



Πανεπιστήμιο Πατρών  
Τμήμα Μηχανικών Η/Υ & Πληροφορικής

Πολυτεχνική Σχολή

**Ανέυρεση ιδιοτήτων που μπορούν να αυξήσουν την εμπιστοσύνη των  
Πληροφοριακών Συστημάτων**

Διπλωματική Εργασία

Δρίτσας Ηλίας  
Αριθμός Μητρώου 3369

Επιβλέπων Καθηγητής : Σπυράκης Πάυλος

Πάτρα , Ιούλιος 2011



**Ανεύρεση ιδιοτήτων που μπορούν να αυξήσουν την εμπιστοσύνη  
των Πληροφοριακών Συστημάτων**

Διπλωματική Εργασία

Δρίτσας Ηλίας

**Τριμελής Επιτροπή:**

Σπυρακής Παύλος (επιβλέπων)

Λιάγκου Βασιλική (μέλος επιτροπής)

Σταματίου Ιωάννης (μέλος επιτροπής)

Σχολή : Πολυτεχνική Σχολή

Τμήμα : Μηχανικών Η/Υ & Πληροφορικής



# Περιεχόμενα

<b>Περίληψη .....</b>	<b>σελ.12</b>
<b>Κεφάλαιο 1<sup>ο</sup> : Εισαγωγή.....</b>	<b>σελ.16</b>
1.1 Ιστορική αναδρομή.....	σελ.16
1.2 Ασφαλή και έμπιστα πληροφοριακά συστήματα.....	σελ.18
1.3 Συνεισφορά της εργασίας.....	σελ.26
1.4 Περιληπτική σύνοψη.....	σελ.27
<b>Κεφάλαιο 2<sup>ο</sup> : Κρυπτογραφία.....</b>	<b>σελ.29</b>
2.Η έννοια και η χρησιμότητα της Κρυπτογραφίας.....	σελ.29
2.1 Η έννοια της κρυπτογράφησης και αποκρυπτογράφησης.....	σελ.30
2.2 Είδη Κρυπτογραφίας.....	σελ.31
2.2.1 Συμμετρική Κρυπτογραφία.....	σελ.32
2.2.2 Ασύμμετρη Κρυπτογραφία.....	σελ.33
2.2.2.1 Πλεονεκτήματα της Ασύμμετρης Κρυπτογραφίας.....	σελ.35
2.2.2.2 Προβλήματα της Ασύμμετρης Κρυπτογραφίας.....	σελ.36
2.2.3 Σύγκριση των δύο τύπων Κρυπτογραφίας.....	σελ.37
<b>Κεφάλαιο 3<sup>ο</sup> : Το Ψηφιακό Πιστοποιητικό.....</b>	<b>σελ.38</b>
3.1 Η έννοια του Ψηφιακού Πιστοποιητικού.....	σελ.38
3.2 Πλεονεκτήματα της χρήσης Ψηφιακών Πιστοποιητικών.....	σελ.40
3.3 Επιθυμητές ιδιότητες των νέων μη παραδοσιακών Ψηφιακών Πιστοποιητικών.....	σελ.41
3.3.1 Μη συνδεσιμότητα πολλαπλών παρουσιάσεων.....	σελ.41
3.3.2 Επιλεκτική παρουσίαση των στοιχείων ενός πιστοποιητικού.....	σελ.42
3.3.3 Υπό όρους παρουσίαση των στοιχείων ενός πιστοποιητικού.....	σελ.42
3.3.4 Απόδειξη σχέσεων μεταξύ των στοιχείων ενός πιστοποιητικού.....	σελ.43
3.3.5 Τυφλή Πιστοποίηση ενός Ψηφιακού Πιστοποιητικού.....	σελ.43

<b>Κεφάλαιο 4<sup>ο</sup> :</b>	<b>Προηγούμενες Εργασίες.....</b>	<b>σελ.44</b>
<b>4.1</b>	<b>Εισαγωγή .....</b>	<b>σελ.44</b>
<b>4.2</b>	<b>Περιγραφή προηγούμενων εργασιών.....</b>	<b>σελ.44</b>
<b>4.2.1</b>	<b>Τυφλές Υπογραφές των David &amp; Chaum.....</b>	<b>σελ.44</b>
<b>4.2.2</b>	<b>Το σχήμα των Camenisch &amp; Nguyen.....</b>	<b>σελ.45</b>
<b>4.2.3</b>	<b>Το σχέδιο του Brickell.....</b>	<b>σελ.46</b>
<b>4.2.4</b>	<b>Το σχέδιο του Damgard.....</b>	<b>σελ.47</b>
<b>4.2.5</b>	<b>Το σχέδιο των τυφλών υπογραφών του Chen.....</b>	<b>σελ.47</b>
<b>4.2.6</b>	<b>Το σχέδιο των Lysyanskaya , Rivest , Sahai &amp; Wolf.....</b>	<b>σελ.47</b>
<b>4.2.7</b>	<b>Το σύστημα πιστοποιητικού του Brand.....</b>	<b>σελ.48</b>
<b>4.2.7.1</b>	<b>Διαδικασία δημιουργίας δημόσιου &amp; μυστικού κλειδιού ενός χρήστη.....</b>	<b>σελ.49</b>
<b>4.2.7.2</b>	<b>Παρουσίαση ενός πιστοποιητικού από ένα χρήστη του συστήματος σε κάποιο Παροχέα Υπηρεσιών.....</b>	<b>σελ.50</b>
<b>4.2.7.3</b>	<b>Ιδιότητες που ικανοποιούν τα χαρακτηριστικά ενός πιστοποιητικού.....</b>	<b>σελ.51</b>
<b>4.2.7.4</b>	<b>Βασικές Ιδιότητες του συστήματος του Brand.....</b>	<b>σελ.53</b>
<b>4.3</b>	<b>Σύγκριση συστήματος του Brand με προηγούμενα συστήματα πιστοποιητικού.....</b>	<b>σελ.54</b>
<b>Κεφάλαιο 5:</b>	<b>Το νέο σύστημα πιστοποιητικού.....</b>	<b>σελ.57</b>
<b>5.1</b>	<b>Εισαγωγή.....</b>	<b>σελ.57</b>
<b>5.2</b>	<b>Οντότητες που αλληλεπιδρούν στο σύστημα ανώνυμου πιστοποιητικού.....</b>	<b>σελ.58</b>
<b>5.3</b>	<b>Βασικές επιθυμητές ιδιότητες.....</b>	<b>σελ.60</b>
<b>5.4</b>	<b>Πρωτόκολλο ανάκτησης ψευδωνύμου.....</b>	<b>σελ.61</b>
<b>5.4.1</b>	<b>Βασικά χαρακτηριστικά πρωτοκόλλου ανάκτησης ψευδωνύμου.....</b>	<b>σελ.62</b>
<b>5.5</b>	<b>Ανάκληση ανωνυμίας χρήστη.....</b>	<b>σελ.63</b>

<b>5.6 Εγγραφή Ψευδωνύμου με τον Παροχέα Υπηρεσιών .....</b>	<b>σελ.64</b>
<b>5.6.1 Προτάσεις που αφορούν την εγγραφή ψευδωνύμου.....</b>	<b>σελ.64</b>
<b>5.7 Πως ένας χρήστης αποκτά πρόσβαση σε μια υπηρεσία.....</b>	<b>σελ.66</b>
<b>5.8 Περιγραφή των βασικών συναλλαγών στο νέο σύστημα πιστοποιητικού.....</b>	<b>σελ.68</b>
<b>5.8.1 Δημιουργία Ψευδωνύμου.....</b>	<b>σελ.68</b>
<b>5.8.2 Χορήγηση Πιστοποιητικού.....</b>	<b>σελ.69</b>
<b>5.8.3 Επαλήθευση Πιστοποιητικού.....</b>	<b>σελ.69</b>
<b>5.8.4 Επαλήθευση πιστοποιητικού ως προς ένα ψευδώνυμο.....</b>	<b>σελ.70</b>
<b>5.8.5 Ιδανική επικοινωνία.....</b>	<b>σελ.70</b>
<b>5.9 Το βασικό σύστημα ανώνυμου πιστοποιητικού και οι παράμετροι του.....</b>	<b>σελ.71</b>
<b>5.9.1 Δημιουργία δημόσιου και μυστικού κλειδιού από την πλευρά των οργανισμών.....</b>	<b>σελ.72</b>
<b>5.9.2 Δημιουργία Ψευδωνύμου-Πρωτόκολλο 1.....</b>	<b>σελ.72</b>
<b>5.9.3 Δημιουργία Πιστοποιητικού-Πρωτόκολλο 2.....</b>	<b>σελ.74</b>
<b>5.9.4 Παρουσίαση Πιστοποιητικού-Πρωτόκολλο 3.....</b>	<b>σελ.74</b>
<b>5.9.5 Παρουσίαση Πιστοποιητικού ως προς Ψευδώνυμο-Πρωτόκολλο 4.....</b>	<b>σελ.75</b>
<b>5.10 Η έννοια της μη μεταφερισιμότητας στο σύστημα ανώνυμου πιστοποιητικού.....</b>	<b>σελ.76</b>
<b>5.10.1 Κυκλική Κρυπτογράφηση.....</b>	<b>σελ.76</b>
<b>5.10.2 Επαληθεύσιμη Κρυπτογράφηση ως προς δεσμευμένο δημόσιο κλειδί.....</b>	<b>σελ.78</b>
<b>5.10.2.1 Τρόποι υλοποίησης μιας επαληθεύσιμης κρυπτογράφησης.....</b>	<b>σελ.78</b>
<b>5.10.3 Μη μεταφερισιμότητα.....</b>	<b>σελ.79</b>
<b>5.11 Πιστοποιητικά μιας χρήσης και διαχειριστής ανάκλησης Ανωνυμίας.....</b>	<b>σελ.80</b>
<b>5.11.1 Ο ρόλος του διαχειριστή ανάκλησης ανωνυμίας και σχετικά πρωτόκολλα.....</b>	<b>σελ.84</b>

5.11.2 Δημιουργία δημόσιου και μυστικού κλειδιού διαχειριστή ανάκλησης ανωνυμίας .....	σελ.85
5.11.3 Αλλαγές στο πρωτόκολλο δημιουργίας ψευδωνύμου.....	σελ.85
5.11.4 Ανάκληση ανωνυμίας του χρήστη U από τον επαληθευτή V.....	σελ.86
5.11.5 Πιστοποιητικά μιας χρήσης.....	σελ.87
5.11.5.1 Παρουσίαση πιστοποιητικού μιας χρήσης.....	σελ.88
5.12 Άποψη ενός συστήματος ανώνυμου πιστοποιητικού με ανάκληση ανωνυμίας.....	σελ.90
<b>Κεφάλαιο 6 : Πλαίσιο Κρυπτογραφικών Αρχών .....</b>	<b>σελ.92</b>
6.1 Αλγόριθμοι Μη Συμμετρικής Κρυπτογράφησης.....	σελ.92
6.1.1 Σχέδιο κρυπτογράφησης & αποκρυπτογράφησης των Camenisch και Shoup.....	σελ.93
6.1.1.1 Αλγόριθμος δημιουργίας κλειδιών κρυπτογράφησης & αποκρυπτογράφησης.....	σελ.96
6.1.1.2 Αλγόριθμος κρυπτογράφησης και αποκρυπτογράφησης.....	σελ.97
6.1.1.3 Επαληθεύσιμη κρυπτογράφηση διακριτών λογαρίθμων.....	σελ.97
6.2 Σχέδιο δέσμευσης.....	σελ.98
6.2.1 Ιδιότητες σχεδίου δέσμευσης .....	σελ.99
6.2.2 Σχέδιο δέσμευσης Pedersen.....	σελ.99
6.2.3 Σχέδιο δέσμευσης ακεραίων.....	σελ.100
6.2.4 Απόδειξη μήκους διακριτού λογαρίθμου.....	σελ.100
6.3 Σχέδιο ανάκτησης υπογραφών.....	σελ.102
6.3.1 SRSA σχέδιο υπογραφών και σχετικά πρωτόκολλα.....	σελ.103
6.3.2 Σχέδιο υπογραφών Camenisch& Lysyanskaya που βασίζεται στους διγραμμικούς γράφους.....	σελ.108
6.4 Κρυπτογραφικές αρχές στην πράξη.....	σελ.112



<b>Κεφάλαιο 7 : Εφαρμογές .....</b>	<b>σελ.116</b>
<b>7.1 Το σύστημα ανώνυμου πιστοποιητικού.....</b>	<b>σελ.116</b>
<b>7.2 Ανώνυμο e-cash.....</b>	<b>σελ.117</b>
<b>Παράρτημα .....</b>	<b>σελ.119</b>
<b>Επεξήγηση Μαθηματικών Συμβόλων.....</b>	<b>σελ.129</b>
<b>Ορολογία Κρυπτογραφίας -Ελληνικό Γλωσσάρι.....</b>	<b>σελ.131</b>
<b>Βιβλιογραφία.....</b>	<b>σελ.137</b>

## **Κατάλογος Σχημάτων**

**Σχήμα 1.** Σχήμα Κρυπτογράφησης - Αποκρυπτογράφησης ενός μηνύματος σελ.30

**Σχήμα 2.** Κρυπτογραφία Κλειδιού σελ.31

**Σχήμα 3.** Συμμετρικό κρυπτογραφικό σύστημα (Γενικό) σελ.32

**Σχήμα 4.** Συμμετρική Κρυπτογράφηση σελ.33

**Σχήμα 5.** Παράδειγμα συμμετρικής κρυπτογράφησης για ανταλλαγή μηνυμάτων μέσω του διαδικτύου σελ.33

**Σχήμα 6.** Σχήμα Ασύμμετρης Κρυπτογραφίας σελ.34

**Σχήμα 7.** Παράδειγμα ασύμμετρης κρυπτογραφίας για ανταλλαγή μηνυμάτων μέσω του διαδικτύου σελ.36

**Σχήμα 8 .** Άποψη Ψηφιακού Πιστοποιητικού σελ.39

**Σχήμα 9 .** Άποψη Ψηφιακού Πιστοποιητικού σελ.40

**Σχήμα 10 .** Άποψη Ψηφιακού Πιστοποιητικού σελ.40

**Σχήμα 11. –** Σύστημα Πιστοποιητικού Brand με πιστοποιητικά μιας χρήσης σελ.49

**Σχήμα 12.** Βήματα δημιουργίας ψηφιακής υπογραφής σελ.50

**Σχήμα 13.** Σύγκριση πολυπλοκότητας για διαφορετικά συστήματα πιστοποιητικού σελ.55

**Σχήμα 14.** Άποψη ενός συστήματος Ανώνυμων Πιστοποιητικών από τον πραγματικό κόσμο σελ.57

**Σχήμα 15.** Ανώνυμα πιστοποιητικά βασιζόμενα σε αποδείξεις μηδενικής γνώσης σελ.60

**Σχήμα 16.** Κρυπτογράφηση μυστικού κλειδιού με το δημόσιο κλειδί σελ.78

**Σχήμα 17. -**Σύστημα Πιστοποιητικού με Ανάκληση Ανωνυμίας σελ.87

**Σχήμα 18.** Άποψη συστήματος Ανώνυμου Πιστοποιητικού σελ.90

**Σχήμα 19.** Δημιουργία και επαλήθευση υπογραφής σελ.94

**Σχήμα 20.** Βήματα ανάκτησης υπογραφής σελ.95

**Σχήμα 21.** Πρωτόκολλο ανταλλαγής κλειδιού Diffie Hellman σελ.119

**Σχήμα 22.** Πρόβλημα διακριτού λογάριθμου σελ.120

**Σχήμα 23.** Υποδομή Δημόσιου Κλειδιού σελ.125

**Σχήμα 24.** Άποψη Single Sign On συστήματος σελ.128

## Περίληψη

Η παρούσα διπλωματική εργασία έχει ως κεντρικό θέμα την μελέτη ενός νέου μοντέλου συστήματος ανώνυμων πιστοποιητικών οι ιδιότητες του οποίου αυξάνουν την εμπιστοσύνη ενός Πληροφοριακού Συστήματος . Για την ανάπτυξη του νέου συστήματος βασιστήκαμε σε σημαντικά μαθηματικά εργαλεία και αρχές της κρυπτογραφίας . Πρωτόκολλα που διαδραμάτισαν σημαντικό ρόλο στην ανάπτυξη του νέου συστήματος , είναι τα RSA και Diffie Hellman. Σχετικές πληροφορίες για αυτά βρίσκονται στο παράρτημα της εργασίας. Η βασική ιδέα είναι το νέο σύστημα να παρέχει ασφάλεια και ανωνυμία στους χρήστες του , ενώ ταυτόχρονα αυτοί πρέπει να είναι καλά ορισμένοι (συνοχή) ώστε αν καταχραστούν την ανωνυμία τους να μπορεί να ανακτηθεί είτε το ψευδώνυμο είτε η ταυτότητά τους από τον Διαχειριστή Ανάκλησης Ανωνυμίας. Δύο ακόμα σημαντικές αρχές που περιγράφονται στην εργασία αποτελούν η κυκλική και η επαθληθεύσιμη κρυπτογράφηση ως προς δεσμευμένο δημόσιο κλειδί. Με τη βοήθεια αυτών εισήχθει μια ακόμα ιδιότητα που αποτελεί ακρογωνιαίό λίθο για την αύξηση της εμπιστοσύνης του νέου συστήματος, η μη μεταφερσιμότητα. Η μη μεταφερσιμότητα ψευδωνύμων και πιστοποιητικών αποθαρρύνει ή αποτρέπει του χρηστές να μοιράζονται ή και να δανείζουν τα ψευδώνυμα και πιστοποιητικά τους σε άλλους χρήστες. Κανένας χρήστης δεν μπορεί να αποκτήσει πιστοποιητικό για κάποιον άλλο χρήστη-φίλο του, δεδομένου ότι όλα τα πιστοποιητικά ενός χρήστη υπάγονται στο ίδιο κύριο κλειδί  $K_U$  . Μια ακόμα χρήσιμη ιδιότητα του νέου συστήματος , είναι η δυνατότητα χρήσης πιστοποιητικών πολλαπλής χρήσης. Αυτό σημαίνει ότι το ίδιο πιστοποιητικό μπορεί να χρησιμοποιηθεί όσες φορές κριθεί απαραίτητο χωρίς να απαιτείται επανέκδοση του ίδιου πιστοποιητικού. Ταυτόχρονα εξασφαλίζεται η μη συνδεσιμότητα πιστοποιητικών και ψευδωνύμων. Αυτό σημαίνει ότι δεν μπορεί να προσδιοριστεί η ταυτότητα ή το ψευδώνυμο ενός χρήστη απλά από διαφορετικές χρήσεις του ίδιου πιστοποιητικού , παρά μόνο αν ο συγκεκριμένος χρήστης προβεί σε παράνομες συναλλαγές και καταχραστεί την ανωνυμία που του παρέχει το νέο σύστημα.

Επιπλέον , η διπλωματική εργασία περιλαμβάνει χρήσιμες πληροφορίες για σχέδια κρυπτογράφησης –αποκρυπτογράφησης μηνυμάτων , σχέδια απόκτησης και ελέγχου εγκυρότητας υπογραφής και σχέδια δέσμευσης ποσοτήτων (δεσμευμένα μηνύματα , δεσμευμένο δημόσιο κλειδί ). Όσον αφορά τα σχέδια δέσμευσης , αντί να χρησιμοποιήσουμε άμεσα κάποια ποσότητα χρησιμοποιούμε τη δέσμευση αυτής. Κάποιος που γνωρίζει την τιμή αυτή είναι υπολογιστικά δύσκολο να εκτιμήσει τη σωστή ποσότητα γεγονός που αυξάνει την ασφάλεια του νέου συστήματος. Όλα τα πρωτόκολλα βασίζονται σε αποδείξεις μηδενικής γνώσης γεγονός που ενισχύει ακόμα περισσότερο την ασφάλεια του νέου συστήματος.Επίσης παρουσιάζουμε και ένα σχέδιο υπογραφών που θεμελιώνεται όχι μόνο σε αποδείξεις μηδενικής γνώσης αλλά και στους διγραμμικούς γράφους. Οι διγραμμικοί γράφοι αποτελούν ένα εργαλείο της κρυπτογραφίας το οποίο προσεγγίζει με έναν διαφορετικό τρόπο τη δημιουργία και επαλήθευση μιας υπογραφής καθώς και τις αποδείξεις γνώσης υπογραφής ως προς δεσμευμένα μηνύματα. Η παραπάνω μελέτη ολοκληρώνεται παρουσιάζοντας δύο παραδείγματα από τον πραγματικό κόσμο που ικανοποιούν τις ιδιότητες ,αρχές και σχέδια που αναφέρθηκαν παραπάνω. Τέλος , στο παράρτημα της διπλωματικής εργασίας υπάρχει κώδικας υλοποιημένος σε Java του πρωτοκόλλου Diffie Hellman και εκτίμηση του χρόνου εκτέλεσης του πρωτοκόλλου για διάφορα μήκη κλειδιού.

## **Λέξεις Κλειδιά**

Κρυπτογραφία , Ασφάλεια, Πιστοποιητικό,Ψευδώνυμο,Ψηφιακή Υπογραφή,  
Ασφαλές Πληροφοριακό Σύστημα,Εμπιστοσύνη

## **Ευχαριστίες**

Στο σημείο αυτό θα ήθελα να ευχαριστήσω την οικογένειά μου, την κ.Λιάγκου Βασιλική για τη βοήθεια και την καθοδήγηση σε όλη τη διάρκεια εκπόνησης της διπλωματικής εργασίας, τον κ.Σταματίου Ιωάννη για την ενθάρρυνση και την καθοδήγησή του καθώς επίσης και τον καθηγητή κ.Σπυράκη Παύλο για την εμπιστοσύνη που μου έδειξε όταν μου έδωσε το συγκεκριμένο θέμα. Τέλος, θα ήθελα να ευχαριστήσω τη φίλη μου Τρίγκα Μαρία τελειόφοιτη του τμήματος Ηλεκτρολόγων Μηχανικών & Τεχνολογίας Η/Υ για την επίσης πολύτιμη βοήθεια και υποστήριξή της όλο αυτό το διάστημα.



## Κεφάλαιο 1<sup>ο</sup> : Εισαγωγή

### 1.1 Ιστορική αναδρομή

Η εμπιστοσύνη είναι ένα βασικό χαρακτηριστικό της ανθρώπινης ζωής. Συχνά αναφέρεται σε μηχανισμούς για να αποδείξει κάποιος ότι η πηγή των πληροφοριών είναι η πηγή που πραγματικά παρουσιάζει ότι είναι. Η διαχείριση της εμπιστοσύνης μπορεί να ερμηνευτεί με δύο τρόπους. Πρώτον, σαν μια διαδικασία όπου κάποιο άτομο Α είναι αξιόπιστο για άλλα άτομα. Αυτή η εμπιστοσύνη αποτελεί σημαντικό κριτήριο επιτυχίας και επιβίωσης καθώς επιτρέπει σε διάφορα άτομα να συνεργάζονται με τον Α. Δεύτερον, σαν μια διαδικασία εκτίμησης της αξιοπιστίας άλλων ανθρώπων, διαδικασία η οποία είναι τόσο σημαντική όσο η προηγούμενη. Λαμβάνοντας υπόψη και τις δύο παραπάνω απόψεις καταλήγουμε στον παρακάτω ορισμό της διαχείρισης εμπιστοσύνης όπως αναφέρεται από τους Grudexewski, Hejduk, Sankoska και Wantuchwicz:

«Οι δραστηριότητες για τη δημιουργία συστημάτων και μεθόδων που επιτρέπουν έμπιστες ομάδες να :

1. Κάνουν εκτιμήσεις και να παίρνουν αποφάσεις λαμβάνοντας υπόψη την αξιοπιστία πιθανών συναλλαγών που περιλαμβάνουν ρίσκο.
2. Επιτρέπουν στους χρήστες και τους δημιουργούς συστημάτων να αυξήσουν και να παρουσιάσουν σωστά την αξιοπιστία των ιδίων όπως και των συστημάτων τους».[4]

Η ουσία της διαχείρισης εμπιστοσύνης δεν είναι η εμπιστοσύνη η ίδια, αλλά να παίρνουμε σωστές αποφάσεις για τα όρια της εμπιστοσύνης και τον τρόπο που θα δημιουργήσουμε έμπιστες σχέσεις. Το «σταδιακό χτίσιμο» της εμπιστοσύνης είναι η καλύτερη στρατηγική για τη Διαχείριση Εμπιστοσύνης, γιατί δεν επικεντρώνεται τόσο στο παρόν, αλλά κυρίως σε μελλοντικές συνεργασίες.

Σε όλους του τομείς της ανθρώπινης καθημερινότητας (ανθρώπινες σχέσεις, οικονομία, πολιτική κ.α.), συνήθως πριν πραγματοποιηθεί οποιαδήποτε μορφή συναλλαγής μια σχέση αμοιβαίας εμπιστοσύνης πρέπει να εγκατασταθεί μεταξύ των συναλλασσομένων.



Το πιο εύκολο και απλό είναι να αποκαλύψουν και οι δύο την ταυτότητα τους· ωστόσο η κοινοποίηση στοιχείων που συνδέονται μοναδικά με ένα συγκεκριμένο άτομο δεν είναι ασφαλής αφού παραβιάζεται η ιδιωτικότητα των ατόμων. Το πρόβλημα προστασίας της ιδιωτικότητας είναι μεγίστης σημασίας και αφορά την ελεγχόμενη δημοσιοποίηση προσωπικών στοιχείων. Υπάρχουν διάφορα μέσα που ως στόχο έχουν την προστασία της ιδιωτικότητας. Για παράδειγμα το δικαίωμα ενός ατόμου να έχει πρόσβαση στα προσωπικά δεδομένα του και να απαιτεί τη διόρθωση αυτών, καθώς και η συγκατάθεση του στην κοινοποίηση προσωπικών δεδομένων του. Ένας ακόμα τρόπος έχει σχέση με την ελαχιστοποίηση των στοιχείων που αποκαλύπτονται. Σύμφωνα με αυτόν κάθε άτομο μπορεί να αποκαλύπτει το ελάχιστο, αναγκαίο ποσό πληροφορίας που απαιτείται για το συγκεκριμένο σκοπό. Ο καθορισμός των στοιχείων αυτών είναι δύσκολος διότι πρέπει να βρεθεί η χρυσή τομή ανάμεσα στο προσωπικό και το νομικό συμφέρον των συναλλασσομένων.

Όταν τα δεδομένα αποθηκεύονται σε ψηφιακή μορφή το πρόβλημα της ιδιωτικότητας γίνεται ακόμα πιο σοβαρό σε σχέση με τις σε χαρτί διαδικασίες. Από τη στιγμή που τα ψηφιακά δεδομένα δημοσιοποιηθούν, μπορούν πολύ εύκολα να αποθηκευτούν, να διανεμηθούν, και να συνδεθούν με άλλα δεδομένα, γεγονός που παραβιάζει το ιδιωτικό απόρρητο. Από τη μία η χρήση ψηφιακών μέσων επιβαρύνει το πρόβλημα προστασίας της ιδιωτικότητας, από την άλλη όμως δίνει την ευκαιρία σε νέες τεχνολογίες να υλοποιήσουν αρχές (κρυπτογραφικές) που να εξασφαλίζουν και να βελτιώνουν την προστασία της.

Το θέμα της ασφάλειας είναι εξαιρετικά δύσκολο να καθοριστεί με ακριβή τρόπο. Εντούτοις, οι περισσότεροι άνθρωποι διαφένεται να συμφωνούν ότι στην ασφάλεια των πληροφοριακών συστημάτων, υπάρχουν ορισμένες θεμελιώδεις πτυχές, μερικές φορές καλούμενες ως στόχοι ασφάλειας που είναι σημαντικό και απαραίτητο να εκτιμηθούν πριν από την κατασκευή ενός ασφαλούς και έμπιστου πληροφοριακού συστήματος. Έτσι λοιπόν, στην ενότητα που ακολουθεί κρίνεται απαραίτητο να μελετήσουμε εκτενώς οτιδήποτε αφορά την ασφάλεια (κινδύνους, μηχανισμούς, υπηρεσίες) ενός πληροφοριακού συστήματος

## 1.2 Ασφαλή και έμπιστα Πληροφοριακά Συστήματα

Πολλές εφαρμογές της κρυπτογραφίας καθώς επίσης και εργαλεία της εφαρμόζονται έτσι ώστε να μπορέσουν να αυξήσουν την εμπιστοσύνη και την ασφάλεια στα πληροφοριακά συστήματα. Στην παρούσα διπλωματική εργασία το σύστημα ανώνυμων πιστοποιητικών που παρουσιάζεται είναι εφαρμόσιμο σε πληροφοριακά συστήματα. Έτσι λοιπόν, πριν αναλύσουμε το νέο σύστημα είναι απαραίτητο να δούμε τι είναι ένα πληροφοριακό σύστημα, βασικές αρχές ασφαλούς λειτουργίας, κινδύνους ασφαλείας, απαιτήσεις ασφαλείας, υπηρεσίες ασφαλείας και μηχανισμούς υλοποίησης της ασφάλειας σε ένα πληροφοριακό σύστημα.

### Βασικές αρχές

Οι θεμελιακές αρχές χρήσης και λειτουργίας των πληροφοριακών συστημάτων πρέπει να ικανοποιούν τις ακόλουθες απαιτήσεις ασφαλείας:

- Οι πληροφορίες που συσχετίζονται με προσωπικά δεδομένα θα πρέπει να διαχειρίζονται από το συνολικό σύστημα με σκοπό τη βελτίωση των παρεχομένων υπηρεσιών προς τους πολίτες.
- Η διαχείριση των πληροφοριών θα πρέπει να γίνεται αποκλειστικά από κατάλληλο εξουσιοδοτημένο προσωπικό.
- Τα δικαιώματα πρόσβασης στο σύστημα θα πρέπει να έχουν προσδιοριστεί με διαδικασίες ανεξάρτητες της φάσης υλοποίησης του πληροφοριακού συστήματος. Ο καθορισμός των διαδικασιών αυτών γίνεται σε επίπεδο νομοθετικό (νόμοι, διατάγματα), οργανωτικό (κανόνες λειτουργίας οργανισμού, καθηκοντολόγιο) και δομικό (κατάλληλη στελέχωση, υπεύθυνη επιτροπή ασφαλείας).
- Η παροχή εμπιστευτικών πληροφοριών προς τρίτους θα επιτρέπεται κατόπιν έγγραφης άδειας του άμεσα ενδιαφερόμενου.
- Οι μηχανισμοί ασφαλείας, δε θα πρέπει να μειώνουν τη συνολική αποτελεσματικότητα του συστήματος. Στη περίπτωση που δεν είναι δυνατή η εφαρμογή του προηγούμενου αξιώματος, θα πρέπει να υπάρχει ικανοποιητική ισορροπία μεταξύ απόδοσης και ασφαλείας του συστήματος.

Συμπερασματικά, η σωστή ανάπτυξη και η αποδοτική λειτουργία πληροφοριακών συστημάτων είναι μια διαδικασία, που εμπεριέχει αναπόσπαστα τη ταυτόχρονη δόμηση ενός πλαισίου ασφάλειας, το οποίο να εξασφαλίζει τις απαιτήσεις ορθότητας, διαθεσιμότητας και μυστικότητας των περιεχομένων πληροφοριών.

### **Σχεδιασμός ασφαλών πληροφοριακών συστημάτων**

Οι διαδικασίες καθορισμού των απαιτήσεων ασφάλειας ενός συστήματος θα πρέπει να σχηματοποιούνται κατά την αρχική φάση καταγραφής και σχεδιασμού του. Στην πραγματικότητα, όμως, οι μηχανισμοί ασφάλειας (στις περιπτώσεις που υπάρχουν), αναπτύσσονται στα τελευταία στάδια ή μετά την υλοποίησή τους, με στόχο την αντιμετώπιση των προβλημάτων ασφάλειας που προέκυψαν στα πρώτα στάδια λειτουργίας τους.

### **Επιτακτική η ανάγκη για την ασφάλεια ενός πληροφοριακού συστήματος**

#### **Ορισμός Πληροφοριακού Συστήματος (Π.Σ.)**

Πληροφοριακό σύστημα σημαίνει ότι ένας αριθμός αλληλεπιδρώντων στοιχείων έχουν οργανικά συναρμολογηθεί σε μια ολότητα, έτσι ώστε να εκτελέσουν μια ορισμένη λειτουργία. Τα στοιχεία αυτά είναι:

- α) Ο άνθρωπος, αφού τα Π.Σ. δημιουργούνται από αυτόν και λειτουργούν με τη βοήθειά του, έτσι ώστε να υπηρετήσουν πάλι αυτόν.
- β) Η πληροφορία, ένα αγαθό με πολύ μεγάλη ζήτηση.
- γ) Η πληροφορική, η επιστήμη/τεχνολογία που σκοπό έχει την επεξεργασία της πληροφορίας.

Με άλλα λόγια το Πληροφοριακό Σύστημα είναι μια συλλογή από το μηχανικό/υλικό μέρος, το λογισμικό, τα μέσα αποθήκευσης, τα δεδομένα και τους ανθρώπους που ένας οργανισμός χρησιμοποιεί για να πετύχει τα λειτουργικά βήματα που θέλει.

Εξαιτίας του ρόλου που παίζει το Π.Σ. σε μια επιχείρηση και όχι μόνο, είναι φυσικό να απαιτεί ασφάλεια και προστασία.

Συνεπώς τα Π.Σ. θα πρέπει να προστατεύονται από κάθε μορφή απειλής, χωρίς όμως η προστασία αυτή να παρεμποδίζει τη ροή των πληροφοριών.

*Ασφάλεια Πληροφοριακού Συστήματος* είναι το οργανωμένο πλαίσιο από έννοιες, αντιλήψεις, αρχές, πολιτικές, διαδικασίες, τεχνικές και μέτρα που απαιτούνται για να προστατευθούν τα στοιχεία του Π.Σ., αλλά και το σύστημα ολόκληρο από κάθε σκόπιμη ή τυχαία απειλή. Μια αναγκαία συνθήκη για να είναι δυνατή η αποτίμηση της ασφάλειας, είναι η ύπαρξη ενός συνόλου απαιτήσεων που δεν πρέπει για κανένα λόγο να απουσιάζουν ή να αγνοούνται.

### **Απαιτήσεις ασφαλείας**

Η ευρεία χρήση των πληροφοριακών συστημάτων για την αποθήκευση ,επεξεργασία και μετάδοση της ψηφιακής πληροφορίας αποτελεί μια αναγκαιότητα της σημερινής κοινωνίας. Η πληροφορία που παράγει ή διαχειρίζεται ένας οργανισμός κατά την λειτουργία του , είναι ένα αντικείμενο ζωτικής σημασίας.

Αυτό ισχύει σε μικρότερο ή μεγαλύτερο βαθμό για όλους τους οργανισμούς ανεξάρτητα από το είδος , το μέγεθος, και τον επιχειρηματικό κλάδο στον οποίο δραστηριοποιείται ο κάθε οργανισμός. Για το λόγο αυτό, είναι ιδιαίτερα σημαντικό θέμα , η προστασία τη πληροφορίας του οργανισμού. Η πληροφορία εδώ νοείται με την πλέον γενική της έννοια και μπορεί να διατεθεί σε διάφορες μορφές όπως , έντυπη ή χειρόγραφη , σε ηλεκτρονική μορφή αποθηκευμένη σε συστήματα υπολογιστών ή διακινούμενη σε δίκτυα κάθε είδους , μέσω ηλεκτρονικού ταχυδρομείου ή άλλων υπηρεσιών.

Στο σημερινό ανταγωνιστικό χώρο των επιχειρήσεων αλλά και άλλων οργανισμών κάθε τύπου , η πληροφορία είναι ένα επαπειλούμενο αντικείμενο και οι απειλές μπορούν να προέρχονται από πολλές πηγές. Οι απειλές μπορούν να είναι εσωτερικές ή εξωτερικές. Μπορούν να είναι συμπτωτικές ή να προέρχονται από ηθελημένη κακή πρόθεση πρόκλησης ζημιών στον οργανισμό.

Υπάρχει λοιπόν η ανάγκη για κάθε οργανισμό να προστατέψει την ζωτική του πληροφορία , καθώς και την πληροφορία που αφορά τους πελάτες του , αναπτύσσοντας την κατάλληλη Πολιτική Ασφάλειας Πληροφοριών και λαμβάνοντας όλα τα απαραίτητα μέτρα για την υλοποίησή της.

Οι απαιτήσεις ασφαλείας του οργανισμού προκύπτουν ύστερα από μεθοδική καταγραφή των κινδύνων που αντιμετωπίζει ο οργανισμός. Το κόστος των μηχανισμών ασφαλείας θα πρέπει να δικαιολογείται από πιθανή ζημιά στον οργανισμό σε περίπτωση που παραβιαστεί η ασφάλειά του.

## **Κίνδυνοι Ασφαλείας**

Η αποτίμηση των κινδύνων ασφαλείας είναι μια συστηματική εξέταση των ακόλουθων παραγόντων:

- Της πιθανής ζημιάς που θα υποστεί ο οργανισμός σε περίπτωση που προκύψει κάποιος κίνδυνος ασφαλείας, συμπεριλαμβανομένων των συνεπειών από την απώλεια της εμπιστευτικότητας, της ακεραιότητας ή της διαθεσιμότητας των πληροφοριών.
- Της ρεαλιστικής εκτίμησης της πιθανότητας να εμφανιστεί ένας τέτοιος κίνδυνος ασφαλείας σε σχέση με τους υπάρχοντες μηχανισμούς ελέγχου.

Τα αποτελέσματα αυτής της αποτίμησης καθορίζουν τις κατάλληλες ενέργειες και προτεραιότητες του οργανισμού, καθώς και τους τρόπους υλοποίησης των μηχανισμών ελέγχου της ασφάλειας απέναντι σε αυτούς τους κινδύνους. Η διαδικασία αποτίμησης των κινδύνων και η επιλογή των κατάλληλων μηχανισμών ελέγχου μπορεί να επαναληφθεί πολλές φορές προκειμένου να καλύψει διαφορετικά τμήματα του οργανισμού.

Είναι σημαντικό να γίνεται περιοδικός έλεγχος των κινδύνων ασφαλείας όπως και των μηχανισμών προστασίας προκειμένου να επιτυγχάνεται προσαρμογή στις ανάγκες και τις προτεραιότητες του οργανισμού, επέκταση στην προστασία από νέους κινδύνους, καθώς και επιβεβαίωση της ορθής και αποτελεσματικής λειτουργίας των υπάρχοντων μηχανισμών προστασίας.

## **Υπηρεσίες ασφαλείας**

Σκοπός των υπηρεσιών ασφαλείας είναι να εξασφαλίσουν ότι το δίκτυο θα μπορεί να παρέχει συνεχώς τις υπηρεσίες του στο επίπεδο και με την ποιότητα που απαιτούνται για να ανταποκριθεί στο σκοπό που εξυπηρετεί. Οι υπηρεσίες ασφαλείας κατηγοριοποιούνται ως εξής:

**Υπηρεσία αυθεντικοποίησης:** Η υπηρεσία αυθεντικοποίησης παρέχει εγγύηση για την ταυτότητα μιας οντότητας. Αυτό σημαίνει ότι όταν ισχυρίζεται κάποιος ότι έχει μια συγκεκριμένη ταυτότητα (ή ένα συγκεκριμένο συνθηματικό), η υπηρεσία εξακρίβωσης ταυτότητας θα παρέχει τα μέσα για να επιβεβαιώσει την ορθότητα αυτού του ισχυρισμού. Υπάρχουν δύο είδη εξακρίβωσης ταυτότητας:

1. Εξακρίβωση ταυτότητας χρήστη
2. Εξακρίβωση ταυτότητας προέλευσης δεδομένων

Δηλαδή ο αποστολέας και ο νόμιμος παραλήπτης επιζητούν να επιβεβαιώνει ο ένας την ταυτότητα του άλλου , έτσι ώστε ο παραλήπτης να μπορεί να είναι σίγουρος ότι ο αποστολέας είναι πράγματι αυτός που ισχυρίζεται. Για παράδειγμα , εάν ο χρήστης Β λάβει ένα μήνυμα από τον χρήστη Α , θα πρέπει να πιστοποιήσει την ταυτότητα του Α και να ξέρει ότι το μήνυμα που έλαβε είναι πράγματι από αυτόν.

**Υπηρεσία ακεραιότητας:** Η υπηρεσία προστασίας ακεραιότητας πρέπει να εξασφαλίσει την ακεραιότητα ενός μηνύματος. Δηλαδή το μήνυμα δεν έχει παραποιηθεί και προέρχεται από τον «νόμιμο» αποστολέα. Επομένως πρέπει να προστατευτούν τα δεδομένα των υπολογιστικών κι επικοινωνιακών πόρων από την τροποποίηση , διαγραφή ή αντικατάσταση τους από μη εξουσιοδοτημένες οντότητες , χωρίς αυτό να γίνει αντιληπτό.

Οποιοδήποτε μη εξουσιοδοτημένο άτομο δεν θα πρέπει να είναι σε θέση να παραποιήσει την πληροφορία κατά τη μετάδοση της. Δηλαδή ένας χρήστης Α στέλνει ένα μήνυμα στο χρήστη Β , το περιεχόμενο του μηνύματος θα πρέπει να μην αλλαχθεί και να παραμείνει ίδιο με αυτό που έστειλε ο Α.

Η ακεραιότητα δεδομένων από μόνη της δεν έχει νόημα, γιατί δεν αρκεί η πληροφορία να μην μεταβάλλεται κατά τη μετάδοση της , αλλά πρέπει ταυτόχρονα και η πηγή προέλευσης της να είναι αυθεντική. Για αυτό το λόγο η υπηρεσία ακεραιότητας δεδομένων πρέπει αν συνδυάζεται με την εξακρίβωση ταυτότητας της πηγής προέλευσης των δεδομένων. Τα δεδομένα σε κάθε σύστημα πρέπει να παραμένουν πλήρη και ορθά.

**Υπηρεσίες μη αποποίησης ευθύνης :** Ο σκοπός των υπηρεσιών αυτών είναι να προστατεύει από την άρνηση συμμετοχής μιας οντότητας σε μια σύνοδο επικοινωνίας. Επίσης, σκοπός τους είναι να εξασφαλίσουν ότι η οντότητα που έλαβε το μήνυμα να μην μπορεί να αρνηθεί ότι πράγματι το έλαβε. Δηλαδή , ο αποστολέας της πληροφορίας δεν μπορεί, σε κάποια μεταγενέστερη χρονική στιγμή , να αρνηθεί την πρόθεση, τη δημιουργία και την αποστολή της πληροφορίας.

Αντίστοιχα , ο παραλήπτης της πληροφορίας δεν μπορεί σε κάποια μεταγενέστερη χρονική στιγμή να αρνηθεί την παραλαβή και την επεξεργασία της πληροφορίας.Η μη αποποίηση ευθύνης μαζί με τον έλεγχο της προέλευσης δεδομένων προστατεύει από τις προσπάθειες του αποστολέα να αρνηθεί ότι έστειλε το μήνυμα , ενώ μαζί με τον έλεγχο παράδοσης προστατεύει από προσπάθειες του παραλήπτη να αρνηθεί ψευδώς,την παραλαβή του μηνύματος.Μπορούμε να επιτυγχάνουμε μη αποποίηση ευθύνης με τη χρήση των ψηφιακών υπογραφών.

**Υπηρεσίες εμπιστευτικότητας:** Σκοπός των υπηρεσιών εμπιστευτικότητας είναι να προστατεύουν τα δεδομένα που διακινούνται στο διαδίκτυο από αποκάλυψη σε μη εξουσιοδοτημένες οντότητες.Αν δεν υπάρχει εμπιστευτικότητα παραβιάζεται το δικαίωμα των ατόμων και των εταιριών για μυστικότητα.Η εμπιστευτικότητα παίζει ουσιαστικό και σημαντικό ρόλο στο χώρο των τηλεπικοινωνιών και των ηλεκτρονικών συναλλαγών.Η πληροφορία πρέπει να γίνεται κατανοητή μόνο από τον νόμιμο αποδέκτη της. Για κάθε άλλον η πληροφορία θα παραμένει σε ακατανόητη μορφή.Για παράδειγμα ο χρήστης Α στέλνει ένα μήνυμα στο χρήστη Β τότε θα ο Β (και μόνο ο Β) να είναι σε θέση να διαβάσει και να κατανοήσει την πληροφορία.

**Υπηρεσίες ελέγχου πρόσβασης:** Ο σκοπό των υπηρεσιών αυτών είναι να προστατεύουν τους πόρους , τα στοιχεία ,τα αρχεία ,τα δεδομένα και τις εφαρμογές του δικτύου από μη εξουσιοδοτημένη προσπέλαση.Πιθανότατα είναι οι υπηρεσίες εκείνες που έρχονται πρώτες στο μυαλό μας,όταν αναφεόμαστε σε ασφάλεια υπολογιστών ή δικτύων. Οι υπηρεσίες αυτές σχετίζονται πολύ στενά με την αναγνώριση του χρήστη και την αυθεντικοποίηση, χρησιμοποιούνται σε δικτυακά περιβάλλοντα για να ελέγξουν την πρόσβαση σε πόρους και υπηρεσίες του δικτύου , σε εφαρμογές και σε δεδομένα.

### **Μηχανισμοί ασφαλείας**

Οι υπηρεσίες ασφαλείας που περιγράψαμε πιο πάνω υλοποιούνται με ένα σύνολο μηχανισμών ασφαλείας.Οι μηχανισμοί , τους οποίους θα περιγράψουμε με λεπτομέρεια αμέσως μετά , είναι οι εξής:

**Κρυπτογράφηση:** Ο μηχανισμός της κρυπτογράφησης χρησιμοποιείται για την υλοποίηση της υπηρεσίας της εμπιστευτικότητας , είτε πρόκειται για δεδομένα είτε για πληροφορίες δρομολόγησης. Ο μηχανισμός μπορεί να χρησιμοποιηθεί και από άλλους μηχανισμούς ασφαλείας. Οι αλγόριθμοι κρυπτογράφησης είναι αντιστρέψιμοι ή μη αντιστρέψιμοι. Οι αντιστρέψιμοι αλγόριθμοι διακρίνονται σε συμμετρικούς και ασύμμετρους. Οι συμμετρικοί χρησιμοποιούν ένα μυστικό κλειδί κρυπτογράφησης και η γνώση του κλειδιού αυτού συνεπάγεται και τη γνώση επίσης του κλειδιού αποκρυπτογράφησης. Αντίθετα, οι ασύμμετροι αλγόριθμοι κρυπτογράφησης χρησιμοποιούν ένα δημόσιο κλειδί κρυπτογράφησης του οποίου η γνώση δε συνεπάγεται τη γνώση του ιδιωτικού κλειδιού αποκρυπτογράφησης. Οι μη αντιστρέψιμοι αλγόριθμοι κρυπτογράφησης είναι δυνατόν να μη χρησιμοποιούν κλειδί. Αν χρησιμοποιείται κλειδί , αυτό μπορεί να είναι δημόσιο ή ιδιωτικό.

**Ψηφιακές Υπογραφές:** Ο μηχανισμός αυτός αποδεικνύει σε κάποιον τρίτο ότι ο υπογράφων και μόνο αυτός είναι δυνατόν να παράγει την υπογραφή αυτή. Ο μηχανισμός εμπεριέχει δύο διαδικασίες : τη διαδικασία υπογραφής μιας ομάδας δεδομένων και τη διαδικασία επαλήθευσης της υπογραφής που συνοδεύει μια ομάδα δεδομένων. Η διαδικασία υπογραφής χρησιμοποιεί το ιδιωτικό κλειδί του υπογράφοντα για να κρυπτογραφήσει ολόκληρη την ομάδα δεδομένων ή μια κρυπτογραφική τιμή που παράγεται από την ομάδα δεδομένων.

Η διαδικασία επαλήθευσης υπογραφής χρησιμοποιεί το δημόσιο κλειδί υπογράφοντα για να καθορίσει αν πράγματι η υπογραφή παράχθηκε από το ιδιωτικό κλειδί.

**Έλεγχος Πρόσβασης:** Οι μηχανισμοί ελέγχου πρόσβασης καθορίζουν και επιβάλλουν τα δικαιώματα πρόσβασης μιας οντότητας , χρησιμοποιώντας την αυθεντικοποιημένη ταυτότητα της οντότητας , πληροφορίες σχετικές με την οντότητα ή τις δυνατότητες της οντότητας. Οι απόπειρες προσπέλασης ενός πόρου χωρίς να υπάρχει ανάλογη εξουσιοδότηση, καθώς και απόπειρες προσπέλασης ενός πόρου με μη εξουσιοδοτημένο τύπο προσπέλασης , απορρίπτονται και το σχετικό γεγονός μπορεί να καταγραφεί στο ίχνος ελέγχου ασφάλειας.

Οι μηχανισμοί αυτοί μπορεί να χρησιμοποιούν βάσεις πληροφοριών ελέγχου πρόσβασης στις οποίες είναι αποθηκευμένα τα δικαιώματα πρόσβασης των οντοτήτων, πληροφορίες αυθεντικοποίησης, δυνατότητες , ετικέτες ασφάλειας , χρόνο απόπειρας πρόσβασης, δρόμο απόπειρας πρόσβασης , διάρκεια πρόσβασης.



Μηχανισμοί ελέγχου πρόσβασης μπορεί να απαιτούνται είτε στο αρχικό σημείο σύνδεσης της οντότητας είτε και σε ενδιάμεσα σημεία του δρόμου επικοινωνίας με το τελικό σύστημα , έτσι ώστε να είναι δυνατός ο καθορισμός του δικαιώματος πρόσβασης στην απαιτούμενη υπηρεσία επικοινωνίας και η παροχή της εξουσιοδότησης για επικοινωνία με το άλλο μέρος.

**Ακεραιότητα δεδομένων:** Οι μηχανισμοί αυτοί χρησιμοποιούνται για την εξασφάλιση της ακεραιότητας μιας και μόνο μονάδας (ή ενός πεδίου) δεδομένων ή ακολουθίας μονάδων (ή πεδίων) δεδομένων.Υπάρχουν δύο διαδικασίες που καθορίζουν την ακεραιότητα μιας μονάδας δεδομένων.Η πρώτη διαδικασία εφαρμόζεται στην πηγή δεδομένων και παράγει μια τιμή που την επισυνάπτει στη μονάδα δεδομένων.Η τιμή αυτή μπορεί να παράγεται από έναν απλό κώδικα ελέγχου δεδομένων ( π.χ. CRC ) ή έναν αλγόριθμο κρυπτογράφησης. Η δεύτερη διαδικασία εφαρμόζεται στο δέκτη των δεδομένων και δημιουργεί την αντίστοιχη τιμή χρησιμοποιώντας την ληφθείσα μονάδα δεδομένων. Συγκρίνοντας τις δύο τιμές μπορούμε να αποφασίσουμε αν υπήρξε τροποποίηση των δεδομένων κατά τη μετάδοση.Η εξασφάλιση της ακεραιότητας μιας ακολουθίας δεδομένων απαιτεί συμπληρωματική προστασία.

**Έλεγχος δρομολόγησης :** Ο μηχανισμός αυτός καλύπτει θέματα δρομολόγησης δεδομένων σε δίκτυα.Δύο τελικά συστήματα είναι δυνατόν να επιθυμούν να συνδεθούν μέσω διαφορετικών δρομολογίων,για να εμποδίσουν εκδήλωση επιθέσεων εναντίον τους.Πολλές φορές είναι επίσης επιθυμητή η απαγόρευση διέλευσης δεδομένων που φέρουν συγκεκριμένες ετικέτες ασφάλειας μέσω συγκεκριμένων υποδικτύων,μεταγωγέων ή ζεύξεων.Τέλος ,μερικές φορές είναι επιθυμητή η χρήση προσυμφωνημένων ,φυσικά ασφαλών, δικτύων για μετάδοση πληροφοριών,αντί δυναμικά καθοριζόμενων δρομολογίων.

**Αρχές Πιστοποίησης:** Ο μηχανισμός αυτό εξασφαλίζει ότι τα δεδομένα που μεταδίδονται μεταξύ δύο ή περισσότερων μερών χαίρουν κάποιων ιδιοτήτων , όπως για παράδειγμα,ακεραιότητα των δεδομένων,αυθεντικότητα προέλευσης και προορισμού ,ορθότητα χρόνου αποστολής.Η εξασφάλιση αυτή παρέχεται από ένα τρίτο συμβαλλόμενο μέρος.

Κάθε επικοινωνιακό στιγμιότυπο μπορεί να προστατεύεται χρησιμοποιώντας τους μηχανισμούς των ψηφιακών υπογραφών ,της κρυπτογράφησης,της ακεραιότητας ή οποιουδήποτε άλλους μηχανισμούς που είναι διαθέσιμοι από τις Αρχές Πιστοποίησης.

### **1.3 Συνεισφορά της εργασίας**

Με γνώμονα τους κινδύνους που εγκυμονεί ένα πληροφοριακό σύστημα , τις απαιτήσεις ασφάλειας και τους μηχανισμούς υλοποίησης των απαιτήσεων αυτών, προχωρήσαμε στην μελέτη και υλοποίηση της διπλωματικής εργασίας. Στόχος της διπλωματικής εργασίας είναι να δούμε την υλοποίηση της ιδιωτικότητας σε ψηφιακά μέσα , γνωστά ως ψηφιακά πιστοποιητικά ,να αναλύσουμε το λεγόμενο «Νέο Σύστημα» ή αλλιώς «Σύστημα Ανώνυμων Πιστοποιητικών» και να δούμε τις ιδιότητες και τα οφέλη που προκύπτουν από τη χρήση του σε σχέση με τα προηγούμενα συστήματα πιστοποιητικού . Επιπλέον , συνεισφορά της διπλωματικής εργασίας αποτελεί η ανάλυση ενός πλαισίου κρυπτογραφικών αρχών ( σχέδια υπογραφών, δεσμεύσεων,κρυπτογράφησης-αποκρυπτογράφησης) πάνω στο οποίο θεμελιώνεται το νέο σύστημα πιστοποιητικού και κατά συνέπεια όλες οι (ηλεκτρονικές ) συναλλαγές , με την αποκάλυψη του ελάχιστου αναγκαίου ποσού πληροφορίας. Ο κάθε συμμετέχων θα καθορίζει πόσα και ποια στοιχεία θα αποκαλύπτει , διαδικασία που την ονομάζουμε «Ελεγχόμενη Δημοσιοποίηση Δεδομένων» . Το κλειδί στην περίπτωση αυτή είναι ότι για τα στοιχεία που αποκαλύπτονται , κάποια οντότητα μπορεί να επαληθεύσει την εγκυρότητα τους.

Σημαντικό κομμάτι της παρούσας διπλωματικής εργασίας αποτελεί και η εκτίμηση της απόδοσης του πρωτοκόλλου **Diffie – Hellman** για διάφορα μήκη κλειδιών (512 ,1024 ψηφία) σε γλώσσα προγραμματισμού Java. Η εκτίμηση της απόδοσης θα γίνει μέσω της εκτίμησης του χρόνου εκτέλεσης του πρωτόκολλου.Επίσης , θα γίνει παρουσίαση των εκτιμώμενων χρόνων σε πίνακα ώστε να μπορεί να γίνει καλύτερη αξιολόγηση του χρόνου και κατά συνέπεια της απόδοσης.

## 1.4 Περιληπτική Σύνοψη

Στο **δεύτερο κεφάλαιο** εισάγουμε την έννοια της κρυπτογραφίας και τη χρησιμότητά της , τις έννοιες κρυπτογράφηση –αποκρυπτογράφηση ,τα είδη κρυπτογραφίας (συμμετρική , ασύμμετρη ) , πλεονεκτήματα αυτών και μια σύντομη σύγκριση των δύο τύπων. Στο **τρίτο κεφάλαιο** παρουσιάζουμε τον ορισμό και τη μορφή ενός ψηφιακού πιστοποιητικού , ορισμένες βασικές ιδιότητες των νέων ψηφιακών πιστοποιητικών έναντι των παραδοσιακών και τέλος τα οφέλη που προκύπτουν από τη χρήση τους.

Στο **τέταρτο κεφάλαιο** , κάνουμε μια ιστορική αναδρομή σε προηγούμενα σχήματα πιστοποιητικών και αναφέρουμε με ιδιαίτερη λεπτομέρεια το σύστημα πιστοποιητικού του Brand πάνω στο οποίο θεμελιώνεται και το νέο σύστημα πιστοποιητικού , που αποτελεί βασικό θέμα της συγκεκριμένης διπλωματικής εργασίας και θα αναλύσουμε στο κεφάλαιο πέντε.

Συνεπώς , **στο κεφάλαιο πέντε** θα αναλύσουμε τις οντότητες που αλληλεπιδρούν στο νέο σύστημα ανώνυμων πιστοποιητικών, τις ιδιότητες του , βασικές συναλλαγές και σχετικά πρωτόκολλα (π.χ. δημιουργίας ψευδωνύμου κ.α.) , την πολύ σημαντική ιδιότητα της μη μεταφερσιμότητας πιστοποιητικών και ψευδωνύμων μεταξύ χρηστών του συστήματος, τα πιστοποιητικά μιας χρήσης -βασικά χαρακτηριστικά και ιδιότητες τους , το ρόλο του διαχειριστή ανάκλησης ανωνυμίας ,τα είδη της και σχετικά πρωτόκολλα και ένα παράδειγμα συστήματος ανώνυμων πιστοποιητικών από τον πραγματικό κόσμο.

Στο **έκτο κεφάλαιο** θα αναλύσουμε βασικά σχέδια κρυπτογράφησης- αποκρυπτογράφησης δεδομένων, σχέδια υπογραφής πιστοποιητικών , πρωτόκολλα παρουσίασης και επαλήθευσης της εγκυρότητας πιστοποιητικών ,πρωτόκολλα που βασίζονται σε αποδείξεις μηδενικής γνώσης , στην έννοια των διγραμμικών γράφων καθώς και πρωτόκολλα δέσμευσης στοιχείων που συνδέονται με κάποιο πιστοποιητικό.

Στο **έβδομο κεφάλαιο** της διπλωματικής εργασίας , θα κάνουμε μια σύντομη περιγραφή δύο εφαρμογών όσων αναλύσαμε στα προηγούμενα κεφάλαια για να δούμε πως αυτά εφαρμόζονται στην πράξη.

Τέλος, ακολουθεί ένα **παράρτημα** με επεξήγηση κάποιων βασικών εννοιών , μαθηματικών συμβόλων που συναντώνται στην παρουσίαση των διαφόρων πρωτοκόλλων , μια απλή υλοποίηση σε Java του πρωτοκόλλου Diffie-Hellman , και αξιολόγηση της απόδοσης του πρωτοκόλλου για μήκος κλειδιού 512 και 1024 αντίστοιχα.

## Κεφάλαιο 2<sup>ο</sup> : Κρυπτογραφία

### 2.1 Η έννοια και η χρησιμότητα της κρυπτογραφίας

Η λέξη κρυπτογραφία προέρχεται από τα συνθετικά "κρυπτός" + "γράφω" και είναι ένας επιστημονικός κλάδος που ασχολείται με τη μελέτη, την ανάπτυξη και τη χρήση τεχνικών κρυπτογράφησης και αποκρυπτογράφησης με σκοπό την απόκρυψη του περιεχομένου των μηνυμάτων. Η κρυπτογραφία ασχολείται με τη μελέτη της ασφαλούς επικοινωνίας. Ο κύριος στόχος της είναι να παρέχει μηχανισμούς για δύο ή περισσότερα μέλη να επικοινωνήσουν χωρίς κάποιος άλλος να είναι ικανός να διαβάσει την πληροφορία εκτός από τα μέλη. Η κρυπτογραφία είναι η επιστήμη που αποσκοπεί, χρησιμοποιώντας μαθηματικές τεχνικές, στο να εγγυηθεί την εμπιστευτικότητα, την ακεραιότητα και την αυθεντικότητα των πληροφοριών και να εξασφαλίσει το απόρρητο των ηλεκτρονικών συναλλαγών, μέσω της εξουσιοδοτημένης πρόσβασης στα ευαίσθητα δεδομένα.

Η κρυπτογραφία παρέχει λοιπόν τέσσερις βασικές λειτουργίες:

- **Εμπιστευτικότητα:** Η πληροφορία προς μετάδοση είναι προσβάσιμη μόνο στα εξουσιοδοτημένα μέλη. Η πληροφορία είναι ακατανόητη σε κάποιον τρίτο.
- **Ακεραιότητα:** Η πληροφορία μπορεί να αλλοιωθεί μόνο από τα εξουσιοδοτημένα μέλη και δεν μπορεί να αλλοιώνεται χωρίς την ανίχνευση της αλλοίωσης.
- **Μη απάρνηση:** Ο αποστολέας ή ο παραλήπτης της πληροφορίας δεν μπορεί να αρνηθεί την αυθεντικότητα της μετάδοσης ή της δημιουργίας της.
- **Πιστοποίηση:** Οι αποστολέας και παραλήπτης μπορούν να εξακριβώνουν τις ταυτότητές τους καθώς και την πηγή και τον προορισμό της πληροφορίας με διαβεβαίωση ότι οι ταυτότητές τους δεν είναι πλαστές.

Η ανάγκη προστασίας του περιεχομένου μηνυμάτων που μεταδίδονται σε ένα τηλεπικοινωνιακό κανάλι οδήγησε στην επινόηση και χρήση κρυπτογραφικών τεχνικών και συστημάτων, τα οποία επιτρέπουν το μετασχηματισμό μηνυμάτων ή δεδομένων κατά τέτοιο τρόπο ώστε να είναι αδύνατη η υποκλοπή του περιεχομένου του κατά τη μετάδοσή ή αποθήκευση του. Η ανάγκη διατήρησης της μυστικότητας μιας πληροφορίας είναι βασική και στις σύγχρονες τηλεπικοινωνίες.

Η κρυπτογραφία δίνει λύση στα εξής προβλήματα :

- Ασφαλή επικοινωνία
- Ταυτοποίηση και πιστοποίηση
- Κοινοποίηση μυστικής πληροφορίας
- Ηλεκτρονικό Εμπόριο
- Ηλεκτρονικά πιστοποιητικά
- Ασφαλή πρόσβαση σε υπολογιστικά συστήματα

### 2.1.1 Η έννοια της κρυπτογράφησης και αποκρυπτογράφησης

Δύο σημαντικές μέθοδοι που εξασφαλίζουν την ασφάλεια των ηλεκτρονικών συναλλαγών αποτελούν η κρυπτογράφηση ενός απλού κειμένου και η αποκρυπτογράφηση για την ανάκτηση του απλού κειμένου που έχει κρυπτογραφηθεί.

Η διαδικασία μετασχηματισμού της πληροφορίας καλείται *κρυπτογράφηση* ενώ η αντίστροφη διαδικασία , δηλαδή η αποκάλυψη του περιεχομένου ενός μηνύματος , *αποκρυπτογράφηση* . Η συνάρτηση ή το σύνολο των κανόνων , στοιχείων και βημάτων που καθορίζουν την κρυπτογράφηση και αποκρυπτογράφηση ονομάζεται *κρυπτογραφικός αλγόριθμος*. Η υλοποίηση του κρυπτογραφικού αλγόριθμου καλείται *κρυπτογραφικό σύστημα* .



**Σχήμα 1. - Σχήμα Κρυπτογράφησης - Αποκρυπτογράφησης ενός μηνύματος**

Κατά τη διαδικασία της κρυπτογράφησης , ένας κρυπτογραφικός αλγόριθμος σε συνδυασμό με ένα μυστικό κλειδί , μετατρέπει το αρχικό κατανοητό κείμενο που περιέχει την μυστική πληροφορία , το λεγόμενο απλό κείμενο , σε κρυπτοκείμενο , το οποίο για τον μη νόμιμο αποδέκτη είναι ακατανόητο. Μόνο ο νόμιμος αποδέκτης του κρυπτογραφημένου μηνύματος μπορεί να μετατρέψει το κρυπτοκείμενο σε απλό κείμενο και έτσι να ανακτήσει τη μυστική πληροφορία , μια διαδικασία που ονομάζεται αποκρυπτογράφηση.

Ο μετασχηματισμός της κρυπτογράφησης παίρνει ως είσοδο εκτός από το απλό κείμενο , και το κρυπτογραφικό κλειδί. Όμοια , για την αποκρυπτογράφηση χρειάζεται το κατάλληλο κλειδί αποκρυπτογράφησης. Τα κλειδιά αυτά είναι ένας αριθμός από τυχαία ψηφία. Στη σύγχρονη κρυπτογραφία , η δυνατότητα να διατηρείται κρυφή η κρυπτογραφημένη πληροφορία δεν βασίζεται στον κρυπτογραφικό αλγόριθμο , ο οποίος είναι ευρέως γνωστός αλλά στο κλειδί που χρησιμοποιείται με τον αλγόριθμο για την κρυπτογράφηση ή αποκρυπτογράφηση. Η αποκρυπτογράφηση με το σωστό κλειδί είναι πολύ απλή . Αλλά χωρίς το σωστό κλειδί είναι πολύ δύσκολη , και στις περισσότερες περιπτώσεις αδύνατη. Για αυτό είναι σημαντικό να διαχειριζόμαστε σωστά τα κλειδιά και να τα κρατάμε μυστικά όταν είναι απαραίτητο.

Το κρυπτογραφικό σύστημα παρέχει διασφάλιση του απορρήτου των πληροφοριών που στέλνονται μεταξύ των συναλλασσομένων οντοτήτων . Έτσι , αν βρεθούν στα «χέρια» τρίτων , θα τους είναι άχρηστες , μιας και δεν θα μπορούν να αντιληφθούν το περιεχόμενό τους , αφού δεν θα γνωρίζουν το κλειδί της αποκρυπτογράφησης.

## 2.2 Είδη Κρυπτογραφίας

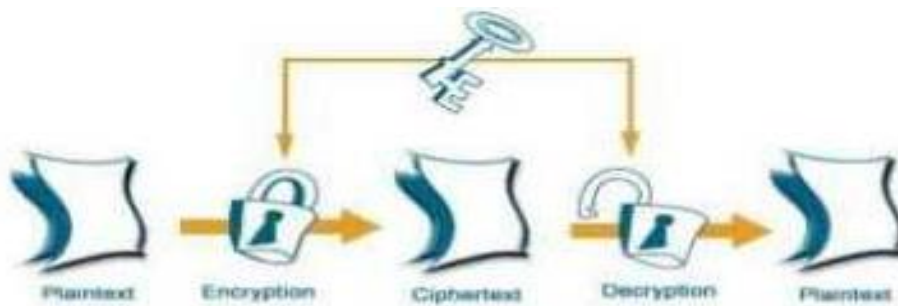
Οι δύο πιο διαδεδομένοι τρόποι κρυπτογραφίας , που χρησιμοποιούνται στις μέρες μας, είναι η συμμετρική ή μυστικού κλειδιού και η ασύμμετρη ή δημόσιου κλειδιού κρυπτογραφία.



Σχήμα 2.- Κρυπτογραφία Κλειδιού

### 2.2.1 Συμμετρική Κρυπτογραφία

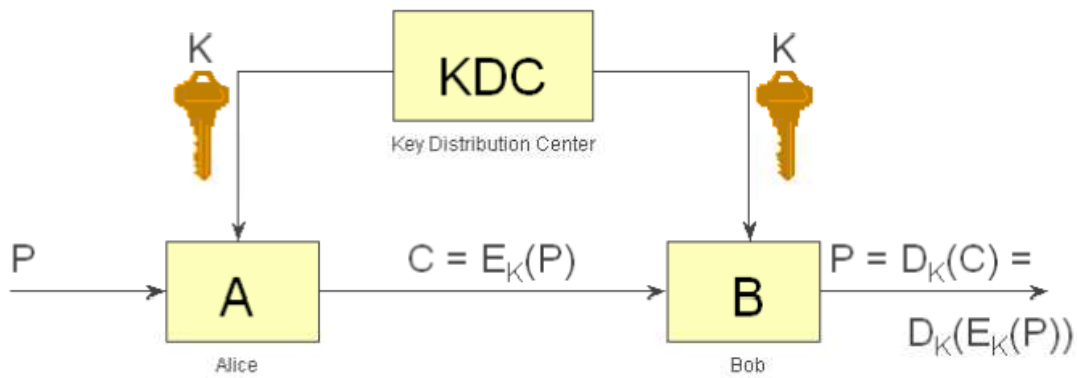
Η συμμετρική κρυπτογραφία βασίζεται στην ιδέα ότι για την ανταλλαγή κρυπτογραφημένων μηνυμάτων, ο αποστολέας και ο παραλήπτης είναι οι μοναδικές οντότητες που γνωρίζουν μια συγκεκριμένη μυστική πληροφορία. Η μυστική αυτή πληροφορία αποτελεί το συμμετρικό κλειδί του συμμετρικού κρυπτογραφημένου αλγόριθμου και χρησιμοποιείται για την κρυπτογράφηση και την αποκρυπτογράφηση του μηνύματος. Οι αλγόριθμοι σε αυτή την περίπτωση λέγονται συμμετρικοί, ακριβώς επειδή χρησιμοποιούμε το ίδιο κλειδί για την κρυπτογράφηση και αποκρυπτογράφηση. Τα συναλλασσόμενα μέρη πρέπει να συμφωνήσουν εκ των προτέρων για το κλειδί που θα χρησιμοποιηθεί και η προστασία του κλειδιού αποτελεί κρίσιμο πρόβλημα.



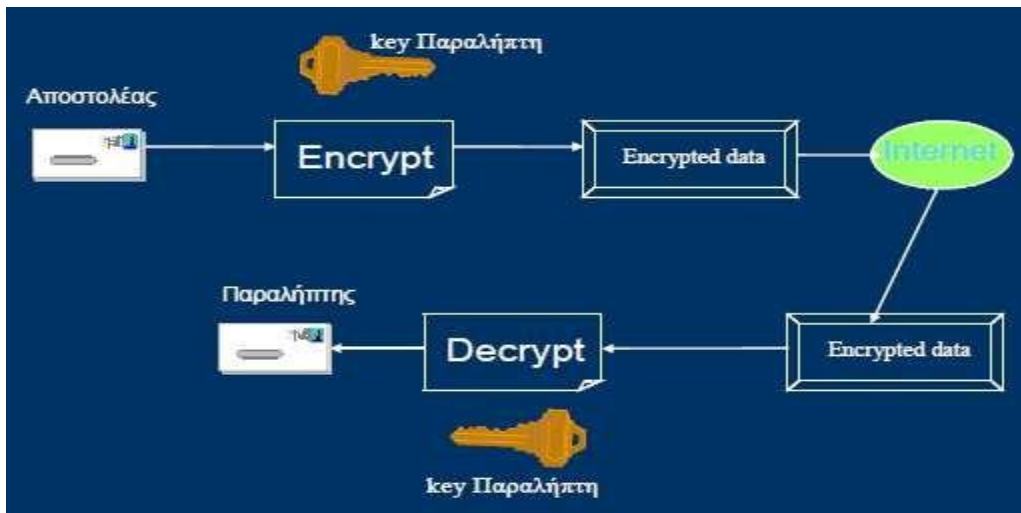
**Σχήμα 3. Συμμετρικό κρυπτογραφικό σύστημα (Γενικό)**

Δύο ζητήματα τα οποία προκύπτουν όσον αφορά την συμμετρική κρυπτογραφία αφορούν, πρώτον, το πώς θα γίνει η ανταλλαγή του μυστικού κλειδιού μεταξύ των συναλλασσομένων προκειμένου να επιτευχθεί η κρυπτογράφηση και η αποκρυπτογράφηση ενός μηνύματος και δεύτερον, πώς μπορεί να γίνει πιστοποίηση της αυθεντικότητας μεταξύ αποστολέα και παραλήπτη. Με βάση το σχήμα 4 υπάρχει ένα κέντρο διανομής κλειδιών μεταξύ των συναλλασσομένων.





Σχήμα 4. Συμμετρική Κρυπτογράφηση



Σχήμα 5. Παράδειγμα συμμετρικής κρυπτογράφησης για ανταλλαγή μηνυμάτων μέσω του διαδικτύου

### 2.2.2 Ασύμμετρη Κρυπτογραφία

Στα μέσα της δεκαετίας του 1970 οι Whitfield Diffie και Martin Hellman πρότειναν μια νέα τεχνική γνωστή ως ασύμμετρη κρυπτογραφία ή κρυπτογραφία δημόσιου κλειδιού. Η τεχνική αυτή βασίζεται στην ύπαρξη ενός ζεύγους κλειδιών, το οποίο αποτελούν το δημόσιο κλειδί και το ιδιωτικό κλειδί. Τα δύο κλειδιά, αν και είναι διαφορετικά, συσχετίζονται μαθηματικά με μονόδρομες συναρτήσεις έτσι η γνώση του ενός δεν επιτρέπει τον υπολογισμό ή την παραγωγή του άλλου.

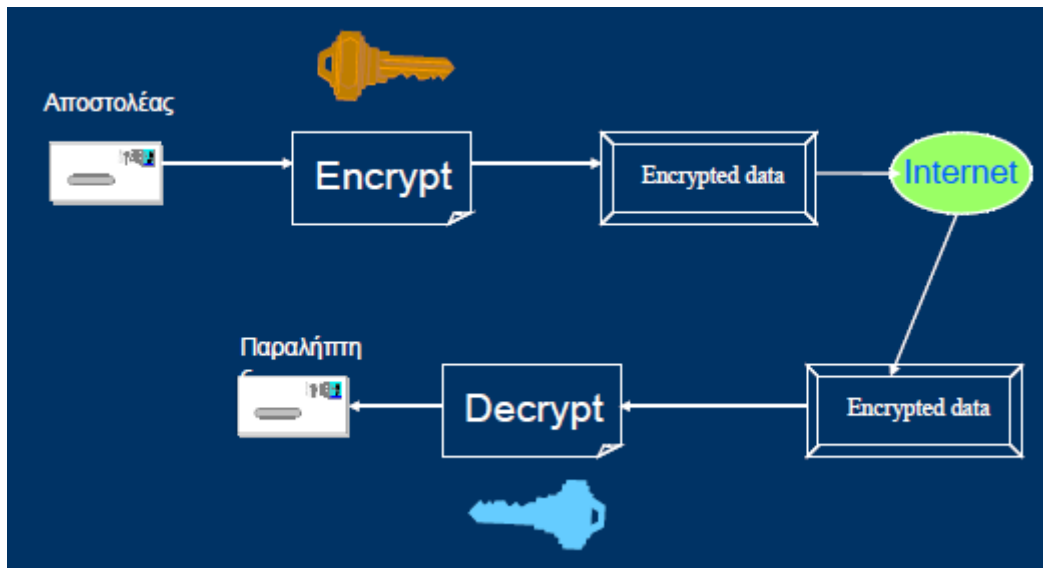
Επίσης, το ζεύγος κλειδιών έχει την ιδιότητα ότι μπορεί να αποκρυπτογραφήσει ότι κρυπτογράφησε το άλλο κλειδί. Δηλαδή, αν η κρυπτογράφηση γίνεται με το δημόσιο κλειδί η αποκρυπτογράφηση γίνεται με το ιδιωτικό κλειδί και αντίστροφα. Ο κάτοχος του ζεύγους κλειδιών διανέμει το δημόσιο κλειδί ελεύθερα χωρίς να υπονομεύει την ασφάλεια του συστήματος, ενώ είναι υποχρεωμένος να προστατεύει με αυστηρότητα το ιδιωτικό κλειδί, καθώς διαρροή του ιδιωτικού κλειδιού συνεπάγεται κατάρρευση των μηχανισμών ασφαλείας του ζεύγους κλειδιών. Γνωστοί αλγόριθμοι δημόσιου κλειδιού είναι οι Diffie-Hellman ανταλλαγή κλειδιού, ElGamal, Digital Signature Standard (DSS). Ο κυριότερος αλγόριθμος δημόσιου κλειδιού είναι ο RSA (Rivest, Shamir, Adleman 1977).



Σχήμα 6. Σχήμα Ασύμμετρης Κρυπτογραφίας

### **2.2.2.1 Πλεονεκτήματα της Ασύμμετρης Κρυπτογραφίας ή Κρυπτογραφίας Δημόσιου Κλειδιού**

- Τα δημόσια κλειδιά δεν χρήζουν προστασίας
- Τα ιδιωτικά κλειδιά δεν κοινοποιούνται και δεν διανέμονται σε τρίτους σε καμία περίπτωση. Για να σταλεί ένα εμπιστευτικό μήνυμα, χρησιμοποιείται το δημόσιο κλειδί του παραλήπτη. Από την άλλη , μόνο το ιδιωτικό κλειδί που κατέχει ο παραλήπτης μπορεί να το αποκρυπτογραφήσει.
- Είναι υπολογιστικά αδύνατο να υπολογιστεί το κλειδί της αποκρυπτογράφησης από τη γνώση του κλειδιού κρυπτογράφησης και του αλγορίθμου που χρησιμοποιήθηκε
- Για να υπογραφεί ένα μήνυμα χρησιμοποιείται το ιδιωτικό κλειδί του αποστολέα. Οποιοσδήποτε τρίτος μπορεί να επαληθεύσει την υπογραφή με το δημόσιο κλειδί του αποστολέα.
- Ελαχιστοποίηση της διαχείρισης κλειδιών – Δεν χρειάζεται κέντρο διανομής κλειδιών όπως στην συμμετρική κρυπτογραφία
- Μεγάλος κύκλος ζωής των κλειδιών
- Δίνουν τη δυνατότητα επαλήθευσης της ακεραιότητας δεδομένων
- Το δημόσιο κλειδί διανέμεται ελεύθερα με αποτέλεσμα την εύκολη σύσταση ασφαλών καναλιών επικοινωνίας μεταξύ δυο απομακρυσμένων χρηστών.



**Σχήμα 7. Παράδειγμα ασύμμετρης κρυπτογραφίας για ανταλλαγή μηνυμάτων μέσω του διαδικτύου**

#### **2.2.2.2 Προβλήματα της Ασύμμετρης Κρυπτογραφίας**

- ❖ Πώς επαληθεύεται η ταυτότητα του κατόχου ενός ζεύγους κλειδιών;
- ❖ Πώς διασφαλίζεται η ιδιωτικότητα και η ακεραιότητα των κλειδιών κατά τη δημιουργία και τη χρήση τους;
- ❖ Πώς διανέμονται στο κοινό τα δημόσια κλειδιά έτσι ώστε να διασφαλίζεται η σύνδεση τους με μία φυσική οντότητα;
- ❖ Πώς τελειώνει ο κύκλος ζωής τους όταν αυτό κριθεί αναγκαίο;
- ❖ Διαφαίνεται η ανάγκη ύπαρξης μίας «Εμπιστης Τρίτης Οντότητας» που

διαχειρίζεται «Ψηφιακά Πιστοποιητικά».

### 2.2.3 Σύγκριση των δύο τύπων κρυπτογραφίας

- Η ασύμμετρη κρυπτογραφία είναι μη αποτελεσματική για την κρυπτογράφηση μεγάλου όγκου δεδομένων, αντίθετα από τη συμμετρική.
- Συνηθισμένη χρήση της ασύμμετρης κρυπτογραφίας είναι η αποστολή ενός συμμετρικού κρυπτογραφικού κλειδιού μέσω ενός ανασφαλούς καναλιού.
- Ένα «Κέντρο Διανομής Κλειδιών» διανέμει με ασφάλεια στα συναλλασσόμενα μέρη ένα συμμετρικό κλειδί, κρυπτογραφημένο με τα δημόσια κλειδιά των εμπλεκομένων.
- Οι συναλλασσόμενοι αποκρυπτογραφούν το κλειδί και ξεκινούν εμπιστευτικές συνόδους μεταξύ τους χρησιμοποιώντας συμμετρικούς αλγόριθμους

## Κεφάλαιο 3: Το Ψηφιακό Πιστοποιητικό

### 3.1 Ο ορισμός και τα χαρακτηριστικά ενός ψηφιακού πιστοποιητικού

Το ψηφιακό πιστοποιητικό (Σχήμα 8-Σχήμα 9-Σχήμα 10) είναι κάτι αντίστοιχο με το διαβατήριό και το δίπλωμα οδήγησης, με τη διαφορά ότι ο χρήστης επιβεβαιώνει την ταυτότητά του σε τρίτους με ηλεκτρονικό τρόπο και παρέχει τα μέσα σε αυτούς να επιβεβαιώσουν αυτή την ταυτότητα. Είναι ψηφιακά έγγραφα με συγκεκριμένη μορφή και τα περισσότερα ακολουθούν τη δομή X.509 v3 που είναι η πιο πρόσφατη έκδοση του πρότυπου X.509.

Ένα ψηφιακό πιστοποιητικό περιλαμβάνει στοιχεία όπως:

- Το όνομα του κατόχου
- Ηλικία & Ημερομηνία Γέννησης κατόχου
- Επάγγελμα, Τόπο κατοικίας
- Ένα σειριακό αριθμό
- Το δημόσιο κλειδί του κατόχου
- Τον τύπο του πιστοποιητικού
- Το όνομα της Αρχής Πιστοποίησης
- Την ημερομηνία λήξης της ισχύος του πιστοποιητικού
- Την ψηφιακή υπογραφή της Αρχής Πιστοποίησης

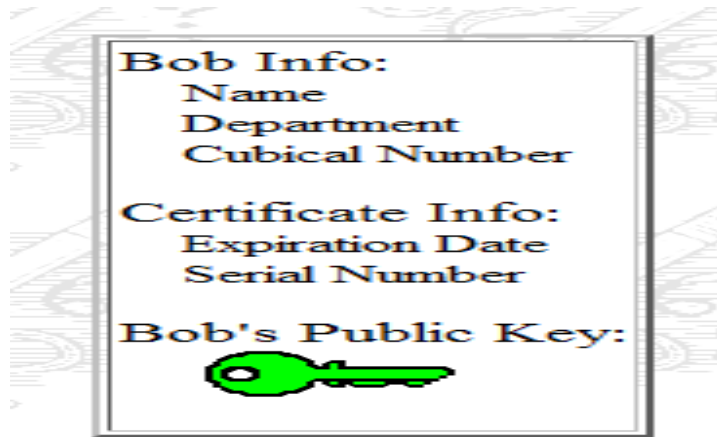
Το *Ψηφιακό Πιστοποιητικό* είναι μία ψηφιακά υπογεγραμμένη δομή δεδομένων, η οποία αντιστοιχίζει μία ή περισσότερες ιδιότητες μιας φυσικής οντότητας στο δημόσιο κλειδί που της ανήκει. Το πιστοποιητικό είναι υπογεγραμμένο από μία Τρίτη Οντότητα, η οποία είναι έμπιστη και καλείται *Αρχή Πιστοποίησης*. Η οντότητα αυτή διασφαλίζει με τεχνικά αλλά και νομικά μέσα ότι ένα δημόσιο κλειδί ανήκει σε μία και μόνο μία, συγκεκριμένη οντότητα και συνεπώς ότι η οντότητα αυτή είναι ο νόμιμος κάτοχος του αντίστοιχου ιδιωτικού κλειδιού.

Η υπογραφή της στα στοιχεία του πιστοποιητικού του χρήστη πιστοποιεί ότι έχει ελέγξει την εγκυρότητα των στοιχείων (όλων ή μερικών) που κωδικοποιεί στο πιστοποιητικό και την εξουσιοδότηση του χρήστη να εκτελέσει κάποια δεδομένη εργασία με το συγκεκριμένο πιστοποιητικό.

Όταν ο χρήστης θα παρουσιάσει το πιστοποιητικό σε κάποιον επαληθευτή, αυτός θα ελέγξει την εγκυρότητα του πιστοποιητικού επαληθεύοντας της ορθότητα της υπογραφής του εκδότη. Η Αρχή Πιστοποίησης είναι αρμόδια για την έκδοση πιστοποιητικών ταυτότητας. Κατέχει ένα ζεύγος κλειδιών (*SK*, *PK*) , όπου *PK* το δημόσιο κλειδί της και *SK* το μυστικό κλειδί της μέσω του οποίου υπογράφει ψηφιακά τα πιστοποιητικά ταυτότητας τα οποία εκδίδει. Παράλληλα , είναι υπεύθυνη για την επικύρωση της ταυτότητας ηλεκτρονικών καταστημάτων και άλλων χρηστών του διαδικτύου.



Σχήμα 8 . Αποψη Ψηφιακού Πιστοποιητικού



Σχήμα 9-Άποψη Ψηφιακού Πιστοποιητικού



Σχήμα 10-Άποψη Ψηφιακού Πιστοποιητικού

### 3.2 Πλεονεκτήματα της χρήσης ψηφιακών πιστοποιητικών

- Δημιουργούν σχέσεις εμπιστοσύνης μεταξύ οντοτήτων που δεν γνωρίζονται, μέσω της Έμπιστης Τρίτης Οντότητας (Αρχή Πιστοποίησης )
- Μπορούν να χρησιμοποιούνται off-line
- Μπορούν να περιέχουν επιπλέον στοιχεία που επιβεβαιώνει ένας τρίτος εγγυητής, για χρήση σε διάφορες εφαρμογές
- Βεβαιώνουν την ακεραιότητα του δημόσιου κλειδιού.
- Βεβαιώνουν τη σύνδεση ενός δημόσιου κλειδιού με ένα άτομο ή οργανισμό μέσω της Έμπιστης Τρίτης Οντότητας .



### **3.3 Επιθυμητές ιδιότητες των νέων , μη παραδοσιακών πιστοποιητικών**

Στην ενότητα αυτή θα αναλύσω τις ιδιότητες των μη παραδοσιακών πιστοποιητικών τα οποία επιτρέπουν σε ένα χρήστη να ελέγχει τα στοιχεία που αυτός αποκαλύπτει είτε στον εκδότη του πιστοποιητικού είτε στον επαληθευτή. Συγκεκριμένα , θα περιγράψω τις ιδιότητες που σχετίζονται με την παρουσίαση ενός πιστοποιητικού<sup>1</sup>. Οι ιδιότητες είναι ακόλουθες.

#### **3.3.1 Μη συνδεσιμότητα πολλαπλών παρουσιάσεων**

Γενικά , η συνδεσιμότητα είναι μια έμφυτη ιδιότητα των παραδοσιακών πιστοποιητικών ανεξάρτητη από τα στοιχεία του πιστοποιητικού και αποτελεί μια σοβαρή απειλή στη μυστικότητα των ατόμων.

Τα συμβατικά , δημόσιου κλειδιού πιστοποιητικά κωδικοποιούνται από μοναδικά αλφαριθμητικά. Για αυτό αν ένας χρήστης έστειλε στον επαληθευτή το πραγματικό πιστοποιητικό που απέκτησε από τον εκδότη , ο εκδότης με τον επαληθευτή θα μπορούσαν να συνδέσουν τις διαφορετικές συναλλαγές του ίδιου χρήστη. Επιπλέον , πολλαπλές παρουσιάσεις του ίδιου πιστοποιητικού στον ίδιο ή σε διαφορετικούς επαληθευτές θα ήταν συνδέσιμες . Απαιτούμε λοιπόν ότι η παρουσίαση ενός πιστοποιητικού δεν μπορεί να συνδεθεί με την έκδοση του πιστοποιητικού καθώς επίσης και με άλλες παρουσιάσεις του ίδιου πιστοποιητικού ακόμα και αν τα στοιχεία που αποκαλύπτονται απαιτούν κάτι τέτοιο. Έτσι λοιπόν διατηρείται και διασφαλίζεται η ανωνυμία των χρηστών στο σύστημα.

#### **3.3.2 Επιλεκτική παρουσίαση των στοιχείων ενός ψηφιακού πιστοποιητικού**

Ο χρήστης σε κάθε παρουσίαση πιστοποιητικού επιλέγει ποια στοιχεία θέλει να αποκαλύψει στον επαληθευτή. Για αριθμητικά στοιχεία , είναι δυνατό να δείξει ότι ένα στοιχείο λαμβάνει τιμές μέσα σε κάποιο διάστημα χωρίς να αποκαλύψει την ακριβή τιμή του στοιχείου .Ας θεωρήσουμε το πιστοποιητικό άδειας οδήγησης ενός οδηγού .

---

<sup>1</sup> Όταν ένας χρήστης παρουσιάζει ένα πιστοποιητικό προσπαθεί να πείσει τον επαληθευτή για την εγκυρότητα του περιεχομένου του πιστοποιητικού και δεν αποστέλλει απαραίτητα το πραγματικό πιστοποιητικό.

Ο οδηγός μπορεί να το παρουσιάσει όταν τον σταματούν στο δρόμο σε ένα σημείο ελέγχου αστυνομίας χωρίς αποκάλυψη των στοιχείων του , αλλά και σε μια υπεραγορά όταν αγοράζει αλκοόλ ώστε να αποκαλύψει μόνο ότι δεν είναι ανήλικος.

### **3.3.3 Υπό όρους παρουσίαση των στοιχείων ενός ψηφιακού πιστοποιητικού**

Ένας χρήστης μπορεί να αποκαλύπτει τα στοιχεία ενός πιστοποιητικού του παρά μόνο αν πληρούνται συγκεκριμένοι όροι. Σε αυτή τη διαδικασία εμπλέκεται και μια τρίτη οντότητα και προτεραιότητα στην παρουσίαση ενός πιστοποιητικού είναι ο χρήστης-κάτοχος του πιστοποιητικού να επιλέξει τα στοιχεία που επιθυμεί να παρουσιάσει υπό όρους στον εκδότη του πιστοποιητικού .

Επίσης ,ο χρήστης με τον επαληθευτή συμφωνούν για τους όρους κάτω από τους οποίους ο επαληθευτής μπορεί να μάθει για τα συγκεκριμένα επιλεγμένα στοιχεία.

Σε μια υπό όρους παρουσίαση , ο χρήστης αποκαλύπτει πληροφορίες στον επαληθευτή τέτοιες που δεν μπορεί να ανακτήσει τα υπό όρους παρουσιασμένα στοιχεία από τις πληροφορίες αυτές. Ακόμα, ο επαληθευτής μπορεί να βεβαιωθεί ότι η τρίτη οντότητα μπορεί να ανακτήσει τα στοιχεία αυτά. Έτσι λοιπόν, αν η τρίτη οντότητα ανακτήσει τα στοιχεία , εφόσον ο συμφωνηθείς όρος ικανοποιείται , τότε λέμε ότι υλοποιείται *ο μηχανισμός παρουσίασης πιστοποιημένων στοιχείων υπό τον συμφωνηθέντα όρο.*

Ας υποθέσουμε ότι ένας χρήστης έχει πρόσβαση στο αναγνωστήριο της πανεπιστημιακής βιβλιοθήκης και ότι η τρίτη οντότητα είναι η πανεπιστημιακή διοίκηση. Το ρόλο του επαληθευτή παίζει ο βιβλιοθηκάριος. Η ταυτότητα του χρήστη που περιέχεται στην φοιτητική ταυτότητα , θα αποκαλυφθεί στον βιβλιοθηκάριο εφόσον ο χρήστης κλέψει κάποιο βιβλίο από τη βιβλιοθήκη . Για να ανακαλύψει την ταυτότητα ο βιβλιοθηκάριος θα πρέπει να εμπλακεί με την πανεπιστημιακή διοίκηση.

### 3.3.4 Απόδειξη σχέσεων μεταξύ των στοιχείων ενός πιστοποιητικού

Κατά την παρουσίαση πολλαπλών πιστοποιητικών από διαφορετικούς εκδότες, ο χρήστης πρέπει να είναι σε θέση να καταδείξει ότι τα στοιχεία, στα πιστοποιητικά που παρουσιάζει, συσχετίζονται χωρίς αποκάλυψη των στοιχείων που καταγράφονται σε καθένα από αυτά.

Για παράδειγμα, όταν παρουσιάζει το πιστοποιητικό οδήγησης του και το πιστοποιητικό πιστωτικών καρτών του σε μια επιχείρηση ενοικίασης αυτοκινήτων, ο χρήστης δεν πρέπει να αποκαλύψει το όνομά του που περιλαμβάνεται στα πιστοποιητικά, αλλά μόνο να καταδείξει ότι και τα δύο πιστοποιητικά εκδίδονται στο ίδιο όνομα.

### 3.3.5 Τυφλή πιστοποίηση ενός ψηφιακού πιστοποιητικού

Η τυφλή πιστοποίηση αποτελεί μια ιδιότητα που σχετίζεται με την απόκτηση πιστοποιητικού από κάποιον εκδότη πιστοποιητικών, σύμφωνα με την οποία ο εκδότης του πιστοποιητικού δεν λαμβάνει καμία απολύτως πληροφορία για τα στοιχεία (όλα ή μερικά) τα οποία υπογραφεί ψηφιακά με το δημόσιο κλειδί του.

Με μαθητικούς όρους μπορεί να περιγραφεί ως εξής. Έστω  $\{N_1, \dots, N_S\}$  ένα σύνολο μηνυμάτων και  $H$  ένα υποσύνολο αυτών. Είναι δυνατό για το χρήστη να λάβει πιστοποιητικό πάνω στα  $\{N_1, \dots, N_S\}$  έτσι ώστε ο εκδότης να μην μάθει καμία πληροφορία για τα στοιχεία  $H$ , ενώ μαθαίνει για τα υπόλοιπα<sup>2</sup>. Για τα στοιχεία που παραμένουν κρυφά στον εκδότη, ο χρήστης πρέπει να είναι σε θέση να βεβαιώσει ότι κάποια απ' αυτά πιστοποιήθηκαν προηγουμένως από έναν άλλο εκδότη.

---

<sup>2</sup> Προφανώς, τα στοιχεία στο  $H$  επιλέγονται από το χρήστη, εντούτοις τα υπόλοιπα θα μπορούσαν να επιλεγούν από τον εκδότη ή και από τον χρήστη.

## **Κεφάλαιο 4: Προηγούμενες εργασίες**

### **4.1 Εισαγωγή**

Πριν προχωρήσω στην ανάλυση του νέου συστήματος πιστοποιητικού είναι απαραίτητο να παρουσιάσω εν συντομία κάποια προηγούμενα σχήματα. Τα σχήματα αυτά θα βοηθήσουν να κατανοήσει κάποιος τους λόγους για τους οποίους μεταβήκαμε στο λεγόμενο « νέο σύστημα» πιστοποιητικού. Καθένα από τα παρακάτω σχήματα χρησιμοποιεί διάφορα εργαλεία της κρυπτογραφίας τα οποία σχετίζονται με την ανωνυμία και την ιδιωτικότητα, τις τυφλές υπογραφές και τους δυναμικούς συσσωρευτές.

### **4.2 Περιγραφή προηγούμενων εργασιών**

#### **4.2.1 Οι τυφλές υπογραφές των David & Chaum**

Το πρώτο σχήμα πιστοποιητικού είναι το σχήμα των τυφλών υπογραφών το οποίο εισήχθει από τους David & Chaum. Η τυφλή υπογραφή δεν είναι παρά μια μέθοδος που επιτρέπει σε έναν υπογράφο να ταυτοποιήσει την εγγυρότητα ενός εγγράφου χωρίς να έχει κάποια πληροφορία για αυτό. Οι δύο βασικοί στόχοι μιας τυφλής υπογραφής είναι η μη πλαστογράφιση και η τυφλότητα, όπου η τυφλότητα αναφέρεται στην αδυναμία του υπογράφοντα να αντλήσει κάποια πληροφορία από το έγγραφο που υπογράφει.

Οι τυφλές υπογραφές παίζουν το ρόλο των ψευδωνύμων και επιτρέπουν στους χρήστες να επικυρώνονται μη συνδέσιμα. Εντούτοις, χρησιμοποιώντας τις τυφλές υπογραφές ως ψευδώνυμα, είναι αδύνατο να ανακληθούν τα ψευδώνυμα ενός ψευδούς χρήστη, είτε βάσει της ταυτότητας που έχει εγκαταστήσει ο χρήστης με τον εκδότη του πιστοποιητικού είτε βάσει της κακής χρήσης οποιασδήποτε υπηρεσίας από την πλευρά του χρήστη. Κατά συνέπεια, οι τυφλές υπογραφές παρέχουν μυστικότητα για τους χρήστες αλλά όχι ασφάλεια για τους παροχείς υπηρεσιών.

Διάφορες αλλαγές στο σχέδιο των τυφλών υπογραφών έχουν προταθεί για να επιτρέψουν τη σφαιρική ανάκληση στα πλαίσια των συστημάτων ηλεκτρονικών πληρωμών και να εξασφαλίσουν είτε ότι ένα συμβαλλόμενο μέρος μπορεί να προσδιορίσει όλες τις πληρωμές ηλεκτρονικών νομισμάτων ενός συγκεκριμένου κατόχου λογαριασμού είτε ότι όλες οι πληρωμές ενός χρήστη μπορούν να προσδιοριστούν εάν αυτός συμμετέχει σε μια ψευδή συναλλαγή πληρωμής. Στα πλαίσια των συστημάτων *SSO (Single-Sign-On)*<sup>3</sup>, αυτά τα δύο χαρακτηριστικά γνωρίσματα αντιστοιχούν στη δυνατότητα να ανακληθούν όλα τα ψευδώνυμα ενός χρήστη για έναν γνωστό χρήστη βάσει της ταυτότητας του χρήστη με τον εκδότη του πιστοποιητικού και ενός άγνωστου χρήστη, αντίστοιχα.

#### **4.2.1 Το σχήμα των Camenisch & Nguyen που βασίζεται στους δυναμικούς συσσωρευτές**

Οι *Camenisch* και *Nguyen* πρότειναν μηχανισμούς ανάκλησης πιστοποιητικού βασισμένους στους δυναμικούς συσσωρευτές. Οι δυναμικοί συσσωρευτές επιτρέπουν σε κάποιον να αποδείξει την ιδιότητα μέλους λίστας σε σταθερό χρόνο ως προς το μέγεθος των καταλόγων. Η ασφάλεια των συσσωρευτών στηρίζεται στο ισχυρό πρωτόκολλο *RSA* και στην υπόθεση *Diffie Hellman*.

Επιπλέον, επιτρέπει την ανάκληση όλων των πιστοποιητικών ενός χρήστη βάσει της ταυτότητας που αυτός έχει ανακτήσει με τον εκδότη του πιστοποιητικού. Δεν είναι δυνατό να ανακληθούν όλα τα ψευδώνυμα ενός άγνωστου χρήστη. Τέλος, οι αποδείξεις γνώσης είναι στατιστικά μηδενικής γνώσης μόνο, και το σύνολο των συσσωρευμένων τιμών περιορίζεται σε πρώτους αριθμούς σε ένα προκαθορισμένο διάστημα.

Μια απόδειξη ιδιότητας μέλους, βασισμένη στους συσσωρευτές αποτελείται από δύο βήματα: 1) ο υπολογισμός του τρέχοντος «μάρτυρα» του χρήστη (που είναι μια μυστική τιμή σχετική με τη συσσωρευμένη τιμή του χρήστη) και 2) η εκτέλεση μιας απόδειξης μηδενικής γνώσης.

---

<sup>3</sup> SSO: συστήματα όπου ο χρήστης μπορεί να έχει πρόσβαση σε πολλαπλές υπηρεσίες εισάγοντας μια φορά τα διαπιστευτήρια

Αν και τα τελευταία μπορούν να εκτελεσθούν σε σταθερό χρόνο, το πρώτο απαιτεί μια χρονική πολυπλοκότητα που είναι τουλάχιστον γραμμική ως προς τον αριθμό των στοιχείων που διαγράφονται από το συσσωρευτή.

Θεωρούμε, παραδείγματος χάριν, έναν συσσωρευτή στον οποίο κανένα στοιχείο δεν προστίθεται και του οποίου τα  $n$  στοιχεία αφαιρούνται, και υποθέστε ότι μια μικρή εκθετικοποίηση έχει μέγεθος εκθέτη ίσο με το μέγιστο μέγεθος της συσσωρευμένης τιμής.

Σε αυτήν την ρύθμιση, ο επανυπολογισμός ενός μάρτυρα μπορεί να απαιτήσει  $n$  μικρές εκθετικοποιήσεις. Επιπλέον, ο τελικός μάρτυρας μπορεί μόνο να υπολογιστεί όταν η τελική μαύρη λίστα είναι γνωστή. Ως εκ τούτου, δεν μπορούν να είναι προϋπολογιστούν όλες οι εκθετικοποιήσεις ενός χρήστη.

### 4.2.3 Το σχέδιο του Brickell

Ο Brickell προτείνει μια τεχνική άμεσης, ανώνυμης επιβεβαίωσης στην οποία ένας χρήστης παρέχει στο παροχέα υπηρεσιών ένα ψευδώνυμο  $N_v = \zeta^f$  όπου  $f$  μια μυστική τιμή (κάτι ανάλογο με το μυστικό κλειδί στο νέο σύστημα) γνωστή μονάχα στον χρήστη και  $\zeta$  ένας τυχαίος γεννήτορας μιας ομάδας. Ο σκοπός του ψευδωνύμου  $N_v$  είναι, να παρέχει στον παροχέα υπηρεσιών ένα ψευδώνυμο και να επιτρέπει την ανάκληση της ανωνυμίας του χρήστη είτε βάσει της γνώσης του  $f$  είτε βάσει μιας λίστας άλλων ψευδωνύμων  $\{N_{v^f} = (\zeta^v)^{f^f}, \dots\}$ . Το τελευταίο μπορεί να επιτευχθεί αποδεικνύοντας με μηδενική γνώση τη σχέση  $\log_{\zeta^f}(N_{v^f}) \neq \log_{\zeta}(N_v)$  για όλα τα ψευδώνυμα  $N_v$  της λίστας.

Έτσι αποδεικνύει ότι το συγκεκριμένο ψευδώνυμο δεν ταυτίζεται με κανένα από τα ψευδώνυμα της λίστας. Αυτή η λύση έχει δύο σημαντικά μειονεκτήματα. Πρώτον, η μη συνδεσιμότητα του χρήστη είναι μόνο υπολογιστική. Δεύτερον, η απόδειξη ότι ένα ψευδώνυμο δεν ανακαλείται βάσει ενός καταλόγου ψευδωνύμων απαιτεί έναν αριθμό εκθετικοποιήσεων που είναι γραμμικός ως προς το μήκος της μαύρης λίστας. Συνεπώς δεν είναι πρακτικό το σχέδιο του Brickell για μεγάλες μαύρες λίστες.

#### **4.2.4 Το σχέδιο του Damgard**

Το επόμενο σχέδιο προτάθηκε από τον Damgard . Το σχέδιο αυτό απασχολεί θεωρητικά πολύπλοκες αρχές όπως είναι οι αποδείξεις μηδενικής γνώσης και μονόδρομες συναρτήσεις και για αυτό δεν είναι πρακτικά εφαρμόσιμο . Επιπλέον , οι οργανισμοί δεν προστατεύονται από χρήστες που μπορεί να «συνωμοτήσουν» με σκοπό να εξαπατήσουν προς δικό τους όφελος.

#### **4.2.5 Το σχέδιο των τυφλών υπογραφών του Chen**

Ακολουθώντας , το σχέδιο που πρότεινε ο Chen βασίζεται στο σχέδιο των τυφλών υπογραφών το οποίο θεμελιώνεται στην έννοια του διακριτού λογάριθμου. Όταν λέμε τυφλές υπογραφές εννοούμε ότι ο εκδότης υπογράφει το πιστοποιητικό που εκδίδει χωρίς να γνωρίζει την ταυτότητα του χρήστη .

Είναι αποδοτικό , αλλά μειονεκτεί και αυτό στην περίπτωση χρηστών που συνωμοτούν με άλλους χρήστες και διενεργούν παράνομες συναλλαγές. Επίσης , ένα ακόμα μειονέκτημα του σχεδίου αυτού σε σχέση με τα προηγούμενα, είναι ότι κάποιος χρήστης δεν μπορεί να χρησιμοποιήσει παραπάνω από μια φορά το ίδιο πιστοποιητικό και κάθε φορά ο συγκεκριμένος οργανισμός πρέπει να επανεκδίδει και συνεπώς να υπογράφει τυφλά το ίδιο πιστοποιητικό.

#### **4.2.6 Το σχέδιο των Lysyanskaya, Rivest, Sahai & Wolf**

Οι Lysyanskaya , Rivest , Sahai και Wolf πρότειναν ένα πιο γενικό σύστημα πιστοποιητικού. Παρόλο που το σχέδιο που προτείνουν ικανοποιεί πολλές από τις επιθυμητές ιδιότητες δεν είναι εφαρμόσιμο στην πράξη διότι οι δομές του βασίζονται στις μονόδρομες συναρτήσεις και σε γενικές αποδείξεις μηδενικής γνώσης. Η δομή τους βασίζεται σε μια μη πρότυπη διακριτού λογάριθμου υπόθεση και εμφανίζει το ίδιο πρόβλημα με τον Chen. Δηλαδή , ο εκδίδων ο οργανισμός ενός συγκεκριμένου πιστοποιητικού πρέπει να επανεκδίδει το ίδιο πιστοποιητικό ώστε ο χρήστης να μπορεί μη συνδέσιμα να το χρησιμοποιήσει αρκετές φορές.

#### 4.2.7 Το σύστημα πιστοποιητικού του Brand

Ο Brand πρότεινε ένα πρακτικό μηχανισμό ψηφιακού πιστοποιητικού στον οποίο εμπλέκονται χρήστες , οργανισμοί έκδοσης πιστοποιητικών , παροχείς υπηρεσιών και επαληθευτές πιστοποιητικών.

Ένας εκδότης πιστοποιητικού μπορεί να κωδικοποιήσει «αόρατα» - χωρίς να γνωρίζει , έναν μοναδικό αριθμό σε όλα τα πιστοποιητικά ενός χρήστη . Παράλληλα ο εκδότης του πιστοποιητικού μπορεί να βάλει τους αριθμούς αυτούς στη μαύρη λίστα που διαθέτει , προκειμένου να ανακαλέσει τα πιστοποιητικά αυτού του χρήστη. Αυτός ο μηχανισμός διατηρεί την άνευ όρων μη ανιχνευσιμότητα και μη συνδεσιμότητα των πιστοποιητικών.

Προσφέρει την ίδια δύναμη μυστικότητας με το νέο σύστημα που θα συζητήσουμε παρακάτω. Η τεχνική της μαύρης λίστας δεν είναι τίποτε άλλο από την επανάληψη μιας απόδειξης *not* για κάθε στοιχείο της μαύρης λίστας ,ότι ο αριθμός που συνδέεται με κάποιο ψευδώνυμο του χρήστη δεν ταυτίζεται με κανέναν από αυτούς που περιέχονται στη μαύρη λίστα. Ευαπόδεικτα η τεχνική αυτή είναι πιο ασφαλής υπό τη υπόθεση του διακριτού λογάριθμου.

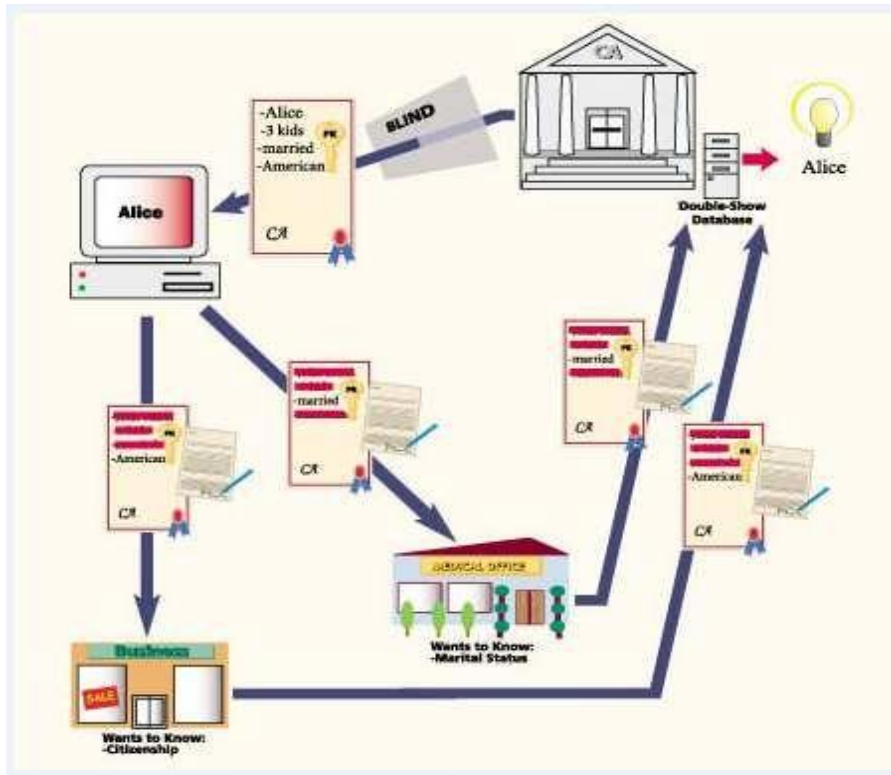
Εντούτοις, ο μηχανισμός που προτείνει ο Brand δεν επιτρέπει την ανάκληση όλων των ψευδωνύμων ενός άγνωστου χρήστη. Επιπλέον, η πολυπλοκότητα της κρυπτογραφικής απόδειξης ότι ο «αόρατα» κωδικοποιημένος αριθμός που σχετίζεται με κάποιο πιστοποιητικό δεν περιλαμβάνεται σε μια μαύρη λίστα, αυξάνεται γραμμικά ως προς το μέγεθος της μαύρης λίστας. Έτσι, η πρόταση δεν είναι πρακτική για μεγάλες μαύρες λίστες. Τέλος , σύμφωνα με τον Brand, ένα πιστοποιητικό ενός χρήστη δεν μπορεί να παρουσιαστεί μη συνδέσιμα παραπάνω από μια φορά. Αυτό σημαίνει ότι παρουσίαση<sup>4</sup> του ίδιου πιστοποιητικού στον ίδιο παροχέα υπηρεσιών ή και σε διαφορετικούς παροχείς υπηρεσιών παραπάνω από μια φορά έχει ως αποτέλεσμα την ανακάλυψη της ταυτότητας του χρήστη.

Το ακόλουθο σχήμα (Σχήμα. 11) απεικονίζει ακριβώς το μειονέκτημα όσον αφορά την ανωνυμία των χρηστών του συστήματος του Brand.

---

<sup>4</sup> Σε κάθε παρουσίαση του ίδιου πιστοποιητικού ο χρήστης αποκαλύπτει ένα διαφορετικό χαρακτηριστικό.





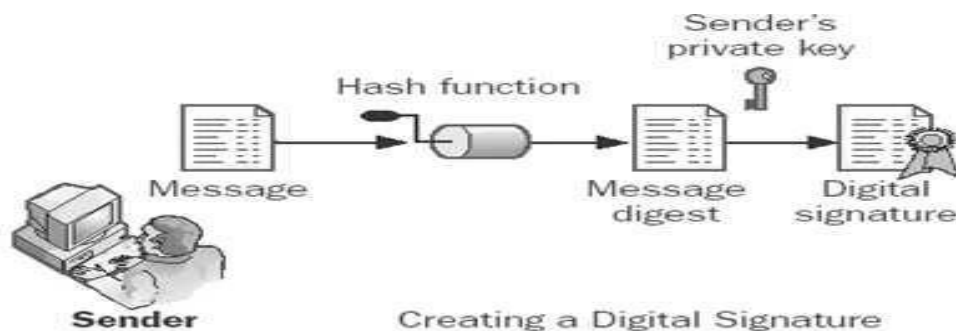
Σχήμα 11. – Σύστημα Πιστοποιητικού Brand με πιστοποιητικά μιας χρήσης

#### 4.1.7.1 Διαδικασία δημιουργίας του μυστικού και δημόσιου κλειδιού ενός χρήστη

Έστω ότι στο ψηφιακό πιστοποιητικό ενός χρήστη κωδικοποιούνται από την Αρχή Πιστοποίησης,  $l$  χαρακτηριστικά τα οποία συμβολίζονται ως  $(x_1, x_2, \dots, x_s)$ . Ο χρήστης παράγει τυχαία μια ποσότητα  $s$  από το σύνολο  $Z_q = \{1, 2, \dots, q\}$  την οποία γνωρίζει μόνο αυτός. Η ποσότητα  $(x_{1s}, x_{2s}, \dots, x_{ss})$  αποτελεί το μυστικό κλειδί του χρήστη, ενώ η ποσότητα  $h = (g_1^{s_1} g_2^{s_2} \dots g_s^{s_l})^c$  αποτελεί το δημόσιο κλειδί του χρήστη. Οι ποσότητες  $g_1, g_2, \dots, g_s$  είναι τυχαίες γεννήτριες της ομάδας  $G_q$  πρώτης τάξης  $q$  οι οποίες αποτελούν μέρος και του δημόσιου κλειδιού της Αρχής Πιστοποίησης.

Επίσης, η Αρχή Πιστοποίησης υπογράφει ψηφιακά το πιστοποιητικό το οποίο εκδίδει και με αυτόν τον τρόπο δεσμεύει «τυφλά» στο δημόσιο κλειδί του πιστοποιητικού ένα ή περισσότερα χαρακτηριστικά τα οποία σχετίζονται με το συγκεκριμένο χρήστη (ο οποίος δεν μπορεί να τα τροποποιήσει).

Το σύνολο των χαρακτηριστικών αυτών , το δημόσιο κλειδί καθώς και η υπογραφή της Αρχής Πιστοποίησης είναι μοναδικά για κάθε πιστοποιητικό και συνεπώς για κάθε χρήστη που είναι κάτοχος του συγκεκριμένου πιστοποιητικού. Με τον όρο *τυφλή υπογραφή* εννοούμε ότι η Αρχή Πιστοποίησης (υπογράφων) δεν μαθαίνει καμία πληροφορία για το (έγγραφο) πιστοποιητικό το οποίο υπογράφει και κατά συνέπεια για την ταυτότητα του κατόχου του. Το σχήμα 11 απεικονίζει τη διαδικασία απόκτησης ψηφιακής υπογραφής .



**Σχήμα 12. Βήματα δημιουργίας ψηφιακής υπογραφής**

#### **4.1.7.2 Παρουσίαση ενός πιστοποιητικού από ένα χρήστη του συστήματος σε κάποιον παροχέα υπηρεσιών**

Ας υποθέσουμε ότι κάποιος χρήστης θέλει να κάνει χρήση κάποιας υπηρεσίας. Η διαδικασία την οποία θα ακολουθήσει είναι η εξής. Θα παρουσιάσει το αντίστοιχο πιστοποιητικό στον παροχέα υπηρεσιών παρέχοντας το δημόσιο κλειδί του πιστοποιητικού και την υπογραφή της Αρχής Πιστοποίησης . Αν επιθυμεί αποκαλύπτει επιλεκτικά μια ιδιότητα για τα χαρακτηριστικά του πιστοποιητικού του χωρίς να δώσει στον παροχέα υπηρεσιών καμία επιπλέον πληροφορία για αυτά τα χαρακτηριστικά.

Ο παροχέας υπηρεσιών με τη σειρά του , για να επιτρέψει στον χρήστη να κάνει χρήση της υπηρεσίας του θα πρέπει να ταυτοποιήσει ότι ο χρήστης είναι πράγματι αυτός που παρουσιάζει.

Προκειμένου να επιτευχθεί κάτι τέτοιο , ο χρήστης υπογράφει ψηφιακά ένα *nonce* χρησιμοποιώντας το μυστικό κλειδί του και το στέλνει στον παροχέα υπηρεσιών . Το *nonce* δεν είναι τίποτε άλλο παρά ένας τυχαίος ή ψευδοτυχαίος αριθμός που κωδικοποιεί για παράδειγμα το όνομα ή οποιαδήποτε άλλη πληροφορία που αφορά τον παροχέα υπηρεσιών. Με αυτό τον τρόπο ο χρήστης αποδεικνύει ότι γνωρίζει το μυστικό κλειδί του και ότι τα χαρακτηριστικά του πιστοποιητικού του ικανοποιούν την ιδιότητα που αποκαλύπτει στον παροχέα υπηρεσιών. Άρα, είναι πράγματι αυτός που παρουσιάζει.

Ο χρήστης αποκαλύπτει επιλεκτικά κάποια πληροφορία για κάποια από τα χαρακτηριστικά του πιστοποιητικού του, π.χ. αποκαλύπτει ότι είναι άγαμος ή ότι είναι ενήλικας. Ωστόσο την ποσότητα  $s$  που εμπλέκεται στο μυστικό κλειδί του την γνωρίζει μόνο αυτός , άρα το μυστικό κλειδί του το γνωρίζει εξ ολοκλήρου αυτός. Για δεδομένο σύνολο χαρακτηριστικών και για δεδομένο δημόσιο κλειδί  $h$  η ποσότητα  $s$  είναι μοναδική ώστε να ικανοποιείται η σχέση του δημόσιου κλειδιού  $h = (g_1^{s_1} g_2^{s_2} \dots g_s^{s_s})^c$ . Δηλαδή δεν υπάρχει για το ίδιο δημόσιο κλειδί  $h$  ποσότητα  $s^u$  διαφορετική της  $s$  η οποία να επαληθεύει τον τύπο του δημόσιου κλειδιού. Αυτό σημαίνει ότι σε κάθε χρήστη του συστήματος αντιστοιχεί ένα μοναδικό ζεύγος  $(h, s)$ .

#### 4.1.7.3 Ιδιότητες που ικανοποιούν τα χαρακτηριστικά ενός πιστοποιητικού

Ο χρήστης μπορεί να αποδείξει οποιαδήποτε από τις ακόλουθες ιδιότητες όσον αφορά τα χαρακτηριστικά του πιστοποιητικού του.

##### 1) Γνώση μια παράστασης που περιέχει τιμές των χαρακτηριστικών :

Ο χρήστης αποδεικνύει γνώση μιας αναπαράστασης  $(x_1, x_2, \dots, x_s)$  του δημόσιου κλειδιού  $h \in G_q$  ως προς οποιεσδήποτε τυχαίες γεννήτριες

$(g_1, g_2, \dots, g_s) \in G_q^s$  . Για να το επιτύχει αυτό αποκαλύπτει οποιοδήποτε υποσύνολο  $D$  του συνόλου των χαρακτηριστικών  $(x_1, x_2, \dots, x_s)$ .

Για ένα υποσύνολο  $D = \{x_{j-1}, x_j\}$  σημειώνουμε το ακόλουθο πρωτόκολλο :

$PK \{(z_1, z_2, \dots, z_{j-2}, z_{j+1}, \dots, z_s) :$

$$(z_1, z_2, \dots, z_{j-2}, x_{j-1}, x_j, z_{j+1}, \dots, z_s) = \text{ree}_{(g_1, g_2, \dots, g_l)} h \}$$

Οι μεταβλητές με ελληνικούς χαρακτήρες αναπαριστούν τιμές που παραμένουν άγνωστες στον παροχέα υπηρεσιών ενώ αποκαλύπτονται μόνο δύο από αυτές .

## 2) Γνώση και ισότητα διακριτών λογαρίθμων

Δεδομένων των τιμών  $h_1, h_2, h_3, \dots, h_s, g_1, g_2, g_3, g_4$  στο  $G_q$ , ο χρήστης Alice αποδεικνύει γνώση της τριπλέτας χαρακτηριστικών  $(x_1, x_2, x_3)$  έτσι ώστε

$$h_1 = g_1^{s_1} g_2^{s_2} \text{ και } h_2 = g_3^{s_1} g_4^{s_2} .$$

Το πρωτόκολλο που αποδεικνύει τη γνώση και την ισότητα διακριτών λογαρίθμων σημειώνεται ως εξής :

$$PK \{(x_1, x_2, x_3) : (x_1, x_2) \text{ree}_{(g_1, g_2)} h_1 \wedge (x_1, x_3) \text{ree}_{(g_3, g_4)} h_2 \}$$

## 3) Γνώση διακριτών λογαρίθμων που αποτελούνται από διαδοχικές δυνάμεις

Έστω  $h_1, h_2, h_3, \dots, h_s, g_1, g_2$  στο  $G_q$ . Ο χρήστης μπορεί να αποδείξει γνώση των τιμών  $x_1, y_1, \dots, y_n \in \mathbb{Z}_q$  έτσι ώστε  $h_i = g_1^{s_i} g_2^{y_i}$  για  $i \in \{1, 2, \dots, n\}$ .

Σημειώνουμε αυτό το πρωτόκολλο ως εξής :

$$PK\{(z, y_1, y_2, \dots, y_n) :$$

$$(z, y_1) = \text{ree}_{g_1 g_2} h_1 \wedge (z^2, y_1) = \text{ree}_{g_1 g_2} h_2 \wedge \dots \wedge (z^n, y_n) = \text{ree}_{g_1 g_2} h_n \}$$

## 4) Γνώση διακριτού λογάριθμου διάφορου του μηδενός

Έστω το δημόσιο κλειδί  $h$  στο  $G_q$ . Ο χρήστης Alice επιδεικνύει στον παροχέα υπηρεσιών Bob ότι γνωρίζει μια αναπαράσταση  $(x_1, x_2)$  του δημόσιου κλειδιού  $h$  ως προς τις βάσεις  $(g_1, g_2) \in G_q^2$ , έτσι ώστε  $x_1 \neq 0$ . Το πρωτόκολλο σημειώνεται ως εξής :

$$PK\{(x_1, x_2) : (x_1, x_2) = \text{ree}_{g_1 g_2} h \wedge x_1 \neq 0 \}$$

Αυτό αποτελεί μια απόδειξη **not** σύμφωνα με τον Brand.

**5) ΚΑΙ συνδέσεις :** Οι προηγούμενοι τύποι μπορούν να συνδυαστούν με ΚΑΙ συνδέσεις. Δεδομένων των τύπων  $F_1(x_{1,1}, \dots, x_{1,s_1}), \dots, F_n(x_{n,1}, \dots, x_{n,s_n})$  για τις μυστικές ποσότητες  $x_{i,1}, \dots, x_{i,s_i}, i = 1, 2, \dots, n$ . Σημειώνουμε αυτό το πρωτόκολλο ως εξής:

$$PK \{ (x_{1,1}, \dots, x_{n,s_n}) : F_1(x_{1,1}, \dots, x_{1,s_1}) \wedge \dots \wedge F_n(x_{n,1}, \dots, x_{n,s_n}) \}$$

Υπό την υπόθεση του διακριτού λογάριθμου, όλα τα πρωτόκολλα είναι ιδανικοί, έντιμοι επαληθευτές μηδενικής γνώσης.

#### 4.1.7.4 Βασικές ιδιότητες του συστήματος του Brand

Το σύστημα πιστοποιητικού του Brand βασίζεται στο πρωτόκολλο έκδοσης πιστοποιητικών των Chaum-Pedersen και ικανοποιεί τις ακόλουθες ιδιότητες.

1. Εάν ένας τίμιος χρήστης αποδεχτεί το πρωτόκολλο έκδοσης πιστοποιητικού, ανακτά ένα μυστικό κλειδί πιστοποιητικού  $(x_1, x_2, \dots, x_s, s)$ , ένα αντίστοιχο δημόσιο κλειδί  $h$  και μια υπογραφή  $sign(h)$  έτσι ώστε το ζεύγος δημόσιο κλειδί-υπογραφή  $(h, sign(h))$  είναι ομοιόμορφα κατανεμημένο στο  $\{(h, sign(h)) \mid h \in G_q - \{1\}\}$

Αν το δημόσιο κλειδί ήταν μονάδα υποχρεωτικά το μυστικό κλειδί του χρήστη θα έπρεπε να ήταν μηδέν, άρα οποιοσδήποτε θα γνώριζε εκ των προτέρων την τιμή του, γεγονός που θα έθετε σε κίνδυνο την ασφάλεια του συστήματος.

2. Δεδομένου ότι το πρωτόκολλο των Chaum Pedersen είναι ασφαλές, είναι ανέφικτο ένα πιστοποιητικό να πλαστογραφηθεί.

3. Για οποιοδήποτε πιστοποιητικό δημόσιου κλειδιού  $h$  και υπογραφής  $sign(h)$ , για οποιοδήποτε χαρακτηριστικά  $(x_1, x_2, \dots, x_s)$ , και για οποιαδήποτε άποψη της αρχής πιστοποίησης σε ένα πρωτόκολλο έκδοσης πιστοποιητικού στο οποίο χρησιμοποιείται το  $e = g_1^{s_1} g_2^{s_2} \dots g_s^{s_s}$  ως αρχική είσοδος (με  $x_1, x_2, \dots, x_s$  γνωστά από την CA), υπάρχει ακριβώς ένα σύνολο τυχαίων επιλογών που ένας τίμιος χρήστης θα μπορούσε να έχει κάνει κατά τη διάρκεια της εκτέλεσης αυτού του πρωτοκόλλου έτσι που θα είχε αποκτήσει ένα πιστοποιητικό που θα περιείχε και το δημόσιο κλειδί  $h$  και την υπογραφή  $sign(h)$ .

4. Έστω  $h$  ένα έγκυρο δημόσιο κλειδί πιστοποιητικού .Υπό την υπόθεση  $\mathcal{P}$

διακριτού λογάριθμου και εφόσον  $s \neq 0$  , η απόδειξη της γνώσης μιας αναπαράστασης  $(x_1^*, \dots, x_s^*, s^*)$  του  $h^{-1}$  ως προς το  $(g_1, g_2, \dots, g_s, h)$  , είναι

ισοδύναμη με την απόδειξη γνώσης ενός έγκυρου μυστικού κλειδιού  $(x_1^*s, \dots, x_s^*s, s)$  ως προς το  $h$  . Επιπλέον , ισχύει η σχέση  $s^* = s^{-1}$  .

5. Θεωρούμε έναν αυθαίρετο αριθμό από διαδοχικές επαναλήψεις ενός πρωτοκόλλου παρουσίασης με έναν παροχέα υπηρεσιών στον οποίο ο χρήστης αποκαλύπτει μόνο μια σχέση για τα χαρακτηριστικά ,η οποία δεν περιέχει το μυστικό κλειδί  $s$ , και η οποία χρησιμοποιεί μόνο αποδείξεις γνώσης που είναι στατιστικά μη ευδιάκριτες από τον μάρτυρα.

6. Δεδομένου του διακριτού λογάριθμου, ένας κακόβουλος χρήστης (ή αλλιώς εισβολέας )  $A$  , αφού δεσμεύσει μια εκτέλεση ενός πρωτόκολλου έκδοσης με την

Αρχή Πιστοποίησης στο οποίο χρησιμοποιείται σαν είσοδος η ποσότητα  $e$

$(e = g_1^{s_1^*} g_2^{s_2^*} \dots g_s^{s_s^*})$  , εξάγει ένα έγκυρο πιστοποιητικό που περιέχει μυστικό κλειδί  $(x_1, x_2, \dots, x_s, s)$  για το οποίο ισχύει ότι  $(x_1, x_2, \dots, x_s, s) = (x_1^*s, \dots, x_s^*s, s)$

με μεγάλη πιθανότητα. Αυτή η υπόθεση παραμένει έγκυρη ακόμα και όταν πολυωνυμικά πολλές εκτελέσεις του πρωτοκόλλου έκδοσης επαναλαμβάνονται αυθαίρετα.

#### 4.1.8 Σύγκριση του συστήματος του Brand με προηγούμενα συστήματα πιστοποιητικού

Πριν προχωρήσουμε στην ανάλυση του νέου συστήματος , θα συγκρίνουμε το σύστημα του Brand με τα συστήματα πιστοποιητικού των Camenisch και Lysyanskaya (CL-RSA και CL-DL ). Η σύγκριση αφορά το μέγεθος σε bytes ενός πιστοποιητικού για καθένα από τα τρία συστήματα, το μέγεθος της επικοινωνίας σε bytes και τον αριθμό των εκθετικοποιήσεων που απαιτούνται για την έκδοση και την παρουσίαση ενός πιστοποιητικού σε κάθε σύστημα ξεχωριστά.

Το σύστημα των Camenisch και Lysyanskaya (εν συντομία CL) βασίζεται σε ένα σχέδιο υπογραφών με πρωτόκολλα για την απόκτηση μιας υπογραφής πάνω σε δεσμευμένες τιμές και πρωτόκολλα για την απόδειξη κατοχής υπογραφών μέσω αποδείξεων μηδενικής γνώσης. Ένα πιστοποιητικό μπορεί να παρουσιαστεί μη συνδεδεσιμα πολλαπλές φορές και όλα τα ψευδώνυμα ενός χρήστη που βασίζονται στο ίδιο πιστοποιητικό μπορούν να ανακληθούν απλά με ανάκληση του πιστοποιητικού.

Το σύστημα των CL το διακρίνουμε σε αυτό που βασίζεται στο πρωτόκολλο RSA και το σημειώνουμε ως CL-RSA και σε αυτό που βασίζεται στο διακριτό λογάριθμο και το σημειώνουμε ως CL-DL ( **D**iscrete **L**ogarithm ).

Για την αξιολόγηση των συστημάτων οι πολλαπλασιασμοί και οι προσθέσεις παραλείπονται , καθώς η απαίτησή τους σε υπολογιστικούς πόρους είναι αμελητέα . Θα αξιολογήσουμε ένα πρωτόκολλο έκδοσης πιστοποιητικού με  $l$  ιδιότητες επιλεγμένες από το χρήστη ( που είναι άγνωστες στην CA) και ένα πρωτόκολλο παρουσίασης στο οποίο καμία ιδιότητα των χαρακτηριστικών δεν καταδεικνύεται. Ο πίνακας που ακολουθεί συνοψίζει τα αποτελέσματα.

Table 1. A comparison of complexity for different credential systems

size of credentials

Brands	$32l + 328$ bytes
CL-RSA	$32l + 473$ bytes
CL-DL	$96l + 128$ bytes

issuing protocol

	#expon. Alice		#expon. CA		comm.
	offline	online	offline	online	
Brands	$2l + 6$	3	2	$l + 3$	$32l + 1116$ bytes
CL-RSA	$3l + 14$	7	-	$2l + 21$	$62l + 1405$ bytes
CL-DL	$2l + 2$	-	$2l + 3$	$l + 3$	$96l + 213$ bytes

showing protocol

	#expon. Alice		#expon. Bob		comm.
	offline	online	offline	online	
Brands	$l + 2$	-	-	$l + 7$	$32l + 748$ bytes
CL-RSA	$2l + 18$	-	-	$2l + 9$	$62l + 785$ bytes
CL-DL	$4l + 8$	-	-	$6l + 8$	$96l + 380$ bytes

### Σχήμα 13. Σύγκριση πολυπλοκότητας για διαφορετικά συστήματα πιστοποιητικού

Όπως φαίνεται και από τον πίνακα, τα πιστοποιητικά του Brand είναι «φτηνότερα» σε όλες τις πτυχές σε σχέση με το σχέδιο CL-RSA. Όσον αφορά τα πιστοποιητικά CL-DL, είναι πολύ «φτηνότερα» ως προς την παρουσίαση και ελαφρώς «ακριβότερα» για την ανάκτηση.

Επιπλέον, τα πιστοποιητικά του Brand παρόλο που είναι πρακτικά ως προς την παρουσίαση και παρέχουν απεριόριστη μυστικότητα, δεν μπορούν να παρουσιαστούν παραπάνω από μια φορά μη συνδέσιμα. Αυτό το «πρόβλημα» μπορεί να αντιμετωπιστεί με τη χρησιμοποίηση πολλαπλών αντιγράφων του ίδιου πιστοποιητικού. Ωστόσο, η έκδοση τουλάχιστον ενός επιπλέον πιστοποιητικού για τις ίδιες ιδιότητες καταλαμβάνει 296 δυαδικά ψηφία και μπορεί να ανακτηθεί μετά από 7 εκθετικοποιήσεις από τον χρήστη Alice.

Τέλος, για πιστοποιητικά  $l$  χαρακτηριστικών,  $\frac{S}{5}$  περίπου πιστοποιητικά του Brand καταλαμβάνουν τον ίδιο χώρο όπως ένα πιστοποιητικό CL-DL ενώ η ανάκτηση  $\frac{S}{7} + 2$  πιστοποιητικών του Brand κοστίζει κατά προσέγγιση για την Alice τόσο όσο η ανάκτηση ενός πιστοποιητικού CL-RSA.



## Κεφάλαιο 5: Το νέο σύστημα πιστοποιητικού

### The Problem: Pseudonym System



Σχήμα 14. Άποψη ενός συστήματος Ανώνυμων Πιστοποιητικών από τον πραγματικό κόσμο

### 5.1 Εισαγωγή

Μια σημαντική πρακτική εφαρμογή αποτελεί το σύστημα ανώνυμου πιστοποιητικού. Ένα τέτοιο σύστημα καλείται ανώνυμο διότι ο χρήστης είναι γνωστός μόνο μέσω των ψευδωνύμων του και οι συναλλαγές που πραγματοποιούνται από τον ίδιο χρήστη δεν μπορούν να διασυνδεθούν και να αποκαλυφθεί η ταυτότητα του. Για αυτό το λόγο αποτελεί το καλύτερο μέσο παροχής προστασίας στους χρήστες. Θεμελιώνεται σε δύο πολύ σημαντικά πρωτόκολλα, το RSA και το Diffie Hellman και θεωρείται ανώτερο σε σχέση με τα προηγούμενα συστήματα που είδαμε στο κεφάλαιο 3, διότι παρουσιάζει ορισμένα πλεονεκτήματα.

Το πρώτο βασικό πλεονέκτημα του, αποτελεί το γεγονός ότι ένας χρήστης μπορεί να χρησιμοποιήσει το ίδιο πιστοποιητικό όσες φορές χρειαστεί, χωρίς να μπορούν να διασυνδεθούν οι διαφορετικές χρήσεις, και χωρίς να έχει καμία εμπλοκή ο χρήστης με τον εκδότη του πιστοποιητικού.

Επίσης , από τη μία παρέχει ανωνυμία σε έναν χρήστη που είναι κάτοχος διάφορων πιστοποιητικών από διαφορετικούς οργανισμούς, από την άλλη όμως , αν ο χρήστης καταχραστεί την ανωνυμία που του προσφέρεται και προβεί σε παράνομες συναλλαγές το ίδιο το σύστημα μπορεί να εντοπίσει την ταυτότητα ή το ψευδώνυμο του συγκεκριμένου χρήστη μέσω ενός διαχειριστή ανάκλησης ανωνυμίας.

Ακόμα , οι οργανισμοί που εμπλέκονται στο σύστημα έχουν τα δικά τους κρυπτογραφικά κλειδιά (δημόσιο – μυστικό κλειδί) ανεξάρτητα ο ένας από τον άλλο. Τέλος , χαρακτηρίζεται από την ιδιότητα της μη μεταφερισιμότητας πιστοποιητικών και ψευδωνύμων μεταξύ διαφορετικών χρηστών του συστήματος. Δηλαδή παρέχει μέσα που αποτρέπουν τους χρήστες να χρησιμοποιούν από κοινού τα πιστοποιητικά τους και για να το ενισχύσει εισάγει μια νέα μέθοδο , την οριστική μη δυνατότητα κοινής χρήση , η οποία θεμελιώνεται στην αρχή της κυκλικής κρυπτογράφησης. Τις έννοιες αυτές θα τις αναλύσω στις παραγράφους που ακολουθούν.

## **5.2 Περιγραφή των οντοτήτων που αλληλεπιδρούν στο νέο σύστημα ανώνυμου πιστοποιητικού**

Το νέο σύστημα ανήκει στην κατηγορία των συστημάτων ανώνυμου πιστοποιητικού όπου οι χρήστες του έχουν τη δυνατότητα πρόσβασης σε πολλαπλές υπηρεσίες εισάγοντας τα διαπιστευτήριά τους μια φορά και μόνο όταν συνδέονται αρχικά στο σύστημα. Η δομή και η λειτουργία του βασίζεται στο σχέδιο του Brand.

Αποτελείται από τέσσερις βασικές οντότητες , τους χρήστες τους οποίους συμβολίζει με  $U$  , έναν κεντρικό παροχέα ταυτότητας  $IP$ , παροχείς υπηρεσιών τους οποίους σημειώνει με  $S_i$ <sup>5</sup> και οργανισμούς χορήγησης και επικύρωσης πιστοποιητικών. Οι χρήστες είναι οντότητες που λαμβάνουν πιστοποιητικά και είναι γνωστοί στους παροχείς υπηρεσιών (οργανισμούς ) μόνο μέσω των ψευδωνύμων τους. Ένας οργανισμός μπορεί να χορηγεί έναν μοναδικό τύπο πιστοποιητικού (εναλλακτικά και διαφορετικούς τύπους) και γνωρίζει τους χρήστες μόνο με τα ψευδώνυμα τους .

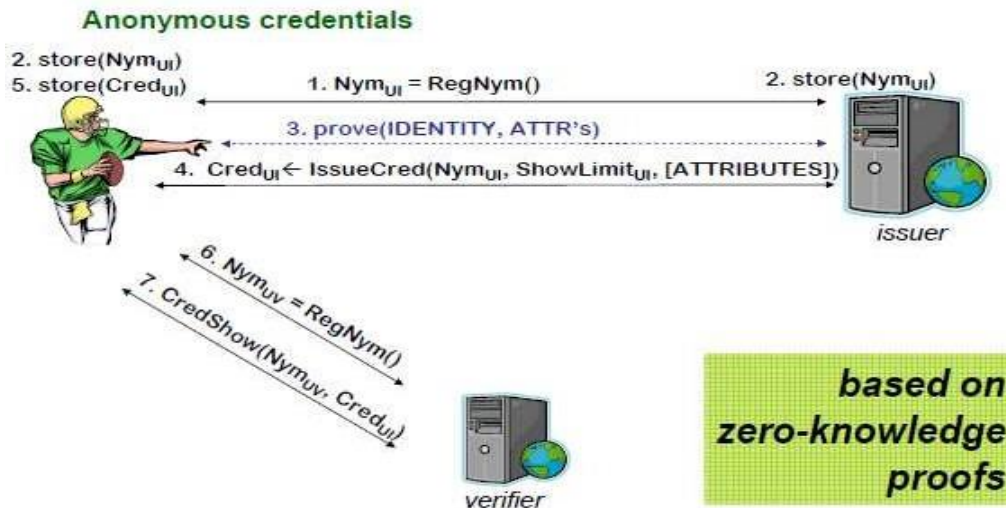
---

<sup>5</sup> Με  $S_i$  επίσης συμβολίζεται και η  $i$  υπηρεσία όπου  $i = 1, 2, \dots, l$ .

Ο παροχέας ταυτότητας δημιουργεί το δικό του δημόσιο και μυστικό κλειδί τα οποία συμβολίζονται με  $(P_k, S_k)$  αντίστοιχα. Το μυστικό κλειδί το χρησιμοποιεί για να υπογράφει ψηφιακά τα πιστοποιητικά ταυτότητας τα οποία εκδίδει. Σε κάθε πιστοποιητικό κωδικοποιείται ένα πλήθος  $l + 1$  χαρακτηριστικών (όπου το  $l + 1$  χαρακτηριστικό είναι ο χρόνος έκδοσης του πιστοποιητικού  $t$ ).

Οι αποφάσεις του παροχέα ταυτότητας λαμβάνονται πάνω στην ομάδα  $G_q$  στην οποία ανήκουν και οι γεννήτριες  $g_1, g_2, \dots, g_{s+1}, h_0$ . Το δημόσιο κλειδί είναι της μορφής  $(g_1^{s_1} g_2^{s_2} \dots g_s^{s_l} g_{s+1}^t, h_0)^c$  όπου  $(x_1, x_2, \dots, x_s, s, t)$  το μυστικό κλειδί. Ο παροχέας ταυτότητας είναι αρμόδιος για τη διανομή σε κάθε χρήστη ψηφιακών ψευδωνύμων. Ακόμα, ένας οργανισμός μπορεί να εκδώσει ένα πιστοποιητικό σε ένα ψευδώνυμο, και ο αντίστοιχος χρήστης να αποδεικνύει κατοχή του σε έναν άλλο οργανισμό (που τον γνωρίζει με διαφορετικό ψευδώνυμο), χωρίς να αποκαλύπτει τίποτα περισσότερο από το γεγονός ότι κατέχει ένα τέτοιο πιστοποιητικό.

Ακόμα, για να αποφευχθεί η κοινή χρήση πιστοποιητικών ή ψευδωνύμων στο σύστημα εισήχθη η Αρχή Πιστοποίησης. Πρόκειται για έναν οργανισμό που εγγυάται ότι οι χρήστες που εισέρχονται στο σύστημα κατέχουν ένα κύριο δημόσιο και μυστικό κλειδί που τους καθιστά μοναδικούς στο σύστημα. Μια άλλη οντότητα στο σύστημα είναι ο επαληθευτής. Ο ρόλος του είναι να πιστοποιεί την εγκυρότητα πιστοποιητικών χρηστών και σε αντίθετη περίπτωση να «επικοινωνεί» είτε με τον οργανισμό έκδοσης του πιστοποιητικού είτε με την Αρχή Πιστοποίησης για να ενημερώνει ότι ο χρήστης δεν είναι ο κάτοχος του συγκεκριμένου πιστοποιητικού που παρουσιάζει.



Σχήμα 15. Ανώνυμα πιστοποιητικά βασισμένα σε αποδείξεις μηδενικής γνώσης

### 5.3 Βασικές επιθυμητές ιδιότητες

Το σύστημα απαιτούμε να έχει κάποιες επιθυμητές ιδιότητες που θα το καθιστούν ασφαλές, αξιόπιστο και αποδοτικό. Όσον αφορά στην αξιοπιστία, επιθυμούμε να μην μπορεί να πλαστογραφηθεί ένα πιστοποιητικό για έναν άλλο χρήστη ακόμα και αν χρήστες και οργανισμοί συνεργαστούν και εκτοξεύσουν προσαρμοστική επίθεση σε κάποιον οργανισμό.

Επίσης, κάθε ψευδώνυμο και πιστοποιητικό θέλουμε να ανήκει σε καλά ορισμένους χρήστες. Συγκεκριμένα, θα πρέπει να είναι αδύνατο για διαφορετικούς χρήστες να συνεργαστούν και να επιδεικνύουν κάποια από τα πιστοποιητικά τους σε έναν οργανισμό και να αποκτούν ένα πιστοποιητικό για κάποιον από αυτούς, το οποίο ο ίδιος ο χρήστης δεν θα μπορούσε να έχει. Συστήματα στα οποία αυτό είναι αδύνατο να συμβεί λέγεται ότι έχουν **συνολική πιστοποιητικών**.

Καθώς οι οργανισμοί είναι αυτόνομες οντότητες, είναι επιθυμητό ότι θα είναι διαχωρίσιμοι, π.χ., ότι θα μπορούν να επιλέγουν τα κρυπτογραφικά κλειδιά τους (δημόσιο και μυστικό κλειδί) ανεξάρτητα από τις άλλες οντότητες, ώστε να εξασφαλίζουν ασφάλεια αυτών των κλειδιών και να διευκολύνουν τη διαχείριση του συστήματος κλειδιού.

Το σχέδιο πρέπει να παρέχει ασφάλεια και να προστατεύει την ιδιωτικότητα του χρήστη. Ο οργανισμός δεν μπορεί να ανακαλύψει τίποτα για έναν χρήστη, εκτός από την κατοχή ενός συνόλου πιστοποιητικών, ακόμα και αν ο οργανισμός συνεργαστεί με άλλους οργανισμούς. Συγκεκριμένα δύο ψευδώνυμα που ανήκουν στον ίδιο χρήστη δεν μπορούν να διασυνδεθούν και να εντοπισθεί η ταυτότητα του όπως συνέβαινε στο σύστημα του Brand, παρά μόνο υπό συγκεκριμένες συνθήκες.

Τέλος, το σύστημα για να είναι αποδοτικό απαιτούμε να βασίζεται σε αποδοτικά πρωτόκολλα. Αυτό σημαίνει ότι κάθε αλληλεπίδραση μεταξύ των οντοτήτων του συστήματος να εμπλέκει όσο το δυνατόν λιγότερες οντότητες, και το ποσό της επικοινωνίας να είναι ελάχιστο. Συγκεκριμένα, αν ένας χρήσης κατέχει ένα πιστοποιητικό που μπορεί να παρουσιαστεί πολλές φορές, μπορεί να το επιδεικνύει κάθε φορά χωρίς να βάζει τον οργανισμό να επανεκδίδει (και κατά συνέπεια να υπογράφει) κάθε φορά το ίδιο πιστοποιητικό.

## 5.4 Πρωτόκολλο ανάκτησης ψευδωνύμου

Ο χρήστης για να ανακτήσει ένα σύνολο ψευδωνύμων εκτελεί το ακόλουθο πρωτόκολλο με τον παροχέα ταυτότητας.

- a) Ο χρήστης  $U$  επιλέγει τυχαία τις ποσότητες  $d_{(1,1)}, d_{(1,2)}, d_{(1,3)}, \dots, d_{(1,s)}$ ,  $e$

όπου το  $e$  το γνωρίζει μόνο αυτός. Υπολογίζει την ποσότητα

$$e = g_1^{d_{(1,1)}} g_2^{d_{(1,2)}} g_3^{d_{(1,3)}} \dots g_s^{d_{(1,s)}} g_{s+1}^e \text{ και τη στέλνει στον παροχέα}$$

ταυτότητας  $IP$ .

- b) Ο παροχέας ταυτότητας ανακτά την ποσότητα  $e_1$ , συλλέγει τυχαία ποσότητες

$d_{(2,1)}, d_{(2,2)}, d_{(2,3)}, \dots, d_{(2,s)}$ , τις στέλνει στον χρήστη και υπολογίζει το

$$\text{γινόμενο } e = e_1 e_2, e_2 = g_1^{d_{(2,1)}} g_2^{d_{(2,2)}} g_3^{d_{(2,3)}} \dots g_s^{d_{(2,s)}}. \text{ Ο χρήστης}$$

δημιουργεί τις ποσότητες  $d_i$  σύμφωνα με τη σχέση  $d_i = d_{(1,i)} + d_{(2,i)}$

$$i = 1, 2, \dots, l \text{ και υπολογίζει την ποσότητα } e = g_1^{d_1} g_2^{d_2} \dots g_s^{d_l}.$$

- c) Ο παροχέας ταυτότητας και ο χρήστης εκτελούν τα παραπάνω βήματα  $l$  φορές

όσα και τα ψευδώνυμα που θέλει να ανακτήσει ο χρήστης έχοντας το  $e$  σαν

αρχική είσοδο του πρωτοκόλλου (ανάκτησης ψευδωνύμου). Έτσι αποκτά  $l$

ζεύγη-ψευδώνυμα  $(P_i, \text{sign}(P_i))$  και  $l$  τιμές  $s_i$  τέτοιες ώστε  $P_i = (e h_0)^{s_i}$

$i = 1, 2, 3, \dots, l$ .

### 5.4.1 Βασικά χαρακτηριστικά του πρωτοκόλλου ανάκτησης ψευδωνύμων

Η δημιουργία του τυχαίου συνόλου  $(d_1, d_2, d_3, \dots, d_s)$  γίνεται έτσι ώστε ούτε ο χρήστης ούτε ο παροχέας ταυτότητας μπορούν να ελέγξουν τη τελική τιμή του. Το  $e$  επιλέγεται τυχαία από τον χρήστη, έτσι παραμένει άνευ όρων άγνωστο στον παροχέα ταυτότητας. Βάσει του συνόλου  $(d_1, d_2, d_3, \dots, d_s, e)$  δημιουργείται μία λίστα από ψευδώνυμα  $(P_i, \text{sign}(P_i))$ ,  $i = 1, 2, 3, \dots, l$  ένα για κάθε υπηρεσία  $S_i$ .

Η ποσότητα  $P_i$  αποτελεί το δημόσιο κλειδί του χρήστη. Ο χρήστης είναι ο ιδιοκτήτης του ψευδωνύμου  $(P_i, \text{sign}(P_i))$  αν γνωρίζει το μυστικό κλειδί που αντιστοιχεί στο δημόσιο κλειδί  $P_i$ . Εφόσον ο χρήστης ακολουθήσει τα βήματα  $(a - c)$ , τα προκύπτοντα ψευδώνυμα θα είναι άνευ όρων μη συνδέσιμα και μη ανιχνεύσιμα. Επίσης, ο χρήστης υπολογίζει και ένα μυστικό κλειδί  $(d_1s_i, d_2s_i, d_3s_i, \dots, d_s s_i, es_i, es_i)$  ένα για κάθε ψευδώνυμο  $(P_i, \text{sign}(P_i))$ .

Στο εξής όταν ο χρήστης συνδέεται με έναν παροχέα υπηρεσιών θα επικυρώνεται αποδεικνύοντας ότι γνωρίζει το μυστικό κλειδί του ψευδωνύμου του, χωρίς να αποκαλύπτει πιο είναι αυτό. Αυτό έχει ως αποτέλεσμα να αποτρέπονται επιθέσεις επανάληψης του ίδιου ψευδωνύμου από άλλους χρήστες. Επίσης, για κάθε ψευδώνυμο με το οποίο ένας παροχέας υπηρεσιών συσχετίζει έναν χρήστη, ο παροχέας υπηρεσιών απαιτεί από τον χρήστη να του αποκαλύψει έναν από αυτούς τους κωδικοποιημένους τυχαίους αριθμούς. *Με την αποκάλυψη ενός διαφορετικού τυχαίου αριθμού για κάθε ψευδώνυμο, οι χρήστες διατηρούν την άνευ όρων μη συνδεσιμότητα των ψευδωνύμων τους.*

Τα ψηφιακά ψευδώνυμα όπως αναφέρθηκε είναι άνευ όρων μη συνδέσιμα και μη ανιχνεύσιμα. Με τον όρο μη συνδέσιμα εννοούμε ότι ακόμα και αν συνεργαστούν οι παροχείς υπηρεσιών με τον παροχέα ταυτότητας δεν μπορούν να συνδέσουν τα διαφορετικά ψευδώνυμα ενός χρήστη και να πιστοποιήσουν ότι ανήκουν στον ίδιο χρήστη.

Έτσι, με τη χρησιμοποίηση ενός διαφορετικού ψευδωνύμου με κάθε παροχέα υπηρεσιών, κάθε χρήστης μπορεί να εξασφαλίσει ότι οι πληροφορίες του λογαριασμού που εγκαθιστά με τους διαφορετικούς παροχείς υπηρεσιών δεν μπορεί να συλλεχθούν σε έναν υπερκατάλογο.

Υπό την υπόθεση του διακριτού λογάριθμου στο  $G_q$  και για σταθερές τιμές  $d \in \mathbb{Z}_q = \{1, 2, \dots, q\}$  και  $i \in \{1, 2, \dots, l\}$ · οποιοσδήποτε κακόβουλος χρήστης  $A$  δεσμεύσει ένα πρωτόκολλο ανάκτησης ψευδώνυμου με τον παροχέα ταυτότητας  $IP$ , και αποκτήσει ένα έγκυρο ψευδώνυμο  $(P, \text{sign}(P))$ , με αμελητέα πιθανότητα η τιμή  $d$  είναι η  $i$  τιμή που κωδικοποιείται στο δημόσιο κλειδί  $P$ . Η πρόταση αυτή είναι προφανές ότι πιστοποιεί την ασφάλεια και την ιδιότητα της μη πλαστογράφησης που το νέο σύστημα παρέχει στους χρήστες του και επιπλέον ενισχύει την εμπιστοσύνη των χρηστών στο σύστημα.

### 5.5 Ανάκληση Ανωνυμίας χρήστη

Επίσης, είναι δυνατή η σφαιρική ανάκληση όλων των ψευδωνύμων ενός χρήστη σε περίπτωση που ο χρήστης κάνει κακή χρήση οποιασδήποτε υπηρεσίας. Αυτό σημαίνει ότι ο χρήστης πλέον δεν θα μπορεί να έχει πρόσβαση σε καμία από τις υπηρεσίες που προηγούμενα χρησιμοποιούσε. Για να μπορεί να συμβεί κάτι τέτοιο ο παροχέας ταυτότητας συνδέει αόρατα όλα αυτά τα ψευδώνυμα. Συγκεκριμένα, κωδικοποιεί αόρατα σε όλα τα ψευδώνυμα ενός χρήστη ένα σύνολο τυχαίων αριθμών που είναι μοναδικοί για τον συγκεκριμένο χρήστη, χωρίς να γνωρίζει αυτούς τους αριθμούς.

Συγχρόνως, οι παροχείς υπηρεσιών μπορούν να βάλουν σε μαύρη λίστα τους αποκαλυπτόμενους αριθμούς. Από την άλλη, οι χρήστες μπορούν αποτελεσματικά να αποδείξουν ότι οι κωδικοποιημένοι αριθμοί τους δεν ανήκουν στη μαύρη λίστα, χωρίς να αποκαλύψουν καμία πρόσθετη πληροφορία για αυτούς.

Αυτή η τεχνική ανάκλησης δεν προσκρούει στην ιδιωτικότητα των χρηστών, ούτε δίνει κρυφές δυνάμεις στους παροχείς υπηρεσιών και στον παροχέα ταυτότητας. Προκειμένου να είναι σε θέση να βάλει στη μαύρη λίστα έναν χρήστη, ένας παροχέας υπηρεσιών πρέπει να ζητήσει από όλους τους χρήστες που ζητούν πρόσβαση να αποδείξουν ότι δεν είναι στη μαύρη λίστα του.

Για να υπολογιστεί μια απόδειξη μαύρης λίστας οι χρήστες απαιτούν τη μαύρη λίστα του παροχέα υπηρεσιών ως είσοδο. Τέλος, ένας χρήστης αποδεικνύοντας ότι δεν είναι στον κατάλογο ανάκλησης δεν αποκαλύπτει καμία πληροφορία για την ταυτότητά του.

## 5.6 Εγγραφή Ψευδωνύμου με τον Παροχέα Υπηρεσιών

Για να εγγράψει ένας χρήστης  $U$  ένα ψευδώνυμο  $(P_i, \text{sign}(P_i))$  με τον παροχέα υπηρεσιών  $S_i$ , ο χρήστης παρουσιάζει το ψευδώνυμο  $(P_i, \text{sign}(P_i))$  και αποκαλύπτει την τιμή  $d_i$  που κωδικοποιείται στο  $P_i$ . Ο χρήστης με τον παροχέα υπηρεσιών εκτελούν την ακόλουθη απόδειξη γνώσης

$$PK\{(\delta_1, \dots, \delta_{i-1}, \delta_{i+1}, \dots, \delta_l, \epsilon, \varsigma) : (\delta_1, \dots, \delta_{i-1}, d, \delta_{i+1}, \dots, \delta_l, \epsilon, \varsigma) = \text{rep}_{(g_1, \dots, g_l, g_{l+1}, P_i)} h_0^{-1}\}$$

Ο παροχέας υπηρεσιών  $S_i$  αποδέχεται αυτό το πρωτόκολλο αν και μόνο αν αποδεχτεί αυτή την απόδειξη και, εφόσον  $P_i \neq 1$ , αν το  $(P_i, \text{sign}(P_i))$  αποτελεί ένα έγκυρο ζευγάρι μήνυμα/υπογραφή. Τότε ο παροχέας υπηρεσιών αποθηκεύει το ζευγάρι τιμών  $(P_i, d_i)$  και το συσχετίζει είτε με ένα καινούργιο λογαριασμό είτε με ένα υπάρχον λογαριασμό του χρήστη. Το πρωτόκολλο αυτό αποδεικνύει ότι η Alice (χρήστης) είναι ο ιδιοκτήτης του ψευδωνύμου  $(P_i, \text{sign}(P_i))$  και αποδεικνύει ότι η αποκαλυφθείσα τιμή  $d_i$  είναι πράγματι η  $i$  τιμή που κωδικοποιείται στο  $P_i$ . Επιπλέον, ο παροχέας υπηρεσιών δεν μπορεί να μάθει καμία επιπλέον πληροφορία για τις ποσότητες  $(d_1^*, d_2^*, \dots, d_s^*, e^*)$  που κωδικοποιούνται στο  $P_i$ , παρά μόνο αυτό που θα μπορούσε να εξάγει από προηγούμενη γνώση και τέλος ότι  $d^* = d_i$ .

### 5.6.1 Προτάσεις που σχετίζονται με τη διαδικασία εγγραφής ενός ψευδωνύμου ενός χρήστη με κάποιον παροχέα υπηρεσιών

#### Πρόταση 1

Υπό την υπόθεση του διακριτού λογαρίθμου, και ότι το δημόσιο κλειδί  $P_i \neq 1$ , το υποπρωτόκολλο στο βήμα 2 είναι μια απόδειξη μηδενικής γνώσης ενός τέλειου, τίμιου επαληθευτή ότι για όλα τα  $j \in \{1, \dots, l\} \setminus \{i\}$ , η τιμή  $j$  που κωδικοποιείται στο  $P_i$  δεν ανήκει στην μαύρη λίστα  $L_j$ .

Θεωρούμε έναν παροχέα υπηρεσιών  $S_i$  και έναν τίμιο χρήστη  $U$ . Θεωρούμε οποιοδήποτε αριθμό αυθαίρετων εκτελέσεων του βήματος 2 για ένα ψευδώνυμο  $(P, \text{sign}(P))$  με  $P \neq 1$  και για τις ίδιες ή διαφορετικές λίστες  $L_j$  ( $j \in \{1, \dots, l\} \setminus \{i\}$ ).



Οποιαδήποτε πληροφορία μπορεί να υπολογίσει ο  $S_i$  για τα  $(d_1, d_2, \dots, d_s)$  που κωδικοποιούνται στο  $P$ , ο  $S_i$  μπορεί επίσης να την υπολογίσει χρησιμοποιώντας μόνο τις εκ των προτέρων πληροφορίες και τον τύπο που παρουσιάζεται ότι το  $d_j$  δεν ανήκει στην  $L_j$  ( $\forall j \in \{1, \dots, l\} \setminus \{i\}$ ).

## Πρόταση 2

Υπό την υπόθεση του διακριτού λογαρίθμου, για οποιαδήποτε καταχωρημένα ψευδώνυμα  $(P_i, \text{sign}(P_i))$  και για οποιαδήποτε τιμή  $d_i$  την οποία ο παροχέας υπηρεσιών  $S_i$  έχει δεχτεί ως έγκυρη<sup>6</sup>, με μεγάλη πιθανότητα ο χρήστης  $U$  είναι ο κάτοχος ενός έγκυρου ψευδώνυμου  $(P_i, \text{sign}(P_i))$  το οποίο δεν έχει ανακληθεί και για το οποίο το  $d_i$  είναι η τιμή  $i$  που κωδικοποιείται στο  $P_i$ . Επιπλέον, ο παροχέας υπηρεσιών  $S_i$  δεν μπορεί να ανακαλύψει άλλες πληροφορίες για τις τιμές που κωδικοποιούνται στο ψευδώνυμο  $P_i$  από αυτές που θα μπορούσε να συναγάγει από τις εκ των προτέρων πληροφορίες, παρά το γεγονός ότι το ψευδώνυμο  $(P_i, \text{sign}(P_i))$  δεν έχει ανακληθεί και ότι η τιμή  $d_i$  που αντιστοιχεί σε αυτό είναι η τιμή  $i$  που κωδικοποιείται στο ψευδώνυμο  $P_i$ .

## Πρόταση 3

Δεδομένων των μη κενών συνόλων  $D_1, \dots, D_s$  που είναι υποσύνολα του  $Z_q$ , για οποιαδήποτε ψευδώνυμα  $(P_i, \text{sign}(P_i))$  τέτοια ώστε το ψευδώνυμο  $P_i$  κωδικοποιεί ένα σύνολο τιμών χαρακτηριστικών  $(d_1, d_2, \dots, d_s) \in (D_1 \times D_2 \times \dots \times D_s)^7$ , και για οποιοδήποτε  $j \in \{1, 2, \dots, l\}$ , υπάρχουν ακριβώς  $\prod_{i=1}^{l-1} |D_i| (q-1)^{l-1} q^{2(l-1)} \neq 0$

σύνολα τυχαίων επιλογών που ένας τίμιος χρήστης θα μπορούσε να έχει κάνει κατά τη διάρκεια της εκτέλεσης του πρωτοκόλλου ανάκτησης ψευδωνύμου, έτσι ώστε να εξάγει το ζεύγος  $(P, \text{sign}(P))$  σαν το  $j$  ψευδώνυμο.

Από την παραπάνω πρόταση συμπεραίνουμε δηλαδή, ότι ένας παροχέας ταυτότητας IP δεν μπορεί να συνδέσει ένα ψευδώνυμο  $(P, \text{sign}(P))$  με το πρωτόκολλο ανάκτησής του, ακόμα κι αν γνώριζε το σύνολο  $(d_1, d_2, \dots, d_s)$  που κωδικοποιείται στο  $P$ .

<sup>6</sup> Υποθέτοντας ότι ο  $S_i$  δέχεται τη απόδειξη μαύρης λίστα του χρήστη  $U$

<sup>7</sup> Για οποιαδήποτε άποψη του παροχέα ταυτότητας IP σε μια εκτέλεση ενός πρωτοκόλλου ανάκτησης

Αυτά είναι ένα άμεσο αποτέλεσμα των προδιαγραφών του πρωτοκόλλου έκδοσης πιστοποιητικού . Δηλαδή, υπάρχουν ακριβώς  $\prod_{i=1}^5 |D_i|$  σύνολα  $(d_1, d_2, \dots, d_5, e)$

έτσι ώστε το  $p$  (και ως εκ τούτου το  $P$ ) να διαμορφωθεί σωστά .

Άρα , το νέο σύστημα προστατεύει την ιδιωτικότητα των χρηστών αφού ο παροχέας υπηρεσιών μόνο, επιβεβαιώνει την εγκυρότητα του χρήστη ενώ ταυτόχρονα το ίδιο το σύστημα προστατεύεται από ανέντιμους χρήστες <sup>8</sup> που θα μπορούσαν να εξαπατήσουν και διαταράξουν την αξιοπιστία και την ασφάλεια του συστήματος.

## 5.7 Πως ένας χρήστης αποκτά πρόσβαση σε μια υπηρεσία

Αφού ο χρήστης εγγράψει ένα ψευδώνυμο με τον παροχέα υπηρεσιών  $S_i$  , για να αποκτήσει πρόσβαση στην υπηρεσία  $S_i$  , ο χρήστης και ο παροχέας υπηρεσιών δεσμεύουν το ακόλουθο πρωτόκολλο για τις μαύρες λίστες  $\{ L_1, L_2, \dots, L_5 \}$  . Στο πρώτο βήμα , ο παροχέας υπηρεσιών  $S_i$  ελέγχει αν το  $d_i$  ανήκει στην δική του μαύρη λίστα  $L_i$  και στο βήμα 2, ο χρήστης αποδεικνύει ότι κάθε τιμή  $d_j$  ( $j \in \{1, 2, \dots, l\} \setminus \{i\}$ ) δεν ανήκει στη μαύρη λίστα  $L_j$ .

### ΒΗΜΑ 1<sup>ο</sup>

Ο παροχέας υπηρεσιών  $S_i$  επαληθεύει αν το  $d_i \in L_i$ . Αν πράγματι ανήκει στη μαύρη λίστα , διακόπτει το πρωτόκολλο και απορρίπτει το αίτημα του χρήστη. Αν όχι , προχωρά στο επόμενο βήμα

### ΒΗΜΑ 2<sup>ο</sup>

Αν όλες οι μαύρες λίστες  $L_j$  για  $j \in \{1, 2, \dots, i-1, i+1, \dots, l\}$  είναι κενές , τότε ο χρήστης πρέπει να αποδείξει στον  $S_i$  ότι γνωρίζει το κλειδί του ψευδωνύμου του . Αυτό μπορεί να γίνει χρησιμοποιώντας τη πρότυπη απόδειξη γνώσης μιας παράστασης , χωρίς να αποκαλύπτει κανένα χαρακτηριστικό ( το  $d_i$  έχει ήδη αποκαλυφθεί και αποδειχθεί ότι είναι σωστό ).

---

<sup>8</sup> Μέσω των αποδείξεων μηδενικής γνώσης ότι η τιμή  $d_i$  δεν ανήκει στη μαύρη λίστα κάποιου παροχέα

υπερσειών

---

Αν όμως δεν είναι όλες οι μαύρες λίστες κενές εκτελούνται τα ακόλουθα βήματα  $\forall i \in \{1, 2, \dots, i-1, i+1, \dots, l\}$  για το οποίο η  $L_j$  δεν είναι κενή:

(a) Χρήστης και παροχέας υπηρεσιών αναζητούν στην μαύρη λίστα

$$L_j = \{y_1, \dots, y_n\}.$$

Θέτουν  $m = \lceil \sqrt{n} \rceil$  για  $n = |L_j|$  και υπολογίζουν του συντελεστές  $a_{i,j} \in \mathbb{Z}_q$

( $i \in \{1, 2, \dots, N\}$ ,  $j \in \{0, 2, \dots, N\}$ ) των ακόλουθων πολυωνύμων στο  $\mathbb{Z}_q$ .

$$\begin{aligned} p_1(x) &= (x - y_1)(x - y_2) \dots (x - y_m) = a_{1,m}x^m + a_{1,m-1}x^{m-1} + \dots + a_{1,0} \\ p_2(x) &= (x - y_{m+1}) \dots (x - y_{2m}) = a_{2,m}x^m + a_{2,m-1}x^{m-1} + \dots + a_{2,0} \\ &\vdots \\ p_m(x) &= (x - y_{(m-1)m+1}) \dots (x - y_n) = a_{m,m}x^m + a_{m,m-1}x^{m-1} + \dots + a_{m,0} \end{aligned}$$

(b) Ο χρήστης επιλέγει τυχαία  $r_1, r_2, \dots, r_N \in_R \mathbb{Z}_q$  και παράγει τις τιμές  $C_k = \prod_{i=1}^n d_i^{r_i} b_i^k$

για όλα τα  $k \in \{1, 2, \dots, N\}$ . Επίσης, υπολογίζει  $v_k = e_k(d_j)$ ,

(c)  $w_k = a_{k,N}r_N + \dots + a_{k,2}r_2 + a_{k,1}r_1$  &  $C_{v_k} = \prod_{i=1}^n a_i^{v_k} b_i^{w_k}$  για  $k = 1, 2, \dots, N$ . Όλες

οι τιμές  $C_{v_k}, C_k$  στέλνονται στον παροχέα υπηρεσιών.

(d) Ο παροχέας υπηρεσιών λαμβάνει τις τιμές  $C_{v_k}, C_k$  και ελέγχει για  $k \in \{1, 2, \dots, N\}$  αν

$$C_{v_k} = (C_m)^{a_{k,m}} (C_{m-1})^{a_{k,m-1}} \dots (C_1)^{a_{k,1}} a_i^{a_{k,0}}$$

Αν αυτό αποτύχει, ο παροχέας υπηρεσιών διακόπτει και απορρίπτει το αίτημα του χρήστη.

(e) Έπειτα, εκτελείται η ακόλουθη απόδειξη γνώσης. Ο παροχέας υπηρεσιών αποδέχεται αν αποδεχτεί την ακόλουθη απόδειξη

$$PK\{(\delta_1, \dots, \delta_l, \epsilon, \varsigma, \rho_1, \dots, \rho_m, v_1, \dots, v_m, \omega_1, \dots, \omega_m) :$$

$$(\delta_1, \dots, \delta_j, \dots, \delta_l, \epsilon, \varsigma) = \text{rep}_{(g_1, \dots, g_{l+1}, P_i)} h_0^{-1} \wedge \quad (1)$$

$$(\delta_j, \rho_1) = \text{rep}_{(a_i, b_i)} C_1 \wedge \dots \wedge (\delta_j^m, \rho_m) = \text{rep}_{(a_i, b_i)} C_m \wedge \quad (2)$$

$$(v_1, \omega_1) = \text{rep}_{(a_i, b_i)} C_{v_1} \wedge v_1 \neq 0 \wedge \dots \wedge$$

$$(v_m, \omega_m) = \text{rep}_{(a_i, b_i)} C_{v_m} \wedge v_m \neq 0\} \quad (3)$$

Στο βήμα 2a , τα στοιχεία της λίστας  $L_j$  διαιρούνται σε υποσύνολα  $L_{j,k}$  μεγέθους  $N = |\mathcal{F}[L_j]|$ . Τα πολυώνυμα  $e_k(\cdot)$  για  $k = 1, 2, \dots, N$  κατασκευάζονται έτσι ώστε να περιέχουν μόνο στοιχεία των υποσυνόλων  $L_{j,k}$  ως ρίζες . Στο βήμα 2b κατασκευάζονται τα  $C_{v_k}, C_k$  .

Για κάθε  $k \in \{1, 2, \dots, N\}$  το  $C_k$  κρύβει μια δύναμη  $d_j^k$  του  $d_j$ , ενώ το  $C_{v_k}$  κρύβει την απεικόνιση  $e_k(d_j)$  , του  $d_j$ . Σημειώνουμε ότι

$$\begin{aligned} & (C_m)^{a_{k,m}} (C_{m-1})^{a_{k,m-1}} \dots (C_1)^{a_{k,1}} a_i^{a_{k,0}} \\ &= a_i^{a_{k,m} d_j^m + \dots + a_{k,1} d_j + a_{k,0}} b_i^{a_{k,m} r_m + \dots + a_{k,1} r_1} \\ &= C_{v_k}. \end{aligned}$$

Στο βήμα 2d , ο χρήστης αποδεικνύει ότι οι τιμές που κρύβονται στα  $C_1, C_2, \dots, C_k$  είναι διαδοχικές δυνάμεις της τιμής  $d_j$  (εξίσωση 2) , ότι η τιμή  $d_j$  είναι επίσης η  $j$  τιμή που κωδικοποιείται στο  $P_j$  (εξίσωση 1) , και ότι οι τιμές  $e_k(d_j)$  που κρύβονται στο  $C_{v_k}$  για  $k = 1, 2, \dots, N$  είναι διαφορετικές από το μηδέν (εξίσωση 3). Το τελευταίο αποδεικνύει ότι το  $d_j$  δεν είναι ρίζα κανενός πολυωνύμου  $e_k$  ( $k \in 1, 2, \dots, l$ ) και για αυτό δεν ανήκει στην μαύρη λίστα  $L_j$  .

## 5.8 Περιγραφή των βασικών συναλλαγών που πραγματοποιούνται στο νέο σύστημα πιστοποιητικού

### 5.8.1 Δημιουργία Ψευδωνύμου

Αυτό το πρωτόκολλο είναι μια συνεδρία μεταξύ ενός χρήστη  $U$  και ενός οργανισμού  $O$ . Ο χρήστης  $U$  επικοινωνεί με τον διαμεσολαβητή  $T$  για να εγκαταστήσει ένα ψευδώνυμο ανάμεσα σε αυτόν και τον οργανισμό. Ο χρήστης καθορίζει το όνομα σύνδεσης  $L_U$  με το οποίο ο διαμεσολαβητής τον γνωρίζει και το αντίστοιχο κλειδί επικύρωσης  $K_U$  . Εάν ο χρήστης δεν έχει λογαριασμό με τον διαμεσολαβητή , πρώτα εγκαθιστά έναν παρέχοντας ένα όνομα σύνδεσης  $L_U$  και αποκτώντας ένα  $K_U$  ως ανταπόδοση. Καθορίζει ένα πρόθεμα  $N_1$ .

Ο διαμεσολαβητής επιβεβαιώνει την εγκυρότητα των  $\{L_U, K_U\}$  και εάν το  $K_U$  είναι έγκυρο κλειδί που αντιστοιχεί στο  $L_U$  επικοινωνεί με τον οργανισμό  $O$  και του «λέει» ότι κάποιος χρήστης θέλει να εγκαταστήσει ένα ψευδώνυμο με αυτόν με πρόθεμα  $N_1$ . Ο οργανισμός  $O$  είτε αποδέχεται είτε απορρίπτει. Αν αυτό γίνει αποδεκτό, στέλνει ένα ψευδώνυμο με κατάληξη  $N_2$ , έτσι το ψευδώνυμο γίνεται  $N_{(U,O)} = N_1/N_2$ . Ο διαμεσολαβητής  $T$  προωθεί το απορρέον ψευδώνυμο  $N_{(U,O)}$  στον  $U$  σε περίπτωση αποδοχής, ή γνωστοποιεί τον χρήστη με απόρριψη.

### 5.8.2 Χορήγηση Πιστοποιητικού

Αυτό το πρωτόκολλο είναι μια συνεδρία ανάμεσα σε έναν χρήστη  $U$  και σε έναν οργανισμό  $O$ . Ο χρήστης  $U$  προσεγγίζει τον διαμεσολαβητή  $T$  και του υποβάλλει το όνομα σύνδεσης  $L_U$ , το κλειδί  $K_U$ , το ψευδώνυμο  $N$  και το όνομα του οργανισμού  $O$ . Αν το κλειδί δεν είναι έγκυρο για το συγκεκριμένο όνομα σύνδεσης  $L_U$  ή αν το ψευδώνυμο  $N$  δεν είναι το ψευδώνυμο του χρήστη με τον  $O$ , ο  $T$  απαντά με ένα μήνυμα αποτυχίας.

Αλλιώς, ο διαμεσολαβητής επικοινωνεί με τον οργανισμό. Αν ο οργανισμός αποδεχθεί, έπειτα ο διαμεσολαβητής γνωστοποιεί στον χρήστη ότι ένα πιστοποιητικό του έχει χορηγηθεί, αλλιώς απαντά με «Απόρριψη».

### 5.8.3 Επαλήθευση Πιστοποιητικού

Αυτό το πρωτόκολλο είναι μια συνεδρία μεταξύ ενός χρήστη  $U$  και ενός επαληθευτή  $V$ . Ένας χρήστης προσεγγίζει τον διαμεσολαβητή  $T$  και του δίνει το όνομα σύνδεσης  $L_U$ , το κλειδί  $K_U$ , το όνομα του επαληθευτή  $V$ , ένα ψευδώνυμο  $N$  και ένα όνομα οργανισμού χορήγησης πιστοποιητικών. Αν το κλειδί  $K_U$  είναι έγκυρο για το συνθηματικό  $L_U$  και αν  $N$  είναι ένα ψευδώνυμο με τον οργανισμό  $O$  και αν ένα πιστοποιητικό έχει χορηγηθεί από τον οργανισμό  $O$  στο ψευδώνυμο  $N$ , έπειτα ο διαμεσολαβητής γνωστοποιεί στον επαληθευτή ότι ο χρήστης που μιλούσε στην τρέχουσα συνεδρία  $S_{id}$  έχει ένα πιστοποιητικό από τον οργανισμό. Αλλιώς απαντά με ένα μήνυμα αποτυχίας.

#### 5.8.4 Επαλήθευση ενός πιστοποιητικού ως προς ένα ψευδώνυμο

Αυτό το πρωτόκολλο είναι μια συνεδρία μεταξύ χρήστη  $U$  και επαληθευτή  $V$ . Ο χρήστης  $U$  προσεγγίζει τον διαμεσολαβητή  $T$  και του δίνει το όνομα σύνδεσης  $L_U$ , το κλειδί  $K_U$ , ένα όνομα επαληθευτή, τα ψευδώνυμα  $N_V$  και  $N_O$  και ένα όνομα για τον οργανισμό χορήγησης πιστοποιητικού. Αν το  $K_U$  είναι έγκυρο κλειδί για το  $L_U$  και αν το  $N_V$  είναι το ψευδώνυμο του χρήστη με τον επαληθευτή  $V$  ενώ  $N_O$  το ψευδώνυμο του χρήστη με τον  $O$  και αν ένα πιστοποιητικό έχει χορηγηθεί από τον οργανισμό, τότε ο διαμεσολαβητής γνωστοποιεί ότι ο χρήστης έχει πιστοποιητικό από τον οργανισμό  $O$ .

#### 5.8.5 Ιδανική επικοινωνία

Όλη η επικοινωνία δρομολογείται μέσω του διαμεσολαβητή  $T$ . Εάν ο αποστολέας επιθυμεί να είναι ανώνυμος ζητά από τον διαμεσολαβητή να μην αποκαλυφθεί η ταυτότητα του στον παραλήπτη. Επίσης ο αποστολέας μπορεί να ζητήσει από τον διαμεσολαβητή να εγκαταστήσει μια συνεδρία ανάμεσα σε αυτόν και τον παραλήπτη. Σε αυτή τη συνεδρία αντιστοιχεί ένας κωδικός συνεδρίας  $S_{id}$ .

Για παράδειγμα, έστω ένας χρήστης  $U$  που θέλει να πάρει ένα πιστοποιητικό από έναν οργανισμό  $O$ . Ο οργανισμός  $O$  ζητά την κατοχή πιστοποιητικών από δύο άλλους οργανισμούς  $O_1$  και  $O_2$  για να χορηγήσει πιστοποιητικό στο συγκεκριμένο χρήστη. Υποθέτουμε ότι ο χρήστης κατέχει αυτά τα πιστοποιητικά. Έπειτα, ο χρήστης  $U$  μπορεί να πάρει πιστοποιητικό από τον  $O$  ως εξής.

Αρχικά, εγκαθιστά ένα ψευδώνυμο με τον οργανισμό  $O$  εκτελώντας  $\text{FormNym}(U, O)$ . Στη συνέχεια, επιδεικνύει στον οργανισμό τα πιστοποιητικά του από τον  $O_1$  και τον  $O_2$  εκτελώντας τα πρωτόκολλα  $\text{VerifyCredOnNym}(O, N_O, N_{O1}, O_1)$  και  $\text{VerifyCredOnNym}(O, N_O, N_{O2}, O_2)$ . Έτσι ο οργανισμός γνωρίζει ότι ο χρήστης κατέχει πιστοποιητικά από τους  $O_1$  και  $O_2$  και χορηγεί στον χρήστη  $U$  ένα πιστοποιητικό, δηλ., ο χρήστης  $U$  μπορεί να εκτελέσει  $\text{GrantCred}(N_O)$ .



## 5.9 Το βασικό σύστημα ανώνυμου πιστοποιητικού και οι παράμετροί του

Κάθε οργανισμός  $O$  κατέχει το δικό του δημόσιο κλειδί  $PK_O$  ως προς ένα RSA modulus  $n_O$  και πέντε στοιχεία του  $QR_n : \{a_O, b_O, d_O, g_O, h_O\}$ . Ο χρήστης  $U$  θα έχει το δικό του κύριο μυστικό κλειδί  $x_U$ . Στο ψευδώνυμο  $N_{(U,O)}$  του χρήστη με τον οργανισμό  $O$  διαμορφώνεται μια ετικέτα εγκυρότητας  $P_{(U,O)} = a_O^{s_U} b_O^{c_{(U,O)}}$  όπου η τιμή  $s_{(U,O)}$  είναι τυχαίο αλφαριθμητικό που το γνωρίζει μόνο ο χρήστης αλλά στην τυχειότητα του συνεισφέρει και ο οργανισμός.

Η κατάλληλη επιλογή των παραμέτρων που αφορούν στο μήκος του κύριου κλειδιού  $x_U$  και της τιμής  $s_{(U,O)}$  εξασφαλίζει ότι η ετικέτα που προκύπτει είναι στατιστικώς ανεξάρτητη από το κύριο κλειδί του χρήστη και από οποιαδήποτε άλλη ετικέτα που διαμορφώνει ο ίδιος χρήστης με άλλους οργανισμούς.

Το πιστοποιητικό που εκδίδεται από έναν οργανισμό  $O$  σε ένα ψευδώνυμο  $N_{(U,O)}$  είναι ένα ζεύγος αριθμών  $(e_{(U,O)}, c_{(U,O)})$ , όπου  $e_{(U,O)}$  είναι ένας επαρκώς μεγάλος πρώτος αριθμός που ικανοποιεί τη σχέση  $c_{(U,O)}^{e_{(U,O)}} \equiv P_{(U,O)} \pmod{n_O}$ . Συμφωνά με το πρωτόκολλο RSA το ζεύγος  $(e_{(U,O)}, c_{(U,O)})$  δεν μπορεί να πλαστογραφηθεί αν οι ετικέτες έχουν διαμορφωθεί σωστά ακόμα και μετά από μια προσαρμοστική επίθεση.

Το σύστημα για να προστατεύσει τους χρήστες, τους παρέχει τη δυνατότητα απόδειξης ότι είναι οι πραγματικοί κάτοχοι ενός πιστοποιητικού μέσω μιας απόδειξης μηδενικής γνώσης. Για να πετύχουν κάτι τέτοιο, αποδεικνύουν ότι η ετικέτα και το πιστοποιητικό που αντιστοιχεί σε αυτή, έχουν διαμορφωθεί σωστά.

Ο χρήστης δημοσιεύει δεσμεύσεις και στην ετικέτα επικύρωσης και στο πιστοποιητικό, και αποδεικνύει σχέσεις μεταξύ αυτών. Επίσης περιλαμβάνει μια απόδειξη ότι το ίδιο κύριο μυστικό κλειδί χρησιμοποιείται και στην ετικέτα επικύρωσης του ψευδώνυμου που διαμορφώνεται με τον εκδίδοντα οργανισμό του πιστοποιητικού καθώς και στην ετικέτα επικύρωσης με τον οργανισμό επαλήθευσης.

### 5.9.1 Δημιουργία δημόσιου και μυστικού κλειδιού από την πλευρά των οργανισμών

Το μήκος όλων των RSA moduli είναι  $l_n$ , τα ακέραια διαστήματα είναι

$$\Gamma = [-2^{S_T}, 2^{S_T}] \quad \Delta = [-2^{S_A}, 2^{S_A}] \quad \Lambda = [-2^{S_L}, 2^{S_L + S_Z}] \text{ έτσι ώστε}$$

$l_A = \epsilon (l_{fl} + l_n) + 1$ , όπου το  $\epsilon > 1$  είναι παράμετρος ασφαλείας και  $l_{fl} > l_X + l_A + 4$ .

Κάθε οργανισμός  $O_i$  επιλέγει τυχαίους πρώτους αριθμούς  $e'_{O_i}, q'_{O_i}$  μήκους  $\frac{l_n}{2}$

τέτοιους ώστε  $e_0 = e'_{O_i} + 1$  και  $q_0 = q'_{O_i} + 1$  να είναι πρώτοι και θέτει modulus

$n_{O_i} = e_{O_i} q_{O_i}$ . Επίσης επιλέγει τυχαία στοιχεία  $\{a_{O_i}, b_{O_i}, d_{O_i}, g_{O_i}, h_{O_i}\} \in QR_n$ .

Επίσης αποθηκεύει σαν μυστικό κλειδί  $SK_{O_i} := (e_{O_i}, n_{O_i})$  και δημοσιεύει

$PK := (n_{O_i}, a_{O_i}, b_{O_i}, d_{O_i}, g_{O_i}, h_{O_i})$  σαν δημόσιο κλειδί.

Στο μοντέλο δημόσιου κλειδιού υποθέτουμε ότι υπάρχει μια οντότητα που επαληθεύει, μέσω αποδείξεων μηδενικής γνώσης, με τον οργανισμό  $O_i$  ότι το  $n_{O_i}$  είναι γινόμενο ασφαλών πρώτων αριθμών και ότι τα στοιχεία  $a_{O_i}, b_{O_i}, d_{O_i}, g_{O_i}, h_{O_i}$  ανήκουν πράγματι στο  $QR_n$ .

Η παράμετρος  $l_{fl}$  επιλέγεται έτσι ώστε να είναι δύσκολος ο υπολογισμός του διακριτού λογάριθμου στο  $QR_n$  με  $l_{fl}$  δυαδικών ψηφίων εκθετικοποιήσεις.

### 5.9.2 Δημιουργία Ψευδωνύμου

Ένας χρήστης  $U$  δημιουργεί ψευδώνυμο  $N_{(U,O)}$  σε μια ετικέτα εγκυρότητας  $P_{(U,O)}$  με τον οργανισμό  $O$ . Με  $x_U \in \Gamma$  συμβολίζω το κύριο κλειδί του χρήστη. Το πρωτόκολλο δημιουργίας ψευδωνύμου εξασφαλίζει ότι η ετικέτα επικύρωσης που αντιστοιχεί στο συγκεκριμένο ψευδώνυμο έχει διαμορφωθεί σωστά, δηλαδή  $P_{(U,O)} = a_0^{s_U} b_0^{c(U,O)}$  όπου  $x_U \in \Gamma$  και  $s_{(U,O)} \in \Delta$ .

Η τιμή  $s_{(U,O)}$  επιλέγεται από κοινού από τον οργανισμό  $O$  και τον χρήστη  $U$  χωρίς ο οργανισμός να γνωρίζει τίποτε είτε για το  $x_U$  είτε για την τιμή  $s_{(U,O)}$ . Στο πρωτόκολλο αυτό ο χρήστης δεν είναι υποχρεωμένος να χρησιμοποιήσει το ίδιο κύριο κλειδί μυστικό  $x_U$ .

## Πρωτόκολλο 1

**1.1** Ο χρήστης  $U$  επιλέγει  $N_1 \in \{0,1\}^k$ , και  $r_1 \in_R \Delta$  και  $r_2, r_3 \in_R \{0,1\}^{2s_n}$  και θέτει

$$C_1 := g_0^{r_1} b_0^{r_2}, C_2 := g_0^{s_u} b_0^{r_3} \text{ και τα στέλνει στον οργανισμό } O.$$

**1.2** Για να αποδείξει ο χρήστης ότι οι ποσότητες  $C_1, C_2$  διαμορφώθηκαν σωστά εκτελεί μια απόδειξη γνώσης

$$PK \{ (\alpha, \beta, \gamma, \delta) : C_1^2 = (g_0^2)^\alpha (h_0^2)^\beta \wedge C_2^2 = (g_0^2)^\gamma (h_0^2)^\delta \}$$

**1.3** Ο οργανισμός  $O$  επιλέγει  $r \in_R \Delta$  και μια τιμή  $N_2$  και τα στέλνει στον χρήστη  $U$

**1.4** Ο χρήστης θέτει ως ψευδώνυμο του  $N_{(U,O)} = N_1 // N_2$ . Υπολογίζει

$s_{(U,O)} = (r_1 + r \text{ Nod}(2^{s_A+1})) - (2^{s_A} + 1)$  (η τιμή  $s_{(U,O)}$  είναι το άθροισμα των  $r_1$   $r$  κατάλληλα προσαρμοσμένο ώστε να πέφτει στο διάστημα  $\Delta$ ). Έπειτα, θέτει ως ετικέτα εγκυρότητας  $P_{(U,O)} = a_0^{s_u} b_0^{c_{(U,O)}}$  και την στέλνει στον οργανισμό.

**1.5** Τώρα, ο χρήστης πρέπει να δείξει ότι η ετικέτα  $P_{(U,O)}$  διαμορφώθηκε σωστά. Για αυτό το σκοπό υπολογίζει  $\tilde{s} = \frac{r_1 + r}{2^{l_A+1}-1}$ , επιλέγει  $r_4 \in_R \{0,1\}^{s_n}$ , θέτει

$C_3 := g_0^{c_1} b_0^{r_4}$  και στέλνει το  $C_3$  στον οργανισμό  $O$ . Επιπλέον, ο χρήστης αποδεικνύει στον οργανισμό  $O$  ότι το προηγούμενο βήμα εκτελέστηκε σωστά εκτελώντας την ακόλουθη απόδειξη γνώσης

$PK \{ (\alpha, \beta, \gamma, \delta, \varepsilon, \zeta, \theta, \xi) :$

$$C_1^2 = (g_0^2)^\alpha (h_0^2)^\beta \wedge C_2^2 = (g_0^2)^\gamma (h_0^2)^\delta \wedge C_3^2 = (g_0^2)^\varepsilon (h_0^2)^\xi$$

$$\wedge \frac{C_1^2 (g_0^2)^{(r-2^{l_A}+1)}}{(C_3^2)^{(2^{l_A}-1)}} = (g_0^2)^8 (h_0^2)^\varepsilon \wedge P_{(U,O)}^2 = (g_0^2)^\gamma (h_0^2)^8 \wedge \gamma \in \Gamma \wedge$$

$$\theta \in \Delta \}$$

**1.6** Ο οργανισμός  $O$  αποθηκεύει  $P_{(U,O)}^2, P_{(U,O)}, N_{(U,O)}$

**1.7** Ο χρήστης αποθηκεύει  $P_{(U,O)}^2, P_{(U,O)}, N_{(U,O)}$  και  $s_{(U,O)}$ .

### 5.9.3 Δημιουργία Πιστοποιητικού

Ένα πιστοποιητικό  $(P_{(U,O)}, N_{(U,O)})$  που εκδίδεται από έναν οργανισμό  $O$  είναι ένα ζεύγος  $(c, e) \in \mathbb{Z}_{n_O}^* \times \Lambda$  τέτοια που  $P_{(U,O)} d_O = c^e$ . Για τη δημιουργία πιστοποιητικού σε ένα προηγούμενα εγκατεστημένο ψευδώνυμο  $N_{(U,O)}$  με ετικέτα εγκυρότητας  $P_{(U,O)}$ , ο οργανισμός  $O$  και ο χρήστης  $U$  διεξάγουν το ακόλουθο πρωτόκολλο.

#### Πρωτόκολλο 2

**2.1** Ο χρήστης  $U$  στέλνει το ζεύγος  $(P_{(U,O)}, N_{(U,O)})$  στον οργανισμό  $O$  και πιστοποιεί ότι είναι ο κάτοχος του συγκεκριμένου ψευδωνύμου με ετικέτα  $P_{(U,O)}$  εκτελώντας μια απόδειξη γνώσης  $PK(\alpha, \beta, \gamma, \delta) : C_1^2 = (g_O^2)^{\alpha} (h_O^2)^{\beta} \wedge C_2^2 = (g_O^2)^{\gamma} (h_O^2)^{\delta}$

**2.2** Ο οργανισμός  $O$  βεβαιώνεται ότι το  $(N_{(U,O)}, P_{(U,O)})$  υπάρχει στη βάση

δεδομένων του, επιλέγει έναν τυχαίο πρώτο αριθμό  $e_{(U,O)} \in_R \Lambda$ , υπολογίζει

$c_{(U,O)} = (P_{(U,O)} d_O)^{1/e_{(U,O)}} \bmod n_O$ , στέλνει  $c_{(U,O)}$  και  $e_{(U,O)}$  στον χρήστη  $U$  και

αποθηκεύει  $(c_{(U,O)}, e_{(U,O)})$  στο συγκεκριμένο ψευδώνυμο  $N_{(U,O)}$ .

**2.3** Ο χρήστης  $U$  ελέγχει αν  $c_{(U,O)}^{e_{(U,O)}} \equiv P_{(U,O)} d_O$  και αποθηκεύει  $(c_{(U,O)}, e_{(U,O)})$

στην συγκεκριμένη καταγραφή πιστοποιητικού με τον οργανισμό  $O$ .

Το  $(P_{(U,O)}, c_{(U,O)}, e_{(U,O)})$  ονομάζεται καταγραφή πιστοποιητικού.

Το βήμα 2.1 θα μπορούσε να παραληφθεί αν στην ίδια συνεδρία εκτελεστεί το πρωτόκολλο δημιουργίας ψευδωνύμου.

### 5.9.4 Παρουσίαση ενός πιστοποιητικού

Ο χρήστης  $U$  κατά την παρουσίαση ενός πιστοποιητικού στον επαληθευτή έχει ως σκοπό να αποδείξει ότι είναι ο ιδιοκτήτης ενός πιστοποιητικού που εκδόθηκε από τον οργανισμό  $O$ , δηλαδή να αποδείξει ότι είναι κάτοχος των τιμών

$(P_{(U,O)} = a_O^{su} b_O^{c_{(U,O)}}, c_{(U,O)}, e_{(U,O)})$ . Συνεπώς ο χρήστης με τον επαληθευτή εκτελούν το ακόλουθο πρωτόκολλο.

### Πρωτόκολλο 3

**3.1** Ο χρήστης  $U$  επιλέγει  $r_1, r_2 \in_R \{0,1\}^{25n}$ , υπολογίζει  $A = c_{(U,O)} h^{r_1}_O$  και  $B = h^{r_1}_O g^{r_2}_O$  και στέλνει τα  $A, B$  στον επαληθευτή.

**3.2** Ο χρήστης  $U$  και ο επαληθευτής  $V$  εκτελούν το ακόλουθο πρωτόκολλο

$$\text{PK} \{(\alpha, \beta, \gamma, \delta, \varepsilon, \zeta, \xi) : d_O^2 = (A^2)^{\alpha} (\frac{1}{a_O^2})^{\beta} (\frac{1}{b_O^2})^{\gamma} (\frac{1}{h_O^2})^{\delta} \wedge B^2 = (h_O)^{\varepsilon} (g_O)^{\xi} \\ \wedge 1 = (B^2)^{\alpha} (\frac{1}{h_O^2})^{\delta} (\frac{1}{g_O^2})^{\xi} \wedge \beta \in \Gamma \wedge \gamma \in \Delta \wedge \alpha \in \Lambda\}$$

Έτσι ο χρήστης αποδεικνύει ότι αυτός είναι ο κάτοχος ενός πιστοποιητικού που εκδόθηκε από τον οργανισμό  $O$  σε κάποιο ψευδώνυμο που έχει καταγραφεί με αυτόν.

### 5.9.5 Παρουσίαση ενός πιστοποιητικού ως προς ένα ψευδώνυμο

Ο χρήστης  $U$  πρέπει να αποδείξει στον οργανισμό  $O_i$  με τον οποίο έχει δημιουργήσει ένα ψευδώνυμο  $(P_{(U,O_i)}, N_{(U,O_i)})$  ότι κατέχει ένα πιστοποιητικό  $(P_{(U,O_j)} = a^{su} b^{c_{(U,O_j)}}, c_{(U,O_j)}, e_{(U,O_j)})$ .

Που σημαίνει ότι ο οργανισμός  $O_i$  όχι μόνο θέλει να βεβαιωθεί ότι ο χρήστης κατέχει ένα πιστοποιητικό από έναν άλλο οργανισμό  $O_j$  αλλά και ότι το ψευδώνυμο που αντιστοιχεί στο συγκεκριμένο πιστοποιητικό βασίζεται στο ίδιο κύριο κλειδί όπως η ετικέτα  $P_{(U,O_i)}$ .

### Πρωτόκολλο 4

**4.1** Ο χρήστης  $U$  επιλέγει τυχαία  $r_1, r_2, r_3 \in_R \{0,1\}^{25n}$ , υπολογίζει  $A = c_{(U,O_j)} h^{r_1}_j$  και  $B = h^{r_1}_{O_j} g^{r_2}_{O_j}$  και στέλνει το ψευδώνυμο  $N_{(U,O_j)}$  καθώς και τα  $A, B$  στον  $O_i$ .

**4.2** Ο χρήστης  $U$  δεσμεύεται με τον οργανισμό  $O_i$  στην ακόλουθη απόδειξη γνώσης

$$\text{PK} \{(\alpha, \beta, \gamma, \delta, \varepsilon, \zeta, \xi, \eta) : d_{O_j}^2 = (A^2)^{\alpha} (\frac{1}{a_{O_j}^2})^{\beta} (\frac{1}{b_{O_j}^2})^{\gamma} (\frac{1}{h_{O_j}^2})^{\delta} \wedge B^2 = (h_{O_j})^{\varepsilon} (g_{O_j})^{\xi} \\ \wedge 1 = (B^2)^{\alpha} (\frac{1}{h_{O_j}^2})^{\delta} (\frac{1}{g_{O_j}^2})^{\xi} \wedge P^2_{(U,O_j)} = (a^2)^{\beta} (b^2)^{\gamma}$$

$$\beta \in \Gamma \wedge \gamma \in \Delta \wedge \alpha \in \Lambda \})$$

## 5.10. Η έννοια της μη μεταφερσιμότητας στο σύστημα ανώνυμου πιστοποιητικού

Πριν προχωρήσω στην ανάλυση της μη μεταφερσιμότητας θα περιγράψω δύο σημαντικές κρυπτογραφικές αρχές, την κυκλική κρυπτογράφηση και την επαληθεύσιμη κρυπτογράφηση που έχουν άμεση σχέση με την μη μεταφερσιμότητα.

### 5.10.1 Κυκλική κρυπτογράφηση

Ο ορισμός που ακολουθεί διατυπώνει τις συνθήκες κάτω από τις οποίες ένα σημειολογικά ασφαλές σχέδιο κρυπτογράφησης είναι κυκλικά ασφαλές.

#### Ορισμός

Έστω  $n, m \in \text{poly}(k)$ . Ένα σημειολογικά ασφαλές<sup>9</sup> σχέδιο κρυπτογράφησης

$\mathcal{G} = (\mathcal{E}, \mathcal{D})$  είναι ασφαλές αν

1. Υπάρχει μήνυμα το οποίο σημειώνεται ως  $\theta$ , τέτοιο ώστε για όλα τα  $E \in \mathcal{E}(1^k)$ , το  $\theta$  να βρίσκεται στο χώρο μηνυμάτων του  $E$ .
2. Για όλα τα  $E_1 \in \mathcal{E}(1^k)$ ,  $D_2 \in \mathcal{D}(1^k)$ , ο χώρος μηνυμάτων του  $E_1$  περιλαμβάνει το  $D_2$ .
3. Για έναν  $n$  κόμβων κατευθυνόμενο γράφο  $G$  με  $m$  ακμές, δεδομένων  $n$  τυχαία επιλεγμένων δημόσιων κλειδιών  $\{E_i\}_{i=1}^n$ , έχουμε  $\{E_i(D_j)\}_{(i,j) \in E(G)} \approx \{E_i(\theta)\}_{(i,j) \in E(G)}$ .

Κάποιος που μπορεί να έχει πρόσβαση σε κρυπτογραφήσεις των μυστικών κλειδιών δεν βοηθά τον ανταγωνιστή στο σπάσιμο της ασφάλειας του συστήματος.

Παράλληλα, αν είχαμε περιορίσει την προσοχή μας σε άκυκλους γράφους οποιοδήποτε σημασιολογικά ασφαλές σχέδιο κρυπτογράφησης θα ήταν αρκετό για τον ορισμό. Καθώς ο ορισμός είναι πιο ισχυρός αν συμπεριλάβουμε γράφους με κύκλους, καλούμε την έννοια αυτή *κυκλική κρυπτογράφηση*.

<sup>9</sup> Ένα σχήμα κρυπτογράφησης δημόσιου κλειδιού ονομάζεται σημειολογικά ασφαλές όταν είναι αδύνατον για έναν παθητικό εχθρό (passive adversary) που υποκλέπτει ένα κρυπτογράφημα να εξαγάγει οποιαδήποτε πληροφορία σχετικά με το κείμενο που περιέχεται στο κρυπτογράφημα.

Έστω ένα κρυπτογραφικό σύστημα που ικανοποιεί τον ορισμό του **random oracle** μοντέλου<sup>10</sup>. Υποθέτουμε ότι το μήκος του μυστικού κλειδιού είναι  $p(k)$ . Έστω ένα τυχαίο oracle model  $H: \{0,1\}^* \rightarrow \{0,1\}^{p(k)}$  και με  $\oplus$  συμβολίζουμε την πράξη xor. Έστω  $\mathcal{G} = (\mathcal{E}, \mathcal{D})$  ένα σημειολογικά ασφαλές σύστημα κρυπτογράφησης με έναν αποδοτικά μεγάλο χώρο μηνυμάτων. Κατασκευάζουμε  $\mathcal{G}^u = \{\mathcal{E}^u, \mathcal{D}^u\}$  ως εξής. Δημιουργούμε  $(E, D)$  ως προς  $\mathcal{G}$ . Για να κρυπτογραφήσουμε  $\kappa$  μήνυμα  $m \in \{0,1\}^{p(k)}$  το  $\mathcal{E}^u$  επιλέγει τυχαίο  $r \in_R \{0,1\}^s$  και θέτει  $\mathcal{E}^u(N) := (E(r), H(r) \oplus N)$ . Για να αποκρυπτογραφήσει ένα ζεύγος  $(a, b)$ , το  $\mathcal{D}^u$  υπολογίζει  $\tilde{N} := H(D(a)) \oplus b$ .

Για αυτή τη δομή ισχύει ότι αν το  $\mathcal{G}$  είναι σημειολογικά ασφαλές, το  $\mathcal{G}^u$  είναι κυκλικά ασφαλές.

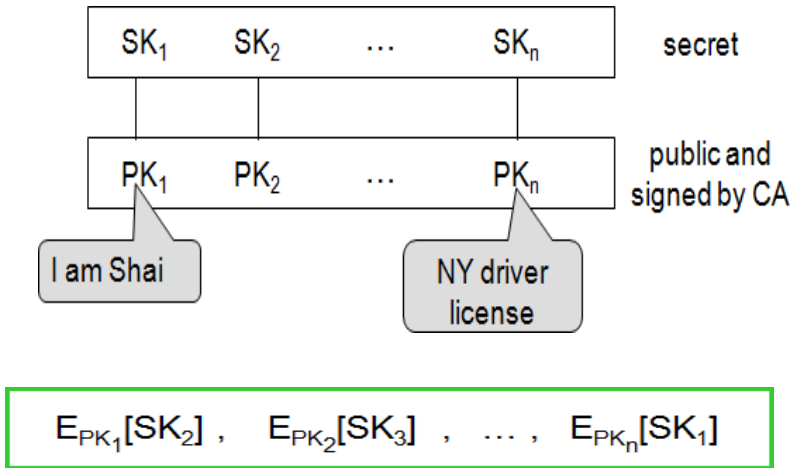
Σαν βάση του σχεδίου κυκλικής κρυπτογράφησης χρησιμοποιούμε το σχέδιο El Gamal για κάποια ομάδα  $G = \langle g \rangle$ . Βάσει του πρωτοκόλλου Diffie Hellman αποδεικνύεται ότι το κρυπτογραφικό σύστημα του El Gamal είναι κυκλικά ασφαλές.

Ας υποθέσουμε ότι  $P = g^s$  είναι το δημόσιο κλειδί. Το προκύπτον σχέδιο κυκλικής κρυπτογράφησης είναι το ακόλουθο. Για να κρυπτογραφήσουμε το μήνυμα  $m \in \{0,1\}^k$ , επιλέγουμε τυχαίο  $r_1 \in G$  και τυχαίο  $r_2 \in \{0,1\}^{2s}$  και υπολογίζουμε  $\kappa$  κρυπτογράφηση  $(u, v, z) := (P^{r_2} r_1, g^{r_2}, H(r_1) \oplus m)$ . Η αποκρυπτογράφηση θα λειτουργήσει υπολογίζοντας  $H(u/v^z) \oplus z$ . Αυτό σημειώνεται ως *κρυπτογράφηση CEIG*.

Αν ο χρήστης έχει  $n$  πιστοποιητικά υπογεγραμμένα από την Αρχή Πιστοποίησης CA, κρυπτογραφεί τα μυστικά κλειδιά του  $SK_i$ ,  $i = 1, 2, \dots, n$  χρησιμοποιώντας τα αντίστοιχα δημόσια κλειδιά  $PK_i$ ,

<sup>10</sup> Το μοντέλο *random oracle* είναι ένα τυπικό μοντέλο απόδειξης ασφάλειας στο οποίο οι συναρτήσεις κατακερματισμού (hash functions) αντιμετωπίζονται ως συναρτήσεις τυχαιότητας





Σχήμα 16. Κρυπτογράφηση μυστικού κλειδιού με το δημόσιο κλειδί

### 5.10.2 Επαληθεύσιμη κρυπτογράφηση ως προς δεσμευμένο δημόσιο κλειδί

Η επαληθεύσιμη κρυπτογράφηση αποτελεί ένα πρωτόκολλο μεταξύ ενός **αποδεικνύων** και ενός **επαληθευτή**. Με είσοδο το δημόσιο κλειδί  $E$  και την τιμή  $v$ , ο επαληθευτής λαμβάνει μια κρυπτογράφηση  $e$  κάποιας τιμής  $s$  κάτω από το κλειδί  $E$ .

Έστω  $(E, D)$  ένα σημειολογικά ασφαλές σχέδιο κρυπτογράφησης. Ένα πρωτόκολλο μεταξύ ενός αποδεικνύων  $P(R, E, s, v)$  και ενός επαληθευτή  $V(R, E, v)$  είναι ένα επαληθεύσιμο πρωτόκολλο κρυπτογράφησης ως προς το δημόσιο κλειδί  $E$  για μια πολυωνυμικού χρόνου σχέση  $R$  αν ισχύουν τα ακόλουθα σημεία.

1. Για όλα τα  $(E, D) \in \mathcal{G}(1^k)$  και για όλα τα  $(s, v) \in R$ , και αν  $P, V$  έντιμοι τότε

$$V_{(P(R, E, s, v))} \neq \perp$$

2. Υπάρχει ένας αποδοτικός αλγόριθμος  $C$  τέτοιος που για όλα τα επαρκώς μεγάλα  $k$  και  $\forall (E, D) \in \mathcal{G}(1^k)$

$$\Pr [(C(D, e), v) \in R \mid e = V_{(P(R, E, s, v))} \neq \perp \wedge e \neq \perp] = 1 - \text{neg}(k)$$

3. Υπάρχει ένα μαύρο κουτί προσομοιωτή  $S$  τέτοιο ώστε  $\forall \tilde{V}, \forall (s, v) \in R$  έχουμε ότι

$$S^{\tilde{V}(R, E, v)}(R, E, v) \stackrel{c}{\approx} \tilde{V}_{P(R, E, s, v)}(R, E, v).$$

Η ποσότητα  $e$  δεν είναι ένα απλό μήνυμα από τον αποδεικνύων αλλά ολόκληρο το αντίγραφο του πρωτοκόλλου του επαληθευτή. Επίσης, ο αλγόριθμος  $C$  δεν εξάγει απαραίτητα το ίδιο  $s$  που δόθηκε σαν είσοδο στον αποδεικνύων. Θα μπορούσε να εξάγει ένα  $s^u \neq s$ , αλλά μόνο αν  $(s^u, v) \in R$ .

### 5.10.2.1 Πως μπορούμε να υλοποιήσουμε μια επαληθεύσιμη κρυπτογράφηση

Ένας (μη αποδοτικός) τρόπος υλοποίησης της επαληθεύσιμης κρυπτογράφησης θα ήταν ο αποδεικνύων να κρυπτογραφήσει το  $s$  χρησιμοποιώντας το δημόσιο κλειδί  $E$  και να εκτελέσει μια απόδειξη μηδενικής-γνώσης ότι η κρυπτογραφημένη τιμή ικανοποιεί τη σχέση  $R$  όσον αφορά το  $v$ . Στην πράξη όμως κάτι τέτοιο δεν είναι επιθυμητό.

Από την άλλη, οι Camenisch & Damgard ( γενίκευση πρωτόκολλου Asokan) προτείνουν ένα πρακτικό, επαληθεύσιμο σχέδιο κρυπτογράφησης για όλες τις σχέσεις  $R$  που εμπλέκουν μια απόδειξη μηδενικής γνώσης, τριών βημάτων ενός έντιμου αποδεικνύων, όπου το δεύτερο μήνυμα είναι μια τυχαία πρόκληση και ο «μάρτυρας» μπορεί να υπολογιστεί από δύο αντίγραφα με το ίδιο πρώτο μήνυμα αλλά με διαφορετικές προκλήσεις.

Ένα επαληθεύσιμο πρωτόκολλο για το σχέδιο κυκλικής κρυπτογράφησης El Gamal, μέσω του οποίου ο  $\log_b a$  κρυπτογραφείται στο  $e$  υπό το δημόσιο κλειδί  $(y, g)$  σημειώνεται ως  $e := VE(ElGamal, (g, \ell)) \{ (\ell) : a = (\ell) : a = b^\ell \}$ . Αν ο επαληθευτής δεν γνωρίζει το δημόσιο κλειδί με το οποίο έγινε η κρυπτογράφηση, δεν λειτουργούν οι προηγούμενες δομές, διότι ο επαληθευτής πρέπει να μπορεί να ελέγξει αν ένα συγκεκριμένο κρυπτογράφημα είναι κρυπτογράφηση μιας δεδομένης τιμής.

Για αυτό το λόγο προτείνουμε μια νέα δομή που βασίζεται σε μια παραλλαγή του κυκλικά ασφαλούς σχεδίου κρυπτογράφησης του El Gamal. Έστω ότι ο αποδεικνύων γνωρίζει το μυστικό κλειδί της κρυπτογράφησης. Αν  $P = g^s$  το δημόσιο κλειδί, και  $x$  το αντίστοιχο μυστικό κλειδί. Έστω  $C := Ph^r$  μια δέσμευση για το δημόσιο  $κλειδί$ , όπου το  $h$  είναι μια ακόμα γεννήτρια του  $G = \langle g \rangle$  και έστω  $(u, v, z) := (P^{r_2} r_1, g^{r_2}, H(r_1) \oplus N)$  μια κρυπτογράφηση του  $N$ .

Για να πείσει τον επαληθευτή ότι η τριπλέτα  $(u, v, z)$  είναι μια κρυπτογράφηση του  $N$  κάτω από το δεσμευμένο δημόσιο κλειδί  $C$ , ο αποδεικνύων αποκαλύπτει το  $r_1$  και δεσμεύει με τον επαληθευτή το ακόλουθο πρωτόκολλο

$$PK \{ (a, b, y): C = g^a h^b \text{ fl } v = g^y \text{ fl } \frac{u}{r_1} = v^a \}$$

και επιπλέον ελέγχει αν  $z = H(r_1) \oplus N$ .

Έτσι προκύπτει ένα επαληθεύσιμο *key-oblivious* σχέδιο κρυπτογράφησης. Ένα τέτοιο σχέδιο κρυπτογράφησης ως προς ένα δεσμευμένο δημόσιο κλειδί σημειώνεται ως εξής,

$$CoN - VE (CEIG, (H, g, h, C)) \{ (x): a = b^x \}$$

Λόγω του πρωτοκόλλου Diffie Hellman το σχέδιο της επαληθεύσιμης κρυπτογράφησης είναι *key-oblivious*.

### 5.10.3 Μη μεταφερσιμότητα

Όπως αναφέρθηκε και παραπάνω στόχος του συστήματος είναι να αποθαρρύνει ή ακόμα καλύτερα να αποτρέψει του χρηστές να μοιράζονται ή και να δανείζουν τα ψευδώνυμα και πιστοποιητικά τους σε άλλους χρήστες. Η διαδικασία αυτή καλείται *μη μεταφερσιμότητα*.

Τα πρωτόκολλα που περιγράψαμε παραπάνω εξασφαλίζουν τη συνοχή των πιστοποιητικών. Τα πιστοποιητικά ανήκουν σε καλά ορισμένους χρήστες και κανένας χρήστης δεν μπορεί να αποκτήσει πιστοποιητικό για κάποιον άλλο χρήστη-φίλο του. Όλα τα πιστοποιητικά ενός χρήστη υπάγονται στο ίδιο κύριο κλειδί  $K_U$ . Αυτό σημαίνει ότι η από κοινού χρήση πιστοποιητικών δεν είναι δυνατή, διότι ο οργανισμός έκδοσης πιστοποιητικού μπορεί να διαπιστώσει ότι το πιστοποιητικό που εκδίδει και το πιστοποιητικό που του παρουσιάζει ο χρήστης (αν το έχει εκδώσει κάποιος φίλος του για αυτόν) δεν έχουν το ίδιο κύριο κλειδί άρα δεν ανήκουν στον ίδιο χρήστη.

Ωστόσο, ο δανεισμός πιστοποιητικού ή ψευδωνύμου είναι ακόμα δυνατός.

Συγκεκριμένα, κάποιος χρήστης αποκαλύπτει σε κάποιο φίλο του το κύριο κλειδί  $K_U$  και την ποσότητα  $S_{(U,O_i)}$  που προσαρτώνται στο πιστοποιητικό του με τον οργανισμό  $O_i$ . Επειδή η ποσότητα  $S_{(U,O)}$  είναι διαφορετική για κάθε οργανισμό, αυτό σημαίνει ότι δεν μπορεί αποκτήσει οποιαδήποτε άλλη μυστική ποσότητα που εμπλέκεται σε κάποιο άλλο πιστοποιητικό, παραμόνο για κάποιο συγκεκριμένο.

Το παραπάνω πρόβλημα μπορεί να αντιμετωπιστεί με δύο τρόπους . Ο πρώτος και από πριν χρησιμοποιούμενος βασίζεται στη δομή δημόσιου κλειδιού και ο χρήστης υποχρεούται να παρέχει στην Αρχή Πιστοποίησης μια επαληθεύσιμη κρυπτογράφηση του δημόσιου κλειδιού του , το οποίο μπορεί να αποκρυπτογραφηθεί με το κύριο κλειδί του.

Σύμφωνα με αυτή η από κοινού κατοχή ενός πιστοποιητικού συνεπάγεται από κοινού κατοχή ενός μυστικού κλειδιού (π.χ. το μυστικό κλειδί που δίνει πρόσβαση στον τραπεζικό λογαριασμό κάποιου). Ωστόσο ένα τέτοιο πολύτιμο κλειδί δεν υπάρχει πάντα.

Ας υποθέσουμε ότι ο χρήστης κατέχει κάποιο εξωτερικό δημόσιο κλειδί  $PK_U$ . Η Αρχή Πιστοποίησης ελέγχει αν το δημόσιο κλειδί, είναι πράγματι το δημόσιο κλειδί του χρήστη, και απαιτεί από το χρήστη να κρυπτογραφήσει επαληθεύσιμα το αντίστοιχο μυστικό κλειδί  $SK_U$  ως προς το κύριο μυστικό κλειδί  $K_U$ .

Η επαληθεύσιμη κρυπτογράφηση δημοσιεύεται έπειτα από την Αρχή Πιστοποίησης. Τώρα, εάν ο χρήστης αποκαλύψει σε κάποιον το κύριο μυστικό κλειδί  $K_U$ , κατόπιν αυτός με την ανάγνωση των δημόσιων αρχείων της Αρχής Πιστοποίησης , θα ανακτήσει την επαληθεύσιμη κρυπτογράφηση , και θα πετύχει την αποκρυπτογράφηση της .

Τεχνικά μοιάζει με την οριστική δυνατότητα μη μεταφερσιμότητας . Η κύρια διαφορά τους έγκειται στο γεγονός ότι δεν χρησιμοποιεί την κυκλική κρυπτογράφηση αλλά το σχέδιο El Gamal .

## Πρωτόκολλο 5

Έστω χρήστης  $U$  ο οποίος κατέχει ένα εξωτερικό δημόσιο κλειδί  $Y_U$

**5.1** Ο χρήστης  $U$  στέλνει τα  $Y_U$ ,  $g$  και το πιστοποιητικό πάνω στο  $Y_U$  στην Αρχή Πιστοποίησης η οποία ελέγχει την εγκυρότητα τους

**5.2** Ο χρήστης  $U$  επιλέγει  $r \in \mathbb{Z}_q$ , θέτει  $C := g^{s_U} h^r$  και το στέλνει στην Αρχή Πιστοποίησης  $CA$ . Έπειτα ο  $U$  αποδεικνύει στην Αρχή Πιστοποίησης ότι η ποσότητα  $C$  αποτελεί δέσμευση στο δημόσιο κλειδί του εκτελώντας την ακόλουθη απόδειξη γνώσης.

$$PK \{ (y, 8, \hat{\mathbf{T}}): P_{(U, O_0)}^2 = (a_{O_0}^2)^y (b_{O_0}^2)^8 \wedge C := g^y h^{\hat{\mathbf{T}}} \}$$

**5.3** Ο χρήστης  $U$  και η Αρχή Πιστοποίησης  $CA$  δεσμεύονται στο ακόλουθο

$$w_{PKI} = \text{Con} - \text{VE} (CEIG, (H, g, h, C)) \{ (a): Y_U = g^a \}.$$

**5.4** Η Αρχή Πιστοποίησης  $CA$  δημοσιεύει  $(w_{PKI}, PKI)$

Ένας δεύτερος πιο καινοτόμος τρόπος είναι η οριστική δυνατότητα μη μεταφερσιμότητας. Δηλαδή κάποιος που μοιράζεται ένα πιστοποιητικό ή ψευδώνυμο κάποιου χρήστη υπαινίσσεται ότι μοιράζεται και όλα τα πιστοποιητικά ή ψευδώνυμα του χρήστη στο σύστημα, άρα και τα μυστικά κλειδιά του χρήστη αυτού μέσα στο σύστημα. Για να επιτευχθεί αυτή η διαδικασία, ο χρήστης θα πρέπει να παρέχει σε κάθε οργανισμό μια επαληθεύσιμη κρυπτογράφηση των μυστικών ποσοτήτων που κρύβονται κάτω από την ετικέτα εγκυρότητας  $P$  του πιστοποιητικού του.

Όπως αναφέρεται ήδη, η οριστική μη-δυνατότητα μεταφερσιμότητας επιτυγχάνεται εξασφαλίζοντας ότι εάν ο χρήστης δώσει το κύριο μυστικό κλειδί του  $x_U$ , κατόπιν θα αποκαλύψει τα μυστικά κλειδιά που κρύβονται κάτω από την ετικέτα εγκυρότητας με τον οργανισμό  $O$ . Ακριβέστερα, ο χρήστης πρέπει να παρέχει στον οργανισμό  $O$  μια επαληθεύσιμη κρυπτογράφηση αυτών των μυστικών ποσοτήτων ως προς το μυστικό κλειδί  $x_U$ . Αυτό γίνεται στο ακόλουθο πρωτόκολλο, το οποίο ο χρήστης  $U$  και ο οργανισμός  $O$  πρέπει να πραγματοποιήσουν ως τμήμα του πρωτοκόλλου δημιουργίας ψευδωνύμου.

Σαν προαπαιτούμενο του πρωτοκόλλου θεωρούμε ότι κατά την εγκατάσταση του συστήματος, μια ομάδα  $G = \langle g \rangle = \langle h \rangle$  πρώτης τάξης  $q > 2^{57}$  επιλέγεται έτσι ώστε ο διακριτός λογάριθμος  $\log_g(h)$  να είναι άγνωστος.

## Πρωτόκολλο 6

**6.1** Ο χρήστης  $U$  επιλέγει  $r \in_R \mathbb{Z}_q$ , θέτει  $C := g^{su} h^r$ , στέλνει τη δέσμευση  $C$  δημόσιου κλειδιού στον οργανισμό  $O$  και αποδεικνύει ότι η ποσότητα  $C$  αποτελεί δέσμευση στο δημόσιο κλειδί του εκτελώντας την ακόλουθη απόδειξη γνώσης:

$$PK \{ (y, \theta, \varphi): P_{(U, O)}^2 = (a_O^2)^y (b_O^2)^8 \wedge C := g^y h^{\hat{\mathbf{T}}} \}$$

**6.2** Ο χρήστης  $U$  και ο οργανισμός  $O$  εκτελούν το ακόλουθο πρωτόκολλο επαληθεύσιμης κρυπτογράφησης :

$$w_{P_{(U,O)}} = \text{Con} - \text{VE}(\text{CEIG}, (H, g, h, C)) \{ (a, b) : P_{(U,O)}^2 = (a^2)_0^a (b^2)_0^b \}$$

**6.3** Έπειτα ο οργανισμός δημοσιεύει το ψευδώνυμο  $N_{(U,O)}$  και την τιμή  $w_{P_{(U,O)}}$

Ωστόσο ,δημοσιεύοντας τις ποσότητες  $N_{(U,O)}$  και  $w_{P_{(U,O)}}$  δεν είναι αρκετό για να χρησιμοποιήσει κάποιος το πιστοποιητικό του χρήστη  $U$  με τον οργανισμό  $O$  ακόμα και αν γνωρίζει το κύριο κλειδί  $x_U$  . Για αυτό οι οργανισμοί πρέπει να δημοσιεύουν όλες τις σχετικές πληροφορίες μαζί με την επαληθεύσιμη κρυπτογράφηση. Ως εκ τούτου , στο τέλος του πρωτοκόλλου δημιουργίας πιστοποιητικού , ο οργανισμός πρέπει να δημοσιεύσει τις ποσότητες  $(C_{(U,O)} , e_{(U,O)})$  μαζί με το ψευδώνυμο  $N_{(U,O)}$  .

Έτσι επιτυγχάνουμε την οριστική μη-δυνατότητα μεταφερσιμότητας σύμφωνα με την οποία όταν κάποιος γνωρίζει το κύριο κλειδί  $x_U$  κάποιου χρήστη , τότε από τις δημόσιες καταγραφές των οργανισμών μπορεί να ανακτήσει όλες τις πληροφορίες που χρειάζεται για τα πιστοποιητικά του χρήστη.

Πρόκειται για δύο διαφορετικές μεθόδους που μπορούν να εγγυηθούν τη μη μεταφερσιμότητα. Δεν είναι ισοδύναμες αλλά και οι δύο είναι επιθυμητές και μπορούν πράγματι να συνδυαστούν προκειμένου να επιτευχθεί ο στόχος μας.

Ωστόσο ,αυτό εγείρει ορισμένα τεχνικά προβλήματα. Πρώτον απαιτεί μια νέα κρυπτογραφική αρχή , την κυκλική κρυπτογράφηση που παρέχει ασφάλεια . Όταν λέμε κυκλική κρυπτογράφηση εννοούμε ότι κάθε χρήστης κρυπτογραφεί κάθε μυστικό κλειδί του με το δημόσιο κλειδί του. Επιπλέον , απαιτεί η κρυπτογράφηση να είναι key-oblivious ώστε ο χρήστης να μην αποκαλύπτει το δημόσιο κλειδί με το οποίο έγινε η κρυπτογράφηση. Επίσης , θέλουμε η κρυπτογράφηση να είναι επαληθεύσιμη . Συγκεκριμένα , θέλουμε να καταστήσουμε δυνατή την επαλήθευση του δημόσιου κλειδιού χωρίς την αποκάλυψη του. Εισάγουμε μια νέα μέθοδο επαλήθευσης που εμπλέκει μια δεσμευμένη τιμή , έτσι κάποιος αντίπαλος που παρακολουθεί την επαληθεύσιμη κρυπτογράφηση δεν μπορεί να ανακαλύψει το υποκείμενο δημόσιο κλειδί.

Για την εγγύηση της οριστικής δυνατότητας μη μεταβίβασης, πρέπει κάθε χρήστης να κρυπτογραφήσει επαληθεύσιμα όλες μυστικές πληροφορίες υπό το δημόσιο κλειδί που αντιστοιχεί στο μυστικό κλειδί του. Εντούτοις, η αποκάλυψη αυτού του δημόσιου κλειδιού θα διαρρεύσει τις πληροφορίες για το χρήστη. Επομένως, πρέπει να πραγματοποιήσουμε την επαληθεύσιμη κρυπτογράφηση με έναν τέτοιο τρόπο που η δημόσια βασική αντιστοιχία στο προκύπτον κρυπτογράφημα να μην μπορεί να συνδεθεί με τον επαληθευτή, δηλαδή θέλουμε ένα key-oblivious επαληθεύσιμο σχέδιο κρυπτογράφησης.

## **5.11 Πιστοποιητικά μιας χρήσης και διαχειριστής ανάκλησης ανωνυμίας**

### **5.11.1 Ο ρόλος του διαχειριστή ανάκλησης ανωνυμίας και σχετικά πρωτόκολλα**

Σε ένα σύστημα ανώνυμων πιστοποιητικών, είναι επιθυμητό να υπάρχει ένας μηχανισμός που να μπορεί να ανακαλύπτει την ταυτότητα του χρήστη που διενεργεί παράνομες συναλλαγές και κατά συνέπεια δεν είναι έγκυρος. Έτσι εισήχθη στο σύστημα ο διαχειριστής ανάκλησης ανωνυμίας  $R$  που σε περίπτωση τοπικής ανάκλησης ανωνυμίας παρέχει πληροφορίες που επιτρέπουν σε έναν οργανισμό να προσδιορίσει το ψευδώνυμο του χρήστη ενώ σε περίπτωση σε γενικής ανάκληση ανωνυμίας και εφόσον ο χρήστης κάνει κακή χρήση της ανωνυμίας παρέχει πληροφορίες που επιτρέπουν στην αρχή πιστοποιητικών να ανακτήσει την ταυτότητα του χρήστη.

Ωστόσο, ο χρήστης έχει την δυνατότητα να καθορίσει υπό ποιους όρους η ανωνυμία του μπορεί να ανακληθεί (ανάλογα με τους όρους των άλλων συμβαλλόμενων μερών στη συναλλαγή). Ο χρήστης μπορεί επίσης να επιλέξει απεριόριστη ανωνυμία, και έπειτα η ταυτότητά του δεν θα είναι ανακτήσιμη κάτω από οποιεσδήποτε περιστάσεις.

### 5.11.2 Δημιουργία δημόσιου και μυστικού κλειδιού του διαχειριστή ανωνυμίας R

Ο διαχειριστής ανάκλησης ανωνυμίας επιλέγει ομάδα  $G = \langle g \rangle = \langle h \rangle$  πρώτης τάξης  $q$  όπου για το  $q$  ισχύει ότι  $q > 2^{57}$ . Έπειτα επιλέγει πέντε κλειδιά  $x_1, x_2, \dots, x_5 \in_R \mathbb{Z}_q$  και υπολογίζει  $(y_1, y_2, \dots, y_5) := (g^{x_1} h^{x_2}, g^{x_3} h^{x_4}, g^{x_5})$  σαν το δημόσιο κλειδί του. Κάθε οργανισμός  $O$  δημοσιεύει επιπλέον μια γεννήτρια  $v_O \in QR_n$ .

### 5.11.3 Αλλαγές στο πρωτόκολλο δημιουργίας ψευδώνυμου

Η ετικέτα εγκυρότητας  $P_{(U,O)}$  σε ένα ψευδώνυμο χρήστη  $N_{(U,O)}$  διαμορφώνεται ελαφρώς διαφορετικά,  $P_{(U,O)} = a_O^{s_U} b_O^{c_{(U,O)}} v_O^{s_{(U,O)}}$  όπου το  $x_{(U,O)}$  επιλέγεται από το χρήστη στο διάστημα  $\Gamma$ . Τα πιστοποιητικά εκδίδονται όπως και προηγουμένως.

Δηλαδή ο χρήστης και πάλι αποκτά  $c_{(U,O)}$ ,  $e_{(U,O)}$  έτσι ώστε  $c_{(U,O)}^{e_{(U,O)}} \equiv P_{(U,O)} d$ .

Αν το πρωτόκολλο διεξαχθεί με την Αρχή Πιστοποίησης CA επεκτείνεται στα ακόλουθα βήματα.

- Ο  $U$  υπολογίζει  $Y_U = g^{s_U}$  και το στέλνει στην CA
- Ο  $U$  και η CA δεσμεύουν το ακόλουθο πρωτόκολλο  

$$PK \{ (\alpha, \beta, \gamma) : P_{(U,CA)}^2 = (a^2_{CA})^\alpha (b^2_{CA})^\beta (v^2_O)^\gamma \wedge Y_U = g^\alpha \wedge \gamma \in \Gamma \}$$
- Και οι δύο αποθηκεύουν  $Y_U$  με  $P_{(U,CA)}$

Αν το πρωτόκολλο διεξαχθεί με έναν οργανισμό  $O$  διαφορετικό από τη CA, επεκτείνεται στα ακόλουθα βήματα

- Ο  $U$  υπολογίζει  $Y_{(U,O)} = g^{s_{(U,O)}}$  και το στέλνει στην CA
- Ο  $U$  και ο  $O$  δεσμεύουν το ακόλουθο πρωτόκολλο  

$$PK \{ (\alpha, \beta, \gamma) : P_{(U,O)}^2 = (a^2_O)^\alpha (b^2_O)^\beta (v^2_O)^\gamma \wedge Y_{(U,O)} = g^\alpha \wedge \gamma \in \Gamma \}$$
- Και οι δύο αποθηκεύουν  $Y_{(U,O)}$  με  $P_{(U,CA)}$



### 5.11.4 Ανάκληση Ανωνυμίας του χρήστη U από τον Επαληθευτή

Έστω ότι ο χρήστης U και ο επαληθευτής V συμφωνούν με τους όρους  $m$  κάτω από τους οποίους ο επαληθευτής μπορεί να ταυτοποιήσει τον χρήστη U. Συγκεκριμένα, το  $m$  περιγράφει τους όρους κάτω από τους οποίους ο επαληθευτής μπορεί να ανακαλύψει το ψευδώνυμο του U με τον εκδίδοντα οργανισμό O (τοπική ανάκληση), καθώς επίσης και τους όρους κάτω από τους οποίους ο V μπορεί να ανακαλύψει την ταυτότητα του U (γενική ανάκληση).

### Πρωτόκολλο 7 (Γενική ανάκληση Ανωνυμίας)

7.1 Ο U επιλέγει  $r_2 \in_R Z_n$  και υπολογίζει  $w_1 := g^{r_2}$ ,  $w_2 := h^{r_2}$ ,  $w_3 := y_3^{r_2} Y_U$ ,

$$w_4 := y_1^{r_2} y_2^{r_2 K(w_1, w_2, w_3, N_0)} \text{ και στέλνει στον V } W_{(U,R)} = (w_1, w_2, w_3, w_4)$$

7.2 Ο U και ο V δεσμεύουν το ακόλουθο πρωτόκολλο

$$PK \{(\alpha, \beta, \gamma, \delta, \varepsilon, \xi) : d^2 = (A^2)^{\alpha} \left(\frac{1}{a_0^2}\right)^{\beta} \left(\frac{1}{b_0^2}\right)^{\gamma} \left(\frac{1}{v_0^2}\right)^{\varepsilon} \left(\frac{1}{h_0^2}\right)^{\delta} \wedge w_1 = g^s$$

$$w_2 = h^s \wedge w_3 = g^{\beta} y_3^s \wedge w_4 := (y_1^{r_2} y_2^{r_2 K(w_1, w_2, w_3, N_0)})^s \}$$

### Πρωτόκολλο 8 (Τοπική ανάκληση Ανωνυμίας)

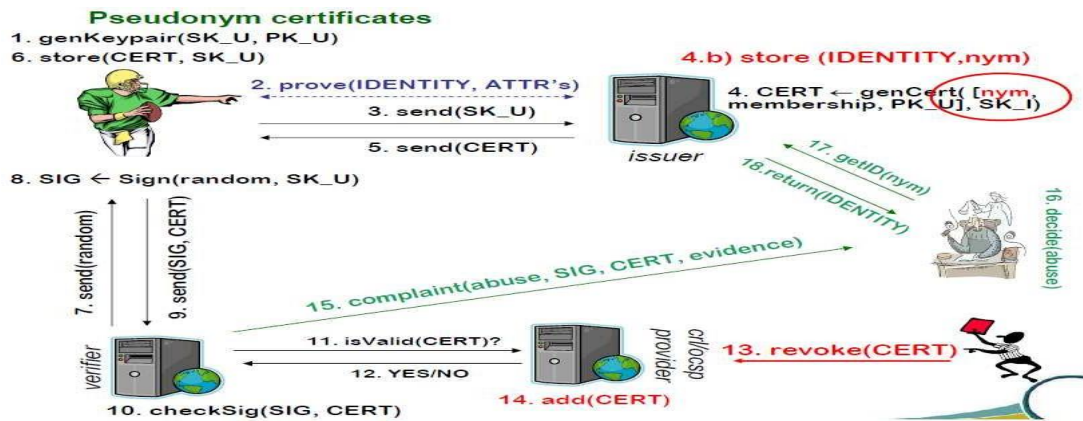
8.1 Ο U επιλέγει  $r_1 \in_R Z_n$  και υπολογίζει  $w_1 := g^{r_1}$ ,  $w_2 := h^{r_1}$ ,  $w_3 := y_3^{r_1} Y_{(U,O)}$ ,

$$w_4 := y_1^{r_1} y_2^{r_1 K(w_1, w_2, w_3, N_0)} \text{ και στέλνει στον V } W_{(U,R_j)} = (w_1, w_2, w_3, w_4)$$

8.2 Ο U και ο V δεσμεύουν το ακόλουθο πρωτόκολλο

$$PK \{(\alpha, \beta, \gamma, \delta, \varepsilon, \xi) : d^2 = (A^2)^{\alpha} \left(\frac{1}{a_0^2}\right)^{\beta} \left(\frac{1}{b_0^2}\right)^{\gamma} \left(\frac{1}{v_0^2}\right)^{\varepsilon} \left(\frac{1}{h_0^2}\right)^{\delta} \wedge w_1 = g^s$$

$$w_2 = h^s \wedge w_3 = g^{\varepsilon} y_3^s \wedge w_4 := (y_1^{r_2} y_2^{r_2 K(w_1, w_2, w_3, N_0)})^s \}$$



Σχήμα 17. -Σύστημα Πιστοποιητικού με Ανάκληση Ανωνυμίας

### 5.11.5 Πιστοποιητικά μιας χρήσης

Μέχρι τώρα τα πιστοποιητικά στα οποία αναφερθήκαμε μπορούν να χρησιμοποιηθούν όσες φορές είναι αναγκαίο. Ωστόσο πολλές υπηρεσίες απαιτούν πιστοποιητικά τα οποία δεν μπορούν να χρησιμοποιηθούν παραπάνω από μια φορά. Βέβαια σε μια τέτοια περίπτωση αν ένας χρήστης αποκάλυπτε το πιστοποιητικό στον επαληθευτή, ο χρήστης δεν θα ήταν πλήρως ανώνυμος και ο επαληθευτής με τον εκδότη του πιστοποιητικού θα μπορούσαν να συνδέσουν τη συναλλαγή με το ψευδώνυμο του χρήστη. Παραδοσιακά ένα τέτοιο πρόβλημα λύνονταν με τις τυφλές υπογραφές. Εδώ προτείνουμε έναν πιο καινοτόμο τρόπο για να προσεγγίσουμε το πρόβλημα, δηλαδή «τυφλώνουμε» τον επαληθευτή.

Έτσι λοιπόν, θα περιγράψω πως το σχέδιο του βασικού συστήματος πιστοποιητικού μπορεί να επεκταθεί ώστε να είναι δυνατή η έκδοση πιστοποιητικών μιας χρήσης. Όσον αφορά στη δημιουργία του δημόσιου και του μυστικού κλειδιού ενός οργανισμού, κάθε οργανισμός  $O$  δημοσιεύει μια επιπλέον γεννήτρια  $z_0 \in \mathbb{Q}R_{n_0}$ . Η ετικέτα εγκυρότητας  $P_{(u,o)}$  που αντιστοιχεί σε ένα ψευδώνυμο  $N_{(u,o)}$  ενός χρήστη διαμορφώνεται ως  $P_{(u,o)} = a_0^{su} b_0^{c(u,o)} z_0^{r(u,o)}$ , όπου το  $r(u,o)$  επιλέγεται από τον οργανισμό  $O$  και από τον χρήστη  $U$  μαζί με το ίδιο τρόπο όπως το  $S_{(u,o)}$ .

Τα πιστοποιητικά εκδίδονται με τον ίδιο τρόπο όπως περιέγραψα παραπάνω, και ο χρήστης  $U$  αποκτά  $c_{(u,o)}$  και  $e_{(u,o)}$  τέτοια που  $c_{(u,o)} e_{(u,o)} \equiv P_{(u,o)} d_0 \pmod{n_0}$ .

### 5.11.5.1 Παρουσίαση ενός πιστοποιητικού μιας χρήσης

Ο χρήστης  $U$  για να αποδείξει την κατοχή ενός πιστοποιητικού μιας χρήσης από έναν οργανισμό  $O$  (ως προς ένα ψευδώνυμο ή όχι) παρέχει στον επαληθευτή  $V$  την τιμή  $H_{(U,O)} = h_0^{r(U,O)}$  και αποδεικνύει ότι είναι διαμορφωμένη σωστά ως προς το

ψευδώνυμο που αυτός έχει εγκαταστήσει με τον  $O$ .

Τώρα, διαφορετικές παρουσιάσεις του ίδιου πιστοποιητικού μπορούν να διασυνδεθούν αλλά όχι με το ψευδώνυμο που ο χρήστης έχει εγκαταστήσει με τον εκδότη του πιστοποιητικού. Όμως, ο επαληθευτής μπορεί να ελέγχει με τον εκδίδοντα οργανισμό αν η ετικέτα  $H_{(U,O)}$  χρησιμοποιήθηκε ήδη ή όχι, και αυτό αποτρέπει τους χρήστες από το να χρησιμοποιήσουν το ίδιο πιστοποιητικό αρκετές φορές. Επίσης, επαλήθευση διπλής χρήσης ενός πιστοποιητικού μιας χρήσης θα μπορούσε να γίνει με off-line έλεγχο.

Συνεπώς, ένας μηχανισμός αναγνώρισης διπλών-χρηστών απαιτείται. Αυτό θα μπορούσε να γίνει χρησιμοποιώντας τον μηχανισμό ανάκλησης ανωνυμίας ή παρόμοιες τεχνικές που χρησιμοποιούνται στο ανώνυμο off-line e-cash.

Χρησιμοποίηση ενός πιστοποιητικού μιας χρήσης δύο φορές θα μπορούσε να εκθέσει τα μυστικά κλειδιά του χρήστη που συνδέονται με το αντίστοιχο ψευδώνυμο. Η διπλή χρήση ενός πιστοποιητικού μπορεί μόνο να ανιχνευθεί αλλά όχι να αποτραπεί. Τα πιστοποιητικά μιας χρήσης και η μη-μεταφερσιμότητα αποτελούν ισχυρό κίνητρο για τους χρήστες να μην χρησιμοποιούν τα πιστοποιητικά αυτά δύο φορές.

Η κύρια ιδέα είναι ότι ο επαληθευτής επιλέγει μια τυχαία πρόκληση  $c$  ακέραιου τύπου από ένα κατάλληλα μεγάλο σύνολο, για παράδειγμα,  $\{0,1\}^{s_c}$  με  $l_c=60$  και ο χρήστης  $U$  απαντά με  $r = cX_U + S_{(U,O)}$  και αποδεικνύει την ορθότητα του. Όταν ένας χρήστης χρησιμοποιεί το ίδιο πιστοποιητικό δύο φορές, κάποιος μπορεί να υπολογίσει το κύριο κλειδί  $X_U$  από τις διαφορετικές απαντήσεις που ο χρήστης παρέχει.

## Πρωτόκολλο 9

**9.1** Ο χρήστης  $U$  επιλέγει  $r_1, r_2 \in_R \{0,1\}^{25n}$  υπολογίζει  $A = c_{(u,0)} h^{r_1}_0$  και  $B = h^{r_1}_0 g^{r_2}_0$

και στέλνει τα  $A, B, H_{(u,0)}$  στον  $V$ .

**9.2** Ο επαληθευτής  $V$  επιλέγει  $c \in_R \{0,1\}^{25c}$  και το στέλνει στον χρήστη

**9.3** Ο χρήστης απαντά με  $r = cXu + S_{(u,0)}$  υπολογισμένο στο  $Z$

**9.4** Ο χρήστης δεσμεύεται με τον οργανισμό  $V$  στην ακόλουθη απόδειξη γνώσης

$$PK \{(\alpha, \beta, \gamma, \varphi, \delta, \varepsilon, \zeta, \xi, \eta) : d^2_0 = (A^2)^\alpha \left(\frac{1}{a^2_0}\right)^\beta \left(\frac{1}{b^2_0}\right)^\gamma \left(\frac{1}{z^2_0}\right)^\delta \left(\frac{1}{h^2_0}\right)^\varepsilon \wedge$$

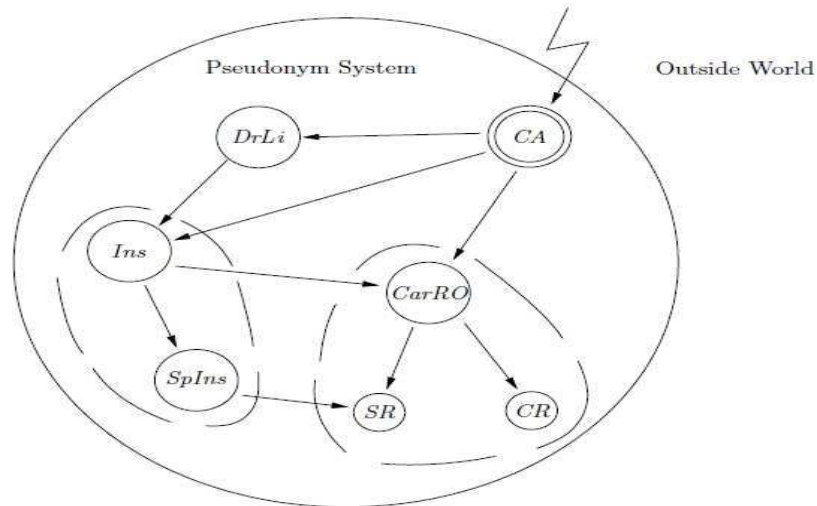
$$B^2 = (h^2_0)^\zeta (g^2_0)^\xi \wedge 1 = (B^2)^\alpha \left(\frac{1}{h^2_0}\right)^\delta \left(\frac{1}{g^2_0}\right)^\varepsilon \wedge H_{(u,0)} = (h_0)^\eta \wedge$$

$$g^r_0 = (g^c_0)^\beta (g_0)^\gamma \wedge \beta \in \Gamma \wedge \gamma \in \Delta \wedge \varphi \in \Delta \wedge \alpha \in \Lambda\}$$

Με την παρουσίαση της κρυπτογράφησης  $W = (w_1, w_2, w_3, w_4)$  και του όρου που αν ικανοποιηθεί θα έχουμε ανάκληση της ανωνυμίας, ο διαχειριστής ανάκλησης ανωνυμίας ελέγχει αν  $w_4 = w^{s_1 + s_3 K(w_1 || w_2 || w_3 || N)}_1 w^{s_2 + s_4 K(w_1 || w_2 || w_3 || N)}_2$  και αν το  $m$  ικανοποιείται. Αν ο έλεγχος είναι επιτυχής, επιστρέφει  $\hat{Y} := \frac{w_3}{w_1^{x_5}}$ . Στην περίπτωση

που έχω τοπική ανάκληση ανωνυμίας το  $\hat{Y}$  επιτρέπει την ανάκτηση του ψευδωνύμου του χρήστη με τον οργανισμό που του εξέδωσε το πιστοποιητικό και του οποίου απέδειξε κατοχή. Στην περίπτωση που έχω σφαιρική ανάκληση ανωνυμίας το  $\hat{Y}$  θα επιτρέψει στην CA να ανακτήσει την ταυτότητα του χρήστη.

## 5.12.Άποψη ενός συστήματος ανώνυμου πιστοποιητικού με ανάκληση ανωνυμίας



**Σχήμα 18. Άποψη συστήματος Ανώνυμου Πιστοποιητικού**

Το παραπάνω σχήμα απεικονίζει τον πραγματικό κόσμο και ένα σύστημα ανώνυμου πιστοποιητικού ή σύστημα ψευδωνύμων. Ο διπλός κύκλος αντιπροσωπεύει την Αρχή Πιστοποίησης, οι μεγάλοι κύκλοι αντιπροσωπεύουν τους οργανισμούς και οι μικροί κύκλοι τους επαληθευτές. Το βέλος αντιπροσωπεύει την παρουσίαση ενός πιστοποιητικού κάποιου χρήστη του συστήματος. Για παράδειγμα ένα βέλος από την οντότητα X στην οντότητα Y σημαίνει ότι ο χρήστης παρουσιάζει στην οντότητα Y ένα πιστοποιητικό το οποίο έχει εκδώσει σε αυτόν η οντότητα X.

Το παράδειγμα το οποίο θα περιγράψω αφορά ένα σύστημα ψευδωνύμων στο οποίο ένας χρήστης μπορεί να αποκτήσει δίπλωμα οδήγησης μέσω του οργανισμού DrLi, ασφάλεια αυτοκινήτου μέσω του οργανισμού Ins, ασφάλεια για αυτοκίνητο sport μέσω του οργανισμού SpIns, και πρόσβαση σε ένα κατάστημα ενοικίασης αυτοκινήτων μέσω του οργανισμού ενοικίασης αυτοκινήτων CaRO. Για να αποκτήσει πρόσβαση σε ένα κατάστημα ενοικίασης αυτοκινήτων ακολουθεί την παρακάτω διαδικασία.

Αρχικά, εγγράφεται με τον οργανισμό ενοικίασης αυτοκινήτων CaRO. Το πρώτο πράγμα που θα κάνει ο οργανισμός είναι να επαληθεύσει ότι είναι έγκυρος χρήστης. Για να το επιτύχει, ελέγχει την εγκυρότητα του πιστοποιητικού του από την Αρχή Πιστοποίησης CA.

Επίσης , επαληθεύει ότι έχει ασφάλεια αυτοκινήτου δηλαδή ότι έχει πιστοποιητικό από τον οργανισμό Ins . Το κατάστημα ενοικίασης αυτοκινήτων δεν ελέγχει αν ο χρήστης έχει δίπλωμα οδήγησης διότι για αυτό είναι υπεύθυνος ο οργανισμός παροχής ασφάλειας αυτοκινήτου. Απαραίτητη προϋπόθεση για να αποκτήσει κάποιος πιστοποιητικό ασφάλειας αυτοκινήτου από τον οργανισμό Ins είναι να έχει ήδη πιστοποιητικό από τον οργανισμό παροχής πιστοποιητικού άδειας οδήγησης . Αν κάποιος θέλει να ενοικιάσει ένα απλό αυτοκίνητο επικοινωνεί με τον car rental agency CR , ο οποίος παίζει το ρόλο του επαληθευτή. Στον επαληθευτή CR θα παρουσιάσει το πιστοποιητικό από τον οργανισμό CaRO και θα πάρει αυτοκίνητο. Ωστόσο , αν ο χρήστης θέλει να πάρει ένα sports αυτοκίνητο επικοινωνεί με τον επαληθευτή των sports αυτοκινήτων SR και αποδεικνύει όχι μόνο ότι κατέχει ένα πιστοποιητικό από τον οργανισμό CaRO αλλά και από τον οργανισμό Sp/ns, δηλαδή ότι έχει ασφάλεια για σπορ αυτοκίνητο.

Παρόλο που ο χρήστης κατά την παρουσίαση των πιστοποιητικών του δεν αποκαλύπτει καμία πληροφορία για την πραγματική του ταυτότητα ή το ψευδώνυμο του, ο διαχειριστής ανάκλησης ανωνυμίας μπορεί αργότερα να ανακαλύψει την ταυτότητα ή τα ψευδώνυμα του. Για παράδειγμα σε περίπτωση που ο χρήστης προκαλέσει ένα μη θανατηφόρο αυτοκινητιστικό ατύχημα ο διαχειριστής ανάκλησης ανωνυμίας αποκαλύπτει το ψευδώνυμο του χρήστη με την αντίστοιχη ασφαλιστική εταιρία και το κόστος της ασφάλειας του ανεβαίνει. Στην περίπτωση που το ατύχημα ήταν θανατηφόρο ο διαχειριστής ανωνυμίας αποκαλύπτει αυτή τη φορά την πραγματική ταυτότητα του χρήστη και ο χρήστης οδηγείται στην φυλακή.

## Κεφάλαιο 6: Πλαίσιο κρυπτογραφικών αρχών

Στην ενότητα αυτή θα αναλύσω κάποια σχέδια μη συμμετρικής κρυπτογράφησης , σχέδια δεσμεύσεων, σχέδια ανάκτησης υπογραφών και αποδείξεων μηδενικής γνώσης τα οποία χρησιμοποιούνται για την υλοποίηση πιστοποιητικών με τις παραπάνω ιδιότητες .

### 6.1 Αλγόριθμοι σχεδίου μη συμμετρικής κρυπτογράφησης

Το σχέδιο μη συμμετρικής κρυπτογράφησης αποτελείται από τρεις βασικούς αλγόριθμους. Τον αλγόριθμο δημιουργίας των κλειδιών που εμπλέκονται στην κρυπτογράφηση και αποκρυπτογράφηση μηνυμάτων και τους αλγόριθμους κρυπτογράφησης και αποκρυπτογράφησης μηνυμάτων.

Ο αλγόριθμος δημιουργίας του ζεύγους κλειδιών (κρυπτογράφησης – αποκρυπτογράφησης) καλείται **SetupEnc** και εξάγει το κλειδί που εμπλέκεται στην κρυπτογράφηση το οποίο συμβολίζεται ως **EK (Encryption Key)** και το κλειδί που εμπλέκεται στην αποκρυπτογράφηση το οποίο συμβολίζεται ως **DK (Decryption Key)**. Ο αλγόριθμος κρυπτογράφησης ενός μηνύματος καλείται **Enc (Encryption)** και δέχεται ως είσοδο ένα μήνυμα  $m$  , μια ετικέτα  $L$ , και το κλειδί κρυπτογράφησης **EK** και εξάγει μια κρυπτογράφηση  $E$  του μηνύματος  $N$  , δηλαδή  $E = Enc(N, L, EK)$ . Ο αλγόριθμος αποκρυπτογράφησης **Dec (Decryption)** λαμβάνει ως είσοδο την κρυπτογράφηση  $E$  ενός μηνύματος  $N$ , την ετικέτα  $L$  και το κλειδί της αποκρυπτογράφησης **DK** και εξάγει το μήνυμα  $N$  , δηλαδή  $N = Dec(E, L, DK)$ .

Ένα σχέδιο κρυπτογράφησης είναι ασφαλές, εάν μια κρυπτογράφηση  $E = Enc(N, L, EK)$  δεν περιέχει καμία πληροφορία για τον τρόπο υπολογισμού του μηνύματος  $N$  σε έναν αντίπαλο στον οποίο δίνεται η κρυπτογράφηση  $E$  και το κλειδί **EK** , ακόμα κι αν ο αντίπαλος επιτρέπεται να αλληλεπιδράσει με τον αποκωδικοποιητή.

Στις εφαρμογές , ο χρήστης θα μπορούσε να επισυνάπτει την ετικέτα μιας κρυπτογράφησης  $E$  η οποία θα επιλαμβάνει τους όρους κάτω από οποίους αυτή μπορεί αποκρυπτογραφηθεί ώστε να ανακτηθεί το μήνυμα  $N$ .

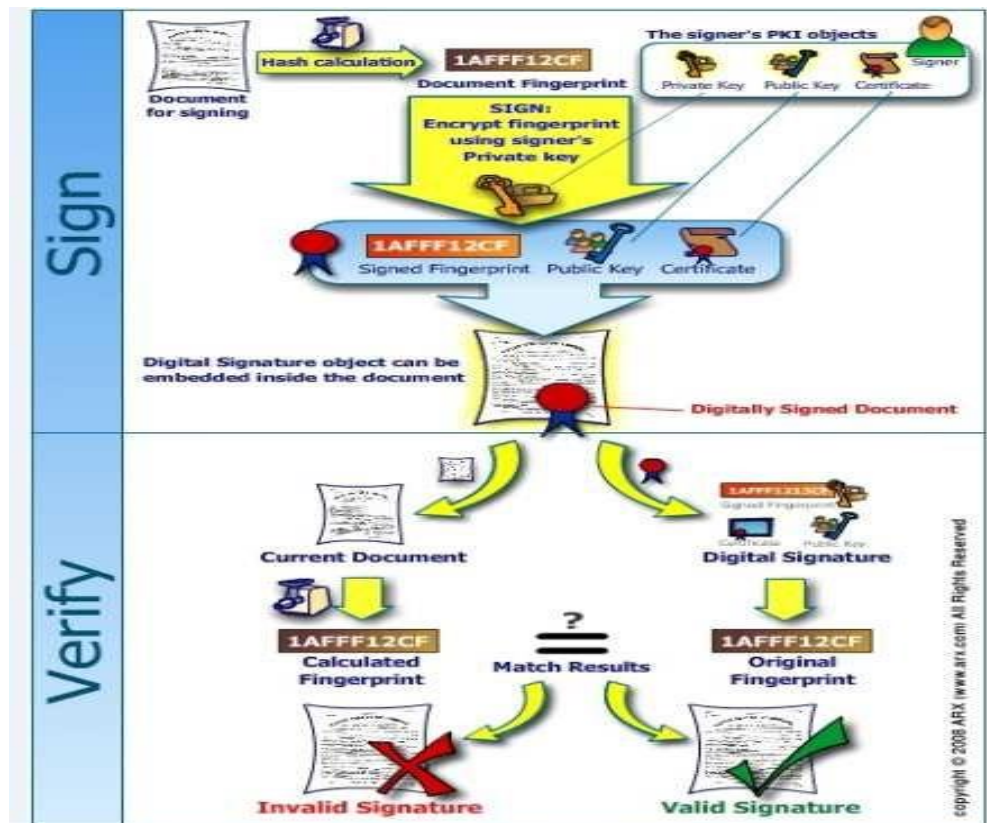
Μέχρι τώρα είδαμε ένα γενικό πλάνο για το πώς μπορούμε να κρυπτογραφήσουμε και να αποκρυπτογραφήσουμε ένα μήνυμα  $N$  βάσει των κλειδιών κρυπτογράφησης και αποκρυπτογράφησης αντίστοιχα. Ακολούθως θα περιγράψουμε κάποια συγκεκριμένα σχέδια τα οποία χρησιμοποιούνται στην πράξη.

### 6.1.1 Σχέδιο κρυπτογράφησης & αποκρυπτογράφησης των Camenisch & Shoup

Ένα σχέδιο κρυπτογράφησης που ικανοποιεί τις απαιτήσεις είναι των Camenisch & Shoup. Το σχέδιο αυτό παρέχει ένα επιπλέον πρωτόκολλο που επιτρέπει σε ένα κωδικοποιητή να αποδείξει αποτελεσματικά ότι ένα κρυπτογράφημα περιέχει έναν διακριτό λογάριθμο και ένα πρωτόκολλο που επιτρέπει σε ένα αποκωδικοποιητή να αποδείξει ότι η αποκρυπτογράφηση ενός δεδομένου κρυπτογραφήματος αποκαλύπτει έναν διακριτό λογάριθμο.

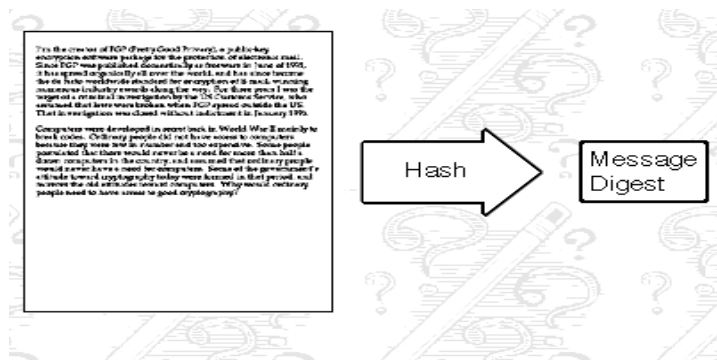
Το σχέδιο κρυπτογράφησης χρησιμοποιεί μια συνάρτηση κατακερματισμού  $H(\cdot)$  που χαρτογραφεί μια τριπλέτα  $(u, \{e_i\}, L)$  σε έναν μοναδικό αριθμό στο  $[2^5]$ . Η συνάρτηση κατακερματισμού έχει την ιδιότητα (*collision resistant*) ότι, για δύο διαφορετικές τριπλέτες  $(u, \{e_i\}, L) \neq (u', \{e'_i\}, L')$ , είναι ανέφικτο να προκύψει το ίδιο αποτύπωμα, δηλαδή  $H(u, \{e_i\}, L) = H(u', \{e'_i\}, L')$ .





Σχήμα 19. Δημιουργία και επαλήθευση υπογραφής

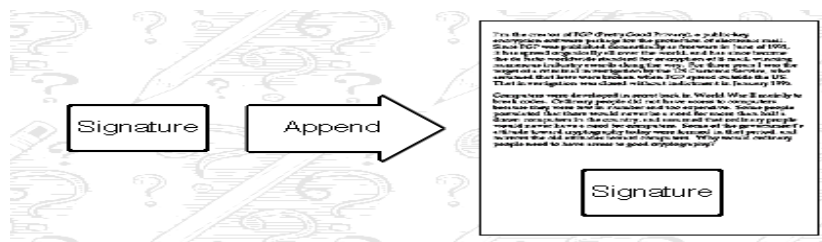
1<sup>ο</sup> βήμα



2<sup>ο</sup> βήμα



### 3<sup>ο</sup> βήμα



**Σχήμα 20. Βήματα ανάκτησης υπογραφής**

Η έξοδος μιας συνάρτησης κατακερματισμού ονομάζεται τιμή κατακερματισμού ή σύνοψη μηνύματος και έχει ένα συγκεκριμένο μήκος ανάλογα με το είδος του αλγόριθμου κατακερματισμού που χρησιμοποιείται , συνήθως πολύ μικρότερο από αυτό του αρχικού μηνύματος . Επειδή η συνάρτηση κατακερματισμού παράγει την σύνοψη ενός μηνύματος , οι συναρτήσεις αυτές ονομάζονται και αλγόριθμοι σύνοψης μηνύματος .

Όπως το δακτυλικό αποτύπωμα ενός ανθρώπου είναι μοναδικό και είναι αδύνατο δύο διαφορετικοί άνθρωποι να έχουν το ίδιο αποτύπωμα , την ίδια ακριβώς λογική ακολουθούμε και στην περίπτωση αυτών των συναρτήσεων. Μια εφαρμογή στην οποία χρησιμοποιούνται αφορά την υπογραφή ενός ψηφιακού εγγράφου.

Συγκεκριμένα , αντί να υπογράψουμε το έγγραφο απευθείας με το μυστικό κλειδί υπογράφουμε το «μοναδικό ψηφιακό αποτύπωμα» του που μας επιστρέφει η συνάρτηση κατακερματισμού . Στο σχήμα 19 απεικονίζεται πιστά αυτή η διαδικασία .

Οι αλγόριθμοι σύνοψης μηνύματος πρέπει να είναι μονόδρομες συναρτήσεις. Ο σκοπός του αλγόριθμου αυτού είναι να παράγει μια αναπαράσταση ενός μηνύματος , που είναι μικρότερη από αυτό και να κρυπτογραφείται γρηγορότερα.

Αυτό σημαίνει ότι η συνάρτηση πρέπει να μπορεί να υπολογίσει εύκολα τη σύνοψη ενός μηνύματος όταν της δίνουμε το μήνυμα , αλλά πρέπει να είναι σχεδόν αδύνατο να υπολογίσει το μήνυμα όταν της δίνουμε την σύνοψη ενός μηνύματος. Με αυτή την προϋπόθεση εξασφαλίζουμε το γεγονός , ότι άτομα που έχουν πρόσβαση στην σύνοψη μηνύματος είναι δύσκολο να ανακαλύψουν το μήνυμα από τη σύνοψη του.

Όταν λοιπόν θέλουμε να υπογράψουμε ένα μήνυμα , πρώτα δημιουργούμε τη σύνοψή του και ύστερα το κρυπτογραφούμε με το μυστικό ( αλλιώς ιδιωτικό ) μας κλειδί. Ύστερα επισυνάπτουμε στο μήνυμα τη σύνοψη του μηνύματος και το αποστέλλουμε . Ο αποδέκτης θα δημιουργήσει και αυτός μιας σύνοψη του μηνύματος με τον ίδιο αλγόριθμο που χρησιμοποιήσαμε και εμείς , μετά θα αποκρυπτογραφήσει με το δημόσιο κλειδί την κρυπτογραφημένη σύνοψη του μηνύματος που στείλαμε και θα το συγκρίνει με αυτό που υπολόγισε ο ίδιος. Οποιαδήποτε διαφορά θα σήμαινε ότι υπήρξε παραποίηση του μηνύματος.

Επομένως τα χαρακτηριστικά του αλγόριθμου σύνοψης μηνύματος περιγράφονται ως εξής :

- Δεν είναι δυνατή η αντιστροφή μιας συνάρτησης κατακερματισμού ,έτσι ώστε από τη σύνοψη να προκύψει το αρχικό κείμενο
- Η σύνοψη δεν δίνει καμία πληροφορία για το αρχικό κείμενο
- Είναι υπολογιστικά ανέφικτο να βρεθεί απλό κείμενο , που να έχει ως σύνοψη μια συγκεκριμένη τιμή
- Διαφορετικό απλό κείμενο , έστω και κατά πολύ μικρό βαθμό , πρέπει να δίνει πάντοτε διαφορετική σύνοψη. Οι περιπτώσεις , όπου δύο διαφορετικά αρχικά κείμενα δίνουν την ίδια σύνοψη , λέγονται συγκρούσεις της συνάρτησης κατακερματισμού και αποτελούν προβληματικές περιπτώσεις.

### 6.1.1.1 Αλγόριθμος δημιουργίας κλειδιών κρυπτογράφησης & αποκρυπτογράφησης

Επιλέγουμε 2 τυχαίους  $l$  δυαδικών ψηφίων Sophie Germain πρώτους αριθμούς  $e'$  ,  $q'$  με  $e' \neq q'$  . Εν συνεχεία υπολογίζουμε  $e = 2e' + 1$  ,  $q = 2q' + 1$  ώστε  $n = eq$  και  $n' = e'q'$  . Επιλέγουμε τυχαία  $x_{(1,1)} , x_{(1,2)} , \dots , x_{(1,L')}$  ,  $x_2 , x_3 \in \mathbb{Z}_{n^2/4}$  ,

επιλέγουμε τυχαίο  $g' \in \mathbb{Z}_{n^2}^*$  και υπολογίζουμε  $g := (g')^{2n}$  ,  $y_{(1,i)} := g^{s_{(1,i)}}$  ,  $y_2 := g^{s_2}$  ,  $y_3 := g^{s_3}$  . Το δημόσιο κλειδί θα είναι  $(n, g, \{y_{(1,i)}\}, y_2, y_3)$  .

Το μυστικό κλειδί είναι  $(n, g, \{x_{(1,i)}\}, x_2, x_3)$  . Ακολουθώς θεωρώ ότι  $h = (1 + n \bmod n^2) \in \mathbb{Z}_{n^2}^*$  το οποίο είναι στοιχείο τάξης  $n$ .

Η κρυπτογράφηση θα γίνει με το δημόσιο κλειδί ενώ η αποκρυπτογράφηση ενός μηνύματος θα γίνει με μυστικό κλειδί το οποίο όπως αναφέραμε γνωρίζει μόνο ο παραλήπτης του μηνύματος και συνεπώς μόνο αυτός μπορεί να αποκρυπτογραφήσει σωστά το κρυπτογραφημένο μήνυμα.

### 6.1.1.2 Αλγόριθμος κρυπτογράφησης & αποκρυπτογράφησης

Για να **κρυπτογραφήσουμε** τα μηνύματα  $(N_1, N_2, \dots, N_{L'})$ ,  $N_i \in [n]$ , με ετικέτα  $L \in \{0,1\}^*$  υπό το δημόσιο κλειδί όπως το υπολογίσαμε παραπάνω επιλέγουμε τυχαίο  $r \in_R [n/4]$  και υπολογίζουμε  $u := g^r$ ,  $e_i := g_{(i)}^r h^{N_i}$  για  $i = 1, 2, \dots, L'$  και  $v := \text{abs}((y_2 y_3^{K(u, \{e_i\}_L)})^r)$ . Το κρυπτογράφημα που αντιστοιχεί στα μηνύματα  $(N_1, N_2, \dots, N_{L'})$  είναι  $(u, \{e_i\}, v)$ .

Για να **αποκρυπτογραφήσουμε** το κρυπτογράφημα  $(u, \{e_i\}, v) \in Z_{n^2}^* \times (Z_{n^2}^*)^{L'}$  με ετικέτα  $L$  υπό το μυστικό κλειδί, ελέγχουμε πρώτα  $\text{abs}(v) = v$  και  $v^{2(s_2 + K(u, \{e_i\}_L)s_3)} = v^2$ . Αν αυτό δεν ισχύει τότε η έξοδος απορρίπτεται και σταματά. Έπειτα, θέτουμε  $t = 2^{-1} \text{Nod } n$ , υπολογίζουμε  $\mathfrak{K}_t = (e_i / u^{s_{(1,i)}})^{2t}$ .

Αν όλα τα  $\mathfrak{K}_t$  είναι της μορφής  $h^{N_i}$  για κάποιο  $N_i \in [n]$ , τότε η έξοδος είναι  $(N_1, N_2, \dots, N_{L'})$ , αλλιώς απορρίπτεται.

### 6.1.1.3 Επαληθεύσιμη κρυπτογράφηση διακριτών λογαρίθμων

Έστω  $c_1 = g^{N_1} h^{r_1}$ ,  $c_2 = g^{N_2} h^{r_2}$ , ...,  $c_{L'} = g^{N_{L'}} h^{r_{L'}}$  δεσμεύσεις στα μηνύματα  $(N_1, N_2, \dots, N_{L'}) \in Z_q$ . Δεν θα χρησιμοποιήσω απευθείας τα μηνύματα  $(N_1, N_2, \dots, N_{L'})$  αλλά το διακριτό λογάριθμο αυτών και θα παρουσιάσω ένα πρωτόκολλο που επιτρέπει σε έναν αποδεικνύων να κρυπτογραφήσει τα  $(N_1, N_2, \dots, N_{L'}) \in Z_q$  και έπειτα να πείσει έναν επαληθευτή ότι το προκύπτον κρυπτογράφημα πράγματι κρυπτογραφεί τις τιμές που περιλαμβάνονται μέσα στις δεσμεύσεις αυτές.

Ονομάζουμε  $\iota_c$  μια παράμετρο ασφαλείας που ελέγχει το μέγεθος του χώρου πρόκλησης στα πρωτόκολλα δημόσιου κλειδιού. Τέλος απαιτούμε ότι  $q < n^{2^{-\iota_c - \delta_c - 3}}$  και ότι  $N_i \in Z_q$  εμπεριέχεται σε μια κρυπτογράφηση.

Αν αυτή η συνθήκη δεν ισχύει τότε το  $N_i$  μπορεί να σπάσει σε μικρότερα κομμάτια τα οποία μπορούν να κρυπτογραφηθούν επαληθεύσιμα . Ωστόσο κάτι τέτοιο δεν θα μας απασχολήσει εδώ.

Έτσι λοιπόν , κοινή είσοδος και στον αποδεικνύων και στον επαληθευτή είναι το δημόσιο κλειδί  $(n, g, \{y_{(1,i)}\}, y_2, y_3)$  του σχεδίου κρυπτογράφησης , επιπλέον οι παράμετροι  $(\eta, g, h)$  , ένα στοιχείο ομάδας  $(\delta)$  , ένα κρυπτογράφημα  $(u, \{e_i\}, v) \in Z_{n^2}^* \times (Z_{n^2}^*)^L$  και ετικέτα  $L$ . Ο αποδεικνύων έχει επιπλέον εισόδους  $(N_1,$

$N_2, \dots, N_L)$   $N_i \in Z_q$  και  $r \in_R [N/4]$  τέτοιο ώστε

$$u := g^r, e := y_{(1,i)}^r h^{N_i} \text{ και } v := \text{abs}((y_2 y_3^{K(u,e,L)})^r).$$

Το πρωτόκολλο περιλαμβάνει τα ακόλουθα βήματα:

1. Ο αποδεικνύων επιλέγει τυχαίο  $s \in_R [N/4]$  , υπολογίζει και στέλνει στον επαληθευτή την ποσότητα  $b = g^s h^c$
2. Και οι δύο μαζί δεσμεύουν το ακόλουθο πρωτόκολλο

$PK \{ (r, m, s) : (v, q_1, \dots, q_L, \mu_1, \dots, \mu_L) \}$

$$c_1 = g^{\mu_1} h^{q_1}, c_2 = g^{\mu_2} h^{q_2}, \dots, c_L = g^{\mu_L} h^{q_L} \wedge$$

$$u^2 = g^{2r} \wedge v^2 = (y_2 y_3^{K(u,e,L)})^{2r} \wedge$$

$$e^2 = y_{(1,1)}^{2r} h^{\mu_1} \wedge \dots \wedge e^2 = y_{(1,L)}^{2r} h^{\mu_L} \wedge$$

$$b_1 = g^{\mu_1} h^c \wedge \dots \wedge b_L = g^{\mu_L} h^c \wedge -N/4 < N_i < N/4 \}$$

2

2

## 6.2 Σχέδιο δέσμευσης

Το σχέδιο δέσμευσης αποτελείται από δύο κύριους αλγόριθμους. Τον αλγόριθμο δέσμευσης ενός μηνύματος ο οποίος ονομάζεται *Commit* και έναν αλγόριθμο επαλήθευσης της δέσμευσης ενός μηνύματος ο οποίος καλείται *VerifyCommit* .

Ο αλγόριθμος δέσμευσης μετασχηματίζει το αρχικό μήνυμα το οποίο θέλουμε να αποστείλουμε σε μια νέα μορφή γνωστή ως δέσμευση και μετά χρησιμοποιώντας έναν αλγόριθμο κρυπτογράφησης κρυπτογραφούμε τη δέσμευση αυτού , ενισχύοντας ακόμα περισσότερο την ασφάλεια του νέου συστήματος ανώνυμων πιστοποιητικών.

Συνεπώς , ακόμα και αν κάποιος γνώριζε το κλειδί της αποκρυπτογράφησης δεν θα μπορούσε να ανακτήσει το σωστό μήνυμα .

Ο αλγόριθμος *Commit* λαμβάνει είσοδο ένα μήνυμα  $\mathbf{N}$  , ένα τυχαίο αλφαριθμητικό  $r$  και εξάγει μια δέσμευση  $C$  για το μήνυμα  $\mathbf{N}$ , δηλαδή  $C = \text{Commit}(m, r)$ . Ο αλγόριθμος επαλήθευσης δέσμευσης , *VerifyCommit* παίρνει ως είσοδο τη δέσμευση  $C$  , το μήνυμα  $m$  και το  $r$  και εξάγει 1 εάν  $C = \text{Commit}(m, r)$  και 0 σε αντίθετη περίπτωση. Με τη βοήθεια του αλγόριθμου *VerifyCommit* μπορούμε να επαληθεύσουμε ότι η συγκεκριμένη δέσμευση  $C$  αντιστοιχεί στο συγκεκριμένο μήνυμα  $\mathbf{N}$ .

### 6.2.1 Ιδιότητες του σχεδίου δέσμευσης

Ένα σχέδιο δέσμευσης παρουσιάζει κάποιες ιδιότητες ασφαλείας. Την ιδιότητα της απόκρυψης σύμφωνα με την οποία μια δέσμευση  $C = \text{Commit}(m, r)$  ενός μηνύματος  $m$ , δεν περιέχει πληροφορίες που επιτρέπουν σε κάποιον τρίτο τον υπολογισμό του μηνύματος  $\mathbf{N}$ , και την ιδιότητα της σύνδεσης η οποία δεδομένη της δέσμευσης  $C$  ενός μηνύματος  $\mathbf{N}$  και του αλφαριθμητικού  $r$  τα οποία ικανοποιούν τον αλγόριθμο επαλήθευσης δέσμευσης (  $I = \text{VerifyCommit}(C, m, r)$  ), αναφέρει ότι είναι υπολογιστικά αδύνατο να βρεθεί ένα δεύτερο μήνυμα  $\mathbf{N}^u \neq \mathbf{N}$  και ένα αλφαριθμητικό  $r^u \neq r$  τα οποία επαληθεύουν το αλγόριθμο *VerifyCommit* , δηλαδή  $I = \text{VerifyCommit}(C, \mathbf{N}^u, r^u)$ .

Συνεπώς σε κάθε δέσμευση  $C$  αντιστοιχεί ένα μοναδικό ζεύγος  $\mathbf{N}, r$  και δεν είναι δυνατόν δύο διαφορετικά ζεύγη  $(\mathbf{N}, r)$  να έχουν την ίδια δέσμευση  $C$ .

### 6.2.2 Σχέδιο δέσμευσης του Pedersen

Υπάρχουν διάφορα σχέδια δέσμευσης που ικανοποιούν τις απαιτήσεις. Το πρώτο είναι το σχέδιο του Pedersen. Χρησιμοποιεί στοιχεία  $g$  και  $h$  τάξης  $q$  (πρώτος αριθμός) έτσι ώστε  $g \in \langle h \rangle$ , όπου το  $q$  είναι ένας αριθμός  $l_q$  δυαδικών ψηφίων. Για να δεσμεύσει σε ένα μήνυμα  $m \in_{\mathbb{R}} \mathbb{Z}_q$  κάποιος επιλέγει ένα τυχαίο  $r$  και υπολογίζει την δέσμευση  $C := g^m h^r$ . Η δέσμευση μπορεί να ανοίξει με την αποκάλυψη του  $m$  και του  $r$ . Μια απόδειξη γνώσης της τιμής που περιλαμβάνεται σε μια δέσμευση  $C$  σημειώνεται ως  $\text{PK}\{ (m, r): C = g^m h^r \}$ .

Το σχέδιο του Pedersen έχει την ιδιότητα ότι μια δέσμευση δεν διαρρέει καμία πληροφορία για το δεσμευμένο μήνυμα. Ωστόσο κάποιος που είναι σε θέση να υπολογίσει τον διακριτό λογάριθμο  $\log_h(\mathbf{g})$  μπορεί να «ανοίξει» τη δέσμευση σε διαφορετικά μηνύματα. Έστω  $\mathbf{C} = (\mathbf{C}_1, \mathbf{C}_2) = (\mathbf{g}^N h^r, h^r)$ . Μια τέτοια δέσμευση μπορεί να ανοίξει με την αποκάλυψη του  $\mathbf{N}$  και του  $r$  και η απόδειξη γνώσης  $\text{PK}\{(\mu, q): \mathbf{C}_1 = \mathbf{g}^\mu h^q \wedge \mathbf{C}_2 = h^q\}$  μπορεί να χρησιμοποιηθεί για να αποδείξει η γνώση του μηνύματος που δεσμεύεται από αυτό.

### 6.2.3 Σχέδιο δέσμευσης ακεραίων

Το σχέδιο του Pedersen έχει το «μειονέκτημα» ότι δεσμεύει μόνο στοιχεία από το  $\mathbb{Z}_q$ . Εντούτοις, πρέπει μερικές φορές να δεσμεύσουμε στοιχεία από το  $\mathbb{Z}$ . Για αυτό θα περιγράψουμε ένα ακόμα σχέδιο, το σχέδιο δέσμευσης ακεραίων των Damgard & Fujisaki.

Έστω  $n = pq$  το γινόμενο δύο ασφαλών πρώτων αριθμών μήκους  $\frac{5n}{2}$  δυαδικά ψηφία όπου  $p = 2p' + 1$ ,  $q = 2q' + 1$  και  $(\mathbf{g}, )$  γεννήτριες του  $\mathcal{B}_{n^F}$ , όπου  $n' = p' q'$ . Το  $\mathcal{B}_{n^F}$  είναι υποομάδα του  $\mathbb{Z}_n^*$  τάξης  $n'$ . Ας υποθέσουμε  $n, g, h$  έτσι ώστε η παραγοντοποίηση του  $n$  καθώς επίσης και η τιμή  $\log(\mathbf{g})$  είναι άγνωστη τουλάχιστον στο μέρος που υπολογίζει την δέσμευση.

Κάποιος μπορεί να δεσμεύσει έναν ακεραίο  $\mathbf{N} \in \{0, 1\}^{5n}$  όπου  $l_N$  (δημόσια παράμετρος), επιλέγοντας τυχαίο  $r \in_{\mathbb{R}} [N/4]$  και υπολογίζοντας τη δέσμευση  $\mathbf{C} := (\mathbf{g}^N)^r$ . Η δέσμευση μπορεί να ανοίξει αν αποκαλυφθούν τα  $\mathbf{N}, r$ . Για να αποδείξει κάποιος ότι γνωρίζει την τιμή που κρύβεται κάτω από τη δέσμευση μπορεί να χρησιμοποιήσει το πρωτόκολλο-απόδειξη γνώσης  $\text{PK}\{(\mu, q): \mathbf{C} := \mathbf{g}^\mu)^q \bmod n\}$  όπου οι ποσότητες  $\mu, r$  παραμένουν άγνωστες στον επαληθευτή.

### 6.2.4 Απόδειξη Μήκους διακριτού λογάριθμου

Υποθέτουμε ότι είναι διαθέσιμα  $n, g, h$ . Έστω  $G = \langle \mathbf{g} \rangle$  ομάδα τάξης  $q$  ( $q$  πρώτος αριθμός) και  $y = \mathbf{g}^N$  τέτοιο ώστε  $-2^{5n} < N < 2^{5n}$ , όπου  $2^{5n} < q 2^{-5c-5c-1}$ .

Για να πείσει τον επαληθευτή ότι  $-2^{s_c + s_c + s_N} < N < 2^{s_c + s_c + s_N}$ , ο αποδεικνύων δεσμεύει στο  $\chi$  χρησιμοποιώντας το σχέδιο δέσμευσης ακεραίων, δηλαδή επιλέγει ένα τυχαίο  $r \in_R [N/4]$ , υπολογίζει  $C := g^N)^r$  και τρέχει το πρωτόκολλο

PK  $\{(\mu, q) : y = g^\mu \text{ fl } C := g^\mu)^q \wedge -2^{s_c + s_c + s_N} < \mu < 2^{s_c + s_c + s_N}\}$  με τον επαληθευτή.

Ένα παράδειγμα πως λειτουργεί αυτό το πρωτόκολλο είναι το ακόλουθο. Η είσοδος και στα δύο μέρη είναι  $g, y, n, g, C, l_c, l_n$  όπου  $l_c$  και  $l_n$  είναι δυο παράμετροι ασφαλείας. Ο αποδεικνύων, επιπλέον λαμβάνει στην είσοδο του  $N$  και  $r$ .

1. Ο αποδεικνύων επιλέγει ένα τυχαίο  $r_\mu \in \{0,1\}^{s_c + s_c + s_N}$  και  $r_q \in \{0,1\}^{s_c + s_c + s_N}$  όπου  $l_n$  είναι μήκους  $[N/4]$ , υπολογίζει  $\tilde{y} = g^{r_\mu}$  και  $\tilde{C} = g^{r_\mu})^{r_q}$  και τα στέλνει στον επαληθευτή.
2. Ο επαληθευτής απαντά με ένα τυχαία επιλεγμένο  $c \in \{0,1\}^{s_c}$
3. Ο αποδεικνύων υπολογίζει  $s_\mu := r_\mu + C_N$  και  $s_q := r_q + C_r$  και στέλνει τις τιμές αυτές στον επαληθευτή.
4. Ο επαληθευτής αποδέχεται αν ισχύουν οι εξισώσεις  

$$\tilde{y} = y^{-c} g^{s_\mu}, \quad \tilde{C} = C^{-c} g^{s_q})^{c_q} \text{ mod } n \quad \text{και } s_\mu \in \{0,1\}^{s_c + s_c + s_N}$$
Αλλιώς απορρίπτει.

Το παραπάνω πρωτόκολλο μπορεί να επεκταθεί για να αποδεικνύει την ισότητα διακριτών λογαρίθμων σε δύο ομάδες  $\langle g_1 \rangle$ ,  $\langle g_2 \rangle$  διαφορετικής τάξης  $q_1$  και  $q_2$  αντίστοιχα.

Δηλαδή, για  $y_1 = g_1^{N_1}$  και  $y_2 = g_2^{N_2}$  με  $N_0 \in \{0,1\}^{s_N}$  έτσι ώστε  $2^{s_c + s_c + s_N + 1} <$

$\min(q_1, q_2)$  το ακόλουθο πρωτόκολλο επιτυγχάνει αυτό το σκοπό, όπου  $C$  είναι μια δέσμευση στο  $m$

PK  $\{(\mu, q) : y_1 = g_1^N \wedge y_2 = g_2^N \wedge C \equiv g^\mu)^q \text{ mod } n$   
 $\wedge -2^{s_c + s_c + s_N} < \mu < 2^{s_c + s_c + s_N}\}.$



### 6.3 Σχέδιο ανάκτησης υπογραφών

Η Ψηφιακή Υπογραφή είναι δεδομένα συνημμένα ή συσχετισμένα με ένα ηλεκτρονικό κείμενο, τα οποία χρησιμεύουν στην επαλήθευση της αυθεντικότητας του. Η υπογραφή σε ένα κείμενο είναι ένα στοιχείο το οποίο επικυρώνει το κείμενο και επαληθεύει την προέλευση του.

Επίσης ,χρησιμοποιείται από τον παραλήπτη ως αποδεικτικό στοιχείο.

Έχει τα εξής χαρακτηριστικά:

- Είναι μονοσήμαντα συνδεδεμένη με τον υπογράφοντα
- Παρέχει τη δυνατότητα αναγνώρισης του υπογράφοντα
- Δημιουργείται με μέσα που βρίσκονται στον αποκλειστικό έλεγχο του υπογράφοντα
- Είναι μονοσήμαντα συνδεδεμένη με το σχετικό κείμενο, με τρόπο ώστε να διασφαλίζεται η ακεραιότητά του
- Δεν μπορεί να δημιουργηθεί από άλλη οντότητα και δεν μπορεί να μεταφερθεί σε άλλο κείμενο
- Ο υπογράφων δεν μπορεί να αρνηθεί ότι δημιούργησε μια υπογραφή
- Η χρήση *ψηφιακών υπογραφών*, κατά την ανταλλαγή πληροφοριών , εγγυάται την αυθεντικότητα της ταυτότητας του αποστολέα και την ακεραιότητα της πληροφορίας.

Το σχέδιο υπογραφών περιλαμβάνει τρεις βασικούς αλγορίθμους , τον αλγόριθμο δημιουργίας των κλειδιών που εμπλέκονται στην δημιουργία μιας υπογραφής και στον έλεγχο της εγκυρότητάς της, **SetupSign**, τον αλγόριθμο δημιουργίας υπογραφής ο οποίος καλείται **Sign** και και τον αλγόριθμος επαλήθευσης της εγκυρότητας υπογραφής ο οποίος καλείται **VerifySign**.

Ο αλγόριθμος δημιουργίας κλειδιού **SetupSign** εξάγει ένα κλειδί επαλήθευσης υπογραφής **VK (Verification Key)** και ένα κλειδί δημιουργίας υπογραφής **SK (Sign Key )**. Ο αλγόριθμος υπογραφής **Sign** παίρνει ως είσοδο μήνυμα **N** και το κλειδί **SK** και εξάγει μια υπογραφή **S** στο μήνυμα **m** , δηλαδή  $S = \text{Sign}(N; SK)$ . Ο αλγόριθμος επαλήθευσης υπογραφής **VerifySign** παίρνει ως είσοδο την υπογραφή **S**, το μήνυμα **N** , το κλειδί επαλήθευσης υπογραφής **VK**.

Αν πράγματι πρόκειται για μια έγκυρη υπογραφή που αντιστοιχεί στο μήνυμα  $N$  τότε την «αποδέχεται» αλλιώς την απορρίπτει. Το σχέδιο ανάκτησης υπογραφών είναι ασφαλές εάν, με είσοδο το κλειδί επαλήθευσης υπογραφής  $VK$  (Verification Key), κανένας αντίπαλος δεν μπορεί να παράγει μια έγκυρη υπογραφή σε οποιοδήποτε μήνυμα  $N$ .

Μια παραλλαγή του αλγόριθμου **Sign** παίρνει ως είσοδο μια λίστα μηνυμάτων  $N_1, \dots, N_s$  και ένα κλειδί υπογραφής  $SK$  και εξάγει μια υπογραφή  $S$  πάνω στα μηνύματα  $N_1, \dots, N_s$ , δηλαδή  $S = \text{Sign}(N_1, \dots, N_s; SK)$ . Αντίστοιχα ο αλγόριθμος επαλήθευσης **VerifySign** εξετάζει αν μια υπογραφή  $S$  αποτελεί έγκυρη υπογραφή που αντιστοιχεί σε μια λίστα μηνυμάτων  $N_1, \dots, N_s$ . Αν η  $S$  αποτελεί έγκυρη υπογραφή, ο αλγόριθμος επιστρέφει 1 (αληθές), διαφορετικά επιστρέφει 0 (μη έγκυρη υπογραφή).

Μια επέκταση του σχεδίου υπογραφών περιλαμβάνει το πρωτόκολλο **HiddenSign** μεταξύ ενός υπογράφοντος και ενός αιτούντος υπογραφής. Σύμφωνα με αυτό, θεωρούμε τα μηνύματα  $N_1, \dots, N_s$  και τις δεσμεύσεις  $C_1 = \text{CONNit}(N_1), \dots, C_{s_F} = \text{CONNit}(N_{s_F})$  ορισμένων από αυτά με  $l^u < l$ . Κοινή είσοδος του πρωτοκόλλου και στα δύο συμβαλλόμενα μέρη είναι οι δεσμεύσεις  $C_1, \dots, C_{s_F}$  και τα μηνύματα  $N_{s_F+1}, \dots, N_s$ . Η είσοδος του υπογράφοντος είναι ένα κλειδί υπογραφής  $SK$ .

Η έξοδος του αιτούντος είναι μια υπογραφή  $S$  στα  $N_1, \dots, N_s$ . Μια εκτέλεση αυτού πρωτοκόλλου είναι η εξής  $S = \text{HiddenSign}(C_1, \dots, C_{s_F}, N_{s_F+1}, \dots, N_s; SK)$ . Χάριν της ιδιότητας απόκρυψης των δεσμεύσεων ο υπογράφων δεν μαθαίνει καμία πληροφορία για τα μηνύματα  $N_1, \dots, N_{s_F}$  κατά την εκτέλεση του πρωτοκόλλου **HiddenSign**.

### 6.3.1 SRSA ΣΧΕΔΙΑ ΥΠΟΓΡΑΦΩΝ & ΠΡΩΤΟΚΟΛΛΑ

Το πρώτο σχέδιο υπογραφών, κατάλληλο για τους σκοπούς μας προτάθηκε από τους Camenisch & Lysyanskaya. Θεμελιώθηκε πάνω στο ισχυρό (Strong) πρωτόκολλο RSA για αυτό και ονομάζεται **SRSA** σχέδιο υπογραφών. Παράλληλα με τους αλγόριθμους του σχεδίου υπογραφών θα παρουσιάσω και ορισμένα πρωτόκολλα με τα οποία ένας χρήστης μπορεί να αποκτήσει μια υπογραφή πάνω σε δεσμευμένα μηνύματα, καθώς και αποδείξεις γνώσης υπογραφής πάνω σε δεσμευμένα μηνύματα.

## Ανάλυση του σχεδίου υπογραφών

Έστω  $l_n, l_N$  nat  $l_e = l_N + 3$  παράμετροι και  $N_1, \dots, N_L : N_i \in \pm \{0,1\}^{S_N}$

ο χώρος μηνυμάτων .

## Δημιουργία Δημόσιου και Μυστικού Κλειδιού

Για είσοδο έναν δυαδικό αριθμό μήκους  $l_n, 1^{S_n}$ , επιλέγουμε ένα  $l_n$  δυαδικών ψηφίων RSA modulus  $n = e \cdot q$ , όπου τα  $e, q$  είναι πρώτοι αριθμοί  $e = 2 \cdot e^u + 1$ ,  $q = 2 \cdot q^u + 1$ .

Επιλέγουμε ομοιόμορφα, τυχαία  $S \in \mathbb{Q}R_n$  και  $R_1, \dots, R_L, Z \in \mathbb{R} < S >$ .

$SPK\{(q_1, \dots, q_L, \zeta): R_1 \equiv S^{q_1} \pmod{n} \dots \dots \dots R_L \equiv S^{q_L} \pmod{n} \text{ fl}$

$$Z \equiv S^{\zeta} \pmod{n}\}$$

Έτσι λοιπόν το μυστικό κλειδί είναι  $e$  και το δημόσιο κλειδί είναι  $(n, R_1, \dots, R_L, Z, l_N)$ .

## Αλγόριθμος Απόκτησης Υπογραφής

Με είσοδο ένα σύνολο μηνυμάτων  $N_1, \dots, N_L$  επιλέγουμε έναν τυχαίο πρώτο αριθμό  $e$  μήκους  $l_e = l_c + l_c + l_c + 1 > l_N + l_c + l_c + 3$  και έναν τυχαίο πρώτο αριθμό  $v$  μήκους  $l_v = l_n + l_N + l_r$  όπου  $l_r$  είναι μια παράμετρος ασφαλείας. Υπολογίζουμε την τιμή  $A$  έτσι ώστε  $Z \equiv R_1^{N_1} R_2^{N_2} \dots R_L^{N_L} S A^e \pmod{n}$ .

Η υπογραφή στο μήνυμα  $(N_1, \dots, N_L)$  αποτελείται από  $(e, A, v)$ .

## Αλγόριθμος Επαλήθευσης Υπογραφής

Ο αλγόριθμος επαλήθευσης πιστοποιεί ότι η τριπλέτα  $(e, A, u)$  αποτελεί υπογραφή πάνω στα μηνύματα  $(N_1, \dots, N_L)$  ελέγχοντας αν  $Z \equiv R_1^{N_1} R_2^{N_2} \dots R_L^{N_L} S A^e \pmod{n}$  και  $2^{S_e + S_c + S_c + 2} > e > 2^{S_e + S_c + S_c + 1}$ .

## Παρατήρηση

Επειδή το σχέδιο υπογραφών που περιέγραψα παραπάνω θεμελιώνεται στο ισχυρό RSA (Strong RSA) πρωτόκολλο, θα είναι ασφαλές απέναντι σε προσαρμοστικές επιθέσεις διότι είναι δύσκολο να υπολογιστούν δύο πρώτοι αριθμοί  $e, q$  τέτοιοι ώστε  $n = e \cdot q$ .

Το αρχικό σχέδιο θεωρεί μηνύματα στο διάστημα  $[0, 2^{S_N} - 1]$ . Ωστόσο θα θεωρήσουμε ένα ευρύτερο, συμμετρικό διάστημα  $[-2^{S_N} + 1, 2^{S_N} - 1]$ .

Αυτό όμως απαιτεί να ισχύει ότι η παράμετρος  $l_e > l_N + 2$  αντί για  $l_e > l_N + 1$  και  $e > 2^{S_e + S_c + S_c + 1}$  ενώ στο αρχικό σχέδιο ήταν αρκετό να ισχύει ότι  $e > 2^{S_e - 1}$ . Επίσης μετά από ανάλυση της ασφάλειας του σχεδίου αποδεικνύεται ότι αρκεί η παράμετρος  $v$  να επιλεγεί από το σύνολο  $Z_q$ .

Από την άλλη όμως αν κάποιος χρησιμοποιήσει αυτό το σχέδιο υπογραφών για να υπογράψει δεσμευμένα μηνύματα, τότε το  $v$  επιλέγεται από ένα ευρύτερο διάστημα έτσι ώστε αυτά τα μηνύματα να είναι στατιστικά «κρυφά».

Τέλος, πρέπει να σημειώσω ότι οι ενώ οι Camenisch & Lysyanskaya απαιτούν από τον υπογράφων να αποδείξει ότι το  $n$  είναι γινόμενο δύο ασφαλών πρώτων αριθμών προκειμένου να αποδείξει τη γνώση κάποιας υπογραφής<sup>11</sup>, στα βελτιωμένα πρωτόκολλα που θα αναλύσω ακολούθως ο υπογράφων πρέπει να αποδείξει μόνο ότι  $R_i, Z \in \langle S \rangle$ , το οποίο είναι σημαντικά πιο αποδοτικό.

## Απόκτηση υπογραφής σε δεσμευμένα μηνύματα

Έστω  $C_1 = g^{N_1} h^{r_1}$ ,  $C_2 = g^{N_2} h^{r_2}$ , ...,  $C_{L^F} = g^{N_{L^F}} h^{r_{L^F}}$  δεσμεύσεις στα μηνύματα  $N_1, N_2, \dots, N_{L^F}$  και έστω ότι τα μηνύματα  $N_{L^F+1}, N_{L^F+2}, \dots, N_L$  είναι γνωστά και πιθανά επιλεγμένα από τον υπογράφων. Για να αποκτήσει υπογραφή πάνω στα μηνύματα αυτά ο αποδέκτης της υπογραφής και ο υπογράφων εκτελούν το ακόλουθο πρωτόκολλο: Κοινή είσοδος και στα δύο συμβαλλόμενα μέρη είναι οι δεσμεύσεις των  $C_1, C_2, \dots, C_{L^F}$ , τα μηνύματα  $N_{L^F+1}, N_{L^F+2}, \dots, N_L$ , και το δημόσιο κλειδί  $(n, R_1, \dots, R_L, Z, l_N)$ .

<sup>11</sup> Με απόδειξη μηδενικής γνώσης

Μυστική είσοδος στον υπογράφων είναι τα  $e, q$  ενώ στον αποδέκτη της υπογραφής κρυφές παραμένουν οι ποσότητες  $N_1, N_2, N_3, \dots, N_{L^F}, r_1, r_2, r_3, \dots, r_{L^F}$ .

Και τα δύο μέρη εκτελούν τα ακόλουθα βήματα:

**Πρώτον**, ο αποδέκτης της υπογραφής επιλέγει ομοιόμορφα τυχαία ακέραιο αριθμό  $v^u$  που ανήκει στο διάστημα  $\{0,1\}^{S_n+S_c}$ , υπολογίζει

$$C := R_1^{N_1} R_2^{N_2} \dots R_{L^F}^{N_{L^F}} S^{v^F} \text{ Nod } n \text{ και στέλνει την ποσότητα } C \text{ ο δημιουργός της υπογραφής.}$$

**Δεύτερον**, ο αποδέκτης και ο δημιουργός της υπογραφής τρέχουν το ακόλουθο πρωτόκολλο :

$PK\{s, \mu_1, \mu_2, \dots, \mu_{L^F}, q_1, q_2, \dots, q_{L^F}\}$ :

$$C_1 = g^{\mu_1} h^{q_1} \wedge C_2 = g^{\mu_2} h^{q_2} \wedge \dots \wedge C_{L^F} = g^{\mu_{L^F}} h^{q_{L^F}},$$

$$\wedge C \equiv R_1^{N_1} R_2^{N_2} \dots R_{L^F}^{N_{L^F}} S^{v^F} \text{ Nod } n \wedge \mu_1, \mu_2, \dots, \mu_{L^F} \in \{0,1\}^{S_n+S_c+S_c}$$

**Τρίτον**, ο δημιουργός της υπογραφής επιλέγει τυχαία έναν  $l_e$  δυαδικών ψηφίων

ακέραιο αριθμό  $e^u$  τέτοιον ώστε ο αριθμός  $e := 2^{S_e+S_c+S_c+1} + e^u$  να είναι πρώτος

Επίσης επιλέγει τυχαίο  $u^w \in Z_q$ , και υπολογίζει  $A := \left( \frac{N_{L^F+1}^Z}{C R_{L^F+1}^{L^F+1} \dots R_L^{N_L} S^{v^{FF}}} \right)^{1/e} \text{ Nod } n$

και στέλνει το  $(e, A, v^u)$  στον αποδέκτη.

**Τέταρτον**, για να πείσει ο δημιουργός της υπογραφής ότι  $A \in < S >$  τρέχει το

ακόλουθο πρωτόκολλο απόδειξη γνώσης με τον αποδέκτη της υπογραφής

$$PK\{(\delta): A \equiv \pm \left( \frac{N_{L^F+1}^Z}{C R_{L^F+1}^{L^F+1} \dots R_L^{N_L} S^{v^{FF}}} \right)^\delta \text{ Nod } n \}$$

**Τέλος**, ο αποδέκτης της υπογραφής πιστοποιεί ότι ο αριθμός  $e > 2^{S_e+S_c+S_c+1}$  είναι

πρώτος και αποθηκεύει  $(A, e, u = u^u + u^w)$  σαν υπογραφή στο σύνολο μηνυμάτων

$N_1, \dots, N_L$ .

Εδώ ο δημιουργός της υπογραφής αποδεικνύει στον παραλήπτη της υπογραφής ότι το  $A \in \langle S \rangle$ . Αυτό είναι απαραίτητο για να πιστοποιήσουμε ότι ο παραλήπτης μπορεί με απόδειξη μηδενικής γνώσης, να αποδείξει ότι γνωρίζει την υπογραφή πάνω στα δεσμευμένα μηνύματα χωρίς να αποκαλύψει καμία πληροφορία για την υπογραφή ή τα μηνύματα αυτά.

### Απόδειξη γνώσης υπογραφής σε δεσμευμένα μηνύματα

Έστω  $C_1 = g^{N_1} h^{r_1}$ ,  $C_2 = g^{N_2} h^{r_2}$ , ...,  $C_{L^F} = g^{N_{L^F}} h^{r_{L^F}}$  δεσμεύσεις στα μηνύματα  $N_1, N_2, \dots, N_{L^F}$  τα οποία δεν αποκαλύπτονται στον επαληθευτή και έστω ότι τα μηνύματα  $N_{L^F+1}, N_{L^F+2}, \dots, N_L$  αποκαλύπτονται.

Έστω ότι η τριπλέτα  $(e, A, u)$  είναι η υπογραφή πάνω στα  $N_1, N_2, \dots, N_L$ ,  $L > L^u$ . Για να αποδείξει ότι γνωρίζει την υπογραφή αυτή, διατηρώντας κρυφά τα μηνύματα  $N_1, N_2, \dots, N_{L^F}$  ο αποδεικνύων και ο επαληθευτής εκτελούν το ακόλουθο πρωτόκολλο. Κοινή είσοδος στους δύο είναι  $C_1, C_2, C_3, \dots, C_{L^F}, N_{L^F+1}, N_{L^F+2}, \dots, N_L, (n, R_1, \dots, R_L, Z, l_N)$ . Μυστική είσοδος στον αποδεικνύων είναι  $N_1, N_2, \dots, N_{L^F}, r_1, r_2, r_3, \dots, r_{L^F}$  και η υπογραφή  $(e, A, u)$ .

Και οι δύο εκτελούν τα ακόλουθα βήματα:

1. Ο αποδεικνύων επιλέγει ομοιόμορφα τυχαία την τιμή  $r_e \in_R \{0,1\}^{s_n+s_c}$ , υπολογίζει την τιμή  $\tilde{A} := AS^A$  και την στέλνει στον επαληθευτή.

2. Και οι δύο εκτελούν την απόδειξη πρωτοκόλλου

$PK\{s, \mu_1, \mu_2, \dots, \mu_{L^F}, q_1, q_2, \dots, q_{L^F}, v\}$ :

$$C_1 = g^{\mu_1} h^{q_1} \wedge C_2 = g^{\mu_2} h^{q_2} \wedge \dots \wedge C_{L^F} = g^{\mu_{L^F}} h^{q_{L^F}}, \wedge$$

$$\frac{Z}{\tilde{A}^{2l_e+l_c+l_c+1} R_{L^F+1}^{N_{L^F+1}} \dots R_L^{N_L}} \equiv \tilde{A}^s R_1^{N_1} R_2^{N_2} \dots R_{L^F}^{N_{L^F}} S^v \text{ Mod } n$$

$$\wedge s \in \{0,1\}^{s_e+s_c+s_c} \wedge \mu_1, \mu_2, \dots, \mu_{L^F} \in \{0,1\}^{s_n+s_c+s_c}$$

### 6.3.2 Το σχέδιο υπογραφών των Camenisch & Lysyanskaya που βασίζεται στους διγραμμικούς γράφους

Ένα δεύτερο σχέδιο υπογραφών κατάλληλο για τους σκοπούς μας προτάθηκε από τους Camenisch & Lysyanskaya. Το **χώρο μηνυμάτων** του σχεδίου υπογραφών αποτελεί το σύνολο  $\{(N_1, N_2, \dots, N_L) : N_i \in Z_q\}$ .

#### Αλγόριθμος Δημιουργίας Κλειδιών SK και VK

Τρέχουμε τον αλγόριθμο BiLinMapSetup (βλ. Παράρτημα) για να δημιουργήσουμε

$(q, G, G, g, \mathbf{g}, e)$ . Επιλέγουμε  $x \in_R Z_q, y \in_R Z_q$ , και  $z_i \in_R Z_q$  για  $i = 1, 2, \dots, L$ . Έστω ότι  $X = g^x, Y = g^y$  και  $Z_i = g^{z_i}$  και  $W_i = g^{w_i}$  για  $i = 1, 2, \dots, L$ . Θέτουμε ως κλειδί υπογραφής  $SK = (x, y, z_1, \dots, z_L)$  και ως κλειδί επαλήθευσης υπογραφής την ποσότητα  $VK = (q, G, G, g, \mathbf{g}, e, X, Y, \{Z_i\}, \{W_i\})$ .

#### Αλγόριθμος υπογραφής μηνυμάτων

Σαν είσοδο στον αλγόριθμο δίνεται ένα σύνολο μηνυμάτων  $\{(N_1, N_2, \dots, N_L) : N_i \in Z_q\}$ , το μυστικό κλειδί  $SK = (x, y, z_1, \dots, z_L)$  και

δημόσιο κλειδί  $VK = (q, G, G, g, \mathbf{g}, e, X, Y, \{Z_i\}, \{W_i\})$ .

Για την ανάκτηση υπογραφής πάνω στο σύνολο των μηνυμάτων αυτών ακολουθούμε τα εξής βήματα:

1. Επιλέγουμε τυχαίο  $u \in_R Z_q$
2. Επιλέγουμε τυχαίο  $a \in_R G$
3. Θέτουμε  $A_i = a^{z_i}$  για  $1 \leq i \leq L$
4. Θέτουμε  $b = a^y, B_i = (A_i)^y$
5. Θέτουμε  $c = a^{s+syv} \prod_{i=1}^L (A_i)^{syN_i}$

Σαν έξοδο λαμβάνουμε την υπογραφή  $\sigma = (a, \{A_i\}, b, \{B_i\}, c, v)$

## Αλγόριθμος Επαλήθευσης Υπογραφής

Σαν είσοδο του αλγόριθμου δίνουμε το δημόσιο κλειδί

$VK = (q, G, G, g, g, e, X, Y, \{Z_i\}, \{W_i\})$ , το σύνολο των μηνυμάτων

$(N_1, N_2, \dots, N_L) \in Z_q$ , και την υπογραφή  $\sigma = (a, \{A_i\}, b, \{B_i\}, c, v)$ .

Για να ελέγξουμε την εγκυρότητα της υπογραφής εκτελούμε τα ακόλουθα βήματα :

1. Ελέγχουμε αν τα  $\{A_i\}$  δημιουργήθηκαν σωστά, ελέγχοντας αν ισχύει η ιδιότητα:

$$e(a, Z_i) = e(g, A_i)$$

2. Ελέγχουμε αν τα  $b$  και  $\{B_i\}$  δημιουργήθηκαν σωστά, ελέγχοντας αν :

$$e(a, Y) = e(g, b) \text{ και } e(A_i, Y) = e(g, B_i)$$

3. Ελέγχουμε αν το  $c$  δημιουργήθηκε σωστά, επαληθεύοντας τη σχέση :

$$e(X, a) \cdot e(X, b)^v \cdot \prod_{i=1}^L e(X, B_i)^{N_i} = e(g, c)$$

## Απόκτηση υπογραφής σε δεσμεύσεις μηνυμάτων

Έστω  $C_1 = g^{N_1} h^{r_1}$ ,  $C_2 = g^{N_2} h^{r_2}$ , ...,  $C_{L^F} = g^{N_{L^F}} h^{r_{L^F}}$  δεσμεύσεις στα μηνύματα  $N_1, N_2, \dots, N_{L^F}$  που επιλέγονται από τον παραλήπτη της υπογραφής και δεν αποκαλύπτονται στον υπογράφων. Έστω  $N_{L^F+1}, N_{L^F+2}, \dots, N_L$  τα υπόλοιπα μηνύματα τα οποία είναι γνωστά ή επιλεγμένα από τον υπογράφων.

Για να αποκτήσει ο παραλήπτης της υπογραφής, υπογραφή στα μηνύματα αυτά, εκτελεί με τον υπογράφων το ακόλουθο πρωτόκολλο:

Κοινή είσοδος και στις δύο πλευρές είναι οι δεσμεύσεις  $C_1, C_2, \dots,$

$C_{L^F}$ , τα μηνύματα  $N_{L^F+1}, N_{L^F+2}, \dots, N_L$ , και το δημόσιο κλειδί  $VK = (q, G, G, g, g, e, X, Y, \{Z_i\}, \{W_i\})$ . Μυστική είσοδος στον υπογράφων είναι το μυστικό κλειδί

$SK = (x, y, z_1, \dots, z_L)$  ενώ στον αποδέκτη της υπογραφής κρυφές παραμένουν οι ποσότητες  $N_1, N_2, N_3, \dots, N_{L^F}, r_1, r_2, r_3, \dots, r_{L^F}$ .



Και τα δύο μέρη εκτελούν τα ακόλουθα βήματα:

1.Ο παραλήπτης επιλέγει τυχαίο  $u \in_R \mathbb{Z}_q$  και υπολογίζει την ποσότητα

$M_i = g^v \prod_{i=1}^L Z_i^{N_i}$  και ο χρήστης εκτελεί μια απόδειξη μηδενικής γνώσης ότι το σύνολο  $M$  περιέχει τα ίδια μηνύματα όπως οι δεσμεύσεις  $C_1, C_2, \dots, C_{L^F}$ .

PK  $\{(v, q_1, q_2, \dots, q_{L^F}, \mu_1, \mu_2, \dots, \mu_{L^F})$ :

$$C_1 = g^{\mu_1} h^{q_1} \wedge C_2 = g^{\mu_2} h^{q_2} \wedge \dots \wedge C_{L^F} = g^{\mu_{L^F}} h^{q_{L^F}}$$

$$\wedge M = g^v \prod_{i=1}^{L^F} Z_i^{\mu_i}$$

2. (a) Ο υπογράφων επιλέγει τυχαίο  $a \in_R \mathbb{Z}_q$  και υπολογίζει την ποσότητα  $a = g^a$ .

(b) Για  $1 \leq i \leq L$ , έστω ότι  $A_i = a^{z_i}$ , θέτει  $b = a^y$  και έστω  $B_i = A_i^y$

(c) Θέτει  $c = a^s M^{asy}$  και

(d) Στέλνει στον παραλήπτη τις τιμές  $(a, \{A_i\}, b, \{B_i\}, c)$

3.Ο παραλήπτης αποθηκεύει την υπογραφή  $\sigma = (a, \{A_i\}, b, \{B_i\}, c, v)$

### **Απόδειξη γνώσης υπογραφής σε δεσμευμένα μηνύματα**

Έστω  $C_1 = g^{N_1} h^{r_1}, C_2 = g^{N_2} h^{r_2}, \dots, C_{L^F} = g^{N_{L^F}} h^{r_{L^F}}$  οι δεσμεύσεις στα μηνύματα  $N_1, N_2, \dots, N_{L^F}$  τα οποία δεν αποκαλύπτονται στον επαληθευτή και έστω ότι τα υπόλοιπα μηνύματα  $N_{L^F+1}, N_{L^F+2}, \dots, N_L$  αποκαλύπτονται στον επαληθευτή. Έστω  $(a, \{A_i\}, b, \{B_i\}, c, v)$  η υπογραφή στα μηνύματα  $N_1, N_2, \dots, N_{L^F}$  όπου  $L^u \leq L$ .

Για να αποδείξει γνώση αυτής της υπογραφής, διατηρώντας «μυστικά» τα μηνύματα  $N_1, N_2, \dots, N_{L^F}$ , ο χρήστης-αποδεικνύων και ο επαληθευτής εκτελούν το ακόλουθο πρωτόκολλο.

Κοινή είσοδος και στα δύο μέρη είναι οι ποσότητες  $C_1, C_2, \dots, C_{L^F}, N_{L^F+1}, N_{L^F+2}, \dots, N_L$ , η παράμετρος ασφαλείας  $l_N$  και το κλειδί επαλήθευσης  $(q, G, G, g, g, e, X, Y, \{Z_i\}, \{W_i\})$ . Μυστική είσοδος στον χρήστη είναι οι ποσότητες  $r_1, r_2, r_3, \dots, r_{L^F}$  και η υπογραφή  $(a, \{A_i\}, b, \{B_i\}, c, v)$ .

## Βήματα Πρωτοκόλλου

1. Ο αποδεικνύων υπολογίζει μια «τυφλωμένη» έκδοση της υπογραφή του,  $\sigma$  :  
επιλέγει τυχαία  $r, r^u \in \mathbb{Z}_q$  και σχηματίζει την υπογραφή  $\tilde{a} = (\tilde{a}, \{\tilde{A}_i\}, \tilde{b}, \{\tilde{B}_i\}, \tilde{c})$  ως εξής:

$$\tilde{a} = a^r, \tilde{b} = b^r, \tilde{c} = c^r, \tilde{A}_i = A_i^r, \tilde{B}_i = B_i^r \text{ για } i = 1, 2, \dots, L$$

Επιπλέον, τυφλώνει το  $\tilde{c}$  για να αποκτήσει την τιμή  $\hat{c}$  η οποία είναι ανεξάρτητα κατανεμημένη από οτιδήποτε άλλο και ορίζεται ως  $\hat{c} = \tilde{c}^{r^F}$ . Έπειτα στέλνει  $\mathfrak{w}$  επαληθευτή την ποσότητα  $\tilde{a} = (\tilde{a}, \{\tilde{A}_i\}, \tilde{b}, \{\tilde{B}_i\}, \tilde{c})$ .

2. Έστω  $v_s = e(X, \tilde{a}), v_y = e(X, \tilde{b}), v_{(sy,i)} = e(X, \tilde{B}_i)$  και  $v_c = e(g, \hat{c})$ .

Ο αποδεικνύων και ο επαληθευτής υπολογίζουν τοπικά τις προηγούμενες τιμές και εκτελούν το ακόλουθο πρωτόκολλο απόδειξης μηδενικής γνώσης:

$PK\{(s, q_1, q_2, \dots, q_{L^F}, \mu_1, \mu_2, \dots, \mu_{L^F}, v, q)\}$ :

$$C_1 = g^{\mu_1} h^{q_1} \wedge C_2 = g^{\mu_2} h^{q_2} \wedge \dots \wedge C_{L^F} = g^{\mu_{L^F}} h^{q_{L^F}}$$

$$\bigwedge_{s, i=L^F+1}^{L^F} (V_{(sy,i)})^{-N_i} = v^{-q} v^v \prod_{sy, i=1}^{L^F} (V_{(sy,i)})^{-\mu_i} \}$$

Ο επαληθευτής αποδέχεται αν επαληθευτεί η παραπάνω απόδειξη και επιπλέον αν τα  $\{\tilde{A}_i\}, \{\tilde{B}_i\}$  έχουν διαμορφωθεί σωστά. Για να διαπιστώσει ότι το  $\{\tilde{A}_i\}$  έχει διαμορφωθεί σωστά ελέγχει αν ικανοποιείται η ισότητα  $e(\tilde{a}, Z_i) = e(g, \tilde{A}_i)$ , και για το  $\{\tilde{B}_i\}$  ελέγχει : αν ικανοποιούνται οι σχέσεις  $e(\tilde{a}, Y) = e(g, \tilde{b})$  και  $e(\tilde{A}_i, Y) = e(g, \{\tilde{B}_i\})$ .

## 6.4 Οι κρυπτογραφικές αρχές στην πράξη

Στην ενότητα αυτή θα δούμε πως οι κρυπτογραφικές δομικές μονάδες που παρουσιάσαμε παραπάνω υλοποιούνται στην πράξη.

Ας υποθέσουμε ότι υπάρχουν δύο εκδότες πιστοποιητικών τους οποίους συμβολίζω με  $I_1$  και  $I_2$  αντίστοιχα. Ο καθένας από αυτούς έχει δημιουργήσει ένα ζεύγος κλειδιών  $(VK_1, SK_1)$  και  $(VK_2, SK_2)$  αντίστοιχα. Τα κλειδιά  $SK_1, SK_2$  λέγονται κλειδιά υπογραφής και χρησιμεύουν στο να υπογράψουν ψηφιακά τα πιστοποιητικά τα οποία εκδίδουν. Από την άλλη τα κλειδιά  $VK_1, VK_2$  χρησιμεύουν στο να επαληθεύουν οι εκδότες την εγκυρότητα υπογραφών άλλων πιστοποιητικών τα οποία ο χρήστης καταθέτει προκειμένου ο εκδότης να του εκδώσει ένα συγκεκριμένο τύπο πιστοποιητικού. Τα κλειδιά επαλήθευσης  $VK_1, VK_2$  κοινοποιούνται σε έναν δημόσιο φάκελο αφού ελεγχθεί η εγκυρότητα τους.

Έστω  $Cert_1 = \text{Sign}(N_1, N_2, \dots, N_{s_1}, SK_1)$  το πιστοποιητικό από τον εκδότη  $I_1$  το οποίο ουσιαστικά προκύπτει από την εκτέλεση του αλγορίθμου **Sign** του σχεδίου υπογραφών. Αντίστοιχα  $Cert_2 = \text{Sign}(N_1, N_2, \dots, N_{s_2}, SK_2)$  το πιστοποιητικό από τον εκδότη  $I_2$ .

Η βασική ιδέα για την υπό έλεγχο παρουσίαση ενός πιστοποιητικού είναι, ο χρήστης μέσω αποδείξεων μηδενικής γνώσης να πιστοποιήσει την εγκυρότητα των στοιχείων που κωδικοποιούνται στο πιστοποιητικό του χωρίς να αποκαλύψει τίποτα για τα στοιχεία αυτά.

Συγκεκριμένα, για να παρουσιάσει το πιστοποιητικό  $Cert_1$  στον επαληθευτή χωρίς για παράδειγμα να αποκαλύψει τα στοιχεία  $N_1, N_2, \dots, N_{s_1}$  όπου  $1 \leq s_1$ , ο χρήστης σαν αποδεικνύων και ο επαληθευτής του πιστοποιητικού εκτελούν το ακόλουθο πρωτόκολλο:

PK  $\{(Cert_1, N_1, N_2, \dots, N_{s_1})$ :

$$\text{VerifySign}(Cert_1, N_1, N_2, \dots, N_{s_1}, N_{s_1+1}, N_{s_1+2}, \dots, N_{s_1}; VK_1) = 1\} \quad (1)$$

Το πρωτόκολλο (1) αποδεικνύει ότι ο χρήστης γνωρίζει ένα έγκυρο πιστοποιητικό ως προς το κλειδί  $VK_1$ . Σύμφωνα με την ιδιότητα του πρωτοκόλλου απόδειξης μηδενικής γνώσης ο επαληθευτής δεν λαμβάνει καμία πληροφορία για το πιστοποιητικό  $Cert_1$  και για τα στοιχεία  $N_1, N_2, \dots, N_{s_1}^F$ . Μετά από παρατήρηση προκύπτει ότι πολλαπλές παρουσιάσεις του ίδιου πιστοποιητικού, εν προκειμένω του  $Cert_1$ , χρησιμοποιώντας το πρωτόκολλο (1) δεν είναι συνδέσιμες αν τα στοιχεία  $N_{s_1^F+1}^F, N_{s_1^F+2}^F, \dots, N_{s_1}^F$  που περιλαμβάνονται στο πιστοποιητικό και αποκαλύπτονται στον επαληθευτή δεν είναι συνδέσιμα. Δηλαδή αν σε κάθε διαφορετική παρουσίαση του ίδιου πιστοποιητικού αποκαλύπτεται και ένα διαφορετικό στοιχείο από τα  $N_{s_1^F+1}^F, N_{s_1^F+2}^F, \dots, N_{s_1}^F$ .

Πέραν από την έννοια της μη συνδεσιμότητας των διαφορετικών παρουσιάσεων του ίδιου πιστοποιητικού, μας ενδιαφέρει να αποδείξουμε σχέσεις μεταξύ των στοιχείων διαφορετικών πιστοποιητικών. Ας υποθέσουμε ότι θέλουμε να αποδείξουμε σχέσεις μεταξύ των πιστοποιητικών  $Cert_1$  και  $Cert_2$ . Για να το πετύχουμε αυτό εκτελούμε το ακόλουθο πρωτόκολλο :

$$PK\{(Cert_1, N_1, N_2, \dots, N_{s_1}^F, Cert_2, \tilde{N}_1, \tilde{N}_2, \dots, \tilde{N}_{s_2}^F):$$

$$VerifySign(Cert_1, N_1, N_2, \dots, N_{s_1}^F, N_{s_1^F+1}^F, N_{s_1^F+2}^F, \dots, N_{s_1}^F; VK_1) = 1$$

$$\wedge VerifySign(Cert_2, \tilde{N}_1, \tilde{N}_2, \dots, \tilde{N}_{s_2}^F, \tilde{N}_{s_2^F+1}^F, \tilde{N}_{s_2^F+2}^F, \dots, \tilde{N}_{s_2}^F; VK_2) = 1\} \quad (2)$$

Χρησιμοποιώντας το πρωτόκολλο (2) κάποιος χρήστης μπορεί να αποδείξει ότι κατέχει ένα πιστοποιητικό  $Cert_1$  από τον εκδότη  $I_1$  και ένα πιστοποιητικό  $Cert_2$ . Επιπλέον, αποδεικνύει ότι τα πρώτα στοιχεία  $N_1, \tilde{N}_1$  των δύο πιστοποιητικών είναι ίσα. Ακόμα, από την ιδιότητα της απόδειξης μηδενικής γνώσης ο επαληθευτής δεν μαθαίνει καμία πληροφορία για τα στοιχεία των πιστοποιητικών.

Συνεπώς, βλέπουμε ότι για να αποδείξουμε σχέσεις μεταξύ των στοιχείων πιστοποιητικών χρησιμοποιούμε τεχνικές όπως είναι η ισότητα μεταξύ στοιχείων ώστε να αποδείξουμε γνώση των σχέσεων αυτών.

Σε μια υπό όρους παρουσίαση των στοιχείων ενός πιστοποιητικού υποθέτουμε ότι υπάρχει και μια τρίτη οντότητα. Χρησιμοποιώντας τον αλγόριθμο **SetUeEnc** η οντότητα αυτή δημιουργεί ένα κλειδί κρυπτογράφησης **EK** και ένα κλειδί αποκρυπτογράφησης **DK**. Το κλειδί **EK** γίνεται δημόσια γνωστό και πιστοποιείται η εγκυρότητα του. Ο χρήστης για να παρουσιάσει υπό όρους το στοιχείο **N<sub>1</sub>** που περιέχεται στο πιστοποιητικό **Cert<sub>1</sub>**, αρχικά, υπό έναν όρο που σημειώνεται στην ετικέτα **Cond** χρησιμοποιώντας το κλειδί κρυπτογράφησης **EK**, δημιουργεί το κρυπτογράφημα **E = Enc(N<sub>1</sub>, Cond; EK)** του **N<sub>1</sub>**. Ουσιαστικά η ετικέτα **Cond** περιγράφει υπό ποιες συνθήκες μπορεί να αποκαλυφθεί η τιμή του **N<sub>1</sub>** στον επαληθευτή του πιστοποιητικού. Ο κάτοχος και αντίστοιχα ο επαληθευτής του πιστοποιητικού εκτελούν το ακόλουθο πρωτόκολλο.

**PK{(Cert<sub>1</sub>, N<sub>1</sub>, N<sub>2</sub>, ..., N<sub>S<sub>F</sub>})</sub>**:

$$\text{VerifySign}(\text{Cert}_1, N_1, N_2, \dots, N_{S_F}, N_{S_F+1}, N_{S_F+2}, \dots, N_{S_1}; VK_1) = 1$$

$$\text{fl } E = \text{Enc}(N_1, \text{Cond}; EK) \} \quad (3)$$

Μέσω του πρωτοκόλλου (3) ο χρήστης όχι μόνο παρουσιάζει το πιστοποιητικό του στον επαληθευτή αλλά παράλληλα αποδεικνύει ότι το **E** αποτελεί κρυπτογράφημα του πρώτου στοιχείου που περιέχεται στο πιστοποιητικό υπό το κλειδί **EK**. Ένα τέτοιο πρωτόκολλο ονομάζεται επαληθεύσιμη κρυπτογράφηση.

Από την ιδιότητα της απόδειξης μηδενικής γνώσης και την ιδιότητα της ασφάλειας του σχεδίου κρυπτογράφησης, συμπεραίνουμε ότι ο επαληθευτής δεν μαθαίνει καμία πληροφορία υπολογισμού της τιμής που κρυπτογραφείται υπό το κλειδί **EK**.

Για να λάβει το στοιχείο **N<sub>1</sub>**, ο επαληθευτής στέλνει το κρυπτογράφημα **E** και τον όρο **Cond** στην Τρίτη οντότητα. Η Τρίτη οντότητα ελέγχει αν ικανοποιείται ο συμφωνηθείς όρος, και αν ναι, επιστρέφει την αποκρυπτογράφιση του **E**, δηλαδή το **N<sub>1</sub>** στον επαληθευτή. Εδώ πρέπει να σημειώσω ότι για λόγους ασφάλειας η Τρίτη οντότητα δεν μπορεί παραπλανηθεί και να αποκρυπτογραφήσει το **E**, αν δεν ικανοποιείται ο συμφωνηθείς όρος που περιέχεται στην ετικέτα **Cond**.

Τέλος θα δούμε την έννοια της τυφλής πιστοποίησης. Ας , υποθέσουμε ότι ο χρήστης έχει λάβει ένα ακόμα πιστοποιητικό  $Cert_3$  πάνω στα στοιχεία  $N_1$  και  $N^u$ , από τον εκδότη  $I_2$  χωρίς να αποκαλύψει το  $N_1$  στον εκδότη του πιστοποιητικού , ενώ ο εκδότης  $I_2$  μπορεί να βεβαιωθεί ότι το στοιχείο  $N_1$  έχει πιστοποιηθεί από τον εκδότη  $I_1$ . Το στοιχείο  $N^u$  δεν αποκαλύπτεται στον εκδότη  $I_2$ . Καλούμε το πιστοποιητικό  $Cert_1 = \text{Sign}(N_1, \dots, N_{s_1}; SK_1)$  . Ο χρήστης δεν χρησιμοποιεί άμεσα το  $N_1$  , αλλά τη δέσμευση  $C = \text{Connit}(N_1, r)$  . Έπειτα , ο χρήστης και ο εκδότης ο οποίος παίζει το ρόλο του επαληθευτή εκτελούν το πρωτόκολλο.

$PK\{(Cert_1, N_1, N_2, \dots, N_{s_F}):$

$$\text{VerifySign}(Cert_1, N_1, N_2, \dots, N_{s_F}, N_{s_F+1}, N_{s_F+2}, \dots, N_{s_1}, VK_1) = 1$$

$$\wedge C = \text{Connit}(N_1, r)\} \quad (4)$$

Μέσω του πρωτοκόλλου (4) ο χρήστης αποδεικνύει στον εκδότη ότι το  $C$  αποτελεί δέσμευση του πρώτου στοιχείου που περιέχεται στο πιστοποιητικό  $Cert_1$  το οποίο εκδόθηκε από τον  $I_1$  . Από την ιδιότητα της απόδειξης μηδενικής γνώσης και την ιδιότητα της απόκρυψης του σχεδίου δέσμευσης , ο εκδότης  $I_2$  του πιστοποιητικού  $Cert_3$  δεν λαμβάνει καμία πληροφορία που θα διευκολύνει τον τρόπο υπολογισμού του  $N^u$  .

Εφόσον , ο εκδότης αποδεχθεί το πρωτόκολλο (4) , που σημαίνει ότι είναι βέβαιος ότι ο συγκεκριμένος χρήστης είναι ο κάτοχος του συγκεκριμένου πιστοποιητικού  $Cert_1$ , εκδίδει το πιστοποιητικό  $Cert_3$  πάνω στο στοιχείο  $N^u$  και αποκρύπτει το  $N_1$  , χρησιμοποιώντας το πρωτόκολλο  $Cert_3 = \text{HiddenSign}(C, N^u; SK_2)$  (5). Εδώ είναι σημαντικό να σημειώσω ότι το  $C$  είναι η ίδια δέσμευση που χρησιμοποιείται στο πρωτόκολλο (4).

Τώρα , από τις ιδιότητες του αλγόριθμου  $\text{HiddenSign}$  ο εκδότης δεν μαθαίνει καμία πληροφορία για το  $N_1$ . Τέλος , ο εκδότης για να ελέγξει την ορθότητα του πιστοποιητικού  $Cert_3$  ελέγχει αν  $\text{VerifySign}(N_1, N^u; SK_2) = 1$  .

## Κεφάλαιο 7: Εφαρμογές

Θα δούμε πως μπορεί να υλοποιηθεί ένα σύστημα ανώνυμων πιστοποιητικών με δυνατότητα ανάκλησης της ανωνυμίας των χρηστών και ένα σύστημα ηλεκτρονικών συναλλαγών (e-cash ) με offline ελέγχους διπλής χρήσης πιστοποιητικών , χρησιμοποιώντας τις τεχνικές που ανάλυσα παραπάνω.

### 7.1 Το σύστημα ανώνυμου πιστοποιητικού

Κάθε χρήστης στο σύστημα έχει ένα μοναδικό ID που το γνωρίζει μόνο αυτός. Ένα πιστοποιητικό από έναν οργανισμό είναι απλά μια πιστοποίηση στο ID του εκάστοτε χρήστη , το οποίο εκδίδεται από τον οργανισμό. Τα πιστοποιητικά παρουσιάζονται μέσω πρωτοκόλλων με τρόπο που το ID του χρήστη δεν αποκαλύπτεται στον επαληθευτή του πιστοποιητικού. Τα πιστοποιητικά εκδίδονται χρησιμοποιώντας την τυφλή πιστοποίηση έτσι ώστε η ταυτότητα του χρήστη δεν αποκαλύπτεται στον εκδίδοντα οργανισμό.

Η μη πλαστογράφηση των πιστοποιητικών προκύπτει από την ιδιότητα της μη πλαστογράφησης του σχεδίου υπογραφών που χρησιμοποιείται για την τυφλή πιστοποίηση . Ένα σύστημα πιστοποιητικού καλείται συνεκτικό , εάν είναι αδύνατο για διαφορετικούς χρήστες να συνεργαστούν και να παρουσιάσουν μερικά από τα πιστοποιητικά τους σε έναν οργανισμό και να λάβουν ένα πιστοποιητικό για έναν χρήστη που από μόνος του δεν θα είχε πάρει .Επιτυγχάνουμε τη συνοχή ως εξής. Όταν ο χρήστης παρουσιάζει πολλαπλά πιστοποιητικά από διαφορετικούς οργανισμούς αποδεικνύει ότι το ίδιο ID κρύβεται κάτω από όλα τα πιστοποιητικά που παρουσιάζονται, δηλαδή ότι τα πιστοποιητικά ανήκουν στον ίδιο χρήστη.

Κατά την έκδοση πιστοποιητικού , ο εκδότης βεβαιώνει ότι το ID που υπογράφει χωρίς να γνωρίζει είναι το ίδιο όπως στα πιστοποιητικά που ο χρήστης κατέχει. Αυτό μπορεί να επιτυγχάνεται χρησιμοποιώντας τα πρωτόκολλα τυφλής πιστοποίησης .Τα πιστοποιητικά μπορούν να έχουν και ιδιότητες όπως ημερομηνία λήξης , η ηλικία χρηστών πέραν από το ID του χρήστη. Κατά την παρουσίαση του πιστοποιητικού, ο χρήστης μπορεί να επιλέξει ποια χαρακτηριστικά επιθυμεί να αποδείξει ότι γνωρίζει, και τι να αποδείξει για αυτά .

Για παράδειγμα, κατά την παρουσίαση ενός πιστοποιητικού που έχει ημερομηνία λήξης 2002/05/19, ηλικία χρήστη 55 ετών μπορεί να αποφασίσει να αποδείξει μόνο ότι είναι ενήλικας και όχι την ακριβή του ηλικία. Τα χαρακτηριστικά του πιστοποιητικού υλοποιούνται με την προσθήκη στοιχείων πέραν από το ID του χρήστη. Κατά την παρουσίαση πιστοποιητικών, ο χρήστης μπορεί αποφασίσει ποιες πληροφορίες αποκαλύπτει για τα χαρακτηριστικά χρησιμοποιώντας τεχνικές επιλεκτικής παρουσίασης. Σε πολλές εφαρμογές πιστοποιητικών η ανωνυμία του χρήστη μπορεί να ανακληθεί χρησιμοποιώντας τις υπό όρους τεχνικές παρουσίασης με υπό όρους αποκάλυψη της ταυτότητας του χρήστη.

## 7.2 Ανώνυμο E-cash

Στην ενότητα αυτή θα μελετήσουμε τη λειτουργία του συστήματος ανώνυμων ηλεκτρονικών συναλλαγών. Ένα τέτοιο σύστημα αποτελείται από τράπεζες που εκδίδουν ηλεκτρονικά νομίσματα τα οποία οι χρήστες ξοδεύουν σε καταστήματα τα οποία με τη σειρά τους καταθέτουν τα νομίσματα αυτά σε τράπεζες.

Το **e-coin** δεν είναι παρά ένα πιστοποιητικό που εκδίδεται από την τράπεζα. Για να ανακτήσει ένα e-coin ο χρήστης αρχικά πιστοποιεί ότι είναι έγκυρος και τότε η τράπεζα ορίζει έναν μοναδικό ID στο χρήστη. Ο χρήστης επιλέγει κρυφά έναν τυχαίο σειριακό αριθμό  $s$  και έναν τυχαίο (στα τυφλά) αριθμό  $b$ . Η τράπεζα εκδίδει το πιστοποιητικό  $Cert_{ecoin}$  στα συγκεκριμένα ID,  $s$ , και  $b$  χρησιμοποιώντας την τυφλή πιστοποίηση. Δηλαδή δεν μαθαίνει τις τιμές των  $s$  και  $b$ . Σε ένα κατάστημα ο χρήστης για να ξοδέψει τα ηλεκτρονικά νομίσματα χρησιμοποιεί το πιστοποιητικό  $Cert_{ecoin}$ . Το κατάστημα επιλέγει μια τυχαία πρόκληση  $c$  ακέραιου τύπου και ο χρήστης υπολογίζει ένα  $u$  σύμφωνα με τη σχέση  $u = ID \cdot c + b$  και χρησιμοποιεί μια παραλλαγή του πρωτοκόλλου επιλεκτικής παρουσίασης.

$$PK\{ (Cert_{ecoin}, ID, b, ID^u, b^u) : VerifySign(Cert_{ecoin}, ID, b; VK) = 1 \wedge u = (ID^u \cdot c + b^u) \wedge u = (ID \cdot c + b) \wedge ID = ID^u \wedge b = b^u \}$$

Το VK αποτελεί το κλειδί επαλήθευσης υπογραφής της τράπεζας. Όπως φαίνεται, το κατάστημα δεν μαθαίνει την τιμή του  $s$  στην απόδειξη (6). Εδώ επιπλέον η απόδειξη (6) μπορεί να πραγματοποιηθεί μη-αλληλεπιδραστικά, δηλαδή, αυτό μπορεί να αντιπροσωπευθεί σε σχέση με το αλφαριθμητικό  $\Pi$  που στέλνεται από τον χρήστη στο κατάστημα.



Μια τέτοια μη-αλληλεπιδραστική απόδειξη μπορεί να επικυρωθεί από το κατάστημα με την εφαρμογή ενός κατάλληλου αλγορίθμου επαλήθευσης. Επίσης, κατά αναλογία με την ιδιότητα μηδενικής γνώσης των αλληλεπιδραστικών αποδείξεων, μια μη-αλληλεπιδραστική απόδειξη δεν αποκαλύπτει καμία (υπολογιστική) πληροφορία για τα  $\text{Cert}_{\text{ecoin}}$ ,  $\text{ID}$ , και  $b$ . Για να καταθέσει το *e-coin* το κατάστημα στέλνει  $(c, s, u, \Pi)$  στην τράπεζα. Η τράπεζα επαληθεύει αρχικά τη μη-αλληλεπιδραστική απόδειξη  $\Pi$  για να δει εάν τα  $(c, s, u)$  αντιστοιχεί σε ένα έγκυρο *e-coin*.

Σε περίπτωση διπλής χρήσης του πιστοποιητικού η τράπεζα μπορεί να ανακτήσει την ταυτότητα του χρήστη ως εξής. Η τράπεζα ελέγχει εάν ήδη υπάρχει ένα *e-coin* με αριθμό  $s$  στη βάση δεδομένων των ήδη κατατεθειμένων *e-coins*. Σε αυτή την περίπτωση, ανακτά το αντίστοιχο  $(c^u, s, u^u, M^u)$ . Μπορούμε με ασφάλεια να υποθέσουμε ότι  $c \neq c^u$ , και επίσης υπενθυμίζουμε ότι από την απόδειξη (6) η εγκυρότητα του  $\Pi$  βεβαιώνει ότι  $u = \text{ID} \cdot c + b$  και  $u^u = \text{ID} \cdot c^u + b$ . Επομένως από τις τιμές των  $u, u^u, c$  και  $c^u$  η τράπεζα μπορεί να υπολογίσει την ταυτότητα του χρήστη από τη σχέση  $\text{ID} = \frac{(u - u^F)}{(c - c^F)}$ . Οι μη αλληλεπιδραστικές αποδείξεις

απαιτούνται για να μπορεί να ελέγχει η τράπεζα την ορθότητα της απόδειξης (6) και για να εξασφαλίσει ότι υπολογίζει σωστά την ταυτότητα ενός χρήστη ο οποίος δίνει ψευδή στοιχεία για την ταυτότητα του.

## Παράρτημα

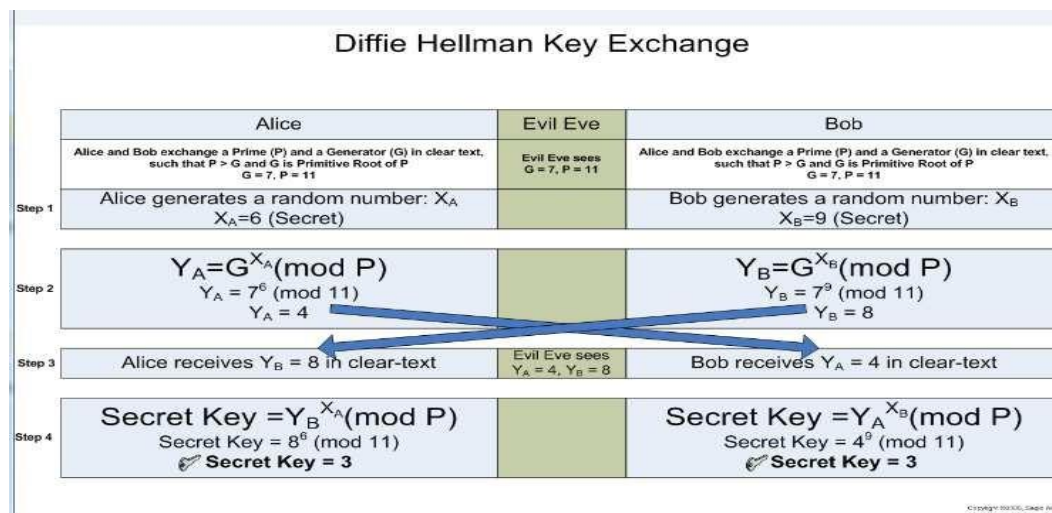
### 1.Πρωτόκολλο δημόσιου κλειδιού RSA

Βασίζεται στην ευκολία εύρεσης μεγάλων πρώτων αριθμών και τη δυσκολία παραγοντοποίησης του γινομένου σε δύο μεγάλους πρώτους αριθμούς

Κάθε χρήστης δημιουργεί το δημόσιο (public key) και το μυστικό κλειδί(secret key) με την ακόλουθη διαδικασία :

1. Επιλέγει τυχαία 2 μεγάλους πρώτους αριθμούς  $p$  και  $q$  έτσι ώστε  $p \neq q$ .
2. Υπολογίζει το  $n=p*q$
3. Επιλέγει έναν μικρό περιττό ακέραιο  $e$  ο οποίος είναι σχετικά πρώτος<sup>12</sup> με το  $\phi(n)$ , το οποίο ισούται με  $(p-1)*(q-1)$
4. Υπολογίζει το  $d$ , το οποίο είναι το πολλαπλασιαστικό αντίστροφο<sup>13</sup> του  $e$  modulo  $\phi(n)$  το οποίο υπάρχει και είναι μοναδικό.
5. Δημοσιοποιεί το ζεύγος  $P=(e, n)$  το οποίο είναι το δημόσιο RSA κλειδί του.
6. Κρατά μυστικό το ζεύγος  $S=(d, n)$  το οποίο είναι το μυστικό RSA κλειδί του

### 2.Πρωτόκολλο Diffie-Hellman (βασίζεται στον διακριτό λογάριθμο)



Σχήμα 21. Πρωτόκολλο ανταλλαγής κλειδιού Diffie Hellman

<sup>12</sup> Δύο ακέραιοι  $a, b$  είναι σχετικά πρώτοι αν ο μοναδικός κοινός τους διαιρέτης είναι το 1

<sup>13</sup> Για κάθε  $n > 1$  αν  $\gcd(a, n) = 1$  η εξίσωση  $a*x = 1 \pmod{n}$  έχει μοναδική λύση

### Πρόβλημα Διακριτού Λογαρίθμου

Έστω  $F_p$  πεπερασμένο σώμα και  $p$  πρώτος αριθμός.

Αν  $g, x, y$  στοιχεία του που ικανοποιούν την εξίσωση :

$$g^x = y$$

Τότε το πρόβλημα του διακριτού λογαρίθμου είναι η εύρεση της τιμής του  $x$  αν τα άλλα 2 στοιχεία είναι γνωστά.

### Σχήμα 22. Πρόβλημα διακριτού λογάριθμου

Το πρωτόκολλο ανταλλαγής κλειδιών των Diffie και Hellman (1976) είναι το πρώτο ασύμμετρο πρωτόκολλο εδραίωσης κλειδιού και η ασφάλειά του συνδέεται με το πρόβλημα του διακριτού λογαρίθμου. Πιστοποιεί ότι ένα δημόσιο κλειδί ανήκει σε κάποια οντότητα. Το πρωτόκολλο των Diffie και Hellman είναι σχετικά απλό στην περιγραφή. Η Alice και ο Bob επιλέγουν δημόσια έναν πρώτο αριθμό  $P$  και έναν γεννήτορα  $G$ . Στη συνέχεια επιλέγουν χωριστά από έναν κρυφό τυχαίο ακέραιο  $X_a$  και  $X_b$  αντίστοιχα, όπου  $0 < X_a, X_b < P-1$  και εκτελούν το πρωτόκολλο φαίνεται στο προηγούμενο σχήμα.

### Κώδικας υλοποίησης πρωτοκόλλου Diffie-Hellman σε JAVA

```
import java.math.BigInteger;

import java.security.*;

import java.security.spec.*;

import java.security.interfaces.*;

/*

 * A simple test program about a Diffie-Hellman Protocol between Bob and Alice .

 */

public class DH

{

    public static void main(String[] args) {

        try {
```

```

long start, end, total;

long Average_Time;

long total1=0;

int          i;

for(i=0;i<1000;i++){

start = System.currentTimeMillis();

/***** generate parameters P & G*****/

int bitLength =512;

SecureRandom rnd = new SecureRandom();//generate a random number

System.out.println("BitLength : " + bitLength);

BigInteger P = BigInteger.probablePrime(bitLength,rnd);//generate prime
number P

//A number is prime if it is divisible by 1 and the number itself and no other
number.

BigInteger G ;

float c;

// base G should be less than prime modulus P , c=0 if P=G ,c=-1 if P<G and c=1
if P>G

do{

G = new BigInteger(bitLength,rnd);

c=P.compareTo(G);

}while(c!= 1);//generate G ,while P<G or P=G generate new G until P>G

BigInteger Xa ,Xb;

do{

//Alice Private Value

Xa = new BigInteger(bitLength,rnd);

}while( Xa.compareTo(P.subtract(BigInteger.ONE))!=-1) ;//Xa should be in
interval 0<Xa<P-1

```

```

do{

    //Bob Private Value

    Xb = new BigInteger(bitLength,rnd);

    }while( Xb.compareTo(P.subtract(BigInteger.ONE))!=-1) ;//Xb should be
interval 0<Xb<P-1

    //Alice Public Key

    BigInteger Ya = G.modPow(Xa,P);//PublicKey = G^Xa mod(P)

    System.out.println("Base generator G has value :" + G);

    System.out.println("Modulus P has value :" + P);

    System.out.println("Alice private value Xa is :" + Xa);

    System.out.println("Alice public key Ya is :" + Ya);

    //Bob Public Key

    BigInteger Yb = G.modPow(Xb,P);//PublicKey = G^Xb mod(P)

    System.out.println("Bob private value Xb is :" + Xb);

    System.out.println("Bob public key Yb is :" + Yb);

    //Alice Shared Secret Key

    BigInteger SharedSecretKey_A = Yb.modPow(Xa,P);//SecretKey= Yb^Xa
mod(P)

    System.out.println("Alice shared secret key" + SharedSecretKey_A);

    //Bob Shared Secret Key

    BigInteger SharedSecretKey_B = Ya.modPow(Xb,P);//SecretKey= Ya^Xb
mod(P)

    System.out.println("Bob shared secret key" + SharedSecretKey_B);

    //Check if these keys are the same

    if(SharedSecretKey_A.equals(SharedSecretKey_B))

    System.out.println("Shared secret keys are the same");

    end = System.currentTimeMillis();

    total = end - start;

```

```

        total1=total1+total;
    }

    Average_Time= total1/1000;

    System.out.println("Elapsed milliseconds: " + Average_Time);

} catch (Exception e) {

    System.err.println("Error: " + e);

    System.exit(1);

}

}

}

```

### Περιγραφή πρωτοκόλλου και αντίστοιχου κώδικα σε Java

Η Alice & ο Bob παράγουν έναν μεγάλο πρώτο αριθμό  $P$  και μια γεννήτρια (βάση)  $G$  έτσι ώστε  $P > G$ . Οι παράμετροι αυτές είναι γνωστές και ορατές σε κάποιον που 'κρυφακούει' το κανάλι επικοινωνίας (Evil).

#### Δημιουργία παραμέτρων $P, G$ μέσω της Java:

Ορίζω μια ακέραια μεταβλητή τη `bitLength` που καθορίζει το μέγεθος όχι μόνο των παραμέτρων  $P, G$  αλλά και των μυστικών ποσοτήτων  $X_a, X_b$ . Μέσω της κλάσης `SecureRandom` δημιουργώ στιγμιότυπα τυχαίων αριθμών `rnd`. Ακολουθώντας, μέσω της κλάσης `BigInteger`<sup>14</sup> παράγω δύο μεγάλους ακέραιους  $P, G$  έτσι ώστε  $P > G$ .

Η συνάρτηση `compareTo` συγκρίνει τις τιμές των παραμέτρων  $P, G$ . Μια μεταβλητή  $c$  κρατά την τιμή που επιστρέφει το αποτέλεσμα της σύγκρισης. Η  $c$  παίρνει τιμές  $-1, 0$  ή  $1$  αν  $P = G, P < G$  nat  $P > G$  αντίστοιχα. Η `do - while` εκτελείται όσο  $P = G, P < G$  (δηλαδή  $c \neq 1$ ) μέχρι να ικανοποιηθεί η ανισότητα  $P > G$  οπότε  $c = 1$ . Άρα, όταν  $c = 1$  έχω το κατάλληλο ζεύγος παραμέτρων  $P, G$ .

<sup>14</sup> Κλάση που παράγει τυχαίους, πρώτους, μεγάλους ακέραιους μήκους `bitLength` ομοιόμορφα κατανεμημένους στο διάστημα  $0 - (2^{\text{bitLength}} - 1)$ .

Η παράμετρος  $P$  θέλω να είναι πρώτος αριθμός. Πρώτοι είναι οι αριθμοί που διαιρούνται μόνο από τον εαυτό τους και τη μονάδα. Έτσι, την παράμετρο  $P$  τη δημιουργώ με χρήση επιπλέον της μεθόδου `probablePrime`. Συνεπώς, έχω παράγει δύο τυχαίους, μεγάλου μήκους ακέραιους, εκ των οποίων ο ένας είναι και πρώτος αριθμός και επιπλέον ικανοποιείται η συνθήκη  $P > G$ .

#### **Δημιουργία των μυστικών ποσοτήτων $X_a, X_b$ μέσω της Java**

Alice & Bob μέσω της κλάσης `BigInteger` παράγουν αντίστοιχα δύο μεγάλους τυχαίους ακέραιους αριθμούς  $X_a, X_b$  αντίστοιχα, τους οποίους γνωρίζουν μόνο αυτοί, όπου  $0 < X_a, X_b < P - 1$ .

Μέσω της κλάσης `BigInteger` οι ποσότητες  $X_a, X_b$  είναι μεγαλύτερες ή ίσες του μηδενός. Από την άλλη πρέπει να είναι και μικρότερες από  $P - 1$ .

Για αυτό χρησιμοποιώ 2 `do-while` οι οποίες εκτελούνται όσο  $X_a, X_b \geq P - 1$  και σταματάει όταν  $X_a, X_b < P - 1$  οπότε ικανοποιείται η ζητούμενη συνθήκη.

#### **Υπολογισμός του δημόσιου κλειδιού**

Μέσω της μεθόδου `modPow` και των παραμέτρων  $P, G$  για αντικείμενα τύπου `BigInteger`, παράγω τα δημόσια κλειδί τους  $Y_a, Y_b$  αντίστοιχα, που είναι επίσης `BigInteger`.

#### **Ανταλλαγή των δημόσιων κλειδιών**

Ανταλλάσσουν τα δημόσια κλειδιά τους σε καθαρό κείμενο, όχι κρυπτογραφημένο. Δηλαδή, η Alice στέλνει απευθείας στον Bob το δημόσιο κλειδί της και ο Bob στέλνει αντίστοιχα στην Alice το δικό του δημόσιο κλειδί.

#### **Δημιουργία του κοινού μυστικού κλειδιού**

Βάσει των δημόσιων κλειδιών  $Y_a, Y_b$ , των μυστικών ποσοτήτων  $X_a, X_b$ , των παραμέτρων  $P, G$  και με χρήση της μεθόδου `modPow` υπολογίζουν ένα μυστικό κλειδί ο καθένας. Τα κλειδιά αυτά πρέπει να είναι ίδια, καλούνται `Shared Secret Key` και είναι τύπου `BigInteger`.

## Συμπεράσματα

Ο αντίπαλος (Evil) έχει γνώση των ποσοτήτων  $P$ ,  $G$ ,  $G^{X_a}$ ,  $G^{X_b}$  και καλείται να ανακαλύψει τον  $G^{X_a X_b}$ . Αυτό μπορεί να επιτευχθεί με δύο τρόπους:

- εύρεση του διακριτού λογάριθμου του  $G^{X_a} \text{ mod } P$  με βάση τον  $G$ , το οποίο είναι υπολογιστικά αδύνατο για μεγάλο  $P$ .
- εύρεση του  $G^{X_a X_b}$ , υψώνοντας τον  $G^{X_a}$  σε διάφορους εκθέτες, έως ότου βρεθεί ο  $G^{X_a X_b}$ . Η καταλληλότητα της επίθεσης αυτής εξαρτάται από τη δυνατότητα του αντιπάλου να ελέγχει αν βρήκε το σωστό εκθέτη. Αυτή η επίθεση ισοδυναμεί με εξαντλητική αναζήτηση, η οποία θα πρέπει να είναι πρακτικά ανέφικτη.

**Μετά από 1000 επαναλήψεις ο μέσος χρόνος εκτέλεσης σε milliseconds , του πρωτοκόλλου Diffie Hellman για μήκος κλειδιών 512 και 1024 φαίνεται στον ακόλουθο πίνακα.**

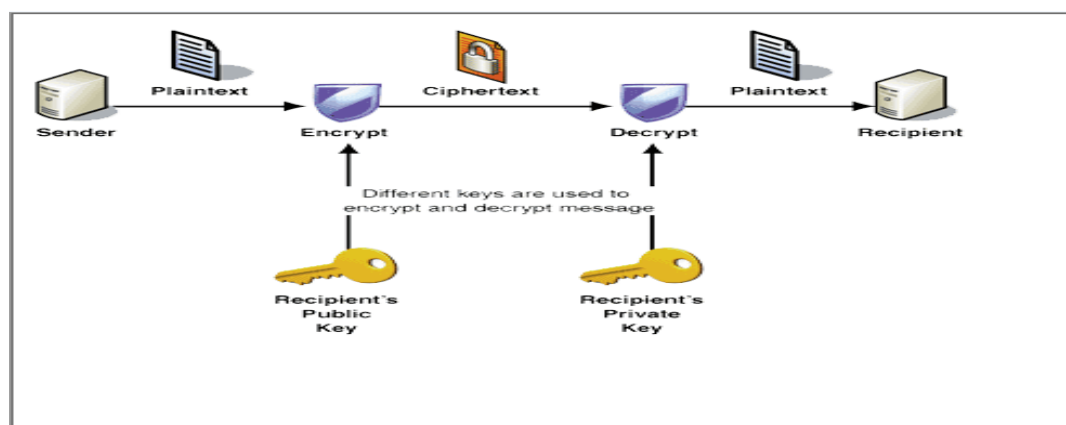
Μήκος Κλειδιού (bits) \ Χρόνος (msec)	512	1024
1 <sup>η</sup> μέτρηση	31	237
2 <sup>η</sup> μέτρηση	29	233
3 <sup>η</sup> μέτρηση	28	231
4 <sup>η</sup> μέτρηση	29	228
5 <sup>η</sup> μέτρηση	29	228

Παρατηρούμε ότι όσο αυξάνει το μήκος κλειδιού , αυξάνει σημαντικά και ο χρόνος εκτέλεσης του πρωτοκόλλου. Τώρα, αν δούμε κάθε στήλη χρόνων ξεχωριστά από κάποιο σημείο και μετά ο χρόνος είναι ίδιος. Αν πάρουμε το μέσο όρο των παραπάνω πειραματικών μετρήσεων, για μήκος κλειδιού 512 ο μέσος χρόνος είναι 29 msec και για μήκος κλειδιού 1024 3είναι 231.



### 3. Υποδομή δημόσιου κλειδιού (Public Key Infrastructure)

Το σύστημα δημόσιου κλειδιού μπορεί να χρησιμοποιηθεί για να κρυπτογραφηθούν μηνύματα που δύο οντότητες **Αποστολέας- Παραλήπτης** θέλουν να ανταλλάξουν κατά την επικοινωνία τους. Ο στόχος είναι να μην μπορεί κάποιος που «κρυφακούει» το κανάλι επικοινωνίας να καταλάβει το περιεχόμενο του , ενώ ταυτόχρονα επιτρέπει στον αποστολέα να επισυνάψει στο μήνυμα μια ψηφιακή υπογραφή που δεν γίνεται να πλαστογραφηθεί. Επομένως παρέχει έναν τρόπο να πιστοποιείται τόσο η ταυτότητα του χρήστη-αποστολέα όσο και το περιεχόμενο του μηνύματος.



Σχήμα 23. Υποδομή Δημόσιου Κλειδιού

### 4. Απόδειξη μηδενικής γνώσης

Μια απόδειξη μηδενικής γνώσης είναι ένα πρωτόκολλο μεταξύ μας οντότητας (αποδεικνύων) που επιχειρεί να αποδείξει τη γνώση ενός αλφαριθμητικού, και ενός επαληθευτή ο οποίος ελέγχει την εγκυρότητα όσων του παρουσιάζονται . Κοινή είσοδος αποτελεί η συνάρτηση  $W^{15}$  . Η είσοδος στον αποδεικνύων είναι ένα αλφαριθμητικό  $w$  το οποίο επαληθεύει τη συνάρτηση  $W$  , συνεπώς  $1 = W(w)$  . Ο επαληθευτής εξάγει είτε 1 σε περίπτωση αποδοχής είτε 0 σε περίπτωση απόρριψης. Βασική ιδιότητα αποτελεί το γεγονός ότι , εάν ο επαληθευτής «δεχτεί» , μπορεί να βεβαιωθεί ότι ο αποδεικνύων γνωρίζει ένα αλφαριθμητικό  $w^u$  έτσι ώστε  $W(w^u) = 1$ .

<sup>15</sup>  $W$  είναι μια δυαδική συνάρτηση που παίρνει είσοδο ένα αλφαριθμητικό  $a$  και εξάγει είτε 1 είτε 0.

Το πρωτόκολλο χαρακτηρίζεται μηδενικής γνώσης διότι ο επαληθευτής δεν μαθαίνει καμία υπολογιστική πληροφορία για το αλφαριθμητικό  $w$ . Μια απόδειξη μηδενικής γνώσης σημειώνεται ως  $PK \{(w): W(w) = 1\}$ . Η ποσότητα  $w$  αποτελεί ποσότητα τη γνώση της οποίας θέλει να αποδείξει ο αποδεικνύων στον επαληθευτή.

## 5. Διγραμμικοί Γράφοι (Bilinear Maps)

Ένας διγραμμικός γράφος από το  $G \times G$  στο  $G$  είναι μια συνάρτηση  $e: G \times G \rightarrow G$  τέτοια ώστε έχει τις ακόλουθες ιδιότητες.

1. **Διγραμμικότητα:** αν για όλα τα  $P, Q \in G$ , για όλα τα  $a, b \in \mathbb{Z}$   $e(P^a, Q^b) = e(P, Q)^{ab}$ .
2. **Μη εκφυλισμένος:** αν υπάρχουν  $P, Q \in G$  τέτοια ώστε  $e(P, Q) \neq 1$  όπου 1 είναι η ταυτότητα/εικόνα του  $G$ .
3. **Αποδοτικός:** Αν υπάρχει ένας αποδοτικός αλγόριθμος υπολογισμού του  $e$ .

Ας υποθέσουμε ότι έχουμε στη διάθεση μας έναν αλγόριθμο  $BiLinMapSetup$  ο οποίος για είσοδο μια παράμετρο ασφαλείας  $l_q$  εξάγει την εγκατάσταση ενός μη εκφυλισμένου, αποδοτικά υπολογίσιμου διγραμμικού γράφου  $e$  για τις ομάδες  $G = \langle g \rangle$  και  $G = \langle g \rangle$  τάξης  $q = \mathcal{O}(2^{S_q})$ .

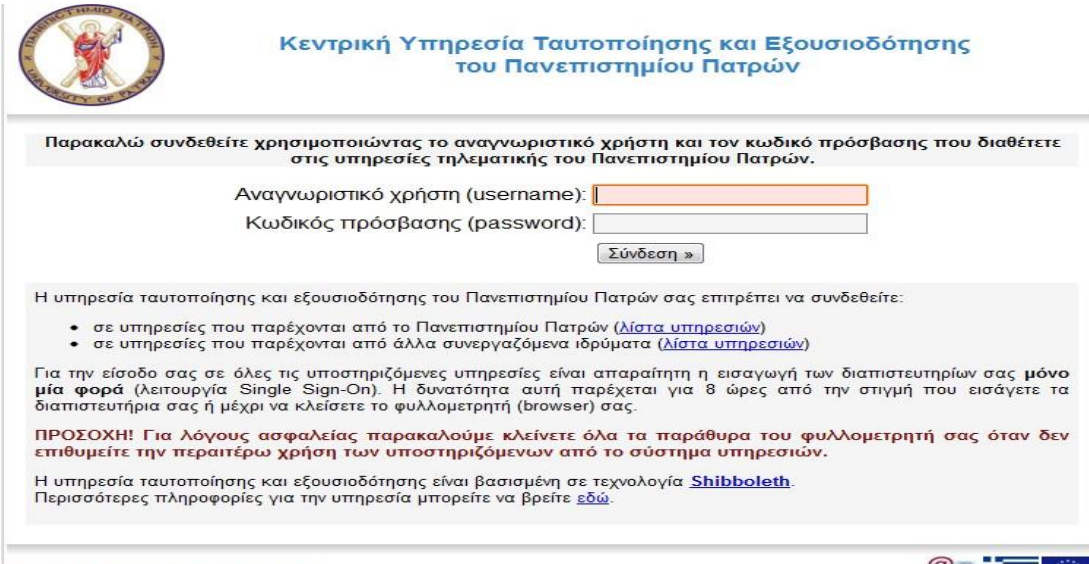
Σημειώνουμε ότι  $(q, G, G, g, g, e) \in BiLinMapSetup(l_q)$ . Σύμφωνα με τις ιδιότητες και το γεγονός ότι οι δύο ομάδες είναι ίδιας τάξης  $q$ , συμπεραίνουμε ότι αν  $g$  είναι γεννήτρια του  $G$ , τότε  $g = e(g, g)$ .

## 6. Single Sign On Συστήματα

Συνήθως κάποιος χρήστης αποκτά πρόσβαση σε υπηρεσίες βάσει ενός συνθηματικού και ενός κωδικού πρόσβασης. Δεδομένου ότι οι χρήστες αλληλεπιδρούν με όλο και περισσότερες (on-line) υπηρεσίες, οι κωδικοί πρόσβασης γίνονται όλο και περισσότερο ευαίσθητοι σε αλίευση και επανάληψη από ανέντιμους παροχείς υπηρεσιών. Επιπλέον, οι χρήστες δυσκολεύονται να θυμηθούν πολλά διαφορετικά διαπιστευτήρια. Ως εκ τούτου, πολύ συχνά χρήστες εισάγουν λάθος τα διαπιστευτήρια τους με αποτέλεσμα να επιβαρύνεται σημαντικά το σύστημα υποστήριξης των παροχών υπηρεσιών.

Ως αποτέλεσμα των παραπάνω όλο και περισσότεροι οργανισμοί «μεταναστεύουν» στα συστήματα όπου οι χρήστες τους θα μπορούν να έχουν πρόσβαση σε πολλαπλές υπηρεσίες εισάγοντας τα διαπιστευτήρια τους μία φορά μόνο κατά την είσοδο στο σύστημα. Στο σύστημα αυτό κάθε χρήστης έχει **ένα** συνθηματικό και **έναν** κωδικό πρόσβασης για όλα τα συστήματα , συσκευές , και εφαρμογές στις οποίες έχει πρόσβαση .

Συγκεκριμένα ο χρήστης εισάγει τα διαπιστευτήρια του μια φορά μόνο και από εκεί και ύστερα μπορεί να έχει πρόσβαση σε πολλές υπηρεσίες. Χαρακτηριστικό παράδειγμα αποτελεί η Κεντρική Υπηρεσία Ταυτοποίησης και Εξουσιοδότησης του πανεπιστημίου Πατρών στην οποία ο χρήστης αποκτά πρόσβαση εισάγοντας μια μόνο φορά τα διαπιστευτήρια του και ακολούθως μπορεί να έχει πρόσβαση σε οποιαδήποτε υπηρεσία αυτή παρέχει.



**Κεντρική Υπηρεσία Ταυτοποίησης και Εξουσιοδότησης του Πανεπιστημίου Πατρών**

Παρακαλώ συνδεθείτε χρησιμοποιώντας το αναγνωριστικό χρήστη και τον κωδικό πρόσβασης που διαθέτετε στις υπηρεσίες τηλεματικής του Πανεπιστημίου Πατρών.

Αναγνωριστικό χρήστη (username):

Κωδικός πρόσβασης (password):

Η υπηρεσία ταυτοποίησης και εξουσιοδότησης του Πανεπιστημίου Πατρών σας επιτρέπει να συνδεθείτε:

- σε υπηρεσίες που παρέχονται από το Πανεπιστήμιο Πατρών ([λίστα υπηρεσιών](#))
- σε υπηρεσίες που παρέχονται από άλλα συνεργαζόμενα ιδρύματα ([λίστα υπηρεσιών](#))

Για την είσοδο σας σε όλες τις υποστηριζόμενες υπηρεσίες είναι απαραίτητη η εισαγωγή των διαπιστευτηρίων σας **μόνο μία φορά** (λειτουργία Single Sign-On). Η δυνατότητα αυτή παρέχεται για 8 ώρες από την στιγμή που εισάγετε τα διαπιστευτήρια σας ή μέχρι να κλείσετε το φυλλομετρητή (browser) σας.

**ΠΡΟΣΟΧΗ!** Για λόγους ασφαλείας παρακαλούμε κλείνετε όλα τα παράθυρα του φυλλομετρητή σας όταν δεν επιθυμείτε την περαιτέρω χρήση των υποστηριζόμενων από το σύστημα υπηρεσιών.

Η υπηρεσία ταυτοποίησης και εξουσιοδότησης είναι βασισμένη σε τεχνολογία [Shibboleth](#).  
Περισσότερες πληροφορίες για την υπηρεσία μπορείτε να βρείτε [εδώ](#).

Copyright © 2009-2011 Πανεπιστήμιο Πατρών

## Σχήμα 24. Αποψη Single Sign On συστήματος

Η χρήση των συστημάτων αυτών είναι σημαντική διότι δίνει στους οργανισμούς τη δυνατότητα να ανακαλέσουν συνολικά όλα τα προνόμια πρόσβασης των χρηστών τους για οποιοδήποτε λόγο. Αυτό είναι επιθυμητό σε σύστημα SSO που θέλουν να δώσουν στους υπαλλήλους μιας εταιρείας πρόσβαση σε online πόρους της . Ωστόσο , όταν ένας υπάλληλος απολυθεί ή φεύγει οικειοθελώς από μια επιχείρηση , η ίδια η εταιρία μπορεί κεντρικά να ανακαλέσει όλα τα προνόμια πρόσβασής του.

## *Επεξήγηση Μαθηματικών Συμβόλων*

$Z_n^* = \{[a]_n \in Z_n : \gcd(a, n) = 1\}$  : ομάδα πολλαπλασιασμού modulo  $n$

$Z_n = \{1, 2, \dots, n - 1\}$

$E_R$  : ομοιόμορφα τυχαία

$\forall$  : για κάθε

$\{0, 1\}^k$  : αριθμός μήκους  $k$  δυαδικών ψηφίων

$\lfloor x \rfloor$  : επιλογή του αμέσως μικρότερου θετικού ακέραιου από το  $x$

$\lceil x \rceil$  : επιλογή του αμέσως μεγαλύτερου θετικού ακέραιου από το  $x$

$\neq$  : διαφορετικό

$\equiv$  : ταυτοτικά ίσο

$\cong, \approx$  : περίπου ίσα

$\sim$  : περίπου

$N$  : το σύνολο των φυσικών

$Z$  : το σύνολο των ακεραίων

$R$  : το σύνολο των πραγματικών

$\emptyset$  : κενό σύνολο

$\infty$  : σύμβολο του απείρου

$x \in X$  : ένα στοιχείο  $x$  ανήκει στο σύνολο  $X$

$x \notin X$  : ένα στοιχείο  $x$  δεν ανήκει στο σύνολο  $X$

$\{u_n\}$  : ακολουθία με γενικό όρο  $u_n$ ,

$[a, b]$  : αριθμητικό τμήμα

$\left. \begin{array}{l} [a, b) \\ (a, b] \end{array} \right\}$  : αριθμητικά ημι-διαστήματα

$(a, b)$  : αριθμητικό διάστημα

$\implies$  : ακολουθεί

$\Leftrightarrow$  : σύμβολο ισοδυναμίας

$\perp$  : σύμβολο καθετότητας

$\parallel$  : παράλληλο

$//$  : αλληλουχία

## ***Ορολογία Κρυπτογραφίας - Ελληνικό Γλωσσάρι***

***Κρυπτογράφηση – encryption***

***Αποκρυπτογράφηση – decryption***

***Κρυπτογραφικό σύστημα – cryptosystem***

***Απλό κείμενο – plaintext***

***Κρυπτοκείμενο – cipher-text***

***Αριθμός από τυχαία ψηφία – random bit number***

***Συμμετρική Κρυπτογραφία – Symmetric Cryptography***

***Κρυπτογραφία Μυστικού Κλειδιού – Secret Key Cryptography***

***Ασύμμετη Κρυπτογραφία – Asymmetric Cryptography***

***Κρυπτογραφία Δημόσιου Κλειδιού – Public Key Cryptography***

***Κυκλική Κρυπτογράφηση- Circular Encryption***

***Ζεύγος κλειδιών – Key Pair***

***Δημόσιο κλειδί – Public Key***

***Ιδιωτικό (Μυστικό ) Κλειδί - Private ( Secret) Key***

***Κύριο κλειδί-Master Key***

***Στατιστικά ανεξάρτητα-Statistically independent***

***Ανταλλαγή Κλειδιού – Key Exchange***

***Πρότυπο Ψηφιακής Υπογραφής – Digital Signature Standard (DSS)***

***Διαχείριση Κλειδιού – Key Administration***

***Κέντρο Διανομής Κλειδιών – Key Distribution Center (KDC)***

***Ακεραιότητα – Integrity***

***Ιδιωτικότητα – Privacy***

*Ασφάλεια – Security*

*Εμπιστευτικότητα – Confidentiality*

*Αποδοτικό-efficient*

*Εμπιστοσύνη - trust*

*Διαχωρισιμότητα - separability*

*Εμπιστη Τρίτη Όντοτητα – Trusted Third Party*

*Ψηφιακό Πιστοποιητικό – Digital Credential*

*Πιστοποιητικά Μιας Χρήσης – One-Show Credentials*

*Πιστοποιητικά Πολλαπλής Χρήσης – Multi-Show Credentials*

*Σύνοδος – Session*

*Αρχη Πιστοποίησης – Certification Authority*

*Τυφλή υπογραφή – blind signature*

*Δυναμικός Συσσωρευτής – dynamic accumulator*

*Απόδειξη Μηδενικής Γνώσης – Zero Knowledge Proof*

*Ψηφιακό Ψευδώνυμο – Digital Pseudonym*

*Μαύρη Λίστα – Black List*

*Μη μεταφερσιμότητα – non-transferability*

*Δημόσιου Κλειδιού Μη μεταφερσιμότητα- PKI non-transferability*

*Οριστική Μη μεταφερσιμότητα-All-or-nothing non-transferability*

*Μη συνδεσιμότητα - unlinkability*

*Άγνωστοι χρήστες – Unknown users*

*Ανάκληση Ανωνυμίας – Anonymity Revocation*

*Τυχαίος – random*

*διακριτός λογάριθμος – discrete logarithm*

*Ψευδοτυχαίος – Pseudorandom*

*Παροχέας Ταυτότητας- Identity Provider*

*Χρήστης - User*

*Παροχέας Υπηρεσιών – Service Provider*

*Υπηρεσίες – Services*

*Οργανισμός – Organisation*

*Διαμεσολαβητής- Intermediator*

*Επαληθευτής- Verifier*

*Διαχειριστής Ανάκλησης Ανωνυμίας - Revocation Anonymity Manager*

*Γενική Ανάκληση Ανωνυμίας- Global Revocation Anonymity*

*Τοπική Ανάκληση Ανωνυμίας- Local Revocation Anonymity*

*Διπλή χρήση(πιστοποιητικού)- double-spending*

*Ταυτότητα - Identity*

*Γεννήτρια/Γεννήτορας - generator*

*Πρώτος – prime*

*Ασφαλής πρώτος-safe prime*

*Τάξη-order*

*Ομάδα - group*

*Κρυπτογραφική απόδειξη - cryptographic proof*

*Πρωτόκολλο - protocol*

*Πλαστογράφηση-forgery*

*Παράνομες συναλλαγές - illegal transactions*



*Προσαρμοστική επίθεση - adaptive attack*

*Μη μεταφερσιμότητα- non-transferability*

*Έγκυρο κλειδί – valid key*

*Κρυπτογραφικά κλειδιά-cryptographic keys*

*Συνοχή πιστοποιητικού-credential consistency*

*Κακόβουλος χρήστης- attacker*

*Μεγάλη πιθανότητα- high probability*

*Πρόθεμα – Prefix*

*Όνομα Σύνδεσης- Login Name*

*Κλειδί Επικύρωσης- Authenticating Key*

*Αρχή- Primitive*

*Συνθηματικό – Username*

*Κωδικός Πρόσβασης-Password*

*Κλειδί Κρυπτογράφησης- Encryption Key*

*Κλειδί Αποκρυπτογράφησης – Decryption Key*

*Εξωτερικό δημόσιο κλειδί – External Public Key*

*Δεσμευμένο δημόσιο κλειδί – Committed Public Key*

*Επαληθεύσιμη Κρυπτογράφηση- Verifiable Encryption*

*Πρόκληση- Challenge*

*Δέσμευση-Committment*

*Επιλήσμων Κλειδιού-Key-Oblivious*

*Μήκος Κλειδιού- Key length*

*Ετικέτα Εγκυρότητας-Validating Tag*

*Σημειολογικά ασφαλές – Semantically safe*

*Κυκλικά ασφαλές – Circular safe*

*Συνάρτηση κατακερματισμού- hash function*

*Τιμή κατακερματισμού- hash value*

*Σύνοψη μηνύματος-message digest*

*Αλγόριθμος σύνοψης μηνύματος-message digest algorithm*

*Σχέδιο επαληθεύσιμης κρυπτογράφησης-Verifiable Encryption Scheme*

*Αποδεικνύων- Prover*

*Διγραμμικός γράφος-Bilinear Map*

*(Μη-)Αλληλεπιδραστική απόδειξη-(Non-)Interactive proof*

*Ψηφιακό χρήμα – e-coin*

*Εξακρίβωση ταυτότητας χρήστη -user authentication*

*Εξακρίβωση ταυτότητας προέλευσης δεδομένων -data origin authentication*

*Υπηρεσία Αυθεντικοποίησης-Authentication Service*

*Χ.509 –Πρότυπο Ψηφιακού Πιστοποιητικού*



## Βιβλιογραφία

- [1] : A Practical System for Globally Revoking the Unlinkable Pseudonyms of Unknown Users  
Stefan Brands, Liesje Demuynck, and Bart De Decker  
Credentica & McGill School of Comp. Science 1010 Sherbrooke St. W., Suite 1800, Montreal, QC, Canada H3A 2R7 brands@{credentica.com,cs.mcgill.ca}  
[www.credentica.com](http://www.credentica.com)  
K.U.Leuven, Department of Computer Science  
Celestijnenlaan 200A, B-3001 Heverlee, Belgium  
{Liesje.Demuynck , Bart.DeDecker} @cs.kuleuven.be [www.cs.kuleuven.be](http://www.cs.kuleuven.be)
- [2] :An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation , Jan Camenisch IBM Research Zurich Research Laboratory CH{8803 Rüschlikon [jca@zurich.ibm.com](mailto:jca@zurich.ibm.com) & Anna Lysyanskaya MIT LCS 545 Technology Square Cambridge, MA 02139 USA [anna@theory.lcs.mit.edu](mailto:anna@theory.lcs.mit.edu) Abstract
- [3]: A Cryptographic Framework for the Controlled Release Of Certified Data  
Endre Bangerter<sup>1</sup>, Jan Camenisch<sup>1</sup>, and Anna Lysyanskaya  
IBM Zurich Research Laboratory, Säumerstrasse 4, 8803 Rüschlikon, Switzerland, {ebaljca} @zurich.ibm.com  
Computer Science Department, Brown University, Providence, RI 02912 USA, [anna@cs.brown.edu](mailto:anna@cs.brown.edu)
- [4] : Grudzewski W. M., Hejduk I. K., Sankowska A. (2008), “Trust Management - The New Way in The Information Society”, *Economics and Organization of Enterprise*, Vol. 2, chapter 2, p. 2-8
- [5]: Άλλο εικονογραφικό υλικό από το διαδίκτυο
- [6]: Wikipedia





