Tweakable blockciphers with beyond-birthday-bound security

Will Landecker, Thomas Shrimpton, and **Seth Terashima**

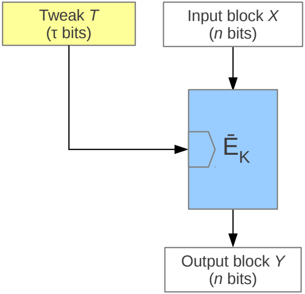
Portland State University

Tweakable blockciphers (TBCs)

- Add an extra input, a τ-bit *tweak*, to a blockcipher:

  $$\widetilde{E}_K : \{0,1\}^\tau \times \{0,1\}^n \to \{0,1\}^n$$

- Each tweak gives new permutation



Tweak provides variability, giving a more natural starting point for designing symmetric-key constructions.

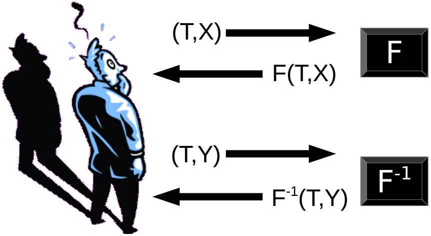
What are TBCs used for?

TBCs are used in algorithms for

- Authenticated encryption (OCB)
- MACs/PRFs (PMAC, PMAC_Plus)
- Hash functions (Skein)
- Blockcipher domain extenstion (LargeBlock1/2)

Other constructions can be viewed as TBC-based, even if this is not explicit (e.g., CBC, EME, EME*)

STPRP experiment for a TBC $\widetilde{E}$



World 1

$F(T, X) = \widetilde{E}_K(T, X)$

For a random key K

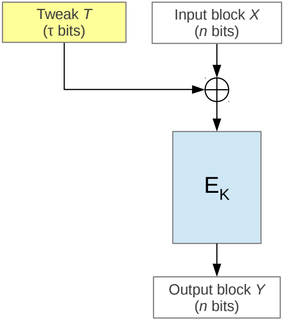
World 0

$F(T, X) = \Pi_T(X)$

Where Π is a random blockcipher

Adversary tries to guess if his oracle is the TBC $\widetilde{E}$ with a random key, or a random blockcipher (an ideal cipher) that uses T as its key.

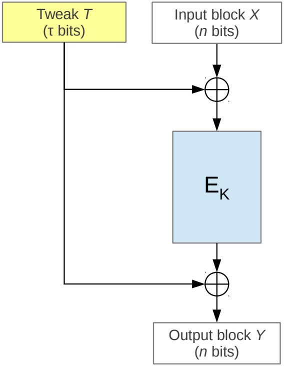
Building a TBC



CBC block operation is a TBC

Problem:
$\widetilde{E}(T, X \oplus C) = \widetilde{E}(T \oplus C, X)$

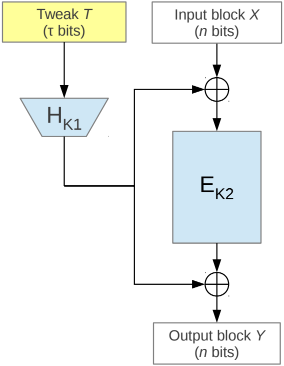
Building a TBC



Adding another XOR doesn't accomplish much. . .

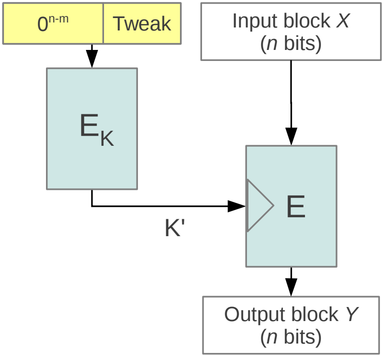
$$\widetilde{E}(T, X \oplus C) = \widetilde{E}(T \oplus C, X) \oplus C$$

The LRW2 tweakable blockcipher [LRW'02]



- **Birthday-bound** secure STPRP
  (Assuming E is a SPRP and H is ϵ-AXU$_2$)
- Matching attacks exist

Minematsu's Tweak-Dependent-Rekeying TBC [Min'09]



Provides beyond-birthday-bound security!

But...

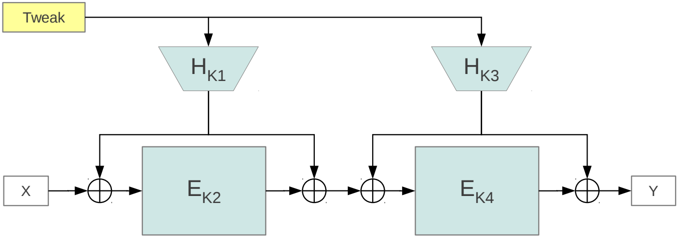
- Tweak length must be significantly shorter than $n/2$ bits
- Need to change E's key with each tweak

Our design goals

Build a TBC that

- Provides beyond-birthday-bound-security
- Uses standard primitives (such as blockciphers)
- Does not rekey underlying components
- Permits arbitrarily-sized tweaks

Our construction: Chained LRW2 (CLRW2)



- Provides beyond-birthday-bound-security
- Uses standard primitives (such as blockciphers)
- Does not rekey underlying components
- Permits arbitrarily-sized tweaks

Main result

Theorem

Let CLRW2 *be defined as above, using a blockcipher E and an ϵ-AXU_2 hash function family, H. Then*

$$\mathbf{Adv}^{\widetilde{\mathrm{sprp}}}_{\mathsf{CLRW2}}(q,t) \le 2\mathbf{Adv}^{\mathrm{sprp}}_{E}(q,t') + \frac{6q^3\hat{\epsilon}^2}{1-q^3\hat{\epsilon}^2}$$

where $\hat{\epsilon} = \max\{\epsilon, 1/(2^n - 2q)\}$ *and* $t' \approx t$.

Main result

Theorem

Let CLRW2 *be defined as above, using a blockcipher E and an ϵ-AXU_2 hash function family, H. Then*

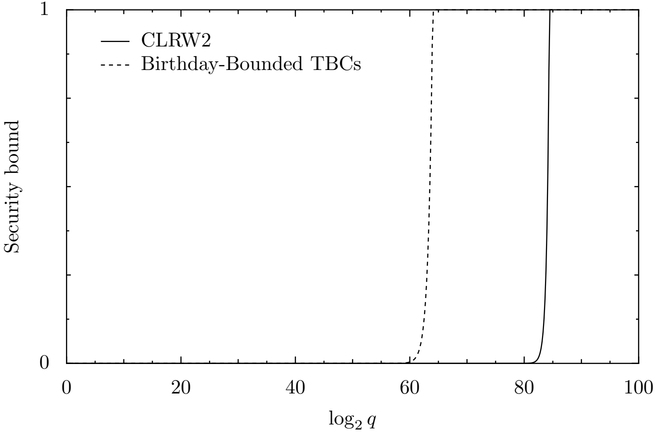
$$\mathbf{Adv}^{\widetilde{\mathrm{sprp}}}_{\mathrm{CLRW2}}(q,t) \leq 2\mathbf{Adv}^{\mathrm{sprp}}_{E}(q,t') + \frac{6q^3\hat{\epsilon}^2}{1-q^3\hat{\epsilon}^2}$$

where $\hat{\epsilon} = \max\{\epsilon, 1/(2^n - 2q)\}$ *and* $t' \approx t$.

With practical $\hat{\epsilon}$,

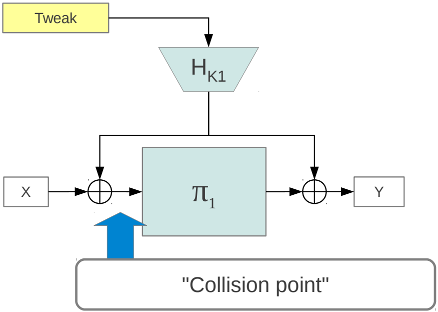
$$\frac{q^3\hat{\epsilon}^2}{1-q^3\hat{\epsilon}^2} \approx \frac{q^3}{2^{2n}}.$$

Concrete security bounds



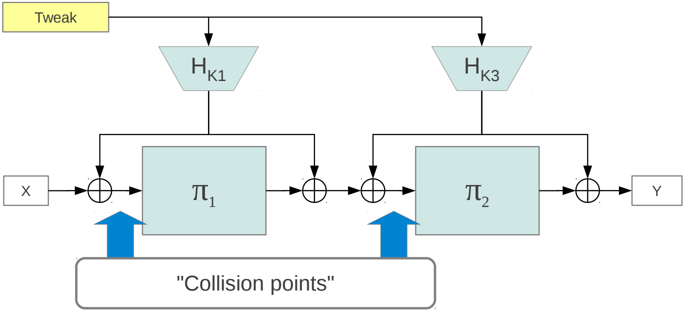
Security bound after q queries (assuming a secure 128-bit blockcipher).

Proof intuition



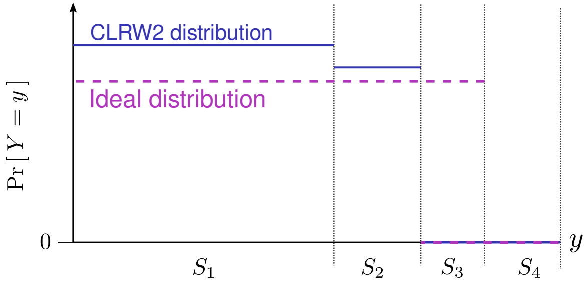
Behaves very similarly to an ideal cipher unless there is a collision.

Proof intuition



Behaves very similarly to an ideal cipher unless there are **two independent** collisions on the same query.

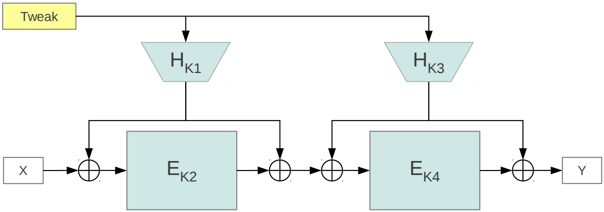
Key proof trick



If there's no first-round collision, the CLRW2 output space $\{0, 1\}^n$ can be partitioned into four sets, with outputs uniformly distributed within each set.

Statistical distance between this distribution and ideal distribution proportional to $|S_3|$.

Some natural questions



Can we reduce the number of keys?
Possibly secure, would require substantive proof changes

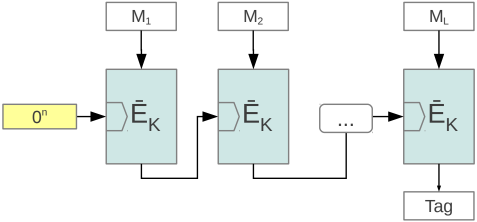
Would more rounds give even better security?
Conjecture: r rounds secure against $q \ll 2^{rn/(r+1)}$ queries

Can this be simplified?
Removing any $\oplus$ operation permits attacks with $\mathcal{O}(2^{n/2})$ queries

CLRW2 is our main new result. But let's look at another. . .

TBC-MAC

- Proposed (but not analyzed) in LRW paper
- Similar to CBC-MAC, but chains through the tweak

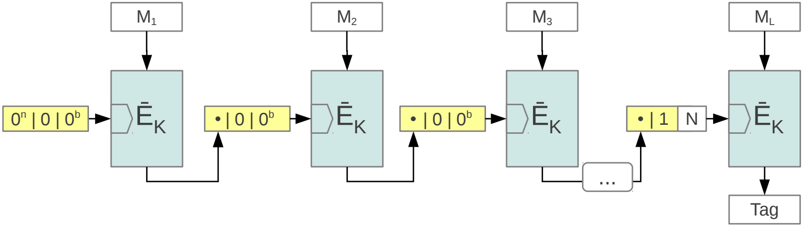


$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{TBCMAC}[\overline{E}]}(A) \leq \mathbf{Adv}^{\widetilde{\mathrm{prp}}}_{\overline{E}}(B) + \frac{(q\ell)^2}{2^n}$$

Seems like we should be able to do better...

TBC-MAC2

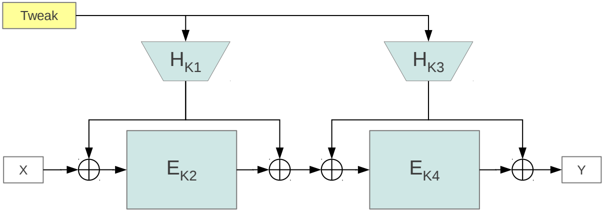
Nonce-based PRF resistant to nonce-misuse.

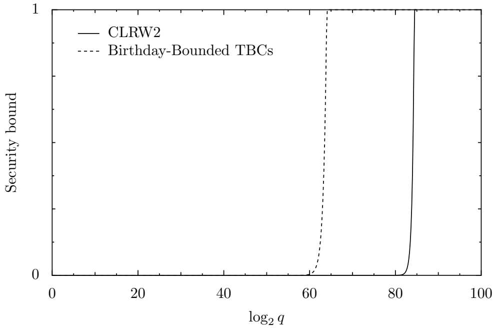


$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{TBCMAC2}[\overline{E}]}(A) \leq \begin{cases} \mathbf{Adv}^{\widetilde{\mathrm{prp}}}_{\overline{E}}(B) & \text{if nonces are distinct,} \\ \mathbf{Adv}^{\widetilde{\mathrm{prp}}}_{\overline{E}}(B) + \frac{q^2(\ell+1)^2}{2^{n-1}} & \text{constant “nonce”} \end{cases}$$

In general, the second term is quadratic in the maximum number of times a given nonce is repeated.

Thank you!


Tweak
H_{K1}
H_{K3}
X
E_{K2}
E_{K4}
Y


1
0
CLRW2
Birthday-Bounded TBCs
Security bound
0
20
40
60
80
100
$\log_2 q$