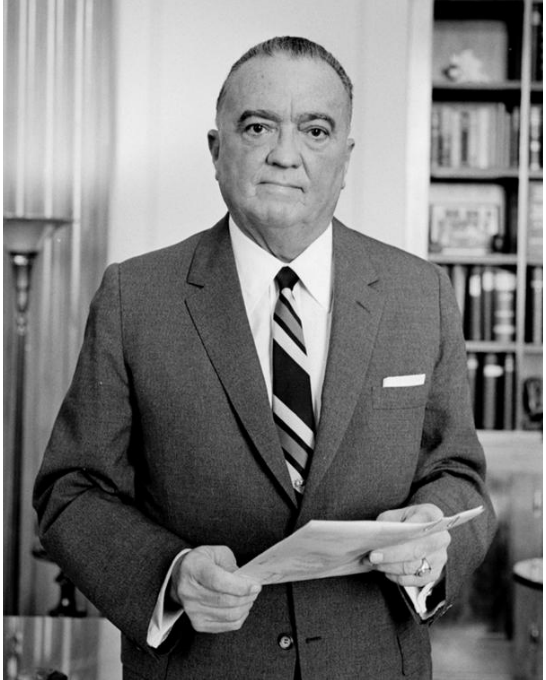
Post-quantum cryptography

Daniel J. Bernstein

University of Illinois at Chicago; Ruhr University Bochum

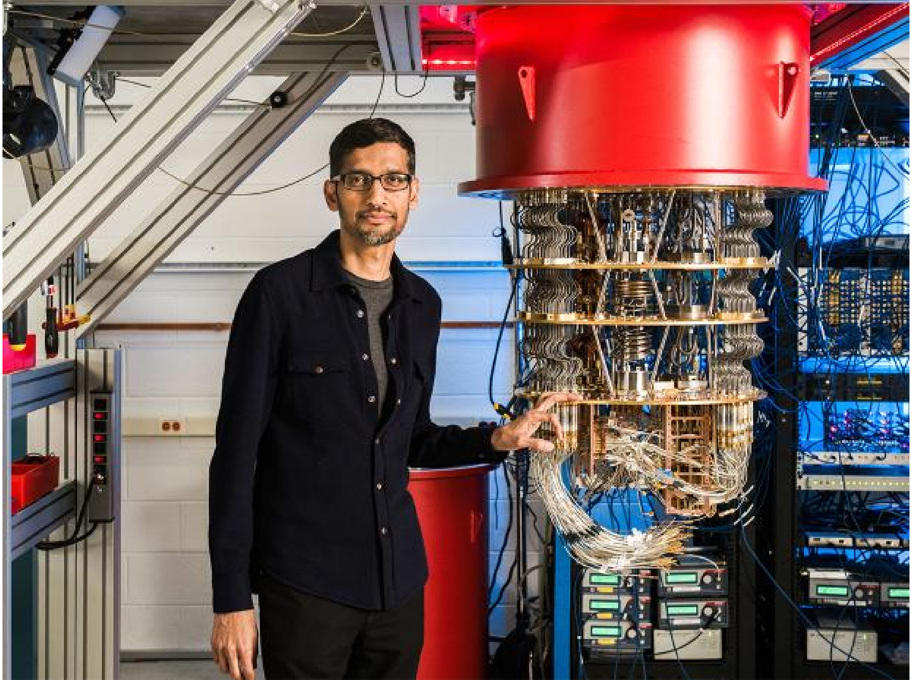


Wikipedia: “Hoover became a controversial figure as evidence of his secretive abuses of power began to surface. He was found to have exceeded the jurisdiction of the FBI, and to have used the FBI to harass political dissenters and activists, to amass secret files on political leaders, and to collect evidence using illegal methods. Hoover consequently amassed a great deal of power and was in a position to intimidate and threaten others, including sitting presidents of the United States.”

Wikipedia: "The **2016 Democratic National Committee email leak** is a collection of Democratic National Committee (DNC) emails stolen by one or more hackers operating under the pseudonym 'Guccifer 2.0' who are alleged to be Russian intelligence agency hackers, according to indictments carried out by the Mueller investigation. These emails were [published] just before the 2016 Democratic National Convention."

Wikipedia: "The **2016 Democratic National Committee email leak** is a collection of Democratic National Committee (DNC) emails stolen by one or more hackers operating under the pseudonym 'Guccifer 2.0' who are alleged to be Russian intelligence agency hackers, according to indictments carried out by the Mueller investigation. These emails were [published] just before the 2016 Democratic National Convention."

Thought experiment: Start from 2016 election results. Switch 5353+11375+22147 R voters to D in MI+WI+PA. $\Rightarrow$ Clinton wins. (Of course there were many other influences on election results.)



Simons Institute “Quantum Wave in Computing” advertising: “The most promising algorithmic application for quantum computers in the long run, their ‘killer app,’ is expected to be the simulation of quantum systems and quantum chemistry.”

Simons Institute “Quantum Wave in Computing” advertising: “The most promising algorithmic application for quantum computers in the long run, their ‘killer app,’ is expected to be the simulation of quantum systems and quantum chemistry.”

— Really? Are you sure the killer app isn’t breaking cryptosystems?

Simons Institute "Quantum Wave in Computing" advertising: "The most promising algorithmic application for quantum computers in the long run, their 'killer app,' is expected to be the simulation of quantum systems and quantum chemistry."

— Really? Are you sure the killer app isn't breaking cryptosystems?

Claimed answer by Troyer, 2015: "Not a long-term 'killer-app' since we can switch to post-quantum encryption."

Simons Institute "Quantum Wave in Computing" advertising: "The most promising algorithmic application for quantum computers in the long run, their 'killer app,' is expected to be the simulation of quantum systems and quantum chemistry."

— Really? Are you sure the killer app isn't breaking cryptosystems?

Claimed answer by Troyer, 2015: "Not a long-term 'killer-app' since we can switch to post-quantum encryption."

— Large-scale attackers are already recording encrypted data today. Nothing we do tomorrow can retroactively protect this data.

Simons Institute "Quantum Wave in Computing" advertising: "The most promising algorithmic application for quantum computers in the long run, their 'killer app,' is expected to be the simulation of quantum systems and quantum chemistry."

— Really? Are you sure the killer app isn't breaking cryptosystems?

Claimed answer by Troyer, 2015: "Not a long-term 'killer-app' since we can switch to post-quantum encryption."

— Large-scale attackers are already recording encrypted data today. Nothing we do tomorrow can retroactively protect this data. Also, *are* we switching to post-quantum crypto?

Simons Institute “Quantum Wave in Computing” advertising: “The most promising algorithmic application for quantum computers in the long run, their ‘killer app,’ is expected to be the simulation of quantum systems and quantum chemistry.”

— Really? Are you sure the killer app isn’t breaking cryptosystems?

Claimed answer by Troyer, 2015: “Not a long-term ‘killer-app’ since we can switch to post-quantum encryption.”

— Large-scale attackers are already recording encrypted data today. Nothing we do tomorrow can retroactively protect this data. Also, *are* we switching to post-quantum crypto? And is it secure?

The goals of cryptography

(Col. Carrington tells me he has sent you the first

volume of the federalist, and adds the 2d. by this conveyance.

mentioned to you that publication

I believe I never have yet 942. 1709. 770. 1234. 698. 802. 193. 310. It

was undertaken last fall by Jay Hamilton and myself

1293. 1054. 475. 640. 293. 139. 1461. 227. 1247. 770. 487. 1004. 872. 951. 440

proposal came from the two former execution was thrown

The 497. 470. 1321. 252. 862. 1090. 1042. 1061. The 577. 918. 1293. 872. 1256.

by the sickness of Jay mostly on the two others

1461. 812. 491. 942. 546. 1302. 227. 1247. 1619. 1898. 1179. 812. 1091. 1727.

carried on in concert the writers are not mutually

Though 1326. 1709. 145. 1557. 1143. 860. 812. 1476. 1155. 470. 549. 757. 929.

all the 471. 812.

answerable ideas of each other

575. 157. 1049. 1645. 979. for 464. 764. 1302. 320. 1727. there being

seldom time for even a perusal pieces by

718. 1440. 1020. 248. 344. 101. 976. 1162. 450. of the 1095. 1186. 683. 1461.

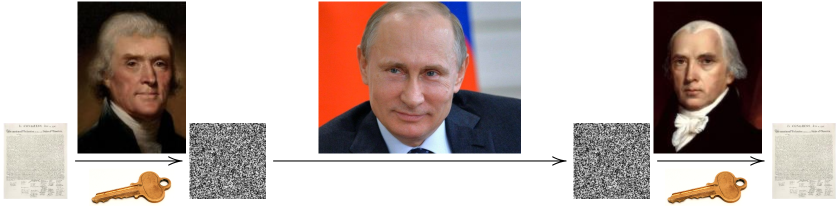
any but the writer before they were wanted at the press

426. 567. 812. 1470. 1155. 172. 1174. 1260. 1201. 920. 1709. 301. 812. 497.

sometimes hardly by the writer himself

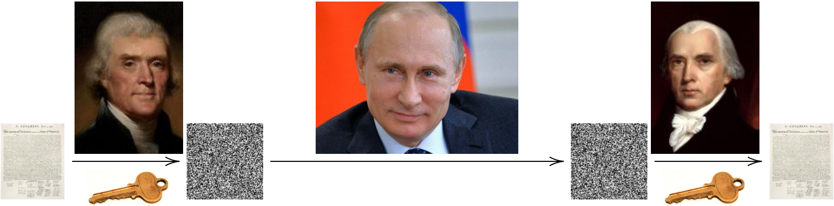
and 475. 1020. 1288. 1597. 1461. 812. 1470. 1155. 925. 440.)

Secret-key encryption



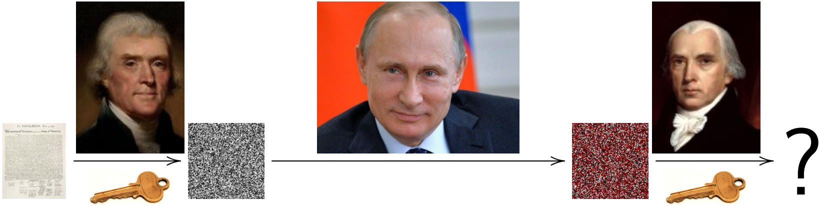
Prerequisite: Thomas and James share a secret key .
Prerequisite: Vladimir doesn't know .
Thomas and James exchange any number of messages.
Security goal #1: **Confidentiality** despite Vladimir's espionage.

Secret-key authenticated encryption



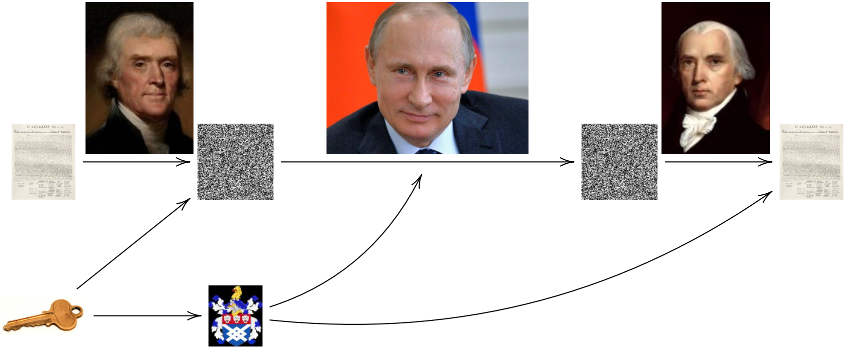
Prerequisite: Thomas and James share a secret key .
Prerequisite: Vladimir doesn't know .
Thomas and James exchange any number of messages.
Security goal #1: **Confidentiality** despite Vladimir's espionage.
Security goal #2: **Integrity**, i.e., recognizing Vladimir's sabotage.

Secret-key authenticated encryption



Prerequisite: Thomas and James share a secret key .
Prerequisite: Vladimir doesn't know .
Thomas and James exchange any number of messages.
Security goal #1: **Confidentiality** despite Vladimir's espionage.
Security goal #2: **Integrity**, i.e., recognizing Vladimir's sabotage.

Public-key signatures



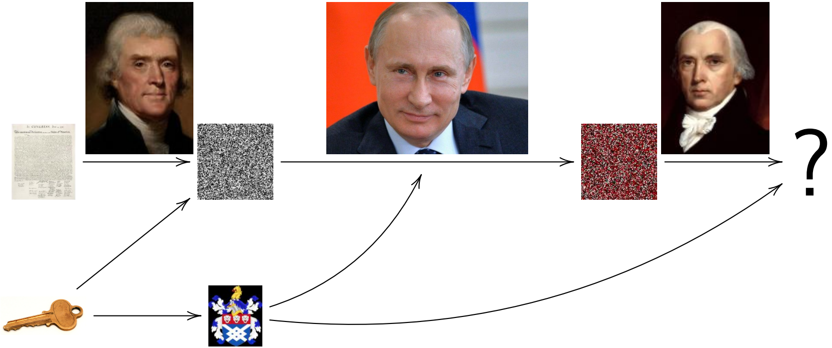
Prerequisite: Thomas has a secret key  and public key .

Prerequisite: Vladimir doesn't know . Everyone knows .

Thomas publishes any number of messages.

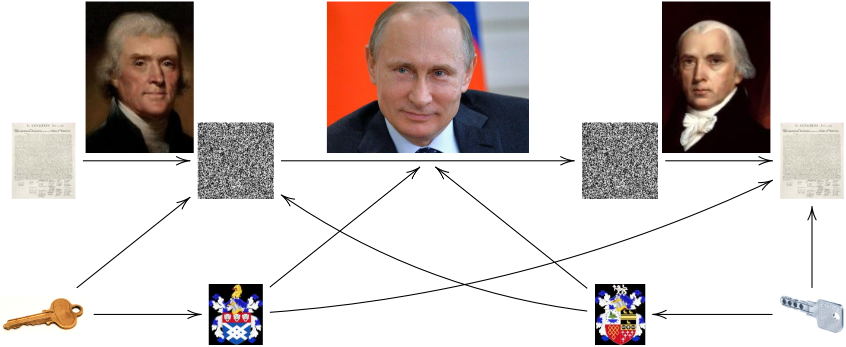
Security goal: Integrity.

Public-key signatures



Prerequisite: Thomas has a secret key  and public key .
Prerequisite: Vladimir doesn't know . Everyone knows .
Thomas publishes any number of messages.
Security goal: Integrity.

Public-key authenticated encryption (“DH” data flow)



Prerequisite: Thomas has a secret key  and public key .
Prerequisite: James has a secret key  and public key .
Thomas and James exchange any number of messages.
Security goal #1: Confidentiality. Security goal #2: Integrity.

Cryptographers study many more security goals

Protecting against denial of service; stopping traffic analysis; securely tallying votes; searching encrypted data; much more.

Cryptographers study many more security goals

Protecting against denial of service; stopping traffic analysis; securely tallying votes; searching encrypted data; much more.

Many intellectually challenging cryptographic research topics

Cryptographers study many more security goals

Protecting against denial of service; stopping traffic analysis; securely tallying votes; searching encrypted data; much more.

Many intellectually challenging cryptographic research topics—distracting attention from the quantum apocalypse.

Cryptographers study many more security goals

Protecting against denial of service; stopping traffic analysis; securely tallying votes; searching encrypted data; much more.

Many intellectually challenging cryptographic research topics— distracting attention from the quantum apocalypse.

Assuming quantum attacks become cheap enough:

- Attackers forge messages if we don't change our systems.
- Attackers read messages if we don't change our systems.
- Attackers read older messages no matter what we do.

How cryptographers try to reach the goals

Many stages of research from design to deployment

Define the goals

Explore space of cryptosystems

Study algorithms for the attackers

Focus on secure cryptosystems

Study algorithms for the users

Study implementations on real hardware

Study side-channel attacks, fault attacks, etc.

Focus on secure, reliable implementations

Focus on implementations meeting performance requirements

Integrate securely into real-world applications

Many stages of research from design to deployment

Warning: waterfall data flow, undesirable.

Define the goals

Explore space of cryptosystems

Study algorithms for the attackers

Focus on secure cryptosystems

Study algorithms for the users

Study implementations on real hardware

Study side-channel attacks, fault attacks, etc.

Focus on secure, reliable implementations

Focus on implementations meeting performance requirements

Integrate securely into real-world applications

Example: The McEliece cryptosystem (1978)

McEliece public key: matrix A over $\mathbf{F}_2 = \{0, 1\}$.
Normally $s \mapsto As$ is injective.

Example: The McEliece cryptosystem (1978)

McEliece public key: matrix A over $\mathbf{F}_2 = \{0, 1\}$.
Normally $s \mapsto As$ is injective.

Ciphertext: vector $C = As + e$.
Uses secret "codeword" As; weight-w "error vector" e.
"Weight" = "Hamming weight" = number of nonzero entries.

Example: The McEliece cryptosystem (1978)

McEliece public key: matrix A over $\mathbf{F}_2 = \{0, 1\}$.
Normally $s \mapsto As$ is injective.

Ciphertext: vector $C = As + e$.
Uses secret "codeword" As; weight-w "error vector" e.
"Weight" = "Hamming weight" = number of nonzero entries.

1978 sizes for 2^{64} security goal: 1024×512 matrix, $w = 50$.
2008 sizes for 2^{256} security goal: 6960×5413 matrix, $w = 119$.

Example: The McEliece cryptosystem (1978)

McEliece public key: matrix A over $\mathbf{F}_2 = \{0, 1\}$.
Normally $s \mapsto As$ is injective.

Ciphertext: vector $C = As + e$.
Uses secret "codeword" As; weight-w "error vector" e.
"Weight" = "Hamming weight" = number of nonzero entries.

1978 sizes for 2^{64} security goal: 1024×512 matrix, $w = 50$.
2008 sizes for 2^{256} security goal: 6960×5413 matrix, $w = 119$.

Public key is secretly generated with "binary Goppa code" structure that allows efficient decoding: $C \mapsto As, e$.

One-wayness (“OW-CPA” $=$ “OW-Passive”)

Fundamental security question:
Given random public key A and ciphertext $As + e$ for random s, e,
can attacker efficiently find s, e?

One-wayness (“OW-CPA” $=$ “OW-Passive”)

Fundamental security question:
Given random public key A and ciphertext $As + e$ for random s, e, can attacker efficiently find s, e?

1962 Prange: simple attack idea guiding sizes in 1978 McEliece.

One-wayness (“OW-CPA” = “OW-Passive”)

Fundamental security question:
Given random public key A and ciphertext $As + e$ for random s, e,
can attacker efficiently find s, e?

1962 Prange: simple attack idea guiding sizes in 1978 McEliece.

The McEliece system (with later key-size optimizations)
uses $(c_0 + o(1))\lambda^2(\lg \lambda)^2$-bit keys as $\lambda \to \infty$ to achieve 2^λ security
against Prange's attack. Here $c_0 \approx 0.7418860694$.

Is the McEliece system really one-way?

25 subsequent papers studying one-wayness of McEliece system:
1981 Clark–Cain, crediting Omura. 1988 Lee–Brickell. 1988 Leon.
1989 Krouk. 1989 Stern. 1989 Dumer. 1990 Coffey–Goodman.
1990 van Tilburg. 1991 Dumer. 1991 Coffey–Goodman–Farrell.
1993 Chabanne–Courteau. 1993 Chabaud. 1994 van Tilburg.
1994 Canteaut–Chabanne. 1998 Canteaut–Chabaud.
1998 Canteaut–Sendrier. 2008 Bernstein–Lange–Peters.
2009 Bernstein–Lange–Peters–van Tilborg. 2009 Finiasz–Sendrier.
2011 Bernstein–Lange–Peters. 2011 May–Meurer–Thomae.
2012 Becker–Joux–May–Meurer. 2013 Hamdaoui–Sendrier.
2015 May–Ozerov. 2016 Canto Torres–Sendrier.

Impact of all this work

The McEliece system
uses $(c_0 + o(1))\lambda^2(\lg \lambda)^2$-bit keys as $\lambda \to \infty$ to achieve 2^λ security against all attacks known today. Same $c_0 \approx 0.7418860694$.

Impact of all this work

The McEliece system
uses $(c_0 + o(1))\lambda^2(\lg \lambda)^2$-bit keys as $\lambda \to \infty$ to achieve 2^λ security against all attacks known today. Same $c_0 \approx 0.7418860694$.

Replacing λ with 2λ stops all known quantum attacks.

Impact of all this work

The McEliece system
uses $(c_0 + o(1))\lambda^2(\lg \lambda)^2$-bit keys as $\lambda \to \infty$ to achieve 2^λ security against all attacks known today. Same $c_0 \approx 0.7418860694$.

Replacing λ with 2λ stops all known quantum attacks.

The attack papers have had an effect on the $o(1)$ terms,
and have slightly changed results for specific λ.
Exact analysis and optimization: harder than asymptotics.
Example of current work: count # quantum gates in algorithms.

Some questions regarding provability

Do we have proofs of these attack costs?

Some questions regarding provability

Do we have proofs of these attack costs?
— No. Analyses make heuristic randomness assumptions.
(But the attack experiments are moderately convincing.)

Some questions regarding provability

Do we have proofs of these attack costs?
— No. Analyses make heuristic randomness assumptions.
(But the attack experiments are moderately convincing.)

Best attack *known*: is there a proof that this is optimal?

Some questions regarding provability

Do we have proofs of these attack costs?
— No. Analyses make heuristic randomness assumptions.
(But the attack experiments are moderately convincing.)

Best attack *known*: is there a proof that this is optimal?
— No. There could be a much better attack.

Some questions regarding provability

Do we have proofs of these attack costs?
— No. Analyses make heuristic randomness assumptions.
(But the attack experiments are moderately convincing.)

Best attack *known*: is there a proof that this is optimal?
— No. There could be a much better attack.

Don't we have "provable security"? One-wayness attack against McEliece provably implies one-wayness attack against uniform random matrix A or distinguisher between McEliece public key and uniform random matrix!

Some questions regarding provability

Do we have proofs of these attack costs?
— No. Analyses make heuristic randomness assumptions.
(But the attack experiments are moderately convincing.)

Best attack *known*: is there a proof that this is optimal?
— No. There could be a much better attack.

Don't we have "provable security"? One-wayness attack against McEliece provably implies one-wayness attack against uniform random matrix A or distinguisher between McEliece public key and uniform random matrix! — Yes, but that doesn't prove security.

Some questions regarding provability

Do we have proofs of these attack costs?
— No. Analyses make heuristic randomness assumptions.
(But the attack experiments are moderately convincing.)

Best attack *known*: is there a proof that this is optimal?
— No. There could be a much better attack.

Don't we have "provable security"? One-wayness attack against McEliece provably implies one-wayness attack against uniform random matrix A or distinguisher between McEliece public key and uniform random matrix! — Yes, but that doesn't prove security.

Are other security systems in better shape?

Some questions regarding provability

Do we have proofs of these attack costs?
— No. Analyses make heuristic randomness assumptions.
(But the attack experiments are moderately convincing.)

Best attack *known*: is there a proof that this is optimal?
— No. There could be a much better attack.

Don't we have "provable security"? One-wayness attack against McEliece provably implies one-wayness attack against uniform random matrix A or distinguisher between McEliece public key and uniform random matrix! — Yes, but that doesn't prove security.

Are other security systems in better shape? — No. Even worse.

Binary Goppa codes (1970)

Parameters: $q \in \{8, 16, 32, \ldots\}$;
$w \in \{2, 3, \ldots, \lfloor (q-1)/\lg q \rfloor\}$; $n \in \{w \lg q + 1, \ldots, q-1, q\}$.

Binary Goppa codes (1970)

Parameters: $q \in \{8, 16, 32, \ldots\}$;
$w \in \{2, 3, \ldots, \lfloor (q-1)/\lg q \rfloor\}$; $n \in \{w \lg q + 1, \ldots, q-1, q\}$.

Secrets: distinct $\alpha_1, \ldots, \alpha_n \in \mathbf{F}_q$;
monic irreducible degree-w polynomial $g \in \mathbf{F}_q[x]$.

Binary Goppa codes (1970)

Parameters: $q \in \{8, 16, 32, \ldots\}$;
$w \in \{2, 3, \ldots, \lfloor (q-1)/\lg q \rfloor\}$; $n \in \{w \lg q + 1, \ldots, q-1, q\}$.

Secrets: distinct $\alpha_1, \ldots, \alpha_n \in \mathbf{F}_q$;
monic irreducible degree-w polynomial $g \in \mathbf{F}_q[x]$.

Goppa code: kernel of the map $v \mapsto \sum_i v_i/(x - \alpha_i)$
from $\mathbf{F}_2^n$ to $\mathbf{F}_q[x]/g$. Normal dimension $n - w \lg q$.

Binary Goppa codes (1970)

Parameters: $q \in \{8, 16, 32, \ldots\}$;
$w \in \{2, 3, \ldots, \lfloor (q-1)/\lg q \rfloor\}$; $n \in \{w \lg q + 1, \ldots, q-1, q\}$.

Secrets: distinct $\alpha_1, \ldots, \alpha_n \in \mathbf{F}_q$;
monic irreducible degree-w polynomial $g \in \mathbf{F}_q[x]$.

Goppa code: kernel of the map $v \mapsto \sum_i v_i/(x - \alpha_i)$
from $\mathbf{F}_2^n$ to $\mathbf{F}_q[x]/g$. Normal dimension $n - w \lg q$.

McEliece uses random matrix A whose image is this code.

Niederreiter key compression (1986)

Generator matrix for code Γ of length n and dimension k:
$n \times k$ matrix G with $\Gamma = G \cdot \mathbf{F}_2^k$.

McEliece public key: G times random $k \times k$ invertible matrix.

Niederreiter key compression (1986)

Generator matrix for code Γ of length n and dimension k:
$n \times k$ matrix G with $\Gamma = G \cdot \mathbf{F}_2^k$.

McEliece public key: G times random $k \times k$ invertible matrix.

Niederreiter instead reduces G to the unique generator matrix in "systematic form": bottom k rows are $k \times k$ identity matrix I_k.
Public key T is top $n - k$ rows.

Niederreiter key compression (1986)

Generator matrix for code Γ of length n and dimension k:
$n \times k$ matrix G with $\Gamma = G \cdot \mathbf{F}_2^k$.

McEliece public key: G times random $k \times k$ invertible matrix.

Niederreiter instead reduces G to the unique generator matrix in "systematic form": bottom k rows are $k \times k$ identity matrix I_k.
Public key T is top $n - k$ rows.

e.g. $n = 6960$, $k = 5413$: was 37674480 bits, now 8373911 bits.

Niederreiter key compression (1986)

Generator matrix for code Γ of length n and dimension k:
$n \times k$ matrix G with $\Gamma = G \cdot \mathbf{F}_2^k$.

McEliece public key: G times random $k \times k$ invertible matrix.

Niederreiter instead reduces G to the unique generator matrix in "systematic form": bottom k rows are $k \times k$ identity matrix I_k.
Public key T is top $n - k$ rows.

e.g. $n = 6960$, $k = 5413$: was 37674480 bits, now 8373911 bits.

Pr $\approx$29% that systematic form exists. Security loss: $<$2 bits.

Niederreiter ciphertext compression (1986)

Use Niederreiter key $A = \begin{pmatrix} T \\ I_k \end{pmatrix}$. McEliece ciphertext: $As + e \in \mathbf{F}_2^n$.

Niederreiter ciphertext compression (1986)

Use Niederreiter key $A = \begin{pmatrix} T \\ \hline I_k \end{pmatrix}$. McEliece ciphertext: $As + e \in \mathbf{F}_2^n$.

Niederreiter ciphertext, shorter: $He \in \mathbf{F}_2^{n-k}$ where $H = (I_{n-k}|T)$.

Niederreiter ciphertext compression (1986)

Use Niederreiter key $A = \begin{pmatrix} T \\ I_k \end{pmatrix}$. McEliece ciphertext: $As + e \in \mathbf{F}_2^n$.

Niederreiter ciphertext, shorter: $He \in \mathbf{F}_2^{n-k}$ where $H = (I_{n-k} | T)$.

e.g. $n = 6960$, $k = 5413$: was 6960 bits, now 1547 bits.

Niederreiter ciphertext compression (1986)

Use Niederreiter key $A = \binom{T}{I_k}$. McEliece ciphertext: $As + e \in \mathbf{F}_2^n$.

Niederreiter ciphertext, shorter: $He \in \mathbf{F}_2^{n-k}$ where $H = (I_{n-k}|T)$.

e.g. $n = 6960$, $k = 5413$: was 6960 bits, now 1547 bits.

Given H and Niederreiter's He, can attacker efficiently find e?

Niederreiter ciphertext compression (1986)

Use Niederreiter key $A = \binom{T}{I_k}$. McEliece ciphertext: $As + e \in \mathbf{F}_2^n$.

Niederreiter ciphertext, shorter: $He \in \mathbf{F}_2^{n-k}$ where $H = (I_{n-k}|T)$.

e.g. $n = 6960$, $k = 5413$: was 6960 bits, now 1547 bits.

Given H and Niederreiter's He, can attacker efficiently find e?

If so, attacker can efficiently find s, e given A and $As + e$: compute $H(As + e) = He$; find e; compute s from As.

Performance concerns have led to much more work

Algorithms and software and hardware for McEliece users: e.g.,

- Efficiently generating weight-w vector e.

Performance concerns have led to much more work

Algorithms and software and hardware for McEliece users: e.g.,

- Efficiently generating weight-w vector e.
- Efficiently decoding binary Goppa codes.

Performance concerns have led to much more work

Algorithms and software and hardware for McEliece users: e.g.,

- Efficiently generating weight-w vector e.
- Efficiently decoding binary Goppa codes.
- Fitting the McEliece cryptosystem into tiny Internet servers.

Performance concerns have led to much more work

Algorithms and software and hardware for McEliece users: e.g.,

- Efficiently generating weight-w vector e.
- Efficiently decoding binary Goppa codes.
- Fitting the McEliece cryptosystem into tiny Internet servers.

Many modified cryptosystems whose security has not been studied as thoroughly: e.g.,

- Replacing binary Goppa codes with other families of codes.

Performance concerns have led to much more work

Algorithms and software and hardware for McEliece users: e.g.,

- Efficiently generating weight-w vector e.
- Efficiently decoding binary Goppa codes.
- Fitting the McEliece cryptosystem into tiny Internet servers.

Many modified cryptosystems whose security has not been studied as thoroughly: e.g.,

- Replacing binary Goppa codes with other families of codes.
- Lattice-based cryptography.

The claimed maturity of lattice attacks

Case study: SVP, the most famous lattice problem.

2006 Silverman: "Lattices, SVP and CVP, have been intensively studied for more than 100 years, both as intrinsic mathematical problems and for applications in pure and applied mathematics, physics and cryptography."

The claimed maturity of lattice attacks

Case study: SVP, the most famous lattice problem.

2006 Silverman: "Lattices, SVP and CVP, have been intensively studied for more than 100 years, both as intrinsic mathematical problems and for applications in pure and applied mathematics, physics and cryptography."

Best SVP algorithms known by 2000:
time $2^{\Theta(N \log N)}$ for almost all dimension-N lattices
(assuming reasonable input lengths, various reasonable heuristics).

The immaturity of lattice attacks

Best SVP algorithms known today: $2^{\Theta(N)}$.

The immaturity of lattice attacks

Best SVP algorithms known today: $2^{\Theta(N)}$.

Approximate c for some algorithms believed to take time $2^{(c+o(1))N}$:
0.415: 2008 Nguyen–Vidick.
0.415: 2010 Micciancio–Voulgaris.

The immaturity of lattice attacks

Best SVP algorithms known today: $2^{\Theta(N)}$.

Approximate c for some algorithms believed to take time $2^{(c+o(1))N}$:
0.415: 2008 Nguyen–Vidick.
0.415: 2010 Micciancio–Voulgaris.
0.384: 2011 Wang–Liu–Tian–Bi.

The immaturity of lattice attacks

Best SVP algorithms known today: $2^{\Theta(N)}$.

Approximate c for some algorithms believed to take time $2^{(c+o(1))N}$:
0.415: 2008 Nguyen–Vidick.
0.415: 2010 Micciancio–Voulgaris.
0.384: 2011 Wang–Liu–Tian–Bi.
0.378: 2013 Zhang–Pan–Hu.

The immaturity of lattice attacks

Best SVP algorithms known today: $2^{\Theta(N)}$.

Approximate c for some algorithms believed to take time $2^{(c+o(1))N}$:
0.415: 2008 Nguyen–Vidick.
0.415: 2010 Micciancio–Voulgaris.
0.384: 2011 Wang–Liu–Tian–Bi.
0.378: 2013 Zhang–Pan–Hu.
0.337: 2014 Laarhoven.

The immaturity of lattice attacks

Best SVP algorithms known today: $2^{\Theta(N)}$.

Approximate c for some algorithms believed to take time $2^{(c+o(1))N}$:
0.415: 2008 Nguyen–Vidick.
0.415: 2010 Micciancio–Voulgaris.
0.384: 2011 Wang–Liu–Tian–Bi.
0.378: 2013 Zhang–Pan–Hu.
0.337: 2014 Laarhoven.
0.298: 2015 Laarhoven–de Weger.
0.292: 2015 Becker–Ducas–Gama–Laarhoven.

The immaturity of lattice attacks

Best SVP algorithms known today: $2^{\Theta(N)}$.

Approximate c for some algorithms believed to take time $2^{(c+o(1))N}$:
0.415: 2008 Nguyen–Vidick.
0.415: 2010 Micciancio–Voulgaris.
0.384: 2011 Wang–Liu–Tian–Bi.
0.378: 2013 Zhang–Pan–Hu.
0.337: 2014 Laarhoven.
0.298: 2015 Laarhoven–de Weger.
0.292: 2015 Becker–Ducas–Gama–Laarhoven.

Lattice crypto: more attack avenues; even less understanding.

Is post-quantum crypto moving quickly enough?

1994: Shor's algorithm.

PQCrypto 2006: International Workshop on Post-Quantum Cryptography. (Coined phrase in 2003.)

Is post-quantum crypto moving quickly enough?

1994: Shor's algorithm.

PQCrypto 2006: International Workshop on Post-Quantum Cryptography. (Coined phrase in 2003.) PQCrypto 2008, PQCrypto 2010, PQCrypto 2011, PQCrypto 2013, PQCrypto 2014.

Is post-quantum crypto moving quickly enough?

1994: Shor's algorithm.

PQCrypto 2006: International Workshop on Post-Quantum Cryptography. (Coined phrase in 2003.) PQCrypto 2008, PQCrypto 2010, PQCrypto 2011, PQCrypto 2013, PQCrypto 2014.

2014: EU solicits grant proposals in post-quantum crypto.

2014: ETSI starts working group on "Quantum-safe" crypto.

2015.04: NIST hosts workshop on post-quantum cryptography.

2015.08: NSA wakes up.

NSA announcements

2015.08.11 announcement:

> *IAD recognizes that there will be a move, in the not distant future, to a quantum resistant algorithm suite.*

NSA announcements

2015.08.11 announcement:

> *IAD recognizes that there will be a move, in the not distant future, to a quantum resistant algorithm suite.*

2015.08.19 revised announcement:

> *IAD will initiate a transition to quantum resistant algorithms in the not too distant future.*

NSA comes late to the party and botches its grand entrance.

NSA announcements

2015.08.11 announcement:

> *IAD recognizes that there will be a move, in the not distant future, to a quantum resistant algorithm suite.*

2015.08.19 revised announcement:

> *IAD will initiate a transition to quantum resistant algorithms in the not too distant future.*

NSA comes late to the party and botches its grand entrance.

Some interesting reactions: "Don't use post-quantum crypto; NSA wants you to use it".

NSA announcements

2015.08.11 announcement:

> *IAD recognizes that there will be a move, in the not distant future, to a quantum resistant algorithm suite.*

2015.08.19 revised announcement:

> *IAD will initiate a transition to quantum resistant algorithms in the not too distant future.*

NSA comes late to the party and botches its grand entrance.

Some interesting reactions: "Don't use post-quantum crypto; NSA wants you to use it". Or "NSA says NIST P-384 is post-quantum secure".

NSA announcements

2015.08.11 announcement:

> *IAD recognizes that there will be a move, in the not distant future, to a quantum resistant algorithm suite.*

2015.08.19 revised announcement:

> *IAD will initiate a transition to quantum resistant algorithms in the not too distant future.*

NSA comes late to the party and botches its grand entrance.

Some interesting reactions: "Don't use post-quantum crypto; NSA wants you to use it". Or "NSA says NIST P-384 is post-quantum secure". Or "NSA has abandoned ECC."

NSA announcements

2015.08.11 announcement:

> *IAD recognizes that there will be a move, in the not distant future, to a quantum resistant algorithm suite.*

2015.08.19 revised announcement:

> *IAD will initiate a transition to quantum resistant algorithms in the not too distant future.*

NSA comes late to the party and botches its grand entrance.

Some interesting reactions: "Don't use post-quantum crypto; NSA wants you to use it". Or "NSA says NIST P-384 is post-quantum secure". Or "NSA has abandoned ECC." Or "NSA can break lattices and wants you to use them."

PQCrypto 2016: >200 people

PQCrypto 2018: 350 people

Rewinding to 2016 . . .

More reactions by government agencies:

- NSA posts another statement.
- NCSC UK posts statement on the threat to cryptography and statement on quantum key distribution.
- NCSC NL posts statement.
- After public input, NIST calls for submissions of public-key systems to "Post-Quantum Cryptography Standardization Project". Deadline 2017.11.

2017: Submissions to the NIST competition

21 December 2017: NIST posts 69 submissions from 260 people.

BIG QUAKE. BIKE. CFPKM. Classic McEliece. Compact LWE. CRYSTALS-DILITHIUM. CRYSTALS-KYBER. DAGS. Ding Key Exchange. DME. DRS. DualModeMS. Edon-K. EMBLEM and R.EMBLEM. FALCON. FrodoKEM. GeMSS. Giophantus. Gravity-SPHINCS. Guess Again. Gui. HILA5. HiMQ-3. HK17. HQC. KINDI. LAC. LAKE. LEDAkem. LEDApkc. Lepton. LIMA. Lizard. LOCKER. LOTUS. LUOV. McNie. Mersenne-756839. MQDSS. NewHope. NTRUEncrypt. pqNTRUSign. NTRU-HRSS-KEM. NTRU Prime. NTS-KEM. Odd Manhattan. OKCN/AKCN/CNKE. Ouroboros-R. Picnic. pqRSA encryption. pqRSA signature. pqsigRM. QC-MDPC KEM. qTESLA. RaCoSS. Rainbow. Ramstake. RankSign. RLCE-KEM. Round2. RQC. RVB. SABER. SIKE. SPHINCS+. SRTPI. Three Bears. Titanium. WalnutDSA.

Some submissions are broken within days

By end of 2017: 8 out of 69 submissions attacked.

BIG QUAKE. BIKE. CFPKM. Classic McEliece. Compact LWE. CRYSTALS-DILITHIUM. CRYSTALS-KYBER. DAGS. Ding Key Exchange. DME. DRS. DualModeMS. Edon-K. EMBLEM and R.EMBLEM. FALCON. FrodoKEM. GeMSS. Giophantus. Gravity-SPHINCS. Guess Again. Gui. HILA5. HiMQ-3. HK17. HQC. KINDI. LAC. LAKE. LEDAkem. LEDApkc. Lepton. LIMA. Lizard. LOCKER. LOTUS. LUOV. McNie. Mersenne-756839. MQDSS. NewHope. NTRUEncrypt. pqNTRUSign. NTRU-HRSS-KEM. NTRU Prime. NTS-KEM. Odd Manhattan. OKCN/AKCN/CNKE. Ouroboros-R. Picnic. pqRSA encryption. pqRSA signature. pqsigRM. QC-MDPC KEM. qTESLA. RaCoSS. Rainbow. Ramstake. RankSign. RLCE-KEM. Round2. RQC. RVB. SABER. SIKE. SPHINCS+. SRTPI. Three Bears. Titanium. WalnutDSA.

Some less secure than claimed; some smashed; some attack scripts.

Do cryptographers have any idea what they're doing?

By end of 2018: 22 out of 69 submissions attacked.

BIG QUAKE. BIKE. CFPKM. Classic McEliece. Compact LWE. CRYSTALS-DILITHIUM. CRYSTALS-KYBER. DAGS. Ding Key Exchange. DME. DRS. DualModeMS. Edon-K. EMBLEM and R.EMBLEM. FALCON. FrodoKEM. GeMSS. Giophantus. Gravity-SPHINCS. Guess Again. Gui. HILA5. HiMQ-3. HK17. HQC. KINDI. LAC. LAKE. LEDAkem. LEDApkc. Lepton. LIMA. Lizard. LOCKER. LOTUS. LUOV. McNie. Mersenne-756839. MQDSS. NewHope. NTRUEncrypt. pqNTRUSign. NTRU-HRSS-KEM. NTRU Prime. NTS-KEM. Odd Manhattan. OKCN/AKCN/CNKE. Ouroboros-R. Picnic. pqRSA encryption. pqRSA signature. pqsigRM. QC-MDPC KEM. qTESLA. RaCoSS. Rainbow. Ramstake. RankSign. RLCE-KEM. Round2. RQC. RVB. SABER. SIKE. SPHINCS+. SRTPI. Three Bears. Titanium. WalnutDSA.

Some less secure than claimed; some smashed; some attack scripts.

Do cryptographers have any idea what they're doing?

By end of 2019: 30 out of 69 submissions attacked.

BIG QUAKE. BIKE. CFPKM. Classic McEliece. Compact LWE. CRYSTALS-DILITHIUM. CRYSTALS-KYBER. DAGS. Ding Key Exchange. DME. DRS. DualModeMS. Edon-K. EMBLEM and R.EMBLEM. FALCON. FrodoKEM. GeMSS. Giophantus. Gravity-SPHINCS. Guess Again. Gui. HILA5. HiMQ-3. HK17. HQC. KINDI. LAC. LAKE. LEDAkem. LEDApkc. Lepton. LIMA. Lizard. LOCKER. LOTUS. LUOV. McNie. Mersenne-756839. MQDSS. NewHope. NTRUEncrypt. pqNTRUSign. NTRU-HRSS-KEM. NTRU Prime. NTS-KEM. Odd Manhattan. OKCN/AKCN/CNKE. Ouroboros-R. Picnic. pqRSA encryption. pqRSA signature. pqsigRM. QC-MDPC KEM. qTESLA. RaCoSS. Rainbow. Ramstake. RankSign. RLCE-KEM. Round2. RQC. RVB. SABER. SIKE. SPHINCS+. SRTPI. Three Bears. Titanium. WalnutDSA.

Some less secure than claimed; some smashed; some attack scripts.

An attempt to explain the situation

People often categorize submissions. Examples of categories:

- Code-based encryption and signatures.
- Hash-based signatures.
- Isogeny-based encryption.
- Lattice-based encryption and signatures.
- Multivariate-quadratic encryption and signatures.

An attempt to explain the situation

"What's safe is lattice-based cryptography." — Are you sure?

An attempt to explain the situation

"What's safe is lattice-based cryptography." — Are you sure?

Lattice-based submissions: Compact LWE. CRYSTALS-DILITHIUM. CRYSTALS-KYBER. Ding Key Exchange. DRS. EMBLEM and R.EMBLEM. FALCON. FrodoKEM. HILA5. KINDI. LAC. LIMA. Lizard. LOTUS. NewHope. NTRUEncrypt. NTRU-HRSS-KEM. NTRU Prime. Odd Manhattan. OKCN/AKCN/CNKE. pqNTRUSign. qTESLA. Round2. SABER. Titanium.

An attempt to explain the situation

"What's safe is lattice-based cryptography." — Are you sure?

Lattice-based submissions: Compact LWE. CRYSTALS-DILITHIUM. CRYSTALS-KYBER. Ding Key Exchange. DRS. EMBLEM and R.EMBLEM. FALCON. FrodoKEM. HILA5. KINDI. LAC. LIMA. Lizard. LOTUS. NewHope. NTRUEncrypt. NTRU-HRSS-KEM. NTRU Prime. Odd Manhattan. OKCN/AKCN/CNKE. pqNTRUSign. qTESLA. Round2. SABER. Titanium.

Lattice security estimates are so imprecise that nobody is sure whether the remaining submissions are damaged by a 2019 paper solving a lattice problem "more than a million times faster".

Call for merged submissions

"NIST would like to encourage any submissions which are quite similar to consider merging."

Call for merged submissions

"NIST would like to encourage any submissions which are quite similar to consider merging."

"While the selection of candidates for the second round will primarily be based on the original submissions, NIST may consider a merged submission more attractive than either of the original schemes if it provides improvements in security, efficiency, or compactness and generality of presentation. At the very least, NIST will accept a merged submission to the second round if either of the submissions being merged would have been accepted."

Call for merged submissions

“NIST would like to encourage any submissions which are quite similar to consider merging.”

“While the selection of candidates for the second round will primarily be based on the original submissions, NIST may consider a merged submission more attractive than either of the original schemes if it provides improvements in security, efficiency, or compactness and generality of presentation. At the very least, NIST will accept a merged submission to the second round if either of the submissions being merged would have been accepted.”

“Submissions should only merge which are similar, and the merged submission should be in the span of the two original submissions.”

2018.08: first merge announcement

2018.08.04: HILA5 and Round2 merge to form Round5.

“The papers show that Round5 is a leading lattice-based candidate in terms of security, bandwidth and CPU performance.”

2018.08: first merge announcement

2018.08.04: HILA5 and Round2 merge to form Round5.

“The papers show that Round5 is a leading lattice-based candidate in terms of security, bandwidth and CPU performance.”

2018.08.24: Hamburg announces major vulnerability in Round5.

- Decryption failures are much more likely than claimed.
- For many earlier lattice systems, presumably also for Round5: can break system using a small number of decryption failures.
- Underlying mistake wasn’t in HILA5, wasn’t in Round2.

2018.08: first merge announcement

2018.08.04: HILA5 and Round2 merge to form Round5.

"The papers show that Round5 is a leading lattice-based candidate in terms of security, bandwidth and CPU performance."

2018.08.24: Hamburg announces major vulnerability in Round5.

- Decryption failures are much more likely than claimed.
- For many earlier lattice systems, presumably also for Round5: can break system using a small number of decryption failures.
- Underlying mistake wasn't in HILA5, wasn't in Round2.

Round5 response: "proposed fix"; "looking at the security proof adjustments"; "actual Round5 proposal to NIST is still months away."

National Academy of Sciences report

Don't panic. "Key Finding 1: Given the current state of quantum computing and recent rates of progress, it is highly unexpected that a quantum computer that can compromise RSA 2048 or comparable discrete logarithm-based public key cryptosystems will be built within the next decade."

National Academy of Sciences report

Don't panic. "Key Finding 1: Given the current state of quantum computing and recent rates of progress, it is highly unexpected that a quantum computer that can compromise RSA 2048 or comparable discrete logarithm-based public key cryptosystems will be built within the next decade."

Panic. "Key Finding 10: Even if a quantum computer that can decrypt current cryptographic ciphers is more than a decade off, the hazard of such a machine is high enough—and the time frame for transitioning to a new security protocol is sufficiently long and uncertain—that prioritization of the development, standardization, and deployment of post-quantum cryptography is critical for minimizing the chance of a potential security and privacy disaster."