Towards Stronger Functional Signatures

Carlo Brunetta, Bei Liang and Aikaterini Mitrokotsa
Chalmers University of Technology, Gothenburg, Sweden

Manuscript
Abstract: Functional digital Signatures (FS) schemes introduced by Boyle, Goldwasser and Ivan (PKC 2014) provide a method to generate fine-grained digital signatures in which a master key-pair (msk, mkv) is used to generate a signing secret-key sk_f for a function f that allows to sign any message m into the message f(m) and signature σ. The verification algorithm takes the master verification-key mkv and checks that the signature σ corresponding to f(m) is valid. In this paper, we enhance the FS primitive by introducing a function public-key pk_f that acts as a commitment for the specific signing key sk_f. This public-key is used during the verification phase and guarantees that the message-signature pair is indeed the result generated by employing the specific key sk_f in the signature phase, a property not achieved by the original FS scheme. This enhanced FS scheme is defined as Strong Functional Signatures (SFS) for which we define the properties of unforgeability as well as the function hiding property. Finally, we provide an unforgeable, function hiding SFS instance in the random oracle model based on Boneh-Lynn-Shacham signature scheme (ASIACRYPT 2001) and Fiore-Gennaro’s publicly verifiable computation scheme (CCS 2012).

Keywords: Functional Signatures, Verifiable Computation, Function Privacy
1 Introduction

Digital signatures, introduced by Diffie and Hellman [DH76], is a valuable cryptographic primitive that provides important integrity guarantees, i.e., a signed message allows the receiver to verify that the message was indeed signed by the claimed signer. **Functional digital signatures** (FS), introduced by Boyle, Goldwasser and Ivan [BGI14] as a general extension of classic digital signatures [GMR88], allow generating signatures in a more fine-grained manner; thus, being very useful in multiple applications, e.g., scenarios where the delegation of signing rights has to be considered. Functional digital signatures require a **trusted authority** to hold a **master secret key**. Given a description of a function \( f \), the authority, using the master secret key, can generate a limited functional signing key \( sk_f \) associated with the function \( f \). Anyone that has access to the signing key \( sk_f \) and a message \( m \), can compute \( f(m) \) and the corresponding functional signature \( \sigma \) of \( f(m) \).

Let us employ an example related to photo-processing given by Boyle et al. [BGI14] to explain how FS works. When performing photo-processing, a digital camera is required to produce signed photos. One may want to allow photo-processing software to perform minor touch-ups of the photos, such as changing the contrast, but not allow more significant changes such as merging two photos or cropping a photo. Boyle et al. argued that FS could be used in such a setting to provide the photo-processing software with a restricted key, which enables it to sign only specific modifications of an original photo. Let us assume there are three different pictures partitioned into three areas and coloured in red, blue and yellow but in different order, as represented in Figure 31.

![Figure 31: An illustrated example of collisions from different messages and functions in a functional signature scheme.](image)

The functionality of \( f_1 \) is to exchange the colour of areas 2 and 3, while \( f_2 \) is used to exchange the colour of areas 1 and 3, and \( f_3 \) to exchange the colour of areas 1 and 2. Using the secret key \( sk_{f_1} \) to sign the photo \( \phi_1 \), we obtain the signed new photo \( y_1 \). With the restricted keys \( sk_{f_2} \) and \( sk_{f_3} \), we can obtain two signed photos with the same picture on it, namely \( y_2 \) and \( y_3 \). Using functional signatures, given \( y_1, y_2, y_3 \), the appreciator (not the one who provides the original picture) only knows they are three certified photos.

Generally, if we consider two functions \( f \) and \( g \) and two messages \( m, m' \) such that \( f(m) = g(m') = y \), then, given \( y \) and the corresponding functional signature \( \sigma \), FS cannot be used to certify that the function value \( y \) is indeed computed from the queried
function $f$ and $m$ rather than from $g$ and $m'$. The latter yields from the function privacy property of FS [BGI14], namely given $y$ and $σ$, any adversary is unable to tell which function $f$ or $g$ was used to compute the value $y$ even when given both functional signing keys $sk_f$ and $sk_g$.

What if we wish to make the appreciator classify that a signed photo $y$, is indeed the outcome of applying an “allowed” function without revealing “which” one? Our idea to allow an appreciator/verifier to distinguish between the usage of different secret keys, e.g. $sk_f$ and $sk_g$, we introduce a function public key, i.e. $pk_f$ and $pk_g$, that is just used in the verification phase. The public key $pk_f$ can be seen as a commitment for the specific and related secret key $sk_f$ allowing to distinguish between the evaluation and signatures $(f(m), σ_1)$ and $(g(m'), σ_2)$ even in the case that $f(m) = g(m')$. This “key-addition” directly affects the FS function privacy property that changes from “the verifier cannot retrieve which function was computed” to the stronger concept of “the verifier cannot retrieve which function was computed despite knowing the related public key”. We capture this idea into the enhanced definition of Strong Functional Signature (SFS), an Functional Signature (FS)-like scheme with function public keys that allows the verification of function evaluations’ signatures and guarantees the correct function evaluation while maintaining the function hidden.

Example - Computational Authorisation for Cloud Computing our SFS primitive could be used in the example previously described, as well as in more general applications related to the cloud-assisted setting which are alike to the certification authorities’ infrastructure but for function application and not only for identity authentication.

As depicted in Fig. 32, let us consider a cloud service $S$ that offers to service providers $S_i$ the possibilities to register their functionalities $f_i$ in exchange of guaranteeing function hiding and the correct authentication whenever a user $U_i$ wants to verify the authenticity and correctness of the output of such hidden functionalities. In other words, $S_i$ will register the function $f_i$, obtain $sk_{f_i}$ from $S$ and, at the same time, $S$ will publish the public key $pk_{f_i}$ with some application label, e.g. it might be published into an “Authorised” functionality list. Later on, the user $U_i$ requires $S_i$ to process their data, obtains the output $y$ with signature $σ$ and wants to verify that $y$ is indeed correctly computed by an authorised function. Therefore, $U_i$ obtains the list of authorised public keys $pk_{f_i}$ and verifies that $(y, σ)$ is valid by finding a public key $pk_{f_i}$ that pass the SFS validation algorithm. Additionally, $U_i$ is unable to infer the precise function $f$ from the public key $pk_f$ thus the cloud service $S$ guarantees to the service provider $S_i$ that the function is kept private.

Observe that the cloud service $S_i$ has the power to modify the status of the public keys, e.g. a public key $pk_y$ might be completely “revoked” by removing it from all the public key’s lists.

It is obvious that FS [BGI14, BF14, BMS16] does not have the features of checking if the outcome is resulted from the authorised functions, neither achieves this concept of “revocability”. In fact, in FS, since only $mvk$ is required to verify the validity of $(y, σ)$, it is not possible to check if a specific function was applied to output $y$, while our SFS make it possible by providing restricted public keys w.r.t. each function, which are employed in the verification process.

Moreover, in traditional FS schemes, it is indeed impossible to “revoke” a specific signing key, since the verification process would always work. However, in our introduced SFS notion, by incorporating the public keys in the verification process, we are able to revoke the signing capability for a restricted signing key thus allowing the trusted third party that owns the master key pair, to create a more fine-grained control over the generated function key pairs.
Our Results

Our results can be summarised as follows:

- we formally define the notion of SFS with unforgeability and function hiding properties;
- we provide a variation of Boneh et al.’s BLS signature scheme [BLS04] and a variation of Fiore and Gennaro’s verifiable computation scheme [FG12]. We prove that the Fiore and Gennaro’s VC scheme satisfies the Public Verifiable Computation (PVC) privacy properties;
- based on our variations, we give an instantiation in the random oracle model of an SFS scheme for the polynomial function family which is adaptively unforgeable and satisfies the function hiding property.

The starting point of our instantiation of SFS is to use the BLS signature scheme [BLS04] in combination with the Fiore-Gennaro’s publicly VC scheme [FG12] that is compatible with the algebraic structure and assumptions of the BLS signatures. We denote with BLS the variation of the BLS signature and with VC the variation of the Fiore-Gennaro’s VC scheme, that we propose. The design-trick behind our instantiation is to create a master key-pair as an algebraic one-way instance and use it as a “transposition” for the secret key of the schemes, e.g. $\text{BLS\,Setup}(\lambda) \to (\text{MSK}, \text{MPK})$ is equal to $(\beta, e(g_1, g_2)^\beta)$ for some $\beta \in \mathbb{Z}_p$ and whenever we sample a fresh secret value $\alpha \in \mathbb{Z}_p$ in order to compute the BLS and the VC keys, we just consider the new secret $\alpha + \beta$ obtained by translating $\alpha$ by $\beta$. Thus, all the evaluation/secret-keys are computed as if $\alpha + \beta$ is the randomness sampled while the verification/public-keys are published as “local keys”, e.g. we publish $\epsilon(g_1, g_2)^\alpha$ and not $\epsilon(g_1, g_2)^{\alpha + \beta}$. In this way, the two variated schemes become “entangled” thus implying a stricter relation during execution and verification.

In a nutshell, the SFS instantiation combines the two schemes such that the verifiable computation VC computes the secret function and provide the proof of correct computation while the signature scheme BLS is used to sign the result and forcedly relate it to the VC results.

Related Work

SFS are inspired by Boyle et al. [BGI14] FS construction and are closely related to Signatures of Correct Computation (SCC) proposed by Papamanthou, Shi.
and Tamassia [PST13] as well as PVC proposed by Parno et al. [PRV12] and Fiore and Gennaro [FG12].

**Functional Signatures.** This work is inspired by the notion of Functional Signatures (FS) introduced by Boyle et al. [BGI14]. They firstly proposed the formal definition of FS with unforgeability security as well as two additional desirable properties: function privacy and succinctness. Boyle et al. defined FS and gave a construction for an FS scheme, based on one-way functions and satisfying the unforgeability but not the succinctness or function privacy properties. Furthermore, they showed how to convert any FS without the function privacy or succinctness properties into an FS scheme that is succinct and function-private by using a SNARK scheme [GW11, BCCT12, BCCT13]. They also showed how to use an FS scheme to construct a delegation scheme [GGP10], i.e., non-interactive verifiable computation.

**Signatures of Correct Computation.** Papamanthou, Shi and Tamassia introduced Signatures of Correct Computation (SCC) for verifying the correctness of a computation outsourced in the cloud [PST13]. In the SCC model, an authority wishes to outsource the execution of a function $f$ to an untrusted server. It generates a pair of master keys along with a verification key $FK(f)$ for that function which will be used during verification. Note that the existence of such a verification key for a function $f$ and the requirement of being used for verification are similar to our formulation of SFS. The server can then return a signature $\sigma$ on a value $y$, which certifies that the result $y$ is indeed the correct outcome of the function $f$ evaluated on some input. In the syntax of SCC [PST13], anyone with the public verification key can verify that an untrusted server correctly computed a function $f$ on a specific input $m$. However, the verification algorithm requires the specific input $m$, used to compute $f(m)$, to be taken as input, which means that only the client or someone who knows the input $m$ can verify the correctness of the computation. Therefore, SCC would not achieve any privacy with respect to the input $m$. In contrast, our SFS allows anyone to perform the verification without knowledge of the specific input $m$.

**Publicly Verifiable Computation.** Parno et al. [PRV12] have proposed a publicly verifiable computation (PVC) in which they consider a PVC scheme achieving two desirable properties: public delegatability and public verifiability. Their definition of PVC includes a $\text{ProbGen}$ algorithm, which encodes a user’s inputs $m$ to a server’s inputs $\sigma_m$ and simultaneously prepares an element $\rho_m$ to be used for verification. Thus, $\rho_m$ can be used to publicly verify that the server returned a correct value. The public delegation property refers to the existence of a public delegation key $pk_f$ for the function $f$, i.e., the key used in the $\text{ProbGen}$ algorithm, and publicly available to anyone. Thus, anyone can use the key and delegate the computation to the cloud.

Parno et al. [PRV12] also gave a construction of a VC scheme with public delegation and public verifiability from any Attribute-Based Encryption (ABE), which is unfortunately not appropriate to be employed in order to instantiate a SFS since additional transformations are needed.

Another closely related work is the one by Fiore and Gennaro [FG12], who presented a very efficient PVC scheme tailored for multivariate polynomials over a finite field based on bilinear maps. We present a variation of their VC scheme by introducing a separate $\text{Setup}$ algorithm to generate a master key pair for the scheme so that the keys for the evaluation of different functions could be executed multiple times using the same parameters for the scheme, which allows the evaluation of multiple functions on the same instance produced by $\text{ProbGen}$.

**Paper organisation.** In Sec. 2, we describe the notations and review the primitives used in the paper. In Sec. 3, we propose two variances: one of Boneh et al.’s signature
scheme, denoted $\text{BLS}$, and one of the Fiore-Gennaro’s PVC scheme, denoted $\text{VC}$. In Sec. 4, we provide the definition of SFS and its security properties and we instantiate an unforgeable and function hiding SFS using the $\text{BLS}$ and the $\text{VC}$ schemes.

2 Preliminaries

In the following section, we define the notations used throughout the paper. We also provide the assumptions and the definitions of the building blocks that our constructions rely on.

2.1 Notations and Assumptions

In the paper, we denote with $x \leftarrow_R X$ the random uniform sampling in the set $X$, with $\lambda$ the security parameter. We denote with $v$ a vector and with $Z_p$ the ring with $p$ elements. When not specified, $p$ always represents a prime or a power of it. Let $\Pr[E]$ denote the probability that the event $E$ occurs. Let $G_1, G_2, G_T$ be groups of the same order with generators $g_1, g_2, g_T$ correspondingly and the bilinear map $\epsilon : G_1 \times G_2 \rightarrow G_T$ of type-3, i.e. there does not exist an efficient homomorphism map $\psi : G_2 \rightarrow G_1$.

**Definition 24** (co-Computation Diffie Hellman [BLS04, FG12]). Let $G_1, G_2, G_T$ be groups of prime order $p$. Let $g_1 \in G_1, g_2 \in G_2$ be generators and $\epsilon : G_1 \times G_2 \rightarrow G_T$ bilinear map of type-3, i.e. there does not exist an efficient homomorphism map $\psi : G_2 \rightarrow G_1$.

We sample uniformly at random $a, b \in_R Z_p$ and define the advantage of an adversary $A$ in solving the co-Comutational Diffie Hellman (co-CDH) problem as

$$\text{Adv}_{A}^{\text{co-CDH}}(\lambda) = \Pr\left[ A(p, g_1, g_2, g_T) = g_1^a g_T^b \right]$$

If for all adversaries $A$ it exists a negligible $\epsilon$ such that $\text{Adv}_{A}^{\text{co-CDH}}(\lambda) \leq \epsilon$, then the co-CDH Assumption $\epsilon$-holds for the groups $G_1, G_2$.

2.2 Closed Form Efficient PRFs

A closed form efficient PRF (Closed Form Efficient (CFE)-Pseudo Random Function (PRF)), defined by Fiore and Gennaro [FG12] consists of three algorithms $\text{CF.KGen}, \text{CF.H}$ and $\text{CF.Eval}$. $\text{CF.KGen}$ takes as input a security parameter $\lambda$ and outputs a secret key $K$, from the key space $K$, and some public parameters $pp$ that specify the domain $X$ and range $Y$ of the function. For a fixed secret key $K$, $\text{CF.H}_K$ takes as input a value $x \in X$ and outputs a value $y \in Y$. It satisfies the pseudo-randomness property: for every PPT adversary $A$, $(K, pp) \leftarrow \text{CF.KGen}(\lambda)$ and any random function $\xi : \lambda \rightarrow Y$:

$$\epsilon_{\text{PRF}} = \left| \Pr\left[ A^{\text{CF.H}_K}(\lambda, pp) = 1 \right] - \Pr\left[ A^{\xi}(\lambda, pp) = 1 \right] \right| \leq \text{negl}(\lambda)$$

Additionally, the scheme is required to achieve closed form efficiency: consider a generic computation $\phi$ that has as input $l$ random values $R_1, ..., R_l \in Y$ and a vector of $m$ arbitrary values $x = (x_1, ..., x_m)$. Assume that the fastest computation time that takes to compute $\phi(R_1, ..., R_l, x_1, ..., x_m)$ is $T$. Let $z = (z_1, ..., z_l)$ be a $l$-tuple of arbitrary values in the domain $X$. The CF.PRF is said to achieve closed form efficiency for $(\phi, z)$ if the algorithm CF.Eval has running time $o(T)$ and it holds

$$\text{CF.Eval}_{(\phi, z)}(K, x) = \phi(\text{CF.H}_K(z_1), ..., \text{CF.H}_K(z_l), x_1, ..., x_m)$$

Fiore and Gennaro [FG12] give constructions of closed form efficient PRFs for multivariate polynomials and matrix multiplication, based on the decision linear assumption.
2.3 Functional Signatures

Boyle et al. [BGI14] introduced functional digital signatures (FS), a cryptographic primitive that can be employed to achieve signing delegation.

Definition 25 (Functional Signature [BGI14]). A Functional Signature scheme for a message space $\mathcal{M}$ and function family $\mathcal{F} = \{ f : D_f \to \mathcal{M} \}$ consists of the PPT algorithms $FS = (FS.Setup, FS.KGen, FS.Sign, FS.Ver)$ defined as:

- $FS.Setup(\lambda) \to (\overline{\text{msk}}, \overline{\text{mvk}})$: the setup algorithm takes as input the security parameter $\lambda$ and outputs the master signing key $\overline{\text{msk}}$ and the master verification key $\overline{\text{mvk}}$.
- $FS.KGen(\overline{\text{msk}}, f) \to \overline{sk}_f$: the key generation algorithm takes as input the master signing key and a function $f \in \mathcal{F}$ and outputs a signing key $\overline{sk}_f$.
- $FS.Sign(f, \overline{sk}_f, m) \to (f(m), \overline{\sigma})$: the signing algorithm takes as input the signing key for a function $f$ and an input $m \in D_f$, and outputs $f(m)$ and a signature $\overline{\sigma}$ of $f(m)$.
- $FS.Ver(\overline{mvk}, m', \overline{\sigma}) \to \{0, 1\}$: the verification algorithm takes as input the master verification key $\overline{mvk}$, a message $m'$ and a signature $\overline{\sigma}$, and outputs $1$ if the signature is valid.

The definition requires the following conditions to hold:

Correctness a Functional Signature (FS) scheme is correct if for all functions $f \in \mathcal{F}$, messages $m \in D_f$, $(\overline{\text{msk}}, \overline{\text{mvk}})$ obtained from $FS.Setup(\lambda)$, $\overline{sk}_f$ obtained from $FS.KGen(\overline{\text{msk}}, f)$ and $(m', \overline{\sigma})$ obtained from $FS.Sign(f, \overline{sk}_f, m)$, it holds that $FS.Ver(\overline{mvk}, m', \overline{\sigma}) = 1$.

Succinctness there exists a polynomial $s(.)$ such that for every $\lambda \in \mathbb{N}$, function $f \in \mathcal{F}$, message $m \in D_f$, master keys $(\overline{\text{msk}}, \overline{\text{mvk}}) \leftarrow FS.Setup(\lambda)$, function key $\overline{sk}_f$ obtained from $FS.KGen(\overline{\text{msk}}, f)$, and $(f(m), \overline{\sigma}) \leftarrow FS.Sign(\overline{sk}_f, m)$, it holds with probability 1 that $|\overline{\sigma}| \leq s(\lambda, |f(m)|)$.

Unforgeability FS is unforgeable if the probability of any PPT algorithm $A$ in the FS unforgeability experiment $\text{Exp}_{FS}^{FS} \text{UNF}(A)$, depicted in Figure 33, to output 1 is negligible. Namely,

$$\text{Adv}_{A,FS}^{FS \text{UNF}}(\lambda) = \text{Pr}[\text{Exp}_{FS}^{FS \text{UNF}}(A) = 1] \leq \text{negl}(\lambda)$$

Function privacy FS is function private if the advantage of any PPT algorithm $A$ in the FS function privacy experiment $\text{Exp}_{FS}^{FS \text{FP}}(A)$, depicted in Figure 33 is negligible. Namely,

$$\text{Adv}_{A,FS}^{FS \text{FP}}(\lambda) = \text{Pr}[\text{Exp}_{FS}^{FS \text{FP}}(A) = 1] - \frac{1}{2} \leq \text{negl}(\lambda)$$

2.4 The BLS Signature Scheme

In this section, we will report the Boneh et al.’s signature scheme [BLS04].

Let $(p, g_1, g_2, \xi_1, \xi_2, \xi_T, e)$ where $e : \xi_1 \times \xi_2 \to \xi_T$ is a bilinear map in the security parameter $\lambda$. Let $H : \{0,1\}^* \to \xi_1$ be a full-domain hash function. The BLS signature scheme [BLS04] with the message space $\mathcal{M} = \{0,1\}^*$ comprises of the following three algorithms:

- $BLS.KGen(\lambda) \to (PK, SK)$: given a security parameter $\lambda$, sample a secret value $SK \leftarrow \mathbb{Z}_p$ and compute as the public key $PK = g_2^SK$. 

We describe the definition of a scheme that allows a client to delegate the computation of a function to a server so that the client is able to verify the correctness of the result returned by the server with less computation cost than evaluating the function directly.

### 2.5 Verifiable Computation

A verifiable computation (VC) scheme allows a client to delegate the computation of a function to a server so that the client is able to verify the correctness of the result returned by the server with less computation cost than evaluating the function directly. We describe the definition of a verifiable computation (VC) scheme introduced by Parno et al. [PRV12] and Fiore and Gennaro [FG12].

**Definition 26** (Verifiable Computation [PRV12, FG12]). A verifiable computation scheme VC is defined by the following algorithms:

- **VC.KGen(λ, f)** → (śk_f, ĭk_f, ĭk_f): the key generation algorithm takes as input a security parameter λ and the description of a function f, and outputs a secret key śk_f that will be used for input delegation, a corresponding verification key ĭk_f, and an evaluation key ĭk_f, which will be used for the evaluation of f.

- **VC.ProbGen(śk_f, m)** → (˜σ_m, ˜ρ_m): the problem generation algorithm uses the secret key śk_f to encode the function input m as an encoded value ˜σ_m and a corresponding decoding value ˜ρ_m.
VC.Compute(ek_f, σ_m) → σ_y : the computing algorithm takes as input the evaluation key ek_f and the encoded input σ_m, and outputs σ_y, an encoded version of the function’s output y = f(m).

VC.Ver(νk_f, ˜ρ_m, ˜σ_y) → y or ⊥ : the verification algorithm takes as input the verification key νk_f, the decoding value ˜ρ_m and the encoded output ˜σ_y. The algorithm outputs y if and only if y = f(m) is correctly computed. Otherwise ⊥ is the output.

A publicly verifiable computation scheme is a VC scheme with an additional property that the verification key νk_f is published publicly such that anyone can check the correctness of a performed computation.

Remark 10. The original VC [FG12] is with “secret-key” nature. In the earlier definition, KGen produces a secret key that was used as an input to ProbGen and, in turn, ProbGen produces a secret verification value needed for Ver. Later, Parno et al. [PRV12] introduced the “public-key” VC definition which has both the public delegation and public verification properties. The delegation being public or private depends on whether the evaluation key sk is published or kept secret. In our case, we consider the scenario where the Public Verifiable Computation (PVC) scheme is publicly verifiable but privately delegatable, i.e., the evaluation key ek_f is secret while the verification key νk_f is public. In the paper, we abuse terminology and refer to a PVC scheme when discussing about a Verifiable Computation (VC) scheme.

Correctness a verifiable computation scheme VC is correct for a class of functions F if for any f ∈ F, for any tuple of keys (sk_f, νk_f, ek_f) ← VC.KGen(λ, f), for any m ∈ D_f, for any (σ_m, ˜ρ_m) ← VC.ProbGen(ek_f, m) and any computed ˜σ_y obtained from VC.Compute(ek_f, σ_m), it holds that VC.Ver(νk_f, ˜ρ_m, ˜σ_y) = y = f(m).

Security a VC scheme is secure w.r.t. a static attacker if the probability of any PPT algorithm A in the VC static security experiment Exp_VC^VC StaticVer(A) of Figure 34, to output 1 is negligible. Namely,

\[ \text{Adv}_{A, VC}^{VC StaticVer}(λ) = \Pr[\text{Exp}_{VC}^{VC StaticVer}(A) = 1] \leq \text{negl}(\lambda) \]

Privacy [FGP14] a VC scheme is said to be private w.r.t. a static attacker if the advantage of any PPT algorithm A winning in the VC privacy experiment Exp_VC^VC Priv(A) of Figure 34 is negligible. Namely,

\[ \text{Adv}_{A, VC}^{VC Priv}(λ) = \Pr[\text{Exp}_{VC}^{VC Priv}(A) = 1] - \frac{1}{2} \leq \text{negl}(\lambda) \]

2.6 Fiore-Gennaro’s PVC Scheme

Fiore and Gennaro [FG12] propose a publicly VC scheme for the function family F containing all multivariate polynomials f(x_1, ..., x_m) with coefficients in Z_p for some prime p, m variables and degree at most d in each variable. Let h : Z^m_p → Z^d_p which expands the input x to the vector (h_1(x), ..., h_l(x)) of all the monomials as follows: for all j ∈ [1, ..., l] where l = (d + 1)m, write j = (i_1, ..., i_m) with i_k ∈ [0, ..., d_l], then h_j(x) = x_1^{i_1} · · · x_m^{i_m}. Thus, by using this notation, it is possible to write the polynomial as f(x) = (f, h(x)) = l \sum_{j=1}^{l} f_j · h_j(x) where the f_j’s are its coefficients and f_j ∈ Z_p. The construction works over the groups G_1, G_2, G_T of the same prime order p, equipped with a bilinear map e : G_1 × G_2 → G_T. Let us define Poly(R, x) = \prod_{j=1}^{l} R_f_j(x) where R is a random l-dimensional vector of G_1.
classification algorithm while the accordingly modified security games reduce to the ones.

Fiore-Gennaro’s public verifiable computation scheme \[3\] Construction Blocks: Variated Schemes

In a nutshell, the variations add to the schemes a privacy

\[
\begin{cases}
\text{Exp}_{\text{VC, Static Ver}}(A) \\
\end{cases}
\]

\[
\begin{array}{l}
f \leftarrow A (1^n) \\
(\bar{\sigma}_f, \bar{\nu}_f, \bar{e}_f) \leftarrow \text{VC.KGen}(\lambda, f) \\
(\bar{\sigma}_0, \bar{\nu}_0) = (0, 0) \\
\text{for } i \in \{1, \ldots, t = \text{poly}(\lambda)\} \text{ do} \\
m_i \leftarrow A \left( \bar{\sigma}_f, \bar{\nu}_f, \ldots, \bar{\nu}_{i-1} \right) \\
(\bar{x}_i, \bar{y}_i) \leftarrow \text{VC.ProbGen}(\bar{\sigma}_f, m_i) \\
m^* \leftarrow A \left( \bar{\sigma}_f, \bar{\nu}_1, \ldots, \bar{\nu}_t \right) \\
(\bar{\sigma}, \bar{\nu}) \leftarrow \text{VC.ProbGen}(\bar{\sigma}_f, m^*) \\
\tilde{y}^* \leftarrow A(\bar{\nu}_f, \bar{\nu}, \tilde{y}^*) \\
\text{if } (\tilde{y}^* \neq \bot) \land (\tilde{y}^* \neq f(m^*)) \\
\text{then return 1} \\
\text{else return 0} 
\end{array}
\]

\[
\begin{cases}
\text{Exp}_{\text{VC, Priv}}(A) \\
\end{cases}
\]

\[
\begin{array}{l}
(f_0, f_1, m_0, m_1) \leftarrow A (1^n) \\
\text{if } f_0(m_0) \neq f_1(m_1) \text{ then return } \bot \\
b \leftarrow \{0, 1\} \\
(\bar{\sigma}_f, \bar{\nu}_f, \bar{e}_f) \leftarrow \text{VC.KGen}(\lambda, f) \\
(\bar{\sigma}_0, \bar{\nu}_0) \leftarrow \text{VC.ProbGen}(\bar{\nu}_f, m_0) \\
\tilde{b} \leftarrow A(\bar{\nu}_f, \bar{\nu}_0, \tilde{b}, f_0, f_1, m_0) \\
\text{if } \tilde{b} = b \text{ then return 1} \\
\text{else return 0} 
\end{array}
\]

Figure 34: VC static security and privacy experiments.

Let CF = (CF.KGen, CF.H, CF.Eval) be a CFE PRF defined in Section 2.2. Fiore-Gennaro’s public verifiable computation scheme \[FG12\] VC is constructed as the follows:

- \(\text{VC.KGen}(\lambda, f) \rightarrow (\tilde{\sigma}_f, \tilde{\nu}_f, \tilde{e}_f)\): Generate the description of a bilinear group \(\langle p, g_1, g_2, G_1, G_2, e \rangle\) in the security parameter \(\lambda\), a key of a PRF \(K\) with range in \(G_1\) as \(K \leftarrow \text{CF.KGen}(\lambda, \log d, m)\). Randomly sample \(a \leftarrow R_p\) and, for all the indices \(i \in \{0, 1, \ldots, l\}\), compute \(W_i = g_1^{a_i} \cdot \text{CF.H}_e(i)\) and define \(W\) as \((W_0, \ldots, W_l) \in G_1^l\). Output the key tuple \((\tilde{\sigma}_f, \tilde{\nu}_f, \tilde{e}_f)\) as the values \((K, e(g_1, g_2)^a, (f, W))\).

- \(\text{VC.ProbGen}(\tilde{\sigma}_f, m) \rightarrow (\tilde{\sigma}_m, \tilde{\nu}_m)\): Output the tuple \((\tilde{\sigma}_m, \tilde{\nu}_m)\) where \(\tilde{\sigma}_m = m\) and \(\tilde{\nu}_m = e(CF.Eval_pg_e(\tilde{K}, h(m))), g_2)\).

- \(\text{VC.Compute}(\tilde{\nu}_f, \tilde{\nu}_m) \rightarrow \tilde{\nu}_y\): Compute \(y\) by evaluating \(f(m) = \sum_{i=1}^l f_i h_i(m)\) and \(V = \prod_{i=1}^l W_i^{h_i(m)}\). Output \(\tilde{\nu}_y = (y, V)\).

- \(\text{VC.Ver}(\tilde{\nu}_f, \tilde{\nu}_m, \tilde{\nu}_y) \rightarrow \{y, \bot\}\): Output \(y\) if it holds that \(e(V, g_2) = \tilde{\nu}_y \cdot \tilde{\nu}_m\). Otherwise output \(\bot\).

Fiore and Gennaro \[FG12\] proved that the construction is secure if the co-CDH assumption holds and CF.PRF is a close form efficient PRF. In Lemma 3, we prove that Fiore-Gennaro PVC scheme satisfies privacy as defined in the experiment depicted in Figure 34.

3 Construction Blocks: Variated Schemes

In this section, we provide our variations of the Boneh-Lynn-Shacham signature scheme \[BLS04\] and Fiore-Gennaro publicly verifiable computation scheme \[FG12\].

In a nutshell, the variations add to the schemes a “setup algorithm” that outputs a master key-pair used in the original key-generation algorithm and in the final verification algorithm while the accordingly modified security games reduce to the ones.
of the original schemes. The final purpose of these modifications is to later allowing
the instantiation of both the two schemes with a single common master key-pair in a
stronger security setting, where the master secret-key is kept secure as in the act of
"merging" the schemes into a single one. Intuitively, with the shared schemes’ master
public-key, the final verification algorithm will compute the two schemes’ verification
algorithms independently and will verify that the schemes are indeed "merged" into a
single one.

3.1 A variation of the BLS signature

We introduce, in the BLS signature scheme, a Setup algorithm that outputs a master
key-pair (MPK, MSK) used in the KeyGen algorithm to produce a local signing key in
order to generate a signature for a message together with a local verification key. The
Verify algorithm will take both the master public key and the local verification key to
check the validity of a message-signature pair. We provide the unforgeability game for
our BLS variation in Figure 35 and prove the unforgeability of it in the random oracle
model.

Definition 27 (BLS Variation). Let \((p, g_1, G_1, \ldots, G_r, e)\) where \(e : G_1 \times G_2 \rightarrow G_r\) is
a bilinear map in the security parameter \(\lambda\). Let \(H : \{0, 1\}^* \rightarrow G_1\) be a full-domain hash
function and \(F : K \times \{0, 1\}^* \rightarrow Z_p\) a PRF. Let the additional information \(\alpha \in Z_p\) be
a field element known just to the signer. Our variation \(BLS\) scheme is defined as the
algorithms:

- \(BLS.\text{Setup}(\lambda) \rightarrow (MPK, MSK)\): sample \(\beta \leftarrow Z_p\) and set \(MSK = \beta\). Compute
  \(MPK = e(g_1, g_2)^\beta\) and output \((MPK, MSK) \in G_r \times Z_p\).

- \(BLS.\text{KGen}(MSK, \alpha) \rightarrow (PK, SK)\): given \(MSK \in Z_p\) and \(\alpha \in Z_p\),
  sample \(k \leftarrow Z_p\), \(r \in Z_p\) and compute secret key as \(SK = (SK_1, SK_2) = (g_1^{MSK + \alpha + r}, k)\)
  and the public
  key as \(PK = (PK_1, PK_2) = (e(g_1, g_2)^{\alpha + r}, g_2^{SK_2})\).

- \(BLS.\text{Sign}(SK, m) \rightarrow \sigma\): given a secret key \(SK = (SK_1, SK_2)\) and a message \(m \in M\),
  compute and output the signature \(\sigma = SK_1 \cdot H(m)^{SK_2}\).

- \(BLS.\text{Ver}(MPK, PK, m, \sigma) \rightarrow \{0, 1\}\): given a public key \(PK = (PK_1, PK_2)\), a message
  \(m\), a signature \(\sigma\) and an environmental public key \(MPK\), verify and output the result
  of the check \(e(\sigma, g_2) = MPK \cdot PK_1 \cdot e(H(m), PK_2)\).

![Figure 35: BLS and BLS unforgable experiments.](image)

We present in Fig. 35 a modified unforgeability experiment for the BLS scheme
which, differently from the BLS standard unforgeability experiment, must consider the
generation of the master key pair and the value $\alpha^*$. We prove that, despite the modification, unforgeability is preserved.

**Proposition 8.** If the advantage for all PPT adversaries $B$ for the unforgeability experiment $\text{Exp}^{BLS\text{-UNF}}(B)$ is negligible, then all the PPT adversaries $A$ for the experiment $\text{Exp}^{\text{BLS\text{-UNF}}}_{\mathcal{A}}(A)$ have a negligible advantage. Formally:

$$\text{Adv}^{\text{BLS\text{-UNF}}}_{\mathcal{A},\mathcal{B}}(\lambda) \leq \text{Adv}^{BLS\text{-UNF}}(\lambda) \leq \text{negl}(\lambda)$$

**Proof.** Assume that there exists a PPT adversary $A$ for the experiment $\text{Exp}^{\text{BLS\text{-UNF}}}(\lambda)$ with non-negligible advantage $\Delta$. The oracles $O_{\text{BLS\text{-Sign}}}(\lambda)$ and $O_{\text{BLS\text{-Sign}}}(\lambda)$ are to respond with the signatures on the messages $m$ submitted to each challenger and then keep a track of the message-signature pair in its queried set $\mathcal{L}_\Delta$. Now we construct an adversary $\mathcal{R}$, running $A$ as a subroutine, which attacks the underlying BLS scheme. Receiving from the challenger the public key $\mathcal{PK}_\star$, $\mathcal{R}$ sets it to be $\mathcal{PK}_\star$. $\mathcal{R}$ runs $\mathcal{BLS\text{-Setup}}(\lambda) \rightarrow (\mathcal{MPK}, \mathcal{MSK})$. It then outputs $\mathcal{MPK}$ to $A$. $A$ will reply with $\xi$ and $\alpha$. $\mathcal{R}$ fixes $\mathcal{SK}_1 = g_1^{\mathcal{MSK} + \alpha} \cdot e(\mathcal{MPK}, \mathcal{PK}_\star)$ and computes $\mathcal{PK}_1 = e(g_1^{\mathcal{MSK} + \alpha}, g_2)$ and outputs $\mathcal{PK} = (\mathcal{PK}_1, \mathcal{PK}_\star)$ to $A$. After the key generation phase, for every signing query $O_{\text{BLS\text{-Sign}}}(\lambda)$ from $A$, the reduction $\mathcal{R}$ queries $\mathcal{B}$’s oracle with $O_{\text{BLS\text{-Sign}}}(\lambda)$ and obtains $\sigma$. For any hash query $O_h(m)$ from $A$, $\mathcal{R}$ queries $\mathcal{B}$’s hash oracle with $O_h(m)$ and obtains $H(m)$. $\mathcal{R}$ computes $\tilde{\sigma} = \mathcal{SK}_1 \cdot \sigma$, and returns it to $A$. When $A$ outputs the forgery $(m^\star, \tilde{\sigma}^\star)$, the reduction $\mathcal{R}$ outputs $(m^\star, \tilde{\sigma}^\star, g_1^{\mathcal{MSK} - \alpha})$. It is direct to check that $\mathcal{R}$ output is a correct forgery for the BLS signature scheme since:

$$\text{BLS\text{-Ver}}(\mathcal{PK}_\star, m^\star, \tilde{\sigma}^\star, g_1^{\mathcal{MSK} - \alpha}) \Leftrightarrow e(\tilde{\sigma}^\star, g_1^{\mathcal{MSK} - \alpha}, g_2) = e(H(m^\star), \mathcal{PK}_\star)$$

$$\Leftrightarrow e(\tilde{\sigma}^\star, g_1^\mathcal{MSK} - \alpha) = e(g_1, g_2)^{\alpha + \mathcal{MSK} + \alpha} \cdot e(H(m^\star), \mathcal{PK}_\star)$$

$$\Leftrightarrow e(\tilde{\sigma}^\star, g_1^\mathcal{MSK} - \alpha) = \mathcal{MPK} \cdot \mathcal{PK}_1 \cdot e(H(m^\star), \mathcal{PK}_\star)$$

$$\Leftrightarrow \text{BLS\text{-Ver}}(\mathcal{MPK}, \mathcal{PK}, m^\star, \tilde{\sigma}^\star)$$

therefore $\Delta = \text{Adv}^{\text{BLS\text{-UNF}}}_{\mathcal{A},\mathcal{B}}(\lambda) \leq \text{Adv}^{\text{BLS\text{-UNF}}}(\lambda)$ which is a contradiction. \qed

### 3.2 A variation of Fiore-Gennaro’s PVC

In our PVC variation, we introduce a *master key-pair* $(\mathcal{mk}, \mathcal{mpk})$ that is generated in the *Setup* phase and set as $(\beta, e(g_1, g_2)^\beta)$, which adds additional randomness to the evaluation key of function $f$ such that $W_i$ in Fiore-Gennaro’s PVC is rerandomized to $W_i^\beta$. By forcing the master secret-key to be zero, i.e. $\beta = 0$, we obtain the original Fiore-Gennaro’s scheme.

**Definition 28** (Fiore-Gennaro PVC Variation). Let $pp$ be the description of a bilinear group $(p, g_1, g_2, \mathcal{G}_1, \mathcal{G}_2, \mathcal{G}_T, e)$ in the security parameter $\lambda$. Our publicly verifiable computation scheme $\mathcal{VC}$ is defined by the following algorithms:

- **$\mathcal{VC\text{-Setup}}(\lambda) \rightarrow (\mathcal{mk}, \mathcal{mpk})$** : the setup algorithm randomly sample $\beta \leftarrow \mathcal{R}_p$ and outputs $(\mathcal{mk}, \mathcal{mpk}) = (\beta, e(g_1, g_2)^\beta)$.

- **$\mathcal{VC\text{-KGen}}(\lambda, \mathcal{mk}, f) \rightarrow (\mathcal{sk}_f, \mathcal{vk}_f, \mathcal{ek}_f)$** : let $\mathcal{mk} = \beta$. The algorithm samples $\alpha \leftarrow \mathcal{R}_p$ and generates a PRF key $K \leftarrow \mathcal{CF\text{-KGen}}(\lambda, \lceil \log d \rceil, m)$ with range in $\mathcal{G}_1$. For all $i \in \{1, \ldots, l\}$, it computes $W_i = g_1^{\alpha + \beta} \cdot \mathcal{CF\text{-H}}(i)$ and let $W$ be defined as $(W_1, \ldots, W_l) \in \mathcal{G}_1$. It outputs $(\mathcal{sk}_f, \mathcal{vk}_f, \mathcal{ek}_f)$ as $((\alpha, g_2^\mathcal{MSK}), e(g_1, g_2)^\alpha, (f, W))$. 

and, negligible advantage, then all the PPT adversaries Fiore-Gennaro role of building a bridge between

3. CONSTRUCTION BLOCKS: VARIATED SCHEMES

We describe the security and privacy experiments in Fig. 36.

Figure 36: The static security and privacy experiments for \( \overline{VC} \) scheme. In \( \square \) are highlighted the variations introduced in the \( \overline{VC} \) experiments in comparison to the original Fiore-Gennaro \( VC \) scheme.

Proposition 9. If all PPT adversaries \( B \) for the experiment \( Exp_{\overline{VC}}^{VC:\text{StaticVar}}(B) \) have a negligible advantage, then all the PPT adversaries \( A \) for the experiment \( Exp_{\overline{VC}}^{VC:\text{StaticVar}}(A) \) have a negligible advantage. Formally:

\[
\text{Adv}_{\overline{VC}}^{VC:\text{StaticVar}}(\lambda) \leq \text{Adv}_{\overline{B}}^{VC:\text{StaticVar}}(\lambda) \leq \text{negl}(\lambda)
\]

and, mutatis mutandis, it holds:

\[
\text{Adv}_{\overline{VC}}^{VC:\text{Priv}}(\lambda) \leq \text{Adv}_{\overline{VC}}^{VC:\text{Priv}}(\lambda)
\]
Proof. let us assume by contradiction that there exists a PPT adversary $A$ for the experiment $\text{Exp}_{\text{VC}}^{\text{StaticVer}}(A)$ with non-negligible advantage $\Delta$. We build an adversary $\mathcal{R}$, running $A$ as a subroutine, which attacks the security of the underlying VC scheme. $\mathcal{R}$ runs $\text{VC.Setup}(\lambda) \rightarrow (\text{mpk}, \text{msk})$ and then outputs $\text{mpk}$ to $A$ that will reply with the challenging function $f$. The reduction $\mathcal{R}$ just forwards it to the challenger of VC scheme and obtains $(\tilde{\text{vk}}_f, \tilde{ek}_f)$ where $\tilde{ek}_f = (f, W_i)$. $\mathcal{R}$ modifies $W_i$ into $W$ by computing, for all $i \in \{1, \ldots, l\}$, the new values $W_i = W_i \cdot g_1^{\text{mak}_i}$. It then returns $(\tilde{\text{vk}}_f, (f, W))$ to $A$. All the ProbGen queries from $A$ are just forwarded to the challenge of VC scheme and are responded with the same response from VC challenger. When the adversary $A$ outputs the forgery $(t^*, \tilde{\sigma}^*)$ where $\tilde{\sigma}^* = (y^*, V^*)$, the reduction $\mathcal{R}$ and outputs $(i^*, (y^*, V^* \cdot g_1^{-\text{mak}_i}))$. It is straightforward to check that $\mathcal{R}$ output is a correct tamper for the VC scheme since:

$$\text{VC.Ver}(\tilde{\text{vk}}_f, \tilde{\rho}_i \cdot (y^*, V^* \cdot g_1^{-\text{mak}_i})) \iff$$

$$e(V^*, g_2) e(g_1, g_2)^{-\text{mak}_i} = \tilde{\text{vk}}_f \cdot \tilde{\rho}_i \iff$$

$$e(V^*, g_2) = (g_1, g_2)^{\text{mak}_i} \cdot \tilde{\text{vk}}_f \cdot \tilde{\rho}_i \iff$$

$$e(V^*, g_2) = (\text{mpk}, \tilde{\text{vk}}_f)^y \cdot \tilde{\rho}_i \iff$$

$$\text{VC.Ver}(\text{mpk}, \tilde{\text{vk}}_f, \tilde{\rho}_i, \tilde{\sigma}^*)$$

therefore $\Delta = \text{Adv}_{A,\text{VC}}^{\text{StaticVer}}(\lambda) \leq \text{Adv}_{A,\text{VC}}^{\text{StaticVer}}(\lambda) \leq \text{negl}$ which is a contradiction. Similarly, it is easy to define a reduction $\mathcal{R}$ for an adversary $A$ for the VC privacy experiments such that $\text{Adv}_{A,\text{VC}}^{\text{Priv}}(\lambda) \leq \text{Adv}_{A,\text{VC}}^{\text{Priv}}(\lambda)$. 

We complement Fiore-Gennaro’s results by providing the proof that their original VC scheme is indeed private, since this is needed to prove the function hiding property of the SFS construction.

Lemma 3. If CF.PRF is a close form efficient PRF, then the Fiore-Gennaro PVC scheme is private.

Proof. in order to prove the privacy of the Fiore-Gennaro scheme, we define a sequence of games that has the random bit $b$ as input.

- **Game$_1$(b, $A$):** the experiment $\text{Exp}_{\text{VC}}^{\text{Priv}}(A)$ is executed by using the original Fiore-Gennaro scheme;

- **Game$_2$(b, $A$):** in this game, the $\tilde{\rho}_{m_b}$ value is computed as

$$\tilde{\rho}_{m_b} = e\left(\prod_{i=1}^{l} \text{CF.H}_K(i)^{h_i(m_b)}, g_2\right)$$

- **Game$_3$(b, $A$):** we exchange all the PRF evaluations $\text{CF.H}_K(i)$ with random elements $R_i$;

- **Game$_4$(b, $A$):** we split the definition of $W$ into a left and a right component $W = \{(W_{L_i}, W_{R_i})\}_{i=1}^{l}$ and we substitute $W_i$ with $W_{L_i} \cdot W_{R_i}$;

- **Game$_5$(b, $A$):** after the challenge, we compute $y$ which is equal to $f_b(m_b) = f_1(m_b)$, define $W_L = g_2^y$ and then substitute $W$ with just the right component $W = \{W_{R_i}\}_{i=1}^{l}$. The game computes $V$ as $W_L \cdot \prod_{i=1}^{l} R_i^{h_i(m_b)}$.
We highlight the difference between the games in Figure 37 in which we describe the challenger computations made after the challenger bit b sampling and before the bit b’ guess. For compactness, we refer to CF.H_κ with just H_κ and the notation {·}, where the index i is contained in the set {1, ..., l}.

<table>
<thead>
<tr>
<th>Game_1(b)</th>
<th>Game_2(b)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1: ( (K, e(g_1, g_2)^\alpha, (f_b, {g_1^{\alpha B_i} H_\kappa(i)})_i) )</td>
<td>1: ( (K, e(g_1, g_2)^\alpha, (f_b, {g_1^{\alpha B_i} H_\kappa(i)})_i) )</td>
</tr>
<tr>
<td>2: ( (m_b, e(\text{CF.Eval}_{poly}(K, h(m_b)), g_2)) )</td>
<td>2: ( (m_b, e(\prod_{i=1}^l H_\kappa(i)^{B_i(m_b)}, g_2)) )</td>
</tr>
<tr>
<td>3: ( y, \prod_{i=1}^l W_{h_i}(m_b) )</td>
<td>3: ( y, \prod_{i=1}^l W_{h_i}(m_b) )</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Game_3(b)</th>
<th>Game_4(b)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1: ( y = f_1(m_1) )</td>
<td>1: ( y = f_0(m_0) )</td>
</tr>
<tr>
<td>2: ( (e(g_1, g_2)^\alpha, (f_b, {g_1^{\alpha B_i} R_i})_i) )</td>
<td>2: ( (e(g_1, g_2)^\alpha, (f_b, {g_1^{\alpha B_i} R_i})_i) )</td>
</tr>
<tr>
<td>3: ( m_1, e(\prod_{i=1}^l R_{h_1(m_1)}, g_2) )</td>
<td>3: ( m_0, e(\prod_{i=1}^l R_{h_1(m_0)}, g_2) )</td>
</tr>
<tr>
<td>4: ( y, g_1^{\alpha y} \prod_{i=1}^l R_{h_1(m_1)} )</td>
<td>4: ( y, g_1^{\alpha y} \prod_{i=1}^l R_{h_1(m_0)} )</td>
</tr>
</tbody>
</table>

Figure 37: The games used for proving the privacy of Fiore-Gennaro PVC scheme.

**Claim 1.** \( Pr[\text{Game}_1(b, A) = 1] = Pr[\text{Game}_2(b, A) = 1] \)

**Proof.** The only difference is on “how to evaluate” the CF.Eval_{poly} and by its correctness, the two are equivalent. \( \square \)

**Claim 2.** \( |Pr[\text{Game}_2(b, A) = 1] - Pr[\text{Game}_3(b, A) = 1]| \leq \epsilon_{PRF} \)

**Proof.** The difference between the games is that we replace the evaluation of the PRF with random elements. It is easy to see that an adversary A able to distinguish between the two games with non-negligible advantage can be used to define an adversary B able to distinguish the security of the CF.PR.F with non-negligible advantage. \( \square \)

**Claim 3.** \( Pr[\text{Game}_4(b, A) = 1] = Pr[\text{Game}_1(b, A) = 1] \)

**Proof.** The two games are equivalent since there is no difference between the two distributions. \( \square \)

**Claim 4.** \( Pr[\text{Game}_2(b, A) = 1] = Pr[\text{Game}_5(b, A) = 1] \)
Proof. The difference between the two games is merely a computational optimisation since \( \prod_{i=1}^{l} (g_i^{\alpha h_i} m_i) = g_i^{\alpha y} \) where \( y = f_0(m_0) = f_1(m_1) \). Thus, there is no difference between the two games distributions.

Claim 5. \( \Pr[\text{Game}_5(1, A) = 1] = \Pr[\text{Game}_5(0, A) = 1] \)

Proof. in order to prove the equality between the two probabilities, it is important to observe that, since the exponents \( h_i(m_0) \) and \( h_i(m_1 - b) \) are fixed, the probability is measured on the random values \( R_i \) and \( R_i' \). Fixed \( R_i \), dually \( R_i' \), there exists random values \( R_i' \) such that the product \( \prod_{i=1}^{l} R_i h_i(m_0) \) is equal to \( \prod_{i=1}^{l} R_i' h_i(m_1 - b) \). Thus, by duality, the probabilities are the same.

Therefore, the advantage is

\[
\text{Adv}_{A:\text{VC}}^{\text{StaticVer}}(\lambda) = \\
= |\Pr[\text{Game}_1(1, A) = 1] − \Pr[\text{Game}_1(0, A) = 1]| \\
\leq 2 \cdot \sum_{i=1}^{l} |\Pr[\text{Game}_i(1, A) = 1] − \Pr[\text{Game}_i+1(1, A) = 1]| + \\
+ |\Pr[\text{Game}_5(1, A) = 1] − \Pr[\text{Game}_5(0, A) = 1]| \\
\leq 2 \cdot \epsilon_{\text{PRF}}
\]

4 Strong Functional Signatures

In this section, we define the Strong Functional Signature (SFS) primitive and the related unforgeability and function hiding experiments. We provide a specific SFS instantiation using the variated schemes introduced in Sec. 3 and prove it achieves unforgeability and function hiding.

4.1 SFS Definition

Our definition of an SFS scheme can be seen as a combination of a PVC and a FS scheme: similar to FS, an SFS scheme achieves delegation of the signing capability w.r.t. the master key-pair and it also allows the verification of the correct computation of the signing function \( f \) through an additional function public key \( \text{pk}_f \), as a PVC scheme.

Definition 29 (Strong Functional Signature). A Strong Functional Signature (SFS) scheme for a message space \( \mathcal{M} \) and function family \( \mathcal{F} \) consists of the PPT algorithms \( \text{SFS} = (\text{SFS.Setup}, \text{SFS.KGen}, \text{SFS.Sign}, \text{SFS.Ver}) \) defined as:

- \( \text{SFS.Setup}(\lambda) \rightarrow (\text{msk}, \text{mvk}) \): the setup algorithm takes as input the security parameter \( \lambda \) and outputs the master signing key and the master verification key.

- \( \text{SFS.KGen}(\text{msk}, f) \rightarrow (\text{pk}_f, \text{sk}_f) \): the key generation algorithm takes as input the master signing key and a function \( f \in \mathcal{F} \) and outputs a secret signing key \( \text{sk}_f \) and a public verification key \( \text{pk}_f \) w.r.t. the function \( f \).

- \( \text{SFS.Sign}(\text{sk}_f, m) \rightarrow (y, \sigma) \): the signing algorithm takes as input the secret signing key for a function \( f \in \mathcal{F} \) and a message in the function domain \( m \in \mathcal{D}_f \), and outputs a value \( y = f(m) \) and a signature of \( f(m) \).
• \( \text{SFS.Ver} (\text{mk}, pk_f, y', \sigma) \rightarrow \{0,1\} \): the verification algorithm takes as input the master verification key \( \text{mk} \), the public verification key \( pk_f \) for the function \( f \), a message \( y' \) and a signature \( \sigma \), and outputs 1 if the signature is valid and a correct computation of \( f \), 0 if it is not a correct computation of \( f \) or the signature is not valid.

We require the following conditions to hold:

**Correctness** for any function \( f \in \mathcal{F} \), for any message \( m \in \mathcal{D}_f \), master keys \( (\text{mk}, \text{mk}) \leftarrow \text{SFS.Setup}(\lambda) \), function keys \( (pk_f, sk_f) \leftarrow \text{SFS.KGen}(\text{mk}, f) \), and \( (y, \sigma) \) obtained from \( \text{SFS.Sign}(sk_f, m) \), it holds that \( \text{SFS.Ver} (\text{mk}, pk_f, y, \sigma) = 1 \).

**Succinctness** there exists a polynomial \( s(\cdot) \) such that for every \( \lambda \in \mathbb{N} \), function \( f \in \mathcal{F} \), message \( m \in \mathcal{D}_f \), master keys \( (\text{mk}, \text{mk}) \leftarrow \text{SFS.Setup}(\lambda) \), function keys \( (pk_f, sk_f) \) obtained from \( \text{SFS.KGen}(\text{mk}, f) \), and \( (f(m), \sigma) \leftarrow \text{SFS.Sign}(sk_f, m) \), it holds with probability \( 1 \) that \( |\sigma| \leq s(\lambda, |f(m)|) \).

![Figure 38: SFS unforgeability and function hiding experiments.](image)

**Unforgeability** an SFS scheme is said to be unforgeable if the probability of any PPT algorithm \( \mathcal{A} \) in the SFS unforgeability experiment \( \text{Exp}_{\text{SFS}}^{\text{SFS.UNF}} (\mathcal{A}) \) depicted in Fig. 38 to output 1 is negligible. Namely,

\[
\text{Adv}_{\mathcal{A}, \text{SFS}}^{\text{SFS.UNF}} (\lambda) = \Pr \left[ \text{Exp}_{\text{SFS}}^{\text{SFS.UNF}} (\mathcal{A}) = 1 \right] \leq \text{negl}(\lambda)
\]

The main idea behind the unforgeability game is that an adversary \( \mathcal{A} \) must present a tamper \( (pk^*, m^*, \sigma^*) \) for an existing honestly generated public key, whose corresponding secret key is not revealed to \( \mathcal{A} \). We allow the adversary to arbitrarily request correct signatures and new key pairs that can be corrupted depending on the value of \( v \), i.e. if \( \mathcal{A} \)
can obtain a corrupted key pair by querying $O_{\text{SFS}}(f, i, 1)$ where $v = 1$. We deliberately do not allow $A$ to corrupt already generated key since this would imply that the third party that generates the key pairs is able to identify whenever a specific public key is compromised. Despite being possible in the ideal world, this property is hard to realise in a realistic scenario thus we force $A$ to declare at the generation, if a key pair is compromised or not.

**Function Hiding** an SFS scheme is said to be function hiding if the advantage of any PPT algorithm $A$ in the SFS function hiding experiment $\text{Exp}^{\text{SFS FHid}}(A)$, of Figure 38 to output 1 is negligible. Namely,

$$\text{Adv}^{\text{SFS FHid}}(\lambda) = \left| \Pr \left[ \text{Exp}^{\text{SFS FHid}}(A) = 1 \right] - \frac{1}{2} \right| \leq \text{negl}(\lambda)$$

Informally, it is impossible for an adversary to distinguish between two different function evaluations and signatures, i.e., given the public verification key of a single function, the adversary cannot infer information on “what function does the key verify”. When comparing to the FS function privacy property, the SFS function hiding requirement might appear counter-intuitive since, in the verification phase, it is necessary to use the public-key $pk_f$, which is related to the function $f$ that must be hidden. The SFS function hiding property requires that “a public-key should just allow the verification of the computation but must not provide any information of the function”. This means that from a public-key $pk_f$, it must be hard to retrieve the corresponding function $f$.

### 4.2 An SFS Instantiation

In this subsection, we provide the instantiation of SFS scheme which is a combination of the Fiore-Gennaro’s PVC variation (as given in Def. 28) and the BLS variation (as given in Def. 27).

**Definition 30.** Let $\mathcal{BLS}$ be the variated BLS signature scheme of Def. 27 and $\mathcal{VC}$ the variated Fiore-Gennaro PVC scheme of Def. 28. Let the public parameter $pp$ be the description of a bilinear group $(y, g_1, g_2, G_1, G_2, G_T, e)$ shared between the $\mathcal{BLS}$ and the $\mathcal{VC}$ schemes. Define the SFS scheme for the polynomial function family $\mathcal{F}$, where every function can be expressed in a binary string representation, with the following algorithms:

- **SFS.Setup$(\lambda)$ :** on input the security parameter $\lambda$, the algorithm runs $\mathcal{BLS}.\text{Setup}(\lambda)$ to $(\text{MSK}, \text{MPK})$, or equivalently $\mathcal{VC}.\text{Setup}$, and outputs the master key-pair $(\text{msk}, \text{mvk}) = (\text{MSK}, \text{MPK})$

- **SFS.KGen$(\text{msk}, f)$ :** on input the master secret key msk and a polynomial function $f$, execute $(\text{sk}_f, \text{vk}_f, \text{ek}_f) \leftarrow \mathcal{BLS}.\text{KGen}(pp, \text{msk}, f)$, parse the secret key $\text{sk}_f = (\alpha, g_2^\alpha, K)$ and run the algorithm $(\text{PK}_f, \text{SK}_f) \leftarrow \mathcal{BLS}.\text{KGen}(\lambda, \text{msk}, \alpha)$. Output $(\text{pk}_f, \text{sk}_f)$ defined as $\left( (\text{PK}_f, \text{vk}_f), (\text{SK}_f, (g_2^\alpha, K), \text{ek}_f) \right)$

- **SFS.Sign$(\text{sk}_f, m)$ :** given as input a secret key $\text{sk}_f$ and a message $m$, parse $\text{sk}_f = (\text{SK}_f, (g_2^\alpha, K), \text{ek}_f)$ and execute $(\tilde{\sigma}_m, \tilde{\rho}_m) \leftarrow \mathcal{VC}.\text{ProbGen}(g_2, m)$, then $\tilde{\sigma}_y = (y, V) \leftarrow \mathcal{VC}.\text{Compute}(\tilde{\text{ek}}_f, \tilde{\sigma}_m)$ and consequently compute the signature $\tilde{\sigma}_y \leftarrow \mathcal{BLS}.\text{Sign}(\text{SK}_f, (y, \tilde{\rho}_m, V))$. Output $(y, \sigma) = (y, (\tilde{\rho}_m, V, \tilde{\sigma}_y))$

- **SFS.Ver$(\text{mvk}, \text{pk}_y, y', \sigma')$ :** parse the inputs $\sigma' = (\tilde{\rho}_m', V, \tilde{\sigma}_y')$ and $\text{pk}_y = (\text{PK}_y, \text{vk}_y)$. Execute and output:

$$\bigwedge_{\mathcal{VC}.\text{Ver}(\text{mvk}, \text{vk}_y, \tilde{\rho}_m', (y', V)) \Rightarrow y'} \mathcal{BLS}.\text{Ver}(\text{mvk}, \text{pk}_y, (y', \tilde{\rho}_m', V), \tilde{\sigma}_y') \Rightarrow 1$$
Correctness for all SFS.Setup(λ) → (msk, mkv), functions f ∈ F, SFS.KGen(msk, f) → (pkf, skf) and messages m and SFS.Sign(skf, m) → (yk, σ), it holds SFS.Ver(msk, y, σ) = 1 which translates into
\[ \forall c, \forall \beta, \forall \gamma, \forall (y, V) \in G_T \times G_1 \times G_1, \text{trivially achieving the succinctness property.} \]

Unforgeability in order to prove our instantiation to be unforgeable, we will prove a reduction from the BLS unforgeability experiment \( \text{Exp}_{\text{BLS}}^{\text{unf}}(B) \) to the SFS unforgeability experiment \( \text{Exp}_{\text{SFS}}^{\text{unf}}(A) \).

**Theorem 6.** If for all PPT adversaries B it holds that the advantage \( \text{Adv}_{B, \text{BLS}}^{\text{unf}}(\lambda) \leq \text{negl}(\lambda) \), then for all PPT adversaries A it holds \( \text{Adv}_{A, \text{SFS}}^{\text{unf}}(\lambda) \leq \text{negl}(\lambda) \).

**Proof.** Assume that there exists a PPT adversary \( A \) such that \( \text{Adv}_{A, \text{SFS}}^{\text{unf}}(\lambda) = \Delta \) for some non-negligible \( \Delta > 0 \). We construct an adversary \( R \), running \( A \) as a subroutine, to break the unforgeability of the underlying BLS scheme. \( R \) executes \( \forall \text{C.Setup} \) and obtains the master keys (msk, mkv). \( R \) receives from the BLS challenger the public key \( PK \).

Whenever \( A \) queries a compromised key pair via \( O_{\text{SFS, kG}}(f, i, 1) \), \( R \) can generate the keys using \( \forall \text{C.KGen} \) and \( \text{BLS.KGen} \) and therefore can generate keys and compute the signing algorithm and answer to any adversarial signing query. On the other hand, whenever \( A \) queries a uncompromised pair \( O_{\text{SFS, kG}}(g, i, 0) \), \( R \) executes \( \forall \text{C.KGen} \) and generates the keys (skg, ekg, vkg). \( R \) samples a random value \( z(g, i) \) sets the public key \( PK_g = PK \cdot q_{g, i, r}^{z(g, i)} \).

By considering \( MSK = msk \), \( R \) samples \( r, s \in Z_p \), computes \( SK_g = q_r^{MSK+s+r} \) and \( PK_g = PK_1 = PK_2 = PK_3 \). Finally, it sends \( PK_g = (PK_g, PK_g) \) to \( A \).

In a nutshell, since the reduction \( R \) can create all the keys except the challenged \( SK \), \( R \) is always able to correctly execute the verifiable computation scheme but not to sign the final output of a computation of any message \( m \) on the uncompromised functions \( q \). This means that, whenever \( A \) queries the signing oracle \( O_{\text{SFS, sign}}(g, i, m) \) for an uncompromised function \( (g, i) \), \( R \) will sequentially execute \( \forall \text{C.ProgGn}(sk_g, m) \) and the algorithm \( \forall \text{C.Proc}(sk_g, \sigma_m) \) to obtain \( \sigma_m = (y, \sigma) \) which afterwards modifies the value \( \sigma_m = SK_1 \cdot \sigma \cdot H((y, \rho_m, V))^{z(g, i)} \). \( R \) replies to \( A \) with \( (y, \rho_m, V) \).

Whenever \( A \) outputs the forgery \( (pk_g, y^*, \sigma^*) \), the reduction \( R \) parses the output \( \sigma^* = (\rho^*, V^*, \sigma^*) \) and outputs the BLS forgery:
\[ (y^*, \rho^*, V^*, \sigma^* \cdot SK_1^{-1} \cdot H((y^*, \rho^*, V^*))^{-z(g, i)}) \]

Observe that \( A \) must output a forgery for an uncompromised function that, by construction, is always based on the challenged BLS scheme. The SFS unforgeability experiment’s requirements forces \( A \) to always tamper at least one between \( (y^*, \sigma^*) \) which always translates into \( R \) creating a new tamper never queried before to BLS. Thus, we can conclude that \( \Delta = \text{Adv}_{A, \text{SFS}}^{\text{unf}}(\lambda) \leq \text{Adv}_{B, \text{BLS}}^{\text{unf}}(\lambda) \) which is a contradiction. \( \square \)
Remark 12. The unforgeability experiment $\text{Exp}_{\text{SFS,UNF}}(A)$ requires the adversary $A$ to provide a tamper for a challenged public key $pk^*$ of a function $g$ which must exist and be uncompromised. This means that $A$ queried $O_{\text{SFS,UNF}}(g, *, 0)$ explicitly or implicitly via the signing oracle, and only owns the public key $pk^*$.

As a matter of curiosity, Thm. 6’s proof can be interpreted as the case where $A$ cannot forge even if the secret keys are partially compromised. In particular, consider the proof’s reduction $R$ returns to $A$ all the $\text{VC, KGen}$ generated keys $(\sk_A, \ek_A, \vk_A)$ which would allow $A$ to always pass the verification $\text{VC, Ver}$. Despite this additional concession, the proof shows that $A$ is still unable to provide a tamper for $\text{BLS}$, since $A$ does not hold the $\text{BLS}$ signing secret key, thus making it impossible to create a $\text{SFS}$ tamper.

**Function Hiding** in order to prove our instantiation to be function hiding, we will show a reduction from the VC function privacy experiment $\text{Exp}_{\text{C, Priv}}^\lambda(B)$ to the $\text{SFS}$ function hiding experiment $\text{Exp}_{\text{SFS,FHid}}(A)$.

**Theorem 7.** If for all PPT adversaries $B$ it holds that the advantage $\text{Adv}_{B,\text{VC}}^\lambda(\text{Val}) \leq \text{negl}(\lambda)$, then for all PPT adversaries $A$ it holds $\text{Adv}_{A,\text{SFS,FHid}}(\lambda) \leq \text{negl}(\lambda)$.

**Proof.** Assume the existence of a PPT adversary $A$ such that $\text{Adv}_{A,\text{SFS,FHid}}(\lambda) = \Delta$ for some non-negligible $\Delta > 0$. We then construct an adversary $B$, running $A$ as a subroutine, to break the privacy security of the underlying VC scheme. Let $R$ be the reduction from the $\text{VC, Priv}$ experiment to the $\text{SFS, FHid}$ one and therefore $B$ the final adversary that uses $R$ and $A$. $R$ executes $\text{VC, Setup}(\lambda) \rightarrow (\sk, \pk)$ and sends $\sk = \pk$ to the $\text{SFS}$ adversary $A$. $A$ replies with the challenge $(f_0, m_0, f_1, m_1)$ which is forwarded to the $\text{VC, Priv}$ challenger by $R$. $R$ receives $(\vk, \sigma, \rho, \phi)$ where $\sigma = (y, V_b)$ with $y$ which is equal to $f_0(m_0) = f_1(m_1)$. $R$ executes $\text{BLS, KGen}(\lambda, \sk, \phi)$ for some random $\phi \in \mathbb{Z}$ and obtain $\sk = (\sk_1, \sk_2) = (g^\sk \cdot \alpha, k)$ and $\pk = (\pk_1, \pk_2) = (e(g_1, g_2)^\alpha, g_2^k)$, then it signs $\text{BLS, Sign}(\sk, y)$ and obtains $\phi$. The reduction $R$ then replies to the $A$ with the tuple $(\vk, \sigma, \rho, \phi, \pk)$ where $\sigma_b = (y, V_b)$ which is equal to $(y, V_b, g^{\sk \cdot g_2})$. Finally, $A$’s guess is just forwarded to the challenger in $\text{VC}$’s privacy game.

By observing the $\text{SFS, Ver}$ algorithm, we get

$$\text{VC, Ver}(\sk, \vk, \rho, (y, V_b)) \iff y$$

and since the right side is always true, the left side is equivalent to

$$\text{VC, Ver}(\sk, \vk, \rho, (y, V_b)) \iff e(V_b, g_2) = e(\sk \cdot \vk, g_2) \equiv e(V_b, g_2) = e(V_b, g_2) \equiv e(V_b, g_2) = e(V_b, g_2) \equiv \text{VC, Ver}(\sk, \rho, (y, V_b))$$

Therefore, if the adversary $A$ has an advantage $\Delta$, the built adversary $B$ for $\text{VC, Priv}$ that uses $R$ has advantage $\Delta$. In other word, we conclude that $\Delta = \text{Adv}_{A,\text{SFS,FHid}}(\lambda) \leq \text{Adv}_{B,\text{VC}}^\lambda(\lambda)$ which is a contradiction.\[\square\]
5 Conclusion

Verifying the correctness of computations is a very valuable property considering the ever-increasing cloud-assisted computing paradigm. This paper defines Strong Functional Signature (SFS) as an enhanced version of functional signatures with verifiable computation properties. In a nutshell, SFS introduces a functional public key $pk_f$ that works as a commitment for a function $f$. This public-key allows in verification to guarantee the correct computation of the committed function without revealing any information on the function and to distinguish between different computed functions in a privacy-preserving way. Furthermore, we provide a concrete instantiation of an SFS scheme and prove that it satisfies the properties of unforgeability and function hiding.

5.1 Future Investigation (as of July 2021)

During the submission process, an anonymous reviewer brought to our attention a realistic attack not handled by the unforgeability experiment. The attacker $A$ obtains a key pair $((PK_f, vk_f), (SK_f, (g_2^0, K, ek_f)))$ for a function $f$. Given the knowledge of $K$, $A$ selects a different function $g$ with decomposition $(g_1, \ldots, g_l)$ and computes

$$W'_i = \left(\frac{W_i}{\text{CF.H}_K(i)}\right)^{\frac{g_i}{g_1}} \cdot \text{CF.H}_K(i) \quad \forall i \in \{1, \ldots, l\}$$

Observe that the $W'_i$ are indeed the evaluation values that are used to evaluate the function $g$, i.e. $W'_i = g_i^{(\alpha + \beta) g_1} \cdot \text{CF.H}_K(i)$. In this way, $A$ creates a key pair for the evaluation of $g$ and allows him/her to correctly sign $\text{SFS.Sign}(sk_f, m)$ and obtain a correctly verifiable output $(y, \sigma)$ such that $g(m) = y \neq f(m)$.

In other words, this attack allows an adversary that owns a secret key pair for $f$ to sign any function $g$ evaluation, making it impossible to correctly identify the computation correctness. Our unforgeability experiment of Fig. 38 does not incorporate such type/kind of attack as a valid forgery, because we exclude the case of forgery for any compromised secret key of function $f$. For this reason, we leave open for future development an augmented notion of unforgeability as intuitively represented in Fig. 39 and that incorporates the hypothesis of the FS unforgeability experiment SFS.UNF of Fig. 33. The stronger unforgeability experiment would require the adversary to output a tamper $m'$ such that $m' = f(m')$. As future work, we will consider how to give an instantiation that can achieve such an augmented security requirement.

![Figure 39: SFS stronger unforgeability experiment.](image)
Acknowledgment

We thank the anonymous reviewers for pointing out the security concern. This work was partially supported by the Swedish Research Council (Vetenskapsrådet) through the grant PRECIS (621-2014-4845).