Korea univ.
CIST

Higher Order Universal One-Way Hash Functions

Deukjo Hong[1], Bart Preneel[2], Sangjin Lee[1]

[1]CIST, Korea University

[2]ESAT-COSIC, K.U. Leuven

Contents

1. CRHFs and UOWHFs
2. Merkle-Damgård construction
3. Constuctions for extending UOWHFs
4. Motivation of our work
5. Higher order UOWHFs
6. Two constructions based on Higher Order UOWHFs – MD construction and Tree construction
7. Conclusion

Collision-Resistant Hash Function (CRHF)

Let $H : \Sigma^k \times \Sigma^m \rightarrow \Sigma^c$ be a hash function family, where $m \geq c$. H is (t,ε)-CRHF if any adversary A with at most running time t cannot win the following game with at least success probability ε :

Game(CRHF, A, H)
$K \leftarrow_R \Sigma^k$
$A(K) \rightarrow (x, x')$

If $x \neq x'$ and $H(K,x)=H(K,x')$ then A wins the game.

Universal One-Way Hash Function (UOWHF)

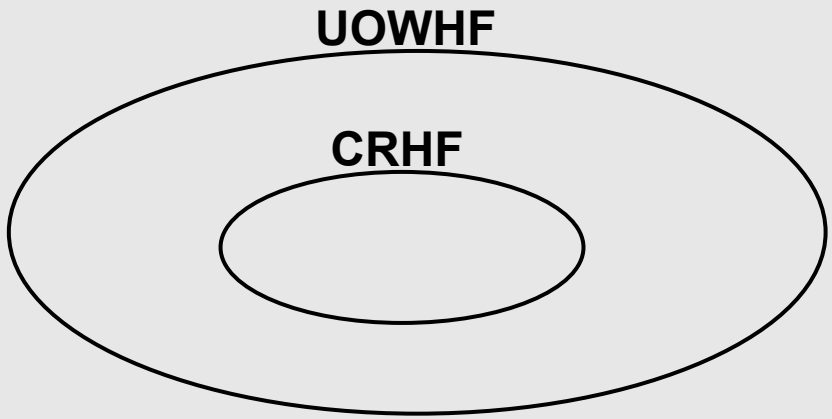
Let $H : \Sigma^k \times \Sigma^m \rightarrow \Sigma^c$ be a hash function family, where $m \geq c$. H is (t,ε)-UOWHF if any adversary $A=(A_1,A_2)$ with at most running time t cannot win the following game with at least success probability ε :

Game(UOWHF, A, H)
$A_1(\cdot) \rightarrow (x,State)$
$K \leftarrow_R \Sigma^k$
$A_2(K,x,State) \rightarrow x'$

If $x \neq x'$ and $H(K,x)=H(K,x')$ then A wins the game.

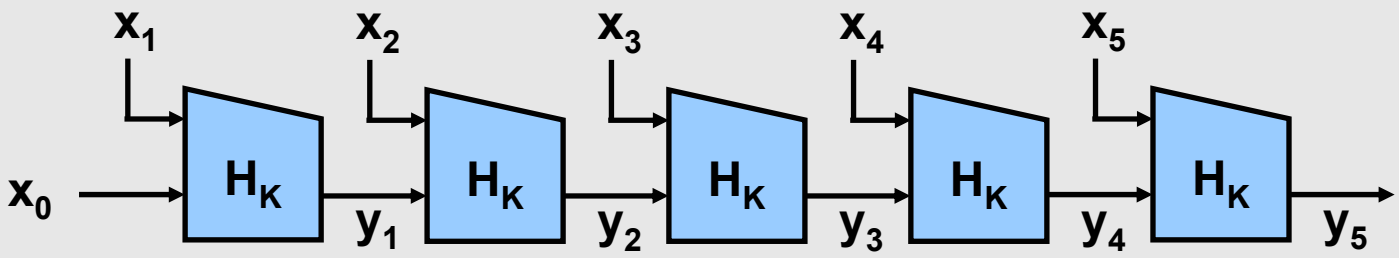
CRHFs vs UOWHFs

- H is (t,ε)-CRHF ⇒ H is (t,ε)-UOWHF.
- Definition of CRHF is stronger than Definition of UOWHF.
- UOWHF can be used as an alternative primitive for CRHF. (e.g. digital signature)



Merkle-Damgård Construction

- The most popular way for extending hash functions.
- It preserves the collision resistance.
- $MD_r[H]$: r-round Merkle-Damgård construction based on H.



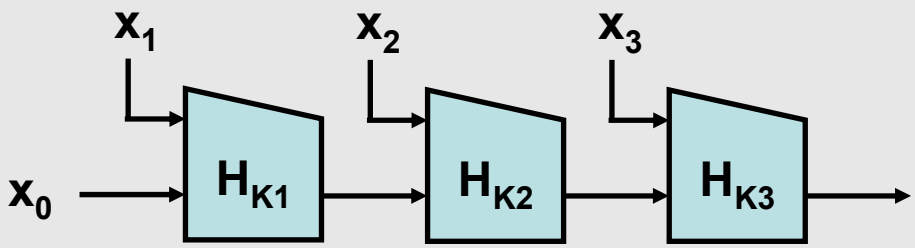
Constructions for extending UOWHFs

- MD construction cannot be used for UOWHFs.
- Bellare and Rogaway showed there exists a H; H is UOWHF but $MD_2[H]$ is not UOWHF.
- Bellare and Rogaway proposed 4 constructions for extending UOWHF hashing finite-length messages to one hashing arbitrary-length messages. The other suggested constructions for extending UOWHFs are based on them.
- Problem: The key size grows with the message length.

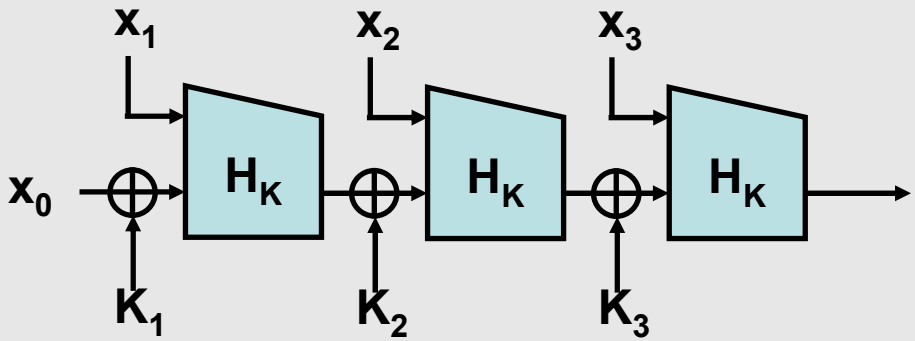
Constructions for extending UOWHFs

< Bellare and Rogaway's constructions (1) >

Linear Hash



XOR Linear Hash

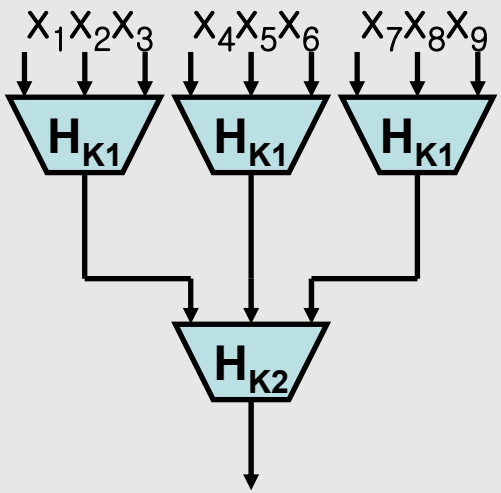


(XOR Linear hash construction is optimalized by Shoup.)

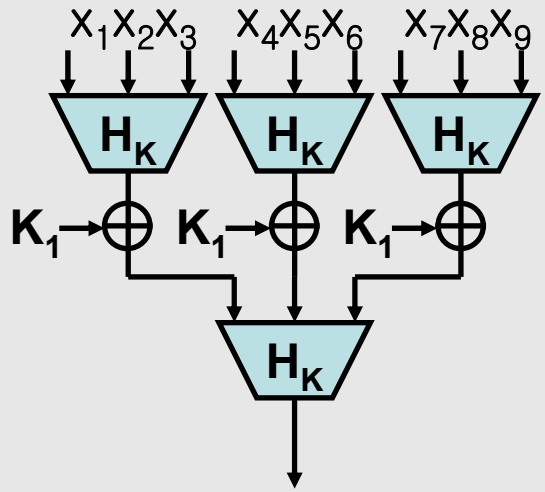
Constructions for extending UOWHFs

< Bellare and Rogaway's constructions (2) >

Tree Hash



XOR Tree Hash



Motivation

- The most important thing to constructions for extending UOWHFs is reducing the total length of the key as small as possible.
- MD construction is more efficient in key size than any other schemes for UOWHFs.
- If $MD_r[H]$ is UOWHF, then extending $MD_r[H]$ is better than extending H.
- It seems that there exists H such that $MD_r[H]$ is UOWHF in spite of Bellare and Rogaway's counterexample.

Contribution

- We propose the new definition, Higher Order Universal One-Way Hash Function.
- We prove that if H is a higher order UOWHF, then $MD_r[H]$ and $TR_l[H]$ are UOWHF.
- Thereby, the notion of higher order UOWHF helps reducing key sizes of any constructions for extending UOWHFs.
- We focus on the security about equal-length collisions (Theorems 1 and 3). Theorems 2 and 4 are also interesting but less useful in this issue.

Higher Order UOWHF (of order r)

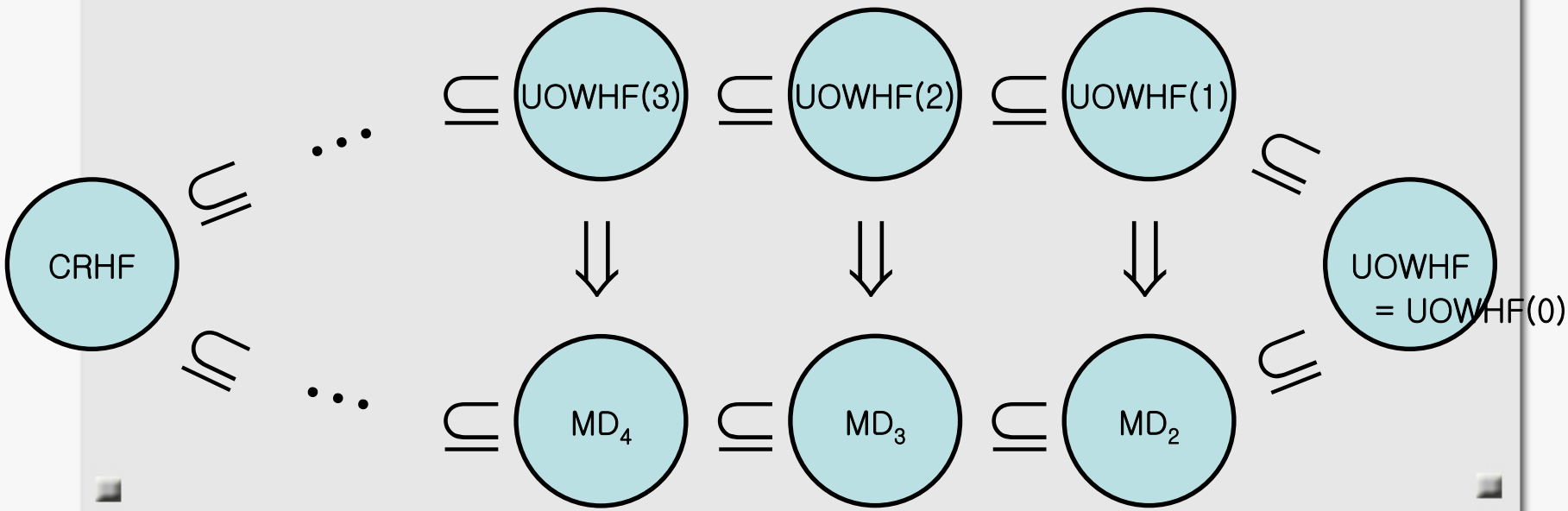
Let $H : \Sigma^k \times \Sigma^m \rightarrow \Sigma^c$ be a hash function family, where $m \geq c$. H is (t,ε)-UOWHF(r) if any adversary $A=(A_1,A_2)$ with at most running time t cannot win the following game with at least success probability ε :

Game(UOWHF(r), A, H)
$K \leftarrow_R \Sigma^k$; $Q \leftarrow \varnothing$
$A_1(Q)$ ask adaptively r queries to $O^{H(K,\cdot)}$.
$A_1(Q) \rightarrow (x,State)$
$A_2(K,x,State) \rightarrow x'$

If $x \neq x'$ and $H(K,x)=H(K,x')$ then A wins the game.

MD construction and UOWHF(r)

- The following sets of functions are considered under same key space, domain, and range.
  - CRHF = {h : h is CRHF}
  - MD_r = {h : h and MD_r[h] is UOWHF}
  - UOWHF(r) = {h : h is UOWHF(r)}



Theorem 1

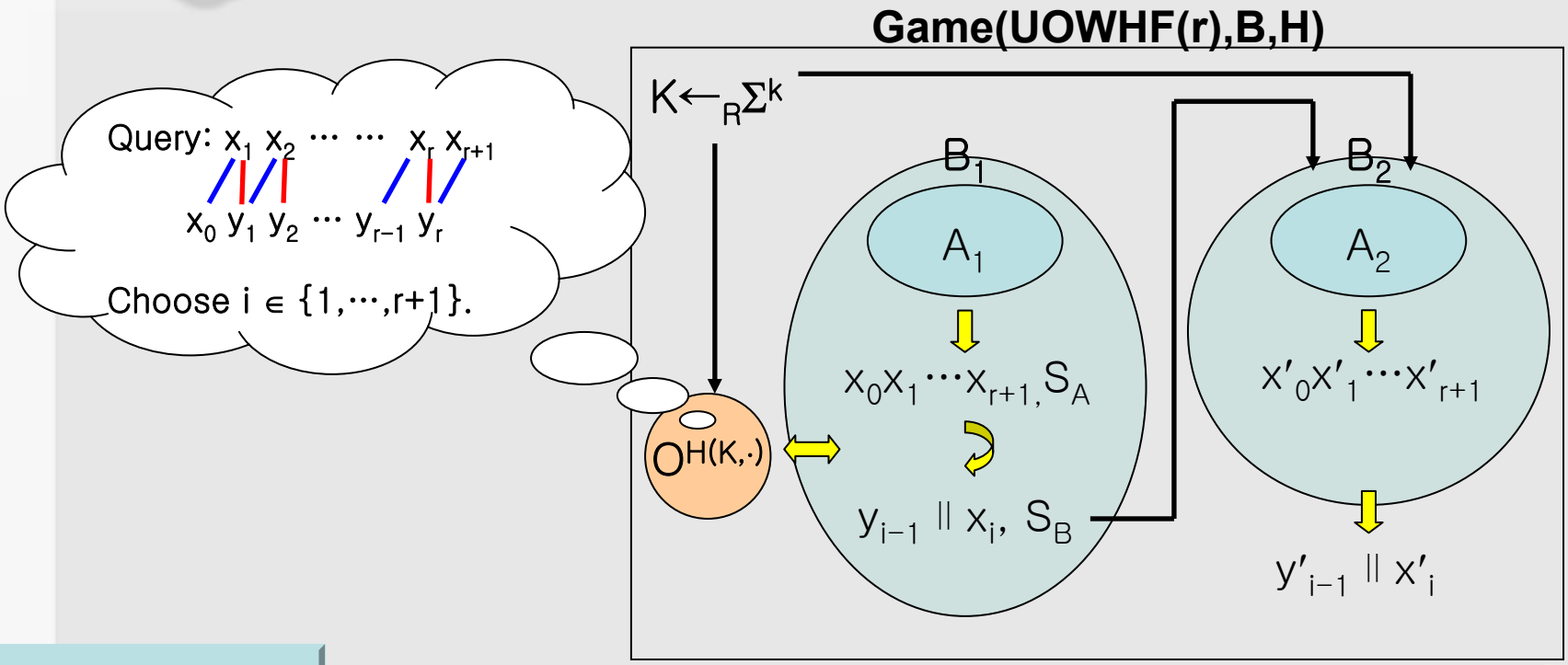
- $H : \Sigma^k \times \Sigma^{c+m} \rightarrow \Sigma^c$ is (t', ε')-UOWHF(r).

- $MD_{r+1}[H] : \Sigma^k \times \Sigma^{c+(r+1)m} \rightarrow \Sigma^c$ is (t, ε)-UOWHF, where
  - $\varepsilon = (r+1)\varepsilon'$ and
  - $t = t' - \Theta(r)(T_H + m + c)$.

Proof of Theorem 1

Assume that A is an adversary for $MD_{r+1}[H]$ in the UOWHF sense.

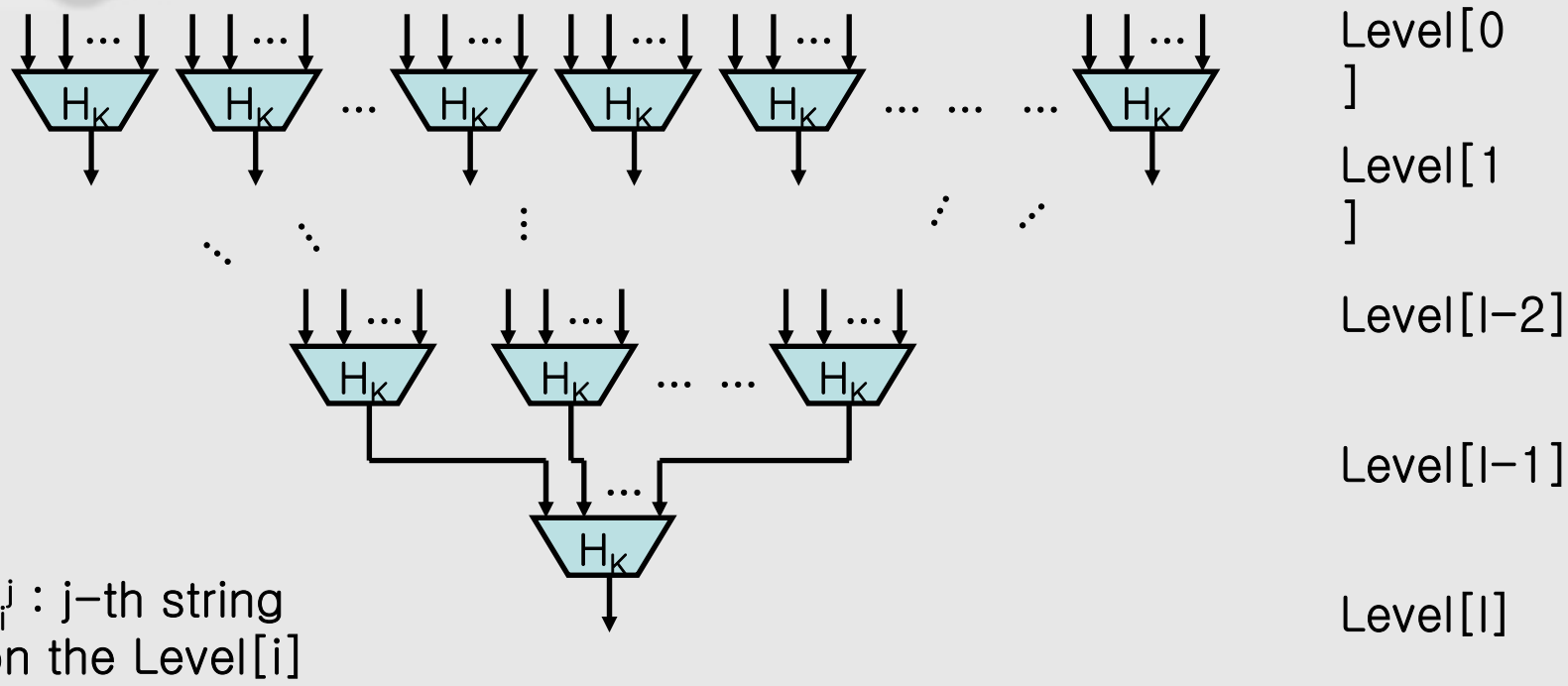
Build an adversary B for H in the UOWHF(r) sense.



Theorem 1

Tree Construction

Let $H : \Sigma^k \times \Sigma^{dc} \rightarrow \Sigma^c$. $TR_l[H]$ is as follows.



Theorem 3

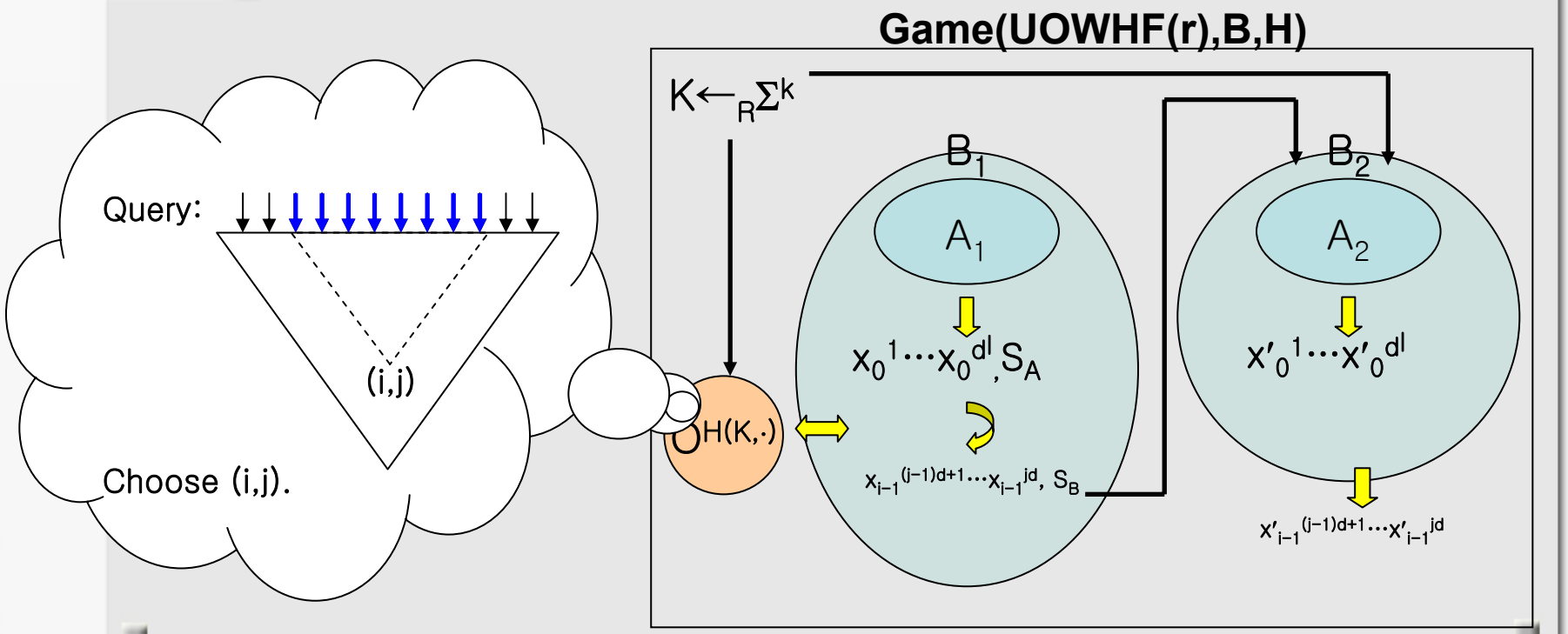
- $H : \Sigma^k \times \Sigma^{dc} \rightarrow \Sigma^c$ is (t', ε')-UOWHF(r).
  - $r = (d^l - d)/(d-1)$.

- $TR_l[H] : \Sigma^k \times \Sigma^{cd^l} \rightarrow \Sigma^c$ is (t, ε)-UOWHF, where
  - $\varepsilon = (r+1)\varepsilon'$ and,
  - $t = t' - \Theta(d^l)(T_H + dc)$.

Proof of Theorem 3

Assume that A is adversary for $MD_{r+1}[H]$ in the UOWHF sense.

Build an adversary B for H in the UOWHF(r) sense.



Conclusion

- If the order of the underlying UOWHF H is r, then $MD_{r+1}[H]$ is also a UOWHF. If $MD_{r+1}[H]$ is used as a compression function in any other linear structural constructions, the key size can be reduced with at most a factor of (r+1).
- If the order of the underlying UOWHF H is $r = (d^l - d)/(d-1)$, then $TR_l[H]$ is also a UOWHF. If $TR_l[H]$ is used as a compression function in any other tree structural constructions, the key size can be reduced with at most a factor of l.