2040

LOGO1

LOGO2

THESIS / MY BELOVED UNIVERSITY
university subtitle

Requirement for the degree of
DOCTOR OF PHILOSOPHY OF X UNIVERSITY

Computer Science Department

by

John Doe

prepared in Nashville, Calizona

The title of your thesis on several lines ... many lines ...

Thesis defended in Nashville on February, 30th 2040

Jury :

Alice ABSOLUTIST
University 1 / reviewer

Bob BROWN
University 2 / reviewer

Charlie COURAGEOUS
University 3 / some dude

Eve EVIL
University 4 / examiner

Jane SMITH
X UNIVERSITY / PhD Advisor

An amazing PhD topic

Great things you did

John DOE

Supervisors : Jane SMITH

Remerciements

Merci, Merci !

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula.

Fusce mauris. Vestibulum luctus nibh at lectus. Sed bibendum, nulla a faucibus semper,

leo velit ultricies tellus, ac venenatis arcu wisi vel nisl. Vestibulum diam. Aliquam pellentesque, augue quis sagittis posuere, turpis lacus congue quam, in hendrerit risus eros eget felis. Maecenas eget erat in sapien mattis porttitor. Vestibulum porttitor. Nulla facilisi. Sed a turpis eu lacus commodo facilisis. Morbi fringilla, wisi in dignissim interdum, justo lectus sagittis dui, et vehicula libero dui cursus dui. Mauris tempor ligula sed lacus. Duis cursus enim ut augue. Cras ac magna. Cras nulla. Nulla egestas. Curabitur a leo. Quisque egestas wisi eget nunc. Nam feugiat lacus vel est. Curabitur consectetuer.

Suspendisse vel felis. Ut lorem lorem, interdum eu, tincidunt sit amet, laoreet vitae, arcu. Aenean faucibus pede eu ante. Praesent enim elit, rutrum at, molestie non, nonummy vel, nisl. Ut lectus eros, malesuada sit amet, fermentum eu, sodales cursus, magna. Donec eu purus. Quisque vehicula, urna sed ultricies auctor, pede lorem egestas dui, et convallis elit erat sed nulla. Donec luctus. Curabitur et nunc. Aliquam dolor odio, commodo pretium, ultricies non, pharetra in, velit. Integer arcu est, nonummy in, fermentum faucibus, egestas vel, odio.

Sed commodo posuere pede. Mauris ut est. Ut quis purus. Sed ac odio. Sed vehicula hendrerit sem. Duis non odio. Morbi ut dui. Sed accumsan risus eget odio. In hac habitasse platea dictumst. Pellentesque non elit. Fusce sed justo eu urna porta tincidunt. Mauris felis odio, sollicitudin sed, volutpat a, ornare ac, erat. Morbi quis dolor. Donec pellentesque, erat ac sagittis semper, nunc dui lobortis purus, quis congue purus metus ultricies tellus. Proin et quam. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Praesent sapien turpis, fermentum vel, eleifend faucibus, vehicula eu, lacus.

Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Donec odio elit, dictum in, hendrerit sit amet, egestas sed, leo. Praesent feugiat sapien aliquet odio. Integer vitae justo. Aliquam vestibulum fringilla lorem. Sed neque lectus, consectetuer at, consectetuer sed, eleifend ac, lectus. Nulla facilisi. Pellentesque eget lectus. Proin eu metus. Sed porttitor. In hac habitasse platea dictumst. Suspendisse eu lectus. Ut mi mi, lacinia sit amet, placerat et, mollis vitae, dui. Sed ante tellus, tristique ut, iaculis eu, malesuada ac, dui. Mauris nibh leo, facilisis non, adipiscing quis, ultrices a, dui.

Résumé en Français

Le résumé en Français est probablement la partie de la thèse la plus fastidieuse à écrire. C'est chiant, et tout le monde s'en tamponne ...

Sommaire

Première Section

Première Sous-section

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula.

Problématique du chiffrement de base de données

Fusce mauris. Vestibulum luctus nibh at lectus. Sed bibendum, nulla a faucibus semper, leo velit ultricies tellus, ac venenatis arcu wisi vel nisl. Vestibulum diam. Aliquam pellentesque, augue quis sagittis posuere, turpis lacus congue quam, in hendrerit risus eros eget felis. Maecenas eget erat in sapien mattis porttitor. Vestibulum porttitor. Nulla facilisi. Sed a turpis eu lacus commodo facilisis. Morbi fringilla, wisi in dignissim interdum, justo lectus sagittis dui, et vehicula libero dui cursus dui. Mauris tempor ligula sed lacus. Duis cursus enim ut augue. Cras ac magna. Cras nulla. Nulla egestas. Curabitur a leo. Quisque egestas wisi eget nunc. Nam feugiat lacus vel est. Curabitur consectetuer.

Suspendisse vel felis. Ut lorem lorem, interdum eu, tincidunt sit amet, laoreet vitae, arcu. Aenean faucibus pede eu ante. Praesent enim elit, rutrum at, molestie non, nonummy vel, nisl. Ut lectus eros, malesuada sit amet, fermentum eu, sodales cursus, magna. Donec eu purus. Quisque vehicula, urna sed ultricies auctor, pede lorem egestas dui, et convallis elit erat sed nulla. Donec luctus. Curabitur et nunc. Aliquam dolor odio, commodo pretium, ultricies non, pharetra in, velit. Integer arcu est, nonummy in, fermentum faucibus, egestas vel, odio.

Sed commodo posuere pede. Mauris ut est. Ut quis purus. Sed ac odio. Sed vehicula hendrerit sem. Duis non odio. Morbi ut dui. Sed accumsan risus eget odio. In hac habitasse platea dictumst. Pellentesque non elit. Fusce sed justo eu urna porta tincidunt. Mauris felis odio, sollicitudin sed, volutpat a, ornare ac, erat. Morbi quis dolor. Donec pellentesque, erat ac sagittis semper, nunc dui lobortis purus, quis congue purus metus ultricies tellus. Proin et quam. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Praesent sapien turpis, fermentum vel, eleifend faucibus, vehicula eu, lacus.

Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Donec odio elit, dictum in, hendrerit sit amet, egestas sed, leo. Praesent feugiat sapien aliquet odio. Integer vitae justo. Aliquam vestibulum fringilla lorem. Sed neque lectus, consectetuer at, consectetuer sed, eleifend ac, lectus. Nulla facilisi. Pellentesque eget lectus. Proin eu metus. Sed porttitor. In hac habitasse platea dictumst. Suspendisse eu lectus. Ut mi mi, lacinia sit amet, placerat et, mollis vitae, dui. Sed ante tellus, tristique ut, iaculis eu, malesuada ac, dui. Mauris nibh leo, facilisis non, adipiscing quis, ultrices a, dui.

Mes contributions

Il n'y a pas de doutes, ce que j'ai fait pendant ma thèse était TROP bien.

Premier Aspect

Morbi luctus, wisi viverra faucibus pretium, nibh est placerat odio, nec commodo wisi enim eget quam. Quisque libero justo, consectetuer a, feugiat vitae, porttitor eu, libero. Suspendisse sed mauris vitae elit sollicitudin malesuada. Maecenas ultricies eros sit amet ante. Ut venenatis velit. Maecenas sed mi eget dui varius euismod. Phasellus aliquet volutpat odio. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae ; Pellentesque sit amet pede ac sem eleifend consectetuer. Nullam elementum, urna vel imperdiet sodales, elit ipsum pharetra ligula, ac pretium ante justo a nulla. Curabitur tristique arcu eu metus. Vestibulum lectus. Proin mauris. Proin eu nunc eu urna hendrerit faucibus. Aliquam auctor, pede consequat laoreet varius, eros tellus scelerisque quam, pellentesque hendrerit ipsum dolor sed augue. Nulla nec lacus.

Suspendisse vitae elit. Aliquam arcu neque, ornare in, ullamcorper quis, commodo eu, libero. Fusce sagittis erat at erat tristique mollis. Maecenas sapien libero, molestie et, lobortis in, sodales eget, dui. Morbi ultrices rutrum lorem. Nam elementum ullamcorper leo. Morbi dui. Aliquam sagittis. Nunc placerat. Pellentesque tristique sodales est. Maecenas imperdiet lacinia velit. Cras non urna. Morbi eros pede, suscipit ac, varius vel, egestas non, eros. Praesent malesuada, diam id pretium elementum, eros sem dictum tortor, vel consectetuer odio sem sed wisi.

Sed feugiat. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Ut pellentesque augue sed urna. Vestibulum diam eros, fringilla et, consectetuer eu, nonummy id, sapien. Nullam at lectus. In sagittis ultrices mauris. Curabitur malesuada erat sit amet massa. Fusce blandit. Aliquam erat volutpat. Aliquam euismod. Aenean vel lectus. Nunc imperdiet justo nec dolor.

Second Aspect

Etiam euismod. Fusce facilisis lacinia dui. Suspendisse potenti. In mi erat, cursus id, nonummy sed, ullamcorper eget, sapien. Praesent pretium, magna in eleifend egestas, pede pede pretium lorem, quis consectetuer tortor sapien facilisis magna. Mauris quis magna varius nulla scelerisque imperdiet. Aliquam non quam. Aliquam porttitor quam a lacus. Praesent vel arcu ut tortor cursus volutpat. In vitae pede quis diam bibendum placerat. Fusce elementum convallis neque. Sed dolor orci, scelerisque ac, dapibus nec, ultricies ut, mi. Duis nec dui quis leo sagittis commodo.

Aliquam lectus. Vivamus leo. Quisque ornare tellus ullamcorper nulla. Mauris porttitor pharetra tortor. Sed fringilla justo sed mauris. Mauris tellus. Sed non leo. Nullam elementum, magna in cursus sodales, augue est scelerisque sapien, venenatis congue nulla arcu et pede. Ut suscipit enim vel sapien. Donec congue. Maecenas urna mi, suscipit in, placerat ut, vestibulum ut, massa. Fusce ultrices nulla et nisl.

Etiam ac leo a risus tristique nonummy. Donec dignissim tincidunt nulla. Vestibulum rhoncus molestie odio. Sed lobortis, justo et pretium lobortis, mauris turpis condimentum augue, nec ultricies nibh arcu pretium enim. Nunc purus neque, placerat id, imperdiet sed, pellentesque nec, nisl. Vestibulum imperdiet neque non sem accumsan laoreet. In hac habitasse platea dictumst. Etiam condimentum facilisis libero. Suspendisse in elit quis nisl aliquam dapibus. Pellentesque auctor sapien. Sed egestas sapien nec lectus. Pellentesque vel dui vel neque bibendum viverra. Aliquam porttitor nisl nec pede. Proin mattis libero vel turpis. Donec rutrum mauris et libero. Proin euismod porta felis. Nam lobortis, metus quis elementum commodo, nunc lectus elementum mauris, eget vulputate ligula tellus eu neque. Vivamus eu dolor.

Nulla in ipsum. Praesent eros nulla, congue vitae, euismod ut, commodo a, wisi. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Aenean nonummy magna non leo. Sed felis erat, ullamcorper in, dictum non, ultricies ut, lectus. Proin vel arcu a odio lobortis euismod. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae ; Proin ut est. Aliquam odio. Pellentesque massa turpis, cursus eu, euismod nec, tempor congue, nulla. Duis viverra gravida mauris. Cras tincidunt. Curabitur eros ligula, varius ut, pulvinar in, cursus faucibus, augue.

Table des matières

Call me Ishmael

Moby-Dick – Herman Melville

Introduction 1

THIS THESIS TOOK WAY TO MUCH TIME OF YOUR LIFE, try to make people believe that what you did was actually useful by writing a great introduction. Not easy, but important. Probably one of the most annoying part of writing your manuscript.

Contents

1.1 La cryptographie

Dans son Dictionnaire de la langue française, Émile Littré définissait la cryptographie comme l'art « d'écrire en caractères secrets qui sont ou de convention ou le résultat d'une transposition des lettres de l'alphabet[1] ». Il est vrai qu'en général, en cette seconde moitié du xix^e^ siècle, pour rendre un message inintelligible au cas où celui-ci, confidentiel, viendrait à être intercepté, on écrivait un caractère pour un autre, ou on remplaçait une suite de lettres par une autre (par exemple, selon une substitution dite polyalphabétique) ; la cryptographie était alors, pour ainsi dire, balbutiante. Pourtant, à cette époque déjà, dans ses Recherches arithmétiques[2], Carl Friedrich Gauss avait jeté les bases de la théorie des nombres moderne, et Évariste Galois, dans son fameux mémoire[3] — publié après sa mort par le mathématicien Joseph Liouville —, celles de la théorie qui portera son nom.

La constatation de l'insuffisante valeur de la cryptographie du xix^e^ siècle se retrouve dans l'article en deux parties d'Auguste Kerckhoffs, paru en 1883, intitulé La cryptographie militaire[4], où le cryptographe s'étonne de voir savants et professeurs « enseigner et recommander pour les usages de la guerre des systèmes dont un déchiffreur tant soit peu expérimenté trouverait certainement la clef en moins d'une heure de temps » ; l'auteur ne voit guère d'explication à cet « excès de confiance dans certains chiffres » que par « l'abandon dans lequel la suppression des cabinets noirs et la sécurité des relations postales ont fait tomber les études cryptographiques ».

Ce n'est qu'au siècle suivant, sous l'impulsion, notamment, des grands conflits qui l'ont déchiré, qu'on vit la cryptographie tirer réellement parti des outils de la mathématique moderne et muer en une science complexe, si bien que dans le dernier tiers de ce xx^e^ siècle apparut une nouvelle sorte de cryptographie, qu'on dit asymétrique par opposition à la cryptographie symétrique, son pendant plus ancien.

Jusqu'alors, en effet, pour établir une communication chiffrée, il fallait que les correspondants convinssent au préalable d'une règle secrète de chiffrement qui fixât notamment les caractéristiques du système propres à cette communication dès lors qu'elles étaient à connaître pour réaliser la transformation du texte d'origine, le clair. Avec cette configuration, tout chiffré produit par l'un des correspondants aurait pu l'avoir été par un autre d'entre eux s'il avait eu connaissance du clair ; en outre, tout chiffré produit par l'un des correspondant pouvait être déchiffré naturellement par un autre, sans même qu'il ait été convenu d'une méthode de déchiffrement, simplement par l'application d'un procédé inverse à celui employé pour chiffrer. Par exemple, deux personnes pouvaient convenir qu'à chacune des lettres d'un clair qu'ils souhaiteraient transmettre serait substituée une autre lettre de l'alphabet selon une table de correspondance définit à l'avance : qu'ainsi le C se verrait, en chacune de ses occurences, remplacer par un G, que le E serait remplacé par un S, le F par un M, le H par un C, et ainsi de suite, le mot « CHEF » devenant alors en « GCSM », suite de lettres que les deux personnes serait en mesure non seulement de pro-

[1] Dictionnaire de la langue française, dÉmile Littré, édition de 1873, tome premier, page 922, entrée CRYPTOGRAPHIE.

[2]

[3]

[4]

duire mais de déchiffrer aisément en appliquant la table de substitution dans le sens inverse. La correspondance entre les lettres du clair et du chiffré est dans cet exemple l'information qui doit rester secrète pour que le chiffrement le demeure aussi.

L'information secrète — il en faut une — sur lequel se fonde le chiffrement peut être de deux natures : soit elle correspond au système de chiffrement lui-même, et la sécurité de la communication repose alors sur la méconnaissance par l'adversaire du système employé, soit elle se réduit à un petit ensemble de paramètres du système, appelé clef, et la connaissance de la méthode générale de chiffrement employée est alors supposée ne pas compromettre le système. De ces deux approches du chiffrement, la première a fini par être largement rejetée par les cryptographes. L'article de Kerckhoffs exprimait déjà, au deuxième chef d'une liste de six « desiderata de la cryptographie militaire », la nécessité que le système « n'exige pas le secret et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi ». Par secret, Kerckhoffs entend « non la clef proprement dite, mais ce qui constitue la partie matérielle du système » — ce qui correspondrait, à l'ère numérique, à l'algorithme de chiffrement — car, explique-t-il, « il n'est pas nécessaire de se créer des fantômes imaginaires et de mettre en suspicion l'incorruptibilité des employés ou agents subalternes, pour comprendre que, si un système exigeant le secret se trouvait entre les mains d'un trop grand nombre d'individus, il pourrait être compromis à chaque engagement auquel l'un ou l'autre d'entre eux prendrait part ». Ce desideratum de la cryptographie militaire est ce qui est maintenant connu sous le nom de principe de Kerckhoffs ; il s'applique tout aussi bien en dehors du domaine militaire. À l'époque actuelle, il est en outre considéré comme entendu que le fait qu'un système de chiffrement soit connaissable du monde entier, et donc largement susceptible d'être étudié et mis à l'épreuve par les spécialistes, et qu'aucune faille critique ne se fasse connaître malgré cela, tend à être gage de sa bonne qualité.

Prenons en exemple le système AES[5], qui est le système de chiffrement symétrique par bloc (c'est-à-dire traitant les données à chiffrer bloc par bloc) recommandé par l'ANSSI[6]. Ce système résulte d'un concours public du NIST[7] dont l'ambition affichée était de choisir un algorithme de chiffrement, dans plusieurs déclinaisons déterminées précisément pour que le système fût à la fois robuste et efficace, d'en faire une norme dont les spécifications[8] fussent accessibles à tous, et d'en permettre un usage non dissimulé comme celui qu'en fait par exemple l'environnement de messagerie Signal[9], dont le code-source est ouvert. De ce concours du NIST est sorti gagnant l'algorithme de Rijndael dans trois déclinaisons spécifiques correspondant à trois tailles de clef différentes : 128, 192 et 256 bits. Le libre accès aux spécifications du système AES a permis la réalisation d'analyses précises de celui-ci par le monde de la recherche et la publication de méthodes d'attaques qui, bien que de nature à le fragiliser un peu en certains aspects, ne se sont pas montrées suffisamment puissantes pour le rendre caduc. Notons cependant qu'il apparaît, au nombre des révélations dont fut

[5] Le sigle AES correspond à ńadvanced encryption standardż, littéralement ńnorme de chiffrement avancéż.
[6] LANSSI est lAgence nationale de la sécurité des systèmes dinformation, en France.
[7] Le NIST est lInstitut national des normes et de la technologie des États-Unis.
[8] https ://csrc.nist.gov/csrc/media/publications/fips/197/final/documents/fips-197.pdf
[9] https ://signal.org/docs/specifications/doubleratchet/doubleratchet.pdf

à l'orgine Edward Snowden, que la NSA[10], tout en recommandant l'utilisation d'AES, s'est employée à essayer de trouver des attaques sur ce système ; il ne semble pas déraisonnable de penser qu'un tel organisme de renseignement pourrait garder pour lui toute trouvaille offensive déterminante dans un système de chiffrement à spécifications publiques.

Pour que des systèmes informatiques, directement liés à des êtres humains ou non, puissent employer un système de chiffrement symétrique tel qu'AES, il est nécessaire comme nous l'avons dit, qu'ils aient en commun une clef. Or, si ces systèmes sont distants et sont supposés communiquer de façon sécurisé pour la première fois comment faire en sorte qu'ils puissent convenir d'une clef qui doit être secrète et le rester longtemps ?

C'est ce que permet la cryptographie asymétrique.

Cryptographie asymétrique, définition, utilité.

Problèmes difficiles de la cryptographie asymétriques, logarithme discret, factorisation.

Autres avantages de la cryptographie asymétrique.

Définition complète de la cryptographie.

1.2 History of the Topic

You were probably not the first one to work on this subject. It is time to say what did other people do.

1.2.1 Aspect 1

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet,

[10] National Security Agency, ń Agence nationale de la sécurité ż aux États-Unis.

tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula.

Fusce mauris. Vestibulum luctus nibh at lectus. Sed bibendum, nulla a faucibus semper, leo velit ultricies tellus, ac venenatis arcu wisi vel nisl. Vestibulum diam. Aliquam pellentesque, augue quis sagittis posuere, turpis lacus congue quam, in hendrerit risus eros eget felis. Maecenas eget erat in sapien mattis porttitor. Vestibulum porttitor. Nulla facilisi. Sed a turpis eu lacus commodo facilisis. Morbi fringilla, wisi in dignissim interdum, justo lectus sagittis dui, et vehicula libero dui cursus dui. Mauris tempor ligula sed lacus. Duis cursus enim ut augue. Cras ac magna. Cras nulla. Nulla egestas. Curabitur a leo. Quisque egestas wisi eget nunc. Nam feugiat lacus vel est. Curabitur consectetuer.

Suspendisse vel felis. Ut lorem lorem, interdum eu, tincidunt sit amet, laoreet vitae, arcu. Aenean faucibus pede eu ante. Praesent enim elit, rutrum at, molestie non, nonummy vel, nisl. Ut lectus eros, malesuada sit amet, fermentum eu, sodales cursus, magna. Donec eu purus. Quisque vehicula, urna sed ultricies auctor, pede lorem egestas dui, et convallis elit erat sed nulla. Donec luctus. Curabitur et nunc. Aliquam dolor odio, commodo pretium, ultricies non, pharetra in, velit. Integer arcu est, nonummy in, fermentum faucibus, egestas vel, odio.

Sed commodo posuere pede. Mauris ut est. Ut quis purus. Sed ac odio. Sed vehicula hendrerit sem. Duis non odio. Morbi ut dui. Sed accumsan risus eget odio. In hac habitasse platea dictumst. Pellentesque non elit. Fusce sed justo eu urna porta tincidunt. Mauris felis odio, sollicitudin sed, volutpat a, ornare ac, erat. Morbi quis dolor. Donec pellentesque, erat ac sagittis semper, nunc dui lobortis purus, quis congue purus metus ultricies tellus. Proin et quam. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Praesent sapien turpis, fermentum vel, eleifend faucibus, vehicula eu, lacus.

Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Donec odio elit, dictum in, hendrerit sit amet, egestas sed, leo. Praesent feugiat sapien aliquet odio. Integer vitae justo. Aliquam vestibulum fringilla lorem. Sed neque lectus, consectetuer at, consectetuer sed, eleifend ac, lectus. Nulla facilisi. Pellentesque eget lectus. Proin eu metus. Sed porttitor. In hac habitasse platea dictumst. Suspendisse eu lectus. Ut mi mi, lacinia sit amet, placerat et, mollis vitae, dui. Sed ante tellus, tristique ut, iaculis eu, malesuada ac, dui. Mauris nibh leo, facilisis non, adipiscing quis, ultrices a, dui.

Morbi luctus, wisi viverra faucibus pretium, nibh est placerat odio, nec commodo wisi enim eget quam. Quisque libero justo, consectetuer a, feugiat vitae, porttitor eu, libero. Suspendisse sed mauris vitae elit sollicitudin malesuada. Maecenas ultricies eros sit amet ante. Ut venenatis velit. Maecenas sed mi eget dui varius euismod. Phasellus aliquet volutpat odio. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae ; Pellentesque sit amet pede ac sem eleifend consectetuer. Nullam elementum, urna vel imperdiet sodales, elit ipsum pharetra ligula, ac pretium ante justo a nulla. Curabitur tristique arcu eu metus. Vestibulum lectus. Proin mauris. Proin eu nunc eu urna hendrerit faucibus. Aliquam auctor, pede consequat laoreet varius, eros tellus scelerisque quam, pellentesque hendrerit ipsum dolor sed augue. Nulla nec lacus.

1.2.2 Aspect 2

Suspendisse vitae elit. Aliquam arcu neque, ornare in, ullamcorper quis, commodo eu, libero. Fusce sagittis erat at erat tristique mollis. Maecenas sapien libero, molestie et, lobortis in, sodales eget, dui. Morbi ultrices rutrum lorem. Nam elementum ullamcorper leo. Morbi dui. Aliquam sagittis. Nunc placerat. Pellentesque tristique sodales est. Maecenas imperdiet lacinia velit. Cras non urna. Morbi eros pede, suscipit ac, varius vel, egestas non, eros. Praesent malesuada, diam id pretium elementum, eros sem dictum tortor, vel consectetuer odio sem sed wisi.

Sed feugiat. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Ut pellentesque augue sed urna. Vestibulum diam eros, fringilla et, consectetuer eu, nonummy id, sapien. Nullam at lectus. In sagittis ultrices mauris. Curabitur malesuada erat sit amet massa. Fusce blandit. Aliquam erat volutpat. Aliquam euismod. Aenean vel lectus. Nunc imperdiet justo nec dolor.

Etiam euismod. Fusce facilisis lacinia dui. Suspendisse potenti. In mi erat, cursus id, nonummy sed, ullamcorper eget, sapien. Praesent pretium, magna in eleifend egestas, pede pede pretium lorem, quis consectetuer tortor sapien facilisis magna. Mauris quis magna varius nulla scelerisque imperdiet. Aliquam non quam. Aliquam porttitor quam a lacus. Praesent vel arcu ut tortor cursus volutpat. In vitae pede quis diam bibendum placerat. Fusce elementum convallis neque. Sed dolor orci, scelerisque ac, dapibus nec, ultricies ut, mi. Duis nec dui quis leo sagittis commodo.

Aliquam lectus. Vivamus leo. Quisque ornare tellus ullamcorper nulla. Mauris porttitor pharetra tortor. Sed fringilla justo sed mauris. Mauris tellus. Sed non leo. Nullam elementum, magna in cursus sodales, augue est scelerisque sapien, venenatis congue nulla arcu et pede. Ut suscipit enim vel sapien. Donec congue. Maecenas urna mi, suscipit in, placerat ut, vestibulum ut, massa. Fusce ultrices nulla et nisl.

Etiam ac leo a risus tristique nonummy. Donec dignissim tincidunt nulla. Vestibulum rhoncus molestie odio. Sed lobortis, justo et pretium lobortis, mauris turpis condimentum augue, nec ultricies nibh arcu pretium enim. Nunc purus neque, placerat id, imperdiet sed, pellentesque nec, nisl. Vestibulum imperdiet neque non sem accumsan laoreet. In hac habitasse platea dictumst. Etiam condimentum facilisis libero. Suspendisse in elit quis nisl aliquam dapibus. Pellentesque auctor sapien. Sed egestas sapien nec lectus. Pellentesque vel dui vel neque bibendum viverra. Aliquam porttitor nisl nec pede. Proin mattis libero vel turpis. Donec rutrum mauris et libero. Proin euismod porta felis. Nam lobortis, metus quis elementum commodo, nunc lectus elementum mauris, eget vulputate ligula tellus eu neque. Vivamus eu dolor.

Nulla in ipsum. Praesent eros nulla, congue vitae, euismod ut, commodo a, wisi. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Aenean nonummy magna non leo. Sed felis erat, ullamcorper in, dictum non, ultricies ut, lectus. Proin vel arcu a odio lobortis euismod. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae ; Proin ut est. Aliquam odio. Pellentesque massa turpis, cursus eu, euismod nec, tempor congue, nulla. Duis viverra gravida mauris. Cras tincidunt. Curabitur eros ligula, varius ut, pulvinar in, cursus faucibus, augue.

Nulla mattis luctus nulla. Duis commodo velit at leo. Aliquam vulputate magna et leo. Nam vestibulum ullamcorper leo. Vestibulum condimentum rutrum mauris. Donec id mauris. Morbi molestie justo et pede. Vivamus eget turpis sed nisl cursus tempor. Curabitur mollis sapien condimentum nunc. In wisi nisl, malesuada at, dignissim sit amet, lobortis in, odio. Aenean consequat arcu a ante. Pellentesque porta elit sit amet orci. Etiam at turpis nec elit ultricies imperdiet. Nulla facilisi. In hac habitasse platea dictumst. Suspendisse viverra aliquam risus. Nullam pede justo, molestie nonummy, scelerisque eu, facilisis vel, arcu.

Curabitur tellus magna, porttitor a, commodo a, commodo in, tortor. Donec interdum. Praesent scelerisque. Maecenas posuere sodales odio. Vivamus metus lacus, varius quis, imperdiet quis, rhoncus a, turpis. Etiam ligula arcu, elementum a, venenatis quis, sollicitudin sed, metus. Donec nunc pede, tincidunt in, venenatis vitae, faucibus vel, nibh. Pellentesque wisi. Nullam malesuada. Morbi ut tellus ut pede tincidunt porta. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam congue neque id dolor.

Donec et nisl at wisi luctus bibendum. Nam interdum tellus ac libero. Sed sem justo, laoreet vitae, fringilla at, adipiscing ut, nibh. Maecenas non sem quis tortor eleifend fermentum. Etiam id tortor ac mauris porta vulputate. Integer porta neque vitae massa. Maecenas tempus libero a libero posuere dictum. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae ; Aenean quis mauris sed elit commodo placerat. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Vivamus rhoncus tincidunt libero. Etiam elementum pretium justo. Vivamus est. Morbi a tellus eget pede tristique commodo. Nulla nisl. Vestibulum sed nisl eu sapien cursus rutrum.

Nulla non mauris vitae wisi posuere convallis. Sed eu nulla nec eros scelerisque pharetra. Nullam varius. Etiam dignissim elementum metus. Vestibulum faucibus, metus sit amet mattis rhoncus, sapien dui laoreet odio, nec ultricies nibh augue a enim. Fusce in ligula. Quisque at magna et nulla commodo consequat. Proin accumsan imperdiet sem. Nunc porta. Donec feugiat mi at justo. Phasellus facilisis ipsum quis ante. In ac elit eget ipsum pharetra faucibus. Maecenas viverra nulla in massa.

1.2.3 Aspect 3

Nulla ac nisl. Nullam urna nulla, ullamcorper in, interdum sit amet, gravida ut, risus. Aenean ac enim. In luctus. Phasellus eu quam vitae turpis viverra pellentesque. Duis feugiat felis ut enim. Phasellus pharetra, sem id porttitor sodales, magna nunc aliquet nibh, nec blandit nisl mauris at pede. Suspendisse risus risus, lobortis eget, semper at, imperdiet sit amet, quam. Quisque scelerisque dapibus nibh. Nam enim. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Nunc ut metus. Ut metus justo, auctor at, ultrices eu, sagittis ut, purus. Aliquam aliquam.

Etiam pede massa, dapibus vitae, rhoncus in, placerat posuere, odio. Vestibulum luctus commodo lacus. Morbi lacus dui, tempor sed, euismod eget, condimentum at, tortor. Phasellus aliquet odio ac lacus tempor faucibus. Praesent sed sem. Praesent iaculis. Cras rhoncus tellus sed justo ullamcorper sagittis. Donec quis orci. Sed ut tortor quis tellus euismod tincidunt. Suspendisse congue nisl eu elit. Aliquam tortor diam, tempus id, tristique eget, sodales vel, nulla. Praesent tellus mi, condimentum sed, viverra at, consectetuer quis, lectus. In auctor vehicula orci. Sed pede sapien, euismod in, suscipit in, pharetra placerat, metus. Vivamus commodo dui non odio. Donec et felis.

Etiam suscipit aliquam arcu. Aliquam sit amet est ac purus bibendum congue. Sed in eros. Morbi non orci. Pellentesque mattis lacinia elit. Fusce molestie velit in ligula. Nullam et orci vitae nibh vulputate auctor. Aliquam eget purus. Nulla auctor wisi sed ipsum. Morbi porttitor tellus ac enim. Fusce ornare. Proin ipsum enim, tincidunt in, ornare venenatis, molestie a, augue. Donec vel pede in lacus sagittis porta. Sed hendrerit ipsum quis nisl. Suspendisse quis massa ac nibh pretium cursus. Sed sodales. Nam eu neque quis pede dignissim ornare. Maecenas eu purus ac urna tincidunt congue.

Donec et nisl id sapien blandit mattis. Aenean dictum odio sit amet risus. Morbi purus. Nulla a est sit amet purus venenatis iaculis. Vivamus viverra purus vel magna. Donec in justo sed odio malesuada dapibus. Nunc ultrices aliquam nunc. Vivamus facilisis pellentesque velit. Nulla nunc velit, vulputate dapibus, vulputate id, mattis ac, justo. Nam mattis elit dapibus purus. Quisque enim risus, congue non, elementum ut, mattis quis, sem. Quisque elit.

Maecenas non massa. Vestibulum pharetra nulla at lorem. Duis quis quam id lacus dapibus interdum. Nulla lorem. Donec ut ante quis dolor bibendum condimentum. Etiam egestas tortor vitae lacus. Praesent cursus. Mauris bibendum pede at elit. Morbi et felis a lectus interdum facilisis. Sed suscipit gravida turpis. Nulla at lectus. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae ; Praesent nonummy luctus nibh. Proin turpis nunc, congue eu, egestas ut, fringilla at, tellus. In hac habitasse platea dictumst.

Vivamus eu tellus sed tellus consequat suscipit. Nam orci orci, malesuada id, gravida nec, ultricies vitae, erat. Donec risus turpis, luctus sit amet, interdum quis, porta sed, ipsum. Suspendisse condimentum, tortor at egestas posuere, neque metus tempor orci, et tincidunt urna nunc a purus. Sed facilisis blandit tellus. Nunc risus sem, suscipit nec, eleifend quis, cursus quis, libero. Curabitur et dolor. Sed vitae sem. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Maecenas ante. Duis ullamcorper enim. Donec tristique enim eu leo. Nullam molestie elit eu dolor. Nullam bibendum, turpis vitae tristique gravida, quam sapien tempor lectus, quis pretium tellus purus ac quam. Nulla facilisi.

Duis aliquet dui in est. Donec eget est. Nunc lectus odio, varius at, fermentum in, accumsan non, enim. Aliquam erat volutpat. Proin sit amet nulla ut eros consectetuer cursus. Phasellus dapibus aliquam justo. Nunc laoreet. Donec consequat placerat magna. Duis pretium tincidunt justo. Sed sollicitudin vestibulum quam. Nam quis ligula. Vivamus at metus. Etiam imperdiet imperdiet pede. Aenean turpis. Fusce augue velit, scelerisque sollicitudin, dictum vitae, tempor et, pede. Donec wisi sapien, feugiat in, fermentum ut, sollicitudin adipiscing, metus.

Donec vel nibh ut felis consectetuer laoreet. Donec pede. Sed id quam id wisi laoreet suscipit. Nulla lectus dolor, aliquam ac, fringilla eget, mollis ut, orci. In pellentesque justo in ligula. Maecenas turpis. Donec eleifend leo at felis tincidunt consequat. Aenean turpis metus, malesuada sed, condimentum sit amet, auctor a, wisi. Pellentesque sapien elit, bibendum ac, posuere et, congue eu, felis. Vestibulum mattis libero quis metus scelerisque ultrices. Sed purus.

Donec molestie, magna ut luctus ultrices, tellus arcu nonummy velit, sit amet pulvinar elit justo et mauris. In pede. Maecenas euismod elit eu erat. Aliquam augue wisi, facilisis congue, suscipit in, adipiscing et, ante. In justo. Cras lobortis neque ac ipsum. Nunc fermentum massa at ante. Donec orci tortor, egestas sit amet, ultrices eget, venenatis eget, mi. Maecenas vehicula leo semper est. Mauris vel metus. Aliquam erat volutpat. In rhoncus sapien ac tellus. Pellentesque ligula.

Cras dapibus, augue quis scelerisque ultricies, felis dolor placerat sem, id porta velit odio eu elit. Aenean interdum nibh sed wisi. Praesent sollicitudin vulputate dui. Praesent iaculis viverra augue. Quisque in libero. Aenean gravida lorem vitae sem ullamcorper cursus. Nunc adipiscing rutrum ante. Nunc ipsum massa, faucibus sit amet, viverra vel, elementum semper, orci. Cras eros sem, vulputate et, tincidunt id, ultrices eget, magna. Nulla varius ornare odio. Donec accumsan mauris sit amet augue. Sed ligula lacus, laoreet non, aliquam sit amet, iaculis tempor, lorem. Suspendisse eros. Nam porta, leo sed congue tempor, felis est ultrices eros, id mattis velit felis non metus. Curabitur vitae elit non mauris varius pretium. Aenean lacus sem, tincidunt ut, consequat quis, porta vitae, turpis. Nullam laoreet fermentum urna. Proin iaculis lectus.

1.3 Contributions of this Thesis

Now, it is your turn. You can describe your papers one by one.

1.3.1 First Paper [Doe36]

Sed mattis, erat sit amet gravida malesuada, elit augue egestas diam, tempus scelerisque nunc nisl vitae libero. Sed consequat feugiat massa. Nunc porta, eros in eleifend varius, erat leo rutrum dui, non convallis lectus orci ut nibh. Sed lorem massa, nonummy quis, egestas id, condimentum at, nisl. Maecenas at nibh. Aliquam et augue at nunc pellentesque ullamcorper. Duis nisl nibh, laoreet suscipit, convallis ut, rutrum id, enim. Phasellus odio.

Nulla nulla elit, molestie non, scelerisque at, vestibulum eu, nulla. Ut odio nisl, facilisis id, mollis et, scelerisque nec, enim. Aenean sem leo, pellentesque sit amet, scelerisque sit amet, vehicula pellentesque, sapien.

Sed consequat tellus et tortor. Ut tempor laoreet quam. Nullam id wisi a libero tristique semper. Nullam nisl massa, rutrum ut, egestas semper, mollis id, leo. Nulla ac massa eu risus blandit mattis. Mauris ut nunc. In hac habitasse platea dictumst. Aliquam eget tortor. Quisque dapibus pede in erat. Nunc enim. In dui nulla, commodo at, consectetuer nec, malesuada nec, elit. Aliquam ornare tellus eu urna. Sed nec metus. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas.

1.3.2 Second Paper [DDMS39]

Phasellus id magna. Duis malesuada interdum arcu. Integer metus. Morbi pulvinar pellentesque mi. Suspendisse sed est eu magna molestie egestas. Quisque mi lorem, pulvinar eget, egestas quis, luctus at, ante. Proin auctor vehicula purus. Fusce ac nisl aliquam ante hendrerit pellentesque. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Morbi wisi. Etiam arcu mauris, facilisis sed, eleifend non, nonummy ut, pede. Cras ut lacus tempor metus mollis placerat. Vivamus eu tortor vel metus interdum malesuada.

Sed eleifend, eros sit amet faucibus elementum, urna sapien consectetuer mauris, quis egestas leo justo non risus. Morbi non felis ac libero vulputate fringilla. Mauris libero eros, lacinia non, sodales quis, dapibus porttitor, pede. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Morbi dapibus mauris condimentum nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Etiam sit amet erat. Nulla varius. Etiam tincidunt dui vitae turpis. Donec leo. Morbi vulputate convallis est. Integer aliquet. Pellentesque aliquet sodales urna.

1.3.3 Third Paper [DS38]

Nullam eleifend justo in nisl. In hac habitasse platea dictumst. Morbi nonummy. Aliquam ut felis. In velit leo, dictum vitae, posuere id, vulputate nec, ante. Maecenas vitae pede nec dui dignissim suscipit. Morbi magna. Vestibulum id purus eget velit laoreet laoreet. Praesent sed leo vel nibh convallis blandit. Ut rutrum. Donec nibh. Donec interdum. Fusce sed pede sit amet elit rhoncus ultrices. Nullam at enim vitae pede vehicula iaculis.

Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Aenean nonummy turpis id odio. Integer euismod imperdiet turpis. Ut nec leo nec diam imperdiet lacinia. Etiam eget lacus eget mi ultricies posuere. In placerat tristique tortor. Sed porta vestibulum metus. Nulla iaculis sollicitudin pede. Fusce luctus tellus in dolor. Curabitur auctor velit a sem. Morbi sapien. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Donec adipiscing urna vehicula nunc. Sed ornare leo in leo. In rhoncus leo ut dui. Aenean dolor quam, volutpat nec, fringilla id, consectetuer vel, pede.

My Contributions

[DDMS39] John Doe, Jean Dupont, Pierre Martin et Jane Smith. I had to submit something just before graduating. In : Conf1 proceedings. Sous la dir. de Big Boss. Thief, oct. 2039 (cf. p. 12).

[Doe36] John Doe. My first paper, that I am really proud of, but which never got published. Cryptology ePrint Archive, Report 2036/9999. `http://eprint.iacr.org/2036/9999`. 2036 (cf. p. 11).

[DS38] John Doe et Jane Smith. Your advisor finally helped you ... In : Conf2 proceedings. Sous la dir. de Who Knows. Thief, avr. 2038 (cf. p. 12).

References

[BB04] Dan Boneh et Xavier Boyen. Efficient Selective-ID Secure Identity Based Encryption Without Random Oracles. In : 2004, p. 223-238 (cf. p. 23).

[BCK96] Mihir Bellare, Ran Canetti et Hugo Krawczyk. Keying Hash Functions for Message Authentication. In : 1996, p. 1-15 (cf. p. 27).

[BDJR97] Mihir Bellare, Anand Desai, Eric Jokipii et Phillip Rogaway. A Concrete Security Treatment of Symmetric Encryption. In : 1997, p. 394-403 (cf. p. 29).

[BGI14] Elette Boyle, Shafi Goldwasser et Ioana Ivan. Functional Signatures and Pseudorandom Functions. In : 2014, p. 501-519 (cf. p. 24).

[BM97] Mihir Bellare et Daniele Micciancio. A New Paradigm for Collision-Free Hashing : Incrementality at Reduced Cost. In : 1997, p. 163-192 (cf. p. 28).

[BR06] Mihir Bellare et Phillip Rogaway. The Security of Triple Encryption and a Framework for Code-Based Game-Playing Proofs. In : 2006, p. 409-426 (cf. p. 20, 26).

[BR93] Mihir Bellare et Phillip Rogaway. Random Oracles are Practical : A Paradigm for Designing Efficient Protocols. In : 1993, p. 62-73 (cf. p. 22).

[BW13] Dan Boneh et Brent Waters. Constrained Pseudorandom Functions and Their Applications. In : 2013, p. 280-300 (cf. p. 24).

[DDMS39] John Doe, Jean Dupont, Pierre Martin et Jane Smith. I had to submit something just before graduating. In : Conf1 proceedings. Sous la dir. de Big Boss. Thief, oct. 2039 (cf. p. 12).

[Doe36] John Doe. My first paper, that I am really proud of, but which never got published. Cryptology ePrint Archive, Report 2036/9999. `http://eprint.iacr.org/2036/9999`. 2036 (cf. p. 11).

[DS38] John Doe et Jane Smith. Your advisor finally helped you ... In : Conf2 proceedings. Sous la dir. de Who Knows. Thief, avr. 2038 (cf. p. 12).

[GPS06] S.D. Galbraith, K.G. Paterson et N.P. Smart. Pairings for Cryptographers. Cryptology ePrint Archive, Report 2006/165. https://eprint.iacr.org/2006/165. 2006 (cf. p. 23).

[KM15] Neal Koblitz et Alfred Menezes. The Random Oracle Model : A Twenty-Year Retrospective. Cryptology ePrint Archive, Report 2015/140. https://eprint.iacr.org/2015/140. 2015 (cf. p. 22).

[KPTZ13] Aggelos Kiayias, Stavros Papadopoulos, Nikos Triandopoulos et Thomas Zacharias. Delegatable pseudorandom functions and applications. In : 2013, p. 669-684 (cf. p. 24).

In the beginning, God created the heavens and the earth.

Genesis

Notations, Definitions and Preliminaries 2

TIME TO STEP IN THE REAL STUFF. Define all what you will need the next chapters here. Follows an example for cryptography. Blah blah blah ...

Contents

2.1 Mathematical Notations

Sets and rings. The set of integers is denoted $\mathbb{Z}$, the set of non-negative integers $\mathbb{N}$. If a and b are two integers such that $a \leq b$, we denote by $[\![a, b]\!]$ the set $\{x \in \mathbb{Z} | a \leq x \leq b\}$ of integers between a and b (both included). Also, $\mathbb{Z}_n$ is the ring $\mathbb{Z}/n\mathbb{Z}$ of integers modulo the integer n. For a prime integer p, $\mathbb{F}_p = \mathbb{Z}_p$ is the field with p elements. $\varphi(\cdot)$ is the Euler totient function. For any set S, $\mathcal{P}(S)$ is the set of all finite subsets of S.

Bilinear Groups Some of the cryptographic primitives we will use an additional structure on groups called a pairing (a.k.a. bilinear groups). Let $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ be three cyclic groups of the same order N and with respective generator g_1, g_2 and g_T. $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e)$ is called a *bilinear group* if $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ satisfies the following properties :

- For all $(a, b) \in \mathbb{Z}_N^2$, $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$ (bilinearity);
- The element $e(g_1, g_2)$ generates $\mathbb{G}_T$ (non-degeneracy);
- $e(\cdot, \cdot)$ is efficiently computable.

We explain the next paragraphs what efficient means. Without loss of generality, we can suppose that $e(g_1, g_2) = g_T$. We call bilinear groups with $\mathbb{G}_1 = \mathbb{G}_2$ Type-1 (or symmetric) bilinear groups, and in this case, we suppose that $g = g_1 = g_2$. If $\mathbb{G}_1 \neq \mathbb{G}_2$, and that there is no efficiently computable isomorphism between $\mathbb{G}_1$ and $\mathbb{G}_2$, it is a Type-3 (asymmetric) bilinear group.

Bit strings. A bit b is an element in $\{0, 1\}$; a bit string s of length n is a vector of n bits. ε denotes the *empty* bit string of size 0. The set of bit strings of size n is hence denoted $\{0, 1\}^n$, and the set of bit strings of finite length is $\{0, 1\}^* = \cup_{n \geq 0}\{0, 1\}^n$. The concatenation of two bit strings x and y is denoted $x||y$.

Distributions and Probabilities For a finite set S, $s \xleftarrow{\$} S$ means that s is sampled uniformly at random from S. The probability of an event E to occur is denoted $\mathbb{P}[E]$. Let X be a random variable. The expected value of X is $\mathbb{E}[X]$, and $\mathbb{V}\mathrm{ar}[X]$ its variance. The entropy and min-entropy of a discrete random variable X taking value $\{x_1, \ldots, x_n\}$ are denoted $H_1(X)$ and $H_\infty(X)$ and are defined as

$$\mathrm{H}_1(X) = -\sum_{i=1}^{n} \mathbb{P}[X = x_i] \cdot \log \mathbb{P}[X = x_i],$$
$$\text{and } \mathrm{H}_\infty(X) = -\min_{1 \leq i \leq n} \{\log \mathbb{P}[X = x_i]\} = \max_{1 \leq i \leq n} \{-\log \mathbb{P}[X = x_i]\}$$

where log is the base-2 logarithm. For two random discrete random variable Y and Z over the set $\{x_1, \ldots, x_n\}$, the Kullback–Leibler divergence from Y to Z, $\mathrm{D}_{\mathrm{KL}}(Y||Z)$, is defined as

$$\mathrm{D}_{\mathrm{KL}}(Y||Z) = \sum_{i=1}^{n} \mathbb{P}[Y = x_i] \log \frac{\mathbb{P}[Y = x_i]}{\mathbb{P}[Z = x_i]}.$$

Finally, we define the distance $\Delta(\mathcal{D}_1, \mathcal{D}_2)$ between the two distributions $\mathcal{D}_1$ and $\mathcal{D}_2$ over a set X as

$$\Delta(\mathcal{D}_1, \mathcal{D}_2) = \max_{x \in X} |\mathbb{P}[Y_1 = x] - \mathbb{P}[Y_2 = x]|$$

where Y_1 (resp Y_2) is a random variable following the distribution $\mathcal{D}_1$ (resp. $\mathcal{D}_2$).

Asymptotics. For asymptotics, we use the standard Landau notations $\mathcal{O}(\cdot)$, $\mathrm{o}(\cdot)$, $\Omega(.)$, $\omega(.)$ and $\Theta(.)$. We also use $\Theta(.)$ to hide poly-logarithmic factors in asymptotics :

$$f(n) = \Theta(g(n)) \Leftrightarrow \exists c \in \mathbb{N} \text{ such that } f(n) = \mathcal{O}(g(n) \log^c(n)).$$

In the following, $\mathsf{poly}(n)$ denotes an unspecified function $f(n) = \mathcal{O}(n^c)$ for some fixed constant c, and $\mathsf{negl}(n)$ is a negligible function f such that $f(n) = \mathrm{o}(n^{-c})$ for any constant $c > 0$.

Algorithms, Turing machines, and Oracles Algorithms are programs for Turing machines. They can be probabilistic, and use a tape of the Turing machine filled with random bits (also called random coins). By default algorithms are probabilistic. For an algorithm A, $y \leftarrow A(x)$ means that A is run on input x (with fresh random coins if A is probabilistic), and that the result is stored in y. More generally $y \leftarrow a$ states that the result of the evaluation of the expression a is stored in the variable y.

An interactive Turing machine is a special kind of Turing machines able to communicate with external algorithms. To do so, the interactive Turing machine uses additional tapes to communicate with the other Turing machines, namely an input tape to send messages, and an output tape to receive messages. For an interactive Turing machine $\mathcal{T}$, the Turing machines $\mathcal{T}$ has access to are called its *oracles*. We write $\mathcal{T}^{O_1,O_2}(x)$ to say that the Turing machine $\mathcal{T}$ is called with input x and has access to the oracles O_1 and O_2.

For a distribution $\mathcal{D}$, $A(\mathcal{D})$ denotes the output of the execution of A on an input x sampled from the distribution $\mathcal{D}$.

In this manuscript, we will often abuse notations, and identify a Turing machine and the algorithm it runs.

Finally, we will say that an algorithm is *efficient* if it runs in time polynomial in the size of its arguments.

Protocols. A two-party protocol $P = (A_1, A_2)$ is a pair of algorithms A_1 and A_2, interactively executed by a pair of two Turing machines $\mathcal{T}_1$ and $\mathcal{T}_2$. We will denote the execution of the protocol P as

$$P(\mathtt{input}_1; \mathtt{input}_2) = (A_1(\mathtt{input}_1), A_2(\mathtt{input}_2)),$$

meaning that A_1 (resp. A_2) is executed by $\mathcal{T}_1$ (resp. $\mathcal{T}_2$) with input $\mathtt{input}_1$ (resp. $\mathtt{input}_2$). We write

$$(\mathtt{out}_1; \mathtt{out}_2) \overset{\$}{\leftarrow} A_1(\mathtt{input}_1) \leftrightarrow A_2(\mathtt{input}_2)$$

to mean that $\mathtt{out}_1$ and $\mathtt{out}_2$ are the outputs of the interaction between A_1 on input $\mathtt{input}_1$ and A_2 on input $\mathtt{input}_2$, respectively. We also simplify this notation and denote the result of the execution of P as

$$(\mathtt{out}_1; \mathtt{out}_2) \stackrel{\$}{\leftarrow} P(\mathtt{input}_1; \mathtt{input}_2)$$

In this formalism, we consider the messages $\tau_{1\to 2}$ (resp. $\tau_{1\leftarrow 2}$) sent by $\mathcal{T}_1$ to $\mathcal{T}_2$ (resp. $\mathcal{T}_2$ to $\mathcal{T}_1$) as part of the output $\mathtt{out}_1$ (resp. $\mathtt{out}_2$). These messages are called the *transcript* of $\mathcal{T}_1$ (resp. $\mathcal{T}_2$). Transcripts might be omitted from the output of the protocol for simplicity of the notations.

Miscellaneous. As mentioned earlier, the base-2 logarithm of the value x is $\log x$. When the variable T is a dictionary, $T[v]$ denotes the item associated to v, if there is one, whereas $\perp$ denotes the absence of this item.

2.2 Cryptographic Preliminaries

2.2.1 Cryptographic Tools

Security parameter. In order to properly formalize security notions, we need to bound the computing power of an attacker. Indeed, one can always break cryptosystems using a large enough computer and spending a high amount of time. However, in cryptography, we restrict ourselves to the defence against *reasonable* attackers. To do so, we use the notion of *security parameter*, denoted $\lambda \in \mathbb{N}$. The security parameter is passed as an input to the attacker, under its unary representation 1^λ, and we only consider attackers whose running time is polynomial in λ, and whose success probability is non-negligible in λ.

All these notions are formally defined in the following paragraphs.

Adversaries. An adversary is a probabilistic Turing machine, which, in this manuscript, run in polynomial time, which may carry a state st when they need to be called several times. In most cases, we implicitly give as input to the adversary, both the unary representation of the security parameter, and the state. As a consequence, as adversaries' inputs are always polynomial in the security parameter, the polynomial time adversary runs in time polynomial in the security parameter.

Games. Security notions are often defined using security games (or experiments). Simple games are defined by having an adversary accessing a set of oracles, sometimes with some restrictions on calls to these oracles, and the output of the game is defined as the output of the adversary.

More generally, games are defined using the *code-based games* formalism introduced in [BR06]. Such a game G is a set of oracle procedures – including an initialization Init procedure and a finalization Final procedure – that is executed with an adversary A, *i.e.* A has access to the procedures, with some possible restrictions. For instance, the Init oracle is always the first one to be called and Final the last one, once A halted, taking A's output as input. The output of Final is called the output of the game and is denoted $G^A(1^\lambda)$. When Final is omitted, it just forwards the adversary's output.

In those games, at startup, the boolean variables are initialized to false and the integer variables to 0.

Statistical Indistinguishability Let $\mathcal{D}_1$ and $\mathcal{D}_2$ be two distributions over the set S. $\mathcal{D}_1$ and $\mathcal{D}_2$ are said to be *statistically indistinguishable* if

$$\Delta(\mathcal{D}_1, \mathcal{D}_2) \leq \mathsf{negl}(\lambda).$$

We denote

$$\mathcal{D}_1 \approx \mathcal{D}_2$$

the fact that $\mathcal{D}_1$ and $\mathcal{D}_2$ are statistically indistinguishable.

Computational Indistinguishability Let $\mathcal{D}_1$ and $\mathcal{D}_2$ be two distributions which can be sampled in polynomial-time in λ, and A be a polynomial-time adversary A outputting a single bit. The advantage of A distinguishing $\mathcal{D}_1$ and $\mathcal{D}_2$ is defined by

$$\mathbf{Adv}^{\mathcal{D}_1,\mathcal{D}_2}(A, 1^\lambda) = |\mathbb{P}[A(\mathcal{D}_1) = 1] - \mathbb{P}[A(\mathcal{D}_2) = 1]|\,.$$

Distributions $\mathcal{D}_1$ and $\mathcal{D}_2$ are said to be *computationally indistinguishable* if for any polynomial-time adversary A, the advantage of A in distinguishing $\mathcal{D}_1$ and $\mathcal{D}_2$, denoted $\mathbf{Adv}^{\mathcal{D}_1,\mathcal{D}_2}(A, 1^\lambda)$, is negligible in λ. We denote

$$\mathcal{D}_1 \approx_c \mathcal{D}_2$$

the fact that $\mathcal{D}_1$ and $\mathcal{D}_2$ are computationally indistinguishable. Note that two statistically indistinguishable distributions are computationally indistinguishable.

Similarly, we say that two different games G_0 and G_1, both outputting one bit, are indistinguishable if, for any polynomial-time adversary A, the advantage of A in distinguishing G_0 and G_1, denoted $\mathbf{Adv}^{G_0,G_1}(A, 1^\lambda)$ and defined as

$$\mathbf{Adv}^{G_0,G_1}(A, 1^\lambda) = \left|\mathbb{P}[G_0^A = 1] - \mathbb{P}[G_1^A = 1]\right|,$$

is negligible in λ. In this case, we write $G_0 \approx_c G_1$.

Game-based proofs Many of the security notions that we will define and use in this thesis are based on the indistinguishability of two different games G_0 and G_1. Unfortunately, in many cases, we will not be able to directly prove this indistinguishability. Instead, we proceed by *game hops*, by constructing a sequence of games, starting with G_0, and ending with G_1, and proving that consecutive games are indistinguishable. The distinguishing advantage between G_0 and G_1 of an adversary A will then be the sum of the distinguishing advantages of A between every pair of consecutive games in the games sequence.

The Random Oracle Model (ROM) The Random Oracle Model (or ROM), formally introduced by Bellare and Rogaway in [BR93], is a computational model where all parties have access to a (public) random oracle. As its name indicates, a random oracle outputs a random string for every new input it is given.

To prove the security of some schemes in the ROM, we often use an additional feature, called *programmability*. This feature allows the games to pre-program the output of the random oracle on some inputs, in a way that the programmed random oracle is indistinguishable from a regular random oracle.

The ROM is a very useful tool to show the security of some schemes. However, in practice, random oracles cannot exist (they would require an infinite description), and are often instantiated using hash functions. There actually is much debate among cryptographers on the quality of the ROM as an abstraction to analyze the security of cryptosystems [KM15]. Yet, for applied and real-world cryptography, it is a widely accepted and widely used model, as there is no convincing evidence that ROM-protocols have non-theoretical security weaknesses.

2.2.2 Hardness Assumptions

Cryptographic primitives rely on the hardness of some mathematical problems. We describe here the ones that will be useful for our constructions.

The RSA assumption The RSA assumption, as introduced by Rivest, Shamir and Adleman in [RSA78] states that it is infeasible to compute the e-th root of an element modulo N when N is a product of two large primes, and e is relatively prime with $\varphi(N)$.

Let RSAGen be defined as the function, which, on input the security parameter 1^λ, randomly samples two distinct λ bits primes p and q, computes $N = p \cdot q$, randomly picks an integer e less than and relatively prime to $\varphi(N) = (p-1)(q-1)$, and outputs the pair (N, e). For any adversary A, let $\mathsf{Adv}_A^{\mathrm{RSA}}(\lambda)$ be defined as :

$$\mathsf{Adv}_A^{\mathrm{RSA}}(\lambda) = \mathbb{P}[(N, e) \leftarrow \mathsf{RSAGen}(1^\lambda), y \xleftarrow{\$} \mathbb{Z}_N^*, x \leftarrow A(1^\lambda, N, e, y) : x^e = y \bmod N].$$

The RSA problem is supposed hard : for any polynomial-time adversary A, $\mathsf{Adv}_A^{\mathrm{RSA}}(\lambda)$ is negligible in λ.

Discrete Logarithm Solving the discrete logarithm problem in the cyclic group $\mathbb{G}$ with generator g, and of order N consists in finding the integer $x \in \mathbb{Z}_N$ such that $g^x = h$ for an element $h \in \mathbb{G}$.

In terms of security games, this can be formalized as follows. For any adversary A, let $\mathsf{Adv}_{\mathbb{G},A}^{\mathrm{DL}}(\lambda)$ be the quantity

$$\mathsf{Adv}_{\mathbb{G},A}^{\mathrm{DL}}(\lambda) = \mathbb{P}[h \xleftarrow{\$} \mathbb{G}, x \leftarrow A(1^\lambda, \mathbb{G}, g, h) : g^x = h].$$

We say that the discrete logarithm is hard in $\mathbb{G}$ if for all polynomial-time adversary A, $\mathsf{Adv}_{\mathbb{G},A}^{\mathrm{DL}}(\lambda)$ is negligible in λ. The discrete log is supposed to be hard on large prime order subgroups of $(\mathbb{F}_p^*, \times)$, and on cyclic subgroups of elliptic curves over finite fields.

The Diffie-Hellman Assumptions A strengthening of the discrete logarithm assumption is the Computational Diffie-Hellman (CDH) assumption. It requires that an adversary, given g^a and g^b, for g a generator of the group $\mathbb{G}$ of order N, and $a, b \in \mathbb{Z}_n$, cannot efficiently compute $g^{a \cdot b}$. Formally, for an adversary A, we define the advantage $\mathsf{Adv}^{\mathrm{CDH}}_{\mathbb{G},A}(\lambda)$ as

$$\mathsf{Adv}^{\mathrm{CDH}}_{\mathbb{G},A}(\lambda) = \mathbb{P}[a \xleftarrow{\$} \mathbb{Z}_N, b \xleftarrow{\$} \mathbb{Z}_N, h \leftarrow A(1^\lambda, \mathbb{G}, g^a, g^b) : g^{a\dot{b}} = h].$$

We say that the CDH assumption is hard in $\mathbb{G}$ if for all polynomial-time adversary A, $\mathsf{Adv}^{\mathrm{CDH}}_{\mathbb{G},A}(\lambda)$ is negligible in λ. The CDH assumption is supposed to be hard on large prime order subgroups of $(\mathbb{F}_p^*, \times)$, and on cyclic subgroups of elliptic curves over finite fields.

A stronger assumption is also very commonly encountered, the decisional version of CDH, called the Decisional Diffie-Hellman (DDH) assumption. This time the adversary is asked to distinguish between the triple $(g^a, g^b, g^{a \cdot b})$ and the triple (g^a, g^b, g^c).

$$\begin{aligned}\mathsf{Adv}^{\mathrm{DDH}}_{\mathbb{G},A}(\lambda) = \Big| &\mathbb{P}[(a,b) \xleftarrow{\$} \mathbb{Z}_N^2 : A(1^\lambda, g^a, g^b, g^{ab}) = 1] \\ &- \mathbb{P}[(a,b,z) \xleftarrow{\$} \mathbb{Z}_N^3 : A(1^\lambda, g^a, g^b, g^z) = 1]\Big| .\end{aligned}$$

We say that the DDH assumption is hard in $\mathbb{G}$ if for all polynomial-time adversary A, $\mathsf{Adv}^{\mathrm{DDH}}_{\mathbb{G},A}(\lambda)$ is negligible in λ. The DDH assumption is also supposed to be hard on large prime order subgroups of $(\mathbb{F}_p^*, \times)$, and on cyclic subgroups of elliptic curves over finite fields.

Cryptographic Pairings We will require that bilinear groups satisfy a hardness assumption called the Decisional Bilinear Diffie-Hellman (DBDH) assumption [BB04]. This assumption requires that a bounded adversary cannot distinguish the tuple $(g, g^a, g^b, g^c, e(g,g)^{abc})$ from the tuple $(g, g^a, g^b, g^c, e(g,g)^z)$, where a, b, c and z are randomly generated.

Formally, for a bilinear group $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e)$, the advantage $\mathsf{Adv}^{\mathrm{DBDH}}_{\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T,e,A}(\lambda)$ of an adversary A in the Decisional Bilinear Diffie-Hellman game is defined as :

$$\begin{aligned}\mathsf{Adv}^{\mathrm{DBDH}}_{\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T,e,A}(\lambda) = \Big| &\mathbb{P}[(a,b,c) \xleftarrow{\$} \mathbb{Z}_N^3 : A(1^\lambda, g^a, g^b, g^c, e(g,g)^{abc}) = 1] \\ &- \mathbb{P}[(a,b,c,z) \xleftarrow{\$} \mathbb{Z}_N^4 : A(1^\lambda, g^a, g^b, g^c, e(g,g)^z) = 1]\Big| .\end{aligned}$$

The bilinear group is said to be secure if, for all polynomial-time adversary A, $\mathsf{Adv}^{\mathrm{DBDH}}_{\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T,e,A}(\lambda)$ is negligible in λ.

Note that, in this definition, we only considered the symmetric setting for the bilinear group, but that the definition can trivially be adapted to an asymmetric pairing. In practice, cryptographic pairings are instantiated using elliptic curves, and we will use Type-3 pairings only. We refer to [GPS06] for more details on pairings.

2.3 Cryptographic Primitives

In this Section, we describe and define all the cryptographic primitives that we will use throughout this thesis. Completely formal definitions of most of these objects can be found in [BOOK :Goldreich04]. We often adopt here a simplified formulation.

2.3.1 Pseudorandom Function (PRF)

A pseudorandom function is a function that is indistinguishable from a truly random function. More formally, let $F : \mathcal{K} \times \mathcal{D} \to \mathcal{R}$ be a polynomial-time computable map, where $\mathcal{K}$ and $\mathcal{R}$ are finite. $\mathcal{K}$ is the *key space* of F, and $\mathcal{D}$ its domain, while $\mathcal{R}$ is the range of F. For $K \in \mathcal{K}$, we denote F_K the function that is the partial evaluation of F on K, namely

$$\begin{aligned} F_K : \mathcal{D} &\to \mathcal{R} \\ x &\mapsto F(K, x) \end{aligned}$$

Hence, F can be seen as a *function family.*

Definition 2.1 (Pseudorandom function). Let $F : \mathcal{K} \times \mathcal{D} \to \mathcal{R}$ be a function family, and $\mathsf{Func}(\mathcal{D}, \mathcal{R})$ the set of all functions of domain $\mathcal{D}$ and range $\mathcal{R}$. The pseudorandom function distinguishing advantage $\mathsf{Adv}^{\mathrm{prf}}_{A,F}(\lambda)$ of A against F is defined as

$$\mathsf{Adv}^{\mathrm{prf}}_{F,A}(\lambda) = \left| \mathbb{P}[K \xleftarrow{\$} \mathcal{K} : A^{F_K(\cdot)}(1^\lambda) = 1] - \mathbb{P}[\pi \xleftarrow{\$} \mathsf{Func}(\mathcal{D}, \mathcal{R}) : A^{\pi(\cdot)}(1^\lambda) = 1] \right|.$$

The PRF advantage function of F is defined as follows. For any integers t, q,

$$\mathsf{Adv}^{\mathrm{prf}}_{F}(\lambda, t, q) = \max_{A} \mathsf{Adv}^{\mathrm{prf}}_{F,A}(\lambda)$$

where the maximum is taken over all adversary A with time complexity t, making at most q oracle queries. F is said to be a pseudorandom function if $\mathsf{Adv}^{\mathrm{prf}}_{F,A}(\lambda)$ is negligible in λ for any polynomial-time adversary A.

2.3.2 Constrained Pseudorandom Function (CPRF)

The idea of *constrained PRFs* (CPRF) has been introduced in concurrent work by Boneh and Waters, Boyle *et al.*, and Kiayias *et al.* [BW13; BGI14; KPTZ13]. A constrained PRF is associated with a family of boolean circuits $\mathcal{C} = \{C\}$. The holder of the master PRF key is able to compute a *constrained key* K_C corresponding to a circuit $C \in \mathcal{C}$; the constrained key K_C allows evaluation of the PRF on inputs x such that $C(x) = 1$, but only on these inputs.

More formally, a *constrained PRF* F with respect to a circuit family $\mathcal{C}$ is a mapping $F : \mathcal{K} \times \mathcal{D} \to \mathcal{R}$, together with a pair of algorithms $(F.\mathsf{Constrain}, F.\mathsf{Eval})$, defined as follows.

- $F.\mathsf{Constrain}(K, C)$ is a PPT algorithm taking as input a key $K \in \mathcal{K}$ and a circuit $C \in \mathcal{C}$. It outputs a constrained key K_C.
- $F.\mathsf{Eval}(K_C, x)$ is a deterministic polynomial-time algorithm taking as input a constrained key K_C for circuit C, and $x \in \mathcal{D}$. It outputs $y \in \mathcal{R}$.

Wherever this does not result in ambiguity, we may leave out Eval and write $F.\mathsf{Eval}(K_C, x)$ as $F(K_C, x)$.

Correctness. A CPRF F is correct if and only if, $C(x) = 1$ implies $F(K, x) = F.\mathsf{Eval}(K_C, x)$, where $K_C = F.\mathsf{Constrain}(K, C)$, for all $K \in \mathcal{K}$, $x \in \mathcal{D}$, and $C \in \mathcal{C}$.

Security Definition. The security properties of a constrained PRF can be formalized using a security game G_{cprf} described in Figure 2.1. Informally, the adversary A wins the game (the game outputs 1) when he is able to distinguish between real evaluations of F and truly random elements of $\mathcal{R}$ on inputs such that he never queried a constrained key K_C for a circuit C evaluating to 1 on these inputs. The formal definition follows.

<u>$\mathsf{Init}()$</u>
$K \xleftarrow{\$} \mathcal{K}$
$b \xleftarrow{\$} \{0,1\}$
$E \leftarrow \emptyset, Z \leftarrow \emptyset, L \leftarrow \emptyset$
<u>$\mathsf{Challenge}(x)$</u>
$Z \leftarrow Z \cup \{x\}$
if $b = 0$ then
$y \xleftarrow{\$} \mathcal{R}$
else
$y \leftarrow F(K, x)$
end if
return y
	<u>$\mathsf{Eval}(x)$</u>
	$E \leftarrow E \cup \{x\}$
	return $F(K, x)$
	<u>$\mathsf{Constrain}(C)$</u>
	$L \leftarrow L \cup C$
	return $F.\mathsf{Constrain}(C)$
	<u>$\mathsf{Final}(b')$</u>
	if $b = b'$, $E \cap Z = \emptyset$
	and $\forall (C, z) \in (L, Z),\ C(z) = 0$
	return 1 ▷ The adversary wins
	return 0 ▷ The adversary looses

Fig. 2.1 – Procedures of the G_{cprf} security game. The lists E, Z, and L are, respectively, the list of evaluated inputs, challenged inputs and constraints. The condition in Final ensures that the game is only challenged on constrained inputs, and never on an evaluated input.

Definition 2.2 (Constrained PRF). Let F be a constrained function as defined previously. We define $\mathsf{Adv}^{\text{cprf}}_{F,A}(\lambda)$, the advantage of the adversary A in the constrained PRF security game, as

$$\mathsf{Adv}^{\text{cprf}}_{F,A}(\lambda) = \mathbb{P}[G^{A}_{\text{cprf}}(1^{\lambda}) = 1].$$

We say that F is a constrained pseudorandom function if, for any polynomial-time adversary A, $\mathsf{Adv}^{\text{cprf}}_{F,A}(\lambda)$ is negligible in the security parameter λ.

2.3.3 Pseudorandom Permutation (PRP)

A pseudorandom permutation is a permutation that is indistinguishable from a truly random permutation. Let $F : \mathcal{K} \times \mathcal{D} \to \mathcal{R}$ be a function family. We say that F is a family of permutation if for every $K \in \mathcal{K}$, F_K is a bijection between $\mathcal{D}$ and $\mathcal{R}$. Here, we will always be in the case where $\mathcal{D} = \mathcal{R}$.

Definition 2.3 (Pseudorandom permutation). Let $F : \mathcal{K} \times \mathcal{D} \to \mathcal{D}$ be a permutation family, and $\mathsf{Perm}(\mathcal{D})$ the set of all permutations of $\mathcal{D}$. The pseudorandom function distinguishing advantage $\mathsf{Adv}^{\mathrm{prp}}_{F,A}(\lambda)$ of A against F is defined as

$$\mathsf{Adv}^{\mathrm{prp}}_{F,A}(\lambda) = \left| \mathbb{P}[K \xleftarrow{\$} \mathcal{K} : A^{F_K(\cdot)}(1^\lambda) = 1] - \mathbb{P}[\pi \xleftarrow{\$} \mathsf{Perm}(\mathcal{D}) : A^{\pi(\cdot)}(1^\lambda) = 1] \right| .$$

The PRF advantage function of F is defined as follows. For any integers t, q,

$$\mathsf{Adv}^{\mathrm{prp}}_{F}(\lambda, t, q) = \max_A \mathsf{Adv}^{\mathrm{prp}}_{F,A}(\lambda)$$

where the maximum is taken over all adversary A with time complexity t, making at most q oracle queries. F is said to be a pseudorandom permutation if $\mathsf{Adv}^{\mathrm{prp}}_{F,A}(\lambda)$ is negligible in λ for any polynomial-time adversary A.

PRF switching lemma. It will be useful in the security proofs to be able to switch from a PRP to a PRF (to avoid considering non-collision among the PRP outputs). To do so, we will use the PRF switching lemma that states that a PRP is also a PRF. We refer the reader to [BR06, Lemma 1] for the proof.

Lemma 2.1. Let F be a PRP over the set $\mathcal{D}$. For any adversary A making at most q queries,

$$\left| \mathsf{Adv}^{\mathrm{prf}}_{F,A}(\lambda) - \mathsf{Adv}^{\mathrm{prp}}_{F,A}(\lambda) \right| \leq \frac{q^2}{2|\mathcal{D}|}.$$

2.3.4 Trapdoor Permutation (TDP)

Informally, a trapdoor permutation (TDP) π is a permutation over a set $\mathcal{M}$ such that, using a public key PK, π can be easily evaluated, but the inverse π^{-1} can be efficiently computed only with the secret SK.

More formally, a family of trapdoor permutations over a set $\mathcal{M}$ is a triple π of algorithms $(\mathsf{KeyGen}, \mathsf{Eval}, \mathsf{Invert})$ such that :

- KeyGen is a randomized algorithm taking as input the security parameter 1^λ that generates a pair $(\mathsf{SK}, \mathsf{PK})$, where SK is the private key and PK the public key ;
- Eval is a deterministic polynomial-time algorithm taking as inputs a public key and an element in $\mathcal{M}$, and such that for every public key PK generated by KeyGen, $\pi(\mathsf{PK}, .)$ is a bijection over $\mathcal{M}$;
- Invert is a deterministic polynomial-time algorithm taking as inputs a secret key and an element in $\mathcal{M}$, such that for every key pair $(\mathsf{PK}, \mathsf{SK})$ generated by KeyGen,

$$\mathsf{Invert}(\mathsf{SK}, \mathsf{Eval}(\mathsf{PK}, x)) = x.$$

In the following, will simplify the notations, and use $\pi_{\mathsf{PK}}(\cdot)$ to denote $\mathsf{Eval}(\mathsf{PK}, \cdot)$ and $\pi^{-1}_{\mathsf{SK}}(\cdot)$ for $\mathsf{Invert}(\mathsf{SK}, \cdot)$.

Definition 2.4 (Secure trapdoor permutation). For an adversary A, the advantage $\mathsf{Adv}^{\mathrm{tdp}}_{\pi,A}(\lambda)$ of A in the trapdoor permutation security game is defined as

$$\mathsf{Adv}^{\mathrm{tdp}}_{\pi,A}(\lambda) = \mathsf{Pr}[y \xleftarrow{\$} \mathcal{M}, (\mathsf{SK}, \mathsf{PK}) \leftarrow \mathsf{KeyGen}(1^\lambda), x \leftarrow A(1^\lambda, \mathsf{PK}, y) : \pi_{\mathsf{PK}}(x) = y].$$

For any integer t, $\mathsf{Adv}^{\mathrm{tdp}}_{\pi}(\lambda, t)$ is defined as

$$\mathsf{Adv}^{\mathrm{tdp}}_{\pi}(\lambda, t) = \max_{A} \mathsf{Adv}^{\mathrm{tdp}}_{\pi,A}(\lambda)$$

where the maximum is taken over all adversary A with time complexity t. The trapdoor permutation π is said to be a secure if, for any polynomial-time adversary A, $\mathsf{Adv}^{\mathrm{OW}}_{\pi,A}(\lambda)$ is negligible in λ.

We also use the notation $\pi^{(c)}_{\mathsf{PK}}(x)$ (resp. $\pi^{(-c)}_{\mathsf{SK}}(x)$) for the iterated application of π_{PK} (resp. π^{-1}_{SK}) c times.

2.3.5 Hash Function

A hash function family is a polynomial-time computable map $H : \mathcal{K} \times \mathcal{D} \rightarrow \mathcal{R}$ where $\mathcal{K}$ and $\mathcal{R}$ are non-empty sets. We denote the partial evaluation of H on K as $H_K(\cdot)$. For hash functions, we are interested in the difficulty with which an adversary is able to find to distinct elements in $\mathcal{D}$ evaluating to the same elements in $\mathcal{R}$.

Definition 2.5. Let $H : \mathcal{K} \times \mathcal{D} \rightarrow \mathcal{R}$ be a hash function family. For every adversary A, we define

$$\mathsf{Adv}^{\mathrm{col}}_{H,A}(\lambda) = \mathbb{P}[K \xleftarrow{\$} \mathcal{K}, (M, M') \leftarrow A(K) : M \neq M' \wedge H_K(M) = H_K(M')].$$

H is said to be collision-resistant family of hash function if, for any polynomial-time adversary A, $\mathsf{Adv}^{\mathrm{col}}_{H,A}(\lambda)$ is negligible in λ.

In practice, we only have access to a single element of the hash function family, which is denoted H.

Instantiating the ROM. Often, the random oracle used in the ROM (cf. Section 2.2.1) will be instantiated using a hash function. Unfortunately, many hash functions share undesirable properties (*e.g.* length-extension attacks) that make them unfit for such direct use as a random oracle. Instead, we will use the HMAC construction [BCK96] with a public key as the random oracle. For a hash function H, HMAC is defined as

$$\mathsf{HMAC}(K, x) = H((K \oplus opad)||H((K \oplus ipad)||x))$$

where $opad$ and $ipad$ are two constants.

(Multi)set hashing. In the case $\mathcal{D}$ is a set of sets, it would be nice to be able to easily compute the hash of $S \cup S'$ from the hashes of S and S'. Multiset hashing was introduced by Clarke *et al.* [AC :CDDGS03], based on the framework proposed by Bellare and Micciancio [BM97] for incremental hashing. Here, we slightly extend their definition so it fits our needs in this thesis.

A *set hashing function* on sets of elements in $\mathcal{D}$ is a quadruple of probabilistic polynomial algorithms $(\mathcal{H}, \equiv_{\mathcal{H}}, +_{\mathcal{H}}, -_{\mathcal{H}})$ such that $\mathcal{H} : \mathcal{P}(\mathcal{D}) \to \mathcal{R}$ maps sets whose elements are in $\mathcal{D}$, and for all $S \subset \mathcal{P}(\mathcal{D})$,

- $\mathcal{H}(S) \equiv_{\mathcal{H}} \mathcal{H}(S)$ (comparability)
- $\forall x \in \mathcal{D} \setminus S, \mathcal{H}(S \cup \{x\}) \equiv_{\mathcal{H}} \mathcal{H}(S) +_{\mathcal{H}} \mathcal{H}(\{x\})$ (insertion incrementality)
- $\forall x \in S, \mathcal{H}(S \setminus \{x\}) \equiv_{\mathcal{H}} \mathcal{H}(S) -_{\mathcal{H}} \mathcal{H}(\{x\})$ (deletion incrementality)

We want multiset hash functions to be secure in the sense of collision resistance : it is infeasible for an adversary to find two sets hashing to the same value.

Definition 2.6. Let $\mathcal{H}$ be a set hashing function. For every adversary A, we define

$$\mathsf{Adv}^{\mathrm{col}}_{\mathcal{H},A}(\lambda) = \mathbb{P}[(S, S') \leftarrow A^{\mathcal{H}(\cdot), \equiv_{\mathcal{H}}(\cdot), +_{\mathcal{H}}(\cdot), -_{\mathcal{H}}(\cdot)}(1^\lambda) : S \neq S' \wedge \mathcal{H}(S) \equiv_{\mathcal{H}} \mathcal{H}(S')].$$

The `MSet-Mu-Hash` construction of Clark *et al.* [AC :CDDGS03] for multisets works as follows : if H is a regular (*i.e.* non incremental) hash function, $\mathcal{H}(x_1^{m_1}, \ldots, x_n^{m_n})$ is defined as $\prod H(x_i)^{m_i}$ ($x_i^{m_i}$ represents the element x_i with multiplicity m_i). Formally, `MSet-Mu-Hash` is defined as follows :

$$\begin{aligned} \mathcal{H}(M) : \mathcal{P}(\mathcal{D}) &\to \mathbb{F}_q \\ M &\mapsto \Pi_{x \in \mathcal{D}} H(x)^{M_x} \end{aligned}$$

where $H : \mathcal{D} \to \mathbb{F}_q$ is a hash function from the set $\mathcal{D}$ to the field $\mathbb{F}_q$, and M_x is the multiplicity of x in M. This construction clearly fits our functional needs : for $S \subset \mathcal{D}$, we can easily compute (*i.e.* in constant time) $\mathcal{H}(S \cup \{x\})$ (resp. $\mathcal{H}(S \setminus \{x\})$) from $\mathcal{H}(S)$ and $\mathcal{H}(\{x\}) = H(x)$ – or even from x if we have access to H – as $\mathcal{H}(S \cup \{x\}) = \mathcal{H}(S) \cdot H(x)$ (resp. $\mathcal{H}(S \setminus \{x\}) = \mathcal{H}(S) \cdot H(x)^{-1}$).

Clarke *et al.* show that $\mathcal{H}$ is collision resistant as long as the discrete log assumption holds in $\mathbb{F}_q$ when H is modeled as a random oracle.

Theorem 2.2 (Theorem 2 of [AC :CDDGS03]). If the discrete log assumption holds in $\mathbb{F}_q$, and H is a (non-programable) random oracle, the multiset hash function $\mathcal{H}$ is collision resistant.

Note that multiset hashing can also be based on elliptic curves for improved efficiency [CJ :MaiTibAra16]. The security of the construction would immediately follow, using the hardness of discrete logarithm on cyclic subgroups of elliptic curves instead of its hardness on finite fields.

2.3.6 Semantically Secure Encryption

A (symmetric) encryption scheme SE is a triple of algorithms $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$. The randomized key generation algorithm KeyGen takes as input the security parameter in its unary form and outputs a key K from the key set $\mathcal{K}$. The encryption algorithm Enc takes a key and a plaintext m in the message space $\mathcal{M}$ and outputs a ciphertext $c \leftarrow \mathsf{Enc}(K, m)$ from the ciphertext space $\mathcal{C}$. Note that Enc can be either randomized or deterministic. The decryption algorithm is deterministic, and as input a key K and a string c, and outputs either an element $m \in \mathcal{M}$ or the symbol $\perp$.

In the following, we will only consider *correct* schemes, that is schemes such that, for all keys $K \in \mathcal{K}$, and all messages $m \in \mathcal{M}$,

$$\mathsf{Dec}(K, \mathsf{Enc}(K, m)) = m.$$

Many security definitions have been developed for (symmetric) encryption. Here we will consider indistinguishability against chosen plaintext attacks (IND-CPA). More precisely, we use the Left-Or-Right (LOR-CPA) definition, as given by Bellare *et al.* [BDJR97].

Definition 2.7. Let $SE = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ be a symmetric encryption scheme. For $b \in \{0, 1\}$, we define LoR as

$$\mathsf{LoR}(x_0, x_1, b) = x_b.$$

For an adversary A, the IND-CPA advantage of A against SE is

$$\begin{aligned}\mathsf{Adv}^{\mathrm{cpa}}_{SE,A}(\lambda) = \Big| &\mathbb{P}[K \xleftarrow{\$} \mathsf{KeyGen}(1^\lambda) : A^{\mathsf{Enc}_K(\mathsf{LoR}(\cdot,\cdot,0)}(1^\lambda) = 1] \\ &- \mathbb{P}[K \xleftarrow{\$} \mathsf{KeyGen}(1^\lambda) : A^{\mathsf{Enc}_K(\mathsf{LoR}(\cdot,\cdot,1)}(1^\lambda) = 1]\Big|,\end{aligned}$$

with the restriction that A must only query the oracle $\mathsf{Enc}_K(\mathsf{LoR}(\cdot, \cdot, b)$ with pairs of messages of equal length. The IND-CPA advantage function of SE is defined as follows. For any integers t, q, μ,

$$\mathsf{Adv}^{\mathrm{cpa}}_{SE}(\lambda, t, q, \mu) = \max_A \mathsf{Adv}^{\mathrm{cpa}}_{SE,A}(\lambda)$$

where the maximum is taken over all adversary A with time complexity t, making at most q oracle queries on messages of total length at most μ. SE is said to be a IND-CPA-secure if $\mathsf{Adv}^{\mathrm{cpa}}_{SE,A}(\lambda)$ is negligible in λ for any polynomial-time adversary A.

In practice, we will suppose that $\mathcal{K} = \{0, 1\}^\lambda$, and $\mathcal{M} = \mathcal{C} = \{0, 1\}^*$, unless otherwise specified. Also, the KeyGen algorithm will just pick a key in $\mathcal{K}$ uniformly at random.

2.3.7 Message Authentication Code (MAC)

A message authentication code is used to ensure that a message comes from the right sender. It is a triple of algorithms $(\mathsf{KeyGen}, \mathsf{MAC}, \mathsf{Vf})$. The randomized key generation algorithm KeyGen takes as input the security parameter in its unary form and outputs a key K from the key set $\mathcal{K}$. The algorithm MAC takes as input $K \in \mathcal{K}$ and a string $m \in \{0,1\}^*$ and outputs a tag $T \in \{0,1\}^\lambda$. Finally Vf, on input a key K, a string m and a tag T, outputs $\perp$ or $\top$.

We require that a MAC is correct, namely that for all $K \in \mathcal{K}$, and all string $m \in \{0,1\}$,

$$\mathsf{Vf}(K, m, \mathsf{MAC}(K, m)) = \top.$$

The security requirement of a MAC will be that it is infeasible for any polynomial-time adversary to forge a valid tag without the secret key.

$\underline{\mathsf{Init}()}$
  $K \xleftarrow{\$} \mathcal{K}$
  $\mathsf{win} \leftarrow \mathsf{false}$
  $Q \leftarrow \emptyset$
$\underline{\mathsf{Query}(x)}$
  $t \leftarrow \mathsf{MAC}(K, x)$
  $Q \leftarrow Q \cup \{(x, t)\}$
  return t

$\underline{\mathsf{Challenge}(x', t')}$
  if $\mathsf{Vf}(K, x', t') = \top$
    and $(x', s') \notin Q$ then
   $\mathsf{win} \leftarrow \mathsf{true}$
  end if
$\underline{\mathsf{Final}()}$
  return win

Fig. 2.2 – Procedures of the $G_{\text{ef-cma}}$ security game.

Definition 2.8. Let $(\mathsf{KeyGen}, \mathsf{MAC}, \mathsf{Vf})$ be a message authentication code. The advantage of A in the existential forgery with chosen messages attack game (EF-CMA), $\mathsf{Adv}^{\text{ef-cma}}_{A,\mathsf{MAC}}(\lambda)$, is defined as

$$\mathsf{Adv}^{\text{ef-cma}}_{\mathsf{MAC},A}(\lambda) = \mathbb{P}[G^A_{\text{ef-cma}}(1^\lambda) = 1].$$

were the $G_{\text{ef-cma}}$ is described in Figure 2.2. The EF-CMA advantage function is defined as follows. For any integers t, q, μ,

$$\mathsf{Adv}^{\text{ef-cma}}_{\mathsf{MAC}}(\lambda, t, q, \mu) = \max_A \mathsf{Adv}^{\text{ef-cma}}_{\mathsf{MAC},A}(\lambda)$$

where the maximum is taken over all adversary A with time complexity t, making at most q oracle queries on messages of total length at most μ. MAC is said to be a EF-CMA-secure if $\mathsf{Adv}^{\text{ef-cma}}_{\mathsf{MAC},A}(\lambda)$ is negligible in λ for any polynomial-time adversary A.

The most handy and practical way to instantiate a MAC is to use a PRF with variable input length, *i.e.* with domain $\mathcal{D}$. For such a PRF F, we will define MAC and Vf as

$$\mathsf{MAC}(K, x) = F(K, x)$$
$$\mathsf{Vf}(K, x, t) = \begin{cases} \top \text{ if } F(K, x) = t \\ \perp \text{ otherwise.} \end{cases}$$

2.3.8 Authenticated Encryption with Associated Data (AEAD)

Using authenticated encryption with associated, one is able to ensure both the confidentiality of a message and the authenticity of the message plus some optional additional data. Am AEAD scheme SE is a triple of algorithms $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$.

The randomized key generation algorithm KeyGen takes as input the security parameter in its unary form and outputs a key K from the key set $\mathcal{K}$. The encryption algorithm Enc takes a key, an optional string a called additional data, and a plaintext m in the message space $\mathcal{M}$ and outputs a ciphertext $c \leftarrow \mathsf{Enc}(K, a, m)$ from the ciphertext space $\mathcal{C}$. The decryption algorithm is deterministic, and as input a key K, the (optional) additional data a, and a string c, and outputs either an element $m \in \mathcal{M}$ or the symbol $\perp$.

In the following, we will only consider *correct* schemes, that is schemes such that, for all keys $K \in \mathcal{K}$, all string $a \in \{0,1\}^*$, and all messages $m \in \mathcal{M}$,

$$\mathsf{Dec}(K, a, \mathsf{Enc}(K, a, m)) = m.$$

Definition 2.9. Let $SE = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ be an authenticated encryption scheme with additional data. For an adversary A, the AE advantage of A against SE is

$$\mathsf{Adv}^{\mathsf{ae}}_{SE,A}(\lambda) = \left|\mathbb{P}[K \xleftarrow{\$} \mathsf{KeyGen}(1^\lambda) : A^{\mathsf{Enc}_K(\cdot,\cdot),\mathsf{Dec}_K(\cdot,\cdot,\cdot)}(1^\lambda) = 1] - \mathbb{P}[A^{\$(\cdot,\cdot),\perp(\cdot,\cdot,\cdot)}(1^\lambda) = 1]\right|$$

where $\$$ is an oracle that, on input (a, m), picks a random string r of size $|m|$ and returns $\mathsf{Enc}_K(a, r)$ and $\perp$ is the oracle always returning the symbol $\perp$.

The AE advantage function of SE is defined as follows. For any integers $t, q_e, \mu_e, q_d, \mu_d$,

$$\mathsf{Adv}^{\mathsf{ae}}_{SE}(\lambda, t, q_e, \mu_e, q_d, \mu_d) = \max_A \mathsf{Adv}^{\mathsf{ae}}_{SE,A}(\lambda)$$

where the maximum is taken over all adversary A with time complexity t, making at most q_e (resp. q_d) encryption (resp. decryption) oracle queries on messages of total length at most μ_e (resp. μ_d). SE is said to be a secure AEAD if $\mathsf{Adv}^{\mathsf{ae}}_{SE,A}(\lambda)$ is negligible in λ for any polynomial-time adversary A.

Again, in practice, we will suppose that $\mathcal{K} = \{0,1\}^\lambda$, and $\mathcal{M} = \mathcal{C} = \{0,1\}^*$, unless otherwise specified, and that the KeyGen algorithm will just pick a key in $\mathcal{K}$ uniformly at random.

References

[BB04] Dan Boneh et Xavier Boyen. Efficient Selective-ID Secure Identity Based Encryption Without Random Oracles. In : 2004, p. 223-238 (cf. p. 23).

[BCK96] Mihir Bellare, Ran Canetti et Hugo Krawczyk. Keying Hash Functions for Message Authentication. In : 1996, p. 1-15 (cf. p. 27).

[BDJR97] Mihir Bellare, Anand Desai, Eric Jokipii et Phillip Rogaway. A Concrete Security Treatment of Symmetric Encryption. In : 1997, p. 394-403 (cf. p. 29).

[BGI14] Elette Boyle, Shafi Goldwasser et Ioana Ivan. Functional Signatures and Pseudorandom Functions. In : 2014, p. 501-519 (cf. p. 24).

[BM97] Mihir Bellare et Daniele Micciancio. A New Paradigm for Collision-Free Hashing : Incrementality at Reduced Cost. In : 1997, p. 163-192 (cf. p. 28).

[BR06] Mihir Bellare et Phillip Rogaway. The Security of Triple Encryption and a Framework for Code-Based Game-Playing Proofs. In : 2006, p. 409-426 (cf. p. 20, 26).

[BR93] Mihir Bellare et Phillip Rogaway. Random Oracles are Practical : A Paradigm for Designing Efficient Protocols. In : 1993, p. 62-73 (cf. p. 22).

[BW13] Dan Boneh et Brent Waters. Constrained Pseudorandom Functions and Their Applications. In : 2013, p. 280-300 (cf. p. 24).

[DDMS39] John Doe, Jean Dupont, Pierre Martin et Jane Smith. I had to submit something just before graduating. In : Conf1 proceedings. Sous la dir. de Big Boss. Thief, oct. 2039 (cf. p. 12).

[Doe36] John Doe. My first paper, that I am really proud of, but which never got published. Cryptology ePrint Archive, Report 2036/9999. `http://eprint.iacr.org/2036/9999`. 2036 (cf. p. 11).

[DS38] John Doe et Jane Smith. Your advisor finally helped you ... In : Conf2 proceedings. Sous la dir. de Who Knows. Thief, avr. 2038 (cf. p. 12).

[GPS06] S.D. Galbraith, K.G. Paterson et N.P. Smart. Pairings for Cryptographers. Cryptology ePrint Archive, Report 2006/165. `https://eprint.iacr.org/2006/165`. 2006 (cf. p. 23).

[KM15] Neal Koblitz et Alfred Menezes. The Random Oracle Model : A Twenty-Year Retrospective. Cryptology ePrint Archive, Report 2015/140. `https://eprint.iacr.org/2015/140`. 2015 (cf. p. 22).

[KPTZ13] Aggelos Kiayias, Stavros Papadopoulos, Nikos Triandopoulos et Thomas Zacharias. Delegatable pseudorandom functions and applications. In : 2013, p. 669-684 (cf. p. 24).

A conclusion is the place where you
get tired of thinking.

Arthur Bloch

Conclusion 3

THIS THESIS PRESENTED new results and new constructions .... It is your problem to find something useful to do with it now!

3.1 Summary of the Results

Nulla ac nisl. Nullam urna nulla, ullamcorper in, interdum sit amet, gravida ut, risus. Aenean ac enim. In luctus. Phasellus eu quam vitae turpis viverra pellentesque. Duis feugiat felis ut enim. Phasellus pharetra, sem id porttitor sodales, magna nunc aliquet nibh, nec blandit nisl mauris at pede. Suspendisse risus risus, lobortis eget, semper at, imperdiet sit amet, quam. Quisque scelerisque dapibus nibh. Nam enim. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Nunc ut metus. Ut metus justo, auctor at, ultrices eu, sagittis ut, purus. Aliquam aliquam.

Etiam pede massa, dapibus vitae, rhoncus in, placerat posuere, odio. Vestibulum luctus commodo lacus. Morbi lacus dui, tempor sed, euismod eget, condimentum at, tortor. Phasellus aliquet odio ac lacus tempor faucibus. Praesent sed sem. Praesent iaculis. Cras rhoncus tellus sed justo ullamcorper sagittis. Donec quis orci. Sed ut tortor quis tellus euismod tincidunt. Suspendisse congue nisl eu elit. Aliquam tortor diam, tempus id, tristique eget, sodales vel, nulla. Praesent tellus mi, condimentum sed, viverra at, consectetuer quis, lectus. In auctor vehicula orci. Sed pede sapien, euismod in, suscipit in, pharetra placerat, metus. Vivamus commodo dui non odio. Donec et felis.

Etiam suscipit aliquam arcu. Aliquam sit amet est ac purus bibendum congue. Sed in eros. Morbi non orci. Pellentesque mattis lacinia elit. Fusce molestie velit in ligula. Nullam et orci vitae nibh vulputate auctor. Aliquam eget purus. Nulla auctor wisi sed ipsum. Morbi porttitor tellus ac enim. Fusce ornare. Proin ipsum enim, tincidunt in, ornare venenatis, molestie a, augue. Donec vel pede in lacus sagittis porta. Sed hendrerit ipsum quis nisl. Suspendisse quis massa ac nibh pretium cursus. Sed sodales. Nam eu neque quis pede dignissim ornare. Maecenas eu purus ac urna tincidunt congue.

Donec et nisl id sapien blandit mattis. Aenean dictum odio sit amet risus. Morbi purus. Nulla a est sit amet purus venenatis iaculis. Vivamus viverra purus vel magna. Donec in justo sed odio malesuada dapibus. Nunc ultrices aliquam nunc. Vivamus facilisis pellentesque velit. Nulla nunc velit, vulputate dapibus, vulputate id, mattis ac, justo. Nam mattis elit dapibus purus. Quisque enim risus, congue non, elementum ut, mattis quis, sem. Quisque elit.

Maecenas non massa. Vestibulum pharetra nulla at lorem. Duis quis quam id lacus dapibus interdum. Nulla lorem. Donec ut ante quis dolor bibendum condimentum. Etiam egestas tortor vitae lacus. Praesent cursus. Mauris bibendum pede at elit. Morbi et felis a lectus interdum facilisis. Sed suscipit gravida turpis. Nulla at lectus. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae ; Praesent nonummy luctus nibh. Proin turpis nunc, congue eu, egestas ut, fringilla at, tellus. In hac habitasse platea dictumst.

Vivamus eu tellus sed tellus consequat suscipit. Nam orci orci, malesuada id, gravida nec, ultricies vitae, erat. Donec risus turpis, luctus sit amet, interdum quis, porta sed, ipsum. Suspendisse condimentum, tortor at egestas posuere, neque metus tempor orci, et tincidunt urna nunc a purus. Sed facilisis blandit tellus. Nunc risus sem, suscipit nec, eleifend quis, cursus quis, libero. Curabitur et dolor. Sed vitae sem. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Maecenas ante. Duis ullamcorper enim. Donec tristique enim eu leo. Nullam molestie elit eu dolor. Nullam bibendum, turpis vitae tristique gravida, quam sapien tempor lectus, quis pretium tellus purus ac quam. Nulla facilisi.

Duis aliquet dui in est. Donec eget est. Nunc lectus odio, varius at, fermentum in, accumsan non, enim. Aliquam erat volutpat. Proin sit amet nulla ut eros consectetuer cursus. Phasellus dapibus aliquam justo. Nunc laoreet. Donec consequat placerat magna. Duis pretium tincidunt justo. Sed sollicitudin vestibulum quam. Nam quis ligula. Vivamus at metus. Etiam imperdiet imperdiet pede. Aenean turpis. Fusce augue velit, scelerisque sollicitudin, dictum vitae, tempor et, pede. Donec wisi sapien, feugiat in, fermentum ut, sollicitudin adipiscing, metus.

Donec vel nibh ut felis consectetuer laoreet. Donec pede. Sed id quam id wisi laoreet suscipit. Nulla lectus dolor, aliquam ac, fringilla eget, mollis ut, orci. In pellentesque justo in ligula. Maecenas turpis. Donec eleifend leo at felis tincidunt consequat. Aenean turpis metus, malesuada sed, condimentum sit amet, auctor a, wisi. Pellentesque sapien elit, bibendum ac, posuere et, congue eu, felis. Vestibulum mattis libero quis metus scelerisque ultrices. Sed purus.

3.2 Open Problems

I am good, but not enough to be able all problems.

First open problem Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Better support of deletions. Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Counter measure against file injections. Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

Bibliography

[BB04] Dan Boneh et Xavier Boyen. Efficient Selective-ID Secure Identity Based Encryption Without Random Oracles. In : 2004, p. 223-238 (cf. p. 23).

[BCK96] Mihir Bellare, Ran Canetti et Hugo Krawczyk. Keying Hash Functions for Message Authentication. In : 1996, p. 1-15 (cf. p. 27).

[BDJR97] Mihir Bellare, Anand Desai, Eric Jokipii et Phillip Rogaway. A Concrete Security Treatment of Symmetric Encryption. In : 1997, p. 394-403 (cf. p. 29).

[BGI14] Elette Boyle, Shafi Goldwasser et Ioana Ivan. Functional Signatures and Pseudorandom Functions. In : 2014, p. 501-519 (cf. p. 24).

[BM97] Mihir Bellare et Daniele Micciancio. A New Paradigm for Collision-Free Hashing : Incrementality at Reduced Cost. In : 1997, p. 163-192 (cf. p. 28).

[BR06] Mihir Bellare et Phillip Rogaway. The Security of Triple Encryption and a Framework for Code-Based Game-Playing Proofs. In : 2006, p. 409-426 (cf. p. 20, 26).

[BR93] Mihir Bellare et Phillip Rogaway. Random Oracles are Practical : A Paradigm for Designing Efficient Protocols. In : 1993, p. 62-73 (cf. p. 22).

[BW13] Dan Boneh et Brent Waters. Constrained Pseudorandom Functions and Their Applications. In : 2013, p. 280-300 (cf. p. 24).

[DDMS39] John Doe, Jean Dupont, Pierre Martin et Jane Smith. I had to submit something just before graduating. In : Conf1 proceedings. Sous la dir. de Big Boss. Thief, oct. 2039 (cf. p. 12).

[Doe36] John Doe. My first paper, that I am really proud of, but which never got published. Cryptology ePrint Archive, Report 2036/9999. http://eprint.iacr.org/2036/9999. 2036 (cf. p. 11).

[DS38] John Doe et Jane Smith. Your advisor finally helped you ... In : Conf2 proceedings. Sous la dir. de Who Knows. Thief, avr. 2038 (cf. p. 12).

[GPS06] S.D. Galbraith, K.G. Paterson et N.P. Smart. Pairings for Cryptographers. Cryptology ePrint Archive, Report 2006/165. https://eprint.iacr.org/2006/165. 2006 (cf. p. 23).

[KM15] Neal Koblitz et Alfred Menezes. The Random Oracle Model : A Twenty-Year Retrospective. Cryptology ePrint Archive, Report 2015/140. https://eprint.iacr.org/2015/140. 2015 (cf. p. 22).

[KPTZ13] Aggelos Kiayias, Stavros Papadopoulos, Nikos Triandopoulos et Thomas Zacharias. Delegatable pseudorandom functions and applications. In : 2013, p. 669-684 (cf. p. 24).

Table des figures

Liste des tableaux

List of Algorithms