On Cipher-Dependent Related-Key Attacks in the Ideal-Cipher Model

M.R. Albrecht[1] **P. Farshim**[2] K.G. Paterson[3]
G.J. Watson[4]

[1]SALSA Project -INRIA, UPMC, Univ Paris 06

[2]Information Security Group, Royal Holloway, University of London
(Moving to NTT soon)

[2]Information Security Group, Royal Holloway, University of London

[3]Department of Computer Science, University of Calgary

Fast Software Encryption – FSE 2011
14 February 2011

Outline

Block Ciphers (Theoretically)

A family of permutations

$$E : \mathcal{K} \times \mathcal{D} \to \mathcal{D}$$

where:

- $\mathcal{K}$ is the key space; and
- $\mathcal{D}$ is the domain or the message space.

PRP Security

Intuition:

- Cannot tell apart the outputs of the block cipher from truly random values.

More formally:

$$\mathbf{Adv}_E^{\mathrm{prp}}(A) := \Pr\left[K \xleftarrow{\$} \mathcal{K} : A^{E(K,\cdot)} = 1\right] - \Pr\left[G \xleftarrow{\$} \mathrm{Perm}(\mathcal{D}) : A^{G(\cdot)} = 1\right]$$

Related-Key Attacks (RKA)

- Denote by $\phi : \mathcal{K} \to \mathcal{K}$ a **related-key deriving function.**
- Φ is the set of available/allowed ϕ's.

Intuition:

- Can query an RK oracle on (ϕ, M) to get $E(\phi(K), M)$.
- E should be still indist. from a random permutation.

Formally, in a Φ-restricted attack:

$$\mathbf{Adv}^{\text{prp-rka}}_{\Phi,E}(A) := \Pr\left[K \stackrel{\$}{\leftarrow} \mathcal{K} : A^{E(\mathrm{RK}(\cdot,K),\cdot)} = 1\right] - \Pr\left[K \stackrel{\$}{\leftarrow} \mathcal{K}; G \stackrel{\$}{\leftarrow} \mathrm{Perm}(\mathcal{K}, \mathcal{D}) : A^{G(\mathrm{RK}(\cdot,K),\cdot)} = 1\right]$$

Why RKA?

- A number of related-key attacks against high-profile ciphers have been discovered.
- Block ciphers are expected to resist related-key attacks.
- There are widely-deployed real-world protocols which make use of related-keys (e.g. EMV and 3GPP).
- Used in analysis of tweakable modes of operation.
- Not clear what a “meaningful” related-key attack is.
- Theoretically interesting: Recent construction of RKA secure PRFs by Bellare and Cash (CRYPTO 2010).

Related-Key Attacks in the Ideal-Cipher Model

- General feasibility results are hard to achieve in standard model.
- Move to the ideal-cipher model: get minimum restrictions on Φ s.t. RKA is provably achievable for an ideal cipher.
- To formalise security in the ICM, as usual, give oracle access to E and E^{-1}.

Formally:

$$\mathbf{Adv}^{\text{prp-rka}}_{\Phi,\mathcal{K},\mathcal{D}}(A) := \Pr\left[K \xleftarrow{\$} \mathcal{K} : E \xleftarrow{\$} \mathrm{Perm}(\mathcal{K},\mathcal{D}) : A^{E,E^{-1},E(\mathrm{RK}(\cdot,K),\cdot)} = 1\right] -$$

$$\Pr\left[K \xleftarrow{\$} \mathcal{K}; E \xleftarrow{\$} \mathrm{Perm}(\mathcal{K},\mathcal{D}); G \xleftarrow{\$} \mathrm{Perm}(\mathcal{K},\mathcal{D}) : A^{E,E^{-1},G(\mathrm{RK}(\cdot,K),\cdot)} = 1\right]$$

Restrictions on the RKD Set Φ

Call Φ **Output-Unpredictable** (UP) if:

- No adversary can predict the output of any ϕ, i.e. it cannot return a ϕ and a K' s.t. $\phi(K) = K'$ for a random K.

Call Φ **Collision-Resistant** (CR) if:

- No adversary can trigger collisions between two ϕ's, i.e. it cannot return ϕ_1 and ϕ_2 s.t. $\phi_1(K) = \phi_2(K)$ for a random K.

The Bellare-Kohno Theorem

Theorem (Bellare and Kohno – EUROCRYPT 2003)

Fix a key space $\mathcal{K}$ and domain $\mathcal{D}$. Let Φ be a set of RKD functions over $\mathcal{K}$. Suppose Φ is both CR and UP. Then no adversary can break an ideal cipher under related-key attacks:

$$\mathbf{Adv}^{\text{prp-rka}}_{\Phi,\mathcal{K},\mathcal{D}}(A) \leq \mathbf{Adv}^{\text{cr}}_{\Phi}(B) + \mathbf{Adv}^{\text{up}}_{\Phi}(C)\,.$$

The Bellare-Kohno Theorem: Proof

$$A^{E(\cdot,\cdot),E(\phi_1(K),\cdot),E(\phi_2(K),\cdot)}$$

Proof.

Assume different ϕ's always lead to different keys:

CR allows separating distinct ϕ_1 and ϕ_2 queries.

UP allows separating ϕ queries from E or E^{-1} queries.

Now answer queries randomly. □

Interpretations of the BK Theorem

The BK theorem is about ideal ciphers.
What does it mean for real block ciphers?

1. For any CR and UP Φ, there is a block cipher E which resists Φ-restricted attacks.
2. There is a block cipher E which resists all Φ-restricted attacks, as long as Φ is CR and UP.

Interpretations of the BK Theorem

The difference is in the **order of quantifiers**.

1. $\forall \Phi, \exists E$, E is Φ-secure.
2. $\exists E, \forall \Phi$, E is Φ-secure.

- In the BK theorem E is chosen randomly after Φ.
- So the **1st interpretation is accurate**, and don't expect natural counterexamples.
- Want E to resist all Φ-restricted attacks, including those which may depend on E: 1st is not as useful as 2nd.
- But we show a natural counterexample to the 2nd interpretation.

Bernstein's Attack - The RKD set

Consider the E-dependent RKD set:

$$\Delta_E := \{K \mapsto K, K \mapsto E(K, 0)\}$$

If E is PRP secure, then this set is both UP and CR.

Bernstein's Attack - The Attack

Algorithm A^f: (where f is either E or G)
Query RK on $(K \mapsto K, 0)$. Get $x := f(K, 0)$
Query RK on $(K \mapsto E(K, 0), 0)$. Get $y := f(E(K, 0), 0)$
Calculate $z := E(x, 0)$
Return $(z = y)$

- $\boxed{f = E}$: have $x = E(K, 0)$, $y = E(E(K, 0), 0)$, and $z = E(E(K, 0), 0)$. Hence $z = y$ with probability 1.

- $\boxed{f = G}$: have $x = G(K, 0)$, $y = G(E(K, 0), 0)$, and $z = E(G(K, 0), 0)$. Since G is a randomly chosen permutation

$$\Pr[z = y] = \Pr\left[E(G(K, 0), 0) = G(E(K, 0), 0)\right] \approx 1/|\mathcal{K}|.$$

Beyond Indistinguishability: Harris's Attack

Harris gives an attack which recovers the key.
Roughly it works as follows:

- The RKD set contains functions ϕ_i such that the i-th bit of $E(\phi_i(K), m)$ matches the i-th bit of K with noticeable prob.
- The key K can then be recovered bit-by-bit (after amplification).
- Slight modification of this set is shown to be UP and CR.
- More details in the paper.

RKD Functions with Oracle Access to E and E^{-1}

Our goal is to capture Bernstein-like attacks, i.e.

Model ϕ's which depend on E.

Extend modelling of RKD functions:

- Allow RKD functions to perform subroutine calls to oracles $\mathcal{O}_1$ and $\mathcal{O}_2$.
- $\mathcal{O}_1$ and $\mathcal{O}_2$ are instantiated with E and E^{-1} respectively.
- Write the set as $\Phi^{E,E^{-1}}$ and functions as $\phi^{E,E^{-1}}$.

The advantage of an adversary A:

$$\mathbf{Adv}^{\text{prp-orka}}_{\Phi^{E,E^{-1}},\mathcal{K},\mathcal{D}}(A)$$

is defined analogously.

Oracle UP and Oracle CR

Call Φ **Oracle-Output-Unpredictable** (OUP) if:

- No adversary can return a $\phi^{E,E^{-1}}$ and a K' such that:

$$\phi^{E,E^{-1}}(K) = K',$$

where K **and** E are randomly chosen.

Call Φ **Oracle-Collision-Resistant** (OCR) if:

- No adversary can return $\phi_1^{E,E^{-1}}$ and $\phi_2^{E,E^{-1}}$ such that:

$$\phi_1^{E,E^{-1}}(K) = \phi_2^{E,E^{-1}}(K),$$

where K **and** E are randomly chosen.

Taking Care of Extra Collisions

- Recall now ϕ's have oracle access to E and E^{-1}.
- New collisions between implicit and explicit queries to E or E^{-1} might arise:
  - Between ϕ's query and A's RK queries on $\phi' \neq \phi$.
  - Between ϕ's query and A's RK queries on $\phi' = \phi$!
  - Between ϕ's query and A's query to E or E^{-1}.
- Take care of this by introducing a new condition which rules out such collisions.

New Condition: Oracle-Independence

Call Φ **Oracle-Independent** (OIND) if:

- No adversary can return a $\phi'^{E,E^{-1}}(K)$ or a key K', another (not necessarily distinct!) $\phi^{E,E^{-1}}(K)$, and an x such that:

  $$(\phi'^{E,E^{-1}}(K) \text{ or } K', x) \in \{\text{Queries by } \phi^{E,E^{-1}}(K) \text{ to } E/E^{-1}\},$$

  where K and E are randomly chosen.

Main Theorem

Theorem

Fix a key space $\mathcal{K}$ and domain $\mathcal{D}$. Let $\Phi^{E,E^{-1}}$ be a set of **oracle** *RKD functions over $\mathcal{K}$. Suppose this set is OCR, OUP, and* **OIND**. *Then no adversary can break the ideal cipher under oracle related-key attacks. More formally:*

$$\mathbf{Adv}^{\text{prp-orka}}_{\Phi^{E,E^{-1}},\mathcal{K},\mathcal{D}}(A) \leq \mathbf{Adv}^{\text{ocr}}_{\Phi^{E,E^{-1}}}(B) + \mathbf{Adv}^{\text{oup}}_{\Phi^{E,E^{-1}}}(C) + \mathbf{Adv}^{\text{oind}}_{\Phi^{E,E^{-1}}}(D)$$

Remark: For standard RKD sets the OIND condition is automatically satisfied. Hence the above is an **extension** of the BK theorem.

Main Theorem: Proof

$$A^{E(\cdot,\cdot),E(\phi_1^{E(\cdot,\cdot)}(K),\cdot),E(\phi_2^{E(\cdot,\cdot)}(K),\cdot)}$$

Proof.

OCR allows separating distinct ϕ_1 and ϕ_2 queries.
OUP allows separating ϕ queries from E/E^{-1} queries.
OIND allows separating E/E^{-1} queries in the exponent from both E/E^{-1} and ϕ queries downstairs. □

Results: Ruling out Bernstein's Attack

Theorem

Let

$$\Delta^E := \{K \mapsto K, K \mapsto E(K,0)\}$$

denote Bernstein's set of oracle RKD functions. Then Δ^E *does not satisfy the oracle-independence property.*

Remark: Harris's attack also doesn't satisfy OIND.

Results: Possibility Results

Theorem (EMV)

Fix a key space $\mathcal{K}$, and let $\mathcal{D} = \mathcal{K}$. Then the following oracle RKD set is OCR, OUP, and OIND.

$$\Omega^E := \{K \mapsto E(K, x) : x \in \mathcal{D}\}.$$

Theorem

Fix a key space $\mathcal{K}$, and let $\mathcal{D} = \mathcal{K}$. Then the following oracle RKD set is OCR, OUP, and OIND.

$$\Theta^E := \{K \mapsto K, K \mapsto E(0, K)\}.$$

Final Remarks

- Bernstein's and Harris's attacks are "illegal" in the new model.
- Even if we forget about the new condition, the attacks can now be replicated in the ICM.
- Expect a good block cipher $E^\star$ to resist $\Omega_{E^\star}$- and $\Theta_{E^\star}$-restricted attacks.
- In Biryukov et al.'s attack on AES the nature of dependency on E is not known, as it uses underlying building blocks. Hence the attack should be seen as interesting.

Thank You

Thank you for your attention.
Questions/Suggestions?