ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ
ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

"Ο Αλγόριθμος κρυπτογράφησης SM4 και οι λειτουργείες του"

ΟΝΟΜΑΤΕΠΩΝΥΜΟ ΦΟΙΤΗΤΗ: **Ιωάννης Π. Παπαγιάννης**

Α.Μ: **2707**

ΕΠΙΒΛΕΠΩΝ: **Παρασκευάς Κίτσος, Καθηγητής**

ΠΑΤΡΑ 2024

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή

Πάτρα, 11/11/2024

ΕΠΙΤΡΟΠΗ ΑΞΙΟΛΟΓΗΣΗΣ

1. Ιωάννης Τζήμας
2. Σωτήριος Χριστοδούλου
3. Παρασκευάς Κίτσος

Υπεύθυνη Δήλωση Φοιτητή

Βεβαιώνω ότι είμαι συγγραφέας αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επίσης βεβαιώνω ότι αυτή η εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για τη συγκεκριμένη εργασία.

Η έγκριση της διπλωματικής εργασίας από το Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Πανεπιστημίου Πελοποννήσου δεν υποδηλώνει απαραιτήτως και αποδοχή των απόψεων του συγγραφέα εκ μέρους του Τμήματος.

Περίληψη

Ο αλγόριθμος κρυπτογράφησης SM4 και οι λειτουργείες του

Ο αλγόριθμος SM4 είναι ένας αλγόριθμος που χρησιμοποιείται για την κρυπτογράφηση δεδομένων που προέρχεται από τα κινέζικο πρότυπο κρυπτογράφησης SM2,SM3 και SM4.

Ο αλγόριθμος SM4 είναι ένας block cipher αλγόριθμος μεγέθους 128 bit και μέγεθος κλειδιού 128 bit επίσης και χρησιμοποιείται κυρίως για κρυπτογράφηση δεδομένων και τη δημιουργία ψηφιακών υπογραφών.

Περιέχει 4 λειτουργείες:

- **Κρυπτογράφηση (Encryption)**
- **Αποκρυπτογράφηση (Decryption)**
- **Κυκλική αριστερά μετατόπιση (Circular Left Shift)**
- **Υπο-κλειδιά (SubKeys)**

Ο αλγόριθμος SM4 προσφέρει ασφάλεια και ταχύτητα στην κρυπτογράφηση δεδομένων και έχει ευρεία χρήση σε πολλές εφαρμογές τεχνολογίας και κρυπτογραφίας.

Abstract

The SM4 Block Cipher Algorithm and Its Modes of Operations

The SM4 algorithm is a cryptographic algorithm used for data encryption originating from the Chinese cryptographic standards SM2, SM3, and SM4.

The SM4 algorithm is a block cipher algorithm with a block size of 128 bits and a key size of 128 bits as well. It is primarily used for data encryption and digital signature generation.

It comprises four operations:

- **Encryption**
- **Decryption**
- **Circular Left Shift**
- **SubKeys**

The SM4 algorithm provides security and speed in data encryption and is widely used in various technology and cryptographic applications.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επιβλέπων καθηγητή μου Παρασκευά Κίτσο για την συνεργασία και τη συμβολή του στην διεκπεραίωση της ερευνητικής αυτής εργασίας καθώς και τις συμβουλές του που με βοήθησαν σημαντικά στην επίτευξη αυτής.

Περιεχόμενα

Εισαγωγή

Στην εποχή της ψηφιοποίησης και της διασύνδεσης, η ασφάλεια των υπολογιστικών συστημάτων αποτελεί ζωτικής σημασίας πτυχή που απαιτεί διαρκή εξέλιξη και προηγμένες τεχνολογικές λύσεις. Η κρυπτογραφία αποτελεί βασικό εργαλείο για την εξασφάλιση των δεδομένων και της επικοινωνίας σε διαδικτυακό περιβάλλον. Στο πλαίσιο αυτό, η παρούσα εργασία επικεντρώνεται στη μελέτη ενός σημαντικού κρυπτογραφικού αλγορίθμου, του αλγορίθμου SM4.

Στο πλαίσιο αυτής της εργασίας, θα πραγματοποιηθεί μια λεπτομερής μελέτη του αλγορίθμου SM4, καλύπτοντας τις βασικές λειτουργίες του, τα χαρακτηριστικά του, και τις εφαρμογές του στον τομέα της κρυπτογραφίας. Επιπλέον, θα εξεταστούν οι προηγμένες τεχνικές και οι πρόσφατες εξελίξεις στον αλγόριθμο, καθώς και η σημασία του για την ασφάλεια των ψηφιακών συστημάτων στο σύγχρονο κυβερνοχώρο. Τέλος, θα αναδειχθούν πιθανές μελλοντικές εξελίξεις και εφαρμογές του αλγορίθμου SM4 στο πλαίσιο μιας συνεχώς εξελισσόμενης κρυπτογραφικής τεχνολογίας.

Κεφάλαιο 1

1.1Εισαγωγή στα FPGA

Οι επαναπρογραμματιζόμενες Πύλες (Field Programmable Gate Arrays - FPGAs) αποτελούν ένα κλειδί για την υλοποίηση προηγμένων ψηφιακών συστημάτων. Τα FPGAs προσφέρουν μια ευέλικτη και προγραμματιζόμενη πλατφόρμα, η οποία επιτρέπει την υλοποίηση σύνθετων λογικών λειτουργιών και εφαρμογών μεγάλης κλίμακας με απίστευτη ταχύτητα και αποτελεσματικότητα.

Ένα FPGA είναι μια ψηφιακή ολοκληρωμένη πλατφόρμα που περιλαμβάνει ένα μεγάλο αριθμό λογικών πυλών και μνήμη που μπορούν να προγραμματιστούν για να υλοποιήσουν διάφορες λειτουργίες και η τεχνολογία τους αντιπροσωπεύει μια σημαντική πτυχή στον τομέα της ψηφιακής σχεδίασης και της ψηφιακής επεξεργασίας σήματος.

Τα FPGAs διαθέτουν μια ευέλικτη δομή που επιτρέπει στους σχεδιαστές να προσαρμόσουν το υλικό τους σύμφωνα με τις απαιτήσεις της εφαρμογής τους. Αυτό τα καθιστά ιδανικά για εφαρμογές όπου οι απαιτήσεις αλλάζουν συχνά ή όπου απαιτείται υψηλή επεξεργαστική ισχύς με χαμηλή καθυστέρηση.

*Η διαδικασία προγραμματισμού ενός FPGA γίνεται με τη χρήση γλώσσας περιγραφής υλικού (HDL – Hardware Description Language) π.χ. Verilog,VHDL κ.α.

1.2 Ιστορική αναδρομή

Τα FPGAs αναπτύχθηκαν για πρώτη φορά τη δεκαετία του '80. Αρχικά, οι πρώτες γενιές FPGA ήταν αρκετά περιορισμένες σε χωρητικότητα και ευελιξία σε σύγκριση με τις σημερινές. Με την πάροδο του χρόνου, τα FPGAs εξελίχθηκαν και έγιναν πολύ πιο ισχυρά και ευέλικτα, με αυξημένη δυνατότητα προγραμματισμού και ευρύτερη γκάμα χρήσεων.

1.3 Λειτουργείες των FPGA

- **Λογικός Προγραμματισμός**: Τα FPGAs μπορούν να προγραμματιστούν ώστε να εκτελέσουν διάφορες λογικές λειτουργίες, συμπεριλαμβανομένων πυλών, μεταγωγέων, και συνδυαστών, που μπορούν να υλοποιήσουν συνθήκες, αλγόριθμους, και άλλες λογικές λειτουργίες.

- **Ανάπτυξη Ψηφιακών Συστημάτων**: Οι σχεδιαστές χρησιμοποιούν τα FPGAs για να αναπτύξουν και να προσαρμόσουν ψηφιακά συστήματα όπως επεξεργαστές σήματος, συστήματα επικοινωνίας, και άλλα.

- **Προσομοίωση και Επιτάχυνση**: Τα FPGAs μπορούν να χρησιμοποιηθούν για την προσομοίωση και την επιτάχυνση εφαρμογών που απαιτούν υψηλή υπολογιστική ισχύ.

- **Εφαρμογές σε πραγματικό χρόνο**: Λόγω της υψηλής απόδοσης και της χαμηλής κατανάλωσης ισχύος, τα FPGAs χρησιμοποιούνται ευρέως σε εφαρμογές πραγματικού χρόνου όπως ρομποτική, ιατρική, και άλλες.

*Αυτή η ιστορική αναδρομή και οι βασικές λειτουργίες των FPGAs θα βοηθήσουν στην κατανόηση του ρόλου τους σε πολλούς τομείς, συμπεριλαμβανομένων και των κρυπτογραφικών εφαρμογών.

1.4 Επιπλέον στοιχεία FPGA

- **Παραμετροποίηση**: Τα FPGAs παρέχουν ευελιξία στην παραμετροποίηση των εσωτερικών δομών τους, όπως ο αριθμός των λογικών πυλών, η μνήμη, και άλλα, προσφέροντας έτσι εξαιρετικά προσαρμόσιμες λύσεις για διάφορες εφαρμογές.

- **Παράλληλη Επεξεργασία**: Λόγω της δομής τους, τα FPGAs μπορούν να εκτελέσουν παράλληλη επεξεργασία πολλών εργασιών ταυτόχρονα, βελτιώνοντας την απόδοση και την αποτελεσματικότητα των εφαρμογών τους.

- **Δικτύωση**: Ορισμένα FPGAs διαθέτουν ενσωματωμένα δίκτυα διασύνδεσης που τους επιτρέπουν να επικοινωνούν μεταξύ τους ή με άλλες συσκευές, προσφέροντας έτσι ευέλικτες λύσεις για διάφορες εφαρμογές δικτύωσης.

- **Υψηλή Απόδοση**: Τα FPGAs προσφέρουν υψηλή απόδοση και χαμηλή κατανάλωση ισχύος, καθιστώντας τα κατάλληλα για εφαρμογές που απαιτούν γρήγορη επεξεργασία και χαμηλή ενέργεια.

- **Ασφάλεια**: Κάποια FPGAs προσφέρουν ενσωματωμένες λειτουργίες ασφαλείας, όπως επιτήρηση του χρόνου εκτέλεσης και ανίχνευση ανωμαλιών, που μπορούν να βελτιώσουν την ασφάλεια του συστήματος που χρησιμοποιεί FPGAs.

- **Επέκταση**: Ορισμένα FPGAs διαθέτουν δυνατότητες επέκτασης μέσω επιπρόσθετων ενσωματωμένων πυρήνων ή εξωτερικών συσκευών, που επιτρέπουν την προσθήκη επιπλέον λειτουργικότητας στο σύστημα.

*Αυτά τα επιπλέον στοιχεία παρέχουν μια πιο πλήρη εικόνα των δυνατοτήτων και των εφαρμογών των FPGAs, καθιστώντας τα ένα εργαλείο με πολλές προοπτικές σε πολλούς τομείς της τεχνολογίας.

1.5 FPGA και ASIC

Τα ASICs (Application-Specific Integrated Circuits) αποτελούν άλλη μια κατηγορία ολοκληρωμένων πυκνοτήτων, διαφορετική από τα FPGAs. Η βασική διαφορά μεταξύ τους έγκειται στη φύση της προγραμματιζόμενης λογικής.

Στην περίπτωση των ASICs, οι λογικές λειτουργίες και η δομή τους ορίζονται κατά τη σχεδίαση τους και είναι αμετάβλητες κατά τη λειτουργία τους. Δηλαδή, τα ASICs κατασκευάζονται για να εκτελούν συγκεκριμένες λειτουργίες ή εφαρμογές, και ο προγραμματισμός τους είναι ανεπανόρθωτος μετά την παραγωγή τους.

Από την άλλη πλευρά, τα FPGAs είναι προγραμματιζόμενα, δηλαδή μπορούν να προγραμματιστούν για να εκτελέσουν διάφορες λογικές λειτουργίες. Οι χρήστες μπορούν να δημιουργήσουν τη δική τους λογική και να την "φορτώσουν" στο FPGA, προσαρμόζοντας έτσι τη λειτουργία του ανάλογα με τις απαιτήσεις της εφαρμογής τους.

Τα FPGAs και τα ASICs έχουν τα δικά τους πλεονεκτήματα και μειονεκτήματα, ανάλογα με τις απαιτήσεις και τις ανάγκες της εφαρμογής. Ωστόσο, υπάρχουν ορισμένοι λόγοι για τους οποίους σε ορισμένες περιπτώσεις τα FPGAs θεωρούνται προτιμότερα από τα ASICs:

- **Ευελιξία**: Τα FPGAs προσφέρουν μεγαλύτερη ευελιξία και δυνατότητα προσαρμογής σε νέες απαιτήσεις ή αλλαγές στις ανάγκες της εφαρμογής, καθώς μπορούν να

επαναπρογραμματιστούν. Αντίθετα, τα ASICs είναι σχεδιασμένα για συγκεκριμένες λειτουργίες και δεν μπορούν να αλλάξουν μετά την παραγωγή τους.

- **Χρόνος και Κόστος Ανάπτυξης**: Η ανάπτυξη ενός ASIC απαιτεί μεγάλο χρόνο και υψηλό κόστος, καθώς απαιτεί την κατασκευή ενός πρωτότυπου κυκλώματος και την παραγωγή προσαρμοσμένων ηλεκτρονικών κυκλωμάτων. Τα FPGAs, από την άλλη πλευρά, προσφέρουν σχεδόν άμεση ανάπτυξη, καθώς οι χρόνοι και τα κόστη που απαιτούνται για την προγραμματισμένη ανάπτυξη είναι σημαντικά μικρότερα.

- **Δυνατότητες Προσαρμογής**: Τα FPGAs μπορούν να προσαρμοστούν σε μεταβαλλόμενες απαιτήσεις ή νέες εκδόσεις του λογισμικού, χωρίς την ανάγκη για ανανέωση του υλικού. Αυτό τα καθιστά ιδανικά για περιβάλλοντα όπου οι απαιτήσεις αλλάζουν συχνά ή όπου απαιτείται γρήγορη ανταπόκριση σε νέες τεχνολογικές ανάγκες.

*Ωστόσο, παρά τα πλεονεκτήματα των FPGAs, τα ASICs παραμένουν πολύτιμα για εφαρμογές όπου απαιτείται υψηλή απόδοση, εξαιρετικά χαμηλή κατανάλωση ενέργειας ή όπου οι όγκοι παραγωγής είναι υψηλοί και μπορούν να δικαιολογήσουν το κόστος ανάπτυξης ενός ASIC.

Κεφάλαιο 2

2.1 Εισαγωγή στην ασφάλεια

Η ασφάλεια των υπολογιστικών συστημάτων αποτελεί ένα ζωτικό ζήτημα στις σύγχρονες εποχές. Καθώς οι υπολογιστές και τα δίκτυα ενσωματώνονται σε κάθε πτυχή της καθημερινής μας ζωής, η ασφάλεια των δεδομένων, των συστημάτων και των επικοινωνιών είναι κρίσιμες για τη διατήρηση της ιδιωτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών.

Η ασφάλεια των υπολογιστικών συστημάτων αφορά την προστασία των ψηφιακών πόρων από ανεπιθύμητη παρέμβαση, κακόβουλες επιθέσεις ή ακόμα και ατυχήματα. Αυτό μπορεί να περιλαμβάνει προληπτικά μέτρα για την αποτροπή εισβολών, τεχνικές για την ανίχνευση και αντίδραση σε επιθέσεις, καθώς και μέτρα ανάκτησης για την αντιμετώπιση των επιπτώσεων πιθανών παραβιάσεων.

Στον ψηφιακό κόσμο, η ασφάλεια αποτελεί σύνθετο και συνεχώς εξελισσόμενο πεδίο. Οι απειλές είναι ποικίλες και πολυδιάστατες, καθιστώντας αναγκαία την υιοθέτηση πολυεπίπεδων προσεγγίσεων για την αντιμετώπισή τους. Αυτό περιλαμβάνει τόσο τεχνικά μέτρα, όπως η κρυπτογράφηση και η προστασία του δικτύου, όσο και οργανωτικές πρακτικές, όπως η εκπαίδευση του προσωπικού και η ανάπτυξη πολιτικών ασφαλείας.

Η σημασία της ασφάλειας των υπολογιστικών συστημάτων είναι προφανής σε κάθε τομέα, από την κυβερνητική ασφάλεια και την οικονομία μέχρι την προσωπική ασφάλεια και την ασφάλεια των καταναλωτών. Με τη συνεχή εξέλιξη των τεχνολογιών και των απειλών, η ασφάλεια των υπολογιστικών συστημάτων παραμένει μια συνεχής πρόκληση που απαιτεί συνεχή επιδεξιότητα και προσοχή.

2.2 Μέθοδοι επίτευξης ασφάλειας

Η ασφάλεια των υπολογιστικών συστημάτων μπορεί να επιτευχθεί με διάφορους τρόπους και μεθόδους. Ορισμένοι από αυτούς περιλαμβάνουν:

- **Κρυπτογράφηση Δεδομένων**: Η κρυπτογράφηση χρησιμοποιείται για την προστασία των δεδομένων από μη εξουσιοδοτημένη πρόσβαση. Τα δεδομένα κρυπτογραφούνται πριν αποσταλούν μέσω δικτύου και αποκρυπτογραφούνται από τον παραλήπτη με τη χρήση κλειδιών κρυπτογράφησης.

- **Διαχείριση Πρόσβασης και Ταυτοποίησης**: Οι μέθοδοι ταυτοποίησης και ελέγχου πρόσβασης, όπως οι κωδικοί πρόσβασης, τα βιομετρικά στοιχεία και οι κάρτες πρόσβασης, μπορούν να χρησιμοποιηθούν για να εξασφαλίσουν ότι μόνο εξουσιοδοτημένα άτομα έχουν πρόσβαση στα συστήματα.

- **Ανίχνευση και Πρόληψη Εισβολών (IDS/IPS)**: Οι λύσεις IDS και IPS επιτρέπουν την παρακολούθηση και ανίχνευση κακόβουλων δραστηριοτήτων στα δίκτυα και τους υπολογιστές, καθώς και τη λήψη μέτρων για την πρόληψη ή αντιμετώπιση των επιθέσεων.

- **Αναβαθμίσεις και Ενημερώσεις Λογισμικού**: Η εγκατάσταση αναβαθμίσεων λογισμικού και η εφαρμογή ενημερώσεων ασφαλείας μπορεί να βοηθήσει στην επίλυση γνωστών ευπαθειών και αδυναμιών στο λογισμικό που μπορεί να εκμεταλλευτούν οι επιτιθέμενοι.

- **Φυσικά Μέτρα Ασφαλείας**: Φυσικά μέτρα όπως κλειδαριές, ανιχνευτές κίνησης και κάμερες ασφαλείας μπορούν να χρησιμοποιηθούν για την προστασία των φυσικών εγκαταστάσεων των υπολογιστικών συστημάτων.

- **Εκπαίδευση και Ευαισθητοποίηση**: Η εκπαίδευση του προσωπικού και η ευαισθητοποίησή του σχετικά με τις απειλές ασφαλείας είναι ουσιώδης. Η ενίσχυση της ασφάλειας απαιτεί τη συνειδητοποίηση των κινδύνων και την τήρηση πρακτικών ασφαλείας από όλους τους χρήστες.

*Η προστασία των υπολογιστικών συστημάτων απαιτεί ολοκληρωμένη προσέγγιση, συνδυάζοντας τεχνικά, οργανωτικά και ανθρώπινα μέτρα για την αντιμετώπιση των διαφόρων απειλών.

2.3 Επιθέσεις

Δυστυχώς, οι μέθοδοι που έχουν υλοποιηθεί για την επίτευξη της ασφάλειας, δε θα είχε χρειαστεί να υπάρξουν αν δεν υπήρχαν και οι επιθέσεις ή αλλιώς οι μέθοδοι υποκλοπής. Οι επιτιθέμενοι μπορούν να προσπαθήσουν να περάσουν τους αμυντικούς μηχανισμούς με διάφορους τρόπους, όπως:

- **Κοινωνική Μηχανική**: Οι επιτιθέμενοι μπορεί να χρησιμοποιήσουν την κοινωνική μηχανική για να πείσουν τους χρήστες να παρέχουν πληροφορίες ή να πραγματοποιήσουν δράσεις που θα ευνοήσουν την επίθεση, όπως η αποκάλυψη κωδικών πρόσβασης ή η εκτέλεση κακόβουλου λογισμικού.

- **Κακόβουλο Λογισμικό**: Οι επιτιθέμενοι μπορεί να χρησιμοποιήσουν κακόβουλο λογισμικό, όπως ιούς, τροϊανούς (trojans) ή κακόβουλα προγράμματα, για να

αποφύγουν τους αμυντικούς μηχανισμούς και να προσπεράσουν τα συστήματα ασφαλείας.

- **Εκμετάλλευση Ευπαθειών**: Οι επιτιθέμενοι μπορεί να αναζητήσουν και να εκμεταλλευτούν ευπαθείς σημεία στα υπολογιστικά συστήματα ή στο λογισμικό, όπως αδυναμίες ασφαλείας ή μη ενημερωμένο λογισμικό, για να προσπεράσουν τους αμυντικούς μηχανισμούς.

- **Αποφυγή Ανίχνευσης**: Οι επιτιθέμενοι μπορεί να προσπαθήσουν να αποφύγουν την ανίχνευση από τους μηχανισμούς IDS/IPS, χρησιμοποιώντας τεχνικές όπως η μηχανική συναρμολόγησης ή η κρυπτογράφηση της επικοινωνίας τους.

- **Επίθεση μέσω Δικτύου**: Οι επιτιθέμενοι μπορεί να εκτελέσουν επιθέσεις μέσω του δικτύου, όπως DDoS επιθέσεις ή επιθέσεις εκμετάλλευσης ευπαθειών σε δικτυακά πρωτόκολλα.

*Για να προστατευθούν από αυτούς τους τρόπους επίθεσης, οι οργανισμοί πρέπει να εφαρμόζουν ολοκληρωμένες πρακτικές ασφαλείας, περιλαμβανομένων της ενίσχυσης των αμυντικών μηχανισμών, της εκπαίδευσης του προσωπικού και της τήρησης των καλών πρακτικών ασφαλείας.

2.4 Αντιμετώπιση επιθέσεων

Η αντιμετώπιση των επιθέσεων στα υπολογιστικά συστήματα είναι ένας συνεχής και πολύπλευρος αγώνας. Με λίγα λόγια, επικρατεί μια κατάσταση διαρκή πολέμου μεταξύ διαφόρων παραγόντων που μπορούν να παρέμβουν στην λειτουργεία ενός υπολογιστή ή ενός δικτύου. Ευτυχώς, πάντως ,έχουν υλοποιηθεί μηχανισμοί αντιμετώπισης κακόβουλων επιθέσεων με τους οποίους μπορεί να επιτευχθεί η ορθή λειτουργεία ενός υπολογιστικού συστήματος ή δικτύου. Μερικοί από αυτούς είναι:

- **Ανίχνευση Επιθέσεων**: Η ανίχνευση επιθέσεων είναι ο πρώτος βασικός βήμα προς την αντιμετώπιση των επιθέσεων. Οι λύσεις IDS/IPS και άλλα εργαλεία ανίχνευσης

επιθέσεων παρακολουθούν την κίνηση στα δίκτυα και τους υπολογιστές για ανωμαλίες και κακόβουλες δραστηριότητες.

- **Ανάκτηση και Αποκατάσταση**: Αν ένα σύστημα έχει πληγεί από επίθεση, η ανάκτηση και η αποκατάσταση πρέπει να γίνει όσο το δυνατόν ταχύτερα. Αυτό περιλαμβάνει την επαναφορά των συστημάτων από αντίγραφα ασφαλείας, τη διόρθωση των ευπαθειών και την ανάκτηση των δεδομένων.

- **Εφαρμογή Προληπτικών Μέτρων**: Η προστασία από επιθέσεις πρέπει να αρχίσει από προληπτικά μέτρα, όπως η ενίσχυση των αμυντικών μηχανισμών, η ενημέρωση των λογισμικών, η εφαρμογή πολιτικών ασφαλείας και η εκπαίδευση των χρηστών.

- **Συνεργασία και Κοινοποίηση Πληροφοριών**: Η συνεργασία με άλλους οργανισμούς και την κοινοποίηση πληροφοριών σχετικά με επιθέσεις και κινδύνους μπορεί να βοηθήσει στην αντιμετώπισή τους και στην προστασία από μελλοντικές απειλές.

Συνολικά, η αντιμετώπιση των επιθέσεων απαιτεί ένα συνδυασμό τεχνολογικών, πρακτικών και ανθρώπινων μέτρων που να είναι συνεχώς ενημερωμένα και προσαρμοσμένα στις εξελίξεις του κυβερνοχώρου.

Κεφάλαιο 3

3.1 Εισαγωγή στους αλγόριθμους τμήματος

Οι αλγόριθμοι τμήματος είναι μια σημαντική κατηγορία αλγορίθμων που χρησιμοποιούνται ευρέως στην επιστήμη των υπολογιστών. Αυτοί οι αλγόριθμοι επικεντρώνονται στο να διαχειρίζονται και να επεξεργάζονται τμήματα δεδομένων με συγκεκριμένο τρόπο. Συνήθως, τα τμήματα δεδομένων αυτά αποτελούνται από μεγάλου μεγέθους σύνολα δεδομένων ή δεδομένα που παράγονται δυναμικά από πολλαπλές πηγές.

Οι αλγόριθμοι τμήματος είναι σημαντικοί για πολλές εφαρμογές, όπως η ανάλυση δεδομένων, η αναγνώριση προτύπων, η επεξεργασία σημάτων, η αναζήτηση πληροφοριών και η μηχανική μάθηση. Συχνά χρησιμοποιούνται σε προβλήματα όπου τα δεδομένα είναι πολύ μεγάλα και πολύπλοκα για να επεξεργαστούν από τα κλασικά αλγοριθμικά μοντέλα.

Τα κύρια χαρακτηριστικά των αλγορίθμων τμήματος περιλαμβάνουν τη δυνατότητα να επεξεργαστούν δεδομένα σε μικρά, ανεξάρτητα τμήματα, την ικανότητα προσαρμογής σε αλλαγές στα δεδομένα και την αποδοτικότητα στην επεξεργασία μεγάλων όγκων δεδομένων.

Οι αλγόριθμοι τμήματος αποτελούν ένα σημαντικό πεδίο έρευνας και ανάπτυξης στην επιστήμη των υπολογιστών και έχουν εφαρμογές σε πολλούς τομείς, από τη βιοπληροφορική και την ρομποτική μέχρι την ανάλυση δεδομένων και την τεχνητή νοημοσύνη. Η κατανόηση της λειτουργίας και της εφαρμογής των αλγορίθμων τμήματος είναι κρίσιμη για την ανάπτυξη νέων τεχνολογιών και εφαρμογών στον ψηφιακό κόσμο.

Οι αλγόριθμοι τμήματος λειτουργούν επεξεργαζόμενοι δεδομένα σε μικρά, αυτόνομα τμήματα, τα οποία συνήθως ονομάζονται "κομμάτια" ή "κεφάλαια". Αυτό επιτρέπει στους αλγορίθμους να εργάζονται παράλληλα σε διαφορετικά τμήματα των δεδομένων ή ακόμα και σε διαφορετικά σύνολα δεδομένων.

Ένα σημαντικό στοιχείο των αλγορίθμων τμήματος είναι η ικανότητά τους να διαχειρίζονται αποδοτικά μεγάλα σύνολα δεδομένων. Αντί να επεξεργάζονται ολόκληρο το σύνολο των δεδομένων σε μία μόνο φάση, διαχωρίζουν τα δεδομένα σε μικρότερα κομμάτια και εργάζονται με αυτά τα κομμάτια ξεχωριστά. Αυτή η διαδικασία ονομάζεται "διάσπαση" ή "διαίρεση" των δεδομένων.

Οι αλγόριθμοι τμήματος μπορούν να εφαρμοστούν σε πολλές εφαρμογές, συμπεριλαμβανομένης της αναζήτησης κειμένου, της επεξεργασίας εικόνας, της αναγνώρισης προτύπων και της ανάλυσης δεδομένων. Στην πράξη, η εφαρμογή αλγορίθμων τμήματος συνήθως επιτυγχάνεται μέσω παράλληλων υπολογιστικών διεργασιών ή υλικού ειδικά σχεδιασμένου για τον σκοπό αυτόν, όπως τα FPGA ή τα GPU (Graphics Processing Units).

Το βασικό πλεονέκτημα των αλγορίθμων τμήματος είναι η δυνατότητα παράλληλης επεξεργασίας των δεδομένων, η οποία οδηγεί σε αυξημένη απόδοση και αποτελεσματικότητα στην επίλυση προβλημάτων που απαιτούν επεξεργασία μεγάλων όγκων δεδομένων.

3.2 Παραδείγματα αλγορίθμων τμήματος

Υπάρχουν πολλοί αλγόριθμοι τμήματος που χρησιμοποιούνται σε διάφορες εφαρμογές. Ας δούμε μερικά παραδείγματα:

- **Αλγόριθμος K-Means**: Χρησιμοποιείται για ομαδοποίηση δεδομένων σε ομάδες (clusters) με βάση την ομοιότητά τους. Αυτός ο αλγόριθμος διαιρεί τα δεδομένα σε k ομάδες και στη συνέχεια επαναλαμβάνει τη διαδικασία, προσπαθώντας να βελτιώσει την ακρίβεια της ομαδοποίησης.

- **Αλγόριθμος PageRank**: Χρησιμοποιείται στην ανάλυση γράφων και την αξιολόγηση της σημαντικότητας των ιστοσελίδων στο Διαδίκτυο. Βασίζεται στην ιδέα ότι η σημαντικότητα μιας ιστοσελίδας καθορίζεται από τον αριθμό και τη σημασία των άλλων ιστοσελίδων που συνδέονται μαζί της.

- **Αλγόριθμος Apriori**: Χρησιμοποιείται στην εξόρυξη δεδομένων και την ανακάλυψη συσχετίσεων μεταξύ στοιχείων σε μια συλλογή δεδομένων. Ο αλγόριθμος εντοπίζει τα συχνά σύνολα αντικειμένων στα δεδομένα και χρησιμοποιεί αυτές τις πληροφορίες για να ανακαλύψει τις συσχετίσεις μεταξύ των δεδομένων.

- **Αλγόριθμος QuickSort**: Είναι ένας αλγόριθμος ταξινόμησης που χρησιμοποιείται για ταξινόμηση μιας λίστας στοιχείων. Ο αλγόριθμος QuickSort διαιρεί τη λίστα σε μικρότερα υποσύνολα, ταξινομεί κάθε υποσύνολο ξεχωριστά και στη συνέχεια συγχωνεύει τα υποσύνολα για να δημιουργήσει την τελική ταξινομημένη λίστα.

Αυτά είναι μερικά παραδείγματα αλγορίθμων τμήματος που χρησιμοποιούνται σε διάφορες εφαρμογές. Κάθε ένας από αυτούς τους αλγορίθμους έχει τα δικά του χαρακτηριστικά και εφαρμογές, ανάλογα με τις ανάγκες του προβλήματος που πρέπει να επιλυθεί.

4. Βιβλιογραφική Ανασκόπηση

4.1 FPGA

1. Brown, Stephen D., and Jonathan Rose. "Field-programmable gate arrays." *Springer Science & Business Media*, 2011.
2. Varghese, Jayaraman. "*FPGA prototyping by VHDL examples: Xilinx Spartan-3 version.*" John Wiley & Sons, 2008.
3. Lavin, César Augusto Martínez, and José María Drake Martínez. "Introduction to reconfigurable computing: architectures, algorithms, and applications." *Springer*, 2016.

4.2 Ασφάλεια Υπολογιστικών Συστημάτων

4. Stallings, William. "Cryptography and network security: principles and practice." Pearson, 2017.
5. Bishop, Matt. "Computer security: art and science." Pearson Education, 2018.
6. Anderson, Ross. "Security engineering: a guide to building dependable distributed systems." John Wiley & Sons, 2008.

4.3 Αλγόριθμοι Τμήματος

7. Cormen, Thomas H., et al. "Introduction to algorithms." MIT press, 2009.
8. Kleinberg, Jon, and Éva Tardos. "Algorithm design." Pearson Education India, 2006.
9. Skiena, Steven S. "The algorithm design manual." Springer Science & Business Media, 2008.

5. Πειραματικό /Ερευνητικό Μέρος

Στη συνέχεια θα δούμε τον κύριο σκοπό αυτής της ερευνητικής εργασίας ο οποίος είναι η ανάλυση του αλγορίθμου ασφαλείας SM4 καθώς και η επεξήγηση του χρησιμοποιώντας παραδειγματικό κώδικα.

Ο Αλγόριθμος Κρυπτογράφησης Πλαισίου SM4 και Οι Λειτουργίες του προσχέδιο-crypto-SM4-00

Περίληψη

Το παρόν έγγραφο περιγράφει τον συμμετρικό αλγόριθμο πλαισίου κρυπτογράφησης SM4 που δημοσιεύθηκε ως GB/T 32907-2016 από τον Οργανισμό Διοίκησης Εμπορικών Δραστηριοτήτων της Κίνας (OSCCA).

Κατάσταση Του Εγγράφου

Το παρόν προσχέδιο Internet υποβάλλεται σύμφωνα με τις πρόνοιες του BCP 78 και του BCP 79.

Τα Internet-Drafts είναι εργασιακά έγγραφα της Ομάδας Εργασίας Μηχανικών Internet (IETF). Σημειώστε ότι άλλες ομάδες μπορεί επίσης να διανέμουν εργασιακά έγγραφα ως Internet-Drafts. Η λίστα των τρεχουσών Internet-Drafts βρίσκεται στο http://datatracker.ietf.org/drafts/current/.

Τα Internet-Drafts είναι προσχέδια έγγραφα έγκυρα για έξι μήνες το πολύ και μπορούν να ενημερωθούν, αντικατασταθούν ή καταργηθούν από άλλα έγγραφα οποτεδήποτε. Είναι ανάρμοστο να χρησιμοποιούνται τα Internet-Drafts ως υλικό αναφοράς ή να αναφέρονται σε αυτά χωρίς τον χαρακτηρισμό "εργασία σε εξέλιξη."

Το παρόν προσχέδιο Internet θα λήξει στις 13 Μαρτίου 2018.

Κοινοποίηση Πνευματικών Δικαιωμάτων

5. 1. Εισαγωγή

Το SM4 [GBT.32907-2016] είναι ένα κρυπτογραφικό πρότυπο που εκδόθηκε από τον Οργανισμό Διοίκησης Εμπορικών Δραστηριοτήτων της Κίνας [OSCCA] ως εξουσιοδοτημένους κρυπτογραφικούς αλγόριθμους για χρήση εντός της Κίνας. Ο αλγόριθμος είναι διαθέσιμος για δημόσια χρήση.

Το SM4 είναι ένας συμμετρικός αλγόριθμος κρυπτογράφησης, συγκεκριμένα ένας αλγόριθμος πλαισίου κρυπτογράφησης, σχεδιασμένος για την κρυπτογράφηση δεδομένων.

Το παρόν έγγραφο δεν στοχεύει στην εισαγωγή ενός νέου αλγορίθμου, αλλά στο να παρέχει μια σαφή και ανοικτή περιγραφή του αλγορίθμου SM4 στα Αγγλικά, καθώς και να λειτουργήσει ως σταθερή αναφορά για έγγραφα του IETF που χρησιμοποιούν αυτόν τον αλγόριθμο.

Αν και το παρόν έγγραφο είναι παρόμοιο με το [SM4-En], το [SM4-En] είναι μια κειμενική μετάφραση του "SMS4" [SM4] που δημοσιεύτηκε το 2006, και το παρόν έγγραφο ακολουθεί το ενημερωμένο κείμενο και τη δομή του [GBT.32907-2016].

Οι ενότητες 1 έως 7 του παρόντος εγγράφου αντιστοιχούν εσκεμμένα στις αντίστοιχες ενότητες 1 έως 7 του προτύπου [GBT.32907-2016] για την ευκολία του αναγνώστη.

5.1.1 Ιστορία

Ο αλγόριθμος "SMS4" (το προηγούμενο όνομα του SM4) εφευρέθηκε από τον Shu-Wang Lu [LSW-Bio], πρωτοδημοσιεύθηκε για πρώτη φορά το 2003 ως μέρος του [GB.15629.11-2003], και στη συνέχεια δημοσιεύτηκε ανεξάρτητα το 2006 [SM4] από τον OSCCA. Επίσημα μετονομάστηκε σε "SM4" το 2012 στο [GMT-0002-2012] που δημοσιεύτηκε από τον OSCCA και τελικά καθιερώθηκε ως πρότυπο το 2016 ως Κινεζικό Εθνικό Πρότυπο (GB Standard) [GBT.32907-2016].

Αρχικά, το SMS4 δημιουργήθηκε για τη χρήση στην προστασία ασύρματων δικτύων [SM4], και είναι υποχρεωτικό στο Κινέζικο Εθνικό Πρότυπο για τα ασύρματα δίκτυα LAN WAPI (Wired Authentication and Privacy Infrastructure) [GB.15629.11-2003]. Υπήρξε πρόταση να υιοθετηθεί το SMS4 στο πρότυπο IEEE 802.11i, αλλά τελικά ο αλγόριθμος δεν περιλήφθηκε λόγω ανησυχιών για την εισαγωγή ανεργίας με υπάρχοντες κρυπτογραφικούς αλγορίθμους.

Το τελευταίο πρότυπο SM4 [GBT.32907-2016] προτάθηκε από τον OSCCA, καθιερώθηκε μέσω της TC 260 της Διοίκησης Προτύπων του Λαού της Λαϊκής Δημοκρατίας της Κίνας (SAC) και

συντάχθηκε από τα ακόλουθα άτομα στο Κέντρο Ερευνών Εγγυημένων Δεδομένων και Ασφάλειας Επικοινωνιών (DAS Center) της Κινεζικής Ακαδημίας Επιστημών, το Κέντρο Εμπορικής Κρυπτογραφικής Δοκιμής της Κίνας και την Ακαδημία Πληροφοριών & Τεχνολογίας του Πεκίνου (BAIST):

Shu-Wang Lu

Dai-Wai Li

Kai-Yong Deng

Chao Zhang

Peng Luo

Zhong Zhang

Fang Dong

Ying-Ying Mao

Zhen-Hua Liu

5. 1.2 Εφαρμογές

Ο SM4 (και ο SMS4) έχει ευρεία υλοποίηση σε υλικό [SM4-FPGA] [SM4-VLSI], λόγω του γεγονότος ότι αποτελεί τον μοναδικό συμμετρικό αλγόριθμο κρυπτογράφησης που έχει εγκριθεί από τον OSCCA για χρήση στην Κίνα.

Οο SM4 μπορεί να χρησιμοποιηθεί με πολλαπλές λειτουργίες (Δείτε την Ενότητα 8).

5. 1.3. Κρυπτανάλυση

Έχουν προσπαθηθεί διάφορες επιθέσεις εναντίον του SM4, όπως το [SM4-Analysis] [SM4-Linear], αλλά δεν υπάρχουν γνωστές εφικτές επιθέσεις κατά του αλγορίθμου SM4 μέχρι την δημοσίευση του παρόντος εγγράφου.

Ωστόσο, υπάρχουν ανησυχίες ασφαλείας όσον αφορά τις επιθέσεις μέσω πλευρικών καναλιών [SideChannel] όταν ο αλγόριθμος SM4 υλοποιείται σε ένα συγκεκριμένο συσκευή [SM4-Power].

Για παράδειγμα, το [SM4-Power] παρουσίασε μια επίθεση με τη μέτρηση της κατανάλωσης ισχύος της συσκευής. Μια επίθεση επιλογής κρυπτοκειμένου, υποθέτοντας μια σταθερή συσχέτιση μεταξύ των υποκλειδιών και της μάσκας δεδομένων, είναι σε θέση να ανακτήσει με επιτυχία τον γύρο κλειδιού. Όταν ο αλγόριθμος SM4 υλοποιείται σε υλικό, οι παράμετροι/κλειδιά ΘΑ ΠΡΕΠΕΙ να παράγονται τυχαία χωρίς σταθερή συσχέτιση.

Υπήρξαν βελτιώσεις στην υλοποίηση υλικού του SM4, όπως το [SM4-VLSI], που μπορεί να αντισταθεί σε τέτοιου είδους επιθέσεις.

Για τη βελτίωση της ασφάλειας της κρυπτογραφικής διαδικασίας του SM4, έχουν προταθεί ασφαλείς υλοποιήσεις λευκού κουτιού όπως το [SM4-WhiteBox]. Επίσης, έχουν προταθεί βελτιώσεις της ταχύτητας, όπως το [SM4-HiSpeed].

5. 2. Όροι και Ορισμοί

Οι λέξεις-κλειδιά "ΠΡΕΠΕΙ", "ΔΕΝ ΠΡΕΠΕΙ", "ΑΠΑΙΤΕΙΤΑΙ", "ΘΑ", "ΔΕΝ ΘΑ", "ΘΑ ΕΠΡΕΠΕ", "ΔΕΝ ΘΑ ΕΠΡΕΠΕ", "ΣΥΝΙΣΤΑΤΑΙ", "ΜΠΟΡΕΙ", και "ΠΡΟΑΙΡΕΤΙΚΟ" σε αυτό το έγγραφο πρέπει να ερμηνευθούν όπως περιγράφεται στο [RFC2119].

Οι ακόλουθοι όροι και ορισμοί ισχύουν για το παρόν έγγραφο:

- μήκος μπλοκ
- Το μήκος σε bits ενός μπλοκ μηνύματος.
- μήκος κλειδιού
- Το μήκος σε bits ενός κλειδιού.
- Αλγόριθμος επέκτασης κλειδιού
- Μια λειτουργία που μετατρέπει ένα κλειδί σε γύρο κλειδιού.
- Γύροι
- Ο αριθμός των επαναλήψεων που λειτουργεί η συνάρτηση γύρου.
- Γύρος κλειδιού
- Ένα κλειδί που χρησιμοποιείται σε κάθε γύρο του πλαισίου κρυπτογράφησης, προερχόμενο από το εισαγόμενο κλειδί, επίσης ονομάζεται υποκλειδί.
- Λέξη
- Μια ποσότητα 32 bits.
- S-κουτί

- Η λειτουργία S (υποκατάσταση) παράγει 8-bit εξόδο από 8-bit είσοδο, αναπαριστάται ως Sbox(.).

5. 3. Σύμβολα και Συντομεύσεις

S xor T

Λογική εξοριστική πύλη XOR δύο διανύσματων των 32 bit, S και T. Τα S και T θα έχουν πάντα τον ίδιο μήκος.

a <<< i

Κυκλική μετατόπιση 32 bit του a με i bits μετατοπισμένη προς τα αριστερά.

5. 4. Δομή Υπολογισμού

Ο αλγόριθμος SM4 είναι ένας blockcipher, με μέγεθος μπλοκ 128 bit και μήκος κλειδιού 128 bit.

Τόσο η κρυπτογράφηση όσο και η επέκταση του κλειδιού χρησιμοποιούν 32 γύρους ενός μη γραμμικού προγράμματος προγραμματισμού κλειδιού ανά μπλοκ. Κάθε γύρος επεξεργάζεται έναν από τους τέσσερις λέξεις των 32 bit που αποτελούν το μπλοκ.

Η δομή της κρυπτογράφησης και της αποκρυπτογράφησης είναι ταυτόσημες, εκτός από το γεγονός ότι το πρόγραμμα προγραμματισμού γύρου κλειδιού έχει την αντίστροφη του σειρά κατά την αποκρυπτογράφηση.

Χρησιμοποιώντας ένα S-box των 8 bit, χρησιμοποιεί μόνο λογική εξοριστική πύλη XOR, κυκλικές μετατοπίσεις bit και αναζητήσεις στο S-box για εκτέλεση.

5. 5. Κλειδί και Παράμετροι Κλειδιού

Το μήκος του κλειδιού κρυπτογράφησης είναι 128 bit, και αναπαρίσταται παρακάτω, όπου κάθε MK_i, (i = 0, 1, 2, 3) είναι μια λέξη.

MK = (MK_0, MK_1, MK_2, MK_3)

Το πρόγραμμα προγραμματισμού γύρου κλειδιού προέρχεται από το κλειδί κρυπτογράφησης, αναπαριστάται ως εξής όπου κάθε rk_i (i = 0, ..., 31) είναι μια λέξη:

(rk_0, rk_1, ... , rk_31)

Οι παράμετροι του συστήματος που χρησιμοποιούνται για την επέκταση του κλειδιού αναπαρίστανται ως FK, όπου κάθε FK_i (i = 0, ..., 3) είναι μια λέξη:

FK = (FK_0, FK_1, FK_2, FK_3)

Σταθερές παράμετροι που χρησιμοποιούνται για την επέκταση του κλειδιού αναπαρίστανται ως CK, όπου κάθε CK_i (i = 0, ..., 31) είναι μια λέξη:

CK = (CK_0, CK_1, ... , CK_31)

5. 6. Συνάρτηση Γύρου F

5.6.1 Δομή Παραμέτρων Γύρου

Δεδομένου του 128-bit εισόδου παρακάτω, όπου κάθε X_i είναι μια λέξη 32-bit:

(X_0, X_1, X_2, X_3)

Και το γύρο κλειδιού rk είναι μια λέξη 32-bit:

Η συνάρτηση γύρου F ορίζεται ως:

F(X_0, X_1, X_2, X_3, rk) = X_0 xor T(X_1 xor X_2 xor X_3 xor rk)

Η συνάρτηση μίξης T είναι μια αντιστρέψιμη συνάρτηση υποκατάστασης που εξάγει 32 bits από μια είσοδο των 32 bits.

Αποτελείται από ένα μη γραμμικό μετασχηματισμό του tau και γραμμικό μετασχηματισμό L.

T(.) = L(tau(.))

5.6.2 Ο μη γραμμικός μετασχηματισμός του tau

Ο tau αποτελείται από τέσσερα παράλληλα S-boxes.

Δεδομένου ενός 32-bit εισόδου A, όπου κάθε a_i είναι ένα 8-bit string:

A = (a_0, a_1, a_2, a_3)

Η έξοδος είναι ένα 32-bit B, όπου κάθε b_i είναι ένα 8-bit string:

B = (b_0, b_1, b_2, b_3)

Το B υπολογίζεται ως εξής:

(b_0, b_1, b_2, b_3) = tau(A)

ταυ(A) = (Sbox(a_0), Sbox(a_1), Sbox(a_2), Sbox(a_3))

Ο πίνακας αναζήτησης Sbox παρουσιάζεται εδώ:

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	D6	90	E9	FE	CC	E1	3D	B7	16	B6	14	C2	28	FB	2C	05
1	2B	67	9A	76	2A	BE	04	C3	AA	44	13	26	49	86	06	99
2	9C	42	50	F4	91	EF	98	7A	33	54	0B	43	ED	CF	AC	62
3	E4	B3	1C	A9	C9	08	E8	95	80	DF	94	FA	75	8F	3F	A6
4	47	07	A7	FC	F3	73	17	BA	83	59	3C	19	E6	85	4F	A8
5	68	6B	81	B2	71	64	DA	8B	F8	EB	0F	4B	70	56	9D	35
6	1E	24	0E	5E	63	58	D1	A2	25	22	7C	3B	01	21	78	87
7	D4	00	46	57	9F	D3	27	52	4C	36	02	E7	A0	C4	C8	9E
8	EA	BF	8A	D2	40	C7	38	B5	A3	F7	F2	CE	F9	61	15	A1
9	E0	AE	5D	A4	9B	34	1A	55	AD	93	32	30	F5	8C	B1	E3
A	1D	F6	E2	2E	82	66	CA	60	C0	29	23	AB	0D	53	4E	6F
B	D5	DB	37	45	DE	FD	8E	2F	03	FF	6A	72	6D	6C	5B	51
C	8D	1B	AF	92	BB	DD	BC	7F	11	D9	5C	41	1F	10	5A	D8
D	0A	C1	31	88	A5	CD	7B	BD	2D	74	D0	12	B8	E5	B4	B0
E	89	69	97	4A	0C	96	77	7E	65	B9	F1	09	C5	6E	C6	84
F	18	F0	7D	EC	3A	DC	4D	20	79	EE	5F	3E	D7	CB	39	48

Για παράδειγμα, η είσοδος "EF" θα παράγει μια έξοδο που διαβάζεται από τον πίνακα S-box στη σειρά E και στη στήλη F, δίνοντας το αποτέλεσμα Sbox(EF) = 84.

5.6.3 Η Γραμμική Υποκατάσταση L

Η έξοδος της μη γραμμικής συνάρτησης μετασχηματισμού του ταυ χρησιμοποιείται ως είσοδος στην γραμμική συνάρτηση μετατροπής Λ.

Δεδομένου του B, ενός 32-bit εισόδου:

Η Λ παράγει μια 32-bit έξοδο C:

C = L(B)

L(B) = B xor (B <<< 2) xor (B <<< 10) xor (B <<< 18) xor (B <<< 24)

5.7. Υπολογισμός

5.7.1 Κρυπτογράφηση SM4

Ο αλγόριθμος κρυπτογράφησης αποτελείται από 32 γύρους και 1 αντίστροφη μετασχηματισμό R.

Δεδομένου ενός 128-bit κειμένου απλού κειμένου, όπου κάθε X_i είναι μια λέξη 32-bit:

(X_0, X_1, X_2, X_3)

Η έξοδος είναι ένα 128-bit κρυπτοκείμενο, όπου κάθε Y_i είναι μια λέξη 32-bit:

(Y_0, Y_1, Y_2, Y_3)

Κάθε γύρο κλειδιού ορίζεται ως rk_i, όπου κάθε rk_i είναι μια λέξη 32-bit και i = 0, 1, 2, ..., 31.

α. 32 γύροι υπολογισμού

i = 0, 1, ..., 31

X_{i+4} = F(X_i, X_{i+1}, X_{i+2}, X_{i+3}, rk_i)

β. αντίστροφη μετατροπή

(Y_0, Y_1, Y_2, Y_3) = R(X_32, X_33, X_34, X_35)

R(X_32, X_33, X_34, X_35) = (X_35, X_34, X_33, X_32)

Παρακαλώ ανατρέξτε στην Ενότητα 12 για ένα δείγμα υπολογισμού.

5.7.2 Αποκρυπτογράφηση SM4

Η αποκρυπτογράφηση ακολουθεί ένα ταυτόσημο διαδικαστικό όπως η κρυπτογράφηση, με τη μοναδική διαφορά στη σειρά της ακολουθίας των κλειδιών του γύρου.

Κατά τη διάρκεια της αποκρυπτογράφησης, η ακολουθία των κλειδιών του γύρου είναι:

(rk_31, rk_30, ..., rk_0)

5.7.3 SM4 Διαδικασία Επέκτασης Κλειδιού

Τα κλειδιά γύρου που χρησιμοποιούνται κατά την κρυπτογράφηση προέρχονται από το κλειδί κρυπτογράφησης.

Ειδικότερα, δεδομένου του κλειδιού κρυπτογράφησης MK, όπου κάθε MK_i είναι μια λέξη 32-bit:

MK = (MK_0, MK_1, MK_2, MK_3)

Κάθε κλειδί γύρου rk_i δημιουργείται ως εξής, όπου i = 0, 1, ..., 31.

(K_0, K_1, K_2, K_3) = (MK_0 xor FK_0, MK_1 xor FK_1, MK_2 xor FK_2, MK_3 xor FK_3)

rk_i = K_{i + 4}

K_{i + 4} = K_i xor T' (K_{i + 1} xor K_{i + 2} xor K_{i + 3} xor CK_i)

Δεδομένου ότι το κλειδί αποκρυπτογράφησης είναι ταυτόσημο με το κλειδί κρυπτογράφησης, τα κλειδιά γύρου που χρησιμοποιούνται στη διαδικασία αποκρυπτογράφησης προέρχονται από το κλειδί αποκρυπτογράφησης μέσω της ίδιας διαδικασίας με αυτήν κατά την κρυπτογράφηση.

5.7.3.1 Η συνάρτηση μετασχηματισμού T'

Η συνάρτηση μετασχηματισμού T' δημιουργείται από το T αντικαθιστώντας τη γραμμική συνάρτηση μετασχηματισμού L με τη L'. L'(B) = B xor (B <<< 13) xor (B <<< 23)

5.7.3.2 Συστημική παράμετρος FK

Συστημική παράμετρος FK δίνεται σε εξαδεκαδική σημειολογία:

FK_0 = A3B1BAC6 FK_1 = 56AA3350 FK_2 = 677D9197 FK_3 = B27022DC

5.7.3.3 Οι σταθερές παράμετροι CK

Η μέθοδος για την ανάκτηση τιμών από τη σταθερή παράμετρο CK είναι η ακόλουθη:

Έστω ότι ck_{i, j} είναι το j-th byte (i = 0, 1, ..., 31; j = 0, 1, 2, 3) του CK_i.

Επομένως, κάθε ck_{i, j} είναι ένα 8-bit string, και κάθε CK_i μια λέξη 32-bit.

CK_i = (ck_{i, 0}, ck_{i, 1}, ck_{i, 2}, ck_{i, 3})

ck_{i, j} = (4i + j) x 7 (mod 256)

Οι τιμές της σταθερής παραμέτρου CK_i, (i = 0, 1, ..., 31), σε εξαδεκαδική μορφή, είναι:

CK_0 = 00070E15

CK_1 = 1C232A31

CK_2 = 383F464D

CK_3 = 545B6269

CK_4 = 70777E85

CK_5 = 8C939AA1

CK_6 = A8AFB6BD

CK_7 = C4CBD2D9

CK_8 = E0E7EEF5

CK_9 = FC030A11

CK_10 = 181F262D

CK_11 = 343B4249

CK_12 = 50575E65

CK_13 = 6C737A81

CK_14 = 888F969D

CK_15 = A4ABB2B9

CK_16 = C0C7CED5

CK_17 = DCE3EAF1

CK_18 = F8FF060D

CK_19 = 141B2229

CK_20 = 30373E45

CK_21 = 4C535A61

CK_22 = 686F767D

CK_23 = 848B9299

CK_24 = A0A7AEB5

CK_25 = BCC3CAD1

CK_26 = D8DFE6ED

CK_27 = F4FB0209

CK_28 = 10171E25

CK_29 = 2C333A41

CK_30 = 484F565D

CK_31 = 646B7279

5.8. Οι λειτουργικές καταστάσεις

Αυτό το έγγραφο καθορίζει πολλαπλές λειτουργικές καταστάσεις για τον αλγόριθμο blockcipher SM4. Οι λειτουργικές καταστάσεις CBC (Cipher Block Chaining), ECB (Electronic CodeBook), CFB (Cipher FeedBack), OFB (Output FeedBack) και CTR (Counter) καθορίζονται στο [NIST.SP.800-38A] και χρησιμοποιούνται με τον αλγόριθμο SM4 στις επόμενες ενότητες.

5. 8.1 Μεταβλητές και Βασικά Στοιχεία

Παρακάτω ορίζουμε:

SM4Encrypt (P, K)

Ο αλγόριθμος SM4 που κρυπτογραφεί το κείμενο απλού κειμένου P με το κλειδί K, όπως περιγράφεται στην Ενότητα 7.1

SM4Decrypt(C, K)

Ο αλγόριθμος SM4 που αποκρυπτογραφεί το κρυπτοκείμενο C με το κλειδί K, όπως περιγράφεται στην Ενότητα 7.2

b

Το μέγεθος του μπλοκ σε bits, ορισμένο ως 128 για τον αλγόριθμο SM4

P_j

Το j-οστό μπλοκ της αλφαριθμητικής P κρυπτοκειμένου

C_j

Το j-οστό μπλοκ της αλφαριθμητικής C κρυπτοκειμένου

NBlocks(B, b)

Ο αριθμός των μπλοκ μεγέθους b-bits στην αλφαριθμητική B

IV

Διανυσματικός παράγοντας αρχικοποίησης

LSB(b, S)

Τα λιγότερο σημαντικά b bits της αλφαριθμητικής S

MSB(b, S)

Τα περισσότερο σημαντικά b bits της αλφαριθμητικής S

5. 8.2 Διανυσματικός Παράγοντας Αρχικοποίησης

Οι λειτουργικές καταστάσεις CBC, CFB και OFB απαιτούν ένα επιπρόσθετο είσοδο στη διαδικασία κρυπτογράφησης, που ονομάζεται διανυσματικός παράγοντας αρχικοποίησης (IV). Το ίδιο IV χρησιμοποιείται τόσο στην είσοδο της κρυπτογράφησης όσο και στην αποκρυπτογράφηση του αντίστοιχου κρυπτοκειμένου.

Το IV ΠΡΕΠΕΙ να πληροί τις ακόλουθες απαιτήσεις για την ασφάλεια:

α) τις Λειτουργικές καταστάσεις CBC, CFB. Το IV για μια συγκεκριμένη εκτέλεση πρέπει να είναι απρόβλεπτο.

β) τη Λειτουργική κατάσταση OFB. Κάθε εκτέλεση πρέπει να δίνεται ένα μοναδικό IV.

5.8.3 Αλγόριθμος SM4-ECB

Στον αλγόριθμο SM4-ECB, χρησιμοποιείται το ίδιο κλειδί για να δημιουργηθεί μια σταθερή αντιστοίχιση για ένα μπλοκ κειμένου σε ένα μπλοκ κρυπτοκειμένου, πράγμα που σημαίνει ότι ένα συγκεκριμένο μπλοκ κειμένου πάντα κρυπτογραφείται στο ίδιο μπλοκ κρυπτοκειμένου. Όπως περιγράφεται στο [NIST.SP.800-38A], αυτή η λειτουργία θα πρέπει να αποφεύγεται αν αυτή η ιδιότητα είναι μη επιθυμητή.

Αυτή η λειτουργία απαιτεί το κείμενο εισόδου να είναι πολλαπλάσιο του μεγέθους του μπλοκ, το οποίο στην περίπτωση του SM4 είναι 128 bits. Επιπλέον, επιτρέπει την υπολογισμό πολλαπλών μπλοκ παράλληλα.

5.8.3.1 Κρυπτογράφηση SM4-ECB

Είσοδοι: ο P, απλό κείμενο, η μήκος πρέπει να είναι πολλαπλάσιο του b ο K, κλειδί κρυπτογράφησης SM4 128 bit Έξοδος: ο C, κρυπτοκείμενο, το μήκος είναι πολλαπλάσιο του b Το C ορίζεται ως εξής. n = NBlocks(P, b) για i = 1 έως n C_i = SM4Encrypt(P_i, K) τέλος για C = C_1 || ... || C_n

5.8.3.2 Αποκρυπτογράφηση SM4-ECB

Είσοδοι:

το C, κρυπτοκείμενο, το μήκος πρέπει να είναι πολλαπλάσιο του b

το K, κλειδί κρυπτογράφησης SM4 128 bit

Έξοδος:

το P, απλό κείμενο, το μήκος είναι πολλαπλάσιο του b

Το P ορίζεται ως εξής.

n = NBlocks(C, b)

for i = 1 to n

P_i = SM4Decrypt(C_i, K)

end for

P = P_1 || ... || P_n

5.8.4 Αλγόριθμος SM4-CBC

Το SM4-CBC είναι παρόμοιο με το SM4-ECB στο ότι το αρχικό απλό κείμενο πρέπει να είναι πολλαπλάσιο του μεγέθους του τμήματος, το οποίο είναι 128 bits στο SM4. Το SM4-CBC απαιτεί μια επιπλέον είσοδο, το Initialization Vector (IV), το οποίο πρέπει να είναι απρόβλεπτο για μια συγκεκριμένη εκτέλεση της διαδικασίας κρυπτογράφησης.

Καθώς η κρυπτογράφηση CBC βασίζεται σε μια κρυπτογράφηση που εξαρτάται από τα αποτελέσματα της προηγούμενης λειτουργίας, δεν είναι δυνατή η παραλληλοποίηση της διαδικασίας.

Ωστόσο, για την αποκρυπτογράφηση, καθώς τα τμήματα κρυπτοκειμένου είναι ήδη διαθέσιμα, είναι δυνατή η παράλληλη αποκρυπτογράφηση CBC.

5.8.4.1 Κρυπτογράφηση SM4-CBC

Είσοδοι:

το P, απλό κείμενο, το μήκος πρέπει να είναι πολλαπλάσιο του b

το K, SM4 128-bit κλειδί κρυπτογράφησης

το IV, 128-bit, απρόβλεπτο, διάνυσμα αρχικοποίησης

Έξοδος:

το C, κρυπτοκείμενο, το μήκος είναι πολλαπλάσιο του b

Το C ορίζεται ως εξής.

n = NBlocks(P, b)

C_1 = SM4Encrypt(P_1 xor IV, K)

for i = 2 to n

C_i = SM4Encrypt(P_i xor C_{i - 1}, K)

end for

C = C_1 || ... || C_n

5.8.4.2 Αποκρυπτογράφηση SM4-CBC

Εισόδοι:

το C, κρυπτοκείμενο, το μήκος πρέπει να είναι πολλαπλάσιο του b

το K, SM4 128-bit κλειδί κρυπτογράφησης

το IV, 128-bit, απρόβλεπτο, διάνυσμα αρχικοποίησης

Έξοδος:

το P, απλό κείμενο, το μήκος είναι πολλαπλάσιο του b

Το P ορίζεται ως εξής.

n = NBlocks(C, b)

P_1 = SM4Decrypt(C_1, K) xor IV

for i = 2 to n

P_i = SM4Decrypt(C_i, K) xor C_{i - 1}

end for

P = P_1 || ... || P_n

5.8.5 Αλγόριθμος SM4-CFB

Ο SM4-CFB βασίζεται στο ανατροφοδότη που παρέχεται από διαδοχικά τμήματα κρυπτοκειμένου για να δημιουργήσει μπλοκ εξόδου. Το δοθέν απλό κείμενο πρέπει να είναι πολλαπλάσιο του μεγέθους του μπλοκ.

Παρόμοια με το SM4-CBC, το SM4-CFB απαιτεί ένα IV που είναι απρόβλεπτο για μια συγκεκριμένη εκτέλεση της διαδικασίας κρυπτογράφησης.

Το SM4-CFB επιπλέον επιτρέπει την ορισμό ενός θετικού ακεραίου παραμέτρου s, που είναι μικρότερη ή ίση με το μέγεθος του μπλοκ, για να καθορίσει το μέγεθος κάθε τμήματος δεδομένων. Το ίδιο μέγεθος τμήματος πρέπει να χρησιμοποιηθεί στην κρυπτογράφηση και αποκρυπτογράφηση.

Στο SM4-CFB, αφού το μπλοκ εισόδου σε κάθε μπροστινή συνάρτηση κρυπτογράφησης εξαρτάται από την έξοδο του προηγούμενου μπλοκ (εκτός του πρώτου που εξαρτάται από το IV), η κρυπτογράφηση δεν μπορεί να παραλληλοποιηθεί. Ωστόσο, η αποκρυπτογράφηση μπορεί να παραλληλοποιηθεί.

5.8.5.1 Παραλλαγές SM4-CFB

Ο SM4-CFB λαμβάνει έναν ακέραιο s για να καθορίσει το μέγεθος του τμήματος στις διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης του. Ορίζουμε τις ακόλουθες παραλλαγές του SM4-CFB για διάφορα s:

SM4-CFB-1, η λεγόμενη κατάσταση 1-bit του SM4-CFB, όπου το s ορίζεται σε 1.

SM4-CFB-8, η λεγόμενη κατάσταση 8-bit του SM4-CFB, όπου το s ορίζεται σε 8.

SM4-CFB-64, η λεγόμενη κατάσταση 64-bit του SM4-CFB, όπου το s ορίζεται σε 64.

SM4-CFB-128, η λεγόμενη κατάσταση 128-bit του SM4-CFB, όπου το s ορίζεται σε 128.

5.8.5.2 Κρυπτογράφηση SM4-CFB

Είσοδοι:

το P#, το κείμενο προς κρυπτογράφηση, το μήκος πρέπει να είναι πολλαπλάσιο του s

το K, κλειδί κρυπτογράφησης SM4 128-bit

το IV, 128-bit, μη προβλέψιμο, διανυσματικός αρχικοποίησης

το s, ένας ακέραιος 1 <= s <= b που καθορίζει το μέγεθος του τμήματος

Έξοδος:

το C#, κρυπτοκείμενο, το μήκος είναι πολλαπλάσιο του s

Το C# ορίζεται ως εξής.

n = NBlocks(P#, s)

I_1 = IV

for i = 2 to n

I_i = LSB(b - s, I_{i - 1}) || C#_{j - 1}

end for

for i = 1 to n

O_j = SM4Encrypt(I_i, K)

end for

for i = 1 to n

C#_i = P#_1 xor MSB(s, O_j)

end for

C# = C#_1 || ... || C#_n

5.8.5.3 Αποκρυπτογράφηση SM4-CFB

Είσοδοι:

το C#, κρυπτοκείμενο, το μήκος πρέπει να είναι πολλαπλάσιο του s

το K, κλειδί κρυπτογράφησης SM4 128-bit

το IV, 128-bit, μη προβλέψιμο, διανυσματικός αρχικοποίησης

το s, ένας ακέραιος 1 <= s <= b που καθορίζει το μέγεθος του τμήματος

Έξοδος:

το P#, κείμενο, το μήκος είναι πολλαπλάσιο του s

Το P# ορίζεται ως εξής.

n = NBlocks(P#, s)

I_1 = IV

for i = 2 to n

I_i = LSB(b - s, I_{i - 1}) || C#_{j - 1}

end for

for i = 1 to n

O_j = SM4Encrypt(I_i, K)

end for

for i = 1 to n

P#_i = C#_1 xor MSB(s, O_j)

end for

P# = P#_1 || ... || P#_n

5.8.6 Αλγόριθμος SM4-OFB

Το SM4-OFB είναι η εφαρμογή του αλγορίθμου SM4 μέσω της λειτουργίας Έξοδου Ανατροφοδότησης. Αυτή η λειτουργία απαιτεί να είναι μοναδικό το αρχικοποιητής (IV), δηλαδή ο IV ΠΡΕΠΕΙ να είναι μοναδικός για κάθε εκτέλεση για ένα κλειδί εισόδου. Το OFB δεν απαιτεί το κείμενο εισόδου να είναι πολλαπλάσιο του μεγέθους του τετραγωνικού μπλοκ.

Στο OFB, οι διαδικασίες για την κρυπτογράφηση και αποκρυπτογράφηση είναι πανομοιότυπες. Δεδομένου ότι κάθε λειτουργία κρυπτογράφησης (εκτός της πρώτης) εξαρτάται από προηγούμενα αποτελέσματα, και οι δύο διαδικασίες δεν μπορούν να παραλληλοποιηθούν. Ωστόσο, γνωρίζοντας έναν γνωστό IV, θα μπορούσαν να δημιουργηθούν τα τμήματα εξόδου πριν την εισαγωγή του κειμένου (κρυπτογράφηση) ή του κρυπτοκειμένου (αποκρυπτογράφηση).

5.8.6.1 Κρυπτογράφηση SM4-OFB

Είσοδοι:

ο P, το απλό κείμενο, αποτελούμενο από (n - 1) μπλοκ του μεγέθους b, με το τελευταίο μπλοκ P_n μεγέθους 1 <= u <= b

ο K, κλειδί κρυπτογράφησης SM4 128 bit

ο IV, ένα nonce (μοναδική τιμή για κάθε εκτέλεση ανά δεδομένο κλειδί)

Έξοδος:

ο C, κρυπτοκείμενο, αποτελούμενο από (n - 1) μπλοκ του μεγέθους b, με το τελευταίο μπλοκ C_n μεγέθους 1 <= u <= b

Το C ορίζεται ως εξής.

n = NBlocks(P, b)

I_1 = IV

for i = 1 to (n - 1)

O_i = SM4Encrypt(I_i)

I_{i + 1} = O_i

end for

for i = 1 to (n - 1)

C_i = P_i xor O_i

end for

C_n = P_n xor MSB(u, O_n)

C = C_1 || ... || C_n

5.8.6.2 Αποκρυπτογράφηση SM4-OFB

Είσοδοι:

ο C, το κρυπτοκείμενο, αποτελούμενο από (n - 1) μπλοκ του μεγέθους b, με το τελευταίο μπλοκ C_n μεγέθους 1 <= u <= b

ο K, κλειδί κρυπτογράφησης SM4 128 bit

ο IV, το nonce που χρησιμοποιήθηκε κατά την κρυπτογράφηση

Έξοδος:

ο P, το απλό κείμενο, αποτελούμενο από (n - 1) μπλοκ του μεγέθους b, με το τελευταίο μπλοκ P_n μεγέθους 1 <= u <= b

Το P ορίζεται ως εξής.

n = NBlocks(C, b)

I_1 = IV

for i = 1 to (n - 1)

O_i = SM4Encrypt(I_i)

I_{i + 1} = O_i

end for

for i = 1 to (n - 1)

P_i = C_i xor O_i

end for

P_n = C_n xor MSB(u, O_n)

P = P_1 || ... || P_n

5.8.7 Αλγόριθμος SM4-CTR

Το SM4-CTR είναι μια υλοποίηση ενός ρεύματος κρυπτογράφησης μέσω μιας πρωταρχικής κρυπτογραφίας μπλοκ. Δημιουργεί ένα "ρεύμα κλειδιών" που χρησιμοποιούνται για να κρυπτογραφήσουν διαδοχικά μπλοκ, με το ρεύμα κλειδιών που δημιουργείται από το κλειδί εισόδου, ένα nonce (το IV) και ένα μετρητή που αυξάνεται κατά μία μονάδα. Ο μετρητής μπορεί να είναι οποιαδήποτε ακολουθία που δεν επαναλαμβάνεται μέσα στο μέγεθος του μπλοκ. Και οι δύο διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης SM4-CTR μπορούν να παραλληλοποιηθούν, ενώ είναι επίσης δυνατή η τυχαία πρόσβαση.

5.8.7.1 Κρυπτογράφηση SM4-CTR

Τα δεδομένα εισόδου είναι τα ακόλουθα:

Το P, το κείμενο προς κρυπτογράφηση, που αποτελείται από (n - 1) μπλοκ του μεγέθους b, με το τελευταίο μπλοκ P_n μεγέθους 1 <= u <= b

Το K, το SM4 128-bit κλειδί κρυπτογράφησης

Το IV, ένα nonce (μοναδική τιμή για κάθε εκτέλεση για ένα δεδομένο κλειδί)

Το T, μια ακολουθία μετρητών από το T_1 μέχρι το T_n

Το αποτέλεσμα είναι το C, το κρυπτογραφημένο κείμενο, το οποίο αποτελείται από (n - 1) μπλοκ του μεγέθους b, με το τελευταίο μπλοκ C_n μεγέθους 1 <= u <= b. Το C καθορίζεται ως εξής:

n = NBlocks(P, b)

for i = 1 to n

O_i = SM4Encrypt(T_i)

end for

for i = 1 to (n - 1)

C_i = P_i xor O_i

end for

C_n = P_n xor MSB(u, O_n)

C = C_1 || ... || C_n

5.8.7.2 Αποκρυπτογράφηση SM4-CTR

n = NBlocks(C, b)

for i = 1 to n

O_i = SM4Encrypt(T_i)

end for

for i = 1 to (n - 1)

P_i = C_i xor O_i

end for

P_n = C_n xor MSB(u, O_n)

C = C_1 || ... || C_n

5.9. Αναγνωριστικό αντικειμένου

Το αναγνωριστικό αντικειμένου για το SM4 είναι η τιμή "1.2.156.10197.1.104", όπως καθορίζεται στο [GMT-0006-2012].

5.10. Θέματα-Ζητήματα ασφαλείας

- Τα προϊόντα και οι υπηρεσίες που χρησιμοποιούν κρυπτογράφηση ελέγχονται από το OSCCA [OSCCA]; πρέπει να εγκριθούν ή να πιστοποιηθούν ρητά από το OSCCA προτού επιτραπεί η πώλησή τους ή η χρήση τους στην Κίνα.

- Το SM4 [GBT.32907-2016] είναι ένας blockcipher που πιστοποιήθηκε από το OSCCA [OSCCA]. Δεν παρέχεται επίσημη απόδειξη ασφαλείας. Δεν υπάρχουν γνωστές εφικτές επιθέσεις κατά του αλγορίθμου SM4 μέχρι τη δημοσίευση του παρόντος εγγράφου. Ωστόσο, υπάρχουν ανησυχίες ασφαλείας σχετικά με επιθέσεις από πλευρικά κανάλια, όταν ο αλγόριθμος SM4 εφαρμόζεται σε μια συσκευή [SM4-Power]. Για παράδειγμα, [SM4-Power] παρουσίασε μια επίθεση μέσω της μέτρησης της κατανάλωσης ενέργειας της συσκευής. Μια επίθεση επιλεγμένου κρυπτοκειμένου, υποθέτοντας μια σταθερή συσχέτιση μεταξύ των υποκλειδιών και της μάσκας δεδομένων, μπορεί να ανακτήσει επιτυχώς τον γύρο κλειδιού. Όταν ο αλγόριθμος SM4 εφαρμόζεται σε υλικό, οι παράμετροι/κλειδιά ΠΡΕΠΕΙ να δημιουργούνται τυχαία χωρίς σταθερή συσχέτιση.

- Το SM4 είναι ένας συμμετρικός αλγόριθμος blockcipher με μήκος κλειδιού 128 bits. Θεωρείται ως εναλλακτική λύση στο AES-128 [NIST.FIPS.197].

- Ο SM4-CFB: Ο λειτουργικός τρόπος OFB απαιτεί ένα μοναδικό IV για κάθε μήνυμα που ποτέ δεν έχει κρυπτογραφηθεί με το συγκεκριμένο κλειδί. Αν, αντίθετα με αυτήν την απαίτηση, το ίδιο IV χρησιμοποιηθεί για την κρυπτογράφηση περισσότερων από ένα μηνύματα, τότε η εμπιστευτικότητα αυτών των μηνυμάτων μπορεί να κινδυνεύσει. Ειδικότερα, εάν ένα μπλοκ κειμένου από οποιοδήποτε από αυτά τα μηνύματα είναι γνωστό, ας πούμε, το j-th μπλοκ κειμένου, τότε το j-th αποτέλεσμα της λειτουργίας κρυπτογράφησης προς τα εμπρός μπορεί να προσδιοριστεί εύκολα από το j-th μπλοκ κρυπτοκειμένου του μηνύματος. Αυτή η πληροφορία επιτρέπει το εύκολο ανάκτηση του j-th μπλοκ κειμένου από οποιοδήποτε άλλο μήνυμα που έχει κρυπτογραφηθεί χρησιμοποιώντας τον ίδιο IV. Η εμπιστευτικότητα μπορεί επίσης να κινδυνεύσει εάν οποιοδήποτε από τα μπλοκ εισόδου στη λειτουργία κρυπτογράφησης προς τα εμπρός

για την κρυπτογράφηση ενός μηνύματος ορίζεται ως IV για την κρυπτογράφηση ενός άλλου μηνύματος υπό το συγκεκριμένο κλειδί.

5.11. Σκέψεις για το IANA

Αυτό το έγγραφο δεν απαιτεί καμία ενέργεια από το IANA.

5.12. Παράρτημα A: Παράδειγμα Υπολογισμών

5.12.1 Παράδειγμα 1

Αυτό το παράδειγμα δείχνει την κρυπτογράφηση ενός κειμένου.

Κείμενο: 01 23 45 67 89 AB CD EF FE DC BA 98 76 54 32 10

Κλειδί κρυπτογράφησης: 01 23 45 67 89 AB CD EF FE DC BA 98 76 54 32 10

Κατάσταση του γύρου του κλειδιού (rk_i) και της έξοδου του γύρου (X_i) ανά γύρο:

rk_0 = F12186F9 X_4 = 27FAD345

rk_1 = 41662B61 X_5 = A18B4CB2

rk_2 = 5A6AB19A X_6 = 11C1E22A

rk_3 = 7BA92077 X_7 = CC13E2EE

rk_4 = 367360F4 X_8 = F87C5BD5

rk_5 = 776A0C61 X_9 = 33220757

rk_6 = B6BB89B3 X_10 = 77F4C297

rk_7 = 24763151 X_11 = 7A96F2EB

rk_8 = A520307C X_12 = 27DAC07F

rk_9 = B7584DBD X_13 = 42DD0F19

rk_10 = C30753ED X_14 = B8A5DA02

rk_11 = 7EE55B57 X_15 = 907127FA

rk_12 = 6988608C X_16 = 8B952B83

rk_13 = 30D895B7 X_17 = D42B7C59

rk_14 = 44BA14AF X_18 = 2FFC5831

rk_15 = 104495A1 X_19 = F69E6888

rk_16 = D120B428 X_20 = AF2432C4

rk_17 = 73B55FA3 X_21 = ED1EC85E

rk_18 = CC874966 X_22 = 55A3BA22

rk_19 = 92244439 X_23 = 124B18AA

rk_20 = E89E641F X_24 = 6AE7725F

rk_21 = 98CA015A X_25 = F4CBA1F9

rk_22 = C7159060 X_26 = 1DCDFA10

rk_23 = 99E1FD2E X_27 = 2FF60603

rk_24 = B79BD80C X_28 = EFF24FDC

rk_25 = 1D2115B0 X_29 = 6FE46B75

rk_26 = 0E228AEB X_30 = 893450AD

rk_27 = F1780C81 X_31 = 7B938F4C

rk_28 = 428D3654 X_32 = 536E4246

rk_29 = 62293496 X_33 = 86B3E94F

rk_30 = 01CF72E5 X_34 = D206965E

rk_31 = 9124A012 X_35 = 681EDF34

Κρυπτοκείμενο: 68 1E DF 34 D2 06 96 5E 86 B3 E9 4F 53 6E 42 46

12.2 Παράδειγμα 2

Αυτό το παράδειγμα δείχνει την κρυπτογράφηση ενός κειμένου που επαναλαμβάνεται 1.000.000 φορές χρησιμοποιώντας ένα σταθερό κλειδί κρυπτογράφησης.

Κείμενο: 01 23 45 67 89 AB CD EF FE DC BA 98 76 54 32 10

Κλειδί κρυπτογράφησης: 01 23 45 67 89 AB CD EF FE DC BA 98 76 54 32 10

Κρυπτοκείμενο: 59 52 98 C7 C6 FD 27 1F 04 02 F8 04 C3 3D 3F 66

5.13. Παραπομπές

5.13.1 Κανονιστικές Αναφορές

[GBT.32907-2016]

Standardization Administration of the People's Republic of China, "GB/T 32907-2016: Information security technology --- SM4 block cipher algorithm", August 2016,

http://www.gb688.cn/bzgk/gb/newGbInfo?hcno=7803DE42D3BC5E80B0C3E5D8E873D56A

[RFC2119]

Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, https://www.rfc-editor.org/info/rfc2119

5.13.2 Ενημερωτικές-πληροφοριακές Αναφορές

[GB.15629.11-2003]

Standardization Administration of the People's Republic of China, "Information technology -- Telecommunications and information exchange between systems -- Local and metropolitan area networks -- Specific requirements -- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", May 2003, http://www.gb688.cn/bzgk/gb/newGbInfo?hcno=74B9DD11287E72408C19C4D3A360D1BD

[GMT-0002-2012]

Organization of State Commercial Administration of China, "GM/T 0002-2012: SM4 block cipher algorithm", March 2012,

http://www.oscca.gov.cn/Column/Column_32.htm

[GMT-0006-2012]

Organization of State Commercial Administration of China, "GM/T 0006-2012: Cryptographic Application Identifier Criterion Specification", March 2012,

http://www.oscca.gov.cn/Column/Column_32.htm

[LSW-Bio]

Sun, M., "Lv Shu Wang -- A life in cryptography", November 2010, http://press.ustc.edu.cn/sites/default/files/fujian/field_fujian_multi/20120113/%E5%90%95%E8%BF%B0%E6%9C%9B%20%E5%AF%86%E7%A0%81%E4%B8%80%E6%A0%B7%E7%9A%84%E4%BA%BA%E7%94%9F.pdf

[NIST.FIPS.197]

National Institute of Standards and Technology, "NIST FIPS 197: Advanced Encryption Standard (AES)", November 2001,

https://doi.org/10.6028/NIST.FIPS.197

[NIST.SP.800-38A]

Dworkin, M., "NIST Special Publication 800-38A: Recommendation for Block Cipher Modes of Operation -- Methods and Techniques", December 2001,

http://dx.doi.org/10.6028/NIST.SP.800-38A

[NIST.FIPS.197]

National Institute of Standards and Technology, "NIST FIPS 197: Advanced Encryption Standard (AES)", November 2001,

https://doi.org/10.6028/NIST.FIPS.197

[NIST.SP.800-38A]

Dworkin, M., "NIST Special Publication 800-38A: Recommendation for Block Cipher Modes of Operation -- Methods and Techniques", December 2001,

http://dx.doi.org/10.6028/NIST.SP.800-38A

[OSCCA]

Organization of State Commercial Administration of China, "Organization of State Commercial Administration of China", May 2017, http://www.oscca.gov.cn

[SideChannel]

Lei, Q., Wu, L., Zhang, S., Zhang, X., Li, X., Pan, L., and Z. Dong, "Software Hardware Co-design for Side-Channel Analysis Platform on Security Chips", December 2015,

https://doi.org/10.1109/CIS.2015.102

[SM4]

Organization of State Commercial Administration of China, "SMS4 Cryptographic Algorithm For Wireless LAN Products", January 2006,

http://www.oscca.gov.cn/UpFile/200621016423197990.pdf

[SM4-Analysis]

Kim, T., Kim, J., Kim, S., and J. Sung, "Linear and Differential Cryptanalysis of Reduced SMS4 Block Cipher", June 2008, https://eprint.iacr.org/2008/281

[SM4-En]

Diffie, W. and G. Ledin, "SMS4 Encryption Algorithm for Wireless Networks", May 2008,

https://www.iacr.org/cryptodb/data/paper.php?pubkey=18006

[SM4-FPGA]

Cheng, H., Zhai, S., Fang, L., Ding, Q., and C. Huang, "Improvements of SM4 Algorithm and Application in Ethernet Encryption System Based on FPGA", July 2014,

https://www.researchgate.net/publication/287081686_Improvements_of_SM4_algorithm_and_application_in_Ethernet_encryption_system_based_on_FPGA

[SM4-HiSpeed]

Lv, Q., Li, L., and Y. Cao, "High-speed Encryption & Decryption System Based on SM4", July 2016,

http://dx.doi.org/10.14257/ijsia.2016.10.9.01

[SM4-Linear]

Liu, M. and J. Chen, "Improved Linear Attacks on the Chinese Block Cipher Standard", November 2014,

https://doi.org/10.1007/s11390-014-1495-9

[SM4-Power]

Du, Z., Wu, Z., Wang, M., and J. Rao, "Improved chosen-plaintext power analysis attack against SM4 at the round- output", October 2015,

http://dx.doi.org/10.6028/NIST.FIPS.180-4

[SM4-VLSI]

Yu, S., Li, K., Li, K., Qin, Y., and Z. Tong, "A VLSI implementation of an SM4 algorithm resistant to power analysis", July 2016, https://doi.org/10.3233/JIFS-169011

[SM4-WhiteBox]

Bai, K. and C. Wu, "A secure white-box SM4 implementation", May 2008,

http://dx.doi.org/10.1002/sec.1394

Ομάδα Εργασίας Δικτύου

Προσχέδιο Internet

Επιθυμητή κατάσταση: Πληροφοριακή

Λήξη: 13 Μαρτίου 2018 Κολλέγιο Διαχείρισης

9 Σεπτεμβρίου 2017

R. Tse

Ribose

W. Wong

Hang Seng