Trick or Tweak

On the (In)security of OTR's Tweaks

Raphael Bost[1,2] Olivier Sanders[3]

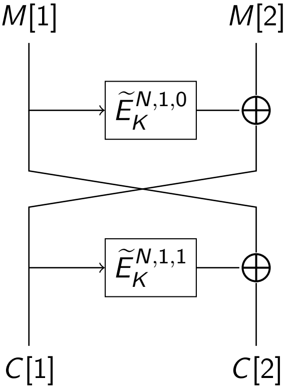
[1]Direction Générale de l'Armement - Maîtrise de l'Information
[2]Université de Rennes 1

[3]Orange Labs

Asiacrypt 2016, Hanoi

Offset Two Rounds (OTR)

- CAESAR submission by K. Minematsu (Eurocrypt '14)
- Inspired by OCB
- Rate-1 AE
- Tweakable blockcipher based
- Inverse-free (only needs E, not E^{-1})
- Two rounds Feistel construction
- Defined for any block size n.



Tweakable Blockcipher (TBC) [LRW02]

Add a public input to a blockcipher – the tweak – to add variability.

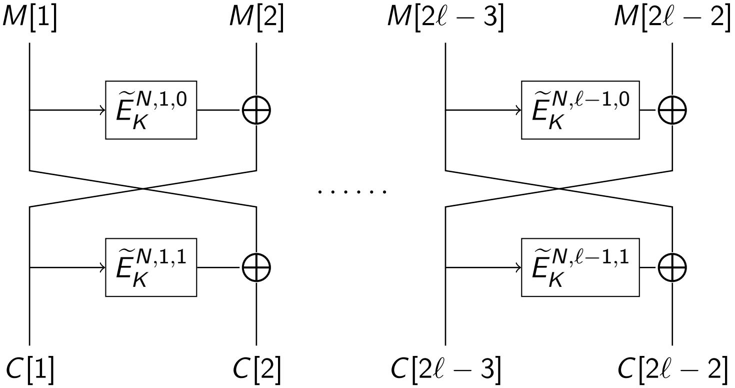
Each tweak $T \in \mathcal{T}$ (the tweak space) yields an independent pseudo-random permutation.

Tweakable Blockcipher (a.k.a tweakable PRP)

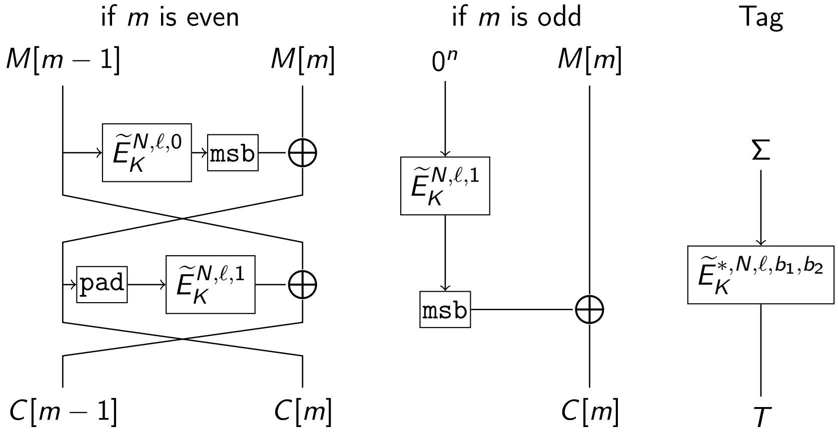
The $T \in \mathcal{T}$ indexed permutation family $\widetilde{E}_K(T, .)$ is indistinguishable from a random permutation family $\pi(T, .)$

$$\mathbb{P}[K \xleftarrow{\$} \mathcal{K} : \mathcal{A}^{\widetilde{E}_K(.,.)} \Rightarrow 1] - \mathbb{P}[\widetilde{\pi} \xleftarrow{\$} \mathsf{Perm}(\mathcal{T}, n) : \mathcal{A}^{\widetilde{\pi}(.,.)} \Rightarrow 1] \leq \mathrm{negl}(\lambda)$$

OTR Encryption (1/2)



OTR Encryption (2/2)



$$\Sigma = M[2] \oplus \ldots \oplus M[m-2] \oplus Z \oplus \underline{C[m]}$$

$$\Sigma = M[2] \oplus \ldots \oplus M[m-1] \oplus \underline{M[m]}$$

OTR's security

Theorem (Theorem 3 of [Min14])

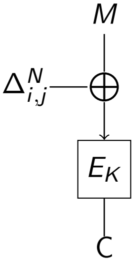
If $\widetilde{E}$ is a tweakable PRP, OTR is CPA-secure (confidentiality) and INT-CTXT-secure (unforgeability).

Instantiating the TBC

Remark

We are working in $\mathbb{F}_{2^n}$ represented as $\mathbb{F}_2[X]/(P(X))$ with P is a degree n primitive polynomial in $\mathbb{F}_2$.

- Use the XE construction
- In [Rog04]: $\widetilde{E}_K^{N,i,j}(M) = E_K(M + X^i(X+1)^j\delta)$ with $\delta = E_K(N)$



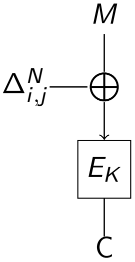
Instantiating the TBC

Remark

We are working in $\mathbb{F}_{2^n}$ represented as $\mathbb{F}_2[X]/(P(X))$ with P is a degree n primitive polynomial in $\mathbb{F}_2$.

In OTRv1-v2 [Min14], for efficiency, an other masking scheme is used:

$$\Delta_{i,b}^{N} = (X^{i+1} + b)\delta$$
$$\Delta_{\ell,b_1,b_2}^{*,N} = [(X+1)X^{\ell+1} + X \cdot b_1 + b_1 + b_2]\delta$$



The flaw

Lemma (Lemma 1 of [Min14])

The TBC is indistinguishable from a tweakable PRP.

The proof of this lemma relies on the following claim

Claim

$$\begin{aligned}\text{Let } \mathcal{S}_1(\delta) = \big\{ & X^{i+1}\delta, (X^{i+1}+1)\delta, \big\} \\ & \cup \big\{(X^{i+2}+X^{i+1}+b_1X+b_2)\delta\big\}_{i=1, b_1\in\{0,1\}, b_2\in\{0,1\}}\end{aligned}$$

The elements of $\mathcal{S}_1(\delta)$ are pairwise different.

The flaw

Lemma (Lemma 1 of [Min14])

The TBC is indistinguishable from a tweakable PRP.

The proof of this lemma relies on the following claim

Claim

$$\text{Let } \mathcal{S}_1(\delta) = \left\{X^{i+1}\delta, (X^{i+1}+1)\delta, \right\} \\ \cup \left\{(X^{i+2}+X^{i+1}+b_1X+b_2)\delta\right\}_{i=1, b_1\in\{0,1\}, b_2\in\{0,1\}}$$

The elements of $\mathcal{S}_1(\delta)$ are pairwise different.

Our attack

This is not true in general!

The trick

- In [Rog04], for $\log_X(X+1) = \alpha$, as long as $0 \leq i + \alpha j \leq 2^n - 1$, $\{X^i(X+1)^j\}$ are pairwise distinct
  $\Rightarrow$ bound i and j.

The trick

- In [Rog04], for $\log_X(X+1) = \alpha$, as long as $0 \leq i + \alpha j \leq 2^n - 1$, $\{X^i(X+1)^j\}$ are pairwise distinct
  $\Rightarrow$ bound i and j.
- In [Min14], we cannot show that, for some q, elements are pairwise distinct in

$$\left\{X^{i+1}, X^{i+1}+1\right\} \cup \left\{X^{i+2}+X^{i+1}+b_1X+b_2\right\}_{1\leq i\leq q,(b_1,b_2)\in\{0,1\}^2}.$$

The trick

- In [Rog04], for $\log_X(X+1) = \alpha$, as long as $0 \leq i + \alpha j \leq 2^n - 1$, $\{X^i(X+1)^j\}$ are pairwise distinct
  $\Rightarrow$ bound i and j.
- In [Min14], we cannot show that, for some q, elements are pairwise distinct in

$$\left\{X^{i+1}, X^{i+1}+1\right\} \cup \left\{X^{i+2}+X^{i+1}+b_1X+b_2\right\}_{1\leq i\leq q,(b_1,b_2)\in\{0,1\}^2}.$$

- If $P(X) = X^n + X^j + 1$, there is a collision between X^n and $X^j + 1$ in $\mathbb{F}_{2^n} = \mathbb{F}_2[X]/(P(X))$.

For actual block sizes ($n = 64, 128$)?

- If $8|n$, $\mathbb{F}_{2^n} = \mathbb{F}_2[X]/(P(X))$ with P with at least 5 non-zero coefficient ($P(X) = X^n + X^{j_1} + X^{j_2} + X^{j_3} + 1$).
  $\Rightarrow$ no immediate collision in general.

For actual block sizes ($n = 64, 128$)?

- If $8|n$, $\mathbb{F}_{2^n} = \mathbb{F}_2[X]/(P(X))$ with P with at least 5 non-zero coefficient ($P(X) = X^n + X^{j_1} + X^{j_2} + X^{j_3} + 1$).
  $\Rightarrow$ no immediate collision in general.
- For SW/HW efficiency, we usually choose P such that its non-zero coefficients are close to each other, preferably in the least significant bytes.

$$P_{64}(X) = X^{64} + X^4 + X^3 + X + 1$$
$$P_{128}(X) = X^{128} + X^7 + X^2 + X + 1$$

For actual block sizes ($n = 64, 128$)?

- If $8|n$, $\mathbb{F}_{2^n} = \mathbb{F}_2[X]/(P(X))$ with P with at least 5 non-zero coefficient ($P(X) = X^n + X^{j_1} + X^{j_2} + X^{j_3} + 1$).
  $\Rightarrow$ no immediate collision in general.
- For SW/HW efficiency, we usually choose P such that its non-zero coefficients are close to each other, preferably in the least significant bytes.

$$P_{64}(X) = X^{64} + X^4 + X^3 + X + 1$$
$$P_{128}(X) = X^{128} + X^7 + X^2 + X + 1$$

- For $n = 64$ with the usual P, we have a collision of the type $X^i = X^{j+1} + X^j + X + 1$:

$$X^{64} = X^4 + X^3 + X + 1$$

Consequences

Problem

There is a flaw in the proof of OTR, even for practical parameters.

Does the confidentiality of OTR break?
Does the unforgeability of OTR break?

Typology of collisions

$$\left\{X^{i+1}, X^{i+1}+1\right\}_{1\leq i\leq q} \cup \left\{X^{i+2}+X^{i+1}+b_1X+b_2\right\}_{1\leq i\leq q,(b_1,b_2)\in\{0,1\}^2}$$

There are three types of collision among the tweaks' polynomials:

$$X^i = X^j + 1 \tag{1}$$

$$X^i = X^{j+1} + X^j + r(X) \tag{2}$$

$$X^{i+1} + X^i = X^{j+1} + X^j + r(X) \tag{3}$$

with $r(X) \in \{0, 1, X, X+1\}$.

Attacks

Out attack

Type 1 ($X^i = X^j + 1$)

Break confidentiality *and* unforgeability.

Type 2 ($X^i = X^{j+1} + X^j + r(X)$)

Break confidentiality if $i < j$. Break unforgeability o/w.

Type 3 ($X^{i+1} + X^i = X^{j+1} + X^j + r(X)$)

Break unforgeability.

Idea: use the collision to have relations between block cipher's inputs and create collisions on the outputs.
Only *one* query to the encryption oracle, with a message of $\max(i, j)$ blocks.

$n = 128$ in practice

Usually, for $n = 128$, we choose

$$P(X) = X^{128} + X^7 + X^2 + X + 1.$$

There is no trivial collision.

Remark

This is not true for all irreducible P of degree 128.
Ex: $P(X) = X^{128} + X^{127} + X^{61} + X^{60} + 1$

Can we find a collision among tweaks polynomial?

In search for lost collision

- We are only interested in collisions with i and $j < 2^{64}$: the security proof of OTR only holds up to the birthday bound.

In search for lost collision

- We are only interested in collisions with i and $j < 2^{64}$: the security proof of OTR only holds up to the birthday bound.
- We cannot find such collisions by constructing a collision in $\mathbb{F}_{2^{64}}$ and then 'moving' it to $\mathbb{F}_{2^{128}}$.

In search for lost collision

- We are only interested in collisions with i and $j < 2^{64}$: the security proof of OTR only holds up to the birthday bound.
- We cannot find such collisions by constructing a collision in $\mathbb{F}_{2^{64}}$ and then 'moving' it to $\mathbb{F}_{2^{128}}$.
- Our only hope: exhaustive search.

In search for lost collision

- We are only interested in collisions with i and $j < 2^{64}$: the security proof of OTR only holds up to the birthday bound.
- We cannot find such collisions by constructing a collision in $\mathbb{F}_{2^{64}}$ and then 'moving' it to $\mathbb{F}_{2^{128}}$.
- Our only hope: exhaustive search.
- Generate, sort and match tweak polynomials (Embarrassingly parallelizable).

In search for lost collision

- We are only interested in collisions with i and $j < 2^{64}$: the security proof of OTR only holds up to the birthday bound.
- We cannot find such collisions by constructing a collision in $\mathbb{F}_{2^{64}}$ and then 'moving' it to $\mathbb{F}_{2^{128}}$.
- Our only hope: exhaustive search.
- Generate, sort and match tweak polynomials (Embarrassingly parallelizable).
- Problem: requires $O(n2^n)$ memory and $O(n2^n)$ time ...

In search for lost collision

We used time/memory tradeoffs to search for any collision with $i, j < 2^{45}$.

Theorem

There is no collision among the tweaks polynomials for $i, j < 2^{45}$ when $F_{2^{128}}$ is defined as $F_2[X]/(X^{128} + X^7 + X^2 + X + 1)$.

The exhaustive search took 15 CPU-years using 3TB of RAM.

In search for lost collision

We used time/memory tradeoffs to search for any collision with $i, j < 2^{45}$.

Theorem

There is no collision among the tweaks polynomials for $i, j < 2^{45}$ when $F_{2^{128}}$ is defined as $F_2[X]/(X^{128} + X^7 + X^2 + X + 1)$.

The exhaustive search took 15 CPU-years using 3TB of RAM.

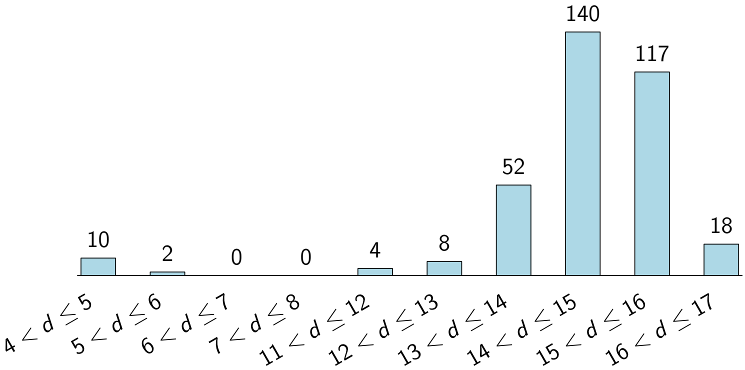
Question

What about $2^{45} \leq i, j$?

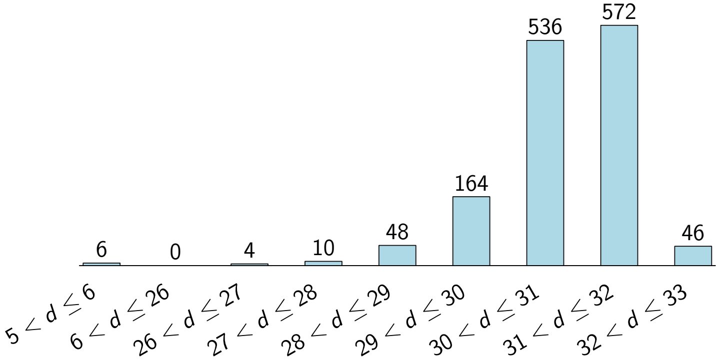
Probable collision before the birthday bound

- If tweak polynomials behaved like random polynomials, we should have a collision just before the birthday bound.
- For $n = 32, 64$, we enumerated the irreducible polynomials over $\mathbb{F}_2$ of degree n and search for the lowest degree colliding polynomials.

First collision for $n = 32$



First collision for $n = 64$



Conjecture for $n = 128$

Conjecture

There is no collision among the tweaks polynomials for $i, j < 2^{60}$ when $F_{2^{128}}$ is defined as $F_2[X]/(X^{128} + X^7 + X^2 + X + 1)$.

Conclusion

- OTRv2 is insecure for many block sizes.
- OTRv2 is secure for $n = 128$ when the message length is limited to 2^{45} blocks.
- OTRv2 is probably secure for $n = 128$ almost up to the birthday bound.
- OTRv3 fixes the issue.

Thank you!

Paper: ia.cr/2016/234