BIKE - Bit-Flipping Key Encapsulation

Presented to the 2nd NIST Post-Quantum Cryptography Standardization Conference
August, 24th 2019, Santa Barbara, California, USA

Authors:	**Affiliations:**
Nicolas Aragon	University of Limoges, France
Paulo S. L. M. Barreto	University of Washington Tacoma, USA
Slim Bettaieb	Worldline, France
Loïc Bidoux	Worldline, France
Olivier Blazy	University of Limoges, France
Jean-Christophe Deneuville	Federal University of Toulouse, ENAC, France
Philippe Gaborit	University of Limoges, France
Shay Gueron	University of Haifa, and Amazon Web Services, Israel
Tim Güneysu	Ruhr-Universität Bochum, and DFKI, Germany,
Carlos Aguilar Melchor	University of Toulouse, France
Rafael Misoczki (presenter)	Intel Corporation, USA
Edoardo Persichetti	Florida Atlantic University, USA
Nicolas Sendrier	INRIA, France
Jean-Pierre Tillich	INRIA, France
Valentin Vasseur (new member)	INRIA, France
Gilles Zémor	IMB, University of Bordeaux, France

https://bikesuite.org – team@bikesuite.org

BIKE Recap

- **McEliece-like KEM with QC-MDPC Codes**
- **Well-Understood & Reliable Security**
  - Theoretical Security: Reduction based on well-known coding-theory problems
  - Practical Security: ISD-based attacks [Pra62] whose work-factor* barely changed in ~50 years of research
- Performance
  - **Practical performance** for all KeyGen, Encaps, Decaps steps regarding both computational complexity and bandwidth

Tip: Ideal usage as Ephemeral Key Exchange (e.g. SSL/TLS)

*: $WF_A(n,k,t) = 2^{ct(1+o(1))}$

NIST Report 8240 on 1st Round BIKE

"BIKE targets IND-CPA security and makes no attempt to make it difficult for an attacker to mount a chosen ciphertext attack if keys are reused. This design decision was made by the submitters, based on the difficulty of designing a bit-flipping decoder with a low enough decoding failure rate to allow an efficient IND-CCA2-secure construction."

NIST IR Report 8240, page 11, Section 3.12

New Backflip Decoder

- Context
  - Round 1 decoder: efficient but fails with non-negligible probability (10^{-7})
  - To enable IND-CCA variants, negligible decoding probability was needed

- Backflip Rationale
  - Similar to Bit-Flipping
  - Difference: each bit flip keeps a time-to-live counter. After a given number of iterations, the bit flip reaches a time-to-death point and is flipped back
  - Result: Based on an extrapolation argument, it is possible to show that a certain parameter set attains an arbitrarily low failure rate using Backflip

New BIKE CCA Variants

- Core Ingredients
  - Backflip Decoder
  - [HHK17] like conversions (with bounds from [JZC18, JZM19])
- CPA→CCA conversion preserved the strong points of each variant

	Strong Points among CPA Variant	Strong Points among CCA Variant
BIKE-1	Fastest KG+Encaps+Decaps among CPA variants	Fastest KG+Encaps+Decaps among CCA variants
BIKE-2	Smallest ciphertext among CPA variants	Smallest ciphertext among CCA variants
BIKE-3	Security reduction to single problem	Security reduction to single problem

- CCA Variants enable static keys. Current focus remains CPA Ephemeral

NIST Report 8240 on 1st Round BIKE

"BIKE offers key and ciphertext sizes and performance that are competitive with ring and module lattice schemes (especially at the lower security categories)."

NIST IR Report 8240, page 11, Section 3.12

BIKE CCA -- constant time implementations

Nir Drucker [1, 2], Shay Gueron [1, 2], Dusan Kostic [1, 3]
(1) Amazon (2) University of Haifa (3) EPFL

- New BIKE CCA implementation in constant time -- C, AVX2, AVX512
  - Constant time algorithm definition for the CCA decoder
  - Constant time implementation for the CCA BIKE flows

- Conclusions
  - It is possible to define and implement BIKE CCA in constant time
  - Performance costs are tolerable

- "Additional" code package & detailed report to be released/published soon

BIKE CCA -- constant time implementations

Nir Drucker [1, 2], Shay Gueron [1, 2], Dusan Kostic [1, 3]
(1) Amazon (2) University of Haifa (3) EPFL

		CPA Cycles	CCA Cycles	CCA/CPA	CPA Bandwidth	CCA Bandwidth	CCA-CPA
BIKE 1	KeyGen	250K	270K	**1.08x**	→ 2.48KB ← 2.48KB	→ 2.88KB ← 2.88KB	**Δ**=400B
	Encaps	180K	210K	**1.17x**			
	Decaps	1.9M	8.1M	**4.18x**			
BIKE 2	KeyGen	4.8M	6.3M	**1.30x**	→ 1.24KB ← 1.24KB	→ 1.44KB ← 1.47KB	**Δ**=400B
	Encaps	140K	170K	**1.21x**			
	Decaps	1.9M	9.0M	**4.64x**			
BIKE 3	KeyGen	220K	250K	**1.14x**	→ 2.69KB ← 2.69KB → 1.38KB ← 2.69KB	→ 3KB ← 3.03KB → 1.53KB ← 3.03KB	**Δ**=310B
	Encaps	220K	280K	**1.27x**			
	Decaps	2.5M	13.8M	**5.58x**			

Parameter sets targeting NIST Security Level 1

In red message size for BIKE-3 with compressed g

BIKE Real Experiment with **s2n** AWS TLS library

- **s2n** is an AWSLabs open source library for TLS
  - Small, fast, with simplicity as a priority
  - Removes a lot of cruft that has built-up in libssl
  - Currently handles all of the S3 traffic today

- **PQ-TLS 1.2 – hybrid key exchange in s2n**
- Added SIKE and BIKE (reference code) into the s2n code base
- Added a hybrid key exchange cipher suites into s2n
  - TLS_ECDHE_BIKE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_SIKE_RSA_WITH_AES_256_GCM_SHA384
- Applied the same rigor to this new code as in all of s2n
- Open Source implementation will be released soon

Conclusion: feasible to use “Classical + BIKE” hybrid in a real networking application

NIST Report 8240 on 1st Round BIKE

"Security strengths are based on information-set-decoding attacks, which have a long history of analysis during which the complexity of such attacks have not greatly changed.

NIST IR Report 8240, page 11, Section 3.12

"Possible areas for further analysis related to BIKE include … investigating the effect, if any, of the quasi-cyclic code structure on security."

NIST IR Report 8240, page 12, Section 3.12

The Effect of Quasi-Cyclic Code Structure on Security

- QC-MDPC Parameters are selected considering three ISD-related attacks
  - **Key distinguishing attack**: Exhibit one codeword of $C^{\perp}$ of weight w
  - **Key recovery attack**: Exhibit r codewords of $C^{\perp}$ of weight w
  - **Decoding attack**: Decode t errors in a $(n, n-r)$-linear code.
- ISD algorithms assume a list of solution candidates of size L. Each candidate has a probability P to produce a solution. Under optimal conditions: $WF_{ISD}\,(n, r, t) \approx L/P$
- [Sen11] shows that the gain when the decoding problem has N_s solutions and when N_i instances are treated simultaneously is: $N_s/\sqrt{N_i}$

	MDPC	QC-MDPC
Key distinguishing	$\frac{1}{r}\mathrm{WF}_{\mathrm{isd}}(n, n-r, w)$	$\frac{1}{r}\mathrm{WF}_{\mathrm{isd}}(n, n-r, w)$
Key recovery	$\mathrm{WF}_{\mathrm{isd}}(n, n-r, w)$	$\frac{1}{r}\mathrm{WF}_{\mathrm{isd}}(n, n-r, w)$
Decoding	$\mathrm{WF}_{\mathrm{isd}}(n, r, t)$	$\frac{1}{\sqrt{r}}\mathrm{WF}_{\mathrm{isd}}(n, r, t)$

See [Mis13] for a detailed analysis

Smaller Updates & Final Remarks

- Smaller updates
  - BIKE-3 variant that generates g from a seed, saving almost 50% communication
  - Fixed decoding threshold computation in reference & optimization code, which now matches the spec, accelerating decoding. No changes in additional code;
  - Fixed buffer overflows in reference & optimization code;

- Final remarks
  - BIKE has well-understood, reliable security & practical performance
  - BIKE is particularly appealing for low-level security (e.g. Level 1)
  - Given CPA focus, variants with fast key generation (e.g. BIKE-1, BIKE-3) are our priority
  - NIST Report 8240 already highlights benefits of BIKE and the team addressed requests

References

- [BGGM17]: P. S. L. M. Barreto, S. Gueron, T. Güneysu, R. Misoczki, E. Persichetti, N. Sendrier, and J.-P. Tillich. CAKE: Code-based Algorithm for Key Encapsulation. 16th IMA Intl. Conf. on Cryptography and Coding. 2017.
- [DGZ17]: J.-C. Deneuville, P. Gaborit, G. Zémor. Ouroboros: A Simple, Secure and Efficient Key Exchange Protocol Based on Coding Theory. PQCrypto 2017: 18-34
- [HKK17]: D. Hofheinz, K. Hövelmanns, and E. Kiltz. A modular analysis of the Fujisaki-Okamoto transformation. In Theory of Cryptography Conference, pages 341-371. Springer, 2017
- [JZC18]: H. Jiang, Z. Zhang, L. Chen, H. Wang, and Z. Ma. INDCCA-secure key encapsulation mechanism in the Quantum Random Oracle Model, revisited. In CRYPTO’18, pages 96-125.
- [JZM19]: H. Jiang, Z. Zhang, and Z. Ma. Tighter security proofs for generic key encapsulation mechanism in the Quantum Random Oracle Model. ePrint Report 2019/134, 2019
- [MTSB12]: R. Misoczki, J.-P. Tillich, N. Sendrier, and P. L.S.M. Barreto. MDPC McEliece: New McEliece variants from moderate density parity-check codes. In IEEE ISIT, ISIT'2013, pages 2069, 2073, Istanbul, Turkey, 2013
- [Mis13]: R. Misoczki. Two Approaches for Achieving Efficient Code-Based Cryptosystems. PhD Thesis, University of Paris Pierre et Marie Curie, Paris, France, 2013.
- [Pra62]: E. Prange. The use of information sets in decoding cyclic codes. IRE Transactions, IT-8:S5 S9, 1962.

https://bikesuite.org

Authors:	**Affiliation:**
Nicolas Aragon	University of Limoges, France
Paulo S. L. M. Barreto	University of Washington Tacoma, USA
Slim Bettaieb	Worldline, France
Loïc Bidoux	Worldline, France
Olivier Blazy	University of Limoges, France
Jean-Christophe Deneuville	Federal University of Toulouse, ENAC, France
Philippe Gaborit	University of Limoges, France
Shay Gueron	University of Haifa, and Amazon Web Services, Israel
Tim Güneysu	Ruhr-Universität Bochum, and DFKI, Germany,
Carlos Aguilar Melchor	University of Toulouse, France
Rafael Misoczki (presenter)	Intel Corporation, USA
Edoardo Persichetti	Florida Atlantic University, USA
Nicolas Sendrier	INRIA, France
Jean-Pierre Tillich	INRIA, France
Valentin Vasseur (<u>new member</u>)	INRIA, France
Gilles Zémor	IMB, University of Bordeaux, France