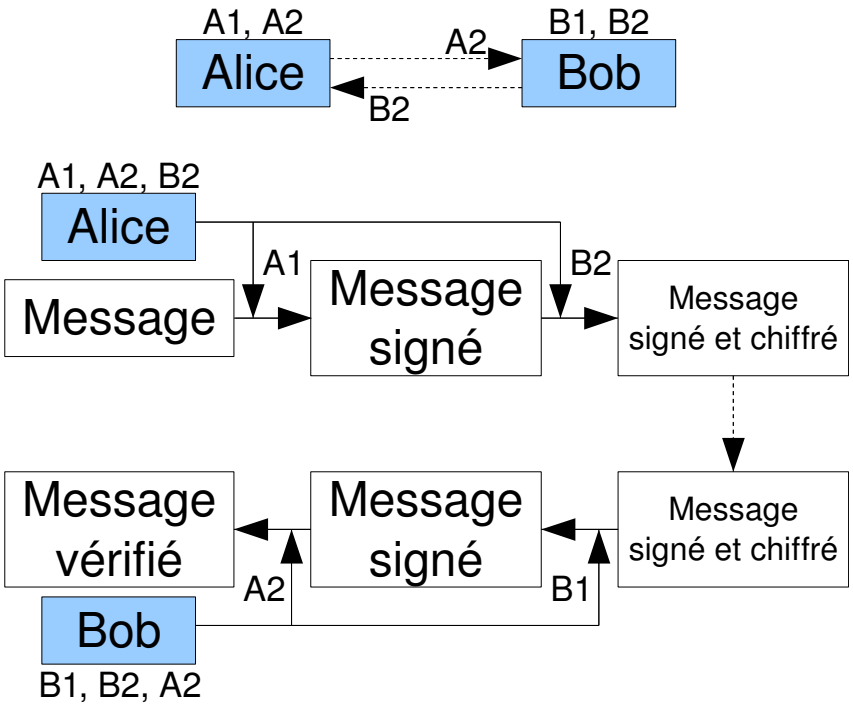

FIG. 1 – Schéma de principe de la communication à l'aide de la cryptographie asymétrique. Les clés A1 et A2 sont respectivement les clés privée et publique d'Alice, B1 et B2 celles de Bob. Les flèches en pointillés indiquent le transfert de données sur un canal vulnérable aux attaques passives. Le protocole assure à Alice que son message n'est lisible que par Bob, et assure à Bob l'authenticité du message reçu.

	.com	.de	.org	.edu	.uk	.net	.fr	.nl	.ch	.at	.au	.se	.ca	.it	
.com	6.43	6.25	6.00	6.53	6.41	6.22	6.28	6.02	6.06	7.22	6.03	6.50	6.13	6.26	.com
.de	5.92	5.27	5.43	6.20	5.92	5.62	5.71	5.44	5.28	6.41	5.61	6.09	5.77	5.69	.de
.org	5.72	5.48	5.21	5.87	5.66	5.49	5.43	5.25	5.28	6.44	5.26	5.80	5.44	5.44	.org
.edu	6.27	6.31	5.90	6.11	6.30	6.12	6.28	5.93	6.04	7.30	5.89	6.26	5.92	6.25	.edu
.uk	6.19	6.04	5.71	6.32	5.88	5.97	5.97	5.72	5.80	6.93	5.71	6.22	5.89	5.95	.uk
.net	6.18	5.89	5.71	6.32	6.14	5.94	5.97	5.72	5.72	6.87	5.79	6.26	5.92	5.96	.net
.fr	6.10	5.85	5.53	6.33	6.00	5.85	5.31	5.50	5.64	6.80	5.69	6.22	5.87	5.72	.fr
.nl	5.78	5.55	5.31	5.91	5.72	5.54	5.52	4.81	5.29	6.59	5.45	5.78	5.58	5.59	.nl
.ch	5.78	5.35	5.29	5.98	5.76	5.51	5.55	5.32	4.72	6.44	5.39	5.89	5.62	5.49	.ch
.at	7.59	7.11	7.05	7.86	7.47	7.30	7.28	7.10	6.92	6.72	7.23	7.68	7.38	7.28	.at
.au	5.84	5.75	5.36	5.95	5.76	5.64	5.66	5.48	5.49	6.63	4.87	5.85	5.44	5.63	.au
.se	6.13	6.08	5.73	6.16	6.12	5.95	6.08	5.73	5.83	7.03	5.74	5.15	5.84	6.00	.se
.ca	6.13	6.02	5.70	6.20	6.12	5.95	6.00	5.81	5.84	6.98	5.67	6.26	5.59	5.98	.ca
.it	6.11	5.85	5.56	6.34	6.04	5.86	5.75	5.62	5.58	6.81	5.64	6.17	5.88	4.98	.it
	.com	.de	.org	.edu	.uk	.net	.fr	.nl	.ch	.at	.au	.se	.ca	.it	

TAB. 1 – Distance moyenne entre les clés d'un TLD et celles d'un autre TLD. Aucune tendance notable ne semble pouvoir être observée. Noter que le tableau n'est pas symétrique, car le graphe du réseau de confiance est orienté. Les distances sont indiquées en partant du TLD de la ligne pour aller jusqu'au TLD de la colonne.

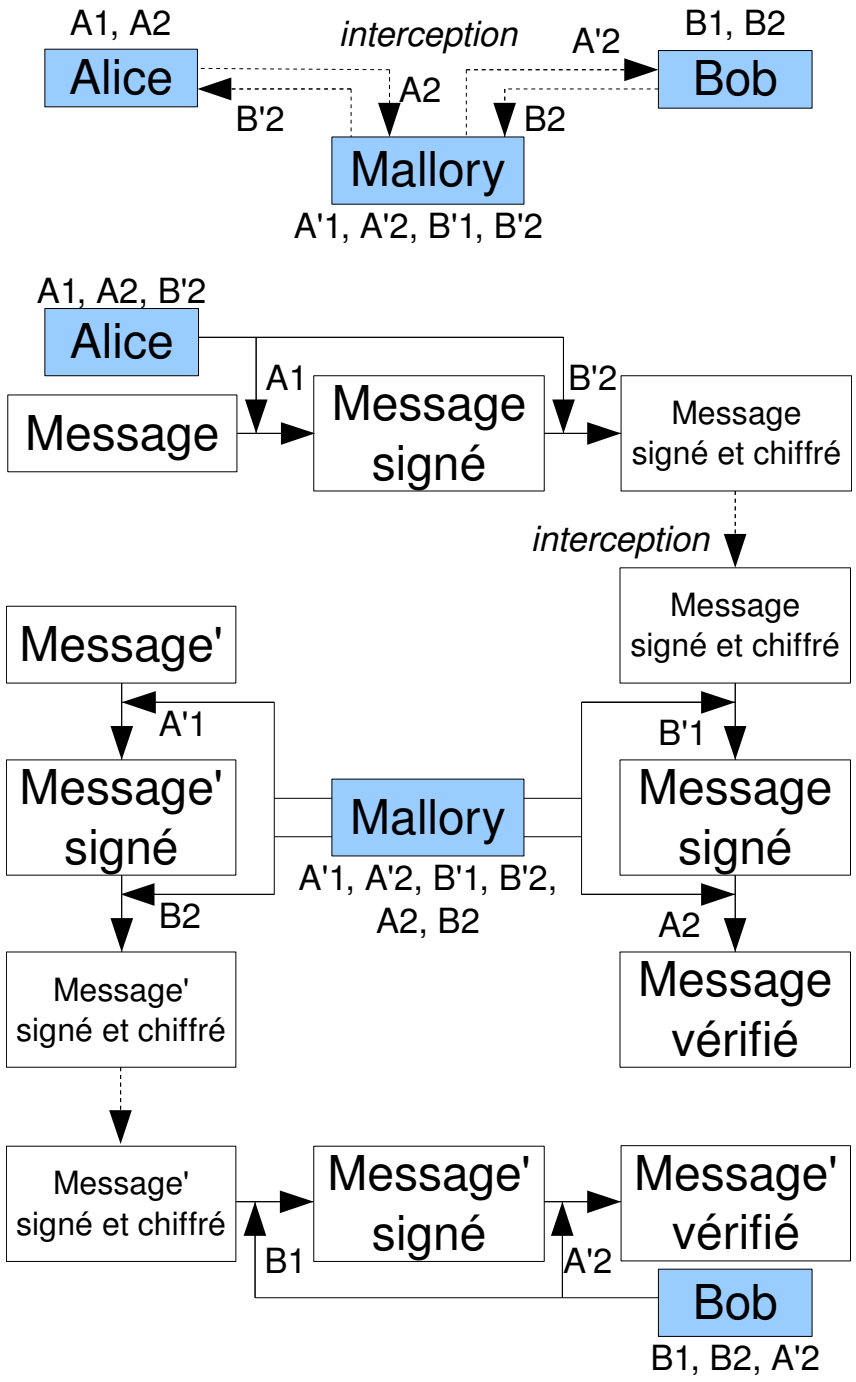

FIG. 2 – Schéma de principe de l'attaque de l'homme du milieu, menée par Mallory. Les clés A1 et A2 sont respectivement les clés privée et publique d'Alice, B1 et B2 celles de Bob, et A'1, A'2, B'1, B'2 des clés factices créées par Mallory. Les flèches en pointillés indiquent le transfert de données sur un canal vulnérable aux attaques actives. En se faisant passer pour Bob auprès d'Alice et pour Alice auprès de Bob, Mallory est en mesure de lire et de modifier le message.

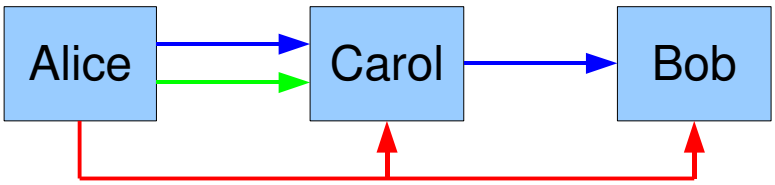

FIG. 3 – Schéma de principe du réseau de confiance. Les flèches bleues, vertes et rouges indiquent la signature de clé, la confiance en une personne, et l'assurance de la validité de la clé respectivement. Alice a vérifié la clé de Carol (elle a donc signé la clé de Carol) et a confiance en Carol, et Carol a vérifié la clé de Bob (elle a donc signé la clé de Bob), donc Alice a une garantie de la validité de la clé de Bob.

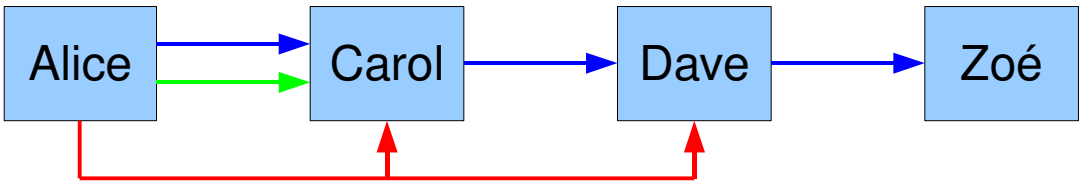

FIG. 4 – Schéma de principe de la non-transitivité du réseau de confiance. La légende est celle de la figure 3. Alice a vérifié la clé de Carol et a confiance en elle, et celle-ci a vérifié la clé de Dave. Alice a donc une garantie de la validité de la clé de Dave, mais pas de celle de Zoé puisqu'Alice n'a pas confiance en Dave.

TLD	Nombre clés	Distance TLD	Distance aléa.	Différence
TOTAL	41229	5.967422	5.967422	0
.de	10195	5.247043	5.966777	0.719734
.com	8793	6.435397	5.964490	-0.470907
.org	4633	5.228405	5.960977	0.732572
.net	4430	5.955349	5.895636	-0.059713
.edu	1855	6.211485	5.915838	-0.295647
.at	1126	6.549152	6.009203	-0.539949
.ch	938	4.812058	5.979436	1.167379
.uk	902	5.874658	5.885630	0.010972
.nl	807	4.832648	5.803330	0.970682
.se	616	5.126112	5.951894	0.825782
.fr	603	5.251495	5.920090	0.668595
.it	494	5.032766	6.019612	0.986846
.au	431	4.849732	5.807026	0.957295
.ca	403	5.612700	5.792844	0.180144
.no	266	5.907768	5.801345	-0.106422
.fi	245	5.428255	6.007280	0.579025
.es	213	4.822213	5.884172	1.061959
.dk	207	4.844570	6.057108	1.212537
.pl	196	5.430810	6.089103	0.658293
.cz	186	5.407966	5.947624	0.539658
.br	181	6.489210	6.159641	-0.329569
.be	181	5.078203	5.999817	0.921614
.nz	172	4.831362	6.060675	1.229313
.info	164	5.354030	5.617787	0.263757
.gov	151	6.435770	5.676988	-0.758783
.jp	149	5.757038	5.895996	0.138958
.name	110	4.895455	6.241157	1.345702
.hu	102	5.557478	5.784218	0.226740
.eu	93	4.972598	6.051914	1.079316
.us	78	5.574129	5.989809	0.415680
.ru	77	6.546298	5.444594	-1.101703
.gr	61	4.504434	5.700349	1.195915
.cx	60	4.619722	6.052222	1.432500
.mil	59	6.289572	5.888251	-0.401321
.ar	59	5.151393	6.166619	1.015226
.nu	55	4.975207	5.650248	0.675041
.ie	51	4.712034	6.086121	1.374087
.cl	49	4.020825	5.748855	1.728030
.cc	49	5.463140	5.857976	0.394835
.li	48	4.193576	5.577257	1.383681
.il	48	4.432292	6.670139	2.237847

Tab. 2 – Distance moyenne entre tout couple de clés pour chaque TLD, comparé aux distances pour un sous-ensemble aléatoire de clés de même taille. Les colonnes indiquent respectivement le nombre de clés dans le TLD, la distance moyenne entre tout couple de clés du TLD, la distance moyenne entre tout couple de clés du sous-ensemble aléatoire, et la différence de ces deux colonnes. Pour les TLD correspondant à un pays, la distance moyenne du TLD est en général plus basse que celle de l'ensemble de clés aléatoires.

TLD	Nombre	Dist. graph. TLD	Dist. graph. rand	Diff. graph.
TOTAL	41518	2734218.640580	2734218.640580	0.000000
.de	10293	2734129.696247	2734177.930927	48.234679
.com	8869	2733828.170516	2733933.050529	104.880013
.org	4633	2733977.717087	2733715.849931	-261.867157
.net	4456	2733992.641092	2732461.801724	-1530.839368
.edu	1825	2731891.350734	2732554.094312	662.743579
.at	1163	2731582.253503	2732115.958488	533.704984
.ch	984	2731321.516533	2732120.941978	799.425445
.uk	903	2732030.791044	2732709.621568	678.830524
.nl	831	2728158.928604	2732165.022434	4006.093830
.se	617	2730642.992385	2731590.759039	947.766655
.fr	609	2729937.588843	2724927.897378	-5009.691465
.it	480	2730961.945102	2724485.792345	-6476.152756
.au	427	2731317.671051	2722117.294296	-9200.376755
.ca	399	2731345.247024	2725666.015186	-5679.231837
.no	266	2728807.302787	2717153.803587	-11653.499200
.fi	248	2721836.257568	2722882.247815	1045.990247
.es	226	2726391.307467	2725909.281392	-482.026075
.dk	202	2725406.693791	2723440.845521	-1965.848270
.pl	199	2701674.611850	2719000.794424	17326.182575
.cz	192	2718595.437915	2695349.156512	-23246.281402
.be	186	2730342.275110	2727246.037406	-3096.237704
.br	182	2695093.651967	2715819.790229	20726.138262
.nz	172	2714471.658352	2726946.900561	12475.242209
.info	158	2722016.231088	2711691.334743	-10324.896344
.gov	155	2709476.691159	2717992.148792	8515.457633
.jp	145	2726965.567007	2715782.797165	-11182.769843
.name	111	2709557.502597	2721646.929417	12089.426820
.hu	103	2674100.096610	2697567.239409	23467.142799
.eu	97	2697815.814930	2694774.577530	-3041.237400
.us	79	2682433.685950	2713789.859772	31356.173822
.ru	75	2715675.548525	2717471.600472	1796.051947
.cx	61	2693122.809399	2683110.290740	-10012.518659
.gr	59	2695408.599987	2705460.704631	10052.104643
.ar	59	2690992.924995	2683882.886890	-7110.038105
.mil	58	2624351.626181	2672674.391637	48322.765456
.nu	57	2672927.687521	2671022.354921	-1905.332600
.ie	54	2719083.826405	2697081.308993	-22002.517412
.cc	54	2711953.537288	2645641.015326	-66312.521962
.li	52	2663439.484475	2694137.930846	30698.446371
.cl	51	2685184.329081	2721458.757083	36274.428002
.il	48	2712402.947470	2702129.847129	-10273.100341

Tab. 3 – Distance moyenne graphique (euclidienne) entre tout couple de clés pour chaque TLD, comparé aux distances pour un sous-ensemble aléatoire de clés de même taille, avant lancement de l'algorithme force-directed. Les colonnes sont les mêmes que celles du tableau 2, à ceci près qu'il s'agit ici de distances graphiques. Aucune tendance notable ne semble pouvoir être observée.

TLD	Nombre	Dist. graph. TLD	Dist. graph. rand	Diff. graph.
TOTAL	41518	3193.064371	3193.064371	0.000000
.de	10293	2506.366864	3230.252117	723.885253
.com	8869	3164.285610	3140.449526	-23.836084
.org	4633	5042.325938	3263.105052	-1779.220886
.net	4456	2815.622084	3318.198797	502.576714
.edu	1825	4300.806350	3538.412800	-762.393550
.at	1163	2271.667924	2959.093469	687.425545
.ch	984	2428.502339	3219.626131	791.123791
.uk	903	2717.983256	3029.249258	311.266002
.nl	831	1944.275874	2944.523480	1000.247606
.se	617	2172.339745	3034.948489	862.608744
.fr	609	2163.335576	2747.032359	583.696783
.it	480	1907.802628	2790.056523	882.253896
.au	427	1906.782654	2845.420643	938.637989
.ca	399	2166.010990	2929.184160	763.173169
.no	266	4132.550155	3990.157557	-142.392598
.fi	248	2241.706746	2664.099467	422.392721
.es	226	2387.264135	3277.433316	890.169181
.dk	202	2278.013934	3010.094538	732.080604
.pl	199	2010.590806	3112.368173	1101.777366
.cz	192	2919.197356	3721.482760	802.285404
.be	186	1782.686669	2534.432093	751.745423
.br	182	2758.758147	3556.436895	797.678748
.nz	172	1540.284712	3639.189005	2098.904293
.info	158	2202.237291	3126.149543	923.912252
.gov	155	2853.553849	3419.255919	565.702070
.jp	145	2729.735426	3254.006170	524.270744
.name	111	1884.525307	2942.834560	1058.309253
.hu	103	1585.385901	3370.923366	1785.537465
.eu	97	2325.132918	4086.783790	1761.650871
.us	79	2048.731833	2891.677212	842.945379
.ru	75	2068.142556	3160.869485	1092.726929
.cx	61	1612.862343	2588.744234	975.881891
.gr	59	2234.572861	2811.852891	577.280030
.ar	59	3661.775134	4416.189455	754.414321
.mil	58	2572.962541	2978.316256	405.353714
.nu	57	2088.583784	2259.275753	170.691968
.ie	54	1681.149227	2430.957943	749.808716
.cc	54	2424.158831	2967.629716	543.470885
.li	52	2266.359168	2441.486862	175.127694
.cl	51	1457.802389	2556.356192	1098.553804
.il	48	1749.870133	1890.371893	140.501760

Tab. 4 – Distance moyenne graphique (euclidienne) entre tout couple de clés pour chaque TLD, comparé aux distances pour un sous-ensemble aléatoire de clés de même taille, après exécution de l'algorithme force-directed pendant quelques heures. Les colonnes sont les mêmes que celles du tableau 3. Pour les TLD correspondant à un pays, la distance moyenne du TLD est en général plus basse que celle de l'ensemble de clés aléatoires.

Entrée	**Effet**
Clic gauche	Sélection de clé(s)
Clic droit	Déplacement de clé(s)
Clic central	Déplacement de la vue
Molette	Zoom
a	Tout sélectionner
c	Colorier les clés
d	Calculer les distances entre clés
e	Sélection par TLD ou adresse de courriel
f	Marquage des clés de départ pour les calculs de distance
g	Affichage de la résultante des forces
i	Affichage des identifiants de clés
k	Sélection par identifiant
l	Recalcul manuel de la résultante
m	Déplacement manuel suivant la résultante
n	Affichage des noms et adresses de courriel
q	Quitter
r	Sélection de clés aléatoires
s	Sélection des clés ayant signé les clés sélectionnées
t	Affichage du nombre de clés dans la sélection
v	Inversion de la sélection
x	Activation ou désactivation de l'algorithme force-directed
z	Zoom automatique
/	Remise à zéro des opérateurs
+	Opérateur union
-	Opérateur différence ensembliste
*	Opérateur intersection
\	Opérateur différence symétrique
A	Tout sélectionner
C	Coloriage rapide
D	Suppression des marques de départ et d'arrivée
F	Marquage des clés d'arrivée pour les calculs de distance
G	Masquage de la résultante des forces
I	Masquage des identifiants de clés
L	Recalcul manuel de la résultante (toutes les clés)
M	Déplacement manuel suivant la résultante (toutes les clés)
N	Masquage des noms et adresses de courriel
S	Sélection des clés ayant été signées par les clés sélectionnées
Z	Centrer la vue
Ctrl+A	Calcul de données pour les tableaux 2, 3 et 4
Ctrl+B	Calcul de données pour le tableau 1
Ctrl+C	Arrangement des clés sélectionnées en cercle

Tab. 5 – Liste des commandes du logiciel.

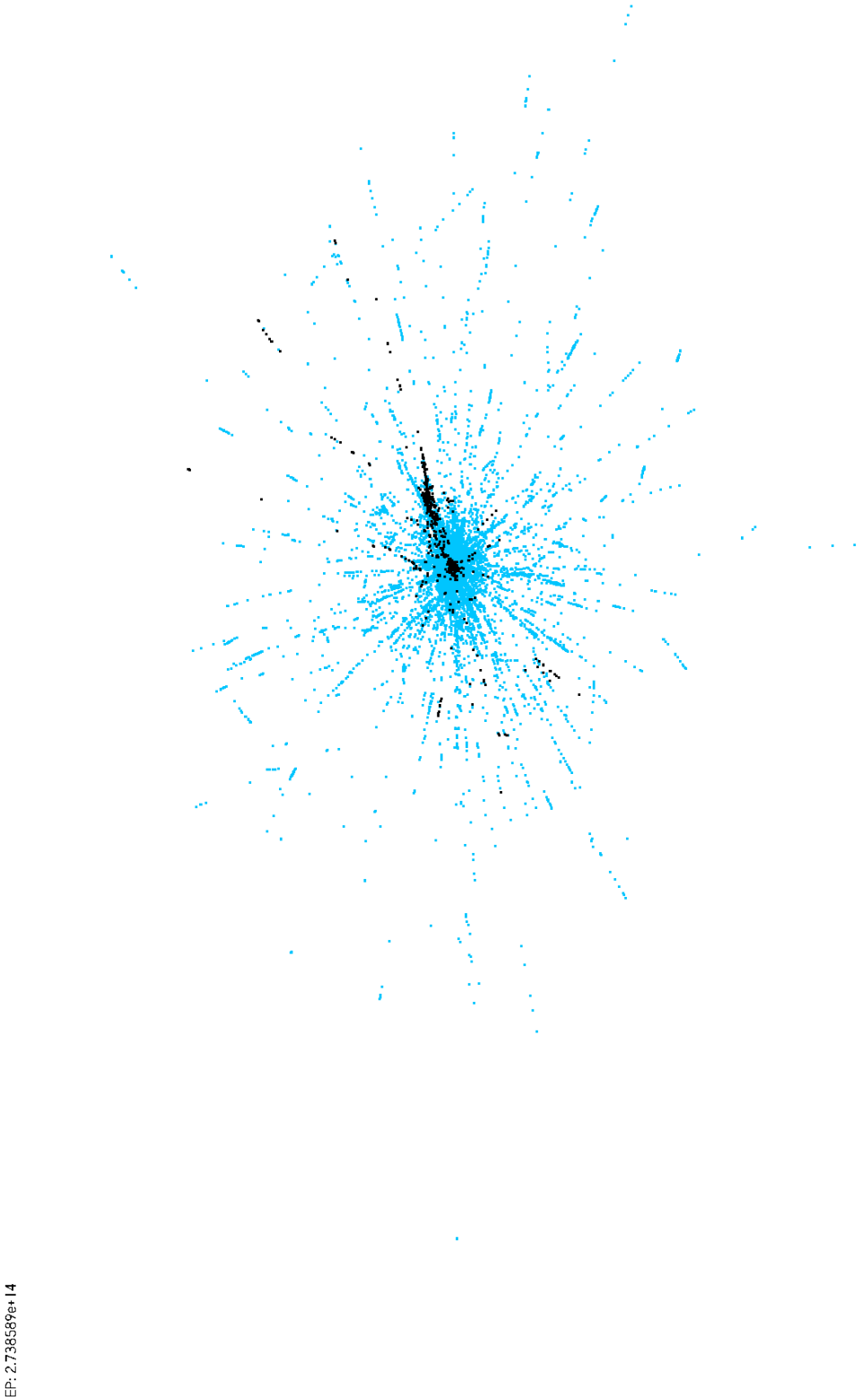

FIG. 5 – Position des clés autrichiennes (en noir) dans le réseau de confiance.

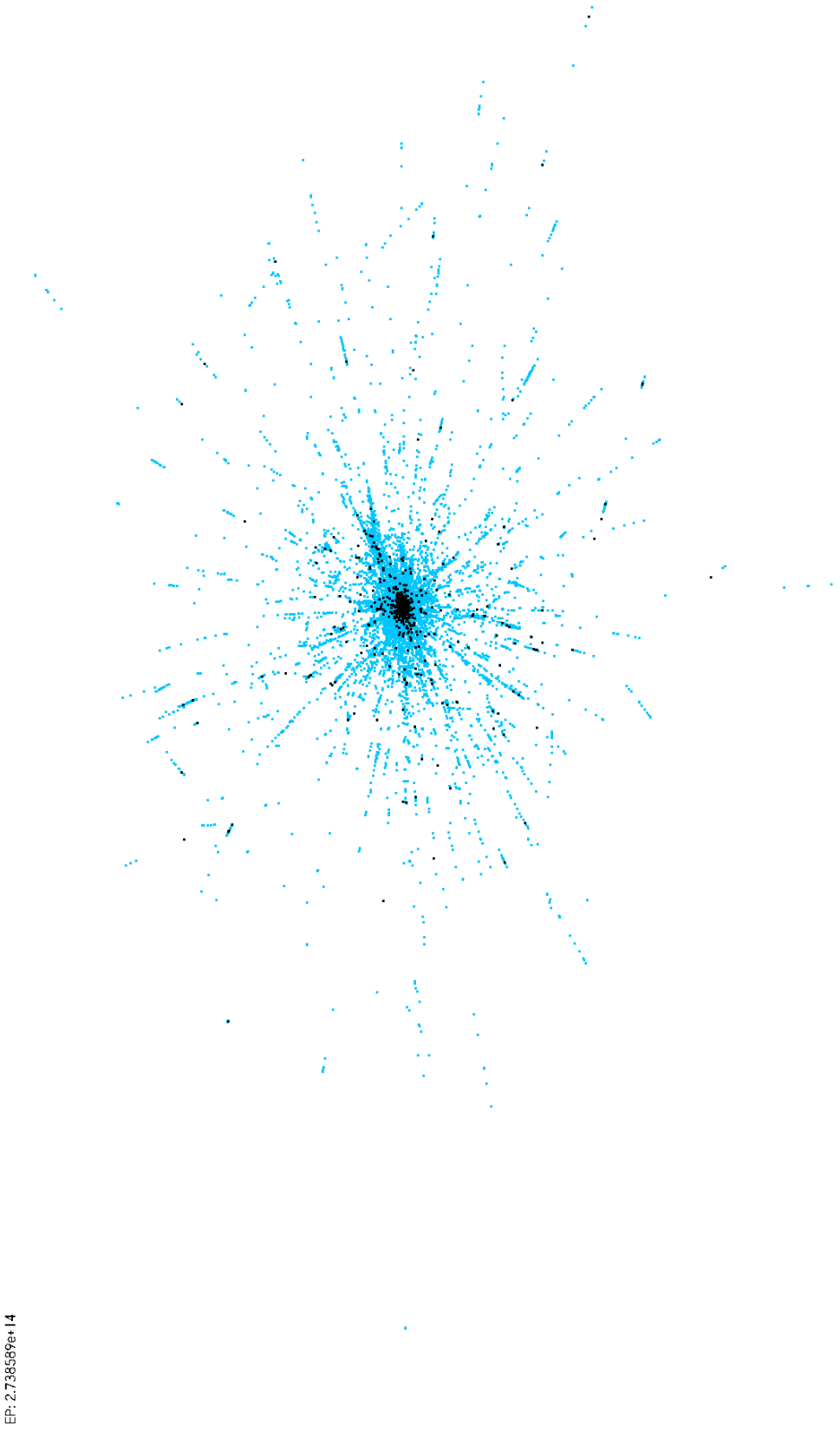

Fig. 6 – Position d'un sous-ensemble de clés aléatoires aussi nombreuses que les clés autrichiennes, à comparer avec la figure 5. On remarque que les clés autrichiennes ont davantage tendance à former des alignements.

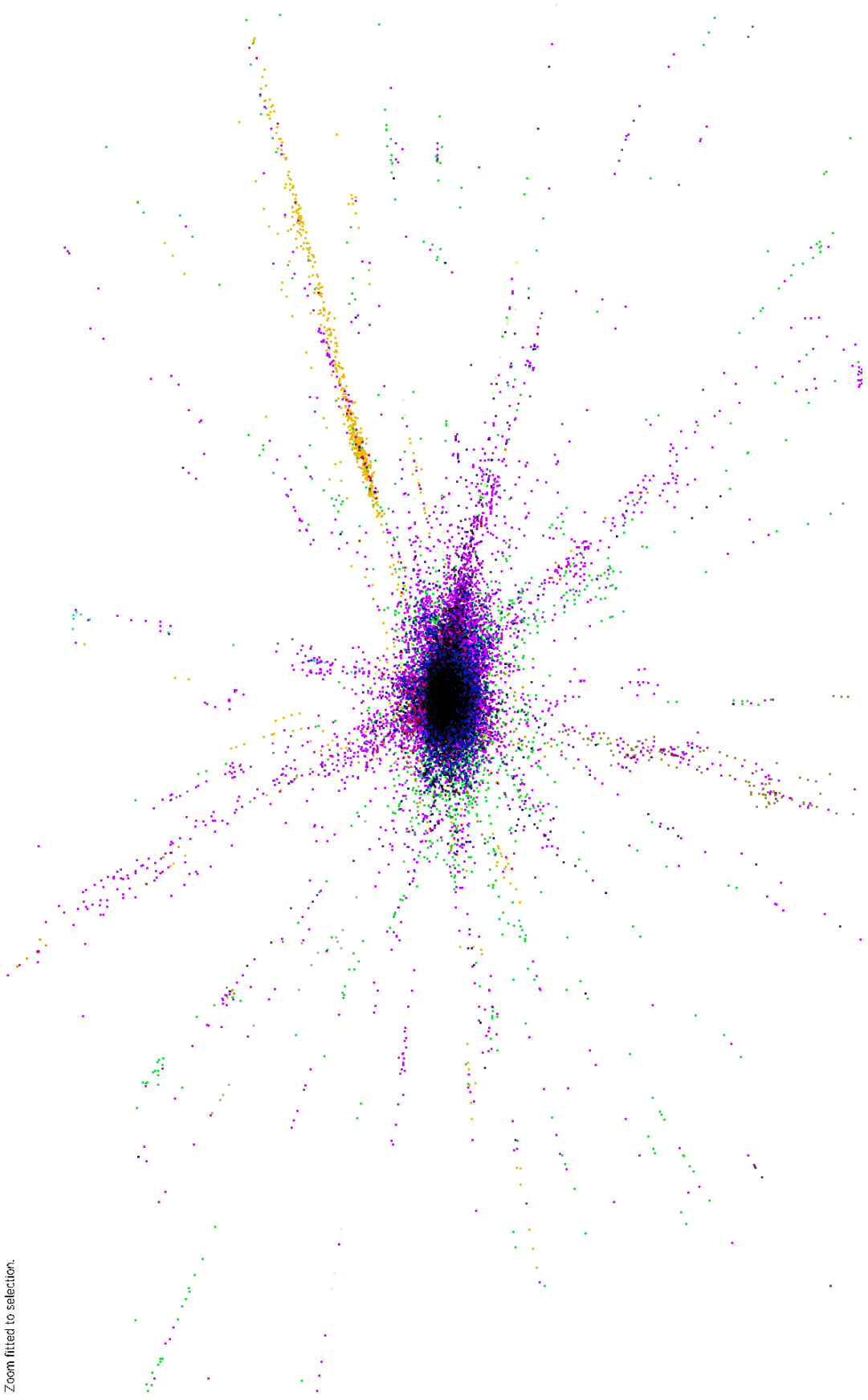

FIG. 7 – Centre du réseau de confiance, avec coloriage des clés selon leur TLD. On observe que les TLD ne sont pas répartis de façon homogène.

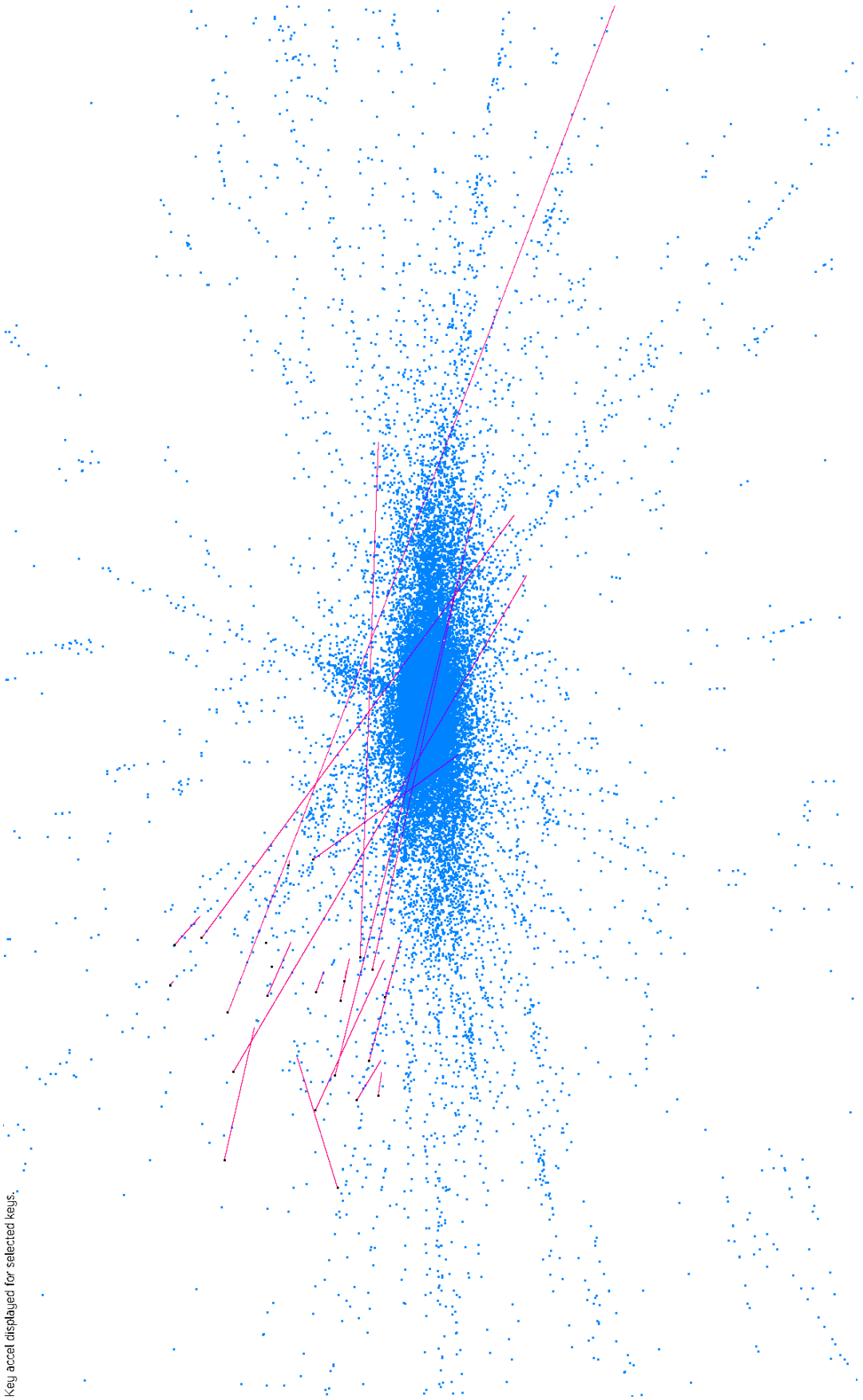

FIG. 8 – Affichage de la résultante des forces de rappel pour quelques sommets aléatoires.

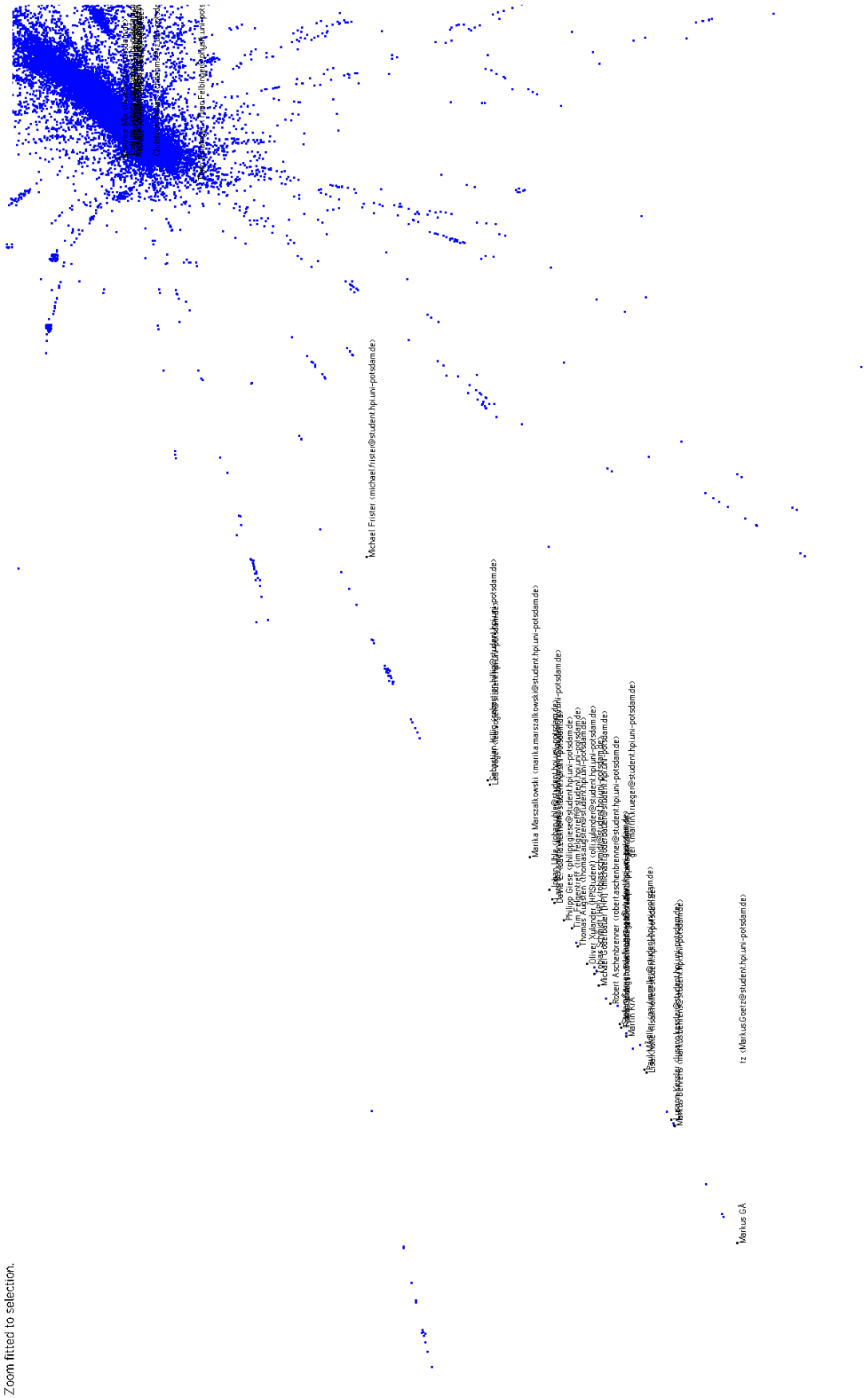

Fig. 9 – Ensemble des clés du nom de domaine `uni-potsdam.de` (Universität Potsdam), qui sont presque toutes au même endroit sur la représentation graphique.

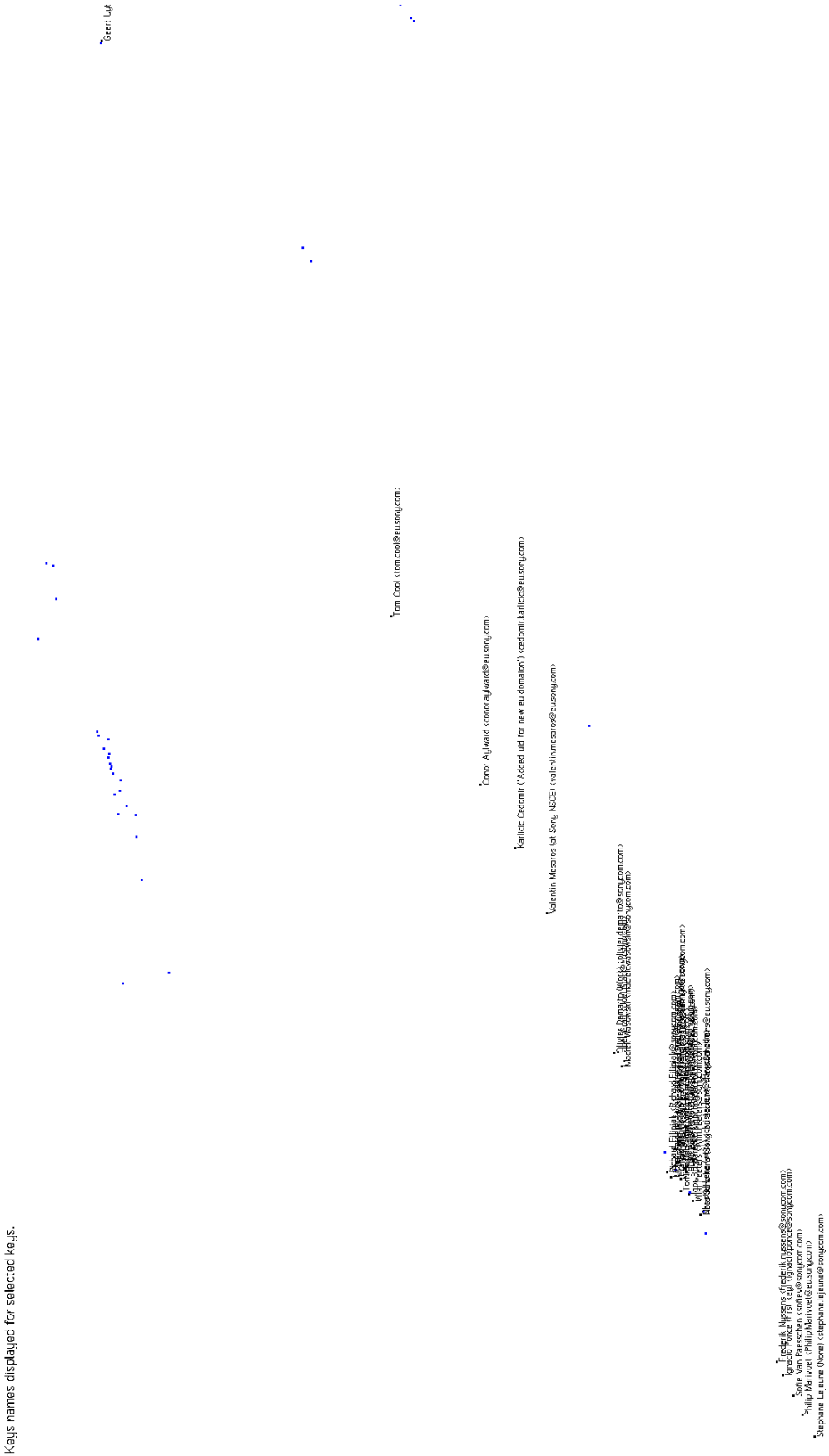

Fig. 10 – Ensemble des clés de noms de domaines associés à l'entreprise Sony, qui sont toutes au même endroit sur la représentation graphique.

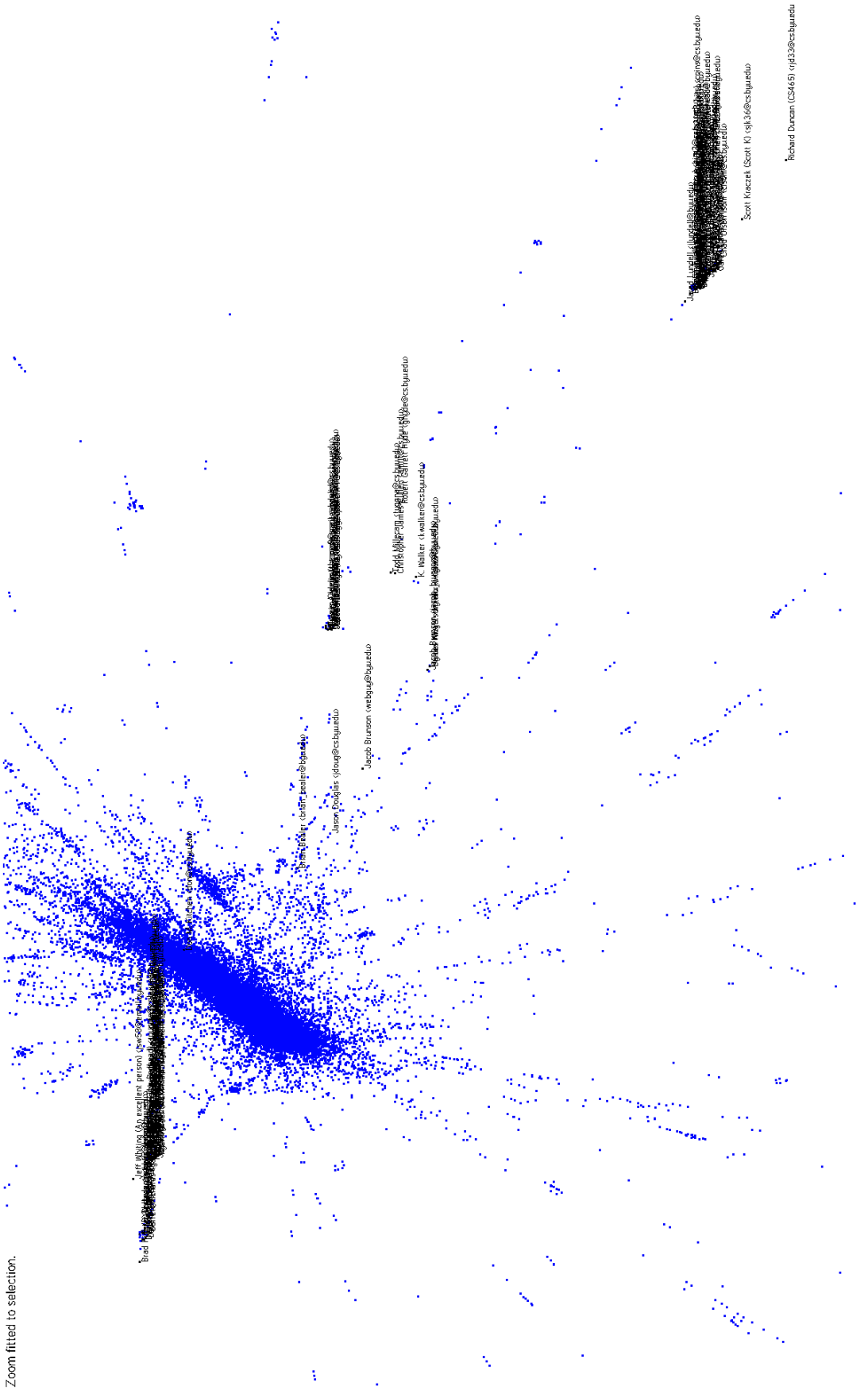

Fig. 11 – Ensemble des clés du nom de domaine `byu.edu` (Brigham Young University), qui sont presque toutes au même endroit sur la représentation graphique.

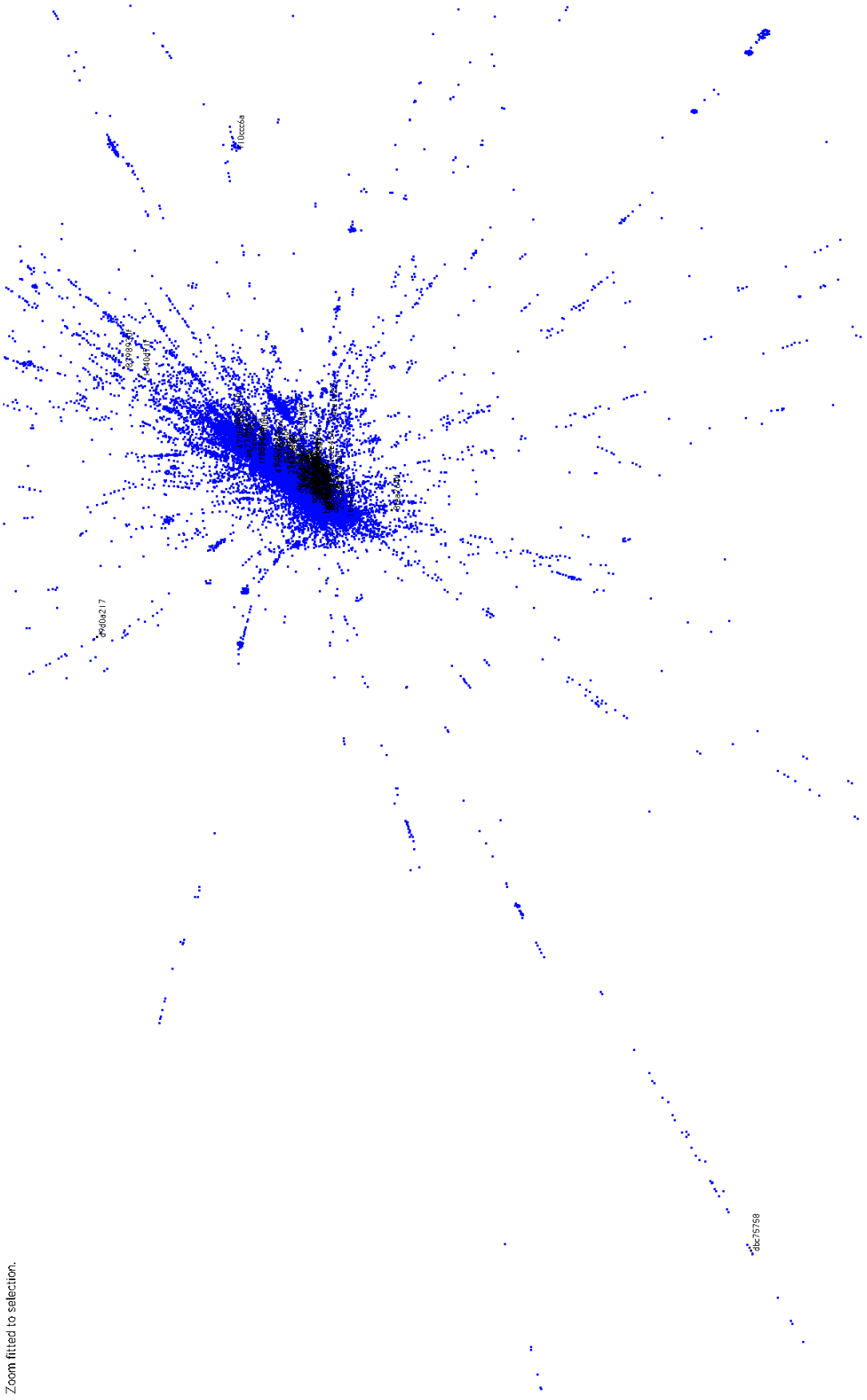

FIG. 12 – Ensemble de clés aléatoires aussi nombreuses que les clés du domaine `byu.edu` (à comparer avec la figure 11).

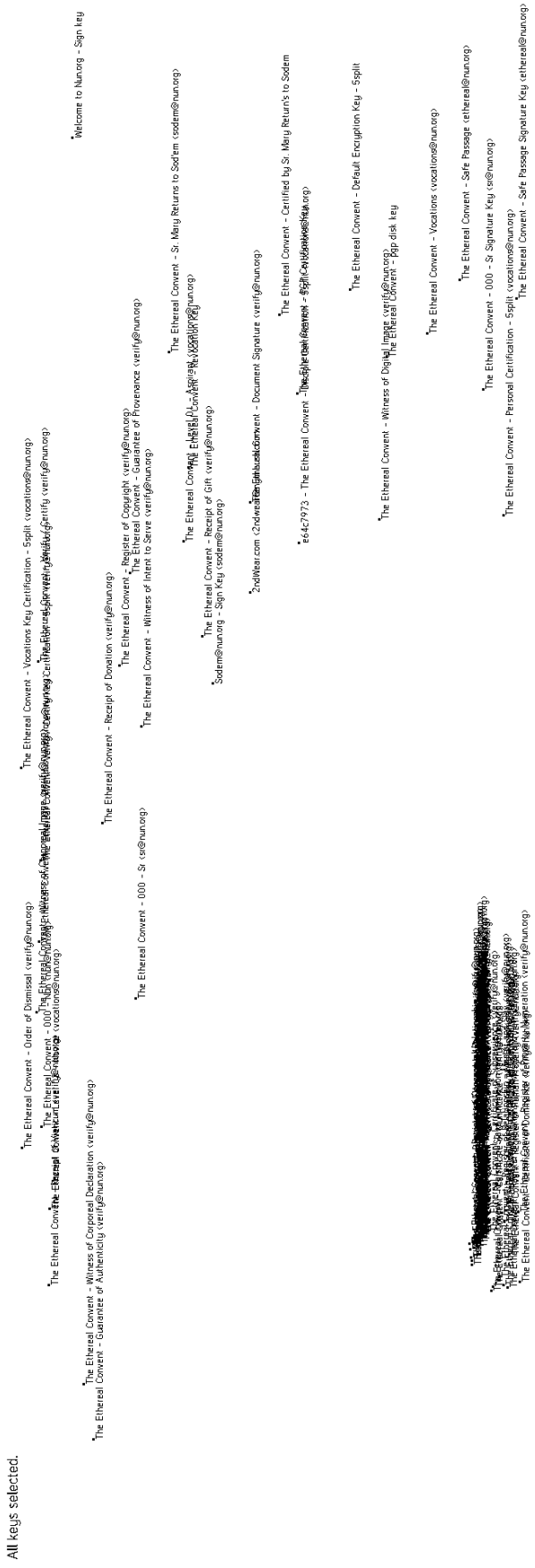

Fig. 13 – Un ensemble de clés assez originales dans le réseau de confiance, qui a été repéré graphiquement avec le logiciel. Elles semblent correspondre aux grades d'une institution religieuse probablement fictive.