A Second Look at  ‘s Transformation

----

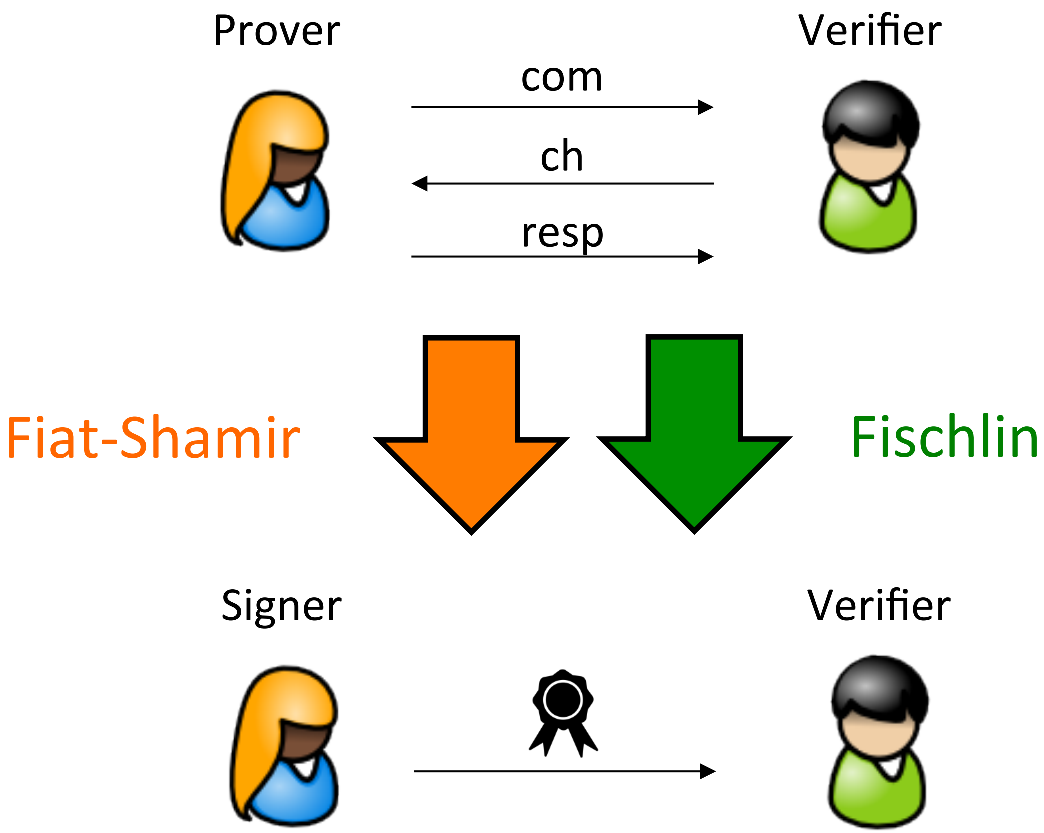
Özgür Dagdelen

Technische Universität Darmstadt

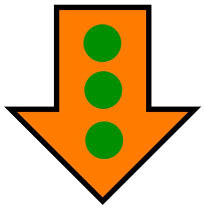
Daniele Venturi

Sapienza University of Rome

From Identication Schemes to Signature Schemes



Identification scheme is **passively secure**.



The resulting signature scheme is **unforgeable** in ROM.

[PS00,OO98,AABC02,F05]

Fiat-Shamir Transformation

Prover P		Verifier V
		
sk,pk ← KGen()		pk
com ← P(pk,sk;ϖ)	com →	
ch ← H(com,m)	← ch	$ch \leftarrow_R CH$
resp ← P(pk,sk,com,ch)	com,ch,resp →	0/1 ← V(pk,com,ch,resp)

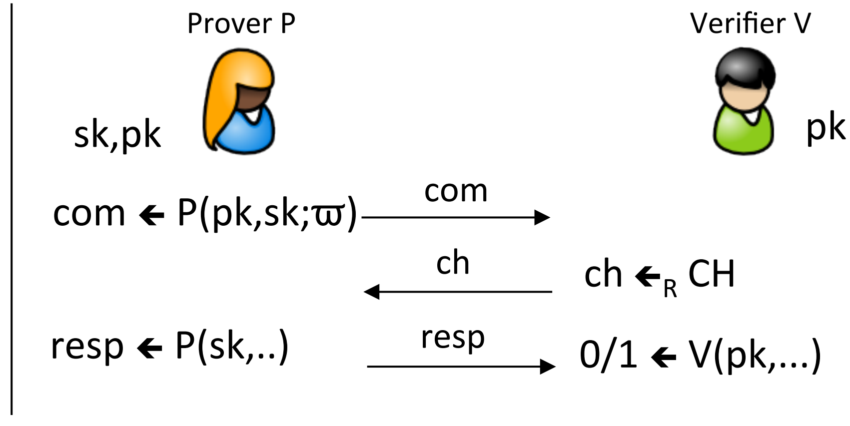
Security:

If H is modeled by a *random oracle* and the identification scheme is *passively secure*, the resulting signature scheme is *unforgeable*.

Fischlin's Transformation

Prover P

sk,pk ← KGen()



1. For all $i \in \{1,\ldots,r\}$: com_i ← P(pk,sk;ϖ)
2. For all $i \in \{1,\ldots,r\}$ and all $ch_i \in \{1,\ldots,2^{\mu}-1\}$
   a. Compute $resp_i$ ← P(pk,sk,com_i,ch_i)
   b. Let ch_i^*:=ch_i which satisfies H(m,pk,com_1,..com_r,i,ch_i,$resp_i$)=0^b
      (If there is no, take the minimum one)
3. Output σ = $(com_i, ch_i^*, resp_i)_{i=1,\ldots,r}$

Security:

If H is modeled by a *random oracle* and the identification scheme is *passively secure*, the resulting signature scheme is *unforgeable* but the reduction is tight !!

Depending on parameters r and b, the extractor in the security proof may fail

$$\varepsilon_{ext} \approx q_h 2^{(\log(e \cdot r/(r-1))-b)r}$$

The Comparison

Fiat-Shamir

Fischlin

- e

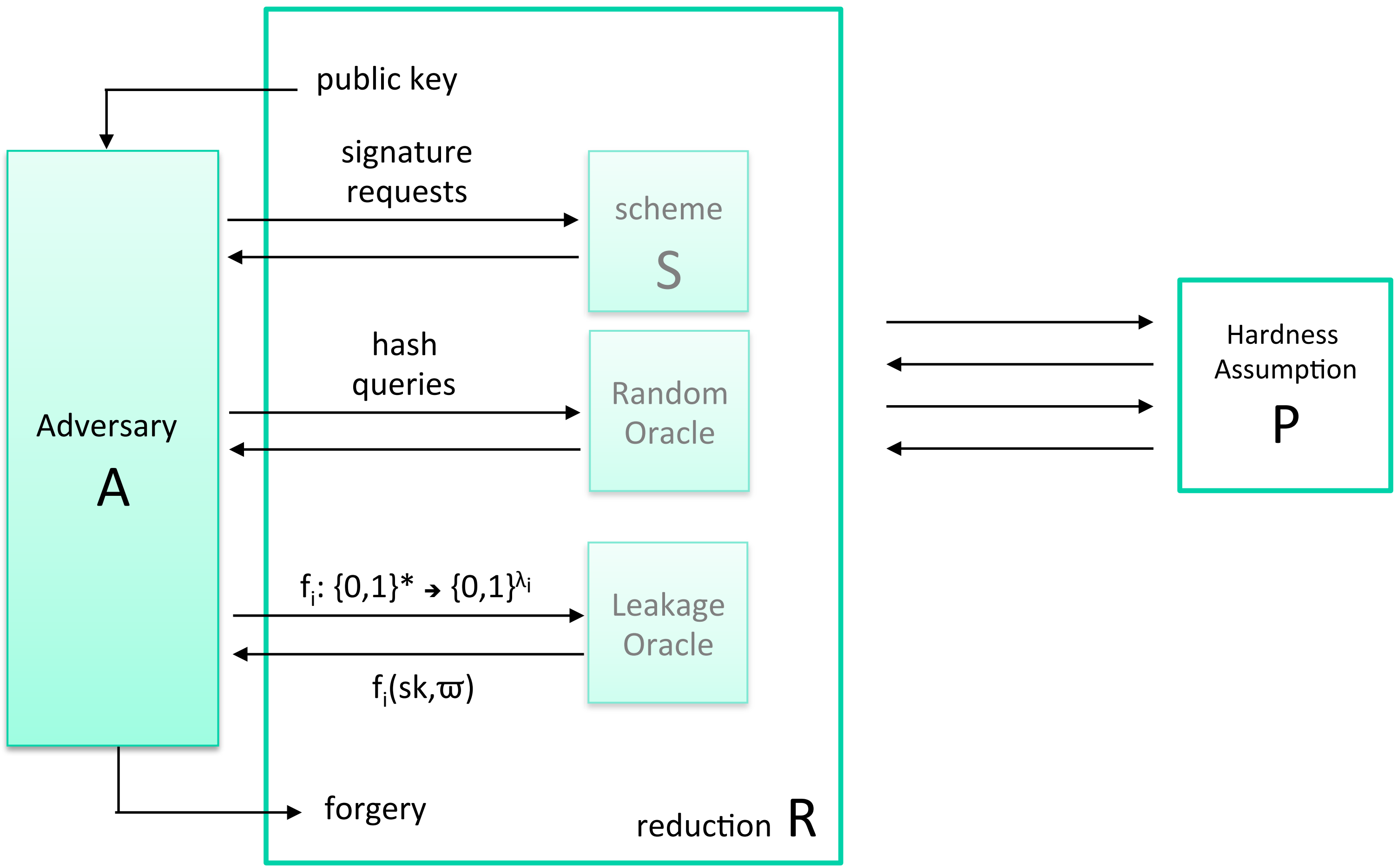
We ask ourselves ...

1. Is Fischlin's transform leakage-resilient?

2. Is Fischlin's transform quantum-resistant?

3. Does tightness compensate massive hash function evaluations?

The Model of Leakage Resilience



Definiton: *S* is secure against chosen message attacks and λ-leakage attacks if A outputs a forgery with negligble probability only with $\lambda = \lambda_1 + \ldots + \lambda_k$.

- Let Σ be an identification scheme for which there exists exponentially many secret keys to a given pk.

  Bsp: $sk = x_1, \ldots, x_n$ and $pk = g_1^{x_1} \bullet \ldots \bullet g_n^{x_n}$

Theorem [ADW09,KV09]**:**
The signature scheme derived by Fiat-Shamir applied on Σ is secure against chosen message attacks and λ-leackage attacks with $\lambda \approx (½ - 1/n)|sk|$.

Theorem [this work]**:**
The signature scheme derived by Fischlin applied on Σ is secure against chosen message attacks and λ-leackage attacks with $\lambda \approx (1 - 1/n)|sk|$.

Again tight !!

Example Instantiation

Cool! But which one is more efficient?

Example: Generalized Okamoto Scheme [Oka92]

Prover P

Verifier V

KGen(κ): pk=(g_1,g_2,…,g_n,h) and sk=(x_1,x_2,…,x_n) such that $h = \prod_{i=1}^{n} g_i^{x_i}$

$a_1,\ldots,a_n \leftarrow Z_p$

$com = \prod_{i=1}^{n} g_i^{a_i}$

com →

ch ←

$ch \leftarrow Z_p^*$

$$resp = \begin{pmatrix} ch \cdot x_1 + a_1 \\ \vdots \\ ch \cdot x_n + a_n \end{pmatrix}$$

resp →

Output 1 if $\prod_{i=1}^{n} g_i^{resp_i} = h^{ch} \cdot com$

Selecting Parameters

We work in Z_p^* where p=2p'+1 (safe prime)

Best attack: Number Field Sieve with complexity $e^{\sqrt[3]{64/9}(\ln p)^{1/3}(\ln\ln p)^{2/3}}$

Reduction Tightness:

FS: If A breaks S in time t' with probability ε',

then R solves DL in time t≈t' with probability $(\varepsilon')^2/q_h$

=> DL broken in time $t = t' q_h/(\varepsilon')^2$

Recall:
$$\varepsilon_{ext} \approx q_h 2^{(\log(e \cdot r/(r-1))-b)r}$$

Fischlin: If A breaks S in time t' with probability ε',

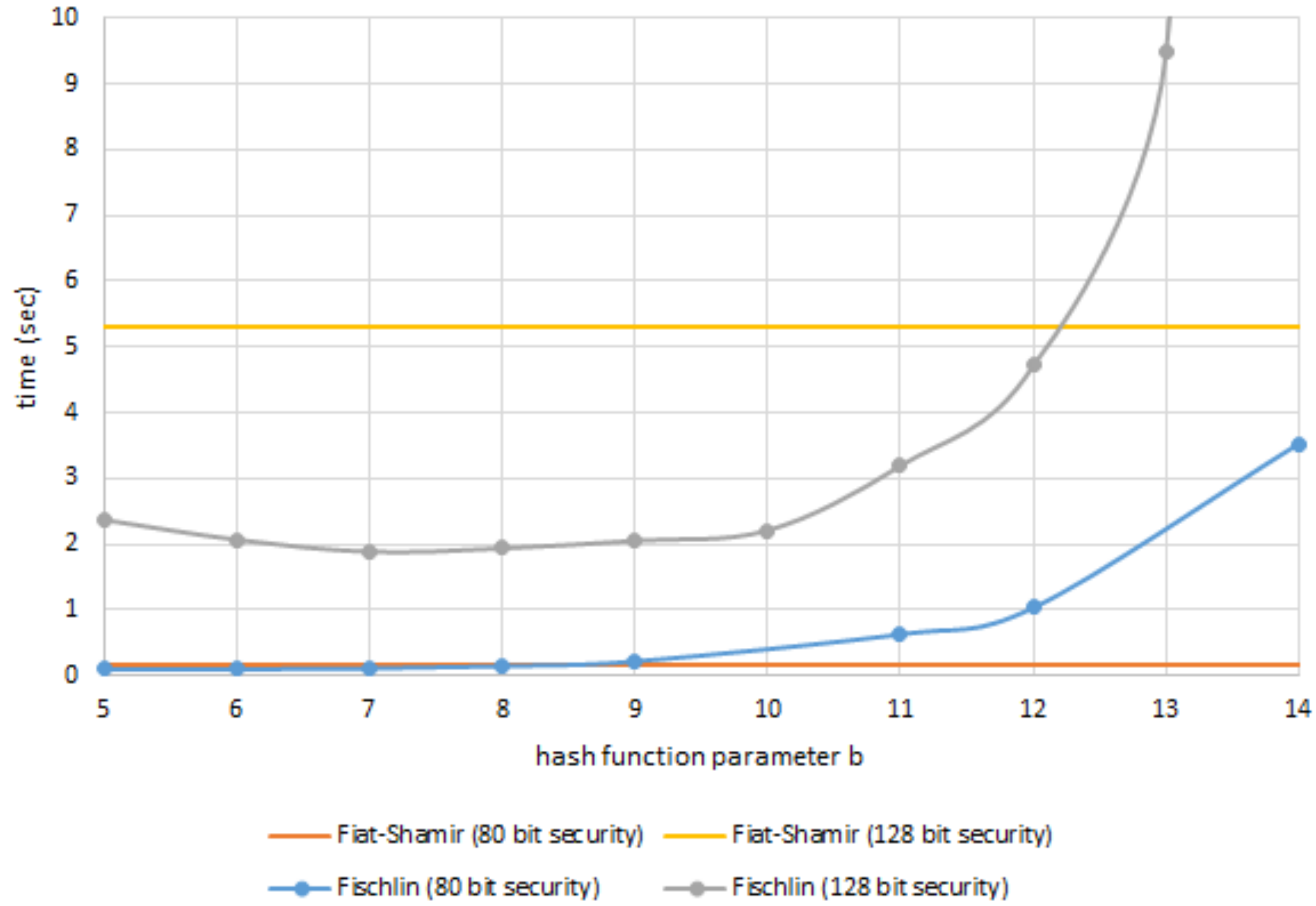
then R solves DL in time t≈t' with probability $\varepsilon' - \varepsilon_{ext} - 2^{-\kappa}$

=> DL broken in time t = t'/ε' if $\varepsilon_{ext} < \varepsilon'$

Selecting Parameters ... cont.

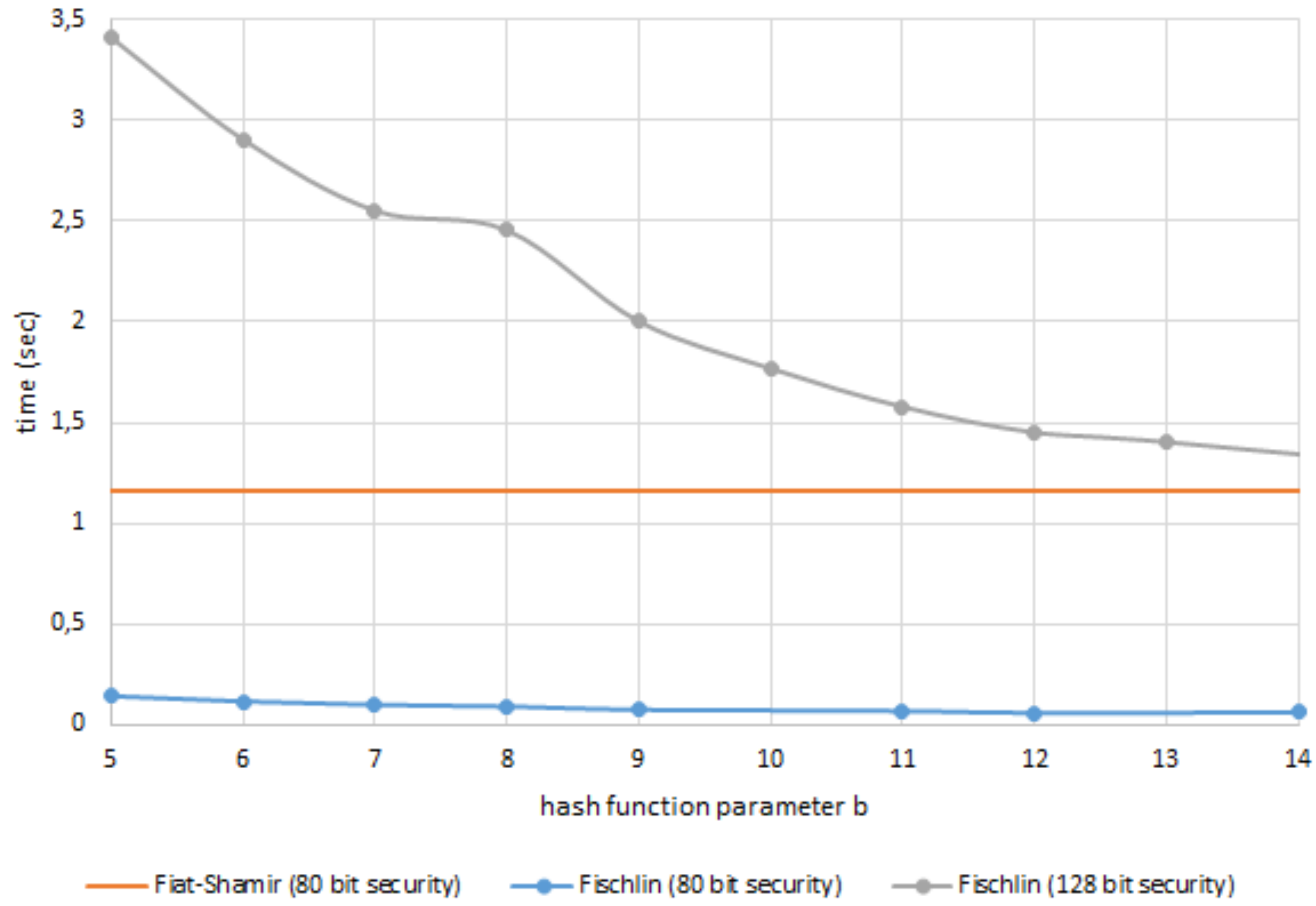
Size of modulus p	**80-bit security**	**128-bit security**
Fiat-Shamir	5400 bits	15000 bits
Fischlin	1130 bits	3048 bits

Signature Generation Performance



Signature sizes collide at b=12 (80) and b=19 (128).

Verification Performance



Signature sizes collide at b=12 (80) and b=19 (128).
FS needs 30.89 seconds for verification for 128 security bits.

Performance

	80-bit security				128-bit security			
	FS	Fischlin $r=7$ $b=12$	Fischlin $r=14$ $b=6$	Fischlin $r=6$ $b=14$	FS	Fischlin $r=7$ $b=19$	Fischlin $r=19$ $b=7$	Fischlin $r=11$ $b=12$
Signing time (in sec)	0.463	1.037	**0.103**	3.531	5.3	290.262	**1.889**	4.715
Verification (in sec)	1.16	**0.060**	0.117	0.062	30.89	**0.993**	2.552	1.451
Signature size (in kB)	1.98	1.94	3.87	**1.67**	5.49	**5.22**	14.15	8.2
Public-key size (in kB)	1.98	**0.41**	**0.41**	**0.41**	5.49	**1.12**	**1.12**	**1.12**
Secret-key size (in kB)	1.32	**0.28**	**0.28**	**0.28**	3.66	**0.37**	**0.37**	**0.37**

Table 1. Comparison between Fiat-Shamir (FS) and Fischlin for the Generalized Okamoto signature scheme. The table shows performance and sizes for $\ell = 2$.

- Fischlin has 80% shorter keys
- Fischlin is up to 30 times faster in verification
- Fischlin takes more time to sign,
  but if flexible in size, Fischlin is up to 4.5 times faster in signing.

Performance on Potential Leakage

Signature running time (in sec)	80-bit security			
	$\lambda \leq 1/4$	$\lambda \leq 3/8$	$\lambda \leq 7/16$	$\lambda \leq 3/4$
	$\ell = 2$	$\ell = 4$	$\ell = 8$	—
	$\ell' = 2$	$\ell' = 2$	$\ell' = 2$	$\ell' = 4$
	$\lvert\sigma\rvert \approx 1.98$	$\lvert\sigma\rvert \approx 3.3$	$\lvert\sigma\rvert \approx 5.93$	$\lvert\sigma\rvert \approx 5.52$
Fiat-Shamir (with ℓ)	0.463	0.951	1.858	—
Fischlin (with ℓ')	1.037	0.114	0.103*	0.287

Table 2. Comparison of Fischlin's transformation and the Fiat-Shamir transform for the Generalized Okamoto signature scheme, with different leakage parameter λ. Fischlin is instantiated with r and b such that the resulting signature size is comparable in both schemes. For the timing (*) we selected the fastest parameters r, b where the resulting signature size is even smaller.

A Second Look at the Comparison

Fiat-Shamir

- easy to implement
- proven secure (in ROM)
- leakage-resilient (non-tight)

- proof is non-tight
- leakage is non-tight
- Not (always) quantum resistant

Fischlin

- proven secure (in ROM)
- tight security reduction
- Leakage-resilient (tight) NEW!
- not so complicated (even faster than FS sometimes) NEW!

- Nothing known about its quantum resistance