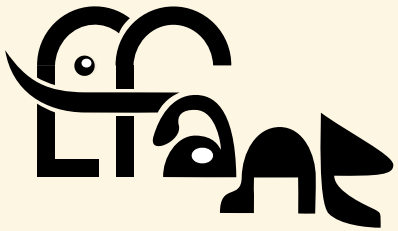
FAST – (Harder Better) FAster STronger Cryptography

2020/02/19 – Bordeaux

Damien Robert

Équipe LFANT, Inria Bordeaux Sud-Ouest



Goal

Cryptology:

- Encryption;
- Authenticity;
- Integrity.

Public key cryptology is based on a one way (trapdoor) function ⇒ asymmetric encryption, signatures, zero-knowledge proofs...

Goal: Improve and extend elliptic curve cryptography to

- Secure the Internet of Things;
- Prepare the next generation of cryptosystems able to resist to quantum computers.

Organisation

- Joint team between LFANT (Lithe and fast algorithmic number theory) https://lfant.math.u-bordeaux.fr/ and PREMA (the Pole of Research in Mathematics and Applications in Africa) http://prmasi.org/;
- Project coordinators: Tony Ezome, Senior Lecturer/Researcher (Cames), University of Sciences and Technology of Masuku (USTM), and Damien Robert (CR Inria).
- PREMA is a Simon's fundation project involving researchers in Cameroun, Gabon, Madagascar, Sénégal along with members in Cote d'Ivoire, Maroc, South Africa and international collaborators in Canada, France, the Netherlands, Singapore.

Results

- Efficiency
  Improving randomness extractions ([KSC+17; CS17]), pseudo-random generators and pseudo-random functions [MV17b].
  - Improving arithmetic and pairing on elliptic curves [GF18; FD17; Fou19; FPE19; MAF19; FD19].
  - Improving normal basis [ES19]
  - Attribute based credentials [SCN19]
- Post quantum cryptography
  - Pairing based signatures [MV17a]
  - Isogenies: modular polynomials for cyclic isogenies between abelian surfaces [MR17], cyclic isogenies given their kernels [DJR+17].
- Misc
  - Attacks [NF19]
  - Arithmetic progression [CM17a; CM17b]
  - Book chapter “Pairings” of the book “Guide to Pairing-Based Cryptography” [EJ17].
- Work in progress:
  - Computing canonical lift of genus 2 curves;
  - Better isogenies in the Hessian model [LF];

Results

- PhDs
  - T. M. Nountu. “Pseudo-Random Generators and Pseudo-Random Functions: Cryptanalysis and Complexity Measures”. PhD thesis. Paris Sciences et Lettres, 2017
  - Aminatou Pecha Njiahouo. Recherche de primitive pour la cryptographie à base de couplage. PhD thesis, Université Paris 8 (France), December 8, 2017.
  - Upcoming PhD thesis: M. Sall: ”Bases Normales, Groupes algébriques et arithmétiques des corps finis” at university Cheikh Anta Diop de Dakar.
  - Upcoming PhD thesis: A. Maiga ”Canonical lift of genus 2 curves” at university Cheikh Anta Diop de Dakar.

Scientific activities for the years 2016–2020

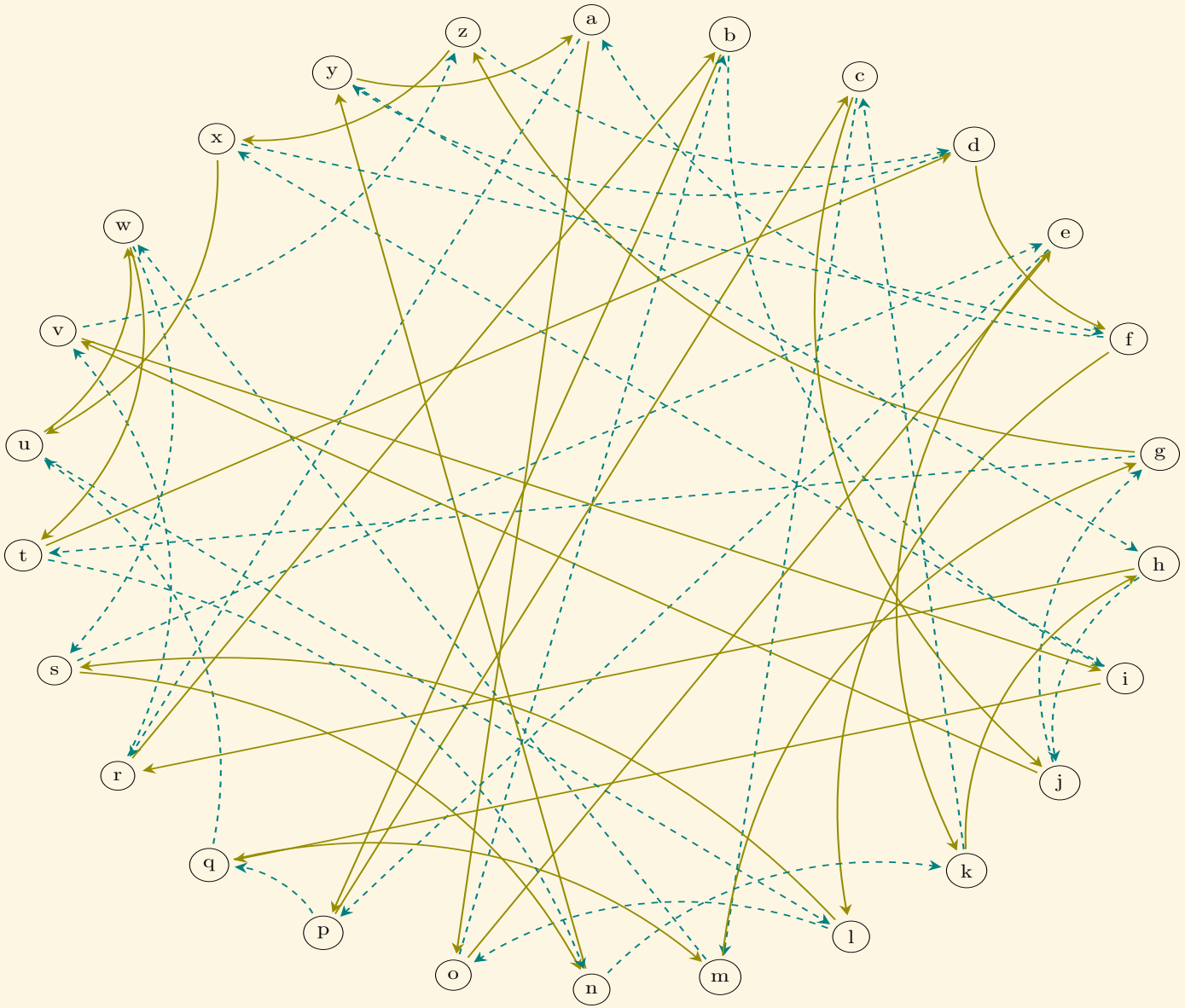
- Lots of short or longer visits;
- One joint workshop at the start;
- Organization of conferences;
- EMA “Mathématiques pour la Cryptographie Post-quantique et Mathématiques pour le Traitement du Signal” at the École Polytechnique de Thiès (Sénégal) from May 10 to May 23 2017 by Djiby Sow and Abdoul Asiz Ciss .
- Ecole Mathématique Africaine (from April 02 to 04 2018 at Franceville), http://prmasi.org/african-mathematical-school-ams-from-april-02-to-april-14-2018 by Tony Ezome;
- Aminatou Pecha organized a CIMPA school (form 2 to 12 July 2019) and the first meeting for women in Mathematics in Central Africa from 13 to 14 July 2019 at AIMS-Cameroon in Limbe.
- Tony Ezome made 4 Teaching stays (two in Burkina Faso, one in The Republic of Congo, and one in Senegal) to introduce Algebraic number theory and algebraic geometry to Master Students.

Assessment and Feedback

- ☺ Lots of teaching and conferences.
- ☺ Four (upcoming) PhD (specific funding for PhD students);
- ☺ Helped opening masters in cryptography in Africa;
- ☹ No industrial collaborations;
- ☹ Not enough visible inter-parternship research collaborations;

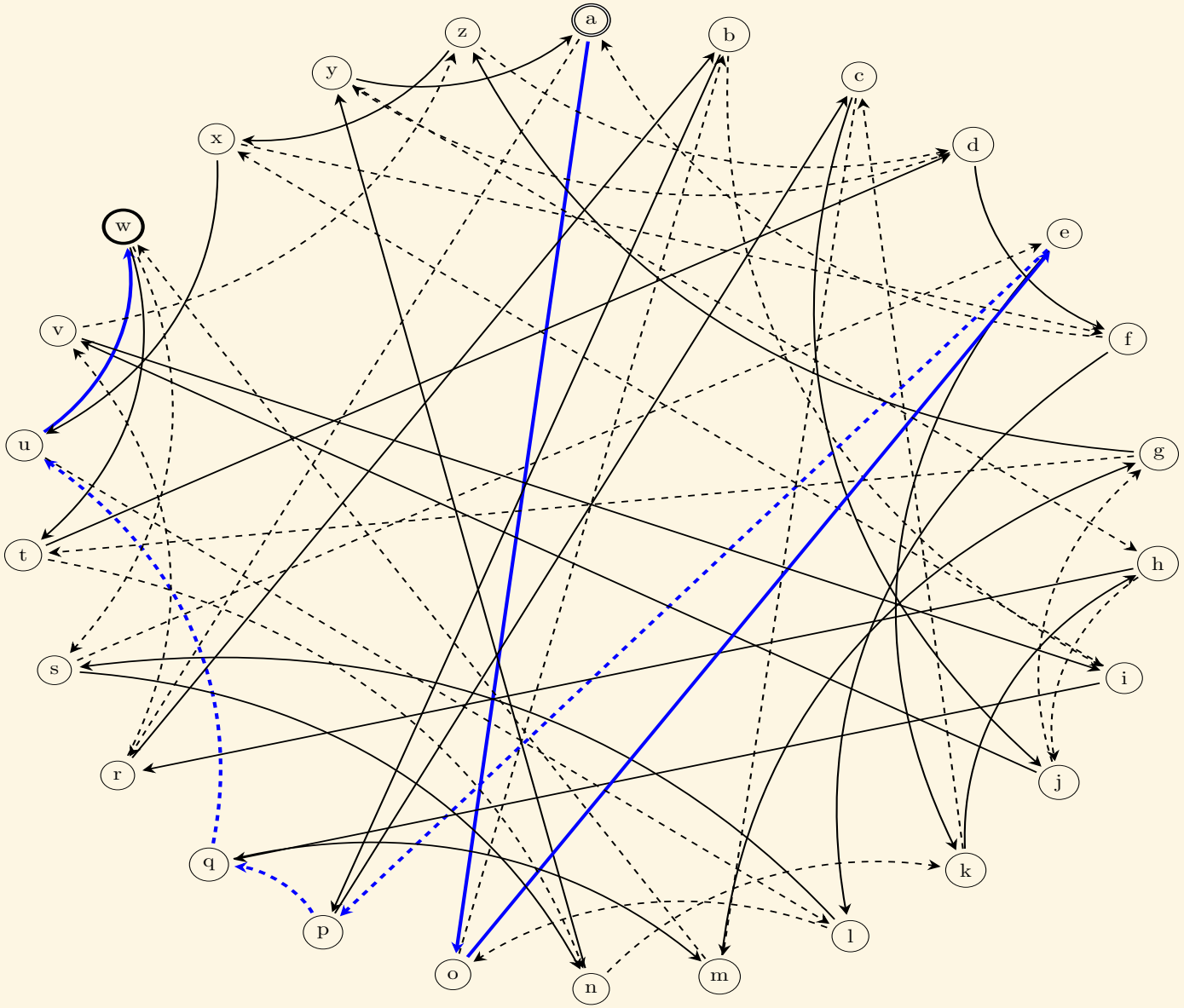
- Lots of Visa problem;
- Administrative burden for long stays;
- Budget cutoff mid December for the last year.

Key exchange on a graph



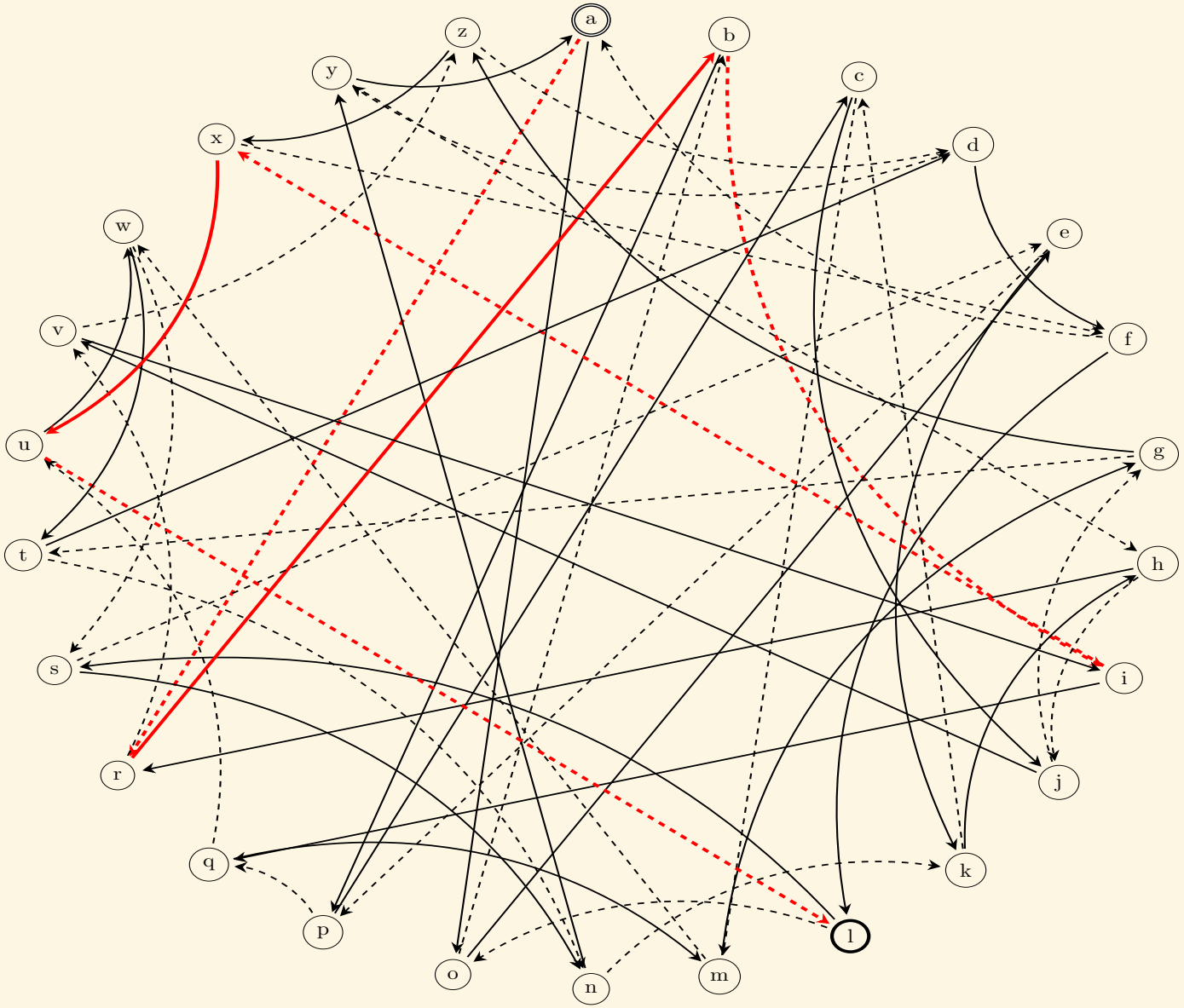
Key exchange on a graph

Alice starts from ‘a’, follow the path 001110, and get ‘w’.



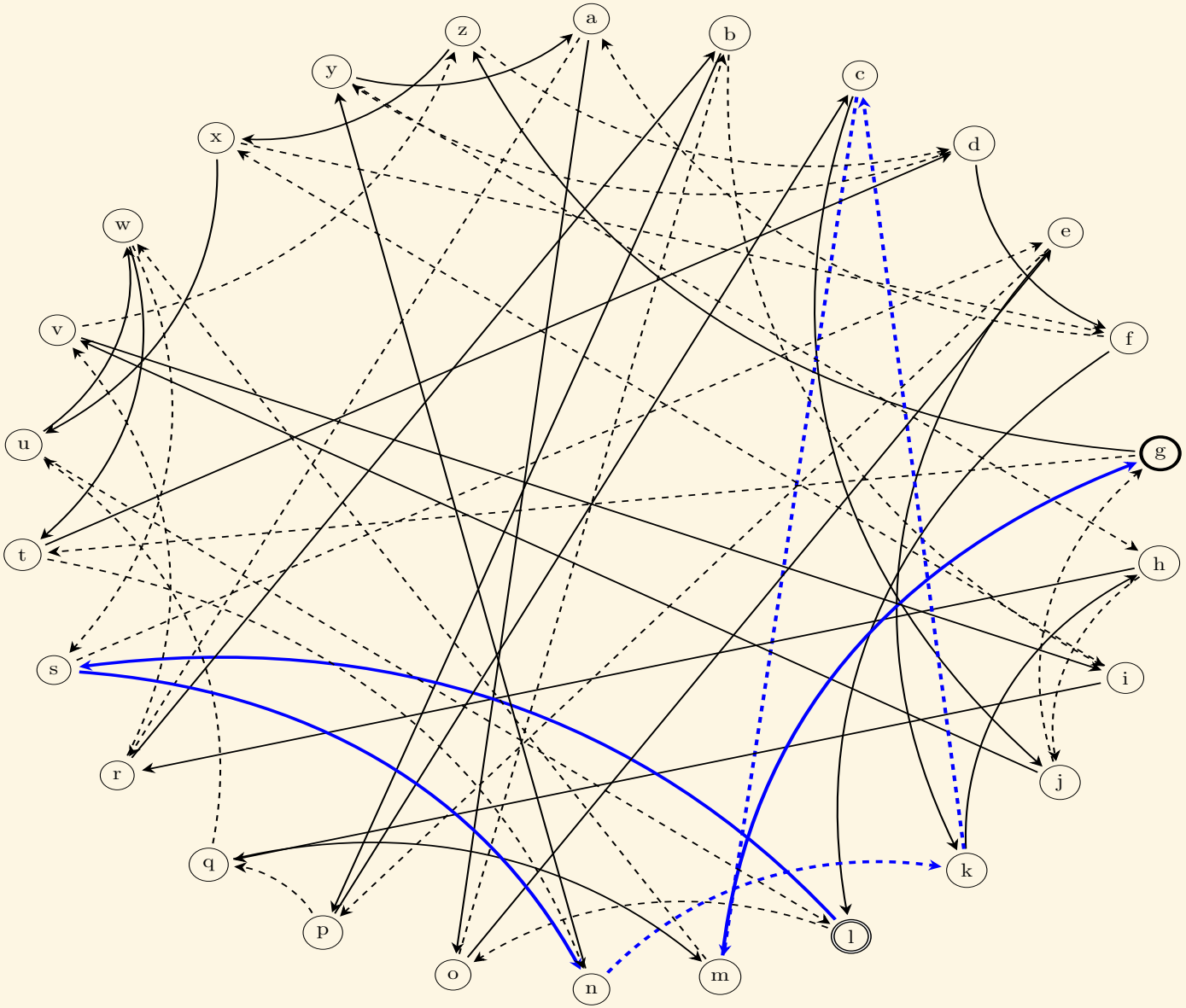
Key exchange on a graph

Bob starts from ‘a’, follow the path 101101, and get ‘l’.



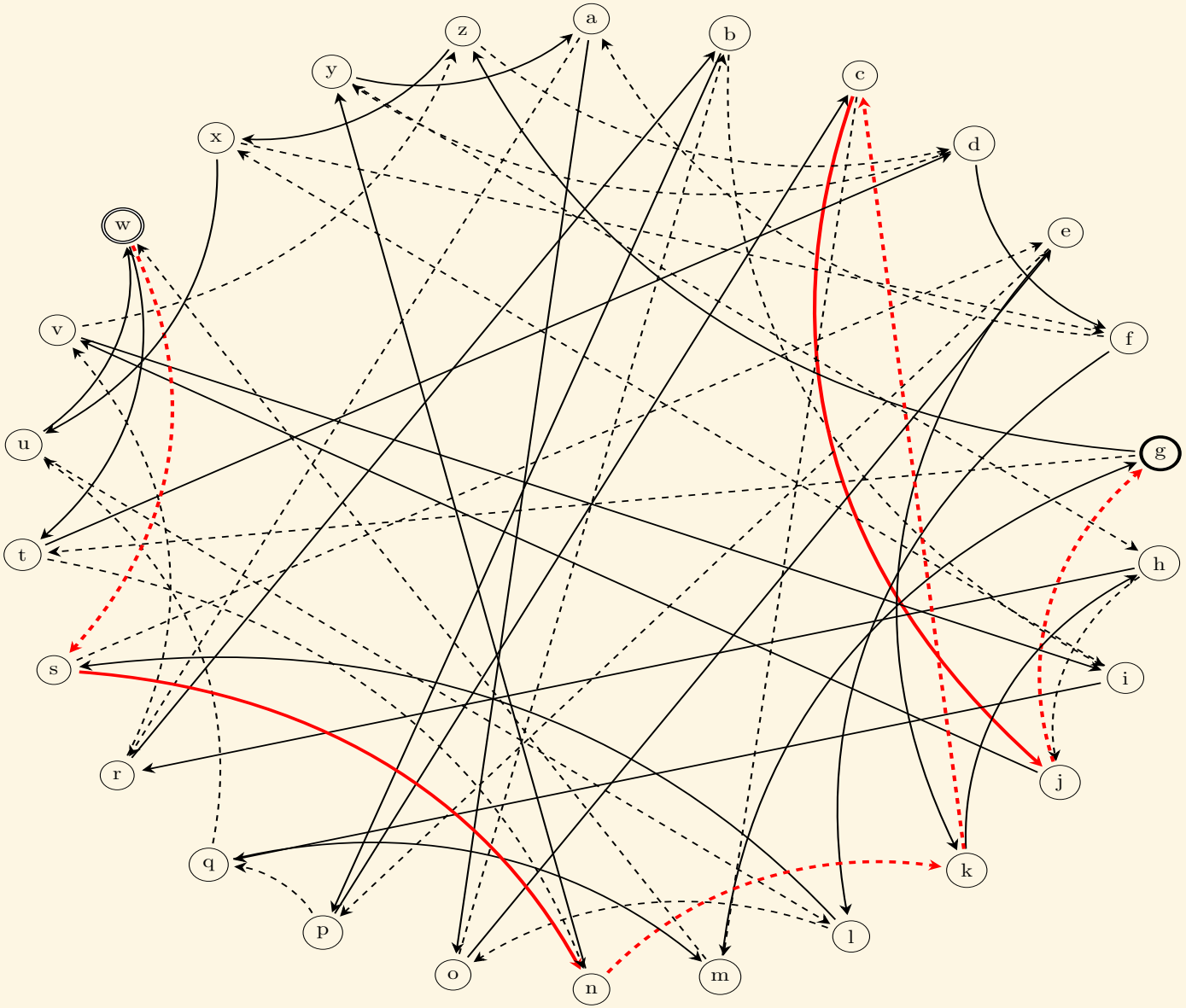
Key exchange on a graph

Alice starts from ‘l’, follow the path 001110, and get ‘g’.



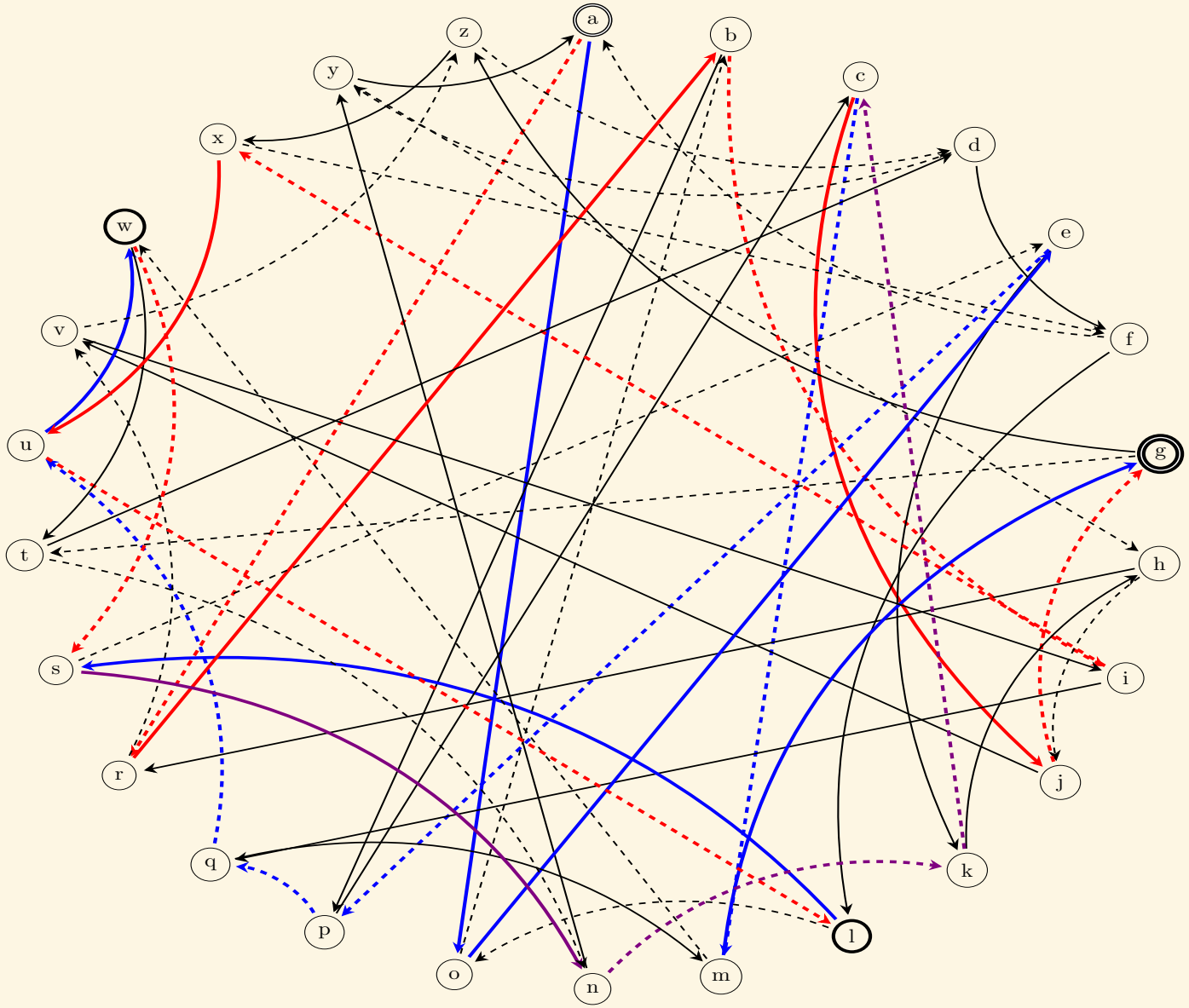
Key exchange on a graph

Bob starts from ‘w’, follow the path 101101, and get ‘g’.



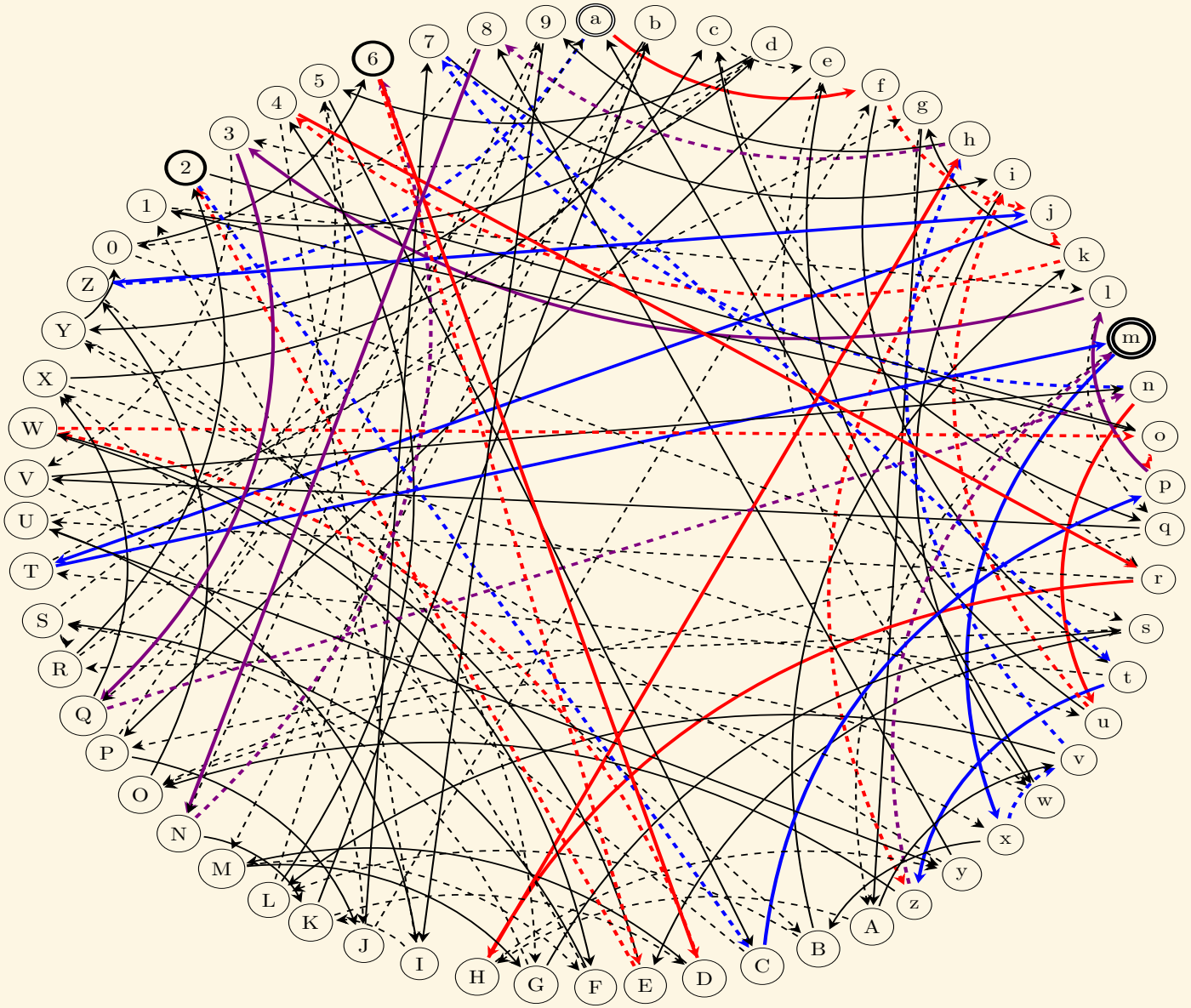
Key exchange on a graph

The full exchange:



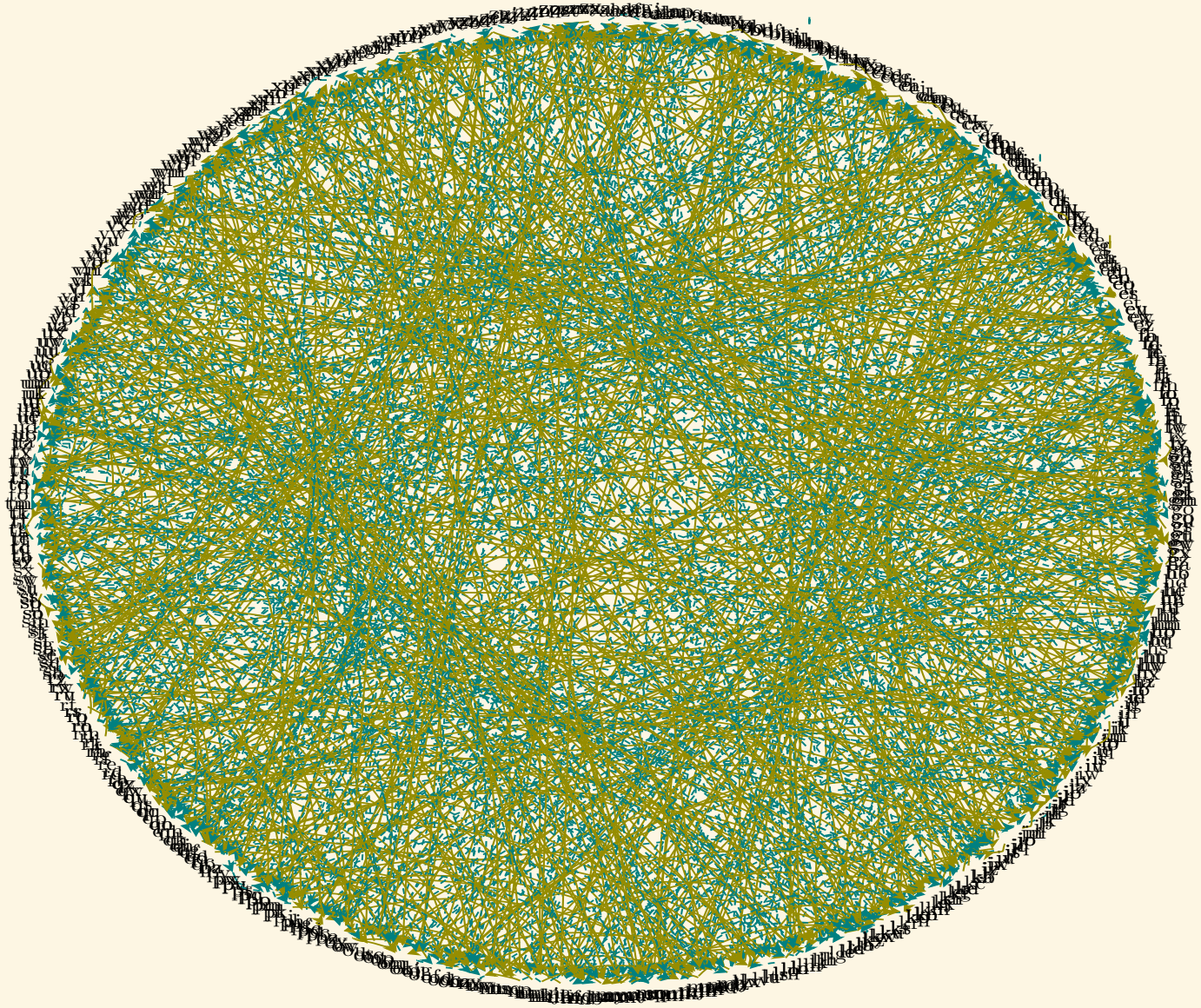
Key exchange on a graph

Bigger graph (62 nodes)



Key exchange on a graph

Even bigger graph (676 nodes)



Elliptic curves isogeny key exchange (Couveignes, Rostovtsev and Stolbunov)

- Use the horizontal isogeny graph of an ordinary elliptic curve E over $\mathbb{F}_q$.
- This is in fact the Cayley graph of the class group of the endomorphism ring of E, which is an imaginary quadratic order.
- For cryptography, choose a curve such that the graph has 2^{256} nodes.

- [LF]: Faster isogenies in the Hessian model of elliptic curves.
- Cost for computing an $\ell = 2s+1$ isogeny in the Hessian model: from $(5s+3)M+4S+8sC$ (Moody2019) to $(3s+3)M+3S+3sC$.

Bibliography

A. A. Ciss and D. Moody. "Arithmetic progressions on conics". In: *Journal of integer sequences* 20.2 (2017), p. 3 (cit. on p. 4).

A. A. Ciss and D. Moody. "Geometric progressions on elliptic curves". In: *Glasnik matemati ki* 52.1 (2017), pp. 1–10 (cit. on p. 4).

A. A. Ciss and D. Sow. "Two-Source Randomness Extractors for Elliptic Curves for Authenticated Key Exchange". In: *International Conference on Codes, Cryptology, and Information Security*. Springer. 2017, pp. 85–95 (cit. on p. 4).

A. Dudeanu, D. Jetchev, D. Robert, and M. Vuille. "Cyclic Isogenies for Abelian Varieties with Real Multiplication". working paper or preprint. Nov. 2017. URL: https://hal.inria.fr/hal-01629829 (cit. on p. 4).

N. El Mrabet and M. Joye. *Guide to Pairing-Based Cryptography*. CRC Press, 2017 (cit. on p. 4).

T. Ezome and M. Sall. "Normal bases from 1-dimensional algebraic groups". In: *Journal of Symbolic Computation* (2019) (cit. on p. 4).

E. Fouotsa. "Parallelizing pairings on Hessian elliptic curves". In: *Arab Journal of Mathematical Sciences* 25.1 (2019), pp. 29–42 (cit. on p. 4).

E. Fouotsa and O. Diao. “A Theta Model for Elliptic Curves”. In: *Mediterranean Journal of Mathematics* 14.2 (2017), p. 65 (cit. on p. 4).

E. Fouotsa and O. Diao. “Complete addition formulas on the level four theta model of elliptic curves”. In: *Afrika Matematika* (2019), pp. 1–17 (cit. on p. 4).

E. Fouotsa, A. Pecha, and N. El Mrabet. “Beta Weil pairing revisited”. In: *Afrika Matematika* 30.3-4 (2019), pp. 371–388 (cit. on p. 4).

L. Ghammam and E. Fouotsa. “Improving the computation of the optimal ate pairing for a high security level”. In: *Journal of Applied Mathematics and Computing* (2018), pp. 1–16 (cit. on p. 4).

D. Kolyang, D. Sow, A. A. Ciss, and H. B. Tchapgnouo. “Two-sources randomness extractors in finite fields and in elliptic curves”. In: *REVUE AFRICAINE DE LA RECHERCHE EN INFORMATIQUE ET MATHÉMATIQUES APPLIQUÉES* 24 (2017) (cit. on p. 4).

P. B. F. Lontouo and E. Fouotsa. “Analogue of Vélu’s Formulas for Computing Isogenies over Hessian Model of Elliptic Curves”. In: () (cit. on pp. 4, 16).

N. B. Mbiang, D. F. Aranha, and E. Fouotsa. “Computing the Optimal Ate Pairing over Elliptic Curves with Embedding Degrees 54 and 48 at the 256-bit security level”. In: *International Journal of Applied Cryptography* (2019) (cit. on p. 4).

T. Mefenza and D. Vergnaud. “Lattice Attacks on Pairing-Based Signatures”. In: *IMA International Conference on Cryptography and Coding*. Springer. 2017, pp. 352–370 (cit. on p. 4).

T. Mefenza and D. Vergnaud. “Polynomial interpolation of the Naor–Reingold pseudo-random function”. In: *Applicable Algebra in Engineering, Communication and Computing* 28.3 (2017), pp. 237–255 (cit. on p. 4).

E. Milio and D. Robert. “Modular polynomials on Hilbert surfaces”. working paper or preprint. Sept. 2017. URL: https://hal.archives-ouvertes.fr/hal-01520262 (cit. on p. 4).

A. Nitaj and E. Fouotsa. “A new attack on RSA and Demytko’s elliptic curve cryptosystem”. In: *Journal of Discrete Mathematical Sciences and Cryptography* 22.3 (2019), pp. 391–409 (cit. on p. 4).

T. M. Nountu. “Pseudo-Random Generators and Pseudo-Random Functions: Cryptanalysis and Complexity Measures”. PhD thesis. Paris Sciences et Lettres, 2017 (cit. on p. 5).

I. Sene, A. A. Ciss, and O. Niang. “I2PA: An Efficient ABC for IoT”. In: *Cryptography* 3.2 (2019), p. 16 (cit. on p. 4).