


From Identification using Rejection Sampling to Signatures via the Fiat-Shamir Transform: Application to the BLISS Signature

Pauline Bert and Adeline Roux-Langlois

IWSEC 2018

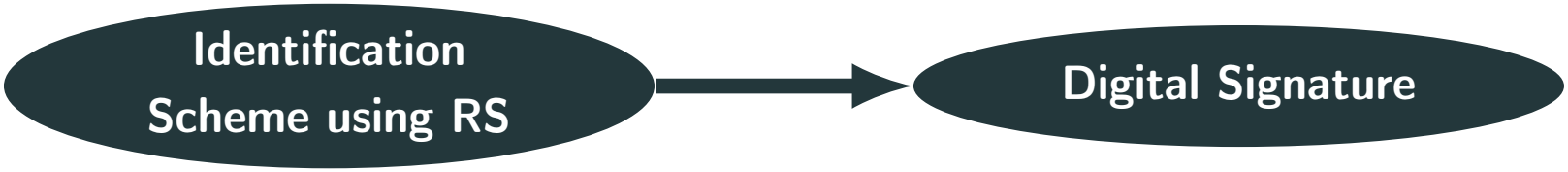
Univ Rennes, CNRS, IRISA

Contribution

- Fiat-Shamir black-box transformation[1] from identification schemes to signature schemes

$\longrightarrow$ We propose a transformation taking into account

1. The rejection sampling technique used mainly in lattice-based schemes,
2. Both lossy and non-lossy cases.

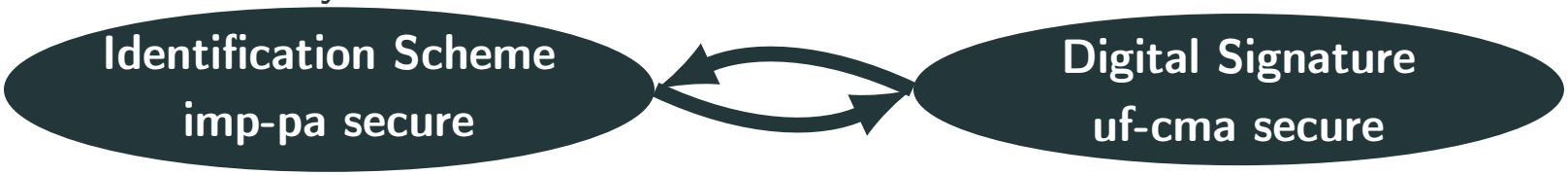


- Application of our black-box transformation to the BLISS lattice-based signature

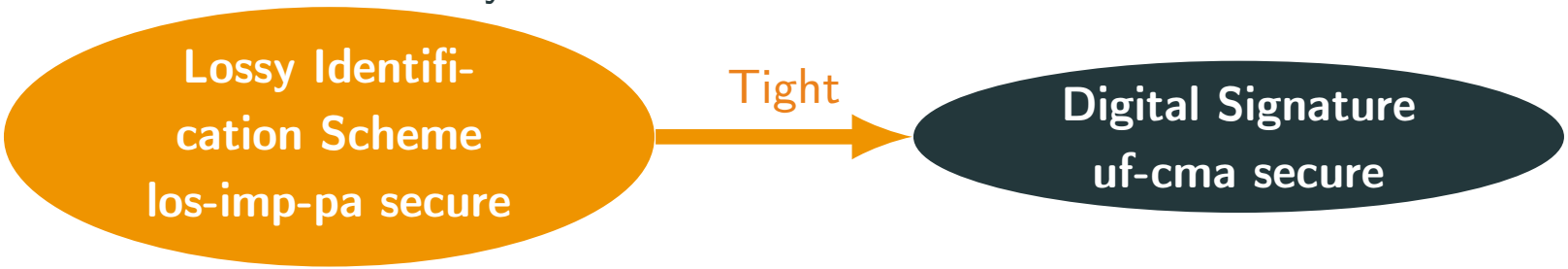
[1] Amos Fiat and Adi Shamir (1986). "How to Prove Yourself: Practical Solutions to Identification and Signature Problems". In: *CRYPTO*.

Context: Fiat-Shamir Transforms

- Minimal security[2]



- Introduction of the lossy case[3]



[2] Michel Abdalla et al. (2002). "From Identification to Signatures via the Fiat-Shamir Transform: Minimizing Assumptions for Security and Forward-Security". In: *EUROCRYPT*.

[3] Michel Abdalla et al. (2012). "Tightly-Secure Signatures from Lossy Identification Schemes". In: *EUROCRYPT*.

Context: Lattice-Based Signatures

Lattice-based cryptography:

1996 Ajtai described the SIS problem $\longrightarrow$ signature, hash function...

2005 Regev described the LWE problem $\longrightarrow$ PKE, FHE...

$\longrightarrow$ post-quantum

NIST Competition:

- Aim to standardize signature, KEM, and PKE
- Using post-quantum hypothesis like codes, lattices, isogenies, MQ...

Lattice-based signatures:

- Hash-and-Sign: GGH, NTRUSign, GPV, Falcon...
- Fiat-Shamir: Lyubashevsky[4], BLISS, qTESLA, Dilithium...

$\longrightarrow$ qTESLA and Dilithium are proved using black-box transformations

[4] Vadim Lyubashevsky (2008). "Lattice-Based Identification Schemes Secure Under Active Attacks". In: *Public Key Cryptography*.

Context: Rejection Sampling

= Technique to sample from an arbitrary probability distribution f given access to another one g_v

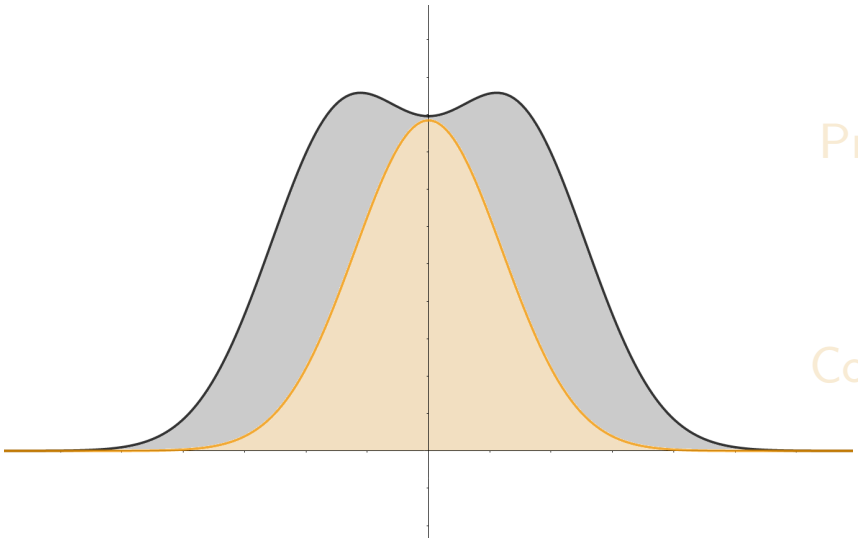
$\longrightarrow$ If $M \cdot g_v(x) \geq f(x)$ for some M, then the two following procedures output the same distribution

$x \xleftarrow{\$} f$

return x with probability $1/M$

$x \xleftarrow{\$} g_v$

return x with probability $\frac{f(x)}{M \cdot g_v(x)}$



Pros: A sample from g_v is made independent from v

$\longrightarrow$ v can depend on a secret

Cons: To get a sample, this procedure will be repeated on average M times

$\longrightarrow$ not constant time

$\longrightarrow$ From bimodal Gaussian to unimodal centered Gaussian

Context: Rejection Sampling

= Technique to sample from an arbitrary probability distribution f given access to another one g_v

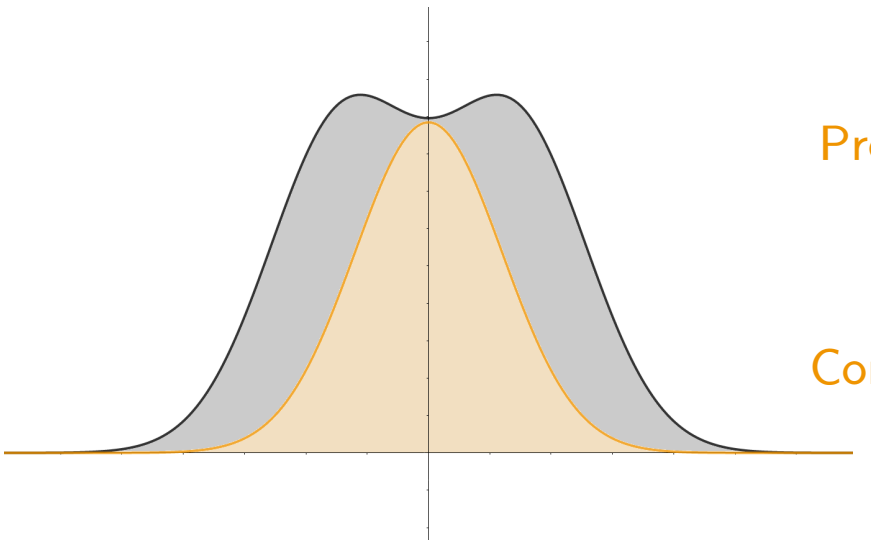
$\longrightarrow$ If $M \cdot g_v(x) \geq f(x)$ for some M, then the two following procedures output the same distribution

$x \xleftarrow{\$} f$

return x with probability $1/M$

$x \xleftarrow{\$} g_v$

return x with probability $\frac{f(x)}{M \cdot g_v(x)}$



$\longrightarrow$ From bimodal Gaussian to unimodal centered Gaussian

Pros: A sample from g_v is made independent from v

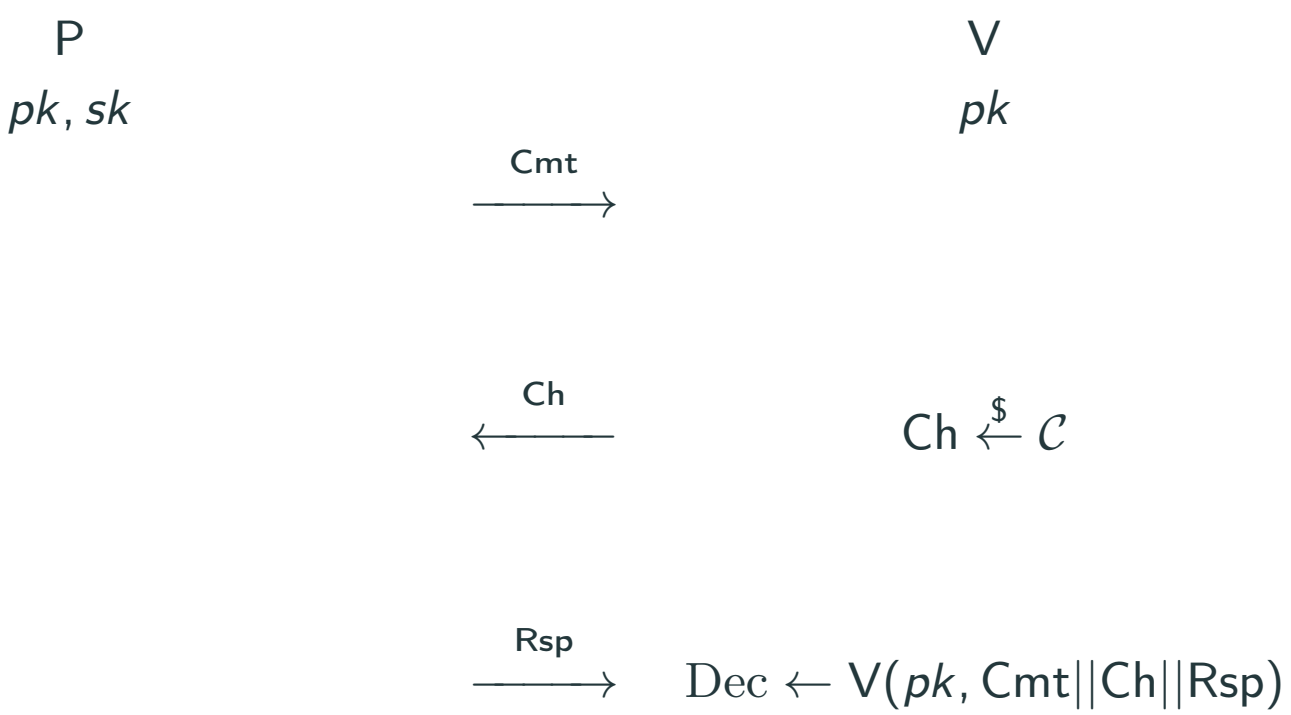
$\longrightarrow$ v can depend on a secret

Cons: To get a sample, this procedure will be repeated on average M times

$\longrightarrow$ not constant time

From Identification using Rejection Sampling to Signatures via the Fiat-Shamir Transform

Classical Identification Scheme



Identification Scheme using Rejection Sampling

P		V
pk, sk		pk
	$\xrightarrow{\text{Cmt}}$	
	$\xleftarrow{\text{Ch}}$	$\text{Ch} \xleftarrow{\$} \mathcal{C}$
$\text{Rsp} \xleftarrow{\$} g_v$ With proba $\frac{f(x)}{M \cdot g_v(x)}$, output Rsp Otherwise output $\text{Rsp} \leftarrow \perp$	$\xrightarrow{\text{Rsp}}$	$\text{Dec} \leftarrow \text{V}(pk, \text{Cmt}\|\|\text{Ch}\|\|\text{Rsp})$

Properties

Non-Lossy | Lossy

Correctness Error

The probability that $\mathsf{Rsp} = \perp$ is small.

Simulatability/naHVZK

We can construct an algorithm Sim that outputs transcripts $\mathsf{Cmt}||\mathsf{Ch}||\mathsf{Rsp}$ statistically closed to the original ones without having access to the secret key.

Key-Indistinguishability

A lossy key generation algorithm $\mathsf{LossyKeyGen}(1^k) \to pk$ outputs a lossy public key pk computationally indistinguishable from a honestly generated one.

Security

Non-Lossy

sim-imp-pa

Passive impersonation where the adversary has access to the public key of the scheme and the simulated algorithm Sim.

Lossy

los-imp-pa

Passive impersonation where the adversary has access to a lossy public key of the scheme and the simulated algorithm Sim.

$\mathbf{Exp}^{\text{imp-pa}}_{\mathcal{ID},\mathcal{I}}(k)$

$(pk, sk) \xleftarrow{\$} \mathrm{KeyGen}(1^k)$ or $pk \xleftarrow{\$} \mathrm{LossyKeyGen}(1^k)$

$st \| \mathrm{Cmt} \xleftarrow{\$} \mathcal{I}^{\mathrm{Sim}}(pk)$

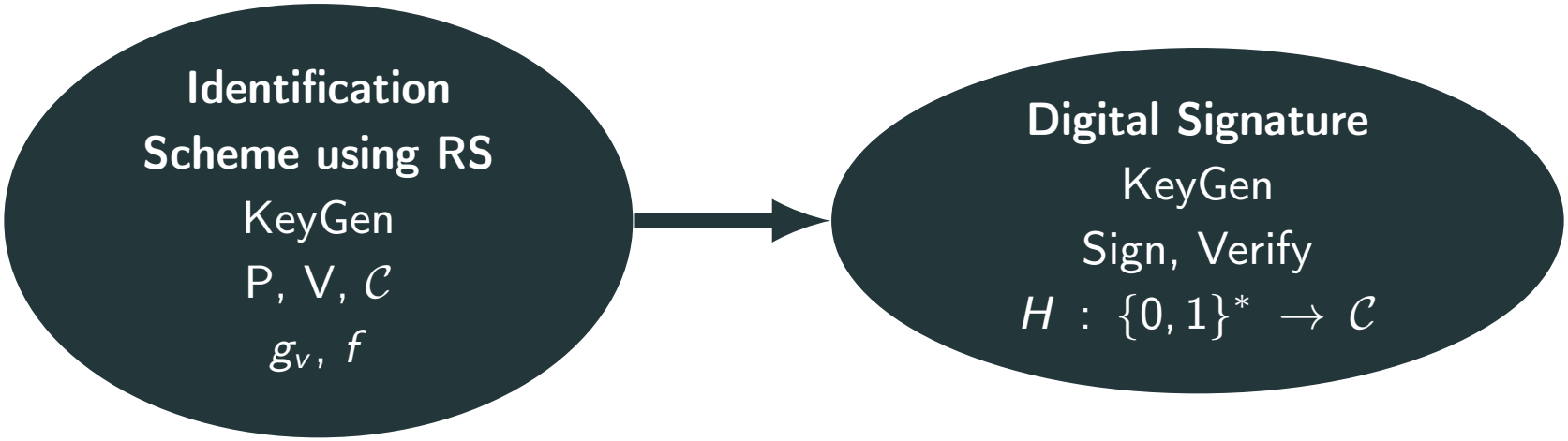
$\mathrm{Ch} \xleftarrow{\$} \mathcal{C}$

$\mathrm{Rsp} \xleftarrow{\$} \mathcal{I}(st, \mathrm{Ch})$

$\mathrm{Dec} \leftarrow \mathrm{V}(pk, \mathrm{Cmt}||\mathrm{Ch}||\mathrm{Rsp})$

return Dec

Fiat-Shamir Transform



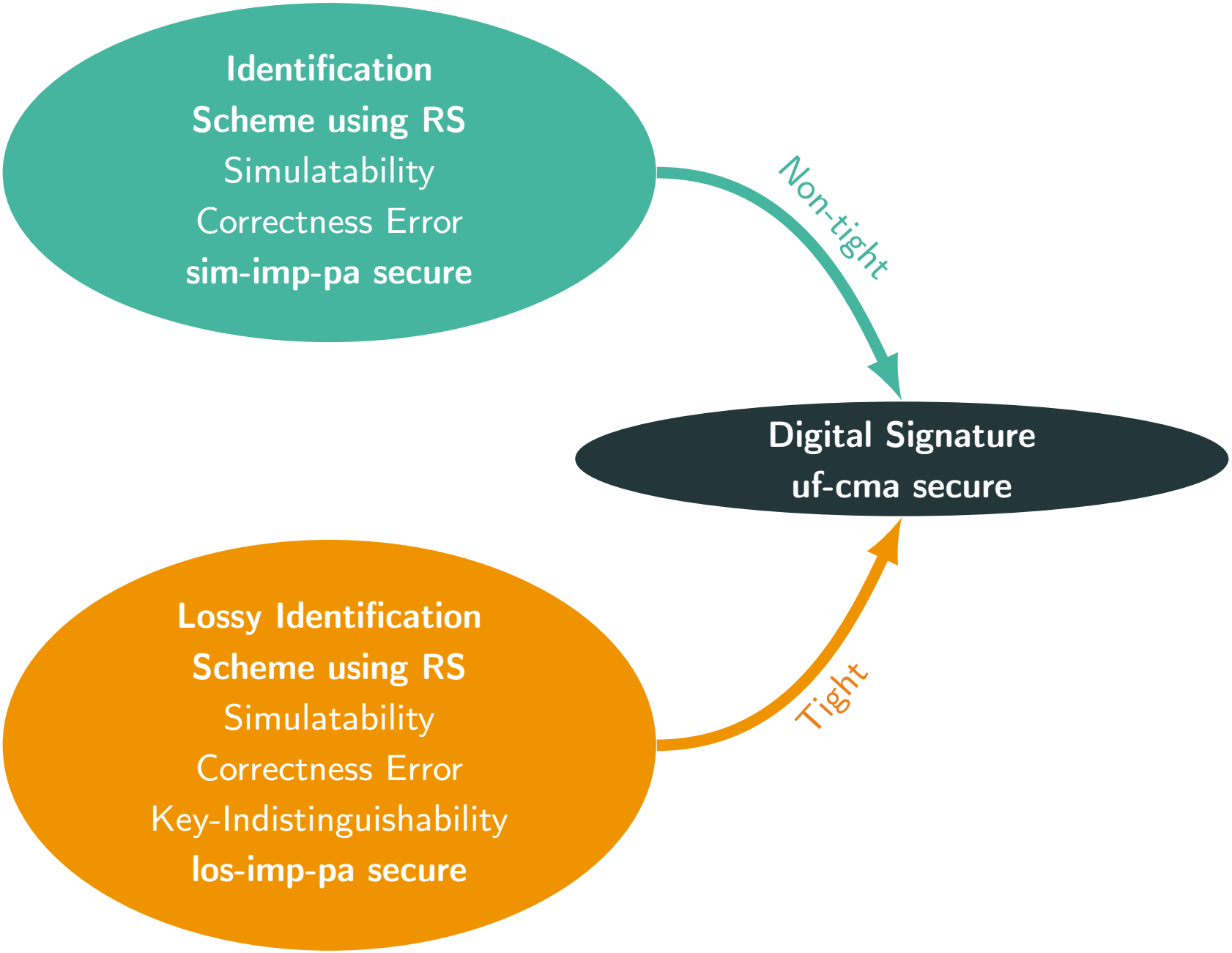
Sign(sk, m):

while Rsp $= \perp$ **do**
  Cmt $\leftarrow$ P(sk)
  Ch $\leftarrow H$(Cmt, m)
  Rsp $\xleftarrow{\$}$ g_v
  return $\sigma =$ (Cmt, Rsp) with probability $\frac{f(x)}{M \cdot g_v(x)}$, otherwise
  Rsp $\leftarrow \perp$
end while

Verify(pk, m, σ):

parse σ as (Cmt, Rsp)
Ch $\leftarrow H$(Cmt, m)
return V(pk, Cmt||Ch||Rsp)

Contribution



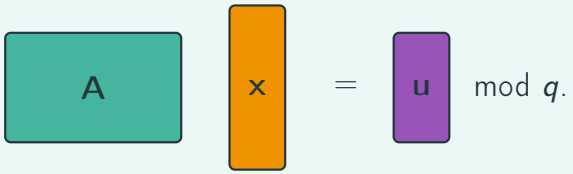
Application to the BLISS Signature

Application to the BLISS signature[6]

- Originally the BLISS signature was proved directly in the ROM
- Its security is based on the SIS[5] problem

Short Integer Solution

Given an uniformly random matrix $\mathbf{A} \hookleftarrow U(\mathbb{Z}_q^{n \times m})$, find a non trivial short vector $\mathbf{x} \in \mathbb{Z}^m$ such that $\|\mathbf{x}\| \leq \beta$ and:



- We can apply our first non-tight reduction as an example to BLISS

---

[5] Miklós Ajtai (1996). "Generating Hard Instances of Lattice Problems (Extended Abstract)". In: *STOC*.

[6] Léo Ducas et al. (2013). "Lattice Signatures and Bimodal Gaussians". In: *CRYPTO (1)*.

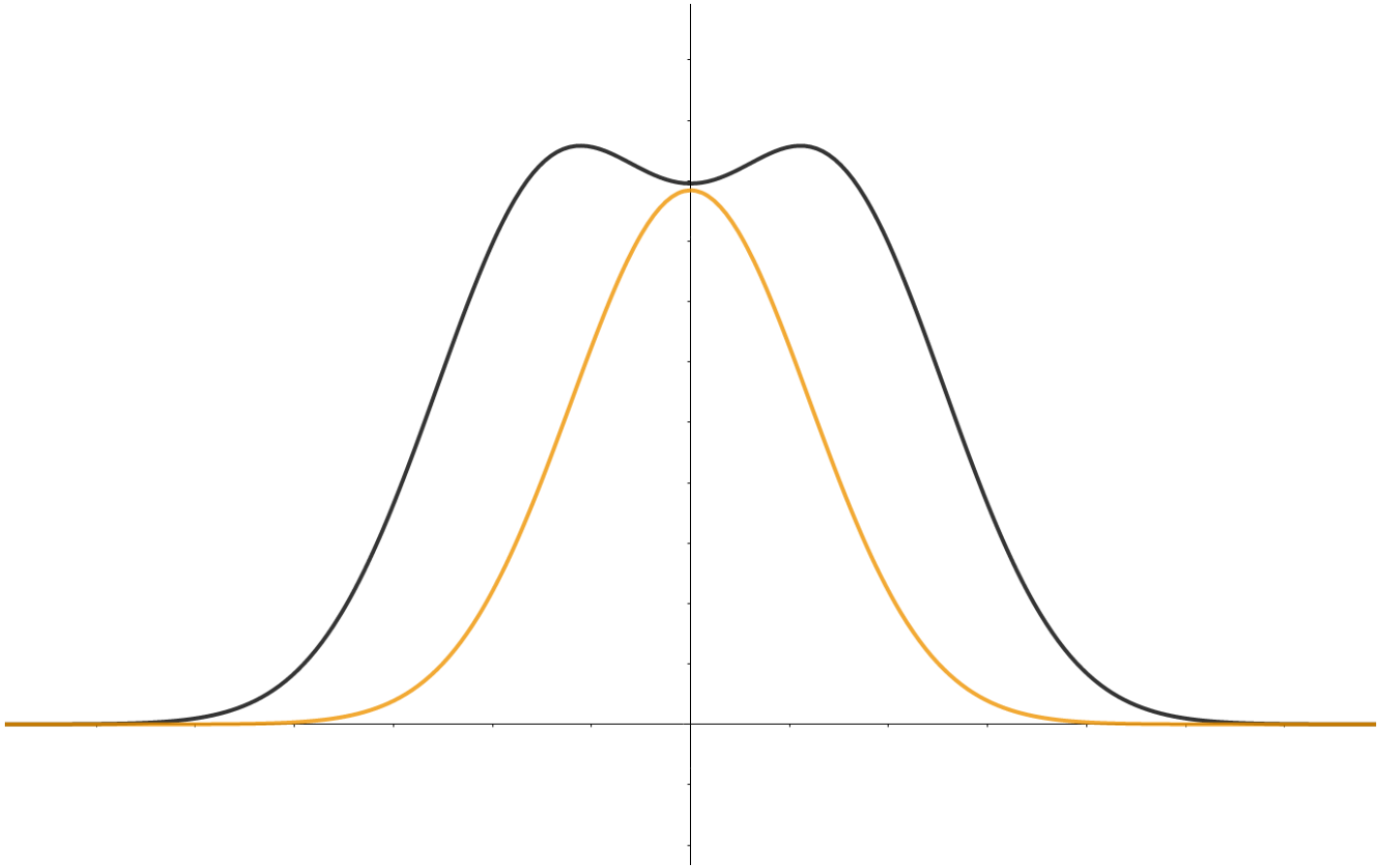
BLISS (1)

Settings

- *Public Key:* $\mathbf{A} \in \mathbb{Z}_{2q}^{n \times m}$
- *Secret Key:* Short $\mathbf{S} \in \mathbb{Z}_{2q}^{m \times n}$ such that $\mathbf{AS} = q\mathbf{I}_n \mod 2q$
- *Challenge Space:* $\mathcal{C} = \{\mathbf{c} : \mathbf{c} \in \{0,1\}^n, \|\mathbf{c}\|_1 \leq \kappa\}$
- *Probability Distributions:* $M \cdot g_{\mathbf{Sc}} = M \cdot \left(\frac{1}{2} D^m_{-\mathbf{Sc},\sigma} + \frac{1}{2} D^m_{\mathbf{Sc},\sigma}\right)$ and $f = D^m_\sigma$

P		V
$pk = \mathbf{A}, sk = \mathbf{S}$		$pk = \mathbf{A}$
$\mathbf{y} \leftarrow D^m_\sigma$	$\xrightarrow{\mathbf{u}}$	
$\mathbf{u} \leftarrow \mathbf{Ay} \mod 2q$		
$b \xleftarrow{\$} \{0,1\}$	$\xleftarrow{\mathbf{c}}$	$\mathbf{c} \xleftarrow{\$} \mathcal{C}$
$\mathbf{z} \leftarrow (-1)^b \mathbf{Sc} + \mathbf{y}$		
Output $\mathbf{z}$ with probability $\frac{f(\mathbf{z})}{M \cdot g_{\mathbf{Sc}}(\mathbf{z})}$	$\xrightarrow{\mathbf{z}}$	**Output** 1 iff $\|\mathbf{z}\| \leq \eta\sigma\sqrt{m}$,
otherwise **output** $\mathbf{z} \leftarrow \perp$		$\mathbf{Az} + q\mathbf{c} = \mathbf{u} \mod 2q$

BLISS (2)

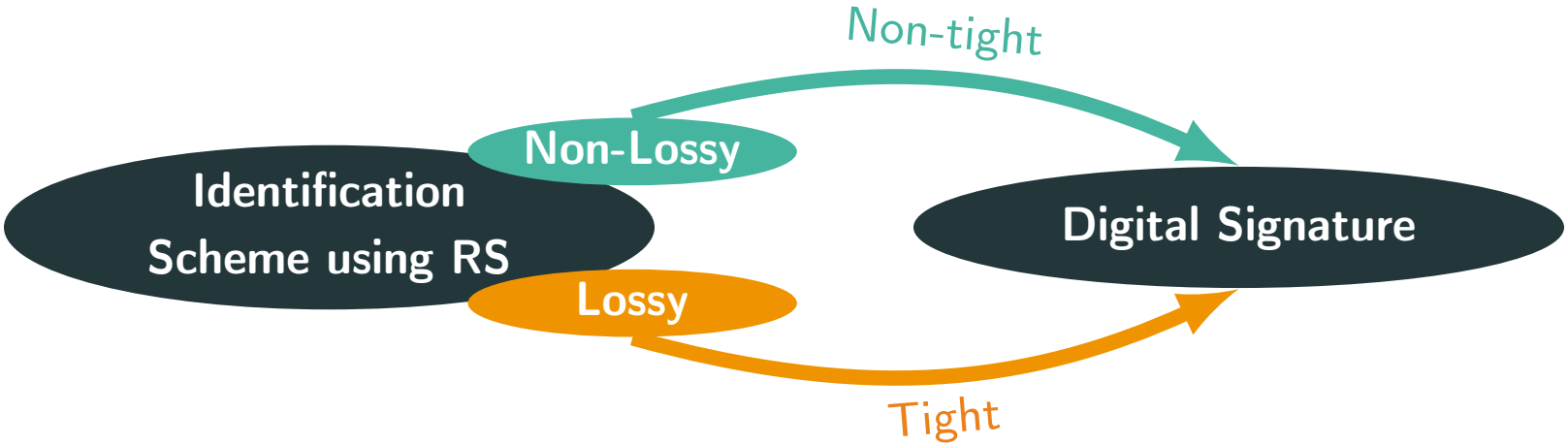


By applying our first non-tight reduction we get

$$\mathbf{Adv}^{\text{uf-cma}}_{\text{BLISS},\mathcal{F}} \lessapprox q_H \sqrt{\mathbf{Adv}_{\text{SIS}}} + \cdots$$

where q_H is the number of hash queries.

Conclusion



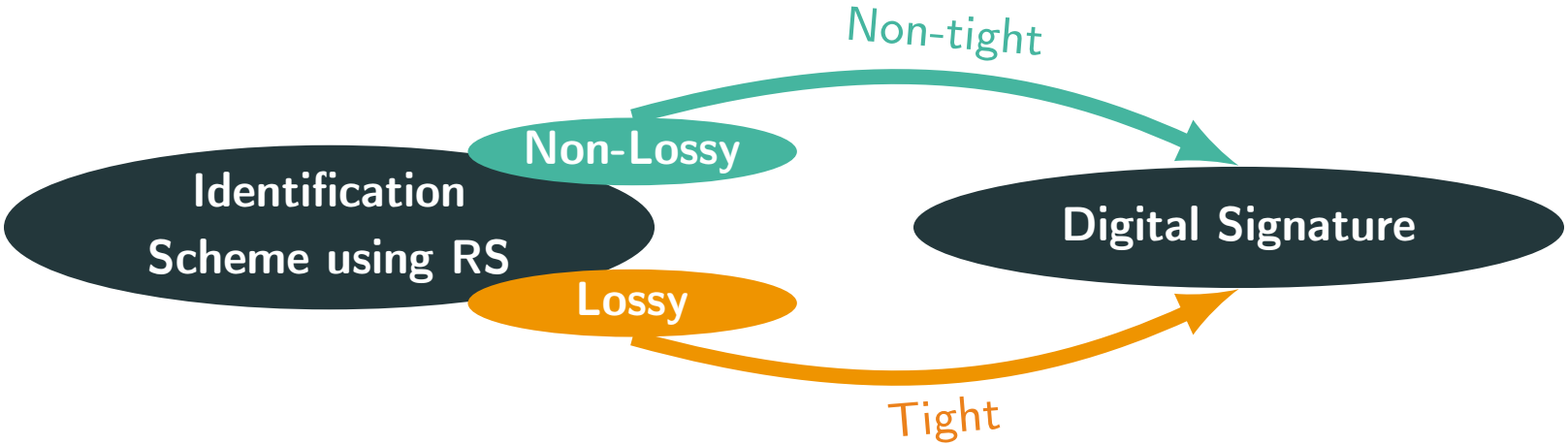
Pros: All mentions of random oracles are delegated to the black-box transformation, it is enough to only prove certain properties

Cons: Looses a factor roughly $\sqrt{q_H}$ compared to the original BLISS proof

$\longrightarrow$ To get a lossy identification scheme and a tight signature, we can use the LWE problem instead of the SIS problem (eg. qTESLA and Dilithium NIST candidates)

Thank You!

Conclusion



Pros: All mentions of random oracles are delegated to the black-box transformation, it is enough to only prove certain properties

Cons: Looses a factor roughly $\sqrt{q_H}$ compared to the original BLISS proof

$\longrightarrow$ To get a lossy identification scheme and a tight signature, we can use the LWE problem instead of the SIS problem (eg. qTESLA and Dilithium NIST candidates)

Thank You!