1 Rue Honoré d'Estienne d'Orves
Laboratoire Informatique de l'X
91120 Palaiseau (France)
olivier.blazy@polytechnique.edu
https://www.blazy.eu
Born 20/03/1986 (France)

Olivier Blazy

Employment

2021–* **Professor**, *Ecole Polytechnique*, Teaching and Research in Cybersecurity / Cryptography

2022–* **Academic Advisor for the Computer Science Bachelor**

2014–2021 **Maître de Conférences (∼ Associate Professor)**, *University of Limoges*, Teaching and Research in Cybersecurity / Cryptography

2016–2021 **Academic Advisor for the Computer Science Cryptis Master**

2012–2014 **Postdoctoral Position**, *Ruhr-University Bochum*, with Eike Kiltz in the Foundation of Cryptography workgroup, Horst Görtz Institute for IT-Security
Zero-Knowledge Proofs, Semi-Functional spaces, Tight Signatures

Education

2019 **Habilitation (HDR) in Computer Science**, *University of Limoges*, Hash Proofs Systems and Applications to Implicit Cryptography

2008–2012 **PhD in Computer Science**, *University Paris 7*, supervised by David Pointcheval (ENS, CNRS), Interactive and Non-Interactive proofs of knowledge

2005–2009 **Predoctoral Studies in Computer Science**, *Ecole Normale Supérieure*

Dissemination

Media Interview, More than 40 interviews in National / International Press (Times, Financial Times, WSJ,...) about security, and it's impact on the population, Ranked 29th most influencial person in french tech by Tyto ranking in 2020

Research Level Teaching, Various Courses in Public Key Cryptography, Secret Key Cryptography, Cryptographical Mecanisms

Invited Talks, More than 20 visits and Invited seminars often coupled with a short stay (1-2 weeks) in various places like Oxford, ENS, X, KIT, UCL, ...

2016–* **PostQuantum Standardization**, Submission of 6 candidates to the NIST PQC competition, 2 were selected as alternate finalists (Final answer soon)

2021–* **Online Age Verification**, Project with french CNIL, and PEReN to propose an open-source privacy-friendly answer to the new legislation mandating age-check on a range of adult websites.

Management / Organization

2020–* **GT-C2/GDR-Secu**, in charge of the french national workgroup on codes and cryptography (roughly 250 members), and part of the national research group committee on Security.

2022–* **Liaison with the European Union**

2020–* **Redocs**, Co-Organizer of the Redocs week, where PhD students meet companies to work on shared project and discover research in the industry

PhD. Supervision, 2 Supervisions in progress, 3 students defended

2019–2020 **Postdoc Supervision**, Sayantan Mukherjee

Skills

- Cryptography: Provable Security, Protocol Design, Zero-Knowledge Proof, Implicit Proof, Post-Quantum.
- Development: Rust, Python, C++, Java, Ruby, OCamL, Charm.
  Recent prototypes: https://github.com/oblazy/
- Languages: French, English (985 Toeic), German (B1), Basic notions of Italian and Russian.

Publications

[ABB+13] Michel Abdalla, Fabrice Benhamouda, Olivier Blazy, Céline Chevalier, and David Pointcheval. SPHF-Friendly Non-Interactive Commitment Schemes. In Kazue Sako and Palash Sarkar, editors, *Advances in Cryptology - Proceedings of ASIACRYPT '13*, volume 8269 of *Lecture Notes in Computer Science*, pages 214–234, Bangalore, India, December 2013. Springer.

[ABB+21] Ghada Arfaoui, Olivier Blazy, Xavier Bultel, Pierre-Alain Fouque, Thibaut Jacques, Adina Nedelcu, and Cristina Onete. How to (legally) keep secrets from mobile operators. In Elisa Bertino, Haya Shulman, and Michael Waidner, editors, *Computer Security - ESORICS 2021 - 26th European Symposium on Research in Computer Security, Darmstadt, Germany, October 4-8, 2021, Proceedings, Part I*, volume 12972 of *Lecture Notes in Computer Science*, pages 23–43. Springer, October 2021.

[ABCG15] Quentin Alamélou, Olivier Blazy, Stéphane Cauchie, and Philippe Gaborit. A Code-Based Group Signature Scheme. In Jean-Pierre Tillich Pascale Charpin, Nicolas Sendrier, editor, *The 9th International Workshop on Coding and Cryptography 2015 WCC2015*, Proceedings of the 9th International Workshop on Coding and Cryptography 2015 WCC2015, Paris, France, April 2015.

[ABCG16] Quentin Alamélou, Olivier Blazy, Stéphane Cauchie, and Philippe Gaborit. A practical group signature scheme based on rank metric. In Sylvain Duquesne and Svetla Petkova-Nikova, editors, *Arithmetic of Finite Fields - 6th International Workshop, WAIFI 2016, Ghent, Belgium, July 13-15, 2016, Revised Selected Papers*, pages 258–275. Springer, July 2016.

[ABCG17] Quentin Alamélou, Olivier Blazy, Stéphane Cauchie, and Philippe Gaborit. A code-based group signature scheme. *Designs, Codes and Cryptography*, 82:1–25, 2017.

[ABD+20] Nicolas Aragon, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Terry Shue Chien Lau, Chik How Tan, and Keita Xagawa. Cryptanalysis of a rank-based signature with short public keys. *Des. Codes Cryptogr.*, 88(4):643–653, 2020.

[ABD+22] Nicolas Aragon, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, and Gilles Zémor. Ouroboros an efficient and provably secure kem family. *IEEE Transactions on Information Theory*, Apr 2022.

[ABFG20] Nicolas Aragon, Olivier Blazy, Neals Fournaise, and Philippe Gaborit. CROOT: code-based round-optimal oblivious transfer. In Pierangela Samarati, Sabrina De Capitani di Vimercati, Mohammad S. Obaidat, and Jalel Ben-Othman, editors, *Proceedings of the 17th International Joint Conference on e-Business and Telecommunications, ICETE 2020 - Volume 2: SECRYPT, Lieusaint, Paris, France, July 8-10, 2020*, pages 76–85. ScitePress, July 2020.

[ABG+19] Nicolas Aragon, Olivier Blazy, Philippe Gaborit, Adrien Hauteville, and Gilles Zémor. Durandal: A rank metric based signature scheme. *Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part III*, 11478:728–758, May 2019.

[AMBD+18] Carlos Aguilar Melchor, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, and Gilles Zémor. Efficient encryption from random quasi-cyclic codes. *IEEE Trans. Information Theory*, 64(5):3927–3943, 2018.

[BBB+19] Olivier Blazy, Angèle Bossuat, Xavier Bultel, Pierre-Alain Fouque, Cristina Onete, and Elena Pagnin. SAID: reshaping signal into an identity-based asynchronous messaging protocol with authenticated ratcheting. In *IEEE European Symposium on Security and Privacy, EuroS&P 2019, Stockholm, Sweden, June 17-19, 2019*, pages 294–309. IEEE, Jun 2019.

[BBB+21] Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Baptiste Cottier, and David Pointcheval. Secure decision forest evaluation. In Delphine Reinhardt and Tilo Müller, editors, *ARES 2021: The 16th International Conference on Availability, Reliability and Security, Vienna, Austria, August 17-20, 2021*, pages 24:1–24:12. ACM, August 2021.

[BBB+22] Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Yann Connan, and Philippe Gaborit. A gapless code-based hash proof system based on rqc and its applications. *Designs, Codes and Cryptography*, pages 1–34, 2022.

[BBBG21] Slim Bettaieb, Loïc Bidoux, Olivier Blazy, and Philippe Gaborit. Zero-knowledge reparation of the véron and ags code-based identification schemes. In Henry Pfister Emina Soljanin Michael Gastpar, Stephen Hanly, editor, *IEEE International Symposium on Information Theory, ISIT 2021, Melbourne, Australia, July 12-20, 2021*, IEEE, pages 55–60. IEEE, July 2021.

[BBC+13a] Fabrice Benhamouda, Olivier Blazy, Céline Chevalier, David Pointcheval, and Damien Vergnaud. Efficient UC-Secure Authenticated Key-Exchange for Algebraic Languages. In Kaoru Kurosawa and Goichiro Hanaoka, editors, *Conference on Practice and Theory in Public-Key Cryptography (PKC '13)*, volume 7778 of *Lecture Notes in Computer Science*, pages 272–291, Nara, Japan, March 2013. Springer.

[BBC+13b] Fabrice Benhamouda, Olivier Blazy, Céline Chevalier, David Pointcheval, and Damien Vergnaud. New Smooth Projective Hash Functions and One-Round Authenticated Key Exchange. Technical report, IACR ePrint Archive, January 2013.

[BBC+13c] Fabrice Benhamouda, Olivier Blazy, Céline Chevalier, David Pointcheval, and Damien Vergnaud. New Techniques for SPHFs and Efficient One-Round PAKE Protocols. In Ran Canetti and Juan Garay, editors, *Advances in Cryptology - Proceedings of CRYPTO '13*, volume 8042 of *Lecture Notes in Computer Science*, pages 449–475, Santa Barbara, California, August 2013. Springer.

[BBC+21] Olivier Blazy, Laura Brouilhet, Céline Chevalier, Patrick Towa, Ida Tucker, and Damien Vergnaud. Hardware security without secure hardware: How to decrypt with a password and a server. *Theoretical Computer Science*, 895:178–211, September 2021.

[BBCF20] Olivier Blazy, Laura Brouilhet, Céline Chevalier, and Neals Fournaise. Round-optimal constant-size blind signatures. In Pierangela Samarati, Sabrina De Capitani di Vimercati, Mohammad S. Obaidat, and Jalel Ben-Othman, editors, *Proceedings of the 17th International Joint Conference on e-Business and Telecommunications, ICETE 2020 - Volume 2: SECRYPT, Lieusaint, Paris, France, July 8-10, 2020*, pages 213–224. ScitePress, June 2020.

[BBCK22] Olivier Blazy, Laura Brouilhet, Emmanuel Conchon, and Mathieu Klingler. Anonymous attribute-based designated verifier signature. *Journal of Ambient Intelligence and Humanized Computing*, pages 1–11, Mar 2022.

[BBDQ18] Fabrice Benhamouda, Olivier Blazy, Léo Ducas, and Willy Quach. Hash proof systems over lattices revisited. In *Public-Key Cryptography - PKC 2018 - 21st IACR International Conference on Practice and Theory of Public-Key Cryptography, Rio de Janeiro, Brazil, Proceedings, Part II*, volume 10770, pages 644–674. Springer, March 2018.

[BBL16a] Olivier Blazy, Xavier Bultel, and Pascal Lafourcade. Anonymizable ring signature without pairing. In Frédéric Cuppens, Lingyu Wang, Nora Cuppens-Boulahia, Nadia Tawbi, and Joaquín García-Alfaro, editors, *Foundations and Practice of Security - 9th International Symposium, FPS 2016, Québec City, QC, Canada, October 24-25, 2016, Revised Selected Papers*, pages 214–222, Québec, Canada, 2016. Springer.

[BBL16b] Olivier Blazy, Xavier Bultel, and Pascal Lafourcade. Two secure anonymous proxy-based data storages. In Christian Callegari, Marten van Sinderen, Panagiotis G. Sarigiannidis, Pierangela Samarati, Enrique Cabello, Pascal Lorenz, and Mohammad S. Obaidat, editors, *Proceedings of the 13th International Joint Conference on e-Business and Telecommunications (ICETE 2016) - Volume 4: SECRYPT, Lisbon, Portugal, July 26-28, 2016.*, pages 251–258. Springer, July 2016.

[BBL+23] Olivier Blazy, Ioana Boureanu, Pascal Lafourcade, Cristina Onete, and Léo Robert. How fast do you heal? a taxonomy for post-compromise security in secure-channel establishment. In *Usenix Security Symposium*, Aug 2023.

[BBLP21] Olivier Blazy, Xavier Bultel, Pascal Lafourcade, and Octavio Perez-Kempner. Generic plaintext equality and inequality proofs. In Claudia Diaz Nikita Borisov, editor, *Financial Cryptography and Data Security - 25th International Conference, FC 2021*, volume 12674 of *Lecture Notes in Computer Science*, pages 415–435. Springer, March 2021.

[BBP19] Olivier Blazy, Laura Brouilhet, and Duong Hieu Phan. Anonymous identity based encryption with traceable identities. In *Proceedings of the 14th International Conference on Availability, Reliability and Security, ARES 2019, Canterbury, UK, August 26-29, 2019*, pages 13:1–13:10. ACM, 2019.

[BC15] Olivier Blazy and Céline Chevalier. Generic Construction of UC-Secure Oblivious Transfer. In Tal Malkin, Vladimir Kolesnikov, Allison Bishop Lewko, and Michalis Polychronakis, editors, *Applied Cryptography and Network Security - 13th International Conference, ACNS 2015, New York, NY, USA, June 2-5, 2015, Revised Selected Papers*, volume 9092 of *Lecture Notes in Computer Science*, pages 65–86, New York, USA, June 2015. Springer.

[BC16] Olivier Blazy and Céline Chevalier. Structure-preserving smooth projective hashing. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *Advances in Cryptology - ASIACRYPT 2016 - 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part II*, pages 339–369, Hanoi, Vietnam, December 2016. Springer.

[BC18a] Olivier Blazy and Céline Chevalier. Non-interactive key exchange from identity-based encryption. In *Proceedings of the 13th International Conference on Availability, Reliability and Security, ARES 2018, Hamburg, Germany, August 27-30, 2018*, pages 13:1–13:10. ACM, August 2018.

[BC18b] Olivier Blazy and Céline Chevalier. Spreading alerts quietly: New insights from theory and practice. *Proceedings of the 13th International Conference on Availability, Reliability and Security, Hamburg, Germany, August 27 - August 30, 2018*, pages 30:1–30:6, August 2018.

[BCB+17] Olivier Blazy, Emmanuel Conchon, Pierre-François Bonnefoi, Damien Sauveron, Raja Naeem Akram, Konstantinos Markantonakis, Keith Mayes, and Serge Chaumette. An efficient protocol for uas security. In *Integrated Communications, Navigation and Surveillance Conference (ICNS), 2017*. IEEE, 2017.

[BCF+11] Olivier Blazy, Sébastien Canard, Georg Fuchsbauer, Aline Gouget, Hervé Sibert, and Jacques Traoré. Achieving optimal anonymity in transferable e-cash with a judge. In Abderrahmane Nitaj and David Pointcheval, editors, *AFRICACRYPT 2011 - 4th International Conference on Cryptology in Africa*, volume 6737 of *Lecture Notes in Computer Science*, pages 206–223, Dakar, Senegal, June 2011. Springer.

[BCG16] Olivier Blazy, Céline Chevalier, and Paul Germouty. Adaptive oblivious transfer and generalization. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *Advances in Cryptology - ASIACRYPT 2016 - 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part II*, pages 217–247, Hanoi, Vietnam, December 2016. Springer.

[BCG17] Olivier Blazy, Céline Chevalier, and Paul Germouty. Almost optimal oblivious transfer from QA-NIZK. In Dieter Gollmann, Atsuko Miyaji, and Hiroaki Kikuchi, editors, *Applied Cryptography and Network Security - 15th International Conference, ACNS 2017, Kanazawa, Japan, July 10-12, 2017, Proceedings*, volume 10355 of *Lecture Notes in Computer Science*, pages 579–598. Springer, 2017.

[BCGJ17] Olivier Blazy, Emmanuel Conchon, Paul Germouty, and Amandine Jambert. Efficient id-based designated verifier signature. In *Proceedings of the 12th International Conference on Availability, Reliability and Security, Reggio Calabria, Italy, August 29 - September 01, 2017*, pages 44:1–44:8. ACM, 2017.

[BCKS21] Olivier Blazy, Emmanuel Conchon, Mathieu Klingler, and Damien Sauveron. An iot attribute-based security framework for topic-based publish/subscribe systems. *IEEE Access*, 9:19066–19077, 2021.

[BCPV12] Olivier Blazy, Céline Chevalier, David Pointcheval, and Damien Vergnaud. Efficient UC-Secure Authenticated Key-Exchange for Algebraic Languages. Technical report, IACR ePrint Archive, May 2012.

[BCPV13] Olivier Blazy, Céline Chevalier, David Pointcheval, and Damien Vergnaud. Analysis and Improvement of Lindell's UC-Secure Commitment Schemes. In Rei Safavi-Naini and Michael E. Locasto, editors,

Conference on Applied Cryptography and Network Security (ACNS '13), volume 7954 of *Lecture Notes in Computer Science*, pages 534–551, Banff, Alberta, Canada, June 2013. Springer.

[BCV15] Olivier Blazy, Céline Chevalier, and Damien Vergnaud. Non-Interactive Zero-Knowledge Proofs of Non-Membership. In K. Nyberg, editor, *Proceedings of CT-RSA*, volume 9048 of *Lecture Notes in Computer Science*, pages 145–164, San Francisco, California, April 2015. Springer.

[BCV16] Olivier Blazy, Céline Chevalier, and Damien Vergnaud. Mitigating server breaches in password-based authentication: Secure and efficient solutions. In Kazue Sako, editor, *Topics in Cryptology - CT-RSA 2016 - The Cryptographers' Track at the RSA Conference 2016, San Francisco, CA, USA, February 29 - March 4, 2016, Proceedings*, pages 3–18, San Francisco, USA, February 2016. Springer.

[BCV19] Olivier Blazy, Céline Chevalier, and Quoc Huy Vu. Post-quantum uc-secure oblivious transfer in the standard model with adaptive corruptions. In *Proceedings of the 14th International Conference on Availability, Reliability and Security, ARES 2019, Canterbury, UK, August 26-29, 2019.*, pages 28:1–28:6. ACM, 2019.

[BDSS16] Olivier Blazy, David Derler, Daniel Slamanig, and Raphael Spreitzer. Non-interactive plaintext (in-)equality proofs and group signatures with verifiable controllable linkability. In Kazue Sako, editor, *Topics in Cryptology - CT-RSA 2016 - The Cryptographers' Track at the RSA Conference 2016, San Francisco, CA, USA, February 29 - March 4, 2016, Proceedings*, pages 127–143, San Francisco, USA, February 2016. Springer.

[BFI+10] Olivier Blazy, Georg Fuchsbauer, Malika Izabachène, Amandine Jambert, Hervé Sibert, and Damien Vergnaud. Batch groth-sahai. In Jianying Zhou and Moti Yung, editors, *Conference on Applied Cryptography and Network Security (ACNS '10)*, volume 6123 of *Lecture Notes in Computer Science*, pages 218–235, Beiing, China, June 2010. Springer.

[BFJ+22] Olivier Blazy, Pierre-Alain Fouque, Thibaut Jacques, Pascal Lafourcade, Cristina Onete, and Léo Robert. Marshal: Messaging with asynchronous ratchets and signatures for faster healing. In *Symposium on Applied Computing (SAC)*, Apr 2022.

[BFPV11] Olivier Blazy, Georg Fuchsbauer, David Pointcheval, and Damien Vergnaud. Signatures on Randomizable Ciphertexts. In Dario Catalano, Nelly Fazio, Rosario Gennaro, and Antonio Nicolosi, editors, *Conference on Practice and Theory in Public-Key Cryptography (PKC '11)*, volume 6571 of *Lecture Notes in Computer Science*, pages 403–422, Taormina, Italy, March 2011. Springer.

[BFPV13] Olivier Blazy, Georg Fuchsbauer, David Pointcheval, and Damien Vergnaud. Short Blind Signatures. *Journal of Computer Security*, 21(5):627–661, November 2013.

[BGM] Olivier Blazy, Philippe Gaborit, and Dang Truong Mac. A correction to a code-based blind signature scheme. *Code-Based Cryptography Workshop*, pages 84–94.

[BGM21] Olivier Blazy, Philippe Gaborit, and Dang Truong Mac. A rank-metric code-based group signature scheme. *Code-Based Cryptography Workshop*, pages 1–21, June 2021.

[BGP19] Olivier Blazy, Paul Germouty, and Duong Hieu Phan. Downgradable identity-based encryption and applications. In Mitsuru Matsui, editor, *Topics in Cryptology - CT-RSA 2019 - The Cryptographers' Track at the RSA Conference 2019, San Francisco, CA, USA, March 4-8, 2019, Proceedings*, volume 11405 of *Lecture Notes in Computer Science*, pages 44–61. Springer, March 2019.

[BGSS17] Olivier Blazy, Philippe Gaborit, Julien Schrek, and Nicolas Sendrier. A code-based blind signature. In *2017 IEEE International Symposium on Information Theory, ISIT 2017, Aachen, Germany, June 25-30, 2017*, pages 2718–2722, 2017.

[BK20] Olivier Blazy and Saqib A. Kakvi. Skipping the q in group signatures. In Karthikeyan Bhargavan, Elisabeth Oswald, and Manoj Prabhakaran, editors, *Progress in Cryptology - INDOCRYPT 2020 - 21st International Conference on Cryptology in India, Virtual Conference, December 13-16, 2020, Proceedings*, volume 12578 of *Lecture Notes in Computer Science*, pages 553–575. Springer, December 2020.

[BK22] Olivier Blazy and Saqib A Kakvi. Identity-based encryption in ddh hard groups. In *International Conference on Cryptology in Africa*, pages 81–102. Springer, Cham, Jul 2022.

[BKKP15] Olivier Blazy, Saqib A. Kakvi, Eike Kiltz, and Jiaxin Pan. Tightly-Secure Signatures from Chameleon Hash Functions. In Jonathan Katz, editor, *Conference on Practice and Theory in Public-Key Cryptography (PKC '15)*, volume 9020 of *Lecture Notes in Computer Science*, pages 257–278, Gaithersburg, Maryland, USA, 2015. Springer.

[BKP14] Olivier Blazy, Eike Kiltz, and Jiaxin Pan. (Hierarchical) Identity-Based Encryption from Affine Message Authentication. In Ran Canetti and Juan Garay, editors, *Advances in Cryptology - Proceedings of CRYPTO '14*, volume 8616 of *Lecture Notes in Computer Science*, pages 408–426, Santa Barbara, California, August 2014. Springer.

[Bla12] Olivier Blazy. *Preuves de connaissance interactives et non-interactives*. PhD thesis, University Paris VII – Denis Diderot, September 2012.

[BM20] Olivier Blazy and Sayantan Mukherjee. Cca-secure abe using tag and pair encoding. In Karthikeyan Bhargavan, Elisabeth Oswald, and Manoj Prabhakaran, editors, *Progress in Cryptology - INDOCRYPT 2020 - 21st International Conference on Cryptology in India, Virtual Conference, December 13-16, 2020, Proceedings*, volume 12578 of *Lecture Notes in Computer Science*, pages 691–714. Springer, December 2020.

[BMN+21] Olivier Blazy, Sayantan Mukherjee, Huyen Nguyen, Duong Hieu Phan, and Damien Stehlé. An anonymous trace-and-revoke broadcast encryption scheme. In Sushmita Ruj Joonsang Baek, editor, *Information Security and Privacy - 26th Australasian Conference, ACISP 2021, Virtual Event, December 1-3, 2021, Proceedings*, volume 13083 of *Lecture Notes in Computer Science*, pages 214–233. Springer, December 2021.

[BP12] Olivier Blazy and David Pointcheval. Traceable Signature with Stepping Capabilities. In David Naccache, editor, *Cryptography and Security: From Theory to Applications*, volume 6805 of Lecture Notes in Computer Science, pages 108–131. Springer, January 2012. Cryptography and Security: From Theory to Applications - Essays Dedicated to Jean-Jacques Quisquater on the Occasion of His 65th Birthday.

[BPV12a] Olivier Blazy, David Pointcheval, and Damien Vergnaud. Compact round-optimal partially-blind signatures. In Ivan Visconti and Roberto De Prisco, editors, *The 8th Conference on Security in Communication Networks (SCN '12)*, volume 7485 of *Lecture Notes in Computer Science*, pages 95–112, Amalfi, Italy, September 2012. Springer.

[BPV12b] Olivier Blazy, David Pointcheval, and Damien Vergnaud. Round-Optimal Privacy-Preserving Protocols with Smooth Projective Hash Functions. In Ronald Cramer, editor, *9th Theory of Cryptography Conference (TCC '12)*, volume 7194 of *Lecture Notes in Computer Science*, pages 94–111, Taormina, Italy, March 2012. Springer.

[BTV20] Olivier Blazy, Patrick Towa, and Damien Vergnaud. Public-key generation with verifiable randomness. In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7-11, 2020, Proceedings, Part I*, volume 12491, pages 97–127, Korea, December 2020. Springer.

[BY19] Olivier Blazy and Chan Yeob Yeun, editors. *Information Security Theory and Practice - 12th IFIP WG 11.2 International Conference, WISTP 2018, Brussels, Belgium, December 10-11, 2018, Revised Selected Papers*, volume 11469 of *Lecture Notes in Computer Science*. Springer, 2019.

[MCB+20] Fatma Merabet, Amina Cherif, Malika Belkadi, Olivier Blazy, Emmanuel Conchon, and Damien Sauveron. New efficient M2C and M2M mutual authentication protocols for iot-based healthcare applications. *Peer-to-Peer Networking and Applications*, 13(2):439–474, 2020.