



EMSEC

UMR IRISA

UNIVERSITÉ DE
RENNES I



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

Pauline Bert and Adeline Roux-Langlois

Journées C2 2018

Univ Rennes, CNRS, IRISA

- Fiat-Shamir black-box transformation¹ from identification schemes to signature schemes



→ 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.



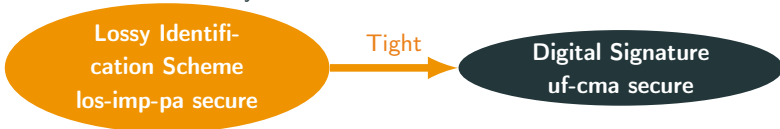
- Application of our black-box transformation to the BLISS lattice-based signature

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

- Minimal security²



- Introduction of the lossy case³



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 → signature, hash function...

2005 Regev described the LWE problem → PKE, FHE...

→ 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: Lyubashevsky⁴, BLISS, qTESLA, Dilithium...

→ qTESLA and Dilithium are proved using black-box transformations

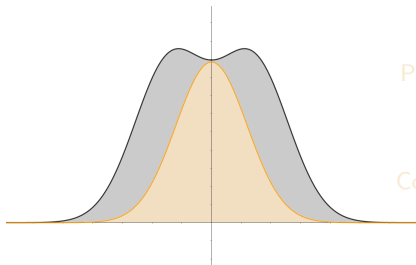
⁴ Vadim Lyubashevsky (2008). "Lattice-Based Identification Schemes Secure Under Active Attacks". In: *Public Key Cryptography*.

Context: Rejection Sampling

- = Technique to sample from an arbitrary probability distribution f given access to another one g_v
- If $M \cdot g_v(x) \geq f(x)$ for some M , then the two following procedures output the same distribution

$x \stackrel{\$}{\leftarrow} f$
return x with probability $1/M$

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



- Pros:** A sample from g_v is made independent from v
→ v can depend on a secret
- Cons:** To get a sample, this procedure will be repeated on average M times
→ not constant time

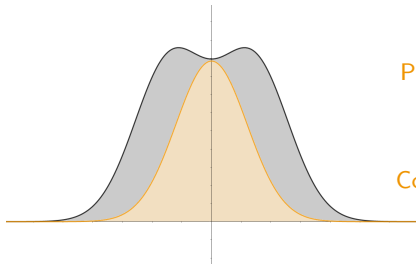
→ From bimodal Gaussian to unimodal centered Gaussian

Context: Rejection Sampling

- = Technique to sample from an arbitrary probability distribution f given access to another one g_v
- If $M \cdot g_v(x) \geq f(x)$ for some M , then the two following procedures output the same distribution

$x \stackrel{s}{\leftarrow} f$
return x with probability $1/M$

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



- Pros:** A sample from g_v is made independent from v
 - v can depend on a secret
- Cons:** To get a sample, this procedure will be repeated on average M times
 - not constant time

→ From bimodal Gaussian to unimodal centered Gaussian

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

Classical Identification Scheme

P
 pk, sk

Cmt
→

V
 pk

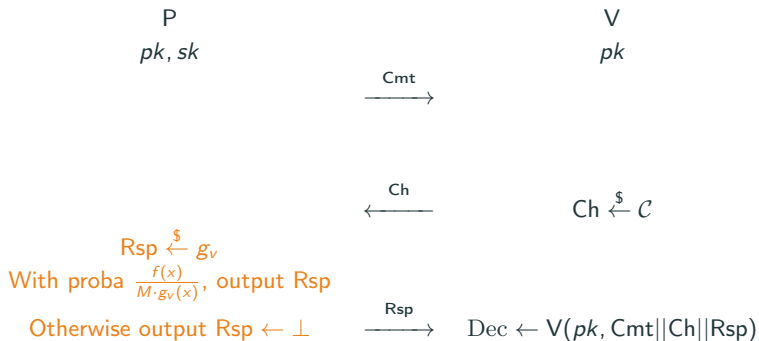
Ch
←

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

Rsp
→

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

Identification Scheme using Rejection Sampling



Non-Lossy

Lossy

Correctness Error

The probability that $Rsp = \perp$ is small.

Simulatability/naHVZK

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

Key-Indistinguishability

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

Non-Lossy

sim-imp-pa

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

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

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

$$st \parallel \text{Cmt} \xleftarrow{\$} \mathcal{I}^{\text{Sim}}(pk)$$

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

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

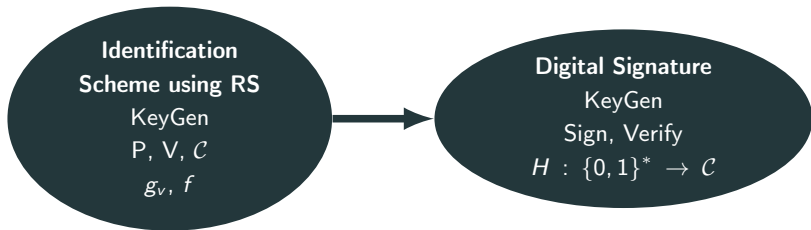
$$\text{Dec} \leftarrow \text{V}(pk, \text{Cmt} \parallel \text{Ch} \parallel \text{Rsp})$$

return Dec

Lossy

los-imp-pa

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

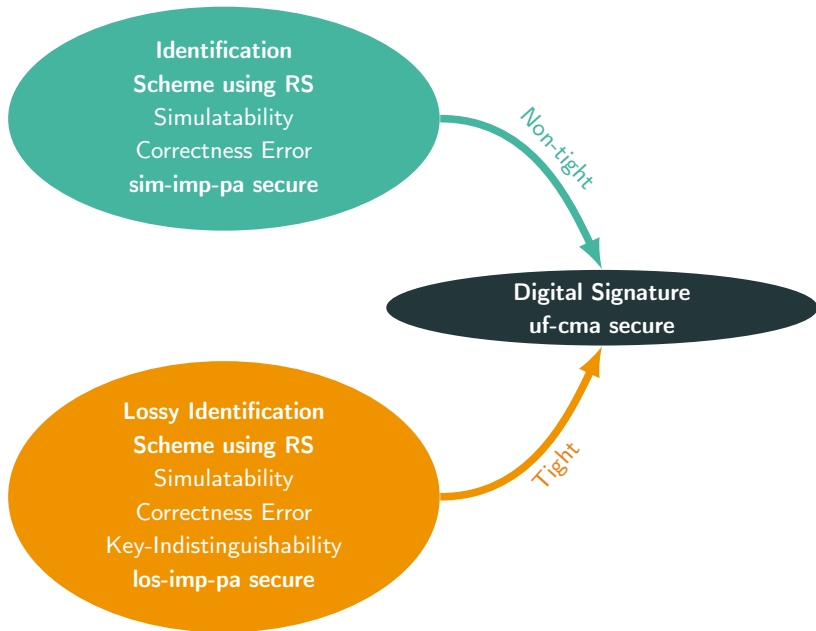


Sign(sk, m):

```
while Rsp =  $\perp$  do
  Cmt  $\leftarrow$  P( $sk$ )
  Ch  $\leftarrow$  H(Cmt,  $m$ )
  Rsp  $\stackrel{\$}{\leftarrow}$   $g_v$ 
  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  $\sigma$  as (Cmt, Rsp)
Ch  $\leftarrow$  H(Cmt,  $m$ )
return V( $pk, \text{Cmt} || \text{Ch} || \text{Rsp}$ )
```



Application to the BLISS Signature

- Originally the BLISS signature was proved directly in the ROM
- Its security is based on the SIS⁵ problem

Short Integer Solution

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

$$\begin{array}{|c|} \hline A \\ \hline \end{array} \begin{array}{|c|} \hline x \\ \hline \end{array} = \begin{array}{|c|} \hline u \\ \hline \end{array} \pmod{q}.$$

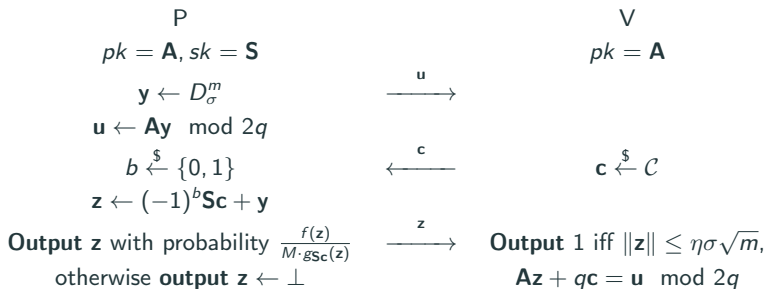
- We can apply our first non-tight reduction as an example to BLISS

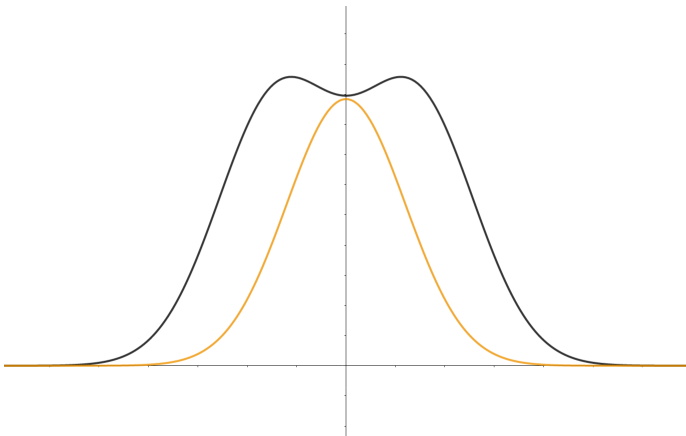
⁵ Miklós Ajtai (1996). "Generating Hard Instances of Lattice Problems (Extended Abstract)". In: *STOC*.

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

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 $\mathbf{AS} = q\mathbf{I}_n \pmod{2q}$
- *Challenge Space:* $\mathcal{C} = \{\mathbf{c} : \mathbf{c} \in \{0, 1\}^n, \|\mathbf{c}\|_1 \leq \kappa\}$
- *Probability Distributions:* $M \cdot g_{\mathbf{S}\mathbf{c}, \sigma} = M \cdot \left(\frac{1}{2}D_{-\mathbf{S}\mathbf{c}, \sigma}^m + \frac{1}{2}D_{\mathbf{S}\mathbf{c}, \sigma}^m\right)$ and $f = D_{\sigma}^m$

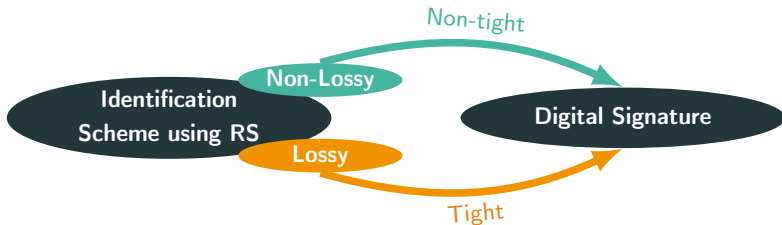




By applying our first non-tight reduction we get

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

where q_H is the number of hash queries.

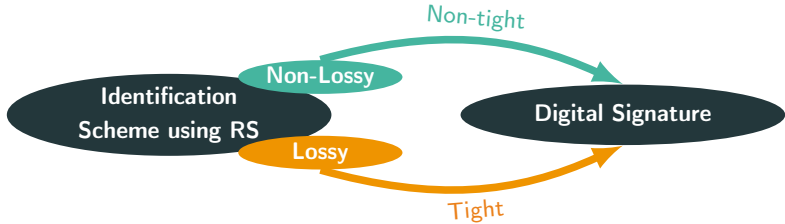


Pros: All mentions of random oracles are delegated to the black-box transformation, it is enough to only prove certain properties

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

- 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!



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

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

- 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!