Towards Tight Adaptive Security of Non-Interactive Key Exchange

Julia Hesse — IBM Research Europe - Zurich
Dennis Hofheinz — ETH Zurich
Lisa Kohl — Cryptology Group, CWI Amsterdam
Roman Langrehr — ETH Zurich

Outline

Non-Interactive Key Exchange (NIKE)

Previous results on tightness for NIKE

Our first result: Tight NIKE with large keys

Our second result: Large keys are necessary

Our third result: Tight semi-adaptively secure NIKE

NIKE

Alice

Bob

$(\mathsf{pk}_A, \mathsf{sk}_A) \xleftarrow{\$} \mathtt{KeyGen}(1^\lambda)$

$(\mathsf{pk}_B, \mathsf{sk}_B) \xleftarrow{\$} \mathtt{KeyGen}(1^\lambda)$

$$\text{Alice} \underset{\mathsf{pk}_B}{\overset{\mathsf{pk}_A}{\rightleftarrows}} \text{PKI} \underset{\mathsf{pk}_A}{\overset{\mathsf{pk}_B}{\leftrightarrows}} \text{Bob}$$

$$K_{AB} \xleftarrow{\$} \mathtt{SharedKey}(\mathsf{sk}_A, \mathsf{pk}_B) \quad = \quad K_{BA} \xleftarrow{\$} \mathtt{SharedKey}(\mathsf{sk}_B, \mathsf{pk}_B)$$

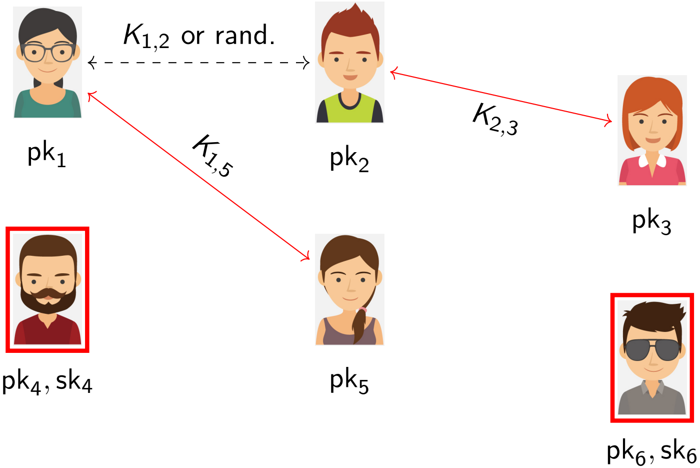
NIKE

- Symmetric keys with minimal communication
  - Fast
  - Low energy usage
- Building block for
  - Deniable authentication
  - Interactive key exchange
  - Designated verifier signatures

NIKE – Security

Adversary can adaptively

- spawn new users
- corrupt users
- reveal shared keys
- get challenged on (one[1]) uncorrupted shared key
- Dishonest key registration: Can be achieved generically.



[1] Our work generalizes to multi-challenge security without additional loss

Tight security

$$\begin{array}{ccc} \text{Scheme} & & \text{Assumption} \\ \text{(e.g. NIKE)} & \xrightarrow{\text{Reduction}} & \text{(e.g. Diffie-Hellman)} \end{array}$$

Can be broken with probability ε using resources ρ.

Can be broken with probability ε/ℓ using resources ρ.

- Large ℓ can be compensated by a larger security parameter.
  $\Rightarrow$ Less efficient
- Tight: ℓ does not depend on the adversary.
  - Especially, ℓ does not grow with the number of users N.

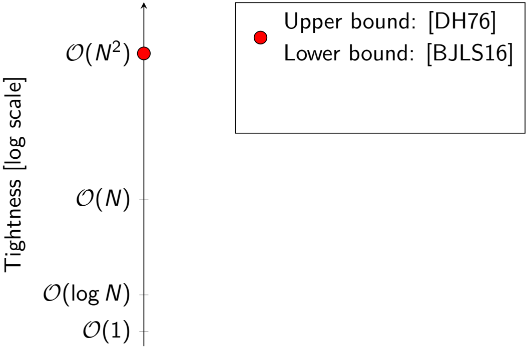
Related works

[DH76]:

- Guess both challenge users (spawn query index)
- Embed challenge in their public key
- Security loss $\mathcal{O}(N^2)$

[BJLS16]:

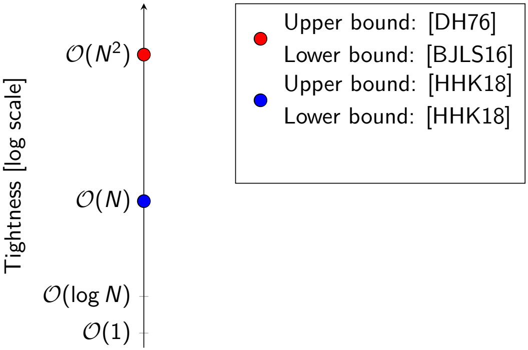
- Loss $\mathcal{O}(N^2)$ is necessary
- if secret keys are unique (given the public key)



Related works

[HHK18]:

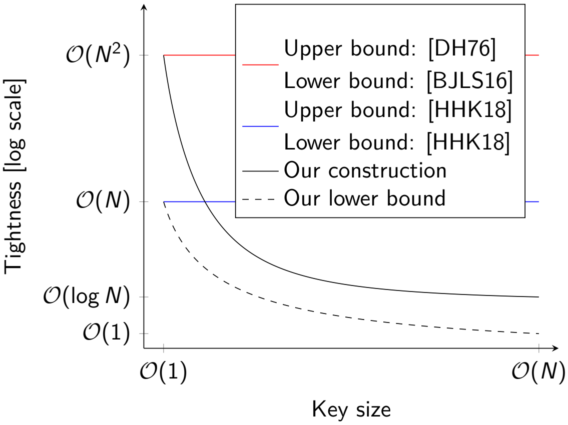
- Guess one of the challenge users (spawn query index)
- Embed challenge in their public key
- Security loss $\mathcal{O}(N)$
- Loss $\mathcal{O}(N)$ is necessary
- if secret keys are unique (given the public key)



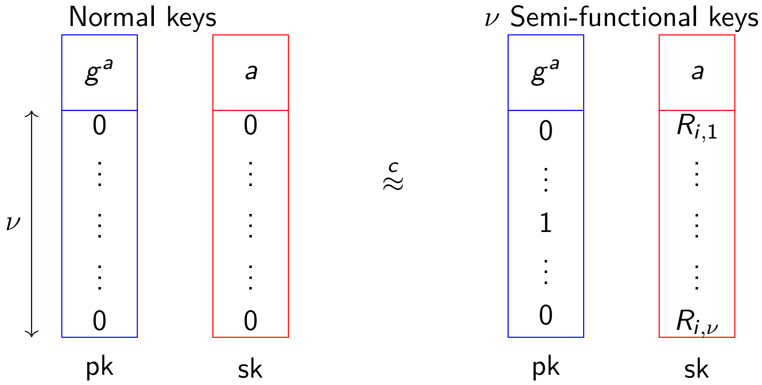
Comparison with related works

Our work:

- NIKE with flexible key length
- Larger keys give less security loss
- Lower bound: Large keys are necessary
- Lower bounds applies to NIKEs where the shared key is inner product of public and secret key.



Our NIKE: Abstract Idea



$R_{i,j} = R_{j,i}$
unif. random

Shared key: Inner product of pk_1 and sk_2.

Our NIKE: Abstract Idea

Shared key between users i and j:

	pk_j normal	pk_j semi-functional
pk_i normal	Real	Real
pk_i semi-functional	Real	Real $+ R_{i,j}$

Uniformly random if sk_i and sk_j are unknown

Implicit notation

$$\left[\begin{pmatrix} a_{11} & \cdots & a_{1,m} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,m} \end{pmatrix}\right] := \begin{pmatrix} g^{a_{11}} & \cdots & g^{a_{1,m}} \\ \vdots & \ddots & \vdots \\ g^{a_{n,1}} & \cdots & g^{a_{n,m}} \end{pmatrix}$$

MDDH assumption

$$\left(\left[\boxed{\mathbf{D}}\right], \left[\boxed{\mathbf{D}}\ \boxed{\mathbf{w}}\right]\right) \stackrel{c}{\approx} \left(\left[\boxed{\mathbf{D}}\right], \left[\boxed{\mathbf{u}}\right]\right)$$

$\mathbf{D}, \mathbf{w}, \mathbf{u}$ are uniformly random

- Tightly implied by well-known assumptions like 2-LIN.
- conjectured to hold even in presence of a symmetric paring

$$e(g^a, g^b) = g_T^{ab}$$

Our NIKE: Implementation

$$\mathsf{pp} = \left([\boxed{\mathbf{D}}], [\boxed{\mathbf{M}}\,\boxed{\mathbf{D}}] \right) \text{ with } \boxed{\mathbf{M}} = \boxed{\mathbf{M}^\top}$$

$$\mathsf{pk}_i = [\boxed{\mathbf{D}}\,\boxed{\mathbf{w}_i}] \qquad \mathsf{sk}_i = [\boxed{\mathbf{M}}\,\boxed{\mathbf{D}}\,\boxed{\mathbf{w}_i}]$$

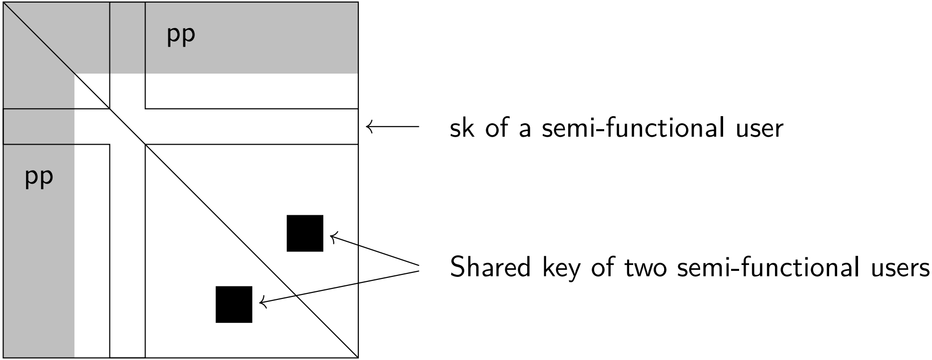
$$K_{i,j} = e(\mathsf{pk}_i, \mathsf{sk}_j) = e(\mathsf{pk}_j, \mathsf{sk}_i)$$

Semi-functional keys:

$$\mathsf{pk}_i = [\boxed{\mathbf{u}_i}] \qquad \mathsf{sk}_i = [\boxed{\mathbf{M}}\,\boxed{\mathbf{u}_i}]$$

Our NIKE: Proof sketch

Leakage of the matrix **M**: (In a suitable basis)



$\Rightarrow$ Shared keys between users with semi-functional keys are uniformly random (even with adaptive corruptions).

Our NIKE: Proof sketch

- N: Number of users
- ν: Number of "Table entries" $\approx$ Size of the keys

Hybrid argument:

- each hybrid randomizes ν^2 shared keys

$\Rightarrow$ $\mathcal{O}((N/\nu)^2)$ are necessary

- in each hybrid:
  - Switch ν keys from normal to semi-functional (and back)
  - can be done with loss $\mathcal{O}(\log \nu)$ (new MDDH rerandomization argument)

Total security loss: $\mathcal{O}(N^2 \log(\nu)/\nu^2)$

Inner-product NIKEs

Definition:

- pk contains (implicitly) a d-dimensional vector $\mathbf{x}$
- sk contains (implicitly) a d-dimensional vector $\mathbf{y}$
- Shared key: $f(\langle \mathbf{x}_i, \mathbf{y}_i \rangle)$ for an invertible function f.

Captures for example:

- Diffie-Hellman
- [HHK18]
- Our first construction

Lower bound for inner-product NIKE

- Reduction sends pk at registration

=> $\mathbf{x}_i$ fixed for each user at registration

- Case $\mathbf{x}_i \in \mathrm{Span}(\mathbf{x}_1, \ldots, \mathbf{x}_{i-1})$: Reduction is committed to shared keys.
- Case $\mathbf{x}_i \notin \mathrm{Span}(\mathbf{x}_1, \ldots, \mathbf{x}_{i-1})$: Can happen at most d times.
- After registering all users, opening $\approx N/2$ secret keys, the reduction is committed to a shared key (among the remaining users) with significant probability.
- Meta-reduction now unveils shared key between two remaining users...
- ...rewinds the reduction...
- ... (hopefully) wins the challenge with this key.

Minimal Security loss: $\Omega(N/d)$

Semi-adaptive security

Selective security

- Adversary has to register all users in one shot
- Adversary has to specify challenge pair before seeing the public key
- Tightness is easy

Semi-adaptive security

- Adversary has to specify challenge pair before making any corruptions (reveal secret key/reveal shared key)

Adaptive security

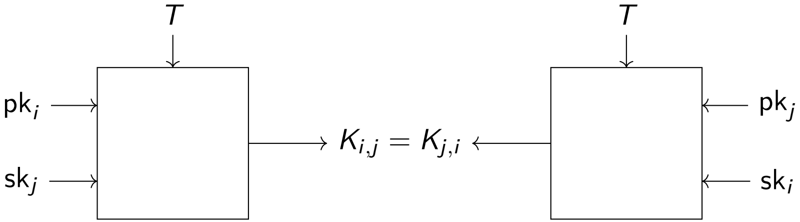
- Tightness is hard

Programmable tags

- Use our first construction (with $\nu = 1$)
- Switch all keys to semi-functional
- Reduction can output all secret keys...
- ...but then there is nothing secret about the shared keys between two semi-functional users
- Still useful:
  - Reduction publishes all the public keys
  - Adversary picks challenge pair
  - Reduction "program" the challenge key

  $\Rightarrow$ Tool to gain adaptivity

Tag-based NIKE



- Correctness holds except for one special tag $T^\star$
- Security holds for $T^\star$
- Can be built from LWE (with a tight security reduction)
- Use as tag the "shared key" from the first construction

$\Rightarrow$ Tight semi-adaptively secure NIKE

- More general security notion when larger keys are used

Summary

$$\begin{tikzcd} & \text{Tightness} \arrow[dl, leftrightarrow] \arrow[dr, leftrightarrow, dotted] & \\ \text{Adaptivity} \arrow[rr, leftrightarrow, dotted] & & \text{Compact keys} \end{tikzcd}$$

$\leftarrow\cdots\rightarrow$ Tradeoff possible

- You can have two of these properties
- Tradeoff between “Compact keys” and “Tightness” is possible
- Tradeoff between “Compact keys” and “Adaptivity” is possible

References I

Christoph Bader, Tibor Jager, Yong Li, and Sven Schäge.
On the impossibility of tight cryptographic reductions.
In Marc Fischlin and Jean-Sébastien Coron, editors, EUROCRYPT 2016, Part II, volume 9666 of LNCS, pages 273–304. Springer, Heidelberg, May 2016.
doi:10.1007/978-3-662-49896-5_10.

Whitfield Diffie and Martin E. Hellman.
New directions in cryptography.
IEEE Transactions on Information Theory, 22(6):644–654, 1976.

References II

Julia Hesse, Dennis Hofheinz, and Lisa Kohl.
On tightly secure non-interactive key exchange.
In Hovav Shacham and Alexandra Boldyreva, editors, CRYPTO 2018, Part II, volume 10992 of LNCS, pages 65–94. Springer, Heidelberg, August 2018.
doi:10.1007/978-3-319-96881-0_3.

Pictures

Alice, Bob, and others: freepik.com