f-Divergences in Statistical Security Proofs

Thomas Prest

PQShield

2021 EWHA-KMS International Workshop on Cryptography

The statistical distance

Given two distributions $\boldsymbol{P}, \boldsymbol{Q}$ over Ω, the statistical distance between them is:

$$\Delta_{\mathrm{SD}}(\boldsymbol{P}; \boldsymbol{Q}) = \frac{1}{2} \sum_{x \in \Omega} |\boldsymbol{P}(x) - \boldsymbol{Q}(x)|$$

Useful properties:

1. **Data-processing inequality:** Given a (randomised) function $g : \mathbb{R} \to \mathbb{R}$,

$$\Delta_{\mathrm{SD}}(g(\boldsymbol{P}); g(\boldsymbol{Q})) \leq \Delta_{\mathrm{SD}}(\boldsymbol{P}; \boldsymbol{Q}).$$

2. **Probability-preservation property (PPP):** Given an arbitrary event $E \subseteq \Omega$:

$$|\boldsymbol{P}(E) - \boldsymbol{Q}(E)| \leq \Delta_{\mathrm{SD}}(\boldsymbol{P}; \boldsymbol{Q}).$$

3. **Tensorisation (sub-additivity):** $\Delta_{\mathrm{SD}}(\prod_i \boldsymbol{P}_i; \prod_i \boldsymbol{Q}_i) \leq \sum_i \Delta_{\mathrm{SD}}(\boldsymbol{P}_i; \boldsymbol{Q}_i)$
4. **Triangle inequality:** $\Delta_{\mathrm{SD}}(\boldsymbol{P}; \boldsymbol{R}) \leq \Delta_{\mathrm{SD}}(\boldsymbol{P}; \boldsymbol{Q}) + \Delta_{\mathrm{SD}}(\boldsymbol{Q}; \boldsymbol{R})$
5. **Symmetry:** $\Delta_{\mathrm{SD}}(\boldsymbol{Q}; \boldsymbol{P}) = \Delta_{\mathrm{SD}}(\boldsymbol{P}; \boldsymbol{Q})$

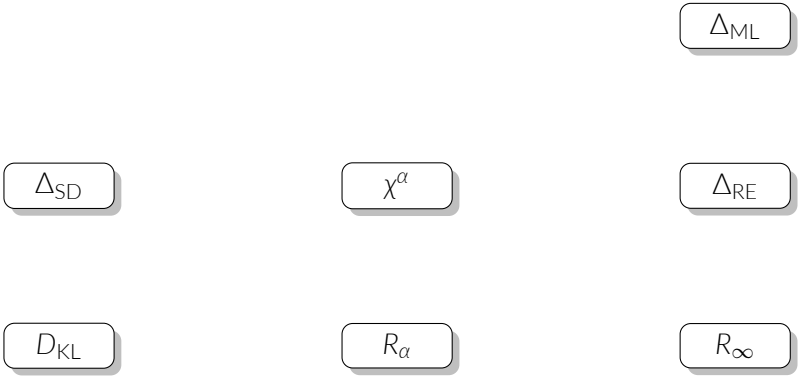


Figure 1: Relations between statistical distance (Δ_{SD}), Kullback-Leibler divergence (D_{KL}), χ^{α} divergence [Vaj73], Rényi divergence (R_{α}), max-log distance (Δ_{ML}), and relative error (Δ_{RE}).

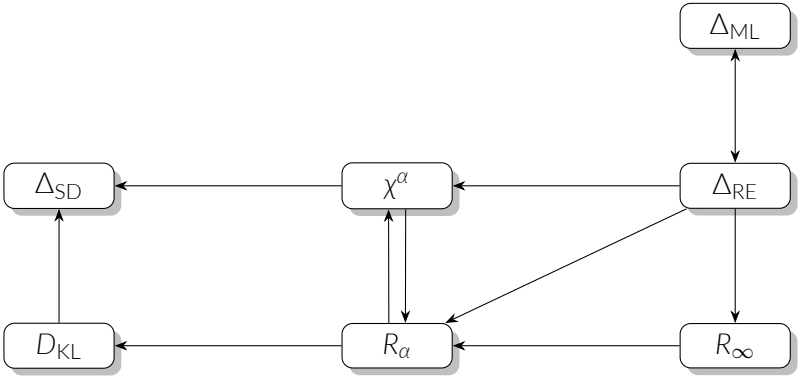


Figure 1: Relations between statistical distance (Δ_{SD}), Kullback-Leibler divergence (D_{KL}), χ^{α} divergence [Vaj73], Rényi divergence (R_{α}), max-log distance (Δ_{ML}), and relative error (Δ_{RE}). $\boxed{\mathrm{X}} \longleftarrow \boxed{\mathrm{Y}}$ means there exists an inequality of the form $X \leq g(Y)$.

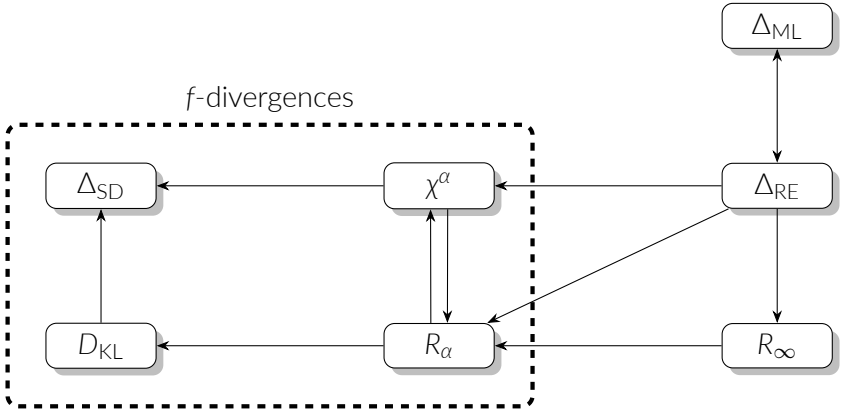


Figure 1: Relations between statistical distance (Δ_{SD}), Kullback-Leibler divergence (D_{KL}), χ^α divergence [Vaj73], Rényi divergence (R_α), max-log distance (Δ_{ML}), and relative error (Δ_{RE}). $\boxed{\mathrm{X}} \longleftarrow \boxed{\mathrm{Y}}$ means there exists an inequality of the form $X \leq g(Y)$.

What are f-divergences?

f-divergence [Mor63, Csi63, AS66]

Let $f : \mathbb{R} \to \mathbb{R}$ be a convex function such that $f(1) = 0$.
The f-divergence between $\boldsymbol{P}$ and $\boldsymbol{Q}$ is:

$$\mathrm{Div}_f(\boldsymbol{P}; \boldsymbol{Q}) = \mathbb{E}_{\boldsymbol{Q}}\left[f\left(\frac{\boldsymbol{P}}{\boldsymbol{Q}}\right)\right] = \sum_{x \in \mathrm{Supp}\,\boldsymbol{Q}} f\left(\frac{\boldsymbol{P}}{\boldsymbol{Q}}\right) \tag{1}$$

Examples

- Statistical distance $\Delta_{\mathrm{SD}}(\boldsymbol{P};\boldsymbol{Q})$
  - $f(x) = \frac{1}{2}|x-1|$
  - Ubiquitous in crypto
- Kullback-Leibler divergence $D_{\mathrm{KL}}(\boldsymbol{P};\boldsymbol{Q})$
  - $f(x) = x \ln x$
  - Ubiquitous in information theory, common in crypto
- Hellinger distance $H^2(\boldsymbol{P};\boldsymbol{Q})$
  - $f(x) = (\sqrt{t}-1)^2$
  - Probabilistic analog of the Euclidean distance
- Rényi divergence $R_\alpha(\boldsymbol{P};\boldsymbol{Q})$
  - $R_\alpha^{\alpha-1} - 1$ is an f-divergence for $f(x) = x^\alpha - 1$
  - Common in lattice-based crypto

Why do we care?

Besides a clean abstraction, f-divergences provide a few properties for free:

- **Data-processing inequality:**

$$\mathrm{Div}_f(g(\boldsymbol{P}); g(\boldsymbol{Q})) \leq \mathrm{Div}_f(\boldsymbol{P}; \boldsymbol{Q}) \tag{2}$$

- **Probability-preservation property (PPP):**
  - Consequence of the data-processing inequality
  - Set g so that $g(\boldsymbol{P})$ (resp. $g(\boldsymbol{Q})$) is the outcome (0/1) of a game
- Joint convexity

But in general:

- No tensorisation
- No triangle inequality
- No symmetry

Why not stick to the statistical distance?

The statistical distance Δ_{SD} is a one-size-fits-all divergence, but not always the best:

- The Rényi (R_α) and Kullback-Leibler (D_{KL}) divergences are more tightly connected to {Shannon, collision, min-}entropies
- Hellinger, Kullback-Leibler and χ^2 divergences' tensorisation properties may provide tighter proofs
- The Rényi divergence has a multiplicative probability-preservation property

Rest of this talk: a few selected examples using the Rényi divergence.

Rényi divergence

Let $\boldsymbol{P}, \boldsymbol{Q}$ such that $\operatorname{Supp} \boldsymbol{P} \subseteq \operatorname{Supp} \boldsymbol{Q} = \Omega$. The Rényi divergence of order $\alpha \in [1, \infty]$ between $\boldsymbol{P}$ and $\boldsymbol{Q}$ is defined, for $1 < \alpha < \infty$, as:

$$R_\alpha(\boldsymbol{P}; \boldsymbol{Q}) := \left(\sum_{x \in X} \frac{\boldsymbol{P}(x)^\alpha}{\boldsymbol{Q}(x)^{\alpha-1}} \right)^{\frac{1}{\alpha-1}}, \tag{3}$$

with the two limit cases $R_1(\boldsymbol{P}; \boldsymbol{Q}) = e^{D_{\mathrm{KL}}(\boldsymbol{P};\boldsymbol{Q})}$ and $R_\infty(\boldsymbol{P}; \boldsymbol{Q}) = \max_{x \in \Omega} \frac{\boldsymbol{P}(x)}{\boldsymbol{Q}(x)}$.

Properties: The Rényi divergence is sub-multiplicative (tensorisation) and verifies a weak triangle inequality, but is not symmetric.

Fun fact: the Shannon (H_1), collision (H_2) and min-entropy (H_∞) are part of the class of Rényi entropies H_α, which can be defined as:

$$H_\alpha(X) = \log_2 |\Omega| - \log_2 R_\alpha(\boldsymbol{P}; \boldsymbol{U}), \tag{4}$$

where $X \sim \boldsymbol{P}$, and $\boldsymbol{U}$ is the uniform distribution over Ω.

Probability-preservation properties (PPP)

Let $p = \boldsymbol{P}(E)$ and $q = \boldsymbol{Q}(E)$, so that $0 \leq p, q \leq 1$. This PPP is immediate from (2):

$$\frac{p^\alpha}{q^{\alpha-1}} + \frac{(1-p)^\alpha}{(1-q)^{\alpha-1}} \leq R_\alpha(\boldsymbol{P};\boldsymbol{Q})^{\alpha-1}. \tag{5}$$

(5) admits two special cases:

- An additive PPP [MTMH19]:

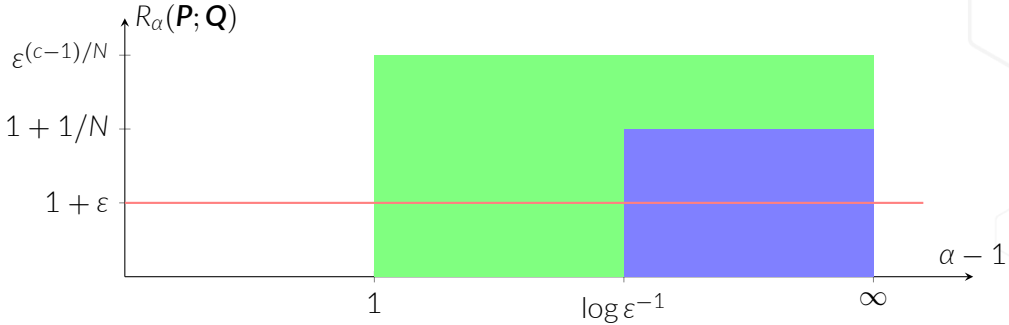
$$|p-q| \leq \sqrt{(R_2(\boldsymbol{P};\boldsymbol{Q})-1)\cdot q} \tag{6}$$

- A multiplicative PPP [LSS14]:

$$p \leq (q \cdot R_\alpha(\boldsymbol{P};\boldsymbol{Q}))^{(\alpha-1)/\alpha}, \tag{7}$$
$$p \leq q \cdot R_\infty(\boldsymbol{P};\boldsymbol{Q}). \tag{8}$$

If N queries to $\boldsymbol{P}$ (resp. $\boldsymbol{Q}$), replace R_α with R_α^N.

Let ε be the advantage when using $\boldsymbol{Q}$ (search: $q = \varepsilon$, decision: $q = 1/2 + \varepsilon$). We want to upper bound the advantage when using $\boldsymbol{P}$. Assume N queries.



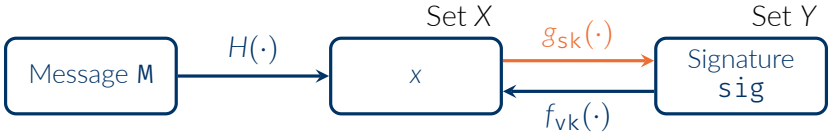
- In green: reductions with polynomial loss (c is a constant > 0)
  - For search problems using (7), see [BLL+15]
  - For decision problems *with the public sampleability property* [BLL+15, MTMH19]
- In blue: search reductions with $O(1)$ loss using (7), see [Pre17]
  - Decision $\Rightarrow$ ad-hoc techniques, e.g. problem switching [NAB+20, DSSS21, LW21]:

$$\text{IND-CPA} \Rightarrow \text{OW-CPA} \Rightarrow \text{IND-CCA} \tag{9}$$

- Below the red line (—): no real advantage over statistical distance

Application 1: Trapdoor Sampling

Most lattice-based H&S constructions [GPV08, MP12, DLP14, PFH+17] rely on trapdoor preimage sampleable functions (TPSFs).



We require that there exists $\boldsymbol{Y}$ of support Y such that for almost all $x \in X$:

$$\{y \leftarrow \boldsymbol{Y} | f_{\mathsf{vk}}(y) = x\} \approx_s \{y \leftarrow g_{\mathsf{sk}}(x)\} \tag{10}$$

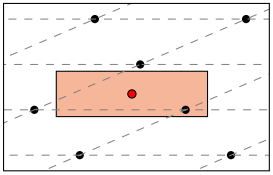
Fun fact/digression: relaxing (10) to hold *on average* over x unlocks more (efficient) constructions [CGM19, DST19, CD20].

Question: Why does $\approx_s$ matter in (10), and how do we assess it?

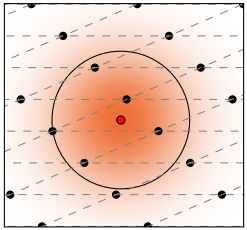
Trapdoor samplers (contained)

Most trapdoor samplers can be seen as randomised variants of (polynomial-time) approximate CVP solvers (e.g. Babai's *nearest plane* and *round-off* algorithms).

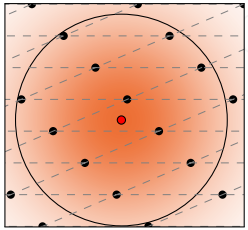
σ too small



The "right" σ

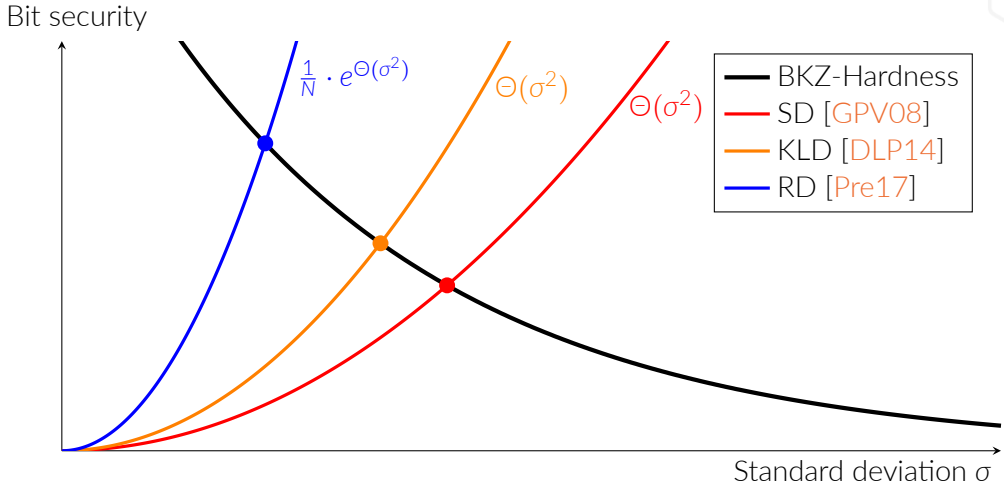


σ too big



1. σ too small $\Rightarrow$ vulnerable to learning attacks [NR06, DN12]
2. σ too large $\Rightarrow$ suboptimal for cryptography

Standard deviation analysis



For Falcon [PFH+17] and $N = 2^{64}$, we gain $\sim$ 30 bits of security (compared to SD).

Application 2: Prime Number Generation in RSA

Prime numbers in RSA

In RSA, the public key is $p \cdot q$.

- Ideally, p, q should be uniform in some high-entropy interval, say $[0, 2^\ell)$
- In practice, most algorithms are very far from providing this guarantee

Can prime number generation be a point of failure in practice? Yes:

1. **Highly structured distributions:** p, q may be recovered by non-generic methods
   - See Coppersmith's attack [Cop96] and its follow-up ROCA [NSS+17]
2. **Insufficient entropy:** distinct public keys may have common factors
   - Compute pairwise GCDs to recover private keys [HDWH12, LHA+12, BCC+13, HFH16, BSTS16, AR18, Kil19]

This is why several prime number generators have been proposed [BD93, Mau95, JPV00, FT14, FT19].

PRIMEINC [BD93]

A simple and popular (PyCrypto, OpenSSL) prime number generator.

PRIMEINC(ℓ, s)

1. Sample odd p uniformly in $\{2^{\ell-1}, \ldots, 2^{\ell}\}$, set $k \leftarrow 0$.
2. While ($k \leq s$) & (p is not prime), set $p \leftarrow p + 2$ and $k \leftarrow k + 1$.
3. If (p is prime) & ($p < 2^{\ell}$), return p, else restart.

Is it secure?

→ **Maybe?**

$$\frac{H_1(PRIMEINC())}{H_1(Uniform)} \underset{\ell \to \infty}{\longrightarrow} 1 \qquad ([BD93])$$

→ **Maybe not?**

$$\Delta_{SD}(PRIMEINC(); Uniform) \underset{\ell \to \infty}{\longrightarrow} 0.86 \qquad ([FT19])$$

Under appropriate conditions (mostly the same as [FT19]):

$$R_\infty(\mathit{PRIMEINC}(); \mathit{Uniform}) = 1 + O(1) \tag{11}$$

Consequence 1: From (8), an RSA-based scheme secure when p, q are sampled uniformly, remains secure (in the single-user setting) when $p, q \leftarrow \mathit{PRIMEINC}()$.

It follows from (11) that:

$$H_2(\mathit{PRIMEINC}()) \geq \ell - O(1) \tag{12}$$

Consequence 2: PRIMEINC is impervious against GCD/common factors attacks.

Conclusion

It is often fruitful to try other divergences than the statistical distance:

- Rényi divergence
  - Lattice-based cryptography [LSS14, BLL+15, Pre17]
  - Differential privacy [Mir17, MTMH19]
  - Prime number generators [AP20]
  - Leakage-resilient cryptography [PGMP19]
- Kullback-Leibler divergence is implicit in the definition of mutual information
- Hellinger distance
  - Key-alternating ciphers [Ste12]
  - Strong randomness extractors [Yas21]
- χ^2 divergence in symmetric cryptography [DHT17]

Not to mention relaxing [DST19, CD20] or strengthening [PGMP19] notions.

Thank You


Marc Abboud and Thomas Prest.
Cryptographic divergences: New techniques and new applications.
In Clemente Galdi and Vladimir Kolesnikov, editors, *SCN 20*, volume 12238 of *LNCS*, pages 492–511. Springer, Heidelberg, September 2020.


Nils Amiet and Yolan Romailler.
Reaping and breaking keys at scale: when crypto meets big data, 2018.
https://research.kudelskisecurity.com/2018/10/16/reaping-and-breaking-keys-at-scale-when-crypto-meets-big-data/


S. M. Ali and S. D. Silvey.
A general class of coefficients of divergence of one distribution from another.
Journal of the Royal Statistical Society. Series B (Methodological), 28(1):131–142, 1966.


Daniel J. Bernstein, Yun-An Chang, Chen-Mou Cheng, Li-Ping Chou, Nadia Heninger, Tanja Lange, and Nicko van Someren.
Factoring RSA keys from certified smart cards: Coppersmith in the wild.
In Kazue Sako and Palash Sarkar, editors, *ASIACRYPT 2013, Part II*, volume 8270 of *LNCS*, pages 341–360. Springer, Heidelberg, December 2013.


Jørgen Brandt and Ivan Damgård.

On generation of probable primes by incremental search.
In Ernest F. Brickell, editor, *CRYPTO'92*, volume 740 of *LNCS*, pages 358–370. Springer, Heidelberg, August 1993.


Shi Bai, Adeline Langlois, Tancrède Lepoint, Damien Stehlé, and Ron Steinfeld.
Improved security proofs in lattice-based cryptography: Using the Rényi divergence rather than the statistical distance.
In Tetsu Iwata and Jung Hee Cheon, editors, *ASIACRYPT 2015, Part I*, volume 9452 of *LNCS*, pages 3–24. Springer, Heidelberg, November / December 2015.


Mihai Barbulescu, Adrian Stratulat, Vlad Traista-Popescu, and Emil Simion.
RSA weak public keys available on the internet.
In *SECITC*, volume 10006 of *Lecture Notes in Computer Science*, pages 92–102, 2016.


André Chailloux and Thomas Debris-Alazard.
Tight and optimal reductions for signatures based on average trapdoor preimage sampleable functions and applications to code-based signatures.
In Aggelos Kiayias, Markulf Kohlweiss, Petros Wallden, and Vassilis Zikas, editors, *PKC 2020, Part II*, volume 12111 of *LNCS*, pages 453–479. Springer, Heidelberg, May 2020.


Yilei Chen, Nicholas Genise, and Pratyay Mukherjee.

Approximate trapdoors for lattices and smaller hash-and-sign signatures.
In Steven D. Galbraith and Shiho Moriai, editors, *ASIACRYPT 2019, Part III*, volume 11923 of *LNCS*, pages 3–32. Springer, Heidelberg, December 2019.

Don Coppersmith.
Finding a small root of a bivariate integer equation; factoring with high bits known.
In Ueli M. Maurer, editor, *EUROCRYPT'96*, volume 1070 of *LNCS*, pages 178–189. Springer, Heidelberg, May 1996.

Imre Csiszár.
Eine informationstheoretische ungleichung und ihre anwendung auf den beweis der ergodizitat von markoffschen ketten.
Magyar. Tud. Akad. Mat. Kutató Int. Közl, 8:85–108, 1963.

Wei Dai, Viet Tung Hoang, and Stefano Tessaro.
Information-theoretic indistinguishability via the chi-squared method.
In Jonathan Katz and Hovav Shacham, editors, *CRYPTO 2017, Part III*, volume 10403 of *LNCS*, pages 497–523. Springer, Heidelberg, August 2017.

Léo Ducas, Vadim Lyubashevsky, and Thomas Prest.
Efficient identity-based encryption over NTRU lattices.

In Palash Sarkar and Tetsu Iwata, editors, *ASIACRYPT 2014, Part II*, volume 8874 of *LNCS*, pages 22–41. Springer, Heidelberg, December 2014.


Léo Ducas and Phong Q. Nguyen.
Learning a zonotope and more: Cryptanalysis of NTRUSign countermeasures.
In Xiaoyun Wang and Kazue Sako, editors, *ASIACRYPT 2012*, volume 7658 of *LNCS*, pages 433–450. Springer, Heidelberg, December 2012.


Julien Devevey, Amin Sakzad, Damien Stehlé, and Ron Steinfeld.
On the integer polynomial learning with errors problem.
In Garay [Gar21], pages 184–214.


Thomas Debris-Alazard, Nicolas Sendrier, and Jean-Pierre Tillich.
Wave: A new family of trapdoor one-way preimage sampleable functions based on codes.
In Steven D. Galbraith and Shiho Moriai, editors, *ASIACRYPT 2019, Part I*, volume 11921 of *LNCS*, pages 21–51. Springer, Heidelberg, December 2019.


Pierre-Alain Fouque and Mehdi Tibouchi.
Close to uniform prime number generation with fewer random bits.

In Javier Esparza, Pierre Fraigniaud, Thore Husfeldt, and Elias Koutsoupias, editors, *ICALP 2014, Part I*, volume 8572 of *LNCS*, pages 991–1002. Springer, Heidelberg, July 2014.


Pierre-Alain Fouque and Mehdi Tibouchi.
Close to uniform prime number generation with fewer random bits.
IEEE Trans. Information Theory, 65(2):1307–1317, 2019.


Juan Garay, editor.
PKC 2021, Part I, volume 12710 of *LNCS*. Springer, Heidelberg, May 2021.


Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan.
Trapdoors for hard lattices and new cryptographic constructions.
In Richard E. Ladner and Cynthia Dwork, editors, *40th ACM STOC*, pages 197–206. ACM Press, May 2008.


Nadia Heninger, Zakir Durumeric, Eric Wustrow, and J. Alex Halderman.
Mining your ps and qs: Detection of widespread weak keys in network devices.
In Tadayoshi Kohno, editor, *USENIX Security 2012*, pages 205–220. USENIX Association, August 2012.


Marcella Hastings, Joshua Fried, and Nadia Heninger.
Weak keys remain widespread in network devices.

In *Internet Measurement Conference*, pages 49–63. ACM, 2016.


Marc Joye, Pascal Paillier, and Serge Vaudenay.
Efficient generation of prime numbers.
In Çetin Kaya Koç and Christof Paar, editors, *CHES 2000*, volume 1965 of *LNCS*, pages 340–354. Springer, Heidelberg, August 2000.


JD Kilgallin.
Factoring RSA keys in the IoT era, 2019.
https://info.keyfactor.com/factoring-rsa-keys-in-the-iot-era#introduction.


Arjen K. Lenstra, James P. Hughes, Maxime Augier, Joppe W. Bos, Thorsten Kleinjung, and Christophe Wachter.
Public keys.
In Reihaneh Safavi-Naini and Ran Canetti, editors, *CRYPTO 2012*, volume 7417 of *LNCS*, pages 626–642. Springer, Heidelberg, August 2012.


Adeline Langlois, Damien Stehlé, and Ron Steinfeld.
GGHLite: More efficient multilinear maps from ideal lattices.
In Phong Q. Nguyen and Elisabeth Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 239–256. Springer, Heidelberg, May 2014.

Xu Liu and Mingqiang Wang.
QCCA-secure generic key encapsulation mechanism with tighter security in the quantum random oracle model.
In Garay [Gar21], pages 3–26.

Ueli M. Maurer.
Fast generation of prime numbers and secure public-key cryptographic parameters.
Journal of Cryptology, 8(3):123–155, September 1995.

Ilya Mironov.
Rényi differential privacy.
In Boris Köpf and Steve Chong, editors, *CSF 2017Computer Security Foundations Symposium*, pages 263–275. IEEE Computer Society Press, 2017.

Tetsuzo Morimoto.
Markov processes and the h-theorem.
Journal of the Physical Society of Japan, 18(3):328–331, 1963.

Daniele Micciancio and Chris Peikert.
Trapdoors for lattices: Simpler, tighter, faster, smaller.

In David Pointcheval and Thomas Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 700–718. Springer, Heidelberg, April 2012.


Takahiro Matsuda, Kenta Takahashi, Takao Murakami, and Goichiro Hanaoka.
Improved security evaluation techniques for imperfect randomness from arbitrary distributions.
In Dongdai Lin and Kazue Sako, editors, *PKC 2019, Part I*, volume 11442 of *LNCS*, pages 549–580. Springer, Heidelberg, April 2019.


Michael Naehrig, Erdem Alkim, Joppe Bos, Léo Ducas, Karen Easterbrook, Brian LaMacchia, Patrick Longa, Ilya Mironov, Valeria Nikolaenko, Christopher Peikert, Ananth Raghunathan, and Douglas Stebila.
FrodoKEM.
Technical report, National Institute of Standards and Technology, 2020.
available at `https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions`.


Phong Q. Nguyen and Oded Regev.
Learning a parallelepiped: Cryptanalysis of GGH and NTRU signatures.
In Serge Vaudenay, editor, *EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 271–288. Springer, Heidelberg, May / June 2006.

Matús Nemec, Marek Sýs, Petr Svenda, Dusan Klinec, and Vashek Matyas.
The return of coppersmith's attack: Practical factorization of widely used RSA moduli.
In Bhavani M. Thuraisingham, David Evans, Tal Malkin, and Dongyan Xu, editors, *ACM CCS 2017*, pages 1631–1648. ACM Press, October / November 2017.

Thomas Prest, Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Ricosset, Gregor Seiler, William Whyte, and Zhenfei Zhang.
FALCON.
Technical report, National Institute of Standards and Technology, 2017.
available at `https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions`.

Thomas Prest, Dahmun Goudarzi, Ange Martinelli, and Alain Passelègue.
Unifying leakage models on a Rényi day.
In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part I*, volume 11692 of *LNCS*, pages 683–712. Springer, Heidelberg, August 2019.

Thomas Prest.
Sharper bounds in lattice-based cryptography using the Rényi divergence.

In Tsuyoshi Takagi and Thomas Peyrin, editors, *ASIACRYPT 2017, Part I*, volume 10624 of *LNCS*, pages 347–374. Springer, Heidelberg, December 2017.


Alfréd Rényi.
On measures of entropy and information.
In *Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability, Volume 1: Contributions to the Theory of Statistics*, pages 547–561, Berkeley, Calif., 1961. University of California Press.


John Steinberger.
Improved security bounds for key-alternating ciphers via hellinger distance.
Cryptology ePrint Archive, Report 2012/481, 2012.
https://eprint.iacr.org/2012/481.


Igor Vajda.
$\chi\alpha$-divergence and generalized fisher information.
In *Transactions of the Sixth Prague Conference on Information Theory, Statistical Decision Functions and Random Processes*, page 223. Academia, 1973.


Kenji Yasunaga.
Replacing probability distributions in security games via hellinger distance.
Cryptology ePrint Archive, Report 2021/110, 2021.

https://eprint.iacr.org/2021/110.