**Αλκιβιάδης Μέρτζιος**

# Παρουσίαση Project 2020

## *PPP-Completeness with Connections to Cryptography,*

***Katerina Sotiraki, Manolis Zampetakis, Giorgos Zirdelis***

## 1. Εισαγωγή-Προαπαιτούμενα

- Δυαδική σύνθεση-αποσύνθεση. Συναρτήσεις bc(), bd() που μας μεταφέρουν από δυαδικό διάνυσμα σε αριθμό και αντίστροφα. bc(010) = 2, bd(7) = 111.
- [s] = {0, 1, ... , s-1}.
- **Χαρακτηριστική συνάρτηση:** Λέμε ότι ένα κύκλωμα $CH_S$ με k δυαδικές εισόδους και μία έξοδο είναι η χαρακτηριστική συνάρτηση του S αν $CH_S(\underline{x})=1$ αν και μόνο αν $\underline{x} \in bd(S)$.
- **Συνάρτηση τιμής:** Έστω (s, $V_S$) μία πλειάδα όπου το $V_S$ είναι ένα κύκλωμα με $\lceil log(s) \rceil$ δυαδικές εισόδους και k εξόδους και $s \in \mathbb{Z}_+$. Έστω $f_{(s,V_S)}: [s] \to \{0,1\}^k$ μια συνάρτηση τέτοια ώστε $f_{(s,V_S)}(bc(\underline{x})) = V_S(\underline{x})$ για όλα τα $\underline{x}$ με $bc(\underline{x}) < s$. Τότε, η (s, $V_S$) είναι μια αναπαράσταση τιμής του S αν και μόνο αν η $f_{(s,V_S)}$ είναι bijection μεταξύ του [s] και του bd(S).

## 1. Εισαγωγή-Προαπαιτούμενα

- **Συνάρτηση δείκτη:** Έστω (s, $I_S$) μία πλειάδα όπου το $I_S$ είναι ένα κύκλωμα με k δυαδικές εισόδους και $\lceil \log(s) \rceil$ εξόδους και $s \in \mathbb{Z}_+$. Έστω $f_{(s,I_S)}: bd(S) \to [s]$ μια συνάρτηση τέτοια ώστε $f_{(s,I_S)}(\underline{x}) = bc(I_S(\underline{x}))$ για όλα τα $\underline{x} \in bd(S)$. Τότε, η (s, $I_S$) είναι μια αναπαράσταση δείκτη του S αν και μόνο αν η $f_{(s,I_S)}$ είναι bijection μεταξύ του bd(S) και του [s].
- Για $S = ([0, L_1] \times [0, L_2] \times \cdots \times [0, L_n]) \cap \mathbb{Z}^n$ οι παραπάνω αναπαραστάσεις υλοποιούνται με πολυωνυμικά κυκλώματα.
- Μπορούμε να σκεφτόμαστε το s ως το μέγεθος του συνόλου (πλήθος στοιχείων), το $V_S$ ως μία συνάρτηση που παίρνει το δείκτη του στοιχείου και μας δίνει τη τιμή στο σύνολο και το $I_S$ ως μία συνάρτηση που παίρνει τη τιμή του στοιχείου στο σύνολο και μας δίνει το δείκτη του.
- Δηλαδή, (καταχρηστικά) $V_S: [s] \to \{0,1\}^k$ και $I_S: \{0,1\}^k \to [s]$

## 2. BLICHFELDT Πρόβλημα

- **Pigeonhole problem.**
  Είσοδος: Ένα κύκλωμα C με n εισόδους και n εξόδους.
  Έξοδος: Ένα από τα ακόλουθα:
  1) Δυαδικό διάνυσμα τ.ω C(x) = 0
  2) Δύο δυαδικά διανύσματα x, y με x ≠ y τ.ω C(x) = C(y).
- **Θεώρημα Blichfeldt.**
  Έστω $B \in \mathbb{Z}^{nxn}$ ένα σύνολο από n γραμμικώς ανεξάρτητα διανύσματα διάστασης n και $S \subseteq \mathbb{R}^n$. Αν vol(S) > det(L(B)) τότε υπάρχουν διανύσματα $x, y \in S$ με x ≠ y τ.ω $x - y \in L(B)$.
- **Blichfeldt problem.**
  Είσοδος: Μία βάση $B \in \mathbb{Z}^{nxn}$ και ένα σύνολο $S \subseteq \mathbb{Z}^n$ σε μορφή αναπαράστασης τιμής (s, $V_S$).
  Έξοδος: Αν s < det(L(B)), τότε το διάνυσμα 0. Αλλιώς:
  0. Έναν αριθμό $z \in [s]$ τέτοιο ώστε $V_S(z) \notin S$ ή δύο αριθμούς $z, w \in [s]$ τέτοιοι ώστε $V_S(z) = V_S(w)$,
  1. Ένα διάνυσμα x τ.ω $x \in S \cap L$,
  2. Δύο διανύσματα x ≠ y, τ.ω $x, y \in S$ και $x - y \in L$

## 2. BLICHFELDT Πρόβλημα

- Το Blichfeldt ανήκει στο PPP
- Είσοδος: B, (s, $V_S$)
- Έστω $R = P(B) \cap \mathbb{Z}^n$, $l = \lceil \log(det(L)) \rceil$ και $m = \lceil \log(s) \rceil$
- $P(B)$ το βασικό παραλληλεπίπεδο
- $det(L(B)) = |P(B) \cap \mathbb{Z}^n|$ και συνεπώς $l = \lceil \log(|R|) \rceil$
- Αν s < det(L) έξοδος 0 και δεν έχουμε κάτι άλλο να κάνουμε.
- Υποθέτουμε χωρίς βλάβη της γενικότητας ότι s = det(L)
- Αν το κύκλωμα είναι πιο μεγάλο (m είσοδοι) βάζουμε μηδενικά στις m-l και δημιουργούμε το σύνολο (det(L), $V_S$') όπου $V_S$' το $V_S$ με σταθερά (μηδέν) τα m-l πιο σημαντικά ψηφία της εισόδου.
- Υποθέτουμε ακόμη (χωρίς βλάβη της γενικότητας) ότι $2^l = det(L)$
- Θέλουμε να απεικονίσουμε τα διανύσματα του S σε ένα coset του L αφού αν ανήκουν στο ίδιο coset η διαφορά τους είναι στο L
- Θα διασπάσουμε το πίνακα B σε Smith κανονική μορφή κάτι το οποίο γίνεται με πολυωνυμικό κύκλωμα.
- B = UDV με U, V ακέραιους πίνακες με μονοδιαία ορίζουσα και D διαγώνιος.

## 2. BLICHFELDT Πρόβλημα

- Θέλουμε να προβάλουμε το διάνυσμα από το P(B) στο P(D).
- Για unimodular V είναι: L(D) = L(DV). Αυτό γιατί Dx = DVV$^{-1}$x = DVy.
- Αρχικά, αφού L(D) = L(DV) έχουμε ένα bijection (1-1 και επί απεικόνιση) ϕ(x) = x (mod P(D)) από το P(DV) στο P(D) και ϕ$^{-1}$(x) = x (mod P(DV))
- Ακόμη, h(x) = U$^{-1}$ x ένα bijection από το R = P(UDV) στο P(DV)
- (U$^{-1}$ x = U$^{-1}$ UDVy = DVy)
- Συνεπώς, π(x) = ϕ(h(x)) είναι ένα bijection από το R στο P(D)
- Αφού $R_D = [0, d_1] \times [0, d_2] \times \cdots \times [0, d_n] \cap \mathbb{Z}^n$ τότε μπορούμε να υπολογίσουμε αποδοτικά τη συνάρτηση δείκτη για το σύνολο έστω $I_{R_D}$
- Έστω $I_R(x) = I_{R_D}(\pi(x))$ και σ(x) = x (mod P(B)) συνάρτηση που απεικονίζει τα διανύσματα στο βασικό παραλληλεπίπεδο.
- Ως κύκλωμα C ορίζουμε το $I_R(\sigma(V_S(\underline{x})))$ και υποθέτουμε det(L) = $2^l$ ώστε το κύκλωμα να έχει l εισόδους και εξόδους.

## 2. BLICHFELDT Πρόβλημα

- Πιθανές λύσεις του pigeonhole
- **1**. Ένα δυαδικό διάνυσμα $\underline{x} \in \{0,1\}^l$ με C(x) = 0
  Έχουμε ότι $I_{R_D}(\pi(\sigma(V_S(x)))) = 0$. Από το ορισμό της $I_{R_D}$ έχουμε ότι $\pi(\sigma(V_S(\underline{x}))) = 0$ και συνεπώς $\sigma(V_S(\underline{x})) = 0$. Αυτό μας λέει πως το στοιχείο $x = V_S(\underline{x})$ του S απεικονίζεται πάνω στο πλέγμα L και συνεπώς έχουμε λύση του Blichfeldt με τη περίπτωση 1).
- **2.** Δύο δυαδικά διανύσματα $\underline{x}, \underline{y} \in \{0,1\}^l$ με C(x) = C(y)
  Όμοια με πριν έχουμε ότι τα $V_S(\underline{x}), V_S(\underline{y})$ ανήκουν στο ίδιο coset του L και συνεπώς η διαφορά τους ανήκει στο L άρα έχουμε τη περίπτωση 2) του Blichfeldt.
- Αν det(L) < $2^l$ ορίζουμε το C ως

$$C(\underline{\mathbf{x}}) = \begin{matrix} \underline{\mathbf{x}} \ if \ bc(\underline{\mathbf{x}}) \geq det(L) \\ I_R(\sigma(V_S(\underline{\mathbf{x}}))) \ if \ bc(\underline{\mathbf{x}}) < det(L) \end{matrix}$$

και δεν έχουμε λύσεις για bc(x), bc(y) > det(L).

## 2. BLICHFELDT Πρόβλημα

- Το Blichfeldt είναι PPP-hard
- Θα κάνουμε Karp αναγωγή από το pigeonhole πρόβλημα στο Blichfeldt.
- Θέτουμε q = 2 και $A = [0\ I_n] \in \mathbb{Z}_2^{n \times 2n}$
- Θέτουμε L(B) = $\Lambda_q^{\perp}(A)$ και $S = \{\begin{bmatrix} \underline{x} \\ C(\underline{x}) \end{bmatrix} \mu\varepsilon\ \underline{x} \in \{0,1\}^n\} \subseteq \mathbb{Z}_2^{2n}$
- $\Lambda_q^{\perp}(A)$ είναι το πλέγμα: $(Ax = 0\ (mod\ q))$
- |S| = $2^n$
- Είσοδος του Blichfeldt είναι το B και το ($2^n$, $V_S$).
- Αναλύουμε τις εξόδους:
- **1.** διάνυσμα με $y = \begin{bmatrix} \underline{x} \\ C(\underline{x}) \end{bmatrix} \in S \cap L(B)$

  Από το $L(B) = \Lambda_q^{\perp}(A)$ έχουμε ότι Ay = 0 (mod 2) και συνεπώς C(x) = 0 και συνεπώς το x να είναι λύση στο pigeonhole πρόβλημα.

## 2. BLICHFELDT Πρόβλημα

- **2.** διανύσματα $x, y \in S$ με $x \neq y$ και $x - y \in L(B)$
  Έχουμε A(x-y) = 0 (mod 2) άρα C(x) = C(y) και αφού x ≠ y τότε x ≠ y άρα αποτελούν λύση του pigeonhole.
- Τέλος, είναι από τη θεωρία πλεγμάτων $det\big(L(B)\big) = det\left(\Lambda_q^{\perp}(A)\right) \leq q^n = 2^n$ και συνεπώς δε θα έχουμε τη τετριμμένη έξοδο 0.
- Συνεπώς το Blichfeldt πρόβλημα είναι PPP-complete.

## 3. Constrained Short Integer Solution

- **Δυαδικός αναστρέψιμος πίνακας**
- Έστω $l \in \mathbb{Z}_+$, $q \leq 2^l$ και $d, k \in \mathbb{N}$. Αρχικά, ας ορίσουμε το βοηθητικό διάνυσμα $\gamma_l = [1 \quad 2 \quad 4 \quad \cdots \quad 2^{l-1}]^T \in \mathbb{Z}_q^l$. Ακόμη, ορίζουμε τον πίνακα $U \in \mathbb{Z}_q^{d \times (d \cdot l)}$ που έχει μη μηδενικά στοιχεία μόνο πάνω από την (l+1) διαγώνιο και $V \in \mathbb{Z}_q^{d \times k}$ ένας τυχαίος πίνακας. Τότε ορίζουμε το πίνακα $G = \left[\left(I_d \otimes \gamma_l^T + U\right) \; V\right] \in \mathbb{Z}_q^{d \times (d \cdot l + k)}$ ως δυαδικό αναστρέψιμο. Ένα απλό παράδειγμα για q=8 και l=3 είναι το παρακάτω:

$$\begin{bmatrix}
1 & 2 & 4 & * & * & * & * & * & * & \cdots & * & * & * & * & * & \cdots & * & * \\
0 & 0 & 0 & 1 & 2 & 4 & * & * & * & \cdots & * & * & * & * & * & \cdots & * & * \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 4 & \cdots & * & * & * & * & * & \cdots & * & * \\
 & \vdots & & & \vdots & & & \vdots & & \ddots & & \vdots & & & & \vdots & & \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 1 & 2 & 4 & * & * & \cdots & * & *
\end{bmatrix}$$

## 3. Constrained Short Integer Solution

- Έστω $G = \left[\left(I_d \otimes \gamma_l^T + U\right)V\right] \in \mathbb{Z}_q^{d\times(d\cdot l+k)}$ ένας δυαδικός αντιστρέψιμος πίνακας και r' ένα τυχαίο διάνυσμα στο $\mathbb{Z}_q^k$. Τότε, για κάθε διάνυσμα $b \in \mathbb{Z}_q^d$ υπάρχει $r \in \{0,1\}^{d\cdot l}$ τέτοιο ώστε $G\begin{bmatrix} r \\ r' \end{bmatrix} = b(mod\ q)$. Ακόμη, αν q=$2^l$ το r είναι μοναδικό και υπολογίζεται από ένα πολυωνυμικό κύκλωμα.
- Αποδεικνύεται εύκολα με ιδέες παρόμοιες με αυτές της μεθόδου απαλοιφής Gauss.
- **cSIS πρόβλημα.**
- Είσοδος: Ένας πίνακας $A \in \mathbb{Z}_q^{n\times m}$, ένας δυαδικός αντιστρέψιμος πίνακας $G \in \mathbb{Z}_q^{d\times m}$ και ένα διάνυσμα $b \in \mathbb{Z}_q^d$ όπου $l \in \mathbb{Z}_+$, $q \le 2^l$ και $m \ge (n+d)\cdot l$

  Έξοδος: Ένα από τα παρακάτω:

  **1.** ένα διάνυσμα $x \in \{0,1\}^m$ τ.ω. $x \in \Lambda_q^{\perp}(A)$ και $Gx = b(mod\ q)$

  **2.** δύο διανύσματα $x, y \in \{0,1\}^m$ τ.ω. $x \ne y$ με $x - y \in \Lambda_q^{\perp}(A)$ και $Gx = Gy = b(mod\ q)$.

## 3. Constrained Short Integer Solution

- Το cSIS ανήκει στο PPP.
- Θα κατασκευάσουμε κύκλωμα C με n*l δυαδικές εισόδους και εξόδους.
- Ορίζουμε $k = m - d \cdot l$ και υπενθυμίζουμε ότι αφού ο G έχει m στήλες τότε οι στήλες του τυχαίου πίνακα V πρέπει να είναι $m - d \cdot l$.
- Για την είσοδο $\underline{x} \in \{0,1\}^{n \cdot l}$ ορίζουμε το διάνυσμα $r' = [\underline{x}_{0^{k-n \cdot l}}] \in \mathbb{Z}_q^k$ και υπολογίζουμε διάνυσμα $r \in \{0,1\}^{d \cdot l}$ ώστε $G \begin{bmatrix} r \\ r' \end{bmatrix} = b (mod\ q)$.
- Έστω $C_1 : \{0,1\}^{n \cdot l} \rightarrow \{0,1\}^{d \cdot l}$ το κύκλωμα που με είσοδο το $\underline{x}$ υπολογίζει το r.
- Ορίζουμε ως C:

$$C(\underline{\mathbf{x}}) = bd\left( A \begin{bmatrix} C_1(\underline{\mathbf{x}}) \\ \underline{\mathbf{x}} \\ \mathbf{0}^{k-n \cdot l} \end{bmatrix} (mod\, q) \right)$$

## 3. Constrained Short Integer Solution

- Αφού το αποτέλεσμα της πράξης των πινάκων ανήκει στο $\mathbb{Z}_q^n$ τότε χρειαζόμαστε l bits για να περιγράψουμε κάθε αριθμό συνεπώς $n \cdot l$ σύνολο.
- Αναλύουμε τις εξόδους του pigeonhole. Υπάρχει σύγκρουση! $(m - dl > nl)$
- **1.** ένα διάνυσμα $\underline{x} \in \{0,1\}^{n \cdot l}$ με C($\underline{x}$) = $\underline{0}^{nl}$.

  Σε αυτή τη περίπτωση με $x = \begin{bmatrix} C_1(\underline{x}) \\ \underline{x} \\ 0^{k-n \cdot l} \end{bmatrix}$ έχουμε C($\underline{x}$) = bd (Ax (mod q)) = $\underline{0}$.

  Έχουμε πως $Ax = 0(mod\ q)$ και συνεπώς $x \in \Lambda_q^{\perp}(A)$. Ακόμη, από τον ορισμό του $C_1$($\underline{x}$) έχουμε ότι $Gx = b\ (mod\ q)$. Συνεπώς το διάνυσμα x αποτελεί λύση του cSIS.

- **2.** δύο διανύσματα $\underline{x}, \underline{y} \in \{0,1\}^{n \cdot l}$ με $\underline{x} \neq \underline{y}$ και $C(\underline{x}) = C(\underline{y})$

  Ορίζουμε τα x, y όμοια όπως παραπάνω και έχουμε

  $$bd(Ax\ (mod\ q)) = C(\underline{x}) = C(\underline{y}) = bd(Ay\ (mod\ q))$$

  Ισχύει $Ax = Ay\ (mod\ q)$ και συνεπώς $A(x - y) = 0(mod\ q)$ με $x - y \in \Lambda_q^{\perp}(A)$. Ακόμη είναι x ≠ y αφού $\underline{x} \neq \underline{y}$ και $Gx = Gy = b(mod\ q)$ λόγω του κυκλώματος $C_1$. Συνεπώς τα x,y αποτελούν λύση του cSIS.

## 3. Constrained Short Integer Solution

- Το cSIS είναι PPP-hard.
- Θα μετατρέψουμε το κύκλωμα C στον πίνακα G
- Έστω ότι είσοδος στο pigeonhole είναι το $C = (C_1, \cdots, C_n)$.
- Υποθέτουμε ότι το C αποτελείται από $\{\overline{\wedge}, \overline{\vee}, \oplus, \wedge, \vee\}$.
- Το κύκλωμα C αναπαριστάται ως n κατευθυνόμενα ακυκλικά γραφήματα.
- Έστω $d_i = |C_i|$ ο μέγεθος του i-κυκλώματος και $Graph^{(i)} = (V^{(i)}, E^{(i)})$ το κατευθυνόμενο ακυκλικό γράφημα.
- Έστω $(u_1^{(i)}, u_2^{(i)}, \ldots, u_{d_i}^{(i)})$ μία τοπολογική διάταξη του Graph$^{(i)}$ όπου οι πρώτοι κόμβοι είναι οι κόμβοι εισόδου και οι τελευταίος είναι αυτός που μας δίνει το αποτέλεσμα.
- n είσοδοι: Συμβολίζουμε με $x_1, x_2, \ldots, x_n$ τις μεταβλητές τιμής και $w_1, w_2, \ldots, w_n$ τις βοηθητικές μεταβλητές.
- Υπόλοιποι $d_i$-n-1 κόμβοι: $z_{n+1}^{(i)}, z_{n+2}^{(i)}, \ldots, z_{d_i-1}^{(i)}$ οι μεταβλητές τιμής και οι βοηθητικές με $r_{n+1}^{(i)}, r_{n+2}^{(i)}, \ldots, r_{d_i-1}^{(i)}$ και ακόμη την έξοδο $y_i$ (ή $z_{d_i}^{(i)}$) και βοηθητική μεταβλητή $t_i$ (ή $r_{d_i}^{(i)}$).

## 3. Constrained Short Integer Solution

- Για την έξοδο $y_i$ η μεταβλητή τιμής και $t_i$ η βοηθητική μεταβλητή.
- Έστω $p_1(j)$ ο δείκτης του πρώτου προγόνου του κόμβου $u_j$ και $p_2(j)$ ο δείκτης του δεύτερου προγόνου. Αφού οι κόμβοι είναι ταξινομημένοι, $p_1(j) < p_2(j) < j$.
- Έχουμε μία γραμμή του G για κάθε κόμβο που δεν είναι κόμβος εισόδου.
- Κάθε γραμμή έχει στοιχεία σύμφωνα με τον πίνακα:

| Λογική Πράξη του $u_j$ | Εξίσωση για τον $u_j$ | $b_j$ |
|---|---|---|
| $\overline{\wedge}$ | $r_j + 2z_j - z_{p1}(j) - z_{p2}(j) = 2(mod4)$ | 2 |
| $\overline{\vee}$ | $r_j + 2z_j - z_{p1}(j) - z_{p2}(j) = 3(mod4)$ | 3 |
| $\oplus$ | $z_j + 2r_j - z_{p1}(j) - z_{p2}(j) = 0(mod4)$ | 0 |
| $\wedge$ | $r_j + 2z_j - z_{p1}(j) - z_{p2}(j) = 0(mod4)$ | 0 |
| $\vee$ | $r_j + 2z_j + z_{p1}(j) + z_{p2}(j) = 0(mod4)$ | 0 |

## 3. Constrained Short Integer Solution

- Η μορφή αυτή βασίζεται στις σχέσεις:

  1. $w + 2z - x - y = 2(mod\ 4) \Leftrightarrow x\ \overline{\wedge}\ y = z, w = x \oplus y$
  2. $w + 2z - x - y = 3(mod\ 4) \Leftrightarrow x\ \overline{\vee}\ y = z, w = \neg(x \oplus y)$
  3. $z + 2w - x - y = 0(mod\ 4) \Leftrightarrow x \oplus y = z, w = x \wedge y$
  4. $w + 2z - x - y = 0(mod\ 4) \Leftrightarrow x \wedge y = z, w = x \oplus y$
  5. $w + 2z + x + y = 0(mod\ 4) \Leftrightarrow x \vee y = z, w = x \oplus y$

- Οι στήλες αφορούν τις μεταβλητές με την εξής σειρά:

$$y_i, t_i, r_{d_i-1}, z_{d_i-1}, \dots, r_{n+1}, z_{n+1}, x_n, \dots, x_1, w_n, \dots, w_1$$

- Σε περίπτωση πύλης XOR αλλάζουμε τη σειρά των r, z ώστε ο συντελεστής του z (που είναι 1) να έρθει πριν από αυτόν του r (που είναι 2). Έτσι, ο πίνακας που προκύπτει είναι δυαδικός αναστρέψιμος.

$$\begin{bmatrix} 1 & 2 & * & * & \cdots & * & * & * & \cdots & * & 0 & \cdots & 0 \\ 0 & 0 & 1 & 2 & \cdots & * & * & * & \cdots & * & 0 & \cdots & 0 \\ & & & & \vdots & & & & \vdots & & & \vdots & \\ 0 & 0 & 0 & 0 & \cdots & 1 & 2 & * & \cdots & * & 0 & \cdots & 0 \end{bmatrix}$$

## 3. Constrained Short Integer Solution

- Οι τιμές που συμβολίζουμε με αστεράκια είναι κατάλληλες για να ικανοποιούνται οι σχέσεις του πίνακα που δείξαμε.
- Η συντεταγμένη που αντιστοιχεί στη μεταβλητή $z_{d_i}$ μας δίνει την έξοδο του κυκλώματος.
- Οι πίνακες G(i) έχουν διαστάσεις $(d_i - n) \times 2d_i$ και έχουν τη μορφή:

$$[I_{d_i-n} \otimes \gamma_2^T + U^{(d_i-n)\times 2(d_i-n)} \quad V^{(d_i-n)\times 2n}]$$

- Ορίζουμε ως $d_i' = d_i - n$ και $d = \sum_{i=1}^{n} d_i'$. Ο πίνακας G έχει διαστάσεις $(d\,) \times 2(d+n)$ και είναι:

$$G = \begin{bmatrix} (I_{d_1'} \otimes \gamma_2^T + U^{(1)}) & \mathbf{0} & \cdots & \mathbf{0} & V^{(1)} \\ \mathbf{0} & (I_{d_2'} \otimes \gamma_2^T + U^{(2)}) & \cdots & \mathbf{0} & V^{(2)} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & (I_{d_n'} \otimes \gamma_2^T + U^{(n)}) & V^{(n)} \end{bmatrix}$$

## 3. Constrained Short Integer Solution

- Ακόμη:

$$\boldsymbol{b}=\begin{bmatrix}\boldsymbol{b}^{(1)}\\ \boldsymbol{b}^{(2)}\\ \vdots\\ \boldsymbol{b}^{(n)}\end{bmatrix}$$

- Ο Α έχει διαστάσεις $n \times 2(d+n)$ και είναι $A_1 \in \mathbb{Z}_q^{n\times 2d}$, $A_2 \in \mathbb{Z}_q^{n\times n}$ και $A_3 \in \mathbb{Z}_q^{n\times n}$ έτσι ώστε $A = [A_1 \quad A_2 \quad A_3]$.
- Είναι $A_2 = 0$ και $A_3 = 2I_n$.
- Τέλος, ο $A_1$ έχει τη τιμή 1 μία φορά σε κάθε γραμμή, στη στήλη που αντιστοιχεί στη μεταβλητή τιμής για την έξοδο του κυκλώματος. Η μορφή του είναι:

$$\begin{bmatrix}
0 & 1 & \cdots & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 2 & \cdots & 0\\
0 & 0 & \cdots & 0 & 1 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0\\
 & & \vdots & & & \vdots & & & & \vdots & & & \vdots & \\
0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 & 0 & \cdots & 2
\end{bmatrix}$$

## 3. Constrained Short Integer Solution

- Ας αναλύσουμε τις εξόδους του cSIS με είσοδο (A, G, b).
- **1**. ένα διάνυσμα $s \in \{0,1\}^{2(n+d)}$ τέτοιο ώστε $s \in \Lambda_4^{\perp}(A)$ και $Gs = b(mod\ 4)$

  Έστω $\underline{x}, \underline{y} \in \{0,1\}^n$οι συντεταγμένες του s που αντιστοιχούν στις εισόδους και τις εξόδους αντίστοιχα. Ακόμη, έστω $\underline{w} \in \{0,1\}^n$ οι τελευταίες n μεταβλητές του s (αντιστοιχούν στις βοηθητικές μεταβλητές της εισόδου). Αφού ο A έχει ακριβώς ένα στοιχείο ίσο με 1 που αντιστοιχεί στο y και ακριβώς ένα στοιχείο ίσο με 2 που αντιστοιχεί στο w τότε η σχέση $Ax = 0\ (mod\ 4)$ μας δίνει $\underline{y} = 0$ και $\underline{w} = 0$. Συνεπώς, $C(\underline{x}) = \underline{y} = 0$ και το x αποτελεί λύση του pigeonhole problem.

## 3. Constrained Short Integer Solution

- **2.** δύο διανύσματα $s, t \in \{0,1\}^{2(n+d)}$ με $s \neq t, s - t \in \Lambda_4^{\perp}(A)$ και $Gs = Gt = b(mod\ 4)$
  Ομοίως με πάνω, ορίζουμε $\underline{x_1}, \underline{x_2}, \underline{y_1}, \underline{y_2}, \underline{w_1}, \underline{w_2} \in \{0,1\}^n$ όπου $\underline{x}$ οι είσοδοι των δύο διανυσμάτων, $\underline{y}$ οι έξοδοι και $\underline{w}$ οι βοηθητικές μεταβλητές των εισόδων. Όπως και στη πρώτη περίπτωση, η σχέση $A(s - t) = 0(mod\ 4)$ μας δίνει $\underline{y_1} = \underline{y_2}$ και $\underline{w_1} = \underline{w_2}$. Λόγω της μοναδικότητας του διανύσματος (το "πάνω" μέρος) που αποτελεί λύση στην εξίσωση $Gs = Gt = b(mod\ 4)$ και από $\underline{w_1} = \underline{w_2}$
  και $s \neq t$ έχουμε $\underline{x_1} \neq \underline{x_2}$. Ακόμη, έχουμε ότι $C(\underline{x_1}) = \underline{y_1} = \underline{y_2} = C(\underline{x_2})$ και συνεπώς τα $\underline{x_1}, \underline{x_2}$ αποτελούν λύση στο pigeonhole problem.

## 4. Collision Resistant Hash Function based on weak-cSIS.

- Θα ορίσουμε μία οικογένεια συναρτήσεων σύνοψης βασισμένη στο πρόβλημα cSIS για b=0.
- Ορίζουμε $l \in \mathbb{Z}_+$, $q = 2^l$ και $d \in \mathbb{Z}_+$. Έστω r = poly(k) τέτοιο ώστε rl < k.
- Με p(k) συμβολίζουμε κάτι μικρότερο του k δηλαδή p(k) < k.
- Ορίζουμε οικογένεια συναρτήσεων σύνοψης:

$$H_{cSIS} = \{H_{\underline{s}}: \{0,1\}^k \to \{0,1\}^{rl}\}_{\underline{s} \in \{0,1\}^{p(k)}}$$

- $Gen_{cSIS}(1^k)$ δειγματοληπτεί ένα ομοιόμορφο $\underline{s} \in \{0,1\}^{p(k)}$ και το ερμηνεύει ως ομοιόμορφο πίνακα $A \in \mathbb{Z}_q^{r \times (k+ld)}$ και ομοιόμορφα επιλεγμένο δυαδικό αναστρέψιμο πίνακα $G \in \mathbb{Z}_q^{d \times (k+ld)}$.
- $H_{(A,G)}(\underline{x})$: Για είσοδο $\underline{x} \in \{0,1\}^k$, υπολόγισε το μοναδικό $\underline{u} \in \{0,1\}^{ld}$ τέτοιο ώστε $G\begin{bmatrix}\underline{u}\\ \underline{x}\end{bmatrix} = 0 (mod\ q)$ και δώσε ως έξοδο $bd(A\begin{bmatrix}\underline{u}\\ \underline{x}\end{bmatrix} (mod\ q))$. Θυμίζουμε ότι αφού το $A\begin{bmatrix}\underline{u}\\ \underline{x}\end{bmatrix} (mod\ q)$ έχει r στοιχεία (mod q) η δυαδική διάσπασή του θα έχει rl δυαδικά ψηφία.

## 4. Collision Resistant Hash Function based on weak-cSIS.

- Ορίζουμε το weak-cSIS πρόβλημα και αποδεικνύουμε ότι ανήκει στη κλάση PWPP και είναι πλήρες για αυτή.
- **weak-cSIS πρόβλημα.**
  Είσοδος: $\underline{s} = (A, G) \in \mathbb{Z}_q^{r\times(ld+k)} \times \mathbb{Z}_q^{d\times(ld+k)}$ που ορίζει μια συνάρτηση $H_{\underline{s}} \in H_{cSIS}$.
  Έξοδος: δύο δυαδικά διανύσματα $\underline{x_1} \neq \underline{x_2}$ με $H_{\underline{s}}(\underline{x_1}) = H_{\underline{s}}(\underline{x_2})$
- **PWPP (weak PPP complexity class)**
  Ένα πρόβλημα ανήκει στη κλάση πολυπλοκότητας PWPP αν υπάρχει αναγωγή Karp από αυτό προς το Collision problem.
- **Collision problem.**
  Είσοδος: Ένα κύκλωμα C με n εισόδους και m εξόδους με m < n.
  Έξοδος: Δύο δυαδικά διανύσματα $\underline{x} \neq \underline{y}$ τέτοια ώστε $C(\underline{x}) = C(\underline{y})$
- Ως $\text{Collision}_{p(k)}$ συμβολίζουμε το Collision πρόβλημα με k εισόδους και p(k) εξόδους.

## 4. Collision Resistant Hash Function based on weak-cSIS.

- Το weak-cSIS ανήκει στην PWPP
- Θα δώσουμε μία Karp αναγωγή από το weak-cSIS στο Collision. Έστω $\underline{s}$ η είσοδος του weak-cSIS και C ένα κύκλωμα μεγέθους poly(|$\underline{s}$|) που για είσοδο $\underline{x}$ δίνει $H_{\underline{s}}(\underline{x})$. Επειδή rl < k, το C είναι έγκυρη είσοδος του Collision. Έστω $\underline{x}, \underline{y}$ οι δύο έξοδοι του Collision. Από τον ορισμό του C παρατηρούμε ότι τα $\underline{x}, \underline{y}$ αποτελούν λύση του weak-cSIS.
- Τώρα θέλουμε να δείξουμε ότι το weak-cSIS είναι PWPP-hard.
- Αρχικά, θα δείξουμε μία αναγωγή από το Collision στο $\text{Collsion}_{k-2}$.
- Παρατηρούμε ότι υπάρχει Karp αναγωγή από το Collision στο $\text{Collsion}_{k-1}$. Αυτό επειδή κάθε κύκλωμα με k εισόδους και m εξόδους μπορεί να μετατραπεί σε κύκλωμα C’ με k-1 εξόδους κάνοντας pad με μηδενικά. Κάθε σύγκρουση του C’ είναι και σύγκρουση του C. Συνεπώς, αρκεί να δείξουμε αναγωγή από το $\text{Collsion}_{k-1}$ στο $\text{Collsion}_{k-2}$.

## 4. Collision Resistant Hash Function based on weak-cSIS.

- Μετασχηματίζουμε το κύκλωμα C του $\text{Collision}_{k-1}$ σε C'.
- Το C' έχει k+1 εισόδους και k-1 εξόδους. Είναι $C'(\underline{x}, b) = C(C(\underline{x}), b)$
- Τότε το $\text{Collision}_{k-2}$ με είσοδο το C' δίνει εξόδους $\underline{y_1} = (\underline{x_1}, b_1)$ και $\underline{y_2} = (\underline{x_2}, b_2)$ με $\underline{y_1} \neq \underline{y_2}$ και $C'(\underline{y_1}) = C'(\underline{y_2})$.
- Αν $b_1 \neq b_2$ τότε τα $(C(\underline{x_1}), b_1), (C(\underline{x_2}), b_2)$ αποτελούν σύγκρουση για το C.
- $b_1 = b_2$ τότε $\underline{x_1} \neq \underline{x_2}$ και ισχύει ένα από τα ακόλουθα: $C(\underline{x_1}) \neq C(\underline{x_2})$ ή $C(\underline{x_1}) = C(\underline{x_2})$. Στη πρώτη περίπτωση τα $(C(\underline{x_1}), b_1), (C(\underline{x_2}), b_2)$ αποτελούν σύγκρουση για το C ενώ στη δεύτερη τα $\underline{x_1} \neq \underline{x_2}$.

## 4. Collision Resistant Hash Function based on weak-cSIS.

- Το weak-cSIS είναι PWPP-hard.
- Αρκεί να δείξουμε μια αναγωγή από το $\text{Collision}_{k-2}$ στο weak-cSIS.
- C είσοδος, με n δυαδικές εισόδους, r = n-2 εξόδους και d πύλες.
- Θέτουμε q = 4 και l = 2.
- Υποθέτουμε μόνο $\{\vee, \oplus, 1\}$ αφού $(x \vee y) \oplus 1 = x \bar{\vee} y$.
- Θα εκμεταλλευθούμε τις σχέσεις του πίνακα που παρουσιάσαμε προηγουμένως.
- C’ με μόνο OR ή XOR. Αντικαθιστούμε τους **1** κόμβους με $z = x_1 \vee x_2 \vee \cdots \vee x_n$.
- Ισχύει, ότι $C'(\underline{x}) = C(\underline{x})$ για $\underline{x} \neq \underline{0}$ και $C'(\underline{0}) = \underline{0}$ αφού οι πύλες OR και XOR δίνουν 0 για μηδενική είσοδο.

## 4. Collision Resistant Hash Function based on weak-cSIS.

- Έστω $G \in \mathbb{Z}_q^{d \times 2(n+r)}$ ο δυαδικός αντιστρέψιμος πίνακας που κωδικοποιεί το C' όπως αναλύσαμε στη απόδειξη του PPP-hardness του cSIS.
- Ακόμη, κατά τα ίδια, έστω $A \in \mathbb{Z}_q^{r \times 2(n+r)}$
- Το b είναι ίσο με 0 αφού έχουμε μόνο OR και XOR πύλες.
- Μετασχηματίζουμε το C' για να χειριστούμε τις περιπτώσεις όπου $\underline{x} = \underline{0}$
- Το C'' έχει ακόμα μία έξοδο $z = x_1 \vee x_2 \vee \cdots \vee x_n$.
- Έστω (A', G') ή νέα είσοδος του weak-cSIS.
- Έστω $(\underline{x_1}, \underline{x_2})$ η έξοδος του weak-cSIS. Πρέπει λοιπόν τουλάχιστον ένα να είναι διάφορο του $\underline{0}$. Και δεν υπάρχει σύγκρουση $\underline{0}$, $\underline{x}$ επειδή θα διαφέρουν στο z.
- Συνεπώς, είναι $\underline{x_1}, \underline{x_2} \neq \underline{0}$ και αποτελούν μία σύγκρουση για το C ολοκληρώνοντας την αναγωγή μας.

## 4. Collision Resistant Hash Function based on weak-cSIS.

- Αποδείξαμε την ασφάλεια της $H_{cSIS}$ μόνο στη χειρότερη περίπτωση. Αλλά μας ενδιαφέρει η μέση περίπτωση.
- **$SIS_{q,n,m,\beta,p}$ πρόβλημα.**
  Είσοδος: Ένας ομοιόμορφα τυχαίος πίνακας $A \in \mathbb{Z}_q^{n \times m}$ όπου $m > 2nlog(q)$
  Έξοδος: Ένα διάνυσμα $r \in \mathbb{Z}_q^m$ τέτοιο ώστε $\| r \|_p \leq \beta$ και $Ar = 0 \ (mod \ q)$
- Αν το SIS είναι δύσκολο στη μέση περίπτωση τότε η $H_{cSIS}$ είναι ανθεκτική σε συγκρούσεις. Αυτό γιατί αν $(\underline{x_1}, \underline{x_2})$ μια σύγκρουση της $H_{(A,\ 0)}$ τότε το $\underline{x_1} - \underline{x_2}$ είναι λύση του SIS με είσοδο A.
- Αφού όλες οι οικογένειες ανθεκτικών σε συγκρούσεις συναρτήσεων σύνοψης ανήκουν στην PWPP (εξ ορισμού) και το weak-cSIS είναι PWPP-complete τότε υπάρχει κατανομή κλειδιών $\underline{s} \in \{0,1\}^{p(k)}$ ώστε η $H_{cSIS}$ να είναι ανθεκτική σε συγκρούσεις αν υπάρχει τουλάχιστον μία CRHF.

## 5. Προβλήματα Lattice και η κλάση PPP.

- Θα δώσουμε μερικούς ορισμούς και προβλήματα που έχουν σχέση με πλέγματα και ύστερα θα αποδείξουμε τη σχέση τους με τις κλάσεις πολυπλοκότητας που αναφέραμε.
- $dist(t, L) = min_{x \in L} \| x - t \|$
- $\lambda_i(L(B)) = min_{x \in L \setminus span(v_1, \ldots, v_{i-1}), x \neq 0} \| x \|$
- **γ-SVP Πρόβλημα.**
  Είσοδος: Μία βάση $B \in \mathbb{Z}^{n \times n}$
  Έξοδος: Ένα διάνυσμα $v \in L$ τέτοιο ώστε $\| v \| \leq \gamma(n) \cdot \lambda_1(L(B))$
- **γ-CVP Πρόβλημα.**
  Είσοδος: Μία βάση $B \in \mathbb{Z}^{n \times n}$ και ένα διάνυσμα στόχο $t \in \mathbb{Q}^n$
  Έξοδος: Ένα διάνυσμα του πλέγματος τέτοιο ώστε $\| v - t \| \leq \gamma(n) \cdot dist(v, L(B))$
- **Minkowski$_p$ Πρόβλημα.**
  Είσοδος: Μία βάση $B \in \mathbb{Z}^{n \times n}$ και το πλέγμα $L = L(B)$
  Έξοδος: Ένα διάνυσμα $x \in L$ τέτοιο ώστε $\| x \|_p \leq n^{1/p} det(L)^{1/n}$

## 5. Προβλήματα Lattice και η κλάση PPP.

- **Για $p \geq 1$ και $p = \infty$, Minkowski$_p$ ανήκει στο PPP**
  Για κάθε $p \geq 1$ ισχύει $\| x \|_p \leq n^{1/p} \| x \|_\infty$. Συνεπώς, αν $\| x \|_\infty \leq det(L)^{1/n}$ τότε $\| x \|_p \leq n^{1/p} det(L)^{1/n}$ και το Minkowski$_p$ ανάγεται στο Minkowski$_\infty$.
- Άρα αρκεί να δείξουμε μια αναγωγή από το Minkowski$_\infty$ στο Blichfeldt.
- Έστω $B \in \mathbb{Z}^{n \times n}$ η είσοδος του Minkowski.
- Ακόμη, $l = \lfloor det(L)^{1/n} \rfloor$, $S = ([0, l]^n \cap \mathbb{Z}^n) \setminus \{0\}$
  και $s = |S| = (l + 1)^n - 1$.
- Ορίζουμε αναπαράσταση τιμής του S $(s, V_S(x)) = (s, V_{[0,l]^n}(x + 1))$
- Ισχύει $|S| \geq det(L) \Leftrightarrow (\lfloor det(L)^{1/n} \rfloor + 1)^n \geq det(L)^{1/n} + 1$
- Έστω B και S οι είσοδοι του Blichfeldt.
  1. Ένα διάνυσμα x με $x \in S \cap L$. Αφού $x \in S \Rightarrow \| x \|_\infty \leq \lfloor det(L)^{1/n} \rfloor$ και συνεπώς είναι λύση του Minkowski$_\infty$.
  2. Δύο διανύσματα $x \neq y$ με $x, y \in S$ και $x - y \in L$. Αφού $x, y \in S$ τότε $x - y \in [-l, l]^n$ και $\| x - y \|_\infty \leq det(L)^{1/n}$ και το $x - y$ είναι λύση του Minkowski$_\infty$.

## 5. Προβλήματα Lattice και η κλάση PPP.

- **Το $\sqrt{n} - iSVP$ ανήκει στο PPP για ιδανικά πλέγματα.**
- Για τα ιδανικά πλέγματα ισχύει $\lambda_1(L) = \lambda_2(L) = \cdots = \lambda_n(L)$ και από το δεύτερο θεώρημα του Minkowski έχουμε: $\lambda_1\lambda_2 \cdots \lambda_n \geq det(L)$. Επομένως είναι $\lambda_1 \geq det(L)^{1/n}$. Μαζί με το δεύτερο θεώρημα του Minkowski που λέει ότι $\lambda_1 \leq \sqrt{n}\, det(L)^{1/n}$ το Minkowski$_2$ με είσοδο L λύνει το $\sqrt{n} - SVP$ στο L.

## 6. Κρυπτογραφικές υποθέσεις στο PPP.

- Αν PPP=FP τότε δεν υπάρχουν μονόδρομες μεταθέσεις οι οποίες βασίζονται στο πρόβλημα διακριτού λογαρίθμου σε ομάδα $\mathbb{Z}_p^*$ αλλά και σε κρυπτογραφικές υποθέσεις όπως αυτή του RSA, ειδικά είδη ελλειπτικών καμπυλών και το πρόβλημα παραγοντοποίησης Blum ακεραίων (γινόμενο δύο Blum πρώτων). Οπότε, αν PPP=FP τα παραπάνω γίνονται ανασφαλή.
- Αν PWPP=FP τότε δεν υπάρχουν συναρτήσεις σύνοψης ανθεκτικές σε συγκρούσεις. Μιας και η κατασκευή τους μπορεί να βασισθεί στο πρόβλημα του διακριτού λογαρίθμου σε ομάδα $\mathbb{Z}_p^*$ οπότε η υπόθεση για την ασφάλεια του διακριτού λογαρίθμου γίνεται ανασφαλής ακόμη και αν PWPP=FP.
- Στη συνέχεια, ορίζουμε τι σημαίνει γενική ομάδα. Ακόμη, ορίζουμε το DLOG πρόβλημα και αποδεικνύουμε ότι ανήκει στη κλάση PPP.

## 6. Κρυπτογραφικές υποθέσεις στο PPP.

- **Γενική ομάδα.**
  Γενική ομάδα (G,*) είναι μία κυκλική ομάδα για την οποία υπάρχει ένα κύκλωμα που περιγράφει bijection $I_G: G \to [ord(G)]$, την οποία αναφέρουμε ως συνάρτηση δείκτη.
- Υπάρχει κύκλωμα $f: [ord(G)] \times [ord(G)] \to [ord(G)]$, το οποίο ονομάζουμε συνάρτηση λειτουργίας ομάδας και ισχύει $x, y \in G, I_G(x * y) = f(I_G(x), I_G(y))$.
- Η γενική ομάδα περιγράφεται από:
  1. Ένα αριθμό *g* στο [ord(G)] τέτοιο ώστε $I_G(\boldsymbol{g}) = g$ όπου $\boldsymbol{g}$ γεννήτορας της G.
  2. Ένα αριθμό *id* στο [ord(G)] τέτοιο ώστε $I_G(\boldsymbol{id}) = id$ όπου **id** το ουδέτερο στοιχείο της G.
  3. Ένα πολυωνυμικό κύκλωμα για τη συνάρτηση λειτουργίας ομάδας f.
- Για παράδειγμα για την $\mathbb{Z}_p^*$ έχουμε *g* = c-1, *id* = 0 και $f(x, y) = (x + 1)(y + 1) - 1(mod\ p)$ όπου c ένας γεννήτορας της G.

## 6. Κρυπτογραφικές υποθέσεις στο PPP.

- **DLOG πρόβλημα.**
  Είσοδος: Μία υποτιθέμενη γενική ομάδα (G,*) που περιγράφεται ως (g, id, $f_G$, $I_G$) και ένας στόχος $y \in [s]$
  Έξοδος: Ένα από τα ακόλουθα:
  1. Ένα $x \in [s]$ με $I_G(\boldsymbol{g}^x) = y$
  2. δύο $x, y \in [s], x \neq y$ τέτοια ώστε $I_G(\boldsymbol{g}^x) = I_G(\boldsymbol{g}^y)$
- Στον ορισμό του DLOG δεν απαιτούμε η ομάδα να είναι γενική. Στη δεύτερη περίπτωση η ομάδα δεν είναι γενική. Αυτός ο ορισμός μας βοηθά να αποδείξουμε εύκολα ότι το πρόβλημα ανήκει στο PPP.
- **Το DLOG ανήκει στο PPP.**
- Έστω η είσοδος (g, id, $f_G$, $I_G$) η είσοδος και $n = \lceil \log(s) \rceil$.
- Κατασκευάζουμε $C: \{0,1\}^n \to \{0,1\}^n$ τ.ω $C(\underline{x}) = |I_G(\boldsymbol{g}^{bc(\underline{x})}) - y|$

## 6. Κρυπτογραφικές υποθέσεις στο PPP.

- Οι έξοδοι μπορεί να είναι:
- **1.** ένα δυαδικό διάνυσμα $\underline{x}$ με C($\underline{x}$) = $\underline{0}$. Τότε, ισχύει το x = bc($\underline{x}$) είναι ο διακριτός λογάριθμος του y από τη κατασκευή του C.
- **2.** δύο δυαδικά διανύσματα $\underline{x} \neq \underline{y}$ με C($\underline{x}$) = C($\underline{y}$). Σε αυτή τη περίπτωση έχουμε $I_G(\boldsymbol{g}^{bc(\underline{x})}) = I_G(\boldsymbol{g}^{bc(\underline{y})})$ υποδεικνύει ένα από τα επόμενα:

  a) H $f_G$ δεν είναι έγκυρη συνάρτηση λειτουργίας ομάδας

  b) Το $I_G$ δεν είναι έγκυρο κύκλωμα δείκτη για το G

  c) $\boldsymbol{g}^{bc(\underline{x})} = \boldsymbol{g}^{bc(\underline{y})}$

Σε οποιαδήποτε περίπτωση, το (g, id, $f_G$, $I_G$) δεν αποτελεί έγκυρη είσοδο του DLOG προβλήματος.

- Το πρόβλημα του αν το DLOG είναι PPP-hard είναι ανοικτό. Ακόμη, επειδή δεν γνωρίζεται αν οι ελλειπτικές καμπύλες είναι γενικές ομάδες, δε ξέρουμε αν το πρόβλημα ανήκει στο PPP για ομάδες πάνω σε ελλειπτικές καμπύλες.

## 7. Τελευταίες σκέψεις

- Τα προβλήματα Blichfeldt και cSIS είναι PPP-πλήρη ενώ το weak-cSIS είναι PWPP-πλήρες.
- Το πρόβλημα cSIS μας βοηθά να φτιάξουμε μια οικογένεια συναρτήσεων σύνοψης (hash functions) βασιζόμενοι στη δυσκολία του προβλήματος SIS (και είναι collision resistant αν το SIS είναι hard on average).
- Αν PPP = FP ή PWPP = FP το πρόβλημα του διακριτού λογαρίθμου είναι εύκολο και πολλές κρυπτογραφικές υποθέσεις καταρρέουν.

# Σας ευχαριστώ!