Gradually Convertible Undeniable Signatures
(Michels-Petersen-Horster Convertible Undeniable Signatures Revisited)

Laila El Aimani and Damien Vergnaud

b-it COSEC - Bonn/Aachen International Center for Information Technology
Computer Security Group, Dahlmannstr. 2, D-53113 Bonn, Germany
{elaimani,vergnaud}@bit.uni-bonn.de

Abstract. In 1990, Boyar, Chaum, Damgård and Pedersen introduced *convertible undeniable signatures* which limit the self-authenticating property of digital signatures but can be converted by the signer to ordinary signatures. Michels, Petersen and Horster presented, in 1996, an attack on the Elgamal-based seminal scheme of Boyar *et al.* and proposed a repaired version without formal security analysis. In this paper, we modify their protocol so that it becomes a generic one and it provides an advanced feature which permits the signer to universally convert *achronously* all signatures pertaining to a specific time period. We supply a formal security treatment of the modified scheme: we prove, in the generic group model, that the protocol is existentially unforgeable and anonymous under chosen message attacks, assuming new assumptions (though reasonable) on the underlying hash function.

1 Introduction

In 1996, Michels, Petersen and Horster [14] proposed a convertible undeniable signature protocol whose security relies on the difficulty of the discrete logarithm problem in the multiplicative group of a finite field. This scheme has received little attention from the cryptographic community whereas we are convinced that it deserves better than oblivion. This paper focuses on the security treatment and on the proposal of an additional functionality for Michels-Petersen-Horster convertible undeniable signatures. Our analysis points out new security properties for the underlying hash functions which may be of independent interest.

Related work. A property of conventional digital signature schemes is that once a signature is released, everybody can check its validity. However there are numerous situations where this *self-authenticating* property is not desirable. In 1989 Chaum and van Antwerpen [7] introduced the concept of *undeniable signatures* whose purpose is to perform public key digital signatures which cannot be verified without interacting with the signer. In addition to the confidentiality and privacy concerns in themselves, this primitive finds applications in such different fields as electronic payment systems, certificate management or cyberdemocracy.

J. Katz and M. Yung (Eds.): ACNS 2007, LNCS 4521, pp. 478–496, 2007.

In 1991, the concept has been refined by giving the possibility to transform an undeniable signature into an ordinary digital signature. These *convertible undeniable signatures*, proposed in [4] by Boyar, Chaum, Damgård and Pedersen, provide individual and universal conversions of the signatures. Unfortunately, this Elgamal-like scheme has been broken in 1996 by Michels, Petersen, and Horster [14] who proposed a repaired version with heuristic security.

The universal conversion of all convertible undeniable signature protocols proposed before 2005, consists in revealing a part of the signer's secret key. This conversion makes all signatures, *past as well as future*, be universally verifiable. This property may be undesirable in some context since the corresponding keys cannot be used to generate undeniable signatures any more. To overcome this problem, Laguillaumie and the second author introduced and formalized, in 2005 [13], the *time-selective convertible undeniable signatures* which supports signers in gradually converting the undeniable signatures in a controlled fashion. They proposed a scheme which permits the signer to universally convert *chronologically* signatures pertaining only to a specific time period: given a time-selective convertible undeniable signature σ for a time period t, it is computationally infeasible to determine which signing secret key was used to generate σ; but with the knowledge of a matching universal receipt for some time period $p' \geq p$, it is easy to determine whether σ is a valid time-selective convertible undeniable signature or not. A tantalizing challenge is to generalize the concept of time-selective convertible signature to *event-selective* convertible signature where a signature becomes universally verifiable if a specific event happens that makes the signer publish the corresponding receipt information. This primitive will enable the signer to gradually convert signatures *achronously* (*i.e.* with time periods made completely independent of each other). Up to now, no concrete realization of this concept has been proposed in the literature.

Our contributions. In this paper, we revisit the Michels-Petersen-Horster convertible undeniable signature scheme. First of all, we modify it such that it becomes a generic algorithm. This point of view allows to look at cryptographic constructions in an abstract way and "move" them to other groups without the original restriction of subgroup of the multiplicative group of a finite field. In addition, we suggest a slight modification of this scheme which gives the first realization of *achronous* gradually convertible undeniable signatures.

The security of many cryptographic tools relies on assumptions about the hardness of certain algorithmic problems. Techniques from [17] suggest that it is highly improbable to reduce the security of the Michels-Petersen-Horster signatures to the discrete logarithm problem in the standard security model. Therefore, we investigate their security in the so-called *generic group model*, following previous work from [5,21] where the security of a generic version of the protocol DSA was analyzed. However, it is worth noting that the real, non-generic security of the scheme may be completely different in different groups [8].

This security analysis points out new sufficient security properties for the underlying hash functions. These new notions of *random affine preimage resistance* and *random linear collision resistance* are satisfied by generic hash functions (*i.e.* in the random oracle model [3]). The former property is necessary for our scheme to be secure, while the latter is for the RSA-FDH signature scheme [3].

Notations. The set of n-bit strings is denoted by $\{0,1\}^n$ and the set of all finite binary strings (or messages) is denoted by $\{0,1\}^*$. Let $\mathcal{A}$ be a probabilistic Turing machine running in polynomial time (a PPTM, for short), and let x be an input for $\mathcal{A}$. The probability space that assigns to a string σ the probability that $\mathcal{A}$, on input x, outputs σ is denoted by $\mathcal{A}(x)$. The support of $\mathcal{A}(x)$ is denoted by $\mathcal{A}[x]$. Given a probability space S, a PPTM that samples a random element according to S is denoted by $x \overset{R}{\longleftarrow} S$. For a finite set X, $x \overset{R}{\longleftarrow} X$ denotes a PPTM that samples a random element uniformly at random from X. A *two-party protocol* is a pair of interactive PPTMs $(\mathsf{Prove}, \mathsf{Verify})$.

2 Gradually Convertible Undeniable Signatures

2.1 Definition

As in ordinary digital signatures, undeniable signature schemes establish two complimentary algorithms: one for signing (Sign) and the other for controlling the signature at some later time (Cont), but this algorithm is not publicly available since it requires the knowledge of the signer's secret key to be executed. Besides, the signer can prove his authorship of an undeniable signature by running a confirmation protocol (Conf) with a verifier and a falsely implicated signer may deny his involvement by running a denial protocol (Deny) with a verifier.

Designated verifier proofs were introduced by Jakobsson, Sako and Impagliazzo in 1996 [11] and have been widely used for undeniable signature schemes. In [12], Kudla and Paterson present a security model for these signatures where the confirmation and denial protocols are actually implemented with such proofs. They proposed non-interactive designated verifier proofs suited to combination with Chaum-van Antwerpen original undeniable signature scheme resulting in a secure[1] and efficient undeniable signature scheme. Unfortunately, we cannot use these non-interactive non-transferable proofs, to obtain the security results without the random oracle model. Therefore, in this paper, we will use interactive version of the designated verifier proofs described in [12].

In addition, the signer has at its disposal an algorithm (Conv) which permits to:

- convert a given undeniable signature into a regular, universally verifiable signature. This operation does not affect other undeniable signatures.
- publish a universal trapdoor relative to a specific time period p by the means of which all undeniable signatures for the time period p become universally verifiable.

[1] In the random oracle model, assuming the intractability of the decisional Diffie-Hellman problem in the underlying group [9,15,16].

The verification of the converted signatures is performed thanks to the algorithm Vf.

Definition 1 (Gradually Convertible Undeniable Signature). *Let* $\pi \in \mathbb{N}$. *A* gradually convertible undeniable signature scheme *with* π *time periods* Σ *is a 9-tuple* $\Sigma = (\mathsf{Setup}, \mathsf{SKg}, \mathsf{VKg}, \mathsf{Sign}, \mathsf{Cont}, \mathsf{Conf}, \mathsf{Deny}, \mathsf{Conv}, \mathsf{Vf})$ *such that:*

- $\Sigma.\mathsf{Setup}$, *the* common parameter generation algorithm, *is a PPTM which takes an integer* k *as input. The output are the* public parameters $\mathcal{P}$. k *is called the* security parameter.
- $\Sigma.\mathsf{SKeyGen}$, *the* signer key generation algorithm, *is a PPTM which takes the public parameters as input. The output is a pair* $(\mathbf{sk_s}, \mathbf{pk_s})$ *where* $\mathbf{sk_s}$ *is called a* signing secret key *and* $\mathbf{pk_s}$ *a* signing public key.
- $\Sigma.\mathsf{VKeyGen}$, *the* verifier key generation algorithm, *is a PPTM which takes the public parameters as input. The output is a pair* $(\mathbf{sk_v}, \mathbf{pk_v})$ *where* $\mathbf{sk_v}$ *is called a* verifying secret key *and* $\mathbf{pk_v}$ *a* verifying public key.
- $\Sigma.\mathsf{Sign}$, *the* signing algorithm, *is a PPTM which takes the public parameters, a message, an integer in* $[\![1, \pi]\!]$ *and a signing secret key as inputs and outputs a bit string.*
- $\Sigma.\mathsf{Cont}$, *the* controlling algorithm, *is a PPTM which takes the public parameters, a message* m, *a bit string* σ, *an integer* $p \in [\![1, \pi]\!]$ *and a signing key pair* $(\mathbf{sk_s}, \mathbf{pk_s})$ *as inputs and outputs a bit. If the bit output is 1 then the bit string* σ *is said to be a* signature *on* m *for* $\mathbf{pk_s}$ *for the time period* p.
- $\Sigma.\{\mathsf{Conf}.\mathsf{Deny}\}$, *the* confirming/denying protocols *(respectively), are two-party protocols* $(\mathsf{Prove}, \mathsf{Verify})$ *such that:*
  - Prove *and* Verify *take as input a message* m, *an integer* $p \in [\![1, \pi]\!]$, *a bit-string* σ, *a signing public key* $\mathbf{pk_s}$ *and a verifying public key* $\mathbf{pk_v}$ *and the public parameters;*
  - Prove *takes as input* $\mathbf{sk_s}$ *the signing secret key corresponding to* $\mathbf{pk_s}$*;*
  - Verify *takes as input* $\mathbf{sk_v}$ *the verifying secret key corresponding to* $\mathbf{pk_v}$*;*

  $\mathsf{Conf.Verify}$ *(*resp. $\mathsf{Deny.Verify}$ *) outputs an element in* $\{\perp, 1\}$ *(*resp. $\{\perp, 0\}$*).*
- $\Sigma.\mathsf{Conv}$, *the* conversion algorithm, *is a PPTM which takes as input the public parameters, an integer in* $[\![1, \pi]\!]$, *a signing key pair and a bit string* Υ *(either a pair message/signature or the empty string) and outputs a bit string.*
- $\Sigma.\mathsf{Vf}$, *the* verifying algorithm for converted signature, *is a PPTM which takes as input the public parameters, a message* m, *and a bit string* σ, *an integer* $p \in [\![1, \pi]\!]$, *a signing public key* $\mathbf{pk_s}$ *and a bit string* Λ *and outputs a bit. If the bit output is* 1 *then the bit string* Λ *is said to be a* receipt *of the validity of* σ.

where the protocols $\Sigma.\mathsf{Conf}$ *and* $\Sigma.\mathsf{Deny}$ *are a designated verifier proof of membership system for the languages (respectively):*

$$\{(\mathcal{P}, m, \sigma, p, \mathbf{pk_s}) \in \Sigma.\mathsf{Setup}[k] \times \{0,1\}^{*2} \times [\![1, \pi]\!] \times \Sigma.\mathsf{SKg}[\mathcal{P}] \big| \Sigma.\mathsf{Vf}[\mathcal{P}, m, \sigma, p]\} = \{1\}$$

$$\{(\mathcal{P}, m, \sigma, p, \mathbf{pk_s}) \in \Sigma.\mathsf{Setup}[k] \times \{0,1\}^{*2} \times [\![1, \pi]\!] \times \Sigma.\mathsf{SKg}[\mathcal{P}] \big| \Sigma.\mathsf{Vf}[\mathcal{P}, m, \sigma, p]\} = \{0\}$$

and for all $k \in \mathbb{N}$*, for all* $\mathcal{P} \in \Sigma.\mathsf{Setup}[k]$*, for all* $\mathcal{S} = (\mathbf{pk_s}, \mathbf{sk_s}) \in \Sigma.\mathsf{SKg}[\mathcal{P}]$*, for all* $m \in \{0,1\}^*$ *and for all* $p \in [\![1, \pi]\!]$*, we have:*

$$\forall \sigma \in \Sigma.\mathsf{Sign}[\mathcal{P}, m, p, \mathbf{sk_s}], \Sigma.\mathsf{Cont}[\mathcal{P}, m, \sigma, p, (\mathbf{sk_s}, \mathbf{pk_s})] = \{1\}$$

$$\forall \sigma \in \Sigma.\mathsf{Sign}[\mathcal{P}, m, p, \mathbf{sk_s}], \forall \Lambda \in \Sigma.\mathsf{Conv}[\mathcal{P}, p, \mathcal{S}, (m, \sigma)], \Sigma.\mathsf{Vf}[\mathcal{P}, m, \sigma, p, \mathbf{pk_s}, \Lambda] = \{1\}$$

$$\forall \sigma \in \Sigma.\mathsf{Sign}[\mathcal{P}, m, p, \mathbf{pk_s}], \forall \Lambda \in \Sigma.\mathsf{Conv}[\mathcal{P}, p, \mathcal{S}, \varepsilon], \Sigma.\mathsf{Vf}[\mathcal{P}, m, \sigma, p, \mathbf{pk_s}, \Lambda] = \{1\}$$

$$\forall \sigma, \Lambda \in \{0,1\}^*, \Sigma.\mathsf{Vf}[\mathcal{P}, m, \sigma, p, \mathbf{pk_s}, \Lambda] = \{1\} \Rightarrow \Sigma.\mathsf{Cont}[\mathcal{P}, m, \sigma, p, (\mathbf{sk_s}, \mathbf{pk_s})] = \{1\}.$$

Remark 1. The first two properties capture the validity and the non-transferable property of the protocols Conf and Deny (*i.e.* the use of designated verifier proofs insures that a verifier will gain no information in an execution of one of these protocols [12]). The three last properties are the properties of *correctness*:

- a well-formed signature is always accepted by the algorithm Cont;
- a receipt correctly constructed is always accepted by the algorithm Vf;
- and if there exists a bit-string Λ which makes accepted a bit-string σ by the algorithm Vf, then σ is a valid signature.

2.2 Security Model

Registered public key model. In public key cryptography, the notion of anonymity is to be handled with great attention. For instance, in order to ensure anonymity, it is important that users register their public key by a certifying authority. Hence, in our security analysis, it is assumed that the users' keys have been already registered to an authority. The registration procedure would always contain a proof of knowledge of the associated private key. To further simplify the security analysis, we will assume that this procedure will be the *direct registration of the keys*[2].

Security against existential forgery under chosen message attack. The standard notion of security for digital signatures was defined by Goldwasser, Micali and Rivest [10] as *existential forgery against adaptive chosen message attacks* (EF-CMA). In [13], the corresponding notion for time-selective convertible undeniable signatures is defined along the same lines. The definition of *resistance to forgery* for gradually convertible undeniable signatures that we propose is similar. In fact, we suppose that the adversary has access to the universal receipts for every time period $p \in [\![1, \pi]\!]$ and is allowed to query a converting oracle $\mathfrak{Cv}$, a confirming oracle $\mathfrak{C}$ amd a denying oracle $\mathfrak{D}$ on any couple message/signature of its choice. As usual, in the adversary answer, there is the natural restriction that the returned message/signature has not been obtained from the signing oracle.

Definition 2 (Unforgeability - EF-CMA). *Let* π *be a positive integer, let* $\Sigma = (\mathsf{Setup}, \mathsf{SKg}, \mathsf{VKg}, \mathsf{Sign}, \mathsf{Cont}, \mathsf{Conf}, \mathsf{Deny}, \mathsf{Conv}, \mathsf{Vf})$ *be a gradually convertible*

[2] It is often necessary to require the security of the schemes even if the adversary is the key registration center. In this case, one must replace the proof of knowledge associated to the key registration by a zero-knowledge one.

undeniable signature scheme with π time periods and let $\mathcal{A}$ be an PPTM. We consider the following random experiment, where k is a security parameter:

```
$\boxed{\textit{Experiment } \mathbf{Exp}^{\mathsf{ef-cma}}_{\Sigma,\mathcal{A}}(k)}$
$\mathcal{P} \overset{R}{\longleftarrow} \Sigma.\mathit{Setup}(k)$,
$(\mathbf{pk_s}, \mathbf{sk_s}) \overset{R}{\longleftarrow} \Sigma.\mathit{SKg}(\mathcal{P})$
for $j = 1$ to $\pi$ do $\Lambda_j \leftarrow \Sigma.\mathit{Conv}(\mathcal{P}, j, (\mathbf{sk_s}, \mathbf{pk_s}), \varepsilon)$
$(m^\star, \sigma^\star, p^\star) \overset{R}{\longleftarrow} \mathcal{A}^{\mathfrak{S},\mathfrak{Cv},\mathfrak{C},\mathfrak{D}}(\mathcal{P}, \mathbf{pk_s}, \{\Lambda_j\}_{j \in [\![1,\pi]\!]})$
                    | $\mathfrak{S} : (m, p) \longrightarrow \Sigma.\mathit{Sign}(\mathcal{P}, m, p, \mathbf{sk_s})$
                    | $\mathfrak{Cv} : (m, p, \sigma) \longrightarrow \Sigma.\mathit{Conv}(\mathcal{P}, p, (\mathbf{sk_s}, \mathbf{pk_s}), (m, \sigma))$
                    | $\mathfrak{C} : (m, p, \sigma, \mathbf{pk_v}) \longrightarrow \Sigma.\mathit{Conf}(m, p, \sigma, \mathbf{pk_v}, \mathbf{pk_s})$
                    | $\mathfrak{D} : (m, p, \sigma, \mathbf{pk_v}) \longrightarrow \Sigma.\mathit{Deny}(m, p, \sigma, \mathbf{pk_v}, \mathbf{pk_s})$
return 1 if and only if the following properties are satisfied:
    - $\Sigma.\mathit{Vf}[\mathcal{P}, \mathbf{pk_s}, m^\star, \sigma^\star, \Lambda_{p^\star}] = \{1\}$
    - $m$ was not queried to $\mathfrak{S}$
```

We define the success *of $\mathcal{A}$,* via $\mathbf{Succ}^{\textit{ef-cma}}_{\Sigma,\mathcal{A}}(k) \Pr\left[\mathbf{Exp}^{\textit{ef-cma}}_{\Sigma,\mathcal{A}}(k) = 1\right]$.

Given $(k, t) \in \mathbb{N}^2$ and $\varepsilon \in [0, 1]$, the scheme Σ is said to be (k, t, ε)-EF-CMA secure, if no EF-CMA-adversary $\mathcal{A}$ running in time t has $\mathbf{Succ}^{\textit{ef-cma}}_{\Sigma,\mathcal{A}}(k) \geq \varepsilon$. The scheme Σ is said to be EF-CMA secure if, for any security parameter $k \in \mathbb{N}$, any polynomial function $t : \mathbb{N} \to \mathbb{N}$, and any negligible function $\varepsilon : \mathbb{N} \to [0, 1]$, it is $(k, t(k), \varepsilon(k))$-EF-CMA secure.

Anonymity. We state the precise definition of *anonymity* under a chosen message attack (Ano-CMA) which captures the notion that an attacker cannot determine under which key a signature was performed [9]. We consider a Ano-CMA-adversary $\mathcal{A}$ that runs in two stages. In the find stage, it takes as input two signing public keys $\mathbf{pk_{s0}}$ and $\mathbf{pk_{s1}}$ and outputs a message $m^\star$, a time period $p^\star$ together with some state information $\mathcal{I}$. In the guess stage, $\mathcal{A}$ gets a challenge gradually convertible undeniable signature $\sigma^\star$ formed by signing at random the message $m^\star$ under one of the two keys for the time period $p^\star$ and it must say which key was chosen. In both stages, the adversary has access to a signing oracle $\mathfrak{S}$ for both signing key pairs, to a converting oracle $\mathfrak{Cv}$, to a confirming oracle $\mathfrak{C}$ and to a denying oracle $\mathfrak{D}$. The attacker is also given the universal receipts of both potential signers for all[3] time period $p \in [\![1, \pi]\!] \setminus \{p^\star\}$. The only restriction on $\mathcal{A}$ is that it cannot query the triple $(m^\star, \sigma^\star, p^\star)$ on the converting and confirming/denying oracles.

Definition 3 (Anonymity - Ano-CMA). *Let π be a positive integer, let $\Sigma = (\mathit{Setup}, \mathit{SKg}, \mathit{VKg}, \mathit{Sign}, \mathit{Cont}, \mathit{Conf}, \mathit{Deny}, \mathit{Conv}, \mathit{Vf})$ be a gradually convertible undeniable signature scheme with π time periods and let $\mathcal{A}$ be an PPTM. We consider the following random experiment, for $r \in \{0, 1\}$, where k is a security parameter:*

[3] This is the main difference with time-selective convertible undeniable signatures from [13] where this universal receipts was given only for $p \in [\![1, p^\star - 1]\!]$.

```
$\boxed{\textit{Experiment } \mathbf{Exp}_{\Sigma,\mathcal{A}}^{\textsf{ano-cma}-r}(k)}$
$\mathcal{P} \overset{R}{\longleftarrow} \Sigma.\mathsf{Setup}(k)$
$(\mathbf{pk_{s}}_0, \mathbf{sk_{s}}_0) \overset{R}{\longleftarrow} \Sigma.\mathsf{SKeyGen}(\mathcal{P})$,
$(\mathbf{pk_{s}}_1, \mathbf{sk_{s}}_1) \overset{R}{\longleftarrow} \Sigma.\mathsf{SKeyGen}(\mathcal{P})$
$(m^\star, p^\star, \mathcal{I}) \overset{R}{\longleftarrow} \mathcal{A}^{\mathfrak{S},\mathfrak{Cv},\mathfrak{C},\mathfrak{D}}(\mathsf{find}, \mathcal{P}, \mathbf{pk_{s}}_0, \mathbf{pk_{s}}_1)$
        | $\mathfrak{S} : (m, p, i) \longrightarrow \Sigma.\mathsf{Sign}(\mathcal{P}, m, p, \mathbf{sk_{s}}_i)$
        | $\mathfrak{Cv} : (m, p, \sigma, i) \longrightarrow \Sigma.\mathsf{Conv}(\mathcal{P}, p, (\mathbf{sk_{s}}_i, \mathbf{pk_{s}}_i), (m, \sigma))$
        | $\mathfrak{C} : (m, p, \sigma, \mathbf{pk_v}, i) \longrightarrow \Sigma.\mathsf{Conf}(m, p, \sigma, \mathbf{pk_v}, \mathbf{pk_{s}}_i)$
        | $\mathfrak{D} : (m, p, \sigma, \mathbf{pk_v}, i) \longrightarrow \Sigma.\mathsf{Deny}(m, p, \sigma, \mathbf{pk_v}, \mathbf{pk_{s}}_i)$
$\sigma^\star \overset{R}{\longleftarrow} \Sigma.\mathsf{Sign}(\mathcal{P}, m, \mathbf{sk_{s}}_r, p^\star)$
for $j$ from $1$ to $\pi$ do
    $\Lambda_j^0 \leftarrow \Sigma.\mathsf{Conv}(\mathcal{P}, j, \mathbf{pk_{s}}_0, \mathbf{sk_{s}}_0, \varepsilon)$ and $\Lambda_j^1 \overset{R}{\longleftarrow} \Sigma.\mathsf{Conv}(\mathcal{P}, j, \mathbf{pk_{s}}_1, \mathbf{sk_{s}}_1, \varepsilon)$
$d \leftarrow \mathcal{A}^{\mathfrak{S},\mathfrak{Cv},\mathfrak{C},\mathfrak{D}}(\mathsf{guess}, \mathcal{I}, \{\Lambda_j^0, \Lambda_j^1\}_{j \in [\![1,\pi]\!] \setminus \{p^\star\}})$
Return $d$
```

We define the advantage *of $\mathcal{A}$,* via

$$\mathbf{Adv}_{\Sigma,\mathcal{A}}^{\textsf{ano-cma}}(k) \left| \Pr\left[\mathbf{Exp}_{\Sigma,\mathcal{A}}^{\textsf{ano-cma}-1}(k) = 1\right] - \Pr\left[\mathbf{Exp}_{\Sigma,\mathcal{A}}^{\textsf{ano-cma}-0}(k) = 1\right]\right|.$$

Given $(k, t) \in \mathbb{N}^2$ and $\varepsilon \in [0, 1]$, the scheme Σ is said to be (k, t, ε)-Ano-CMA secure, if no Ano-CMA-adversary $\mathcal{A}$ running in time t has $\mathbf{Adv}_{\Sigma,\mathcal{A}}^{\textsf{ano-cma}}(k) \geq \varepsilon$. The scheme Σ is said to be Ano-CMA secure if, for any security parameter $k \in \mathbb{N}$, any polynomial function $t : \mathbb{N} \to \mathbb{N}$, and any negligible function $\varepsilon : \mathbb{N} \to [0, 1]$, it is $(k, t(k), \varepsilon(k))$-Ano-CMA secure.

3 Hash Functions and New Security Properties

Hash functions take messages of arbitrary length and outputs a fixed length string. In cryptographic uses of a hash function $\mathcal{H} : \{0, 1\}^* \longrightarrow H$, these properties are considered prerequisites:

- *Preimage resistance*: given $h \in H$, it should be computationally intractable to find a message m such that $\mathcal{H}(m) = h$.
- *Collision-resistant:* it should be computationnally intractable to find two different messages m_1 and m_2 such that $\mathcal{H}(m_1) = \mathcal{H}(m_2)$.

In this section, we formulate generalization of these security notions and study their properties.

Definitions. The proof of security of our variant of Michels-Petersen-Horster signatures makes use of new non-standard variations of the preimage resistance and the collision resistance assumptions for hash functions. These assumptions are of independent interest as they have interesting relations with the classical ones. We call them *random affine preimage resistance* and *random linear collision resistance.* Although stronger than the standard assumptions, they are quite realistic.

According to [18], an hash function family is a family of functions $(\mathcal{H}_k : \mathcal{K}_k \times \{0,1\}^* \longrightarrow \{0,1\}^k)_{k\in\mathbb{N}}$, where $\mathcal{K}_k$ is a finite non-empty set. We will write the first argument of $\mathcal{H}_k$ as a subscript, so that $\mathcal{H}_{K,k}(m) = \mathcal{H}_k(K,m)$. In the following, we denote elements from $\{0,1\}^k$ as the corresponding k-bits integers in binary representation and we will denote for every integer $N \in \mathbb{Z}$, $\mathcal{H}^N_{K,k}$ the map defined by: $\mathcal{H}^N_{K,k} : \begin{cases} \{0,1\}^* \longrightarrow \mathbb{Z}_N \\ \quad m \longmapsto \mathcal{H}_{K,k}(m) \mod N. \end{cases}$

The new security definitions can be quantified as follows:

Definition 4 (Random affine preimage resistance). *Let n be an integer, let $(\mathcal{H}_k : \mathcal{K}_k \times \{0,1\}^* \longrightarrow \{0,1\}^k)_{k\in\mathbb{N}}$ be an hash function family and let $\mathcal{A}$ be a PPTM. The success $\mathbf{Succ}^{raPre(n)}_{\mathcal{H},\mathcal{A}}(k)$ of $\mathcal{A}$ against the n-random affine preimage resistance of $\mathcal{H} = (\mathcal{H}_k)_{k\in\mathbb{N}}$ is defined by:*

$$\max_{\substack{2^{k-1}\le N<2^k \\ \alpha_1,\dots,\alpha_n\in\mathbb{Z}_N^* \\ \beta_1,\dots,\beta_n\in\mathbb{Z}_N^*}} \left\{ \Pr\left[\begin{array}{c} K \overset{R}{\longleftarrow} \mathcal{K}_k; (m,i,j) \overset{R}{\longleftarrow} \mathcal{A}(K,\alpha_1,\dots,\alpha_n,\beta_1,\dots,\beta_n) \\ m\in\{0,1\}^*, (i,j)\in[\![1,n]\!]^2, i\neq j \\ \alpha_i + \beta_j \mathcal{H}^N_{K,k}(m) = 0 \mod N \end{array} \right] \right\}.$$

An adversary $\mathcal{A}$ against the n-random affine preimage resistance of a hash function family $(\mathcal{H}_k)_{k\in\mathbb{N}}$ can be transformed easily into an adversary against the classical preimage resistance of $(\mathcal{H}_k)_{k\in\mathbb{N}}$ with success probability greater than $\mathbf{Succ}^{raPre(n)}_{\mathcal{H},\mathcal{A}}(k)/n^2$ and time-complexity of $\mathcal{A}$ increased by the time necessary to compute n modular multiplications modulo N. In particular, the 1-random affine preimage resistance is equivalent to the classical preimage resistance.

Definition 5 (Random linear collision resistance). *Let n be an integer, let $(\mathcal{H}_k : \mathcal{K}_k \times \{0,1\}^* \longrightarrow \{0,1\}^k)_{k\in\mathbb{N}}$ be an hash function family and let $\mathcal{A}$ be a PPTM. The success $\mathbf{Succ}^{rlColl(n)}_{\mathcal{H},\mathcal{A}}(k)$ of $\mathcal{A}$ against the n-random affine preimage resistance of $\mathcal{H} = (\mathcal{H}_k)_{k\in\mathbb{N}}$ is defined by:*

$$\max_{\substack{2^{k-1}\le N<2^k \\ \lambda_1,\dots,\lambda_n\in\mathbb{Z}_N^*}} \left\{ \Pr\left[\begin{array}{c} K \overset{R}{\longleftarrow} \mathcal{K}_k; (m,m',i,j) \overset{R}{\longleftarrow} \mathcal{A}(K,\lambda_1,\dots,\lambda_n) \\ m,m'\in\{0,1\}^*, (i,j)\in[\![1,n]\!]^2, m\neq m' \\ \lambda_i \cdot \mathcal{H}_{K,N}(m) = \lambda_j \cdot \mathcal{H}_{K,N}(m') \mod N \end{array} \right] \right\}.$$

As for random affine preimage resistance, the 1-random linear collision resistance is equivalent to the classical collision resistance. Unfortunately, it is impossible to prove that the n-random linear collision resistance can be reduced generically to the collision resistance for $n \geq 2$.

Remark 2. This security requirement is however reasonable since if the hash function family underlying the protocol RSA-FDH [3] does not satisfy it, then it is existential forgeable against a *one* chosen-message attack: given an RSA public key (N,e), the adversary can simply pick at random $r_1,\dots,r_n \in \mathbb{Z}_N$, compute $\lambda_i = r_i^e \mod N$ for all $i \in [\![1,n]\!]$, and try to find a random linear collision with parameters $N,\lambda_1,\dots,\lambda_n$. If a collision $m,m' \in \{0,1\}^*$, $(i,j) \in [\![1,n]\!]^2$, (such that

$\lambda_i \cdot \mathcal{H}_{K,N}(m) = \lambda_j \cdot \mathcal{H}_{K,N}(m') \mod N$ is found), then the adversary queries the signature σ on m to the signing oracle and can compute the signature of m' as $\sigma' = r_i \cdot \sigma \cdot r_j^{-1} \mod N$.

Generic security. The best known general collision-finding attack against a hash function family is the so-called birthday-attack. If we assume that the values of the hash-function family $(\mathcal{H}_k)_{k\in\mathbb{N}}$ are uniformly distributed over $\{0,1\}^k$ and that the generalisation of the birthday attack[4] against the random affine preimage resistance and the random linear collision resistance of $(\mathcal{H}_k)_{k\in\mathbb{N}}$ is the best possible attack (which is true in the random oracle model), then it is possible to give exponential lower bounds on the minimum of n and of the number of hash functions evaluation required to have non-negligible probability of success. Indeed, for any integer $N \geq 2$, and for $(i,k) \in \mathbb{Z}_N$, it is straightforward [20] that

$$\#\{j \in \mathbb{Z}_N | i \cdot j \mod N \leq k\} = \gcd(i,N) \times \left(\left\lfloor \frac{k}{\gcd(i,N)} \right\rfloor + 1 \right).$$

Therefore if D denotes the product of two independent random variables uniformly distributed over $\mathbb{Z}_N$, we have $\forall k \in \mathbb{Z}_N$

$$\Pr(D \leq k) = \frac{1}{N^2} \sum_{i=0}^{N-1} \gcd(i,N) \left(\left\lfloor \frac{k}{\gcd(i,N)} \right\rfloor + 1 \right),$$

and consequently, D is close to the uniform distribution ove $\mathbb{Z}_N$. The results from [2] are sufficient to conclude; details will appear elsewhere.

4 Michels-Petersen-Horster Convertible Undeniable Signatures Revisited

4.1 Description of the Scheme

Let π be an integer. Following the notations from § 2.1, we describe in this section our variant of Michels-Petersen-Horster scheme. It is parameterized by a prime order group generator [1], an hash function family and two pseudo-random function families [18].

Let $\mathbb{G}$ be a group of prime order q generated by the prime order group generator. A *reduction function* is a map that sends an element of the group $\mathbb{G}$ [5,21] to an integer in $\mathbb{Z}_q$. In our security analysis, the reduction function must satisfy the so called *almost-invertibility*: given an arbitrary integer in $\mathbb{Z}_q$, then with nonnegligeable probability one can efficiently find one preimage.

[4] These attacks consist in picking messages $m_1, \ldots, m_r$, computing $h_i = \mathcal{H}_k(m_i) \mod N$ for $i \in [\![1,r]\!]$ and $\gamma_{i,j} = -h_i\beta_j \mod N$ (*resp.* $\gamma_{i,j} = h_i\lambda_j \mod N$) for $j \in [\![1,n]\!]$. They are successful if there is a triple $(i,j,\ell) \in [\![1,r]\!] \times [\![1,n]\!]^2$ (*resp.* a 4-tuple $(i,i',j,j') \in [\![1,r]\!]^2 \times [\![1,n]\!]^2$) s. t. $\gamma_{i,j} = \alpha_\ell$ (*resp.* $\gamma_{i,j} = \gamma_{i',j'}$ and $j \neq j'$).

Definition 6. *Let F be a reduction function $F : \mathbb{G} \to \mathbb{Z}_q$. An almost-inverse of F is a probabilistic algorithm G, possibly outputting $\perp$, such that:*

$$\Pr_{b \in_R \mathbb{Z}_q} [G(b) \in S \wedge F(G(b)) = b] \geq \frac{1}{3}.$$

A reduction function F is (δ, t)-almost-invertible, with almost-inverse G, if furthermore: $\mathcal{D} \approx_\delta \mathcal{U}$ where $\mathcal{D} = \{G(b) \mid b \overset{R}{\longleftarrow} \mathbb{Z}_q \wedge G(b) \in \mathbb{G}\}$ and $\mathcal{U} = \{a \mid a \overset{R}{\longleftarrow} \mathbb{G}\}$. The notation $\mathcal{D} \approx_\delta \mathcal{U}$ means that no distinguisher with running time t can get an advantage greater than δ.

Description of the scheme

- Σ.Setup: on input a security parameter k, the underlying generators output a group $\mathbb{G}$ of prime order q generated by an element P, a reduction function $F : \mathbb{G} \to \mathbb{Z}_q$, a hash function $h : \{0,1\}^* \to \mathbb{Z}_q$ and two pseudo-random functions $H^1 : \mathbb{Z}_q \times [\![1, \pi]\!] \to \{0,1\}^k$ and $H^2 : \{0,1\}^k \times \{0,1\}^* \times \mathbb{G} \to \mathbb{Z}_q$. The public parameters are $(q, \mathbb{G}, P, h, H^1, H^2)$.
- Σ.SKg: The signer picks at random its secret key $u, v \overset{R}{\longleftarrow} [\![1, q-1]\!]$, computes $U \leftarrow uP$ and $V \leftarrow vP$ and sets (U, V) as its public key.
- Σ.VKg: The verifier picks at random its secret key $w \overset{R}{\longleftarrow} [\![1, q-1]\!]$, computes $W \leftarrow wP$. and set it as its public key.

```
Protocol EDL.Prove
Common input: $(U_1, U_2, V_1, V_2)$, $Y$
$\mathcal{P}$'s input: $x$
$\mathcal{V}$'s output: $b$

① $\mathcal{P} \xrightarrow{C_1, C_2, C_3} \mathcal{V}$
$(a, b, k) \overset{R}{\longleftarrow} [\![1, q-1]\!]^3$
$C_1 \leftarrow [k] \cdot U_1$ ; $C_2 \leftarrow [k] \cdot U_2$
$C_3 \leftarrow [a] \cdot U_1 + [b] \cdot Y$
❶ $\mathcal{V} \xrightarrow{r} \mathcal{P}$
$r \overset{R}{\longleftarrow} [\![1, q-1]\!]$
② $\mathcal{P} \xrightarrow{a, b, c} \mathcal{V}$
$c \leftarrow k - x(r+b) \mod q$

• $\mathcal{V}$'s execution ending
$\widetilde{C_1} \leftarrow [c] \cdot U_1 + [r+b] \cdot V_1$
$\widetilde{C_2} \leftarrow [c] \cdot U_2 + [r+b] \cdot V_2$
$\widetilde{C_3} \leftarrow [a] \cdot U_1 + [b] \cdot Y$
if $(C_1, C_2, C_3)(\widetilde{C_1}, \widetilde{C_2}, \widetilde{C_3})$
    then $b \leftarrow$ Accept else $b \leftarrow \perp$
```

```
Protocol EDL.Fake
Common input: $(U_1, U_2, V_1, V_2)$, $Y$
$\mathcal{P}$'s input: $y$
$\mathcal{V}$'s output: $b$

① $\mathcal{P} \xrightarrow{C_1, C_2, C_3} \mathcal{V}$
$(c, d, k) \overset{R}{\longleftarrow} [\![1, q-1]\!]^3$
$C_1 \leftarrow [c] \cdot U_1 + [d] \cdot V_1$ ; $C_2 \leftarrow [c] \cdot U_2 + [d] \cdot V_2$
$C_3 \leftarrow [k] \cdot U_1$
❶ $\mathcal{V} \xrightarrow{r} \mathcal{P}$
$r \overset{R}{\longleftarrow} [\![1, q-1]\!]$
② $\mathcal{P} \xrightarrow{a, b, c} \mathcal{V}$
$b \leftarrow d - r \mod q$ ; $a \leftarrow k - by \mod q$

• $\mathcal{V}$'s execution ending
$\widetilde{C_1} \leftarrow [c] \cdot U_1 + [r+b] \cdot V_1$
$\widetilde{C_2} \leftarrow [c] \cdot U_2 + [r+b] \cdot V_2$
$\widetilde{C_3} \leftarrow [a] \cdot U_1 + [b] \cdot Y$
if $(C_1, C_2, C_3)(\widetilde{C_1}, \widetilde{C_2}, \widetilde{C_3})$
    then $b \leftarrow$ Accept else $b \leftarrow \perp$
```

Fig. 1. Interactive designated verifier proof of membership of the language EDL($\mathbb{G}$)

```
Protocol IDL.Prove
Common input: $(U_1, U_2, V_1, V_2)$, $Y$
$\mathcal{P}$'s input : $x$
$\mathcal{V}$'s output : $b$
① $\mathcal{P} \xrightarrow{C_0, C_1, C_2, C_3} \mathcal{V}$
$(a, b, k_0, k_1, k_2) \overset{R}{\longleftarrow} [\![1, q-1]\!]^5$
$C_0 \leftarrow [k_0] \cdot (V_2 - [x] \cdot U_2)$
$C_1 \leftarrow [k_1] \cdot U_1 - [k_2] \cdot V_1$
$C_2 \leftarrow [k_1] \cdot U_2 - [k_2] \cdot V_2$
$C_3 \leftarrow [a] \cdot U_1 + [b] \cdot Y$
❶ $\mathcal{V} \xrightarrow{r} \mathcal{P}$
$r \overset{R}{\longleftarrow} [\![1, q-1]\!]$
② $\mathcal{P} \xrightarrow{a, b, c, d} \mathcal{V}$
$c \leftarrow k_1 - xk_0(r + b) \mod q$
$d \leftarrow k_2 - k_0(r + b) \mod q$

• $\mathcal{V}$'s execution ending
$\widetilde{C_1} \leftarrow [c] \cdot U_1 - [d] \cdot V_1$
$\widetilde{C_2} \leftarrow C_0 + [c] \cdot U_2 - [r + b] \cdot V_2$
$\widetilde{C_3} \leftarrow [a] \cdot U_1 + [b] \cdot Y$
if $(C_1, C_2, C_3)(\widetilde{C_1}, \widetilde{C_2}, \widetilde{C_3}) \wedge C_0 \neq \mathbb{O}_{\mathbb{G}_2}$
    then $b \leftarrow$ Accept else $b \leftarrow \perp$
```

```
Protocole IDL.Fake
Common input: $(U_1, U_2, V_1, V_2)$, $Y$
$\mathcal{P}$'s input: $y$
$\mathcal{V}$'s output: $b$
① $\mathcal{P} \xrightarrow{C_0, C_1, C_2, C_3} \mathcal{V}$
$(c, d, k_1, k_2) \overset{R}{\longleftarrow} [\![1, q-1]\!]^4$
$C_0 \overset{R}{\longleftarrow} \mathbb{G} \setminus \{\mathbb{O}_{\mathbb{G}}\}$ ; $C_1 \leftarrow [c] \cdot U_1 - [d] \cdot V_1$
$C_2 \leftarrow C_0 + [c] \cdot U_2 - [k_1] \cdot V_2$
$C_3 \leftarrow [k_2] \cdot U_1$
❶ $\mathcal{V} \xrightarrow{r} \mathcal{P}$
$r \overset{R}{\longleftarrow} [\![1, q-1]\!]$
② $\mathcal{P} \xrightarrow{a, b, c, d} \mathcal{V}$
$b \leftarrow k_1 - r \mod q$ ; $a \leftarrow b - k_2 y \mod q$

• $\mathcal{V}$'s execution ending
$\widetilde{C_1} \leftarrow [c] \cdot U_1 - [d] \cdot V_1$
$\widetilde{C_2} \leftarrow C_0 + [c] \cdot U_2 - [r + b] \cdot V_2$
$\widetilde{C_3} \leftarrow [a] \cdot U_1 + [b] \cdot Y$
if $(C_1, C_2, C_3)(\widetilde{C_1}, \widetilde{C_2}, \widetilde{C_3}) \wedge C_0 \neq \mathbb{O}_{\mathbb{G}_2}$
    then $b \leftarrow$ Accept else $b \leftarrow \perp$
```

Fig. 2. Interactive designated verifier proof of membership to the language $\mathsf{IDL}(\mathbb{G})$

- Σ.Sign: on message m and period p, the signer does the following:
  - $r \overset{R}{\longleftarrow} [\![1, q-1]\!]$, $R \leftarrow rP$. If $F(R) = 0$ it tries with another value r.
  - $e_p \leftarrow H_v^1(p)$, $d \leftarrow H_{e_p}^2(m, R)$, $T \leftarrow dP$
  - $s \leftarrow (F(T) \cdot d \cdot h(m) \cdot v - u \cdot F(R) - 1)r^{-1} \bmod q$

  The signature is the tuple (R, T, s).
- Σ.Cont: to control the validity of a signature (R, T, s), the signer checks that: $(v \cdot F(T) \cdot h(m)) \cdot T = F(R) \cdot U + s \cdot R + P$ using its private key v.
- Σ.{Conf/Deny}: the signer provides a designated verifier proof of the equality/inequality of two discrete logarithms, namely, $F(R) \cdot U + s \cdot R + P$ to the base $(F(T).h(m)) \cdot T$ and V to the base P (see § 4.2).
- Σ.Conv: there exist two types of conversions, namely
  - The gradual conversion for the signature corresponding to the time period p could be done by releasing the value e_p.
  - The individual conversion can be achieved by releasing the value of d.
- Σ.Vf: The signature corresponding to the period p, once e_p or d is revealed, could be checked by any verifier using the equations: $(d \cdot F(T) \cdot h(m))V = F(R) \cdot U + s \cdot R + P$ and $T = dP$.

4.2 Proofs of Equality/Inequality of Discrete Logarithms

Let $\mathbb{G}$ be a group. To confirm or deny that a bit string is a signature in our undeniable signature scheme, it is necessary to prove that a given quadruple $(U_1, V_1, U_2, V_2) \in \mathbb{G}^4$ is a Diffie-Hellman quadruple (or not), *i.e.* belongs to the set $\mathsf{EDL}(\mathbb{G}) = \{(U_1, V_1, U_2, V_2) \in \mathbb{G}^4, \log_{U_1}(V_1) = \log U_2(V_2)\}$, (or to the set $\mathsf{IDL}(\mathbb{G}) = \mathbb{G}^4 \setminus \mathsf{EDL}(\mathbb{G})$).

To face *blackmailing* or *mafia* attacks against our undeniable signatures, we use interactive designated verifier proofs, as introduced in [11] by Jakobsson, Sako, and Impagliazzo, in Chaum's proofs of equality (*cf.* Fig. 1) and inequality (*cf.* Fig. 2) of discrete logarithm of [6]. The idea is to replace the generic commitment scheme by a *trapdoor commitment* [11] and using classical techniques, the proofs are readily seen to be complete, sound, and above all non-transferable. The protocols, involve a point $Y = yU_1$ where y is the secret key of the verifier, and the prover must be convinced that Y is well-formed (in the registered public key model, the registration procedure is used to force the users to know the secret-key corresponding to their public key).

5 Security Analysis

We note first that the property of non-transferability is fulfilled by our scheme as a direct consequence of the use of designated-verifier proofs in the confirm/deny protocols. Further, we state that our scheme resists existential forgeries and that signatures are anonymous. Both security reductions stand in the generic group model [19].

5.1 Resistance to Forgery

The theorem below states that our variant of Michels-Petersen-Horster scheme is $\mathsf{EF\text{-}CMA}$-secure in the generic group model assuming the preimage resistance, the random affine preimage resistance and the random linear collision resistance of the underlying hash function family.

Theorem 1. *Let $\mathcal{A}$ be an $\mathsf{EF\text{-}CMA}$-adversary in the generic group model, operating in time t, after n group queries and m signing queries, such that $m \ll n^2$ and $n \gg 1$, with success probability $\mathbf{Succ}^{\textsf{ef-cma}}_{\Sigma,\mathcal{A}}$.*

There exist adversaries $\mathcal{B}$, $\mathcal{C}$, and $\mathcal{D}$ operating in time t' against the n-random affine preimage resistance, the n-random linear collision resistance and the preimage resistance of the underlying hash function (respectively) such that:

$$t' \leq t + 5n\tau_G \ln n + 5m \ln n(2\tau_G + \tau_{H^1} + \tau_{H^2} + \tau_F + \tau_h)$$

and

$$6 \cdot \mathbf{Succ}^{raPre(n)}_{h,\mathcal{B}} + 2 \cdot \mathbf{Succ}^{rlColl(n)}_{h,\mathcal{C}} + 3 \cdot n^2 \mathbf{Succ}^{Pre(n)}_{h,\mathcal{D}} \geq \frac{\mathbf{Succ}^{\textsf{ef-cma}}_{\Sigma,\mathcal{A}}}{8} - 5n^4/q - 3mn^3$$

where δ is the advantage of an adversary playing a distinguisher for G, τ_g, τ_F, τ_{H^1}, τ_{H^2} and τ_h are the running time for G, F, H^1, H^2 and h respectively.

The $\mathsf{EF\text{-}CMA}$-adversary $\mathcal{A}$ will output a valid signature $\sigma^\star = (R^\star, T^\star, s^\star)$ on a message $m^\star$ for the time period $p^\star$ with success probability $\mathbf{Succ}^{\mathsf{ef\text{-}cma}}_{\Sigma,\mathcal{A}}$. In our security analysis, this event is divided into subevents according to whether $R^\star$ and $T^\star$ are created during the simulation by a signature query or a group query.

In the list used to maintain the group oracle, a group element created during a group query will have a "group" tag, while the tag "sign" will correspond to elements created in a signature query. Moreover, a signature query on a message m_i for the time period p_i will be answered by a triple (R_i, T_i, s_i), where $R_i, T_i \in \mathbb{G}$. Hence, in addition we will specify the type of an element that has the tag sign: we denote $\mathsf{Type}(R_i) = 0$ and $\mathsf{Type}(T_i) = 1$. The different forgeries output by $\mathcal{A}$ will be classified as follows:

- **Type 0:** $\mathsf{Tag}(R^\star) = \mathsf{group}$, $\mathsf{Tag}(T^\star) = \mathsf{group}$
- **Type 1:** $\mathsf{Tag}(R^\star) = \mathsf{group}$, $\mathsf{Tag}(T^\star) = \mathsf{sign}$ and $\mathsf{Type}(T^\star) = 0$
- **Type 2:** $\mathsf{Tag}(R^\star) = \mathsf{group}$, $\mathsf{Tag}(T^\star) = \mathsf{sign}$ and $\mathsf{Type}(T^\star) = 1$
- **Type 3:** $\mathsf{Tag}(R^\star) = \mathsf{sign}$, $\mathsf{Tag}(T^\star) = \mathsf{group}$ and $\mathsf{Type}(R^\star) = 0$
- **Type 4:** $\mathsf{Tag}(R^\star) = \mathsf{sign}$, $\mathsf{Tag}(T^\star) = \mathsf{group}$ and $\mathsf{Type}(R^\star) = 1$
- **Type 5:** $\mathsf{Tag}(R^\star) = \mathsf{sign}$, $\mathsf{Tag}(T^\star) = \mathsf{sign}$, $\mathsf{Type}(R^\star) = 0$ and $\mathsf{Type}(T^\star) = 0$
- **Type 6:** $\mathsf{Tag}(R^\star) = \mathsf{sign}$, $\mathsf{Tag}(T^\star) = \mathsf{sign}$, $\mathsf{Type}(R^\star) = 0$ and $\mathsf{Type}(T^\star) = 1$
- **Type 7:** $\mathsf{Tag}(R^\star) = \mathsf{sign}$, $\mathsf{Tag}(T^\star) = \mathsf{sign}$, $\mathsf{Type}(R^\star) = 1$ and $\mathsf{Type}(T^\star) = 0$
- **Type 8:** $\mathsf{Tag}(R^\star) = \mathsf{sign}$, $\mathsf{Tag}(T^\star) = \mathsf{sign}$, $\mathsf{Type}(R^\star) = 1$ and $\mathsf{Type}(T^\star) = 1$

We denote ε_i the probability that the forgery $\sigma^\star = (R^\star, T^\star, s^\star)$ output by $\mathcal{A}$ is of type **Type i** (for $i \in \{1, \ldots, 8\}$). We have:

$$\sum_{i=1}^{8} \varepsilon_i = \mathbf{Succ}^{\mathsf{ef\text{-}cma}}_{\Sigma,\mathcal{A}}$$

The adversaries, $\mathcal{B}$, $\mathcal{C}$ and $\mathcal{D}$ will simulate the group and signing oracles according to the alleged kind of forgery returned by $\mathcal{A}$. More precisely, adversary $\mathcal{C}$ will use the forgery to find a random linear collision if it is of type **Type 6**, $\mathcal{D}$ will exploit a forgery of the type **Type 0** to break the preimage resistance and finally, the adversary $\mathcal{B}$ will utilize all the remaining cases to find a random affine preimage.

The group oracle. In this model [19], one assumes that group operations can be perfomed only by means of an oracle. More specifically, suppose that $\mathbb{G}$ is an (additive) group of prime order q generated by P. Then $\mathbb{G}$ is isomorphic to the additive group $\mathbb{Z}_q$ and in the generic model, one assumes that instead of having explicit formulas for the group element iP, the adversary has only access to an "encoding" $\sigma(i) \in S \subset \{0,1\}^*$, that represents the element iP. The generic algorithm $\mathcal{A}$ will then consult the oracle for two types of queries:

- $\mathcal{A}$ requests the encoding of i: the oracle will select randomly a value $\sigma(i)$, to represent the element iP, from the given set of bit-srings.
- Given two encodings $\sigma(i)$ and $\sigma(j)$, $\mathcal{A}$ requests (without knowing necessarily i and j) the encoding of $(\sigma(i \pm j)$. Again the oracle responds with a randomly chosen bit-string.

The only condition on the oracle responses is that if the same group element is queried a second time, the same corresponding encoding must be returned. We will group the above queries in a single type of query, namely, $(\overrightarrow{i}, \overrightarrow{\alpha})$ where $\overrightarrow{i}$ refers to the set of indices of the group elements whereas $\overrightarrow{\alpha}$ denotes the set of exponents. The answers to such queries are elements z_i of $S \subset \{0.1\}^*$. Let $\mathcal{L} = \{z_1, z_2, z_3, \ldots, z_{n+2}\}$ be the sequence of queries' answers where n denotes the total number of queries to the group oracle. We use an interpretation similar to the one in [21], using polynomials $F_i(X)$ over $\mathbb{F}_q$:

- Polynomials F_1 and F_2 are set to $F_1 = 1$ and $F_2 = X$, which correspond to the generator and the public key U respectively. The corresponding bit-strings are z_1 and z_2 respectively.
- At the ℓ-th query $(\overrightarrow{i}, \overrightarrow{\alpha})$, the polynomial F_ℓ is defined as $\sum_{j=1}^{|\overrightarrow{\alpha}|} \alpha_j \mathcal{F}_{\overrightarrow{i}_j}$. If F_ℓ is already listed[5] as F_h, then F_ℓ is marked and the corresponding answer to F_h is returned. Otherwise, z_ℓ is selected at random from S, recorded[6] using $\texttt{Record}(z_\ell \| F_\ell \| \mathsf{group} \| \mathsf{notype})$ and then returned to $\mathcal{A}$.

It is easy to see that the simulation driven by this interpretation is similar to the one of the regular algorithm provided that all the answers corresponding to unmarked polynomials are distinct and no polynomial F_ℓ vanishes at $X = u$. In these conditions, we call the sequence of encodings a safe sequence. The probability of such a sequence is given by the following lemma [21]:

Lemma 1. *Assume $n^2 \leq q$. The probability of unsafe sequence is upper-bounded by $5(n+1)^2/q$.*

The signing oracle. Basically, the signing oracle Σ will receive queries, of the form (m, p) and will respond with a valid signature $\sigma = (R, T, s)$ according to the following simulation:

Simulation of Σ: on query (m, p) do the following:

- $R \xleftarrow{R} S$, $e_p \leftarrow H_v^1(p)$, $d \leftarrow H_{e_p}^2(m, R)$,
- $\texttt{Repeat:}$ $a, b \xleftarrow{R} \mathbb{Z}_q$, $t \leftarrow (a - b \cdot F(R))a^{-1}d^{-1}v^{-1}h(m)^{-1} \bmod q$
  $\texttt{Until}$ $T = g(t) \neq \perp$,
- $\texttt{Record}(R \| aX + b \| \mathsf{sign} \| 0)$, $\texttt{Record}(T \| d \| \mathsf{sign} \| 1)$,
- $s \leftarrow (d \cdot v \cdot t \cdot h(m) - 1)b^{-1} \bmod q$,
- $\texttt{Return}$ (R, T, s).

The confirming/denying oracles. The use of designated verifier proofs of membership and of the registered public key model makes these oracles useless for the attacker. Therefore, we do not describe them in our security proof.

[5] The adversaries $\mathcal{B}$, $\mathcal{C}$ and $\mathcal{D}$ will maintain, in addition to the outputs' list $\mathcal{L}$, three further lists, namely, the list of corresponding polynomials, denoted $\mathcal{F}$, the list of tags $\mathcal{T}$ and the list of types $\mathcal{S}$.

[6] The command $\texttt{Record}(R \| F \| t \| s)$ will abort in some cases, namely when $(R, F', ?, ?)$ already exists and $F' \neq F$. The probability that this event happens can be upper-bounded by n/q, where n is the number of queries to the group oracle.

Proof. Let $(R^\star, T^\star, s^\star)$ be the forgery output by $\mathcal{A}$ on the message $m^\star$ for the time period $p^\star$. Due to space limitations, we will detail only the reduction in the case where this forgery is of type **Type 0**, **Type 2** and **Type 6**.

Description of $\mathcal{B}$. $\mathcal{B}$ picks uniformly at random an integer $i \in \{1, 2, 3, 4, 5, 7, 8\}$ which is its guess for the type of the forgery output by $\mathcal{A}$. In the following simulation, we suppose that $\mathcal{A}$ returns a forgery of type **Type 2** and that $i = 2$ (the other cases are treated similarly).

The forgery produced by A satisfies the following equation[7]

$$a - b \cdot F(R^\star) = (ad - bc) \cdot v \cdot F(T^\star) \cdot h(m),$$

where $R^\star = aU + bP$ and $T^\star = cU + dP$. Since $T^\star$ was generated during a signature query as a "T" ($\mathsf{Type}(T) = 1$) we have $c = 0$ (the adversary must know the discrete logarithm of T in base P in case the attacker asks for the signature conversion). Hence, the equation turns out to be $a - b \cdot F(R) = a \cdot d \cdot v \cdot F(T) \cdot h(m)$ or

$$1 - \frac{a}{b} F(R) = d \cdot v \cdot v \cdot F(T) \cdot h(m).$$

Thus, in order to find a random affine preimage, $\mathcal{B}$ must plug the values α_i and β_j in answers to the group and the signature queries (respectively). More precisely, he must answer group queries (a, b) by R such that $1 - aF(R)/b = \alpha$, similarly, signature queries must be answered by (R, T, s), such that $-d \cdot v \cdot v \cdot F(T) = \beta$:

Game 0: We consider an $\mathsf{EF\text{-}CMA}$-adversary $\mathcal{A}$ in the generic group model. In any game **Game i**, we denote S_i the event "$(R^\star, T^\star, s^\star)$ is a valid forgery of type **Type 2** and $i = 2$". By definition, we have $\Pr[S_0] = \varepsilon_2/7$.

Game 1: We use the interpretation described above for the generic oracle which considers a safe sequence $\mathcal{L}$. This event' s probability $\Pr[S_1]$ satisfies

$$|\Pr[S_1] - \Pr[S_0]| \leq 5(n+1)^2/q.$$

Game 2: In this game we modify the simulation of the group oracle. On query (a, b) such that the corresponding polynomial $F = aX + b$ is new, $\mathcal{B}$ does the following:

```
• Repeat
      pick $\alpha$ from the corresponding oracle
      compute $r \leftarrow (1 - \alpha)ab^{-1}$
      compute $\tilde{R} \leftarrow g(r)$
• Until $\tilde{R} \neq$ Fail.
• Return $\tilde{R}$.
```

However, $\mathcal{B}$ stops after $5 \ln n$ trials. The event S_2 differs from the previous one if $\tilde{R}$ remains undefined. Since the experiments are mutually independent (a and b are uniformly distributed), we may use

[7] This follows from the verification equation $(v \cdot F(T^\star) \cdot h(m))T^\star = F(R^\star) \cdot U + s^\star \cdot R^\star + P$.

a lemma from elementary probability theory [21, Lemma 5] to bound the corresponding probability by $1/n^2$. The overall probability when l ranges the set of queries indices is then $1/n$. Hence, we have

$$\Pr[S_2] \geq (1 - 1/n) \Pr[S_1].$$

Game 3: In this simulation, the groupe oracle replaces $\tilde{R}$ from the previous game by R a new random encoding. It executes $\texttt{Record}(R \| aX + b \| \mathsf{group})$ and return the value R as the response to the oracle query. Since the inputs to G are uniformly distributed (α is picked at random), we can use n times the almost-invertibility of F (the so-called *Hybrid Technique*) to bound the probability of S_3:

$$|\Pr[S_3] - \Pr[S_2]| \leq n\delta_G.$$

Game 4: In this game, $\mathcal{B}$ changes the simulation of the signing oracle. On query (m, p) it does the following:

- Compute $e_p \leftarrow H_v^1(p)$
- Pick the next α in the instance of the random affine preimage problem
- Pick $a \in \mathbb{Z}_q^*$,
- Compute $b \leftarrow a(\alpha h(m) - 1)F(R)^{-1}$
- $\texttt{Record}(R \| aX + b \| \mathsf{sign} \| 0)$
- Compute $d \leftarrow H_{e_p}^2(m, R)$.
- Repeat

  Pick the next β in the instance of the random affine preimage problem

  Compute $t \leftarrow -d^{-1}v^{-1}\beta$

  Until $\tilde{T} = G(t) \neq \text{Fail}$.
- Compute $s \leftarrow -F(R)a^{-1}$.
- Return $(R, \tilde{T}, s)$

Here again, $\mathcal{B}$ aborts after $5 \ln n$ trials. Using the hybrid technique as above, we have

$$\Pr[S_4] \geq (1 - m/n^2) \Pr[S_{3,}].$$

Game 5: In this game, $\mathcal{B}$ replaces $\tilde{T}$ by T and executes $\texttt{Record}(T \| d \| \mathsf{sign} \| 1)$. Applying the same technique, we get

$$|\Pr[S_5] - \Pr[S_4]| \leq m\delta_G + mn/q.$$

Game 6: In this game, $\mathcal{B}$ exploits the forgery $(R^\star, T^\star, s^\star)$ returned by $\mathcal{A}$. Since $\mathsf{Tag}(R^\star, T^\star) = (\mathsf{group}, \mathsf{sign})$ and $\mathsf{Type}(R^\star, T^\star) = (0, 1)$ and $\mathcal{B}$ generated the correct i, there exist i, j such that $R^\star = R_i, T^\star = T_j$ and $1 - \frac{a_i}{b_i}F(R_i) = \alpha_i$ and $-d_j \cdot v \cdot F(T_j) = \beta_j$, the equation satisfied by the forgery turns out to be $\alpha_i + \beta_j h(m) = 0$. $\mathcal{B}$ would then find a random affine preimage with success probability greater than

$$\epsilon_2/7 + 5n^2/q - n\delta - m\delta - 2mn/q$$

and time

$$t' \leq t + 5n \ln n + m(\tau_{H^1} + \tau_{H^2} + 5\tau_g \ln n + \tau_h + 2\tau_F).$$

Description of $\mathcal{C}$. $\mathcal{C}$ will simulate Γ and Σ such that the simulation exploits a forgery $(R^\star, T^\star, s^\star)$ of the type **Type 6**. Hence $\mathcal{C}$ will simulate Γ in the standard way described in 5.1. Furthermore, he will have to plug the λ's in answers to signature queries in a way that the returned signature $(R^\star, T^\star, s^\star)$ satisfies $1 - \frac{b}{a}F(R^\star) = \lambda$. More precisely, on (m, p), $\mathcal{C}$ does the following:

```
– Pick the next $\lambda$ in the instance of the random affine preimage problem -
– Compute $e_p = H_v^1(p)$
– Repeat
      Pick $\alpha \in_R \mathbb{Z}_q$,
      Compute $r \leftarrow \frac{\lambda-1}{\alpha}$
  Until $R = g(r) \neq Fail$
– Compute $d = H_{e_p}^2(m, R)$
– Repeat
      Pick $a \in_R \mathbb{Z}_q$, Compute $b = \alpha a$ and $t = (a - bF(R))(a \cdot d \cdot v \cdot h(m))^{-1}$
  Until $T = g(t) \neq Fail$
– Record $(R||aX + b||sign, 0)$ - Record $(T||d||sign||1)$
– Compute $s = (d \cdot v \cdot h(m) \cdot F(T) - 1) \cdot b^{-1}$
– Return $(R, T, s)$.
```

It is easy to conclude that this simulation, together with the above forgery returned by the attacker will lead to a find a random linear collision.

Description of $\mathcal{D}$. $\mathcal{D}$ will attempt to exploit a forgery $(R^\star, T^\star, s^\star)$ such that $\mathsf{Tag}(R^\star, T^\star) = (\mathsf{group}, \mathsf{group})$ (**Type 0**) to find a preimage of a certain value, say a. The equation satisfied by the forgery is $a_i - b_i F(R_i) = (a_i b_j - a_j b_i) F(R_j) \cdot v \cdot h(m)$. For this, $\mathcal{D}$ will simulate the signing oracle in the standard way given in 5.1. To simulate Γ, $\mathcal{D}$ selects in advance $i, j \in_R [\![1, n]\!]$. If $i < j$, then on the i-th query (a_i, b_i), $\mathcal{D}$ will select $R_i \in_R S$ and record it using $\mathtt{Record}(R_i \| a_i X + b_i \| \mathsf{group})$. On the $j-$th query (a_j, b_j), $\mathtt{compute}$ $T_j \leftarrow g(a \cdot (a_i - b_i F(R))(a_i b_j - a_j b_i)^{-1} v^{-1})$. With probability at least $1/n^2$, $\mathcal{D}$ would have chosen the correct i, j and the success of having $T_j \neq \perp$ is at least $1/3$ (almost invertibility of F and randomness of a). If $j \leq i$, $\mathcal{D}$ will proceed in a similar manner. □

5.2 Anonymity

Theorem 2. *Let $\mathcal{A}$ be an Ano-CMA-adversary operating in time t, after n group queries and m signing queries, with success advantage ε, such that $m \ll n^2$, $m \ll q$ and $n \gg 2$, then there exist adversaries $\mathcal{B}_1$, $\mathcal{B}_2$ and $\mathcal{C}$, operating in time t' and attempting to break the pseudo-randomness property of H^1, the pseudo-randomness of H^2 and the random linear collision of h (respectively) with success probability $\mathbf{Succ}^{prf}_{H^1,\mathcal{B}_1}$, $\mathbf{Succ}^{prf}_{H^2,\mathcal{B}_2}$ and $\mathbf{Succ}^{rlColl(n)}_{h,\mathcal{C}}$ such that:*

$$t' \leq t + 5n\tau_g \ln n + 5m \ln n(\tau_{H^2} + \tau_h + \tau_g) + m\tau_{H^1}$$

and

$$\mathbf{Succ}^{prf}_{H^1,\mathcal{B}_1} + \mathbf{Succ}^{prf}_{H^2,\mathcal{B}_2} + 2\frac{\mathbf{Succ}^{rlColl(n)}_{h,\mathcal{C}}}{n} \geq \frac{\varepsilon}{n} + \frac{18n}{q} - n\delta + \delta + \frac{3m\delta}{n}$$

where δ is the advantage of an adversary playing a distinguisher for g, τ_g, τ_F, τ_{H^1}, τ_{H^2} and τ_h are the running time for g, F, H^1, H^2 and h respectively.

Proof. The proof is similar to the previous one and will be given in the full version of the paper. □

6 Conclusion

We properly defined security notions for convertible undeniable signatures that support the additional property of *achronous* gradual conversion. Adapting the scheme proposed by Michels, Petersen and Horster in 1996, we realized the first scheme featuring this usefull notion of conversion. In addition, we gave the first security analysis of the Michels-Petersen-Horster protocol, thereby addressing a problem left open since 1996. We have modified this scheme such that it becomes a generic one, which allows to use it for instance in the setting of elliptic curves (and therefore offers attractive practical advantages in terms of signature length and performances). In this context, in comparison with the time-selective convertible undeniable signatures from [13], the computational costs for the confirmation/disavowal protocols and the conversion algorithms, are much smaller.

References

1. M. Bellare, A. Boldyreva, A. Desai, and D. Pointcheval, *Key-Privacy in Public-Key Encryption.*, Advances in Cryptology - Asiacrypt 2001 (C. Boyd, ed.), Lect. Notes Comput. Sci., vol. 2248, Springer, 2001, pp. 566–582.
2. M. Bellare and T. Kohno, *Hash Function Balance and its Impact on Birthday Attacks.*, Advances in Cryptology - Eurocrypt 2004 (C. Cachin and J. Camenisch, eds.), Lect. Notes Comput. Sci., vol. 3027, Springer, 2004, pp. 401–418.
3. M. Bellare and P. Rogaway, *Random Oracles are Practical: A Paradigm for Designing Efficient Protocols.*, Proceedings of the First ACM Conference on Computer and Communications Security (D. Denning, R. Pyle, R. Ganesan, R. Sandhu, and V. Ashby, eds.), ACM Press, 1993, pp. 62–73.
4. J. Boyar, D. Chaum, I. B. Damgård, and T. B. Pedersen, *Convertible undeniable signatures.*, Advances in Cryptology - Crypto'90 (A. J. Menezes and S. A. Vanstone, eds.), Lect. Notes Comput. Sci., vol. 537, Springer, 1991, pp. 189–205.
5. D. R. L. Brown, *Generic Groups, Collision Resistance, and ECDSA.*, Des. Codes Cryptography **35** (2005), no. 1, 119–152.
6. J. Camenisch and V. Shoup, *Practical Verifiable Encryption and Decryption of Discrete Logarithms.*, Advances in Cryptology - Crypto 2003 (D. Boneh, ed.), Lect. Notes Comput. Sci., vol. 2729, Springer, 2003, pp. 126–144.
7. D. Chaum and H. van Antwerpen, *Undeniable Signatures.*, Advances in Cryptology - Crypto'89 (G. Brassard, ed.), Lect. Notes Comput. Sci., vol. 435, Springer, 1990, pp. 212–216.
8. A. W. Dent, *Adapting the Weaknesses of the Random Oracle Model to the Generic Group Model.*, Advances in Cryptology - Asiacrypt 2002 (Y. Zheng, ed.), Lect. Notes Comput. Sci., vol. 2501, Springer, 2002, pp. 100–109.

9. S. D. Galbraith and W. Mao, *Invisibility and Anonymity of Undeniable and Confirmer Signatures.*, Topics in Cryptology - CT-RSA 2003 (M. Joye, ed.), Lect. Notes Comput. Sci., vol. 2612, Springer, 2003, pp. 80–97.
10. S. Goldwasser, S. Micali, and R. L. Rivest, *A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks.*, SIAM J. Comput. **17** (1988), no. 2, 281–308.
11. M. Jakobsson, K. Sako, and R. Impagliazzo, *Designated Verifier Proofs and Their Applications.*, Advances in Cryptology - Eurocrypt'96 (U. M. Maurer, ed.), Lect. Notes Comput. Sci., vol. 1070, Springer, 1996, pp. 143–154.
12. C. Kudla and K. G. Paterson, *Non-interactive Designated Verifier Proofs and Undeniable Signatures.*, Cryptography and Coding, 10th IMA International Conference (N. P. Smart, ed.), Lect. Notes Comput. Sci., vol. 3796, Springer, 2005, pp. 136–154.
13. F. Laguillaumie and D. Vergnaud, *Time-Selective Convertible Undeniable Signatures.*, Topics in Cryptology - CT-RSA 2005 (A. J. Menezes, ed.), Lect. Notes Comput. Sci., vol. 3376, Springer, 2005, pp. 154–171.
14. M. Michels, H. Petersen, and P. Horster, *Breaking and Repairing a Convertible Undeniable Signature Scheme.*, Proceedings of the Third ACM Conference on Computer and Communications Security (L. Gong and J. Stern, eds.), ACM Press, 1996, pp. 148–152.
15. W. Ogata, K. Kurosawa, and S.-H. Heng, *The Security of the FDH Variant of Chaum's Undeniable Signature Scheme*, IEEE Trans. Inf. Theory **52** (2006), no. 5, 2006 – 2017.
16. T. Okamoto and D. Pointcheval, *The Gap-Problems: a New Class of Problems for the Security of Cryptographic Schemes.*, 4th International Workshop on Practice and Theory in Public Key Cryptography, PKC 2001 (K. Kim, ed.), Lect. Notes Comput. Sci., vol. 1992, Springer, 2001, pp. 104–118.
17. P. Paillier and D. Vergnaud, *Discrete-Log Based Signatures May Not Be Equivalent to Discrete-Log.*, Advances in Cryptology - Asiacrypt 2005 (B. Roy, ed.), Lect. Notes Comput. Sci., vol. 3788, Springer, 2005, pp. 1–20.
18. P. Rogaway and T. Shrimpton, *Cryptographic Hash-Function Basics: Definitions, Implications, and Separations for Preimage Resistance, Second-Preimage Resistance, and Collision Resistance.*, Fast Software Encryption, 11th International Workshop, FSE 2004 (B. K. Roy and W. Meier, eds.), Lect. Notes Comput. Sci., vol. 3017, Springer, 2004, pp. 371–388.
19. V. Shoup, *Lower Bounds for Discrete Logarithms and Related Problems.*, Advances in Cryptology - Eurocrypt'97 (W. Fumy, ed.), Lect. Notes Comput. Sci., vol. 1233, Springer, 1997, pp. 256–266.
20. W. Stadje, *The Residues modulo m of Products of Random Integers.*, Comb. Probab. Comput. **11** (2002), no. 5, 529–540.
21. J. Stern, D. Pointcheval, J. Malone-Lee, and N. P. Smart, *Flaws in applying proof methodologies to signature schemes.*, Advances in Cryptology - Crypto 2002 (M. Yung, ed.), Lect. Notes Comput. Sci., vol. 2442, Springer, 2002, pp. 93–110.