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

Ruxandra F. Olimid and Dragoş Alin Rotaru

University of Bucharest, Romania
ruxandra.olimid@fmi.unibuc.ro,r.dragos0@gmail.com

Abstract. Constrained pseudorandom functions are pseudorandom functions that admit constrained keys to evaluate the function on predefined subsets of the domain, while in rest they remain secure. Boneh and Waters used this concept to introduce a two-party identity-based non-interactive key exchange. Our work reviews their construction and considers a straightforward extension to multi-party settings.

Keywords: pseudorandom functions, non-interactive key exchange

1 Introduction

Constrained pseudorandom functions (cPRF) were recently (and independently) introduced by Boneh and Waters [1], Kiayias et al. [2] and Boyle et al. [3]. In a traditional PRF there exists a key that enables the evaluation of the function at all points of the domain; a cPRF extends this capability and allows the derivation of constrained keys that enable the evaluation of the function at predefined subsets of the domain, while in rest it remains secure.

Boneh and Waters used this concept to construct an identity-based non-interactive key exchange (ID-NIKE) [1]. NIKE is an important cryptographic primitive that allows distinct users to share a common secret key without being online in the same time (i.e. NIKE does not require interaction between parties), a property often required in practice. The key is subsequently used for cryptographic purposes (e.g. encrypted communication). Nowadays, applications like digital conferences, collaborative work and shared access to resources impose the necessity of multi-party key exchange. Although Diffie and Hellman defined a two-party NIKE back in 1976 [4], the existence of a multi-party NIKE is one of the most famous open-problems in cryptography. In 2003 Joux extended Diffie-Hellman protocol to three parties by using bilinear maps [5]; Boneh and Silverberg defined multi-party NIKE under the multi-linear assumptions [6], but no multi-linear candidates where proposed until very recently.

Identity-based cryptography allows a party to use his identity (e.g. name, email addresses, phone numbers) instead of generating and properly authenticate a public key. A NIKE protocol in the ID-settings is preferred in mobile or wireless networks where energy preserving is a main concern due to a significant reduction in comparison to PKI-based protocols [7].

2 Constrained PRF

We review the notions from [1], but restrict to the particular types of cPRF and the informal security definition of cPRF, which we use through our work.

A cPRF function F is similar to a standard PRF $F : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$ (where $\mathcal{K}$ denotes the key space) 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 of $\mathcal{X}$. Analogues to the standard PRF, a cPRF is secure if no probabilistic polynomial-time (PPT) adversary $\mathcal{B}$ can distinguish between the value of the function and a uniformly random chosen value in $\mathcal{Y}$, even if $\mathcal{B}$ is given evaluations at points and constrained keys on his choice; i.e. for $k \in \mathcal{K}$ fixed, $\mathcal{B}$ has access to two oracles: (1) $\mathsf{F.eval}(x)$ returns $F(k, x)$, the evaluation of F at x and (2) $\mathsf{F.constrain}(S)$ returns the constrained key k_S that enables the evaluation of F at any $x \in S$. To eliminate trivial win, $\mathcal{B}$ is not allowed to make any real-or-random challenge at points x he can evaluate by himself (i.e. he queried $\mathsf{F.eval}(x)$ or $\mathsf{F.constrain}(S)$, such that $x \in S$).

Definition 1. *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 $(w, x) \in \mathcal{X}^2$ (the left part is fixed), respectively $(x, w) \in \mathcal{X}^2$ (the right part is fixed). We denote a left/right cPRF by $PRF^{L/R}$.*

Definition 2. *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. We denote a bit-fixing cPRF by PRF^{bf}.*

3 ID-NIKE from cPRF

Fig.1 reviews the Boneh-Waters ID-NIKE from left/right cPRF [1].

$\mathsf{Setup}(\lambda)$: let $F : \mathcal{K} \times \mathcal{X}^2 \to \mathcal{Y}$ be a secure left/right PRF, selects a random master secret key $msk \leftarrow^R \mathcal{K}$ and outputs the public parameters of the cPRF as $params$;
$\mathsf{Extract}(msk, id_i)$: computes $\mathsf{F.constrain}(msk, \{(id_i, \cdot)\})$ to obtain $k_{id_i}^L$ and $\mathsf{F.constrain}(msk, \{(\cdot, id_i)\})$ to obtain $k_{id_i}^R$, then outputs $sk_{id_i} = (k_{id_i}^L, k_{id_i}^R)$;
$\mathsf{KeyGen}(params, sk_{id_i}, id_j)$: outputs $F(msk, (id_i, id_j))$ if $id_i < id_j$ and $F(msk, (id_j, id_i))$ if $id_i > id_j$ (in lexicographic order).

Fig. 1. Boneh-Waters ID-NIKE [1]

Correctness. For correctness, we require that both parties obtain the same key. This follows directly from the correctness of the left/right cPRF: WLOG

let $id_i < id_j$; the party identified by id_i uses $k^L_{id_i}$ to evaluate $F(msk, (id_i, \cdot))$ at id_j and the party identified by id_j uses $k^R_{id_j}$ to evaluate $F(msk, (\cdot, id_j))$ at id_i.

Security. We skip the security proof, but invite the reader to address the original paper [1].

4 Multi-Party ID-NIKE from cPRF

A generalization of Boneh-Waters ID-NIKE to N parties ($N > 2$) is immediate: each party receives a N-tuple of constrained keys $\{k^1_{id_i}, \ldots k^N_{id_i}\}$ that enable the evaluation of F at all points of $\mathcal{X}^N$ that contain id_i. The construction uses a natural approach: it replaces the left/right cPRF by the bit-fixing cPRF.

Fig.2 introduces the multi-party ID-NIKE.

$\mathsf{Setup}(\lambda)$: let $F : \mathcal{K} \times \mathcal{X}^N \to \mathcal{Y}$ be a secure bit-fixing cPRF, selects a random master secret key $msk \leftarrow^R \mathcal{K}$ and outputs the public parameters of the cPRF as $params$;
$\mathsf{Extract}(msk, id_i)$: computes $\mathsf{F.constrain}(msk, \{(id_i, \cdot, \ldots, \cdot)\})$ to obtain $k^1_{id_i}$,
$\mathsf{F.constrain}(msk, \{(\cdot, id_i, \cdot, \ldots, \cdot)\})$ to obtain $k^2_{id_i}$, $\cdots$,
$\mathsf{F.constrain}(msk, \{(\cdot, \ldots, \cdot, id_i)\})$ to obtain $k^N_{id_i}$,
then outputs $sk_{id_i} = (k^1_{id_i}, \ldots, k^N_{id_i})$;
$\mathsf{KeyGen}(params, sk_{id_i}, \{id_1, \ldots, id_N\})$: outputs $F(msk, (id_{\pi(1)}, id_{\pi(2)}, \ldots, id_{\pi(N)}))$, where $id_{\pi(1)} < id_{\pi(2)} < \cdots < id_{\pi(N)}$ (in lexicographic order).

Fig. 2. Multi-party ID-NIKE

We remark that the construction allows any $M < N$ parties to share a key by replacing a missing id with a dummy value id_{dummy}. As a major drawback of the scheme, the private key sk_{id_i} is linear in the number of parties N.

Correctness. For correctness, we require that all parties obtain the same key. This follows directly from the correctness of the bit-fixing cPRF: each party identified by id_i uses $k^{\pi(i)}_{id_i}$ to evaluate F at $(id_{\pi(1)}, \ldots, id_{\pi(N)})$.

Security. The security definition for multi-party ID-NIKE can be seen as a natural generalization of ID-NIKE security model, hence we only describe it informally. A multi-party ID-NIKE is secure if no PPT adversary $\mathcal{A}$ can distinguish between the shared key of a set of parties and a uniformly random chosen value in the key space, even if $\mathcal{A}$ is given private keys of some of the parties and shared keys on his choice; i.e. for $k \in \mathcal{K}$ fixed, $\mathcal{A}$ has access to two oracles: (1) $\mathsf{Ext}(id_i)$ returns the secret key sk_{id_i} and (2) $\mathsf{Rev}(id_1, \ldots, id_N)$ returns the shared key $k_{id_1,\ldots,id_N}$. To eliminate trivial win, $\mathcal{A}$ is not allowed to make any real-or-random challenge at groups of identities $(id_1, \ldots, id_N)$ he can evaluate by himself (i.e. $\mathcal{A}$ queried $\mathsf{Rev}(id_1, \ldots, id_N)$ or $\mathsf{Ext}(id_i)$, such that $id_i \in \{id_1, \ldots, id_N\}$). We denote a real-or-random challenge as a Test query.

The security of the system derives from the security of the bit-fixing cPRF (as a straightforward generalization of the Boneh-Waters ID-NIKE security proof). The proof is complete if an adversary $\mathcal{B}$ against the bit-fixing cPRF perfectly simulates the adversary $\mathcal{A}$ against the multi-party ID-NIKE. Whenever $\mathcal{A}$ makes a query in the multi-party ID-NIKE security game, $\mathcal{B}$ makes a query in the constrained security game and returns the answer to $\mathcal{A}$:

- $\mathsf{Ext}(id_i)$: $\mathcal{B}$ queries $\mathsf{F.Constrain}$ oracle on S, where S denotes the set of all points of $\mathcal{X}^N$ that contain id_i and returns the answer to $\mathcal{A}$;
- $\mathsf{Rev}(id_1, \ldots, id_N)$: $\mathcal{B}$ queries $\mathsf{F.Eval}$ oracle on $(id_{\pi(1)}, id_{\pi(2)}, \ldots, id_{\pi(N)})$ and returns the answer to $\mathcal{A}$;
- $\mathsf{Test}(id_1, \ldots, id_N)$: $\mathcal{B}$ makes a real-or-random challenge to the cPRF oracle and returns the answer to $\mathcal{A}$.

Note that $\mathcal{B}$ can always ask for a correct challenge, since all Rev and Test queries are distinct and no Ext is allowed for an identity in Test. Therefore, if $\mathcal{A}$ can distinguish the correct shared key $F(msk, (id_{\pi(1)}, id_{\pi(2)}, \ldots, id_{\pi(N)}))$ from random, then $\mathcal{B}$ can solve the challenge in the constrained security game.

Acknowledgements. Ruxandra F. Olimid was supported by the strategic grant POSDRU/159/1.5/S/137750, Project Doctoral and Postdoctoral programs support for increased competitiveness in Exact Sciences research cofinanced by the European Social Found within the Sectorial Operational Program Human Resources Development 2007-2013.

References

1. Boneh, D., Waters, B.: Constrained pseudorandom functions and their applications. In: ASIACRYPT (2). (2013) 280–300
2. Kiayias, A., Papadopoulos, S., Triandopoulos, N., Zacharias, T.: Delegatable pseudorandom functions and applications. In: ACM Conference on Computer and Communications Security. (2013) 669–684
3. Boyle, E., Goldwasser, S., Ivan, I.: Functional signatures and pseudorandom functions. In: Public Key Cryptography. (2014) 501–519
4. Diffie, W., Hellman, M.E.: New directions in cryptography. IEEE Trans. on Info. Theory **22** (1976) 644–654
5. Joux, A.: A one round protocol for tripartite diffie-hellman. J. Cryptology **17** (2004) 263–276
6. Boneh, D., Silverberg, A.: Applications of multilinear forms to cryptography. Contemporary Mathematics **324** (2003) 71–90
7. Capar, C., Goeckel, D., Paterson, K.G., Quaglia, E.A., Towsley, D., Zafer, M.: Signal-flow-based analysis of wireless security protocols. Inf. Comput. **226** (2013) 37–56