Ψηφιακές υπογραφές με εφαρμογή στα περιβάλλοντα του Διαδκικτύου των Πραγμάτων

Πέτρος Αμανάκης

Πανεπιστήμιο Μακεδονίας
Τμήμα Εφαρμοσμένης Πληροφορικής, Εγνατίας 156, 54636, Θεσσαλονίκη

1η Νοεμβίου 2021

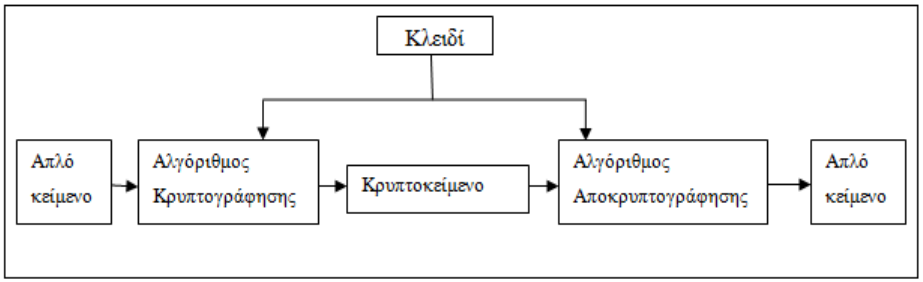
Περιεχόμενα της παρουσίασης

- Κρυπτογραφία
- Συναρτήσεις κατακερματισμού
- Μοντέλο ψηφιακής υπογραφής
- Κριτήρια εφαρμογής στο Διαδίκτυο των Πραγμάτων
- Μελέτες περίπτωσης
- Συγκριτική μελέτη και σύνοψη
- Συμπεράσματα

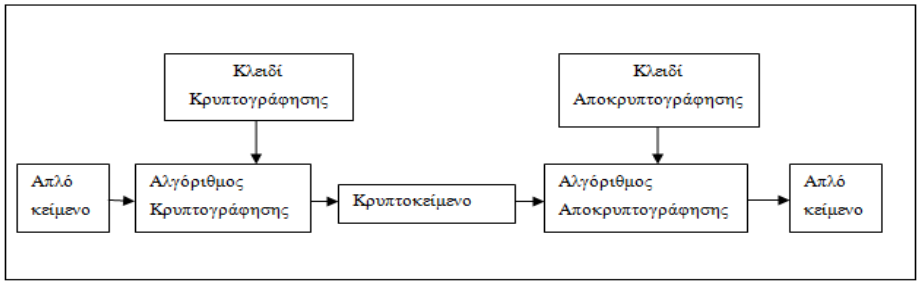
Κρυπτογραφία

Η μελέτη των μαθηματικών τεχνικών που σχετίζονται με πτυχές της ασφάλειας και του απόρρητου των πληροφοριών, όπως η εμπιστευτικότητα, η ακεραιότητα των δεδομένων, η αυθεντικοποίηση οντοτήτων και η εξακρίβωση της προέλευσης των δεδομένων (Menezes et al., 1997)

Συμμετρική



Ασύμμετρη

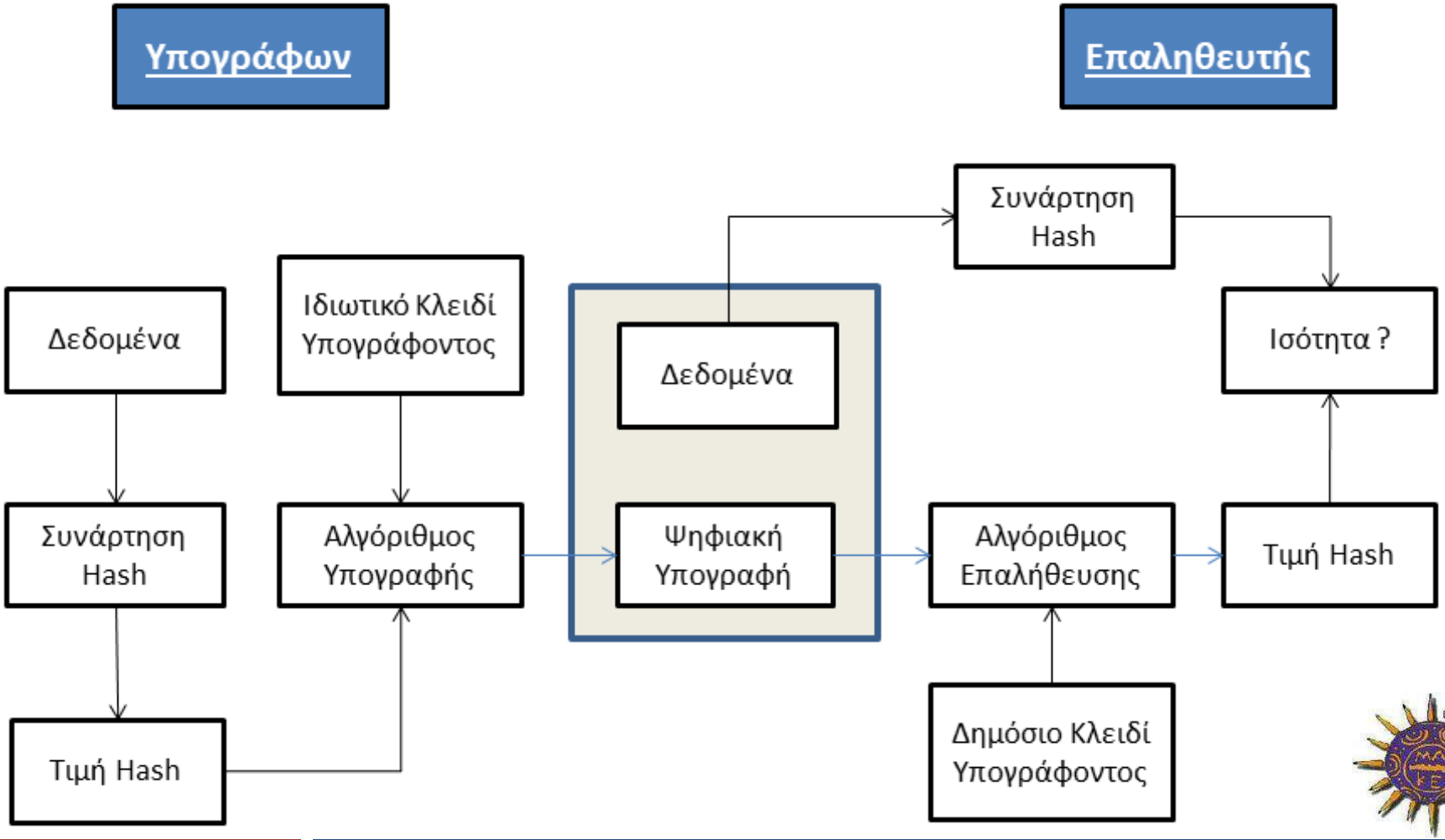


Συναρτήσεις κατακερματισμού

Λαμβάνουν ένα δυνητικά μεγάλο μήνυμα ως είσοδο και δημιουργούν μία μοναδική τιμή εξόδου (Hash) από το περιεχόμενο.

- ✓ Η είσοδος μπορεί να είναι οποιδήποτε μήκους
- ✓ Η έξοδος έχει σταθερό μήκος
- ✓ Μπορεί να υπολογίστεί σχετικά εύκολα για οποιαδήποτε είσοδο
- ✓ Είναι μονόδρομη. Είναι δύσκολο να υπολογιστεί η είσοδος από την έξοδο
- ✓ Είναι μοναδική. Δεν μπορεί να υπάρχουν δύο διαφορετικά μηνύματα που να παράγουν την ίδια τιμή κατακερματισμού.

Το μοντέλο της ψηφιακής υπογραφής



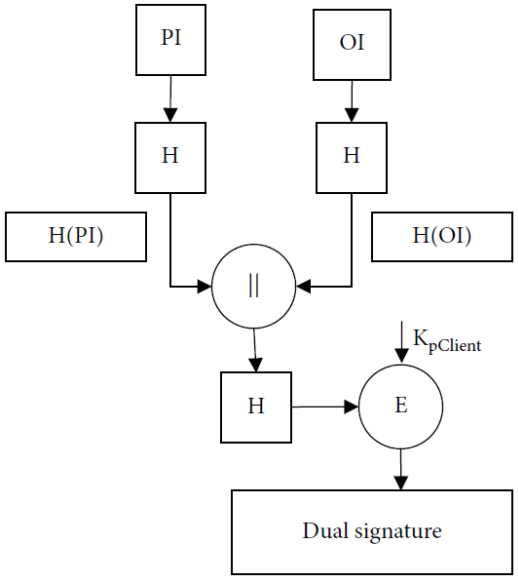
Κριτήρια εφαρμογής για το Διαδίκτυο των Πραγμάτων

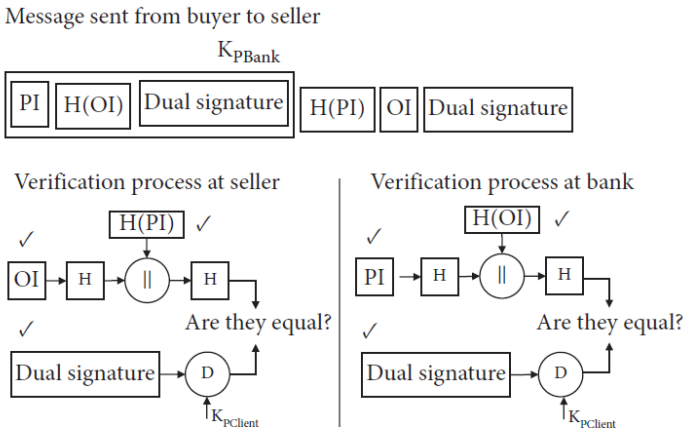
Οι συσκευές ή τα συστήματα IoT παρέχουν ποικίλες λειτουργίες, συμπεριλαμβανομένης της συλλογής, επεξεργασίας και κοινής χρήσης μεγάλων ποσοτήτων δεδομένων οποτεδήποτε και οπουδήποτε.

- ✓ Θέματα ασφαλείας για την προστασία των προσωπικών πληροφοριών
- ✓ Απαιτήσεις επεξεργαστή
- ✓ Απαιτήσεις μνήμης
- ✓ Χαμηλή κατανάλωση ενέργειας για την παροχή συνεχούς εξυπηρέτησης στους χρήστες
- ✓ Απόδοση για γρήγορη απόκριση για να διασφαλιστεί η ευκολία του χρήστη

Διατήρηση της ιδιωτικότητας των δεδομένων στο Διαδίκτυο των Ιατρικών Πραγμάτων

Οι Cano & Canavate-Sanchez (2020) ασχολήθηκαν με το ζήτημα της διασφάλισης της ιδιωτικότητας των δεδομένων στο Διαδίκτυο των Ιατρικών Πραγμάτων (IoMT) με την χρήση Διπλής Υπογραφής (Dual Signature) μέσω του Αλγόριθμου Ψηφιακής Υπογραφής Ελλειπτικής Καμπύλης (ECDSA).



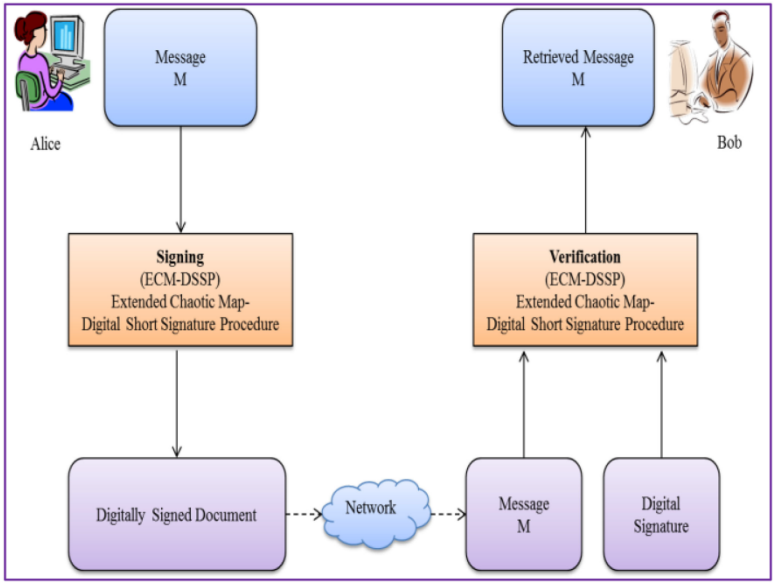


Διατήρηση της ιδιωτικότητας των δεδομένων στο Διαδίκτυο των Ιατρικών Πραγμάτων

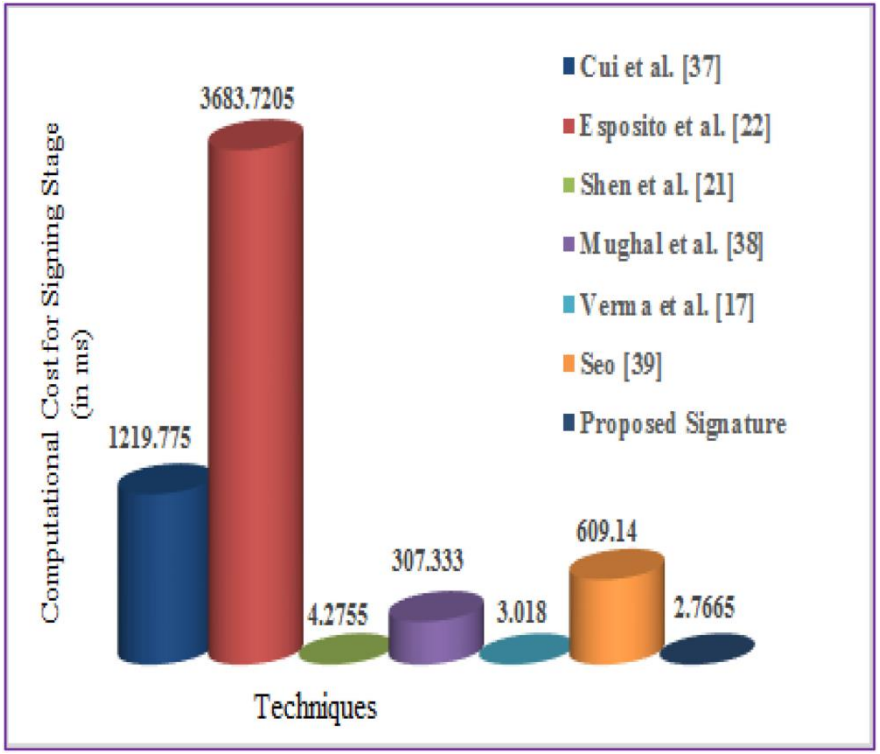
Symbol	Meaning	Time cost				
		Cryptool [40]	Boneh–Goh–Nissim [21]	Castagnos–Laguillaumie [22]	Homomorphic identity-based method [23]	Our proposal
T_{Sig}	Signature creation	2.88 ms	0.969 ms	0.924 ms	0.629 ms	0.918 ms
T_{Ver}	One signature verification	8.53 ms	14.339 ms	27.974 ms	27.349 ms	26 ms
T_{Hash}	SHA-256	15.8 cycles/byte	5.174 μs/byte	—	—	4.726 μs/byte
T_{Enc}	Time for encryption	18.2 cycles/byte	0.828 ms	0.756 ms	1.098 ms	99.82 μs/byte
T_{TOTAL_TD}	Total time at TD	—	1.7968 ms	29.656 ms	1.727 ms	21.009 ms

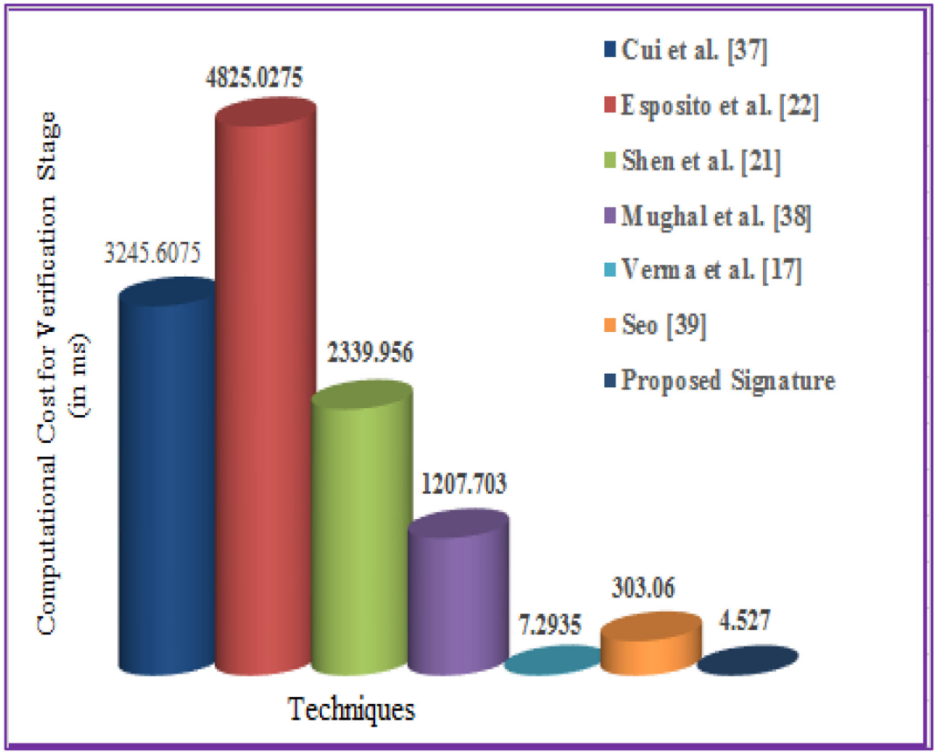
Χρήση Chaotic Maps σε ανθρωποκεντρικό Διαδίκτυο των Πραγμάτων

Οι Meshram et al. (2020) ασχολήθηκαν με την τεχνική ασφαλείας Digital Short Signature (DSST) χρησιμοποιώντας εκτεταμένους Χαοτικούς Χάρτες (Chaotic Maps) για το Ανθρωποκεντρικά συστήματα του Διαδικτύου των Πραγμάτων (HCIoT).



Χρήση Chaotic Maps σε ανθρωποκεντρικό Διαδίκτυο των Πραγμάτων





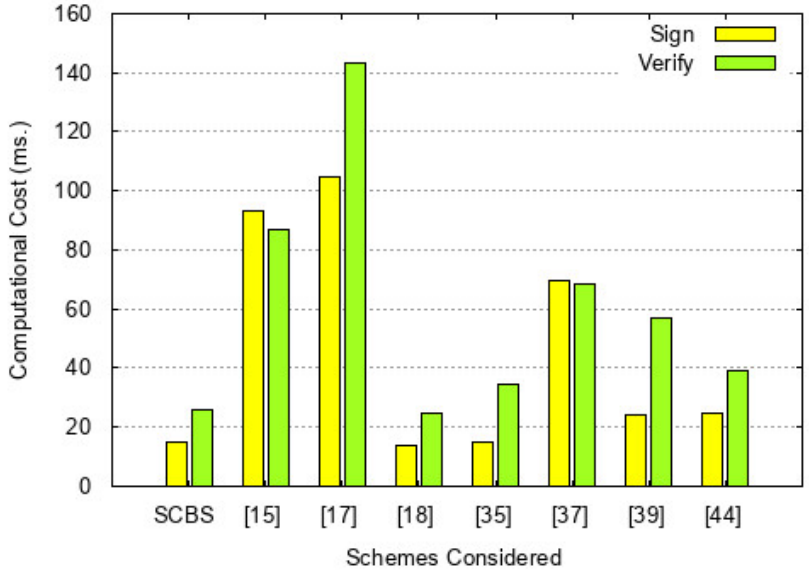
Σύντομες υπογραφές για το Βιομηχανικό Διαδίκτυο των Πραγμάτων

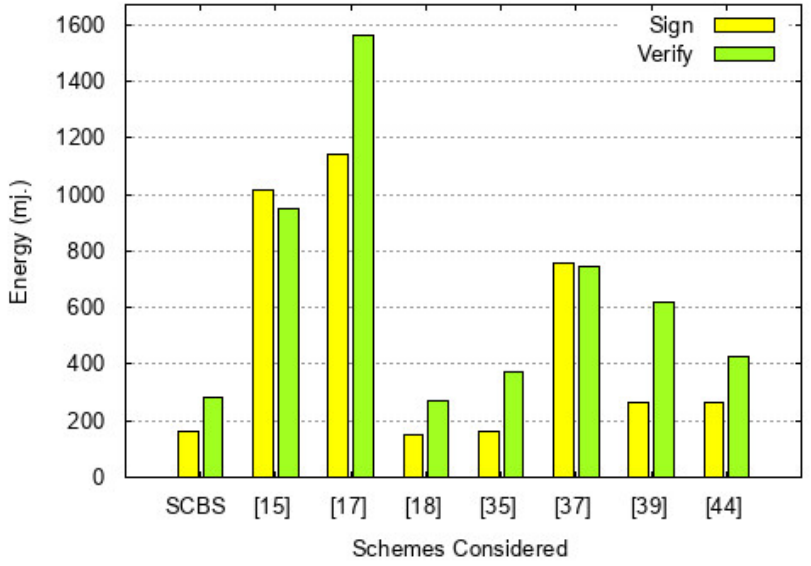
Οι Verma et al. (2021) ασχολήθηκαν με το σχήμα SCBS (Short Certificate-Based Signature) για περιβάλλον του Βιομηχανικού Διαδικτύου των Πραγμάτων (IIoT).

- Κάθε υπογράφων/χρήστης δημιουργεί τα δύο (δημόσια και μυστικά) κλειδιά του και παίρνει πιστοποιητικό για ζεύγος (ID, δημόσιο κλειδί) από την CA.
- Τα πιστοποιητικά αποστέλλονται μέσω δημόσιου καναλιού.
- Κατά τη διάρκεια της φάσης υπογραφής, ο υπογράφων απαιτεί το ενημερωμένο πιστοποιητικό του μαζί με το μυστικό κλειδί. Από την άλλη πλευρά, ο παραλήπτης χρειάζεται το ζεύγος (ID, δημόσιο κλειδί) για να επαληθεύσει την υπογραφή. Από αυτήν την κατασκευή είναι προφανές ότι η CA δεν μπορεί να έχει πρόσβαση στο μυστικό κλειδί του υπογράφοντος.

Σύντομες υπογραφές για το Βιομηχανικό Διαδίκτυο των Πραγμάτων

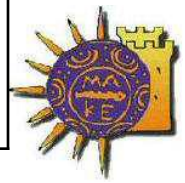
Scheme	Sign	ms.	SignVer	ms.	SignAggVer	ms.	Length	in Bits
Liu *et al.* [15]	$8T_{Exp}$	93.04	$2T_{Exp} + 4T_e$	87	NA	NA	$3\|G_T\|$	768
Li *et al.* [17]	$9T_{Exp}$	104.67	$2T_{Exp} + 7T_e$	143.37	NA	NA	$5\|G_T\|$	1280
Li *et al.* [44]	$1T_{Exp} + 1T_H$	24.52	$1T_e + 1T_{Exp} + 2T_H$	39.29	NA	NA	$\|G_T\|$	256
Li *et al.* [18]	$1T_{Exp} + 2T_m$	14.05	$4T_{Exp} + 3T_m$	24.7	NA	NA	$3\|Z_p\|$	768
Zhang *et al.* [39]	$1T_{Exp} + 1T_H$	24.52	$2T_{Exp} + 2T_e + 1T_H$	56.71	NA	NA	$2\|G_T\|$	512
Liu *et al.* [37]	$6T_{Exp}$	69.78	$2T_{Exp} + 3T_e$	68.21	NA	NA	$3\|Z_p\|$	768
Verma *et al.* [35]	$1T_{S_m}$	14.76	$4T_{S_m}$	34.48	$2(n+1)T_{S_m}$	2(n+1)8.62	$2\|G_T\| + \|Z_p\|$	768
SCBS	$1T_{S_m}$	14.76	$3T_{S_m}$	25.86	$(n+2)T_{S_m}$	(n+2)8.62	$\|G_T\| + \|Z_p\|$	512





Σύγκριση συστημάτων

	Αυθεντικοποίηση υπογραφής	Μικρές απαιτήσεις επεξεργαστή	Μικρές απαιτήσεις μνήμης	Χαμηλό εύρος ζώνης	Χαμηλή κατανάλωση ενέργειας	Απόδοση για γρήγορη απόκριση
ECDSA	√	√	√	X	X	√
DSST	√	√	√	√	X	√
SCBS	√	√	√	√	√	√



Σύγκριση συστημάτων

- ✓ ECDSA: Παρουσιάζει μεγαλύτερη κατανάλωση πόρων σε σχέση με τα υπόλοιπα.
- ✓ DSST: Τον χαμηλότερο χρόνο υπολογισμού στις λειτουργίες υπογραφής και επαλήθευσης
- ✓ SCBS: Χαμηλή κατανάλωση πόρων, χαμηλό εύρος ζώνης, χαμηλό υπολογιστικό κόστος για το στάδιο της υπογραφης

Συμπεράσματα

- ✓ Οι ψηφιακές υπογραφές χρησιμοποιούνται σχεδόν σε όλες τις μορφές των καθημερινών αναγκών, από το ηλεκτρονικό εμπόριο μέχρι και το τραπεζικό σύστημα και αποτελούν μια αποτελεσματική τεχνική για την επαλήθευση της αυθεντικότητας και της μη απόρριψης του μηνύματος.
- ✓ Οι τεχνικές ψηφιακής υπογραφής μας παρέχουν σίγουρα νέους βελτιωμένους αλγόριθμους με καλύτερη ασφάλεια από τους προηγούμενους αλγόριθμους.
- ✓ Ενδιαφέρον αποτελεί η πολλαπλότητα της χρήσης τους σε διάφορα περιβάλλοντα IoT.
- ✓ Η σχολαστική ανάλυση από την ερευνητική κοινότητα των διαφόρων συστημάτων ψηφιακής υπογραφής αντικατοπτρίζει τα πλεονεκτήματά τους όσον αφορά την απόδοση, την ορθότητα, την πολυπλοκότητα, την καταλληλότητα στα περιβάλλοντα του IoT και τη σταθερότητα απέναντι στις απειλές ασφαλείας που βρέθηκαν ως μια σημαντική πρόκληση για το IoT.

Τέλος της παρουσίασης

Σας ευχαριστώ για τον χρόνο σας και την προσοχή σας !