Beyond Birthday Bound Secure Fresh Rekeying: Application to Authenticated Encryption

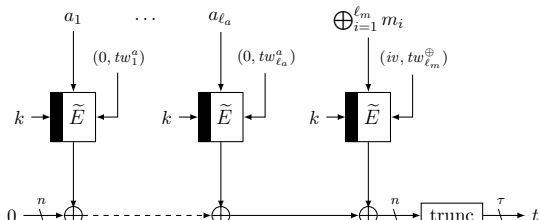
Bart Mennink

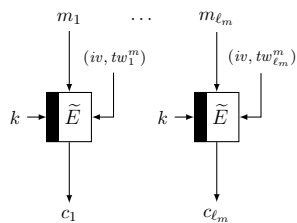
Radboud University (The Netherlands)

ASIACRYPT 2020
December 7–11, 2020

Introduction

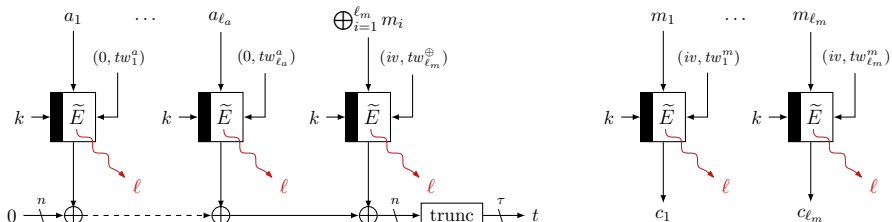
- Block cipher based constructions invoke the secret key many times
- Typical examples:
  - CTR and CBC encryption
  - OCBx, and its generalization ΘCB [KR11] (depicted for integral data)





Introduction

- Block cipher based constructions invoke the secret key many times
- Typical examples:
  - CTR and CBC encryption
  - OCBx, and its generalization ΘCB [KR11] (depicted for integral data)



Repeated evaluation of the key ⟶ repeated leakage of the key

Countermeasures Against Leakage

Implementation Protection

- Protection on top
- Masking or hiding

Countermeasures Against Leakage

Implementation Protection

- Protection on top
- Masking or hiding

Leakage Resilience

- Protection by design
- Sometimes less efficient

Countermeasures Against Leakage

Implementation Protection

- Protection on top
- Masking or hiding

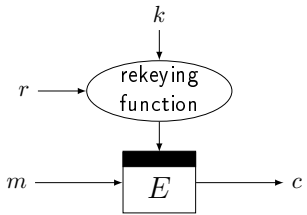
Rekeying

- Method-in-the-middle
- Leveled implementation

Leakage Resilience

- Protection by design
- Sometimes less efficient

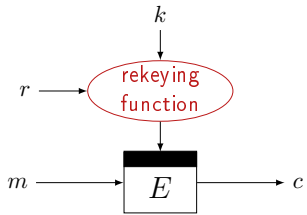
Fresh Parallel Rekeying



Idea

- Make scarce use of key material
- Strong protection only needed for cryptographically light building blocks

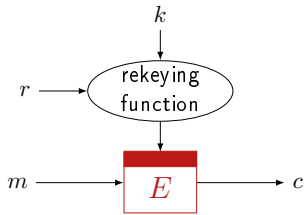
Fresh Parallel Rekeying



Idea

- Make scarce use of key material
- Strong protection only needed for cryptographically light building blocks
- Rekeying: strong protection (e.g., against DPA), but not necessarily cryptographically strong

Fresh Parallel Rekeying

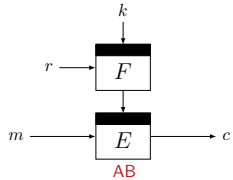


Idea

- Make scarce use of key material
- Strong protection only needed for cryptographically light building blocks
- Rekeying: strong protection (e.g., against DPA), but not necessarily cryptographically strong
- Core: must be cryptographically strong, but only needs lighter protection (e.g., against SPA)

Rekeying

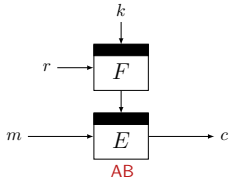
2000 — AB — Abdalla and Bellare
formalized idea of rekeying

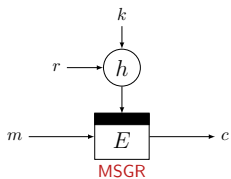


Rekeying

2000 — AB — Abdalla and Bellare
formalized idea of rekeying

2010 — MSGR — Medwed et al.
minimalized subkeying



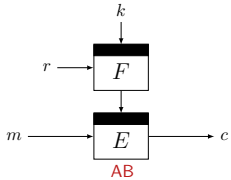


Rekeying

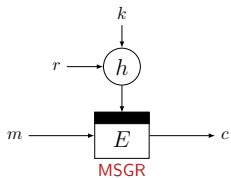
2000 — AB — Abdalla and Bellare
formalized idea of rekeying

2010 — MSGR — Medwed et al.
minimalized subkeying

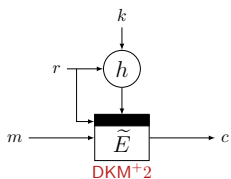
2014 — DKM$^+$1/DKM$^+$2 — Dobraunig et al.
attack and 2 remedies for MSGR



AB



MSGR



DKM$^+$2

Rekeying Versus Tweakable Block Ciphers

- The idea of rekeying reminds a bit of tweakable block ciphers
- Only difference, tweak change implies key change

Rekeying Versus Tweakable Block Ciphers

- The idea of rekeying reminds a bit of tweakable block ciphers
- Only difference, tweak change implies key change
- Known as tweak-rekeyable tweakable block ciphers

Rekeying

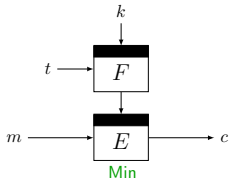
2000 — AB — Abdalla and Bellare
formalized idea of rekeying

2010 — MSGR — Medwed et al.
minimalized subkeying

2014 — DKM$^+$1/DKM$^+$2 — Dobaunig et al.
attack and 2 remedies for MSGR

Tweak-Rekeyable TBC

2009 — Minematsu — Min
first tweak-rekeyable TBC



Rekeying

2000 — AB — Abdalla and Bellare
formalized idea of rekeying

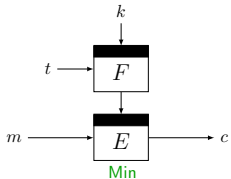
2010 — MSGR — Medwed et al.
minimalized subkeying

2014 — DKM$^+$1/DKM$^+$2 — Dobaunig et al.
attack and 2 remedies for MSGR

Tweak-Rekeyable TBC

Minematsu — Min — **2009**
first tweak-rekeyable TBC

Mennink — Men1/Men2 — **2015**
beyond birthday bound security



Rekeying

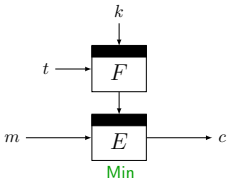
2000 — AB — Abdalla and Bellare
formalized idea of rekeying

2010 — MSGR — Medwed et al.
minimalized subkeying

2014 — DKM$^+$1/DKM$^+$2 — Dobaunig et al.
attack and 2 remedies for MSGR

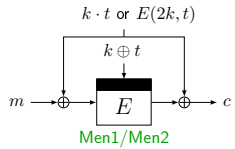
Tweak-Rekeyable TBC

2009 — Minematsu — Min
first tweak-rekeyable TBC



Min

2015 — Mennink — Men1/Men2
beyond birthday bound security

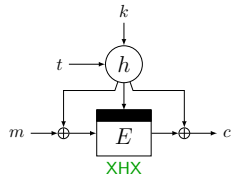


Men1/Men2

2016 — Wang et al. — WGZ^+i
generalization of Men$i$: 32 schemes

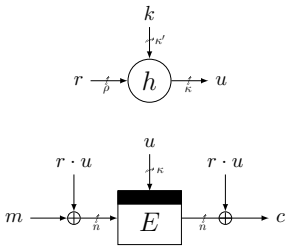
2017 — Naito — XKX
targeting AE

2017 — Jha et al. — XHX
generalized construction



XHX

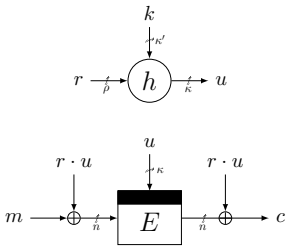
Beyond Birthday Bound Secure Fresh Rekeying



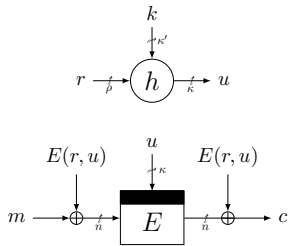
R1

- Derivative of Men1
- $\kappa = \rho = n$
- $\approx 2n/3$-bit security

Beyond Birthday Bound Secure Fresh Rekeying



R1

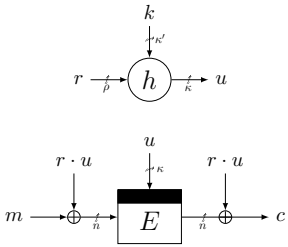


R2

- Derivative of Men1
- $\kappa = \rho = n$
- $\approx 2n/3$-bit security

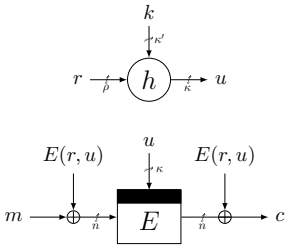
- Inspired by WGZ+12
- $\kappa = \rho = n$
- $\approx n$-bit security

Beyond Birthday Bound Secure Fresh Rekeying



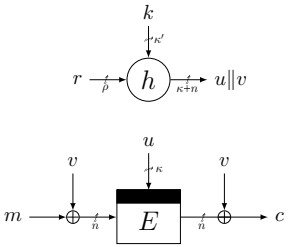
R1

- Derivative of Men1
- $\kappa = \rho = n$
- $\approx 2n/3$-bit security



R2

- Inspired by WGZ$^+$12
- $\kappa = \rho = n$
- $\approx n$-bit security



R3

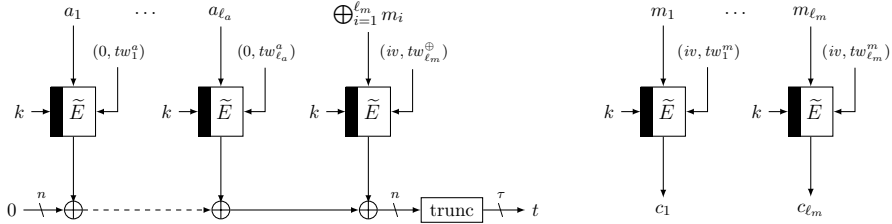
- Adaptation of XHX
- $\approx (\kappa + n)/2$-bit security
- Covers p-based rekeying

Cost Comparison

- Keep $\kappa = \rho = n$ for simplicity
- F is RF, $\widetilde{E}$ is TBC, E is BC
- For sake of counting: consider n-bit finite field multiplication for h

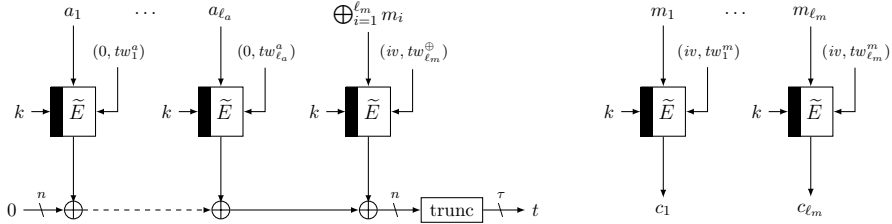
	subkey		core				
scheme	F	$\otimes/h$	$\widetilde{E}$	E	$\otimes$	keysize	security
AB (2000)	1	0	0	1	0	n	2^n (as PRF)
MSGR (2010)	0	1	0	1	0	n	$2^{n/2}$
DKM$^+$1 (2014)	0	1	0	2	0	n	$2^{n/2}$
DKM$^+$2 (2014)	0	1	1	0	0	n	2^n
R1	**0**	**1**	**0**	**1**	**1**	$\boldsymbol{n}$	$\boldsymbol{2^{2n/3}}$
R2	**0**	**1**	**0**	**2**	**0**	$\boldsymbol{n}$	$\boldsymbol{2^n}$
R3	**0**	**2**	**0**	**1**	**0**	$\boldsymbol{2n}$	$\boldsymbol{2^n}$

Application to Authenticated Encryption



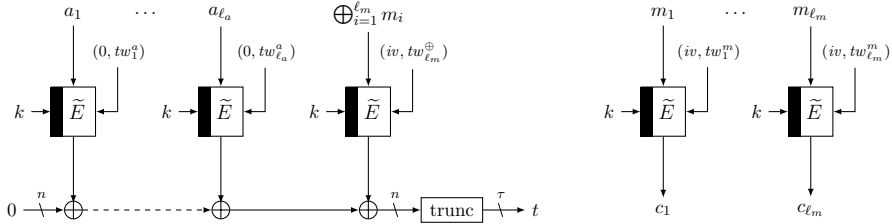
- TBCs are a popular primitive for mode design
- Typical example: ΘCB [KR11]

Application to Authenticated Encryption



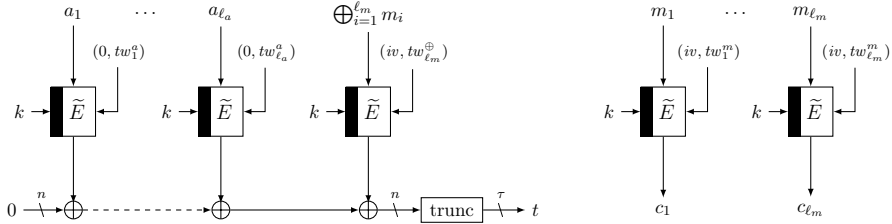
- TBCs are a popular primitive for mode design
- Typical example: ΘCB [KR11]
  - OCB3 [KR11] ≡ ΘCB instantiated with XEX construction

Application to Authenticated Encryption



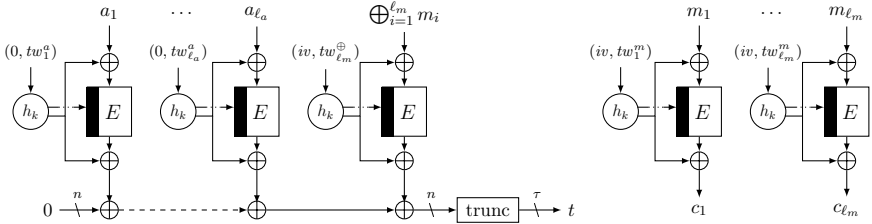
- TBCs are a popular primitive for mode design
- Typical example: ΘCB [KR11]
  - OCB3 [KR11] $\equiv$ ΘCB instantiated with XEX construction
  - Deoxys-I [JNPS16] $\equiv$ ΘCB instantiated with Deoxys-BC design

Application to Authenticated Encryption



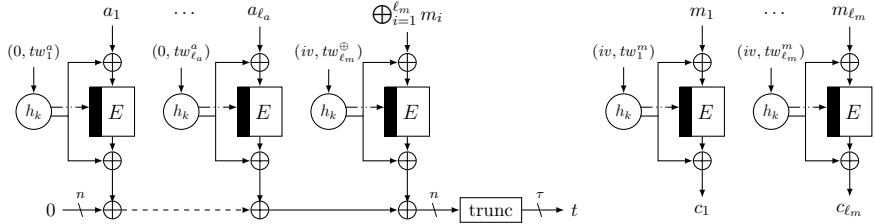
- TBCs are a popular primitive for mode design
- Typical example: ΘCB [KR11]
  - OCB3 [KR11] $\equiv$ ΘCB instantiated with XEX construction
  - Deoxys-I [JNPS16] $\equiv$ ΘCB instantiated with Deoxys-BC design
  - One can just as well instantiate it with a rekeying scheme

Application to Authenticated Encryption: ΘCB-R3



- Instantiation of ΘCB with R3

Application to Authenticated Encryption: ΘCB-R3



- Instantiation of ΘCB with R3
- Features:
  - n-bit security (in ideal model)
  - $\ell_a + \ell_m + 1$ lightly protected E calls
  - $2(\ell_a + \ell_m + 1)$ strongly protected h calls
  - By design easier to protect against side-channel attacks

Application to Authenticated Encryption: Comparison

ΘCB-R3

- n-bit security (in ideal model)
- $\ell_a + \ell_m + 1$ lightly protected E calls
- $2(\ell_a + \ell_m + 1)$ strongly protected h calls

Application to Authenticated Encryption: Comparison

ΘCB-R3

- n-bit security (in ideal model)
- $\ell_a + \ell_m + 1$ lightly protected E calls
- $2(\ell_a + \ell_m + 1)$ strongly protected h calls

Comparison to OCB3 [KR11]

- $n/2$-bit security (but in standard model)
- $\ell_a + \ell_m + 2$ strongly protected E calls

Application to Authenticated Encryption: Comparison

ΘCB-R3

- n-bit security (in ideal model)
- $\ell_a + \ell_m + 1$ lightly protected E calls
- $2(\ell_a + \ell_m + 1)$ strongly protected h calls

Comparison to OCB3 [KR11]

- $n/2$-bit security (but in standard model)
- $\ell_a + \ell_m + 2$ strongly protected E calls

Comparison to DTE [BKP+17]

- Different goal: nonce-misuse resistance
- $\ell_a + \ell_m + 1$ unprotected E calls (approx., for hashing)
- $2\ell_m$ lightly protected E calls
- 2 strongly protected E calls

Conclusion

Fresh Rekeying Versus Tweak-Rekeyable TBCs

- Two disjoint directions considered same problem
- New fresh rekeying solutions for easier side-channel protection

Conclusion

Fresh Rekeying Versus Tweak-Rekeyable TBCs

- Two disjoint directions considered same problem
- New fresh rekeying solutions for easier side-channel protection

Strength of Subkey Generation Function

- Multiplication is not strong enough [BFG14,BCF+15,GJ16,PM16]
- Rekeying approach of ISAP [DEM+17] appears solid!

Conclusion

Fresh Rekeying Versus Tweak-Rekeyable TBCs

- Two disjoint directions considered same problem
- New fresh rekeying solutions for easier side-channel protection

Strength of Subkey Generation Function

- Multiplication is not strong enough [BFG14,BCF+15,GJ16,PM16]
- Rekeying approach of ISAP [DEM+17] appears solid!

Thank you for your attention!