Range Extension for Weak PRFs

Krzysztof Pietrzak (CWI Amsterdam)
Johan Sjödin(ETH Zürich)
(weak) pseudorandom functions

\[ \mathcal{F} = \{ \mathcal{F}_1, \mathcal{F}_2, \ldots \}, \mathcal{F}_n : \mathcal{K}_n \times \mathcal{X}_n \rightarrow \mathcal{Y}_n \]

is a pseudorandom function (PRF) if

- \( F(k, x) \) can be efficiently computed.
- \( F(k, \cdot) \) (with a random key \( k \in \mathcal{K}_n \)) cannot be efficiently distinguished from a uniformly random function \( \mathcal{R} \).
(weak) pseudorandom functions

\[ \mathcal{F} = \{ \mathcal{F}_1, \mathcal{F}_2, \ldots \}, \mathcal{F}_n : \mathcal{K}_n \times \mathcal{X}_n \to \mathcal{Y}_n \]

is a weak pseudorandom function (wPRF) if

- \( F(k, x) \) can be efficiently computed.
- \( F(k, .) \) (with a random key \( k \in \mathcal{K}_n \)) cannot be efficiently distinguished from a uniformly random function \( \mathcal{R} \) when queried on random inputs.
(weak) pseudorandom functions

\[ \mathcal{F} = \{ \mathcal{F}_1, \mathcal{F}_2, \ldots \}, \mathcal{F}_n : \mathcal{K}_n \times \mathcal{X}_n \rightarrow \mathcal{Y}_n \]

is a weak pseudorandom function (wPRF) if

- \( \mathcal{F}(k, x) \) can be efficiently computed.
- \( \mathcal{F}(k, \cdot) \) (with a random key \( k \in \mathcal{K}_n \)) cannot be efficiently distinguished from a uniformly random function \( \mathcal{R} \) when queried on random inputs.

wPRFs are weaker primitives than PRFs, so relying on the security of a block-cipher like AES as a wPRF is more secure than assuming it to be a PRF.
black-box range extension

Let $C$ be a circuit with oracle gates, such that for any

$$F : \mathcal{K} \times \{0, 1\}^n \rightarrow \{0, 1\}^n$$

we have

$$C_F : \mathcal{K}^t \times \{0, 1\}^{n'} \rightarrow \{0, 1\}^{n\cdot e}$$
Let $C$ be a circuit with oracle gates, such that for any 

$$F : \mathcal{K} \times \{0, 1\}^n \rightarrow \{0, 1\}^n$$

we have 

$$C_F : \mathcal{K}^t \times \{0, 1\}^{n'} \rightarrow \{0, 1\}^{n \cdot e}$$

- $t$ is the key expansion factor of $C$. 
black-box range extension

Let $C$ be a circuit with oracle gates, such that for any

$$F : \mathcal{K} \times \{0, 1\}^n \rightarrow \{0, 1\}^n$$

we have

$$C_F : \mathcal{K}^t \times \{0, 1\}^{n'} \rightarrow \{0, 1\}^{n \cdot e}$$

- $t$ is the key expansion factor of $C$.
- $e$ is the range expansion factor of $C$. 
black-box range extension

Let $C$ be a circuit with oracle gates, such that for any

$$F : \mathcal{K} \times \{0, 1\}^n \rightarrow \{0, 1\}^n$$

we have

$$C_F : \mathcal{K}^t \times \{0, 1\}^{n'} \rightarrow \{0, 1\}^{n \cdot e}$$

- $t$ is the key expansion factor of $C$.
- $e$ is the range expansion factor of $C$.

**Definition**

$C$ is a secure range extension for PRFs, if for any PRFs $F$, also $C_F$ is PRF.
black-box range extension

Let $C$ be a circuit with oracle gates, such that for any

$$F : \mathcal{K} \times \{0, 1\}^n \rightarrow \{0, 1\}^n$$

we have

$$C_F : \mathcal{K}^t \times \{0, 1\}^{n'} \rightarrow \{0, 1\}^{n \cdot e}$$

- $t$ is the key expansion factor of $C$.
- $e$ is the range expansion factor of $C$.

**Definition**

$C$ is a secure range extension for \textit{w}PRFs, if for any \textit{w}PRFs $F$, also $C_F$ is \textit{w}PRF.
For a wPRF $F$ and a secure expansion $C$, $(Enc, Dec)$ as below is a secure encryption scheme.

$Enc(k, M)$ : sample $X$ at random and output 
\[(C_F(k, X) \oplus M, X)\]

$Dec(k, (C, X))$ : output $C_F(k, X) \oplus C$. 

applications
For a wPRF $F$ and a secure expansion $C$, $(Enc, Dec)$ as below is a secure encryption scheme.

$Enc(k, M)$ : sample $X$ at random and output $(C_F(k, X) \oplus M, X)$

$Dec(k, (C, X))$ : output $C_F(k, X) \oplus C$.

Overhead just one block. Key length depends on the key-expansion of $C_F$. 
example 1: parallel evaluation

\[ C_F(\{k_1, \ldots, k_t\}, X) = F(k_1, X), \ldots, F(k_t, X) \]
example 1: parallel evaluation

\[ C_F(\{k_1, \ldots, k_t\}, X) = F(k_1, X), \ldots, F(k_t, X) \]

\[ X \]

\[ F_1 \quad F_2 \quad \ldots \quad F_t \]

+ Secure range extension for PRF and wPRF.
example 1: parallel evaluation

\[
C_F(\{k_1, \ldots, k_t\}, X) = F(k_1, X), \ldots, F(k_t, X)
\]

+ Secure range extension for PRF and wPRF.
- Range expansion = Key expansion (very low).
example 2: parallel evaluation with one key

\[ C_F(k, X) = F(k, X\|[0]), \ldots, F(k, X\|\,[e-1]) \]

\[ e = 2^z, \; X \in \{0, 1\}^{n-z} \]

[i] is binary representation of [i] padded to length z.

```
X
  /\  /\  /\ ...
 X\|[0] X\|[1] X\|[e-1]
  |  |  | ... |
  F  F  F
```
example 2: parallel evaluation with one key

\[ C_F(k, X) = F(k, X||[0]), \ldots, F(k, X||[e - 1]) \]

\( e = 2^z, \ X \in \{0, 1\}^{n-z} \)

[i] is binary representation of [i] padded to length z.

+ Just one key.
example 2: parallel evaluation with one key

\[ C_F(k, X) = F(k, X\|[0]), \ldots, F(k, X\|e - 1) \]

\[ e = 2^z, \ X \in \{0, 1\}^{n-z} \]

[i] is binary representation of [i] padded to length z.

+ Just one key.
+ Secure range extension for PRF.
example 2: parallel evaluation with one key

\[ C_F(k, X) = F(k, X\|[0]), \ldots, F(k, X\|[e - 1]) \]

\[ e = 2^z, \ X \in \{0, 1\}^{n-z} \]

[i] is binary representation of [i] padded to length z.

Just one key.

Secure range extension for PRF.

Not Secure range extension for wPRF.

E.g. for a wPRF where \( F(k, X\|[0]) = F(k, X\|[1]) \).
a general class of range extensions

\[ X \rightarrow F_1 \rightarrow F_2 \rightarrow F_3 \rightarrow C_F[1,12,2,321] \]
a general class of range extensions

Definition

Let \( s = \{s_1, \ldots, s_e\} \), each \( s_i \in \{1, \ldots, t\}^* \). Define

\[
C_F^s(k_1, \ldots, k_t, X) = Y_1, \ldots, Y_e
\]

where \( Y_i \) is computed by applying \( F \) on input \( X \) sequentially as defined by \( s_i \), i.e. with \( m = |s_i| \)

\[
Y_i = F(k_{s_i[m]}, F(k_{s_i[m-1]}, \ldots, F(k_{s_i[1]}, X) \ldots))
\]
a general class of range extensions

Definition

Let \( s = \{s_1, \ldots, s_e\} \), each \( s_i \in \{1, \ldots, t\}^* \). Define

\[
C^s_F(k_1, \ldots, k_t, X) = Y_1, \ldots, Y_e
\]

where \( Y_i \) is computed by applying \( F \) on input \( X \) sequentially as defined by \( s_i \), i.e. with \( m = |s_i| \)

\[
Y_i = F(k_{s_i[m]}, F(k_{s_i[m-1]}, \ldots, F(k_{s_i[1]}, X) \ldots))
\]

All known (efficient) secure range expansion for wPRFs are of this form (like in the previous talk).
a general class of range extensions

Definition

Let \( s = \{s_1, \ldots, s_e\} \), each \( s_i \in \{1, \ldots, t\}^* \). Define

\[
C^s_F(k_1, \ldots, k_t, X) = Y_1, \ldots, Y_e
\]

where \( Y_i \) is computed by applying \( F \) on input \( X \) sequentially as defined by \( s_i \), i.e. with \( m = |s_i| \)

\[
Y_i = F(k_{s_i[m]}, F(k_{s_i[m-1]}, \ldots, F(k_{s_i[1]}, X), \ldots))
\]

All known (efficient) secure range expansion for wPRFs are of this form (like in the previous talk).
For which \( s \) is \( C^s \) a secure range expansion for wPRFs?
Which of $C^{[12,2]}$, $C^{[11,22]}$, $C^{[12,21]}$ is a secure range extension for wPRFs?
Which of $C^{[12,2]}$, $C^{[11,22]}$, $C^{[12,21]}$ is a secure range extension for wPRFs?

$\blacktriangleright$ $C^{[12,2]}$ is secure via a black-box reduction.
Which of $C^{[12,2]}$, $C^{[11,22]}$, $C^{[12,21]}$ is a secure range extension for wPRFs?

- $C^{[12,2]}$ is secure via a black-box reduction.
- $C^{[11,22]}$ is not secure via a black-box reduction.
Which of $C^{[12,2]}$, $C^{[11,22]}$, $C^{[12,21]}$ is a secure range extension for wPRFs?

$\blacktriangleright$ $C^{[12,2]}$ is secure via a black-box reduction.
$\blacktriangleright$ $C^{[11,22]}$ is not secure via a black-box reduction.
$\blacktriangleright$ $C^{[12,21]}$ cannot be proven secure nor insecure via a black-box reduction.
The Good, the Bad and the Ugly [2]

- $C^\alpha, \alpha \subset \mathbb{N}^*$ is good if the security of $C^\alpha$ (as range expansion for wPRFs) can be proven via a black-box reduction.
The Good, the Bad and the Ugly [2]

- $C^\alpha$, $\alpha \subset \mathbb{N}^*$ is good if the security of $C^\alpha$ (as range expansion for wPRFs) can be proven via a black-box reduction.
- $C^\alpha$ is bad if there is a black-box construction $G$, such that for any $F$
  - If $F$ is a wPRF, so is $G^F$.
  - $C^\alpha_{G^F}$ is not a wPRF.
The Good, the Bad and the Ugly [2]

- $C^\alpha$, $\alpha \subset \mathbb{N}^*$ is **good** if the security of $C^\alpha$ (as range expansion for wPRFs) can be proven via a black-box reduction.
- $C^\alpha$ is **bad** if there is a black-box construction $G$, such that for any $F$
  - If $F$ is a wPRF, so is $G^F$.
  - $C^\alpha_{G^F}$ is not a wPRF.
- $C^\alpha$ is **ugly** if it’s not good and not bad.
The Good, the Bad and the Ugly [2]

- $C^\alpha, \alpha \subset \mathbb{N}^*$ is **good** if the security of $C^\alpha$ (as range expansion for wPRFs) can be proven via a black-box reduction.

- $C^\alpha$ is **bad** if there is a black-box construction $G$, such that for any $F$
  - If $F$ is a wPRF, so is $G^F$.
  - $C^\alpha_{G^F}$ is not a wPRF.

- $C^\alpha$ is **ugly** if it’s not good and not bad.

We completely classify $C^\alpha$ (as good, bad or ugly) by simple properties of $\alpha$. 
Theorem (Complete Classification)

\( C^\alpha, \alpha = \{s_1, \ldots, s_t\} \) is

- **bad** if \( \alpha \) contains a string with two consecutive identical letters or two identical strings.
- **good** if it’s not bad and whenever a letter \( c \) appears before a letter \( d \) in some \( s \in \alpha \), then \( d \) does not appear before \( c \) in any string \( s' \in \alpha \).
- **ugly** if it’s not good nor bad.
Theorem (Complete Classification)

\[ C^\alpha, \alpha = \{s_1, \ldots, s_t\} \text{ is} \]

- **bad** if \( \alpha \) contains a string with two consecutive identical letters or two identical strings.
- **good** if it’s not bad and whenever a letter \( c \) appears before a letter \( d \) in some \( s \in \alpha \), then \( d \) does not appear before \( c \) in any string \( s' \in \alpha \).
- **ugly** if it’s not good nor bad.

We sketch the proof only for our three special cases:
The Good: Security via Black-Box Reduction

- $S_0 \rightarrow S_1$ safe replacement.
- $S_1 \rightarrow S_2$ safe replacement.
- $\Delta^K_{q}(S_2, S_3) \leq q^2/|Range|$
The Bad: Black-Box Counterexample

For a pseudorandom permutation* $G$ define $H^G$:

1. if $X = 0 \ldots 0$ then $H^G(k, X) = 0 \ldots 0$
2. Otherwise, let $Y = L Y || R Y = G^{-1}(k, X)$.

$$H^G(X) = \begin{cases} 0 \ldots 0 & \text{if } L Y = 0 \ldots 0 \\ G(k, 0 \ldots 0 || R X) & \text{otherwise} \end{cases}$$

**Lemma**

$H^G(k, .)$ is a wPRF but $H^G(k, H^G(k, .))$ is not.

*A PRP can be constructed from a wPRF via a black-box reduction (GMM then Luby-Rackoff)*
The Ugly

To prove that $C^{[12,21]}$ is ugly, we must show it’s not good and not bad.
The Ugly

To prove that $C^{[12,21]}$ is ugly, we must show it’s not good and not bad.

- If $C^{[12,21]}$ was good, then its security can be proven via a black-box reduction.
The Ugly

To prove that $C^{[12,21]}$ is ugly, we must show it’s not good and not bad.

- If $C^{[12,21]}$ was good, then its security can be proven via a black-box reduction.
- A black-box reduction holds relative to any oracle.
The Ugly

To prove that $C^{[12,21]}$ is ugly, we must show it’s not good and not bad.

- If $C^{[12,21]}$ was good, then its security can be proven via a black-box reduction.
- A black-box reduction holds relative to any oracle.
- So to show $C^{[12,21]}$ is not good we must come up with an oracle $O$ such that
  - relative to $O$ wPRFs $F^O$ exist
  - $C_{F^O}^{[12,21]}$ is not a wPRF.
The Ugly

To prove that $C^{[12,21]}$ is ugly, we must show it’s not good and not bad.

- If $C^{[12,21]}$ was good, then its security can be proven via a black-box reduction.
- A black-box reduction holds relative to any oracle.
- So to show $C^{[12,21]}$ is not good we must come up with an oracle $O$ such that
  - relative to $O$ wPRFs $F^O$ exist
  - $C^{[12,21]}_{F^O}$ is not a wPRF.

- Similarly, to show $C^{[12,21]}$ is not bad we must come up with an oracle $O$ such that relative to $O$ $C^{[12,21]}_{F^O}$ is a wPRF for any wPRF $F^O$. 
The Ugly

To prove that $C^{[12,21]}$ is ugly, we must show it’s not good and not bad.

► If $C^{[12,21]}$ was good, then its security can be proven via a black-box reduction.

► A black-box reduction holds relative to any oracle.

► So to show $C^{[12,21]}$ is not good we must come up with an oracle $O$ such that
  
  ► relative to $O$ wPRFs $F^O$ exist
  ► $C^{[12,21]}_{F^O}$ is not a wPRF.

$O$ will be a generic group oracle.

► Similarly, to show $C^{[12,21]}$ is not bad we must come up with an oracle $O$ such that relative to $O$ $C^{[12,21]}_{F^O}$ is a wPRF for any wPRF $F^O$. $O$ will be a PSPACE oracle.
The Ugly: Insecure under DDH

\[ G = \langle g \rangle : \text{prime order cyclic group where DDH is hard,} \]
\[ \text{then for random } x \in \mathbb{Z}_{|G|} \]
\[ a \overset{F(x,.)}{\rightarrow} a^x \]

is a wPRF, but \( C_F^{[12,21]} \)

\[ a \overset{F(x,.)}{\rightarrow} a^x \overset{F(y,.)}{\rightarrow} a^{xy} \]

\[ a \overset{F(y,.)}{\rightarrow} a^y \overset{F(x,.)}{\rightarrow} a^{xy} \]

is not!
The Ugly: Secure for Quasirandom

- A weak Quasirandom function is the information theoretical analog of wPRFs.
A weak Quasirandom function is the information theoretical analog of wPRFs.

Using the “random systems framework” we show that any ugly $C^\alpha$ is a secure range extension for QRFs.
The Ugly: Secure for Quasirandom

- A weak Quasirandom function is the information theoretical analog of wPRFs.
- Using the “random systems framework” we show that any ugly $C^\alpha$ is a secure range extension for QRFs.
- Relative to a PSPACE oracle, no computational hardness exists, so all wPRFs are QPRs.
The Ugly: Secure for Quasirandom

- A weak Quasirandom function is the information theoretical analog of wPRFs.
- Using the “random systems framework” we show that any ugly $C^\alpha$ is a secure range extension for QRFs.
- Relative to a PSPACE oracle, no computational hardness exists, so all wPRFs are QPRs.
Questions?