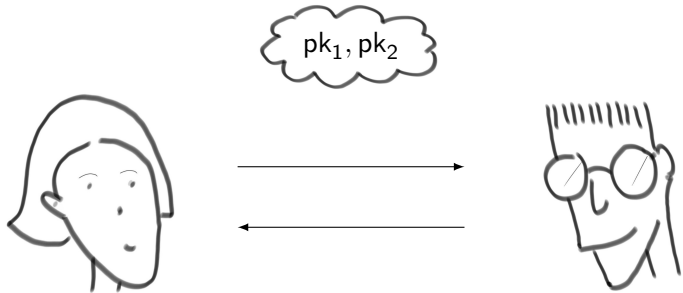
On Tightly Secure Non-Interactive Key Exchange

Julia Hesse (Technische Universität Darmstadt)
Dennis Hofheinz (Karlsruhe Institute of Technology)
Lisa Kohl (Karlsruhe Institute of Technology)

Non-Interactive Key Exchange (NIKE)



$(\mathsf{pk}_1, \mathsf{sk}_1) \leftarrow \texttt{KeyGen}$ $(\mathsf{pk}_2, \mathsf{sk}_2) \leftarrow \texttt{KeyGen}$

$K_{21} = \texttt{SharedKey}(\mathsf{pk}_2, \mathsf{sk}_1) \quad = \quad K_{12} = \texttt{SharedKey}(\mathsf{pk}_1, \mathsf{sk}_2)$

Tight security

Scheme $\mathcal{S}$ secure if problem $\mathcal{P}$ hard:

$\mathcal{A}$ attacks $\mathcal{S}$ $\implies$ $\mathcal{B}$ attacks $\mathcal{P}$ s.t.

$$\text{Advantage}^{\mathcal{S}}_{\mathcal{A}} \leq \underbrace{L}_{\text{security loss}} \cdot \text{Advantage}^{\mathcal{P}}_{\mathcal{B}} \ (+ \text{ similar runtime})$$

- **Asymptotic security:** $L \leq$ polynomial

Tight security

Scheme $\mathcal{S}$ secure if problem $\mathcal{P}$ hard:

$\mathcal{A}$ attacks $\mathcal{S}$ $\implies$ $\mathcal{B}$ attacks $\mathcal{P}$ s.t.

$$\text{Advantage}^{\mathcal{S}}_{\mathcal{A}} \leq \underbrace{L}_{\text{security loss}} \cdot \text{Advantage}^{\mathcal{P}}_{\mathcal{B}} \ (+ \text{ similar runtime})$$

- **Asymptotic security:** $L \leq$ polynomial
- **Tight security:** L small (e.g. small constant)

Tight security

Scheme $\mathcal{S}$ secure if problem $\mathcal{P}$ hard:

$\mathcal{A}$ attacks $\mathcal{S}$ $\implies$ $\mathcal{B}$ attacks $\mathcal{P}$ s.t.

$$\text{Advantage}^{\mathcal{S}}_{\mathcal{A}} \leq \underbrace{L}_{\text{security loss}} \cdot \text{Advantage}^{\mathcal{P}}_{\mathcal{B}} \ (+ \text{ similar runtime})$$

- **Asymptotic security:** $L \leq$ polynomial
- **Tight security:** L small (e.g. small constant)

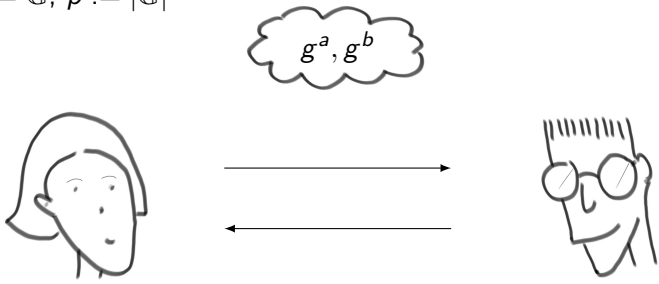
Why do we care?

- **Theory:** closer relation between $\mathcal{P}$ and $\mathcal{S}$
- **Practice:** smaller keys $\Rightarrow$ more efficient instantiations

Recap: Diffie-Hellman Key Exchange

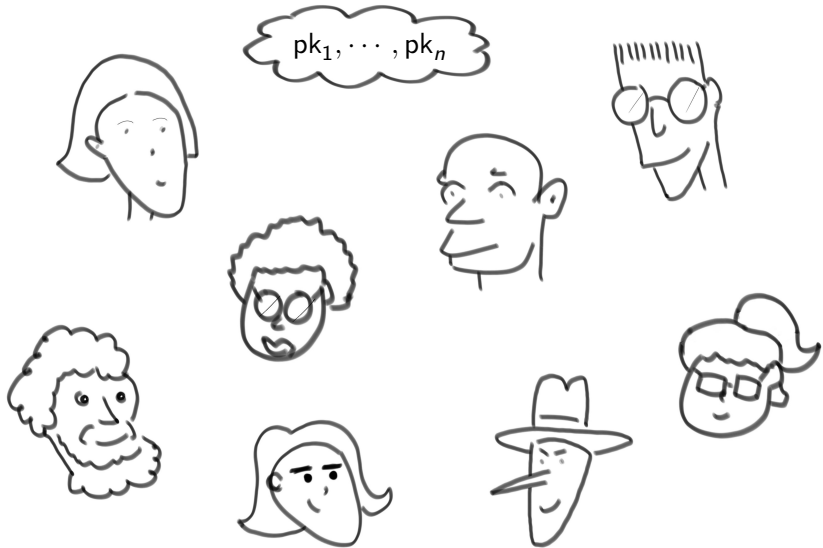
[DH76; CKS08]

$\mathbb{G}$ group, $\langle g \rangle = \mathbb{G}$, $p := |\mathbb{G}|$

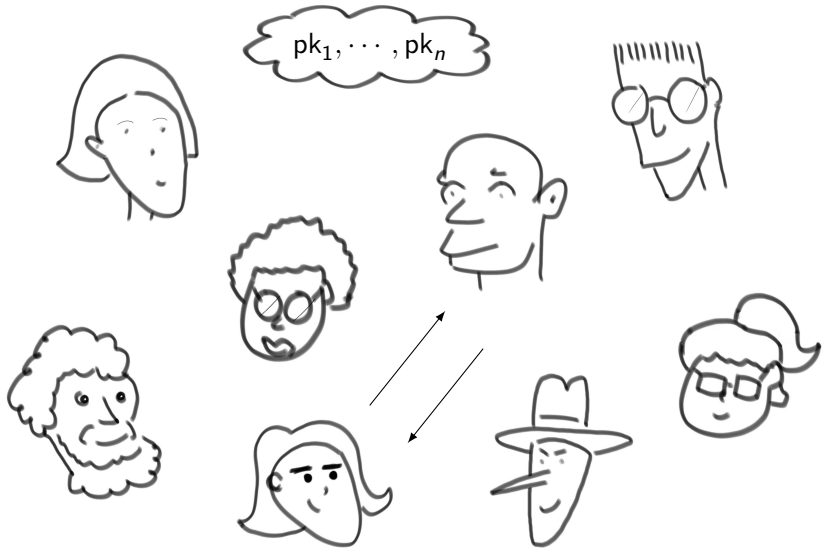


Decisional DH: $a, b, c \leftarrow_R \mathbb{Z}_p$: $(g^a, g^b, g^{ab}) \approx_c (g^a, g^b, g^c)$

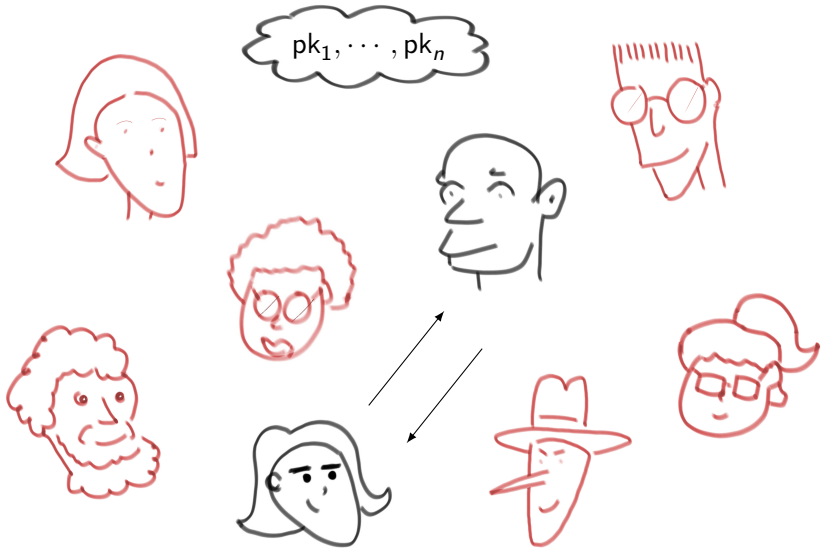
(Simplified) Security model



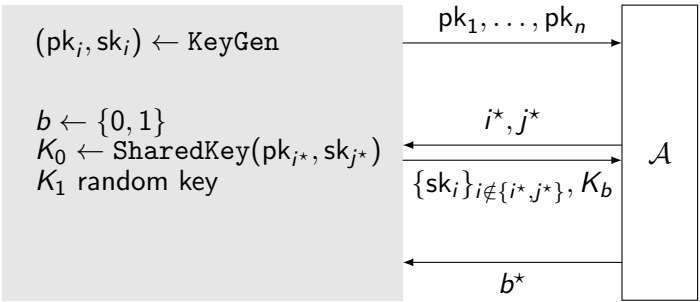
(Simplified) Security model



(Simplified) Security model



(Simplified) Security of NIKE w/ extractions



$$\mathsf{Advantage}^{\mathsf{nike}}_{\mathcal{A}} := |\Pr[b^\star = b] - 1/2|$$

Recap: DH Key Exchange - Security w/ extractions

Idea: $i^\star, j^\star \leftarrow_R \{1, \ldots, n\}$, embed DDH-challenge in $\mathsf{pk}_{i^\star}, \mathsf{pk}_{j^\star}$

Recap: DH Key Exchange - Security w/ extractions

Idea: $i^\star, j^\star \leftarrow_R \{1, \ldots, n\}$, embed DDH-challenge in $\mathsf{pk}_{i^\star}, \mathsf{pk}_{j^\star}$

$\rightsquigarrow$ **security loss** of $\approx n^2$

Reduction knows sk_i

$i \notin \{i^\star, j^\star\}$

Reduction doesn't know sk_i

$i \in \{i^\star, j^\star\}$

Recap: DH Key Exchange - Security w/ extractions

Idea: $i^\star, j^\star \leftarrow_R \{1, \ldots, n\}$, embed DDH-challenge in $\mathsf{pk}_{i^\star}, \mathsf{pk}_{j^\star}$

$\rightsquigarrow$ **security loss** of $\approx n^2$

Reduction knows sk_i

$i \notin \{i^\star, j^\star\}$

Reduction doesn't know sk_i

$i \in \{i^\star, j^\star\}$

[BJLS16]: This loss is inherent!

Our results

Can we do better?

Our results

Can we do better?

- Yes! First NIKE with security loss n (in the standard model).

Our results

Can we do better?

- Yes! First NIKE with security loss n (in the standard model).

Can we do even better?

Our results

Can we do better?

- Yes! First NIKE with security loss n (in the standard model).

Can we do even better?

- Seems hard! Lower bound of security loss n for broad class of NIKEs.

Our results

Can we do better?

- Yes! First NIKE with security loss n (in the standard model).

Can we do even better?

- Seems hard! Lower bound of security loss n for broad class of NIKEs.

\+ **Generic transformation with tight instantiation:**

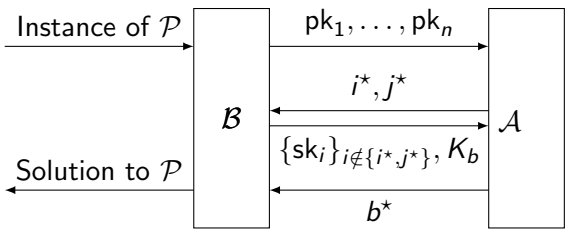
- NIKE with passive security $\rightsquigarrow$ NIKE with active security

The lower bound of [BJLS16]

- applies to all NIKEs w/ **unique secret keys**
- rules out tight **simple black-box** reductions

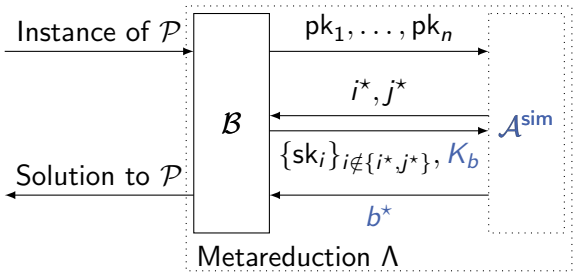
The lower bound of [BJLS16]

- applies to all NIKEs w/ **unique secret keys**
- rules out tight **simple black-box** reductions



The lower bound of [BJLS16]

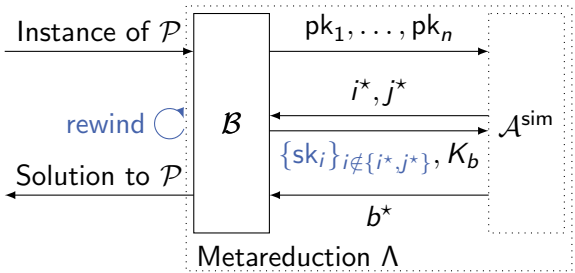
- applies to all NIKEs w/ **unique secret keys**
- rules out tight **simple black-box** reductions



- **Idea:** simulate $\mathcal{A}$ by computing $K_{i^\star j^\star}$

The lower bound of [BJLS16]

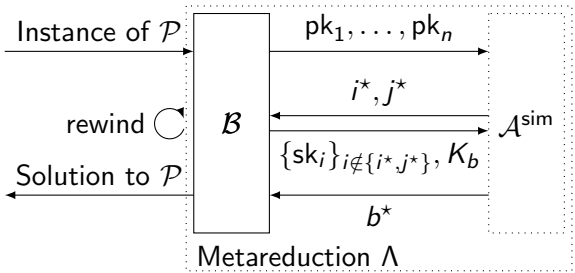
- applies to all NIKEs w/ **unique secret keys**
- rules out tight **simple black-box** reductions



- **Idea:** simulate $\mathcal{A}$ by computing $K_{i^\star j^\star}$ with *extracted* $\mathsf{sk}_{j^\star}$ (or $\mathsf{sk}_{i^\star}$)

The lower bound of [BJLS16]

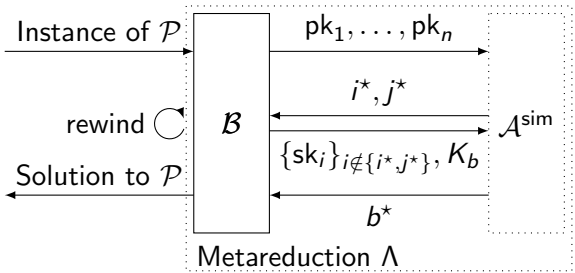
- applies to all NIKEs w/ **unique secret keys**
- rules out tight **simple black-box** reductions



- **Idea:** simulate $\mathcal{A}$ by computing $K_{i^\star j^\star}$ with *extracted* $\mathsf{sk}_{j^\star}$ (or $\mathsf{sk}_{i^\star}$)
- $\exists$ run $\neq (i^\star, j^\star)$ on which $\mathcal{B}$ does not abort

The lower bound of [BJLS16]

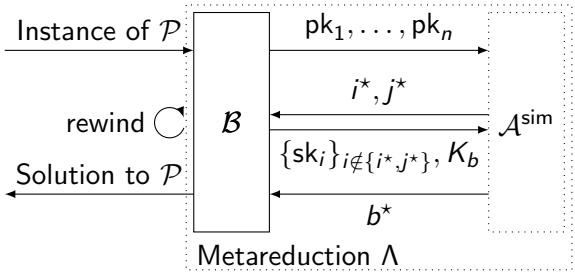
- applies to all NIKEs w/ **unique secret keys**
- rules out tight **simple black-box** reductions



- **Idea:** simulate $\mathcal{A}$ by computing $K_{i^\star j^\star}$ with *extracted* $\mathsf{sk}_{j^\star}$ (or $\mathsf{sk}_{i^\star}$)
- $\exists$ run $\neq (i^\star, j^\star)$ on which $\mathcal{B}$ does not abort $\Rightarrow$ problem $\mathcal{P}$ easy

The lower bound of [BJLS16]

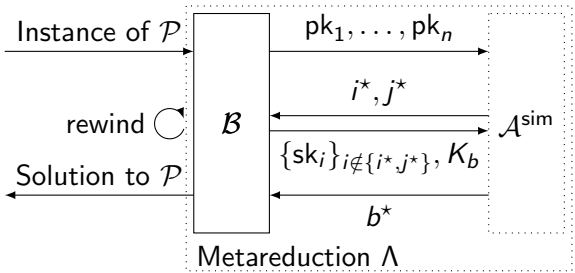
- applies to all NIKEs w/ **unique secret keys**
- rules out tight **simple black-box** reductions



- **Idea:** simulate $\mathcal{A}$ by computing $K_{i^\star j^\star}$ with *extracted* $\mathsf{sk}_{j^\star}$ (or $\mathsf{sk}_{i^\star}$)
- $\exists$ run $\neq (i^\star, j^\star)$ on which $\mathcal{B}$ does not abort $\Rightarrow$ problem $\mathcal{P}$ easy $\lightning$
- $\Rightarrow$ security loss of at least $\Omega(n^2)$

The lower bound of [BJLS16]

- applies to all NIKEs w/ **unique secret keys**
- rules out tight **simple black-box** reductions



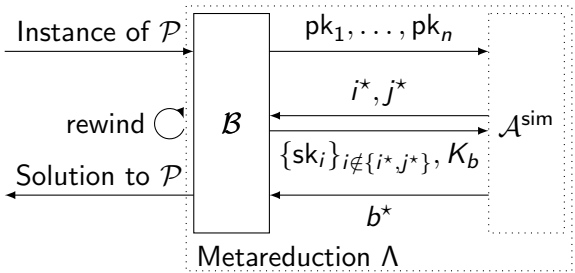
Reduction doesn't know sk_i

$i \in \{i^\star, j^\star\}$

- **Idea:** simulate $\mathcal{A}$ by computing $K_{i^\star j^\star}$ with *extracted* $\mathsf{sk}_{j^\star}$ (or $\mathsf{sk}_{i^\star}$)
- $\exists$ run $\neq (i^\star, j^\star)$ on which $\mathcal{B}$ does not abort $\Rightarrow$ problem $\mathcal{P}$ easy $\lightning$
- $\Rightarrow$ security loss of at least $\Omega(n^2)$

The lower bound of [BJLS16]

- applies to all NIKEs w/ **unique secret keys**
- rules out tight **simple black-box** reductions



Reduction doesn't know sk_i

$i \in \{i^\star, j^\star\}$

$\Rightarrow$ has to abort on all runs $\neq (i^\star, j^\star)$

- **Idea:** simulate $\mathcal{A}$ by computing $K_{i^\star j^\star}$ with *extracted* $\mathsf{sk}_{j^\star}$ (or $\mathsf{sk}_{i^\star}$)
- $\exists$ run $\neq (i^\star, j^\star)$ on which $\mathcal{B}$ does not abort $\Rightarrow$ problem $\mathcal{P}$ easy $\lightning$
- $\Rightarrow$ security loss of at least $\Omega(n^2)$

How to circumvent the lower bound of [BJLS16]?

Key of [BJLS16]: uniqueness of secret keys $\Rightarrow$ uniqueness of shared key

How to circumvent the lower bound of [BJLS16]?

Key of [BJLS16]: uniqueness of secret keys $\Rightarrow$ uniqueness of shared key

Our scheme: public keys have **many** secret keys

How to circumvent the lower bound of [BJLS16]?

Key of [BJLS16]: uniqueness of secret keys $\Rightarrow$ uniqueness of shared key

Our scheme: public keys have **many** secret keys

Not enough! By correctness:

$$\forall(\mathsf{pk}_1, \mathsf{sk}_1), (\mathsf{pk}_2, \mathsf{sk}_2) \colon \mathtt{SharedKey}(\mathsf{pk}_2, \mathsf{sk}_1) = \mathtt{SharedKey}(\mathsf{pk}_1, \mathsf{sk}_2)$$

How to circumvent the lower bound of [BJLS16]?

Key of [BJLS16]: uniqueness of secret keys $\Rightarrow$ uniqueness of shared key

Our scheme: public keys have **many** secret keys

Not enough! By correctness:

$$\forall(\mathsf{pk}_1, \mathsf{sk}_1), (\mathsf{pk}_2, \mathsf{sk}_2) \colon \mathtt{SharedKey}(\mathsf{pk}_2, \mathsf{sk}_1) = \mathtt{SharedKey}(\mathsf{pk}_1, \mathsf{sk}_2)$$

Solution: invalid public keys (w/o secret keys)

How to circumvent the lower bound of [BJLS16]?

Key of [BJLS16]: uniqueness of secret keys $\Rightarrow$ uniqueness of shared key

Our scheme: public keys have **many** secret keys

Not enough! By correctness:

$$\forall(\mathsf{pk}_1, \mathsf{sk}_1), (\mathsf{pk}_2, \mathsf{sk}_2)\colon \mathtt{SharedKey}(\mathsf{pk}_2, \mathsf{sk}_1) = \mathtt{SharedKey}(\mathsf{pk}_1, \mathsf{sk}_2)$$

Solution: invalid public keys (w/o secret keys)

valid public keys $\approx_c$ invalid public keys

How to circumvent the lower bound of [BJLS16]?

Key of [BJLS16]: uniqueness of secret keys $\Rightarrow$ uniqueness of shared key

Our scheme: public keys have **many** secret keys

Not enough! By correctness:

$$\forall(\mathsf{pk}_1, \mathsf{sk}_1), (\mathsf{pk}_2, \mathsf{sk}_2) \colon \mathtt{SharedKey}(\mathsf{pk}_2, \mathsf{sk}_1) = \mathtt{SharedKey}(\mathsf{pk}_1, \mathsf{sk}_2)$$

Solution: invalid public keys (w/o secret keys)

valid public keys $\approx_c$ invalid public keys

$$\forall(\mathsf{pk}_1, \mathsf{sk}_1), \mathsf{pk}_2 \colon (\mathsf{pk}_1, \mathsf{pk}_2, \mathtt{SharedKey}(\mathsf{pk}_2, \mathsf{sk}_1)) \equiv (\mathsf{pk}_1, \mathsf{pk}_2, \mathtt{random})$$

How to circumvent the lower bound of [BJLS16]?

Key of [BJLS16]: uniqueness of secret keys $\Rightarrow$ uniqueness of shared key

Our scheme: public keys have **many** secret keys

Not enough! By correctness:

$$\forall(\mathsf{pk}_1, \mathsf{sk}_1), (\mathsf{pk}_2, \mathsf{sk}_2) \colon \mathtt{SharedKey}(\mathsf{pk}_2, \mathsf{sk}_1) = \mathtt{SharedKey}(\mathsf{pk}_1, \mathsf{sk}_2)$$

Solution: invalid public keys (w/o secret keys)

valid public keys $\approx_c$ invalid public keys

$$\forall(\mathsf{pk}_1, \mathsf{sk}_1), \mathsf{pk}_2 \colon (\mathsf{pk}_1, \mathsf{pk}_2, \mathtt{SharedKey}(\mathsf{pk}_2, \mathsf{sk}_1)) \equiv (\mathsf{pk}_1, \mathsf{pk}_2, \mathtt{random})$$

Note: this requires entropy in sk_1 given pk_1 (and thus many secret keys)!

Recap: Subset membership problem (SMP)

X set, $L \subseteq X$ NP-language

Subset membership assumption for (X, L):

$$\{x \mid x \leftarrow_R L\} \qquad \approx_c \qquad \{x \mid x \leftarrow_R X \setminus L\}$$

Recap: Subset membership problem (SMP)

X set, $L \subseteq X$ NP-language

Subset membership assumption for (X, L):

$$\{x \mid x \leftarrow_R L\} \approx_c \{x \mid x \leftarrow_R X \setminus L\}$$

valid public keys $\approx_c$ invalid public keys

Recap: Hash proof system

[CS98]

$\texttt{HPS} = (\texttt{Gen}, \texttt{PubEval}, \texttt{PrivEval})$ is HPS for language L if:

$$\left.\begin{array}{l}\texttt{PubEval}(hpk, x, w)\\ \texttt{PrivEval}(hsk, x)\end{array}\right\} \text{return } \textbf{the same} \text{ key } K \text{ for all } x \in L \text{ with witness } w$$

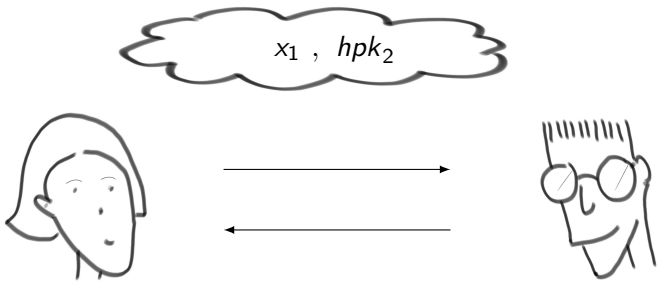
Universality: $\forall x \notin L$, $(hpk, hsk) \leftarrow \texttt{Gen}$:

$$(hpk, x, \texttt{PrivEval}(hsk, x)) \equiv (hpk, x, \texttt{random})$$

Our NIKE

Variation of the PAKE of [KOY01; GL03]

$\texttt{HPS} = (\texttt{Gen}, \texttt{PubEval}, \texttt{PrivEval})$ for L, SMP for $L \subseteq X$ hard



$x_1 \leftarrow L$ with witness w_1

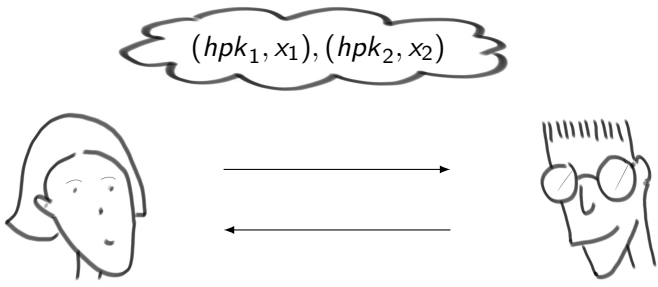
$(hpk_2, hsk_2) \leftarrow \texttt{Gen}$

$K_{21} = \texttt{PubEval}(hpk_2, x_1, w_1) \quad = \quad K_{12} = \texttt{PrivEval}(hsk_2, x_1)$

Our NIKE

Variation of the PAKE of [KOY01; GL03]

$\texttt{HPS} = (\texttt{Gen}, \texttt{PubEval}, \texttt{PrivEval})$ for L, SMP for $L \subseteq X$ hard



$x_1 \leftarrow L$ with witness w_1

$(hpk_1, hsk_1) \leftarrow \texttt{Gen}$

$K_{21} = \texttt{PubEval}(hpk_2, x_1, w_1)$ $=$ $K_{12} = \texttt{PrivEval}(hsk_2, x_1)$

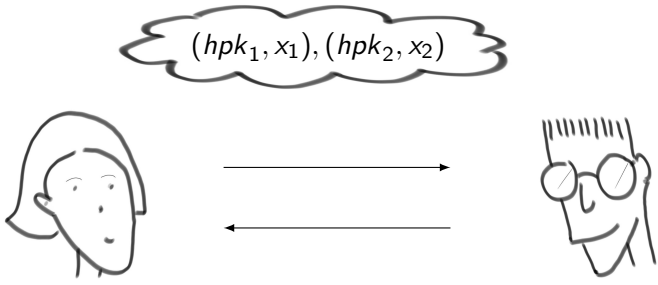
$x_2 \leftarrow L$ with witness w_2

$(hpk_2, hsk_2) \leftarrow \texttt{Gen}$

Our NIKE

Variation of the PAKE of [KOY01; GL03]

$\texttt{HPS} = (\texttt{Gen}, \texttt{PubEval}, \texttt{PrivEval})$ for L, SMP for $L \subseteq X$ hard



Note:

- hsk not unique
- can switch x to $X \backslash L$

$x_1 \leftarrow L$ with witness w_1

$(hpk_1, hsk_1) \leftarrow \texttt{Gen}$

$K_{21} = \texttt{PubEval}(hpk_2, x_1, w_1)$ $=$ $K_{12} = \texttt{PrivEval}(hsk_2, x_1)$

$x_2 \leftarrow L$ with witness w_2

$(hpk_2, hsk_2) \leftarrow \texttt{Gen}$

Proof of Security - Idea

Idea: $i^\star \leftarrow_R \{1, \ldots, n\}$, embed SMP-challenge as $x_{i^\star}$ in $\mathsf{pk}_{i^\star}$

Proof of Security - Idea

Idea: $i^\star \leftarrow_R \{1, \ldots, n\}$, embed SMP-challenge as $x_{i^\star}$ in $\mathsf{pk}_{i^\star}$

$$\forall j > i^\star \colon K_{i^\star j} = \texttt{PrivEval}(hsk_j, x_{i^\star})$$

Proof of Security - Idea

Idea: $i^\star \leftarrow_R \{1, \ldots, n\}$, embed SMP-challenge as $x_{i^\star}$ in $\mathrm{pk}_{i^\star}$

$$\forall j > i^\star \colon K_{i^\star j} = \texttt{PrivEval}(hsk_j, x_{i^\star})$$
$$\approx \text{random if } x_{i^\star} \in X \backslash L \text{ and } hsk_j \text{ unknown}$$

Proof of Security - Idea

Idea: $i^\star \leftarrow_R \{1, \ldots, n\}$, embed SMP-challenge as $x_{i^\star}$ in $\mathrm{pk}_{i^\star}$

$$\forall j > i^\star \colon K_{i^\star j} = \mathtt{PrivEval}(hsk_j, x_{i^\star})$$
$$\approx \text{random if } x_{i^\star} \in X \backslash L \text{ and } hsk_j \text{ unknown}$$

$\rightsquigarrow$ **security loss** of only n

Reduction knows sk_i

$i \neq i^\star$

Reduction doesn't know sk_i

$i = i^\star$

Towards a new lower bound

[BJLS16]:

- obtain $\mathsf{sk}_{i^\star}$ **or** $\mathsf{sk}_{j^\star}$ via rewinding to compute unique $K_{i^\star j^\star}$

Towards a new lower bound

[BJLS16]:

- obtain $\mathsf{sk}_{i^\star}$ **or** $\mathsf{sk}_{j^\star}$ via rewinding to compute unique $K_{i^\star j^\star}$
- reduction aborts on all runs without $i^\star$ **and** all runs without $j^\star \Rightarrow$ loss of $\Omega(n^2)$

Towards a new lower bound

[BJLS16]:

- obtain $\mathsf{sk}_{i^\star}$ **or** $\mathsf{sk}_{j^\star}$ via rewinding to compute unique $K_{i^\star j^\star}$
- reduction aborts on all runs without $i^\star$ **and** all runs without $j^\star \Rightarrow$ loss of $\Omega(n^2)$

Problem: $\mathsf{sk}_{i^\star}, \mathsf{sk}_{j^\star}$ not unique

Towards a new lower bound

[BJLS16]:

- obtain $\mathsf{sk}_{i^\star}$ **or** $\mathsf{sk}_{j^\star}$ via rewinding to compute unique $K_{i^\star j^\star}$
- reduction aborts on all runs without $i^\star$ **and** all runs without $j^\star \Rightarrow$ loss of $\Omega(n^2)$

Problem: $\mathsf{sk}_{i^\star}, \mathsf{sk}_{j^\star}$ not unique

Observation: uniqueness of $K_{i^\star j^\star}$ sufficient

Towards a new lower bound

[BJLS16]:

- obtain $\mathsf{sk}_{i^\star}$ **or** $\mathsf{sk}_{j^\star}$ via rewinding to compute unique $K_{i^\star j^\star}$
- reduction aborts on all runs without $i^\star$ **and** all runs without $j^\star \Rightarrow$ loss of $\Omega(n^2)$

Problem: $\mathsf{sk}_{i^\star}, \mathsf{sk}_{j^\star}$ not unique

Observation: uniqueness of $K_{i^\star j^\star}$ sufficient

- shared keys between valid public keys unique

Towards a new lower bound

[BJLS16]:

- obtain $\mathsf{sk}_{i^\star}$ **or** $\mathsf{sk}_{j^\star}$ via rewinding to compute unique $K_{i^\star j^\star}$
- reduction aborts on all runs without $i^\star$ **and** all runs without $j^\star \Rightarrow$ loss of $\Omega(n^2)$

Problem: $\mathsf{sk}_{i^\star}, \mathsf{sk}_{j^\star}$ not unique

Observation: uniqueness of $K_{i^\star j^\star}$ sufficient

- shared keys between valid public keys unique
- invalid public keys have no secret keys

Towards a new lower bound

[BJLS16]:

- obtain $\mathsf{sk}_{i^\star}$ **or** $\mathsf{sk}_{j^\star}$ via rewinding to compute unique $K_{i^\star j^\star}$
- reduction aborts on all runs without $i^\star$ **and** all runs without $j^\star \Rightarrow$ loss of $\Omega(n^2)$

Problem: $\mathsf{sk}_{i^\star}, \mathsf{sk}_{j^\star}$ not unique

Observation: uniqueness of $K_{i^\star j^\star}$ sufficient

- shared keys between valid public keys unique
- invalid public keys have no secret keys

Our metareduction:

- **Idea:** obtain $\mathsf{sk}_{i^\star}$ **and** $\mathsf{sk}_{j^\star}$ via rewinding to compute unique $K_{i^\star j^\star}$

Towards a new lower bound

[BJLS16]:

- obtain $\mathsf{sk}_{i^\star}$ **or** $\mathsf{sk}_{j^\star}$ via rewinding to compute unique $K_{i^\star j^\star}$
- reduction aborts on all runs without $i^\star$ **and** all runs without $j^\star$ $\Rightarrow$ loss of $\Omega(n^2)$

Problem: $\mathsf{sk}_{i^\star}, \mathsf{sk}_{j^\star}$ not unique

Observation: uniqueness of $K_{i^\star j^\star}$ sufficient

- shared keys between valid public keys unique
- invalid public keys have no secret keys

Our metareduction:

- **Idea:** obtain $\mathsf{sk}_{i^\star}$ **and** $\mathsf{sk}_{j^\star}$ via rewinding to compute unique $K_{i^\star j^\star}$
- reduction aborts on all runs without $i^\star$ **or** on all runs without $j^\star$

Towards a new lower bound

[BJLS16]:

- obtain $\mathsf{sk}_{i^\star}$ **or** $\mathsf{sk}_{j^\star}$ via rewinding to compute unique $K_{i^\star j^\star}$
- reduction aborts on all runs without $i^\star$ **and** all runs without $j^\star$ $\Rightarrow$ loss of $\Omega(n^2)$

Problem: $\mathsf{sk}_{i^\star}, \mathsf{sk}_{j^\star}$ not unique

Observation: uniqueness of $K_{i^\star j^\star}$ sufficient

- shared keys between valid public keys unique
- invalid public keys have no secret keys

Our metareduction:

- **Idea:** obtain $\mathsf{sk}_{i^\star}$ **and** $\mathsf{sk}_{j^\star}$ via rewinding to compute unique $K_{i^\star j^\star}$
- reduction aborts on all runs without $i^\star$ **or** on all runs without $j^\star$ $\Rightarrow$ loss of $\Omega(n)$

From passive to active security

Idea: add **unbounded simulation sound NIZK proof of knowledge** of secret key

- USS-NIZK allows to simulate during the reduction
- PoK allows to extract the secret key from corrupted users

From passive to active security

Idea: add **unbounded simulation sound NIZK proof of knowledge** of secret key

- USS-NIZK allows to simulate during the reduction
- PoK allows to extract the secret key from corrupted users

Instantiation:

- generic instantiation from standard components
- optimized tightly secure instantiation for our NIKE

Our results

Reference	$\lvert pk \rvert$	sec. model	sec. loss	assumption	uses
[DH76]	$1 \times \mathbb{G}$	passive	n^2	DDH	-
Ours	$3 \times \mathbb{G}$	passive	n	DDH	-
[CKS08]	$2 \times \mathbb{G}$	active*	2	CDH	ROM
[FHKP13]	$1 \times \mathbb{Z}_N$	active	n^2	factoring	ROM
[FHKP13]	$2 \times \mathbb{G} + 1 \times \mathbb{Z}_p$	active	n^2	DBDH	pairing
Ours	$12 \times \mathbb{G}$	active	n	DLIN	pairing

*w/o extractions

Modular constructions

New lower bound:

- applies to all schemes where invalid public keys have no secret keys
- yields a loss of $\Omega(n)$ for all simple black-box reductions

Generic transformation from passive to active secure NIKE **Thank you!!**

Bibliography I

Christoph Bader, Tibor Jager, Yong Li, and Sven Schäge. "On the Impossibility of Tight Cryptographic Reductions". In: *EUROCRYPT 2016, Part II*. Ed. by Marc Fischlin and Jean-Sébastien Coron. Vol. 9666. LNCS. Springer, Heidelberg, May 2016, pp. 273–304. DOI: 10.1007/978-3-662-49896-5_10.

David Cash, Eike Kiltz, and Victor Shoup. "The Twin Diffie-Hellman Problem and Applications". In: *EUROCRYPT 2008*. Ed. by Nigel P. Smart. Vol. 4965. LNCS. Springer, Heidelberg, Apr. 2008, pp. 127–145.

Ronald Cramer and Victor Shoup. "A Practical Public Key Cryptosystem Provably Secure Against Adaptive Chosen Ciphertext Attack". In: *CRYPTO'98*. Ed. by Hugo Krawczyk. Vol. 1462. LNCS. Springer, Heidelberg, Aug. 1998, pp. 13–25.

Bibliography II

Whitfield Diffie and Martin E. Hellman. "New Directions in Cryptography". In: *IEEE Transactions on Information Theory* 22.6 (1976), pp. 644–654.

Eduarda S. V. Freire, Dennis Hofheinz, Eike Kiltz, and Kenneth G. Paterson. "Non-Interactive Key Exchange". In: *PKC 2013*. Ed. by Kaoru Kurosawa and Goichiro Hanaoka. Vol. 7778. LNCS. Springer, Heidelberg, 2013, pp. 254–271. DOI: 10.1007/978-3-642-36362-7_17.

Rosario Gennaro and Yehuda Lindell. "A Framework for Password-Based Authenticated Key Exchange". In: *EUROCRYPT 2003*. Ed. by Eli Biham. Vol. 2656. LNCS. http://eprint.iacr.org/2003/032.ps.gz. Springer, Heidelberg, May 2003, pp. 524–543.

Bibliography III

Jonathan Katz, Rafail Ostrovsky, and Moti Yung. "Efficient Password-Authenticated Key Exchange Using Human-Memorable Passwords". In: *EUROCRYPT 2001*. Ed. by Birgit Pfitzmann. Vol. 2045. LNCS. Springer, Heidelberg, May 2001, pp. 475–494.

Eike Kiltz and Hoeteck Wee. "Quasi-Adaptive NIZK for Linear Subspaces Revisited". In: *EUROCRYPT 2015, Part II*. Ed. by Elisabeth Oswald and Marc Fischlin. Vol. 9057. LNCS. Springer, Heidelberg, Apr. 2015, pp. 101–128. DOI: 10.1007/978-3-662-46803-6_4.