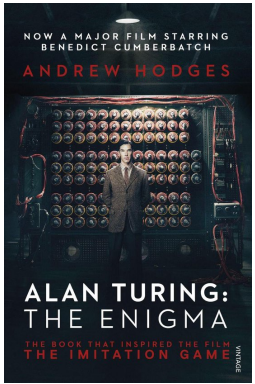
Provably Secure Reflection Ciphers

Tim Beyne and **Yu Long Chen**

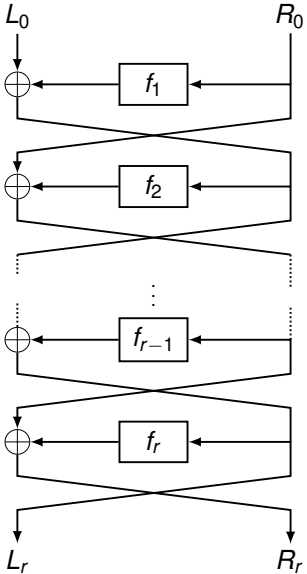
August 18, 2022

Self-Inverse Encryption Schemes



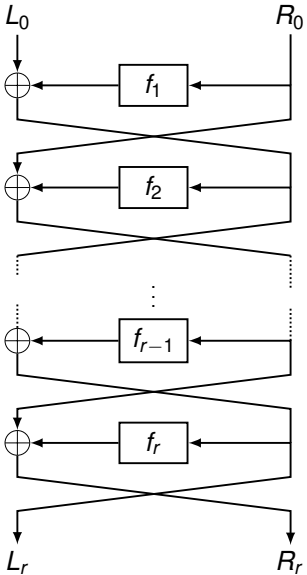
- Fascinating feature: self-inverse
- Enigma: encryption and decryption operations are identical
- Enabled by middle reflector (Umkehrwalze)
- Encryption device considerably more compact

Feistel Ciphers



DES block cipher (Horst Feistel (IBM) + NSA)

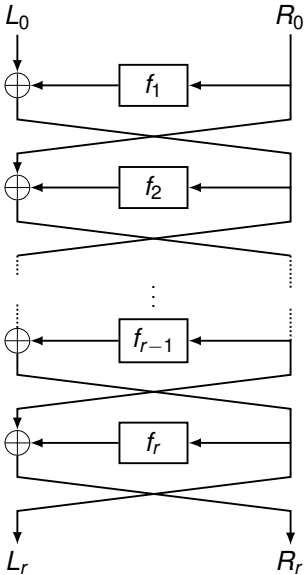
Feistel Ciphers



DES block cipher (Horst Feistel (IBM) + NSA)

- Decryption (always possible) = encryption using round keys in reverse order

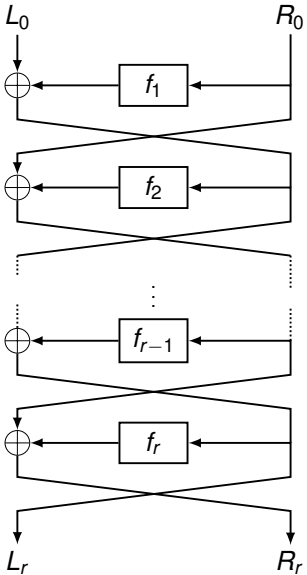
Feistel Ciphers



DES block cipher (Horst Feistel (IBM) + NSA)

- Decryption (always possible) = encryption using round keys in reverse order
- f's do not need to be invertible
  $\rightarrow$ more flexibility in chosen f

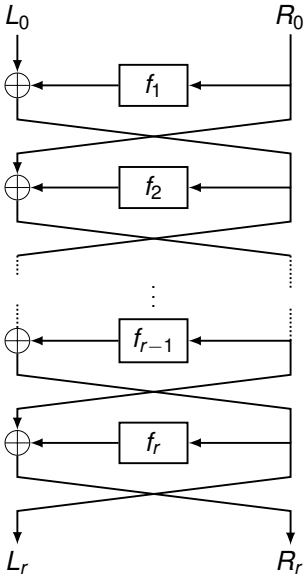
Feistel Ciphers



DES block cipher (Horst Feistel (IBM) + NSA)

- Decryption (always possible) = encryption using round keys in reverse order
- f's do not need to be invertible
  $\rightarrow$ more flexibility in chosen f
- Not entire input is updated each round

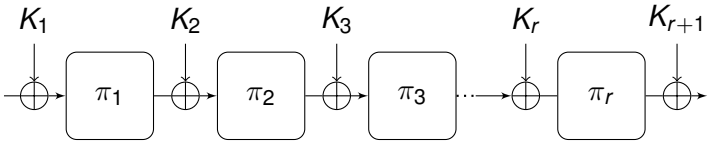
Feistel Ciphers



DES block cipher (Horst Feistel (IBM) + NSA)

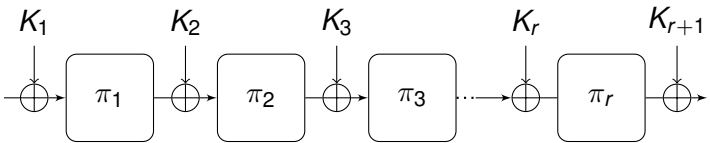
- Decryption (always possible) = encryption using round keys in reverse order
- f's do not need to be invertible
  $\rightarrow$ more flexibility in chosen f
- Not entire input is updated each round
- Luby and Rackoff (1985): generic security

Key-Alternating Cipher



AES block cipher (Daemen and Rijmen)

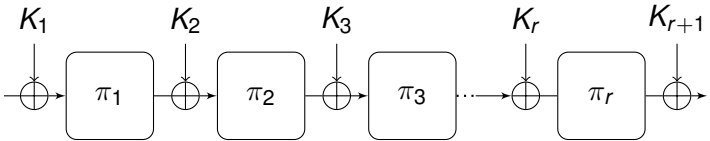
Key-Alternating Cipher



AES block cipher (Daemen and Rijmen)

- Inspired by Shannon's idea

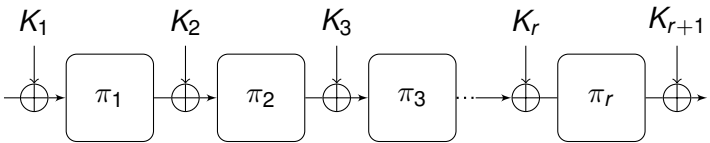
Key-Alternating Cipher



AES block cipher (Daemen and Rijmen)

- Inspired by Shannon's idea
- Require less rounds than Feistel

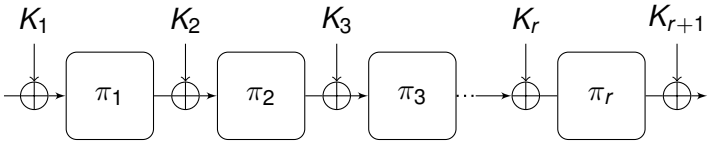
Key-Alternating Cipher



AES block cipher (Daemen and Rijmen)

- Inspired by Shannon's idea
- Require less rounds than Feistel
- Faster diffusion: update entire input string every round

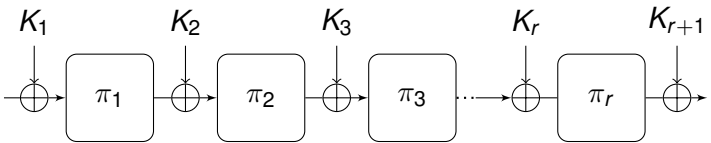
Key-Alternating Cipher



AES block cipher (Daemen and Rijmen)

- Inspired by Shannon's idea
- Require less rounds than Feistel
- Faster diffusion: update entire input string every round
- No self-inverse property

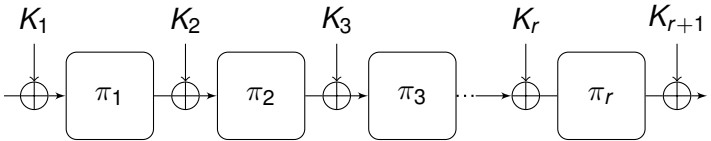
Key-Alternating Cipher



AES block cipher (Daemen and Rijmen)

- Inspired by Shannon's idea
- Require less rounds than Feistel
- Faster diffusion: update entire input string every round
- No self-inverse property
- Even and Mansour (1991): generic security of single round KAC

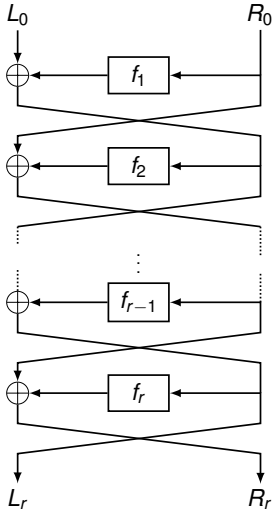
Key-Alternating Cipher

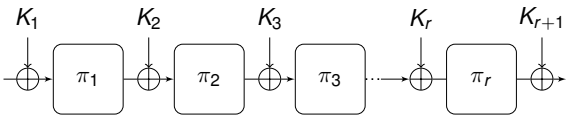


AES block cipher (Daemen and Rijmen)

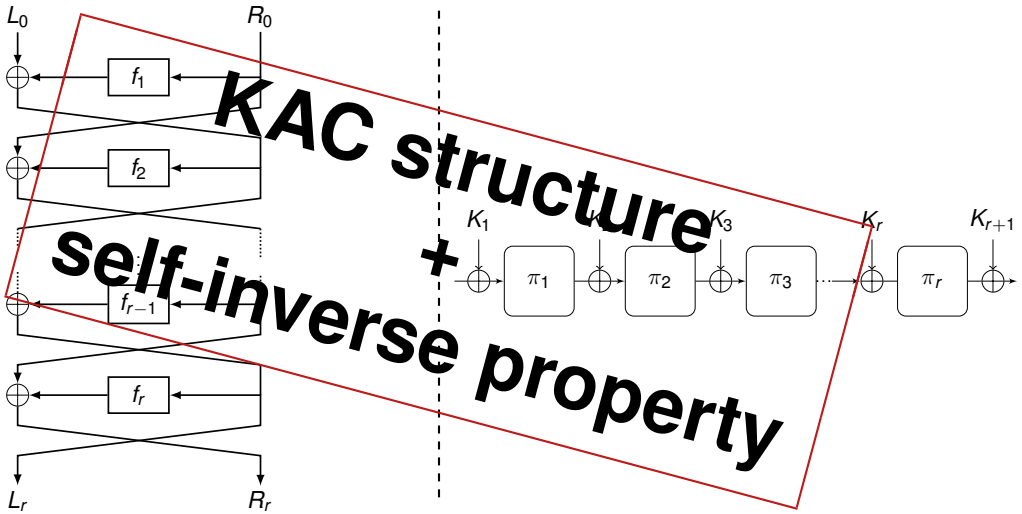
- Inspired by Shannon's idea
- Require less rounds than Feistel
- Faster diffusion: update entire input string every round
- No self-inverse property
- Even and Mansour (1991): generic security of single round KAC
- Bogdanov et al. (2012): generic security of multiple round KAC

Combine the Two Ideas

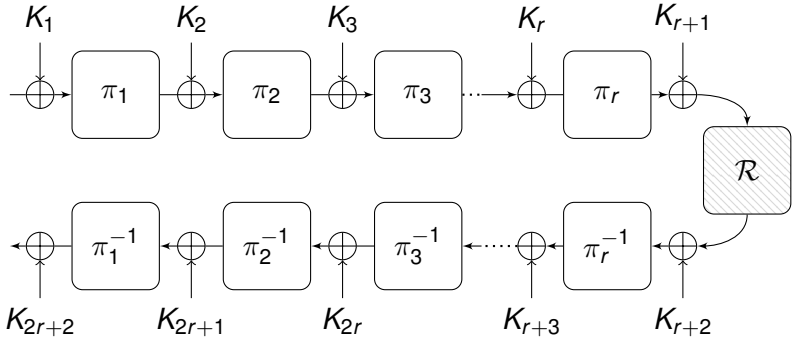




Combine the Two Ideas

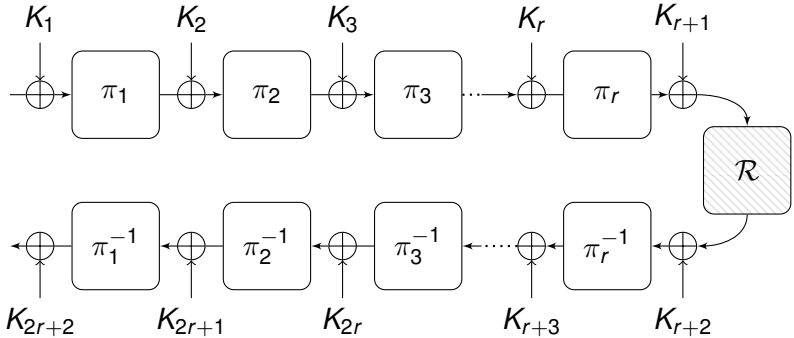


Reflection Ciphers



PRINCE block cipher (Borghoff et al. 2012)

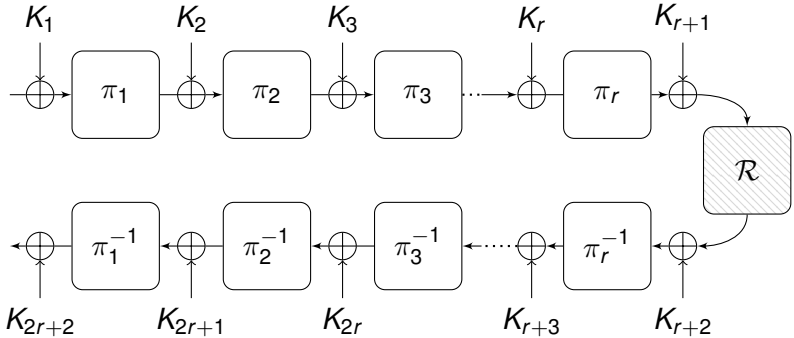
Reflection Ciphers



PRINCE block cipher (Borghoff et al. 2012)

- Key-alternating reflection cipher: reflector $\mathcal{R}$ is an involution

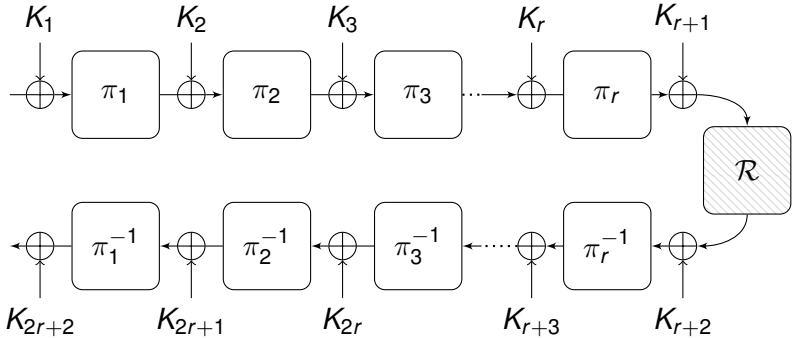
Reflection Ciphers



PRINCE block cipher (Borghoff et al. 2012)

- Key-alternating reflection cipher: reflector $\mathcal{R}$ is an involution
- Reflection property: decryption = encryption using related key

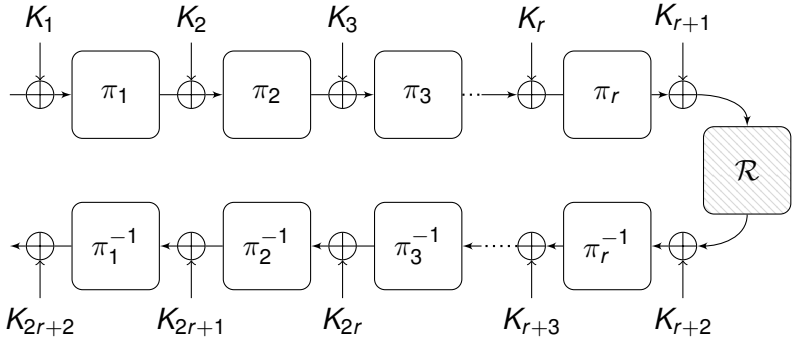
Reflection Ciphers



PRINCE block cipher (Borghoff et al. 2012)

- Key-alternating reflection cipher: reflector $\mathcal{R}$ is an involution
- Reflection property: decryption = encryption using related key
- Low-latency low-area use-case

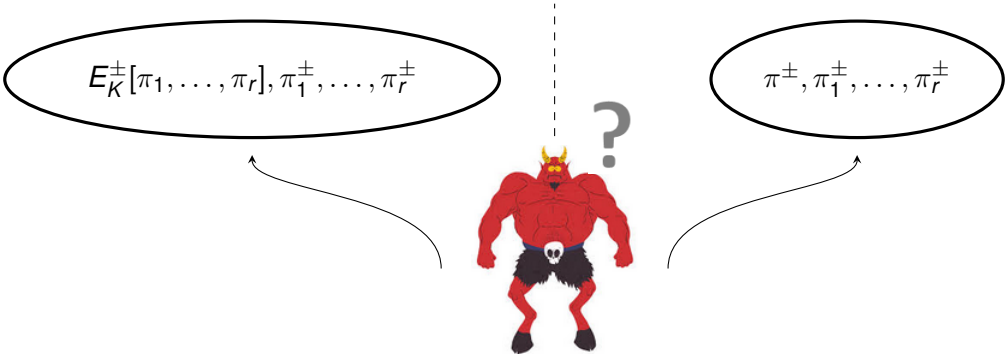
Reflection Ciphers



PRINCE block cipher (Borghoff et al. 2012)

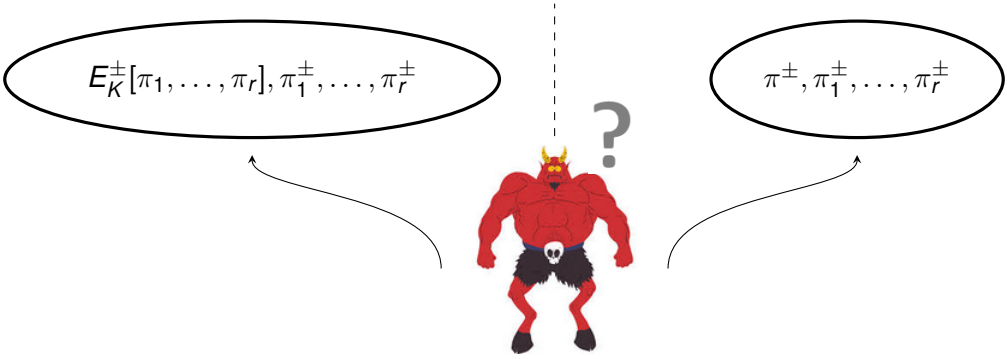
- Key-alternating reflection cipher: reflector $\mathcal{R}$ is an involution
- Reflection property: decryption = encryption using related key
- Low-latency low-area use-case
- Study of generic security is missing

Generic Security of Block Ciphers



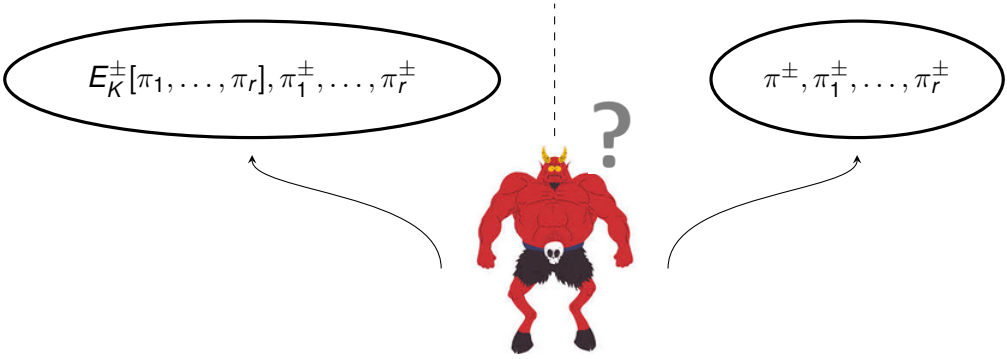
- Attacker $\mathcal{A}$ makes q queries to construction oracle $E_K^{\pm}$ or $\pi^{\pm}$

Generic Security of Block Ciphers



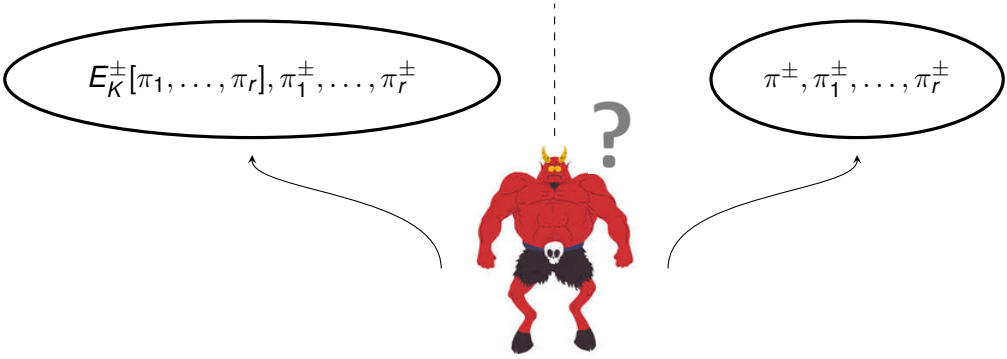
- Attacker $\mathcal{A}$ makes q queries to construction oracle $E_K^{\pm}$ or $\pi^{\pm}$
- Attacker $\mathcal{A}$ makes p queries to each of the primitive oracles $\pi_1^{\pm}, \ldots, \pi_r^{\pm}$

Generic Security of Block Ciphers



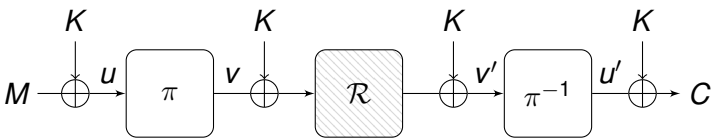
- Attacker $\mathcal{A}$ makes q queries to construction oracle $E_K^{\pm}$ or $\pi^{\pm}$
- Attacker $\mathcal{A}$ makes p queries to each of the primitive oracles $\pi_1^{\pm}, \ldots, \pi_r^{\pm}$
- Security $\rightarrow$ the probability of distinguishing two worlds: $\mathbf{Adv}_E^{\text{sprp}}(\mathcal{A}) = \text{func(q,p)}$

Generic Security of Block Ciphers



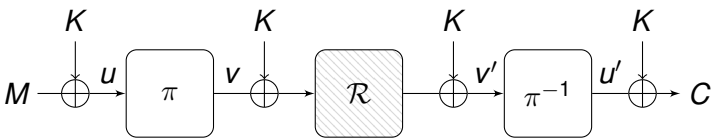
- Attacker $\mathcal{A}$ makes q queries to construction oracle $E_K^{\pm}$ or $\pi^{\pm}$
- Attacker $\mathcal{A}$ makes p queries to each of the primitive oracles $\pi_1^{\pm}, \ldots, \pi_r^{\pm}$
- Security $\rightarrow$ the probability of distinguishing two worlds: $\mathbf{Adv}_E^{\text{sprp}}(\mathcal{A}) = \text{func(q,p)}$
- E_K is secure $\iff$ $\mathbf{Adv}_E^{\text{sprp}}(\mathcal{A})$ is negligible

2-round Key-Alternating Reflection Cipher (Trivial Key Schedule 1)



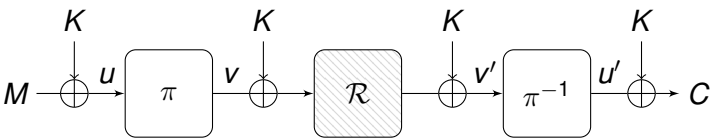
- Is obviously insecure when $\mathcal{R}$ is linear

2-round Key-Alternating Reflection Cipher (Trivial Key Schedule 1)



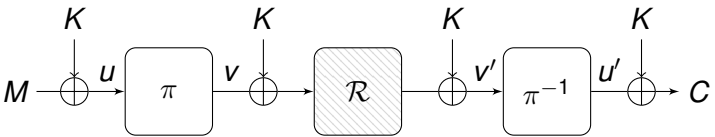
- Is obviously insecure when $\mathcal{R}$ is linear
- Choose a message M to obtain C

2-round Key-Alternating Reflection Cipher (Trivial Key Schedule 1)



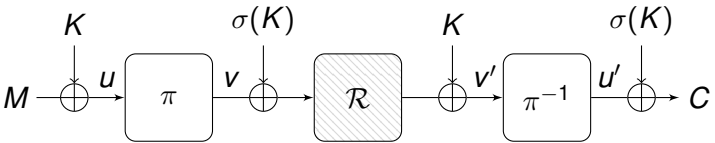
- Is obviously insecure when $\mathcal{R}$ is linear
- Choose a message M to obtain C
- Choose another message $M' = C$ to obtain C'

2-round Key-Alternating Reflection Cipher (Trivial Key Schedule 1)



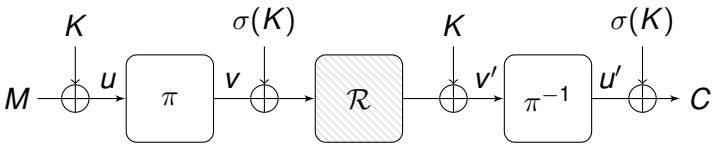
- Is obviously insecure when $\mathcal{R}$ is linear
- Choose a message M to obtain C
- Choose another message $M' = C$ to obtain C'
- If $C' = M$, then we are in the real word

2-round Key-Alternating Reflection Cipher (Trivial Key Schedule 2)



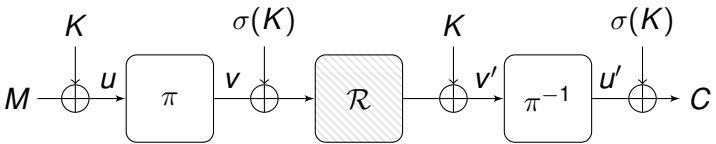
- Linear involution σ

2-round Key-Alternating Reflection Cipher (Trivial Key Schedule 2)



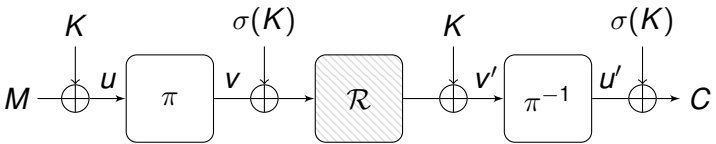
- Linear involution σ
- Is not even secure up to $q^2/2^n$ when σ is linear

2-round Key-Alternating Reflection Cipher (Trivial Key Schedule 2)



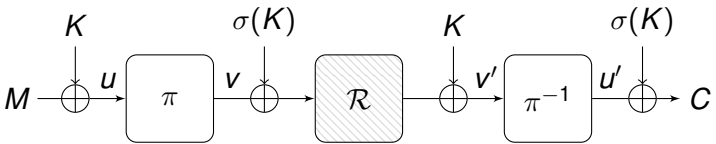
- Linear involution σ
- Is not even secure up to $q^2/2^n$ when σ is linear
- Reason: $K \oplus \sigma(K)$ is not uniform random $\rightarrow$ mirror slide attack

2-round Key-Alternating Reflection Cipher (Trivial Key Schedule 2)



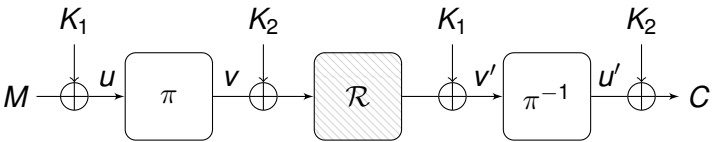
- Linear involution σ
- Is not even secure up to $q^2/2^n$ when σ is linear
- Reason: $K \oplus \sigma(K)$ is not uniform random $\rightarrow$ mirror slide attack
- We focus on constructions with two independent keys

2-round Key-Alternating Reflection Cipher (Trivial Key Schedule 2)



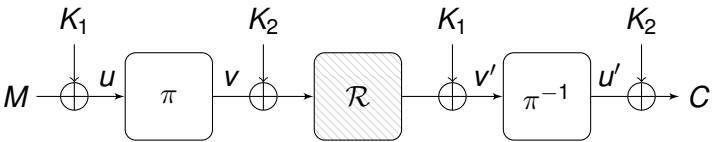
- Linear involution σ
- Is not even secure up to $q^2/2^n$ when σ is linear
- Reason: $K \oplus \sigma(K)$ is not uniform random $\rightarrow$ mirror slide attack
- We focus on constructions with two independent keys
- One key case necessarily requires either a special choice of $\mathcal{R}$ or a nonlinear σ

Security of 2-round Key-Alternating Reflection Cipher



$$\mathbf{Adv}^{\mathrm{sprp}} \leq qp^2/2^{2n} + q^2/2^n$$

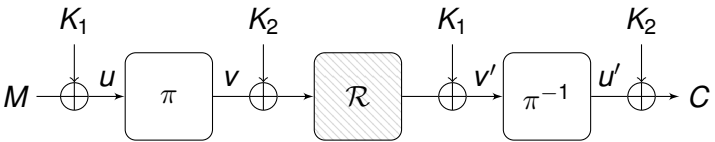
Security of 2-round Key-Alternating Reflection Cipher



$$\mathbf{Adv}^{\mathrm{sprp}} \leq qp^2/2^{2n} + q^2/2^n$$

- Linear reflector $\mathcal{R}$

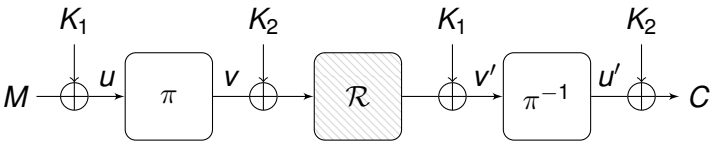
Security of 2-round Key-Alternating Reflection Cipher



$$\mathbf{Adv}^{\mathrm{sprp}} \leq qp^2/2^{2n} + q^2/2^n$$

- Linear reflector $\mathcal{R}$
- Two alternating round keys K_1 and K_2

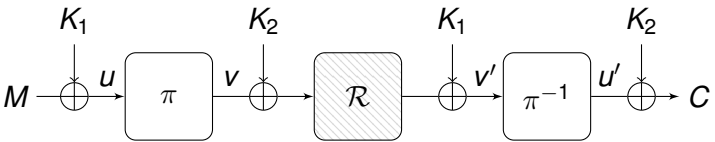
Security of 2-round Key-Alternating Reflection Cipher



$$\mathbf{Adv}^{\mathrm{sprp}} \leq qp^2/2^{2n} + q^2/2^n$$

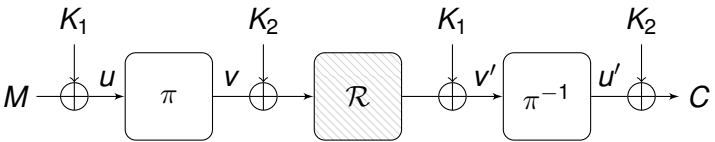
- Linear reflector $\mathcal{R}$
- Two alternating round keys K_1 and K_2
- Decryption = encryption uses swapping keys K_1 and K_2

Information-theoretic attack for $qp^2/2^{2n}$



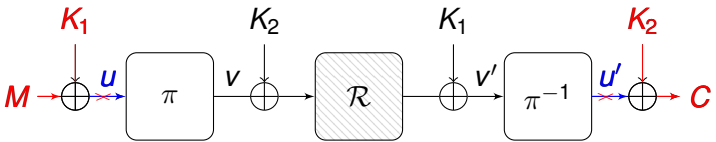
- $2q$ construction queries and p primitive queries such that $p^2q = 2^{2n}$

Information-theoretic attack for $qp^2/2^{2n}$



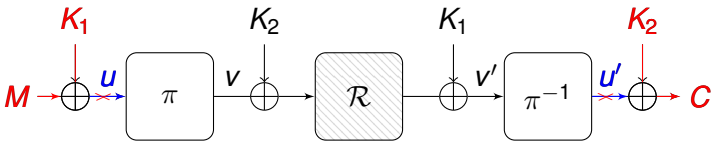
- $2q$ construction queries and p primitive queries such that $p^2q = 2^{2n}$
- For each possible pair K_1 and K_2

Information-theoretic attack for $qp^2/2^{2n}$



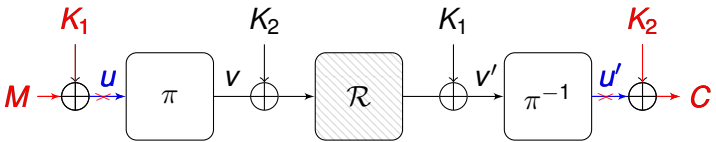
- $2q$ construction queries and p primitive queries such that $p^2q = 2^{2n}$
- For each possible pair K_1 and K_2
- Find a pair primitive queries such that $M \oplus K_1 = u$ and $C \oplus K_2 = u'$

Information-theoretic attack for $qp^2/2^{2n}$



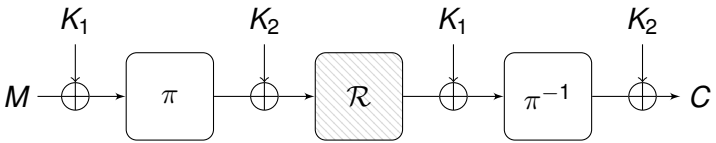
- $2q$ construction queries and p primitive queries such that $p^2q = 2^{2n}$
- For each possible pair K_1 and K_2
- Find a pair primitive queries such that $M \oplus K_1 = u$ and $C \oplus K_2 = u'$
- For each pair, check if $\mathcal{R}(v) \oplus v' = K_1 \oplus \mathcal{R}(K_2)$

Information-theoretic attack for $qp^2/2^{2n}$



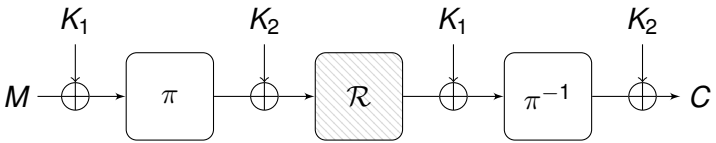
- $2q$ construction queries and p primitive queries such that $p^2q = 2^{2n}$
- For each possible pair K_1 and K_2
- Find a pair primitive queries such that $M \oplus K_1 = u$ and $C \oplus K_2 = u'$
- For each pair, check if $\mathcal{R}(v) \oplus v' = K_1 \oplus \mathcal{R}(K_2)$
- Attack uses $O(2^{2n})$ table lookups $\rightarrow$ impractical

Practical attack for $q^2/2^n$



Mirror slide attack of Dunkelman, Keller and Shamir (EC 2012)

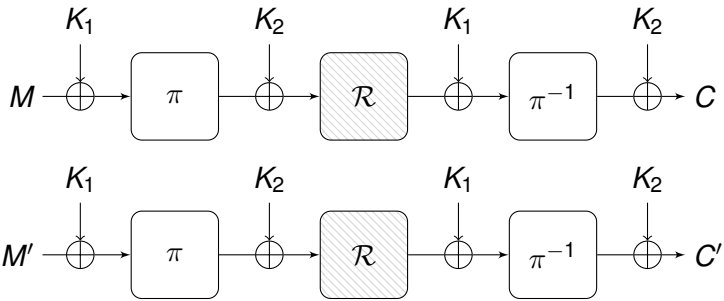
Practical attack for $q^2/2^n$



Mirror slide attack of Dunkelman, Keller and Shamir (EC 2012)

- $\mathcal{R}$ has many fixed points

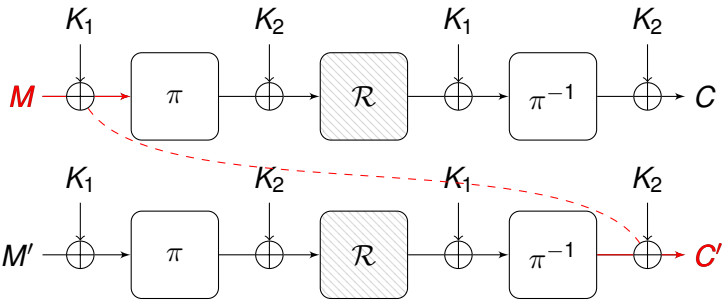
Practical attack for $q^2/2^n$



Mirror slide attack of Dunkelman, Keller and Shamir (EC 2012)

- $\mathcal{R}$ has many fixed points
- Choose $\Theta(2^{n/2})$ distinct values $M_1, M_2, \ldots$ and $C'_1, C'_2, \ldots$

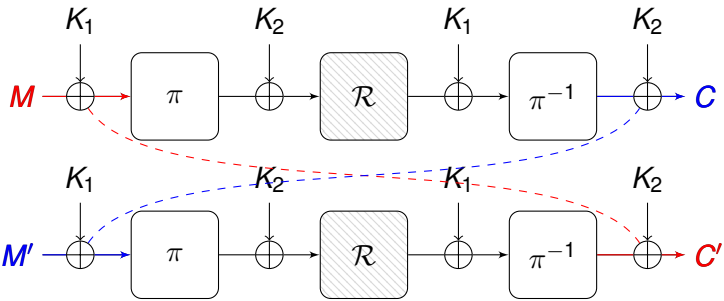
Practical attack for $q^2/2^n$



Mirror slide attack of Dunkelman, Keller and Shamir (EC 2012)

- $\mathcal{R}$ has many fixed points
- Choose $\Theta(2^{n/2})$ distinct values $M_1, M_2, \ldots$ and $C'_1, C'_2, \ldots$
- Find a pair of construction queries such that $M \oplus C' = K_1 \oplus K_2$

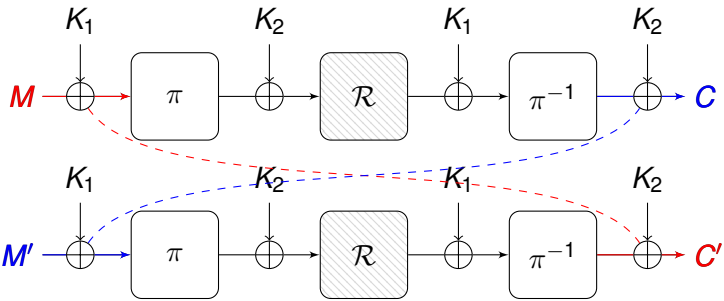
Practical attack for $q^2/2^n$



Mirror slide attack of Dunkelman, Keller and Shamir (EC 2012)

- $\mathcal{R}$ has many fixed points
- Choose $\Theta(2^{n/2})$ distinct values $M_1, M_2, \ldots$ and $C'_1, C'_2, \ldots$
- Find a pair of construction queries such that $M \oplus C' = K_1 \oplus K_2 = M' \oplus C$

Practical attack for $q^2/2^n$



Mirror slide attack of Dunkelman, Keller and Shamir (EC 2012)

- $\mathcal{R}$ has many fixed points
- Choose $\Theta(2^{n/2})$ distinct values $M_1, M_2, \ldots$ and $C'_1, C'_2, \ldots$
- Find a pair of construction queries such that $M \oplus C' = K_1 \oplus K_2 = M' \oplus C$
- Recovers the value of $K_1 \oplus K_2$

Security Analysis

- Patarin's H-coefficient technique

$$\frac{\Pr(X_{\mathcal{O}} = \tau)}{\Pr(X_{\mathcal{P}} = \tau)} \geq 1 - \epsilon$$

$$\mathbf{Adv}(\mathcal{A}) \leq \epsilon + \Pr(X_{\mathcal{P}} \in \mathcal{T}_{\text{bad}})$$

Security Analysis

- Patarin's H-coefficient technique

$$\frac{\Pr(X_{\mathcal{O}} = \tau)}{\Pr(X_{\mathcal{P}} = \tau)} \geq 1 - \epsilon$$

$$\mathbf{Adv}(\mathcal{A}) \leq \epsilon + \Pr(X_{\mathcal{P}} \in \mathcal{T}_{\text{bad}})$$

- Obtain ϵ using ideas of the first iteration of Patarin's mirror theory

Security Analysis

- Patarin's H-coefficient technique

$$\frac{\Pr(X_{\mathcal{O}} = \tau)}{\Pr(X_{\mathcal{P}} = \tau)} \geq 1 - \epsilon$$

$$\mathbf{Adv}(\mathcal{A}) \leq \epsilon + \Pr(X_{\mathcal{P}} \in \mathcal{T}_{\text{bad}})$$

- Obtain ϵ using ideas of the first iteration of Patarin's mirror theory
- Ideal permutation model $\rightarrow \mathcal{A}$ has access to π

Security Analysis

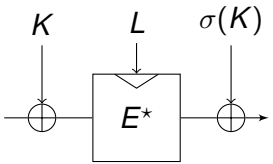
- Patarin's H-coefficient technique

$$\frac{\Pr(X_{\mathcal{O}} = \tau)}{\Pr(X_{\mathcal{P}} = \tau)} \geq 1 - \epsilon$$

$$\mathbf{Adv}(\mathcal{A}) \leq \epsilon + \Pr(X_{\mathcal{P}} \in \mathcal{T}_{\text{bad}})$$

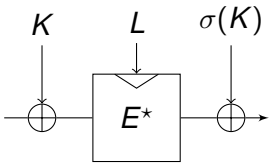
- Obtain ϵ using ideas of the first iteration of Patarin's mirror theory
- Ideal permutation model $\rightarrow \mathcal{A}$ has access to π
- Single permutation case $\rightarrow$ domain separation needed
- Domain separation is covered by a bad event $\rightarrow$ leads to $q^2/2^n$ term

Key-Length Extension



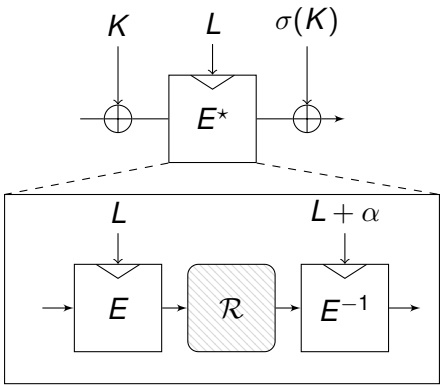
- PRINCE and MANTIS use FX structure to extend the key-length from 64 to 128 bits

Key-Length Extension



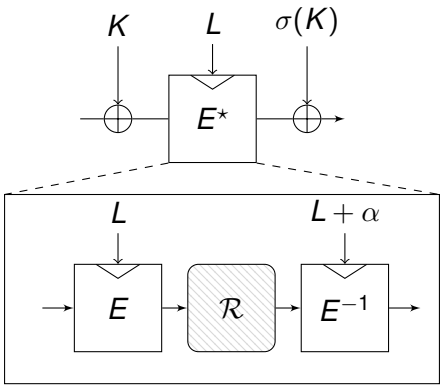
- PRINCE and MANTIS use FX structure to extend the key-length from 64 to 128 bits
- $E^{\star}$ is an ideal reflection cipher

Key-Length Extension



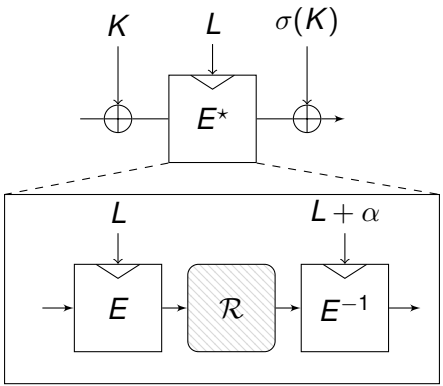
- PRINCE and MANTIS use FX structure to extend the key-length from 64 to 128 bits
- $E^{\star}$ is an ideal reflection cipher

Key-Length Extension



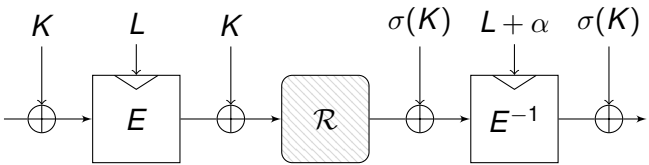
- PRINCE and MANTIS use FX structure to extend the key-length from 64 to 128 bits
- $E^\star$ is an ideal reflection cipher
- Security of PRINCE key-length extender with $\mathbf{Adv}^{\text{sprp}} \leq pq/2^{128}$

Key-Length Extension



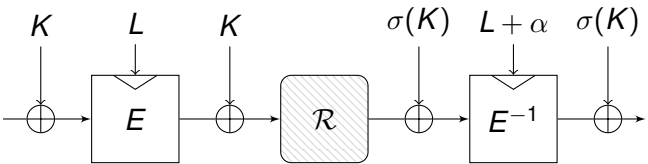
- PRINCE and MANTIS use FX structure to extend the key-length from 64 to 128 bits
- $E^\star$ is an ideal reflection cipher
- Security of PRINCE key-length extender with $\mathbf{Adv}^{\text{sprp}} \leq pq/2^{128}$
- PRINCE v2: alternating round keys + modify the reflector

Our New Key-Length Extender



$$\mathbf{Adv}^{\mathrm{sprp}} \leq p\sqrt{q}/2^{2n}$$

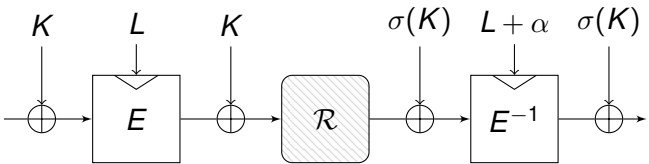
Our New Key-Length Extender



$$\mathbf{Adv}^{\mathrm{sprp}} \leq p\sqrt{q}/2^{2n}$$

- E is an ideal cipher

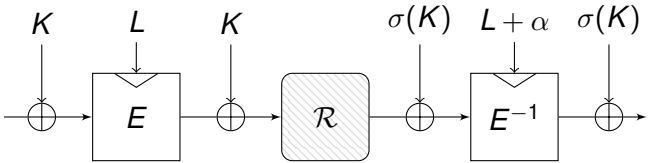
Our New Key-Length Extender



$$\mathbf{Adv}^{\mathrm{sprp}} \leq p\sqrt{q}/2^{2n}$$

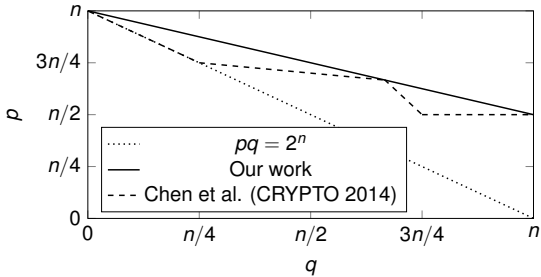
- E is an ideal cipher
- Based on security of 2-round KAC

Our New Key-Length Extender

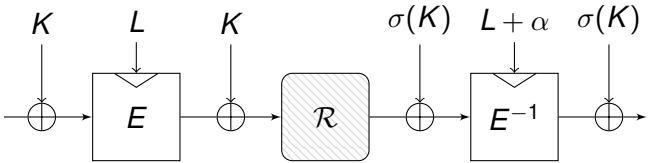


$$\mathbf{Adv}^{\mathrm{sprp}} \leq p\sqrt{q}/2^{2n}$$

- E is an ideal cipher
- Based on security of 2-round KAC
- We improved the security bound of 2-round KAC (improved sum-capture lemma using a variant of Hoeffding's inequality)

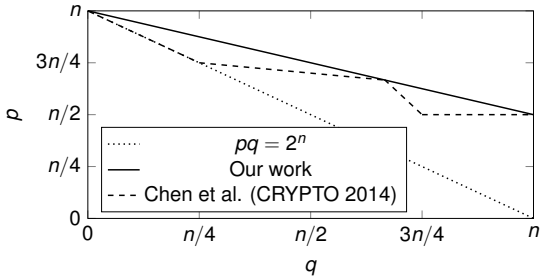


Our New Key-Length Extender



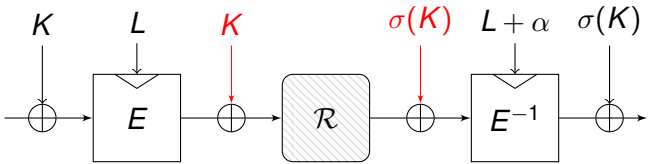
$$\mathbf{Adv}^{\mathrm{sprp}} \leq p\sqrt{q}/2^{2n}$$

- E is an ideal cipher
- Based on security of 2-round KAC
- We improved the security bound of 2-round KAC (improved sum-capture lemma using a variant of Hoeffding's inequality)
- Concrete cryptanalysis is needed



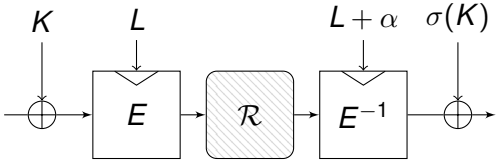
Our New Key-Length Extender: Comparison With FX

Our Construction



$\mathbf{Adv}^{\mathrm{sprp}} \leq p^2 q / 2^{256}$

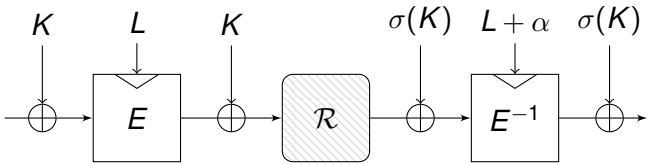
FX



$\mathbf{Adv}^{\mathrm{sprp}} \leq pq / 2^{128}$

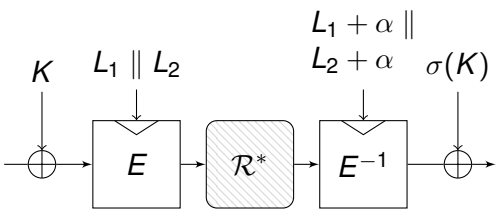
Our New Key-Length Extender: Comparison With PRINCE v2

Our Construction



Minimalist change from PRINCE

PRINCE v2



Two alt keys + $\mathcal{R}^*$ does not preserve refl. property

Conclusion

New results

- First generic treatment of reflection ciphers
- Provable secure results of 2-round key-alternating reflection cipher
- New key-length extender with better security

Conclusion

New results

- First generic treatment of reflection ciphers
- Provable secure results of 2-round key-alternating reflection cipher
- New key-length extender with better security

Future research

- Single key case?
- Better choice of the reflector to avoid the $q^2/2^n$ term?
- Tight security for $2r$-round key-alternating reflection cipher?
- Key-alternating tweakable reflection ciphers?

Conclusion

New results

- First generic treatment of reflection ciphers
- Provable secure results of 2-round key-alternating reflection cipher
- New key-length extender with better security

Future research

- Single key case?
- Better choice of the reflector to avoid the $q^2/2^n$ term?
- Tight security for $2r$-round key-alternating reflection cipher?
- Key-alternating tweakable reflection ciphers?

I am looking for a new job position $\rightarrow$ yulongchen92@gmail.com