carol

Dave

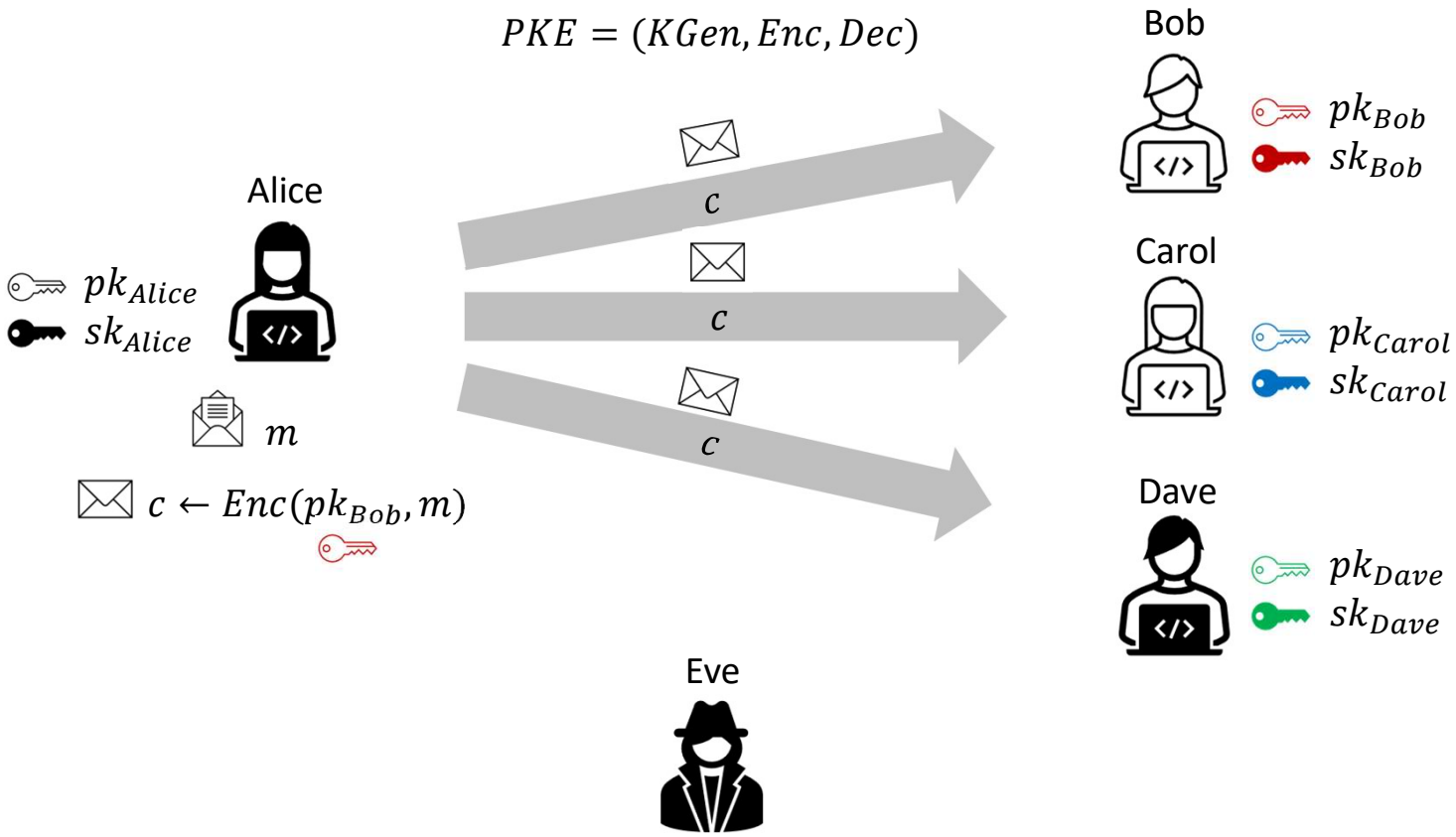
Eve

Anonymity

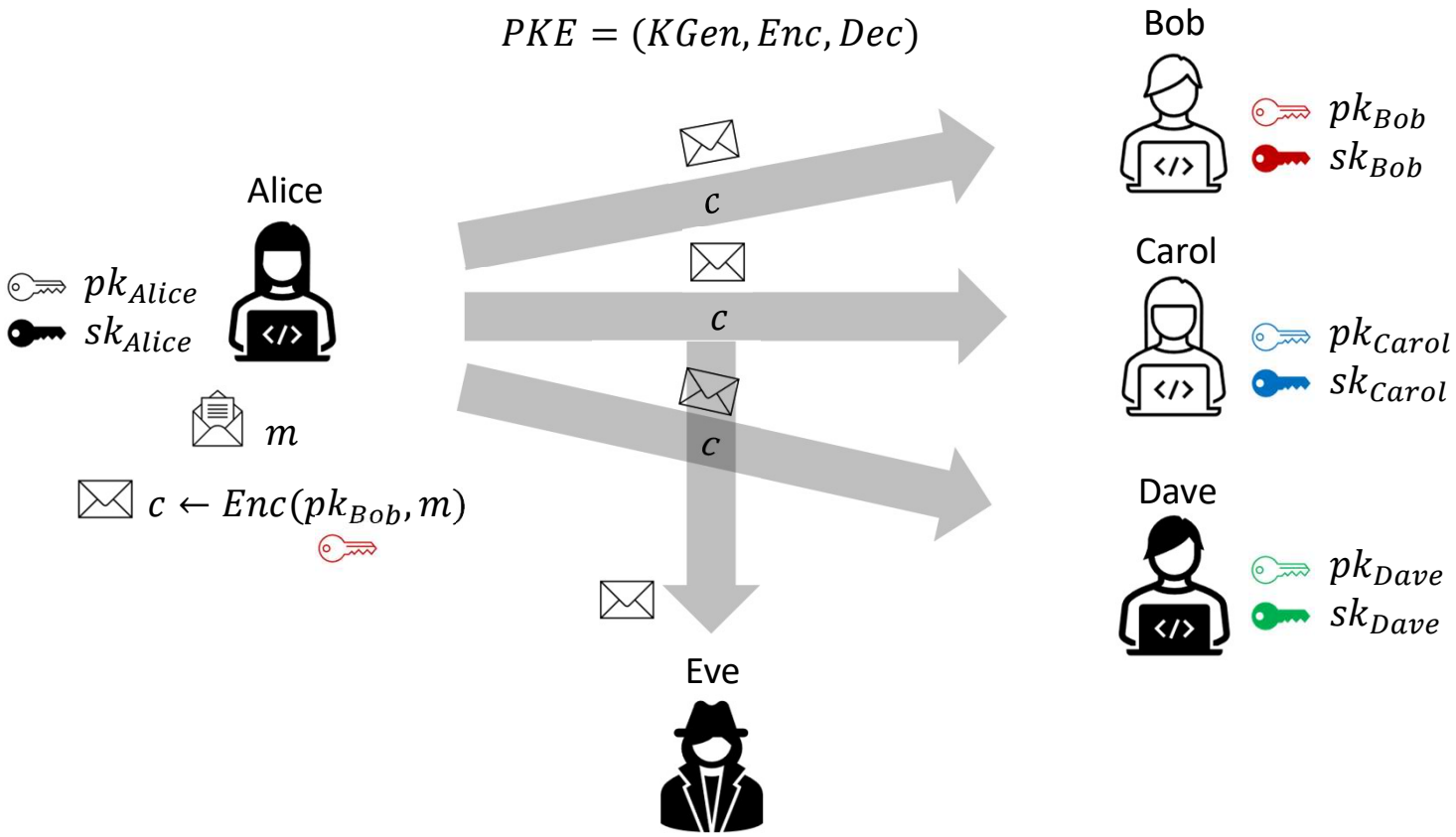
$PKE = (KGen, Enc, Dec)$



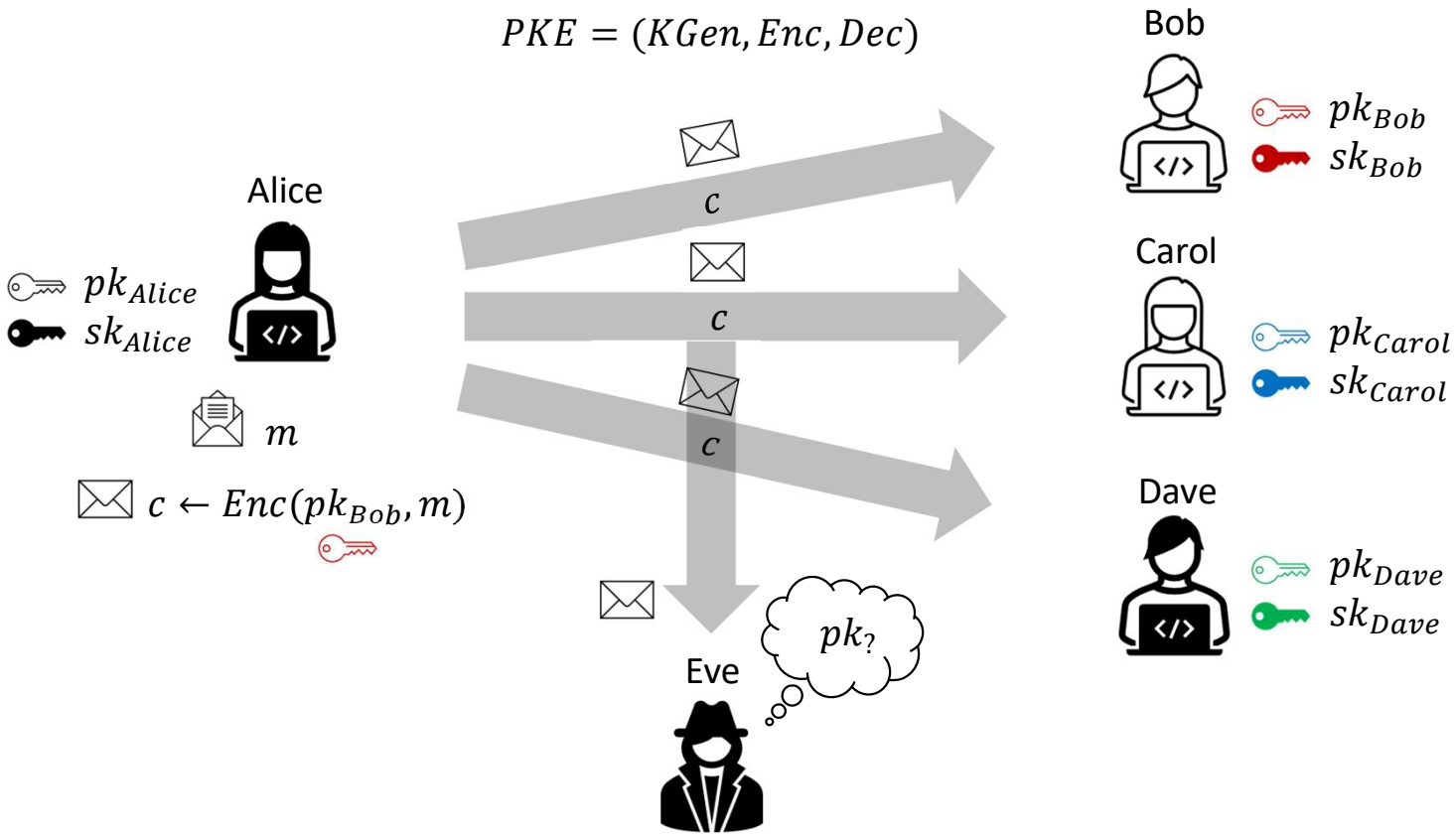
Anonymity


$PKE = (KGen, Enc, Dec)$
Alice
pk_{Alice}
sk_{Alice}
m
$c \leftarrow Enc(pk_{Bob}, m)$
c
c
c
Bob
pk_{Bob}
sk_{Bob}
Carol
pk_{Carol}
sk_{Carol}
Dave
pk_{Dave}
sk_{Dave}
Eve

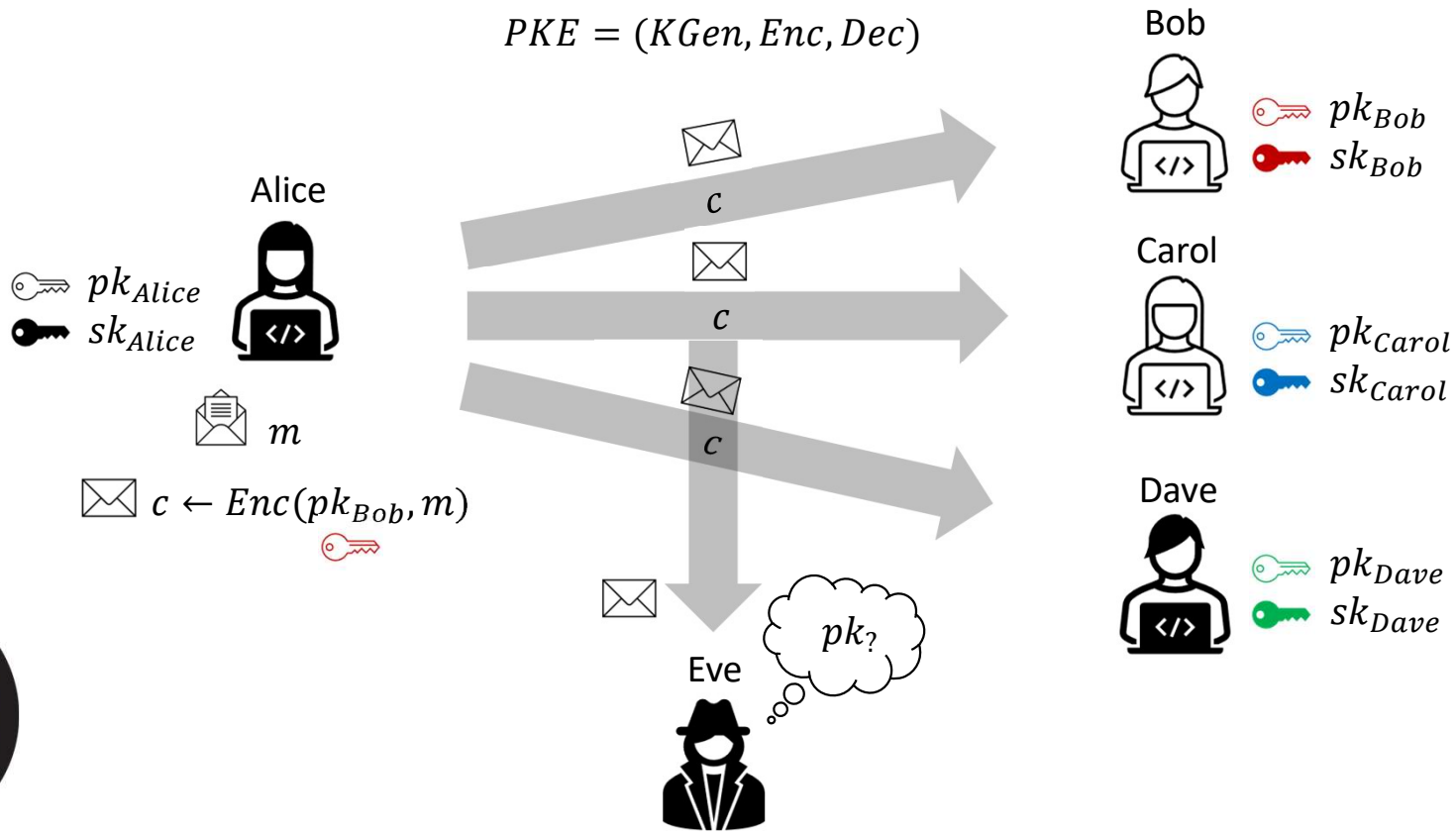
Anonymity


$PKE = (KGen, Enc, Dec)$
Alice
pk_{Alice}
sk_{Alice}
m
$c \leftarrow Enc(pk_{Bob}, m)$
c
c
c
Bob
pk_{Bob}
sk_{Bob}
Carol
pk_{Carol}
sk_{Carol}
Dave
pk_{Dave}
sk_{Dave}
Eve

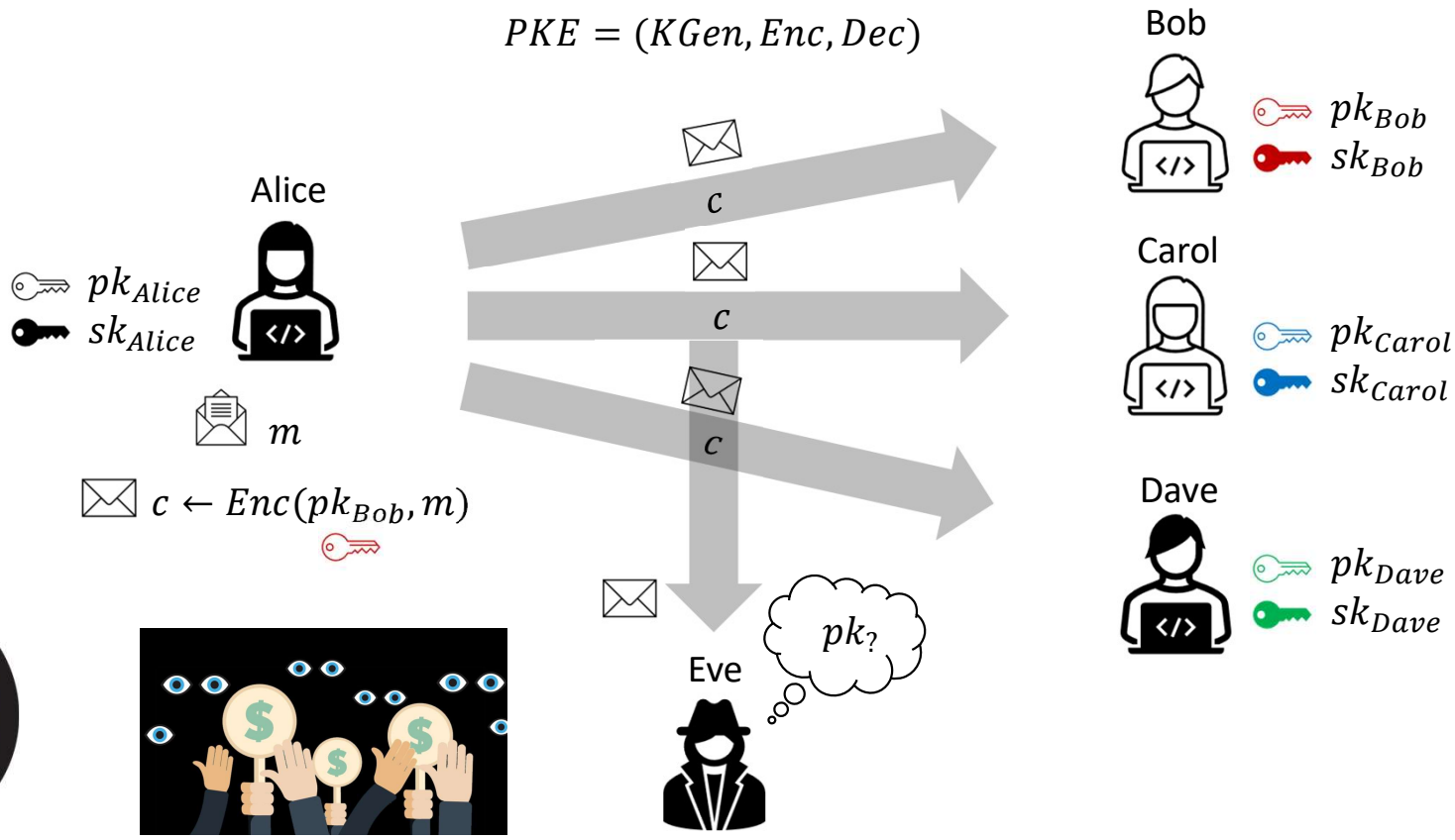
Anonymity


$PKE = (KGen, Enc, Dec)$
Alice
pk_{Alice}
sk_{Alice}
m
$c \leftarrow Enc(pk_{Bob}, m)$
c
c
c
Bob
pk_{Bob}
sk_{Bob}
Carol
pk_{Carol}
sk_{Carol}
Dave
pk_{Dave}
sk_{Dave}
Eve
$pk_?$

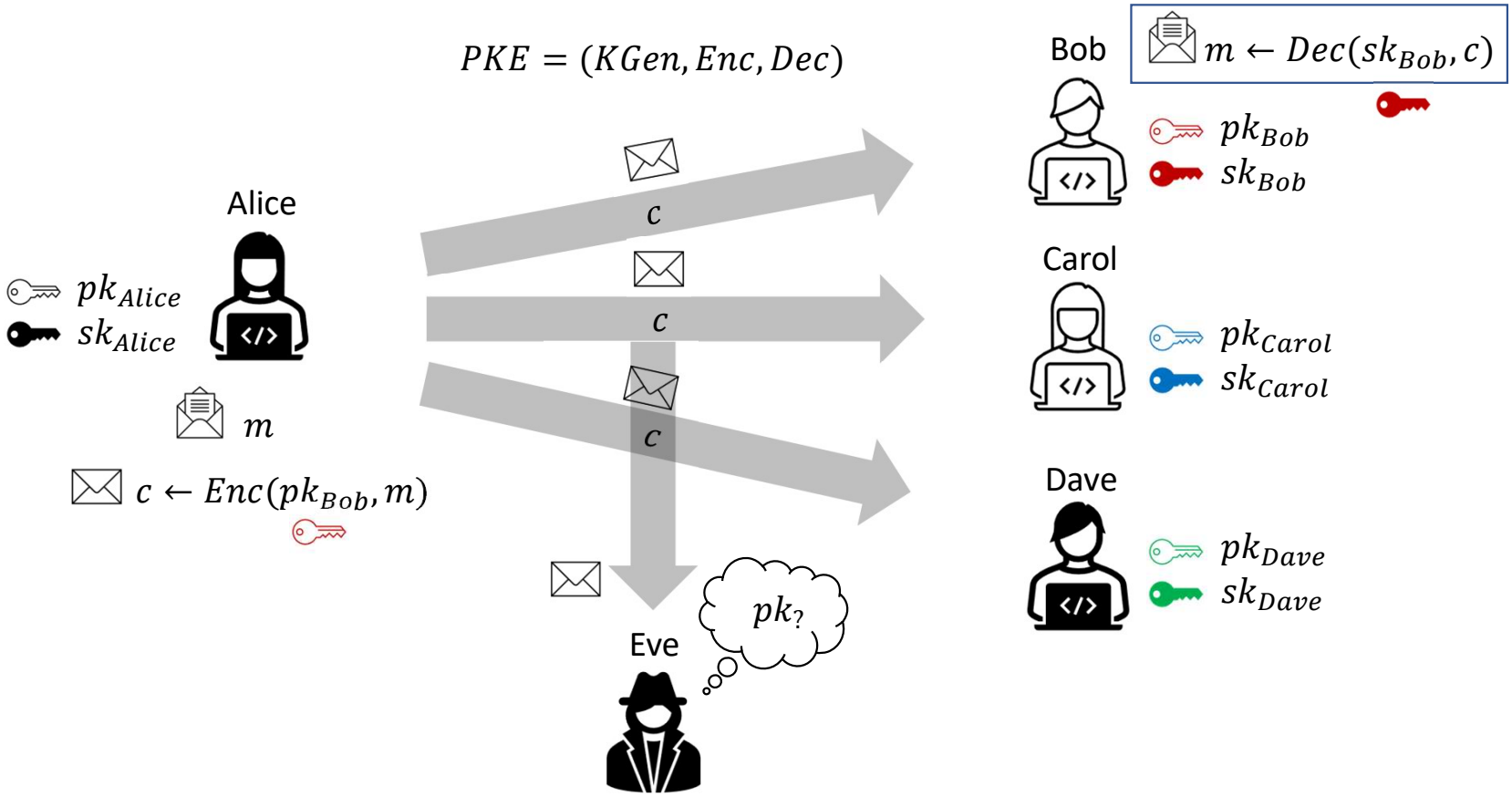
Anonymity


$PKE = (KGen, Enc, Dec)$
Alice
pk_{Alice}
sk_{Alice}
m
$c \leftarrow Enc(pk_{Bob}, m)$
c
c
c
Bob
pk_{Bob}
sk_{Bob}
Carol
pk_{Carol}
sk_{Carol}
Dave
pk_{Dave}
sk_{Dave}
Eve
$pk_?$

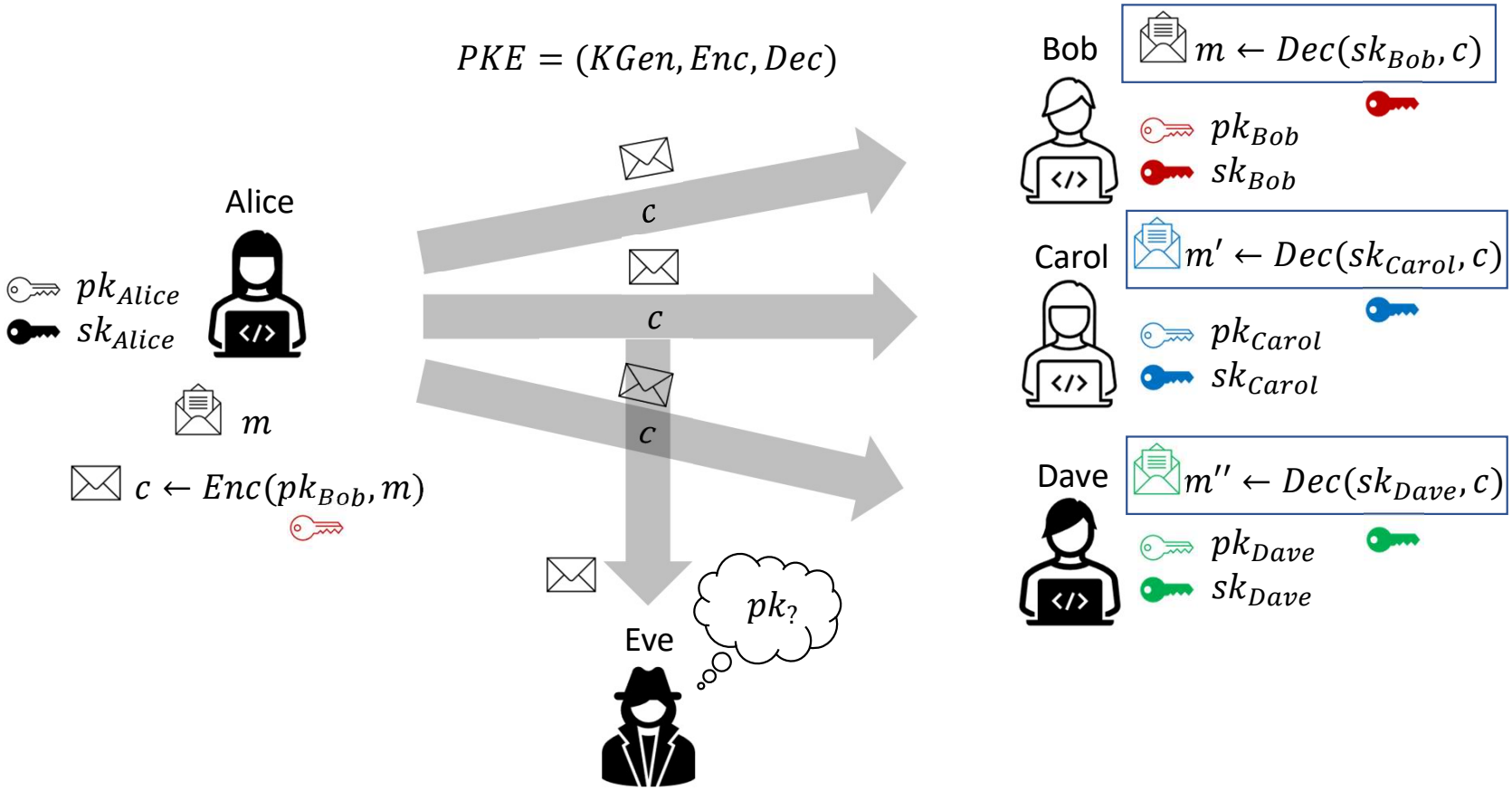
Anonymity


$PKE = (KGen, Enc, Dec)$
Alice
pk_{Alice}
sk_{Alice}
m
$c \leftarrow Enc(pk_{Bob}, m)$
c
c
c
Bob
pk_{Bob}
sk_{Bob}
Carol
pk_{Carol}
sk_{Carol}
Dave
pk_{Dave}
sk_{Dave}
Eve
$pk_?$

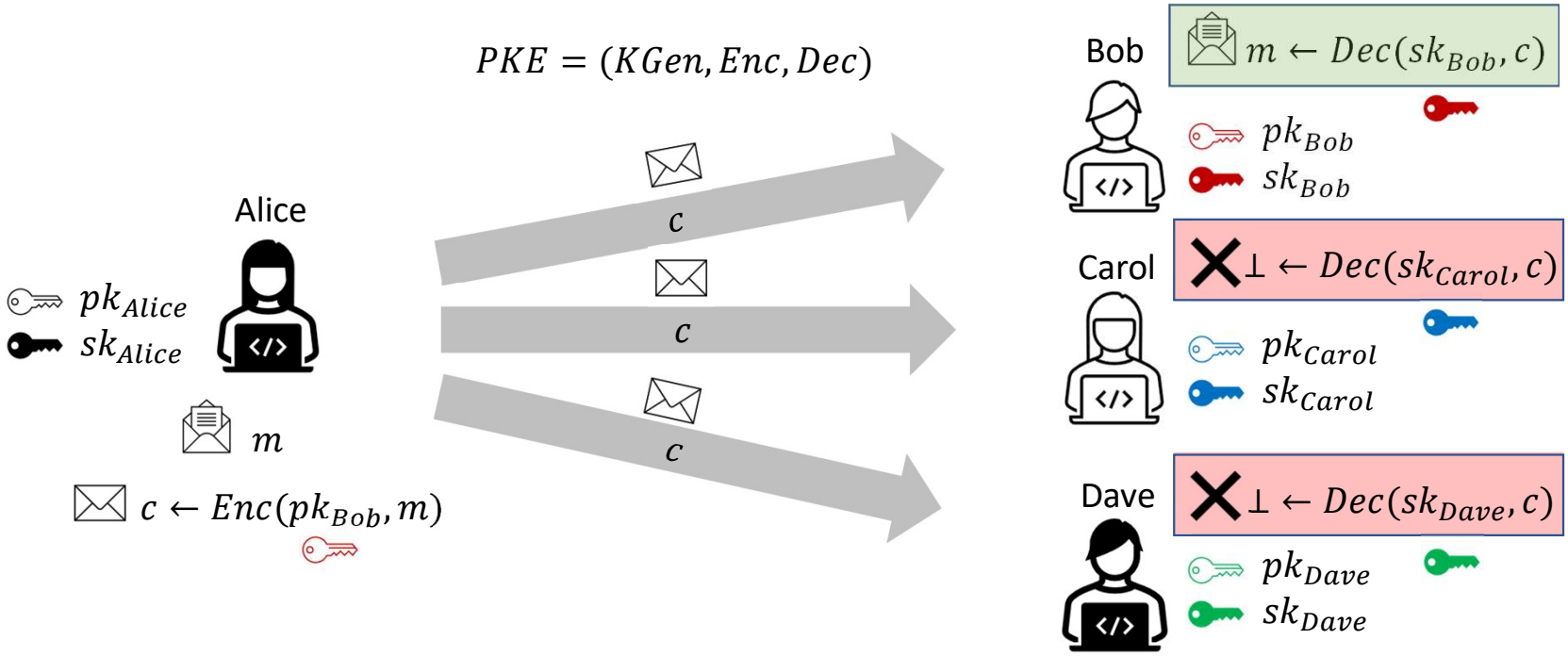
Anonymity


$PKE = (KGen, Enc, Dec)$
Alice
pk_{Alice}
sk_{Alice}
m
$c \leftarrow Enc(pk_{Bob}, m)$
c
c
c
Eve
$pk_?$
Bob
$m \leftarrow Dec(sk_{Bob}, c)$
pk_{Bob}
sk_{Bob}
Carol
pk_{Carol}
sk_{Carol}
Dave
pk_{Dave}
sk_{Dave}

Anonymity


$PKE = (KGen, Enc, Dec)$
Alice
pk_{Alice}
sk_{Alice}
m
$c \leftarrow Enc(pk_{Bob}, m)$
c
c
c
Eve
$pk_?$
Bob
$m \leftarrow Dec(sk_{Bob}, c)$
pk_{Bob}
sk_{Bob}
Carol
$m' \leftarrow Dec(sk_{Carol}, c)$
pk_{Carol}
sk_{Carol}
Dave
$m'' \leftarrow Dec(sk_{Dave}, c)$
pk_{Dave}
sk_{Dave}

Robustness


$PKE = (KGen, Enc, Dec)$
Alice
pk_{Alice}
sk_{Alice}
m
$c \leftarrow Enc(pk_{Bob}, m)$
c
c
c
Bob
$m \leftarrow Dec(sk_{Bob}, c)$
pk_{Bob}
sk_{Bob}
Carol
$\perp \leftarrow Dec(sk_{Carol}, c)$
pk_{Carol}
sk_{Carol}
Dave
$\perp \leftarrow Dec(sk_{Dave}, c)$
pk_{Dave}
sk_{Dave}

PQC and NIST

PQC Standardization Process: Third Round Candidate Announcement

NIST is announcing the third round finalists of the NIST Post-Quantum Cryptography Standardization Process. More details are included in NISTIR 8309.

July 22, 2020

It has been almost a year and a half since the second round of the NIST PQC Standardization Process began. After careful consideration, NIST would like to announce the candidates that will be moving on to the third round.

Third Round Finalists	Alternate Candidates
Public-Key Encryption/KEMs	Public-Key Encryption/KEMs
Classic McEliece	BIKE
CRYSTALS-KYBER	FrodoKEM
NTRU	HQC
SABER	NTRU Prime
	SIKE

ORGANIZATIONS

Information Technology Laboratory

Computer Security Division

Cryptographic Technology Group

PQC and NIST

PQC Standardization Process: Third Round Candidate Announcement

NIST is announcing the third round finalists of the NIST Post-Quantum Cryptography Standardization Process. More details are included in NISTIR 8309.

July 22, 2020

It has been almost a year and a half since the second round of the NIST PQC Standardization Process began. After careful consideration, NIST would like to announce the candidates that will be moving on to the third round.

Third Round Finalists	Alternate Candidates
Public-Key Encryption/KEMs	Public-Key Encryption/KEMs
Classic McEliece	BIKE
CRYSTALS-KYBER	FrodoKEM
NTRU	HQC
SABER	NTRU Prime
	SIKE

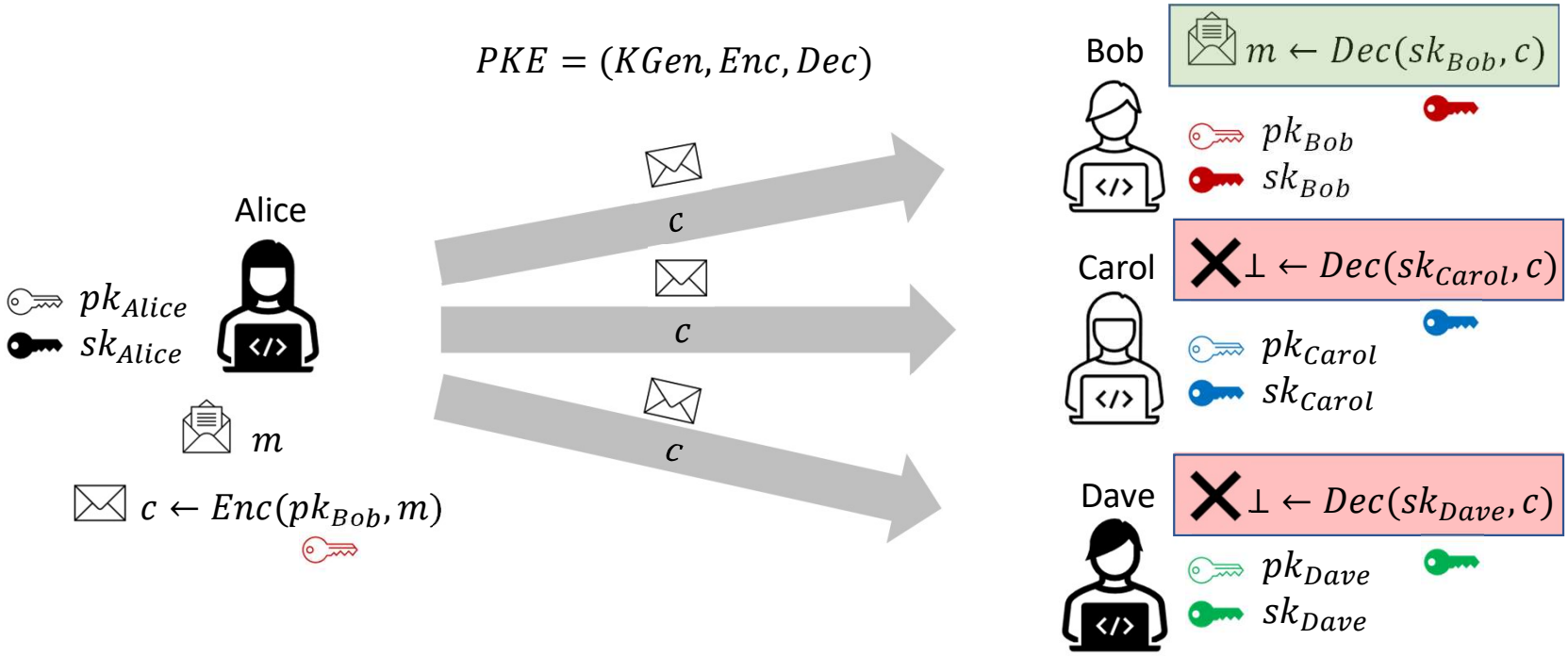
ORGANIZATIONS

Information Technology Laboratory

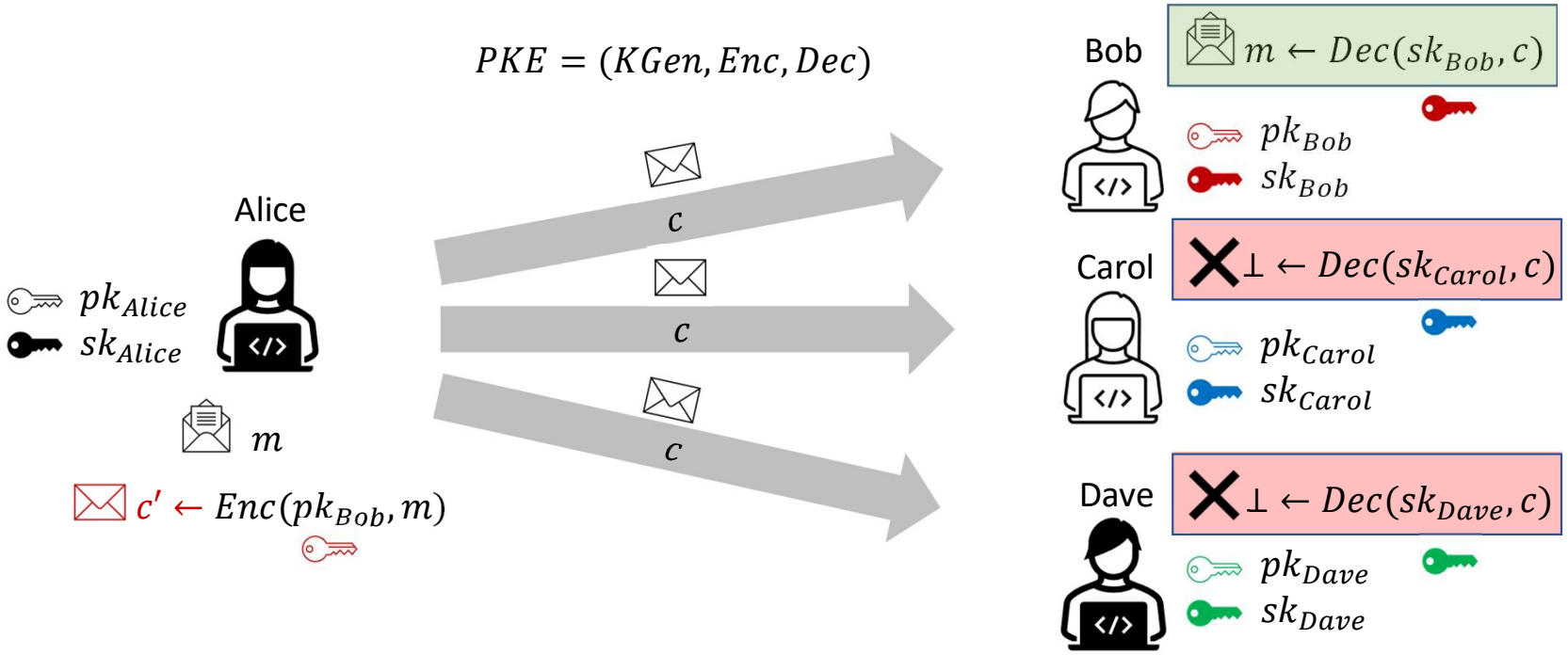
Computer Security Division

Cryptographic Technology Group

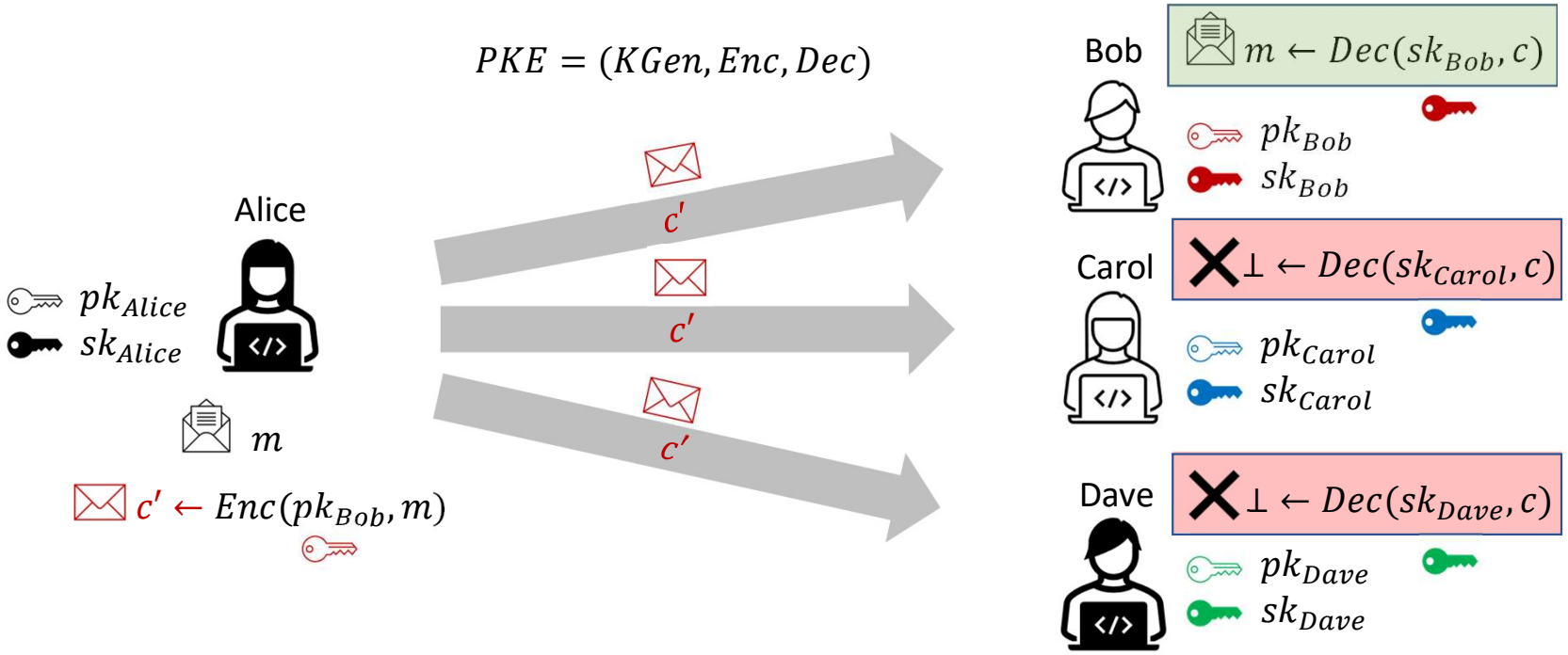
Classic McEliece



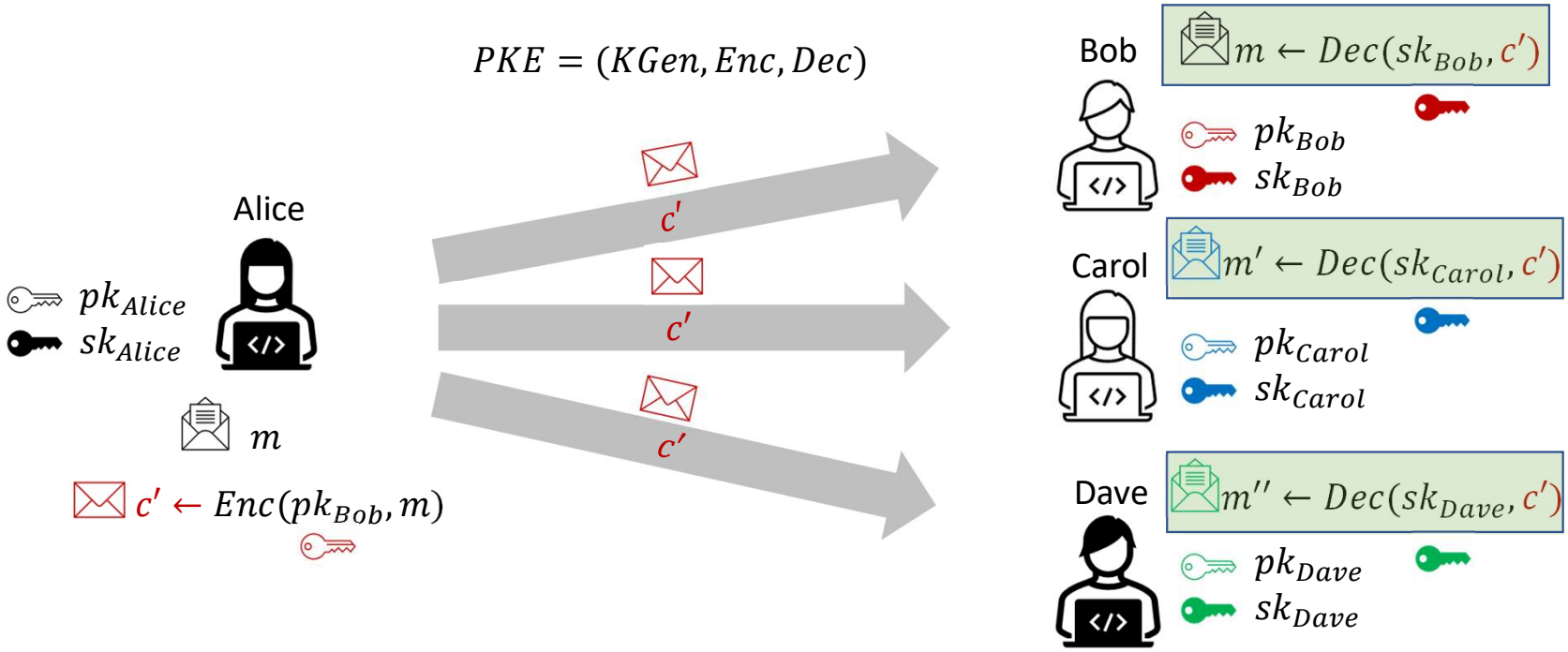
Classic McEliece



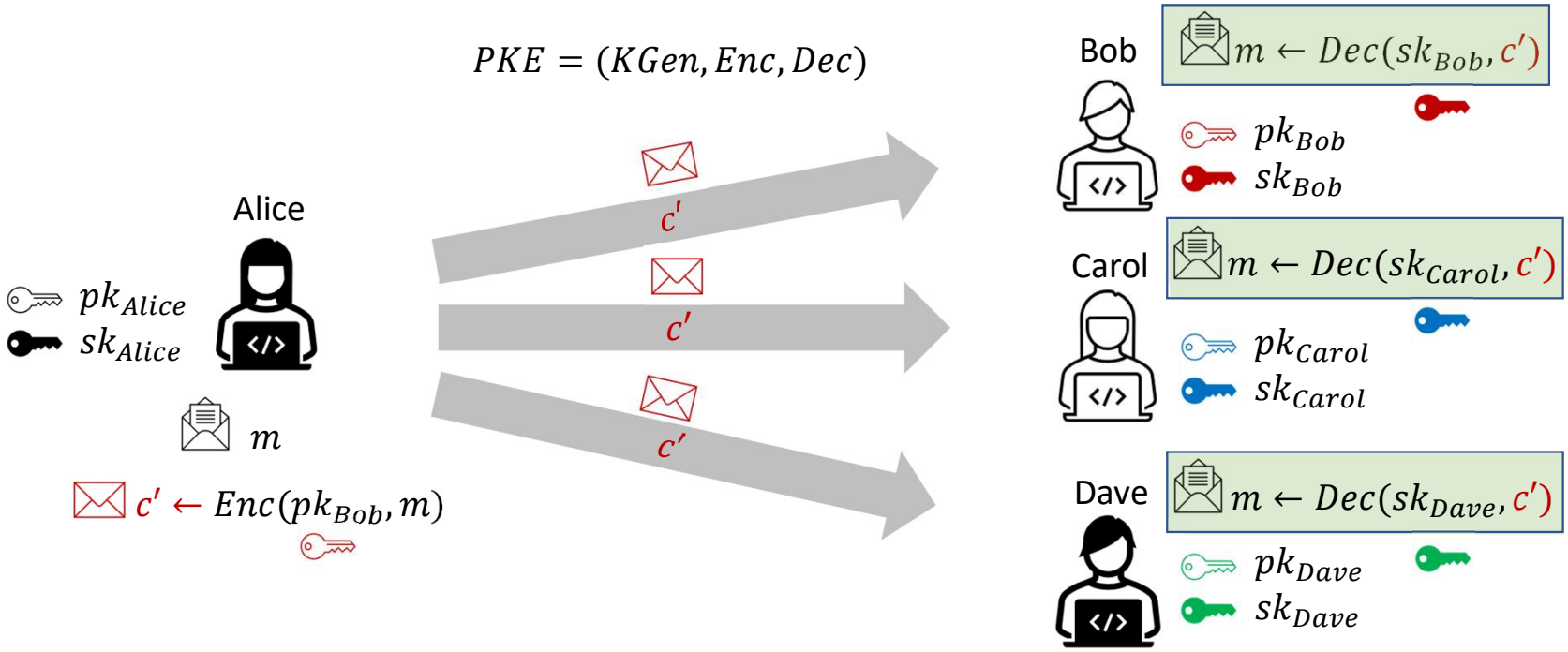
Classic McEliece



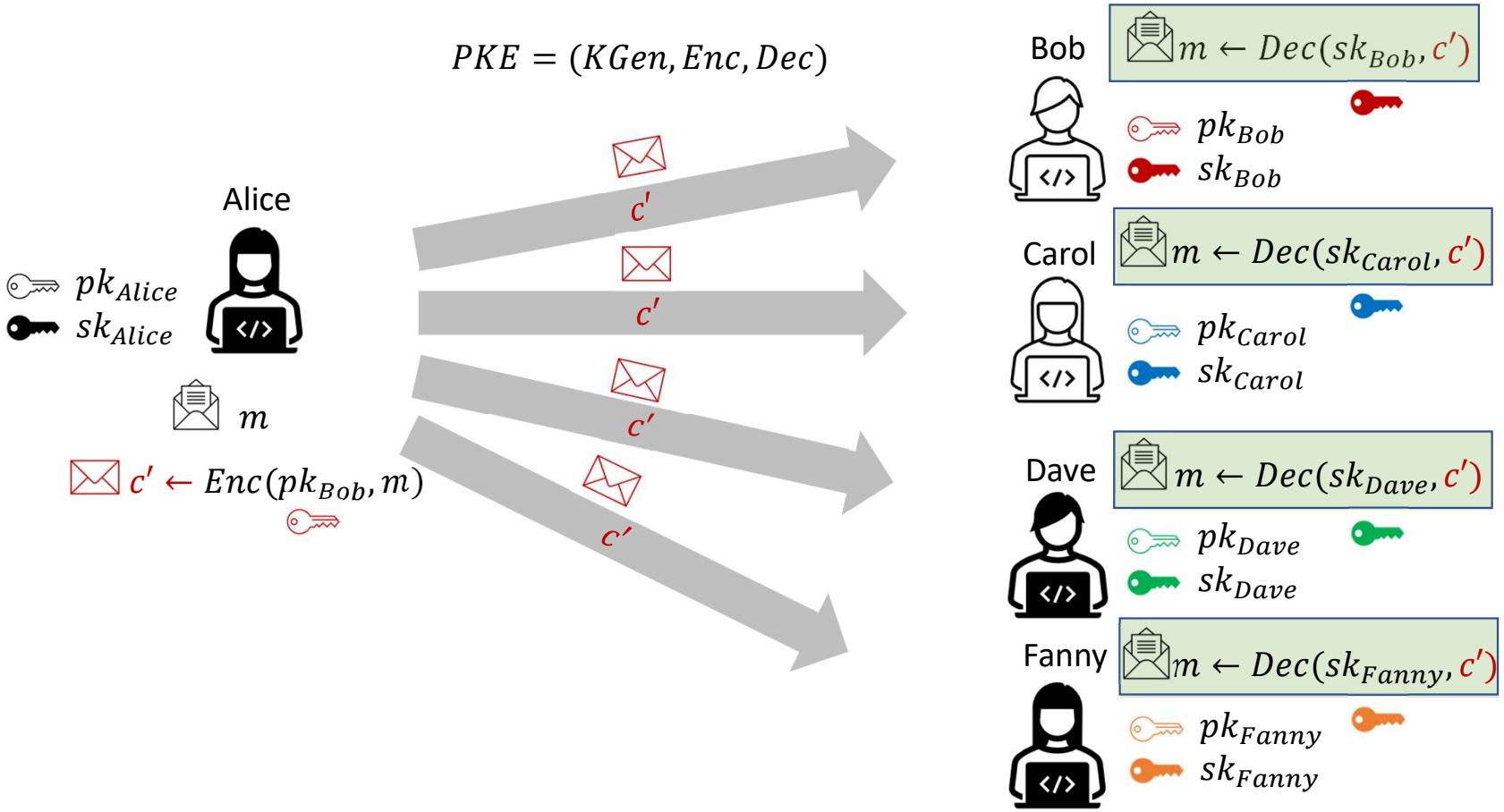
Classic McEliece



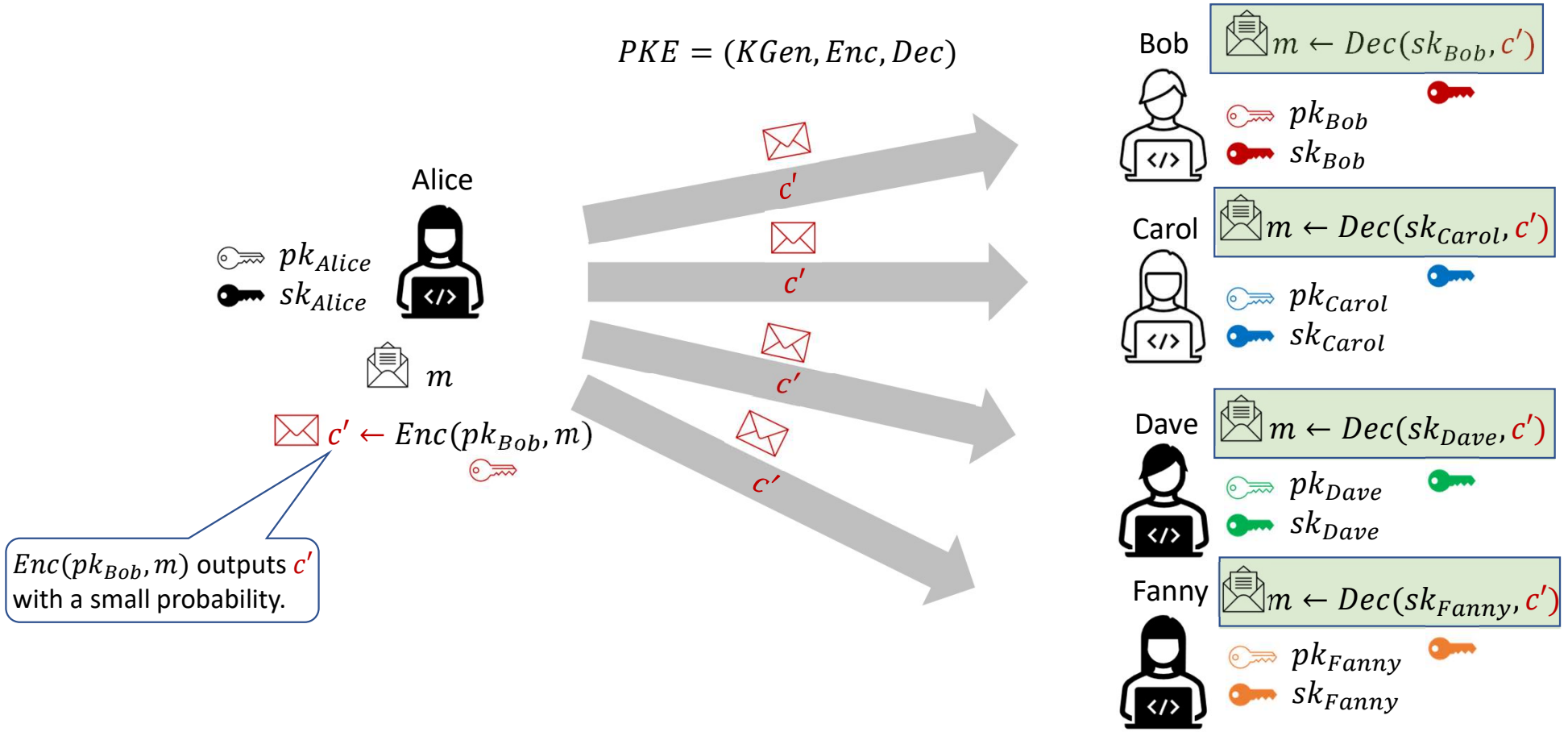
Classic McEliece



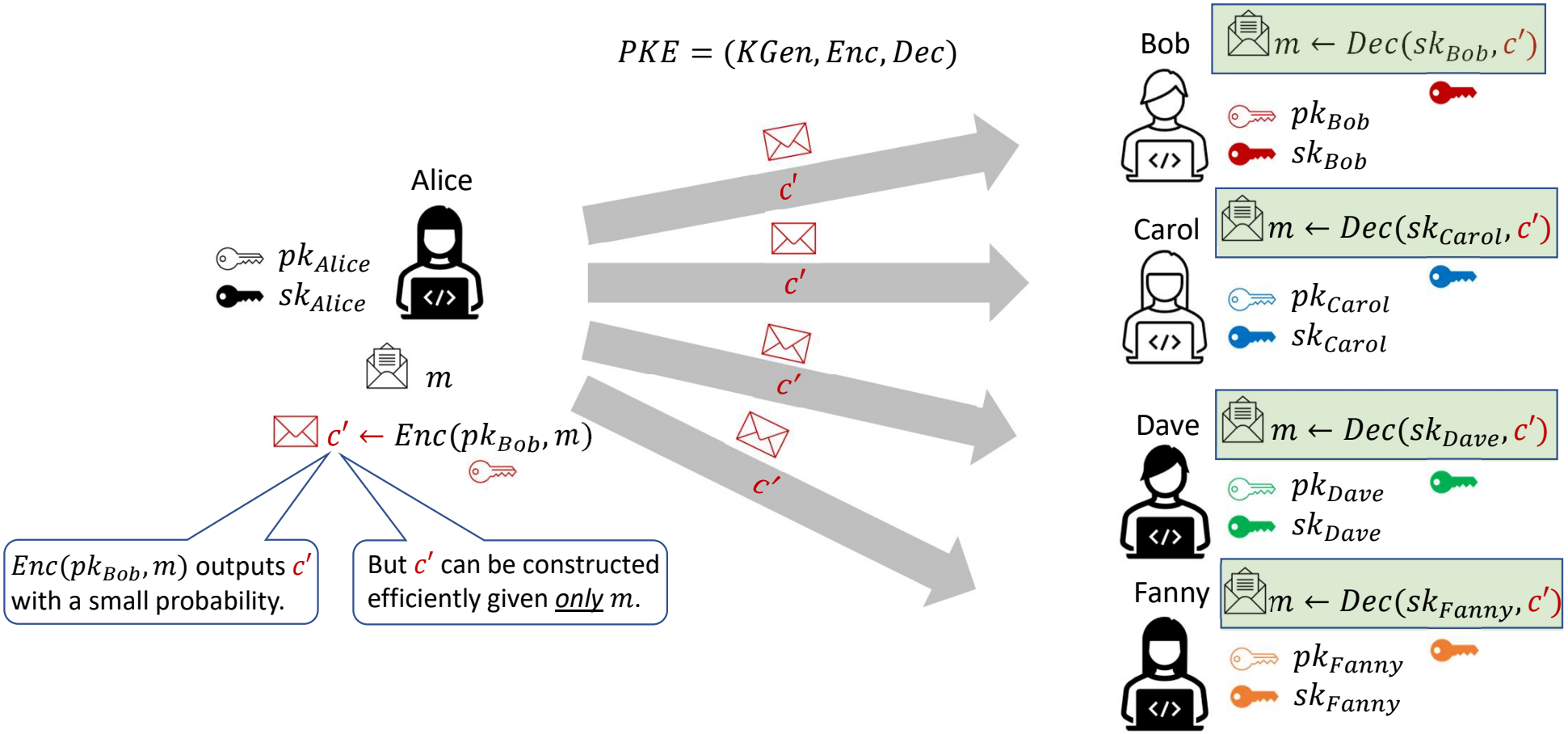
Classic McEliece



Classic McEliece



Classic McEliece



Summary of Our Results

Summary of Our Results

- Classic McEliece cannot be (strongly) robust.

Summary of Our Results

- Classic McEliece cannot be (strongly) robust.
  - As a result, our techniques cannot be used to prove its anonymity.

Summary of Our Results

- Classic McEliece cannot be (strongly) robust.
  - As a result, our techniques cannot be used to prove its anonymity.
  - However, Classic McEliece was shown to offer anonymity in [Xag21].

[Xag21]: Keita Xagawa. *Anonymity of NIST PQC Round 3 KEMs,* EUROCRYPT 2022. [https://eprint.iacr.org/2021/1323.pdf]

Summary of Our Results

- Classic McEliece cannot be (strongly) robust.
  - As a result, our techniques cannot be used to prove its anonymity.
  - However, Classic McEliece was shown to offer anonymity in [Xag21].

- CRYSTALS-KYBER and SABER do result in robust PKE schemes.

[Xag21]: Keita Xagawa. *Anonymity of NIST PQC Round 3 KEMs,* EUROCRYPT 2022. [https://eprint.iacr.org/2021/1323.pdf]

Summary of Our Results

- Classic McEliece cannot be (strongly) robust.
  - As a result, our techniques cannot be used to prove its anonymity.
  - However, Classic McEliece was shown to offer anonymity in [Xag21].

- CRYSTALS-KYBER and SABER do result in robust PKE schemes.
  - But we identified barriers towards proving anonymity of these two schemes.

[Xag21]: Keita Xagawa. *Anonymity of NIST PQC Round 3 KEMs,* EUROCRYPT 2022. [https://eprint.iacr.org/2021/1323.pdf]

Summary of Our Results

- Classic McEliece cannot be (strongly) robust.
  - As a result, our techniques cannot be used to prove its anonymity.
  - However, Classic McEliece was shown to offer anonymity in [Xag21].

- CRYSTALS-KYBER and SABER do result in robust PKE schemes.
  - But we identified barriers towards proving anonymity of these two schemes.
  - Interestingly, these same barriers also imply that the "level" of IND-CCA security offered by these schemes is overestimated by their respective teams.

[Xag21]: Keita Xagawa. *Anonymity of NIST PQC Round 3 KEMs,* EUROCRYPT 2022. [https://eprint.iacr.org/2021/1323.pdf]

Summary of Our Results

- Classic McEliece cannot be (strongly) robust.
  - As a result, our techniques cannot be used to prove its anonymity.
  - However, Classic McEliece was shown to offer anonymity in [Xag21].

- CRYSTALS-KYBER and SABER do result in robust PKE schemes.
  - But we identified barriers towards proving anonymity of these two schemes.
  - Interestingly, these same barriers also imply that the "level" of IND-CCA security offered by these schemes is overestimated by their respective teams.

- FrodoKEM does result in anonymous and robust PKE schemes.

[Xag21]: Keita Xagawa. *Anonymity of NIST PQC Round 3 KEMs,* EUROCRYPT 2022. [https://eprint.iacr.org/2021/1323.pdf]