Unique Signatures and Verifiable Random Functions from the DH–DDH Separation (Lysyanskaya, CRYPTO 2002): A Structured Summary

1 Roadmap (What is built and why)

The paper has two conceptual steps:

1. Build a *unique* (deterministic) signature scheme in a cyclic group where DDH is efficiently decidable but a Diffie–Hellman-like computation remains hard (*DH–DDH separation*).
2. Use the standard Micali–Rabin–Vadhan (MRV) route

$$\text{unique signatures} \Rightarrow \text{VUF} \Rightarrow \text{VRF}$$

to obtain verifiable randomness (in two variants with different assumptions / security loss).

The technical core is the signature: it is a "path of exponentiations" whose correctness is verified by repeated DDH tests.

2 Notation and background primitives

2.1 Groups with easy DDH

Let $\mathsf{S}(1^k)$ output a cyclic group description $(G, *, q, g)$ where $|G| = q$ is prime and g is a generator. All exponents are taken in $\mathbb{Z}_q$.

Definition 1 (DDH decider (easy DDH))**.** *A* DDH *decider for* (G, q, g) *is a deterministic algorithm* D *such that for all* $X, Y, Z \in G$*,*

$$D(G, q, g, X, Y, Z) = 1 \iff \exists x, y \in \mathbb{Z}_q : \ X = g^x,\ Y = g^y,\ Z = g^{xy}.$$

We assume D *runs in time* $\mathrm{poly}(k)$*.*

Remark 1. *In standard discrete-log groups (e.g., generic prime-order subgroups of* $\mathbb{F}_p^\times$*)* DDH *is believed hard. Here we assume* DDH *is* easy *and instead place hardness on a stronger DH-type problem.*

2.2 Error-correcting code for input randomization

Fix a code $\mathsf{C} : \{0,1\}^{n_0} \to \{0,1\}^n$ with relative Hamming distance $c \in (0, 1]$: for all $M \neq M'$, the codewords $\mathsf{C}(M)$ and $\mathsf{C}(M')$ differ in at least cn positions. The paper assumes $n_0 = \omega(\log k)$ (super-logarithmic), so the message space is super-polynomial in k.

3 Primitives: unique signatures, VUFs, VRFs

3.1 Unique signatures

A signature scheme is $(\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$ with $\mathsf{Gen}(1^k) \to (\mathsf{PK}, \mathsf{SK})$, $\mathsf{Sign}(\mathsf{SK}, M) \to \sigma$, and $\mathsf{Vrfy}(\mathsf{PK}, M, \sigma) \in \{0,1\}$.

Definition 2 (Correctness)**.** *For all M, if $(\mathsf{PK},\mathsf{SK}) \leftarrow \mathsf{Gen}(1^k)$ and $\sigma \leftarrow \mathsf{Sign}(\mathsf{SK}, M)$, then $\mathsf{Vrfy}(\mathsf{PK}, M, \sigma) = 1$ except with probability $\mathrm{negl}(k)$ over Gen and Sign.*

Definition 3 (Uniqueness)**.** *The scheme is* unique *if for all $(\mathsf{PK},\mathsf{SK})$ output by $\mathsf{Gen}(1^k)$ and all messages M, there do not exist two distinct signatures $\sigma \neq \sigma'$ such that $\mathsf{Vrfy}(\mathsf{PK}, M, \sigma) = \mathsf{Vrfy}(\mathsf{PK}, M, \sigma') = 1$, except with probability $\mathrm{negl}(k)$ over Gen.*

Definition 4 (EUF-CMA unforgeability)**.** *Let $\mathsf{Exp}^{\mathsf{EUF\text{-}CMA}}_{\mathsf{Sig}}(A)$ be the experiment where $(\mathsf{PK},\mathsf{SK}) \leftarrow \mathsf{Gen}(1^k)$, $A^{\mathsf{Sign}(\mathsf{SK},\cdot)}(\mathsf{PK})$ makes adaptive signing queries and outputs $(M^\star, \sigma^\star)$. The experiment outputs 1 iff $\mathsf{Vrfy}(\mathsf{PK}, M^\star, \sigma^\star) = 1$ and $M^\star$ was not queried. Define $\mathsf{Adv}^{\mathsf{EUF\text{-}CMA}}_{\mathsf{Sig}}(A) = \Pr[\mathsf{Exp}^{\mathsf{EUF\text{-}CMA}}_{\mathsf{Sig}}(A) = 1]$.*

3.2 VUFs and VRFs (MRV-style)

A *verifiable unpredictable function* (VUF) is a triple $(\mathsf{Gen}, \mathsf{Eval}, \mathsf{Ver})$ where $\mathsf{Eval}(\mathsf{SK}, x) \to (y, \pi)$ and $\mathsf{Ver}(\mathsf{PK}, x, y, \pi) \in \{0,1\}$. Intuitively, even with oracle access to $\mathsf{Eval}(\mathsf{SK},\cdot)$, it should be hard to output a *new* $(x^\star, y^\star, \pi^\star)$ with $\mathsf{Ver}(\mathsf{PK}, x^\star, y^\star, \pi^\star) = 1$.

Definition 5 (VUF unpredictability (fresh-point forging))**.** *Let $\mathsf{Exp}^{\mathsf{VUF}}_{\mathsf{VUF}}(A)$ sample $(\mathsf{PK},\mathsf{SK}) \leftarrow \mathsf{Gen}(1^k)$ and run $A^{\mathsf{Eval}(\mathsf{SK},\cdot)}(\mathsf{PK})$ which outputs $(x^\star, y^\star, \pi^\star)$. The experiment outputs 1 iff $x^\star$ was not queried and $\mathsf{Ver}(\mathsf{PK}, x^\star, y^\star, \pi^\star) = 1$. Define $\mathsf{Adv}^{\mathsf{VUF}}_{\mathsf{VUF}}(A) = \Pr[\mathsf{Exp}^{\mathsf{VUF}}_{\mathsf{VUF}}(A) = 1]$.*

A *verifiable random function* (VRF) additionally requires *pseudorandomness* at fresh points: after adaptive oracle access to $\mathsf{Eval}(\mathsf{SK},\cdot)$, the value $y(x^\star)$ at a fresh $x^\star$ should be indistinguishable from uniform (over the output range), even given PK and all query transcripts.

4 Hardness assumption used by the construction

4.1 The Many-DH assumption

The paper's core computational assumption generalizes CDH.

Definition 6 (ManyDH_ℓ)**.** *Sample $y_1, \ldots, y_\ell \xleftarrow{\$} \mathbb{Z}_q$. Given the collection*

$$\left\{ g^{\prod_{j \in J} y_j} \;:\; \emptyset \neq J \subsetneq [\ell] \right\},$$

the goal is to output $g^{\prod_{i=1}^{\ell} y_i}$. An algorithm B's advantage is

$$\mathsf{Adv}^{\mathsf{ManyDH}_\ell}_{G}(B) = \Pr\left[B\left(g, \{ g^{\prod_{j \in J} y_j} \}_{\emptyset \neq J \subsetneq [\ell]} \right) = g^{\prod_{i=1}^{\ell} y_i} \right].$$

Definition 7 (ManyDHhardness (parameter regime))**.** *We assume that for $\ell = \Theta(\log k)$ and $(G, q, g) \leftarrow \mathsf{S}(1^k)$, every* PPT *algorithm has $\mathsf{Adv}^{\mathsf{ManyDH}_\ell}_{G}(\cdot) \leq \mathrm{negl}(k)$.*

4.2 A stronger "very hard" variant (used for the simplest VRF)

The paper also discusses a stronger quantitative assumption (informally, that ManyDH remains hard even against sub-exponential adversaries and/or with parameters chosen to amplify security). We denote this stronger assumption schematically by VMManyDH and keep statements explicit about the loss.

5 Construction 1: Unique signatures from DH–DDH separation

5.1 Key generation

Fix n (code length). Sample secret exponents

$$a_{i,0}, a_{i,1} \xleftarrow{\$} \mathbb{Z}_q \quad \text{for } i = 1, \ldots, n$$

and publish

$$A_{i,b} := g^{a_{i,b}} \in G \quad \text{for } b \in \{0,1\}.$$

Thus $\mathsf{PK} = \{A_{i,b}\}_{i,b}$ and $\mathsf{SK} = \{a_{i,b}\}_{i,b}$.

5.2 Signing (deterministic path exponentiation)

Given $M \in \{0,1\}^{n_0}$, compute its codeword $m = \mathsf{C}(M) = (m_1, \ldots, m_n) \in \{0,1\}^n$ and define a sequence $s_0, s_1, \ldots, s_n \in G$ by

$$s_0 := g, \qquad s_i := (s_{i-1})^{a_{i,m_i}} \quad (i = 1, \ldots, n).$$

Output the signature $\sigma = (s_1, \ldots, s_n) \in G^n$.

Equivalently, for each i there exists $x_i \in \mathbb{Z}_q$ such that $s_i = g^{x_i}$ and

$$x_i = x_{i-1} \cdot a_{i,m_i} \pmod{q}, \qquad \text{so } s_i = g^{\prod_{j=1}^{i} a_{j,m_j}}.$$

5.3 Verification (a chain of DDH checks)

Given $\sigma = (s_1, \ldots, s_n)$, recompute $m = \mathsf{C}(M)$ and set $s_0 := g$. Accept iff for all $i \in [n]$,

$$D(G, q, g,\ s_{i-1},\ A_{i,m_i},\ s_i) = 1.$$

That is, each triple $(s_{i-1}, A_{i,m_i}, s_i)$ must be a DH triple with base g.

6 Construction 1: Theorems (uniqueness and EUF-CMA security)

6.1 Uniqueness is information-theoretic

Theorem 1 (Uniqueness of valid signatures (unconditional))**.** *Fix an honestly generated public key* $\mathsf{PK} = \{A_{i,b}\}_{i,b}$ *where* $A_{i,b} = g^{a_{i,b}}$ *in a prime-order group. For every message* M *there exists* at most one *signature* $\sigma \in G^n$ *such that* $\mathsf{Vrfy}(\mathsf{PK}, M, \sigma) = 1$.

Proof sketch. Let $m = \mathsf{C}(M)$. Suppose $\sigma = (s_1, \ldots, s_n)$ and $\sigma' = (s'_1, \ldots, s'_n)$ both verify. Verification implies for each i that $(s_{i-1}, A_{i,m_i}, s_i)$ and $(s'_{i-1}, A_{i,m_i}, s'_i)$ are DH triples. Write $s_{i-1} = g^x$ and $A_{i,m_i} = g^a$ where $a = a_{i,m_i}$ is uniquely defined modulo q (prime order). Then the DH condition forces $s_i = g^{xa} = (s_{i-1})^a$, which is a *unique* group element. Thus $s_i = s'_i$ for all i by induction from $s_0 = s'_0 = g$, so $\sigma = \sigma'$. □

6.2 EUF-CMA security from ManyDH

The proof embeds a ManyDH instance into ℓ carefully chosen coordinates of the codeword. The error-correcting code guarantees that a new message differs from any previously signed message on many coordinates, so a random subset of ℓ coordinates catches a fresh "pattern" with noticeable probability.

Theorem 2 (EUF-CMA security of the DH–DDH unique signature)**.** *Fix a code* $\mathsf{C} : \{0,1\}^{n_0} \to \{0,1\}^n$ *of relative distance* c *and let* $\ell = \Theta(\log k)$*. Assume: (i) an efficient* DDH *decider exists for* (G, q, g)*, and (ii)* ManyDH_ℓ *is hard in* G*. Let* A *be any adversary that makes at most* Q *signing queries and runs in time* t*. Then there exists an algorithm* B *running in time* $\mathrm{poly}(t, n, Q)$ *such that*

$$\mathsf{Adv}_G^{\mathsf{ManyDH}_\ell}(B) \;\geq\; \frac{\mathsf{Adv}_{\mathsf{Sig}}^{\mathsf{EUF\text{-}CMA}}(A) \;-\; Q \cdot (1-c)^\ell \;-\; \mathrm{negl}(k)}{\mathrm{poly}(n, Q)}.$$

In particular, if ManyDH_ℓ *is* $\mathrm{negl}(k)$*-hard and* $\ell = \omega(\log(1/(1-c))) = \Theta(\log k)$*, then* $\mathsf{Adv}_{\mathsf{Sig}}^{\mathsf{EUF\text{-}CMA}}(A)$ *is negligible.*

Remark 2 (Where the $(1-c)^\ell$ term comes from)**.** *For any distinct messages* $M \neq M'$*, the codewords agree on at most* $(1-c)n$ *positions. If* $J \subseteq [n]$ *is a uniformly random* ℓ*-subset, then*

$$\Pr\left[\mathsf{C}(M)|_J = \mathsf{C}(M')|_J\right] \leq \frac{\binom{(1-c)n}{\ell}}{\binom{n}{\ell}} \leq (1-c)^\ell.$$

A union bound over Q *prior signing queries yields the displayed collision term.*

7 Construction 2: From unique signatures to VRFs (MRV-style pipeline)

7.1 Unique signatures as a VUF

Define a VUF by taking input x to be the message and outputting (a function of) the unique signature as the value. One simple instantiation is:

$$\mathsf{Eval}(\mathsf{SK}, x):\ \sigma \leftarrow \mathsf{Sign}(\mathsf{SK}, x), \quad y := \mathsf{val}(\sigma), \quad \pi := \sigma,$$

where $\mathsf{val}(\sigma)$ can be the final node label s_n (or its binary encoding). Let $\mathsf{Ver}(\mathsf{PK}, x, y, \pi)$ run $\mathsf{Vrfy}(\mathsf{PK}, x, \pi)$ and additionally check that $y = \mathsf{val}(\pi)$.

Theorem 3 (Unique signatures yield a VUF (tight reduction))**.** *If the signature scheme is EUF-CMA secure and unique, then the derived* $(\mathsf{Gen}, \mathsf{Eval}, \mathsf{Ver})$ *above is a secure VUF. Moreover, any VUF forger immediately yields a signature forger with essentially the same running time and success probability:*

$$\mathsf{Adv}_{\mathsf{VUF}}^{\mathsf{VUF}}(A) \leq \mathsf{Adv}_{\mathsf{Sig}}^{\mathsf{EUF\text{-}CMA}}(A') + \mathrm{negl}(k),$$

for a reduction A' *that forwards VUF oracle queries to the signing oracle and reuses the VUF output as a signature forgery.*

7.2 Turning VUF unpredictability into VRF pseudorandomness

The paper follows MRV's approach: treat the VUF value as a bitstring $v(x) \in \{0,1\}^b$ (e.g., the encoding of s_n), choose a random $r \in \{0,1\}^b$ as part of the public key, and output the hard-core predicate

$$\mathsf{out}(x) := \langle r, v(x) \rangle \bmod 2.$$

The proof π remains the VUF proof (here, the unique signature), and verification checks π and then recomputes $\mathsf{out}(x)$ from π.

Theorem 4 (VUF $\Rightarrow$ 1-bit VRF via Goldreich–Levin (quantified))**.** *Let* $(\mathsf{Gen}, \mathsf{Eval}, \mathsf{Ver})$ *be a VUF with* unique provability *(at most one accepting proof per input). Let* $v(x) \in \{0,1\}^b$ *be the canonical encoding of the VUF value and let* $r \xleftarrow{\$} \{0,1\}^b$ *be public. Consider the derived scheme that outputs* $\mathsf{out}(x) = \langle r, v(x) \rangle \bmod 2$ *together with the same proof* π*. If there exists a distinguisher* D *that, after at most* Q *oracle queries, distinguishes* $\mathsf{out}(x^\star)$ *at a fresh challenge point from uniform with advantage* δ*, then there exists a VUF forger* A *such that*

$$\mathsf{Adv}^{\mathsf{VUF}}_{\mathsf{VUF}}(A) \;\geq\; \frac{\mathrm{poly}(\delta)}{\mathrm{poly}(b)} \;-\; \mathrm{negl}(k),$$

and A *runs in time* $\mathrm{poly}(t_D, b, 1/\delta)$*. Equivalently, if the VUF is secure, then* δ *must be negligible (for appropriate parameters).*

Remark 3 (Interpretation)**.** *The Goldreich–Levin theorem says that if a predicate* $\langle r, v(x) \rangle$ *is distinguishable from random, then (with polynomial overhead) one can recover* $v(x^\star)$ *on a fresh point. Unique provability lets one turn recovery of* $v(x^\star)$ *into a valid new proof/value pair, contradicting VUF unpredictability.*

8 Construction 3: Extending the input domain to $\{0,1\}^*$

The MRV framework provides a standard domain-extension technique: starting from a fixed-length VRF, build a VRF on arbitrary-length inputs by evaluating along a prefix-free encoding and using a tree of derived keys/labels. In this paper, a related tree viewpoint already appears in the signature itself (a depth-n path), and the "more secure" VRF variant (Section 8 of the paper) can be seen as parameterizing the depth to trade proof size against security.

Theorem 5 (Fixed-length $\Rightarrow$ unrestricted-length VRF (standard tree extension))**.** *Assume a secure VRF for inputs in* $\{0,1\}^\ell$*. Then there is a VRF for inputs in* $\{0,1\}^*$ *by interpreting an input string as a path in a binary tree, evaluating the fixed-length VRF on successive node labels (using a prefix-free encoding), and concatenating (or hashing) the outputs; the proof consists of the sequence of node proofs. Security reduces to the fixed-length VRF with polynomial overhead and a standard "guess the challenged node" loss.*

9 Summary tables (what each step guarantees)

Object	Guarantee	Assumptions / notes
Unique signature	Deterministic, at most one valid signature per message	Easy DDH for verification; hardness from ManyDH_ℓ; proof uses code distance c.
VUF (from unique sig)	Hard to output a fresh $(x^\star, y^\star, \pi^\star)$ that verifies	Essentially equivalent to EUF-CMA (unique provability gives tightness).
1-bit VRF (GL step)	Output at fresh $x^\star$ is pseudorandom even given proofs	Uses Goldreich–Levin: distinguishing $\langle r, v(x^\star)\rangle$ lets one recover $v(x^\star)$ and forge the VUF.
Domain extension	Supports $\{0,1\}^*$ with proofs along a path	Standard tree technique; adds linear proof size in encoded input length.

10 End-to-end statements (what you obtain)

Theorem 6 (End-to-end outcome (paper-level summary, quantified))**.** *Assume: (i) groups from* S *admit an efficient* DDH *decider, and (ii)* ManyDH_ℓ *is hard for* $\ell = \Theta(\log k)$*. Then there exists a* unique *and* EUF-CMA secure *signature scheme on a super-polynomial message space. Applying MRV-style transformations yields a verifiable random function that outputs at least one pseudorandom bit together with a publicly verifiable proof of correctness, with security that degrades by the (polynomial) overheads and guessing losses stated in the intermediate theorems.*

Remark 4 (Two VRF variants in the paper)**.** *The paper presents (a) a very simple VRF under a stronger quantitative "very hard"* ManyDH*-type assumption, and (b) a more elaborate construction with improved security under a weaker parameterized assumption. The common backbone is: unique signatures* $\rightarrow$ *VUF* $\rightarrow$ *VRF.*

11 Practical reading notes (what to remember)

- The signature is a *chain* $(s_1, \ldots, s_n)$ where each step is certified by an easy-DDH check.
- Uniqueness is unconditional in prime-order cyclic groups (once the public key fixes the exponents).
- The error-correcting code is a reduction tool: it forces any new message to differ from all queried messages on many positions.
- The DH hardness needed is stronger than CDH (Many-DH) because DDH is assumed easy.
- VRF pseudorandomness is obtained by the MRV/GL "hard-core predicate" lift from VUF unpredictability.