Supporting Non-membership Proofs with Bilinear-map Accumulators

Ivan Damgård [*] Nikos Triandopoulos [†]
University of Aarhus Boston University
Denmark USA

December 20, 2008

Abstract

In this short note, we present an extension of Nguyen's bilinear-map based accumulator scheme [8] to support *non-membership witnesses* and corresponding *non-membership proofs*, i.e., cryptographic proofs that an element has not been accumulated to a given set. This complements the non-membership proofs developed by Li *et al.* [7] for the RSA accumulator [2, 3, 5], making the functionality of the bilinear-map accumulator equivalent to that of the RSA accumulator. Our non-membership extension of Nguyen's scheme [8] makes use of the q-Strong Diffie-Hellman assumption the security of the original scheme is based on.

1 Introduction

Dynamic accumulators are cryptographic authentication primitives for optimally verifying set-membership relations. Given a set X of elements, an accumulator can be used to compute an *accumulation value*, a short (namely, of constant size) secure description $A(X)$ of X, subject to which there exist short (namely, of constant size) *witnesses* for any element in X that has been "accumulated" to $A(X)$. Each element-specific witness can be used to provide an efficient (namely, of constant verification time) cryptographic proof that the corresponding element is a member of X. Element insertions in or deletions from set X result in corresponding updates on the accumulation values and the element witnesses.

Accumulators were first introduced by Benaloh and de Mare [3], and were later further studied and extended by Baric and Pfitzmann [2]. Both constructions were based on the RSA exponentiation function and proved secure under the *strong RSA* assumption. Camenisch and Lysyanskaya [5] further advanced the RSA accumulator by introduced dynamic extensions, as well as privacy-preserving membership proofs. Consequently, many extensions of the RSA accumulator have been proposed, including accumulation of composite integers [11], bounded number of accumulated elements [1], set-up without trapdoor [10], and, finally, *non-membership witnesses and corresponding non-membership proofs*, introduced by Li *et al.* [7]. Non-membership witnesses extend the functionality of accumulators by supporting cryptographic proofs that a given element is not a member of the set, that is, it was never accumulated to the current set. Finally, works improving on the efficiency of the RSA accumulator include [6, 9].

[*]Dept. of Computer Science, University of Aarhus, Aarhus, DK 8200, Denmark. Email: `ivan@cs.au.dk`.

[†]Dept. of Computer Science, Boston University, Boston, MA 02215, USA. Email: `nikos@cs.bu.edu`. This research was performed while the author was at University of Aarhus, Denmark.

The first alternative construction of a dynamic accumulator (beyond the one based on RSA) is due to Nguyen [8]. This scheme is based on bilinear pairings and the construction is proven secure under the q-*strong Diffie-Hellman* assumption [4] on general groups. We refer to this accumulator scheme as *bilinear-map accumulator*. Recently a new construction based on *Paillier's encryption* system has been proposed that additionally offers batch element updates [12].

In this short note, we describe an extension of Nguyen's bilinear-map accumulator scheme to support *non-membership witnesses and non-membership proofs* and prove the security of this extended scheme.

2 Non-Membership Verification for Bilinear-map Accumulators

We first present some necessary preliminaries related to the underlying computational hardness assumption our non-membership extension (and also the original scheme by Nguyen [8]) is based on. We then build on Nguyen's original accumulator scheme to define the new non-membership witnesses, describe their corresponding verification test and finally prove their security.

2.1 The q-strong Diffie-Hellman Assumption

We first present the q-strong DH assumption [4] over general groups, which has been used in many contexts.

Definition 2.1 (q-Strong Diffie-Hellman Assumption.) *Let $G =< g >$ be a cyclic group of prime order p and $\kappa \in \mathbb{Z}_p^*$. Under the q-*strong Diffie-Hellman assumption*, any probabilistic polynomial-time algorithm A that is given set $\{g^{\kappa^i} : 0 \leq i \leq q\}$, finds a pair $(x, g^{\frac{1}{x+\kappa}}) \in \mathbb{Z}_p^* \times G$ with at most $O(1/p)$ probability, where the probability is over the random choice of $\kappa \in \mathbb{Z}_p^*$ and the random bits chosen by A.*

In the sequel, whenever operating on group elements in G of prime order p, we always make use of the fact that $g^x = g^{x \mod p}, x \in \mathbb{Z}$; i.e., all operations in the exponent can be reduced modulo the group order p.

2.2 Accumulators Based on Bilinear Maps

We now present Nguyen's scheme and appropriately extend it to support non-membership proofs.

Given the security parameter λ, let G be a multiplicative cyclic group of prime order p that is generated by g, where p grows exponentially with λ.[1] Additionally, group G is chosen such that it supports a (non-degenerate) bilinear pairing to a target cyclic group G_T of prime order p. That is, if G is generated by element g, then there exists a bilinear, non-trivial, map $e : G \times G \to G_T$ from pairs of elements in G to elements of target group G_T, such that for any two integers a, b it holds that $e(g^a, g^b) = e(g, g)^{ab}$ and where, additionally, element $e(g, g) \in G_T$ generates G_T.

Let $A_\kappa : 2^{\mathbb{Z}_p^*} \to G$ be an accumulation function that is parameterized by $\kappa \in \mathbb{Z}_p^*$ and maps sets X of integers in $\mathbb{Z}_p^*$ to elements in G according to the mapping

$$A_\kappa(X) = g^{\prod_{x \in X}(x+\kappa)} .$$

This has been the accumulation function used by Nguyen in [8] to construct the first accumulator scheme that is not based on the RSA exponentiation function. In Nguyen's construction, κ is the trapdoor information and set $\{g^{\kappa^i} | 0 \leq i \leq q\}$ is the public key, q in an upper bound on $|X| = n$ that grows polynomially with

[1]The security parameter can be equal to the bit-length of either a group element or an exponent in the group (integers modulo p).

the security parameter $\lambda = O(\log p)$. Seen as a polynomial on κ of degree $|X| = n$, let $f_X(\kappa)$ denote the product in the exponent of $A_\kappa(X)$, that is,

$$f_X(\kappa) \triangleq \prod_{x \in X} (x + \kappa) \ .$$

As in [8], for any $x \in X$, we define the *membership witness* $w_x \in G$ of x with respect to accumulation value $A_\kappa(X)$ to be the value w_x satisfying the *membership verification test*

$$w_x^{(x+\kappa)} = A_\kappa(X) \ , \tag{1}$$

which, using the bilinear map $e(\cdot,\cdot)$ and the publicly known group element $h = g^\kappa$, is realized in practice as

$$e(w_x, g^x \cdot h) = e(A_\kappa(X), g) \ . \tag{2}$$

That is, any member x of set X has a *unique* corresponding membership witness $w_x \triangleq g^{\frac{f_X(\kappa)}{x+\kappa}} = g^{q_{X,x}(\kappa)}$ (since $(x+\kappa)|f_X(\kappa)$), for some polynomial $q_{X,x}(\kappa)$ of degree $n-1$ that is uniquely defined by set $X - x$.

2.3 Non-membership Verification for Accumulators Based on Bilinear Maps

Inspired by the non-membership test proposed by Li *et al.* in [7] for the RSA accumulator, we introduce *non-membership witnesses* for the accumulation function $A_\kappa(\cdot)$. For any $y \notin X$, the *non-membership witness* $\hat{w}_y$ of y with respect to $A_\kappa(X)$ is a pair of values $(w_y, u_y) \in G \times \mathbb{Z}_p^*$, subject to the requirements (i) $u_y \neq 0$ and (ii) $(y+\kappa)|[f_X(\kappa) + u_y]$, additionally satisfying the *non-membership verification test*

$$w_y^{(y+\kappa)} = A_\kappa(X) \cdot g^{u_y} \ , \tag{3}$$

which, using the bilinear map $e(\cdot,\cdot)$ and the publicly known group element $h = g^\kappa$, is realized in practice as

$$e(w_y, g^y \cdot h) = e(A_\kappa(X) \cdot g^{u_y}, g) \ . \tag{4}$$

In particular, any non-member y of set X has a *unique* corresponding non-membership witness $\hat{w}_y = (w_y, u_y)$, by setting

$$u_y \triangleq -f_X(-y) \mod p = -\prod_{x \in X} (x - y) \mod p \ , \tag{5}$$

and then accordingly setting

$$w_y = g^{\frac{f_X(\kappa) - f_X(-y)}{y+\kappa}} = g^{\hat{q}_X(\kappa)} \ , \tag{6}$$

for some polynomial $\hat{q}_X(\kappa)$ of degree $n-1$ that is uniquely defined by set X. Note that, since $y \notin X$, it holds that $u_y \neq 0$. Also note that, if $h_X(\kappa) = f_X(\kappa) - f_X(-y)$, then $h_X(-y) = 0$, thus it holds that $(y+\kappa)|h_X(\kappa)$ (thus, justifying the last part of Equation 6) and, in fact, that $(y+\kappa)|[f_X(\kappa) + u_y]$. Thus, in addition to Equations 3 and 4, the pair of values (w_y, u_y) defined above satisfies the required conditions $u_y \neq 0$ and $(y+\kappa)|[f_X(\kappa) + u_y]$. We require that the verification process immediately rejects if $u_y = 0$.

Also, observe that the non-membership witness for $y \notin X$ can be computed efficiently (in polynomial in $|X|$ time), using only set X and the public key, by evaluating polynomial $-f_X(\kappa)$ on $-y$ and then computing the group element w_y through Equation 6.

We say that a membership, respectively non-membership, witness w_x, respectively $\hat{w}_y = (w_y, u_y)$, is *fake* if $x \notin X$, respectively $y \in X$, and, still, the corresponding membership. respectively non-membership, verification test (in particular, expressed through Equations 1 and 3 respectively) is satisfied.

The security of non-membership test relies on the following: if y is in X then $y + \kappa$ divides polynomial $f_X(\kappa)$, and therefore $y + \kappa$ cannot divide polynomial $f_X(\kappa) + u_y$ for any choice of $u_y \neq 0$. (Recall that the verifier first checks whether $u_y \neq 0$, according to the definition of non-membership witnesses.) Based on the fact that $(y + \kappa) \nmid [f_X(\kappa) + u_y]$, one can easily reduce any fake non-membership witness to an attack to the q-Strong DH assumption, using a simple polynomial division and the public key. For completeness we present the security proof for both membership and non-membership witnesses.

Lemma 1 *Under the q-Strong Diffie-Hellman assumption, any PPT algorithm B, given any set X, $|X| \leq q$ and set $\{g^{\kappa^i} | 0 \leq i \leq q\}$, finds a fake non-membership witness of a member of X or a fake membership witness of a non-member of X with respect to $A_\kappa(X)$ with probability at most $O(1/p)$, measured over the random choice of $\kappa \in \mathbb{Z}_p^*$ and random bits of B.*

Proof: Consider the case of membership witnesses first. Suppose that there exists PPT algorithm B that with non-negligible probability outputs a fake membership witness w_x for $x \notin X$ with respect to $A_\kappa(X)$. Then, $w_x^{x+\kappa} = A_\kappa(X) = g^{f_X(\kappa)}$, where $f_X(\kappa) = \sum_{i=0}^{|X|} c_i \cdot \kappa^i$, with c_i being a known coefficient that depends on the elements of X, $0 \leq i \leq |X|$. Since $x \notin X$, it is $(x + \kappa) \nmid f_X(\kappa)$. Thus, using polynomial division and given X, x, one can compute a non zero integer c and a polynomial $q(\kappa)$ of degree $|X| - 1$ such that $f_X(\kappa) = c + q(\kappa) \cdot (x + \kappa)$. Therefore, $w_x = g^{q(\kappa)} \cdot g^{\frac{c}{x+\kappa}}$ and $g^{\frac{1}{x+\kappa}} = [w_x \cdot [g^{q(\kappa)}]^{-1}]^{c^{-1}}$, computed efficiently using the public key, which contradicts the q-strong DH assumption.

The case of non-membership witnesses is very similar. Indeed, suppose that there exists PPT algorithm B that with non-negligible probability outputs a fake non-membership witness $\hat{w}_y = (w_y, u_y)$, $u_y \neq 0$, for $y \in X$ with respect to $A_\kappa(X)$. Then, $w_y^{y+\kappa} = g^{f_X(\kappa)+u_y}$. Since $y \in X$, $(y + \kappa) | f_X(\kappa)$, so $(y + \kappa) \nmid [f_X(\kappa) + u_y]$ for any $u_y \neq 0$. Thus, as before, using polynomial division and given u_y, X, y, one can express $f_X(\kappa) + u_y$ as $c + q(\kappa) \cdot (y + \kappa)$ for some non zero c and some polynomial $q(\kappa)$. This again allows the efficient computation of $g^{\frac{1}{y+\kappa}}$, contradicting the q-strong DH assumption.

Note that both reduction arguments can be extended to the case where fake witnesses are defined with respect to the verification tests of Equations 2 and 4. In this case, knowledge of fake witnesses satisfying equations $e(w_x, g)^{x+\kappa} = e(g, g)^{f_X(\kappa)}$ and $e(w_y, g)^{y+\kappa} = e(g, g)^{f_X(\kappa)+u_y}$, implies knowledge of w_x and (w_y, u_y) that correspondingly satisfy $w_x^{x+\kappa} = g^{f_X(\kappa)}$ and $w_y^{y+\kappa} = g^{f_X(\kappa)+u_y}$. $\square$

Therefore, we have a new secure non-membership verification test for the accumulation function $A_\kappa(\cdot)$.

Theorem 1 (Non-membership witnesses.) *Under the q-Strong Diffie-Hellman assumption, for any non-member of set X there exists a unique non-membership witness with respect to the accumulation value $A_\kappa(X)$ and a corresponding efficient and secure non-membership verification test.*

3 Conclusion

In this short note, we extend the accumulator scheme that is based on bilinear pairings, which was introduced by Nguyen in [8], to also support non-membership witnesses and corresponding cryptographic proofs of non-membership in a given set. That is, given the (authentic) accumulation value of a set X, the public key, and a corresponding short (of size that is independent of the size of X) non-membership witness, a verifier can efficiently (in time independent of the size of X) verify that a given element y is not a member of X, i.e., $y \notin X$. The security of this new non-membership verification test is proved using the q-strong Diffie-Hellman assumption on general groups, the exact cryptographic assumption the original scheme [8] by Nguyen is based on. Similar to the non-membership extension of the RSA accumulator (see, e.g., [2, 3, 5]) that was proposed by Li *et al.* in [7], this non-membership extension enriches the functionality of the bilinear-map accumulator [8] and widens its usability in real-life security applications.

Acknowledgments

We thank Melissa Chase for useful discussions related to the topic of this short paper.

References

[1] M. H. Au, Q. Wu, W. Susilo, and Y. Mu. Compact e-cash from bounded accumulator. In *Proceedings of CT-RSA '07*, pages 178–195, 2007.

[2] N. Barić and B. Pfitzmann. Collision-free accumulators and fail-stop signature schemes without trees. In *Proceeding of EUROCRYPT '97*, pages 480–494, 1997.

[3] J. Benaloh and M. de Mare. One-way accumulators: A decentralized alternative to digital signatures. In *Proceeding of EUROCRYPT '93*, pages 274–285, 1994.

[4] D. Boneh, X. Boyen, and H. Shacham. Short group signatures. In *Proceedings of Crypto '04*, pages 41–55, 2004.

[5] J. Camenisch and A. Lysyanskaya. Dynamic accumulators and application to efficient revocation of anonymous credentials. In *Proceedings of CRYPTO '02*, pages 61–76, 2002.

[6] M. T. Goodrich, R. Tamassia, and J. Hasic. An efficient dynamic and distributed cryptographic accumulator. In *Proceeding of Information Security Conference (ISC)*, pages 372–388, 2002.

[7] J. Li, N. Li, , and R. Xue. Universal accumulators with efficient non-membership proofs. In *Proceedings of Conference on Applied Cryptography and Network Security (ACNS)*, pages 253–269, 2007.

[8] L. Nguyen. Accumulators from bilinear pairings and applications. In *Proceedings of CT-RSA '05*, pages 275–292, 2005.

[9] C. Papamanthou, R. Tamassia, and N. Triandopoulos. Authenticated hash tables. In *Proceedings of ACM Conference on Computer and Communications Security (CCS)*, pages 437–448, October 2008.

[10] T. Sander. Efficient accumulators without trapdoor extended abstracts. In *Proceedings of International Conference on Information and Communication Security*, pages 252–262, 1999.

[11] G. Tsudik and S. Xu. Accumulating composites and improved group signing. In *Proceedings of ASIACRYPT '03*, pages 269–286, 2003.

[12] P. Wang, H. Wang, and J. Pieprzyk. A new dynamic accumulator for batch updates. In *Proceedings of ICICS '07*, pages 98–112, 2007.