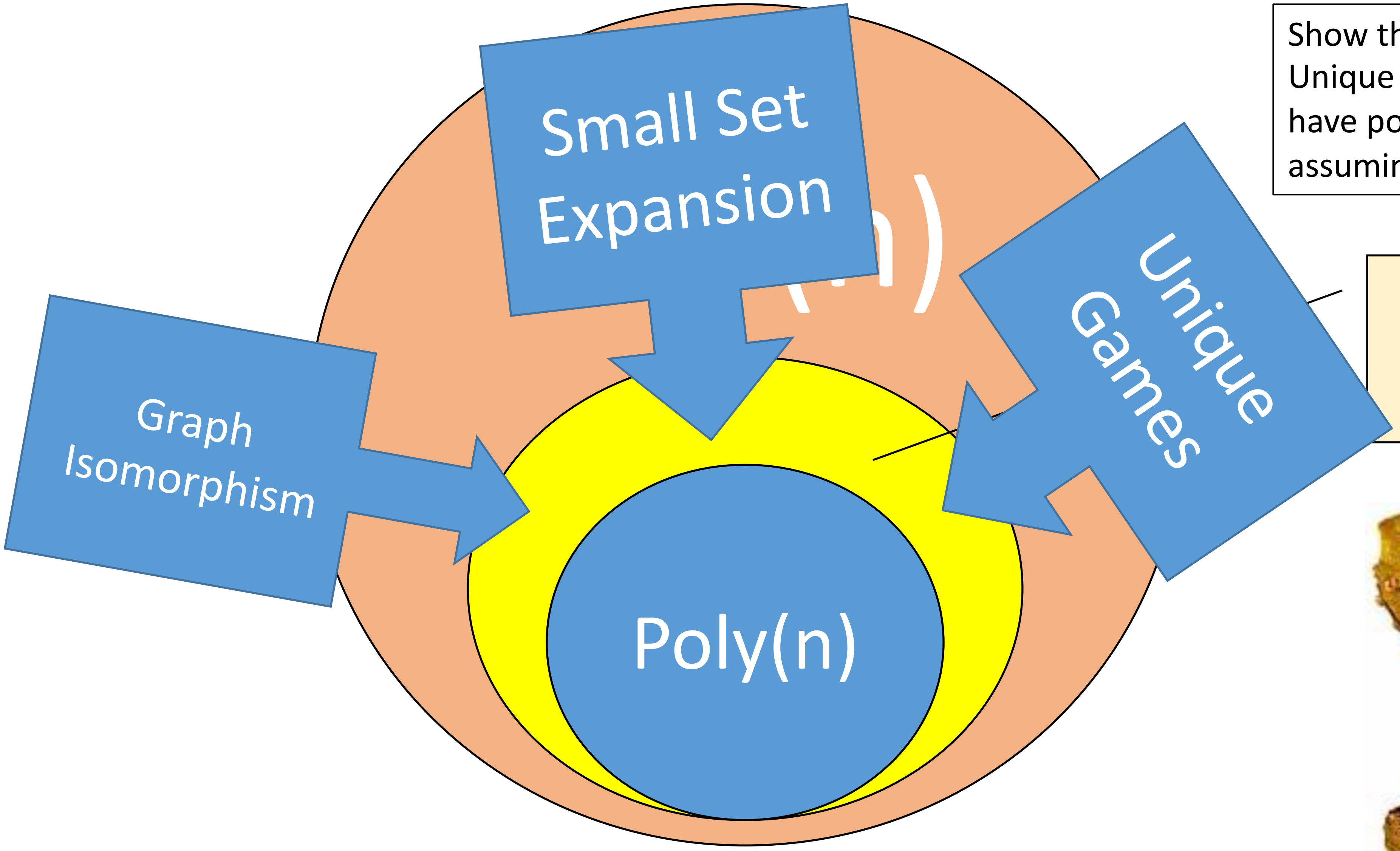
# Birthday Repetition: Tool for proving quasi-poly hardness

Young Kun Ko
Princeton
Dagstuhl 2016

# Motivation




Show that
Unique Games does not
have poly(n) algorithm
assuming – blah

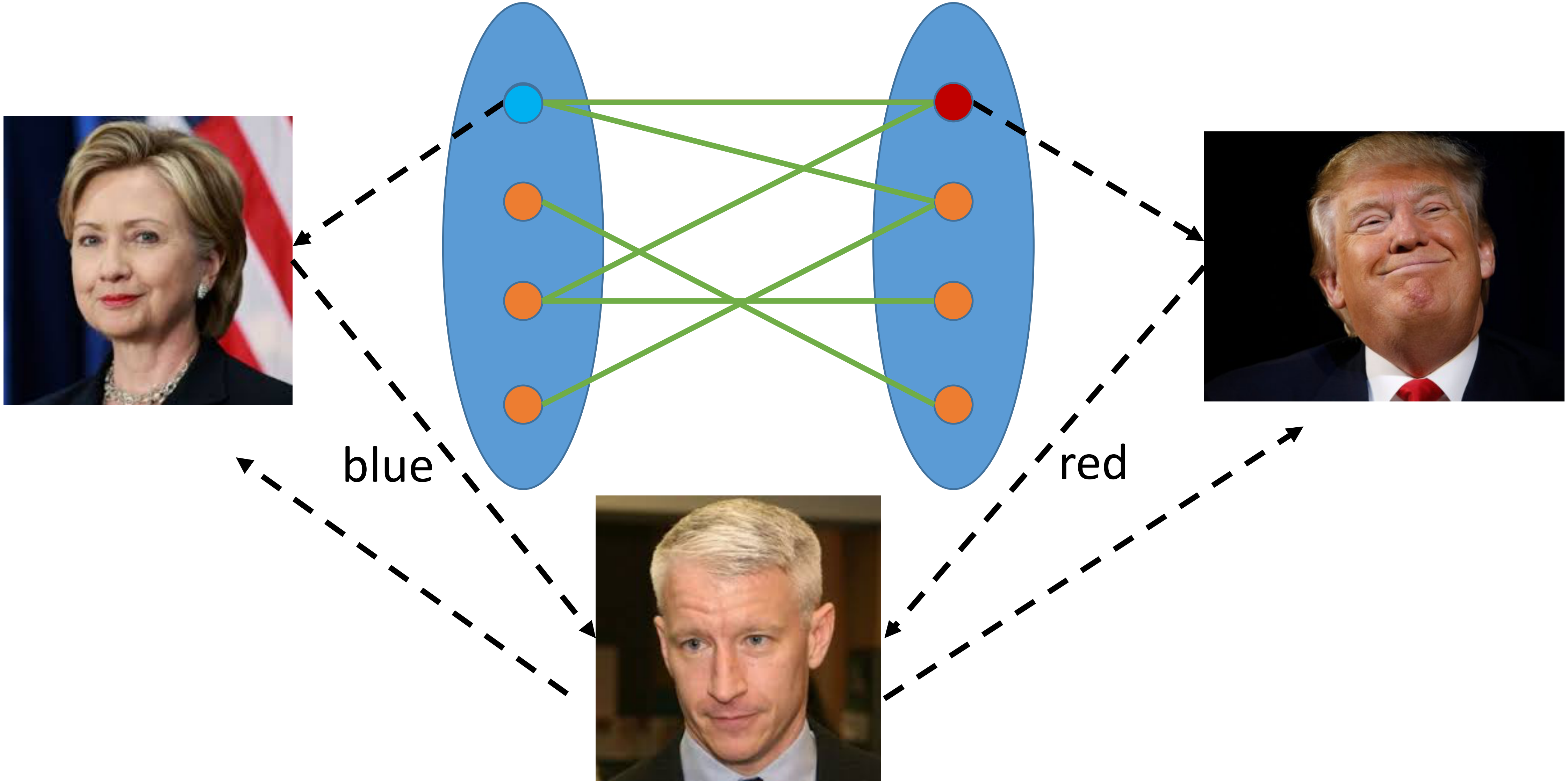
$2^{n^{\epsilon}}$ , $2^{polylog\, n}$

IS SUCH GAP a REAL GAP ?

# I. What is Birthday Repetition?

Based on [Aaronson Impagliazzo Moshkovitz 14], [Manurangsi Ragahavendra 16]

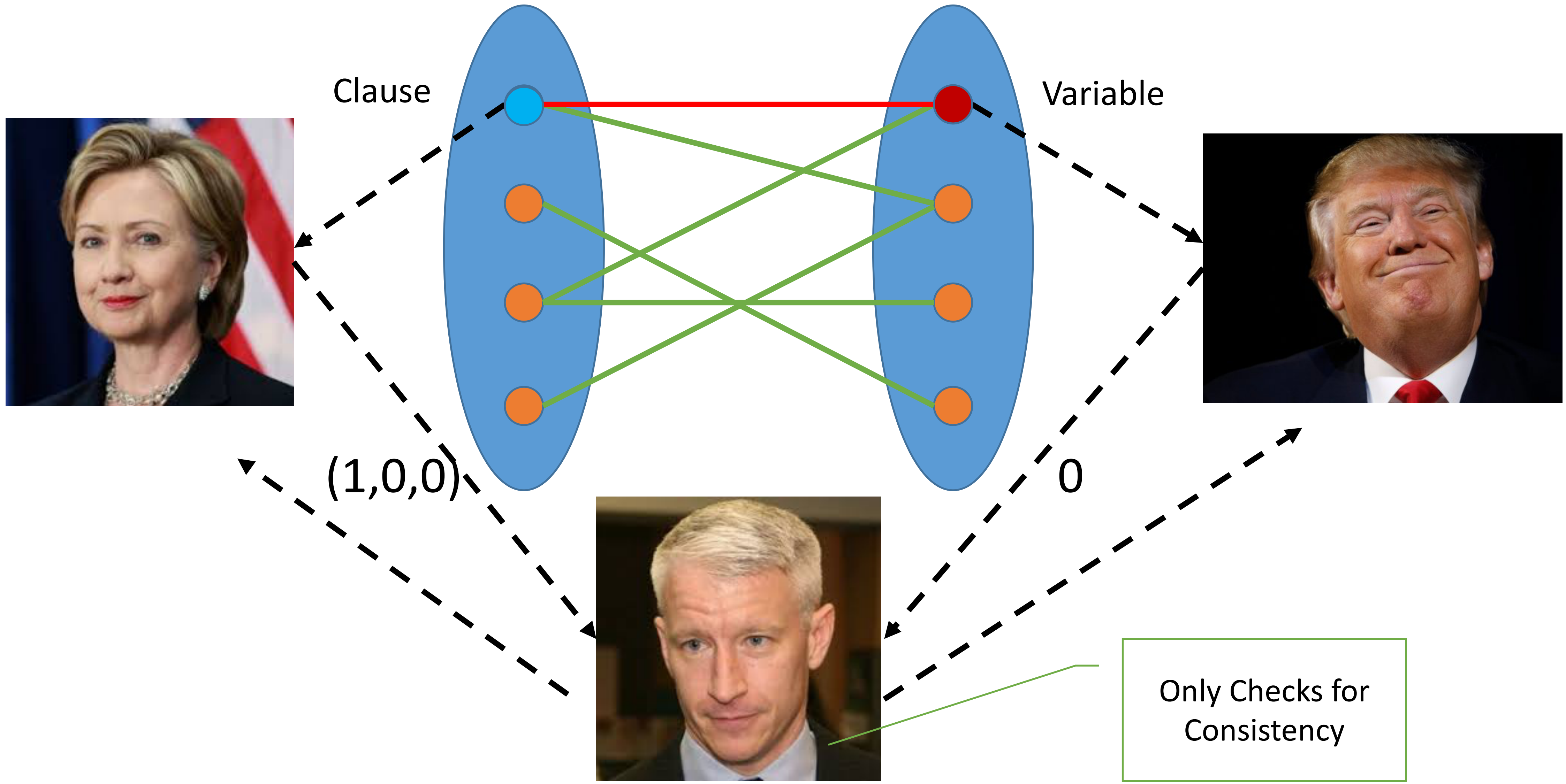
# 2 Prover Game (2CSP)



# More facts on 2-Prover Game

- PCP Theorem can be viewed as a 2-Prover game
  - But Arora et al. PCP is too big for our use
- **Projection Game** : If Alice's answer "projects" Bob's answer
- **Unique Game**: Alice's answer and Bob's answer pair is a permutation
- Dinur ['05] **Quasi-Linear (n polylog n)** constant gap (NP-hard) [3SAT]
- Moshkovitz Raz ['08] **Almost-Linear ($\boldsymbol{n^{1+o(1)}}$)** constant gap for any constant (NP-hard) [Large Alphabet]

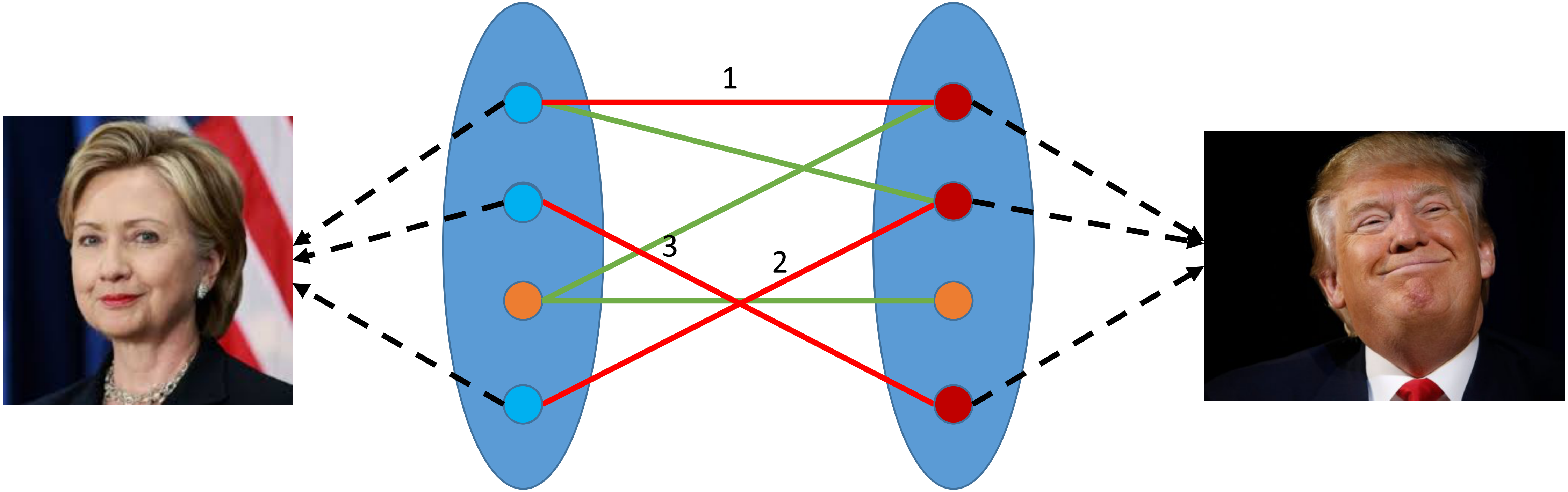
# Why is 2-Prover Game related to 3SAT



# Proof

- Fix any Bob’s assignment
- Note that it is it inconsistent with at least $\epsilon$ fraction of the clauses
- If you choose one of such clauses, the probability of detecting inconsistency is exactly 1/3
- Value of the two-prover game is at most $1-\frac{\epsilon}{3}$ QED.

# (Usual) Parallel Repetition




- Tool to show hardness for any constant
- Reduction blow up : poly(n)
- A tool for having reductions in Exp(n)

# Brief History of Parallel Repetition

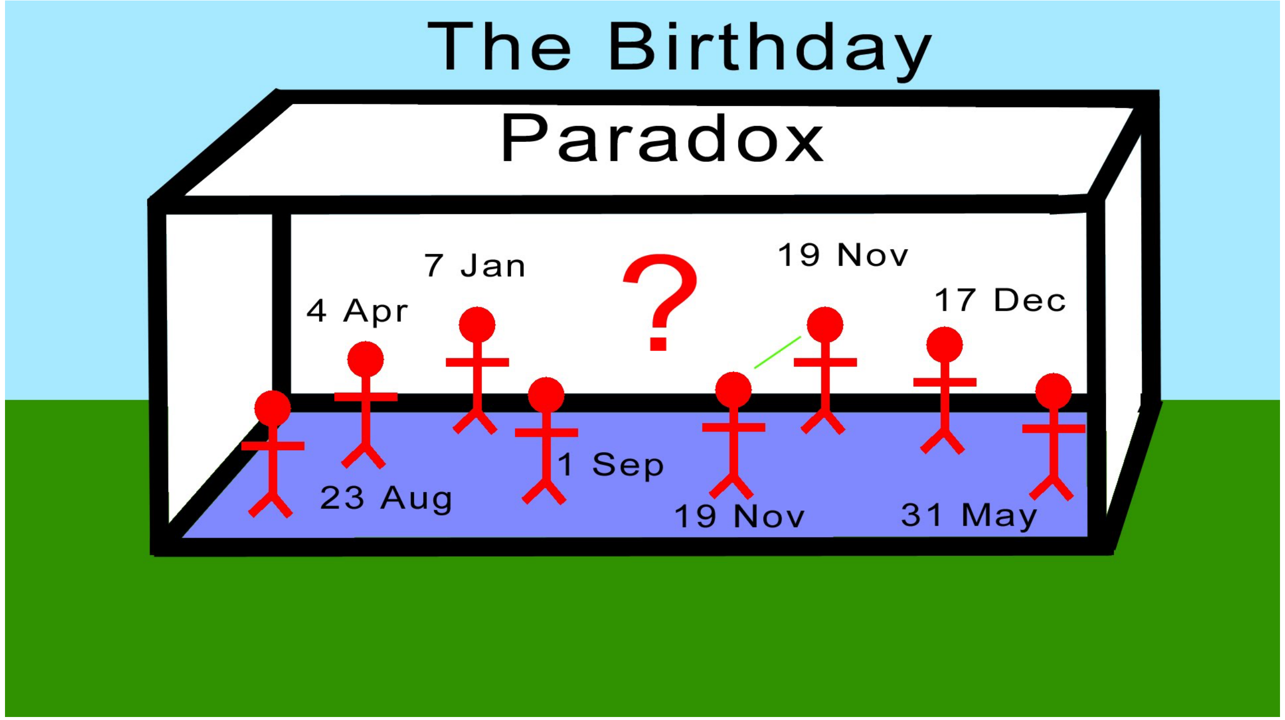
- Theorem stated as but later found as a bug by Fortnow
  - it's obvious that it decays exponentially $(1-\epsilon)^n$ …
- First exponential decay proved by [Raz'98] $(1-\epsilon^{32})^{n/\log s}$
- Simplified by [Hol'07] [BG'15] $(1-\epsilon^{3})^{n/\log s}$
  - Tight by Feige Verbitsky game
- For projection game [Rao '08] [DS '14] [BG'15] $(1-\epsilon^{2})^{n}$
  - Tight via counter-example by Raz'08

Proof extremely hard ☹

# Why is Parallel Repetition hard ?

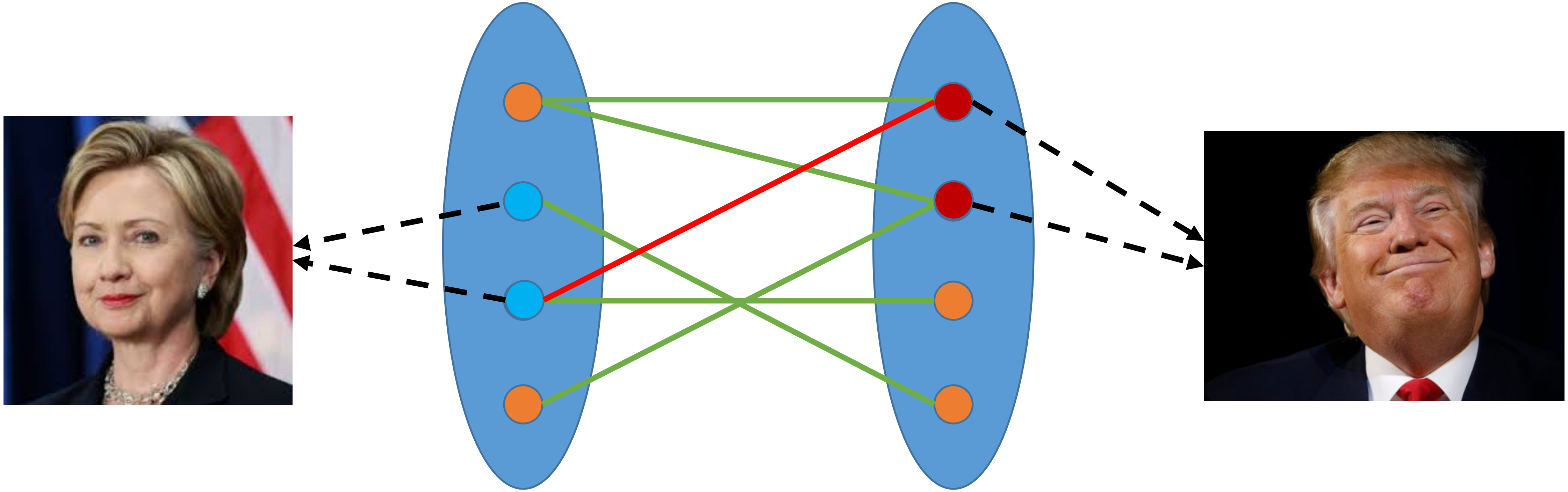
- Inputs and outputs are **CORRELATED** !!! – The answer for each coordinate does not need to depend only on the input on that coordinate !
- Can we BREAK the correlation ??? (i.e. $I(X;Y) = 0$) And at what cost ?
  - If $I(X;Y) = 0$ , then we call such game **Free game**
  - Much easier to prove Parallel Repetition in such cases
  - Barak et al showed **strong exponential decay** for Free Projection game

# Pre-Req: Birthday Paradox




- Given random two sets of size $\widetilde{\Omega}(\sqrt{n})$, from the universe of size $n$ there exists an intersection w.h.p !!
- Proof ) $\dfrac{\binom{n-\sqrt{n}}{\sqrt{n}}}{\binom{n}{\sqrt{n}}} \approx \left(1 - \frac{1}{\sqrt{n}}\right)^{\sqrt{n}} = \Theta(1)$

# Birthday Repetition



- **Birthday Repetition** : Pick two random sets of challenge of size $\widetilde{\Omega}(\sqrt{n})$
- Indeed I(X;Y) = 0 (by design!)
- Introduced in [AIM'14]

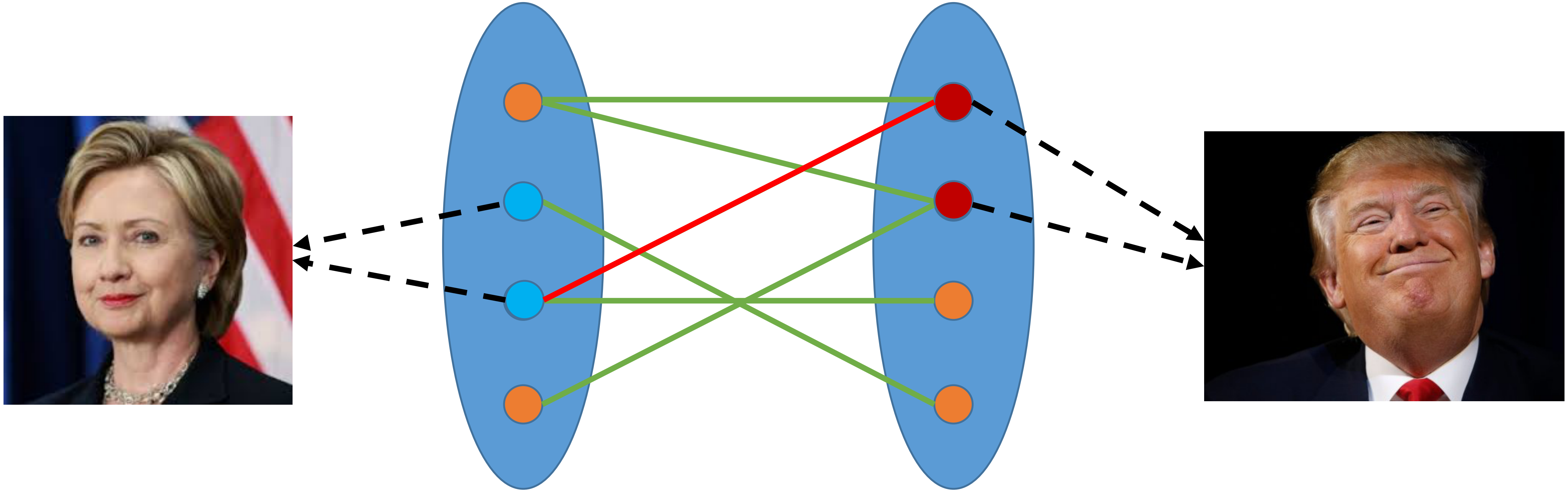
# Size of the Reduction ?

- **# of Variables =** $\binom{n}{\sqrt{n}} \sim 2$ **nential Size**
- **If $N = 2^{\sqrt{n}}$, then $N^{\log N} = 2^{n}$**
- If one assumes n-sized instance **requires $2^{\Omega(n)}$-time**, then we get quasi-polynomial time Hardness!
- Main Question : Does Birthday Repetition preserve the value ?

**ETH (Weak)**

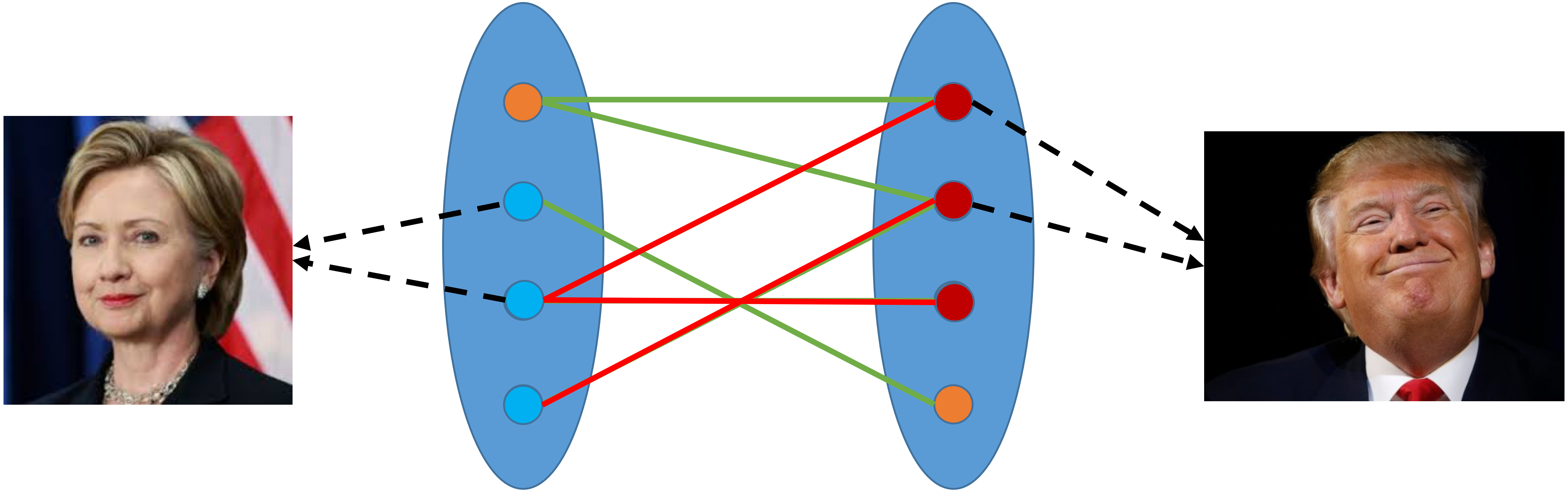
If val(G) = 1, value after the repetition is still 1.
If val(G) < 1 – eps, value after the repetition is $1 - \Omega(\epsilon)$

# Brief Proof – value upper bound



- Suppose Alice and Bob **knows which vertices are going to be checked** by the Referee – makes the game easier
- Then the game is essentially the original game – with some tilted distribution [AIM’14]

# Birthday Repetition + Parallel Repetition



- Picking a larger set will lead to having a larger intersection
- Larger Intersection roughly corresponds to k-repeated value
- Embed the repeated game ! [Proof of MR’16]

# Can we “improve” the Birthday Repetition

- Unfortunately **NO**! (Quasi-Poly Upper-Bound)
- Sub-Sampling 101 : Denser the graph, easier it is to approximate !! (In fact O(log n) samples suffice) [Barak et al ’08]
- Enumerate over **all possible strategies** over some sub-sampled challenges !

# Summary

- Using Birthday Repetition, Can transform any given 2 Prover Game to a **Free game**
- Then starting from known NP-hard two player games (Dinur / Moshkovitz-Raz) , can show that $\varepsilon$-approximation (additive) to Free-game is quasi-poly hard (under ETH) !
- Matching Upper Bounds known [AIM’14] [BH’13]

# Questions about Birthday Repetition

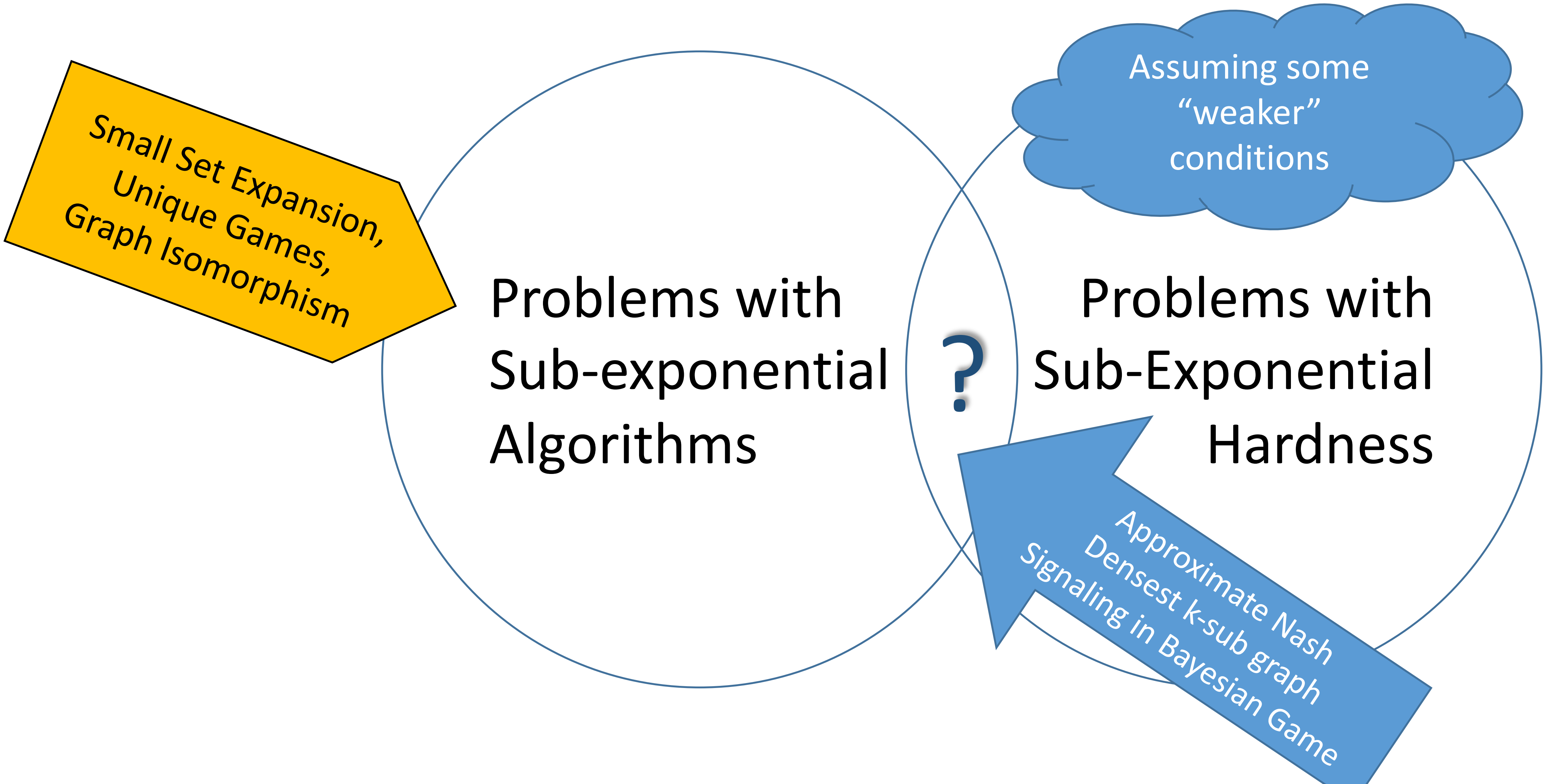
- Avoid using Parallel Repetition as the black-box in [MR ‘16]
- Instead use Birthday Repetition to tell us about Parallel Repetition
- Non-trivial lower bounds in the value of games under Birthday Repetition ??
  - Should be able to **reduce the constant** in Parallel Repetition !!

# Why do we care about the constant?

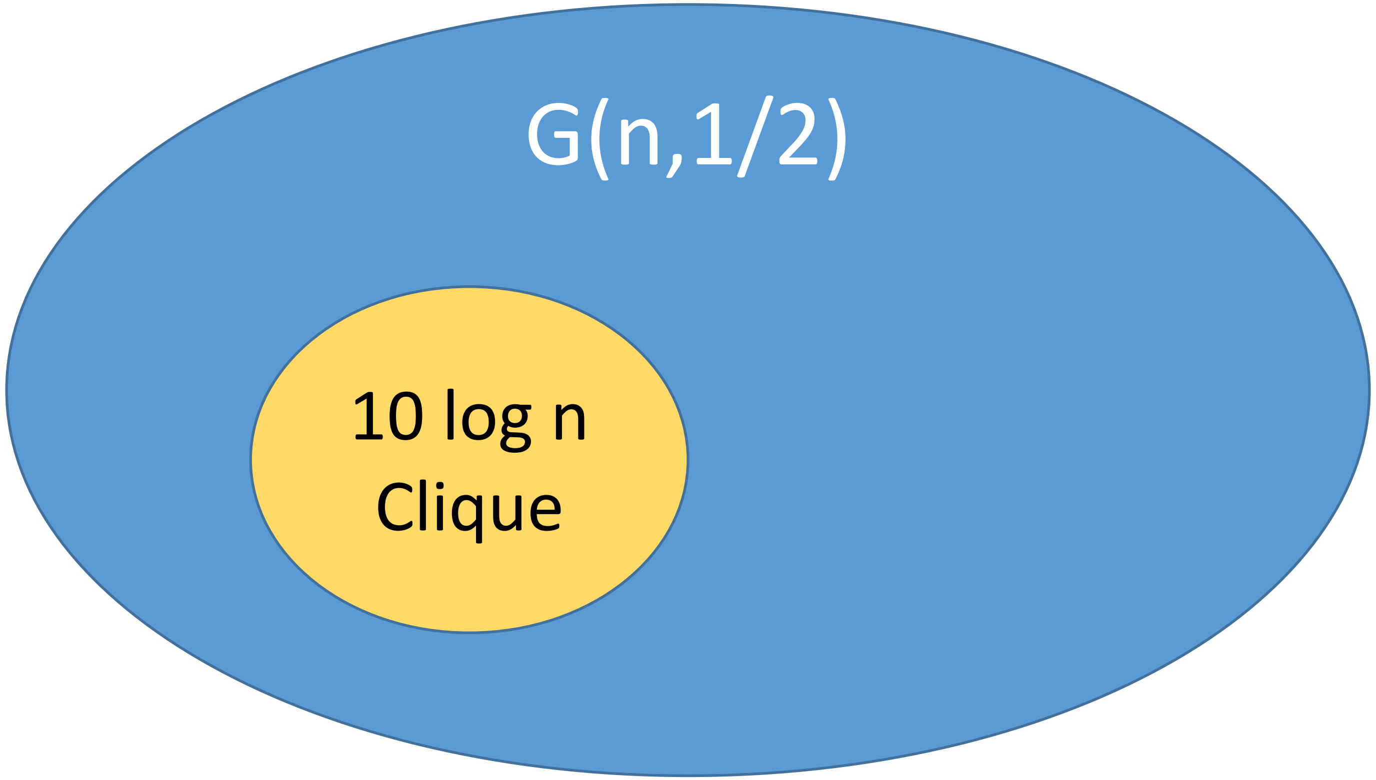
- Any improvement in the constant (2) leads to showing MAX-CUT is equivalent to UG
  - $1-\epsilon$ vs. $1\ -\sqrt{\epsilon}$ MAX-CUT is equivalent to Unique Games
- Lower bound for UG becomes much more accessible !!

# II. Applications

# What kind of problems to look for ?



# Planted Clique Conjecture



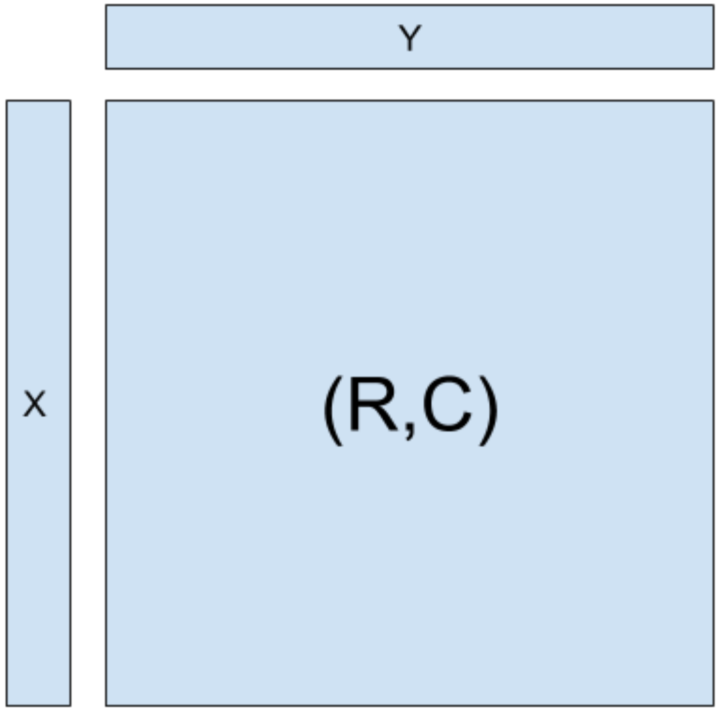

- Is the naïve algorithm ( $n^{\mathrm{O}(\log n)}$ ) the best algorithm ?
- Average-case Hardness – it is hard on average

# Application: 2-Player Games

Based on [Braverman **K** Weinstein' 15], [Cheng **K** '16],

[Bhaskara Cheng **K** Swamy '16], [Rub '16]

# Approximate Nash Equilibrium



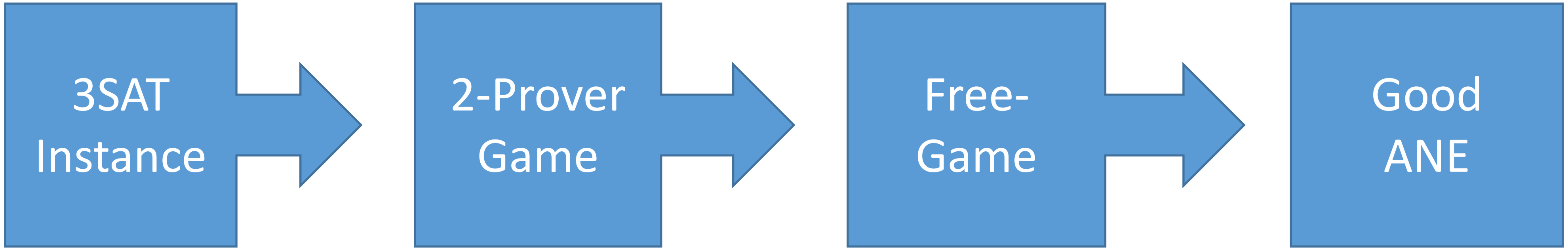

$x^T R\, y > e_i^T Ry + \epsilon$

$x^T C\, y > x^T C e_i + \epsilon$

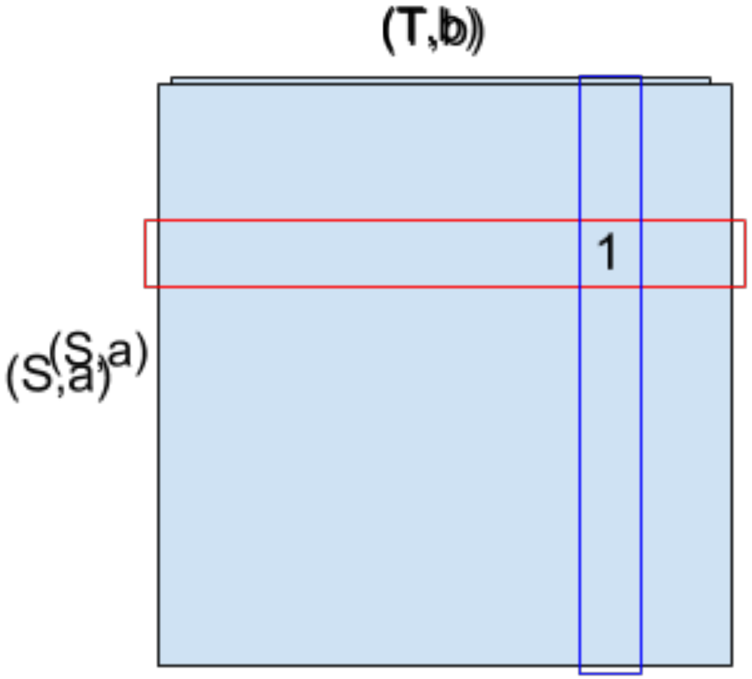
**Good Nash ) Total Payoff must be good !**

- Alice, Bob plays a (strategic) bimatrix game, represented by payoff matrix $(R, C)$
- Equilibrium → No player has incentive to deviate
- $\epsilon$-approximate Nash → No player has more than $\epsilon$ incentive to deviate
- Quasi Poly Upper Bound [LMM'03] Hidden Clique Lower Bound [HK'09]

# Chain of Reduction

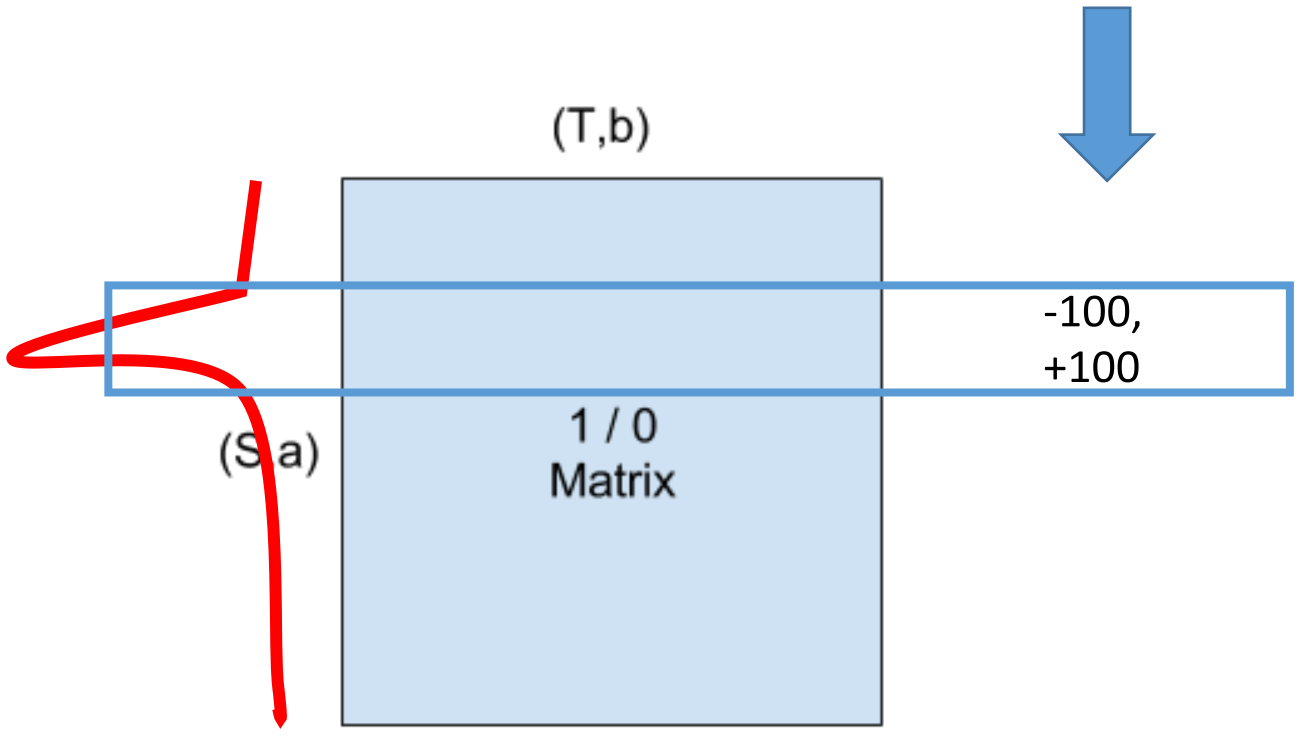


# The "Trivial" Reduction




- Each row corresponds to Alice's choice of $O(\sqrt{n})$-size tuple of challenges and corresponding assig nt to it (column as Bob's)
- Problem with the reduction ?
  - Distribution over the challenges can be mes up by the players (NO REFEREE !)

# Hitting Set Argument in 2-player game



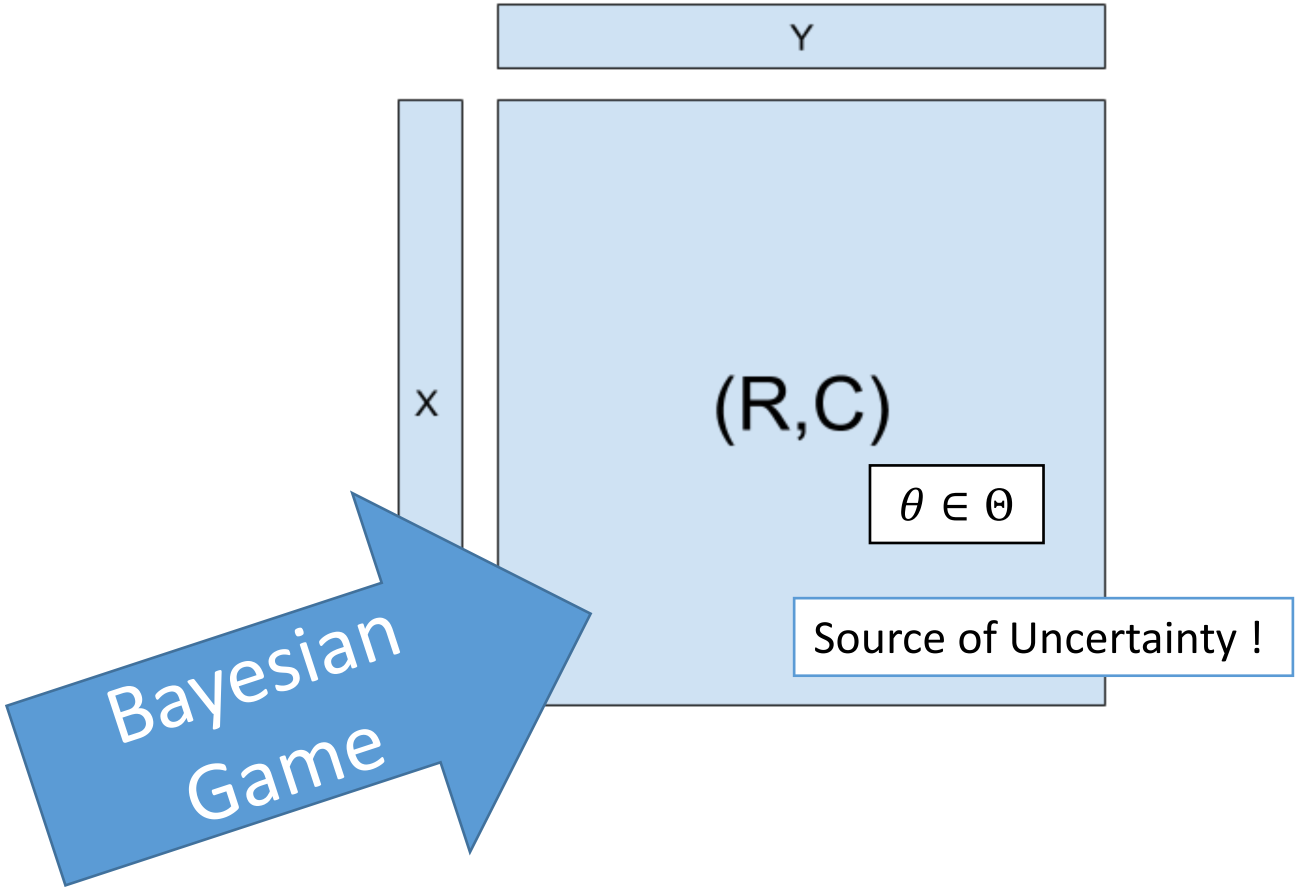

- Inspired by [HK'09]
- Any ”concentrated” strategy gets punished !
- Measure of concentration ?? – appearance of singleton variable

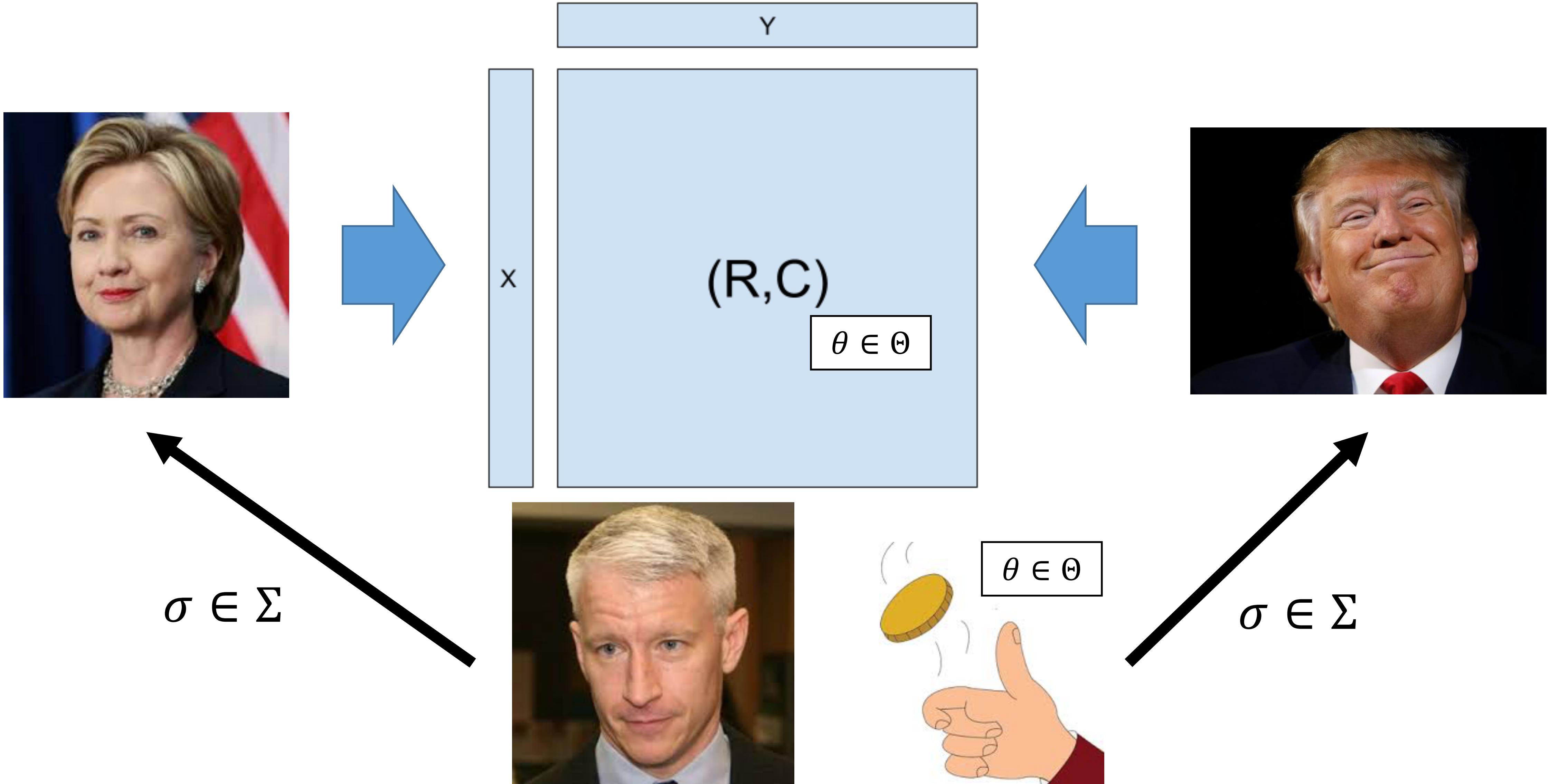
# New Payoff Matrix

- Any good ANE need to have uniform marginals over the singletons
- 5 lines of equation to show that if one has uniform marginals over the singletons, indeed it preserves the value

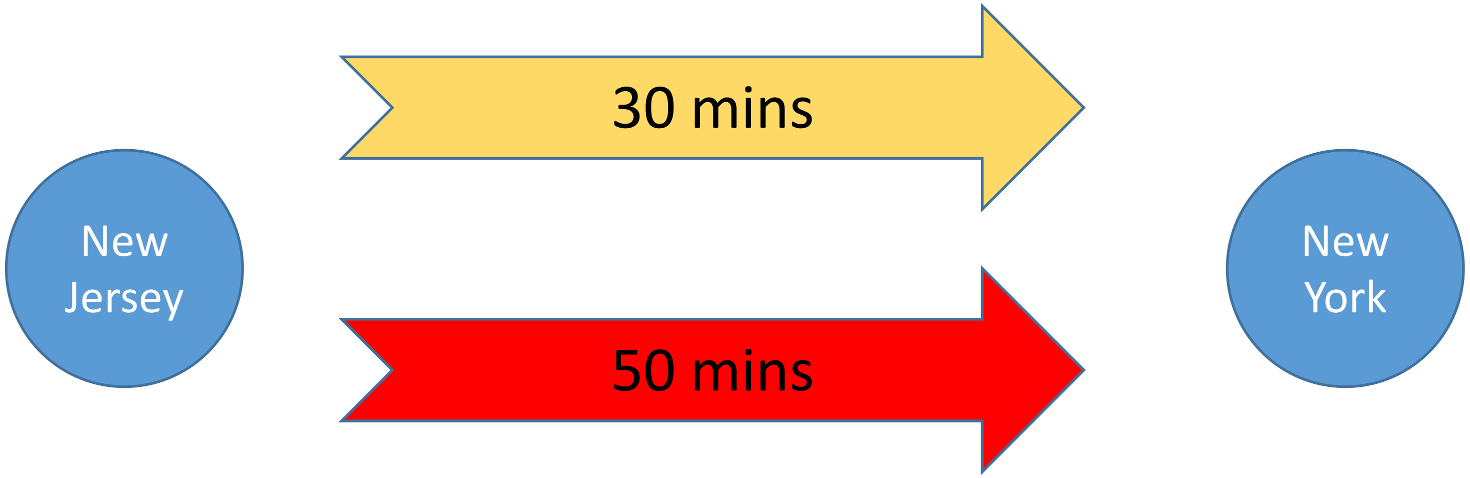
QED

# Signaling in zero-sum Bayesian Game




Y
X
(R,C)
θ ∈ Θ
σ ∈ Σ
θ ∈ Θ
σ ∈ Σ

# Real Life Example – Road Network

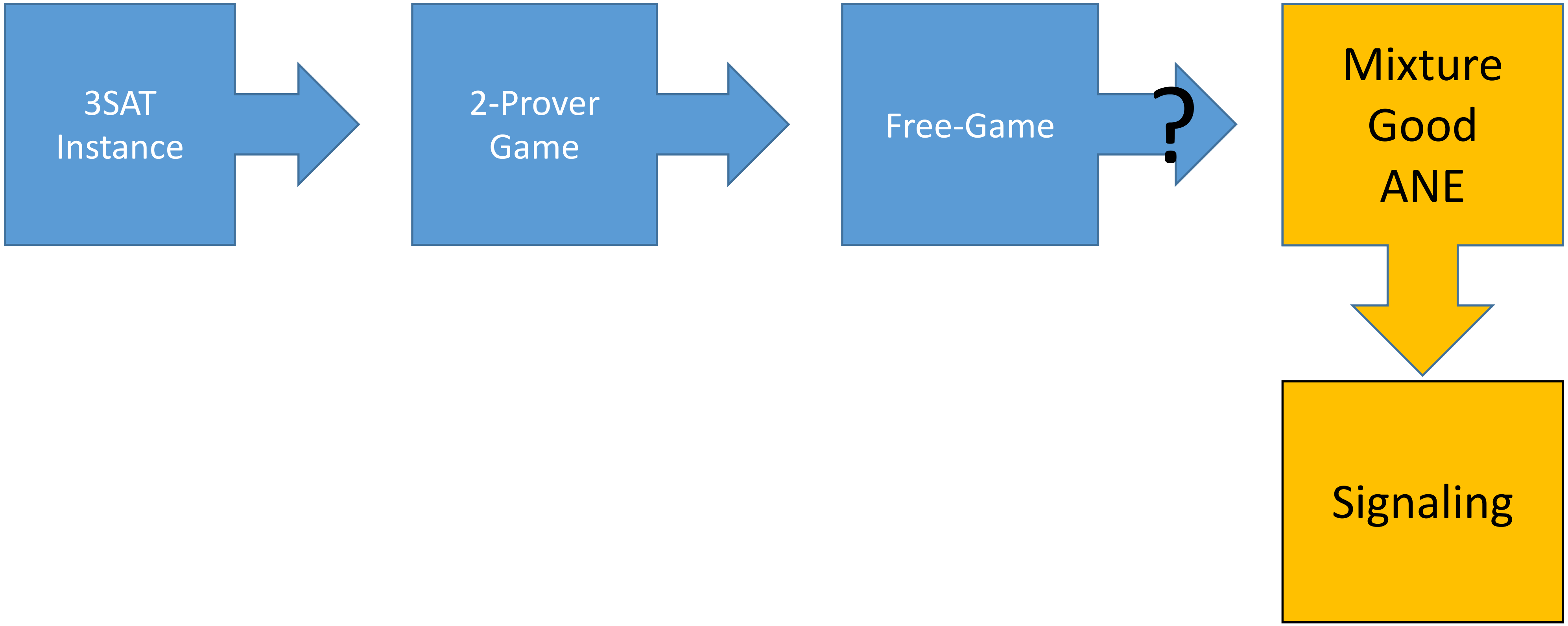



In particular, full information is not necessarily the BEST signaling scheme

# History

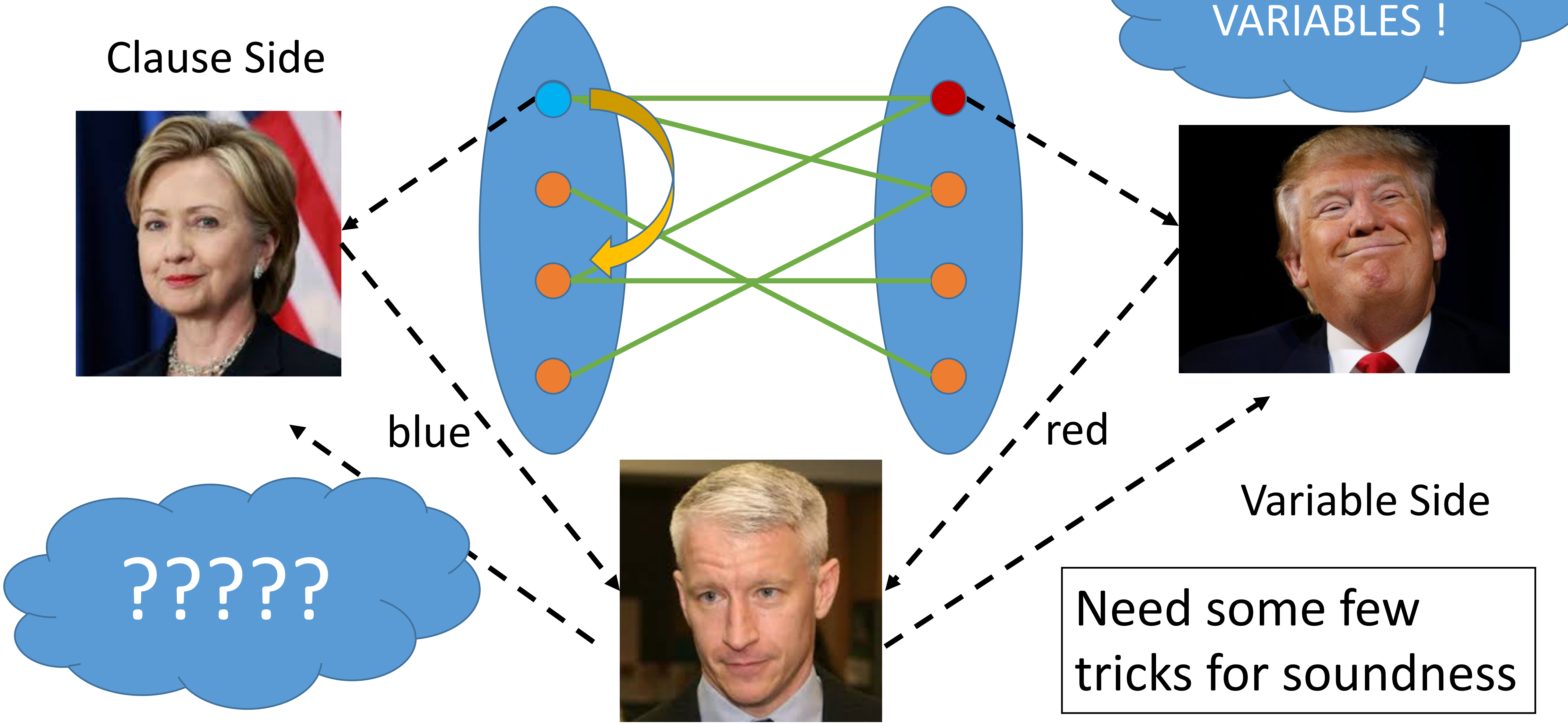
- Focuses on **Zero-Sum** since we want the hardness of the problem to come only from finding the signaling scheme, not finding the equilibrium
- [Dug’14] showed that assuming planted clique, no FPTAS for finding the best signaling scheme (for Alice’s payoff)
- [BC**K**S’15] showed that no PTAS (assuming planted clique)
- Matching QPTAS [Dug’14], [BC**K**S’15]
- Can reduce to checking whether ”uniform” distribution (on Alice’s side) is in convex hull of good ANE via [BC**K**S’15] – Mixture ANE

# Reduction Chain



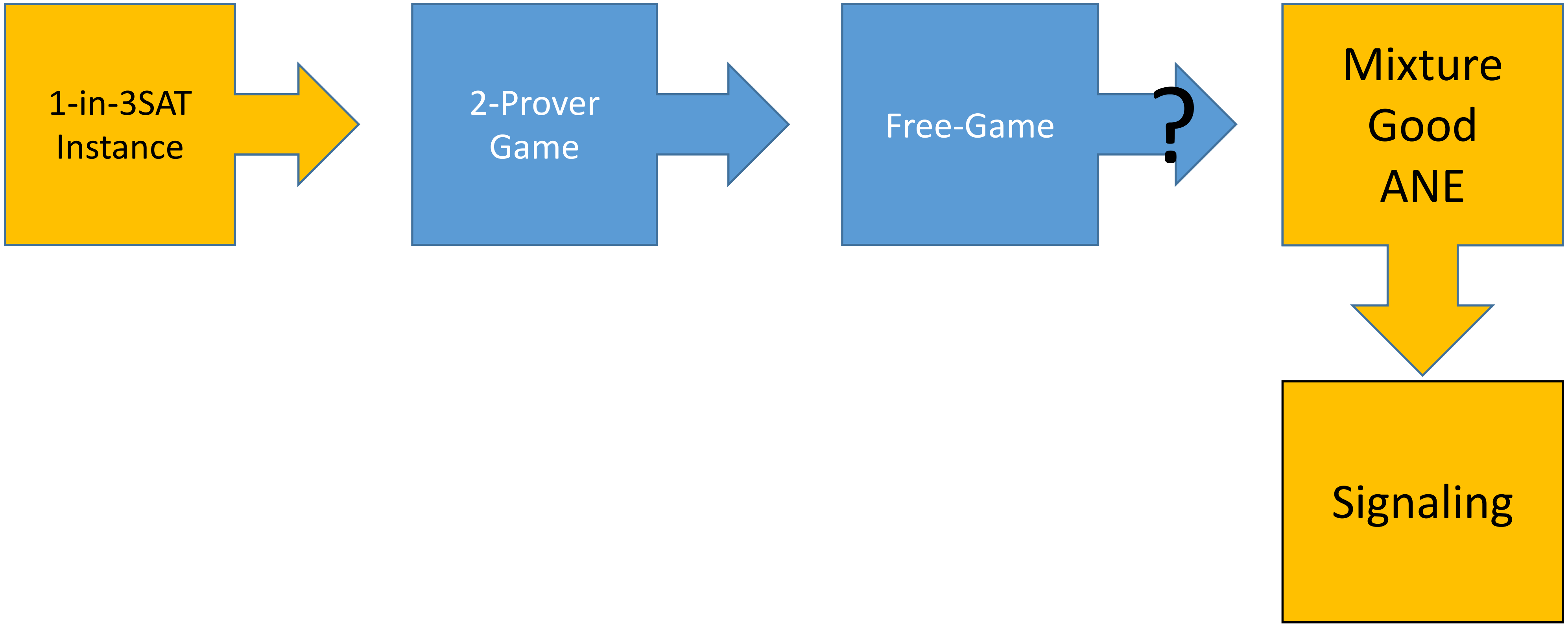
# Key Idea : Obfuscating the instance

PERMUTE THE VARIABLES !




Need some few tricks for soundness

# Reduction Chain



**Completeness**

- Because of the permutation, the satisfying assignment becomes well-spread ! (due to 1-in-3 SAT)

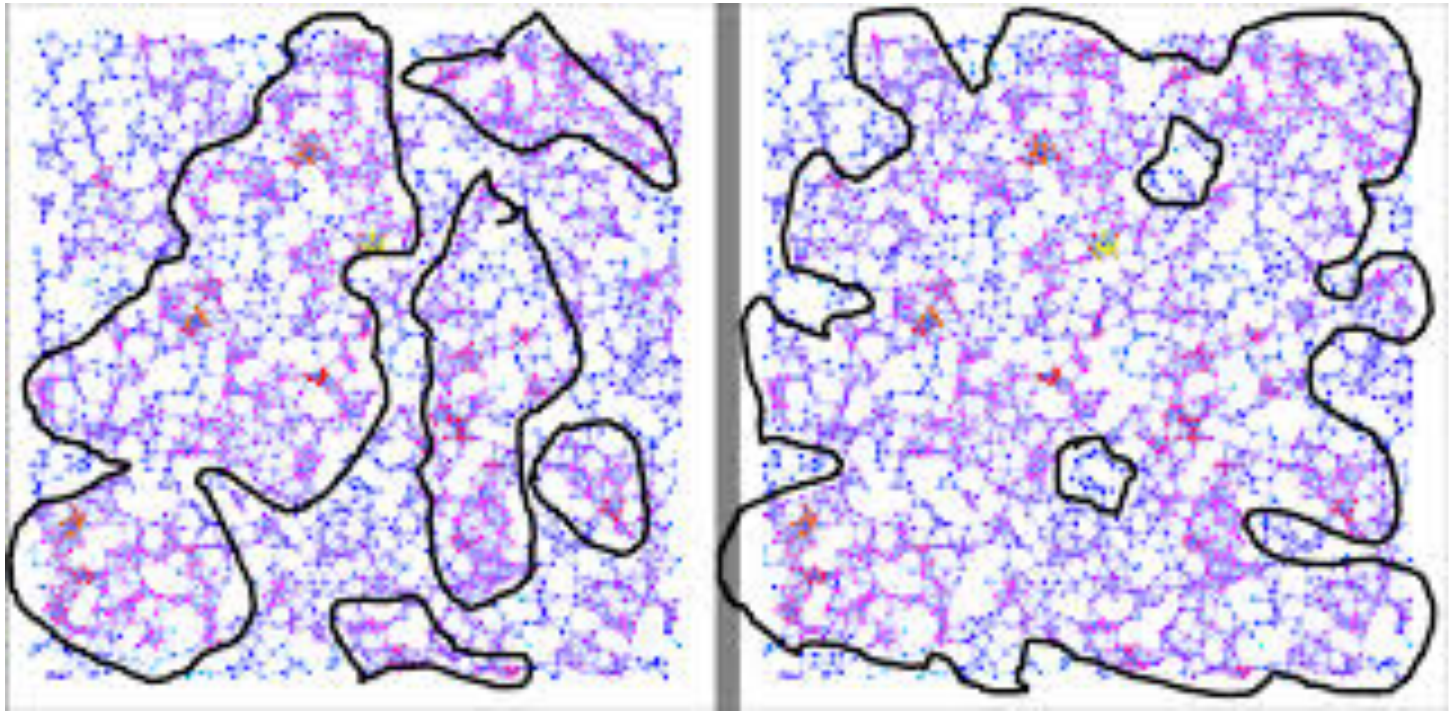
**Soundness**

- Cannot cheat too much by switching the permutation per variable
- Add “cheating” as a measure of concentration !!

# Application: Densest k subgraph

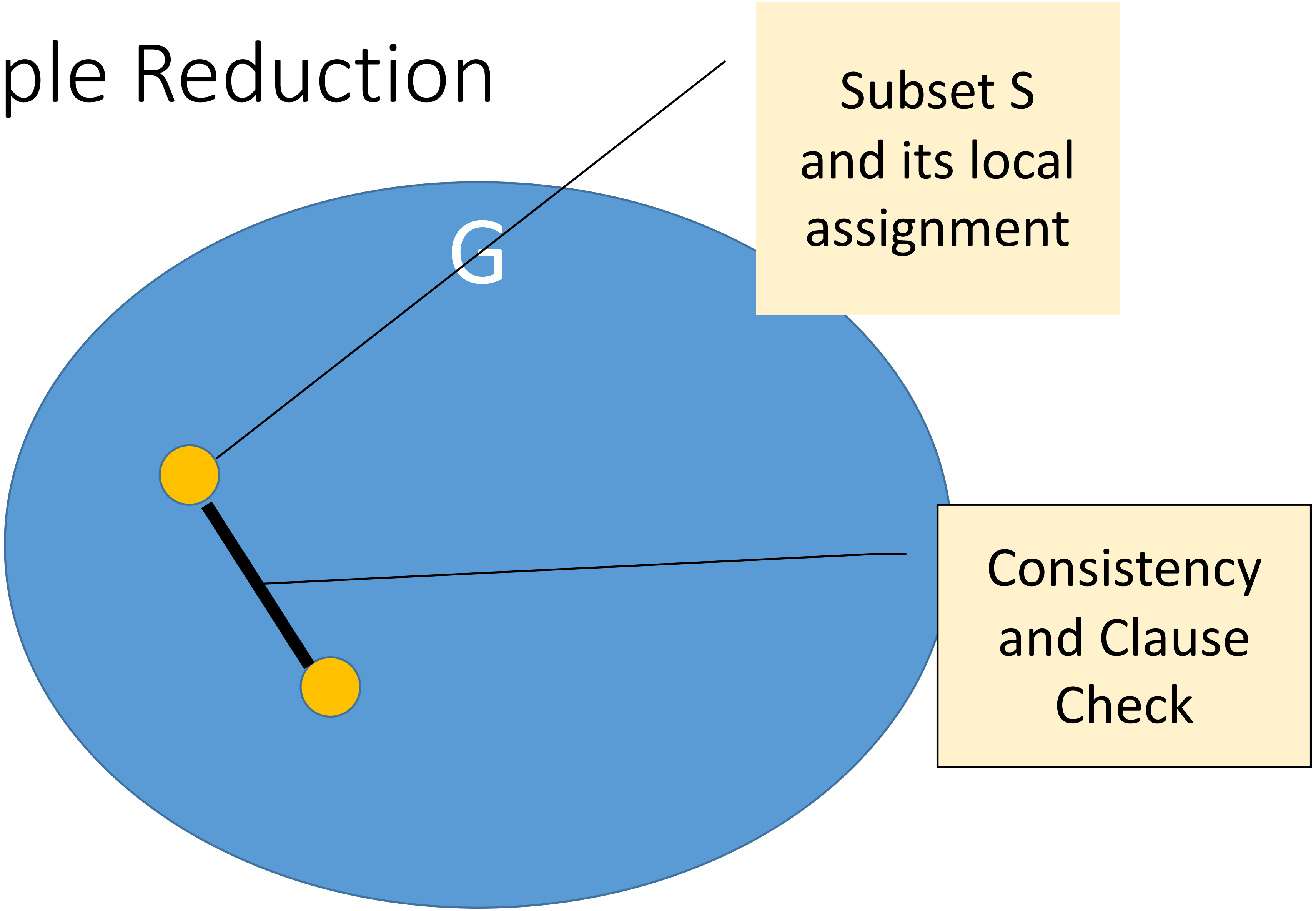
Based on [Braverman **K** Rubinstein Weinstein’ 17]

# Densest-k-Subgraph Problem



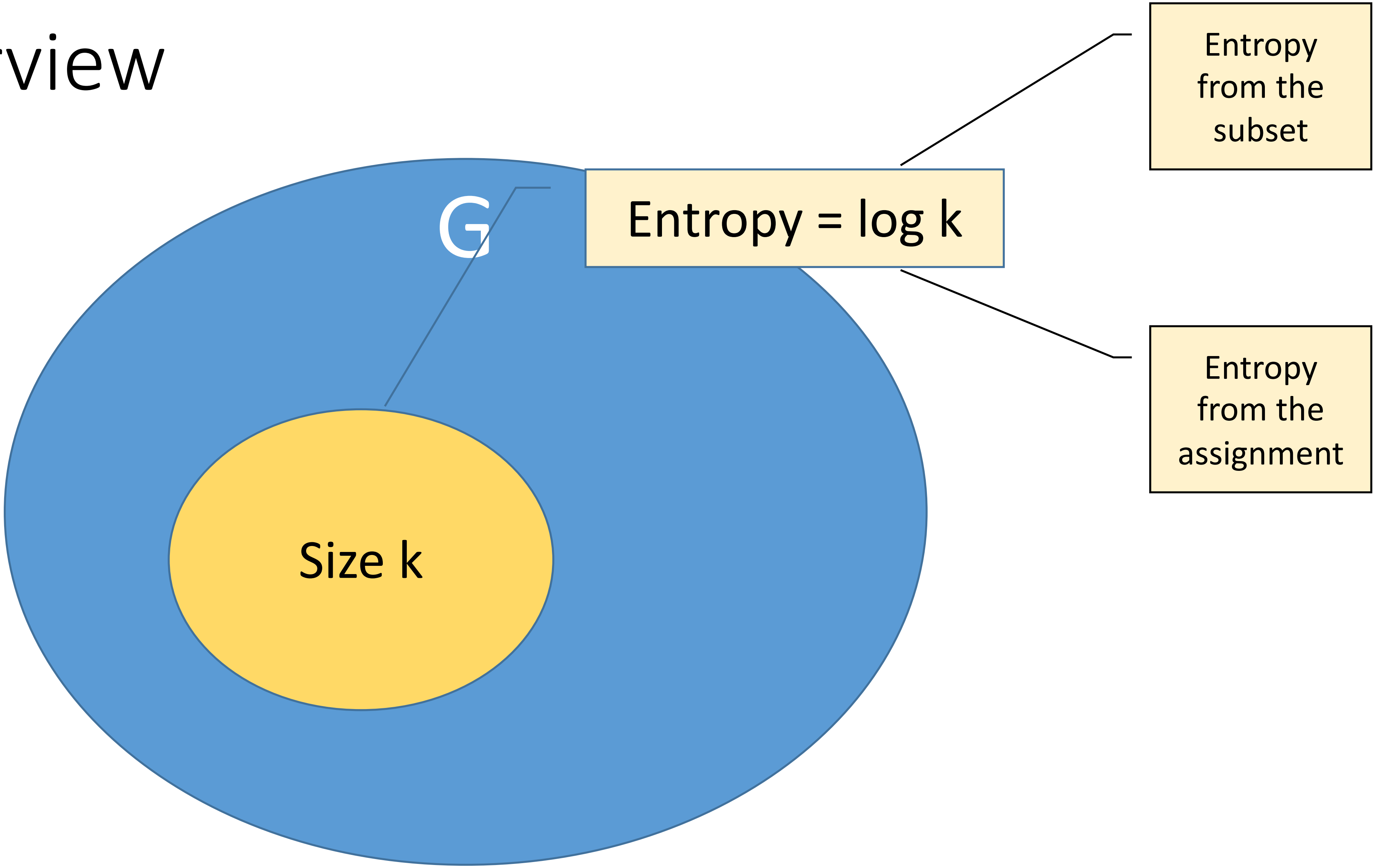
- Given $G = (V, E)$ and $k < |V|$, find $S \subset V$ of size $k$ with the highest density
- Worst case version of Planted Clique Problem
- Quasi-polynomial "additive" approximation is known [FS'97, Bar'15]
- Perfect Completeness : Clique vs. a bit less than a clique

# Very Simple Reduction




FGLSS Graph

# Proof Overview



- **Lemma 1** : If Entropy from the assignment is high then you lose density from consistency
- **Lemma 2** : If Entropy from subset is high then you lose density from Clause Checking

QED

# And many more to come …

# Open Problems

- Amplification of Densest k-subgraph completeness vs. soundness
  - A lot of evidences to believe so …
- Finding good approximate Nash Equilibrium for **anonymous game**
- Expanding the technique to **SETH** regime
- Lower bounds for Small Set Expansion & Unique Games

# Any Questions?