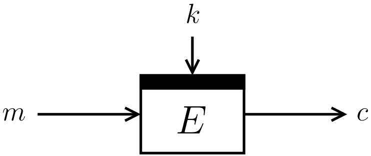
# Insuperability of the Standard Versus Ideal Model Gap for Tweakable Blockcipher Security

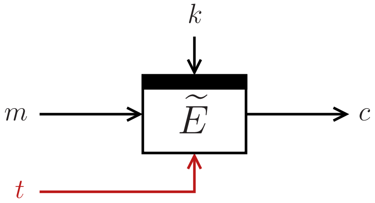
Bart Mennink
Radboud University (The Netherlands)

CRYPTO 2017
August 21, 2017

# Tweakable Blockciphers

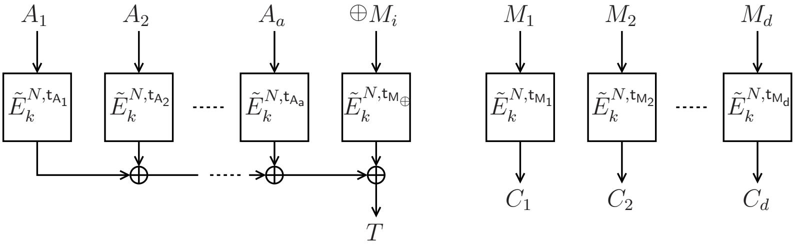


# Tweakable Blockciphers



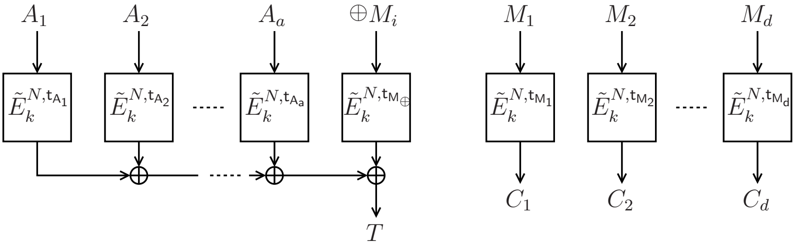
- Tweak: flexibility to the cipher
- Each tweak gives different permutation

# Tweakable Blockciphers in OCBx


$A_1$
$A_2$
$A_a$
$\oplus M_i$
$M_1$
$M_2$
$M_d$
$\widetilde{E}_k^{N,\mathsf{t}_{\mathsf{A}_1}}$
$\widetilde{E}_k^{N,\mathsf{t}_{\mathsf{A}_2}}$
$\widetilde{E}_k^{N,\mathsf{t}_{\mathsf{A}_a}}$
$\widetilde{E}_k^{N,\mathsf{t}_{\mathsf{M}_\oplus}}$
$\widetilde{E}_k^{N,\mathsf{t}_{\mathsf{M}_1}}$
$\widetilde{E}_k^{N,\mathsf{t}_{\mathsf{M}_2}}$
$\widetilde{E}_k^{N,\mathsf{t}_{\mathsf{M}_d}}$
$T$
$C_1$
$C_2$
$C_d$

- Generalized OCB by Rogaway et al. [RBBK01,Rog04,KR11]

# Tweakable Blockciphers in OCBx


$A_1$
$A_2$
$A_a$
$\oplus M_i$
$M_1$
$M_2$
$M_d$
$\widetilde{E}_k^{N,\mathsf{t}_{\mathsf{A}_1}}$
$\widetilde{E}_k^{N,\mathsf{t}_{\mathsf{A}_2}}$
$\widetilde{E}_k^{N,\mathsf{t}_{\mathsf{A}_a}}$
$\widetilde{E}_k^{N,\mathsf{t}_{\mathsf{M}_\oplus}}$
$\widetilde{E}_k^{N,\mathsf{t}_{\mathsf{M}_1}}$
$\widetilde{E}_k^{N,\mathsf{t}_{\mathsf{M}_2}}$
$\widetilde{E}_k^{N,\mathsf{t}_{\mathsf{M}_d}}$
$T$
$C_1$
$C_2$
$C_d$

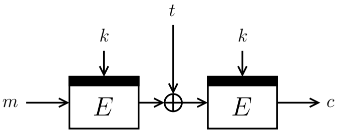
- Generalized OCB by Rogaway et al. [RBBK01,Rog04,KR11]
- Internally based on tweakable blockcipher $\widetilde{E}$
    - Tweak $(N, \text{tweak})$ is unique for every evaluation
    - Different blocks always transformed under different tweak

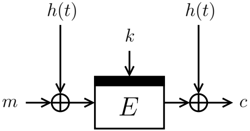
# Dedicated Tweakable Blockciphers

- Hasty Pudding Cipher [Sch98]
  - AES submission, "first tweakable cipher"
- Mercy [Cro01]
  - Disk encryption
- Threefish [FLS+07]
  - SHA-3 submission Skein
- TWEAKEY framework [JNP14]
  - Four CAESAR submissions
  - SKINNY & MANTIS

# Modular Designs

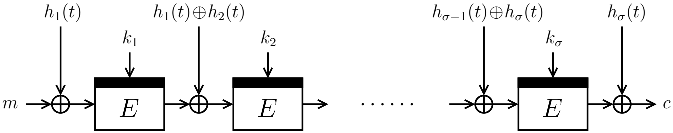
- LRW1 and LRW2 by Liskov et al. [LRW02]:





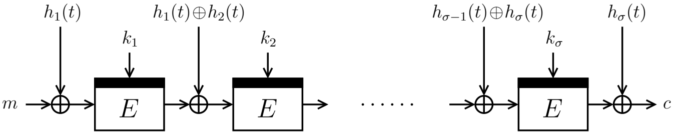
- $h$ is XOR-universal hash
- Related: XEX
- Secure up to $2^{n/2}$ queries

# Modular Designs



- LRW2$[\sigma]$: concatenation of $\sigma$ LRW2's
- $k_1, \ldots, k_\sigma$ and $h_1, \ldots, h_\sigma$ independent

# Modular Designs



- LRW2$[\sigma]$: concatenation of $\sigma$ LRW2's
- $k_1, \ldots, k_\sigma$ and $h_1, \ldots, h_\sigma$ independent

- $\sigma = 2$: secure up to $2^{2n/3}$ queries [LST12,Pro14]
- $\sigma \geq 2$ even: secure up to $2^{\sigma n/(\sigma+2)}$ queries [LS13]
- Conjecture: optimal $2^{\sigma n/(\sigma+1)}$ security

# State of the Art

| scheme | security ($\log_2$) | key length | cost $E$ | $\otimes/h$ |
|---|---|---|---|---|
| LRW1 | $n/2$ | $n$ | 2 | 0 |
| LRW2 | $n/2$ | $2n$ | 1 | 1 |
| XEX | $n/2$ | $n$ | 2 | 0 |
| LRW2$[2]$ | $2n/3$ | $4n$ | 2 | 2 |
| LRW2$[\sigma]$ | $\sigma n/(\sigma+2)$ | $2\sigma n$ | $\sigma$ | $\sigma$ |

Optimal $2^n$ security only if key length and cost $\to \infty$?

# Tweak-Dependent Keys

**Efficiency**

tweak schedule lighter than key schedule

# Tweak-Dependent Keys

**Efficiency**

tweak schedule lighter than key schedule

**Security**

tweak schedule stronger than key schedule

# Tweak-Dependent Keys

**Efficiency**

tweak schedule lighter than key schedule

**Security**

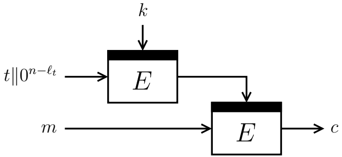
tweak schedule stronger than key schedule

Tweak and key change approximately equally expensive

(as is e.g. done in TWEAKEY [JNP14])

# Tweak-Dependent Keys: Modular Designs

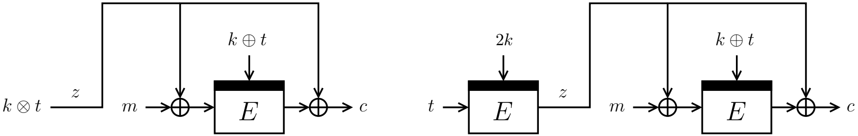
- Minematsu [Min09]:



- Secure up to $\max\{2^{n/2}, 2^{n-\ell_t}\}$ queries
- Beyond birthday bound for $\ell_t < n/2$
- Security gain using XTX [MI15]

# Tweak-Dependent Keys: Modular Designs

- Mennink [Men15]:



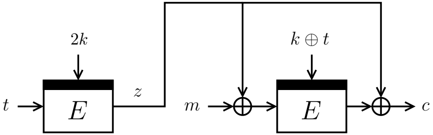
- Secure up to $2^{2n/3}$ and $2^n$ queries
- Generalized by Wang et al. [WGZ+16]
- Proof in ideal cipher model

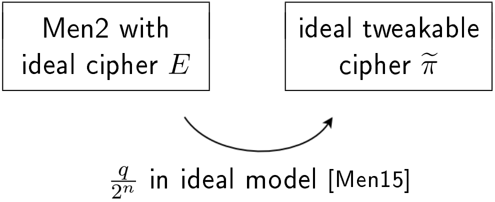
# Tweak-Dependent Keys: State of the Art

| scheme | security ($\log_2$) | key length | cost |  |  |
|---|---|---|---|---|---|
|  |  |  | $E$ | $\otimes/h$ | tdk |
| LRW1 | $n/2$ | $n$ | 2 | 0 | 0 |
| LRW2 | $n/2$ | $2n$ | 1 | 1 | 0 |
| XEX | $n/2$ | $n$ | 2 | 0 | 0 |
| LRW2[2] | $2n/3$ | $4n$ | 2 | 2 | 0 |
| LRW2[$\sigma$] | $\sigma n/(\sigma+2)$ | $2\sigma n$ | $\sigma$ | $\sigma$ | 0 |
| Min | $\max\{n/2, n-\lvert t\rvert\}$ | $n$ | 2 | 0 | 1 |
| Men1 | $2n/3$ ⋆ | $n$ | 1 | 1 | 1 |
| Men2,WGZ+ | $n$ ⋆ | $n$ | 2 | 0 | 1 |

⋆ ideal cipher model

# Why the Ideal Cipher Model?



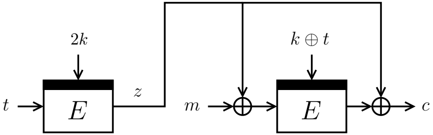


Men2 with ideal cipher $E$

ideal tweakable cipher $\widetilde{\pi}$

$\frac{q}{2^n}$ in ideal model [Men15]

# Why the Ideal Cipher Model?



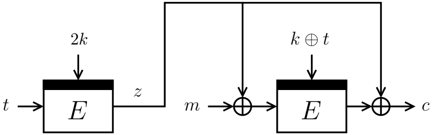
Men2 with any cipher $E$

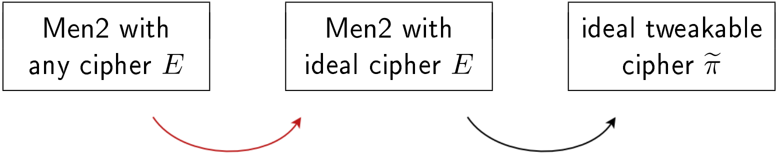
Men2 with ideal cipher $E$

ideal tweakable cipher $\widetilde{\pi}$

$\frac{q}{2^n}$ in ideal model [Men15]

# Why the Ideal Cipher Model?





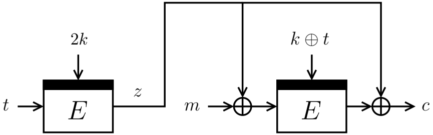
Men2 with any cipher $E$

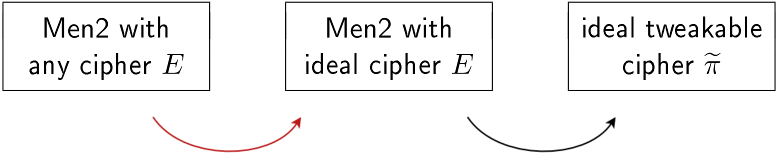
Men2 with ideal cipher $E$

ideal tweakable cipher $\widetilde{\pi}$

generic: security of $E$ $\quad \frac{q}{2^n}$ in ideal model [Men15]

# Why the Ideal Cipher Model?





Men2 with any cipher $E$

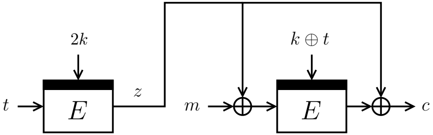
Men2 with ideal cipher $E$

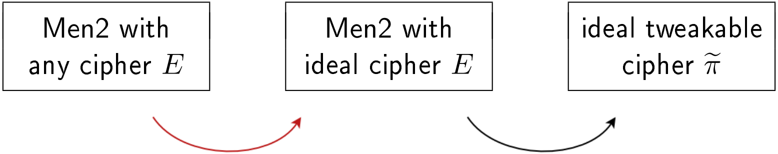
ideal tweakable cipher $\widetilde{\pi}$

generic: security of $E$ $\approx$ $\oplus$-rk security of $E$

$\frac{q}{2^n}$ in ideal model [Men15]

# Why the Ideal Cipher Model?





Men2 with any cipher $E$

Men2 with ideal cipher $E$

ideal tweakable cipher $\widetilde{\pi}$

generic: security of $E$

$\approx$

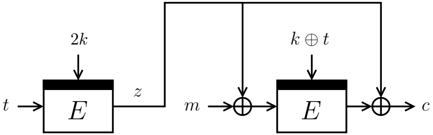
$\oplus$-rk security of $E$

$=$

$\frac{q^2}{2^n}$ only

$\frac{q}{2^n}$ in ideal model [Men15]

# Why the Ideal Cipher Model?



Men2 with any cipher $E$

Men2 with ideal cipher $E$

ideal tweakable cipher $\widetilde{\pi}$

generic: security of $E$

$\approx$

$\oplus$-rk security of $E$

$=$

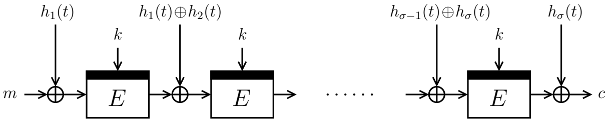
$\frac{q^2}{2^n}$ only

$\frac{q}{2^n}$ in ideal model [Men15]

- Cannot be used to break Men2
- Generic step is unnecessarily loose

# Two Extremes

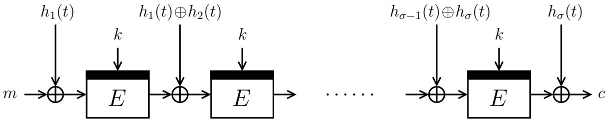
## LRW2$[\sigma]$ (conjectured):



$$\mathbf{Adv}^{\widetilde{\text{sprp}}}_{\mathsf{LRW2}[\sigma]}(q,t) \leq \underbrace{\mathbf{Adv}^{\text{sprp}}_{E}(\sigma q,t)}_{\approx t/2^n \text{ (optimal)}} + \underbrace{O(q^{\sigma+1}/2^{\sigma n})}_{\text{non-optimal}}$$

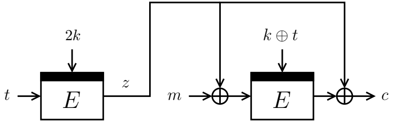
# Two Extremes

## LRW2$[\sigma]$ (conjectured):



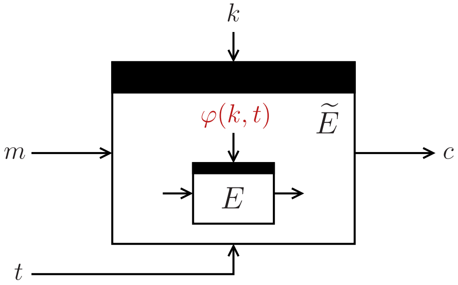
$$\mathbf{Adv}^{\widetilde{\text{sprp}}}_{\text{LRW2}[\sigma]}(q,t) \leq \underbrace{\mathbf{Adv}^{\text{sprp}}_{E}(\sigma q, t)}_{\approx t/2^n \text{ (optimal)}} + \underbrace{O(q^{\sigma+1}/2^{\sigma n})}_{\text{non-optimal}}$$

## Men2:



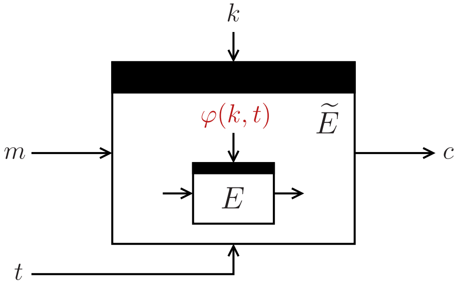
$$\mathbf{Adv}^{\widetilde{\text{sprp}}}_{\text{Men2}}(q,t) \leq \underbrace{\mathbf{Adv}^{\oplus\text{-rk}}_{E}(2q, t)}_{\approx 2qt/2^n \text{ (non-optimal)}} + \underbrace{O(q/2^n)}_{\text{optimal}}$$

# Somewhat Tweak-Rekeyability



- Tweak influence to key present but limited

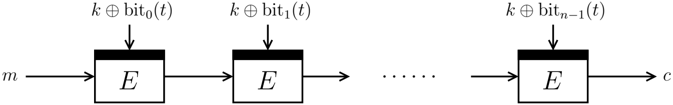
# Somewhat Tweak-Rekeyability



- Tweak influence to key present but limited
- Say $\lambda$ different $E$-instances

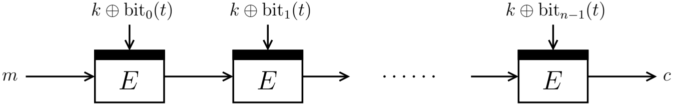
$$\mathbf{Adv}^{\widetilde{\text{sprp}}}_{\widetilde{E}}(q,t) \leq \underbrace{\mathbf{Adv}^{\text{rk}}_{E}(\sigma q,t)}_{\substack{\approx \lambda t/2^n \\ \text{(close to optimal)}}} + \underbrace{O(q/2^n)}_{\substack{\text{hopefully} \\ \text{optimal}}}$$

# Naive Example


$k \oplus \mathrm{bit}_0(t)$
$k \oplus \mathrm{bit}_1(t)$
$k \oplus \mathrm{bit}_{n-1}(t)$
$m$
$E$
$E$
$\cdots\cdots$
$E$
$c$

$$\mathbf{Adv}^{\widetilde{\mathrm{sprp}}}_{\widetilde{E}}(q,t) \leq \underbrace{\mathbf{Adv}^{\mathrm{rk}}_{E}(nq,t)}_{\approx \lambda t/2^n} + \underbrace{O(??)}_{\text{hopefully optimal}}$$

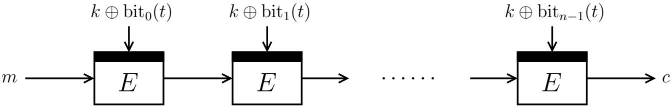
# Naive Example


$k \oplus \mathrm{bit}_0(t)$
$k \oplus \mathrm{bit}_1(t)$
$k \oplus \mathrm{bit}_{n-1}(t)$
$m$
$E$
$E$
$E$
$\cdots\cdots$
$c$

$$\mathbf{Adv}^{\widetilde{\mathrm{sprp}}}_{\widetilde{E}}(q,t) \leq \underbrace{\mathbf{Adv}^{\mathrm{rk}}_{E}(nq,t)}_{\approx \lambda t/2^n} + \underbrace{O(??)}_{\text{hopefully optimal}}$$

- $\lambda = 2$ different $E$-instances

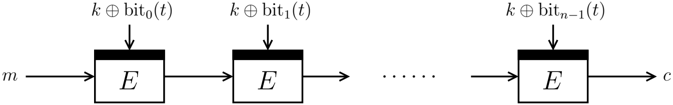
# Naive Example


$k \oplus \mathrm{bit}_0(t)$
$k \oplus \mathrm{bit}_1(t)$
$k \oplus \mathrm{bit}_{n-1}(t)$
$m$
$E$
$E$
$\cdots\cdots$
$E$
$c$

$$\mathbf{Adv}^{\widetilde{\mathrm{sprp}}}_{\widetilde{E}}(q,t) \leq \underbrace{\mathbf{Adv}^{\mathrm{rk}}_{E}(nq,t)}_{\substack{\approx 2t/2^n \\ \text{(optimal)}}} + \underbrace{O(??)}_{\substack{\text{hopefully} \\ \text{optimal}}}$$

- $\lambda = 2$ different $E$-instances

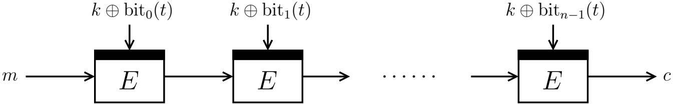
# Naive Example


$k \oplus \mathrm{bit}_0(t)$
$k \oplus \mathrm{bit}_1(t)$
$k \oplus \mathrm{bit}_{n-1}(t)$
$m$
$E$
$E$
$\cdots\cdots$
$E$
$c$

$$\mathbf{Adv}^{\widetilde{\mathrm{sprp}}}_{\widetilde{E}}(q,t) \le \underbrace{\mathbf{Adv}^{\mathrm{rk}}_{E}(nq,t)}_{\substack{\approx 2t/2^n \\ \text{(optimal)}}} + \underbrace{O(1)}_{\text{insecure}}$$

- $\lambda = 2$ different $E$-instances
- $\widetilde{E}$ is of course generically insecure

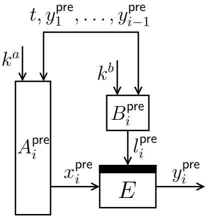
# Naive Example


$k \oplus \mathrm{bit}_0(t)$
$k \oplus \mathrm{bit}_1(t)$
$k \oplus \mathrm{bit}_{n-1}(t)$
$m$
$E$
$E$
$\cdots\cdots$
$E$
$c$

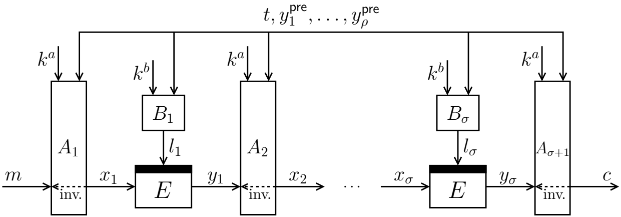
$$\mathbf{Adv}^{\widetilde{\mathrm{sprp}}}_{\widetilde{E}}(q,t) \leq \underbrace{\mathbf{Adv}^{\mathrm{rk}}_{E}(nq,t)}_{\substack{\approx 2t/2^n \\ \text{(optimal)}}} + \underbrace{O(1)}_{\text{insecure}}$$

- $\lambda = 2$ different $E$-instances
- $\widetilde{E}$ is of course generically insecure
- Moreover: $n$ blockcipher calls

# Generalized Design



$m$-independent calls:
$y_1^{\mathsf{pre}}, \ldots, y_\rho^{\mathsf{pre}}$



processing of $m$:
$c$

- $A_i$ need to be invertible
- Some uniformity conditions on $B_i$ apply
- Mixing functions can be anything otherwise

# Generalized Impossibility

If the generic standard-to-ideal reduction is employed,
optimal standard-model security with tweak-rekeying
is at least as hard as without tweak-rekeying

# Generalized Impossibility

If the generic standard-to-ideal reduction is employed,
optimal standard-model security with tweak-rekeying
is at least as hard as without tweak-rekeying

### Proof Idea

- Consider any reasonable tweak-rekeyable scheme

# Generalized Impossibility

If the generic standard-to-ideal reduction is employed,
optimal standard-model security with tweak-rekeying
is at least as hard as without tweak-rekeying

### Proof Idea

- Consider any reasonable tweak-rekeyable scheme
- Threshold for $\lambda = \# \; E$-instances:

# Generalized Impossibility

If the generic standard-to-ideal reduction is employed,
optimal standard-model security with tweak-rekeying
is at least as hard as without tweak-rekeying

### Proof Idea

- Consider any reasonable tweak-rekeyable scheme
- Threshold for $\lambda = \#\ E$-instances:
  - Too high: $\mathbf{Adv}_E^{\mathrm{rk}}$-term dominates and is non-optimal

# Generalized Impossibility

If the generic standard-to-ideal reduction is employed,
optimal standard-model security with tweak-rekeying
is at least as hard as without tweak-rekeying

## Proof Idea

- Consider any reasonable tweak-rekeyable scheme
- Threshold for $\lambda = \#\ E$-instances:
  - Too high: $\mathbf{Adv}_E^{\mathrm{rk}}$-term dominates and is non-optimal
  - Too low:
    - For large set of tweaks: there is no tweak-rekeying
    - Scheme behaves like non-tweak-rekeyable one

# Generalized Impossibility

If the generic standard-to-ideal reduction is employed,
optimal standard-model security with tweak-rekeying
is at least as hard as without tweak-rekeying

## Proof Idea

- Consider any reasonable tweak-rekeyable scheme
- Threshold for $\lambda = \#\ E$-instances:
  - Too high: $\mathbf{Adv}_E^{\mathrm{rk}}$-term dominates and is non-optimal
  - Too low:
    - For large set of tweaks: there is no tweak-rekeying
    - Scheme behaves like non-tweak-rekeyable one
- Even best trade-off will not be optimal!

# Conclusion

## Impossibility Result

- does not say that
  - the generic standard-to-ideal reduction is unavoidable
  - LRW2$[\sigma]$-conjecture holds
  - optimal security cannot be achieved
- but that provable optimality is very unlikely

# Conclusion

## Impossibility Result

- does not say that
  - the generic standard-to-ideal reduction is unavoidable
  - LRW2$[\sigma]$-conjecture holds
  - optimal security cannot be achieved
- but that provable optimality is very unlikely

## Further Questions

- What does this mean for existing x-model results?
- Is the LRW2$[\sigma]$-conjecture reasonable?
- Can we salvage the generic standard-to-ideal reduction?

**Thank you for your attention!**