Multiple-Time Signature Schemes against Adaptive Chosen Message Attacks

Josef Pieprzyk[1], Huaxiong Wang[1], and Chaoping Xing[2]

[1] Centre for Advanced Computing – Algorithms and Cryptography
Department of Computing, Macquarie University, Australia
{josef,hwang}@ics.mq.edu.au
[2] Department of Mathematics, National University of Singapore, Singapore
Department of Mathematics, University of Science and Technology of China, China
matxcp@nus.edu.sg

Abstract. Multiple-time signatures are digital signature schemes where the signer is able to sign a predetermined number of messages. They are interesting cryptographic primitives because they allow to solve many important cryptographic problems, and at the same time offer substantial efficiency advantage over ordinary digital signature schemes like RSA. Multiple-time signature schemes have found numerous applications, in ordinary, on-line/off-line, forward-secure signatures, and multicast/stream authentication. We propose a multiple-time signature scheme with very efficient signing and verifying. Our construction is based on a combination of one-way functions and cover-free families, and it is secure against *the adaptive chosen-message attack*.

1 Introduction

One-time signature schemes proposed by Lamport [18] and Rabin [24] were among the earliest signatures based on the idea of committing to secret keys by one-way functions. For more than 25 years, various variants of Lamport and Rabin's schemes have been proposed and investigated by many researchers (see, for example, [3, 5, 6, 13, 20]). In general, digital signatures can be divided into two classes. The first class includes one-time signatures and their variants based on one-way functions. These schemes can be used to sign a predetermined number of messages, we will call them *multiple-time signature schemes* (e.g., one-time signature by Lamport and Rabin). The second class of schemes is based on public-key cryptography and they can be used to sign unlimited number of messages. Examples of this class of schemes include RSA and ElGamal signatures.

Despite the limit imposed on the number of messages signed, multiple-time signatures are very interesting cryptographic primitives as they typically offer more efficient generation and verification of signatures than the schemes based on public-key cryptography. Besides, multiple-time signatures can be constructed based on an arbitrary one-way function without requiring a trapdoor function. Multiple-time signatures have found many applications, for example, in the design of public-key signature schemes [21, 3, 10], on-line/off-line signatures [12],

M. Matsui and R. Zuccherato (Eds.): SAC 2003, LNCS 3006, pp. 88–100, 2004.

digital signatures with forward security properties [1], broadcast authentication protocol [23] and stream-oriented authentication [27], just to mention a few.

All the previous multiple-time signature schemes follow the general idea that the secret key is used as the input to a sequence of one-way functions which generate a sequence of intermediate results and finally the public key. One-wayness of the functions implies that it is infeasible to compute the secret key, or any intermediate result of the computation, from the public key. For example, the idea of the basic scheme of Lamport [18] is very simple: given a one-way function f, one selects two random strings x_0, x_1 as the secret key, and publishes $f(x_0), f(x_1)$ as the public key. Then, a single-bit message $b \in \{0, 1\}$ can be signed by revealing x_b. Bleichenbacher and Maurer in their series of papers [6, 7, 8], developed the general model of these schemes based on the use of "graphs of one-way functions". The security proof under this model has been investigated recently by Hevia and Micciancio [14].

Motivated by the applications of signatures to stream authentication and broadcast authentication, Perrig in [23] proposes a one-time signature called "BiBa", which has the advantages of fast verification and being short signature (perhaps, BiBa has the fastest verification of all previously known one-time signature schemes). The disadvantage of BiBa is, however, the signing time that is longer than in other previous schemes.

Reyzin and Reyzin in [25] proposed a new one-time (r-time) signature, called *HORS* (for Hash to Obtain Random Subset). HORS improves the BiBa scheme with respect to the time overhead necessary for verifying and signing, and reduces the key and signature sizes. This makes HORS the fastest one-time signature scheme available so far. We note that the security of BiBa can be proved in the random-oracle model while the security of HORS relies on the assumption of the existence of one-way functions and the *subset-resilience*.

Our Contribution In this paper, we propose a new multiple-time signature scheme. The scheme has the following advantages with respect to the security: (i) the security relies solely on one-wayness of the functions used to generate commitments (whereas BiBa is based on the assumption of random oracle and HORS is based on one-wayness and subset-resilience); (ii) the scheme achieves security against the r-adaptive chosen-message attack.

The new multiple-time signature is based on a one-way function and uses a combinatorial object, called the *cover-free family*. It is worth pointing out that the cover-free families introduced by Erdös *et al* [11], have also found numerous other application in cryptography and communication [17, 30].

The main advantage of our new scheme is that it achieves the highest level of security against the adaptive chosen-message attack. In comparison to the BiBa and HORS schemes, however, our scheme is slightly worse with respect to the time overhead needed for signing and verifying, and the length of signature. Moreover, the security of our scheme solely relies on the one-wayness of the function used to generate public keys. This assumption is substantially weaker

than those required for the BiBa and HORS signatures (BiBa uses the random oracle assumption while the HORS security relies on subset resilience).

First, we give the generic construction from cover-free families and show that the efficiency of the scheme can be measured by the parameters of the underlying cover-free families. We then present three, very efficient, constructions. These constructions apply polynomials, error-correcting codes, and algebraic curves over finite fields. We further extend the scheme to increase the number of messages to sign, using the concepts of *one-way hash chains*.

The paper is organised as follows. In Section 2, we review the generic scheme proposed by Reyzin and Reyzin [25] that was used to construct their HORS and our schemes. In Section 3, we propose the new multiple-time signature scheme, the scheme is generic in the sense that is combines any one-way function with a cover-free family with appropriate parameters. In Section 4, we demonstrate efficiency of ne new proposed scheme by giving three constructions from polynomials over finite fields, error-correct codes and algebraic curves over finite fields. In Section 5 we extend our scheme and show how to increase the number of messages to sign, using the hash chains. We conclude the paper in Section 6.

2 Reyzin-Reyzin Scheme

The HORS scheme proposed by Reyzin and Reyzin [25] is an extension of their simpler scheme in the same paper, which we will call the RR scheme. We start with the description of the RR signature.

The RR scheme Let b, t, k be integers such that $\binom{t}{k} \geq 2^b$. Let T denote the set $\{1, 2, \ldots, t\}$ and $\mathcal{T}_k$ be the family of k-subsets of T. Let S be a one-to-one mapping from $\{0, 1, \ldots, 2^b - 1\}$ to $\mathcal{T}_k$ such that $S(m)$ is the m-th k-element subset of $\mathcal{T}_k$. Let f be a one-way function operating on ℓ-bit strings, for a security parameter ℓ. The scheme works as follows.

Key generation: The secret key is $SK = (s_1, \ldots, s_t)$, where s_i are random ℓ-bit strings. The public key is $PK = (v_1, \ldots, v_t)$, where $v_1 = f(s_1), \ldots, v_t = f(s_t)$.

Signing: To sign a b-bit message m, the message is first interpreted as an integer between 0 and $2^b - 1$, and next the mapping S is used to compute $S(m) = \{i_1, \ldots, i_k\} \in \mathcal{T}_k$. The value $s_{i_1}, \ldots, s_{i_k}$ is the signature of m.

Verifying: To verify a signature $(s'_1, s'_2, \ldots, s'_k)$ on a message m, again the message is interpreted as an integer between 0 and $2^b - 1$, and then the sequence $\{i_1, \ldots, i_k\}$ is recalculated as the m-th k-element subset of $\mathcal{T}_k$. Finally, it is checked if $f(s'_1) = v_{i_1}, \ldots, f(s'_t) = v_{i_t}$ holds.

Note that the Bos and Chaum's scheme [2] is a special case of the above RR scheme in which $k = t/2$. We also note that for $k = t/2$, Stinson [29] (page 217) gave an algorithm that reduces the size of signature to half of the original size of Bos-Chaum scheme.

The security of this scheme relies on one-wayness of f. Indeed, in order to forge a signature for a new message (or apply the adaptive chosen-message attack), the adversary is forced to invert at least one of the $t - k$ values in the public key for which the corresponding part of the secret key has not been revealed.

We look at the efficiency of the scheme. The key generation requires t evaluations of one-way function. The secret key size is $t\ell$ bits, and the public key size is $f_\ell t$ bits, where f_ℓ is the length of the one-way function output on the input length ℓ. The signature is $k\ell$ bit long. The signing algorithm takes as long as the running time of the algorithm for S: the time required to find the m-th k-element subset of a t-element set. In [25], Reyzin and Reyzin gives two algorithms for implementation of the mapping S:

Algorithm 1 is based on the following equation:

$$\binom{t}{k} = \binom{t-1}{k-1} + \binom{t-1}{k},$$

and has the computation cost of $O(tk \log^2 t)$, provided $O(k^2 log^2 t)$ bits extra storage available.

Algorithm 2 is based on the following a slightly more complicated equation:

$$\binom{t}{k} = \sum_{i=0}^{k} \binom{\lceil t/2 \rceil}{i} \binom{\lfloor t/2 \rfloor}{k-i},$$

and has the computation cost of $O(k^2 \log t \log k)$, provided $O(k^2 log^2 t)$ bits extra storage available.

The verifying algorithm of the RR scheme takes the same amount of time as signing, plus k evaluations of the one-way function.

Obviously, the most expensive part of the RR scheme is the computation of the function S. Note that for the function S, it is *impossible* to find any two distinct m_1 and m_2 such that $S(m_2) \subseteq S(m_1)$. To improve efficiency of the RR scheme, Reyzin and Reyzin proposed HORS in which the function S in the RR scheme is replaced by another function H with a weaker property that it is *infeasible* to find two messages, m_1 and m_2 such that $H(m_2) \subseteq H(m_1)$, the function H with such a property is called a *subset-resilient* function. In HORS, a **conjectured** subset-resilient function is constructed from certain cryptographic hash functions.

One drawback with the RR scheme is that each public key/private key can be used to sign a single message. Of course, to sign r messages, one can simply apply the scheme r times independently. This means that the cost of the scheme will be linear in the number of messages r. The question is: can we have a more efficient solution for signing r messages, where $r > 1$? Allowing to sign multiple messages introduces a new attack on the scheme: *the adaptive chosen-messages attack*, where the adversary can choose the message for signature after seeing a collection of messages and their signatures. Unlike the

RR scheme, HORS can be used for signing multiple messages, but its security is based on a much stronger assumption, i.e., *subset-resilient* function. In this work, we propose a new multiple-time signature scheme that provides security against the adaptive chosen-message attack, thus our scheme can be viewed as a generalisation of Bos-Chaum scheme with improved efficiency and of HORS with enhanced security.

3 The Scheme

As we have seen, both the Bos-Chaum scheme and the RR scheme can be used to sign a single message. We intend to generalise their scheme so it can be used for multiple signatures. We observe that the the basic requirement of S is such that for any distinct messages m_1, m_2, we have $S(m_1) \not\subseteq S(m_2)$ in the family of subsets $\mathcal{T}$. If the function S has, however, the property that for any $r+1$ messages $m_1, m_2, \ldots, m_{r+1}$, $S(m_{r+1}) \not\subseteq \cup_{i=1}^{r} S(m_i)$, then the scheme can be used to sign up to r messages. The required property of S can be captured by a well known combinatorial object, called the *cover-free family* introduced by Erdös *et al* [11].

Definition 1. *A set system $(X, \mathcal{B})$ with $X = \{x_1, \ldots, x_t\}$ and $\mathcal{B} = \{B_i \subseteq X \mid i = 1, \ldots, n\}$ is called an* (n, t, r)-cover-free family *(or (n, t, r)-CFF for short) if for any subset $\Delta \subseteq \{1, \ldots, n\}$ with $|\Delta| = r$ and any $i \notin \Delta$,*

$$\left| B_i \setminus \bigcup_{j \in \Delta} B_j \right| \geq 1.$$

Our new scheme HORS++ is based on a one-way function and a CFF with appropriate parameters.

HORS++ Scheme Let $(X, \mathcal{B})$ be an (n, t, r)-CFF and let b be an integer such that $2^b \leq n$, where b is the length of the message m to be signed. If the message length is greater than b, then a collision-resistant hash function is used to produce a b-bit digest of m. The signature is generated for the digest.

Assume S is a one-to-one mapping from $\{0,1\}^b$ to $\mathcal{B}$ (Since $n \geq 2^b$ such a mapping S exists). The scheme works as follows.

Key generation: For the given security parameter 1^ℓ, generate t random ℓ-bit numbers s_i and let the secret key be $SK = (s_1, \ldots, s_t)$. Compute the public key as follows: $PK = (v_1, \ldots, v_t)$, where $v_1 = f(s_1), \ldots, v_t = f(s_t)$ and f is a one-way function.

Signing: To sign a message $m \in \{0,1\}^b$, compute $S(m) = \{i_1, \ldots, i_k\} \in \mathcal{B}$. Reveal $(s_{i_1}, s_{i_2}, \ldots, s_{i_k})$ as a signature.

Verifying: To verify a signature $(s'_1, s'_2, \ldots, s'_k)$ on a message m, recompute $S(m) = \{i_1, \ldots, i_k\} \in \mathcal{B}$. Verify that $f(s'_1) = v_{i_1}, \ldots, f(s'_t) = v_{i_t}$.

Security Suppose that the adversary has seen r valid signatures for the message $m_1, \ldots, m_r$ chosen adaptively. In order to forge a signature on a new message, the adversary would have to invert the one-way function f on the value associated to the points of $S(m_{r+1}) \setminus \cup_{i=1}^{r} S(m_i)$ in the public key. Since $(X, \mathcal{B})$ is an (n, t, r)-CFF, it yields that $|S(m_{r+1}) \setminus \cup_{i=1}^{r} S(m_i)| \geq 1$. That means that the adversary has to invert the one-way function on at least one value, and so the security of the signature is reduced to the one-wayness of f. Furthermore, it is fairly easy to see that the property of the r-cover freeness guarantees that the scheme is secure against the r-adaptive chosen-message attack.

Efficiency To measure the efficiency of the scheme, we consider two aspects of performance: (i) the time needed for key generation, signing, and verifying; (ii) the length of secret key, public key, and signature. The key generation requires t evaluations of one-way function, the signing takes as long as the running time of the algorithm for S and the verifying algorithm takes the same time as signing, plus at most t evaluations of the one-way function. The size of public and secret key is determined by t and the size of signature is determined by the size of blocks $|B_i|$ in $\mathcal{B}$.

Thus, the performance of the scheme is virtually determined by the parameters of the underlying cover-free family. Without considering the complexity of algorithm S, it is expected that the underlying (n, t, r)-cover-free family has the desired property that for given n and r, the parameter t is as small as possible. Constructions and bounds for (n, t, r)-CFF were studied by numerous authors (see, for example, [11, 17, 30]). It is shown in [30] that for (n, t, r)-CFF with $t \geq 2$, $t \geq c\frac{r^2}{\log r} \log n$ for some constant $c \approx 1/8$. On the other hand, Erdös *et al* [11] showed that for any $n > 0$, there exists an (n, t, r)-CFF with $t = O(r^2 \log n)$ and $|B_i| = O(r \log n)$. Therefore, we obtain the following theorem.

Theorem 1. *Given a one-way function f with the ℓ-bit input and f_ℓ-bit output. There exists a r-time signature scheme secure against the adaptive chosen-message attack with the secret key size $O(r^2 f_\ell \ell)$-bits, public key size $O(r^2 f_\ell^2)$-bits, and with the size of signature $O(r f_\ell \ell)$.*

Proof. Taking $n = 2^{f_\ell}$ and applying the results of cover-free family, the construction will result in a scheme with the desired properties in Theorem 1.

However, Theorem 1 is only of theoretical interest, because it doesn't take into account the time cost of the implementation for the function S, so it is only an existence result. As in the RR scheme, implementation of the function S is the most time consuming part of the system. To make the proposed scheme practical, we have to specify the function S and provide an algorithm for its evaluation.

4 Constructions

In this section we give several constructions of S for HORS++. Observe that in the RR scheme, the parameters t, k of the function S are chosen in order to min-

imise the expression $\binom{t}{k} - 2^b$ so the size of secret key/public key (corresponding to t) and the size of signature (corresponding to k) is minimal (note that there are some trade-offs between t and k). In other words, the family $\mathcal{T}_k$ of k-subsets of T is minimal such that there is a one-to-one mapping from $\{0, 1, \ldots, 2^b - 1\}$ to $\mathcal{T}_k$. The minimal size of $\mathcal{T}_k$ seems, however, to increase the difficulty (cost) of the implementation of S. To efficiently implement S, we allow the size of the range of S, i.e., the size of the blocks in the cover-free family, to be slightly larger than the minimal value and then we can expect to have an easy implementation for the one-to-one mapping S. We will elaborate this idea in this section, giving several explicit constructions for S.

4.1 Construction of S Based on Polynomials

Consider polynomials of degree less that d over $GF(2^c)$, where $b = dc$. For each such polynomial g, we associate a set

$$B_g = \{(x, g(x)\} \subseteq GF(2^c) \times GF(2^c).$$

Let $X = GF(2^c) \times GF(2^c)$ and

$$\mathcal{B} = \{B_g \mid g \text{ is a polynomial of degree at most } d-1\}.$$

It is easy to see that $|B_g| = 2^c$ and $|\mathcal{B}| = 2^{dc} = 2^b$. Now if $g_1 \neq g_2$, then $|B_{g_1} \cap B_{g_2}| \leq d-1$ since $g(x) = g_1(x) - g_2(x)$ is a polynomial of degree $d-1$ with at most $d-1$ different solution for the equation $g(x) = 0$. We can show that $(X, \mathcal{B})$ is a $(2^b, 2^c, r)$-CFF provided $2^c \geq r(d-1)+1$. Indeed, for any $g, g_1, \ldots, g_r$ of polynomial of degree less than d over $GF(2^c)$, we have

$$\begin{aligned} |B_g \setminus (B_{g_1} \cup \cdots \cup B_{g_r})| &\geq |B_g| - (|B_g \cap B_{g_1}| + \cdots + |B_g \cap B_{g_r}|) \\ &\geq 2^c - r(d-1) \\ &\geq 1. \end{aligned}$$

It should be noted that the above cover-free family construction is not new, it was first given by Erdös in [11] and further extended by many other authors. Our main point is to give the explicit construction of S in an efficient way.

To fulfil the task for signing messages of arbitrary length, we propose using a cryptographic hash function H, for example SHA-1 or RIPEMD and assume that the output of the hash function is of b bits. To sign a message m, we first hash m using H and construct the one-to-one mapping S as follows.

- Split $H(m)$ into d substrings of length c-bit each, where $b = cd$.
- Interpret each c-bit substring as an element in $GF(2^c)$, denote these d elements as $a_0, a_1, \ldots, a_{d-1}$ and construct a polynomial $g_m(x) = a_0 + a_1 x + \cdots, a_{d-1}x^{d-1}$.
- We define the mapping S from $\{0,1\}^b$ to $\mathcal{B}$ as follows,

$$S(H(m)) = \{(\alpha, g_m(\alpha)) \mid \alpha \in GF(2^c)\}.$$

The implementation of S only involves in the direct evaluation of polynomials over the finite field $GF(2^c)$. So both the sign and verification are very fast. The sizes of key and signature are slightly worse than the RR scheme.

4.2 Error-Correcting Code Construction

A more general explicit construction for the mapping S from the above polynomial construction is through error-correcting codes. In fact, the polynomial construction can be seen a special case of the construction from Reed-Solomon codes.

Let Y be an alphabet of q elements. An (N, M, D, q) *code* is a set $\mathcal{C}$ of M vectors in Y^N such that the Hamming distance between any two distinct vectors in $\mathcal{C}$ is at least D.

Consider an (N, M, D, q) code $\mathcal{C}$. We write each codeword as $c_i = (c_{i1}, \ldots, c_{iN})$ with $c_{ij} \in Y$, where $1 \leq i \leq M, 1 \leq j \leq N$. Set $X = \{1, \ldots, N\} \times Y$ and $\mathcal{B} = \{B_i : 1 \leq i \leq M\}$, where for each $1 \leq i \leq M$ we define $B_i = \{(j, c_{ij}) : 1 \leq j \leq N\}$. It is easy to check that $|X| = Nq$, $|\mathcal{B}| = M$ and $|B_i| = N$. For each pair of i, k, we have $|B_i \cap B_k| = |\{(j, c_{ij}) : 1 \leq j \leq N\} \cap \{(j, c_{kj}) : 1 \leq j \leq N\}| = |\{j : c_{ij} = c_{kj}\}| \leq N - D$.

Using an identical argument to the one applied in the polynomial construction, it is easy to see that $(X, \mathcal{B})$ is (M, Nq, r)-CFF if the condition $r < \frac{N}{N-D}$ holds. We thus obtain that if there is an (N, M, D, q) code, then there exists an (M, Nq, r)-CFF provided $r < \frac{N}{N-D}$.

Note that the above coding construction is explicit. That is, given a code word $c_i \in \mathcal{C}$, it is straightforward to find its corresponding block B_i. Now to explicitly construct the mapping S, we only need to find the one-to-one mapping from $\{H(m) \mid m$ in the message space$\}$ to $\mathcal{B}$, which is the same as the encoding algorithm in the error-correcting code, and so can be very efficient. In the following we show how to construct S using a linear error-correcting codes.

Let $\mathcal{C}$ be an (N, q^d, D, q) linear error-correcting code with a d by N generating matrix A. Each code word can be indexed by the elements in $GF(q)^d$, using the encoding algorithm: $(y_1, y_2, \ldots, y_N) = (x_1, x_2, \ldots, x_d)A, \forall (x_1, x_2, \ldots, x_d) \in \mathcal{C}$. For the implementation consideration we may further assume, without loss of generality, that $q = 2^c$ and the hash output of the messages to be signed is of cd bits. The one-to-one mapping S is then constructed as follows.

- Split $H(m)$ into d substrings of length c-bit each, where $b = cd$.
- Interpret each c-bit substrings as an element in $GF(2^c)$, and denote $H(m)$ as a d-vector $(x_1, x_2, \ldots, x_d) \in (GF(2^c))^d$.
- Define the one-to-one mapping $S : \{0,1\}^b \to \mathcal{B}$ as follows,

$$\begin{aligned} S(H(m)) &= \{(j, y_j) : 1 \leq j \leq N\} \\ &= \{(1, y_1), (2, y_2), \ldots, (N, y_N)\}, \end{aligned}$$

where $(y_1, y_2, \ldots, y_N) = (x_1, x_2, \ldots, x_d)A = H(m)A$.

Again, the algorithm for the S implementation is quite efficient as it only involves in the matrix multiplication over a finite field. A further interesting question is to find the good codes satisfying the required conditions that should result in a good performance for the proposed scheme.

4.3 Algebraic Curve Construction

If we apply the code construction of CFFs in Section 4.2 to algebraic geometry codes, we immediately obtain the following result (the reader may refer to [22] for the background on algebraic codes and curves).

Corollary 1. *Let $\mathcal{X}/GF(q)$ be an algebraic curve of genus g with $N+1$ rational points. Then for any integer d with $g \leq d < N$, there exists a $(q^{d-g+1}, Nq, \lfloor (N-1)/d \rfloor)$-CFF.*

To study the asymptotic behaviour of CFFs in Corollary 1, we need some notation from algebraic geometry (see [22]). Define

$$A(q) := \limsup_{g(\mathcal{X})\to\infty} \frac{N(\mathcal{X})}{g(\mathcal{X})},$$

where $N(\mathcal{X})$ stands for the number of the rational points of the curve $\mathcal{X}$ defined over $GF(q)$, and $g(\mathcal{X})$ for the genus of $\mathcal{X}$. By [22] (Example 5.4.1), we know that $A(q) = \sqrt{q} - 1$ if q is a square prime power.

Combining Corollary 1 with the definition of $A(q)$, we obtain the following asymptotic result.

Corollary 2. *For a fixed r and a square prime power q with $r < \sqrt{q} - 1$, there exists a sequence of CFFs with parameters*

$$(q^{d_i-g+1}, N_i q, r)$$

such that

$$\lim_{i\to\infty} \frac{\log q^{d_i-g+1}}{N_i q} = \frac{\log q}{q} \times \left(\frac{1}{r} - \frac{1}{\sqrt{q}-1}\right). \tag{1}$$

Remark Corollary 2 shows that for any fixed r there are infinite families of (n, t, r)-CFF in which $t = O(\log n)$. In fact, the constructions are explicit in the sense that the mapping S can be constructed explicitly as long as the curves have explicit equations.

For the rest of this section, we are going to improve the asymptotic result in Corollary 2.

Let $\mathcal{X}$ be an algebraic curve of genus g with at least $n+g+1$ rational points. By using an identical argument in the proof of [28] (Proposition I.6.10), we can show that there exist $n+1$ rational points $P_\infty, P_1, \ldots, P_n$ such that

$$\mathcal{L}(rdP_\infty - \sum_{i=1}^{n} P_i) = \{0\},$$

if $rd - n \leq g - 1$, where $\mathcal{L}(D)$ stands for the Rieman-Roch space for a divisor D, i.e.,

$$\mathcal{L}(D) := \{\text{functions } f : \text{div}(F) + D \geq 0\}.$$

For each $f \in \mathcal{L}(dP_\infty)$, we denote $B_f = \{(P_i, f(P_i)) \mid i = 1, 2, \ldots, n\}$. For any $r+1$ distinct $f_1, f_2, \ldots, f_r, f \in \mathcal{L}(dP_\infty)$, we have $\prod_{i=1}^{r}(f - f_i) \in \mathcal{L}(dP_\infty)$ as $f \neq f_i$ for any $i = 1, \ldots, r$. On the other hand, Since $\prod_{i=1}^{r}(f - f_i) \neq 0$, we have $\prod_{i=1}^{r}(f - f_i) \notin \mathcal{L}(rdP_\infty - \sum_{i=1}^{n} P_i)$. Therefore, there exists a P_j such that $\prod_{i=1}^{r}(g - g_i)(P_j) \neq 0$, i.e., $f(P_j) \neq f_i(P_j), \quad \forall i = 1, 2, \ldots, n$, We then conclude $(P_j, f(P_j)) \in B_f$ and $(P_j, f(P_j)) \notin \cup_{i=1}^{r} B_{f_i}$. That is,

$$|B_f \setminus \cup_{i=1}^{r} B_{f_i}| \geq 1.$$

This shows that there exists a $(|\mathcal{L}(dP_\infty)|, nq, r)$-CFF or, equivalently, a (q^{d-g+1}, nq, r)-CFF. Moreover, if we let $r = \lfloor g - 1 + n/d \rfloor$ then we obtain a

$$(q^{d-g+1}, nq, \lfloor g - 1 + n/d \rfloor) - \text{CFF}.$$

Thus, we have proved the following corollary.

Corollary 3. *If q is a square prime power, then for a fixed r we obtain a sequence of CFFs with parameters*

$$(q^{d_i - g + 1}, N_i q, r)$$

such that

$$\lim_{i \to \infty} \frac{\log q^{d_i - g + 1}}{N_i q} = \frac{\log q}{q} \times \left(\frac{1}{r} - (1 - \frac{1}{r}) \frac{1}{\sqrt{q} - 2} \right). \tag{2}$$

Obviously, bound (1) improves bound (2) for $r < \sqrt{q} - 1$.

Remarks

(i) Corollary 2 and 3 shows that the existence bounds of CFFs in [11, 30] can be asymptotically met by the explicit constructions.
(ii) Most previous explicit constructions for CFFs typically apply the tricks from coding constructions of Section 4.2. Thus, Corollary 3 can be also used to improve previous results on cover-free families, for example, the explicit construction from algebraic geometry codes in [17].

5 Extensions

Consider the following question: suppose that r is the maximal value that HORS++ scheme can be used to sign up to r messages, i.e., r is maximal for which the set system $(X, \mathcal{B})$ is a (n, t, r)-cover-free family (for the fixed n and t). What will happen if we want the scheme to sign $r+1$ or more than $r+1$ messages? In this section we will suggest a solution to extend the scheme to increase the number of messages to sign.

One-way hash chains, or simply *one-way chains*, are build on using a one-way function repeatly to a random input, they are a frequently used cryptographic primitive in the design of secure protocols [19, 26, 15]. By a one-way chain we mean a sequence of values $< s_0, s_1, \ldots, s_d >$, where s_d is a value chosen uniformly

at random from $\{0,1\}^\ell$, and $s_i = f((s_{i+1})$, where $f : \{0,1\}^* \to \{0,1\}^\ell$ is a hash function or a publicly computable one-way function.

We can employ one-way hash chains to our basic scheme to increase the number of the messages to be signed.

1. Create a sequence of secret keys and their public keys:

$$\begin{array}{llll} s_{1,d}, & s_{1,d-1}, \cdots & s_{1,1}, s_{1,0} \to & v_1 \\ s_{2,d}, & s_{2,d-1}, \cdots & s_{2,1}, s_{2,0} \to & v_2 \\ \vdots & \vdots & \vdots & \\ s_{t,d}, & s_{t,d-1}, \cdots & s_{t,1}, s_{t,0} \to & v_t \end{array}$$

   such that $s_{i,j-1} = f(s_{i,j})$ for $i = 1, \ldots, t$ and $j = 1, \ldots, d$ while $v_i = f(s_{i,0})$ and f is a one-way function. The secret key is $(s_{1,d}, \ldots, s_{t,d})$ and the public key is $(v_1, \ldots, v_t)$.
2. To sign a sequence of messages using HORS++, the signer first uses the first level of secret keys (i.e., $(s_{1,0}, \ldots, s_{t,0})$) to sign the r message and go backwards to the second level of secret keys (i.e., $(s_{1,1}, \ldots, s_{t,1})$ for the next r messages, and so on.
3. Verification of the signatures is exactly the same as HORS++

Using this approach, the scheme can be used to sign up to $(d+1)r$ messages. The properties of one-way chains leave room to improve the time overhead of the signature verification. Note that given an existing authenticated element of a one-way hash chain, it is possible to verify elements later in the sequence of use within the chain, without evaluating all the sequence of the hash function. For example, if $d_{i,j}$ has been used to sign among the $(j+1)$th r messages and its value is revealed, then $d_{i,j+3}$ can be used to sign the message from the $(j+4)$th r messages, by simply computing $f(f(f(s_{i,j+3})))$ and verifying that the resulting value equals $s_{i,j}$, rather than computing $f^{j+4}(s_{i,j+3})$ and verifying its equality with v_i. Recently, Jakobsson [16] and Coppersmith and Jakobsson [9] propose a computation-efficient mechanism for one-way chains, it requires only $O(\log d)$ computation to verify the elements for a one-way chain of d elements, rather than the $O(d)$ computation of the trivial approach. An interesting research problem to ask is whether their techniequs can be incorporated into our scheme to improve the time overhead.

Also, it is worth pointing out that the above extended scheme is not secure against the adaptive chosen-message attacks, but only against the random chosen-message attacks.

6 Conclusion

In this paper, we proposed a multiple-time signature scheme with security against adaptive-chosen-message attacks. Our construction is based on a one-way function and a cover-free family in which the security solely relies on the one-wayness of the one-way function, whereas the efficiency can be measured by the underlying cover-free family. We show several constructions of cover-free families can be used to construct this new multiple-time signature scheme in an effective way.

Acknowledgements

We wish to thank Leonid Reyzin for his insightful comments and suggestions on an earlier draft of the paper. The work is in part supported by Australian Research Council Discovery grants DP0345366 and DP0344444.

References

[1] M. Abdalla and L. Reyzin. A new forward-secure digital signature scheme, *Advances in Cryptology – Asiacrypt'00*, LNCS, **1976**(2000), 116-129. 89

[2] J. N. E. Bos and D. Chaum. Provably unforgeable signature, *Advances in Cryptology – Crypto'92*, LNCS, **740**(1993), 1-14. 90

[3] M. Bellare and S. Micali. How to sign given any trapdoor function. *Journal of Cryptology,* **39**(1992), 214-233. 88

[4] M. Bellare and S. Miner. A forward-secure digital signature scheme, *Advances in Cryptology – Crypto'99*, LNCS, **1666**(1999), 431-448.

[5] M. Ballare and S. G. Neven. Transitive signatures based on factoring and RSA, *Advances in Cryptology – Asiacrypt'02*, LNCS, **2501**(2002), 397-314. 88

[6] D. Bleichenbacher and U. Maurer. Directed acyclic graphs, one-way functions and digital signatures, *Advances in Cryptology – Crypto'94*, LNCS, **839**(1994), 75-82. 88, 89

[7] D. Bleichenbacher and U. Maurer. On the efficiency of one-time digital signatures, *Advances in Cryptology – Asiacrypt'96*, LNCS, **1163**(1996, 145-158. 89

[8] D. Bleichenbacher and U. Maurer. Optimal tree-based one-time digital signature schemes, *STACS'96*, LNCS, **1046**(1996), 363-374. 89

[9] D. Coppersmith and M. Jakobsson. Almost optimal hash sequence traversal, *Financial Cryptography (FC'02)*, LNCS, 2002, to appear. 98

[10] C. Dwork and M. Naor. An efficient existentially unforgeable signature scheme and its applications, *Advances in Cryptology – Crypto'94*, LNCS, **839**(1994), 234-246. 88

[11] P. Erdös, P. Frankl, and Z. Furedi, Families of finite sets in which no set is covered by the union of r others, *Israel Journal of Mathematics*, **51**(1985), 79-89. 89, 92, 93, 94, 97

[12] S. Even, O. Goldreich and S. Micali. On-line/off-line digital signatures, *Journal of Cryptology*, **9**(1996), 35-67. 88

[13] S. Goldwasser, S. Micali and R. Rivest. A digital signature scheme secure against adaptive chosen-message attacks, *SIAM Journal on Computing*, **17**(1988), 281-308. 88

[14] A. Hevia and D. Micciancio. The provable security of graph-based one-time signatures and extensions to algebraic signature schemes. *Advances in Cryptology – Asiacrypt'02*, LNCS, **2501**(2002), 379-396. 89

[15] Y.-C Hu, A. Perrig and D. B. Johnson. Packet Leashes: A defense against wormhole attacks in wireless Ad Hoc Networks, *Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003)*, 2003, to appear. 97

[16] M. Jakobsson. Fractal hash sequence representation and traversal, *Proceedings of the IEEE International Symposium on Information Theory (ISIT02)*, 2002, 437-444. 98

[17] R. Kumar, S. Rajagopalan and A. Sahai, Coding constructions for blacklist in problems without computational assumptions, *Advances in Cryptology – CRYPTO '99*, LNCS, **1666**(1999), 609-623. 89, 93, 97
[18] L. Lamport. Constructing digital signatures from a one way function, *Technical Report CSL-98*, SRI International, 1979. 88, 89
[19] L. Lamport. Password authentication with insecure communication, *Communication of the ACM*, **24**(11), 1981, 770-772. 97
[20] R. C. Merkle. A digital signature based on a conventional function, *Advances in Cryptology – Crypto'87*, LNCS, **293**(1987), 369-378. 88
[21] R. C. Merkle. A certified digital signature. *Advances in Cryptology – Crypto'87*, LNCS, **435**(1990), 218-238. 88
[22] H. Niederreiter and C. P. Xing, *Rational Points on Curves over Finite Fields: Theory and Applications,* Cambridge University Press, LMS 285, 2001. 96
[23] A. Perrig. The BiBa one-time signature and broadcast authentication. *Eighth ACM Conference on Computer and Communication Security*, ACM, 2001, 28-37. 89
[24] M. O. Rabin. Digitalized signatures, *Foundations of Secure Communication*, Academic Press, 1978, 155-168. 88
[25] L. Reyzin and N Reyzin. Better than BiBa: Short one -time signatures with fast signing and verifying. *Information Security and Privacy (ACISP02)*, LNCS 2384, 144-153. 89, 90, 91
[26] R. Rivest and A. Shamir. PayWord and MicroMint: two simple micro payment schemes, *Tech. Rep.,* MIT Lab. for Computer Science, 1996. 97
[27] P. Rohatgi. A compact and fast hybrid signature scheme for multicast packet authentication, *6th ACM conference on Computer and Communication Security*, 1999, 93-100. 89
[28] H. Stichtenoth. *Algebraic function fields and codes*, Berlin: Springer 1993. 96
[29] D. R. Stinson. Cryptography: theory and practice, CRC Press, 1995. 90
[30] D. R. Stinson, R. Wei and L. Zhu. Some new bounds for cover-free families, *Journal of Combinatorial Theory, A*, **90**(2000), 224-234. 89, 93, 97