Odds and ends

Key Derivation

Deriving many keys from one

Typical scenario. a single source key (SK) is sampled from:

- Hardware random number generator
- A key exchange protocol (discussed later)

Need many keys to secure session:

- unidirectional keys; multiple keys for nonce-based CBC.

Goal: generate many keys from this one source key

When source key is uniform

F: a PRF with key space K and outputs in $\{0,1\}^n$

Suppose source key SK is uniform in K

- Define Key Derivation Function (KDF) as:

KDF(SK, CTX, L) :=

$F(SK, (\mathbf{CTX} \,\|\, \mathbf{0})) \,\|\, F(SK, (\mathbf{CTX} \,\|\, \mathbf{1})) \,\|\, \cdots \,\|\, F(SK, (\mathbf{CTX} \,\|\, \mathbf{L}))$

CTX: a string that uniquely identifies the application

KDF(SK, CTX, L) :=

F(SK, (**CTX || 0**)) || F(SK, (**CTX || 1**)) || … || F(SK, (**CTX || L**))

What is the purpose of CTX?

- ○ Even if two apps sample same SK they get indep. keys
- ○ It's good practice to label strings with the app. name
- ○ It serves no purpose
- ○

What if source key is not uniform?

Recall: PRFs are pseudo random only when key is uniform in K

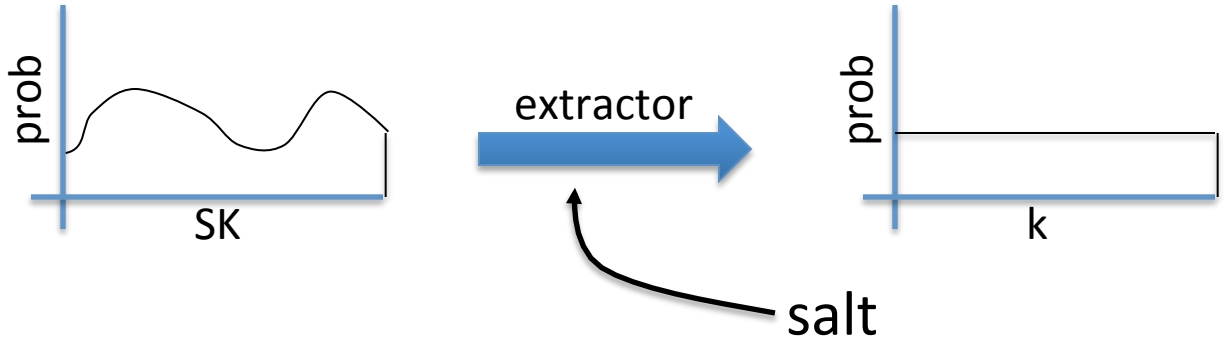
- SK not uniform $\Rightarrow$ PRF output may not look random

Source key often not uniformly random:

- Key exchange protocol: key uniform in some subset of K
- Hardware RNG: may produce biased output

Extract-then-Expand paradigm

Step 1: **extract** pseudo-random key k from source key SK



salt: a fixed non-secret string chosen at random

step 2: **expand** k by using it as a PRF key as before

HKDF: a KDF from HMAC

Implements the extract-then-expand paradigm:

- extract: use **$k \leftarrow$ HMAC(salt, SK)**

- Then expand using HMAC as a PRF with key **k**

Password-Based KDF (PBKDF)

Deriving keys from passwords:

- Do not use HKDF: passwords have insufficient entropy
- Derived keys will be vulnerable to dictionary attacks

(more on this later)

PBKDF defenses: **salt** and a **slow hash function**

Standard approach: **PKCS#5** (PBKDF1)

$H^{(c)}$(pwd || salt): iterate hash function c times

End of Segment