Short Non-Malleable Codes from Related-Key Secure Block Ciphers

Serge Fehr[✧] **Pierre Karpman**[a] Bart Mennink[b]

[✧]CWI, The Netherlands
[a]Université Grenoble Alpes, France
[b]Digital Security Group, Radboud University and CWI, The Netherlands

FSE — Brugge
2018–03–07

Non-Malleable codes

Our construction

Proof intuition

Non-Malleable codes

Our construction

Proof intuition

Non-Malleable Codes (simple def.)

Non-Malleable Code (informal)

An NMC is a pair $(\mathsf{Enc}, \mathsf{Dec})$ where Enc is an *unkeyed* randomized mapping and we have:

1. $\forall m,\ \mathsf{Dec}(\mathsf{Enc}(m)) = m$
2. $\forall\, \mathsf{T} \in \mathcal{T},\ \mathsf{Dec}(\mathsf{T}(\mathsf{Enc}(m_0))) \approx \mathsf{Dec}(\mathsf{T}(\mathsf{Enc}(m_1)))$

for some function space $\mathcal{T}$, for all m_0, m_1.

- Introduced by Dziembowski, Pietrzak and Wichs (2010)

Non-Malleable Codes (why?)

One original application: tamper-resilient crypto

- NMCs well-suited to protect tamper-prone memory; tamper-proof circuits
- $\Rightarrow$ Store encoded secrets, decode before using
- (Less useful in some other fault models)

And there's more, e.g.:

- Efficient non-malleable commitment schemes (Goyal et al., 2016)

Our contribution

We propose an NMC construction:

- With short codewords of size $|m| + 2\tau$ for message m & sec. τ
- Only based on a related-key secure block cipher
  - Also with graceful single-key security degradation

$\Rightarrow$ Related-key secure ciphers are useful (if we needed more evidence)

Non-Malleable Codes (feasibility)

- Restrictions on $\mathcal{T}$ necessary. Cannot include, say $(x \mapsto \mathsf{Enc}(\mathsf{Dec}(x) + 1)$

An approach for $\mathcal{T}$: *split-state tampering* only:

Split-state tampering model

$\mathsf{Enc} : \{0,1\}^{\kappa} \times \mathcal{M} \to \{0,1\}^{\ell_\mathrm{L}} \times \{0,1\}^{\ell_\mathrm{R}}$
$\mathcal{T} = \{\mathsf{T} = \mathsf{T_L} \,\|\, \mathsf{T_R} : \{0,1\}^{\ell_\mathrm{L}} \times \{0,1\}^{\ell_\mathrm{R}} \to \{0,1\}^{\ell_\mathrm{L}} \times \{0,1\}^{\ell_\mathrm{R}}\}$

- Constructions exist in this model (computational or information-theoretic)

Formalizing security (in short)

Tampering experiment

$\mathsf{Tamp}^{\mathsf{T}}(m) := \dot{\mathsf{D}}\mathsf{ec}^{\mathsf{Enc}_K(m)} \circ \mathsf{T} \circ \mathsf{Enc}_K(m)$

For $K \xleftarrow{\$} \{0,1\}^{\kappa}$

NMC advantage

$\mathbf{Adv}_{\mathsf{NMC}}(t) :=$

$$\max_{m_0, m_1} \max_{A, \mathsf{T}} \left| \Pr[A(\mathsf{Tamp}^{\mathsf{T}}(m_0)) = 1] - \Pr[A(\mathsf{Tamp}^{\mathsf{T}}(m_1)) = 1] \right|$$

for A running in time t

Non-Malleable v. Error-Correcting

- Possible to have NMCs with $\mathcal{T} \ni (x \mapsto 0)$ ("ultimate" error pattern)
- If correction is not possible, decoding must fail "catastrophically" ("all-or-nothing")

Non-Malleable codes

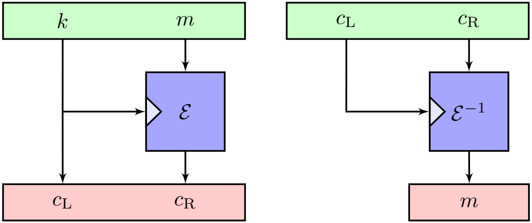
Our construction

Proof intuition

A simple construction

Let $\mathcal{E} : \{0,1\}^\kappa \times \mathcal{M} \to \mathcal{M}$ be a block cipher. Define RKNMC[$\mathcal{E}$] as:

- $\mathsf{Enc}_k := (m \mapsto k || \mathcal{E}_k(m))$
- $\mathsf{Dec} := (c_L || c_R \mapsto \mathcal{E}^{-1}_{c_L}(c_R))$



- Provides $\kappa/2$ bits of security, for "good $\mathcal{E}$" against split-state tampering

Related-work

- $m \mapsto (k, r) \| (\mathcal{E}_k(m), \mathcal{H}_z(r, k))$ (Kiayias & al., 2016)
  - Codewords of length $|m| + 9\kappa + 2\log^2(\kappa)$ or $|m| + 18\kappa$
  - Proof under **KEA**, with **CRS**
- $m \mapsto \mathsf{sk} \| (\mathsf{pk}, \mathcal{E}_{\mathsf{pk}}(m), \pi)$ (Liu and Lysyanskaya, 2012)
  - Codewords of length $|m| + \mathcal{O}(\kappa^2)$
  - Proof uses **CRS**

Related-work

Figure: KEA & CRS?

Related-work

KEA: Knowledge in the exponent assumption

- Not really standard model (not *falsifiable*, (Naor, 2003))

CRS: Common reference string

- "Trusted setup" (implementable with ceremonies?)

Non-Malleable codes

Our construction

Proof intuition

Broken instantiations

Take $\mathsf{EM}_{k_0,k_1}(m) := \mathcal{P}(m \oplus k_0) \oplus k_1$

- Secure in the ideal permutation model (Even & Mansour, 1991)
- But not *related-key* secure: $\mathsf{EM}_{k_0 \oplus \Delta, k_1}(m \oplus \Delta) = \mathsf{EM}_{k_0,k_1}(m)$
- (Or equivalently $\mathsf{EM}^{-1}_{k_0,k_1 \oplus \Delta}(c \oplus \Delta) = \mathsf{EM}^{-1}_{k_0,k_1}(c)$

So:

- Let $\mathsf{T_L} = (x, y \mapsto x, y \oplus \Delta)$; $\mathsf{T_R} = (x \mapsto x \oplus \Delta)$
- Then $\mathsf{Tamp}^{\mathsf{T}}(m) = \mathsf{EM}^{-1}_{k_0,k_1 \oplus \Delta}(\mathsf{EM}_{k_0,k_1}(m) \oplus \Delta) = m$
- $\Rightarrow$ RKNMC[EM] is trivially insecure

Broken instantiations

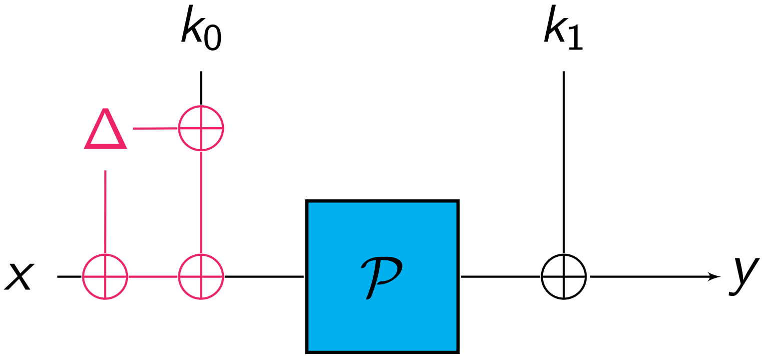


Figure: Trivial RK distinguisher for EM

Broken instantiations

Take $\mathrm{EM}_{k_0,k_1}(m) := \mathcal{P}(m \oplus k_0) \oplus k_1$

- Secure in the ideal permutation model (Even & Mansour, 1991)
- But not *related-key* secure: $\mathrm{EM}_{k_0 \oplus \Delta, k_1}(m \oplus \Delta) = \mathrm{EM}_{k_0,k_1}(m)$
- (Or equivalently $\mathrm{EM}^{-1}_{k_0,k_1 \oplus \Delta}(c \oplus \Delta) = \mathrm{EM}^{-1}_{k_0,k_1}(c)$

So:

- Let $\mathrm{T_L} = (x, y \mapsto x, y \oplus \Delta)$; $\mathrm{T_R} = (x \mapsto x \oplus \Delta)$
- Then $\mathrm{Tamp}^{\mathrm{T}}(m) = \mathrm{EM}^{-1}_{k_0,k_1 \oplus \Delta}(\mathrm{EM}_{k_0,k_1}(m) \oplus \Delta) = m$
- $\Rightarrow$ RKNMC[EM] is trivially insecure

Simulating Tamp from related-key queries

Related-key attacks

The adversary can query $\mathcal{O}_k$, $\mathcal{O}_k^{-1}$, $\mathcal{O}_{\varphi(k)}$, $\mathcal{O}_{\varphi(k)}^{-1}$ for unknown k, chosen $\varphi \in \Phi$ w/ $\mathcal{O} = \mathcal{E}$ or $\mathcal{O} = \mathfrak{E}$

- Objective: distinguish the two worlds

- Take $\mathsf{T} = \varphi \| \mathsf{T_R}$, m, m'
- Query $x := \mathcal{O}_k(m)$, $y := \mathcal{O}_{\varphi(k)}^{-1}(\mathsf{T_R}(x))$
- Run an NMC adversary $A(\mathsf{T}, m, m')$ on y
- $\rightsquigarrow$ $\mathbf{Adv}_{\mathrm{RK}}$ w.r.t. φ is at least *not (much) less* than $\mathbf{Adv}_{\mathrm{NMC}}$ w.r.t. $\mathsf{Tamp}^{\mathsf{T}}$, $\mathsf{T} = \varphi \| \cdot$.

Related-key issues

- Problem: *generic* absence of RK security for unrestricted φ
- For instance, take $\varphi : x \mapsto 0$
- But $\mathsf{T_L} : x \mapsto 0$ *is* allowed
- $\Rightarrow$ upper-bounding $\mathbf{Adv}_{\mathsf{NMC}}$ by the $\mathbf{Adv}_{\mathsf{RK}}$ seems meaningless :(
- A condition for meaningful $\mathbf{Adv}_{\mathsf{RK}}$: $\varphi(K)$ "hard to guess" for uniform K (cf. Bellare & Kohno, 2003)

Switching to single-key security

- Take $\mathsf{T} : x \mapsto 0 \| \mathsf{T}_\mathrm{R}$, m, m'
- Query $x := \mathcal{O}_k(m)$, $y := \mathcal{E}_0^{-1}(\mathsf{T}_\mathrm{R}(x))$
- Run $A(\mathsf{T}, m, m')$ on y
- $\rightsquigarrow$ $\mathbf{Adv}_\mathrm{NMC}$ w.r.t. such T reduces to *single key* security $\mathbf{Adv}_\mathrm{PRP}$ of $\mathcal{E}$!

More with single keys

- Take $\mathsf{T_L} : \{0,1\}^\kappa \to \{k_0, k_1, \ldots, k_w\} \subset \{0,1\}^\kappa$
- ... with $\mathcal{K}_i := \{\mathsf{T_L}^{-1}(k_i)\}$ all large (say size $\geq 2^{\kappa/2}$)
- If $\forall i$, $\mathcal{E}^{\mathcal{K}_i} : \mathcal{K}_i \times \mathcal{M} \to \mathcal{M}$ "is secure", $\mathbf{Adv}_{\mathsf{NMC}}$ is small w.r.t. $\mathsf{Tamp}^{\mathsf{T_L} \| \mathsf{T_R}}$
- (Query $x := \mathcal{O}^{\mathcal{K}_i}(m)$, $y := \mathcal{E}_{k_i}^{-1}(\mathsf{T_R}(x))$)
- Formalized through "PRP-with-leakage" notion

Main proof intuition

- Get a collection of reductions to RK, PRP-with-leakage
- Show that $\forall\, \mathsf{T_L}$, one reduction gives a "strong" bound

$\Rightarrow$

Theorem

$$\mathbf{Adv}_{\mathsf{RKNMC}}(t) \leq$$
$$2\max\left\{\mathbf{Adv}_{\mathcal{E}}^{\text{prp-leak}}(1, 2t+1) + 2^{-\kappa/2}, \mathbf{Adv}_{\mathcal{E}}^{\text{f-rk}}(4, 2t) + \varepsilon + 2^{-n}\right\}$$

N.B.: there is a generic attack w. $\mathbf{Adv}(t) \approx t^2/2^\kappa$

Instantiation matters

Need block ciphers secure w.r.t. PRP-with-leakage and Fixed-RK
$\rightsquigarrow$ No known RK attack with ONE RK-query
$\rightsquigarrow$ No known large weak key classes

- Fixed message-length: e.g. AES-128 ($|m| = 128$, $\kappa = 64$); SHACAL-2 ($|m| = 256$, $\kappa = 256$)
- Variable message-length: VILBC, e.g. MisterMonsterBurrito + IEM
- VILBC with built-in RK resistance?

Fin