NTNU

Norwegian University of Science and Technology

Formal Treatment of Practical Signature Schemes

From single to multi-user security for certain signature schemes

Magnus Ringerud

Department of mathematical sciences, NTNU

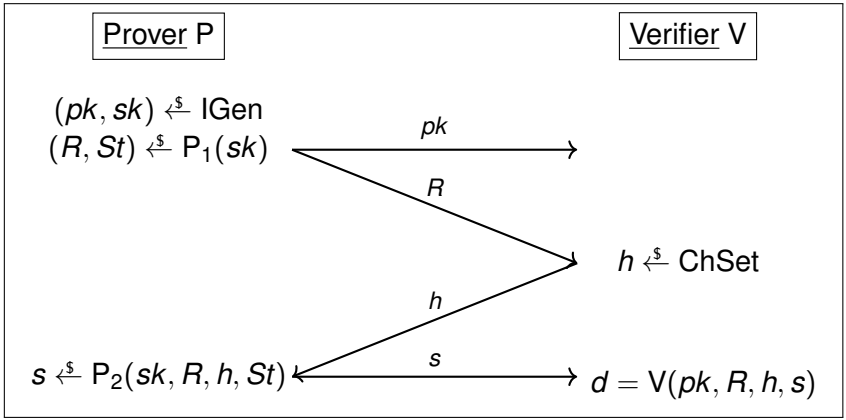
NTNU

Multi-user security

- Security notion UF-CMA
- Real world situation
- Multi-user setting
- Security notion MU-UF-CMA.

Three-Move Identification Protocols

A three-move identification protocol $\mathsf{ID} := (\mathsf{IGen}, \mathsf{P}, \mathsf{ChSet}, \mathsf{V})$, also known as a Σ-*protocol*, is a scheme of the following form:



NTNU

Fiat-Shamir transform

The Fiat-Shamir transform swaps the verifier with a hash function $H\colon \{0,1\}^* \to \text{ChSet}$.

This gives us a signature scheme $\text{SIG}[\text{ID}] := (\text{Gen}, \text{Sign}, \text{Ver})$:

$\underline{\text{Gen}(\text{par})}$:	$\underline{\text{Sign}(sk, m)}$:	$\underline{\text{Ver}(pk, m, \sigma)}$:
$(pk, sk) \xleftarrow{\$} \text{IGen}(\text{par})$	$(R, St) \xleftarrow{\$} \text{P}_1(sk)$	Parse $\sigma := (R, s)$
Return (pk, sk)	$h = H(R, m)$	$h = H(R, m)$
	$s \xleftarrow{\$} \text{P}_2(sk, R, h, St)$	Return $\text{V}(pk, R, h, s)$
	Return $\sigma = (R, s)$	

NTNU

Results

— “Optimal”, but non-tight reduction in one of the step towards the desired security of ID;

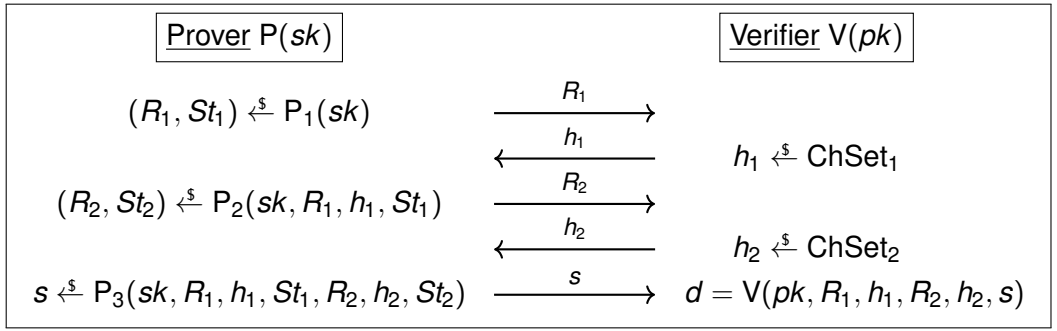
— Fiat-Shamir transformation is tight;

— Tight reduction from multi-user to single-user security.

Thus we have with an “optimal” but non-tight reduction from MU-UF-CMA to KR-KOA.

Five-Move Identification Protocols

A five-move identification protocol $\mathsf{ID} := (\mathsf{IGen}, \mathsf{P}, \mathsf{ChSet}_1, \mathsf{ChSet}_2, \mathsf{V})$ is a scheme of the following form:



Fiat-Shamir transformation

Let $\mathrm{ID} := (\mathrm{IGen}, \mathrm{P}, \mathrm{ChSet}_1, \mathrm{ChSet}_2, \mathrm{V})$ be a five-move identification scheme, and let $H_1 \colon \{0,1\}^* \to \mathrm{ChSet}_1$ and $H_2 \colon \{0,1\}^* \to \mathrm{ChSet}_2$ be two hash functions.

We define the signature scheme $\mathrm{FS}[\mathrm{ID}, \mathrm{H}_1, \mathrm{H}_2] := (\mathrm{Gen}, \mathrm{Sign}, \mathrm{Ver})$ as follows:

$\underline{\mathrm{Gen}(\mathrm{par})}$:	$\underline{\mathrm{Sign}(sk, m)}$:	$\underline{\mathrm{Ver}(pk, m, \sigma)}$:
$(pk, sk) \xleftarrow{\$} \mathrm{IGen}(\mathrm{par})$	$(R_1, St_1) \xleftarrow{\$} \mathrm{P}_1(sk)$	Parse $\sigma := (R_1, R_2, s)$
Return (pk, sk)	$h_1 = H_1(R_1, m)$	$h_1 = H_1(R_1, m)$
	$(R_2, St_2) \xleftarrow{\$} \mathrm{P}_2(sk, R_1, h_1, St_1)$	$h = H(R, m)$
	$h_2 = H_2(R_2, m)$	$h_2 = H_2(R_2, m)$
	$s \xleftarrow{\$} \mathrm{P}_3(sk, R_1, h_1, R_2, h_2, St_2)$	Return
	Return $\sigma = (R_1, R_2, s)$	$\mathrm{V}(pk, R_1, h_1, R_2, h_2, s)$

NTNU

The CDH-problem

Recall the CDH-problem:

Definition

The computational Diffie-Hellman problem CDH is (t, ε)-hard in par if for all adversaries $\mathcal{A}$ running in time at most t,

$$\Pr\left[Z = g^{xy} \mid z, y \xleftarrow{\$} \mathbb{Z}_p; Z \leftarrow \mathcal{A}(g^x, g^y)\right] \leq \varepsilon.$$

Instantiation from CDH

With some small tweaks to the inputs to the hash functions, we get a signature scheme $\mathsf{FS}_{\mathsf{CDH}}$, where $H_1 \colon \{0,1\}^* \to \mathbb{G}$ with $\mathbb{G}$ a cyclic group of prime order p, and $H_2 \colon \{0,1\}^* \to \{0,\ldots,2^k-1\}$.

Gen(par):	Sign(sk, m):	Ver(pk, m, σ):
$sk := x \xleftarrow{\$} \mathbb{Z}_p$	$r \xleftarrow{\$} \mathbb{Z}_p$; $R_1 = g^r$	Parse $\sigma := (R_1, R_2, s)$
$pk := X = g^x$	$h_1 = H_1(R_1)$	$h_2 = H_2(R_1, R_2, m)$
Return (pk, sk)	$R_L = h_1^x \in \mathbb{G}, R_R = h_1^r$	If $R_1 = g^s \cdot X^{-h_2}$
	$R_2 := (R_L, R_R)$	Return 1
	$h_2 = H_2(R_1, R_2, m)$	Else return 0
	$s = x \cdot h_2 + r \in \mathbb{Z}_p$	
	$\sigma = (R_1, R_2, s)$	
	Return σ	

Key prefixing

By adding a public key prefix to this scheme we obtain a new scheme PF-FS_{CDH}.

Gen(par):	Sign(sk, pk, m):	Ver(pk, m, σ):
$sk := x \xleftarrow{\$} \mathbb{Z}_p$	$r \xleftarrow{\$} \mathbb{Z}_p; R_1 = g^r$	Parse $\sigma := (R_1, R_2, s)$
$pk := X = g^x$	$h_1 = H_1(R_1)$	$h_2 = H_2(R_1, R_2, pk, m)$
Return (pk, sk)	$R_L = h_1^x \in \mathbb{G}, R_R = h_1^r$	If $R_1 = g^s \cdot X^{-h_2}$
	$R_2 := (R_L, R_R)$	Return 1
	$h_2 = H_2(R_1, R_2, pk, m)$	Else return 0
	$s = x \cdot h_2 + r \in \mathbb{Z}_p$	
	$\sigma = (R_1, R_2, s)$	
	Return σ	

This scheme has a tight reduction from MU-UF-CMA to the regular UF-CMA security of FS_{CDH}.

NTNU

Results

— The scheme PF-FS_{CDH} has tight reductions all the way back to CDH.

— The same can be done by instantiating from the factoring problem.

— Moving forward, we will try to generalize our proof to a wider class of schemes obtained by the Fiat-Shamir transform.