PPAE: Practical Parazoa Authenticated Encryption Family

Donghoon Chang[2] Sumesh Manjunath R[1]
Somitra Kumar Sanadhya[2]

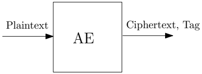
[1]TCS Innovation Labs, Pune [TRDDC]

[2]Indraprastha Institute of Information Technology, Delhi, India [IIIT-D]

25th November 2015

Overview

Motivation



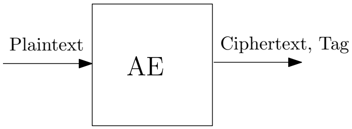
$$E_k(N, A, M) = C, T$$

$$D_k(N, A, C, T) = M/\perp$$

- Most of the underlying primitives for AE are:
  - block ciphers
  - random permutations
- Existing AE schemes do not have feed forward operation.
- Provide AE support to (sub-set) Parazoa hash family, thus propose AE family.
- Provide a generalized security proof to the proposed AE family.

Overview

AE: Introduction

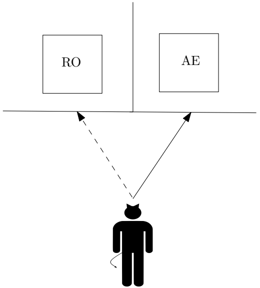


$$E_k(N, A, M) = C, T$$

$$D_k(N, A, C, T) = M/\perp$$

- Nonce based Authenticated Encryption.
- Supports Associated Data.
- Encryption output ciphertext and tag.
- Decryption output plaintext only if tag matches.

AE: Privacy



- Two oracles: Random Oracle and AE oracle.
- Adversary interact with unknown oracle.
- Adversary identifies the unknown oracle.

$$\mathbf{Adv}_{\Pi}^{priv}(\mathcal{A}) = \Pr[\mathcal{A}^{\mathcal{E}_K(.,.),\pi,\pi^{-1}} = 1] - \Pr[\mathcal{A}^{\$(.,.),\pi,\pi^{-1}} = 1]$$

AE: Authenticity

The forging experiment $Exp_{\Pi}^{auth}(\mathcal{A})$, is defined as follows:

1. $\mathcal{A}$ queries π, π^{-1}, $\mathcal{E}_K$ and $\mathcal{D}_K$ at most q_1, q_2, q_e and q_d.

AE: Authenticity

The forging experiment $Exp_{\Pi}^{auth}(\mathcal{A})$, is defined as follows:

1. $\mathcal{A}$ queries π, π^{-1}, $\mathcal{E}_K$ and $\mathcal{D}_K$ at most q_1, q_2, q_e and q_d.
2. For every $\mathcal{E}_K(N, M)$ query, the encryption oracle output C, T and stores (N, C, T) in a set, Z.
3. For every $\mathcal{D}_K(N, C, T)$ query, the decryption oracle decrypt C to get a valid message M. If M is valid and $(N, C, T) \notin Z$, then experiment outputs 1.
4. For every π and π^{-1} queries, corresponding permutations oracles are used.

AE: Authenticity

The forging experiment $Exp_{\Pi}^{auth}(\mathcal{A})$, is defined as follows:

1. $\mathcal{A}$ queries π, π^{-1}, $\mathcal{E}_K$ and $\mathcal{D}_K$ at most q_1, q_2, q_e and q_d.
2. For every $\mathcal{E}_K(N, M)$ query, the encryption oracle output C, T and stores (N, C, T) in a set, Z.
3. For every $\mathcal{D}_K(N, C, T)$ query, the decryption oracle decrypt C to get a valid message M. If M is valid and $(N, C, T) \notin Z$, then experiment outputs 1.
4. For every π and π^{-1} queries, corresponding permutations oracles are used.
5. After all queries are exhausted, the experiment outputs 0.

AE: Authenticity

The forging experiment $Exp_{\Pi}^{auth}(\mathcal{A})$, is defined as follows:

1. $\mathcal{A}$ queries π, π^{-1}, $\mathcal{E}_K$ and $\mathcal{D}_K$ at most q_1, q_2, q_e and q_d.
2. For every $\mathcal{E}_K(N, M)$ query, the encryption oracle output C, T and stores (N, C, T) in a set, Z.
3. For every $\mathcal{D}_K(N, C, T)$ query, the decryption oracle decrypt C to get a valid message M. If M is valid and $(N, C, T) \notin Z$, then experiment outputs 1.
4. For every π and π^{-1} queries, corresponding permutations oracles are used.
5. After all queries are exhausted, the experiment outputs 0.

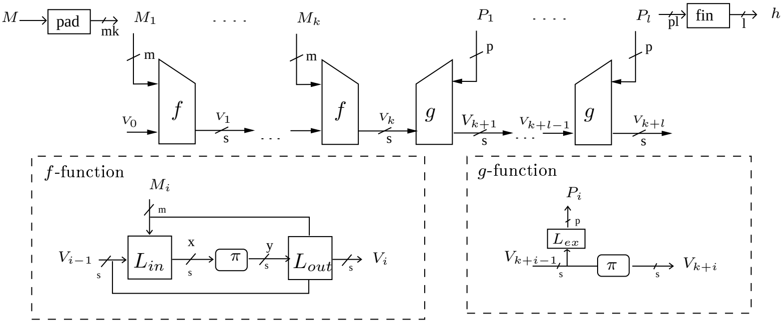
The advantage of the Adversary $\mathcal{A}$ in forging the scheme Π is represented as

$$Adv_{\Pi}^{auth}(\mathcal{A}) = \Pr[Exp_{\Pi}^{auth}(\mathcal{A}) = 1].$$

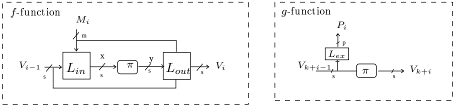
Overview

Parazoa: Construction

- Parazoa Hash family was introduced by E.Andreeva.et al. in 2012 [1].
- Generalization of sponge hash functions (Keccak).
- Supports feed forward operation.

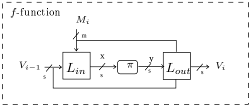


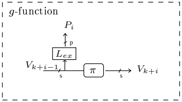
Parazoa: f and g function [1]



- L_{in} Requirement: For any $x \in Z_2^s$ and $v \in C(x)$, there *exist only one* $M \in Z_2^m$ *s.t.* $L_{in}(v, M) = x$. For a given state v, every possible M must results in a unique x.

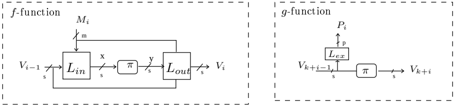
Parazoa: f and g function [1]





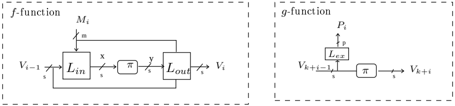
- L_{in} Requirement: For any $x \in Z_2^s$ and $v \in C(x)$, there *exist only one* $M \in Z_2^m$ *s.t.* $L_{in}(v, M) = x$. For a given state v, every possible M must results in a unique x.
- L_{out} Requirement: For any $(v, M) \in Z_2^s X Z_2^m$, $L_{out}(y, v, M)$ is a bijection on the state.

Parazoa: f and g function [1]



- L_{in} Requirement: For any $x \in Z_2^s$ and $v \in C(x)$, there *exist only one* $M \in Z_2^m$ *s.t.* $L_{in}(v, M) = x$. For a given state v, every possible M must results in a unique x.
- L_{out} Requirement: For any $(v, M) \in Z_2^s X Z_2^m$, $L_{out}(y, v, M)$ is a bijection on the state.
- L_{ex} Requirement: It must be a balanced function. For a given v, the probability of a P is uniform.

Parazoa: f and g function [1]



- L_{in} Requirement: For any $x \in Z_2^s$ and $v \in C(x)$, there *exist only one* $M \in Z_2^m$ *s.t.* $L_{in}(v, M) = x$. For a given state v, every possible M must results in a unique x.
- L_{out} Requirement: For any $(v, M) \in Z_2^s X Z_2^m$, $L_{out}(y, v, M)$ is a bijection on the state.
- L_{ex} Requirement: It must be a balanced function. For a given v, the probability of a P is uniform.

Parazoa: Indifferentiability

The indifferentiability theorem of Parazoa Hash family [1] is:

Theorem ([1])

Let H be a Parazoa function. Let D be the distinguisher that makes at most q_1 left queries of maximal length $(U-1)m$ bits, q_2 right queries and runs in time t, where $U \geq 1$. Then:

$$Adv^{pro}_{H,S}(D) = O\left(\frac{((U+l)q_1 + q_2)^2}{2^{s-p-d}}\right),$$

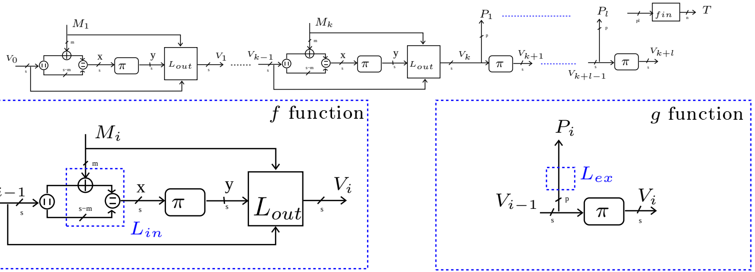
- s-p-d represents number of bits of state such that it
  - cannot be affected by adversary through message
  - cannot be obtained by tag output

That is (s-p-d) bits are not in control of an adversary.

Overview

Practical Parazoa Hash family (PPH)

- We propose, Practical Parazoa Hash (PPH) family which is a sub-family of Parazoa Hash family [1].
- L_{in} and L_{ex} functions are defined.
- XOR is the simplest and practical operation which satisfies required properties.



PPH: Indifferentiability

The indifferentialibility bound of PPH is derived from Parazoa [1].

Lemma

The indifferentiability of PPH hash function is

$$Adv^{pro}_{H,S}(D) = O\left(\frac{((U+l)q_1+q_2)^2}{2^{s-max(m,p)}}\right),$$

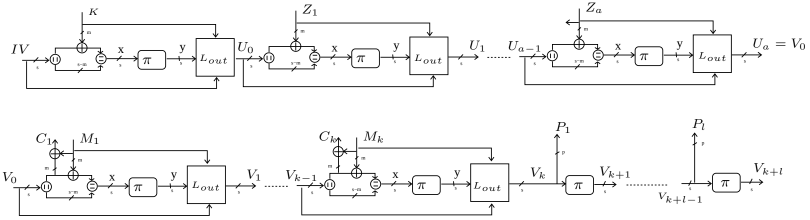
where, m is the size of the message block, p is the size of output block for hash.

- $s - max(m, p)$ bits are NOT in control of adversary

Overview

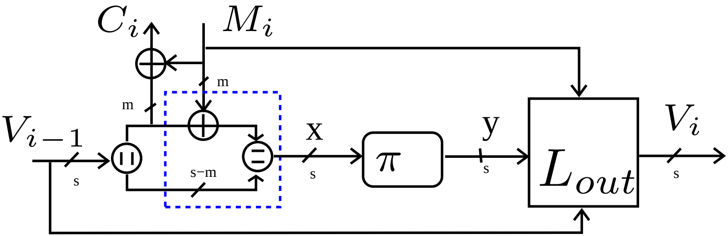
PPAE: Construction

The proposed PPAE family based on PPH



- Nonce based Authenticated Encryption with Associated Data
- size of permutation, π : s-bit
- Key size : m-bit s.t. $m \leq s$
- Tag size : n-bit s.t. $pl \geq n$
- pad() function is same as Parazoa padding function.

PPAE: f



- m Most Significant Bit of V_{i-1} is XOR with M_i to output C_i.
- Similarly, p MSB of V is extracted for tag.
- Only $max(m, p)$ bits of a state is exposed to adversary

PPAE: Privacy

Let **AE** be the PPAE using s-bit ideal permutation π. The message block size is m bits and p bit blocks are output for tag. Game playing framework is followed to provide privacy.

Theorem

The adversary $\mathcal{A}$ is given access to π, π^{-1} and the advantage of $\mathcal{A}$ to differentiate AE from RO is given by:

$$\begin{aligned} \mathbf{Adv}_{AE}^{priv}(\mathcal{A}) &= Pr[\mathcal{A}_{\pi,\pi^{-1}}^{AE} = 1] - Pr[\mathcal{A}_{\pi,\pi^{-1}}^{RO} = 1] \\ &\leq \frac{\sigma}{2^{s-1}} + \frac{q_{ae}}{2^m} + \frac{\sigma(\sigma-1)}{2^{s-max(m,p)+1}}, \end{aligned}$$

where $\sigma = q_{ae} + q_\pi + q_{\pi^{-1}}$. q_{ae} is max queries to AE, q_π and $q_{\pi^{-1}}$ are maxi queries to π and π^{-1}, respectively. One q_{ae} is bounded by $(1 + a + k + l)$ q_π queries.

PPAE: Privacy

- Game Playing Framework [3] is used to provide privacy security.
- Total 7 Games: G0 - PPAE and G7 - VIL Random Oracle
- The main idea of the games are to replace the random permutation primitive with a random function and move towards VIL random oracle.

PPAE: Authenticity

- Forgery adversary of PPAE is reduced to indiferentiability adversary of PPH.

Theorem

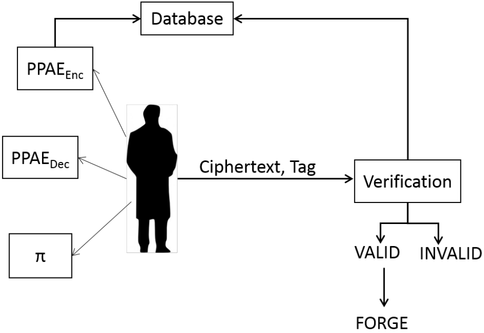
The authenticity of PPAE is defined as the ability of any adversary to forge PPAE after interacting with PPAE, π, π^{-1} oracles. The ability is measured in terms of probability of an adversary to succeed in the forgery experiment.

$$Pr[Exp^{auth}_{PPAE,\pi,\pi^{-1}}(\mathcal{A}) = 1] \leq O\left(\frac{((U+I+1)^2(\sigma_a)^2}{2^{s-max(m,p)}}\right) + \frac{\sigma_a}{2^n} + \frac{\sigma_a}{2^m}.$$

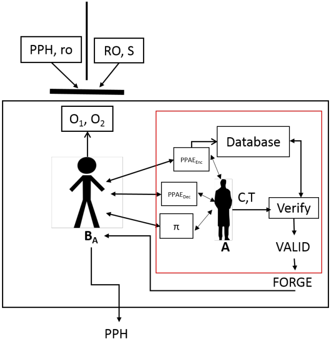
where $\sigma_a = q_e + q_d + q_\pi + q_{\pi^{-1}}$.

PPAE: Authenticity

- Assume, we have a forger A, who can forge PPAE with non-negligible probability.



- Using PPAE forger A, we create an indifferentiability adversary B_A for PPH.



- If the interacting unknown oracle is PPAE, the probability of identifying is equal to the advantage of A.

PPAE: Authenticity

- B_A intereacts with A to forge PPAE and receives the forged plaintext-ciphertext and corresponding tag.
- B_A queries O_u with the received plaintext from A and verify the ciphertext from O_u.
- If verified, then O_u is PPAE.
- Thus, the forger's advantage is reduced to indiffirentiability adversary's B_A advantage.

Overview

Keyak

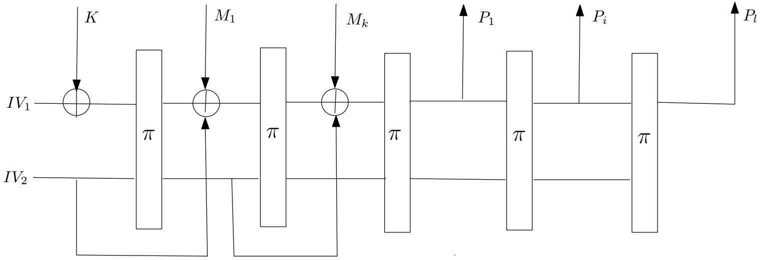
- Keyak is based on DuplexWrap construction.
- The privacy advantage for DuplexWrap is
  $\mathbf{Adv}^{\text{priv}}_{DuplexWrap[f,\rho]}(\mathcal{A}) \leq \frac{q_{ae}}{2^m} + \frac{\sigma(\sigma+1)}{2^{c+1}}$
- The privacy advantage of PPAE is
  $\mathbf{Adv}^{\text{priv}}_{PPAE}(\mathcal{A}) \leq \frac{\sigma}{2^{s-1}} + \frac{\sigma}{2^m} + \frac{\sigma(\sigma-1)}{2^{s-max(m,p)+1}}$
- The security parameter $s - max(m,p) = c$. The privacy advantage for Keyak derived from PPAE
  $\mathbf{Adv}^{\text{priv}}_{DuplexWrap}(\mathcal{A}) \leq \frac{\sigma}{2^{s-1}} + \frac{\sigma}{2^m} + \frac{\sigma(\sigma-1)}{2^{c+1}}$

Theorem (Keyak)

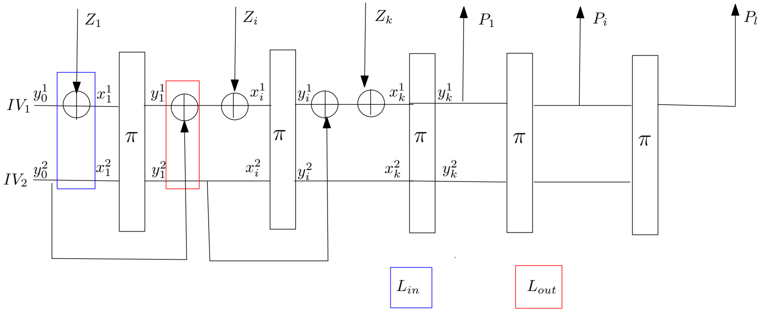
$$\mathbf{Adv}^{priv}_{DuplexWrap}(\mathcal{A}) \leq \frac{q_{ae}}{2^m} + \frac{\sigma(\sigma+1)}{2^{c+1}} \leq \frac{\sigma}{2^{s-1}} + \frac{\sigma}{2^m} + \frac{\sigma(\sigma-1)}{2^{c+1}}$$

DSSAE mode

- We propose DSSAE mode with feedforward operation.
- The internal permutation size = s bits
- The input block size = m bits ($m \leq s$).
- The output block size = p bits ($p \leq s$). Size of tag = pl.
- $IV_1 \| IV_2 = 0^s$.



DSSAE mode



- Let $X_i = (x_i^1 \| x_i^2)$, $Y_i = (y_i^1 \| y_i^2)$, be input and output of π.
- $L_{in}(Y_{i-1}, Z_i) = (y_{i-1}^1 \oplus X_i) \| y_{i-1}^2 = x_{i+1}^1 \| x_{i+1}^2$, where Z_i, is input block.
- $L_{out}(Yi-1, Y_i) = (y_i^1 \oplus y_{i-1}^2) \| y_i^2$
- XOR is a bijective function, hence the bijective requirement on the state for L_{out} is satisfied.

Overview

Summary

- PPH: Sub family of Parazoa hash family.
- PPAE: Proposed Authenticated Encryption mode for PPH.
- PPAE supports feed forward operation.
- Provided privacy and authenticity security for PPAE.
- Proposed DSSAE mode from PPAE family

References

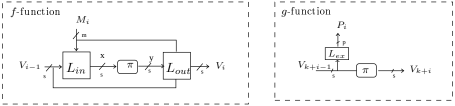
Elena Andreeva, Bart Mennink and Bart Preneel.
The parazoa family: generalizing the sponge hash functions.
International Journal of Information Security, 2012.

Philipp Jovanovic, Atul Luykx and Bart Mennink.
Beyond 2 c/2 Security in Sponge-Based Authenticated Encryption Modes.
In ASIACRYPT 2014 - Kaoshiung, Taiwan, December 7-11, 2014.

Mihir Bellare and Phillip Rogaway.
The Security of Triple Encryption and a Framework for Code-Based Game-Playing Proofs.
In EUROCRYPT 2006, December 7-11, 2014.

Thanks
Any Questions?

Parazoa: f and g function [1]



- L_{in} Requirement: For any $x \in Z_2^s$ and $v \in C(x)$, there *exist only one* $M \in Z_2^m$ *s.t.* $L_{in}(v, M) = x$. For a given state v, every possible M must results in a unique x.
- L_{out} Requirement: For any $(v, M) \in Z_2^s X Z_2^m$, $L_{out}(y, v, M)$ is a bijection on the state.
- L_{ex} Requirement: It must be a balanced function. For a given v, the probability of a P is uniform.
- *pad* Requirement: For last block of message M_k, must satisfy: $L_{in}(x, M_k) \neq x$ and $L_{in}(L_{out}(x, v', M'), M_k) \neq x)$.