Published in M.K. Franklin, L.C.K. Hui, and D.S. Wong, Eds, *Cryptology and Network Security (CANS 2008)*, vol. 5339 of *Lecture Notes in Computer Science*, pp. 98–107, Springer, 2008.

An Efficient On-line/Off-line Signature Scheme Without Random Oracles

Marc Joye

Thomson R&D France
Technology Group, Corporate Research, Security Laboratory
1 avenue de Belle Fontaine, 35576 Cesson-Sévigné Cedex, France
marc.joye@thomson.net

Abstract. On-line/off-line signature schemes allow one to quickly compute a digital signature from a pre-computed coupon. One of the most efficient schemes to date is the GPS scheme, due to Girault, Poupard and Stern. Its security stands in the random oracle model. This paper presents a novel on-line/off-line signature featuring the same on-line efficiency (only a single *small* integer multiplication has to be computed) but without relying on random oracles.

Keywords. Cryptography, digital signature, on-line/off-line signing, standard model.

1 Introduction

Likewise handwritten signatures, digital signatures should feature important requirements making them compelling for a number of applications. Namely, in addition to be unforgeable, they should offer the properties of authenticity, integrity and non-repudiation of signed messages. The advent of public-key cryptographic techniques made possible to allow anyone to perform publicly the verification of signatures. Informally, in a digital signature scheme, each user possesses a pair of matching public key and private key. The private key is used to sign messages while the public key is used to verify signatures.

There exist numerous digital signature schemes, the security of which rely on various intractability assumptions (e.g., discrete logarithms or integer factorization). Several signature schemes are shown to be secure even against chosen-message attacks. Existential unforgeability against chosen-message attacks is the security notion classically retained for signature schemes. Basically, it requires that an adversary having access to a signing oracle returning the signature on messages of its choice is unable to produce a valid signature on a message not previously submitted to the signing oracle [17]. In this paper, we are interested in secure yet efficient signature schemes. By efficiency, we mean here that the signing process should be as fast as possible. This leads us to the paradigm of *on-line/off-line signatures* introduced by Even *et al.* [10] and later improved by Shamir and Tauman [24]. See also [7] for a unifying paradigm encompassing the two approaches.

In an on-line/off-line signature scheme, the signing process is subdivided into two phases. The first phase, performed off-line, is independent of the message to be signed. The second phase, performed on-line, takes on input a value precomputed in the off-line phase and a message and produces a signature. Only the on-line phase is required to be fast. Many applications can afford slower computations as long as they are not performed on-line. Examples include a server pre-computing values at idle time or a low-end smart card with pre-computed values stored in memory. In the latter case, the pre-computed values are sometimes referred to as 'use & throw coupons' [22]. See also [27] for applications in routing protocols.

The so-called GPS signature scheme [16] (see also [15, 23]), obtained from the companion identification scheme using the Fiat-Shamir heuristic [11], is one of the most efficient on-line/off-line signature schemes. The on-line phase boils down to the computation of a *small* integer (i.e., non-modular) multiplication. However, being built via the Fiat-Shamir heuristic, the security of the GPS signature scheme stands in the random oracle model [2]. The random oracle model is an idealized model assuming that the output of a hash function behaves as a random generator. Although guaranteeing that the general design should not be flawed, a proof in the random oracle model cannot be considered as an absolute proof. In [5, 6], Canetti *et al.* show that there exist signature schemes secure in the random oracle model but for which no secure implementations do exist.

Several efficient on-line/off-line signature schemes in the standard model (i.e., without random oracles) are known [24, 3, 21, 8, 28] but none of them features the very fast on-line-phase of the GPS signature scheme. This paper fills the gap and provides such a scheme. The proposed on-line/off-line signature scheme even outperforms the GPS signature scheme for short messages since no prior hashing is required. Moreover, combined with [14], it yields a very efficient identity-based on-line/off-line signature scheme. We note that the GPS signature scheme has been standardized by ISO/IEC in 2008 [20].

The rest of this paper is organized as follows. In the next section, we introduce some definitions. In Section 3, we present our on-line/off-line signature scheme. Then, in Section 4, we prove its security and analyze its performance. Finally, we conclude in Section 5.

2 Preliminaries

2.1 Signature schemes

A *signature scheme* is a triplet, $(\mathsf{Gen}, \mathsf{Sign}, \mathsf{Verify})$, of probabilistic polynomial-time algorithms satisfying:

1. *Key generation algorithm* Gen. On input security parameter k, algorithm Gen produces a pair $(\mathsf{pk}, \mathsf{sk})$ of matching public and private keys.

2. *Signing algorithm* Sign. Given a message m in a set $\mathcal{M}$ of messages and a pair of matching public and private keys $(\mathsf{pk}, \mathsf{sk})$, Sign produces a signature σ.
3. *Verification algorithm* Verify. Given a signature σ, a message $m \in \mathcal{M}$ and a public key pk, Verify checks whether σ is a valid signature on m with respect to pk.

As aforementioned, the classical notion for the security of signature schemes is existential unforgeability against chosen-message attacks (in short, $\mathsf{EUF\text{-}CMA}$).

Definition 1. *A signature scheme* $(\mathsf{Gen}, \mathsf{Sign}, \mathsf{Verify})$ *is said* secure *if the success probability*

$$\mathsf{Succ}^{\mathsf{EUF\text{-}CMA}}(\mathcal{A}) := \Pr\left[\begin{array}{c}(\mathsf{pk},\mathsf{sk}) \leftarrow \mathsf{Gen}(1^k), (m_*, \sigma_*) \leftarrow \mathcal{A}^{\mathsf{Sign}(\mathsf{sk};\cdot)}(\mathsf{pk}) : \\ \mathsf{Verify}(\mathsf{pk}; m_*, \sigma_*) = \mathit{true}\end{array}\right]$$

is negligible, for every probabilistic polynomial-time adversary $\mathcal{A}$ having access to signing oracle $\mathsf{Sign}(\mathsf{sk};\cdot)$, and returning a valid signature σ_* on a message m_* that was not submitted to the signing oracle.

When the signing algorithm is probabilistic, a setting slightly more general than the single-occurrence chosen-message attack scenario can be considered [25]. The corresponding security notion is referred to as *strong unforgeability against chosen-message attacks* ($\mathsf{sEUF\text{-}CMA}$).

Definition 2. *A signature scheme* $(\mathsf{Gen}, \mathsf{Sign}, \mathsf{Verify})$ *is said* [strongly] secure *if the success probability*

$$\mathsf{Succ}^{\mathsf{sEUF\text{-}CMA}}(\mathcal{A}) := \Pr\left[\begin{array}{c}(\mathsf{pk},\mathsf{sk}) \leftarrow \mathsf{Gen}(1^k), (m_*, \sigma_*) \leftarrow \mathcal{A}^{\mathsf{Sign}(\mathsf{sk};\cdot)}(\mathsf{pk}) : \\ \mathsf{Verify}(\mathsf{pk}; m_*, \sigma_*) = \mathit{true}\end{array}\right]$$

is negligible, for every probabilistic polynomial-time adversary $\mathcal{A}$ having access to signing oracle $\mathsf{Sign}(\mathsf{sk};\cdot)$, and returning a valid signature σ_* on a message m_* where (m_*, σ_*) is different from all pairs (m_i, σ_i) of chosen messages m_i submitted to the signing oracle and corresponding signatures σ_i returned by the signing oracle.

2.2 Intractability assumptions

Typically, the security of a signature scheme is conditioned to some intractability assumptions. For the proposed scheme, we will rely on the strong RSA assumption [1, 13] and the short exponent discrete logarithm assumption [26] (also used in the GPS signature scheme).

Definition 3. *The* strong RSA assumption (sRSA) *is that it is hard, on input a safe*[1] *RSA modulus N and a random element $s \in \mathbb{Z}_N^*$, to find a pair $(u, r) \in$*

[1] An RSA modulus $N = pq$ is said safe when prime $p = 2p' + 1$ and prime $q = 2q' + 1$ for some primes p' and q'.

$\mathbb{Z}_N \times \mathbb{Z}_{>1}$ *satisfying* $s \equiv u^r \pmod N$. *More formally, the success probability of any probabilistic polynomial-time adversary* $\mathcal{A}$*:*

$$\Pr\big[N \leftarrow \mathsf{sRSA}(1^k), s \leftarrow \mathbb{Z}_N^*, (u, r) \leftarrow \mathcal{A}(N, s) : u^r \equiv s \pmod N \ \wedge \ r > 1\big]$$

is negligible.

Definition 4. *The* short exponent discrete logarithm assumption (sDL) *is that it is hard, on input a safe RSA modulus* N*, a random element* $s \in \mathbb{Z}_N^*$ *and* $v = s^z \bmod N$ *for a [small] integer* z*, to recover the value of* z*. More formally, the success probability of any probabilistic polynomial-time adversary* $\mathcal{A}$*:*

$$\Pr\big[(N, z) \leftarrow \mathsf{sDL}(1^k), s \leftarrow \mathbb{Z}_N^*, v \leftarrow s^z \bmod N, z' \leftarrow \mathcal{A}(N, s, v) : z' = z\big]$$

is negligible.

3 Proposed On-line/Off-line Signature Scheme

Let ℓ_N, ℓ_Z, ℓ_S, ℓ_E, ℓ_H and ℓ_K be six security parameters, satisfying

$$\ell_N \geq 2(\ell_E + 2), \quad b(\ell_E - 1) \geq \ell_K + 1, \quad \ell_N - 4 \geq \ell_K \geq \ell_Z + \ell_H + \ell_S \qquad (1)$$

for an integer $b \geq 1$. (Typical values for the security parameters are discussed in § 4.2.)

The message space is defined as $\mathcal{M} = \{0,1\}^{\ell_H}$, which can also be viewed as the set of integers in the range $[0, 2^{\ell_H} - 1]$.

Key generation Choose two random primes $p = 2p' + 1$ and $q = 2q' + 1$ where p' and q' are primes of equal length, so that $N = pq$ is of length exactly ℓ_N. Choose at random two quadratic residues g and x in $\mathbb{Z}_N^*$. Finally, for a random ℓ_Z-bit integer z, compute $h = g^{-z} \bmod N$.

The public key is $\mathsf{pk} = \{g, h, x, N\}$ and the private key is $\mathsf{sk} = \{p, q, z\}$.

Signing Let $m \in \mathcal{M}$ denote the message being signed.

- [*Off-line phase*] Randomly pick an ℓ_K-bit integer t and an ℓ_E-bit prime e. Next compute

$$y = (x\, g^{-t})^d \bmod N \quad \text{where } d = e^{-b} \bmod p'q' \ . \qquad (2)$$

- [*On-line phase*] From a triplet (t, y, e) computed off-line, evaluate

$$k = t + m\, z \ . \qquad (3)$$

and return the signature $\sigma = (k, y, e)$.

Verification Signature $\sigma = (k, y, e)$ on message $m \in \mathcal{M}$ is accepted iff

1. e is an odd ℓ_E-bit integer,
2. k is an ℓ_K-bit integer, and

3. $y^{e^b}\, g^k\, h^m \equiv x \pmod{N}$.

As for the Cramer-Shoup signature scheme [9] and its derivatives [29, 4, 12], there is no need to check the primality of e in the verification algorithm. Observe also that the use of a prime power in Eq. (2) as in [12, 18] — rather than simply a prime — speeds up the off-line phase but also reduces the length of the resulting signatures. Moreover, the use of a small value for z as in [16] speeds up the on-line phase and reduces the length of the signatures; in contrast, the schemes in [8, 28] require a multiplication by a full-size integer in the on-line phase.

We note there is no hash function involved in the signing process. Long messages can however be dealt with by first reducing their length to the appropriate range using a collision-resistant function $H : \{0,1\}^* \rightarrow \mathcal{M}$.

4 Analysis

In this section, we show that our signature scheme is strongly secure under the strong RSA assumption and the short exponent discrete logarithm assumption (see Section 2). We also analyze its performance.

4.1 Proof of security

Assume that there exists a polynomial-time chosen-message attacker $\mathcal{A}$, allowed to make q_S queries to a signing oracle $\mathcal{O}^{\Sigma}$, that is able to produce a signature forgery. For $i \in \{1, \ldots, q_S\}$, we let m_i be the i^{th} message queried to $\mathcal{O}^{\Sigma}$ and $\sigma_i = (k_i, y_i, e_i)$ the i^{th} corresponding signature returned by $\mathcal{O}^{\Sigma}$. We let $\sigma_* = (k_*, y_*, e_*)$ denote the forgery returned by $\mathcal{A}$ on a message $m_* \in \mathcal{M}$ and $(m_*, \sigma_*) \neq (m_i, \sigma_i)$ for all $i \in \{1, \ldots, q_S\}$. We will show that the existence of attacker $\mathcal{A}$ contradicts a cryptographic assumption (namely, the strong RSA assumption or the short exponent discrete logarithm assumption), which proves the security of the scheme.

We distinguish 3 types of attackers.

Type Ia: $e_* = e_{\hat{\imath}}$ and $y_* \neq y_{\hat{\imath}}$, for some $\hat{\imath} \in \{1, \ldots, q_S\}$.

In this case, we show that $\mathcal{A}$ can be used to solve the (safe) RSA problem. That is, given a safe RSA modulus N, an ℓ_E-bit prime $r \in \mathbb{Z}^*_{\phi(N)}$ and a random element $s \in \mathbb{Z}^*_N$, we want to find u such that $u \equiv s^{1/r} \pmod{N}$.[2]

- We randomly pick $\hat{\imath} \in \{1, \ldots, q_S\}$. For all $i \in \{1, \ldots, q_S\}$, $i \neq \hat{\imath}$, we let e_i be a random ℓ_E-bit prime; we also set $e_{\hat{\imath}} = r$. We assume that for all $i \in \{1, \ldots, q_S\}$, $i \neq \hat{\imath}$, we have $e_i \neq r$, which occurs with overwhelming probability. We create the public key $\mathsf{pk} = \{g, h, x, N\}$ with

$$g = s^{2 \prod_{i \neq \hat{\imath}} {e_i}^b} \bmod N, \quad h = g^{-z} \bmod N, \quad x = w^{2 \prod_i {e_i}^b}\, g^{t_{\hat{\imath}}} \bmod N$$

where z is a random ℓ_Z-bit integer, w is a random element in $\mathbb{Z}^*_N$ and $t_{\hat{\imath}}$ is a random ℓ_K-bit integer.

[2] Note that such an attacker also breaks the strong RSA assumption.

– The signing oracle can be simulated as follows. On input a message $m_j \in \mathcal{M}$, $j \in \{1, \ldots, q_S\}$, we return
  - $\sigma_{\hat{\imath}} = (k_{\hat{\imath}}, y_{\hat{\imath}}, e_{\hat{\imath}})$ if $j = \hat{\imath}$, with

$$k_{\hat{\imath}} = t_{\hat{\imath}} + m_{\hat{\imath}}\, z, \quad y_{\hat{\imath}} = w^{2 \prod_{i \neq \hat{\imath}} {e_i}^b} \bmod N\,;$$

  - $\sigma_j = (k_j, y_j, e_j)$ otherwise, with

$$k_j = t_j + m_j\, z, \quad y_j = w^{2 \prod_{i \neq j} {e_i}^b}\, s^{2(t_{\hat{\imath}} - t_j) \prod_{i \neq j, \hat{\imath}} {e_i}^b} \bmod N$$

    where t_j is a random ℓ_K-bit integer.
– Let $\sigma_* = (k_*, y_*, e_*)$ with $e_* = e_{\hat{\imath}} = r$ be the signature forgery on a message $m_* \in \mathcal{M}$, returned by $\mathcal{A}$. Letting $t_* = k_* - m_* z$ and $\nu = 2(t_{\hat{\imath}} - t_*) \prod_{i \neq \hat{\imath}} {e_i}^b$, we have

$$\left(\frac{y_*}{y_{\hat{\imath}}}\right)^{r^b} \equiv g^{k_{\hat{\imath}} - k_*}\, h^{m_{\hat{\imath}} - m_*} \equiv s^{\nu} \pmod N\ .$$

  Moreover, we have $t_{\hat{\imath}} \neq t_*$ as otherwise we would have $(y_*/y_{\hat{\imath}})^{r^b} \equiv 1 \pmod N$ and thus $y_* = y_{\hat{\imath}}$ since $\gcd(r^b, 2p'q') = 1$, a contradiction. As a result, we have $\gcd(r^b, \nu) = \gcd(r^b, t_{\hat{\imath}} - t_*) = r^\rho$ for some $\rho \in \{0, \ldots, b-1\}$ since prime power $r^b > |t_{\hat{\imath}} - t_*|$. Hence, by the extended Euclidean algorithm, we can find integers α and β such that $\alpha\, r^b + \beta\, \nu = r^\rho$. This implies

$$s \equiv s^{\alpha\, r^{b-\rho} + \beta\, \frac{\nu}{r^\rho}} \equiv \left(s^\alpha \left(\frac{y_*}{y_{\hat{\imath}}}\right)^\beta\right)^{r^{b-\rho}} \pmod N\ .$$

  Consequently, $u := \left(s^\alpha\, (y_*/y_{\hat{\imath}})^\beta\right)^{r^{b-\rho-1}} \bmod N$ solves the RSA problem: $u \equiv s^{1/r} \pmod N$. □

Type Ib: $e_* = e_{\hat{\imath}}$ and $y_* = y_{\hat{\imath}}$, for some $\hat{\imath} \in \{1, \ldots, q_S\}$.

In this case, we show that $\mathcal{A}$ can be used to solve the short exponent discrete logarithm problem. That is, given a safe RSA modulus N, a random element $s \in \mathbb{Z}_N^*$ and $v = s^z \bmod N$ for an ℓ_Z-bit integer z, we want to recover the value of z.

– For all $i \in \{1, \ldots, q_S\}$, we let e_i be a random ℓ_E-bit prime. We create the public key $\mathsf{pk} = \{g, h, x, N\}$ with

$$g = s^{2 \prod_i {e_i}^b} \bmod N, \quad h = v^{-2 \prod_i {e_i}^b} \bmod N, \quad x = w^{2 \prod_i {e_i}^b} \bmod N$$

  where w is a random element in $\mathbb{Z}_N^*$.
– On input message $m_j \in \mathcal{M}$, $j \in \{1, \ldots, q_S\}$, we simulate the signing oracle by choosing a random ℓ_K-bit integer k_j and returning $\sigma_j = (k_j, y_j, e_j)$ with

$$y_j = \left(s^{-k_j}\, v^{m_j}\, w\right)^{2 \prod_{i \neq j} {e_i}^b} \bmod N\ .$$

– Let $\sigma_* = (k_*, y_*, e_*)$ with $y_* = y_{\hat{\imath}}$ and $e_* = e_{\hat{\imath}}$ be the signature forgery on a message $m_* \in \mathcal{M}$, returned by $\mathcal{A}$. As both σ_* and $\sigma_{\hat{\imath}}$ are valid signatures, we have $g^{k_*} h^{m_*} \equiv g^{k_{\hat{\imath}}} h^{m_{\hat{\imath}}} \pmod{N}$ and so

$$k_* - z\, m_* \equiv k_{\hat{\imath}} - z\, m_{\hat{\imath}} \pmod{p'q'}$$

noting that $h = g^{-z} \bmod N$. Given the definition ranges, the above relation does hold over the integers. Hence, we have $k_* - k_{\hat{\imath}} = z(m_* - m_{\hat{\imath}})$. Moreover, we have $m_* \neq m_{\hat{\imath}}$ as otherwise we would have $k_* = k_j$ and thus $(m_*, \sigma_*) = (m_{\hat{\imath}}, \sigma_{\hat{\imath}})$, a contradiction. Therefore, we get

$$z = \frac{k_* - k_{\hat{\imath}}}{m_* - m_{\hat{\imath}}}\ ,$$

the discrete logarithm of v w.r.t. s. □

Type II: $e_* \neq e_i$ for all $i \in \{1, \ldots, q_S\}$.

In this case, we show that $\mathcal{A}$ can be used to solve the flexible RSA problem (a.k.a. strong RSA problem). That is, given a safe RSA modulus N and a random element $s \in \mathbb{Z}_N^*$, we want to find (u, r) such that $s \equiv u^r \pmod{N}$ and $r > 1$.

– For all $i \in \{1, \ldots, q_S\}$, we let e_i be a random ℓ_E-bit prime. We create the public key $\mathsf{pk} = \{g, h, x, N\}$ with

$$g = s^{2 \prod_i {e_i}^b} \bmod N, \quad h = g^{-z} \bmod N, \quad x = g^a \bmod N$$

where z is a random ℓ_Z-bit integer and a is a random integer in $\{1, \ldots, N^2\}$.

– On input message $m_j \in \mathcal{M}$, $j \in \{1, \ldots, q_S\}$, we simulate the signing oracle by choosing a random ℓ_K-bit integer t_j and returning $\sigma_j = (k_j, y_j, e_j)$ with

$$y_j = \left(s^{2 \prod_{i \neq j} {e_i}^b}\right)^{a - t_j} \bmod N, \quad k_j = t_j + m_j\, z\ .$$

– Let $\sigma_* = (k_*, y_*, e_*)$ be the signature forgery on a message $m_* \in \mathcal{M}$, returned by $\mathcal{A}$. Letting $\nu = 2(a - k_* + z\, m_*) \prod_i {e_i}^b$, we have

$${y_*}^{{e_*}^b} \equiv x\, g^{-k_*}\, h^{-m_*} \equiv s^{\nu} \pmod{N}\ .$$

Since e_* is an odd ℓ_E-bit integer and $e_* \neq e_i$ for all $i \in \{1, \ldots, q_S\}$, it follows that $\delta := \gcd({e_*}^b, \nu) = \gcd({e_*}^b, a - k_* + z\, m_*)$. Hence, by the extended Euclidean algorithm, we can find integers α and β such that $\alpha \frac{{e_*}^b}{\delta} + \beta \frac{\nu}{\delta} = 1$, which, noting that $\gcd(\delta, 2p'q') = 1$, implies

$$s \equiv s^{\alpha \frac{{e_*}^b}{\delta} + \beta \frac{\nu}{\delta}} \equiv s^{\alpha \frac{{e_*}^b}{\delta}}\ {y_*}^{\beta \frac{{e_*}^b}{\delta}} \equiv (s^{\alpha}\, {y_*}^{\beta})^{\frac{{e_*}^b}{\delta}} \pmod{N}\ .$$

If we set $u := s^{\alpha}\, {y_*}^{\beta} \bmod N$ and $r := {e_*}^b / \delta$ then (u, r) is a solution to the flexible RSA problem, provided that $r \neq 1$. Since a is chosen in $\{1, \ldots, N^2\}$ and since attacker $\mathcal{A}$ knows at best the value of $a \bmod p'q'$ from x, the probability that $r = 1$, or equivalently, that ${e_*}^b \mid (a - k_* + z\, m_*)$ is negligible. □

4.2 Efficiency analysis

The proposed signature scheme involves several parameters, namely ℓ_N, ℓ_Z, ℓ_S, ℓ_E, ℓ_H and ℓ_K. We discuss below how to choose those parameters in order to get an adequate security. Our analysis is based on [16].

The security of the proposed signature scheme relies on the strong RSA assumption and the short exponent discrete logarithm assumption. Although in principle easier than the factoring problem, the best known way to solve the strong RSA problem consists in factoring the modulus. Therefore, an RSA modulus of length at least 1536 bits, or equivalently $\ell_N \geq 1536$, should validate the strong RSA assumption. Likewise the most efficient methods for computing short exponent discrete logarithms are in the square root of the size of the exponent. Hence, choosing $\ell_Z \geq 160$ should prevent the recovery of secret parameter z. Parameter ℓ_S must be chosen so as $\ell_K \gg \ell_Z + \ell_H$ in order to guarantee the statistical zero-knowledge property; as in [16], we advise to set $\ell_S \geq 80$. Finally, the length for prime e, ℓ_E, in the signing algorithm is subject to the requirement that it should be very unlikely to generate twice the same prime. To avoid such birthday attacks, the bit-length of prime e must be (roughly) at least $\kappa + \log_2 q_S$ to offer a κ-bit security, where q_S is the maximum number of allowed signature queries [19]. As a result, assuming $q_S \approx 2^{30}$, setting $\ell_E \geq 128$ appears to be a safe choice. The remaining parameters (i.e., ℓ_K and ℓ_H) must be chosen so as to satisfy Eq. (1).

Typically, if we choose $\ell_N = 1536$, $\ell_Z = 160$, $\ell_S = 80$ and $\ell_E = 128$, Eq. (1) yields

$$127b - 1 \geq \ell_K \geq 240 + \ell_H \ .$$

Hence, assuming we are signing 256-bit messages (or longer messages using a standard hash function like SHA-256) —that is, $\ell_H = 256$, we can set $b = 4$ and $\ell_K = 496$. So, for 1536-bit RSA moduli, a signature will be of length 2160 bits. But the main advantage of the proposed scheme resides in the efficacy of the on-line phase (cf. Eq. (3)). It only requires a small integer multiplication for obtaining $k = t + m\,z$. Both m (or a hashed value thereof) and z are short values; namely, of 256 and 160 bits with the above exemplary values —hence for those values, the evaluation of k basically costs 640 single-precision integer multiplications on a low-end 8-bit processor with the basic schoolboy method.

5 Conclusion

This paper proposed an efficient on-line/off-line signature scheme. Advantageously, the proposed scheme features a very fast on-line phase: only a single small integer multiplication is required. We note that this is slightly faster than the GPS signature scheme, at least for short messages. This property is especially desired for time-constrained applications and for low-end devices that do not have much in the way computational resources. Furthermore and contrarily to the GPS signature scheme, the security proof stands in the standard model (i.e., without random oracles).

Acknowledgments

We thank the anonymous reviewers for useful comments.

References

1. N. Barić and B. Pfitzmann. Collision-free accumulators and fail-stop signature schemes without trees. In W. Fumy, editor, *Advances in Cryptology – EUROCRYPT '97*, volume 1233 of *Leture Notes in Computer Science*, pages 480–494. Springer, 1997.
2. M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *1st ACM Conference on Computer and Communications Security*, pages 62–73. ACM Press, 1993.
3. D. Boneh and X. Boyen. Short signatures without random oracles and the SDH assumption in bilinear groups. *Journal of Cryptology*, 21(2):149–177, 2008. An extended abstract appears in Eurocrypt 2004.
4. J. Camenisch and A. Lysyanskaya. A signature scheme with efficient protocols. In *Security in Communication Networks (SCN 2002)*, volume 2676 of *Leture Notes in Computer Science*, pages 268–289. Springer, 2002.
5. R. Canetti, O. Goldreich, and S. Halevi. The random oracle methodology, revisited. In *30th Annual ACM Symposium on Theory of Computing (STOC '98)*, pages 209–217. ACM Press, 1998.
6. R. Canetti, O. Goldreich, and S. Halevi. On the random oracle methodology as applied to length-restricted signature schemes. In M. Naor, editor, *Theory of Cryptography (TCC 2004)*, volume 2951 of *Leture Notes in Computer Science*, pages 40–57. Springer, 2004.
7. D. Catalano, M. Di Raimondo, D. Fiore, and R. Gennaro. Off-line/on-line signatures; theoretical aspects and experimental results. In R. Cramer, editor, *Public Key Cryptography – PKC 2008*, volume 4939 of *Leture Notes in Computer Science*, pages 101–120. Springer, 2008.
8. B. Chevallier-Mames and M. Joye. A practical and tightly secure signature scheme without hash function. In M. Abe, editor, *Topics in Cryptology – CT-RSA 2007*, volume 4377 of *Leture Notes in Computer Science*, pages 339–356. Springer, 2007.
9. R. Cramer and V. Shoup. Signature scheme based on the strong RSA assumption. *ACM Transactions on Information and System Security*, 3(3):161–185, 2000.
10. S. Even, O. Goldreich, and S. Micali. On-line/off-line digital signatures. *Journal of Cryptology*, 9(1):35–67, 1996. A preliminary version appears in Crypto '89.
11. A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. In A.M. Odlyzko, editor, *Advances in Cryptology – CRYPTO '86*, volume 263 of *Leture Notes in Computer Science*, pages 186–194. Springer, 1987.
12. M. Fischlin. The Cramer-Shoup strong-RSA signature scheme revisited. In Y. Desmedt, editor, *Public Key Cryptography – PKC 2003*, volume 2567 of *Leture Notes in Computer Science*, pages 116–129. Springer, 2003.
13. E. Fujisaki and T. Okamoto. Statistical zero-knowledge protocols to prove modular polynomial equations. In B. Kaliski, Jr, editor, *Advances in Cryptology – CRYPTO '97*, volume 1294 of *Leture Notes in Computer Science*, pages 16–30. Springer, 1997.

14. D. Galindo, J. Herranz, and E. Kiltz. On the generic construction of identity-based signatures with additional properties. In X. Lai and K. Chen, editors, *Advances in Cryptology – ASIACRYPT 2006*, volume 4284 of *Leture Notes in Computer Science*, pages 178–193. Springer, 2008.
15. M. Girault. Self-certified signatures. In D.W. Davies, editor, *Advances in Cryptology – EUROCRYPT '91*, volume 547 of *Leture Notes in Computer Science*, pages 490–497. Springer, 1992.
16. M. Girault, G. Poupard, and J. Stern. On the fly authentication and signature schemes based on groups of unknown order. *Journal of Cryptology*, 19(4):463–487, 2006.
17. S. Goldwasser, S. Micali, and R. Rivest. A digital signature scheme secure against adaptive chosen message attacks. *SIAM Journal of Computing*, 17(2):281–308, 1988.
18. J. Groth. Cryptography in subgroups of $\mathbb{Z}_n^*$. In J. Kilian, editor, *Theory of Cryptography (TCC 2005)*, volume 3378 of *Leture Notes in Computer Science*, pages 50–65. Springer, 2005.
19. D. Hofheinz and E. Kiltz. Programmable hash functions and their applications. In D. Wagner, editor, *Advances in Cryptology – CRYPTO 2008*, volume 5157 of *Leture Notes in Computer Science*, pages 21–38. Springer, 2008.
20. ISO/IEC 14888-2. Information technology – Security techniques – Digital signatures with appendix – Part 2: Integer factorisation based mechanisms, April 15, 2008. 2nd edition.
21. K. Kurosawa and K. Schmidt-Samoa. New online/offline signature schemes without random oracles. In M. Yung et al., editors, *Public Key Cryptography – PKC 2006*, volume 3958 of *Leture Notes in Computer Science*, pages 330–346. Springer, 2006.
22. D. Naccache, D. M'Raïhi, S. Vaudenay, and D. Raphaeli. Can D.S.A. be improved? Complexity trade-offs with the digital signature standard. In A. De Santis, editor, *Advances in Cryptology – EUROCRYPT '94*, volume 950 of *Leture Notes in Computer Science*, pages 77–85. Springer, 1995.
23. G. Poupard and J. Stern. Security analysis of a practical "on the fly" authentication and signature generation. In K. Nyberg, editor, *Advances in Cryptology – EUROCRYPT '98*, volume 1403 of *Leture Notes in Computer Science*, pages 422–436. Springer, 1998.
24. A. Shamir and Y. Tauman. Improved online/offline signature schemes. In J. Kilian, editor, *Advances in Cryptology – CRYPTO 2001*, volume 2139 of *Leture Notes in Computer Science*, pages 355–367. Springer, 2001.
25. J. Stern, D. Pointcheval, J. Malone-Lee, and N.P. Smart. Flaws in applying proof methodologies to signature schemes. In *Advances in Cryptology – CRYPTO 2002*, volume 2442 of *Leture Notes in Computer Science*, pages 93–110. Springer, 2002.
26. P.C. van Oorschot and M. Wiener. On Diffie-Hellman key agreement with short exponents. In U. Maurer, editor, *Advances in Cryptology – EUROCRYPT '96*, volume 1070 of *Leture Notes in Computer Science*, pages 332–343. Springer, 1996.
27. S. Xu, Y. Mu, and W. Susilo. Online/offline signatures and multisignatures for AODV and DSR routing security. In L.M. Batten and R. Safavi-Naini, editors, *Information Security and Privacy (ACISP 2006)*, volume 4058 of *Leture Notes in Computer Science*, pages 99–110. Springer, 2006.
28. P. Yu and S.R. Tate. Online/offline signature schemes for devices with limited computing capabilities. In T. Malkin, editor, *Topics in Cryptology – CT-RSA 2008*, volume 4964 of *Leture Notes in Computer Science*, pages 301–317. Springer, 2008.

29. H. Zhu. New digital signature scheme attaining immunity against adaptive chosen message attack. *Chinese Journal of Electronics*, 10(4):484–486, 2001.