Comments on "On the security of XCBC, TMAC and OMAC" by Mitchell

Tetsu Iwata

Department of Computer and Information Sciences,
Ibaraki University
4–12–1 Nakanarusawa, Hitachi, Ibaraki 316-8511, Japan
iwata@cis.ibaraki.ac.jp

September 19, 2003

Abstract. In August 2003, Mitchell published a note "On the security of XCBC, TMAC and OMAC" [8]. We have already pointed out that some of the claims in [8] are incorrect [7], in this note, we further point out limitations of the above note. Our main observations are:

- All of the analysis in [8] are within our security bound, and therefore, it does *not* break the security bound of OMAC,
- The birthday bound is the security for *all* of XCBC, TMAC, OMAC, and EMAC. Security is not what distinguishes these MACs,
- "Significant weakness" in OMAC as claimed in [8] is not significant.

1 Background

OMAC is a variant of CBC MAC to achieve authenticity. OMAC uses modern cryptography (reduction-based proof) in order to establish its security. The efficiency of OMAC is highly optimized. It is almost as efficient as the basic CBC MAC.

In August 2003, Mitchell published a note "On the security of XCBC, TMAC and OMAC" [8]. We have already pointed out that some of the claims in [8] are incorrect [7], in this note, we further point out limitations of the above note. Our main observations are:

- All of the analysis in [8] are within our security bound, and therefore, it does *not* break the security bound of OMAC,
- The birthday bound is the security for *all* of XCBC, TMAC, OMAC, and EMAC. Security is not what distinguishes these MACs,
- "Significant weakness" in OMAC as claimed in [8] is not significant.

2 Does [8] Break Our Security Bound?

After the development of reduction-based provable security paradigm, the best way to guarantee the security of block cipher modes of operation is to prove

its security. When proving the security, there will be bounds, which tell you how good is the proven security. The actual security might be better than the proven security bounds suggest, but it cannot be worse. One should always be pessimistic and assume that the actual security is no better than the proven security.

In case of OMAC, the bound works as follows. Suppose that an adversary obtains q messages of at most σ blocks in total and their MACs. For ease of explanation, suppose that there are essentially no defects in the underlying block cipher. Then OMAC's security theorem [6, Theorem 3.1] tells us that the adversary won't be able to forge a new message-tag pair with success probability exceeding

$$\frac{4\sigma^2 + 1}{2^n} \ , \tag{1}$$

where n denotes the block length of the underlying block cipher in bits.

Now the contribution of Mitchell [8] is to point out that formula (1) is nearly tight: There *is* an adversary that does almost as well in breaking authenticity as formula (1) allows.

OMAC admits attacks that nearly match our security bound. This fact is well-known to the authors of OMAC. In fact, it is obvious to anyone who has thought seriously about our construction and proofs. We know how our proof goes wrong if we reach the birthday bound. Also, Black and Rogaway have already remarked that there is a simple forgery attack against XCBC after $q \approx 2^{n/2}$ messages [2]. We know the same forgery attack can be applied to OMAC. In this aspect, Mitchell's note is very similar to Ferguson's note against OCB mode [3]. Ferguson shows some attack against OCB mode, which seems to be trivial and well-known (One difference between these two notes is that Ferguson clearly remarks that his attack does not violate the security bound on OCB mode, while Mitchell completely ignores the security bound of OMAC).

In [4, 6], we did not show the attack achieving advantage $\Omega(\sigma^2/2^n)$, because every standard mode of operation (including XCBC, TMAC, OMAC, EMAC, other MACs, encryption modes, and authenticated encryption modes) has been susceptible to attacks of this (in)security. It is what everyone expects. And the whole point of provable security is to not have to look at attacks like this in order to know how secure is your construction.

If you are attacking some block cipher mode of operation with reduction-based proof whose security bound is $O(\sigma^2/2^n)$, and you have found the attack using $q \approx 2^{n/2}$ messages, then the result is *well-known* to those who have done their elaborate security proofs. Such results are within the security bound $O(\sigma^2/2^n)$, and simply saying the security bound is tight when $q \approx \sigma$.

We stress that all of the analysis by Mitchell in [8] are trivial, expected, and within our security bound. He does *not* break the security bound of OMAC.

3 Does [8] Show Partial Key Recovery Attacks Against OMAC?

In [8, p. 2, ℓ. 3], *a partial key recovery attack* is defined as follows.

Definition 3.1 (Partial Key Recovery Attacks [8]). *An attacker is able to obtain part of the secret key.*

We review what is a key for OMAC, and what is the goal of partial key recovery attacks against OMAC. OMAC is a function with a signature $\mathrm{OMAC} : \{0,1\}^k \times \{0,1\}^* \to \{0,1\}^\tau$, where k denotes the key length of the underlying block cipher, τ is a tag length which is at most n bits, and n denotes the block length of the underlying block cipher. That is, the key space of OMAC is $\{0,1\}^k$, and $L = E_K(0^n)$ is not part of a key. This is clearly mentioned in the specification of OMAC [4]. To quote:

- ... in OMAC, L is not a part of the key and is generated from K [4, p. 3, ℓ. -9].

Here is another quote from the same document:

- The key space $\mathcal{K}$ of OMAC-family is $\mathcal{K} = \mathcal{K}_E$. It takes a key $K \in \mathcal{K}_E$ and a message $M \in \{0,1\}^*$, and returns a string in $\{0,1\}^n$ [4, p. 7, Sect. 3].

$\mathcal{K}_E$ denotes the key space of the underlying block cipher. That is, if the key length of the underlying block cipher is k bits, then $\mathcal{K}_E = \{0,1\}^k$.

Therefore, the goal of the partial key recovery attack against OMAC is to recover part of the underlying block cipher key.

Now [8, p. 9, Sect. 5.3] claims the partial key recovery attack against OMAC to determine $L = E_K(0^n)$. We have already argued that this is not the goal of the attack. Therefore, Mitchell [8] does *not* show the partial key recovery attack against OMAC.

Now suppose *erroneously* that L is part of the OMAC key, and there is a partial key recovery attack against OMAC as claimed in [8, p. 13, Table. 5].

Mitchell's attacks are based on the fact that there is a collision after $q \approx 2^{n/2}$ messages. This "just waiting for a collision" technique is used for both a forgery attack and a partial key recovery attack against OMAC. That is, from a technical view point, there is no significant difference between these two attacks. It seems that Mitchell gives two different attack names for this "just waiting for a collision" technique (at least for OMAC).

4 The Birthday Bound Is the Security for *all* of XCBC, TMAC, OMAC, and EMAC

We have already argued in [6] that the security bounds for XCBC, TMAC, OMAC, and EMAC are almost the same, and there is no significant difference

among them from a security viewpoint. Indeed, the security bounds of XCBC, TMAC, OMAC, and EMAC are $O(\sigma^2/2^n)$, and attacks exist for all of these MACs after $q \approx 2^{n/2}$ messages.

Nevertheless, if you consider one of these MACs is more secure than some others, then you are probably too optimistic, since you are expecting more than the security bound tells you.

5 What Is "Significant Weakness" in OMAC?

Mitchell claims that there is some "significant weakness" in OMAC [8, Sect. 7, ℓ. 4]. It is not clear what does the significant weakness means, it seems that this means the partial key recovery attack against OMAC (since we do not see significant differences in [8, p. 13, Table 3] and [8, p. 14, Table 4]). We have already argued that Mitchell does not really show the partial key recovery attack against OMAC. Also, even if we *erroneously* assume that L is part of the OMAC key, and there is a partial key recovery attack against OMAC, it is only possible after reaching the birthday bound. After all, partial key recovery attacks against OMAC is useless if we change the secret key before reaching the birthday bound. But this is not a new restriction, and this is the same for all other MACs (and for all other popular block cipher modes).

The only important thing to use OMAC is to make sure that you change your secret key before reaching the birthday bound (that is, $\sigma \ll 2^{n/2}$). This is the same for XCBC, TMAC, and EMAC. Then, for all of these four MACs, it is *impossible* to make a forgery except for a negligible probability.

Nevertheless, if you consider the attack after reaching the birthday bound is serious and a significant weakness, then block ciphers are probably not good for your purpose. When you reach the birthday bound, all popular block cipher encryption modes, which would be used with MACs, begin to leak information about your valuable plaintext [1].

6 Conclusion

Mitchell claimed that OMAC should not be adopted in the current form [8, p. 14, ℓ. 1–2], since there is a "significant weakness" in OMAC. But his "significant weakness" comes after reaching the birthday bound. Also, in a separate note [7], we have shown that his alternative to OMAC cannot achieve provable security.

Authors of OMAC welcome your trials of attacking OMAC. But note that you are attacking the provably secure algorithm, and don't forget to remark "our analysis is within the security bound of OMAC, and does not violate the security claims by the authors of OMAC."

Finally, we stress that Mitchell's claims in [8] are not important, since:

- It does not give any information except for trivial and expected attacks,
- it does not break the security bound of OMAC,
- it does not find any "significant weakness" in OMAC, and

– it proposes a wrong alternative.

NIST announced that OMAC1 will be specified as the recommendation for block cipher modes of operation. There is no reason to change this decision.

References

1. M. Bellare, A. Desai, E. Jokipii, and P. Rogaway. A concrete security treatment of symmetric encryption. Proceedings of *the 38th Annual Symposium on Foundations of Computer Science, FOCS '97,* pp. 394–405, IEEE, 1997.
2. J. Black and P. Rogaway. CBC MACs for arbitrary-length messages: The three key constructions. *Advances in Cryptology — CRYPTO 2000, LNCS 1880,* pp. 197–215, Springer-Verlag, 2000.
3. N. Ferguson. Collision attacks on OCB. Comments to NIST, February 11, 2002. Available from NIST's web page at `http://csrc.nist.gov/CryptoToolkit/modes/`.
4. T. Iwata and K. Kurosawa. OMAC: One-Key CBC MAC. NIST submission, December 20, 2002. Available from NIST's web page at `http://csrc.nist.gov/CryptoToolkit/modes/`.
5. T. Iwata and K. Kurosawa. OMAC: One-Key CBC MAC. Pre-proceedings of *Fast Software Encryption, FSE 2003,* pp. 137–162, 2003. To appear in *LNCS,* Springer-Verlag. See `http://crypt.cis.ibaraki.ac.jp/`.
6. T. Iwata and K. Kurosawa. Stronger security bounds for OMAC, TMAC and XCBC. Comments to NIST, April 30, 2003. Available from NIST's web page at `http://csrc.nist.gov/CryptoToolkit/modes/`.
7. T. Iwata and K. Kurosawa. On the security of two new OMAC variants. Comments to NIST, September 1, 2003. Available from NIST's web page at `http://csrc.nist.gov/CryptoToolkit/modes/`.
8. C.J. Mitchell. On the security of XCBC, TMAC and OMAC. Technical Report RHUL-MA-2003-4, 19 August, 2003. Available at `http://www.rhul.ac.uk/mathematics/techreports`. Also available from NIST's web page at `http://csrc.nist.gov/CryptoToolkit/modes/comments/`.
9. P. Rogaway. Comments on NIST's RMAC proposal. Comments to NIST. Available at `http://www.cs.ucdavis.edu/~rogaway/xcbc/index.html`. Also available at `http://csrc.nist.gov/CryptoToolkit/modes/comments/`.