The KpqC competition & comparisons to other PQC competitions

Tanja Lange

Eindhoven University of Technology

14 November 2023

Attack timeline: month 0 of NIST post-quantum competition

2017.11.30 Deadline for submissions to NIST; some submissions are announced online.

Attack timeline: month 0 of NIST post-quantum competition

2017.11.30 Deadline for submissions to NIST; some submissions are announced online.

2017.12.18 Bernstein–Groot Bruinderink–Panny–Lange: script breaking CCA for HILA5.

Attack timeline: month 0 of NIST post-quantum competition

2017.11.30 Deadline for submissions to NIST; some submissions are announced online.

2017.12.18 Bernstein–Groot Bruinderink–Panny–Lange: script breaking CCA for HILA5.

2017.12.21 NIST posts 69 "complete and proper" submissions from 260 people; very few conservative submissions; heavy emphasis on performance.

Attack timeline: month 0 of NIST post-quantum competition

2017.11.30 Deadline for submissions to NIST; some submissions are announced online.

2017.12.18 Bernstein–Groot Bruinderink–Panny–Lange: script breaking CCA for HILA5.

2017.12.21 NIST posts 69 "complete and proper" submissions from 260 people; very few conservative submissions; heavy emphasis on performance.

2017.12.21 Panny: script breaking Guess Again.

Attack timeline: month 0 of NIST post-quantum competition

2017.11.30 Deadline for submissions to NIST; some submissions are announced online.

2017.12.18 Bernstein–Groot Bruinderink–Panny–Lange: script breaking CCA for HILA5.

2017.12.21 NIST posts 69 "complete and proper" submissions from 260 people; very few conservative submissions; heavy emphasis on performance.

2017.12.21 Panny: script breaking Guess Again.

2017.12.23 Hülsing–Bernstein–Panny–Lange: scripts breaking RaCoSS.

Attack timeline: month 0 of NIST post-quantum competition

2017.11.30 Deadline for submissions to NIST; some submissions are announced online.

2017.12.18 Bernstein–Groot Bruinderink–Panny–Lange: script breaking CCA for HILA5.

2017.12.21 NIST posts 69 "complete and proper" submissions from 260 people; very few conservative submissions; heavy emphasis on performance.

2017.12.21 Panny: script breaking Guess Again.

2017.12.23 Hülsing–Bernstein–Panny–Lange: scripts breaking RaCoSS.

2017.12.25 Panny: script breaking RVB; RVB withdrawn.

Attack timeline: month 0 of NIST post-quantum competition

2017.11.30 Deadline for submissions to NIST; some submissions are announced online.

2017.12.18 Bernstein–Groot Bruinderink–Panny–Lange: script breaking CCA for HILA5.

2017.12.21 NIST posts 69 "complete and proper" submissions from 260 people; very few conservative submissions; heavy emphasis on performance.

2017.12.21 Panny: script breaking Guess Again.

2017.12.23 Hülsing–Bernstein–Panny–Lange: scripts breaking RaCoSS.

2017.12.25 Panny: script breaking RVB; RVB withdrawn.

2017.12.25 Bernstein–Lange: script breaking HK17.

Attack timeline: month 0 of NIST post-quantum competition

2017.11.30 Deadline for submissions to NIST; some submissions are announced online.

2017.12.18 Bernstein–Groot Bruinderink–Panny–Lange: script breaking CCA for HILA5.

2017.12.21 NIST posts 69 "complete and proper" submissions from 260 people; very few conservative submissions; heavy emphasis on performance.

2017.12.21 Panny: script breaking Guess Again.

2017.12.23 Hülsing–Bernstein–Panny–Lange: scripts breaking RaCoSS.

2017.12.25 Panny: script breaking RVB; RVB withdrawn.

2017.12.25 Bernstein–Lange: script breaking HK17.

2017.12.26 Gaborit: attack reducing McNie security level.

Attack timeline: month 0 of NIST post-quantum competition

2017.11.30 Deadline for submissions to NIST; some submissions are announced online.

2017.12.18 Bernstein–Groot Bruinderink–Panny–Lange: script breaking CCA for HILA5.

2017.12.21 NIST posts 69 "complete and proper" submissions from 260 people; very few conservative submissions; heavy emphasis on performance.

2017.12.21 Panny: script breaking Guess Again.

2017.12.23 Hülsing–Bernstein–Panny–Lange: scripts breaking RaCoSS.

2017.12.25 Panny: script breaking RVB; RVB withdrawn.

2017.12.25 Bernstein–Lange: script breaking HK17.

2017.12.26 Gaborit: attack reducing McNie security level.

2017.12.29 Gaborit: attack reducing Lepton security level.

Attack timeline: month 0 of NIST post-quantum competition

2017.11.30 Deadline for submissions to NIST; some submissions are announced online.

2017.12.18 Bernstein–Groot Bruinderink–Panny–Lange: script breaking CCA for HILA5.

2017.12.21 NIST posts 69 "complete and proper" submissions from 260 people; very few conservative submissions; heavy emphasis on performance.

2017.12.21 Panny: script breaking Guess Again.

2017.12.23 Hülsing–Bernstein–Panny–Lange: scripts breaking RaCoSS.

2017.12.25 Panny: script breaking RVB; RVB withdrawn.

2017.12.25 Bernstein–Lange: script breaking HK17.

2017.12.26 Gaborit: attack reducing McNie security level.

2017.12.29 Gaborit: attack reducing Lepton security level.

2017.12.29 Beullens: attack reducing DME security level.

Attack timeline: month 1

2018.01.01 Bernstein, building on Bernstein–Lange, Wang–Malluhi, Li–Liu–Pan–Xie: faster script breaking HK17; HK17 withdrawn.

Attack timeline: month 1

2018.01.01 Bernstein, building on Bernstein–Lange, Wang–Malluhi, Li–Liu–Pan–Xie: faster script breaking HK17; HK17 withdrawn.

2018.01.02 Steinfeld, independently Albrecht–Postlethwaite–Virdia: script breaking CFPKM.

Attack timeline: month 1

2018.01.01 Bernstein, building on Bernstein–Lange, Wang–Malluhi, Li–Liu–Pan–Xie: faster script breaking HK17; HK17 withdrawn.

2018.01.02 Steinfeld, independently Albrecht–Postlethwaite–Virdia: script breaking CFPKM.

2018.01.02 Alperin-Sheriff–Perlner: attack breaking pqsigRM.

Attack timeline: month 1

2018.01.01 Bernstein, building on Bernstein–Lange, Wang–Malluhi, Li–Liu–Pan–Xie: faster script breaking HK17; HK17 withdrawn.

2018.01.02 Steinfeld, independently Albrecht–Postlethwaite–Virdia: script breaking CFPKM.

2018.01.02 Alperin-Sheriff–Perlner: attack breaking pqsigRM.

2018.01.04 Yang–Bernstein–Lange: script breaking SRTPI; SRTPI withdrawn.

Attack timeline: month 1

2018.01.01 Bernstein, building on Bernstein–Lange, Wang–Malluhi, Li–Liu–Pan–Xie: faster script breaking HK17; HK17 withdrawn.

2018.01.02 Steinfeld, independently Albrecht–Postlethwaite–Virdia: script breaking CFPKM.

2018.01.02 Alperin-Sheriff–Perlner: attack breaking pqsigRM.

2018.01.04 Yang–Bernstein–Lange: script breaking SRTPI; SRTPI withdrawn.

2018.01.05 Lequesne–Sendrier–Tillich: attack breaking Edon-K; script posted 2018.02.20; Edon-K withdrawn.

Attack timeline: month 1

2018.01.01 Bernstein, building on Bernstein–Lange, Wang–Malluhi, Li–Liu–Pan–Xie: faster script breaking HK17; HK17 withdrawn.

2018.01.02 Steinfeld, independently Albrecht–Postlethwaite–Virdia: script breaking CFPKM.

2018.01.02 Alperin-Sheriff–Perlner: attack breaking pqsigRM.

2018.01.04 Yang–Bernstein–Lange: script breaking SRTPI; SRTPI withdrawn.

2018.01.05 Lequesne–Sendrier–Tillich: attack breaking Edon-K; script posted 2018.02.20; Edon-K withdrawn.

2018.01.05 Beullens: script breaking DME.

Attack timeline: month 1

2018.01.01 Bernstein, building on Bernstein–Lange, Wang–Malluhi, Li–Liu–Pan–Xie: faster script breaking HK17; HK17 withdrawn.

2018.01.02 Steinfeld, independently Albrecht–Postlethwaite–Virdia: script breaking CFPKM.

2018.01.02 Alperin-Sheriff–Perlner: attack breaking pqsigRM.

2018.01.04 Yang–Bernstein–Lange: script breaking SRTPI; SRTPI withdrawn.

2018.01.05 Lequesne–Sendrier–Tillich: attack breaking Edon-K; script posted 2018.02.20; Edon-K withdrawn.

2018.01.05 Beullens: script breaking DME.

2018.01.05 Li–Liu–Pan–Xie, independently Bootle–Tibouchi–Xagawa: attack breaking Compact LWE; script from 2nd team.

Attack timeline: month 1

2018.01.01 Bernstein, building on Bernstein–Lange, Wang–Malluhi, Li–Liu–Pan–Xie: faster script breaking HK17; HK17 withdrawn.

2018.01.02 Steinfeld, independently Albrecht–Postlethwaite–Virdia: script breaking CFPKM.

2018.01.02 Alperin-Sheriff–Perlner: attack breaking pqsigRM.

2018.01.04 Yang–Bernstein–Lange: script breaking SRTPI; SRTPI withdrawn.

2018.01.05 Lequesne–Sendrier–Tillich: attack breaking Edon-K; script posted 2018.02.20; Edon-K withdrawn.

2018.01.05 Beullens: script breaking DME.

2018.01.05 Li–Liu–Pan–Xie, independently Bootle–Tibouchi–Xagawa: attack breaking Compact LWE; script from 2nd team.

2018.01.11 Castryck–Vercauteren: attack breaking Giophantus.

Attack timeline: month 1

2018.01.01 Bernstein, building on Bernstein–Lange, Wang–Malluhi, Li–Liu–Pan–Xie: faster script breaking HK17; HK17 withdrawn.

2018.01.02 Steinfeld, independently Albrecht–Postlethwaite–Virdia: script breaking CFPKM.

2018.01.02 Alperin-Sheriff–Perlner: attack breaking pqsigRM.

2018.01.04 Yang–Bernstein–Lange: script breaking SRTPI; SRTPI withdrawn.

2018.01.05 Lequesne–Sendrier–Tillich: attack breaking Edon-K; script posted 2018.02.20; Edon-K withdrawn.

2018.01.05 Beullens: script breaking DME.

2018.01.05 Li–Liu–Pan–Xie, independently Bootle–Tibouchi–Xagawa: attack breaking Compact LWE; script from 2nd team.

2018.01.11 Castryck–Vercauteren: attack breaking Giophantus.

2018.01.22 Blackburn: attack reducing WalnutDSA security level.

Attack timeline: month 1

2018.01.01 Bernstein, building on Bernstein–Lange, Wang–Malluhi, Li–Liu–Pan–Xie: faster script breaking HK17; HK17 withdrawn.

2018.01.02 Steinfeld, independently Albrecht–Postlethwaite–Virdia: script breaking CFPKM.

2018.01.02 Alperin-Sheriff–Perlner: attack breaking pqsigRM.

2018.01.04 Yang–Bernstein–Lange: script breaking SRTPI; SRTPI withdrawn.

2018.01.05 Lequesne–Sendrier–Tillich: attack breaking Edon-K; script posted 2018.02.20; Edon-K withdrawn.

2018.01.05 Beullens: script breaking DME.

2018.01.05 Li–Liu–Pan–Xie, independently Bootle–Tibouchi–Xagawa: attack breaking Compact LWE; script from 2nd team.

2018.01.11 Castryck–Vercauteren: attack breaking Giophantus.

2018.01.22 Blackburn: attack reducing WalnutDSA security level.

2018.01.23 Beullens: another attack reducing WalnutDSA security level.

Attack timeline: round 1 continues

2018.02.01 Beullens: attack breaking WalnutDSA.

Attack timeline: round 1 continues

2018.02.01 Beullens: attack breaking WalnutDSA.

2018.02.07 Fabsic–Hromada–Zajac: attack breaking CCA for LEDA.

Attack timeline: round 1 continues

2018.02.01 Beullens: attack breaking WalnutDSA.

2018.02.07 Fabsic–Hromada–Zajac: attack breaking CCA for LEDA.

2018.03.27 Yu–Ducas: attack reducing DRS security level.

Attack timeline: round 1 continues

2018.02.01 Beullens: attack breaking WalnutDSA.

2018.02.07 Fabsic–Hromada–Zajac: attack breaking CCA for LEDA.

2018.03.27 Yu–Ducas: attack reducing DRS security level.

2018.04.03 Debris-Alazard–Tillich: attack breaking RankSign; RankSign withdrawn.

Attack timeline: round 1 continues

2018.02.01 Beullens: attack breaking WalnutDSA.

2018.02.07 Fabsic–Hromada–Zajac: attack breaking CCA for LEDA.

2018.03.27 Yu–Ducas: attack reducing DRS security level.

2018.04.03 Debris-Alazard–Tillich: attack breaking RankSign; RankSign withdrawn.

2018.04.04 Beullens–Blackburn: script breaking WalnutDSA.

Attack timeline: round 1 continues

2018.02.01 Beullens: attack breaking WalnutDSA.

2018.02.07 Fabsic–Hromada–Zajac: attack breaking CCA for LEDA.

2018.03.27 Yu–Ducas: attack reducing DRS security level.

2018.04.03 Debris-Alazard–Tillich: attack breaking RankSign; RankSign withdrawn.

2018.04.04 Beullens–Blackburn: script breaking WalnutDSA.

2018.05.09 Kotov–Menshov–Ushakov: another attack breaking WalnutDSA.

Attack timeline: round 1 continues

2018.02.01 Beullens: attack breaking WalnutDSA.

2018.02.07 Fabsic–Hromada–Zajac: attack breaking CCA for LEDA.

2018.03.27 Yu–Ducas: attack reducing DRS security level.

2018.04.03 Debris-Alazard–Tillich: attack breaking RankSign; RankSign withdrawn.

2018.04.04 Beullens–Blackburn: script breaking WalnutDSA.

2018.05.09 Kotov–Menshov–Ushakov: another attack breaking WalnutDSA.

2018.05.16 Barelli–Couvreur: attack reducing DAGS security level.

Attack timeline: round 1 continues

2018.02.01 Beullens: attack breaking WalnutDSA.

2018.02.07 Fabsic–Hromada–Zajac: attack breaking CCA for LEDA.

2018.03.27 Yu–Ducas: attack reducing DRS security level.

2018.04.03 Debris-Alazard–Tillich: attack breaking RankSign; RankSign withdrawn.

2018.04.04 Beullens–Blackburn: script breaking WalnutDSA.

2018.05.09 Kotov–Menshov–Ushakov: another attack breaking WalnutDSA.

2018.05.16 Barelli–Couvreur: attack reducing DAGS security level.

2018.05.30 Couvreur–Lequesne–Tillich: attack breaking "short" parameters for RLCE.

Attack timeline: round 1 continues

2018.02.01 Beullens: attack breaking WalnutDSA.

2018.02.07 Fabsic–Hromada–Zajac: attack breaking CCA for LEDA.

2018.03.27 Yu–Ducas: attack reducing DRS security level.

2018.04.03 Debris-Alazard–Tillich: attack breaking RankSign; RankSign withdrawn.

2018.04.04 Beullens–Blackburn: script breaking WalnutDSA.

2018.05.09 Kotov–Menshov–Ushakov: another attack breaking WalnutDSA.

2018.05.16 Barelli–Couvreur: attack reducing DAGS security level.

2018.05.30 Couvreur–Lequesne–Tillich: attack breaking "short" parameters for RLCE.

2018.06.11 Beullens–Castryck–Vercauteren: script breaking Giophantus.

Attack timeline: round 1 continues

2018.02.01 Beullens: attack breaking WalnutDSA.

2018.02.07 Fabsic–Hromada–Zajac: attack breaking CCA for LEDA.

2018.03.27 Yu–Ducas: attack reducing DRS security level.

2018.04.03 Debris-Alazard–Tillich: attack breaking RankSign; RankSign withdrawn.

2018.04.04 Beullens–Blackburn: script breaking WalnutDSA.

2018.05.09 Kotov–Menshov–Ushakov: another attack breaking WalnutDSA.

2018.05.16 Barelli–Couvreur: attack reducing DAGS security level.

2018.05.30 Couvreur–Lequesne–Tillich: attack breaking "short" parameters for RLCE.

2018.06.11 Beullens–Castryck–Vercauteren: script breaking Giophantus.

etc.

Attack timeline: round 1 continues

2018.02.01 Beullens: attack breaking WalnutDSA.

2018.02.07 Fabsic–Hromada–Zajac: attack breaking CCA for LEDA.

2018.03.27 Yu–Ducas: attack reducing DRS security level.

2018.04.03 Debris-Alazard–Tillich: attack breaking RankSign; RankSign withdrawn.

2018.04.04 Beullens–Blackburn: script breaking WalnutDSA.

2018.05.09 Kotov–Menshov–Ushakov: another attack breaking WalnutDSA.

2018.05.16 Barelli–Couvreur: attack reducing DAGS security level.

2018.05.30 Couvreur–Lequesne–Tillich: attack breaking "short" parameters for RLCE.

2018.06.11 Beullens–Castryck–Vercauteren: script breaking Giophantus.

etc.

2019.01.30 NIST announces selection of 26 second-round candidates;
keeps 0/13 broken submissions, 3/9 submissions with disproven security claims,
28/47 remaining submissions, biased towards faster submissions; −5 merges.

Attacks keep getting better (2019 – 2022)

2019.08 Zaverucha–Kales: attack reducing security level of “provably secure” MQDSS.

Attacks keep getting better (2019 – 2022)

2019.08 Zaverucha–Kales: attack reducing security level of "provably secure" MQDSS.

More attacks disprove security claims for further submissions.

2020.07 NIST announces selection of 15 third-round candidates;
keeps 0/2 broken submissions, 0/5 submissions with disproven security claims,
16/19 remaining submissions; −1 merge.

Attacks keep getting better (2019 – 2022)

2019.08 Zaverucha–Kales: attack reducing security level of "provably secure" MQDSS.

More attacks disprove security claims for further submissions.

2020.07 NIST announces selection of 15 third-round candidates;
keeps 0/2 broken submissions, 0/5 submissions with disproven security claims,
16/19 remaining submissions; −1 merge.

2020.09 NIST: "The key point here . . . is not that 'attacks have improved, and may continue improving against Rainbow.' . . . the theoretical analysis has been tightened in a way that **matches** the empirical observations of the generic algorithm."

Attacks keep getting better (2019 – 2022)

2019.08 Zaverucha–Kales: attack reducing security level of "provably secure" MQDSS.

More attacks disprove security claims for further submissions.

2020.07 NIST announces selection of 15 third-round candidates;
keeps $0/2$ broken submissions, $0/5$ submissions with disproven security claims,
$16/19$ remaining submissions; -1 merge.

2020.09 NIST: "The key point here ... is not that 'attacks have improved, and may continue improving against Rainbow.' ... the theoretical analysis has been tightened in a way that **matches** the empirical observations of the generic algorithm."

2020.10 Beullens: attack reducing security level of Rainbow.

Attacks keep getting better (2019 – 2022)

2019.08 Zaverucha–Kales: attack reducing security level of "provably secure" MQDSS.

More attacks disprove security claims for further submissions.

2020.07 NIST announces selection of 15 third-round candidates;
keeps 0/2 broken submissions, 0/5 submissions with disproven security claims,
16/19 remaining submissions; −1 merge.

2020.09 NIST: "The key point here . . . is not that 'attacks have improved, and may continue improving against Rainbow.' . . . the theoretical analysis has been tightened in a way that **matches** the empirical observations of the generic algorithm."

2020.10 Beullens: attack reducing security level of Rainbow.

2020.11 Tao–Petzoldt–Ding: attack reducing security level of GeMSS.

Attacks keep getting better (2019 – 2022)

2019.08 Zaverucha–Kales: attack reducing security level of "provably secure" MQDSS.

More attacks disprove security claims for further submissions.

2020.07 NIST announces selection of 15 third-round candidates;
keeps 0/2 broken submissions, 0/5 submissions with disproven security claims,
16/19 remaining submissions; −1 merge.

2020.09 NIST: "The key point here . . . is not that 'attacks have improved, and may continue improving against Rainbow.' . . . the theoretical analysis has been tightened in a way that **matches** the empirical observations of the generic algorithm."

2020.10 Beullens: attack reducing security level of Rainbow.

2020.11 Tao–Petzoldt–Ding: attack reducing security level of GeMSS.

2021.02 Beullens: script breaking smallest Rainbow parameter set.

Attacks keep getting better (2019 – 2022)

2019.08 Zaverucha–Kales: attack reducing security level of "provably secure" MQDSS.

More attacks disprove security claims for further submissions.

2020.07 NIST announces selection of 15 third-round candidates;
keeps 0/2 broken submissions, 0/5 submissions with disproven security claims,
16/19 remaining submissions; −1 merge.

2020.09 NIST: "The key point here . . . is not that 'attacks have improved, and may continue improving against Rainbow.' . . . the theoretical analysis has been tightened in a way that **matches** the empirical observations of the generic algorithm."

2020.10 Beullens: attack reducing security level of Rainbow.

2020.11 Tao–Petzoldt–Ding: attack reducing security level of GeMSS.

2021.02 Beullens: script breaking smallest Rainbow parameter set.

2022.07 NIST selects Kyber, Dilithium, Falcon, SPHINCS+ for standardization.
BIKE, Classic McEliece, HQC, and SIKE for Round 4.
Calls for submission of new signatures.

2022.07.05 NIST selects Kyber, Dilithium, Falcon, SPHINCS+ for standardization.
BIKE, Classic McEliece, HQC, and SIKE for Round 4.
Calls for submission of new signatures.

SIKE badly broken

2022.07.05 NIST selects Kyber, Dilithium, Falcon, SPHINCS+ for standardization.
BIKE, Classic McEliece, HQC, and SIKE for Round 4.
Calls for submission of new signatures.

2022.07.30 Castryck–Decru: "An efficient key recovery attack on SIDH (preliminary version)".
Script breaking *all* proposed SIKE parameters.

2022.08.02 Pope: Sage script reimplementing Castryck–Decru attack with various speedups.
Several others quickly joined the ~~beating~~ optimization efforts.

2022.08.08 Maino–Martindale: "An attack on SIDH with arbitrary starting curve."
(Independent of Castryck–Decru.)

2022.08.11 Robert: "Breaking SIDH in polynomial time."

2022.08.12 Oudompheng, Wesolowski: Papers describing speedups.

3 papers at Eurocrypt 2023, incl. best paper + 2 honorable mentions.

https://github.com/jack4818/Castryck-Decru-SageMath

Breaking SIDH on a Laptop

~ Running Time	SIKEp64	$IKEp217	SIKEp434	SIKEp503	SIKEp610	SIKEp751
Paper Implementation (Magma)	-	6 minutes	62 minutes	2h19m	8h15m	20h37m
Our implementation (SageMath)	5 seconds	2 minutes	10 minutes	15 minutes	25 minutes	1-2 hours
Direct Computation (Oudompheng)	2 seconds	9 seconds	22 seconds	2 minutes	15 minutes	1 hour

Note: Especially for the higher NIST levels, a lot of time is spent getting the first digits, and so performance time varies based on whether or not the first few values are `0` (fastest) or `2` (slowest).

Understanding of the concrete security of SIKE has greatly improved over the past days.

KpqC competition

Many differences between NIST PQC and KpqC

- Restriction on who may submit.
- Extra evaluation criterion: originality.

Many differences between NIST PQC and KpqC

- Restriction on who may submit.
- Extra evaluation criterion: originality.
- Focus on building PQC expertise through workshops, schools, ...

Many differences between NIST PQC and KpqC

- Restriction on who may submit.
- Extra evaluation criterion: originality.
- Focus on building PQC expertise through workshops, schools, ...
  ...and permitting teams to update their submission.

Many differences between NIST PQC and KpqC

- Restriction on who may submit.
- Extra evaluation criterion: originality.
- Focus on building PQC expertise through workshops, schools, ...
  ... and permitting teams to update their submission.
- Less focus on speed and implementations in Round 1.
- Welcomes new submissions (NIST asked for established systems, especially in the new signatures round, but reneged on this later)

KpqC candidates – KEMs

IPCC	graphs	broken and updated to IPCC7
Layered-ROLLO-I	RM codes	several attacks, several updates
PALOMA	Goppa codes	
REDOG	RM codes	attack and fix
NTRU+	ideal lattice	CCA-II attack and fix
SMAUG	ideal lattice	update for meet-LWE, but not attack
TiGER	ideal lattice	meet-LWE and DFP issues and fixes

KpqC candidates – KEMs

IPCC	graphs	broken and updated to IPCC7
Layered-ROLLO-I	RM codes	several attacks, several updates
PALOMA	Goppa codes	
REDOG	RM codes	attack and fix
NTRU+	ideal lattice	CCA-II attack and fix
SMAUG	ideal lattice	update for meet-LWE, but not attack
TiGER	ideal lattice	meet-LWE and DFP issues and fixes

- PALOMA is close to Classic McEliece but has different choice of Goppa polynomial – boon or burden?
- REDOG is interesting as fixable RM-code system.
- NTRU+ is very close to NTTRU, same family as NTRU-HRSS, ...
- SMAUG and TiGER are battling with Kyber – both smaller and faster.

NIST selected only 1 KEM, 3 more in Round 4.

KpqC candidates – KEMs

IPCC	graphs	broken and updated to IPCC7
Layered-ROLLO-I	RM codes	several attacks, several updates
PALOMA	Goppa codes	
REDOG	RM codes	attack and fix
NTRU+	ideal lattice	CCA-II attack and fix
SMAUG	ideal lattice	update for meet-LWE, but not attack
TiGER	ideal lattice	meet-LWE and DFP issues and fixes

- PALOMA is close to Classic McEliece but has different choice of Goppa polynomial – boon or burden?
- REDOG is interesting as fixable RM-code system.
- NTRU+ is very close to NTTRU, same family as NTRU-HRSS, ...
- SMAUG and TiGER are battling with Kyber – both smaller and faster.

NIST selected only 1 KEM, 3 more in Round 4. KEM migration is urgent.

KpqC candidates – signatures

AIMer	MPCitH / symmetric	attacks on AIM block cipher and fixes
enhanced pqsigRM	Reed-Muller code	signatures leak secret code structure
FIBS	isogenies + SPHINCS	very slow, CGL hash not well studied
GCKSign	ideal lattice	problems with MSIS and TMO analysis
HAETAE	ideal lattice	
NCC-Sign	ideal lattice	
Peregrine	ideal lattice	missing rejection sampling leaks private basis
SOLMAE	ideal lattice	
MQ-Sign	multivariates	sparse versions have attacks

KpqC candidates – signatures

AIMer	MPCitH / symmetric	attacks on AIM block cipher and fixes
enhanced pqsigRM	Reed-Muller code	signatures leak secret code structure
FIBS	isogenies + SPHINCS	very slow, CGL hash not well studied
GCKSign	ideal lattice	problems with MSIS and TMO analysis
HAETAE	ideal lattice	
NCC-Sign	ideal lattice	
Peregrine	ideal lattice	missing rejection sampling leaks private basis
SOLMAE	ideal lattice	
MQ-Sign	multivariates	sparse versions have attacks

- HAETAE & NCC-Sign close to Dilithium, with HAETAE shorter.
- SOLMAE close to Falcon but much easier to implement.

1 code, 1 isogeny, 5 lattice, 1 MPCitH/symmetric, 1 MQ.

NIST's onramp for signatures – deadline June 2023

- 6 Code based: CROSS, enhanced pqsigRM (attacks), FuLeeca (lattice attack), LESS (some issues), MEDS (some issues), Wave
- 1 isogeny based: SQIsign
- 8 lattice based: EagleSign (attack), EHTv3 and EHTv4 (attacks), HAETAE, HAWK, HuFu (SUF attack), Raccoon, SQUIRRELS
- 7 MPCitH on math problem: Biscuit (some analysis), MIRA, MiRitH, MQOM, PERK, RYDE, SDitH (some bits lost)
- 10 MQ based: 3WISE (attack), DME-Sign (attack), HPPC (attack), MAYO, PROV, QR-UOV, SNOVA, TUOV, UOV, VOX
- 4 symmetric based: AIMer (attacks on AIM), Ascon-Sign, FAEST, SPHINCS-alpha
  (though AIMer & FEAST could be counted as MPCitH with block cipher instead)
- 5 other: ALTEQ, eMLE-Sig 2.0 (attack), KAZ-SIGN (attacks), Preon, Xifrat1-Sign.I (attack)

NIST's onramp for signatures – deadline June 2023

- 6 Code based: CROSS, enhanced pqsigRM (attacks), FuLeeca (lattice attack), LESS (some issues), MEDS (some issues), Wave
- 1 isogeny based: SQIsign
- 8 lattice based: EagleSign (attack), EHTv3 and EHTv4 (attacks), HAETAE, HAWK, HuFu (SUF attack), Raccoon, SQUIRRELS
- 7 MPCitH on math problem: Biscuit (some analysis), MIRA, MiRitH, MQOM, PERK, RYDE, SDitH (some bits lost)
- 10 MQ based: 3WISE (attack), DME-Sign (attack), HPPC (attack), MAYO, PROV, QR-UOV, SNOVA, TUOV, UOV, VOX
- 4 symmetric based: AIMer (attacks on AIM), Ascon-Sign, FAEST, SPHINCS-alpha
  (though AIMer & FEAST could be counted as MPCitH with block cipher instead)
- 5 other: ALTEQ, eMLE-Sig 2.0 (attack), KAZ-SIGN (attacks), Preon, Xifrat1-Sign.I (attack)

Many more MQ systems and MPCitH systems.

NIST's onramp for signatures – deadline June 2023

- 6 Code based: CROSS, enhanced pqsigRM (attacks), FuLeeca (lattice attack), LESS (some issues), MEDS (some issues), Wave
- 1 isogeny based: SQIsign
- 8 lattice based: EagleSign (attack), EHTv3 and EHTv4 (attacks), HAETAE, HAWK, HuFu (SUF attack), Raccoon, SQUIRRELS
- 7 MPCitH on math problem: Biscuit (some analysis), MIRA, MiRitH, MQOM, PERK, RYDE, SDitH (some bits lost)
- 10 MQ based: 3WISE (attack), DME-Sign (attack), HPPC (attack), MAYO, PROV, QR-UOV, SNOVA, TUOV, UOV, VOX
- 4 symmetric based: AIMer (attacks on AIM), Ascon-Sign, FAEST, SPHINCS-alpha
  (though AIMer & FEAST could be counted as MPCitH with block cipher instead)
- 5 other: ALTEQ, eMLE-Sig 2.0 (attack), KAZ-SIGN (attacks), Preon, Xifrat1-Sign.I (attack)

Many more MQ systems and MPCitH systems. Many more broken systems.

Summary

- Nice portfolio of alternative schemes.
- Improvements over Dilithium, Falcon, and Kyber show progress in last 6 years and new ideas.

Summary

- Nice portfolio of alternative schemes.
- Improvements over Dilithium, Falcon, and Kyber show progress in last 6 years and new ideas.
  Is standardization always too early?

Summary

- Nice portfolio of alternative schemes.
- Improvements over Dilithium, Falcon, and Kyber show progress in last 6 years and new ideas.
  Is standardization always too early?
- Rank-metric and Reed-Muller codes still have issues.
  REDOG might be OK after fixes (targets different regime from ROLLO with length $<$ field size)
- MQ systems still have issues, some core systems OK.