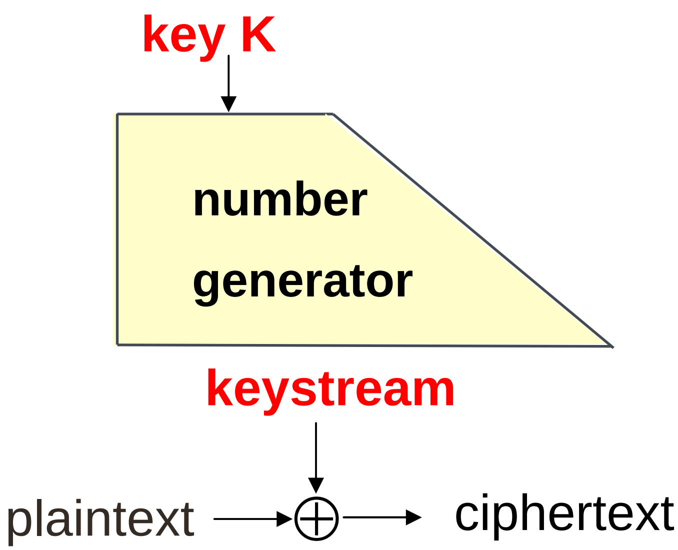
On the Security of IV Dependent Stream Ciphers

Côme Berbain and Henri Gilbert
France Telecom R&D

{firstname.lastname@orange-ftgroup.com}

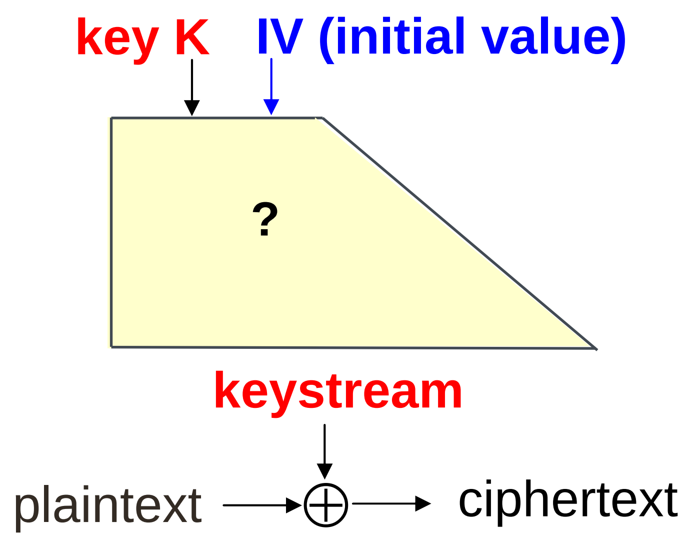
Stream Ciphers

- IV-less



- e.g. RC4, Shrinking Generator
- well founded theory [S81,Y82,BM84]
- practical limitations:
  - no reuse of K
  - synchronisation

- IV-dependent

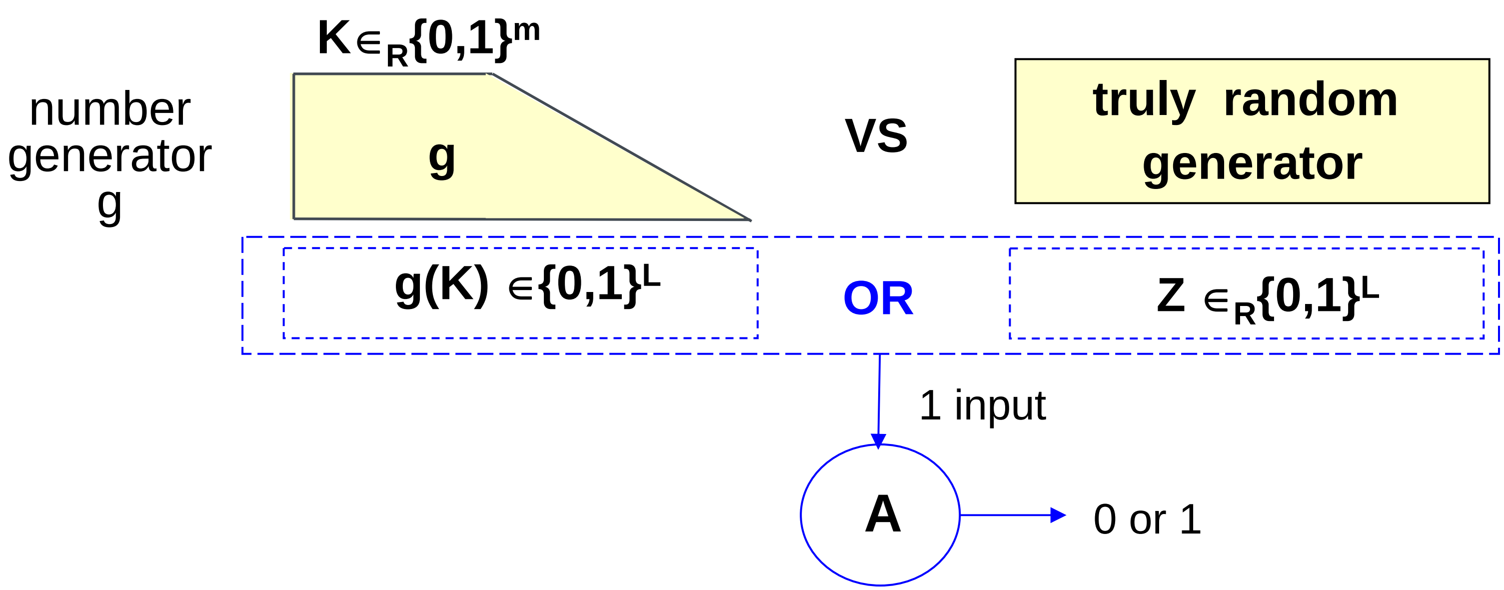


- e.g. SNOW, Scream, eSTREAM ciphers
- less unanimously agreed theory
- prior work [RC94, HN01, Z06]
- numerous chosen IV attacks
  - key and IV setup not well understood

Outline

- security requirements on IV-dependent stream ciphers
  - whole cipher
  - key and IV setup
- key and IV setup constructions satisfying these requirements
  - blockcipher based
  - tree based
- application example: QUAD
  - incorporate key and IV setup in QUAD's provable security argument

Security in IV-less case: PRNG notion



A tests number distributions:

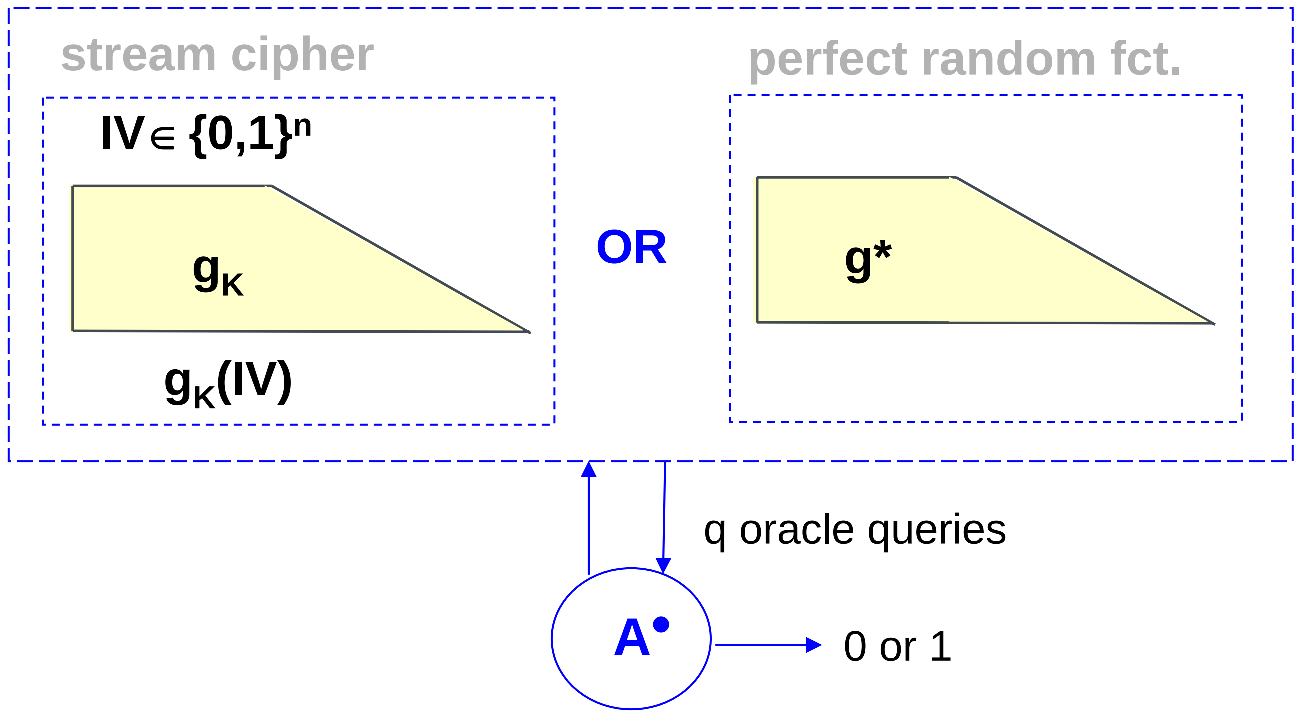
$$\mathrm{Adv}_g^{\mathrm{PRNG}}(A) = \left|\Pr_K[A(g(K)) = 1] - \Pr_Z[A(Z) = 1]\right|$$

$$\mathrm{Adv}_g^{\mathrm{PRNG}}(t) = \max_{A,T(A)\le t}\left(\mathrm{Adv}_g^{\mathrm{PRNG}}(A)\right)$$

g is a secure cipher ⇔ g is a PRNG ⇔ $\mathrm{Adv}_g^{\mathrm{PRNG}}(t < 2^{80}) << 1$

Security in IV-dependent case: PRF notion

function generator $G = \{g_K\}$



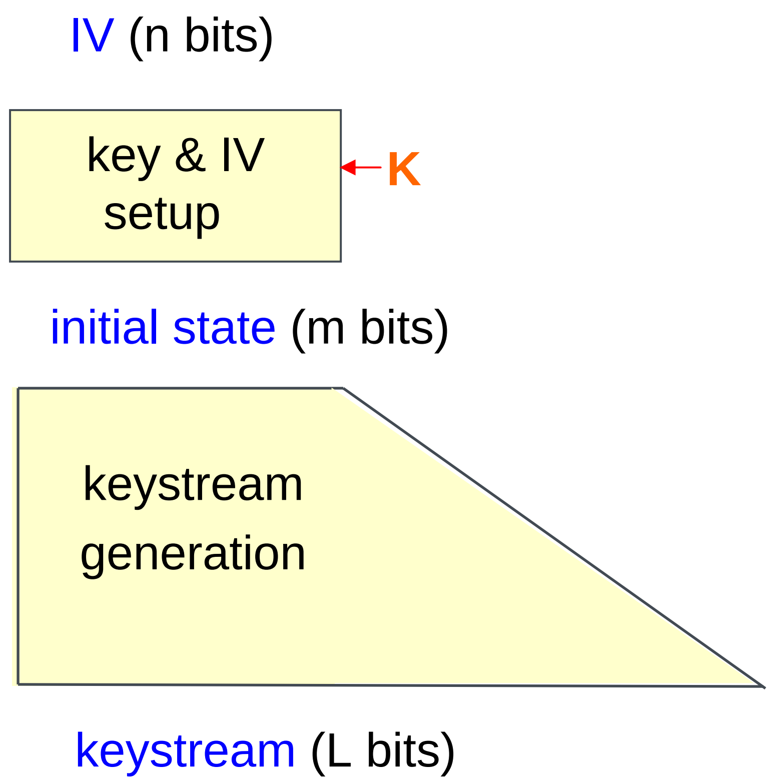
A tests function distributions:

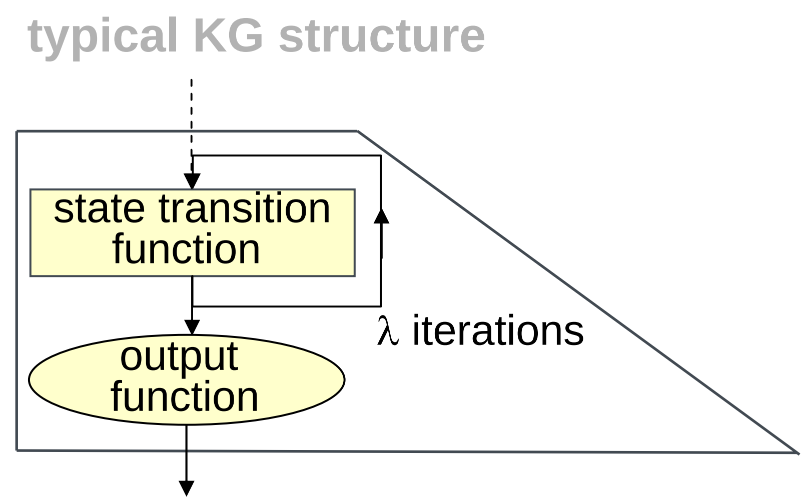
$$\mathrm{Adv}_G^{PRF}(A) = \left|\Pr[A^{g_K} = 1] - \Pr[A^{g^*} = 1]\right|$$

$$\mathrm{Adv}_G^{PRF}(t,q) = \max_A\left(\mathrm{Adv}_G^{PRF}(A)\right)$$

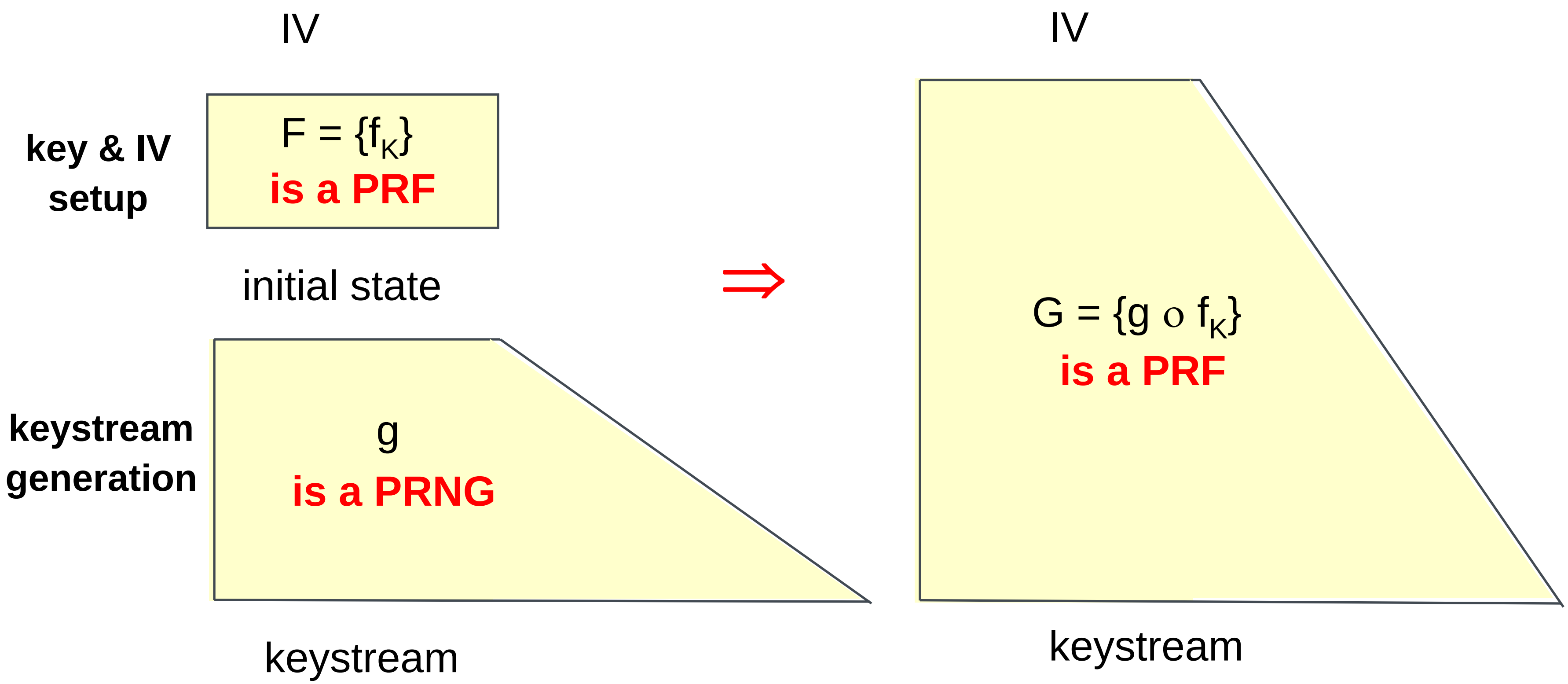
G is a secure cipher ⇔ G is a PRF ⇔ $\mathrm{Adv}_G^{PRF}(t < 2^{80}, 2^{40}) \ll 1$

Structure of the stream ciphers considered here





Security: sufficient conditions

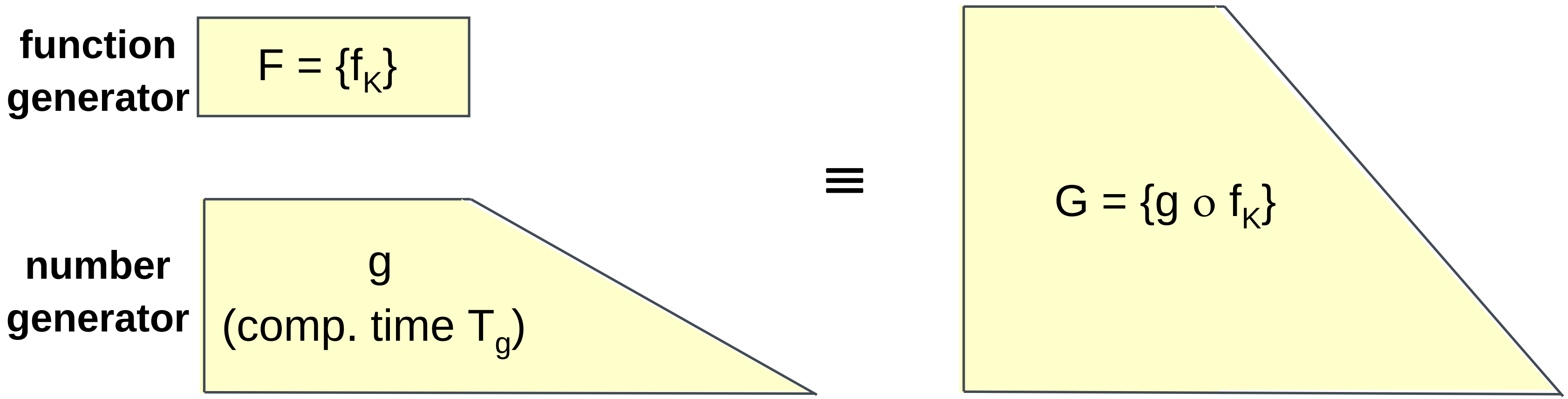


[informally]: the **key & IV setup** is a PRF and the **keystream generator** is a PRNG

⇒ the whole stream cipher is secure

This is due to a simple composition theorem

- Composition of $\{f_K\}$ and g

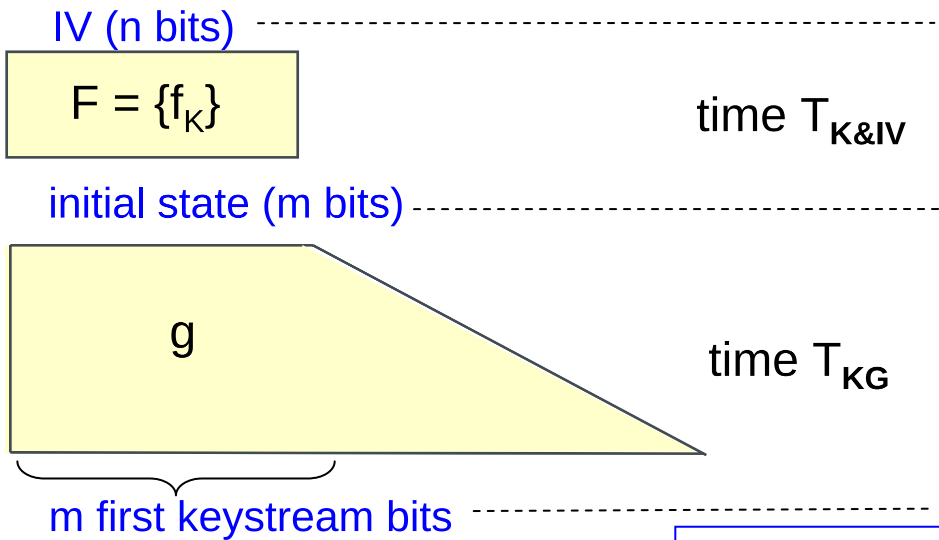


- Composition Theorem:

$$\mathrm{Adv}_G^{PRF}(t,q) \le \mathrm{Adv}_F^{PRF}(t',q) + q\,\mathrm{Adv}_g^{PRNG}(t')$$

where $t' = t + qT_g$

Key & IV setup = PRF is "almost" a necessary condition



time $T_{K\&IV}$ (key and IV setup)

time T_{KG} (keystream generation)

$$T_{K\&IV} + T_{KG} \geq T_{PRF}$$

(where T_{PRF} is the time needed by the fastest n-bit to m-bit PRF)

For a fast cipher, T_{KG} is small, so $T_{K\&IV}$ cannot be much lower than T_{PRF}

Key & IV setup: candidate PRF constructions

- **Block cipher based (not detailed here)**

  Examples: LEX (based on AES), Sosemanuk (based on Serpent)

  Pros: more conservative than many existing constructions

  Cons: heterogeneous construction ⇒ increased implementation complexity (except for LEX)

- **Tree based (detailed in the sequel)**

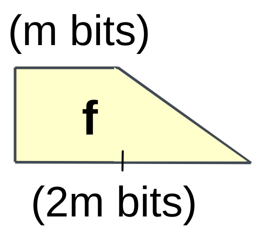
  Example: QUAD

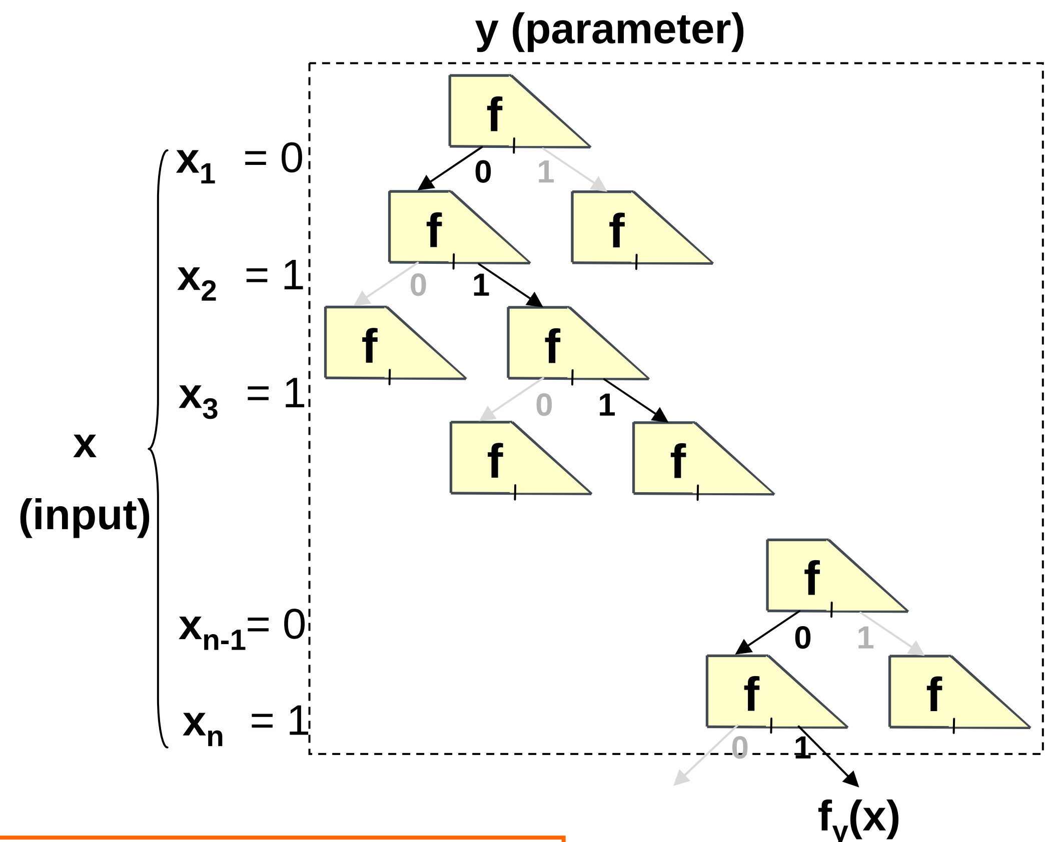
  Conducting idea: re-use essentially the same PRNG as in the keystream generation

  Pros: low implementation complexity   Cons: relatively slow

Tree based construction [GGM86]

m-bit to 2m-bit PRNG f $\Rightarrow$ n-bit to m-bit PRF $F = \{f_y\}$





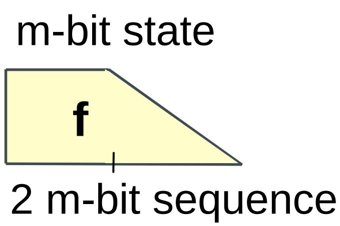
Theorem[≈GGM86]:

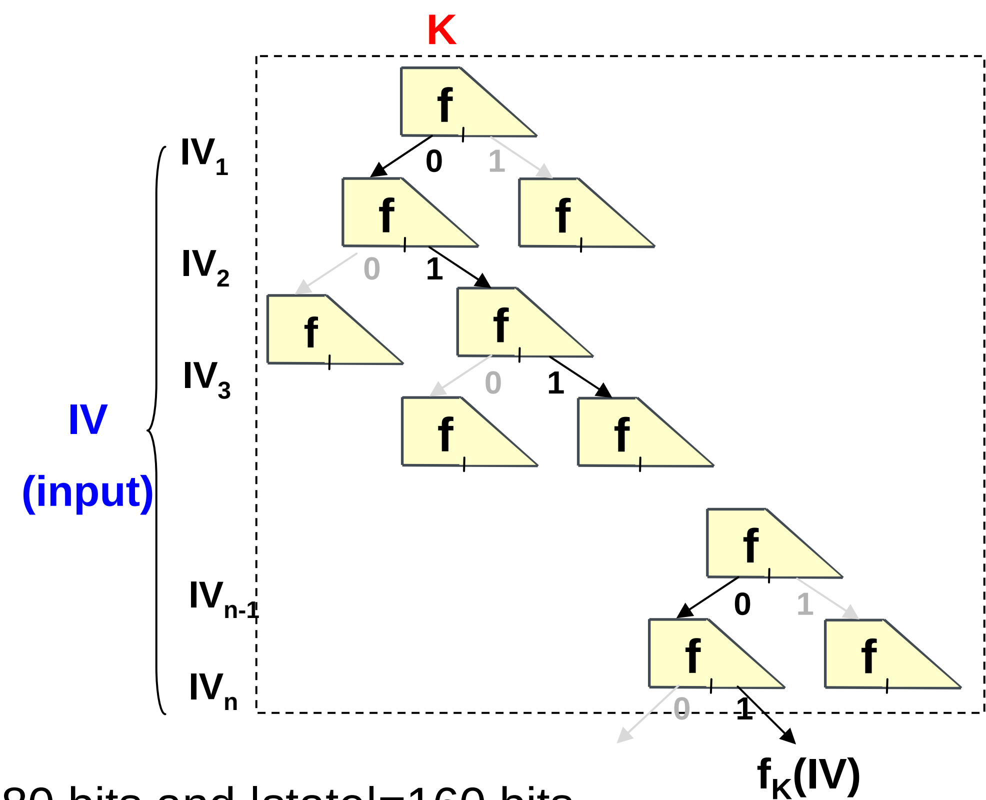
$$Adv_F^{PRF}(t,q) \leq nq\,Adv_f^{PRNG}(t')$$

where $t' = t + q(n+1)T_f$

Tree based key & IV setup

truncated IV-less cipher ⇒ key and IV setup





Is this practical?

Cons: relatively slow. If |IV|=80 bits and |state|=160 bits,

key & IV setup ≡ generation of 3200 keystream bytes

Pros: very low extra implementation complexity in hardware

The Stream Cipher QUAD [BGP06]

- **Based on the multivariate quadratic problem (MQ)**

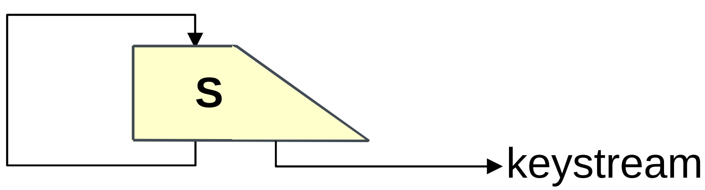
  Given a system of m quadratic equations in n variables over $GF(q)$

  $$Q_k(x_1,\dots,x_n) = \sum_{i\le j} \alpha_{i,j}^k x_i x_j + \sum_i \beta_i^k x_i + \gamma^k = y_k, k = 1,\dots,m$$

  Find a solution $x = (x_1,\dots,x_n) \in GF(q)^n$ (if any)

  - NP hard even over GF(2)
  - best solving algorithms so far are exponential [Faugère, Bardet]

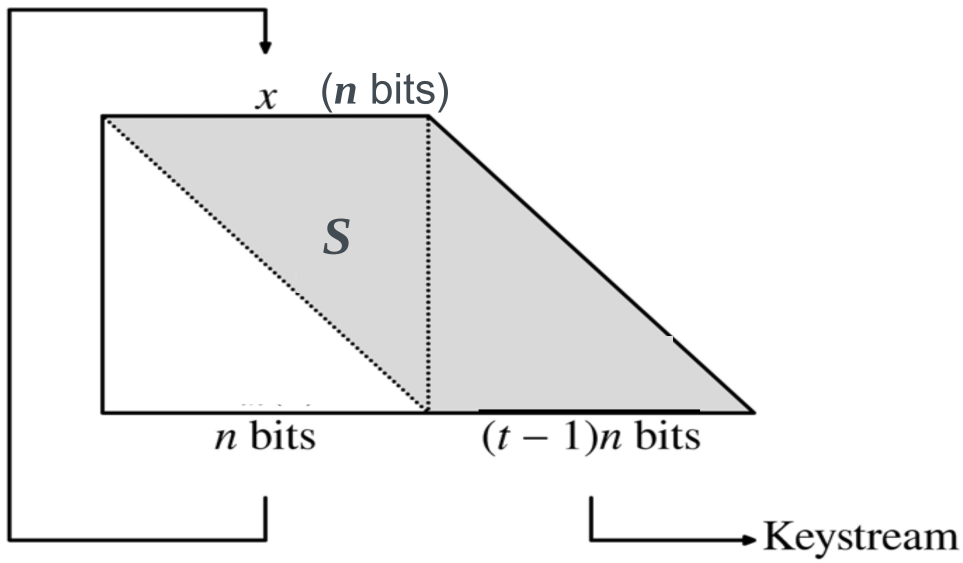
- **QUAD iterates a fixed quadratic function S**



QUAD: keystream generation

- internal state: $x = (x_1,\ldots,x_n) \in GF(q)^n$
- fixed public quadratic function S: n var., m = tn eq. (typically 2n eq.)

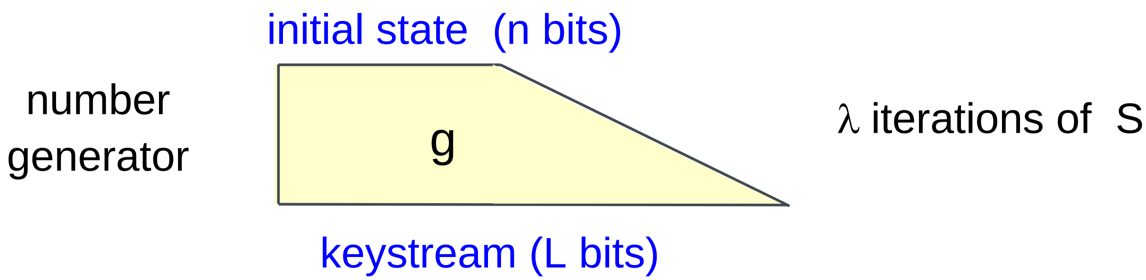
q = 2



- recommended parameters: q=2, n=160 bits, t=2

Security argument for the keystream generation

- Keystream generation, **GF(2) case**



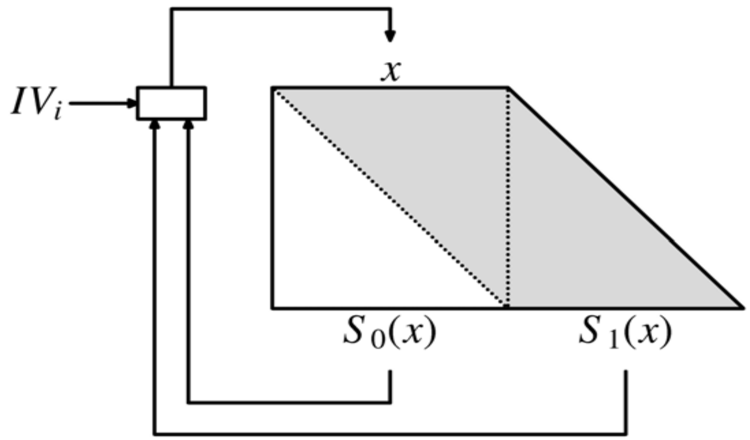
- **Th [BGP06]:** in the GF(2) case, **if** there exists a distinguisher for g allowing to distinguish a sequence of $L = \lambda(t-1)n$ keystream bits associated with a random quadratic systems S and a random initial state value x in time T with advantage ε, **then** there is an MQ solver that solves a random instance of MQ in time $T' \cong O(\frac{n^2\lambda^2 T}{\varepsilon^2})$ with probability $\varepsilon' = \frac{\varepsilon}{2^2\lambda}$.

- **Example of application:** q=2, n = 350 bits, t = 2, $L=2^{40}$, $T=2^{80}$, ε = 1%

(no such concrete reduction for the recommend value n = 160)

QUAD: Key and IV Setup

- uses two public quadratic functions S_0 and S_1 of n eq. in n var. each



- set x with the key K
- for each IV bit IV_i:
  - if $IV_i = 0$ then update x with $S_0(x)$
  - if $IV_i = 1$ then update x with $S_1(x)$

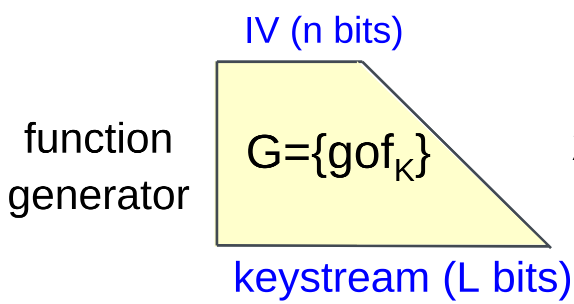
tree based construction

- runup: clock the cipher *n* times without outputting the keystream

typical key and IV lengths: 160 bits each

Extending the proof to the whole cipher

- **Whole cipher, GF(2) case**



$t = 2$

λ iterations of S $\quad (\lambda = \frac{L + n^2}{n})$

- **Th:** in the GF(2) case, **if** there exists a (T,q) PRF-distinguisher for the family G of IV to keystream functions associated with a random key and a random quadratic systems *S* with PRF-advantage ε, **then** there is an MQ solver that solves a random instance of MQ in time $T' \cong O(\frac{n^2\lambda^2 q^2 T}{\varepsilon^2})$ with probability at least $\varepsilon' = \frac{\varepsilon}{3.2^3 q\lambda}$.

- **Example of application:** q=2, n = 760 bits, t = 2, $L=2^{40}$, $T=2^{80}$, ε = 1%

Conclusions

- **Requirements:** a PRF is needed

- **Conservative IV setup**
  - seems demanding w.r.t. computational complexity
  - is not demanding w.r.t. implementation complexity

- **"Provable security"** can be extended to IV-dependent stream ciphers