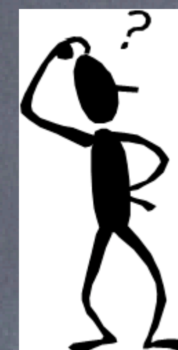
Security Amplification for Interactive Cryptographic Primitives

Yevgeniy Dodis (NYU)
Russell Impagliazzo (UCSD & IAS)
Ragesh Jaiswal (Columbia University)
Valentine Kabanets (SFU)

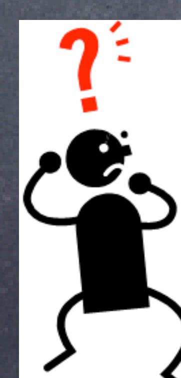
Security Amplification

Weakly secure construction: C



↓ Security Amplification ↓

Strongly secure construction: C'

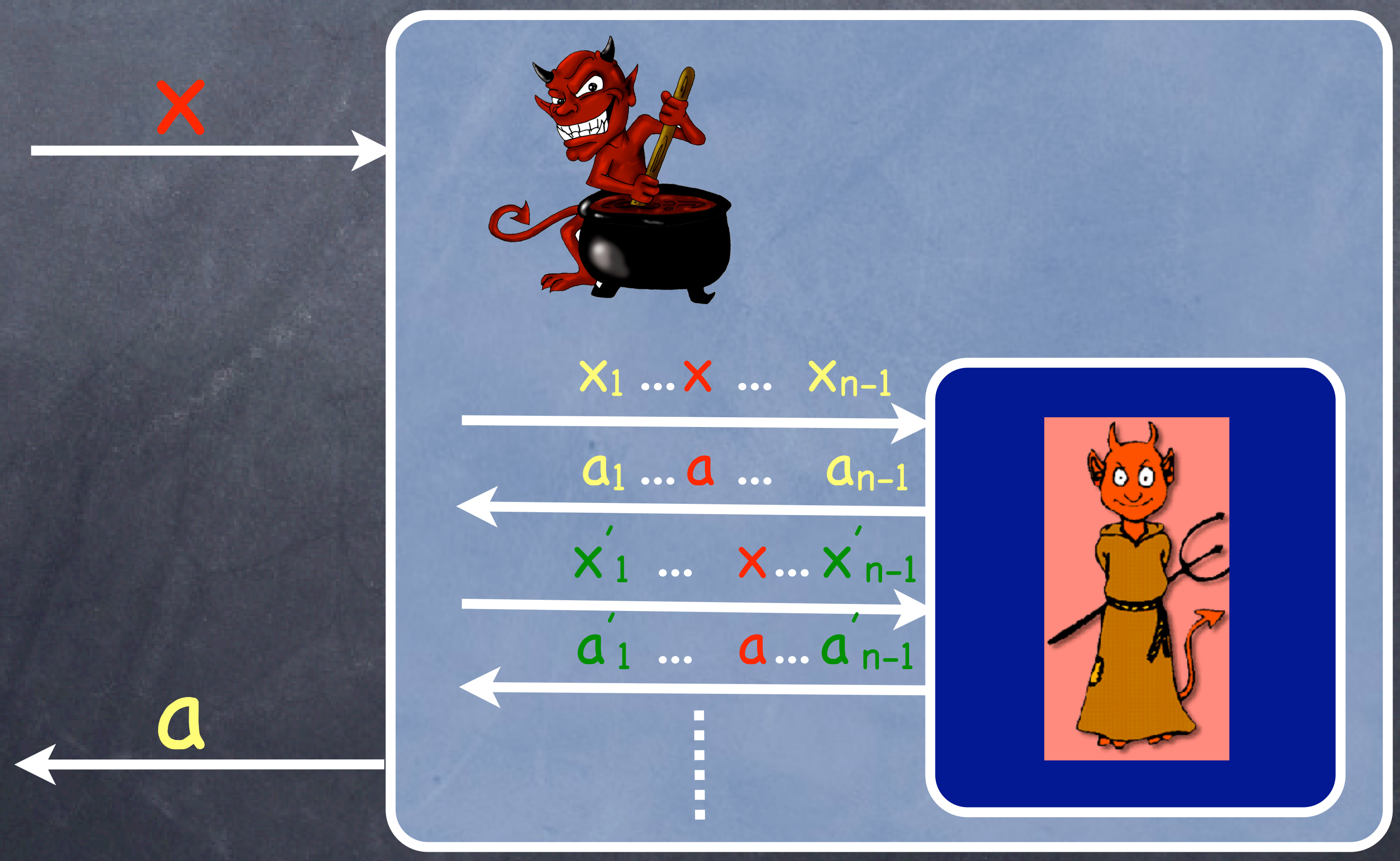


Security Amplification

- A natural approach for security amplification is parallel repetition/Direct Product construction.
- Intuition: Breaking multiple independent copies should be much harder than breaking one copy.
- Ideally, if one copy is δ-hard (can be broken with probability at most $(1-\delta)$), then n copies should be $(1-(1-\delta)^n)$-hard.

Security Amplification

- This is easy to show in an information-theoretic setting.
- We need to show this in a computational setting.



DP Theorems (The success story)

- Non-interactive protocols
  - One-way functions [Yao82, Gol01]
  - Collision Resistant Hash Functions [CRS+07]
  - Encryption schemes [DNR04]
  - Weakly verifiable puzzles [CHS05, IJK08]
- What about interactive protocols?
  - Turns out to be more complicated.

DP Theorems

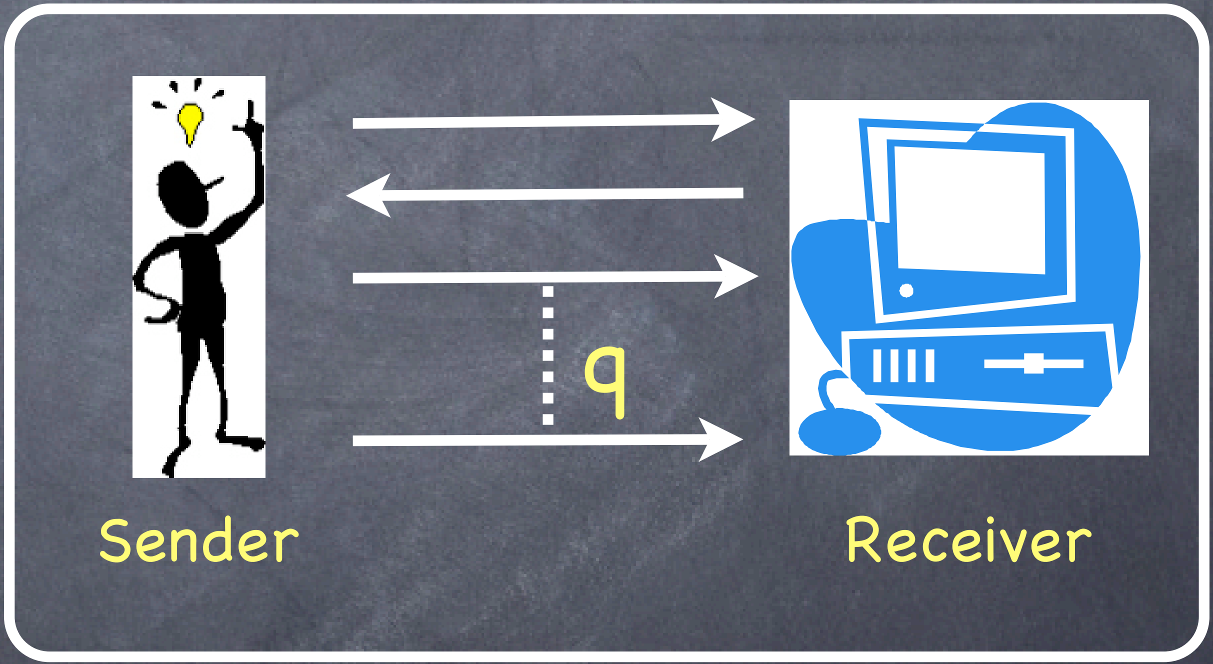
(Primitives with Interaction)

- [BIN97,PW07]: Parallel repetition does not, in general, reduce the soundness error of multi-round protcols.

Security Amplification of Interactive Primitives

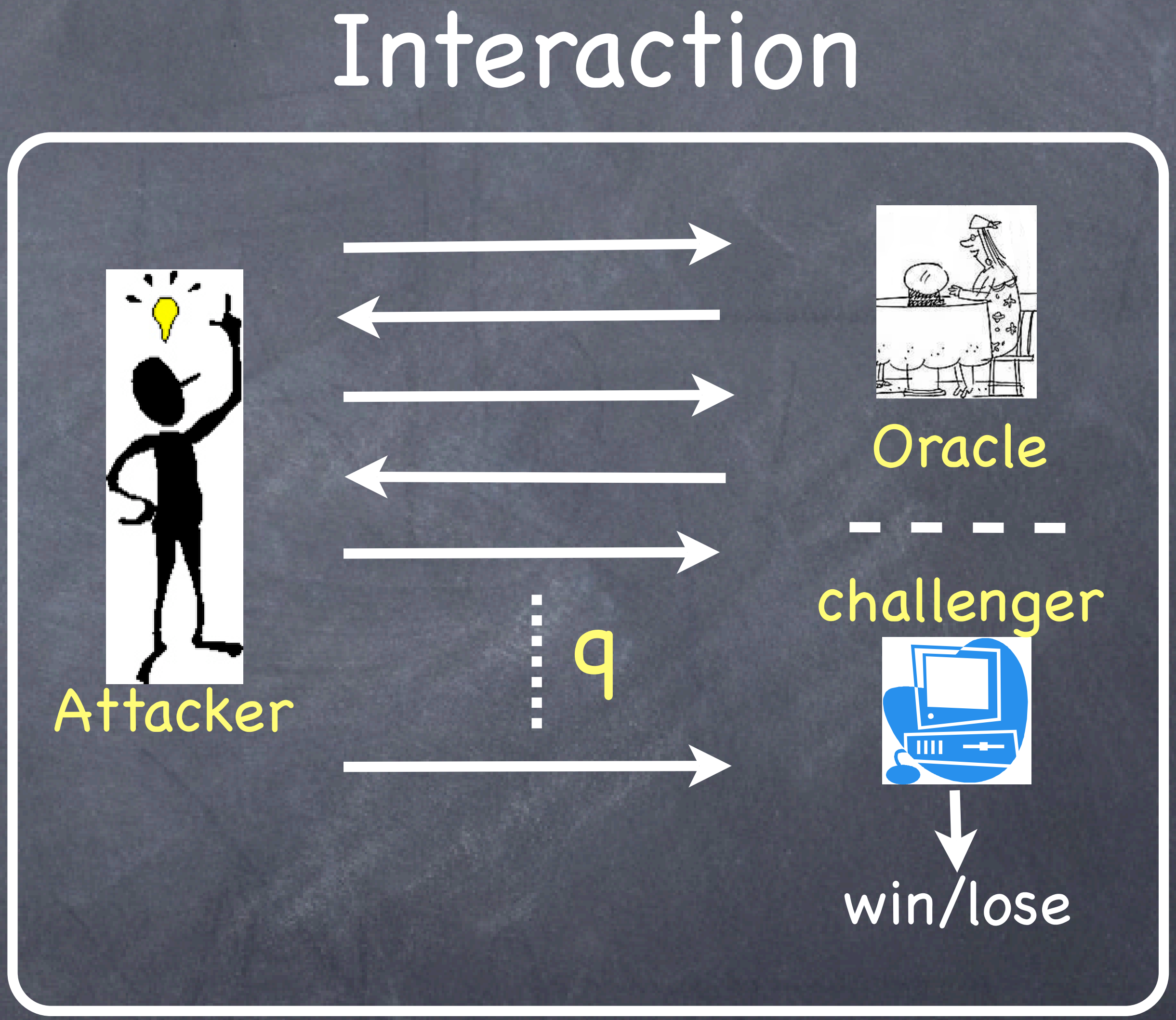
- Category 1: Two party settings (sender/receiver, prover/verifier)
  - Constant round public coin protocol [PV07]
  - 3-round challenge-response protocols [BIN97]
  - Commitments [HR08]
  - Oblivious Transfer [W07]

Interaction



Security Amplification of Interactive Primitives

- Category 2: Oracle setting (e.g., MAC, SIG, PRF)
  - Much less is known
  - [Mye03] talks about PRFs
  - No result about MACs/SIGs



Security Amplification of Interactive Primitives (Category 2)

- Question 1: Is $MAC_{K1}(m),\ldots,MAC_{Kn}(m)$ more secure than $MAC_K(m)$?
  - Similar question for SIGs.
- Question 2: Is $PRF_{K1}(m)\oplus\ldots\oplus PRF_{Kn}(m)$ more secure than $PRF_K(m)$?
  - [Mye03]: The above XOR lemma is false for β-indistinguishable PRFs when $\beta\geq 1/2$
  - [Mye03]: Non-standard XOR lemma (for any $\beta<1$)
  - Does the standard XOR lemma above hold for $\beta<1/2$?

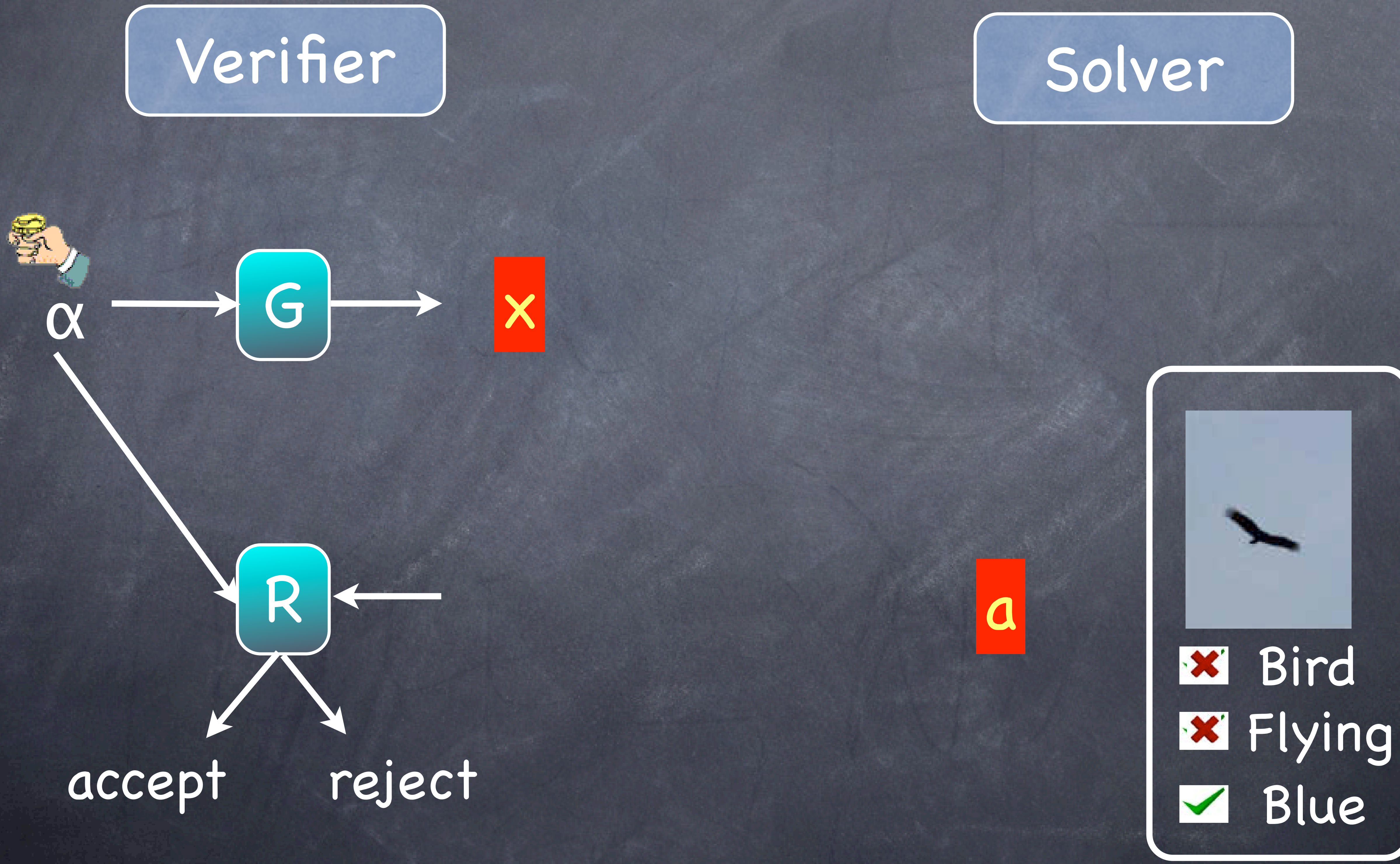
Our Results

1. Natural direct product theorem holds for MACs/SIGs.
   - Chernoff-type version: Even if perfect completeness does not hold.
2. Natural XOR Lemma hold for PRFs when $\beta<1/2$.
   - [Mye03] counter-example is the worst case.
3. Chernoff-type DP Theorem for "Dynamic" Weakly Verifiable Puzzles(DWVP).
   - Generalization to Chernoff-type DP theorem for ordinary WVP [IJK08]
   - Applies to (1) and (2) and is of independent interest

Weakly Verifiable Puzzles (WVP)

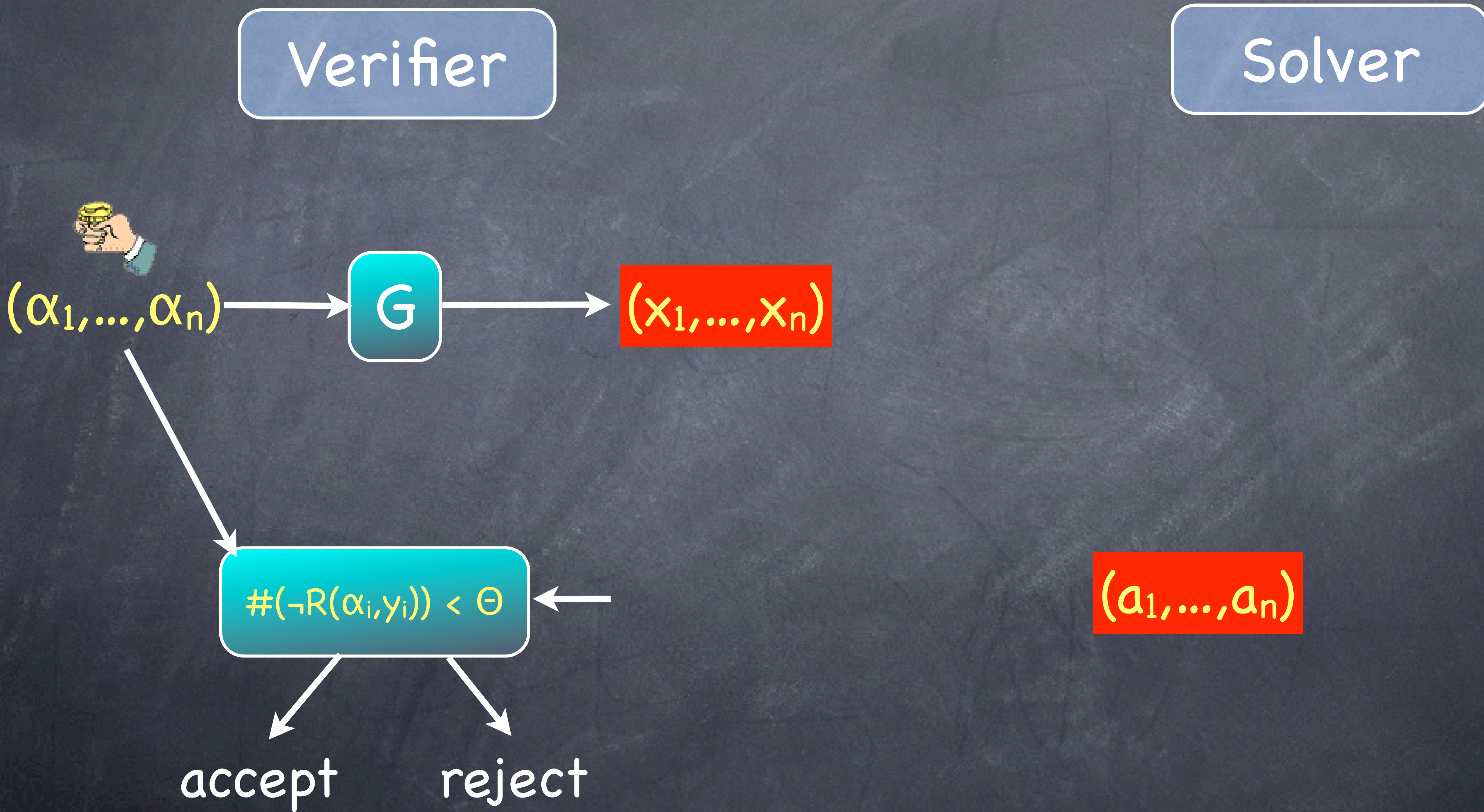
Weakly Verifiable Puzzles [CHS05]

(WVP: P)



Security Amplification for WVP [IJK08]

(parallel repetition with threshold: $P^{n,\Theta}$)



Threshold Vs non-Threshold

(Chernoff-type vs. ordinary DP Theorem)

Advantage of Parallel repetition with threshold:
Gap amplification given some completeness error

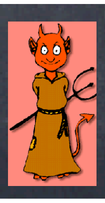
Security Amplification for WVP

- Main Theorem [IJK08]: Suppose there is an algorithm which has success probability at least ε over $P^{n,\Theta}$. Then there is an algorithm which achieves success probability at least $(1-\delta)$ over P. Where
    - $\varepsilon \geq (100/\gamma\delta).\exp(-\gamma^2\delta n/40)$
    - $\Theta = (1-\gamma)\delta n$

Chance of getting at most $(1-\gamma)\delta n$ heads when δ-biased coin is flipped n times

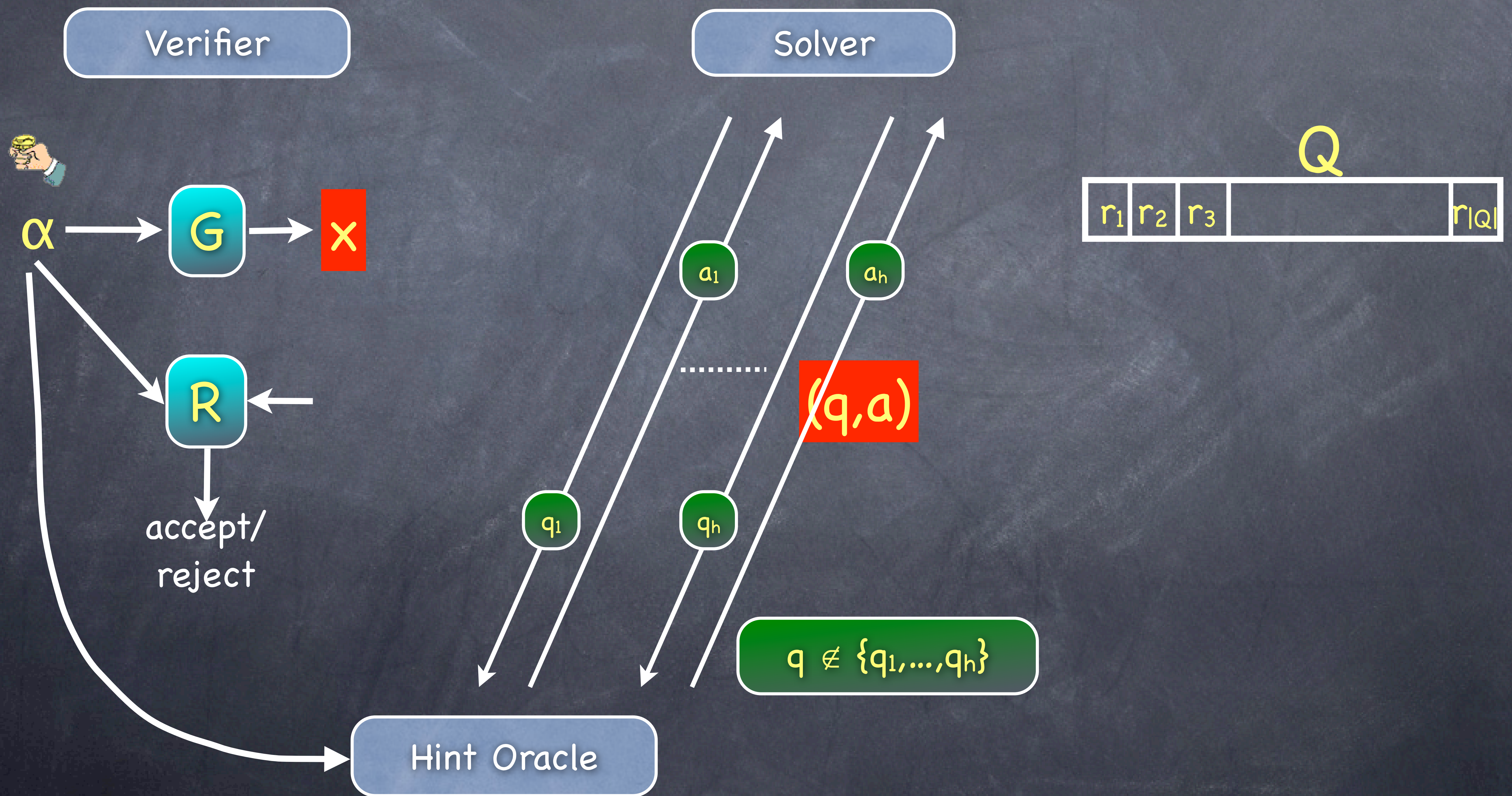
Security Amplification for WVP
(proof sketch)

- We construct an attack for P using the attack for $P^{n,\Theta}$

 uses the self-generated puzzles to evaluate answers from 

Dynamic Weakly Verifiable Puzzles (WVP)

Dynamic Weakly Verifiable Puzzles (DWVP: P)

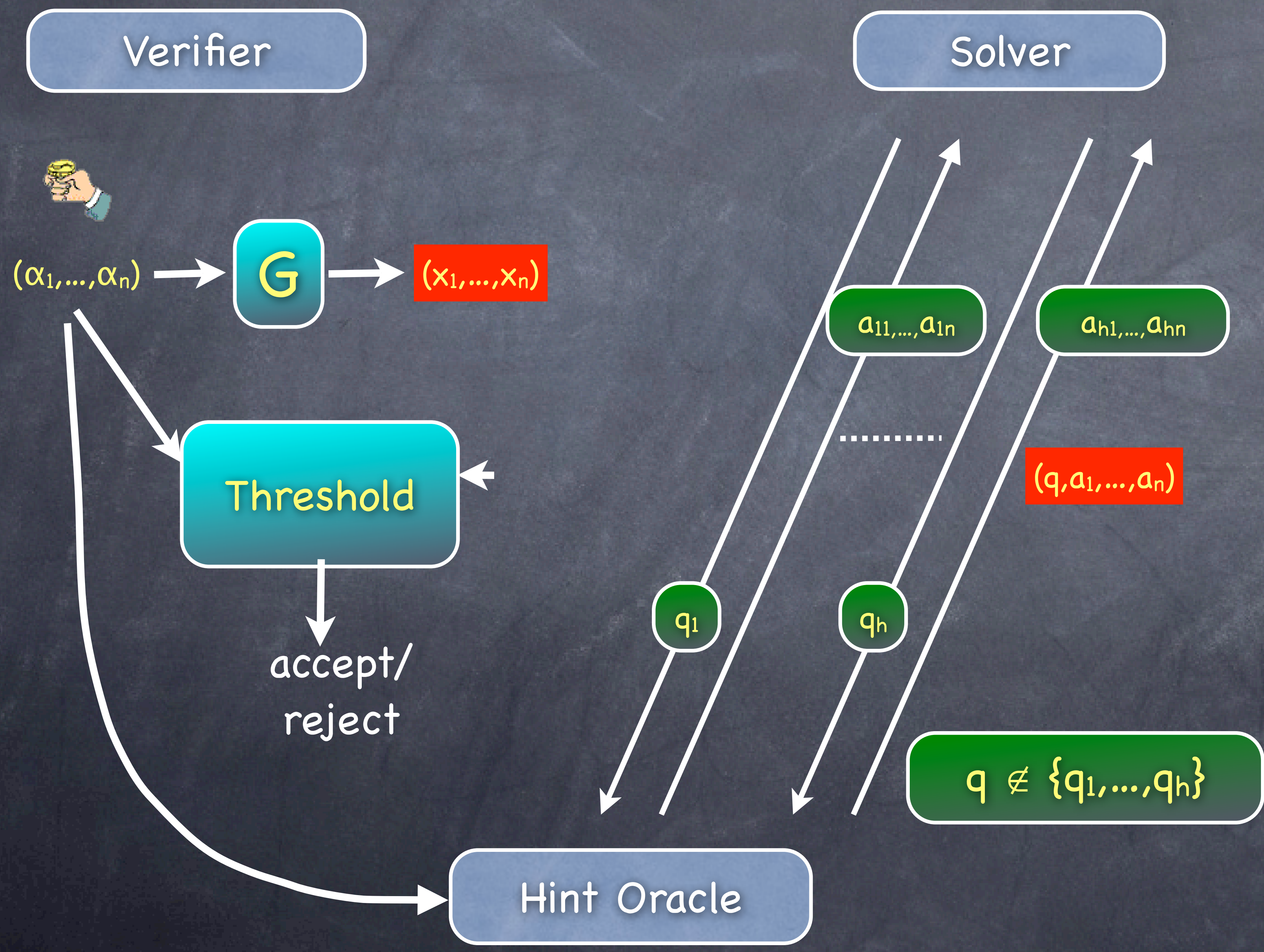


Analogy with MACs/SIGs

- Q ⟷ Message space
- Hint queries ⟷ Chosen Message Attack

Dynamic Weakly Verifiable Puzzles

(Parallel repetition with threshold: $P^{n,\Theta}$)



DP theorem for DWVP

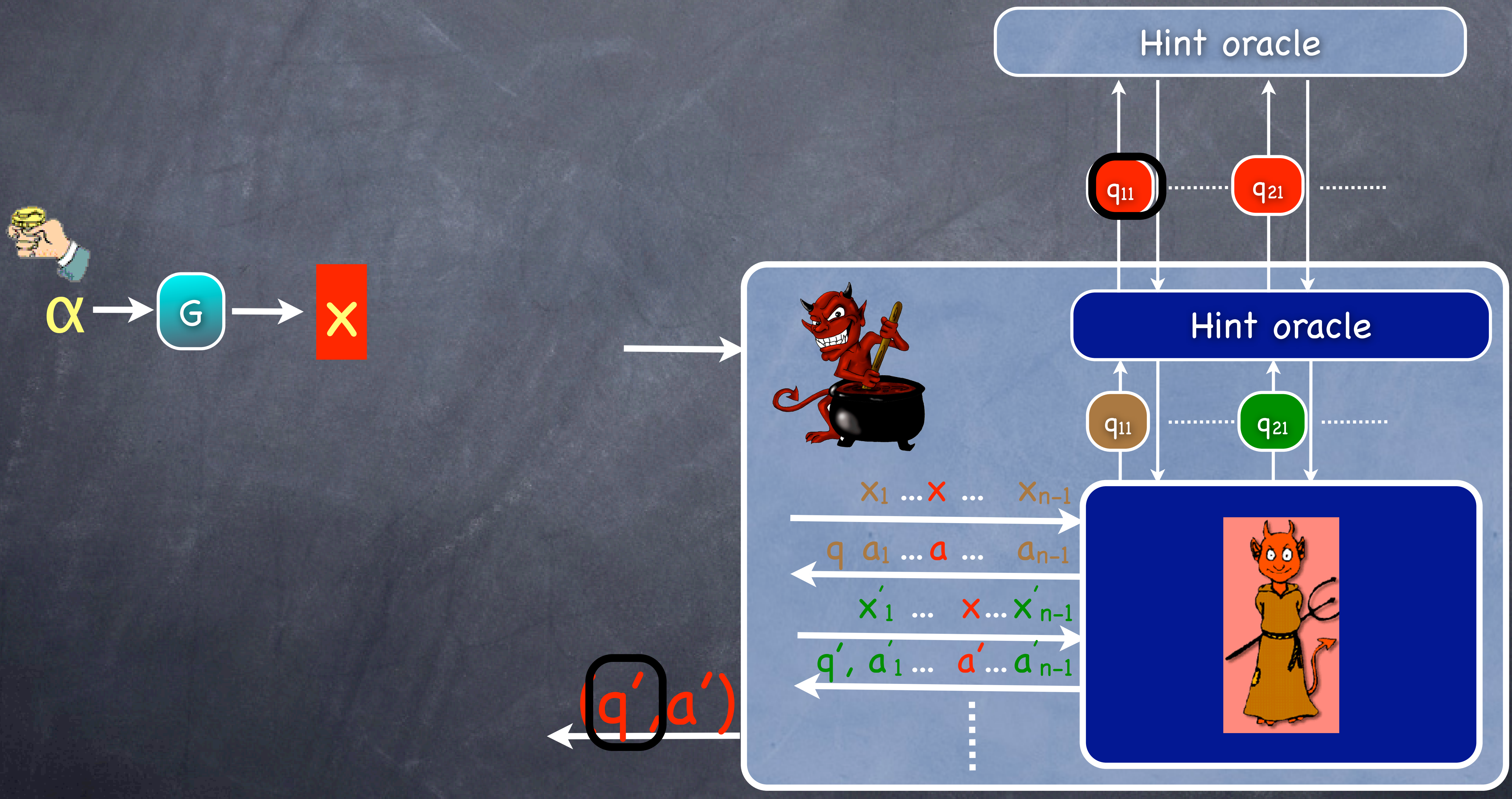
- Main Theorem [DIJK09]: Suppose there is an algorithm which has success probability at least ε over $P^{n,\Theta}$ while making h hint queries. Then there is an algorithm which achieves success probability at least $(1-\delta)$ over P while making H hint queries. Where
  - $\varepsilon \geq (800/\gamma\delta) \,.\, h \,.\, \exp(-\gamma^2\delta n/40)$
  - $H = O((h^2/\varepsilon).\log(1/\gamma\delta))$
  - $\Theta = (1-\gamma)\delta n$

Security amplification: MAC/SIG

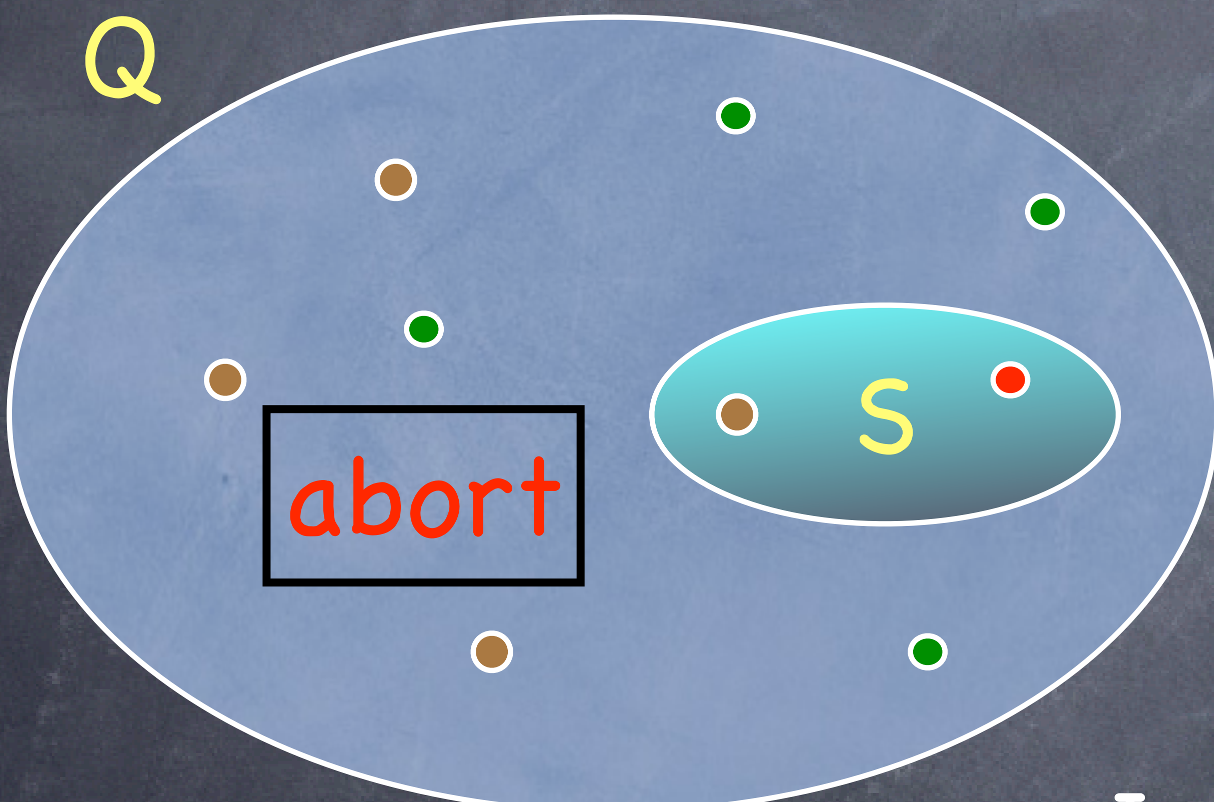
- Weak/Strong MAC/SIG: If the gap between the completeness error (failure probability for honest party) and unforgeability error (failure probability for an attacker) is small/large.
- Theorem[DIJK09]: Given a weak MAC/SIG Π, the direct-product MAC/SIG Π^n is a strong MAC/SIG.

CTDP theorem for DWVP

- We construct an attack for P using the attack for $P^{n,\Theta}$



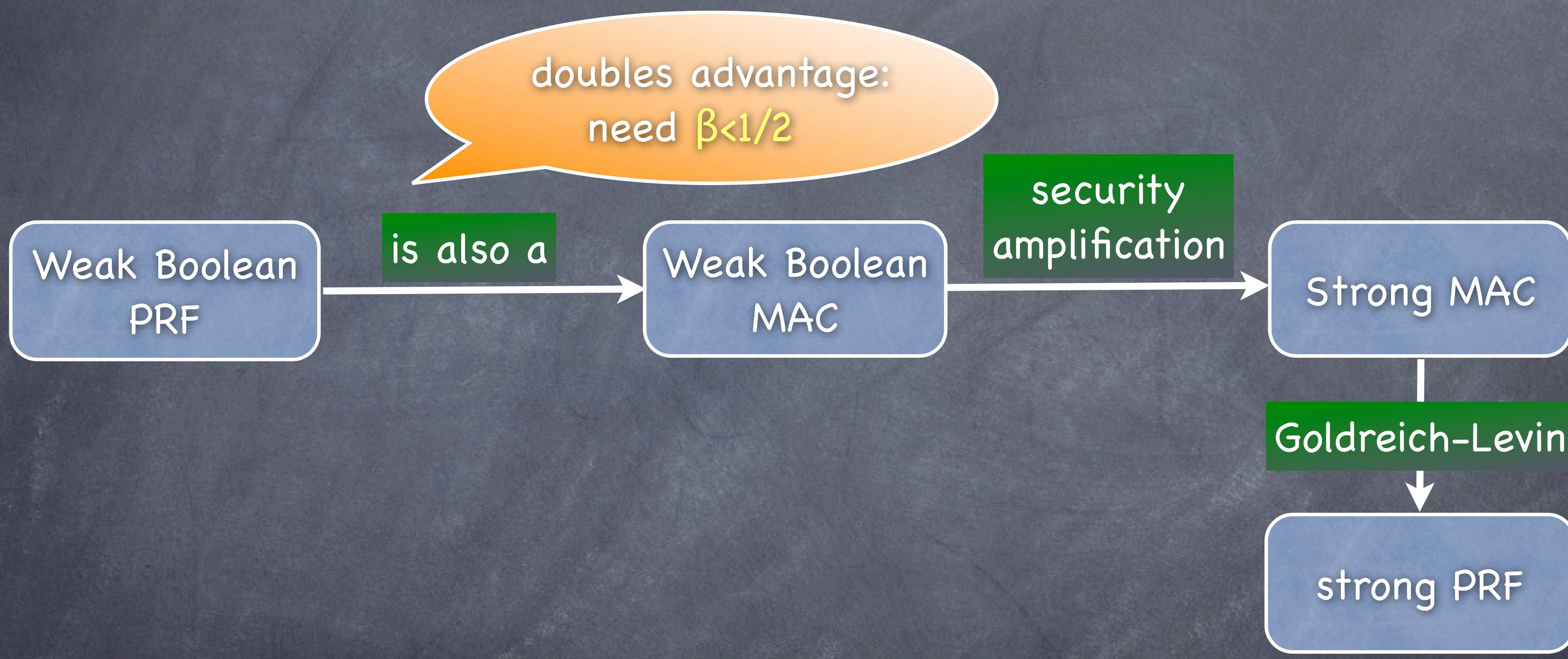
DP theorem for DWVP
(Random partitioning [Cor00])



$|S|/|Q| \approx (1/h)$

- Random Partitioning: For a randomly chosen S, abort a round of attack if any hint query in that round $\in$ S or if attack $\in$ Q\S.
- Intuition: in each round, Pr[all h hints $\notin$ S & forgery $\in$ S] $\leq (1-1/h)^h * (1/h) \leq 1/(eh)$
  - $O(h/\varepsilon)$ rounds is likely enough

Pseudorandom Functions



- GL theorem does not work in general for showing MAC=>PRF [NR98] but works for our construction.

Future Directions

- In our current construction, the size of the MAC as well as the key increases linearly.

  "Can we amplify the security without increasing the size of the MAC and/or keys?"

- Current techniques only amplifies soundness upto negl(k).

  "Can we amplify soundness beyond negl(k) under standard hardness assumption?"

Thank You