# On the Lossiness of the Rabin Trapdoor Function

Yannick Seurin

ANSSI, France

March 27, 2014 — PKC 2014

# Summary of results

- We show that the Rabin Trapdoor Function (modular squaring) is a lossy trapdoor function when adequately restricting its domain, under an extension of the Φ-Hiding assumption for $e = 2$ that we name the 2-Φ/4-Hiding assumption
- We apply this result to the security of Rabin Full Domain Hash signatures, and show that deterministic variants of Rabin-FDH have a tight reduction from the 2-Φ/4-Hiding assumption (tight reductions were previously only known for probabilistic variants)
- By extending a previous "meta-reduction" result by Coron & Kakvi-Kiltz, we show that these deterministic variants of Rabin-FDH are unlikely to have a tight black-box reduction from the Factoring assumption

# Summary of results

- We show that the Rabin Trapdoor Function (modular squaring) is a lossy trapdoor function when adequately restricting its domain, under an extension of the Φ-Hiding assumption for $e = 2$ that we name the 2-Φ/4-Hiding assumption
- We apply this result to the security of Rabin Full Domain Hash signatures, and show that deterministic variants of Rabin-FDH have a tight reduction from the 2-Φ/4-Hiding assumption (tight reductions were previously only known for probabilistic variants)
- By extending a previous "meta-reduction" result by Coron & Kakvi-Kiltz, we show that these deterministic variants of Rabin-FDH are unlikely to have a tight black-box reduction from the Factoring assumption

# Summary of results

- We show that the Rabin Trapdoor Function (modular squaring) is a lossy trapdoor function when adequately restricting its domain, under an extension of the Φ-Hiding assumption for $e = 2$ that we name the 2-Φ/4-Hiding assumption
- We apply this result to the security of Rabin Full Domain Hash signatures, and show that deterministic variants of Rabin-FDH have a tight reduction from the 2-Φ/4-Hiding assumption (tight reductions were previously only known for probabilistic variants)
- By extending a previous "meta-reduction" result by Coron & Kakvi-Kiltz, we show that these deterministic variants of Rabin-FDH are unlikely to have a tight black-box reduction from the Factoring assumption

# Outline

1. Lossiness of the Rabin Trapdoor Function
2. Application to Rabin-Williams-FDH Signatures
3. Extending the Coron-Kakvi-Kiltz Meta-Reduction Result

# Outline

1. Lossiness of the Rabin Trapdoor Function
2. Application to Rabin-Williams-FDH Signatures
3. Extending the Coron-Kakvi-Kiltz Meta-Reduction Result

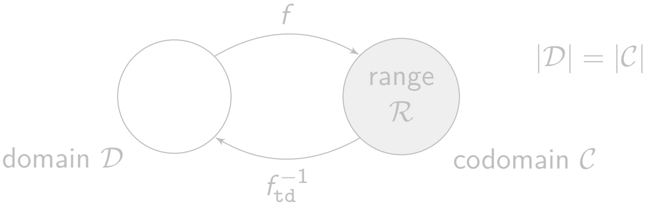
# Lossy Trapdoor Function (LTDF)

- introduced by Peikert and Waters [PW08]
- have found a wide range of applications (black-box construction of IND-CCA2 PKE, etc.)

**Reminder: (classical) Trapdoor Function (TDF)**

A Trapdoor Function (TDF) consists of

- a generation procedure $(f, \mathtt{td}) \leftarrow \mathit{InjGen}(1^k)$ such that $f$ is injective, easy to compute, but hard to invert without the trapdoor $\mathtt{td}$.



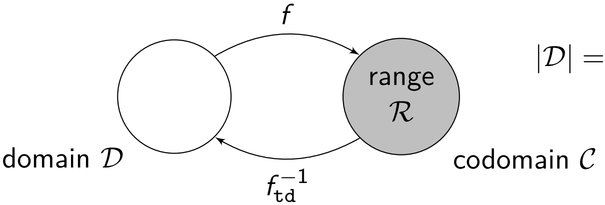
# Lossy Trapdoor Function (LTDF)

- introduced by Peikert and Waters [PW08]
- have found a wide range of applications (black-box construction of IND-CCA2 PKE, etc.)

## Reminder: (classical) Trapdoor Function (TDF)

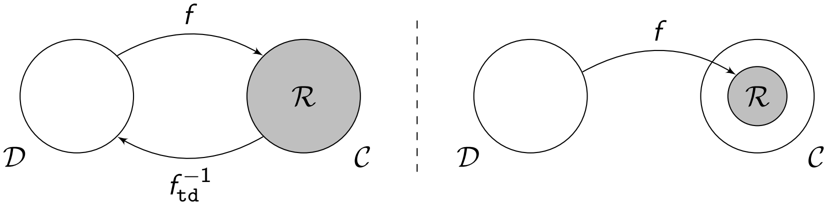
A Trapdoor Function (TDF) consists of

- a generation procedure $(f, \mathtt{td}) \leftarrow \mathit{InjGen}(1^k)$ such that $f$ is injective, easy to compute, but hard to invert without the trapdoor $\mathtt{td}$.




$$|\mathcal{D}| = |\mathcal{C}|$$

# Lossy Trapdoor Function (LTDF)



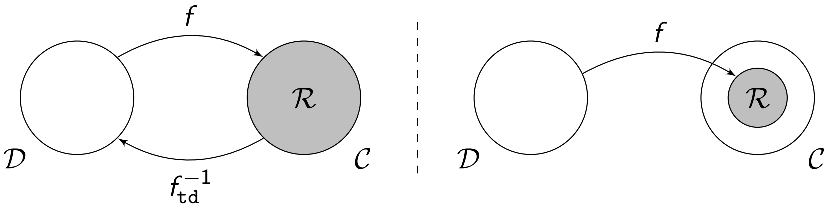

$(f, \texttt{td}) \leftarrow InjGen(1^k)$ $\simeq$ indist. $\simeq$ $f \leftarrow LossyGen(1^k)$

## Definition: LTDF

A Lossy Trapdoor Function (LTDF) consists of

- an (injective) generation procedure *InjGen* as for a classical TDF
- a lossy generation procedure $f \leftarrow LossyGen(1^k)$ such that $f$ has range smaller than domain by a factor $\ell$.

# Lossy Trapdoor Function (LTDF)




$$(f, \mathtt{td}) \leftarrow \mathit{InjGen}(1^k) \quad \simeq \text{indist.} \simeq \quad f \leftarrow \mathit{LossyGen}(1^k)$$

Security requirement:

Lossy and injective functions must be computationally hard to distinguish:

$$\Big| \Pr[(f, \mathtt{td}) \leftarrow \mathit{InjGen}(1^k) : \mathcal{D}(f) = 1] - \Pr[f \leftarrow \mathit{LossyGen}(1^k) : \mathcal{D}(f) = 1] \Big| = \mathtt{negl}(k)$$

# Certified TDF

**Definition (Certified TDF)**

A TDF $(f, \mathtt{td}) \leftarrow \mathit{InjGen}(1^k)$ is said to be certified if there exists a polynomial-time algorithm which tells whether $f$ (possibly adversarially generated) is injective or not

A certified TDF is "somehow" the opposite of a lossy TDF:

TDF is certified $\Longrightarrow$ TDF cannot be lossy

# Certified TDF

**Definition (Certified TDF)**

A TDF $(f, \mathtt{td}) \leftarrow \mathit{InjGen}(1^k)$ is said to be certified if there exists a polynomial-time algorithm which tells whether $f$ (possibly adversarially generated) is injective or not

A certified TDF is "somehow" the opposite of a lossy TDF:

$$\text{TDF is certified} \Longrightarrow \text{TDF cannot be lossy}$$

# The RSA example

## Injective RSA trapdoor function

- pick $N = pq$, with $p, q$ distinct primes
- pick prime $e \geq 3$ with $\gcd(e, \phi(N)) = 1$
- compute $d = e^{-1} \bmod \phi(N)$
- return $(N, e)$ defining $f : x \mapsto x^e \bmod N$ and $\mathtt{td} = d$

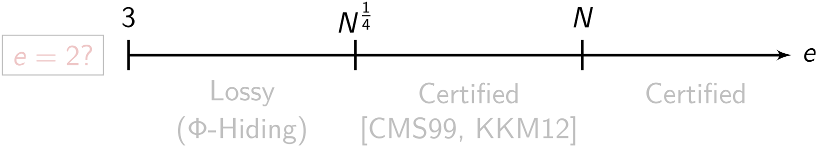
$\Rightarrow f$ is injective over $\mathbb{Z}_N^*$

## Lossy RSA function

- pick $N = pq$ with $p, q$ distinct primes
- pick prime $e \geq 3$ such that $e$ divides $\phi(N)$
- return $(N, e)$ defining $f : x \mapsto x^e \bmod N$

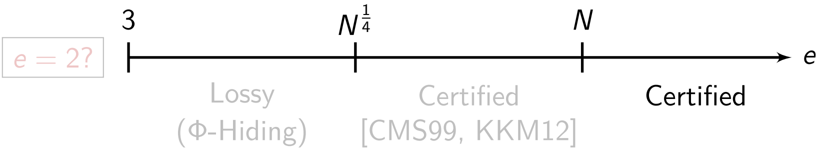
$\Rightarrow f$ is (at least) $e$-to-1 over $\mathbb{Z}_N^*$

# RSA: lossy or certified?



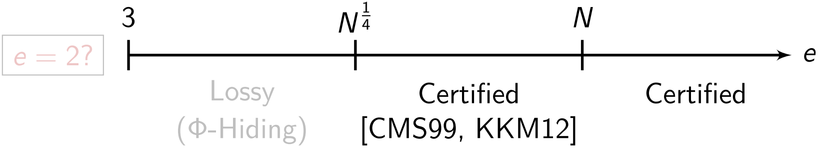

- if $e$ prime and $e > N$, then $e$ must be co-prime with $\phi(N)$
  $\Rightarrow$ certified
- if $e|\phi(N)$, $N^{\frac{1}{4}} < e < N$, Coppersmith alg. allows to factorize $N$
  $\Rightarrow$ certified
- for $e < N^{\frac{1}{4}}$, it is assumed hard to tell, given $(N, e)$, whether $\gcd(e, \phi(N)) = 1$ or $e|\phi(N)$ (Φ-Hiding assumption [CMS99])
  $\Rightarrow$ lossy

# RSA: lossy or certified?



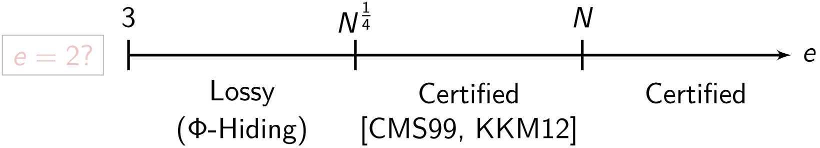

- if $e$ prime and $e > N$, then $e$ must be co-prime with $\phi(N)$
  $\Rightarrow$ certified
- if $e|\phi(N)$, $N^{\frac{1}{4}} < e < N$, Coppersmith alg. allows to factorize $N$
  $\Rightarrow$ certified
- for $e < N^{\frac{1}{4}}$, it is assumed hard to tell, given $(N, e)$, whether $\gcd(e, \phi(N)) = 1$ or $e|\phi(N)$ (Φ-Hiding assumption [CMS99])
  $\Rightarrow$ lossy

# RSA: lossy or certified?



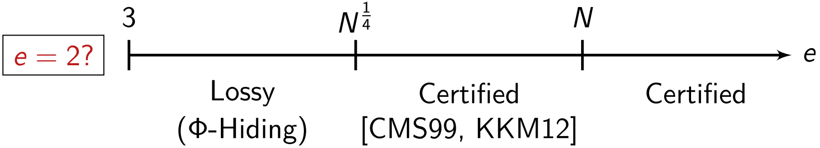

- if $e$ prime and $e > N$, then $e$ must be co-prime with $\phi(N)$
  $\Rightarrow$ certified
- if $e|\phi(N)$, $N^{\frac{1}{4}} < e < N$, Coppersmith alg. allows to factorize $N$
  $\Rightarrow$ certified
- for $e < N^{\frac{1}{4}}$, it is assumed hard to tell, given $(N, e)$, whether $\gcd(e, \phi(N)) = 1$ or $e|\phi(N)$ (Φ-Hiding assumption [CMS99])
  $\Rightarrow$ lossy

# RSA: lossy or certified?




- if $e$ prime and $e > N$, then $e$ must be co-prime with $\phi(N)$
  $\Rightarrow$ certified
- if $e|\phi(N)$, $N^{\frac{1}{4}} < e < N$, Coppersmith alg. allows to factorize $N$
  $\Rightarrow$ certified
- for $e < N^{\frac{1}{4}}$, it is assumed hard to tell, given $(N, e)$, whether $\gcd(e, \phi(N)) = 1$ or $e|\phi(N)$ (Φ-Hiding assumption [CMS99])
  $\Rightarrow$ lossy

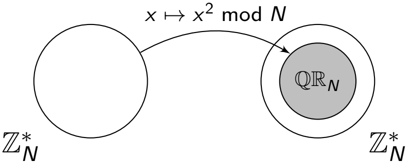
# RSA: lossy or certified?




- if $e$ prime and $e > N$, then $e$ must be co-prime with $\phi(N)$
  $\Rightarrow$ certified
- if $e|\phi(N)$, $N^{\frac{1}{4}} < e < N$, Coppersmith alg. allows to factorize $N$
  $\Rightarrow$ certified
- for $e < N^{\frac{1}{4}}$, it is assumed hard to tell, given $(N, e)$, whether $\gcd(e, \phi(N)) = 1$ or $e|\phi(N)$ (Φ-Hiding assumption [CMS99])
  $\Rightarrow$ lossy

# What about $e = 2$? The Rabin TDF

Modular squaring is never injective over $\mathbb{Z}_N^*$, it is 4-to-1



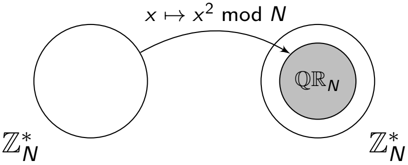

### Theorem (Blum)

*If $N = pq$ is a Blum integer (i.e., $p, q = 3 \bmod 4$), then any quadratic residue has a unique square root which is also a q.r., called its principal square root.*

$\Rightarrow$ when $N$ is Blum, modular squaring is 1-to-1 over $\mathbb{QR}_N$

# What about $e = 2$? The Rabin TDF

Modular squaring is never injective over $\mathbb{Z}_N^*$, it is 4-to-1




**Theorem (Blum)**

*If $N = pq$ is a Blum integer (i.e., $p, q = 3 \bmod 4$), then any quadratic residue has a unique square root which is also a q.r., called its principal square root.*

$\Rightarrow$ when $N$ is Blum, modular squaring is 1-to-1 over $\mathbb{QR}_N$

# What about $e = 2$? The Rabin TDF

Problem: $\mathbb{QR}_N$ is not (known to be) efficiently recognizable without $(p, q)$ (Quadratic Residuosity Assumption)

Another way to make Rabin injective is to restrict the domain to

$$(\mathbb{J}_N)^+ \stackrel{\text{def}}{=} \{1 \leq x \leq (N-1)/2 : \left(\frac{N}{x}\right) = 1\} = \{|x \bmod N| : x \in \mathbb{QR}_N\}$$

$\left(\frac{N}{x}\right)$ = Jacobi symbol, efficiently computable without $(p, q)$
$\Rightarrow (\mathbb{J}_N)^+$ is efficiently recognizable

**Theorem**

*If $N = pq$ is a Blum integer (i.e., $p, q = 3 \bmod 4$), then any quadratic residue has a unique square root in $(\mathbb{J}_N)^+$, called its absolute principal square root.*

$\Rightarrow$ when $N$ is Blum, modular squaring is injective over $(\mathbb{J}_N)^+$

# What about $e = 2$? The Rabin TDF

Problem: $\mathbb{QR}_N$ is not (known to be) efficiently recognizable without $(p, q)$ (Quadratic Residuosity Assumption)

Another way to make Rabin injective is to restrict the domain to

$$(\mathbb{J}_N)^+ \stackrel{\text{def}}{=} \{1 \leq x \leq (N-1)/2 : \left(\frac{N}{x}\right) = 1\} = \{|x \bmod N| : x \in \mathbb{QR}_N\}$$

$\left(\frac{N}{x}\right)$ = Jacobi symbol, efficiently computable without $(p, q)$
$\Rightarrow (\mathbb{J}_N)^+$ is efficiently recognizable

**Theorem**

*If $N = pq$ is a Blum integer (i.e., $p, q = 3 \bmod 4$), then any quadratic residue has a unique square root in $(\mathbb{J}_N)^+$, called its absolute principal square root.*

$\Rightarrow$ when $N$ is Blum, modular squaring is injective over $(\mathbb{J}_N)^+$

# What about $e = 2$? The Rabin TDF

Problem: $\mathbb{QR}_N$ is not (known to be) efficiently recognizable without $(p, q)$ (Quadratic Residuosity Assumption)

Another way to make Rabin injective is to restrict the domain to

$$(\mathbb{J}_N)^+ \stackrel{\text{def}}{=} \{1 \leq x \leq (N-1)/2 : \left(\frac{N}{x}\right) = 1\} = \{|x \bmod N| : x \in \mathbb{QR}_N\}$$

$\left(\frac{N}{x}\right)$ = Jacobi symbol, efficiently computable without $(p, q)$
$\Rightarrow (\mathbb{J}_N)^+$ is efficiently recognizable

### Theorem

*If $N = pq$ is a Blum integer (i.e., $p, q = 3 \bmod 4$), then any quadratic residue has a unique square root in $(\mathbb{J}_N)^+$, called its absolute principal square root.*

$\Rightarrow$ when $N$ is Blum, modular squaring is injective over $(\mathbb{J}_N)^+$

# Making Rabin lossy

**Theorem**

*If $N = pq$ with $p, q = 1 \bmod 4$ (pseudo-Blum integer), then any $x \in \mathbb{QR}_N$ has its four square roots either:*

- *all in $\mathbb{QR}_N$*
- *all in $\mathbb{J}_N \setminus \mathbb{QR}_N$*
- *all in $\mathbb{Z}_N^* \setminus \mathbb{J}_N$*

Hence when $N = pq$ with $p, q = 1 \bmod 4$, modular squaring is

- 4-to-1 over $\mathbb{QR}_N$
- 2-to-1 over $(\mathbb{J}_N)^+$

# Making Rabin lossy

**Theorem**

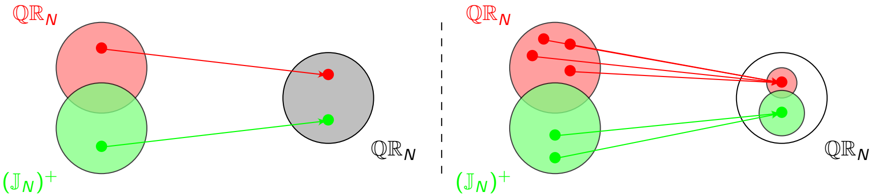
*If $N = pq$ with $p, q = 1 \bmod 4$ (pseudo-Blum integer), then any $x \in \mathbb{QR}_N$ has its four square roots either:*

- *all in $\mathbb{QR}_N$*
- *all in $\mathbb{J}_N \setminus \mathbb{QR}_N$*
- *all in $\mathbb{Z}_N^* \setminus \mathbb{J}_N$*

Hence when $N = pq$ with $p, q = 1 \bmod 4$, modular squaring is

- 4-to-1 over $\mathbb{QR}_N$
- 2-to-1 over $(\mathbb{J}_N)^+$

# Injective vs. lossy Rabin



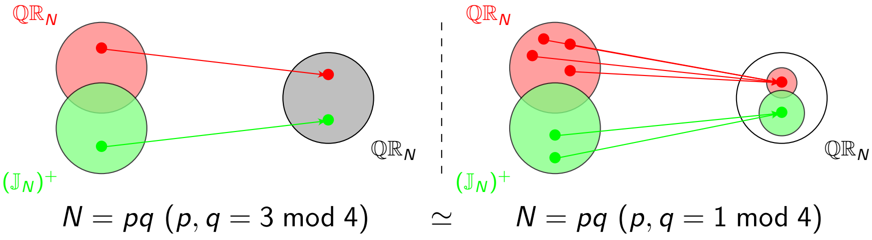

$N = pq$ $(p, q = 3 \bmod 4)$ $\simeq$ $N = pq$ $(p, q = 1 \bmod 4)$

## 2-$\Phi$/4-Hiding Assumption

Given $N = pq$ with $N = 1 \bmod 4$, it is hard to distinguish whether $p, q = 3 \bmod 4$ (Blum) or $p, q = 1 \bmod 4$ (pseudo-Blum)
$\Leftrightarrow$ distinguish whether $\gcd(2, \phi(N)/4) = 1$ or 2 divides $\phi(N)/4$
$\Leftrightarrow$ distinguish whether $-1$ is a quadratic residue mod $N$ or not

2-$\Phi$/4-Hiding $\leq$ Quadratic Residuosity $\leq$ Factoring

# Injective vs. lossy Rabin




## 2-Φ/4-Hiding Assumption

Given $N = pq$ with $N = 1 \bmod 4$, it is hard to distinguish whether $p, q = 3 \bmod 4$ (Blum) or $p, q = 1 \bmod 4$ (pseudo-Blum)
$\Leftrightarrow$ distinguish whether $\gcd(2, \phi(N)/4) = 1$ or 2 divides $\phi(N)/4$
$\Leftrightarrow$ distinguish whether $-1$ is a quadratic residue mod $N$ or not

2-Φ/4-Hiding $\leq$ Quadratic Residuosity $\leq$ Factoring

# Outline

1. Lossiness of the Rabin Trapdoor Function
2. Application to Rabin-Williams-FDH Signatures
3. Extending the Coron-Kakvi-Kiltz Meta-Reduction Result

# FDH signatures based on an arbitrary TDF

### Full Domain Hash signature scheme

Let $(f, f_{\mathtt{td}}^{-1})$ be a TDF with range $\mathcal{R}$, and $H : \{0,1\}^* \to \mathcal{R}$ be a hash function. The FDH signature scheme based on TDF is as follows:

- key generation: private key is $f_{\mathtt{td}}^{-1}$, public key is $f$.
- signing message $m$: compute $h = H(m)$ and $\sigma = f_{\mathtt{td}}^{-1}(h)$, return $\sigma$
- verification of $(m, \sigma)$: check that $f(\sigma) = H(m)$

# FDH signatures based on an arbitrary TDF

## Security of FDH (EUF-CMA in the Random Oracle model)

- [BR93]: reduction from the one-wayness of $f$, loosing factor $q_h$
- [Cor00]: idem, but loosing only a factor $q_s$
- [Cor02]: loosing a factor $q_s$ is unavoidable ("meta-reduction" result)
- [KK12]: previous result only holds if $f$ is certified
- [KK12]: tight reduction from the lossiness of $f$

| Reduction from | Certified TDF | Lossy TDF |
|---|---|---|
| One-wayness | $q_s$-loose (opt.) | ?? |
| Lossiness | NA | tight |

$\Rightarrow$ RSA-FDH with $e < N^{\frac{1}{4}}$ has a tight reduction from $\Phi$-Hiding assumption [KK12]

# FDH signatures based on an arbitrary TDF

## Security of FDH (EUF-CMA in the Random Oracle model)

- [BR93]: reduction from the one-wayness of $f$, loosing factor $q_h$
- [Cor00]: idem, but loosing only a factor $q_s$
- [Cor02]: loosing a factor $q_s$ is unavoidable ("meta-reduction" result)
- [KK12]: previous result only holds if $f$ is certified
- [KK12]: tight reduction from the lossiness of $f$

| Reduction from | Certified TDF | Lossy TDF |
|---|---|---|
| One-wayness | $q_s$-loose (opt.) | ?? |
| Lossiness | NA | tight |

$\Rightarrow$ RSA-FDH with $e < N^{\frac{1}{4}}$ has a tight reduction from Φ-Hiding assumption [KK12]

# FDH signatures based on an arbitrary TDF

## Security of FDH (EUF-CMA in the Random Oracle model)

- [BR93]: reduction from the one-wayness of $f$, loosing factor $q_h$
- [Cor00]: idem, but loosing only a factor $q_s$
- [Cor02]: loosing a factor $q_s$ is unavoidable ("meta-reduction" result)
- [KK12]: previous result only holds if $f$ is certified
- [KK12]: tight reduction from the lossiness of $f$

| Reduction from | Certified TDF | Lossy TDF |
|---|---|---|
| One-wayness | $q_s$-loose (opt.) | ?? |
| Lossiness | NA | tight |

$\Rightarrow$ RSA-FDH with $e < N^{\frac{1}{4}}$ has a tight reduction from $\Phi$-Hiding assumption [KK12]

# FDH signatures based on an arbitrary TDF

## Security of FDH (EUF-CMA in the Random Oracle model)

- [BR93]: reduction from the one-wayness of $f$, loosing factor $q_h$
- [Cor00]: idem, but loosing only a factor $q_s$
- [Cor02]: loosing a factor $q_s$ is unavoidable ("meta-reduction" result)
- [KK12]: previous result only holds if $f$ is certified
- [KK12]: tight reduction from the lossiness of $f$

| Reduction from | Certified TDF | Lossy TDF |
|---|---|---|
| One-wayness | $q_s$-loose (opt.) | ?? |
| Lossiness | NA | tight |

$\Rightarrow$ RSA-FDH with $e < N^{\frac{1}{4}}$ has a tight reduction from $\Phi$-Hiding assumption [KK12]

# FDH signatures based on an arbitrary TDF

## Security of FDH (EUF-CMA in the Random Oracle model)

- [BR93]: reduction from the one-wayness of $f$, loosing factor $q_h$
- [Cor00]: idem, but loosing only a factor $q_s$
- [Cor02]: loosing a factor $q_s$ is unavoidable ("meta-reduction" result)
- [KK12]: previous result only holds if $f$ is certified
- [KK12]: tight reduction from the lossiness of $f$

| Reduction from | Certified TDF | Lossy TDF |
|---|---|---|
| One-wayness | $q_s$-loose (opt.) | ?? |
| Lossiness | NA | tight |

$\Rightarrow$ RSA-FDH with $e < N^{\frac{1}{4}}$ has a tight reduction from $\Phi$-Hiding assumption [KK12]

# FDH signatures based on an arbitrary TDF

## Security of FDH (EUF-CMA in the Random Oracle model)

- [BR93]: reduction from the one-wayness of $f$, loosing factor $q_h$
- [Cor00]: idem, but loosing only a factor $q_s$
- [Cor02]: loosing a factor $q_s$ is unavoidable ("meta-reduction" result)
- [KK12]: previous result only holds if $f$ is certified
- [KK12]: tight reduction from the lossiness of $f$

| Reduction from | Certified TDF | Lossy TDF |
|---|---|---|
| One-wayness | $q_s$-loose (opt.) | ?? |
| Lossiness | NA | tight |

$\Rightarrow$ RSA-FDH with $e < N^{\frac{1}{4}}$ has a tight reduction from $\Phi$-Hiding assumption [KK12]

# FDH signatures based on an arbitrary TDF

## Security of FDH (EUF-CMA in the Random Oracle model)

- [BR93]: reduction from the one-wayness of $f$, loosing factor $q_h$
- [Cor00]: idem, but loosing only a factor $q_s$
- [Cor02]: loosing a factor $q_s$ is unavoidable ("meta-reduction" result)
- [KK12]: previous result only holds if $f$ is certified
- [KK12]: tight reduction from the lossiness of $f$

| Reduction from | Certified TDF | Lossy TDF |
|---|---|---|
| One-wayness | $q_s$-loose (opt.) | ?? |
| Lossiness | NA | tight |

$\Rightarrow$ RSA-FDH with $e < N^{\frac{1}{4}}$ has a tight reduction from $\Phi$-Hiding assumption [KK12]

# Rabin-Williams-FDH signatures

Rabin-FDH = FDH with TDF $f : x \mapsto x^2 \bmod N$
$\Rightarrow$ public key is $N = pq$, signature is "some" square root of $H(m)$

- problem: range $\mathcal{R}$ of the TDF is $\mathbb{QR}_N$, not $\mathbb{Z}_N^*$!
- hashing a message yields a quadratic residue for only $\sim 1/4$ of messages
- probabilistic fix: use a random salt, and compute $h = H(r, m)$ for $r$ random until $h \in \mathbb{QR}_N$ (4 attempts on average)
- deterministic fix: use a tweaked square root

**Fact**

If $N = pq$ with $p = 3 \bmod 8$ and $q = 7 \bmod 8$ (Williams integer), then for any $h \in \mathbb{Z}_N^*$, there is a unique $\alpha \in \{1, -1, 2, -2\}$ such that $\alpha^{-1} h \in \mathbb{QR}_N$

Signature of $m$: $\sigma = (\alpha, s)$ such that (Verif.) $\alpha s^2 = H(m) \bmod N$

# Rabin-Williams-FDH signatures

Rabin-FDH = FDH with TDF $f : x \mapsto x^2 \bmod N$
$\Rightarrow$ public key is $N = pq$, signature is "some" square root of $H(m)$

- problem: range $\mathcal{R}$ of the TDF is $\mathbb{QR}_N$, not $\mathbb{Z}_N^*$!
- hashing a message yields a quadratic residue for only $\sim 1/4$ of messages
- probabilistic fix: use a random salt, and compute $h = H(r, m)$ for $r$ random until $h \in \mathbb{QR}_N$ (4 attempts on average)
- deterministic fix: use a tweaked square root

**Fact**

If $N = pq$ with $p = 3 \bmod 8$ and $q = 7 \bmod 8$ (Williams integer), then for any $h \in \mathbb{Z}_N^*$, there is a unique $\alpha \in \{1, -1, 2, -2\}$ such that $\alpha^{-1}h \in \mathbb{QR}_N$

Signature of $m$: $\sigma = (\alpha, s)$ such that (Verif.) $\alpha s^2 = H(m) \bmod N$

# Rabin-Williams-FDH signatures: square root selection

**Problem: square root selection**

Given $h = H(m)$ and the tweak $\alpha$, which of the 4 square roots of $\alpha^{-1}H(m) \in \mathbb{QR}_N$ should be returned as the signature?

Two solutions:

- probabilistic: choose sq. root randomly ("Fixed Unstructured" [Ber08]), but always return the same when signing twice!
  - ☹ stateful, or requires an additional PRF to choose pseudorandomly
  - ☺ tight reduction from Factoring [Ber08]
- deterministic: use a Blum integer $N$, and always return
  - the principal square root $s \in \mathbb{QR}_N$ (PRW scheme)
  - the absolute principal square root $s \in (\mathbb{J}_N)^+$ (APRW scheme)
  - ☺ stateless and fully deterministic scheme
  - ☹ $q_s$-loose reduction from Factoring [Ber08]

# Rabin-Williams-FDH signatures: square root selection

**Problem: square root selection**

Given $h = H(m)$ and the tweak $\alpha$, which of the 4 square roots of $\alpha^{-1}H(m) \in \mathbb{QR}_N$ should be returned as the signature?

Two solutions:

- probabilistic: choose sq. root randomly ("Fixed Unstructured" [Ber08]), but always return the same when signing twice!
  ☹ stateful, or requires an additional PRF to choose pseudorandomly
  ☺ tight reduction from Factoring [Ber08]
- deterministic: use a Blum integer $N$, and always return
  - the principal square root $s \in \mathbb{QR}_N$ (PRW scheme)
  - the absolute principal square root $s \in (\mathbb{J}_N)^+$ (APRW scheme)

  ☺ stateless and fully deterministic scheme
  ☹ $q_s$-loose reduction from Factoring [Ber08]

# Rabin-Williams-FDH signatures: square root selection

## Problem: square root selection

Given $h = H(m)$ and the tweak $\alpha$, which of the 4 square roots of $\alpha^{-1}H(m) \in \mathbb{QR}_N$ should be returned as the signature?

Two solutions:

- probabilistic: choose sq. root randomly ("Fixed Unstructured" [Ber08]), but always return the same when signing twice!
  ☹ stateful, or requires an additional PRF to choose pseudorandomly
  ☺ tight reduction from Factoring [Ber08]
- deterministic: use a Blum integer $N$, and always return
  - the principal square root $s \in \mathbb{QR}_N$ (PRW scheme)
  - the absolute principal square root $s \in (\mathbb{J}_N)^+$ (APRW scheme)

  ☺ stateless and fully deterministic scheme
  ☹ $q_s$-loose reduction from Factoring [Ber08]

# Tight reduction for PRW and APRW signatures

**Observation**

The PRW and APRW schemes are exactly FDH schemes with TDF:

- modular squaring with domain $\mathbb{QR}_N$ for PRW
- modular squaring with domain $(\mathbb{J}_N)^+$ for APRW

# Tight reduction for PRW and APRW signatures

**Theorem ([KK12])**

*The TDF-FDH scheme has a tight reduction from the lossiness of TDF*

**Theorem**

*Modular squaring with domain $\mathbb{QR}_N$ or $(\mathbb{J}_N)^+$ is a lossy TDF under the 2-$\Phi/4$-Hiding assumption*

$$\Downarrow$$

**Theorem**

*The PRW and APRW schemes have a tight reduction from the 2-$\Phi/4$-Hiding assumption*

# Tight reduction for PRW and APRW signatures

**Theorem ([KK12])**

*The TDF-FDH scheme has a tight reduction from the lossiness of TDF*

**Theorem**

*Modular squaring with domain $\mathbb{QR}_N$ or $(\mathbb{J}_N)^+$ is a lossy TDF under the 2-$\Phi/4$-Hiding assumption*

$$\Downarrow$$

**Theorem**

*The PRW and APRW schemes have a tight reduction from the 2-$\Phi/4$-Hiding assumption*

# Outline


1. Lossiness of the Rabin Trapdoor Function
2. Application to Rabin-Williams-FDH Signatures
3. Extending the Coron-Kakvi-Kiltz Meta-Reduction Result

# What about tight reductions from Factoring?

We know that PRW and APRW signature schemes have:

- a tight reduction from the 2-$\Phi$/4-Hiding assumption
- a $q_s$-loose reduction from the Factoring assumption

**Natural question**

Could there be a tight reduction for these schemes from the Factoring assumption?

# What about tight reductions from Factoring?

We know that PRW and APRW signature schemes have:

- a tight reduction from the 2-$\Phi$/4-Hiding assumption
- a $q_s$-loose reduction from the Factoring assumption

**Natural question**

Could there be a tight reduction for these schemes from the Factoring assumption?

# The Coron-Kakvi-Kiltz Meta-reduction

**Theorem ([Cor02, KK12])**

*If TDF-FDH has a tight (black-box) reduction from one-wayness of TDF and if TDF is certified lossy, then there exists an algorithm (meta-reduction) breaking one-wayness of TDF with the help of a lossiness decision oracle*

*(⇒ $q_s$-loose reduction is optimal assuming inverting TDF with the help of a lossiness decision oracle is hard).*

| Reduction from | Certified TDF | Lossy TDF |
|---|---|---|
| One-wayness | $q_s$-loose (opt.) | ?? |
| Lossiness | NA | tight |

* assuming inverting TDF with the help of a lossiness decision oracle is hard

# The Coron-Kakvi-Kiltz Meta-reduction

**Theorem ([Cor02, KK12] (extended))**

*If TDF-FDH has a tight (black-box) reduction from one-wayness of TDF and if TDF is certified lossy, then there exists an algorithm (meta-reduction) breaking one-wayness of TDF with the help of a lossiness decision oracle*

*($\Rightarrow$ $q_s$-loose reduction is optimal assuming inverting TDF with the help of a lossiness decision oracle is hard).*

| Reduction from | Certified TDF | Lossy TDF |
|---|---|---|
| One-wayness | $q_s$-loose (opt.) | ?? |
| Lossiness | NA | tight |

* assuming inverting TDF with the help of a lossiness decision oracle is hard

# The Coron-Kakvi-Kiltz Meta-reduction

**Theorem ([Cor02, KK12] (extended))**

*If TDF-FDH has a tight (black-box) reduction from one-wayness of TDF and if TDF is certified lossy, then there exists an algorithm (meta-reduction) breaking one-wayness of TDF with the help of a lossiness decision oracle*

*(⇒ $q_s$-loose reduction is optimal assuming inverting TDF with the help of a lossiness decision oracle is hard).*

| Reduction from | Certified TDF | Lossy TDF |
|---|---|---|
| One-wayness | $q_s$-loose (opt.) | $q_s$-loose (opt.*) |
| Lossiness | NA | tight |

* assuming inverting TDF with the help of a lossiness decision oracle is hard

# Conclusion

- new Lossy Trapdoor Function (modular squaring) under a plausible extension of the Φ-Hiding assumption, the 2-Φ/4-Hiding assumption

- completed landscape of security reductions for Rabin-FDH variants

| Square root selection method | Reduction from Factoring | Reduction from 2-Φ/4-Hiding |
|---|---|---|
| (pseudo)-random | tight [Ber08] | — |
| (absolute) principal | $q_s$-loose (opt.*) | tight |

* assuming that factoring with a 2-Φ/4-Hiding decision oracle is hard

# Conclusion

- new Lossy Trapdoor Function (modular squaring) under a plausible extension of the Φ-Hiding assumption, the 2-Φ/4-Hiding assumption
- completed landscape of security reductions for Rabin-FDH variants

| Square root selection method | Reduction from Factoring | Reduction from 2-Φ/4-Hiding |
|---|---|---|
| (pseudo)-random | tight [Ber08] | — |
| (absolute) principal | $q_s$-loose (opt.*) | tight |

* assuming that factoring with a 2-Φ/4-Hiding decision oracle is hard

# The end. . .

Thanks for your attention!
Comments or questions?

# References I


Daniel J. Bernstein.

Proving Tight Security for Rabin-Williams Signatures.

In Nigel P. Smart, editor, *Advances in Cryptology - EUROCRYPT 2008*, volume 4965 of *Lecture Notes in Computer Science*, pages 70–87. Springer, 2008.

Mihir Bellare and Phillip Rogaway.

Random Oracles are Practical: A Paradigm for Designing Efficient Protocols.

In *ACM Conference on Computer and Communications Security*, pages 62–73, 1993.

Christian Cachin, Silvio Micali, and Markus Stadler.

Computationally Private Information Retrieval with Polylogarithmic Communication.

In Jacques Stern, editor, *Advances in Cryptology - EUROCRYPT '99*, volume 1592 of *Lecture Notes in Computer Science*, pages 402–414. Springer, 1999.

# References II


Jean-Sébastien Coron.
On the Exact Security of Full Domain Hash.
In Mihir Bellare, editor, *Advances in Cryptology - CRYPTO 2000*, volume 1880 of *Lecture Notes in Computer Science*, pages 229–235. Springer, 2000.

Jean-Sébastien Coron.
Optimal Security Proofs for PSS and Other Signature Schemes.
In Lars R. Knudsen, editor, *Advances in Cryptology - EUROCRYPT 2002*, volume 2332 of *Lecture Notes in Computer Science*, pages 272–287. Springer, 2002.

Saqib A. Kakvi and Eike Kiltz.
Optimal Security Proofs for Full Domain Hash, Revisited.
In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology - EUROCRYPT 2012*, volume 7237 of *Lecture Notes in Computer Science*, pages 537–553. Springer, 2012.

# References III

Saqib A. Kakvi, Eike Kiltz, and Alexander May.

Certifying RSA.

In Xiaoyun Wang and Kazue Sako, editors, *Advances in Cryptology - ASIACRYPT 2012*, volume 7658 of *Lecture Notes in Computer Science*, pages 404–414. Springer, 2012.

Chris Peikert and Brent Waters.

Lossy trapdoor functions and their applications.

In Cynthia Dwork, editor, *Symposium on Theory of Computing - STOC 2008*, pages 187–196. ACM, 2008.