Pixel Mask 4.0; ElGamal AME mit Passwortschutz

KIM TEREBA, 0232478543 University of Luxembourg, Luxembourg

Dieses Projekt stellt Pixel Mask 4.0 vor, eine Anwendung mit einem anamorphen Verschlüsselungssystem, das auf dem ElGamal-Public-Key-Kryptosystem basiert. Das Ziel des Projekts ist es, eine sichere Kommunikation mit plausibler Abstreitbarkeit zu ermöglichen, indem zwei verschiedene Nachrichten in einen einzigen Chiffretext eingebettet werden können. Je nachdem, welcher Schlüssel bei der Entschlüsselung verwendet wird, kann eine Schein- oder eine geheime Nachricht wiederhergestellt werden, während der Chiffretext von einer Standard-ElGamal-Verschlüsselung nicht zu unterscheiden ist.

Diese Implementierung wurde von Grund auf neu entwickelt, um die in früheren Versionen vorhandenen Einschränkungen hinsichtlich Leistung, Speicher und Benutzerfreundlichkeit zu verbessern. Das neue System basiert auf der Schwierigkeit des diskreten Logarithmusproblems[1] und wurde unter Verwendung einer bekannten 2048-Bit[2] sicheren Primzahl[3] konstruiert. Dies verleiht dem System eine starke mathematische Grundlage und gewährleistet gleichzeitig die Kompatibilität mit der Standard-ElGamal-Verschlüsselung[4]. Daher erscheinen die von Pixel Mask erstellten Chiffretexte in keiner Weise verändert oder verdächtig.

Die anamorphe Funktionalität funktioniert durch sorgfältige Steuerung der bei der Verschlüsselung verwendeten Zufälligkeit. Anstatt den ElGamal-Zufallswert durch Brute-Force-Angriffe oder das Ausprobieren vieler Zufallswerte zu ermitteln, generiert das System einen Pseudozufallswert unter Verwendung von AES im CBC-Modus. Dieser Generator[5] nimmt einen gemeinsamen Doppelschlüssel, einen Initialisierungsvektor und einen Zustandswert als Eingabe und erzeugt eine Zahl, die in die richtige Gruppenreihenfolge passt. Die geheime anamorphe Nachricht wird dann zu diesem pseudozufälligen Wert hinzugefügt, um einen endgültigen Exponenten zu erstellen, der die geheime Nachricht einbettet und gleichzeitig die Standard-ElGamal-Struktur beibehält. Folglich enthält der Chiffretext sowohl eine sichtbare Scheinbotschaft als auch eine versteckte geheime Nachricht, ohne dass sich sein Aussehen ändert.

Während der Entschlüsselung wird derselbe pseudozufällige Wert unter Verwendung der gemeinsamen Parameter neu erstellt. Sobald dieser Wert aus dem Chiffretext-Exponenten entfernt wurde, stellt der verbleibende Wert die versteckte Nachricht als diskreten Logarithmus dar. Um diese Nachricht effizient wiederherzustellen, wird der Baby-Step-Giant-Step-Algorithmus[6] verwendet. Dadurch entfällt die Notwendigkeit großer, vorab berechneter Nachschlagetabellen und der Speicherbedarf wird reduziert, während größere versteckte Nachrichten innerhalb einer gewählten Grenze wiederhergestellt werden können. Im Vergleich zu früheren Versionen ist diese Methode schneller, vorhersehbarer und leichter zu skalieren.

Nach umfangreichen Tests mit Ganzzahlverschlüsselung und Zeichen-zu-Ganzzahl-Konvertierungen unterstützt Pixel Mask 4.0 nun auch anamorphe Textnachrichten. Jedes Wort wird mithilfe einer Zeichen-zu-Ganzzahl-Zuordnung in eine Ganzzahl umgewandelt, Wort für Wort verschlüsselt und dann während der Entschlüsselung wieder zusammengesetzt. Aufgrund der gewählten Grenzen funktioniert dies derzeit nur für Wörter mit einer Zeichenlänge von weniger als 7. Als Nächstes gibt das System je nachdem, ob der Standard-Privatschlüssel oder der Doppelschlüssel verwendet wird, entweder die Täuschungs- oder die versteckte Nachricht preis.

Darüber hinaus verbessert das Projekt die Benutzerfreundlichkeit und Sicherheit auf Anwendungsebene. Der Passwortschutz beschränkt den Zugriff auf die Anwendung, wobei Passwörter sicher gehasht und lokal auf dem System des Benutzers gespeichert werden. Ein animierter Avatar namens Echo wurde hinzugefügt, um die Benutzeroberfläche ansprechender und freundlicher zu gestalten. Sein Erscheinungsbild passt sich dabei an verschiedene Anzeigemodi an. Echo ist zwar noch nicht interaktiv, bildet jedoch eine Grundlage für zukünftige KI-gestützte intelligente Assistenzfunktionen in der Anwendung.

Insgesamt zeigt Pixel Mask 4.0, dass anamorphe Verschlüsselung auf praktische, effiziente und benutzerfreundliche Weise implementiert werden kann. Durch die Kombination eines neu gestalteten ElGamal-basierten Schemas, der Generierung pseudozufälliger Werte, des Baby-Step-Giant-Step-Algorithmus und Verbesserungen der Benutzeroberfläche bietet das Projekt eine solide Plattform

Author's Contact Information: Kim Tereba, kim.tereba.001@student.uni.lu0232478543, University of Luxembourg, Esch-sur-Alzette, Luxembourg.

für plausible Abstreitbarkeit in der verschlüsselten Kommunikation. Zwar gibt es noch Raum für zukünftige Verbesserungen, wie zusätzliche Verschlüsselungsmethoden, praktische Dateiverwaltung, bessere Zeichenunterstützung und interaktive Hilfe, doch bietet diese Version eine starke Grundlage für die anamorphe Kryptografie in der Praxis.

References

[1] S. Agramunt-Puig, "Discrete logarithm problem and Diffie-Hellman key exchange," Medium, Nov. 23, 2020. Available at: https://sebastiaagramunt.medium.com/discrete-logarithm-problem-and-diffie-hellman-key-exchange-821a45202d26.

[2] T. Kivinen and M. Kojo, “More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE). Available at: https://www.rfc-editor.org/rfc/rfc3526page-3

[3] R. Code, "Safe primes and unsafe primes - Rosetta Code," Rosetta Code, Dec. 13, 2025. Available at: https://rosettacode.org/wiki/Safe$_p rimes_a nd_u nsaf e_p rimes$

[4] GeeksforGeeks, "ElGamal Encryption Algorithm," GeeksforGeeks, Nov. 11, 2018. Available at: https://www.geeksforgeeks.org/computer-networks/elgamal-encryption-algorithm/

[5] What is a generator, "What is a generator?," Cryptography Stack Exchange, May 15, 2014. Available at: https://crypto.stackexchange.com/questions/16196/what-is-a-generator

[6] "The Baby-Step-Giant-Step algorithm", M2-HCMC2023. Available at: https://www.mat.uniroma2.it/ geatti/HCMC2023/Lecture4.pdf