The Multi-User Security of Double Encryption

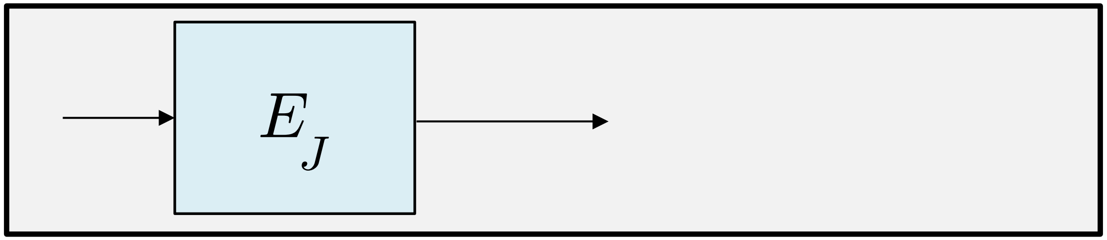
Viet Tung Hoang
Florida State University

Stefano Tessaro
UC Santa Barbara

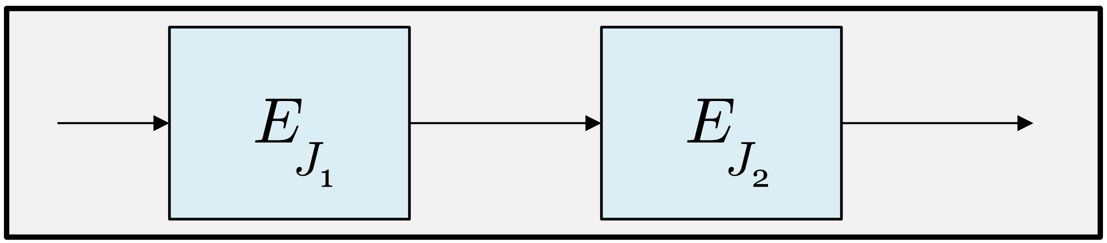
EUROCRYPT 2017
May 3, 2017

Double Encryption

$$E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$$



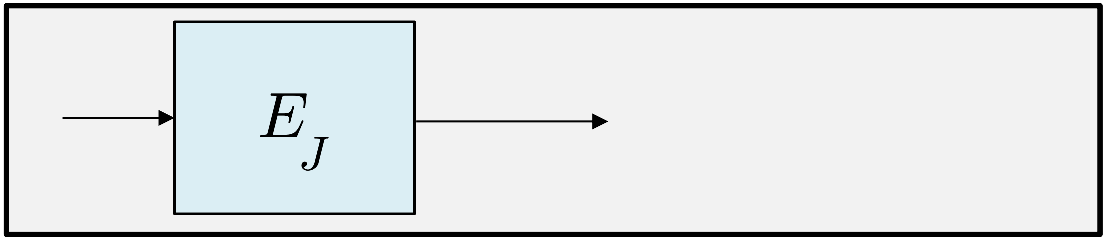
Single Encryption: trivial key-recovery in O(2^k) time.



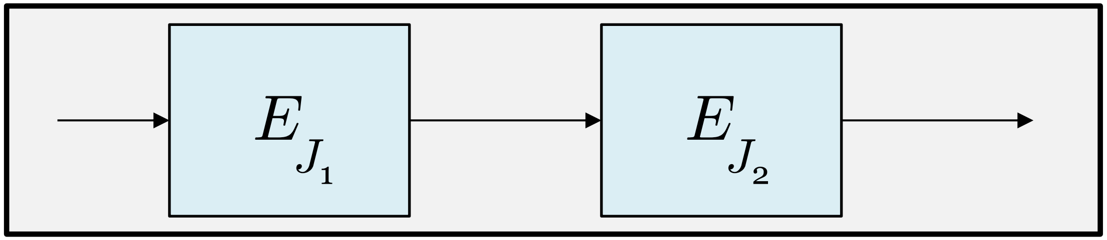
Double Encryption: use meet-in-the-middle attack to recover keys in O(2^k) time.

Double Encryption

$$E : \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$$



Single Encryption: trivial key-recovery in O(2^k) time.

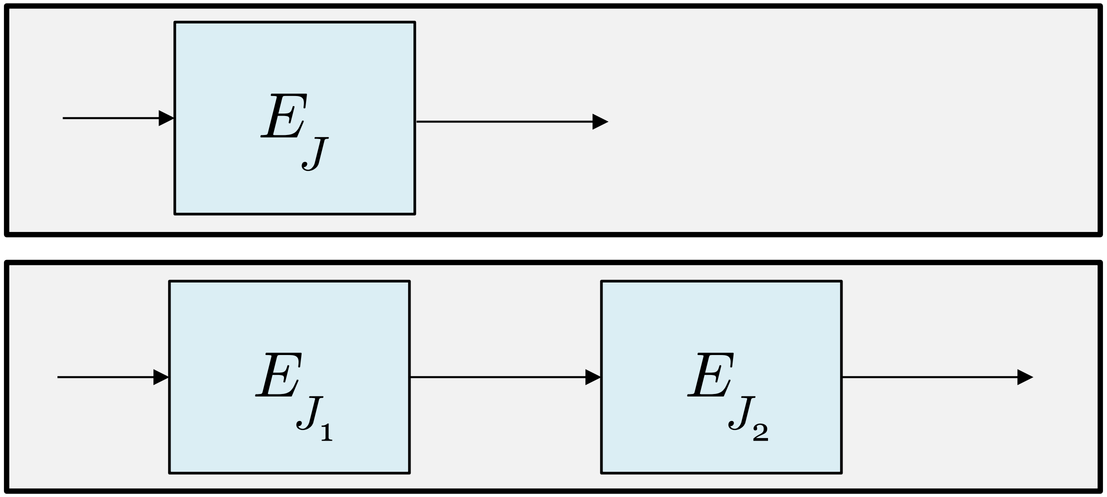


Double Encryption: use meet-in-the-middle attack to recover keys in O(2^k) time.

Conventional wisdom: Double Encryption adds no security

Double Encryption

$$E : \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$$



Single Encryption: trivial key-recovery in O(2^k) time.

Double Encryption: use meet-in-the-middle attack to recover keys in O(2^k) time.

Conventional wisdom: Double Encryption adds no security

Today: Double Encryption adds **some** security, if we look at a broader angle

Conventional Security Definition

$\mathrm{Real}^{A}_{\Pi[E]}$

$K \leftarrow\!\!\$\ \mathcal{K}$

Procedure $\mathrm{Enc}(x)$

Return $\Pi_K[E](x)$

Procedure $\mathrm{Dec}(x)$

Return $\Pi_K^{-1}[E](x)$

$\mathrm{Ideal}^{A}_{\Pi[E]}$

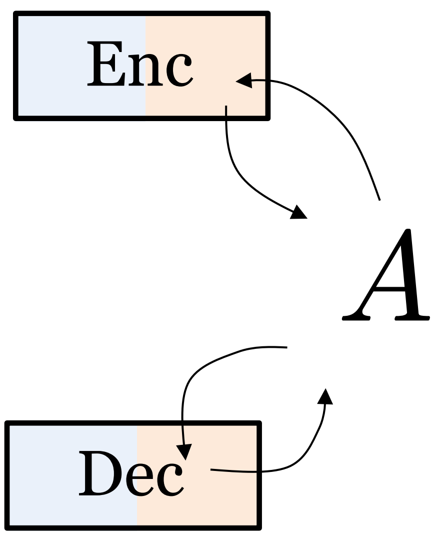
$f \leftarrow\!\!\$\ \mathrm{Perm}(\{0,1\}^n)$

Procedure $\mathrm{Enc}(x)$

Return $f(x)$

Procedure $\mathrm{Dec}(x)$

Return $f^{-1}(x)$



$$\mathbf{Adv}^{\mathrm{cca}}_{\Pi[E]}(A) = \Pr[\mathrm{Real}^{A}[E] \Rightarrow 1] - \Pr[\mathrm{Ideal}^{A}[E] \Rightarrow 1]$$

$$\mathbf{Adv}^{\mathrm{cca}}_{\Pi[E]}(q) = \max_{A \text{ of } q \text{ queries}} \mathbf{Adv}^{\mathrm{cca}}_{\Pi[E]}(A)$$

Conventional Security Definition

$\mathrm{Real}^{A}_{\Pi[E]}$

$K \leftarrow\!\!\$\ \mathcal{K}$

Procedure $\mathrm{Enc}(x)$

Return $\Pi_K[E](x)$

Procedure $\mathrm{Dec}(x)$

Return $\Pi_K^{-1}[E](x)$

$\mathrm{Ideal}^{A}_{\Pi[E]}$

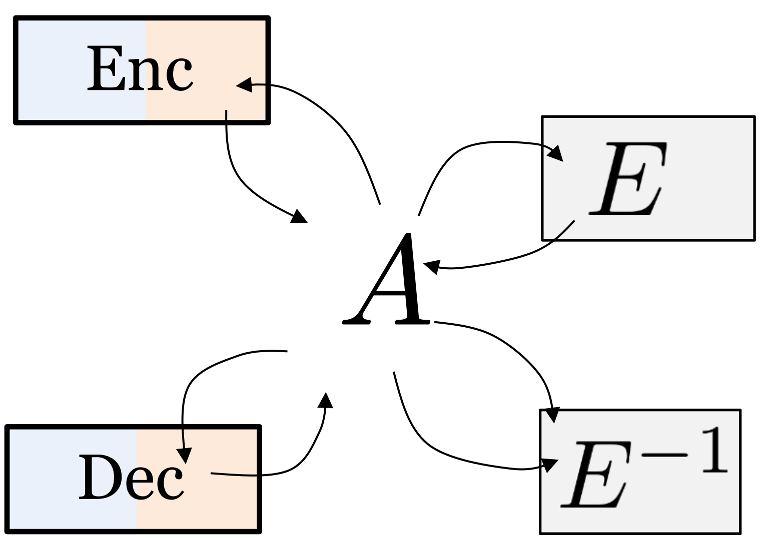
$f \leftarrow\!\!\$\ \mathrm{Perm}(\{0,1\}^n)$

Procedure $\mathrm{Enc}(x)$

Return $f(x)$

Procedure $\mathrm{Dec}(x)$

Return $f^{-1}(x)$



$$\mathbf{Adv}^{\mathrm{cca}}_{\Pi[E]}(A) = \Pr[\mathrm{Real}^{A}[E] \Rightarrow 1] - \Pr[\mathrm{Ideal}^{A}[E] \Rightarrow 1]$$

$$\mathbf{Adv}^{\mathrm{cca}}_{\Pi[E]}(q) = \max_{A \text{ of } q \text{ queries}} \mathbf{Adv}^{\mathrm{cca}}_{\Pi[E]}(A)$$

Multi-user (mu) Security

- The conventional notion consider just single-user (su) security

-In practice, adversary attacks **multiple** users, **adaptively** distributing its resources

$K_1, K_2, \ldots \xleftarrow{\$} \mathcal{K}$ $\quad \mathrm{Real}^{A}_{\Pi[E]}$

Procedure Enc(x, i)

Return $\Pi_{K_i}[E](x)$

Procedure Dec(x, i)

Return $\Pi^{-1}_{K_i}[E](x)$

$f_1, f_2, \ldots \xleftarrow{\$} \mathrm{Perm}(\{0,1\}^n)$ $\quad \mathrm{Ideal}^{A}_{\Pi[E]}$

Procedure Enc(x, i)

Return $f_i(x)$

Procedure Dec(x, i)

Return $f_i^{-1}(x)$

Multi-user (mu) Security

- The conventional notion consider just single-user (su) security

-In practice, adversary attacks **multiple** users, **adaptively** distributing its resources

$K_1, K_2, \ldots \leftarrow\$ \mathcal{K}$ — $\mathrm{Real}^{A}_{\Pi[E]}$

Procedure Enc(x, i)

Return $\Pi_{K_i}[E](x)$

Procedure Dec(x, i)

Return $\Pi^{-1}_{K_i}[E](x)$

$f_1, f_2, \ldots \leftarrow\$ \mathrm{Perm}(\{0,1\}^n)$ — $\mathrm{Ideal}^{A}_{\Pi[E]}$

Procedure Enc(x, i)

Return $f_i(x)$

Procedure Dec(x, i)

Return $f_i^{-1}(x)$

-Mu security can be implicitly obtained via hybrid arguments:

$$\mathbf{Adv}^{\text{mu-cca}}_{\Pi[E]}(q) \leq \#\text{users} \cdot \mathbf{Adv}^{\text{cca}}_{\Pi[E]}(q)$$

Double Encryption Improves Mu Security

Claim: Double Encryption improves mu security

Double Encryption Improves Mu Security

Claim: Double Encryption improves mu security

-AES has only 64-bit security in mu setting due to key-collision attack. [Biham 02]

Choose random keys $K_1, K_2, \ldots, K_p$

A

K_1	K_2	• • •	K_p
$E_{K_1}(0^n)$	$E_{K_2}(0^n)$		$E_{K_p}(0^n)$

User #1	**User #2**	• • •	**User #*q***
$\mathrm{Enc}(1, 0^n)$	$\mathrm{Enc}(2, 0^n)$		$\mathrm{Enc}(q, 0^n)$

Check for matching entries between two tables to recover some user's key

Double Encryption Improves Mu Security

Claim: Double Encryption improves mu security

-AES has only 64-bit security in mu setting due to key-collision attack. [Biham 02]

Choose random keys $K_1, K_2, \ldots, K_p$

A

K_1	K_2	• • •	K_p
$E_{K_1}(0^n)$	$E_{K_2}(0^n)$		$E_{K_p}(0^n)$

User #1	**User #2**	• • •	**User #*q***
$\mathrm{Enc}(1, 0^n)$	$\mathrm{Enc}(2, 0^n)$		$\mathrm{Enc}(q, 0^n)$

Check for matching entries between two tables to recover some user's key

-**Today**: Mu security of DE(AES) ≈ Su security of AES

128-bit security

History of Mu Analyses on SE/DE

k: key length, n: block length, q: # queries

Adv vanishes when $q \approx$

Construction	**Advantage**	**Security level**
SE: matching attack of hybrid argument by [Biham 02]	$\frac{q^2}{2^k}$	$2^{k/2}$
DE: hybrid argument on [ABDV98] bound	$\frac{q^3}{2^{2k}}$	$2^{2k/3}$
DE: dream bound	$\frac{q}{2^k}$	2^k

Goals and Results

-Give a **generic technique** for bounding information-theoretic mu security.

+ Our method can handle any indistinguishability games (PRF, AE, blockcipher), and any ideal primitive (random oracle, ideal cipher, ideal permutation).

Goals and Results

-Give a **generic technique** for bounding information-theoretic mu security.

+ Our method can handle any indistinguishability games (PRF, AE, blockcipher), and any ideal primitive (random oracle, ideal cipher, ideal permutation).

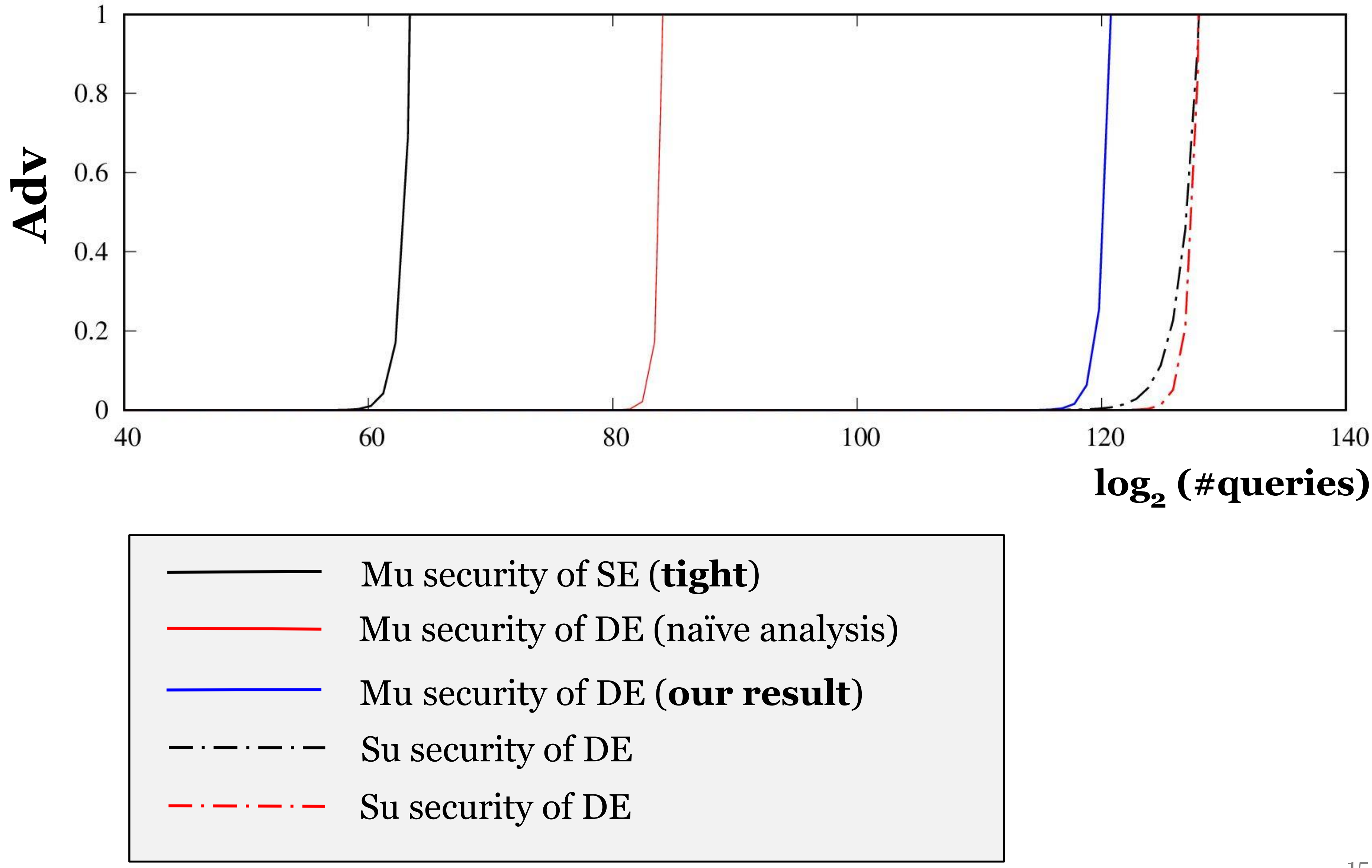
-Showcase the method via Double Encryption

Advantage	**Security level**
$\frac{6qB^2 + 222Bq^2}{2^{2k}}$	$2^k/n$ if $n \geq k$

$$B = 5\max\{n + k/2, 2q/2^n\}$$

Results

Visualization of the mu and su bounds of Single Encryption (SE) and Double Encryption (DE) on AES parameters



The Technique: Almost Proximity

Almost proximity: very general, but can be overly complex in some setting

The Technique: Almost Proximity

Almost proximity: very general, but can be overly complex in some setting

Simplified generic treatment: can handle many settings such as GCM, but not Double Encryption

The Technique: Almost Proximity

Almost proximity: very general, but can be overly complex in some setting

Simplified generic treatment: can handle many settings such as GCM, but not Double Encryption

A treatment for blockcipher: tailored to DE

The Technique: Almost Proximity

Almost proximity: very general, but can be overly complex in some setting

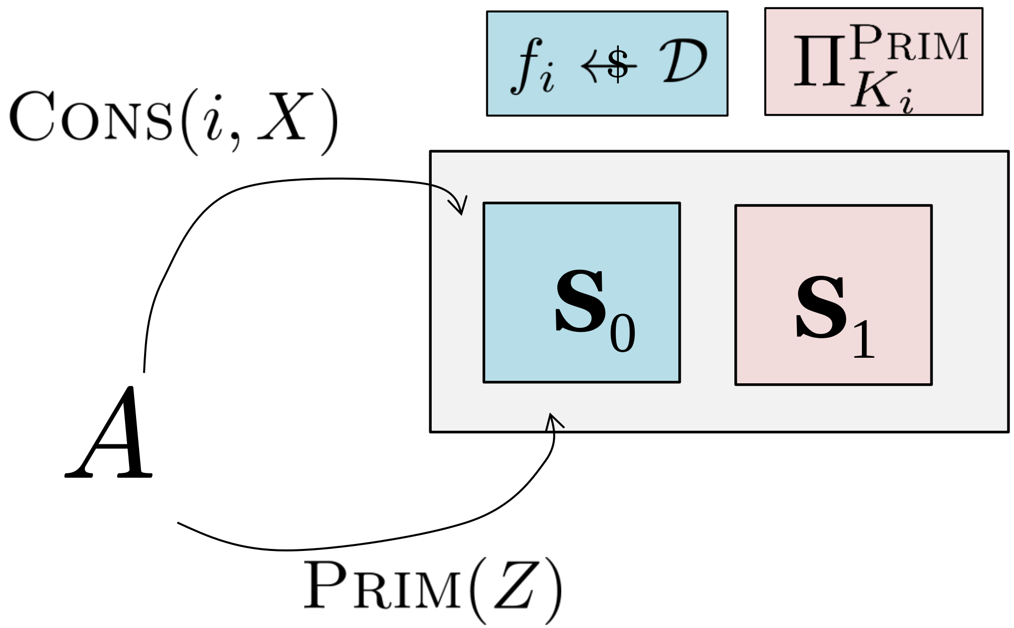
Simplified generic treatment: can handle many settings such as GCM, but not Double Encryption

A treatment for blockcipher: tailored to DE

Generalize the pointwise proximity technique of [Hoang, Tessaro 2016]

Simplified Almost Proximity

- Bound the distinguishing advantage of two randomized systems $\mathbf{S}_0$ and $\mathbf{S}_1$



Cost metrics:

q: # of construction queries

p: # of primitive queries

σ: data complexity, e.g. the total length of CONS queries

X may encode (+, x) or (-, y), and Z may encode (+, K, z) or (-, K, z)

Assume that q CONS queries of data complexity σ invoke σt primitive queries

Simplified Almost Proximity

Transcript τ of the interaction

A

$\mathbf{S}_0$ $\mathbf{S}_1$

Probability that $\mathbf{S}_i$ behaves according to τ

$$\mathbf{Adv}_{\mathbf{S}_1,\mathbf{S}_0}(A) \leq \sum_{\tau} \max\{0, \mathbf{p}_{\mathbf{S}_1}(\tau) - \mathbf{p}_{\mathbf{S}_0}(\tau)\}$$

Classify **su** transcripts to "good" and "bad"

Restriction: Involves only CONS queries

A mu transcript is nice if for any user, the induced su transcript is good

Classify **mu** transcripts to "nice" and "not nice"

Simplified Almost Proximity

$$\mathbf{Adv}_{\mathbf{S}_0,\mathbf{S}_1}(A) \leq \sum_{\tau} \mathbf{p}_{\mathbf{S}_0}(\tau) \cdot \max\left\{0, 1 - \frac{\mathbf{p}_{\mathbf{S}_1}(\tau)}{\mathbf{p}_{\mathbf{S}_0}(\tau)}\right\}$$

- Classify mu transcripts by "nice" and "not nice"

Bound $\Pr[X \text{not nice}] \leq \delta$

Random variable for transcript in $\mathbf{S}_0$

Mu analysis, but for the "ideal" system $\mathbf{S}_0$

Simplified Almost Proximity

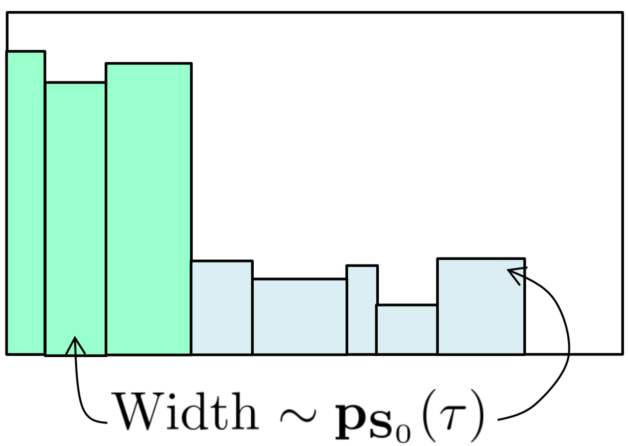
$$\mathbf{Adv}_{\mathbf{S}_0,\mathbf{S}_1}(A) \leq \sum_{\tau} \mathbf{ps}_0(\tau) \cdot \max\left\{0, 1 - \frac{\mathbf{ps}_1(\tau)}{\mathbf{ps}_0(\tau)}\right\}$$

- Classify mu transcripts by “nice” and “not nice”

Bound $\Pr[X \text{not nice}] \leq \delta$

Random variable for transcript in $\mathbf{S}_0$

Mu analysis, but for the “ideal” system $\mathbf{S}_0$



Simplified Almost Proximity

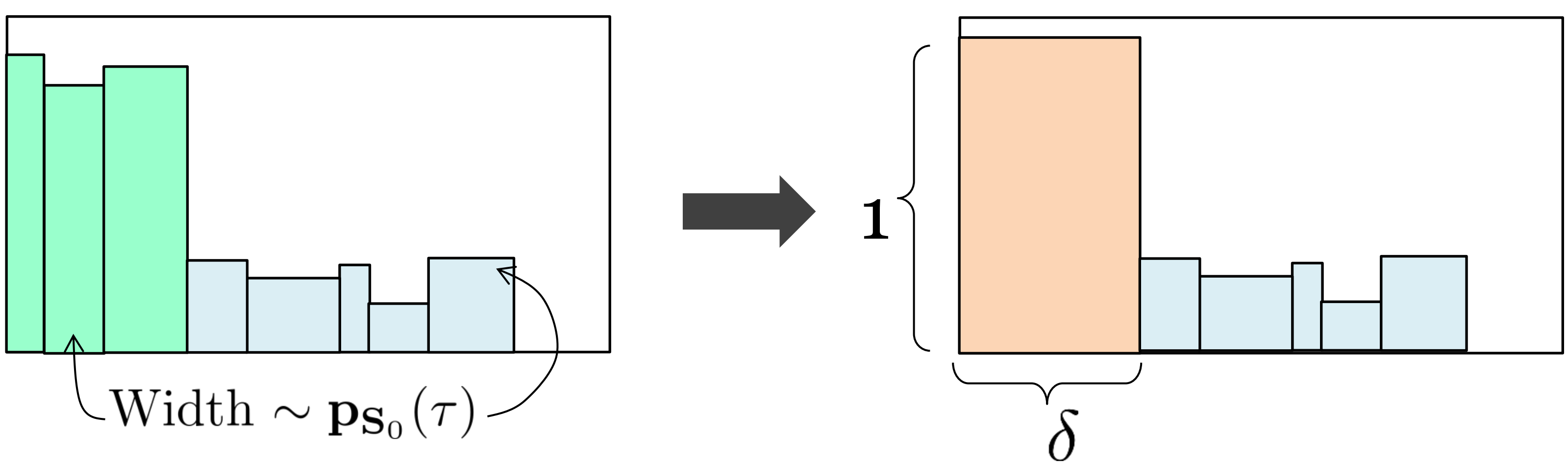
$$\mathbf{Adv}_{\mathbf{S}_0,\mathbf{S}_1}(A) \leq \sum_{\tau} \mathbf{p}_{\mathbf{S}_0}(\tau) \cdot \max\left\{0, 1 - \frac{\mathbf{p}_{\mathbf{S}_1}(\tau)}{\mathbf{p}_{\mathbf{S}_0}(\tau)}\right\}$$

- Classify mu transcripts by “nice” and “not nice”

Bound $\Pr[X \text{ not nice}] \leq \delta$

Random variable for transcript in $\mathbf{S}_0$

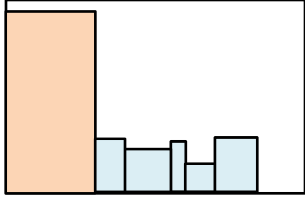
Mu analysis, but for the “ideal” system $\mathbf{S}_0$



$\mathbf{Adv}_{\mathbf{S}_0,\mathbf{S}_1}(A) \leq$ Area + Area $\leq$ Area + Area

Giving Bound on Nice Mu Transcripts

induced su transcripts are good

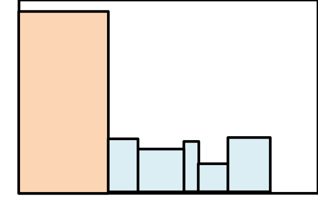


$$\mathbf{Adv}_{\mathbf{S}_0,\mathbf{S}_1}(A) \leq \boxed{\text{Area}} + \boxed{\text{Area}}$$

Goal: bound Area by analyses on **su** good transcripts

Giving Bound on Nice Mu Transcripts

(Nice Mu Transcripts: induced su transcripts are good)



$\mathbf{Adv}_{\mathbf{S}_0,\mathbf{S}_1}(A) \leq$ Area + Area

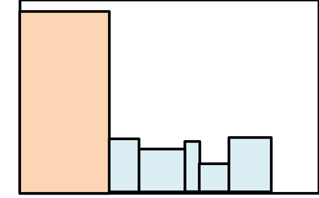
Goal: bound Area by analyses on **su** good transcripts

How: Establish a bound on any good **su** transcript τ of parameters p, q, σ

$$1 - \frac{\mathbf{p}_{\mathbf{S}_1}(\tau)}{\mathbf{p}_{\mathbf{S}_0}(\tau)} \leq \underbrace{\epsilon(p, q, \sigma)}_{\text{super-additive}} + \epsilon'(p, q, \sigma)$$

Used in H-coefficient technique [Patarin 08] to establish su bound

Giving Bound on Nice Mu Transcripts



induced su transcripts are good

$\mathbf{Adv}_{\mathbf{S}_0,\mathbf{S}_1}(A) \leq$ Area + Area

Goal: bound Area by analyses on **su** good transcripts

How: Establish a bound on any good **su** transcript τ of parameters p, q, σ

$$1 - \frac{\mathbf{p}_{\mathbf{S}_1}(\tau)}{\mathbf{p}_{\mathbf{S}_0}(\tau)} \leq \epsilon(p, q, \sigma) + \epsilon'(p, q, \sigma)$$

Used in H-coefficient technique [Patarin 08] to establish su bound

super-additive

Super-additivity: $\epsilon(x, y_0, z_0) + \epsilon(x, y_1, z_1) \leq \epsilon(x, y_0 + y_1, z_0 + z_1)$

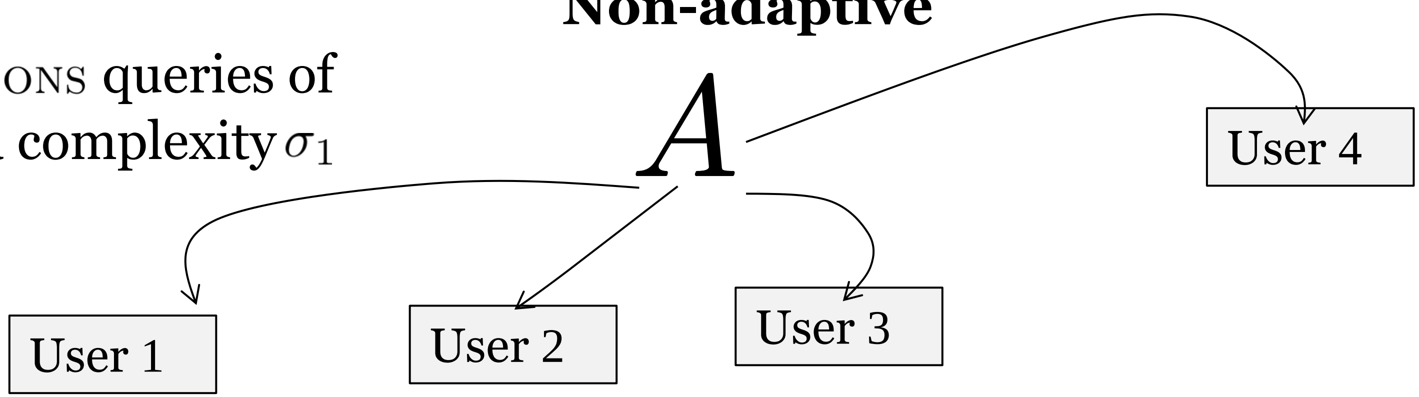
Example: $\epsilon(p, q, \sigma) = \dfrac{\sigma^2 + q^2}{2^n}$ is super-additive

$\epsilon(p, q, \sigma) = \dfrac{p}{2^k}$ is **not** super-additive

Simplified Almost Proximity: From Su to Mu Security

Non-adaptive

q_1 CONS queries of data complexity σ_1



Totally, $\sum_i q_i = q$ CONS queries of data complexity $\sum_i \sigma_i \leq \sigma$ and p PRIM queries

> Suppose that for any su adversary B of parameters p, q, σ
>
> $$\mathbf{Adv}_{\mathbf{S}_0,\mathbf{S}_1}(B) \leq \epsilon(p,q,\sigma) + \epsilon'(p,q,\sigma)$$

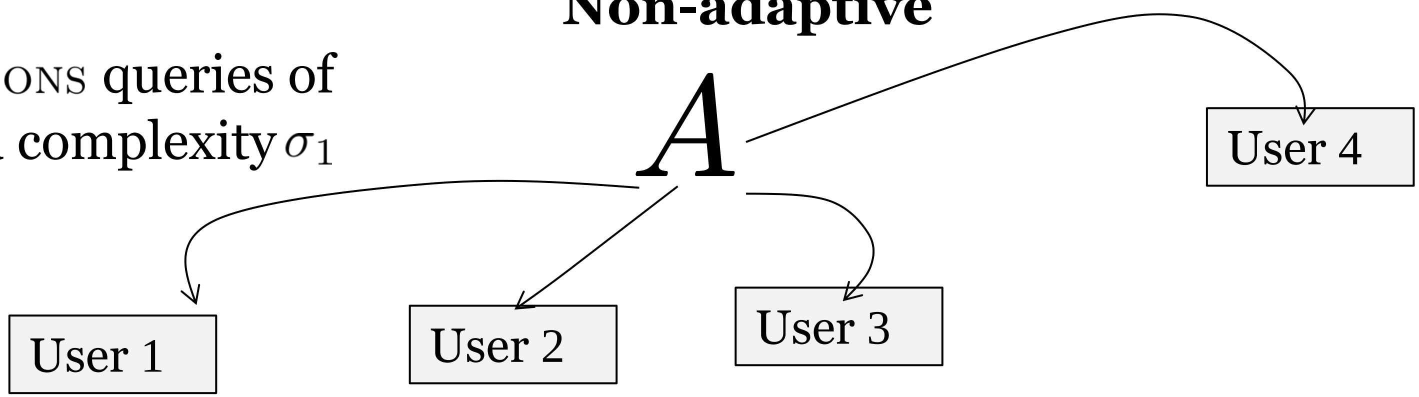
Hybrid argument:

$$\begin{aligned}\mathbf{Adv}_{\mathbf{S}_0,\mathbf{S}_1}(A) &\leq \sum_i \epsilon(p+\sigma t, q_i, \sigma_i) + \epsilon'(p+\sigma t, q_i, \sigma_i) \\ &\leq \epsilon(p+\sigma t, q, \sigma) + q \cdot \epsilon'(p+\sigma t, q, \sigma)\end{aligned}$$

Simplified Almost Proximity: From Su to Mu Security

Non-adaptive

q_1 $\textsc{Cons}$ queries of data complexity σ_1



Totally, $\sum_i q_i = q$ $\textsc{Cons}$ queries of data complexity $\sum_i \sigma_i \le \sigma$ and p $\textsc{Prim}$ queries

Suppose that for any su adversary B of parameters p, q, σ

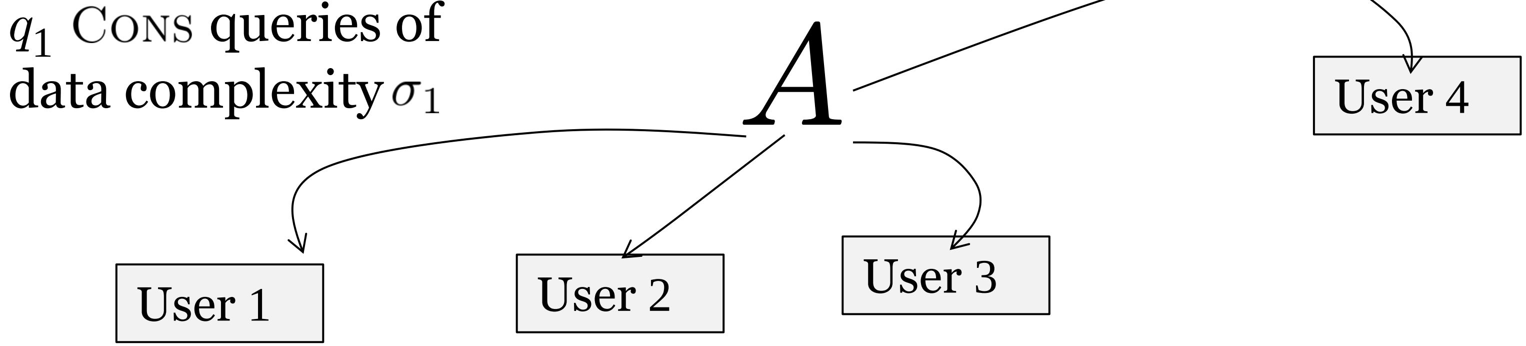
$$\mathbf{Adv}_{\mathbf{S}_0,\mathbf{S}_1}(B) \le \epsilon(p,q,\sigma) + \epsilon'(p,q,\sigma)$$

Accounting for simulated queries

Hybrid argument:
$$\begin{aligned}\mathbf{Adv}_{\mathbf{S}_0,\mathbf{S}_1}(A) &\le \sum_i \epsilon(p+\sigma t, q_i, \sigma_i) + \epsilon'(p+\sigma t, q_i, \sigma_i) \\ &\le \epsilon(p+\sigma t, q, \sigma) + q \cdot \epsilon'(p+\sigma t, q, \sigma)\end{aligned}$$

Simplified Almost Proximity: From Su to Mu Security

Non-adaptive



Totally, $\sum_i q_i = q$ Cons queries of data complexity $\sum_i \sigma_i \leq \sigma$ and p Prim queries

Suppose that for any su adversary B of parameters p, q, σ

$$\mathbf{Adv}_{\mathbf{S}_0,\mathbf{S}_1}(B) \leq \epsilon(p,q,\sigma) + \epsilon'(p,q,\sigma)$$

Accounting for simulated queries

Hybrid argument:
$$\begin{aligned}\mathbf{Adv}_{\mathbf{S}_0,\mathbf{S}_1}(A) &\leq \sum_i \epsilon(p+\sigma t, q_i, \sigma_i) + \epsilon'(p+\sigma t, q_i, \sigma_i) \\ &\leq \epsilon(p+\sigma t, q, \sigma) + q \cdot \epsilon'(p+\sigma t, q, \sigma)\end{aligned}$$

Super-additivity

Simplified Almost Proximity: From Su to Mu Security

Main problem in mu security: Adversary can **adaptively** distribute the resources across multiple users

Simplified Almost Proximity: From Su to Mu Security

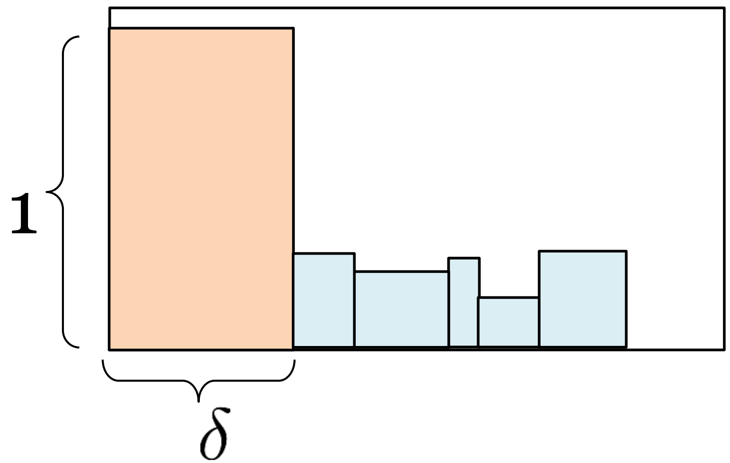
Main problem in mu security: Adversary can **adaptively** distribute the resources across multiple users

To avoid adaptivity, do hybrid argument at the **transcript level**

Simplified Almost Proximity: From Su to Mu Security

Main problem in mu security: Adversary can **adaptively** distribute the resources across multiple users

To avoid adaptivity, do hybrid argument at the **transcript level**



$$1 - \frac{\mathbf{p}_{\mathbf{s}_1}(\tau)}{\mathbf{p}_{\mathbf{s}_0}(\tau)} \le \epsilon(p, q, \sigma) + \epsilon'(p, q, \sigma)$$

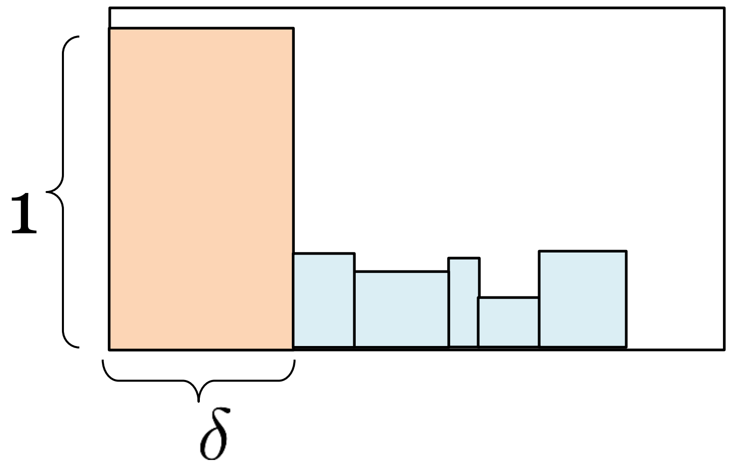
good su transcript

$\mathbf{Adv}_{\mathbf{s}_0,\mathbf{s}_1}(A) \le$ Area + Area

Simplified Almost Proximity: From Su to Mu Security

Main problem in mu security: Adversary can **adaptively** distribute the resources across multiple users

To avoid adaptivity, do hybrid argument at the **transcript level**



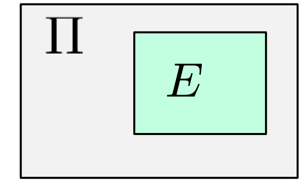
$$1 - \frac{\mathbf{p}_{\mathbf{s}_1}(\tau)}{\mathbf{p}_{\mathbf{s}_0}(\tau)} \leq \epsilon(p, q, \sigma) + \epsilon'(p, q, \sigma)$$

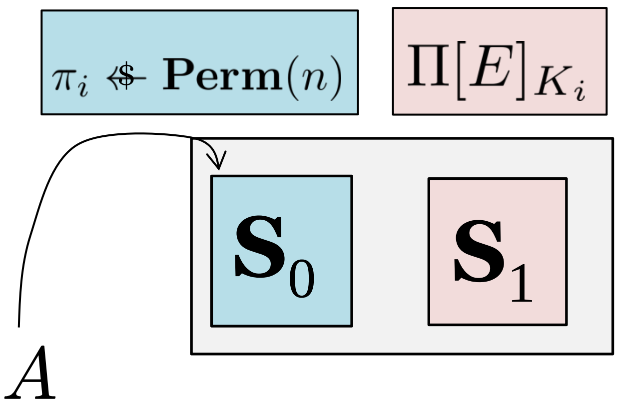
good su transcript

$$\mathbf{Adv}_{\mathbf{s}_0,\mathbf{s}_1}(A) \leq \text{Area} + \text{Area}$$

$$\leq \text{Area} + 2\epsilon(p + \sigma t, q, \sigma) + 2q \cdot \epsilon'(p + \sigma t, q, \sigma)$$

Technique for mu-CCA Security of Blockcipher





Blockcipher $\Pi[E] : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$

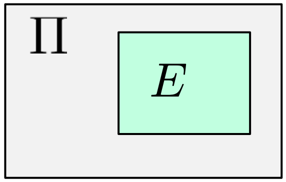
Ideal cipher $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$

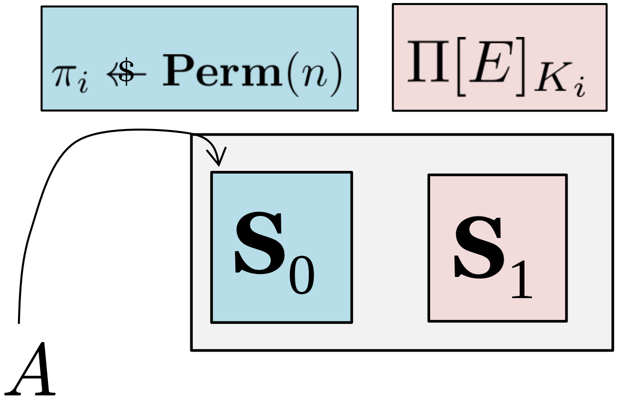
A call to Π/Π^{-1} makes t calls to E/E^{-1}

Accounting A's resources via p and q only

Goal: Do only su analyses, but achieve mu results

Technique for mu-CCA Security of Blockcipher





Blockcipher $\Pi[E] : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$

Ideal cipher $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$

A call to Π/Π^{-1} makes t calls to E/E^{-1}

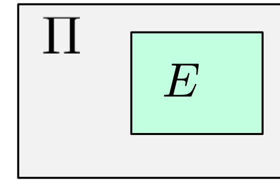
Accounting A's resources via p and q only

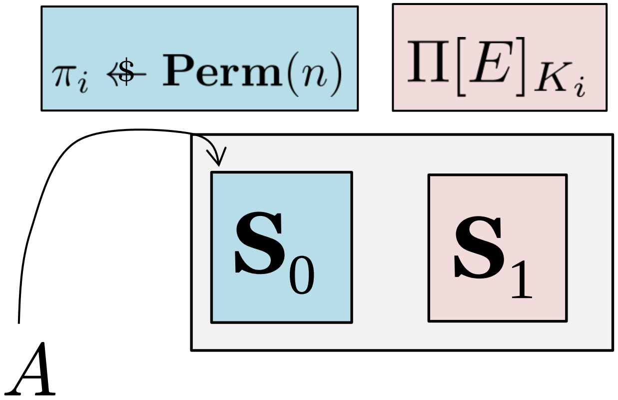
Goal: Do only su analyses, but achieve mu results

Classify **su** transcripts into "good" and "bad"

No restriction

Technique for mu-CCA Security of Blockcipher





Blockcipher $\Pi[E] : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$

Ideal cipher $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$

A call to Π/Π^{-1} makes t calls to E/E^{-1}

Accounting A's resources via p and q only

Goal: Do only su analyses, but achieve mu results

Classify **su** transcripts into "good" and "bad"

No restriction

Bound $\Pr[\text{Getting a bad su transcript in } \mathbf{S}_0] \leq \epsilon^*(p, q)$

using q construction queries and p primitive queries

Giving Bound on Good Su Transcripts

Establish a bound on any good **su** transcript τ of parameters p and q

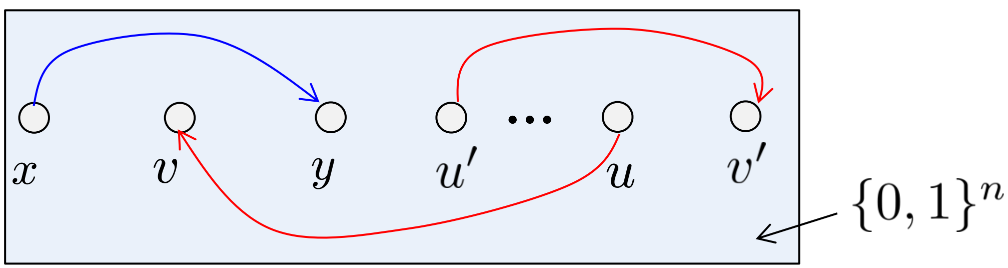
$$1 - \frac{\mathbf{ps}_1(\tau)}{\mathbf{ps}_0(\tau)} \leq \underbrace{\epsilon(p,q)}_{\text{super-additive}} + \epsilon'(p,q) + \epsilon''(p,q) \cdot \mathbf{Coll}(\tau)$$

Giving Bound on Good Su Transcripts

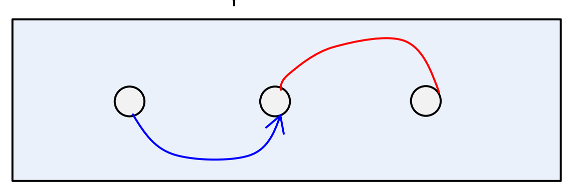
Establish a bound on any good **su** transcript τ of parameters p and q

$$1 - \frac{\mathbf{ps}_1(\tau)}{\mathbf{ps}_0(\tau)} \leq \underbrace{\epsilon(p,q)}_{\text{super-additive}} + \epsilon'(p,q) + \epsilon''(p,q) \cdot \mathbf{Coll}(\tau)$$

Transcript: $(\textsc{Cons}, 1, (+, x), y), (\textsc{Prim}, (-, K_1, u), v), \ldots, (\textsc{Prim}, (+, K_2, u'), v')$



$\mathbf{Coll}(\tau)$: # of primitive queries that have colliding construction queries



From Su to Mu Security

Using transcript-level hybrid argument, when we move from su to mu:

$$\underbrace{\epsilon \longrightarrow 2\epsilon;}_{\text{super-additivity}} \; \epsilon' \longrightarrow 2q \cdot \epsilon'; \; \epsilon^* \longrightarrow 2q \cdot \epsilon^*$$

$$\underbrace{\mathbf{Coll}(\tau)}_{\leq \min\{p, 2^{k+2}q\}} \cdot \epsilon'' \longrightarrow 40(p + qt) \max\{n, 2q/2^n\}\epsilon''$$

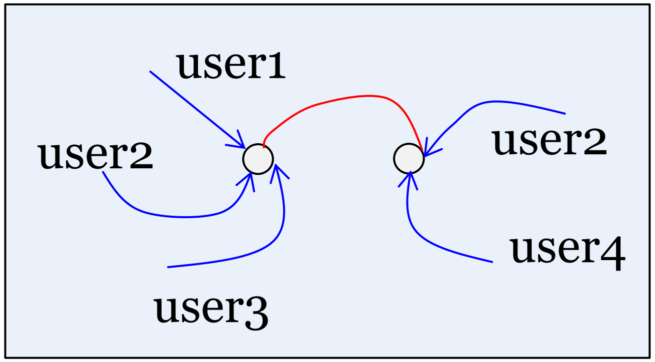
From Su to Mu Security

Using transcript-level hybrid argument, when we move from su to mu:

$$\underbrace{\epsilon \longrightarrow 2\epsilon;}_{\text{super-additivity}} \; \epsilon' \longrightarrow 2q \cdot \epsilon'; \; \epsilon^* \longrightarrow 2q \cdot \epsilon^*$$

$$\underbrace{\mathbf{Coll}(\tau)}_{\leq \min\{p, 2^{k+2}q\}} \cdot \epsilon'' \longrightarrow 40(p+qt)\max\{n, 2q/2^n\}\epsilon''$$

Intuition: In a mu transcript obtained in the ideal world, each red arrow is unlikely to collide with more than $20\max\{n, 2q/2^n\}$ blue ones.



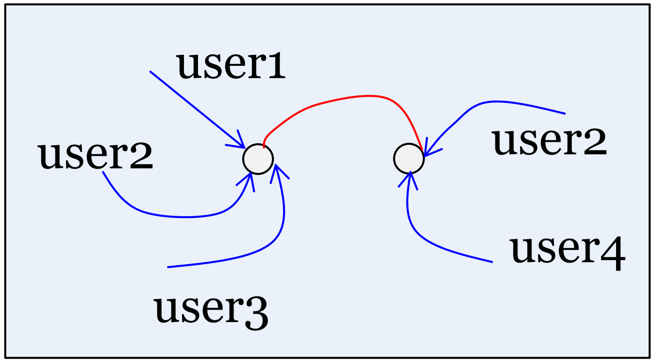
From Su to Mu Security

Using transcript-level hybrid argument, when we move from su to mu:

$$\underbrace{\epsilon \longrightarrow 2\epsilon;}_{\text{super-additivity}} \ \epsilon' \longrightarrow 2q \cdot \epsilon'; \ \epsilon^* \longrightarrow 2q \cdot \epsilon^*$$

$$\underbrace{\mathbf{Coll}(\tau)}_{\leq \min\{p, 2^{k+2}q\}} \cdot \epsilon'' \longrightarrow 40(p+qt)\max\{n, 2q/2^n\}\epsilon''$$

Intuition: In a mu transcript obtained in the ideal world, each red arrow is unlikely to collide with more than $20\max\{n, 2q/2^n\}$ blue ones.



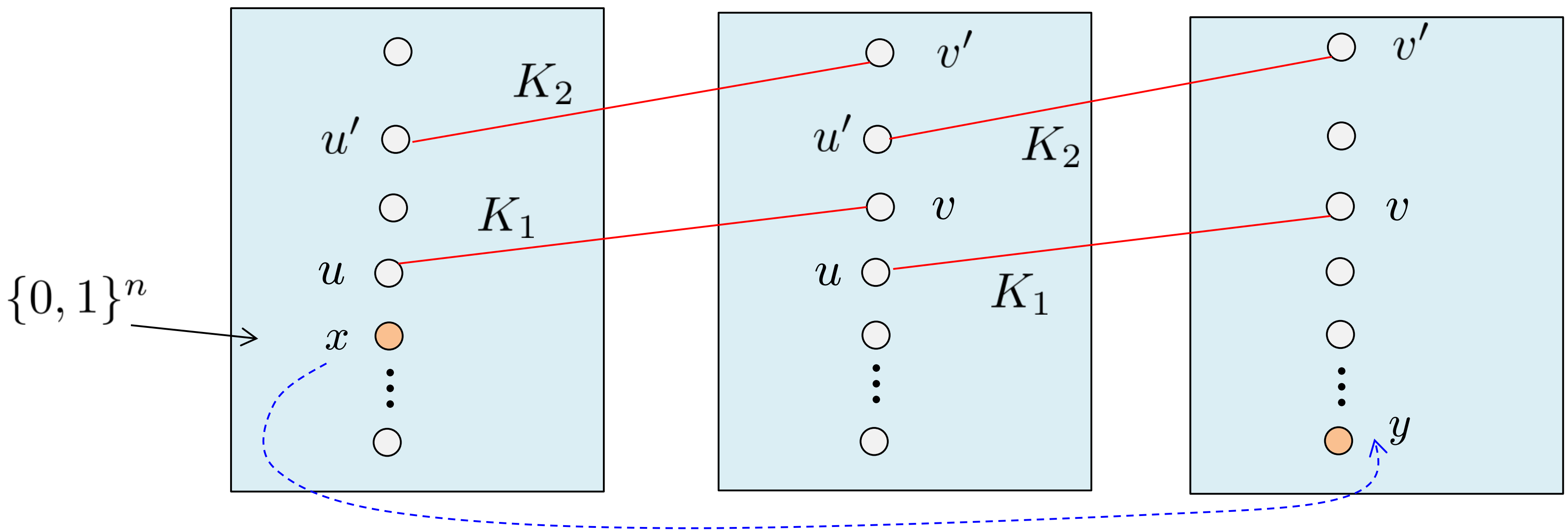
Theorem: Assume the su conditions hold,

$$\mathbf{Adv}^{\text{mu-cca}}_{\Pi[E]}(q) \leq 2^{-n} + 2\epsilon + 2q \cdot (\epsilon' + \epsilon^*) + 40(p+qt)\max\{n, 2q/2^n\}\epsilon''$$

Any function takes arguments $p + qt$ and q

Analyzing Double Encryption

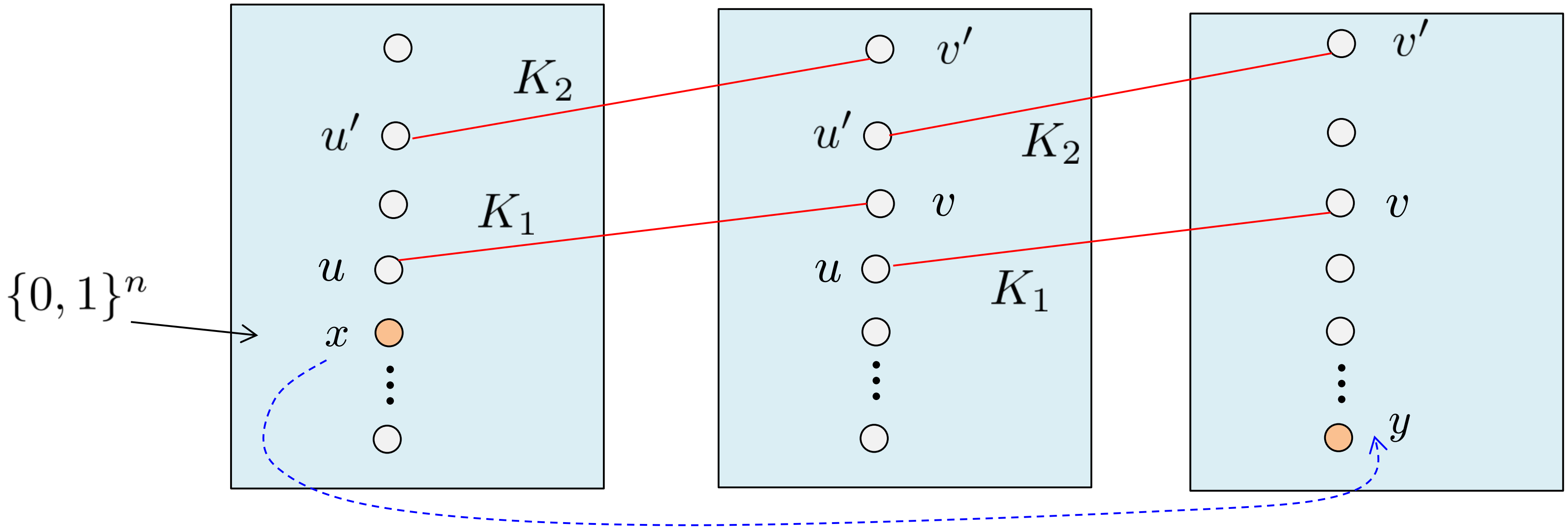
Su Transcript: $(\textsc{Cons}, 1, (+, x), y), (\textsc{Prim}, (-, K_1, u), v), \ldots, (\textsc{Prim}, (+, K_2, u'), v')$



Graphical representation of the transcript

Analyzing Double Encryption

Su Transcript: $(\textsc{Cons}, 1, (+, x), y), (\textsc{Prim}, (-, K_1, u), v), \ldots, (\textsc{Prim}, (+, K_2, u'), v')$



Graphical representation of the transcript

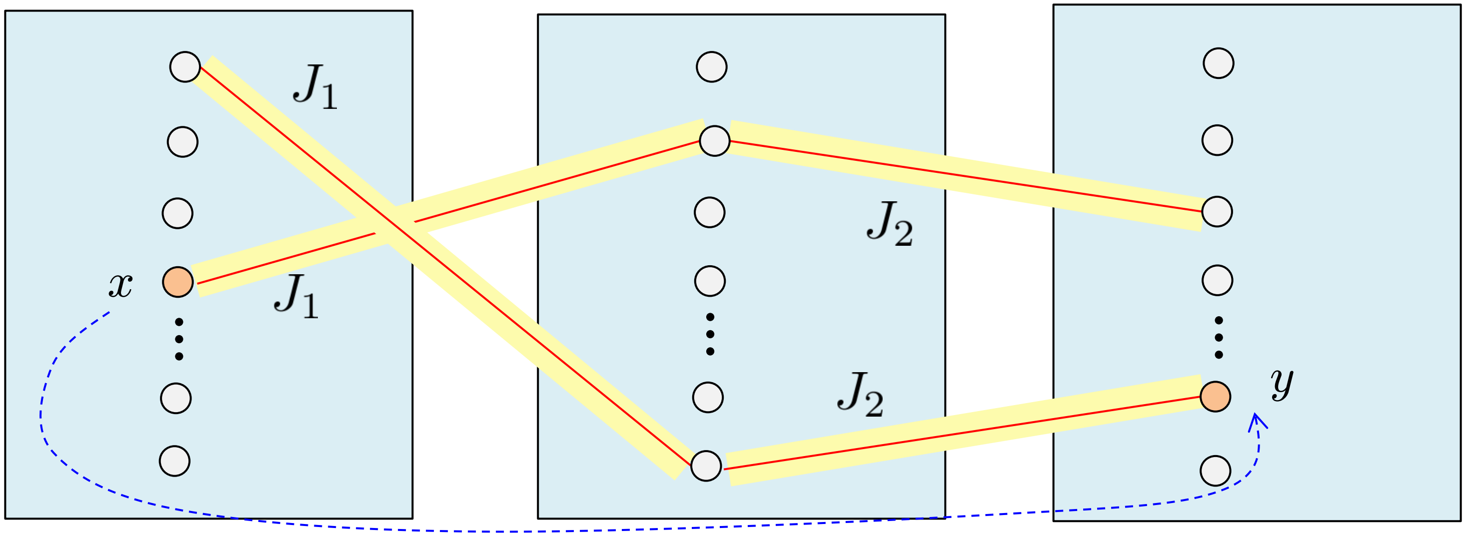
Extend transcripts with keys: (J_1, J_2)

Real world: the real keys (revealed when finish querying)

Ideal world: random strings, independent of anything else

Analyzing Double Encryption

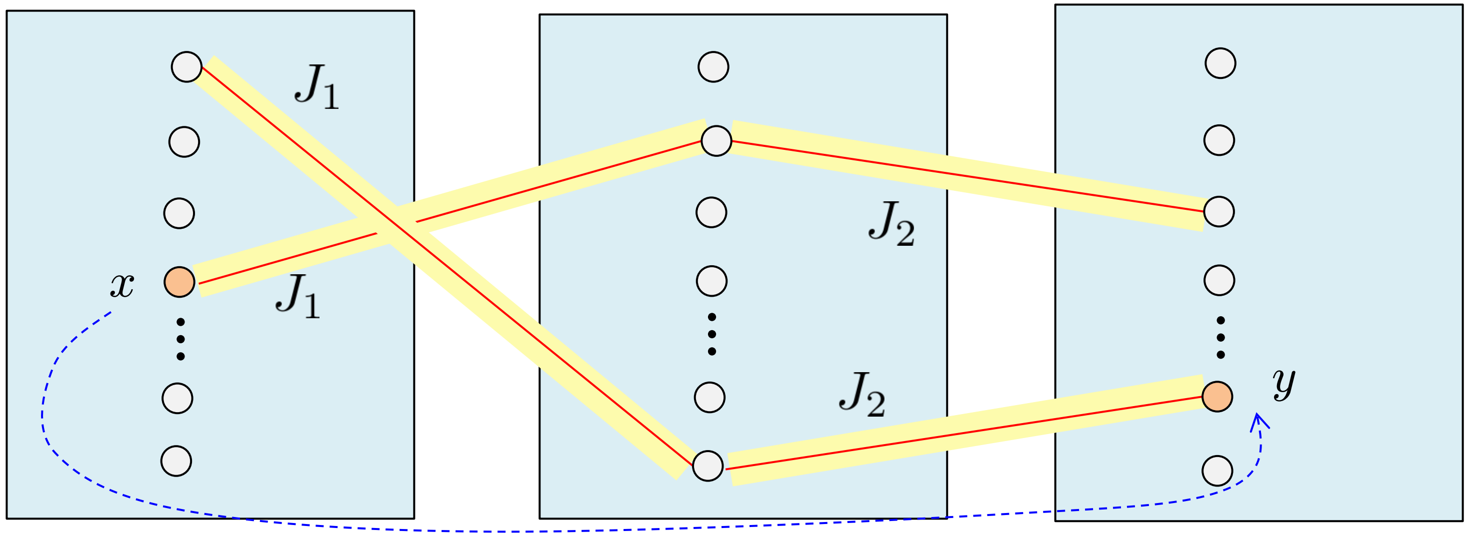
(J_1, J_2) : revealed keys



Trivial to distinguish when "chains" appear

Analyzing Double Encryption

(J_1, J_2) : revealed keys

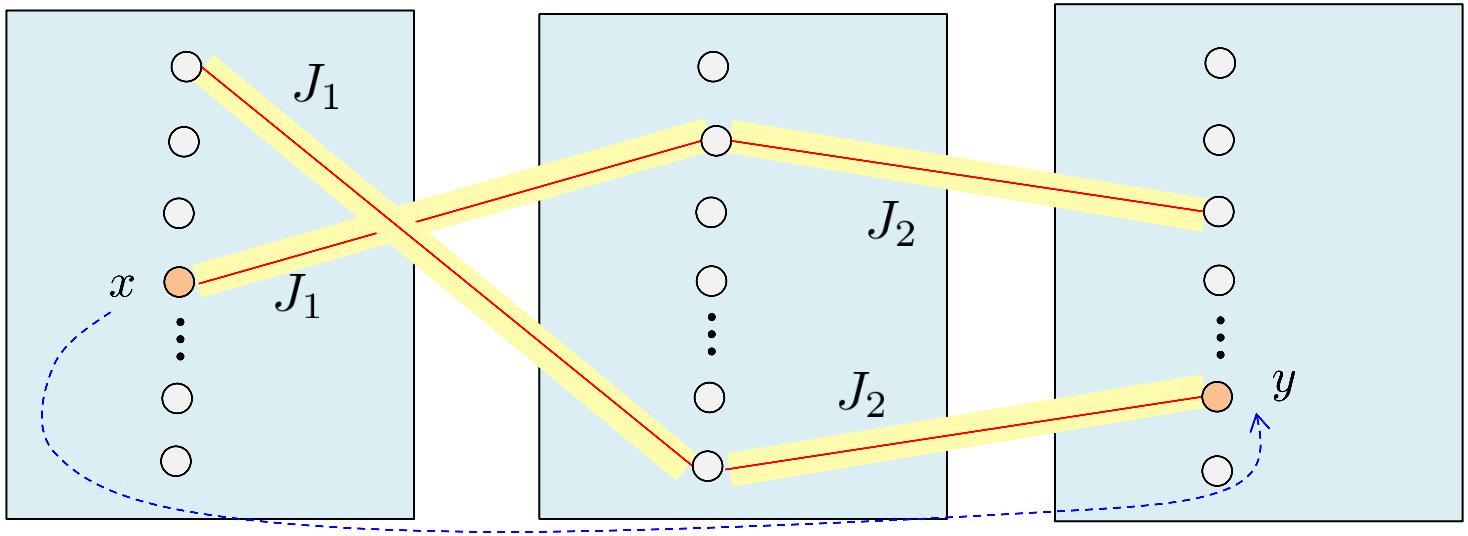


Trivial to distinguish when "chains" appear

Want: Bound $\Pr[\text{extending } \tau \text{ in the ideal world results in chain}]$ via $\mathbf{Coll}(\tau)$

Analyzing Double Encryption

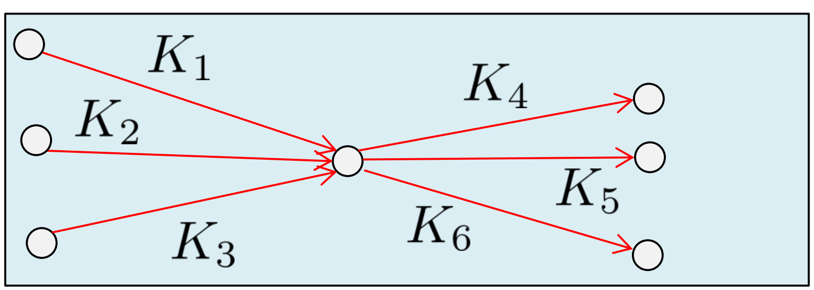
(J_1, J_2) : revealed keys



Trivial to distinguish when "chains" appear

Want: Bound $\Pr[\text{extending } \tau \text{ in the ideal world results in chain}]$ via $\mathbf{Coll}(\tau)$

Inferior bound if too many **red arrows** hit the same point.



Analyzing Double Encryption

p: #primitive queries
q: #construction queries
k: key length
n: block length

Definition: A su transcript is bad if it has $B = 5\max\{n + k/2, 2p/2^n\}$ red arrows hitting the same point.

Analyzing Double Encryption

p: #primitive queries
q: #construction queries
k: key length
n: block length

Definition: A su transcript is bad if it has $B = 5\max\{n + k/2, 2p/2^n\}$ red arrows hitting the same point.

Claim: $\Pr[\text{Getting a bad su transcript in the ideal world}] \leq \frac{1}{2^{n+k}}$

Analyzing Double Encryption

p: #primitive queries
q: #construction queries
k: key length
n: block length

Definition: A su transcript is bad if it has $B = 5\max\{n + k/2, 2p/2^n\}$ red arrows hitting the same point.

Claim: $\Pr[\text{Getting a bad su transcript in the ideal world}] \leq \frac{1}{2^{n+k}}$

No extension

Claim: For any good su transcript τ

$$1 - \frac{\mathbf{ps}_1(\tau)}{\mathbf{ps}_0(\tau)} \leq \frac{2p \cdot \mathbf{Coll}(\tau) + 5Bp + 2qB^2 + 2Bpq}{2^{2k}} + \frac{q}{2^{k+n/2}} + \frac{qB^2}{2^{2k}}$$

Probability that extending τ in the ideal world results in a chain

Conclusion

- The **almost proximity** method is very powerful in obtaining strong mu security

- Contrary to conventional wisdom, Double Encryption does add some security.

+ The analysis here might be not tight: We can't find matching attacks if $n \ll k$