Scientific and Practical Cyber Security Journal (SPCSJ) 1(2):56-60
Scientific Cyber Security Association (SCSA), 2017 ISSN: 2587-4667

ON DIGITAL SIGNATURE SCHEMES

[1]N. Inassaridze, [2]M. Joglidze

[1] A.Razmadze Mathematical Institute of Tbilisi State University, Tamarashvili Str. 6, Tbilisi 0177, Georgia & Georgian Technical University & Tbilisi Centre for Mathematical Sciences
[2]University of Georgia, Kostava Str.77a, Tbilisi 0171, Georgia

ABSTRACT.

Digital signature schemes are fundamental cryptographic primitives, useful as a stand-alone application, and as a building block in the design of secure protocols and other cryptographic objects. In this article, we give general overview of basic notions of digital signature schemes and discuss the multiple-time digital signature scheme given in [8].

1. INTRODUCTION. Nowadays digital signatures have become a key technology for making the Internet and other IT-infrastructures secure. Instead of outdated traditional physical signatures, digital signatures are turning more important tools to implement secure and correct signs. Providing authenticity, integrity, and non-repudiation of data, digital signatures are widely used in identification and authentication protocols. Hence, the existence of secure signature algorithms is crucial for maintaining IT-security. The digital signature algorithms that are used in practice today are RSA [11], DSA [2], and ECDSA [5]. They are not quantum immune since their security relies on the difficulty of factoring large composite integers and computing discrete logarithms.

Hash-based digital signature schemes offer a very promising alternative to RSA and elliptic curve signature schemes, which were invented by Ralph Merkle [7]. Merkle started from fundamental, one-time signature schemes from [6]. One-time signature schemes proposed by Lamport-Diffie [6] and Rabin [9] were among the earliest signatures based on the idea of committing to private keys by one-way functions (see Rompel [12]). A severe disadvantage of these schemes is that one key-pair can only be used to sign and verify a single document, hence they are inadequate for most applications. By this reason multiple-time signature schemes are invented, that can be used to sign a predetermined number of messages [7, 8].

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, and typically are constructed based on an arbitrary one-way function without requiring a trapdoor function.

This article is an expository article about digital signature schemes, while particular attention is paid to multiple-time signature schemes. In Section 2 we discuss the basic notions of digital signature schemes. In Section 3 we draw attention to the multiple-time digital signature scheme HORS++ from [7], which will be the subject of our further investigation and an important component in the construction of a new hybrid multi-time post-quantum signature scheme.

2. FUNDAMENTAL NOTIONS. In this section we discuss digital signature schemes in general manner and recollect their basic fundamental notions (see e.g. [4]). Dealing with digital signatures one should know the following three basic aspects:

(1) The essence of a digital signature scheme;
(2) The types of attacks the adversary is able to mount against a digital signature scheme;
(3) The meaning of "breaking" a digital signature scheme.

2.1. Digital signature schemes. A digital signature schemes in its standard form consists of the following parts:

- A security parameter k, which is chosen by the user when he creates his public and secret keys. This parameter determines a number of quantities (length of signatures, running time of the signing algorithm, length of signable messages, etc).
- A message space M, which is the set of messages to which the signature algorithm may be applied, is assumed to consist of binary strings, i.e. $M \subseteq \{0,1\}^*$. To ensure that the entire signing process is polynomial in the security parameter, the length of the messages is supposed to be bounded by k^c, for some constant $c > 0$.
- A signature bound B, which is an integer bounding the total number of signatures that can be produced with an instance of the signature scheme. This value may be infinite, though it is typically bounded above by a low-degree polynomial in k.
- A key generation algorithm G, which any user can use on input 1^k to generate in polynomial time a pair (K_{priv}, K_{pub}) of matching private, sometimes called the trap-door information, and public keys.
- A signature algorithm σ, which produces a signature $\sigma(m, K_{priv})$ for a message $m \in M$ using the private key K_{priv}. σ may receive other inputs too.
- A verification algorithm V, which tests whether S is a valid signature for a message m using the public key K_{pub}. It means, that $V(S, m, K_{pub})$ is true iff it is valid.

Any of the above algorithms may be *randomized* algorithms that make use of auxiliary random bit stream inputs. We should note that G must be a randomized algorithm, since part of its output is the secret key, which must be unpredictable to an adversary.

2.2. Types of attacks. It is distinguished two basic types of attacks to a digital signature scheme. There is an attack in which the adversary knows only the real signer's public key. This type of attack is called *key-only attack*. In another type of attack the adversary can examine some signatures corresponding to known or chosen messages before his attempt to break the scheme. This type of attack is called *message attack.*

Four kinds of message attacks are identified, divided according to how the messages whose signatures the adversary sees are chosen. Denote by A a user whose signature method is being attacked. Namely,

Known-message attack. The adversary has access to signatures for a set of t (known to him) messages $m_1,\ldots, m_t$, which are not chosen by him.

Generic chosen-message attack. The adversary can obtain valid signatures from A for a list of messages $m_1,\ldots, m_t$, chosen before he attempts to break A's signature scheme (nonadaptive attack). These messages are chosen by the enemy, but they are fixed and independent of A's public key (generic attack).

Directed chosen-message attack. This is similar to the generic chosen-message attack, except that the list of messages to be signed may be created after seeing A's public key but before any signatures are seen. This attack is directed against a particular user A but is still nonadaptive.

Adaptive chosen-message attack. The adversary can request from *A* signatures of messages that depend not only on public key but that depend additionally on previously obtained signatures.

2.3. "Breaking" of a digital signature scheme. It is said that the adversary has "broken" user *A*'s signature scheme if his attack allows him to do any of the following with a non-negligible probability:

Total break. The adversary computes *A*'s secret trap-door information.

Universal forgery. The adversary finds an efficient signing algorithm functionally equivalent to *A*'s signing algorithm, based on possibly different but equivalent trap-door information.

Selective forgery. The adversary forges a signature for a particular message chosen a priori by him.

Existential forgery. The adversary forges a signature for at least one message, which is not controlled by him, so it can be random or nonsensical.

A scheme is respectively totally breakable, universally forgeable, selectively forgeable or existentially forgeable if it is breakable in one of the above senses. Note that it is more desirable to prove that a scheme is not even existentially forgeable than to prove that it is not totally breakable.

3. MULTIPLE-TIME DIGITAL SIGNATURE SCHEME. In this section we discuss the digital signature scheme of Pieprzyk, Wang and Xing [8], called HORS++, and generalizing the one-time signature scheme previously proposed by Reyzin and Reyzin [10]. The HORS++ scheme can be used to sign predetermined number of messages. To construct the scheme, a well-known combinatorial object, called the cover-free family is used, which is introduced by Erdös et al [3]. Let *[t]* denote the set of first *t* natural numbers, *{1,2,..., t}*.

Definition. A pair of sets *([t], B)* with $B = \{B_i \subseteq [t] \mid i = 1, \dots, n\}$ is called an (n, t, r)-cover-free family if for any subset $\Delta \subseteq \{1,\dots n\}$ with $|\Delta| = r$ and any $i \notin \Delta$,

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

Now suppose that *([t], B)* is an *(n, t, r)*-cover-free family and $g:\{0,1\}^* \longrightarrow \{0,1\}^b$ a cryptographic hash function with $2^b \leq n$. Suppose also that $S: \{0, 1\}^b \longrightarrow B$ is an injective mapping and $f:\{0,1\}^l \longrightarrow \{0,1\}^l$ a one-way function operating on *l*-bit strings, for a security parameter. The HORS++ scheme works as follows.

Key generation. For the given security parameter 1^l, the private key of the scheme k_{priv} consists of random *t* bit strings of length *l*

$k_{priv} = (s_1, \dots, s_t)$.

Then the public key of the scheme is

$k_{pub} = (v_1, \dots, v_t)$,

where any $v_i = f(s_i)$, $i \in [t]$.

Signature generation. A message $m \in \{0,1\}^*$ is signed using the pivate key k_{priv}. At first the message digest $g(m) \in \{0,1\}^b$ of *m* is computed. Next the mapping S is used to compute $S(m) = \{i_1, \dots, i_k\} \in B$. Then the signature of the scheme is $(s_{i_1}, \dots, s_{i_k})$.

Signature verification. To verify a signature $(s'_1, \ldots, s'_k)$ on a message m, again it is calculated $S(m) = \{i_1, \ldots, i_k\} \in B$. Finally, it is checked whether
$(f(s'_1), \ldots, f(s'_k)) = (v_{i_1}, \ldots, v_{i_k})$.

As we already mentioned, the HORS++ scheme generalizes the one-time signature scheme proposed by Reyzin and Reyzin in [10], if $n = \binom{t}{k} \geq 2^b$ for some integer $k > 0$, $r = 1$ and (n, t, r)-cover-free family B is the set of all k-subsets of [t]. Note also that the scheme of Reyzin and Reyzin is a simple generalization of that given by Bos and Chaum [1], if $t=2k$. The scheme of Bos and Chaum is in turn a generalization of the scheme of Lamport and Diffie [18], if $b = k$ and the mapping S is given by the algorithm: for any bit string $m = (m_1, \ldots, m_k)$ of length k, compute $S(m)$ as $\{1+m_1, \ldots, 2k-1+m_k\}$.

Security. Suppose that the adversary has seen r valid signatures for the messages $m_1, \ldots, m_r$ 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 $S(m_{r+1}) \setminus \bigcup_{i=1}^{r} S(m_i)$ in the public key. Since $([t], B)$ is an (n, t, r)- cover-free family, it yields that $|S(m_{r+1}) \setminus \bigcup_{i=1}^{r} S(m_i)| \geq 1$. 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.

Efficiency. To measure the efficiency of the scheme, it is considered 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 B. Thus, the performance of the HORS++ scheme is determined by the parameters of the underlying cover-free family. One has the following

Theorem [8]. 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 $O(r^2 f_l l)$-bits, public key size $O(r^2 f_l^2)$-bits, and with the size of signature $O(r f_l l)$.

However, without taking into account the complexity of the mapping S, this theorem has only theoretical interest of its existence. Implementation of the mapping S is the most time consuming part of the system. To make the given HORS++ scheme practical, in [8] some algorithms of the mapping S are proposed based on polynomials, error correcting codes and algebraic curves.

ACKNOWLEDGMENTS

The first author was supported by STCU-2016-08/MTCU 6321 and by the Agencia Estatal de Investigacííon, Spain (European ERDF support included, UE) grant number MTM2016-79661-P.

REFERENCES

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

[2] T.ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, Advances in Cryptology – CRYPTO '84, LNCS 196, Springer (1985), 10-18.

[3] 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.

[4] S.Goldwasser, S.Micali and R.Rivest, A digital signature scheme secure against adaptive chosen-message attacks, SIAM J. Comput. 17(2) (1988), 281-308.

[5] D.Johnson and A.Menezes, The elliptic curve digital signature algorithm (ECDSA), Technical Report CORR 99-34, University of Waterloo, 1999. Available at http://www.cacr.math.uwaterloo.ca.

[6] L.Lamport, Constructing digital signatures from a one way function, Technical Report SRI-CSL-98, SRI International Computer Science Laboratory, 1979.

[7] R.C.Merkle, A certified digital signature. Advances in Cryptology – CRYPTO '89 Proceedings, LNCS 435, Springer (1989), 218-238.

[8] J.Pieprzyk, H.Wang and C.Xing, Multiple-time signature schemes against adaptive Chosen Message Attacks, In: Matsui, M., Zuccherato, R. (eds.) SAC 2003. LNCS 3006 (2004), 88-100.

[9] M.O.Rabin. Digitalized signatures, Foundations of Secure Communication, Academic Press (1978), 155-168.

[10] 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.

[11] R.L.Rivest, A.Shamir and L.Adleman, A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM, 21(2) (1978), 20-126.

[12] J.Rompel, One-way functions are necessary and sufficient for secure signatures, Proceedings of ACM STOC'90 (1990), 387-394.