Continuous Non-Malleable Key Derivation and Its Application to Related-Key Security

Baodong Qin[1,2], Shengli Liu[1], Tsz Hon Yuen[3], Robert H. Deng[4], Kefei Chen[5]

1. Shanghai Jiao Tong University, China
2. Southwest University of Science and Technology, China
3. Huawei, Singapore
4. Singapore Management University, Singapore
5. Hangzhou Normal Unvierity, China

PKC 2015
March 31, NIST

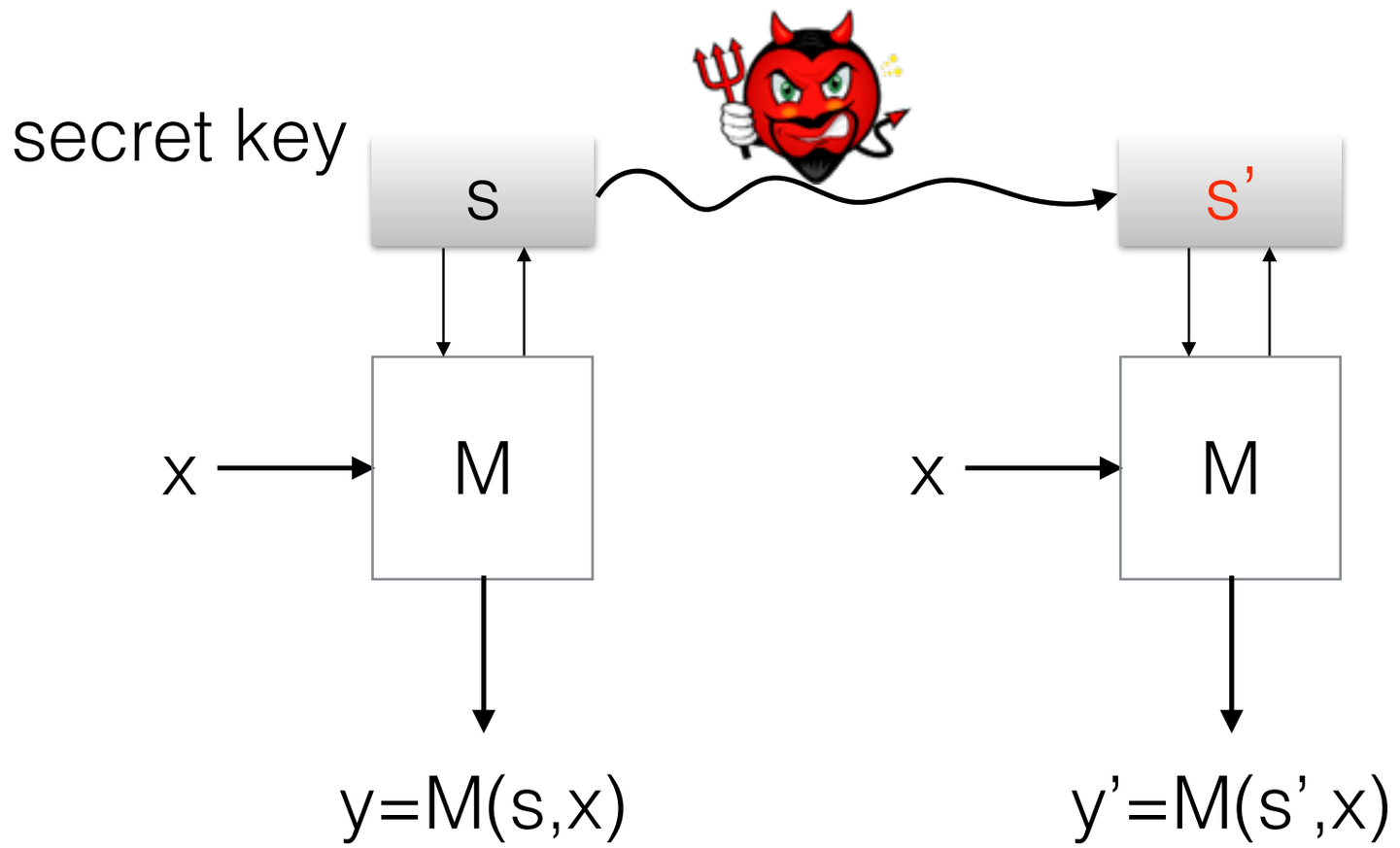
Contents

- Related-Key Attacks
- Previous works
- Continuous NM-KDFs: Definition, construction and security proof
- Application to RKA-security
- Conclusion

Related-Key Attacks

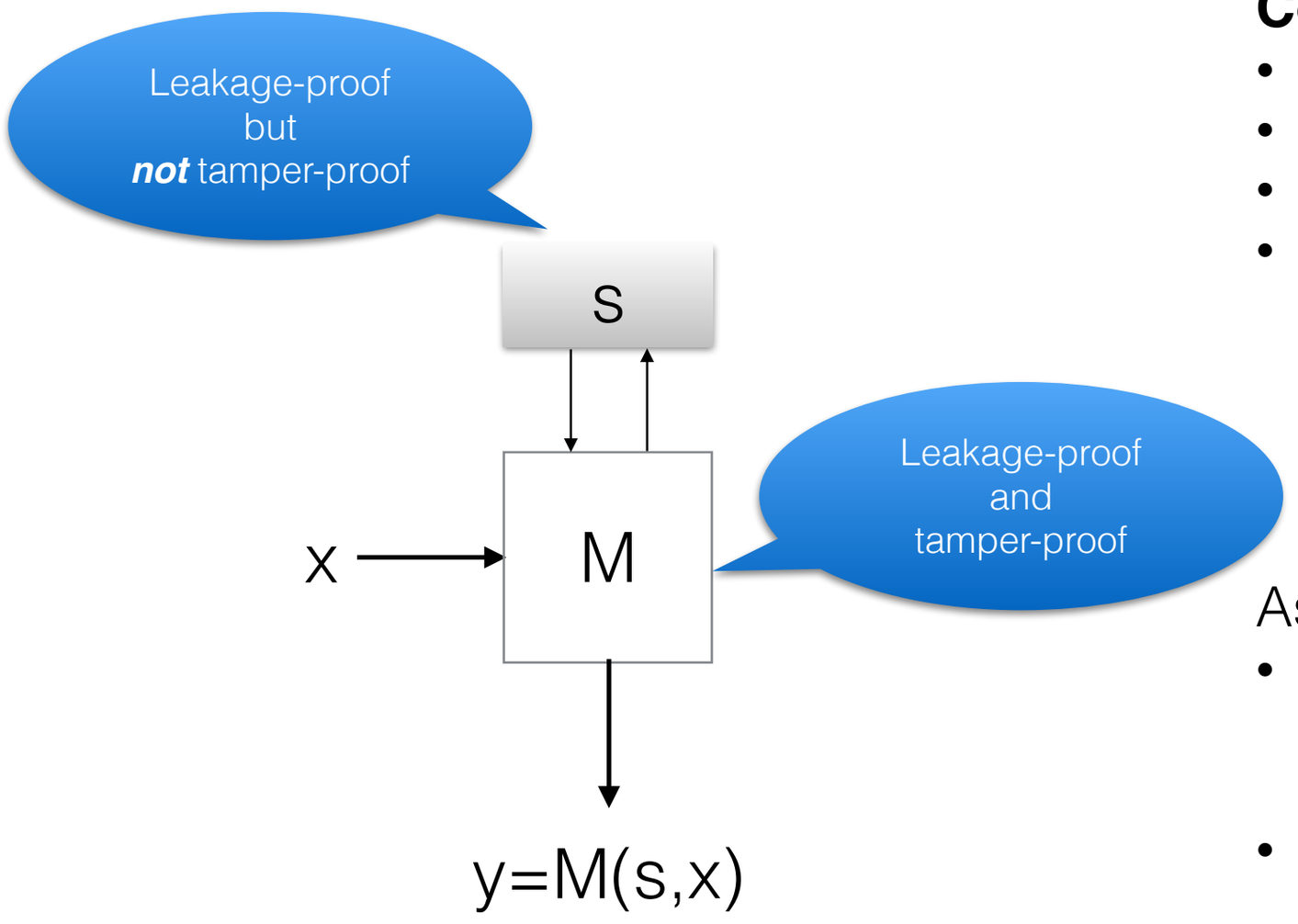
Scenario

- Hardware implementation
- Fault attacks: heat it or cut wires to inject faults.



Related-Key Attacks

Assumption



Composition of a system:

- Algorithm (codes)
- Public parameters
- Public keys (if any)
- Secret keys

Assumptions:

- Algorithm (codes) and PPs in a tamper-proof hardware device
- Only public keys and secret keys may be subjective to tampering attacks.
- The device does not leak any information on the secret key.

Related-Key Attacks

Tamper functions

- Related-key derivation (RKD) functions (following BK03)
  - From SK space to SK space

$$F: S \longmapsto S$$
$$f: \quad s \longmapsto f(s)$$

- If the public key pk is involved in an algorithm M, it might be subject to tampering attacks as well.
- In practice, the adversary has already known pk. So, tampering with pk is just dependent on the adversary's view, not the secret key.
  - pk' is implicitly determined by RKD function f.
  - Different to the split-state model [DP08,FMNV14]: s is divided into two parts (s_1,s_2).

$$F: \quad S \times PK \longmapsto S \times PK$$
$$f: \quad (s,pk) \longmapsto (f(s),pk')$$

fxg: $(s_1,s_2) \longmapsto (f(s_1),g(s_2))$, f, g are independent of each other.

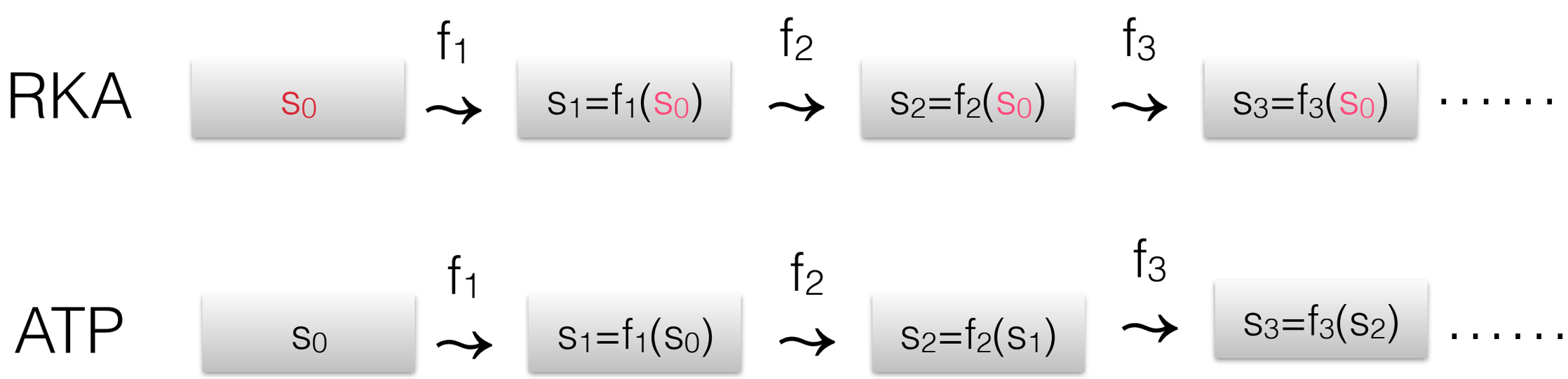
The adversary does not know the result $g(s_2)$.

Related-Key Attacks

Two security models

- Related-key attacks (RKA) security [BK03] and Algorithmic tamper-proof (ATP) security [GLMMR04]

non-persistent vs persistent [JW15]

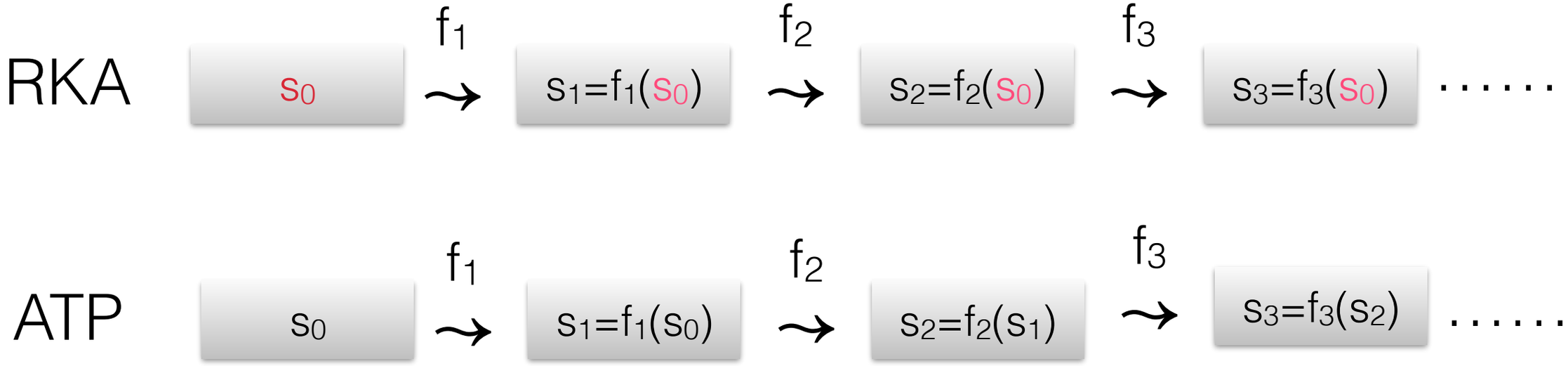


Related-Key Attacks

Two security models

- Related-key attacks (RKA) security [BK03] and Algorithmic tamper-proof (ATP) security [GLMMR04]

non-persistent vs persistent [JW15]

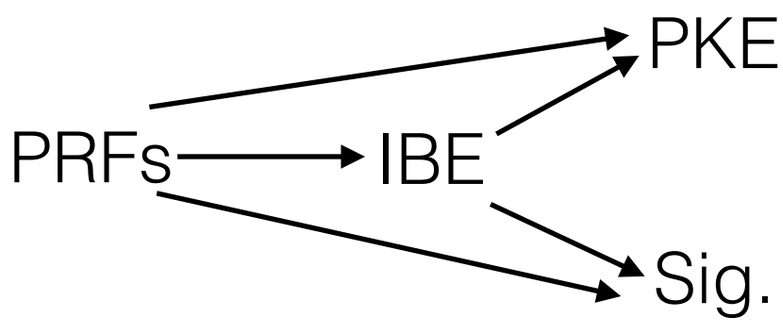


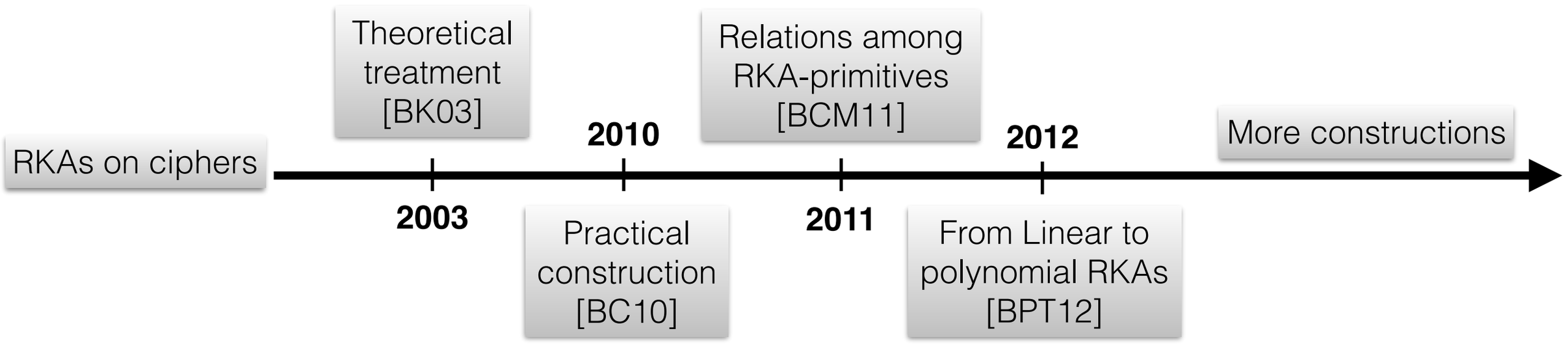
This paper: RKA model.
We would like the RKD function class is as rich as possible.

Previous Works on RKAs

Specific Constructions

- Specific primitives, specific computational assumptions
- RKA secure: PRFs, IBE, Signature, PKE…





Previous Works on RKAs

Specific Constructions

- Limitations:
  1. Simple RKD functions: linear, affine or **polynomials** (bounded degree).
  2. Parameter depends on the RKD functions and based on non-standard assumptions

Example in [BPT12]:

To compute $g^{f(s)}$ without known s for polynomial $f(x)=a_0+a_1x+\ldots+a_dx^d$ public keys must provide the following elements:

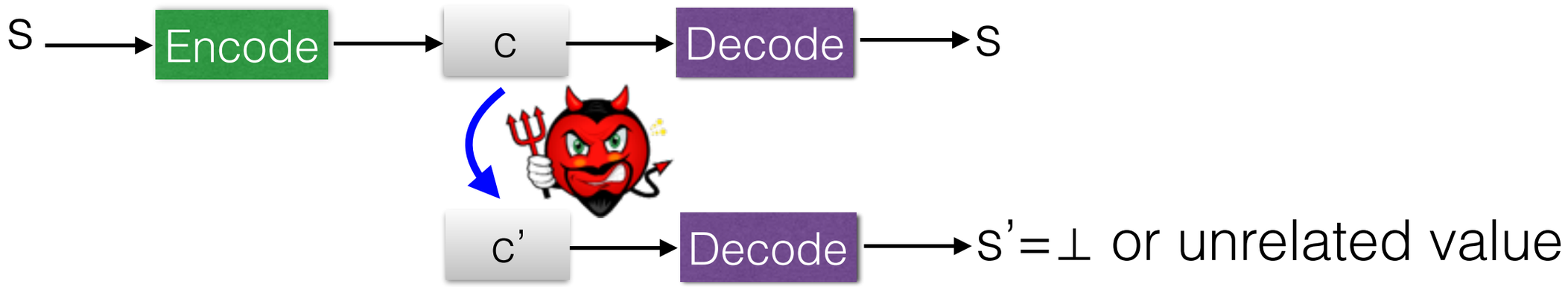
$$g^s, g^{s^2}, \ldots, g^{s^d} \Rightarrow g^{f(s)}=g^{a_0}*(g^s)^{a_1}*\ldots*(g^{s^d})^{a_d}$$

d-extended DBDH assumption

Previous Works

Generic Approach

- Tamper-resilient codes, mainly including
  - Algebraic Manipulation Detection codes [CDF+08]
  - Non-malleable codes [DPW10,FMVW14,…]
  - Continuous NMC [FMNV14,JW15,…]



- AMD and NMC: **single-time** tampering, but RKA multi-time non-persistent tampering.
- Continuous NMC: **multi-time** tampering (persistent or **non-persistent**)
- Concurrent work [JW15]: simple and efficient, but public parameter depends on tamper functions, i.e. O(log |F|).

Contributions

- New notion: Continuous non-malleable key derivation function (cnm-KDF)

- A generic construction from one-time lossy filter, one-time signature and pairwise independent hash functions, instantiated under standard assumptions.

- RKD functions: any bounded-degree polynomials (generalized to functions with high output entropy and input-output collision resistance (HOE&IOCR))

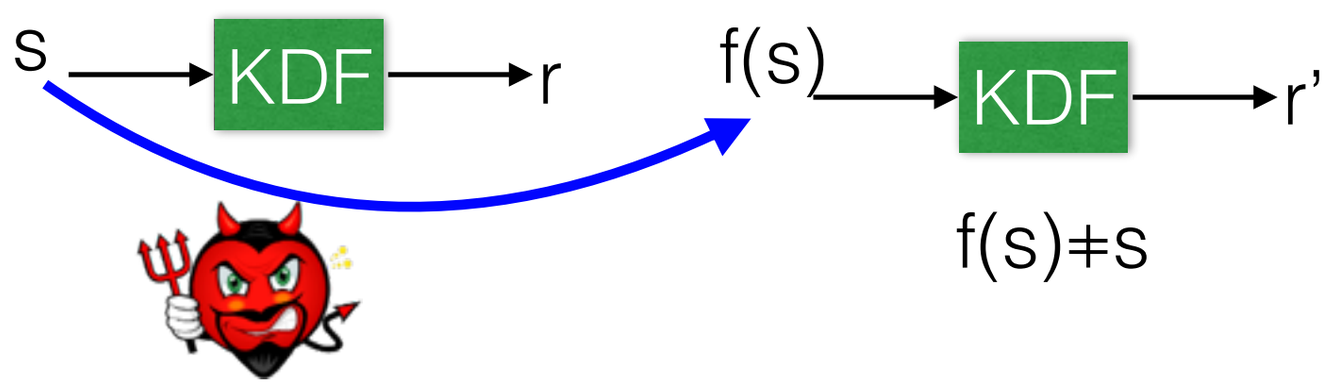
- Application to RKA-IBE, RKA-PKE, RKA-Sig.

Continuous Non-Malleable KDF

Definition and Security

- Inspired by non-malleable KDF [FMVW14]

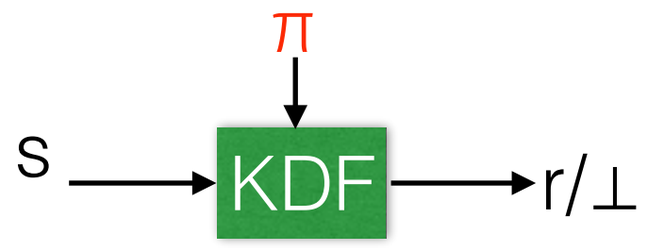
- Standard security: r is random from Adv.'s view (given KDF descriptions)
- Non-malleability: r is random even given one r'.

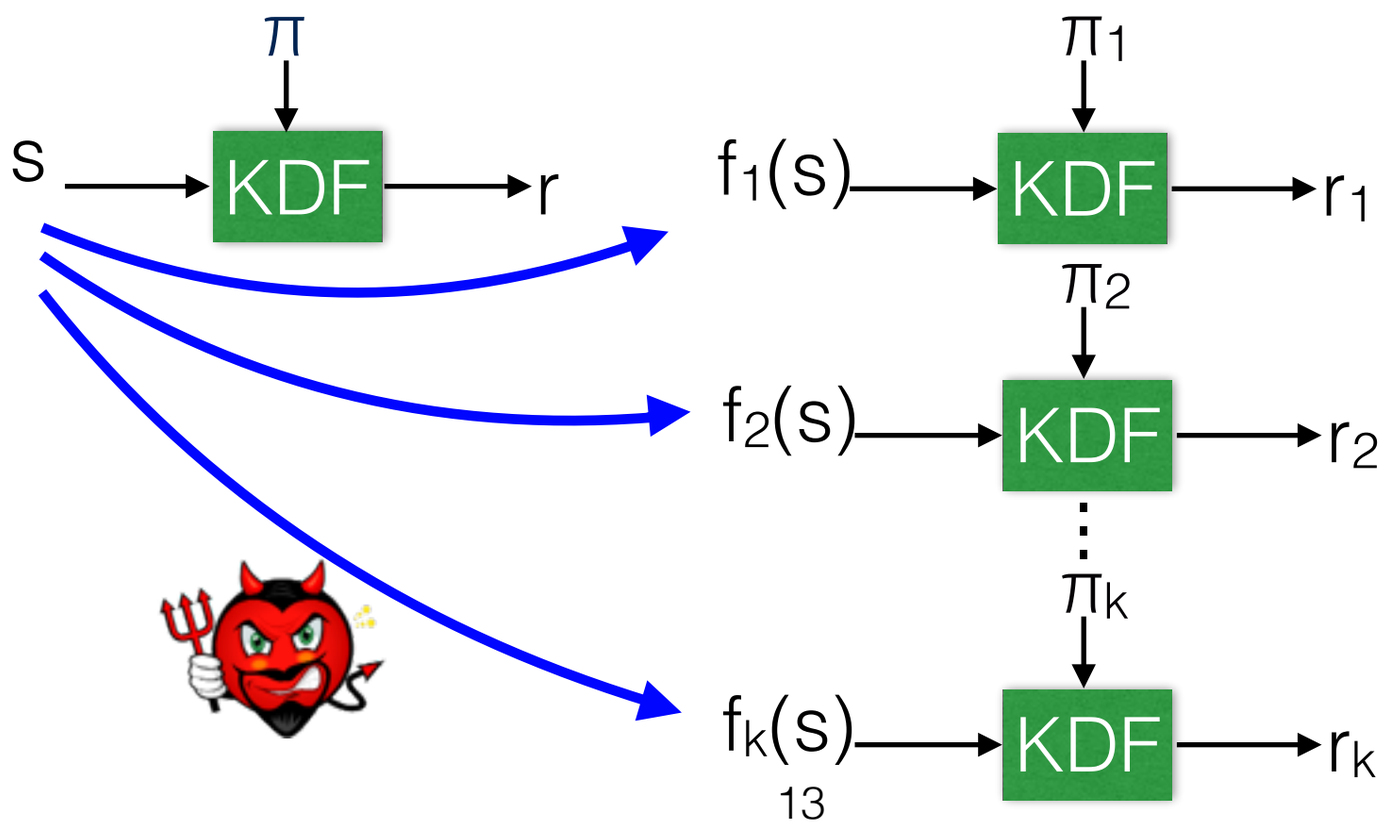


Continuous Non-Malleable KDF

Definition and Security

- cnm-KDF: Input takes an auxiliary input π. Output may be failure symbol.
- View π as a proof or authentication of s. Failure symbol means π is invalid.
- r is random even given multiple r_1, r_2…

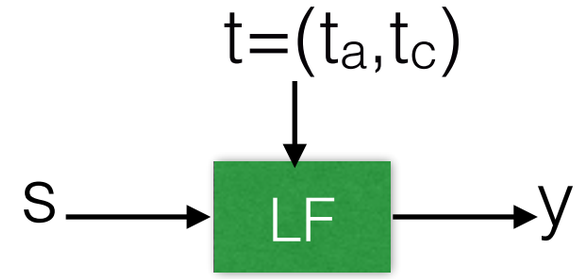




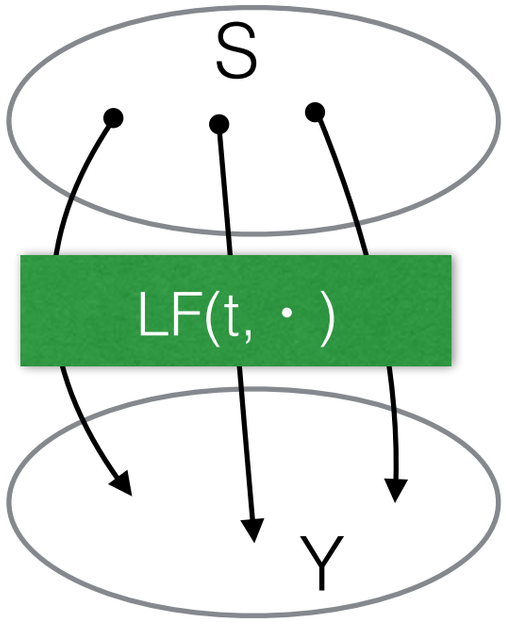
Continuous Non-Malleable KDF

Generic Construction

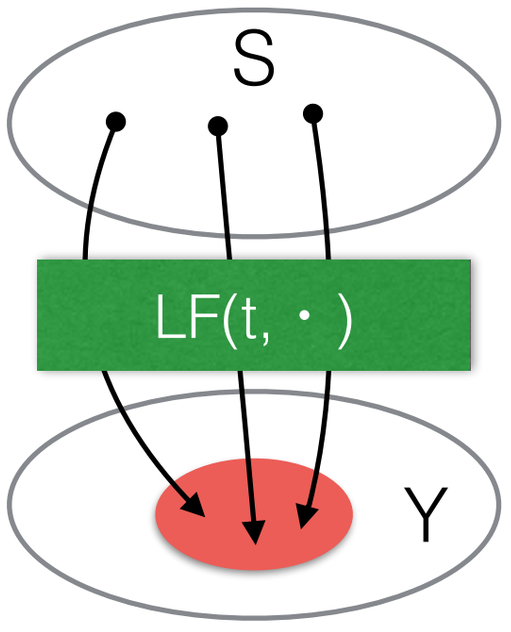
- Components: one-time lossy filter [QL13], one-time signature and pairwise independent hash function.
- Properties of LF:
  - works in two indistinguishable modes.
  - hard to generate a non-injective tag.



Injective



|S|=|Y|



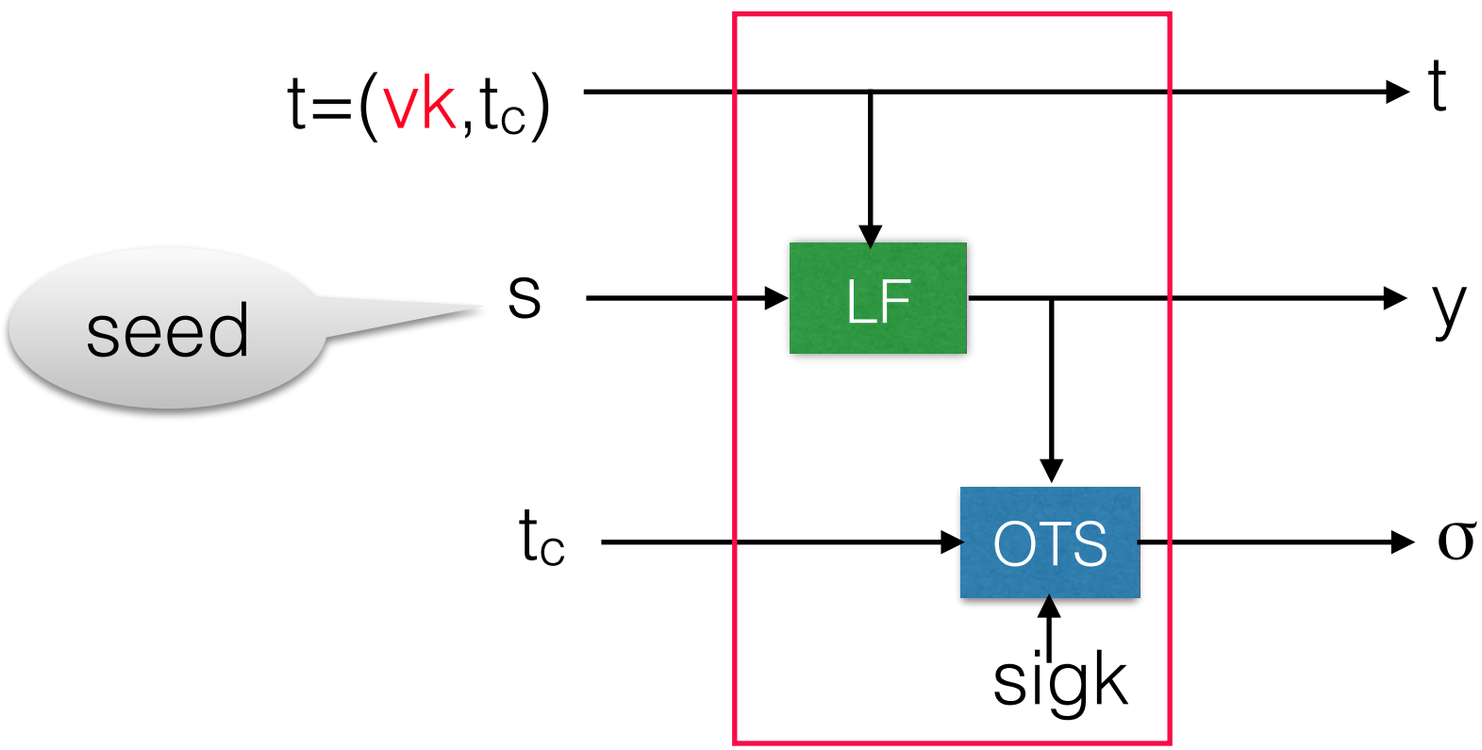
|S|>>|Y|

Lossy

Continuous Non-Malleable KDF

Generic Construction

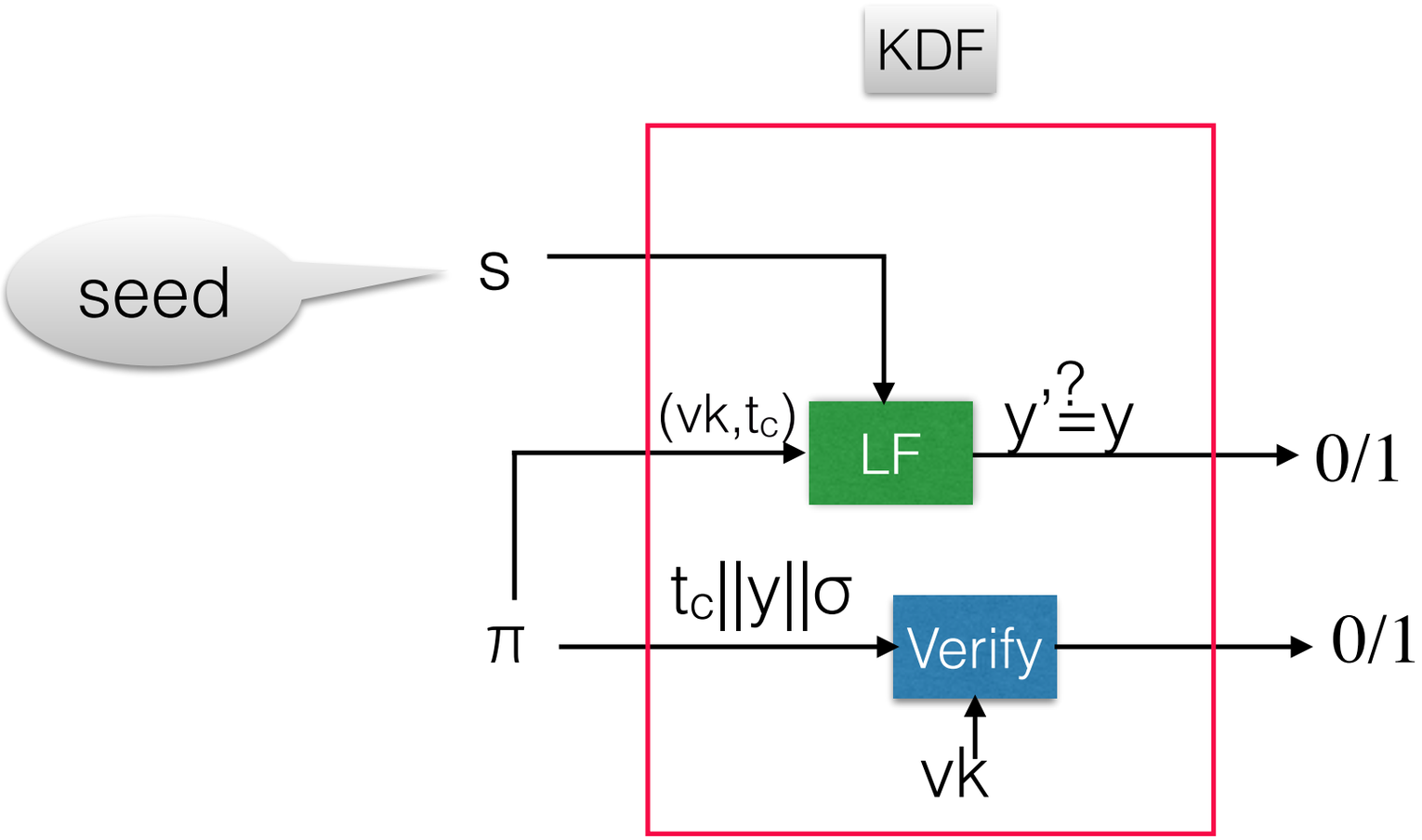
- Sample algorithm: seed s←S and proof π.
- (vk,sigk)← OTS.Gen



Continuous Non-Malleable KDF

Generic Construction

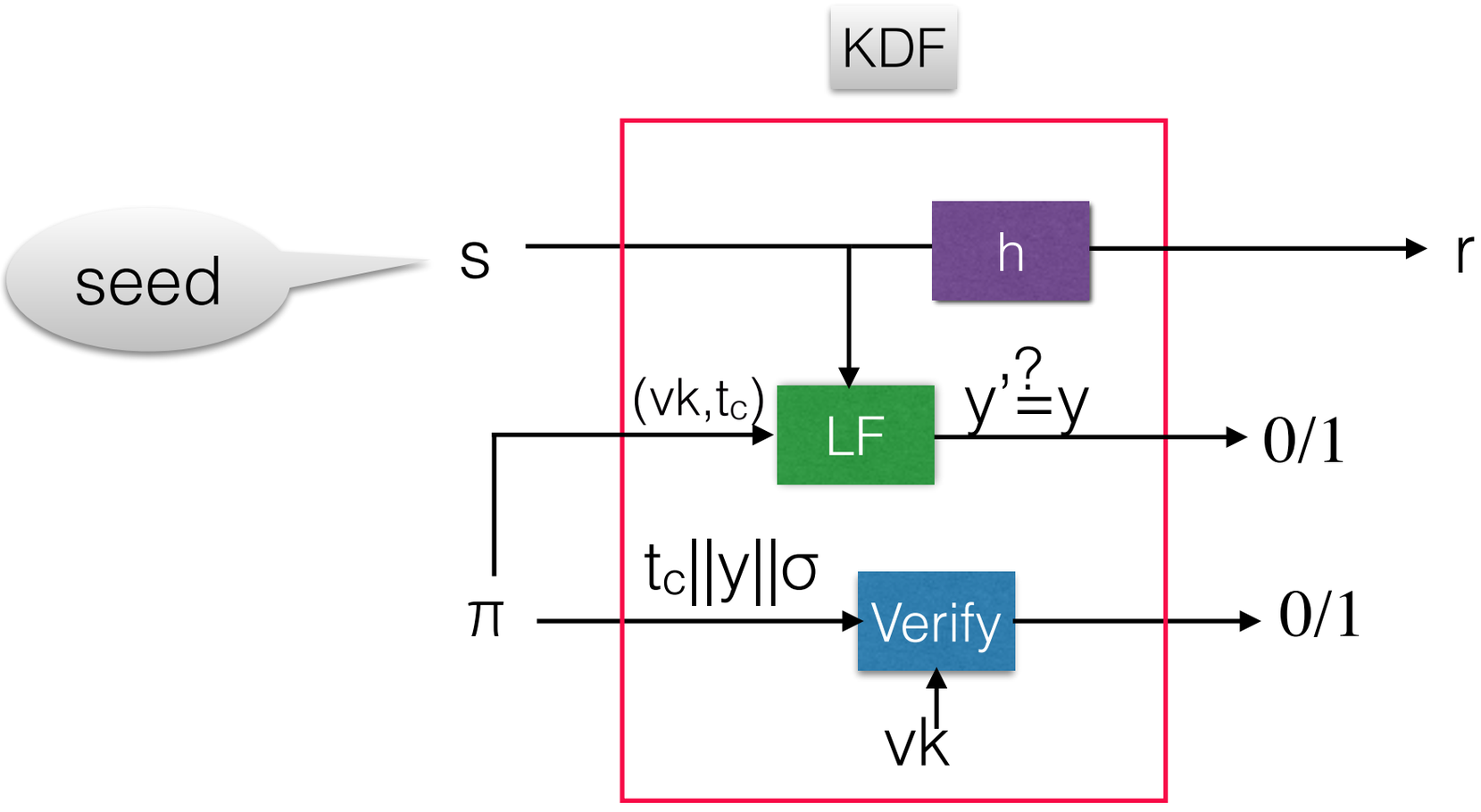
- KDF: input $\pi=(vk,t_c)||y||\sigma$, output $\perp$ or r.



Continuous Non-Malleable KDF

Generic Construction

- KDF: input $\pi=(vk,t_c)||y||\sigma$, output $\perp$ or r.



Continuous Non-Malleable KDF

Security Proof

- RKD functions: all degree-d polynomials over a finite field.
- Two properties of above RKD functions.
- Lemma 3: Suppose X be any random variable over some finite field and $H_\infty(X) \geq n$, then

$H_\infty(f(X)) \geq n - \log d$

f is non-constant

$\Pr[f(X)=X] \leq d/2^n$

f is not identity

Continuous Non-Malleable KDF

Security Proof

- Highlight the idea of our proof: reject all non trivial queries.

Target: $\pi^*=t^*||y^*||\sigma^*$ and $r^*=h(s^*)$ or random)

Query: $(f,\pi'=t'||y'||\sigma')$

Trivial queries without s^*:

- f is a constant function, output $KDF_{\pi'}(f)$
- f=id and $\pi'=\pi^*$, output the symbol same*

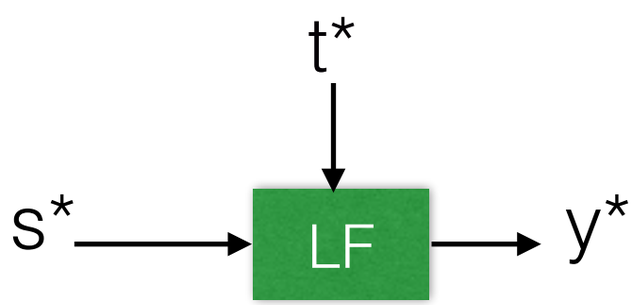
Continuous Non-Malleable KDF

Security Proof

- Highlight the idea of our proof:

Target: $\pi^*=t^*||y^*||\sigma^*$ and $r^*=h(s^*)$ or random) Query: $(f,\pi'=t'||y'||\sigma')$

(1) From injective to lossy: y^* reveals few information on s^*. $f(s^*)$ has high residual entropy.



Continuous Non-Malleable KDF

Security Proof

- Highlight the idea of our proof:

Target: $\pi^*=t^*||y^*||\sigma^*$ and $r^*=h(s^*)$ or random) Query: $(f,\pi'=t'||y'||\sigma')$

(1) From injective to lossy: y^* reveals few information on s^*. $f(s^*)$ has high residual entropy.

(2) One-time signature: t^* can not be re-used.

(3) Hard to generate a fresh non-injective tag even given t^*: t' is injective.

Continuous Non-Malleable KDF

Security Proof

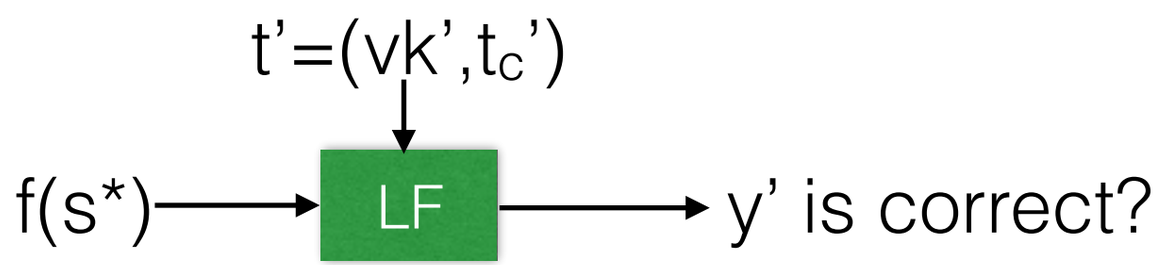
- Highlight the idea of our proof:

Target: $\pi^*=t^*||y^*||\sigma^*$ and $r^*=h(s^*)$ or random) Query: $(f,\pi'=t'||y'||\sigma')$

(1) From injective to lossy: y* reveals few information on s*. f(s*) has high residual entropy.

(2) One-time signature: t* can not be re-used.

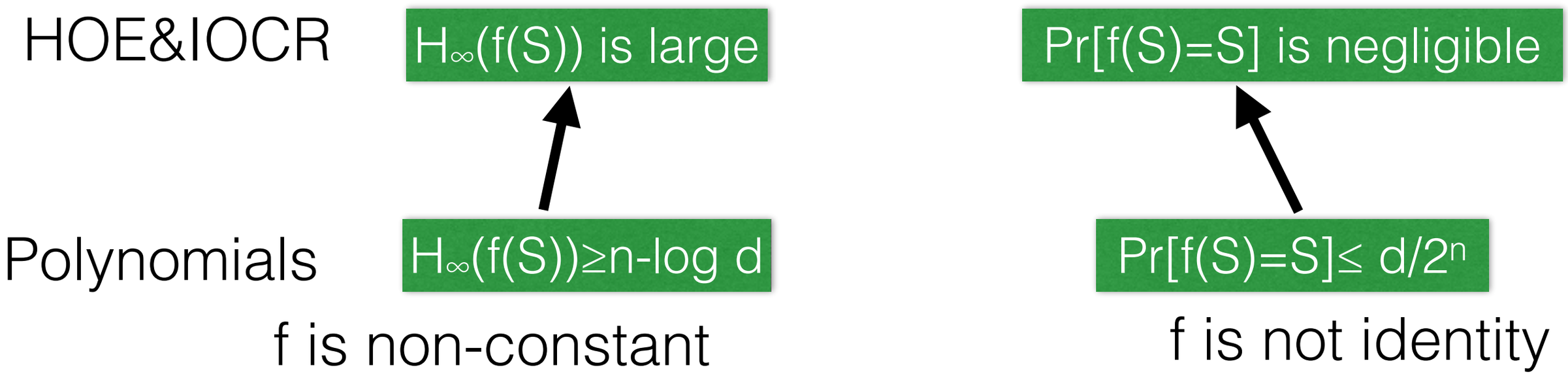
(3) Hard to generate a fresh non-injective tag even given t*: t' is injective.



Continuous Non-Malleable KDF

Generalization

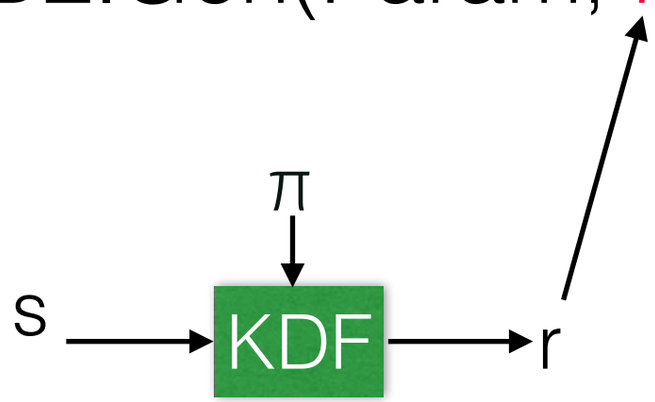
- From polynomial to High Output Entropy and Input-Output Collision Resistance.



Applications

RKA-secure IBE, PKE, Sig.

- (mpk,msk)←IBE.Gen(Param; r)



- mpk'=(mpk,π) and msk'=s
- Thm.: If cnm-KDF is secure w.r.t. F, the new IBE is RKA-secure w.r.t. the same RKD function class.

- RKA-IBE ⇒ RKA-PKE or RKA-Sig. [BCM11]
- Or direct construct RKA-PKE and RKA-Sig.

Conclusion

- A strengthened security model for non-malleable KDFs
- A generic construction of cnm-KDF w.r.t. polynomials or HOE&IOCR.
- Application to RKA-secure IBE, PKE and Signature.

Thanks!

http://eprint.iacr.org/2015/003