Tweaking Even-Mansour Ciphers
CIS 5371 - Paper Summary

Abstract

This paper takes a look at the contributions of Benot Cogliati, Rodolphe Lampe, and Yannick Seurin in their work, "Tweaking Even-Mansour Ciphers," which appeared in Crypto 2015. The version published in the Crypto 2015 conference proceedings is an abbreviated one. The full version [1], as available in the Cryptology ePrint Archive, was pulled instead in order to get a more complete view. "Tweaking Even-Mansour Ciphers" is concerned with transforming the base Even-Mansour cipher, a key-alternating cipher with one round, into a Tweakable Even-Mansour (TEM) cipher. This transformation is possible by the LRW construction presented by Liskov, Rivest, and Wagner. A chained version of this construction (CLRW) using two rounds of the Even-Mansour cipher is found to be secure beyond the birthday-bound. Proofs of security are provided in the random permutation model.

1 Background Information

Whereas a traditional block cipher provides a single permutation per key, a tweakable block cipher can provide a number of different permutations under the same key. The tweakable block cipher was first proposed by Liskov, Rivest, and Wagner in their paper, "Tweakable Block Ciphers" [3]. The so-called LRW construction presented in that paper converts a conventional block cipher into a tweakable block cipher. Given an almost XOR-universal, keyed hash function H which takes key k' and maps a tweak t from some tweak space into the set $\{0,1\}^n$ and a block cipher E which takes key k and maps from $\{0,1\}^n$ to $\{0,1\}^n$, the LRW construction is given by: $H_{k'}(t) \oplus E_k(H_{k'}(t) \oplus x)$, where $x \in \{0,1\}^n$ is the message. The LRW construction provides birthday-bound security; to improve on this, a cascading of two independent-key rounds of the LRW construction gives rise to the Chained-LRW (CLRW) construction, which may further be generalized to r rounds [2].

The necessary components to perform iterated Even-Mansour enciphering are r number of n-bit permutations $(P_1, ..., P_r)$ and r number of n-bit round keys $k_0, ..., k_r$. The ciphertext for a message $x \in \{0,1\}^n$ is given by: $k_r \oplus P_r(k_{r-1} \oplus P_{r-1}(\cdots P_2(k_1 \oplus P_1(k_0 \oplus x)) \cdots))$. Previous work in the area has shown that the two-key one-round Even-Mansour cipher is birthday-bound secure, and that so is the one-key one-round Even-Mansour cipher. Furthermore, it has been shown that increasing this to just two rounds provides beyond birthday-bound security, resistance to several types of key attacks, and indistinguishability from the behavior of an ideal cipher. An iterated two-round Even-Mansour cipher built up from two permutations P_1 and P_2 and two independent round keys k_1 and k_2 is given by: $k_2 \oplus P_2(k_2 \oplus k_1 \oplus P_1(k_1 \oplus x))$.

2 Objective

"Tweaking Even-Mansour Ciphers" attempts to provide an Even-Mansour construction with beyond birthday-bound security. To do this, the authors propose a combination of the iterated Even-Mansour cipher and the CLRW construction over two rounds. The authors build up this two-round construction based on a similar

one-round combination which only only provides birthday-bound security. The iterated Even-Mansour cipher over two rounds makes use of two permutations P_1 and P_2. The CLRW construction over two rounds makes use of an almost XOR-universal hash function H. The resulting construction is given by:

$$\mathrm{TEM}^{P_1,P_2}((k_1,k_2),t,x) = H_{k_2}(t) \oplus P_2(H_{k_2}(t) \oplus H_{k_1}(t) \oplus P_1(H_{k_1}(t) \oplus x)).$$

XOR operations with round keys have been replaced by keyed hash outputs of the tweak t under the different round keys. The authors claim this two-round construction is "secure (against adaptive chosen-plaintext and ciphertext attacks) up to approximately $2^{2n/3}$ adversarial queries" [1].

3 Impact and Significance

The Even-Mansour cipher is a lightweight block cipher that could easily find its way into mobile or embedded device environments. Modifying this block cipher to accept a tweak would further motivate its deployment in limited environments, as the expensive key changing operations can be reduced.

The proposed TEM scheme expands on prior work on both iterative Even-Mansour ciphers and the LRW construction by combining the two to produce a hybrid. Previous work established the means to ensure beyond birthday-bound security of Even-Mansour ciphers and also of the LRW construction, but not how to combine the two. The LRW construction is efficiently instantiated using Even-Mansour permutations instead of heavier encryption operations. Furthermore, adding a tweak into Even-Mansour gives it more utility out of each key.

4 Security of the Proposed TEM

Security proofs are built using the Random Permutation Model, meaning any internal permutations (P_1 and P_2 for 2-round TEM) are modeled as random permutation oracles publicly available to an adversary. The adversary is also given a "construction" oracle which takes a plaintext and provides the corresponding ciphertext. The adversary is referred to as a distinguisher; the distinguisher is tasked with distinguishing between the real and ideal worlds. In the real world, the distinguisher interacts with (TEM_k^P, P), the actual TEM and its constituent tuple of internal permutations, whereas in the ideal world, the distinguisher interacts with $(\tilde{P}_0, P)$, some uniformly random tweakable permutation and an unrelated tuple of internal permutations. Distinguishers are assumed to be computationally unbounded. Furthermore, distinguishers are expected to avoid asking pointless oracle queries for which the answers may be easily derived from previous query results.

$\mathsf{Adv}^{\mathrm{DISTING}}(\mathcal{D})$, the distinguishing advantage of a distinguisher $\mathcal{D}$, is defined as: $\mathsf{Adv}^{\mathrm{DISTING}}(\mathcal{D}) = |Pr[\mathcal{D}^{\mathrm{TEM}_k^P,P} = 1] - Pr[\mathcal{D}^{\tilde{P}_0,P} = 1]|$. The first probability is over the random choice of k, P; the second is over the random choice of $\tilde{P}_0$, P.

Both the non-adaptive chosen-plaintext attack (NCPA) advantage, $\mathsf{Adv}^{\mathrm{NCPA}}_{\mathrm{TEM}[n,r,\mathcal{H}]}(q_c, q_p)$, and the adaptive chosen-plaintext and ciphertext attack (CCA) advantage, $\mathsf{Adv}^{\mathrm{CCA}}_{\mathrm{TEM}[n,r,\mathcal{H}]}(q_c, q_p)$, is claimed to be the same $\mathsf{max}_{\mathcal{D}}\ \mathsf{Adv}(\mathcal{D})$. q_c represents the number of construction oracle queries and q_p represents the number of inner permutation oracle queries. r represents the number of rounds. For establishing tight bounds for one and two rounds, the authors focus on the CCA adversary, capable of making adaptive bidirectional queries to all its oracles.

The advantage of an adversary asking q_c construction oracle queries and q_p internal permutation queries against one-round $\mathrm{TEM}[n,1,\mathcal{H}]$ is given by: $\mathsf{Adv}^{\mathrm{CCA}}_{\mathrm{TEM}[n,1,\mathcal{H}]}(q_c, q_p) \leq q_c^2\varepsilon + \frac{2q_cq_p}{N}$. Against two rounds,

the advantage of an adversary becomes: $\mathsf{Adv}^{\mathrm{CCA}}_{\mathrm{TEM}[n,2,\mathcal{H}]}(q_c, q_p) \leq \frac{29\sqrt{q_c}q_p}{N} + \varepsilon\sqrt{q_c}q_p + 4\varepsilon q_c^{3/2} + \frac{30q_c^{3/2}}{N}$. Therefore, the 2-round TEM has a tight $2^{2n/3}$-security, which is beyond birthday-bound security.

In the proofs, the H-Coefficients technique is used. A distniguisher $\mathcal{D}$'s complete interaction with its oracles is recorded as its transcript. A queries transcript's attainability is related to the existence of ideal-world oracles such that an adversary interacting with these oracles produces the transcript. In the real world, an adversary is provided the true round keys at the end of the experiment; in the ideal world, an adversary gets some randomly chosen keys. A transcript is put together by adding the tuple of keys to the queries transcript. The proofs rely on the probability of getting a bad transcript being small in the ideal world, whereas the probability of getting good transcripts is similar in both worlds.

In the case of 1-round TEM, a bad transcript is attained if XORing the keyed hashes of two different tweaks produces the XORed value of either the produced messages or the ciphertexts, or if a construction oracle query matches an internal permutation oracle query. In the case of 2-round TEM, bad transcripts are attained if similar query collisions occur. In 1-round TEM, collisions are more likely, but in 2-round TEM, the addition of another permutation allows for randomization of the output. Hence, the likelihood of attaining a good transcript becomes similar in both the ideal and real worlds, and security beyond the birthday-bound is obtainable.

5 Open Problems

The authors bring up several open problems. Neither a tight analysis of the TEM construction for more than 2 rounds nor a tight analysis for a CLRW construction for more than 2 rounds is performed. In particular, the authors believe but leave unproven that an r-round cascaded TEM construction has the potential to provide seucirty up to $2^{\frac{rn}{r+1}}$ queries. The authors' proposed TEM scheme makes use of both different round permutations and independent round keys; they wonder about the security offered by similar schemes using the same permutations and/or non-independent round keys. Furthermore, the authors suggest that the TEM scheme could be made more efficient by switching out the necessary almost XOR-universal hash function with linear operations.

The authors built up their proofs of security based on a distinguishability experiment which I had seen for the first time. It would be interesting to explore other experiments applicable to the TEM construction and build up proofs based on those for a clearer understanding.

References

[1] Benot Cogliati, Rodolphe Lampe, and Yannick Seurin. Tweaking even-mansour ciphers. Cryptology ePrint Archive, Report 2015/539, 2015.

[2] Will Landecker, Thomas Shrimpton, and R. Seth Terashima. Tweakable blockciphers with beyond birthday-bound security. Cryptology ePrint Archive, Report 2012/450, 2012.

[3] Moses Liskov, Ronald L. Rivest, and David Wagner. *Advances in Cryptology — CRYPTO 2002: 22nd Annual International Cryptology Conference Santa Barbara, California, USA, August 18–22, 2002 Proceedings*, chapter Tweakable Block Ciphers, pages 31–46. Springer Berlin Heidelberg, Berlin, Heidelberg, 2002.