****

**111-1資訊安全**

**小組作業一：輕量化加密研究**

**Ascon**

**資訊工程學系三年級乙班**

**民國一一一年十二月二十一日**

**授課老師：王忍成　老師**

**組長：10911240　楊大為**

**組員：10911241　楊廣民**

**10911244　曾博詮**

**簡介**

Ascon 是一系列來自奧地利[格拉茨科技大學](https://www.tugraz.at/)、 [英飛凌科技](https://www.infineon.com/)、 [Lamarr Security Research](https://www.lamarr.at/)和 [Radboud 大學](https://www.ru.nl/english/)的密碼學家團隊設計用於輕量級認證加密和雜湊的演算法，該演算法已在 [CAESAR competition (2014–2019)](https://competitions.cr.yp.to/caesar-submissions.html) 中勝出並被評選為主要的輕量級加密演算法，現在正在[NIST Lightweight Cryptography competition (2019–)](https://csrc.nist.gov/projects/lightweight-cryptography/finalists) 決賽競爭中。

**功能**

Ascon 提供了帶有關聯資料的認證加密（AEAD）、雜湊與拓展輸出函式。

* Authenticated encryption

使用符號 表示加密函數、 表示解密函數，其中參數 = 金鑰長度（≤160 單位為bite）、 = 資料區塊長度（單位為bits） 、 = 排列輪數。

在加密函式中需要四個輸入 ，其 key （長度為 ，單位為bits）、 public message number （128 bits的隨機數）、 associated data（任意長度）、 plaintext（任意長度），然後加密完後會輸出 ，其authenticated ciphertext （與同長)、authentication tag（128 bits），完整函式如下表示:

在解密函式中需要五個輸入 ，其意思與加密輸入的 相同，意思與加密輸出的 相同，加密完後輸出 ，其 與加密輸入的 相同（當tag驗證成功時輸出）、error （當tag驗證失敗時輸出），完整函式如下表示:

* Hashing

使用符號 表示雜湊函數，其中參數 輸出長度限制（若 代表無限制）、 資料區塊長度（單位為bits）、 排列輪數。

在雜湊函式中需要兩個輸入 ，其 input message （任意長度）、arbitrary specified length（加解密參數中的 ），然後加密完後會輸出 ，其 雜湊結果（隨機長度 ）完整函式如下表示:

注意：所有的雜湊和拓展輸出均使用此函式，只是參數設置的差異，雜湊函式使用參數 、拓展輸出函式參數 。

**設置建議**

* Authenticated encryption

官方推薦的參數配置方案主要為 Ascon-128： ，次要為 Ascon-128a：。

還有一個加解密配置為 Ascon-80pq ，這個配置主要是提升了金鑰長度以抵抗使用 Grover 演算法的量子攻擊，其配置為 。

* Hashing

官方推薦的參數配置方案主要為 Ascon-Hash：with，次要為Ascon-Hasha： with 。

* Pairing for Authenticated Encryption and Hashing

官方推薦的參數配置方案主要為Ascon-128 and Ascon-Hash（兩者要為相同的r），次要為Ascon-128a and Ascon-Hasha（兩者要為相同的 b）。

* Permutation進階設置

提供了兩個給拓展輸出使用的雜湊函式配置Ascon-Xof：、Ascon-Xofa：

**設計**

Ascon的設計目標是能夠在硬體和軟體之上都能用極少的記憶體儲存量來執行加解密，其套件內部各演算法設計原理如下：

* Ascon加解密、雜湊與拓展輸出函式

遵循於[海綿結構](https://zh.m.wikipedia.org/zh-tw/%E6%B5%B7%E7%B6%BF%E5%87%BD%E6%95%B8)，更正確來說應該要更接近於 [SpongeWrap](https://link.springer.com/chapter/10.1007/978-3-642-28496-0_19)。

* Permutation（應用於上述功能之中）

使用迭代[替換排列網絡（SPN）](https://en.wikipedia.org/wiki/Substitution%E2%80%93permutation_network)，以在低成本情況下提供良好的密碼特性和傳播速率。

Permutation 分為3個階段：（Addition of Constants）、（Substitution Layer）、（Linear Diffusion Layer）

* + ：

使用一個常數值做xor運算。

* + ：

使用[Keccak（目前的SHA-3演算法）](https://zh.wikipedia.org/zh-tw/SHA-3)中的χmapping step為基礎，因χmapping是可高度平行化的，並且具有簡潔的描述和相對較少的指令。使得在軟體和硬體上都有高效能的表現。

* + ：

以[SHA-2的 functions](https://csrc.nist.gov/csrc/media/publications/fips/180/3/archive/2008-10-31/documents/fips180-3_final.pdf)為基礎設計擴散功能。

**為何輕量化:**

Ascon 套件其主要在於底層的 320bits 排列僅使用按位布爾函數（and、not、xor）和 words 的旋轉。

因此，排列非常適合在 64 位元平台上實現快速 bitsliced，而位元交錯允許在 32、16 和 8 位元平台上實現快速 bitsliced、Ascon 的低階 S-box 允許以較小的硬體和軟體開銷實現遮罩。

總結來說，在輕量級設備進行密碼操作的場景下，Ascon 是一個很好的選擇。 也由於在軟件方面的良好表現，Ascon非常適合輕量級設備與高端伺服器通信的場景。