An Immediate Multi-Party Generalization of ID-NIKE from Constrained PRF

Ruxandra F. Olimid and **Dragoș Alin Rotaru**

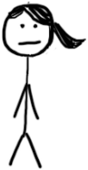
University of Bucharest

September 16, 2014

Asymmetric Crypto Overview

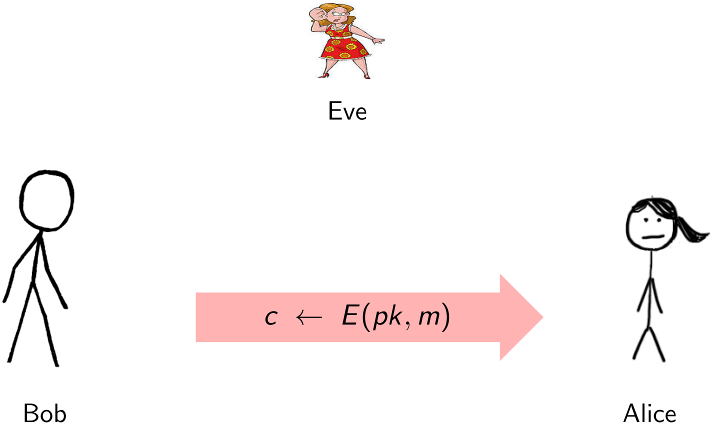
Eve

Bob



Alice

Asymmetric Crypto Overview



Asymmetric Crypto Overview

Eve

I know the message!

$c \leftarrow E(pk, m)$

Bob

Alice

Asymmetric Crypto Overview

Eve

I know the message!

Bob

$$c \leftarrow E(pk, m)$$

Alice

$$m \leftarrow D(sk, c)$$

Asymmetric Crypto Overview

Eve

?

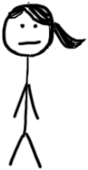
$c \leftarrow E(pk, m)$

Bob

Alice

Eve

$c \leftarrow E(Bob@ex.com, m)$



Bob

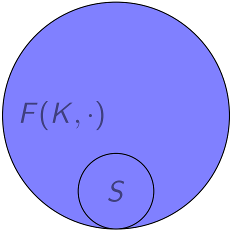
Alice

Constrained PRF

Definition

A PRF is a function $F : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$ such that there is a polynomial algorithm to evaluate $F(k, \cdot)$, $k \in \mathcal{K}$

- A constrained PRF (cPRF) is similar to a PRF, with an additional set of constrained keys $\mathcal{K}_c$ such that a key $k_s \in \mathcal{K}_c$ enables the evaluation of F only in a certain subset $S \in \mathcal{X}$.



Left/Right cPRF, Bit-Fixing cPRF

Definition

Let $F : \mathcal{K} \times \mathcal{X}^2 \to \mathcal{Y}$ be a PRF. Then, $\forall w \in \mathcal{X}$, a left/right cPRF supports two constrained keys k_w^L and k_w^R that enable the evaluation of F at all points $(w, x) \in \mathcal{X}^2$, respectively $(x, w) \in \mathcal{X}^2$.

Left/Right cPRF, Bit-Fixing cPRF

Definition

Let $F : \mathcal{K} \times \mathcal{X}^2 \to \mathcal{Y}$ be a PRF. Then, $\forall w \in \mathcal{X}$, a left/right cPRF supports two constrained keys k_w^L and k_w^R that enable the evaluation of F at all points $(w, x) \in \mathcal{X}^2$, respectively $(x, w) \in \mathcal{X}^2$.

Definition

Let $F : \mathcal{K} \times \{0, 1\}^N \to \mathcal{Y}$ be a PRF. Then, $\forall v \in \{0, 1, ?\}^N$, a bit-fixing cPRF supports a constrained key k_v that enables the evaluation of F at all points $x \in \{0, 1\}^N$ that satisfy the pattern v.

Left/Right cPRF, Bit-Fixing cPRF

Definition

Let $F : \mathcal{K} \times \mathcal{X}^2 \to \mathcal{Y}$ be a PRF. Then, $\forall w \in \mathcal{X}$, a left/right cPRF supports two constrained keys k_w^L and k_w^R that enable the evaluation of F at all points $(w, x) \in \mathcal{X}^2$, respectively $(x, w) \in \mathcal{X}^2$.

Definition

Let $F : \mathcal{K} \times \{0,1\}^N \to \mathcal{Y}$ be a PRF. Then, $\forall v \in \{0,1,?\}^N$, a bit-fixing cPRF supports a constrained key k_v that enables the evaluation of F at all points $x \in \{0,1\}^N$ that satisfy the pattern v.

Example

When $v := 0?1$, $k_{0?1}$ enables the evalation of $F(k_{0?1}, 011)$ and $F(k_{0?1}, 001)$

Boneh-Waters ID-NIKE [BW'13]

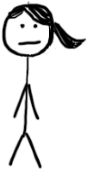
Bob

Alice

Boneh-Waters ID-NIKE [BW'13]

$F(k_{Bob}, (Bob, \cdot))$
$F(k_{Bob}, (\cdot, Bob))$

Bob



Alice

Boneh-Waters ID-NIKE [BW'13]

$F(k_{Bob}, (Bob, \cdot))$
$F(k_{Bob}, (\cdot, Bob))$

$F(k_{Alice}, (Alice, \cdot))$
$F(k_{Alice}, (\cdot, Alice))$

Bob

Alice

Boneh-Waters ID-NIKE [BW'13]

We have a common secret key:
$F(k_{Alice}, (Alice, Bob))$

$F(k_{Bob}, (Bob, \cdot))$
$F(k_{Bob}, (\cdot, Bob))$

$F(k_{Alice}, (Alice, \cdot))$
$F(k_{Alice}, (\cdot, Alice))$

Bob

Alice

Boneh-Waters ID-NIKE [BW'13]

- $\text{Setup}(\lambda)$:
  - let $F : \mathcal{K} \times \mathcal{X}^2 \to \mathcal{Y}$ be $PRF^{L/R}$, $msk \leftarrow^R \mathcal{K}$
  - outputs msk
- $\text{Extract}(msk, id_i)$:
  - computes $\text{F.constrain}(msk, \{(id_i, \cdot)\})$ to obtain $k^L_{id_i}$ and $\text{F.constrain}(msk, \{(\cdot, id_i)\})$ to obtain $k^R_{id_i}$
  - outputs $sk_{id_i} = (k^L_{id_i}, k^R_{id_i})$
- $\text{KeyGen}(sk_{id_i}, id_j)$ outputs:

$$k_{id_i,id_j} = \begin{cases} F(msk, (id_i, id_j)) & \text{if} \quad id_i < id_j \\ F(msk, (id_j, id_i)) & \text{if} \quad id_i > id_j \end{cases}$$

Multi-Party ID-NIKE from cPRF

$F(k_{Bob}, (Bob, \cdot, \cdot))$
$F(k_{Bob}, (\cdot, Bob, \cdot))$
$F(k_{Bob}, (\cdot, \cdot, Bob))$

Bob

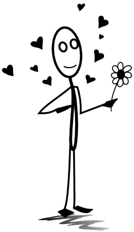
$F(k_{Alice}, (Alice, \cdot, \cdot))$
$F(k_{Alice}, (\cdot, Alice, \cdot))$
$F(k_{Alice}, (\cdot, \cdot, Alice))$

Alice

Multi-Party ID-NIKE from cPRF

$$F(k_{Bob}, (Bob, \cdot, \cdot))$$
$$F(k_{Bob}, (\cdot, Bob, \cdot))$$
$$F(k_{Bob}, (\cdot, \cdot, Bob))$$

Bob



John

$$F(k_{Alice}, (Alice, \cdot, \cdot))$$
$$F(k_{Alice}, (\cdot, Alice, \cdot))$$
$$F(k_{Alice}, (\cdot, \cdot, Alice))$$

Alice

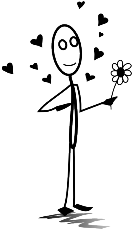
Multi-Party ID-NIKE from cPRF

$$F(k_{Bob}, (Bob, \cdot, \cdot))$$
$$F(k_{Bob}, (\cdot, Bob, \cdot))$$
$$F(k_{Bob}, (\cdot, \cdot, Bob))$$

$$F(k_{John}, (John, \cdot, \cdot))$$
$$F(k_{John}, (\cdot, John, \cdot))$$
$$F(k_{John}, (\cdot, \cdot, John))$$

$$F(k_{Alice}, (Alice, \cdot, \cdot))$$
$$F(k_{Alice}, (\cdot, Alice, \cdot))$$
$$F(k_{Alice}, (\cdot, \cdot, Alice))$$

Bob



John

Alice

Multi-Party ID-NIKE from cPRF

$F(k_{Bob}, (Bob, \cdot, \cdot))$
$F(k_{Bob}, (\cdot, Bob, \cdot))$
$F(k_{Bob}, (\cdot, \cdot, Bob))$

Bob

$F(k_{John}, (John, \cdot, \cdot))$
$F(k_{John}, (\cdot, John, \cdot))$
$F(k_{John}, (\cdot, \cdot, John))$

John

$F(k_{Alice}, (Alice, \cdot, \cdot))$
$F(k_{Alice}, (\cdot, Alice, \cdot))$
$F(k_{Alice}, (\cdot, \cdot, Alice))$

Alice

Secret Shared Key:
$F(k_{Alice}, (Alice, Bob, John))$

Multi-Party ID-NIKE from cPRF

- $\mathrm{Setup}(\lambda)$:
  - let $F : \mathcal{K} \times \mathcal{X}^N \to \mathcal{Y}$ be PRF^{bf}, $msk \leftarrow^R \mathcal{K}$
  - outputs msk
- $\mathrm{Extract}(msk, id_i)$:
  - computes $\mathrm{F.constrain}(msk, \{(id_i, \cdot, \ldots, \cdot)\})$ to obtain $k^1_{id_i}$, $\mathrm{F.constrain}(msk, \{(\cdot, id_i, \cdot, \ldots, \cdot)\})$ to obtain $k^2_{id_i}$, $\cdots$, $\mathrm{F.constrain}(msk, \{(\cdot, \ldots, \cdot, id_i)\})$ to obtain $k^N_{id_i}$
  - outputs $sk_{id_i} = (k^1_{id_i}, \ldots, k^N_{id_i})$
- $\mathrm{KeyGen}(sk_{id_i}, \{id_1, \ldots, id_N\})$ outputs:

$$k_{id_1,\ldots,id_N} = F(msk, (id_{\pi(1)}, id_{\pi(2)}, \ldots, id_{\pi(N)}))$$

where $id_{\pi(1)} < id_{\pi(2)} < \cdots < id_{\pi(N)}$ (in lexicographic order)

Thank you!