Κρυπτογραφία

MAC - Γνησιότητα/Ακεραιότητα μηνύματος

Πέτρος Ποτίκας

Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Περιεχόμενα

- Κρυπτογράφηση κρύβει μήνυμα από αντίπαλο

- Κρυπτογράφηση κρύβει μήνυμα από αντίπαλο
- Φτάνει για ασφαλή επικοινωνία;

- Κρυπτογράφηση κρύβει μήνυμα από αντίπαλο
- Φτάνει για ασφαλή επικοινωνία;
- *Γνησιότητα/ακεραιότητα μηνύματος (message integrity/authentication)*

- Κρυπτογράφηση κρύβει μήνυμα από αντίπαλο
- Φτάνει για ασφαλή επικοινωνία;
- *Γνησιότητα/ακεραιότητα μηνύματος (message integrity/authentication)*
- Παράδειγμα: Η εταιρεία Β παίρνει παραγγελία από την εταιρεία Α να φτιάξει 1000 οθόνες
  Ερωτήματα:

- Κρυπτογράφηση κρύβει μήνυμα από αντίπαλο
- Φτάνει για ασφαλή επικοινωνία;
- *Γνησιότητα/ακεραιότητα μηνύματος (message integrity/authentication)*
- Παράδειγμα: Η εταιρεία Β παίρνει παραγγελία από την εταιρεία Α να φτιάξει 1000 οθόνες
  Ερωτήματα:
  1. Το έστειλε πράγματι η Α;

- Κρυπτογράφηση κρύβει μήνυμα από αντίπαλο
- Φτάνει για ασφαλή επικοινωνία;
- *Γνησιότητα/ακεραιότητα μηνύματος (message integrity/authentication)*
- Παράδειγμα: Η εταιρεία Β παίρνει παραγγελία από την εταιρεία Α να φτιάξει 1000 οθόνες
  Ερωτήματα:
  1. Το έστειλε πράγματι η Α;
  2. Είναι το 1000 σωστό;

Message Authentication Code (MAC)

- Δύο παίκτες θέλουν να επικοινωνήσουν ανταλλάσσοντας 'ακέραια μηνύματα'
- Ανταλλάσουν κοινό μυστικό κλειδί k
- Όταν ένας παίκτης θέλει να στείλει ένα μήνυμα m, υπολογίζει μια ετικέτα t (tag) με βάση το μήνυμα και το κοινό τους κλειδί, με έναν αλγόριθμο παραγωγής ετικέτας Mac
- Στέλνει το μήνυμα μαζί με την ετικέτα (m, t)
- Ο άλλος παίκτης λαμβάνει το (m, t) και επιβεβαιώνει τη γνησιότητα του μηνύματος (αν το t είναι έγκυρο για το m με βάση το κοινό κλειδί που έχει, με έναν αλγόριθμο επαλήθευσης $Vrfy$)

Message Authentication Code (MAC)

Ορισμός

Ένας *κώδικας γνησιότητας μηνύματος (Message Authenthication Code, MAC)* είναι μια πλειάδα PPT αλγορίθμων $(Gen, Mac, Vrfy)$, τέτοιων ώστε:

1. Ο *αλγόριθμος παραγωγής κλειδιού* Gen παίρνει είσοδο την παράμετρο ασφαλείας 1^n και επιστρέφει ένα κλειδί k, με $|k| \geq n$
2. Ο *αλγόριθμος παραγωγής ετικέτας* Mac παίρνει σαν είσοδο ένα κλειδί k και ένα μήνυμα $m \in \{0,1\}^*$ και επιστρέφει μια ετικέτα t $(t \leftarrow Mac_k(m))$
3. Ο *αλγόριθμος επαλήθευσης* $Vrfy$ παίρνει σαν είσοδο ένα k, ένα m και μια ετικέτα t και επιστρέφει 1, αν η ετικέτα είναι έγκυρη, αλλιώς 0 (ντετερμινιστικός αλγόριθμος)

Για κάθε n, κάθε k που παράγεται από τον Gen και κάθε $m \in \{0,1\}^*$, ισχύει $Vrfy_k(m, Mac_k(m)) = 1$
Αν το MAC ορίζεται μόνο για μηνύματα μήκους $l(n)$, τότε λέγεται *σταθερού μήκους*

Ασφάλεια κώδικα γνησιότητας μηνύματος

Διαισθητικά: κανένας αντίπαλος δεν μπορεί να φτιάξει μια έγκυρη ετικέτα για ένα "νέο" μήνυμα που δεν έχει γνησιότητα ακόμα

Ο αντίπαλος βλέπει τα (m, t) που ανταλλάσσονται και μπορεί να τα αλλάζει

Πείραμα γνησιότητας μηνύματος Mac-forge$_{\mathcal{A},\Pi}(n)$

1. Ένα τυχαίο κλειδί παράγεται από τον $Gen(1^n)$
2. Ο αντίπαλος $\mathcal{A}$ παίρνει σαν είσοδο το 1^n και πρόσβαση σε ένα μαντείο $Mac_k()$. Δίνει σαν έξοδο ένα (m, t) και Q το σύνολο των ερωτήσεων που κάνει στο μαντείο
3. Η έξοδος του πειράματος είναι 1, ανν (1) $Vrfy_k(m, t) = 1$ και (2) $m \notin Q$

Ασφάλεια κώδικα γνησιότητας μηνύματος

Ορισμός

Ένας κώδικας γνησιότητας μηνύματος $\Pi = (Gen, Mac, Vrfy)$ είναι *υπαρξιακά μη-παραχαράξιμος σε μια προσαρμοζόμενη επίθεση επιλεγμένου μηνύματος (existentially unforgeable under an adaptive chosen-message attack)* ή *ασφαλής* αν για κάθε PPT αντίπαλο $\mathcal{A}$ υπάρχει μια αμελητέα συνάρτηση $negl$ τέτοια ώστε:

$$Pr[\text{Mac-forge}_{\mathcal{A},\Pi}(n) = 1] \leq negl(n)$$

Επίθεση επανάληψης

Ένας αντίπαλος μπορεί να στείλει ένα μήνυμα και την ετικέτα ενός προηγούμενου έγκυρου μηνύματος

Παράδειγμα:

Η Alice στέλνει μήνυμα στην τράπεζά της να δώσουν 1000 € στον Bob

Επίθεση επανάληψης

Ένας αντίπαλος μπορεί να στείλει ένα μήνυμα και την ετικέτα ενός προηγούμενου έγκυρου μηνύματος

Παράδειγμα:

Η Alice στέλνει μήνυμα στην τράπεζά της να δώσουν 1000 € στον Bob
Ο Bob δεν μπορεί να το κάνει 10.000 €, αλλά μπορεί να το στείλει 10 φορές στην τράπεζα!

Επίθεση επανάληψης

Ένας αντίπαλος μπορεί να στείλει ένα μήνυμα και την ετικέτα ενός προηγούμενου έγκυρου μηνύματος

Παράδειγμα:

Η Alice στέλνει μήνυμα στην τράπεζά της να δώσουν 1000 € στον Bob
Ο Bob δεν μπορεί να το κάνει 10.000 €, αλλά μπορεί να το στείλει 10 φορές στην τράπεζα!

MAC δεν έχουν την ικανότητα να αποφύγουν τέτοιες επιθέσεις, γιατί δε δίνουν σημασιολογία

Είναι θέμα εφαρμογής, τι σημαίνει η επανάληψη μηνύματος

Επίθεση επανάληψης

Ένας αντίπαλος μπορεί να στείλει ένα μήνυμα και την ετικέτα ενός προηγούμενου έγκυρου μηνύματος

Παράδειγμα:

Η Alice στέλνει μήνυμα στην τράπεζά της να δώσουν 1000 € στον Bob
Ο Bob δεν μπορεί να το κάνει 10.000 €, αλλά μπορεί να το στείλει 10 φορές στην τράπεζα!

MAC δεν έχουν την ικανότητα να αποφύγουν τέτοιες επιθέσεις, γιατί δε δίνουν σημασιολογία

Είναι θέμα εφαρμογής, τι σημαίνει η επανάληψη μηνύματος

Άμυνα:

1. Ένας μοναδικός αριθμός μαζί με το μήνυμα
2. Timestamp, η ώρα προστίθεται στο μήνυμα

Επίθεση επανάληψης - Μοναδικός αριθμός

Σε κάθε μήνυμα m αντιστοιχεί ένας μοναδικός αριθμός i, η γνησιότητα υπολογίζεται στο $i||m$

Ο αποστολέας πάντα αναθέτει ένα μοναδικό αριθμό σε κάθε μήνυμα, ο παραλήπτης φυλάει αυτούς τους αριθμούς

Επιτυχημένη επίθεση στο m: δημιουργία έγκυρης ετικέτας σε ένα νέο μήνυμα $i'||m$, όπου i' είναι φρέσκο

Μειονέκτημα: φύλαξη όλων των αριθμών από τον παραλήπτη

Επίθεση επανάληψης - Timestamp

Η τρέχουσα ώρα (στο κοντινότερο millisecond) προστίθεται στο μήνυμα, ο παραλήπτης αποδέχεται αν είναι εντός ενός περιθωρίου

Μειονέκτημα: τα συμβαλλόμενα μέρη πρέπει να έχουν συγχρονισμένα ρολόγια και μπορεί να προλάβει να ξαναστείλει κάτι (πόσο στενό είναι το χρονικό περιθώριο)

Ψευδοτυχαίες συναρτήσεις ως Κώδικες Γνησιότητας

Οι ψευδοτυχαίες συναρτήσεις είναι κατάλληλες για κώδικες γνησιότητητας

Αν t παράγεται από την εφαρμογή μιας ψευδοτυχαίας συνάρτησης σε ένα μήνυμα m, τότε η παραχάραξη απαιτεί να μαντέψει ο αντίπαλος την τιμή μιας ψευδοτυχαίας συνάρτησης σε ένα "νέο" μήνυμα

Πιθανότητα να μαντέψει σωστά: 2^{-n}, όταν μήκος εξόδου συνάρτησης είναι n

Κατασκευή

Έστω F μια ψευδοτυχαία συνάρτηση. Ορίζουμε έναν καθορισμένου μήκους κώδικα γνησιότητας για μηνύματα μήκους n ως:

- *Gen*: με είσοδο 1^n, επίλεξε $k \leftarrow \{0,1\}^n$
- *Mac*: με είσοδο $k, m \in \{0,1\}^n$, δώσε στην έξοδο $t := F_k(m)$ (αν $|m| \neq |k|$ μη δίνεις αποτέλεσμα)
- *Vrfy*: με είσοδο k, m, t, δώσε αποτέλεσμα 1, αν $t = F_k(m)$ (αν $|m| \neq |k|$, δώσε 0)

Ασφάλεια κατασκευής

Θεώρημα

Αν η F είναι μια ψευδοτυχαία συνάρτηση, τότε η παραπάνω κατασκευή είναι ένας καθορισμένου μήκους κώδικας γνησιότητας για μηνύματα μήκους n που είναι υπαρξιακά μη-παραχαράξιμος σε μια προσαρμοζόμενη επίθεση επιλεγμένου μηνύματος

Επέκταση σε μηνύματα μεταβλητού μήκους

Έστω $\Pi = (Gen', Mac', Vrfy')$ ένας κώδικας γνησιότητας καθορισμένου μήκους για μηνύματα μήκους n

Σπάμε το μήνυμα m σε blocks $m_1, \ldots, m_d$ και βρίσκουμε τη γνησιότητα κάθε block με κάποιο τρόπο

Ιδέες:

1. Πάρε το XOR όλων των block και εφάρμοσε την MAC, $t := MAC'_k(\oplus_i(m_i))$

Επέκταση σε μηνύματα μεταβλητού μήκους

Έστω $\Pi = (Gen', Mac', Vrfy')$ ένας κώδικας γνησιότητας καθορισμένου μήκους για μηνύματα μήκους n

Σπάμε το μήνυμα m σε blocks $m_1, \ldots, m_d$ και βρίσκουμε τη γνησιότητα κάθε block με κάποιο τρόπο

Ιδέες:

1. Πάρε το XOR όλων των block και εφάρμοσε την MAC,
   $t := MAC'_k(\oplus_i(m_i))$
   Ο αντίπαλος μπορεί να αλλάξει το αρχικό μήνυμα ώστε το XOR να μείνει ίδιο

Επέκταση σε μηνύματα μεταβλητού μήκους

Έστω $\Pi = (Gen', Mac', Vrfy')$ ένας κώδικας γνησιότητας καθορισμένου μήκους για μηνύματα μήκους n

Σπάμε το μήνυμα m σε blocks $m_1, \ldots, m_d$ και βρίσκουμε τη γνησιότητα κάθε block με κάποιο τρόπο

Ιδέες:

1. Πάρε το XOR όλων των block και εφάρμοσε την MAC,
   $t := MAC'_k(\oplus_i(m_i))$
   Ο αντίπαλος μπορεί να αλλάξει το αρχικό μήνυμα ώστε το XOR να μείνει ίδιο
2. Πάρε κάθε block ξεχωριστά, $t := \langle MAC'_k(m_1), \ldots, MAC'_k(m_d)\rangle$

Επέκταση σε μηνύματα μεταβλητού μήκους

Έστω $\Pi = (Gen', Mac', Vrfy')$ ένας κώδικας γνησιότητας καθορισμένου μήκους για μηνύματα μήκους n

Σπάμε το μήνυμα m σε blocks $m_1, \ldots, m_d$ και βρίσκουμε τη γνησιότητα κάθε block με κάποιο τρόπο

Ιδέες:

1. Πάρε το XOR όλων των block και εφάρμοσε την MAC,
   $t := MAC'_k(\oplus_i(m_i))$
   Ο αντίπαλος μπορεί να αλλάξει το αρχικό μήνυμα ώστε το XOR να μείνει ίδιο
2. Πάρε κάθε block ξεχωριστά, $t := \langle MAC'_k(m_1), \ldots, MAC'_k(m_d)\rangle$
   Αν αλλάξεις σειρά στα blocks;

Επέκταση σε μηνύματα μεταβλητού μήκους

Έστω $\Pi = (Gen', Mac', Vrfy')$ ένας κώδικας γνησιότητας καθορισμένου μήκους για μηνύματα μήκους n

Σπάμε το μήνυμα m σε blocks $m_1, ..., m_d$ και βρίσκουμε τη γνησιότητα κάθε block με κάποιο τρόπο

Ιδέες:

1. Πάρε το XOR όλων των block και εφάρμοσε την MAC,
   $t := MAC'_k(\oplus_i(m_i))$
   Ο αντίπαλος μπορεί να αλλάξει το αρχικό μήνυμα ώστε το XOR να μείνει ίδιο
2. Πάρε κάθε block ξεχωριστά, $t := \langle MAC'_k(m_1), ..., MAC'_k(m_d)\rangle$
   Αν αλλάξεις σειρά στα blocks;
3. Πάρε block ξεχωριστά μαζί με έναν αριθμό
   $t := \langle MAC'_k(1||m_1), ..., MAC'_k(d||m_d)\rangle$

Επέκταση σε μηνύματα μεταβλητού μήκους

Έστω $\Pi = (Gen', Mac', Vrfy')$ ένας κώδικας γνησιότητας καθορισμένου μήκους για μηνύματα μήκους n

Σπάμε το μήνυμα m σε blocks $m_1, \ldots, m_d$ και βρίσκουμε τη γνησιότητα κάθε block με κάποιο τρόπο

Ιδέες:

1. Πάρε το XOR όλων των block και εφάρμοσε την MAC,
   $t := MAC'_k(\oplus_i(m_i))$
   Ο αντίπαλος μπορεί να αλλάξει το αρχικό μήνυμα ώστε το XOR να μείνει ίδιο
2. Πάρε κάθε block ξεχωριστά, $t := \langle MAC'_k(m_1), \ldots, MAC'_k(m_d)\rangle$
   Αν αλλάξεις σειρά στα blocks;
3. Πάρε block ξεχωριστά μαζί με έναν αριθμό
   $t := \langle MAC'_k(1||m_1), \ldots, MAC'_k(d||m_d)\rangle$
   Μπορεί να πετάξει block από τέλος ή να συνδυάσει προηγούμενα μηνύματα

Επέκταση σε μηνύματα μεταβλητού μήκους

Επιπλέον πληροφορία, ένα τυχαίο "αναγνωριστικό μηνύματος" σε κάθε block και το μήκος μηνύματος

Κατασκευή

Έστω $\Pi' = (Gen', Mac', Vrfy')$ ένας MAC καθορισμένου μήκους για μηνύματα μήκους n. Ορίζουμε ένα MAC ως εξής:

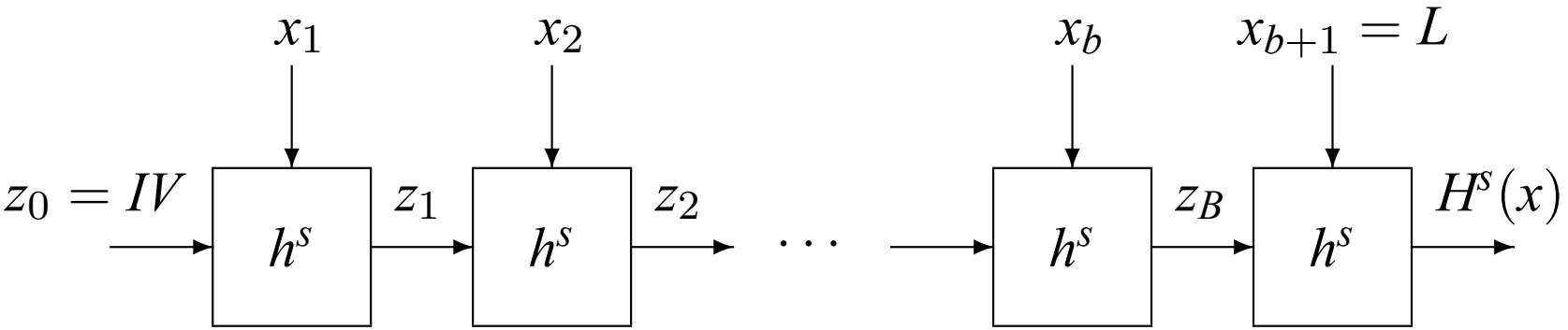
- *Gen*: ίδιο με το Gen'
- *Mac*: με είσοδο $k \in \{0,1\}^n$, $m \in \{0,1\}^*$ μήκους $l < 2^{n/4}$, ανάλυσέ το σε d blocks, $m_1, ..., m_d$, καθένα μήκους $n/4$ (συμπλήρωσε με μηδενικά αν χρειάζεται). Διάλεξε αναγνωριστικό $r \leftarrow \{0,1\}^{n/4}$
  Υπολόγισε $t_i := Mac'_k(r||l||i||m_i)$, $1 \leq i \leq d$, και δώσε έξοδο $t := \langle r, t_1, ..., t_d \rangle$
- *Vrfy*: με είσοδο $k \in \{0,1\}^n$, $m \in \{0,1\}^*$ μήκους $l < 2^{n/4}$ και $t := \langle r, t_1, ..., t_d \rangle$, ανάλυσε το m σε d' blocks, καθένα μήκους $n/4$ (συμπλήρωσε με μηδενικά αν χρειάζεται). Έξοδος 1 ανν (1) $d = d'$ και (2) $Vrfy'_k(r||l||i||m_i) = t_i$, $1 \leq i \leq d$

Ασφάλεια κατασκευής

Θεώρημα

Αν Π' είναι ασφαλής κώδικας γνησιότητας καθορισμένου μήκους για μηνύματα μήκους n, τότε η παραπάνω κατασκευή είναι υπαρξιακά μη-παραχαράξιμη σε μια προσαρμοζόμενη επίθεση επιλεγμένου μηνύματος για μηνύματα μεταβλητού μήκους

Κατασκευή Merkle-Damgård



Σχήμα : Merkle-Damgård

Nested MAC (NMAC)

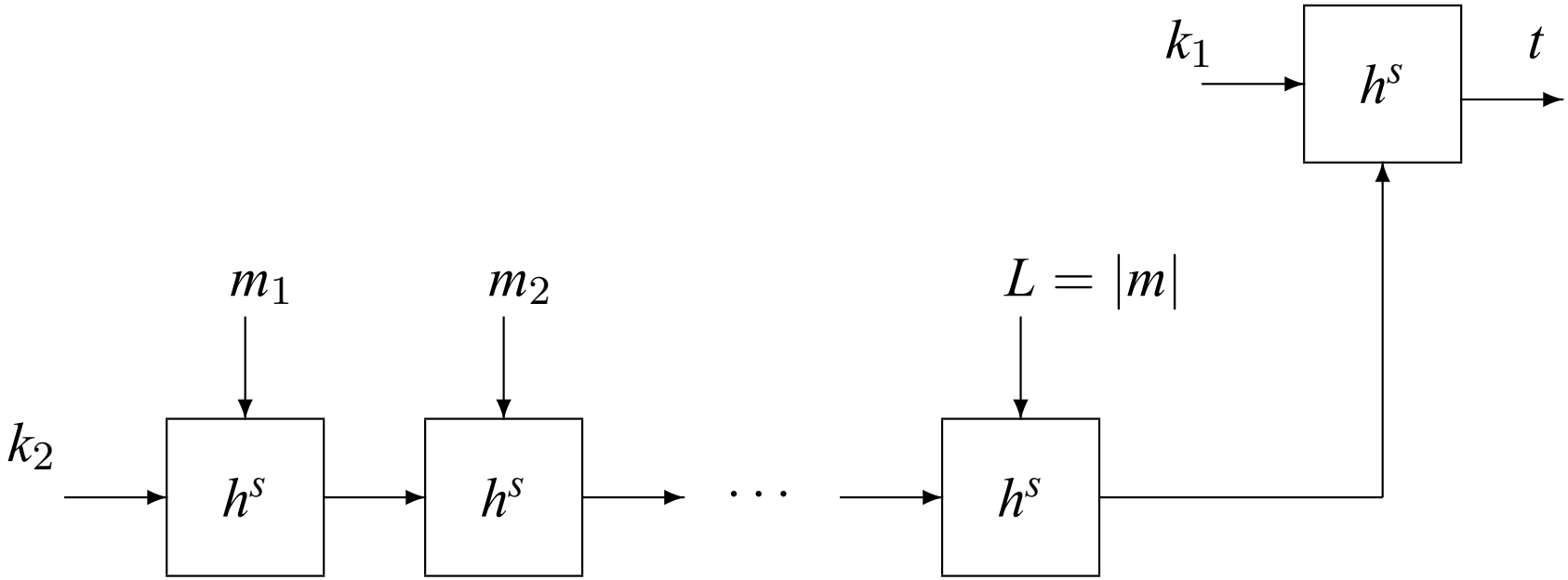
Κατασκευή MAC από συναρτήσεις σύνοψης που αντιστέκονται σε συγκρούσεις

Ασφάλεια στηρίζεται στην αντίσταση στις συγκρούσεις αλλά και στην ψευδοτυχαιότητα των συναρτήσεων σύνοψης

Κατασκευή NMAC

Έστω $(\widetilde{Gen}, h)$ μια συνάρτηση συμπίεσης καθορισμένου μήκους που αντιστέκεται σε συγκρούσεις και (Gen, H) το αποτέλεσμα του Merkle-Damg ård μετασχηματισμού στο $(\widetilde{Gen}, h)$. Ο NMAC ορίζει ένα MAC ως εξής:

- *Gen*: με είσοδο n, τρέξε $\widetilde{Gen}(1^n)$ και πάρε κλειδί s, επίλεξε κλειδιά $k_1, k_2 \leftarrow \{0,1\}^n$ και δώσε το κλειδί (s, k_1, k_2)
- *Mac*: με είσοδο (s, k_1, k_2), ένα $m \in \{0,1\}^*$, μήκους L, δώσε $t := h^s_{k_1}(H^s_{k_2}(m))$
- *Vrfy*: με είσοδο $k \in \{0,1\}^n$, $m \in \{0,1\}^*$ και t, δώσε 1 ανν $t = Mac_{s,k_1,k_2}(m)$



Σχήμα : NMAC

Ασφάλεια NMAC

Η ασφάλεια βασίζεται στην υπόθεση ότι η h^s με κλειδί k αποτελεί έναν ασφαλή MAC

Δοσμένης μιας συνάρτησης σύνοψης καθορισμένου μήκους $(\widetilde{Gen}, h)$ ορίζουμε το καθορισμένου μήκους MAC $\Pi = (Gen, Mac, Vrfy)$ ως εξής:

- τρέξε το $\widetilde{Gen}(1^n)$ για να πάρεις ένα s και $k \leftarrow \{0,1\}^n$. Κλειδί: (s,k)
- Θέσε $Mac_{s,k}(m) = h^s_k(m)$ και $Vrfy$ ορίζεται κατά τα προφανή

Τότε το $(\widetilde{Gen}, h)$ παράγει ένα ασφαλές MAC αν το Π που παράγεται με αυτό τον τρόπο είναι ένας ασφαλές MAC καθορισμένου μήκους

Θεώρημα

Έστω $(\widetilde{Gen}, H)$ το αποτέλεσμα του Merkle-Damgård μετασχηματισμού στο $(\widetilde{Gen}, h)$. Αν $(\widetilde{Gen}, h)$ αντιστέκεται σε συγκρούσεις και παράγει ένα ασφαλές MAC, τότε το NMAC είναι υπαρξιακά μη-παραχαράξιμο σε μια προσαρμοζόμενη επίθεση επιλεγμένου μηνύματος (για μεταβλητού μήκους μηνύματα)

Ασφάλεια NMAC

Πρώτα περνάμε το μήνυμα από μια συνάρτηση σύνοψης και από το αποτέλεσμα φτιάχνουμε την ετικέτα γνησιότητας

Ιδέα απόδειξης ασφάλειας: έστω πως ένας αντίπαλος $\mathcal{A}$ προσβάλλει το σύστημα, με m^* το νέο μήνυμα για το οποίο φτιάχνεται μία έγκυρη ετικέτα και Q το σύνολο των ερωτήσεων στο μαντείο ($m^* \notin Q$)

Δύο περιπτώσεις:

1. Υπάρχει m τ.ω. $H^s_{k_2}(m) = H^s_{k_2}(m^*)$. Τότε όμως η H δεν αντιστέκεται σε συγκρούσεις. Αντίφαση.
2. Για κάθε $m \in Q$, $H^s_{k_2}(m) \neq H^s_{k_2}(m^*)$. Ορίζουμε $Q' = \{H^s_{k_2}(m) \mid m \in Q\}$. Το m^* είναι τέτοιο ώστε $H^s_{k_2}(m^*) \notin Q'$. Άρα ο αντίπαλος παραχαράσσει μια έγκυρη ετικέτα στο "νέο μήνυμα" $H^s_{k_2}(m^*)$ στο Π. Αντίφαση.

Ο αντίπαλος δε βλέπει το $H^s_{k_2}(x)$, αλλά το $h^s_{k_1}(H^s_{k_2}(x))$, άρα το k_2 μπορούσε να είναι και σταθερό όπως στο Merkle-Damgård

Hashed MAC (HMAC)

Μειονέκτημα NMAC: IV της H αλλάζει (σταθερό συνήθως)

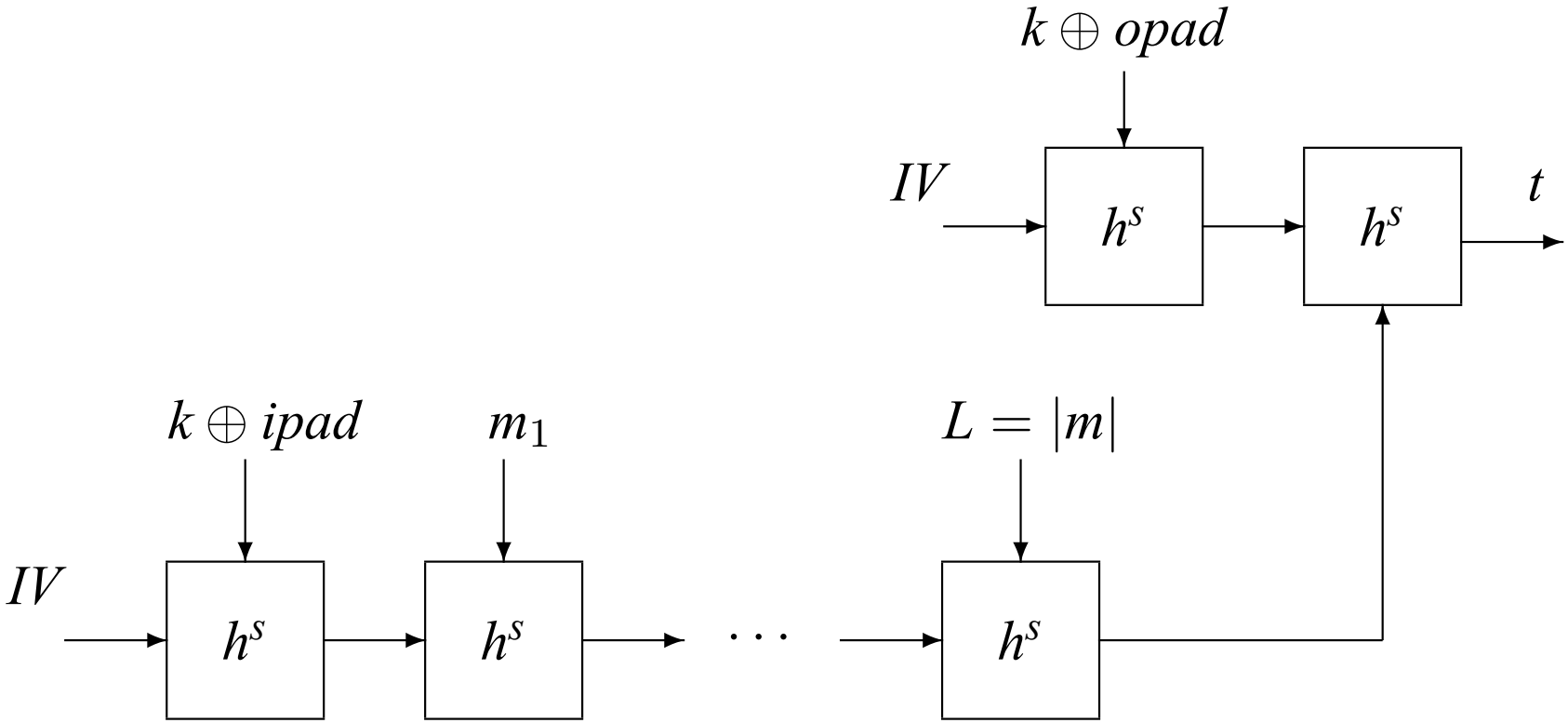
HMAC δίνει κλειδιά με διαφορετικό τρόπο και χρησιμοποιεί μόνο ένα κλειδί

Το IV είναι καθορισμένο (εκτός ελέγχου των παικτών)

Κατασκευή HMAC

Έστω $(\widetilde{Gen}, h)$ μια συνάρτηση συμπίεσης καθορισμένου μήκους που αντιστέκεται σε συγκρούσεις και (Gen, H) το αποτέλεσμα του Merkle-Damg ård μετασχηματισμού. Έστω $IV, ipad, opad$ σταθερές μήκους n. Ο HMAC ορίζει ένα MAC ως εξής:

- Gen: με είσοδο n, τρέξε $\widetilde{Gen}(1^n)$ και πάρε κλειδί s, επίλεξε $k \leftarrow \{0,1\}^n$ και δώσε κλειδί (s,k)
- Mac: με είσοδο (s,k), ένα $m \in \{0,1\}^*$ μήκους L δώσε $t := H^s_{IV}((k \oplus opad)||H^s_{IV}(k \oplus ipad)||m))$
- $Vrfy$: με είσοδο $k \in \{0,1\}^n$, $m \in \{0,1\}^*$ και μια ετικέτα t, δώσε 1 ανν $t = Mac_{s,k}(m)$



Σχήμα : HMAC

Ασφάλεια

- Το HMAC είναι παραλλαγή του NMAC
- Αναγωγή σε ασφάλεια του NMAC (με κάποιες υποθέσεις)

HMAC στην πράξη

- Το HMAC είναι πρότυπο και χρησιμοποιείται στην πράξη (SSL, SSH)
- Είναι αποδοτικό
- Εύκολα υλοποιήσιμο
- Έχει απόδειξη ότι είναι ασφαλές (βασισμένο σε υποθέσεις που πιστεύουμε ότι ισχύουν για συναρτήσεις σύνοψης)

Ιδιωτικότητα και γνησιότητα

Μπορούμε να συνδυάσουμε ένα σύστημα κρυπτογράφησης με ένα γνησιότητας μηνύματος;

Οποιοσδήποτε συνδυασμός δεν είναι σωστός

Έστω k_1 το κλειδί κρυπτογράφησης, k_2 γνησιότητας (ΠΑΝΤΑ ανεξάρτητα)

1. Κρυπτογράφηση-και-γνησιότητα

$$c \leftarrow Enc_{k_1}(m) \text{ και } t \leftarrow Mac_{k_2}(m)$$

2. Γνησιότητα-μετά-κρυπτογράφηση

$$t \leftarrow Mac_{k_2}(m) \text{ και } c \leftarrow Enc_{k_1}(m||t)$$

3. Κρυπτογράφηση-μετά-γνησιότητα

$$c \leftarrow Enc_{k_1}(m) \text{ και } t \leftarrow Mac_{k_2}(c)$$

Ανάλυση ασφαλείας

- Οποιοδήποτε CCA-secure σχήμα κρυπτογράφησης και οποιοδήποτε ασφαλές MAC (με μοναδικές ετικέτες)
- Θέλουμε για όλα τα σχήματα κρυπτογράφησης και όλα τα MACs να είναι ασφαλής ο συνδυασμός
- Μπορεί να υπάρχει ένα σχήμα από καθένα από αυτά ώστε να είναι ασφαλές
- Θέλουμε το “όλα ή τίποτα”, ώστε να ελαχιστοποιήσουμε λάθη στην υλοποίηση (αντικατάσταση με νεότερες εκδόσεις ή αλλαγή των standards)

Κρυπτογράφηση ή κρυπτογράφηση και ακεραιότητα

Στις περισσότερες online εργασίες, ιδίως τραπεζικές συναλλαγές χρειάζονται και τα δύο

Κρυπτογράφηση αρχείων στο δίσκο: κρυπτογράφηση μόνο είναι αρκετή;

Κρυπτογράφηση ή κρυπτογράφηση και ακεραιότητα

Στις περισσότερες online εργασίες, ιδίως τραπεζικές συναλλαγές χρειάζονται και τα δύο

Κρυπτογράφηση αρχείων στο δίσκο: κρυπτογράφηση μόνο είναι αρκετή; Αν κάποιος αλλάξει στοιχεία, τότε π.χ. μια εταιρεία θα βγάλει λάθος εκθέσεις

Συμβουλή: συνδυάζετε πάντα γνησιότητα μηνύματος με ιδιωτικότητα/κρυπτογράφηση (εξαίρεση: λίγους πόρους)

Ανάλυση ασφάλειας

Ορισμός "ασφαλούς συνδυασμού"

Έστω $\Pi_E = (Gen_E, Enc, Dec)$ σχήμα κρυπτογράφησης,
$\Pi_M = (Gen_M, Mac, Vrfy)$ σχήμα γνησιότητας μηνύματος.
Ένα *σχήμα μετάδοσης μηνύματος* $\Pi' = (Gen', EncMac', Dec')$ που παράγεται από τα Π_E, Π_M είναι μια πλειάδα αλγορίθμων που κάνουν τα εξής:

- Ο Gen' τρέχει $Gen_E(1^n), Gen_M(1^n)$ και παίρνει κλειδιά k_1, k_2, αντίστοιχα
- Ο $EncMac'$ με είσοδο τα k_1, k_2 και m δίνει ένα c τρέχοντας κάποιο συνδυασμό των Enc_{k_1}, Mac_{k_2}
- Ο Dec' παίρνει είσοδο τα k_1, k_2 και ένα c και εφαρμόζει κάποιο συνδυασμό των $Dec_{k_1}, Vrfy_{k_2}$ και δίνει έξοδο είτε το m είτε $\perp$ για σφάλμα

Ανάλυση ασφάλειας

Για την ορθότητα του σχήματος απαιτούμε για κάθε n, κάθε κλειδιά k_1, k_2 που παράγονται από την Gen' και κάθε $m \in \{0,1\}^*$ να έχουμε

$$Dec'_{k_1,k_2}(EncMac'_{k_1,k_2}(m)) = m$$

Το Π' ικανοποιεί συντακτικά το σχήμα κρυπτογράφησης ιδιωτικού κλειδιού, γιατί έχουμε κρυπτογράφηση όπου επιπλέον ζητάμε γνησιότητα

Ανάλυση ασφάλειας

Για τον ορισμό της ασφάλειας του Π' θα ορίσουμε ξεχωριστές έννοιες ιδιωτικότητας και γνησιότητας

Η έννοια της ιδιωτικότητας που θεωρούμε είναι ότι το Π' η CCA-secure (αναβάθμιση από CPA-secure)

Για την γνησιότητα θεωρούμε ότι είναι υπαρξιακά μη-παραχαράξιμο σε μια προσαρμοζόμενη επίθεση επιλεγμένου μηνύματος

Το Π' δεν ικανοποιεί το συντακτικό ορισμό ενός σχήματος γνησιότητας μηνύματος, άρα θα πρέπει να κάνουμε αλλαγές

Ανάλυση ασφάλειας

Για σχήμα Π', αντίπαλο $\mathcal{A}$ και παράμετρο ασφαλείας n ορίζουμε:

Πείραμα ασφαλούς μετάδοσης μηνύματος $\mathbf{Auth}_{\mathcal{A},\Pi'}(n)$

1. Ένα κλειδί $k = (k_1, k_2)$ παράγεται από τον $Gen'(1^n)$
2. Ο αντίπαλος $\mathcal{A}$ παίρνει σαν είσοδο το 1^n και πρόσβαση σε ένα μαντείο $EncMac'_k$. Δίνει έξοδο ένα c. Q: το σύνολο των ερωτήσεων που κάνει στο μαντείο
3. Έστω $m := Dec'_k(c)$. Η έξοδος είναι 1, ανν (1) $m \neq \perp$ και (2) $m \notin Q$

Ορισμός

Ένα σχήμα μετάδοσης μηνύματος Π' πετυχαίνει *authenticated communication* αν για όλους τους PPT αντιπάλους $\mathcal{A}$ υπάρχει μια αμελητέα συνάρτηση *negl* τέτοια ώστε:

$$Pr[Auth_{\mathcal{A},\Pi'}(n) = 1] \leq negl(n)$$

Ανάλυση ασφάλειας

Σημείωση: ευκολότερο για αντίπαλο (δε χρειάζεται να γνωρίζει το m ...), άρα πιο ασφαλές

Ορισμός

Ένα σχήμα μετάδοσης μηνύματος $(Gen', EncMac', Dec')$ είναι *ασφαλές* αν είναι CCA-secure σχήμα κρυπτογράφησης και πετυχαίνει authenticated communication

Ανάλυση ασφάλειας Κρυπτογράφηση-και-Γνησιότητα

Για μήνυμα m, στέλνονται τα $\langle c, t \rangle$, όπου:

$$c \leftarrow Enc_{k_1}(m) \text{ και } t \leftarrow Mac_{k_2}(m)$$

Δεν είναι ασφαλές, γιατί παραβιάζει την ιδιωτικότητα

Παράδειγμα: μπορεί το $(Gen, Mac, Vrfy)$ να είναι ασφαλές, όπως και το $Mac'_k = (m, Mac_k(m))$, που δίνει όλο το m!

Ανάλυση ασφάλειας Γνησιότητα-μετά-Κρυπτογράφηση

$$t \leftarrow Mac_{k_2}(m) \text{ και } c \leftarrow Enc_{k_1}(m||t)$$

Δεν είναι απαραίτητα ασφαλές

Ορίζουμε το παρακάτω σχήμα:

- Έστω $Transform(m)$, τ.ώ. το 0 αντιστοιχεί σε 00 και το 1 σε 10 ή 01. Το αντίστροφο αναλύει το κρυπτογραφημένο μήνυμα σε δυάδες, έτσι το 00 είναι το 0, ενώ το 11 δεν είναι ορισμένο
- Ορίζουμε $Enc_k(m) = Enc'_k(Transform(m))$, όπου Enc' αντιστοιχεί σε counter mode encryption χρησιμοποιώντας μια ψευδοτυχαία συνάρτηση (Enc' δημιουργεί ένα ψευδοτυχαίο ρεύμα για κάθε μήνυμα, και μετά παίρνει το XOR με το μήνυμα. Το Enc είναι CPA-secure)

Ανάλυση ασφάλειας Γνησιότητα-μετά-Κρυπτογράφηση

Μη ασφαλές, αν ο αντίπαλος μπορεί να μάθει αν ένα κρυπτοκείμενο είναι έγκυρο ή μη

Στέλνει κρυπτοκείμενα και παρατηρεί την αντίδραση των τίμιων παικτών

Αν δίνεται ένα challenge ciphertext $c = Enc'_{k_1}(Transform(m||Mac_{k_2}(m))$, ο αντίπαλος αντιστρέφει τα δύο πρώτα bit του δεύτερου block (το πρώτο είναι ο μετρητής) και επαληθεύει αν είναι έγκυρο

1. Αν είναι 1, τότε έγκυρο, γιατί τα δύο πρώτα bits του $Transform(m)$ θα είναι 01 ή 10, οπότε με αντιστροφή γίνεται 10 ή 01 αντίστοιχα. Η ετικέτα θα είναι έγκυρη, γιατί η γνησιότητα ελέγχεται στο m
2. Αν είναι 0, τότε το 00 γίνεται 11 που δεν είναι έγκυρο

Συνεχίζοντας ένα-ένα στα υπόλοιπα bits, αποκαλύπτουμε όλο το m

Στο SSL είναι ασφαλές

Ανάλυση ασφάλειας Κρυπτογράφηση-μετά-Γνησιότητα

Μεταδίδεται το $\langle c, t \rangle$, όπου

$$c \leftarrow Enc_{k_1}(m) \text{ και } t \leftarrow Mac_{k_2}(c)$$

Θεώρημα

Έστω Π_E ένα ασφαλές σχήμα κρυπτογράφησης και Π_M ένα ασφαλές σχήμα γνησιότητας μηνύματος με μοναδικές ετικέτες. Τότε ο συνδυασμός $\Pi' = (Gen', EncMac', Dec')$ που παράγεται εφαρμόζοντας πρώτα κρυπτογράφηση και μετά γνησιότητα μηνύματος στα Π_E, Π_M είναι ένα ασφαλές σχήμα μετάδοσης μηνύματος.

π.χ. CCM (CTR+CBC-MAC)

Διαφορετικά κλειδιά για διαφορετικές εφαρμογές

Ίδιο κλειδί μπορεί να οδηγήσει σε μη ασφαλή συνδυασμό

Παράδειγμα: έστω F μια ισχυρή ψευδοτυχαία μετάθεση. Τότε και η F^{-1} είναι ισχυρή ψευδοτυχαία μετάθεση

Για $Enc_k(m) = F_k(m||r)$, όπου $m \in \{0,1\}^{n/2}, r \leftarrow \{0,1\}^{n/2}$ και $Mac_k(c) = F_k^{-1}(c)$, στη προσέγγιση Κρυπτογράφηση-μετά-Γνησιότητα, θα είχαμε:

$$Enc_k(m), Mac_k(Enc_k(m)) => F_k(m||r), F_k^{-1}(F_k(m||r)) => F_k(m||r), m||r$$

άρα θα αποκαλυπτόταν το m!