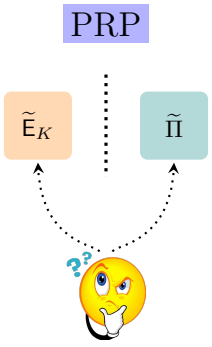
Rugged Pseudorandom Permutations with Beyond-Birthday-Bound Security

Nilanjan Datta Jean Paul Degabriele Avijit Dutta Vukašin Karadžić Hrithik Nandi

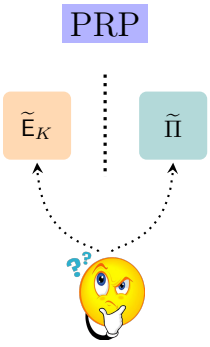
AsiaCCS 2026, Bangalore, India

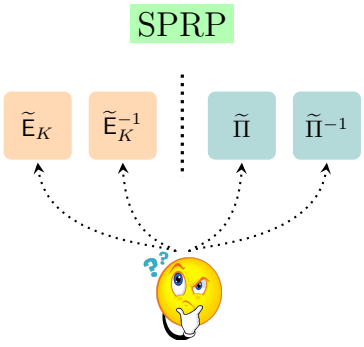
June 3, 2026

PRP vs RPRP vs SPRP

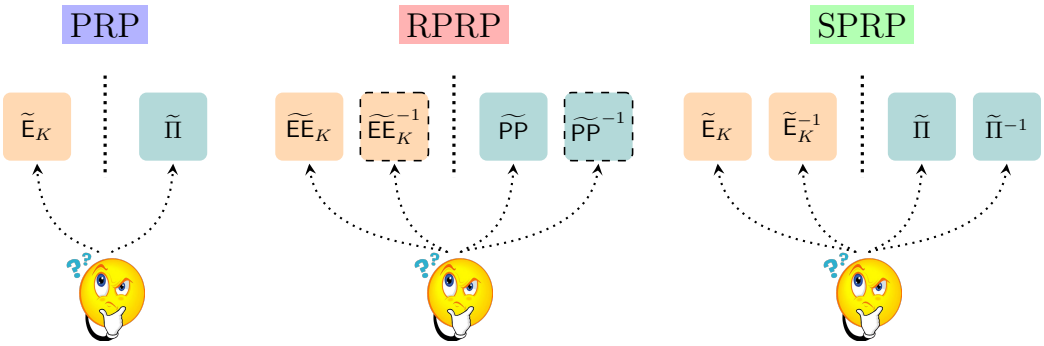


PRP vs RPRP vs SPRP

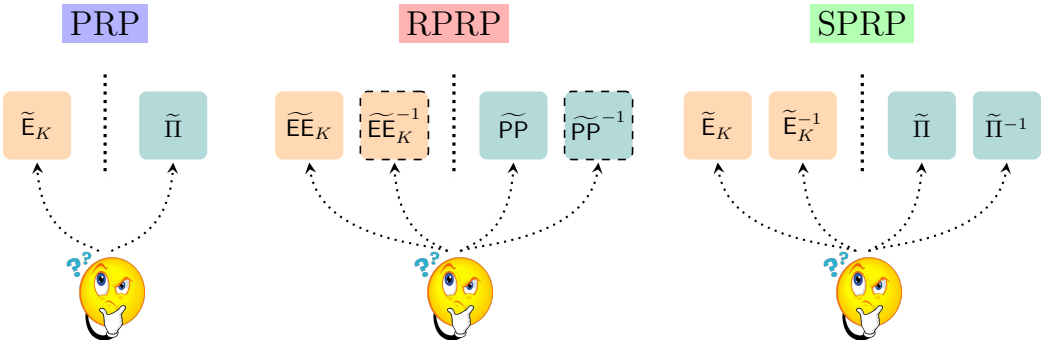




PRP vs RPRP vs SPRP

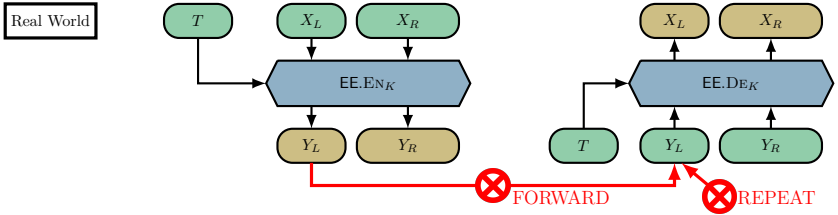


PRP vs RPRP vs SPRP

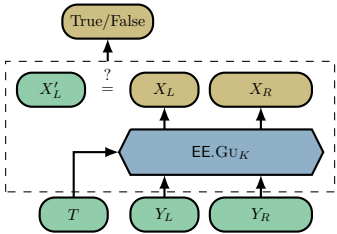


- Proposed by Degabriele et al. at CRYPTO'22.
- It is an intermediate security notion of PRP and SPRP.
- An RPRP is a strictly weaker notion than an SPRP, but at the same time it is more efficient.

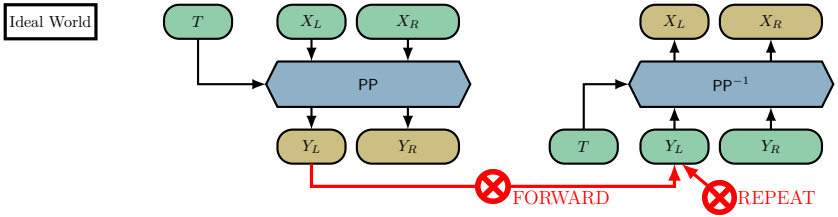
Rugged Pseudorandom Permutations (RPRP)



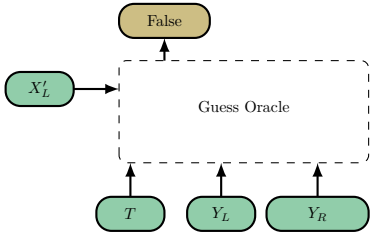
- Deciphering can be accessed via two separate oracles:
  - Decryption Oracle - restricted queries, full output,
  - Guess Oracle - unrestricted queries, 1-bit output.
- Trivial Guess queries should be avoid.



Rugged Pseudorandom Permutations (RPRP)



- Replace EE with an ideal cipher PP.
- Guess oracle always returns False.
- Trivial Guess queries should be avoid.



Existing RPRP Constructions

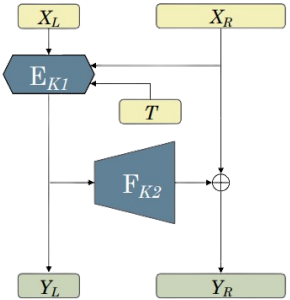


Figure: UIV Construction

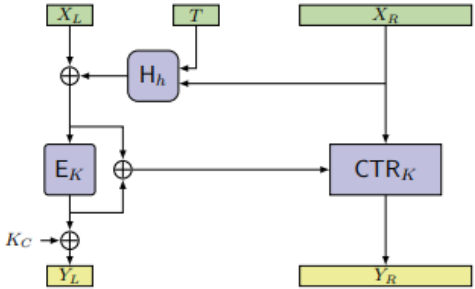


Figure: HEC Construction

- Both the UIV construction and the HEC construction achieve birthday bound security.

Our Contribution: THEC Construction

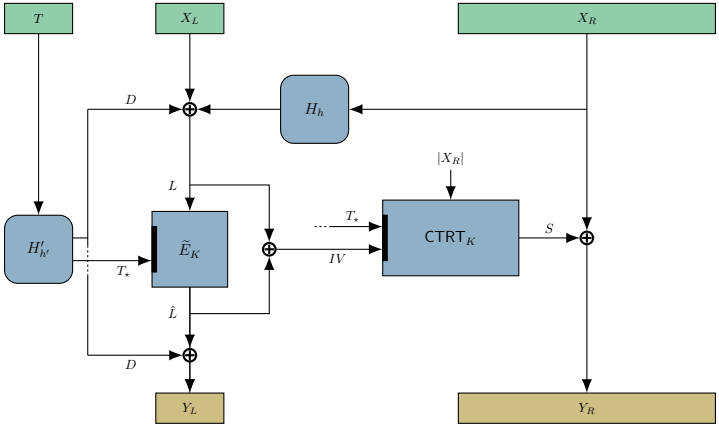


Figure: THEC construction

- THEC offers BBB RPRP security with a graceful security degradation on tweak repetitions.

Our Contribution: DE-THEC Construction

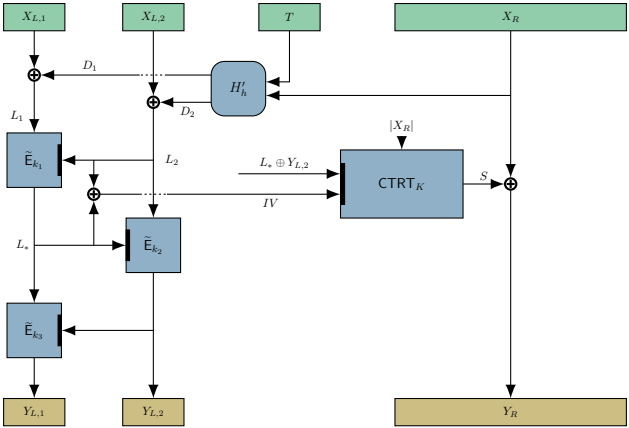


Figure: DE-THEC construction

- DE-THEC achieves optimal RPRP security without any restriction on tweak repetitions.

Security Results of THEC & DE-THEC

Results:

Let H is ϵ-AXU, ρ-almost regular and δ-AU. Let $\widetilde{\mathsf{E}}$ be a tweakable block cipher. Then

$$\mathbf{Adv}^{\mathsf{RPRP}}_{\mathsf{THEC}}(\mathcal{A}, v) \leq \mathbf{Adv}^{\mathsf{STPRP}}_{\widetilde{\mathsf{E}}}(\mathcal{B}) + q(\mu-1)\epsilon + q^2\delta\epsilon + \frac{q(\mu-1)}{2^{n-1}} + \frac{q^2\delta}{2^{n-1}} + \mu\sigma\rho + q\sigma\rho^2 + \frac{q\sigma\rho}{2^{n-1}} + 2\sigma\rho + \frac{q(\mu-1)l_m}{2^{n-1}} + \frac{\min\{q^2 l_m, \sigma^2\}\delta}{2^{n-1}} + \frac{\min\{q^2 l_m, \sigma^2\}}{2^{2n-2}} + q_{gu}v\left(\epsilon + \frac{2}{2^{n-1}}\right) + (\mu-1)\frac{q}{2^n}.$$

$$\mathbf{Adv}^{\mathsf{RPRP}}_{\mathsf{DE\text{-}THEC}}(\mathcal{A}, v) \leq 4\mathbf{Adv}^{\mathsf{STPRP}}_{\widetilde{\mathsf{E}}}(\mathcal{B}) + q^2\epsilon + \frac{2qq_{en}}{2^{2n-2}} + \frac{qq_{de}}{2^{2n-2}} + \frac{2\min\{q^2 l_m, \sigma^2\}}{2^{2n-2}} + q_{gu}v\left(2\epsilon + \frac{1}{2^{2n-2}}\right) + \frac{q^2}{2^{2n}}.$$

where $q \leq 2^{n-1}$, $\mu \leq q$ and $q_{gu}v \leq 2^{n-1}$, μ denotes the maximum number of tweak repetitions.

Applications: Constructing AEAD using RPRP

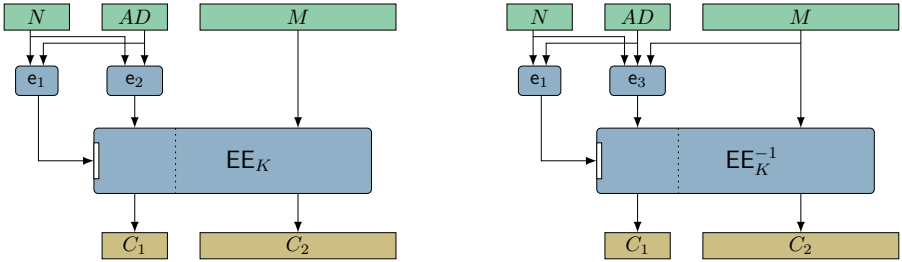


Figure: EtE (**left**) and EtD (**right**) instantiated with a RPRP-secure cipher EE

- EtE[THEC] : a nonce-based or nonce-hiding BBB MRAE secure AEAD (with a graceful security degradation on the nonce repetitions).
- EtE[DE-THEC] : a nonce-based or nonce-hiding BBB MRAE secure AEAD scheme (without graceful degradation).
- EtD[DE-THEC] : a RUP-secure AEAD scheme with full n-bit security with no restrictions.

Performance Comparison

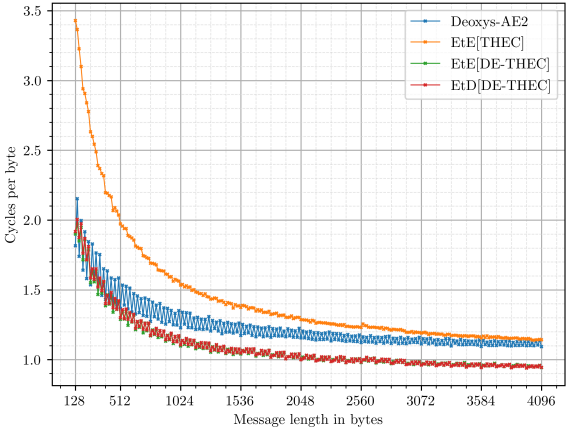


Figure: Benchmarks of encryption algorithm speeds of our derived AEAD schemes and Deoxys-AE2 scheme, for different message length (in bytes) and A of 128 bytes. The plot contains data points for every input length in $\{128, 144, \ldots, 4096\}$.

Applications: Beyond AEAD

- Beyond improved efficiency, RPRP-based constructions can also offer advantages in terms of higher throughput and lower latency .

Applications: Beyond AEAD

- Beyond improved efficiency, RPRP-based constructions can also offer advantages in terms of higher throughput and lower latency.
- RPRPs also find applications beyond AEAD. For example, they can be used to realise onion encryption in Tor.

Applications: Beyond AEAD

- Beyond improved efficiency, RPRP-based constructions can also offer advantages in terms of higher throughput and lower latency.
- RPRPs also find applications beyond AEAD. For example, they can be used to realise onion encryption in Tor.
- Counter Galois Onion (CGO), proposed by Degabriele *et al.*, is an onion encryption scheme for Tor with improved security guarantees that employs an RPRP to encrypt each layer.

Applications: Beyond AEAD

- Beyond improved efficiency, RPRP-based constructions can also offer advantages in terms of higher throughput and lower latency.
- RPRPs also find applications beyond AEAD. For example, they can be used to realise onion encryption in Tor.
- Counter Galois Onion (CGO), proposed by Degabriele *et al.*, is an onion encryption scheme for Tor with improved security guarantees that employs an RPRP to encrypt each layer.
- Recently, the Tor Project announced the implementation of CGO in its next-generation Tor design, marking the first real-world deployment of primitives based on RPRPs.

Applications: Beyond AEAD

- Beyond improved efficiency, RPRP-based constructions can also offer advantages in terms of higher throughput and lower latency.
- RPRPs also find applications beyond AEAD. For example, they can be used to realise onion encryption in Tor.
- Counter Galois Onion (CGO), proposed by Degabriele *et al.*, is an onion encryption scheme for Tor with improved security guarantees that employs an RPRP to encrypt each layer.
- Recently, the Tor Project announced the implementation of CGO in its next-generation Tor design, marking the first real-world deployment of primitives based on RPRPs.
- Both of our RPRP constructions can be integrated into CGO to obtain an onion encryption scheme achieving BBB security.

Future Directions

- Our work primarily focuses on achieving high security levels together with strong software efficiency; however, the hardware footprint and implementation costs of these constructions remain to be thoroughly investigated.
- Another important direction for future research is to study whether the security guarantees of THEC and DE-THEC can be preserved in the multi-user setting.

Thank You!