Pseudo-OTP

Pseudo-OTP Construction

$\mathcal{K} : \{0,1\}^n$
$\mathcal{M} : \{0,1\}^{\ell(n)}$
$\mathcal{C} : \{0,1\}^{\ell(n)}$

$\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$:
$\mathsf{Gen}(1^n) : k \leftarrow \{0,1\}^n$
$\mathsf{Enc}(k, m) : G(k) \oplus m$
$\mathsf{Dec}(k, c) : G(k) \oplus c$

Pseudo-OTP

Pseudo-OTP Construction

$\mathcal{K} : \{0,1\}^n$
$\mathcal{M} : \{0,1\}^{\ell(n)}$
$\mathcal{C} : \{0,1\}^{\ell(n)}$

$\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$:
$\mathsf{Gen}(1^n) : k \leftarrow \{0,1\}^n$
$\mathsf{Enc}(k, m) : G(k) \oplus m$
$\mathsf{Dec}(k, c) : G(k) \oplus c$

Claim: Assume G is a PRG, then Π is a *fixed length encryption scheme* with indistinguishable encryptions in the presence of an eavesdropper.

Pseudo-OTP

Pseudo-OTP Construction

$\mathcal{K} : \{0,1\}^n$
$\mathcal{M} : \{0,1\}^{\ell(n)}$
$\mathcal{C} : \{0,1\}^{\ell(n)}$

$\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$:
$\mathsf{Gen}(1^n) : k \leftarrow \{0,1\}^n$
$\mathsf{Enc}(k, m) : G(k) \oplus m$
$\mathsf{Dec}(k, c) : G(k) \oplus c$

Claim: Assume G is a PRG, then Π is a *fixed length encryption scheme* with indistinguishable encryptions in the presence of an eavesdropper.

If *insecure*: $\exists$ p.p.t. $\mathcal{A}, p(n)$ such that $\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n) = 1] \geq \frac{1}{2} + \frac{1}{p(n)}$

Pseudo-OTP

Pseudo-OTP Construction

$\mathcal{K} : \{0,1\}^n$
$\mathcal{M} : \{0,1\}^{\ell(n)}$
$\mathcal{C} : \{0,1\}^{\ell(n)}$

$\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$:
$\mathsf{Gen}(1^n) : k \leftarrow \{0,1\}^n$
$\mathsf{Enc}(k, m) : G(k) \oplus m$
$\mathsf{Dec}(k, c) : G(k) \oplus c$

Claim: Assume G is a PRG, then Π is a *fixed length encryption scheme* with indistinguishable encryptions in the presence of an eavesdropper.

If *insecure*: $\exists$ p.p.t. $\mathcal{A}, p(n)$ such that $\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n) = 1] \geq \frac{1}{2} + \frac{1}{p(n)}$

If *secure*: $\forall$ p.p.t. $\mathcal{A}, p(n)$, $\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n) = 1] < \frac{1}{2} + \frac{1}{p(n)}$

Pseudo-OTP

Pseudo-OTP Construction

$\mathcal{K} : \{0,1\}^n$
$\mathcal{M} : \{0,1\}^{\ell(n)}$
$\mathcal{C} : \{0,1\}^{\ell(n)}$

$\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$:
$\text{Gen}(1^n) : k \leftarrow \{0,1\}^n$
$\text{Enc}(k, m) : G(k) \oplus m$
$\text{Dec}(k, c) : G(k) \oplus c$

Claim: Assume G is a PRG, then Π is a *fixed length encryption scheme* with indistinguishable encryptions in the presence of an eavesdropper.

If *insecure*: $\exists$ p.p.t. $\mathcal{A}, p(n)$ such that $\Pr[\text{PrivK}^{\text{eav}}_{\mathcal{A},\Pi}(n) = 1] \geq \frac{1}{2} + \frac{1}{p(n)}$

If *secure*: $\forall$ p.p.t. $\mathcal{A}, p(n)$, $\Pr[\text{PrivK}^{\text{eav}}_{\mathcal{A},\Pi}(n) = 1] < \frac{1}{2} + \frac{1}{p(n)}$

Equivalently: $\forall$ p.p.t. $\mathcal{A}$, $\exists$negl(n) such that $\Pr[\text{PrivK}^{\text{eav}}_{\mathcal{A},\Pi}(n) = 1] < \frac{1}{2} + \text{negl(n)}$

Pseudo-OTP

Pseudo-OTP Construction

$\mathcal{K} : \{0,1\}^n$
$\mathcal{M} : \{0,1\}^{\ell(n)}$
$\mathcal{C} : \{0,1\}^{\ell(n)}$

$\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$:
$\text{Gen}(1^n) : k \leftarrow \{0,1\}^n$
$\text{Enc}(k, m) : G(k) \oplus m$
$\text{Dec}(k, c) : G(k) \oplus c$

Claim: Assume G is a PRG, then Π is a *fixed length encryption scheme* with indistinguishable encryptions in the presence of an eavesdropper.

If *insecure*: $\exists$ p.p.t. $\mathcal{A}, p(n)$ such that $\Pr[\text{PrivK}^{\text{eav}}_{\mathcal{A},\Pi}(n) = 1] \geq \frac{1}{2} + \frac{1}{p(n)}$

If *secure*: $\forall$ p.p.t. $\mathcal{A}, p(n)$, $\Pr[\text{PrivK}^{\text{eav}}_{\mathcal{A},\Pi}(n) = 1] < \frac{1}{2} + \frac{1}{p(n)}$

Equivalently: $\forall$ p.p.t. $\mathcal{A}$, $\exists$negl(n) such that $\Pr[\text{PrivK}^{\text{eav}}_{\mathcal{A},\Pi}(n) = 1] < \frac{1}{2} + \text{negl(n)}$

Suppose the contrary:
$\exists$ p.p.t. $\mathcal{A}, p(n)$ such that $\Pr[\text{PrivK}^{\text{eav}}_{\mathcal{A},\Pi}(n) = 1] \geq \frac{1}{2} + \frac{1}{p(n)}$.

We will show that under this assumption that such an $\mathcal{A}$ exists,
$\exists$ p.p.t. $\mathcal{A}_r, q(n)$ such that $\Pr[\text{PrivK}^{\text{prg}}_{\mathcal{A}_r,\text{G}}(n) = 1] \geq \frac{1}{2} + \frac{1}{q(n)}$.

Pseudo-OTP

Pseudo-OTP Construction

$\mathcal{K} : \{0,1\}^n$
$\mathcal{M} : \{0,1\}^{\ell(n)}$
$\mathcal{C} : \{0,1\}^{\ell(n)}$

$\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$:
$\text{Gen}(1^n) : k \leftarrow \{0,1\}^n$
$\text{Enc}(k, m) : G(k) \oplus m$
$\text{Dec}(k, c) : G(k) \oplus c$

Claim: Assume G is a PRG, then Π is a *fixed length encryption scheme* with indistinguishable encryptions in the presence of an eavesdropper.

If *insecure*: $\exists$ p.p.t. $\mathcal{A}, p(n)$ such that $\Pr[\text{PrivK}^{\text{eav}}_{\mathcal{A},\Pi}(n) = 1] \geq \frac{1}{2} + \frac{1}{p(n)}$

If *secure*: $\forall$ p.p.t. $\mathcal{A}, p(n)$, $\Pr[\text{PrivK}^{\text{eav}}_{\mathcal{A},\Pi}(n) = 1] < \frac{1}{2} + \frac{1}{p(n)}$

Equivalently: $\forall$ p.p.t. $\mathcal{A}$, $\exists$negl(n) such that $\Pr[\text{PrivK}^{\text{eav}}_{\mathcal{A},\Pi}(n) = 1] < \frac{1}{2} + \text{negl(n)}$

Suppose the contrary:
$\exists$ p.p.t. $\mathcal{A}, p(n)$ such that $\Pr[\text{PrivK}^{\text{eav}}_{\mathcal{A},\Pi}(n) = 1] \geq \frac{1}{2} + \frac{1}{p(n)}$.

We will show that under this assumption that such an $\mathcal{A}$ exists,
$\exists$ p.p.t. $\mathcal{A}_r, q(n)$ such that $\Pr[\text{PrivK}^{\text{prg}}_{\mathcal{A}_r,\text{G}}(n) = 1] \geq \frac{1}{2} + \frac{1}{q(n)}$.

Put more simply (and informally):
If there exists an adversary $\mathcal{A}$ breaking Π, then
there exists an adversary $\mathcal{A}_r$ breaking G.

Pseudo-OTP

Pseudo-OTP Construction

$\mathcal{K} : \{0,1\}^n$
$\mathcal{M} : \{0,1\}^{\ell(n)}$
$\mathcal{C} : \{0,1\}^{\ell(n)}$

$\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$:
$\text{Gen}(1^n) : k \leftarrow \{0,1\}^n$
$\text{Enc}(k, m) : G(k) \oplus m$
$\text{Dec}(k, c) : G(k) \oplus c$

Claim: Assume G is a PRG, then Π is a *fixed length encryption scheme* with indistinguishable encryptions in the presence of an eavesdropper.

If *insecure*: $\exists$ p.p.t. $\mathcal{A}, p(n)$ such that $\Pr[\text{PrivK}^{\text{eav}}_{\mathcal{A},\Pi}(n) = 1] \geq \frac{1}{2} + \frac{1}{p(n)}$

If *secure*: $\forall$ p.p.t. $\mathcal{A}, p(n)$, $\Pr[\text{PrivK}^{\text{eav}}_{\mathcal{A},\Pi}(n) = 1] < \frac{1}{2} + \frac{1}{p(n)}$

Equivalently: $\forall$ p.p.t. $\mathcal{A}$, $\exists$negl(n) such that $\Pr[\text{PrivK}^{\text{eav}}_{\mathcal{A},\Pi}(n) = 1] < \frac{1}{2} + \text{negl(n)}$

Suppose the contrary:
$\exists$ p.p.t. $\mathcal{A}, p(n)$ such that $\Pr[\text{PrivK}^{\text{eav}}_{\mathcal{A},\Pi}(n) = 1] \geq \frac{1}{2} + \frac{1}{p(n)}$.

We will show that under this assumption that such an $\mathcal{A}$ exists,
$\exists$ p.p.t. $\mathcal{A}_r, q(n)$ such that $\Pr[\text{PrivK}^{\text{prg}}_{\mathcal{A}_r,\text{G}}(n) = 1] \geq \frac{1}{2} + \frac{1}{q(n)}$.

We will use the existence of $\mathcal{A}$ to construct $\mathcal{A}_r$ that breaks G.

Pseudo-OTP

Pseudo-OTP Construction

$\mathcal{K} : \{0,1\}^n$
$\mathcal{M} : \{0,1\}^{\ell(n)}$
$\mathcal{C} : \{0,1\}^{\ell(n)}$

$\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$:
$\text{Gen}(1^n) : k \leftarrow \{0,1\}^n$
$\text{Enc}(k, m) : G(k) \oplus m$
$\text{Dec}(k, c) : G(k) \oplus c$

Claim: Assume G is a PRG, then Π is a *fixed length encryption scheme* with indistinguishable encryptions in the presence of an eavesdropper.

If *insecure*: $\exists$ p.p.t. $\mathcal{A}, p(n)$ such that $\Pr[\text{PrivK}^{\text{eav}}_{\mathcal{A},\Pi}(n) = 1] \geq \frac{1}{2} + \frac{1}{p(n)}$

If *secure*: $\forall$ p.p.t. $\mathcal{A}, p(n)$, $\Pr[\text{PrivK}^{\text{eav}}_{\mathcal{A},\Pi}(n) = 1] < \frac{1}{2} + \frac{1}{p(n)}$

Equivalently: $\forall$ p.p.t. $\mathcal{A}$, $\exists$negl(n) such that $\Pr[\text{PrivK}^{\text{eav}}_{\mathcal{A},\Pi}(n) = 1] < \frac{1}{2} + \text{negl(n)}$

Suppose the contrary:
$\exists$ p.p.t. $\mathcal{A}, p(n)$ such that $\Pr[\text{PrivK}^{\text{eav}}_{\mathcal{A},\Pi}(n) = 1] \geq \frac{1}{2} + \frac{1}{p(n)}$.

We will show that under this assumption that such an $\mathcal{A}$ exists,
$\exists$ p.p.t. $\mathcal{A}_r, q(n)$ such that $\Pr[\text{PrivK}^{\text{prg}}_{\mathcal{A}_r,\text{G}}(n) = 1] \geq \frac{1}{2} + \frac{1}{q(n)}$.

We will use the existence of $\mathcal{A}$ to construct $\mathcal{A}_r$ that breaks G.

Since we assume that G is a PRG, we arrive at a contradiction. Therefore, $\mathcal{A}$ must not exist!