



**HAL**  
open science

# Rapport Scientifique Projet TiNum : Une étude des pratiques sur la sécurité des mots de passe par l'approche ludique du storytelling chez les enfants du cycle 3 en contexte guadeloupéen

Lamprini Chartofylaka, Antoine Delcroix

## ► To cite this version:

Lamprini Chartofylaka, Antoine Delcroix. Rapport Scientifique Projet TiNum : Une étude des pratiques sur la sécurité des mots de passe par l'approche ludique du storytelling chez les enfants du cycle 3 en contexte guadeloupéen. [Rapport Technique] N/A. 2021. hal-03381373

**HAL Id: hal-03381373**

**<https://hal.science/hal-03381373>**

Submitted on 4 Nov 2021

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



# Projet Ti Num



## Projet TiNum

Une étude des pratiques sur la sécurité des mots de passe par l'approche ludique du storytelling chez les enfants du cycle 3 en contexte guadeloupéen

Lauréat de l'appel à projets 2019-2020

PORTEUSE DU PROJET:  
**LAMPRINI CHARTOFLAKA**

CONSEILLER SCIENTIFIQUE:  
**ANTOINE DELCROIX, PROFESSEUR DES UNIVERSITÉS**

**CENTRE DE RECHERCHES ET DE RESSOURCES EN ÉDUCATION ET  
FORMATION (EA-4538), UNIVERSITÉ DES ANTILLES**

# Remerciements

Je tiens à remercier toutes les personnes qui ont contribué à la réalisation du projet de recherche *TiNum*.

Mon professeur, M. Antoine Delcroix, professeur des universités et conseiller scientifique du projet, qui m'a aidée lors de la rédaction et du déroulement de cette étude. Son écoute et ses conseils m'ont permis de donner vie et de faire évoluer ce projet.

Mes collègues au sein de l'Institut national supérieur du professorat et de l'éducation (INSPE) de l'académie de la Guadeloupe - Université des Antilles : M. Kenny Mariette, Mme Mirella Vingatama, Mme Justine Rose, Mme Marie-Gilberte Compper, M. Gilbert Chadru et au sein de mon laboratoire Centre de Recherches et de Ressources en Éducation et Formation (CRREF - EA4538) : M. Thomas Forissier et M. Frédéric Anciaux pour leur aide sur l'organisation matérielle et financière du projet. Je remercie également Mme Muriel Joseph-Théodore pour ses encouragements à présenter ce projet dans le cadre des actions d'innovation et de recherche de la Région académique de la Guadeloupe.

Les élèves qui ont participé avec enthousiasme au projet et les équipes pédagogiques qui m'ont accueillies dans leurs écoles afin de recueillir les données: Mme Martine Thalus, Mme Célia Obertan, Mme Cathy Bonbonne, M. Thierry Phardin, Mme Prisca Aubert, Mme Adonis Katia, ainsi que le personnel d'encadrement suivant : Mme Sandrine Benjamin, M. Mathieu Chalcou, M. Bernard Drymon, M. Fabrice Lomon, M. Jean-Michel Magne.

Enfin, je remercie le Groupement d'Intérêt Scientifique (GIS) Jeu et Sociétés d'avoir financé cette étude et particulièrement M. Boris Noyet pour son soutien constant.

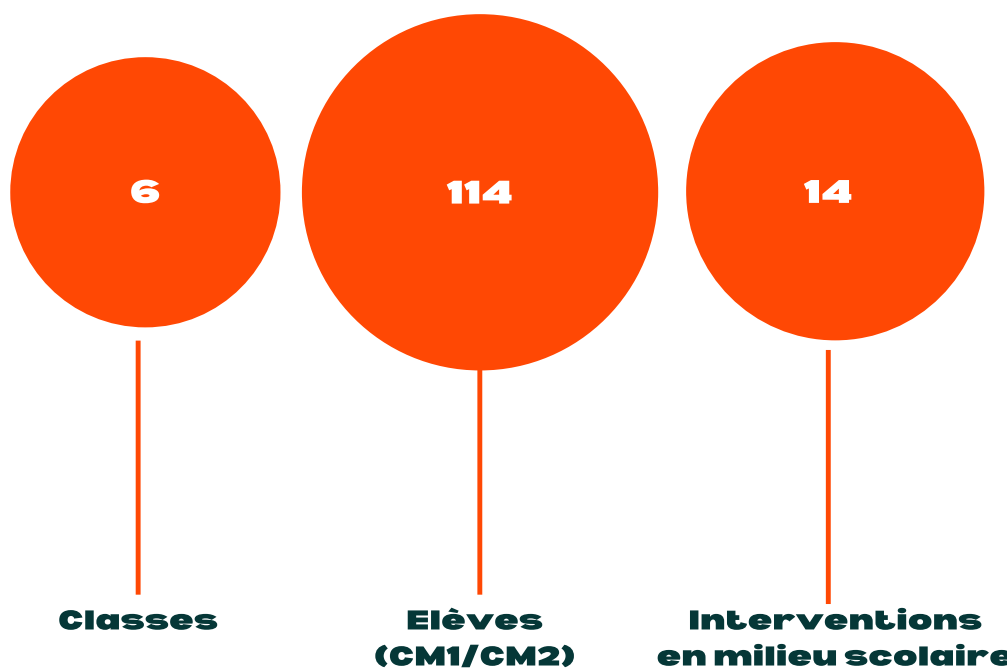


## **ARCHIPEL DE GUADELOUPE (ANTILLES FRANÇAISES)**

**SAINT-FRANÇOIS, CAPESTERRE BELLE-EAU, POINTE-À-PITRE,  
VIEUX-FORT, TERRE-DE HAUT, LA DÉSIRADE**



**NOVEMBRE 2020 - MAI 2021 (7 MOIS)**



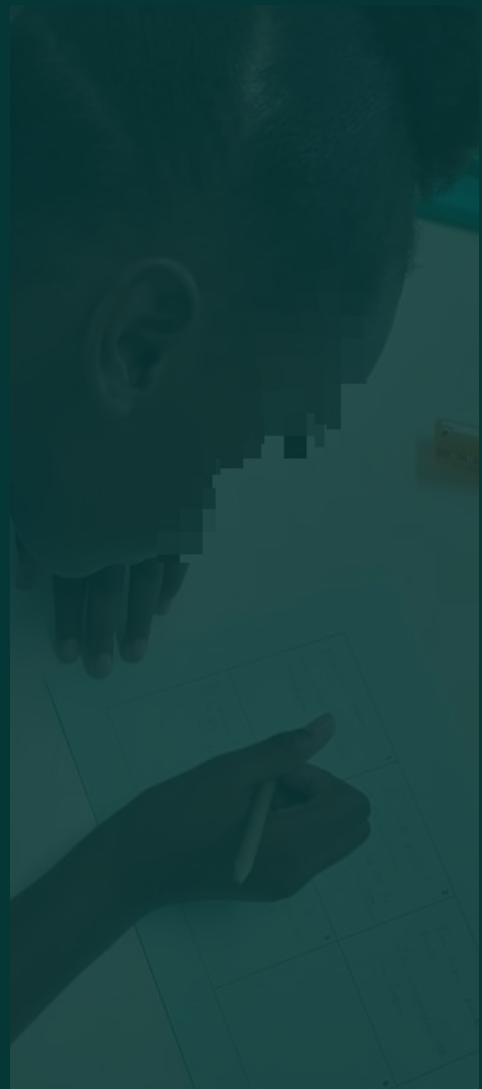
Toutes les mesures de distanciations en vigueur dans la Région académique de la Guadeloupe ont été respectées.

# Introduction

Dans une période façonnée par de nombreuses innovations pour les enfants et par leur accès quotidien aux appareils et ressources numériques, il apparaît pertinent de se pencher sur les enjeux cachés de ses usages et de mener des actions pour rendre les enfants plus responsables, en particulier en favorisant leur sensibilisation et leur apprentissage à la sécurité informatique.

En prenant l'exemple du choix d'un mot de passe fort, notre projet s'inscrit dans cette lignée, en permettant de sensibiliser et d'enseigner les bases de la sécurité informatique, aux élèves du cycle 3 dans l'archipel de la Guadeloupe.

**Mots-clés:** cybersécurité, enfant, mot de passe, dispositif pédagogique, fragilité numérique



# Objectifs de recherche

En **premier lieu**, ce projet tente de renouveler les approches pédagogiques sur l'apprentissage de la sécurité informatique chez le jeune enfant en proposant une activité ludique qui incite au dialogue autour de concepts et d'objets d'études complexes et les sensibilise, par la suite, aux enjeux des activités en ligne.

En **deuxième lieu**, il vise à montrer que des activités ludiques peuvent contribuer au développement des compétences attendues dans les instructions officielles, notamment en enseignement moral et civique en école primaire :

- “Le développement des aptitudes au discernement et à la réflexion critique prend appui sur l'éducation aux médias et à l'information (EMI) et sur la discussion réglée” (Programme du cycle 3, 2020, p.66) ;
- “Le développement de compétences de Connaître ses droits et responsabilités dans l'usage des médias - Citoyenneté et capacité à agir” (Orientations pour l'éducation aux médias et à l'information (EMI) Cycles 2 et 3, 2018, p.4).

En **troisième lieu**, le projet Ti Num s'inscrit dans les démarches conjointes du CRREF et de la Région académique de la Guadeloupe (Territoire Numérique Éducatif depuis septembre 2021) visant à développer des projets scientifiques et pédagogiques. Il s'agit de répondre aux enjeux de réduction des fractures éducatives, sociales et économiques par le numérique dans un territoire où les fragilités sont très sensibles, mais où l'attraction des enfants, au cœur de ce projet, vers le numérique est considérable.



# Problématique

Cette expérimentation s'appuie sur une première étude menée en Guadeloupe en 2018 qui a montré des résultats prometteurs (Chartofylaka et Delcroix, 2018) mais qui méritaient cependant d'être confortés par des tests à une plus grande échelle, ce qui a été à l'origine du projet *TiNum*.

Les enfants - mais pas seulement eux - prennent souvent des mots de passe fragiles car trop courts ou basés sur des éléments familiers. Ceci peut provenir d'une difficulté de mémorisation de mots de passe complexes ou plus éloignés de leur environnement immédiat. En mettant en avant l'idée de la construction d'un mot de passe basé sur un moyen mnémotechnique (en l'occurrence une histoire créée par l'enfant), *TiNum* vise à répondre à la question de la création de mots de passe plus robustes.

Pour le faire, l'activité comporte deux phases en classe. La première est une présentation des enjeux de la sécurité informatique d'une façon ludique et interactive. La seconde est la phase d'activité des élèves proprement dite.

A partir d'un mot de passe "simple", chaque enfant imagine une histoire dont il déduit un mot de passe plus robuste. L'histoire peut lui servir de moyen mnémotechnique.



# Hypothèses

Concernant l'expérience didactique proposée dans le cadre du projet *TiNum*, nous faisons les hypothèses suivantes:

## **Hypothèse Globale:**

Cette expérience peut fournir un point de départ pour accéder aux enjeux et aux défis du développement d'une citoyenneté numérique responsable, en développant leur capacité à produire un mot de passe robuste.

## **Hypothèse Spécifique:**

La technique du storytelling incluse dans cette expérience peut les aider à apprendre les règles à suivre pour construire un mot de passe robuste.





Au travers de cette expérimentation, nous souhaitons mesurer la compréhension des enfants des tâches à exécuter lors de l'activité ludique, ce qui permet de valider l'hypothèse spécifique, et la capacité des élèves à produire un mot de passe robuste, ce qui participe à la validation de l'hypothèse globale.

De manière plus détaillée, lors de la première phase de l'activité en classe, nous commençons par recueillir les connaissances préalables des participants de notre étude (élèves du CM1/CM2 en Guadeloupe) sur la sécurité informatique et, plus précisément, sur les mots de passe, sous forme de "post it". Puis, nous discutons devant le groupe-classe de leurs conceptions sur ce concept. Enfin, nous faisons exprimer aux élèves les stratégies qu'ils connaissent permettant de rendre un mot de passe (MdP) robuste, à partir de mots inducteurs fournis par l'expérimentateur. Cette expression est à nouveau recueillie sous forme de "post-it". Cette activité sert de base à co-construction des règles de construction, reprises des "Recommandations de sécurité relatives aux mots de passe" (2012) de l'Agence nationale de la sécurité des systèmes d'information.



## Méthodologie (2)

Lors de la deuxième phase, nous mettons en place des ateliers participatifs pour créer un mot de passe fort à partir d'une proposition initiale des élèves, en utilisant la technique ludique du storytelling. Nous recueillons les productions des élèves, à savoir les histoires qu'ils produisent et le mot de passe final proposé à partir de celles-ci.

Nous effectuons une analyse descriptive des "post-it" recueillis dans la première phase permettant d'identifier plus précisément les conceptions préalables des enfants sur les mots de passe et les stratégies qu'ils expriment relativement à la construction d'un mot de passe robuste. Concernant la deuxième phase, nous analysons le respect de la consigne (construire un mot de passe à partir d'éléments de l'histoire) et la robustesse du mot de passe produit.

Dans le cadre de cette étude, nous avons également recueilli des enregistrements audios dans lesquels les élèves racontent leurs histoires et s'expriment oralement devant leur classe. Un formulaire d'information et de consentement a été rempli en préalable par les parents/représentants légaux.

# Résultats (1)

Le projet *TiNum* s'est déroulé de novembre 2020 à mai 2021 et a concerné six classes de la Région académique de la Guadeloupe, en incluant des classes des îles de l'Archipel (La Désirade, Les Saintes).

Nous avons recueilli l'ensemble des données concernant ces six expérimentations. Leur exploitation a commencé et nous disposons d'une première analyse concernant les conceptions préalables des enfants relativement au mot de passe. Ces conceptions sont principalement en lien avec : 1) Les différentes formes de déverrouillage ; 2) Les appareils et les ressources numériques ; 3) Les éléments existants dans un mot de passe, comme des chiffres et lettres, soit des dates d'anniversaire, soit des combinaisons de lettres simples (comme "azerty") ; 4) Des éléments associées avec les notions de sécurité et de vie privée.

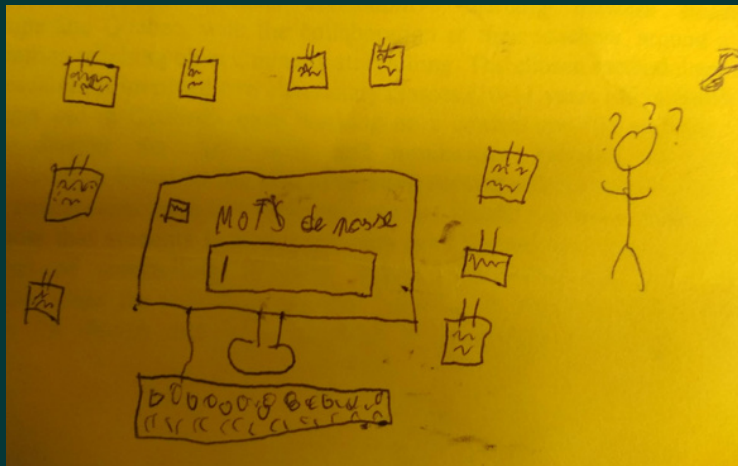
Cette expérimentation menée dans le cadre du primaire intéresse aussi des membres du collège (devant les enjeux de la sécurité informatique des adolescents).

Nous rappelons que certains résultats ont été mis en évidence lors de la première expérience menée en Guadeloupe (Chartofylaka et Delcroix, 2018). La majorité des enfants (91%) de la classe interrogée ont respecté les consignes pour construire un mot de passe en utilisant des mots provenant de leur histoire et en modifiant certains des composants conformément aux directives fournies pour produire un mot robuste. Nous avons, par ailleurs, identifié différentes appropriations et interprétations des consignes par les enfants (sept au total) pour effectuer la tâche demandée.



## Résultats (2)

La première expérimentation, menée en 2018 (Chartofylaka et Delcroix, 2018), a permis de produire une nouvelle version de l'activité, qui fait l'objet de l'expérimentation *TiNum*. Comme indiqué plus haut, nous débutons le traitement des données recueillies par l'analyse des représentations initiales des conceptions préalables des enfants relativement au mot de passe.



Dans le cadre de l'expérimentation initiale, nous avons analysé de manière plus fine les mots de passe proposés par les enfants en identifiant les règles (en référence aux critères ANSSI) qu'ils ont incorporées dans leurs mots de passe. Nous avons également relevé la longueur de leur mot de passe (80% des mots de passe créés contenaient au moins 12 caractères).

En menant le projet *TiNum*, nous souhaitons valider plus largement ces résultats préliminaires et répondre aux nouveaux objectifs de recherche que nous avons mentionnés ci-dessus. La réalisation d'autres analyses est conditionnée au traitement des données actuellement en cours.

# Apports de recherche (1)

Tout d'abord, l'inspiration initiale de cette expérimentation vient de travaux de recherche dans le domaine de la cryptographie, plus précisément sur la robustesse des mots de passe. L'idée du cassage de mot de passe (soit par des personnes qui connaissent des informations personnelles, soit par des attaques par force brute) semble un concept difficile à expliquer aux enfants. En faisant un revue de littérature sur cette thématique et l'apprentissage des enfants, nous avons constaté que les recherches existantes se focalisent plutôt sur leurs connaissances relatives aux protocoles et aux techniques d'authentification (Assal et al., 2016 ; Cole et al., 2017) ou à l'inclusion d'informations personnelles dans un mot de passe qui facilite leur mémorisation (Maqsood et al., 2018).

Par ailleurs, les bienfaits de l'utilisation du jeu dans les apprentissages des jeunes enfants sont connus et multiples. La technique du storytelling, au cœur de l'expérimentation, est perçue comme une méthode simple et efficace pour aborder des concepts plus complexes. De plus, la narration contribue au développement de compétences transversales chez les enfants, notamment liées à leur capacité à communiquer oralement ou à l'écrit.

Ces deux principaux éléments ont été à la base de la construction du scénario pédagogique interactif de *TiNum* qui vise à sensibiliser les enfants aux enjeux de la sécurité informatique d'une façon progressive, au travers d'une activité ludique.



## Apports de recherche (2)

Le contenu du scénario pédagogique a été enrichi par des sources sur les pratiques de mots de passe (par exemple le projet Richelieu (\*) concernant les mots de passe les plus courants, les recommandations de l'Agence Nationale de la Sécurité des Systèmes d'Information (2012) concernant la création d'un mot de passe fort en utilisant des différents groupes de caractères).

Le traitement et l'analyse des données recueillies, les retours d'expérience effectués auprès des acteurs impliqués permettront d'améliorer le protocole, d'envisager l'extension de l'expérimentation et de mettre à disposition un kit pédagogique.

(\*) La liste complète des mots de passe les plus fréquemment utilisés en France (2019) est consultable ici: <https://bit.ly/3cq7kq>

# Modalités de valorisation de la recherche

Outre le rapport pour le Groupement d'Intérêt Scientifique (GIS) "Jeu et sociétés", qui a assuré le financement du projet, un second rapport sera réalisé à destination de la Région académique de la Guadeloupe.

A ce jour, l'expérimentation a été déjà présentée dans les événements suivants :

- La Journée scientifique du laboratoire CRREF (Centre de Recherches et de Ressources en Éducation et Formation) - Université des Antilles, 10/12/2020 ;
- La Journée Académique de l'Innovation Guadeloupe 2021 - académie de la Guadeloupe, 28/4/2021 ;
- Le Colloque PRUNE II 2021 : Perspectives de Recherches sur les Usages du Numérique dans l'Éducation - Université de Poitiers, 7/5/2021.

De plus, un article court est accepté dans le cadre du projet "Children Online: Research and Evidence (CO:RE)" de l'Université de Tampere (Finlande) qui vise à produire un manuel sur les problèmes méthodologiques liés à la recherche sur les usages en ligne des enfants et des jeunes. D'autres publications sont en projet afin de valoriser cette expérience.



# Actions prévues

Une fois l'exploitation des données effectuée, la création d'un kit pédagogique prototype est envisagée permettant la diffusion de l'expérimentation dans un premier temps dans la Région académique de la Guadeloupe.



En synthèse, le projet *TiNum* semble avoir permis de développer chez les élèves participants les compétences numériques figurant parmi les objectifs des programmes scolaires. Plus particulièrement, il semble avoir développé des postures bienveillantes et responsables vis-à-vis de l'usage des médias, de l'information et plus généralement des outils numériques.



# Références

Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), France (2012). Recommandations de sécurité relatives aux mots de passe. Technical report

Assal, H., Imran, A., & Chiasson, S. (2016). An exploration of graphical password authentication for children. *International Journal of Child-Computer Interaction*, 18, 37-46.

Chartofylaka, L. & Delcroix, A. (2018). StoryPass – Password Rules Hidden in a Storytelling Game Activity: Steps towards Its Implementation. 8th International Toy Research Association World Conference

Cole, J., Walsh, G., & Pease, Z. (2017). Click to Enter. Proceedings of the 2017 Conference on Interaction Design and Children. IDC '17.

Maqsood, S., Biddle, R., Maqsood, S., & Chiasson, S. (2018):. An exploratory study of children's online password behaviors. Proceedings of the 17th ACM Conference on Interaction Design and Children. IDC '18.



**LAMPRINI CHARTO FYLAKA**

**lamprini.chartofylaka@gmail.com**