Recent Results on Key-Length Extension

Jooyoung Lee

Faculty of Mathematics and Statistics, Sejong University

August 27, 2013
Introduction to key length extension

Security proof of cascade encryption (Eurocrypt 2013)

Recent results on key length extension schemes
Blockciphers Using Short Keys

DES

\[ k : 56\text{-bit key} \]

\[ u \xrightarrow{\text{DES}} v \]

- Widely-used blockcipher using 56-bit keys
- No feasible attack faster than key exhaustive search
- Advances in computational power made key exhaustive search itself practical
  - Replaced by AES
  - Construction of DES-based encryption schemes employing longer keys: key-length extension
Triple-DES

- Double-DES is vulnerable to a meet-in-the-middle attack
- Security proved up to $2^{\kappa+\frac{\min\{n,\kappa\}}{2}}$ queries
  - Bellare and Rogaway (Eurocrypt 2006)
  - Gaži and Maurer (Asiacrypt 2009): some flaws fixed
Pre/post whitening keys used

Security proved up to $2^{\frac{\kappa+n}{2}}$ queries
  Kilian and Rogaway (Journal of Cryptology, 2001)
Randomized Cascade

- Cascade of DESX with some modification
- Security proved up to $2^{\kappa + n/2}$ queries
  - Gaži and Tessaro (Eurocrypt 2012)
Key Length Extension

A $\lambda$-bit key $m$-bit encryption scheme $C$

- Makes a fixed number of calls to the underlying $\kappa$-bit key $n$-bit blockcipher $E$ ($\lambda > \kappa$)
- Each key $k = \{0, 1\}^\lambda$ defines a permutation on $\{0, 1\}^m$
A distinguisher $\mathcal{A}$ wants to tell apart $(C_k[E], E)$ and $(P, E)$ by adaptively making forward and backward queries to the permutation and the blockcipher.

$$\text{Adv}_{C}^{\text{PRP}}(\mathcal{A}) = \Pr \left[ P \leftarrow\$ \mathcal{P}_n, E \leftarrow\$ \mathcal{B}C(\kappa, n) : \mathcal{A}[P, E] = 1 \right] - \Pr \left[ k \leftarrow\$ \{0, 1\}^\lambda, E \leftarrow\$ \mathcal{B}C(\kappa, n) : \mathcal{A}[C_k[E], E] = 1 \right]$$
Bruce-force Attack of $2^{\kappa+n}$ Queries

1. $A$ makes all possible $2^{\kappa+n}$ queries to $E$.
2. $A$ makes $t$ nonadaptive forward queries to the outer permutation, recording query history $Q = (u^i, v^i)_{1 \leq i \leq t}$.
3. If there is a $\lambda$-bit key $k$ such that $C_k[E](u^i) = v^i$ for every $i = 1, \ldots, t$, then $A$ outputs 0. Otherwise, $A$ outputs 1.

$\text{Adv}_{\text{C}^{\text{PRP}}}(A) \approx 1$ as $t \gg \frac{\lambda}{m}$.

Key length extension with optimal security?
Cascade Encryption CE

- Security asymptotically proved up to $2^{\kappa+\min\left\{ \frac{n}{2}, \kappa \right\}}$ queries
  - Gaži and Maurer (Asiacrypt 2009)
- Proved up to $2^{\kappa+\min\left\{ \kappa, n \right\}} - \frac{16}{7} \left( \frac{n}{2} + 2 \right)$ query complexity
  - Lee (Eurocrypt 2013)
  - Close to $2^{\kappa+\min\left\{ \kappa, n \right\}}$ when the cascade length $l$ is large
  - Asymptotically optimal if $n \leq \kappa$
Xor-cascade Encryption XCE

Security proved up to $2^{\kappa+n-\frac{8}{7}(\frac{n}{2}+2)}$ query complexity

- Lee (Eurocrypt 2013)
- Close to $2^{\kappa+n}$ when the cascade length $l$ is large
- Gazi improved on this bound (Crypto 2013)
Security Proof of 2/-cascade Encryption

Proof Strategy

1. Prove NCPA-security of/-cascade encryption
2. Lift NCPA-security to CCA-security by composing two independent components
   - Mauer, Pietrzak and Renner’s framework (Crypto 2007)
   - Combinatorial interpretation

"Random key space separation" technique needed
NCPA Adversary

1. Makes $q$ queries to the underlying blockcipher

$$\begin{array}{c}
k \\
\downarrow \\
E \\
\downarrow \\
x \\
\quad \longrightarrow \\
y \\
\quad \longrightarrow \\
\end{array}$$

2. Determine $q$ queries $u_1, \ldots, u_q$ to the outer permutation and distinguish two worlds:

World 1

$$\begin{array}{c}
k_1 \\
k_2 \\
k_l \\
\downarrow \\
E \\
\downarrow \\
E \\
\downarrow \\
E \\
\downarrow \\
\downarrow \\
u_1 \\
u_2 \\
\vdots \\
u_q \\
\quad \longrightarrow \\
w_1 \\
w_2 \\
\vdots \\
w_q \\
\quad \longrightarrow \\
\end{array}$$

World 2

$$\begin{array}{c}
\vdots \\
nu_1 \\
u_2 \\
\vdots \\
u_q \\
\quad \longrightarrow \\
w_1 \\
w_2 \\
\vdots \\
w_q \\
\quad \longrightarrow \\
\end{array}$$
For distinct random inputs $z_1, \ldots, z_q$, World 2 and World 3 are exactly the same.
Same Construction, Different Inputs

For distinct random inputs $z_1, \ldots, z_q$, World 2 and World 3 are exactly the same.
Same Construction, Different Inputs

For distinct random inputs $z_1, \ldots, z_q$, World 2 and World 3 are exactly the same.
Hybrid Argument

Input values change one by one

World 0

World 1

World 2

... 

World $q-1$

World $q$
Distinguishing World $m$ and World $m + 1$

For two probability distributions of the outputs ($q$-tuples), we will upper bound their statistical distance.
Coupling Technique

If $X \sim \mu$ and $Y \sim \nu$, then $\|\mu - \nu\| \leq \Pr[X \neq Y]$

Need to carefully design the sampling process such that $X \sim \mu$ and $Y \sim \nu$ (called a "coupling") and $\Pr[X \neq Y]$ is small
How to Couple World $m$ and World $m+1$

$$X = (u_1[l], \ldots, u_m[l], u_{m+1}[l], z_{m+2}, \ldots, z_q)$$

$$Y = (u_1[l], \ldots, u_m[l], z_{m+1}[l], z'_m+2, \ldots, z'_q)$$
Update of $u_1[j - 1], \ldots, u_m[j - 1]$ at the $j$-th Round

Evaluations determined by the queries to the underlying blockcipher $E_{kj}$
Update of $u_1[j - 1], \ldots, u_m[j - 1]$ at the $j$-th Round

For $i = 1, \ldots, m$:

- $u_i[j - 1] \in \text{Dom}(E_{kj})$
- $u_i[j - 1] \notin \text{Dom}(E_{kj})$
Update of $u_{m+1}[j - 1]$ and $z_{m+1}[j - 1]$ at the $j$-th Round

$u_{m+1}[j - 1] \in \text{Dom}(E_{k_j})$ and $z_{m+1}[j - 1] \in \text{Dom}(E_{k_j})$
Update of $u_{m+1}[j-1]$ and $z_{m+1}[j-1]$ at the $j$-th Round

$u_{m+1}[j-1] \in \text{Dom}(E_{kj})$ and $z_{m+1}[j-1] \notin \text{Dom}(E_{kj})$
Update of $u_{m+1}[j-1]$ and $z_{m+1}[j-1]$ at the $j$-th Round

$u_{m+1}[j-1] \notin \text{Dom}(E_{k_j})$ and $z_{m+1}[j-1] \in \text{Dom}(E_{k_j})$
Update of $u_{m+1}[j-1]$ and $z_{m+1}[j-1]$ at the $j$-th Round

$u_{m+1}[j-1] \notin \text{Dom}(E_{k_j})$ and $z_{m+1}[j-1] \notin \text{Dom}(E_{k_j})$
Defining $z_{m+2}, \ldots, z_q$ and $z'_{m+2}, \ldots, z'_q$

If $u_{m+1}[l] \neq z_{m+1}[l]$

Distinct $z_{m+2}, \ldots, z_q \leftarrow \{0, 1\}^n \setminus \{u^1[l], \ldots, u^m[l], u^{m+1}[l]\}$

Distinct $z'_{m+2}, \ldots, z'_q \leftarrow \{0, 1\}^n \setminus \{u^1[l], \ldots, u^m[l], z^{m+1}[l]\}$

If $u_{m+1}[l] = z_{m+1}[l]$

Distinct $z_{m+2}, \ldots, z_q \leftarrow \{0, 1\}^n \setminus \{u^1[l], \ldots, u^m[l], u^{m+1}[l]\}$

$(z'_{m+2}, \ldots, z'_q) \leftarrow (z_{m+2}, \ldots, z_q)$

$X$ and $Y$ sample the outputs of World $m$ and World $m + 1$, respectively
Upper Bounding $\Pr[X \neq Y]$

$\Pr[X \neq Y] = \Pr[u_{m+1}[l] \neq z_{m+1}[l]]$

$$\leq \prod_{h=1}^{\frac{l}{2}} \Pr \left[ u_{m+1}[2h] \neq z_{m+1}[2h] \bigg| u_{m+1}[2h-2] \neq z_{m+1}[2h-2] \right]$$
Upper Bounding

\[ \Pr \left[ u_{m+1}[2h] \neq z_{m+1}[2h] \biggm| u_{m+1}[2h-2] \neq z_{m+1}[2h-2] \right] \]
Upper Bounding

$$\Pr \left[ u_{m+1}[2h] \neq z_{m+1}[2h] \mid u_{m+1}[2h-2] \neq z_{m+1}[2h-2] \right]$$

- The size of $\text{Dom}(E_{k_{2h-1}})$ and $\text{Dom}(E_{k_{2h}}) \leq M$
  - except with probability $\frac{2q}{M2^\kappa}$
Upper Bounding

\[ \Pr \left[ u_{m+1}[2h] \neq z_{m+1}[2h] \mid u_{m+1}[2h-2] \neq z_{m+1}[2h-2] \right] \]

- Upper bound the probability that one of \( u_{m+1}[2h-2] \) and \( z_{m+1}[2h-2] \) maps into \( \text{Dom}(E_{k_{2h}}) \)
  - By choosing key \( k_{2h-1} \): probability \( \frac{2M\beta}{2^\kappa} \) with a parameter \( \beta \)
  - By random sampling: probability \( \frac{2M}{N} \)
Upper Bounding

\[
\Pr \left[ u_{m+1}[2h] \neq z_{m+1}[2h] \mid u_{m+1}[2h-2] \neq z_{m+1}[2h-2] \right]
\]

- The size of \( \text{Dom}(E_{k_{2h-1}}) \) and \( \text{Dom}(E_{k_{2h}}) \) \( \leq M \)
  - except with probability \( \frac{2q}{M2^\kappa} \)
- Upper bound the probability that one of \( u_{m+1}[2h-2] \) and \( z_{m+1}[2h-2] \) maps into \( \text{Dom}(E_{k_{2h}}) \)
  - By choosing key \( k_{2h-1} \): probability \( \frac{2M\beta}{2^\kappa} \) with a parameter \( \beta \)
  - By random sampling: probability \( \frac{2M}{N} \)

- \( \Pr[X \neq Y] \leq \left( \frac{2q}{M2^\kappa} + \frac{2M\beta}{2^\kappa} + \frac{2M}{N} \right)^{\frac{1}{2}} \)
- Optimize the parameters \( \beta \) and \( M \) to obtain the result
Gazi’s Result (Crypto 2013)

Generic Attacks
- Generic attacks on CE\(^l\) with \(2^{\kappa + \frac{l-1}{n}}\) (resp. \(2^{\kappa + \frac{l-2}{n}}\)) queries for odd (resp. even) length \(l\)
- Generic attacks on XCE\(^l\) with \(2^{\kappa + \frac{l-1}{n}}\) queries

Security Proof
- The security of XCE\(^l\) = the security of a key-alternating ciphers of length \(l - 1\) + key length \(\kappa\)
- XCE\(^l\) is secure up to \(2^{\kappa + \frac{l-1}{n}}\) (resp. \(2^{\kappa + \frac{l-2}{n}}\)) query complexity for odd (resp. even) length \(l\)
Chen and Steinberger’s Result (Eprint Archive)

- Proved a key-alternating cipher of length $l$ is secure up to $2^{\frac{l}{l+1}}n$ queries
- Implies XCE$^l$ is secure up to $2^{\kappa + \frac{l-1}{l}}n$ queries
- Closed the security problem of XCE$^l$
- What about CE$^l$?
Thank You