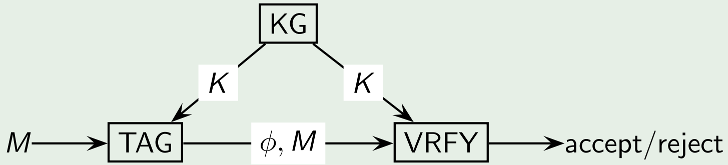
Message Authentication, Revisited

Yevgeniy Dodis, Eike Kiltz, Krzysztof Pietrzak, Daniel Wichs

EUROCRYPT 2012, April 16th, Cambridge UK

Message Authentication Codes

MAC = {KG, TAG, VRFY}



- MACs are fundamental cryptographic primitives.
- Historically constructed from PRFs (with large range)

$$\mathsf{TAG}(K, M) \sim \mathsf{PRF}(K, M) \ , \ \ \mathsf{VRFY}(K, M, \phi) \ \sim \ \mathsf{PRF}(K, M) \stackrel{?}{=} \phi$$

- Domain extension: CBC, HMAC, Hash-then-Encrypt...
- Heuristic: AES, SHA,. . .
- Algebraic: Naor-Reingold PRF, LWE-PRF [BPR'12],... less efficient, but provably secure & ZK-friendly (e.g. for e-cash.)

Algebraic MAC/PRF

- The Naor-Reingold PRF (based on DDH in $\mathbb{G}$)

$$F_{NR}(\underbrace{[h, x_1, \ldots, x_m]}_{\text{key } \in \mathbb{G}\times\mathbb{Z}_p^m}, \underbrace{[b_1, \ldots, b_m]}_{\text{input } \in\{0,1\}^m}) := h^w \text{ where } w = \prod_{i=1}^{m} x_i^{b_1}$$

State of the art algebraic PRFs

either

- Key-size quadratic in security parameter (NR-PRF).

Algebraic MAC/PRF

- The Naor-Reingold PRF (based on DDH in $\mathbb{G}$)

$$F_{NR}(\underbrace{[h, x_1, \ldots, x_m]}_{\text{key } \in \mathbb{G}\times\mathbb{Z}_p^m}, \underbrace{[b_1, \ldots, b_m]}_{\text{input } \in \{0,1\}^m}) := h^w \text{ where } w = \prod_{i=1}^{m} x_i^{b_1}$$

- GGM (algebraic PRG)

State of the art algebraic PRFs

either

- Key-size quadratic in security parameter (NR-PRF).
- Linear number of exponentiations (GGM).

Algebraic MAC/PRF

- The Naor-Reingold PRF (based on DDH in $\mathbb{G}$)

$$F_{NR}(\underbrace{[h, x_1, \ldots, x_m]}_{\text{key } \in \mathbb{G} \times \mathbb{Z}_p^m}, \underbrace{[b_1, \ldots, b_m]}_{\text{input } \in \{0,1\}^m}) := h^w \text{ where } w = \prod_{i=1}^{m} x_i^{b_1}$$

- GGM (algebraic PRG)
- Dodis-Yampolskiy PRF (q-DDHI)

State of the art algebraic PRFs

either

- Key-size quadratic in security parameter (NR-PRF).
- Linear number of exponentiations (GGM).
- Exotic assumptions (q-DDHI).

Algebraic MAC/PRF

- The Naor-Reingold PRF (based on DDH in $\mathbb{G}$)

$$F_{NR}(\underbrace{[h, x_1, \ldots, x_m]}_{\text{key } \in \mathbb{G} \times \mathbb{Z}_p^m}, \underbrace{[b_1, \ldots, b_m]}_{\text{input } \in \{0,1\}^m}) := h^w \text{ where } w = \prod_{i=1}^{m} x_i^{b_1}$$

- GGM (algebraic PRG)
- Dodis-Yampolskiy PRF (q-DDHI)

State of the art algebraic PRFs

either

- Key-size quadratic in security parameter (NR-PRF).
- Linear number of exponentiations (GGM).
- Exotic assumptions (q-DDHI).

Nothing better for MACs known. Previous to this work no MAC construction from DDH with constant # of elements in key and constant # of exponentiations.

MACs vs. PRFs

MACs seem like simpler objects than PRFs

1. Unpredictability vs. indistinguishability.
2. Probabilistic vs. deterministic.

MACs vs. PRFs

MACs seem like simpler objects than PRFs

1. Unpredictability vs. indistinguishability.
   Use search instead decision problems, CDH vs. DDH?
2. Probabilistic vs. deterministic.

MACs vs. PRFs

MACs seem like simpler objects than PRFs

1. Unpredictability vs. indistinguishability.
   Use search instead decision problems, CDH vs. DDH?
2. Probabilistic vs. deterministic.
   Easier from inherently probabilistic assumptions like LPN?

Definitions of MACs

$$\boxed{\text{TAG}(K,.)} \longleftarrow Q_T \longrightarrow \mathcal{A} \longleftarrow Q_V \longrightarrow \boxed{\text{VRFY}(K,.,.)}$$

uf-cmva : unforgeability under chosen message/verification attack

MAC $=$ {KG, TAG, VRFY} is (t, Q_T, Q_V, ϵ)-uf-cmva secure if for all adversaries $\mathcal{A}$ of size t making Q_T/Q_V TAG/VRFY queries: The probability $\mathcal{A}^{\text{TAG}(K,.),\text{VRFY}(K,.,.)}$ makes accepting VRFY query (M, ϕ) and TAG was not queried on M before is $\leq \epsilon$.

Definitions of MACs

$$\boxed{\text{TAG}(K,.)} \longleftarrow Q_T \longrightarrow \mathcal{A} \longleftarrow Q_V \longrightarrow \boxed{\text{VRFY}(K,.,.)}$$

uf-cmva : unforgeability under chosen message/verification attack

MAC $= \{\text{KG}, \text{TAG}, \text{VRFY}\}$ is (t, Q_T, Q_V, ϵ)-uf-cmva secure if for all adversaries $\mathcal{A}$ of size t making Q_T/Q_V TAG/VRFY queries: The probability $\mathcal{A}^{\text{TAG}(K,.),\text{VRFY}(K,.,.)}$ makes accepting VRFY query (M, ϕ) and TAG was not queried on M before is $\leq \epsilon$.

Deterministic MAC with canonical verification.

1. $\text{TAG}(K, M)$ is deterministic.
2. $\text{VRFY}(K, M, \phi) = (\text{TAG}(K, M) \stackrel{?}{=} \phi)$

- No difference between 1 vs. many VRFY queries: $(t, Q_T, 1, \epsilon)$-uf-cmva $\Rightarrow (t, Q_T, Q_V, \epsilon Q_V)$-uf-cmva
- For probabilistic MACs 1 vs. many VRFY queries matters.

Selective security and Indistinguishability

uf-cma : is short for uf-cmva with one verification query

$$(t, Q_T, \epsilon)\text{-uf-cma} \stackrel{\text{def}}{=} (t, Q_T, 1, \epsilon)\text{-uf-cmva}$$

suf-cm(v)a : "selective" unforgeability, defined like uf-cm(v)a but where $\mathcal{A}$ must commit to forged message before making any oracle queries.

ind-cma : MAC is (t, Q_T, ϵ)-ind-cma if tags are indistinguishable

$$\left| \mathbb{P}_K[A^{\mathsf{TAG}(K,.)} = 1] - \mathbb{P}_K[A^{\mathsf{TAG}(K,0)}] \right| \leq \epsilon$$

Our Results (1) Transformations

Efficient generic transformation

1. From one to many verification queries
   uf-cma + ind-cma $\Rightarrow$ uf-cmva.

Our Results (1) Transformations

Efficient generic transformation

1. From one to many verification queries
   uf-cma + ind-cma $\Rightarrow$ uf-cmva.
2. (trivial) Domain extension for uf-cma + ind-cma secure MACs.
3. (trivial) From selective to full security suf-cma $\Rightarrow$ uf-cma for MACs with small range.

Our Results (2) Constructions of algebraic MACs

General templates using

- CCA-secure pubilc-key encryption, Hash-proof systems.
- Key-homomorphic weak PRFs.
- Signatures schemes.

DL based Instantitations

construction	sk $\in$	Tag σ on m	Security	Assumption
$\mathsf{MAC}_{\mathsf{CS}}$	$\mathbb{Z}_p^4 \times \mathbb{G}$	$\mathbb{G}^4$	uf-cmva	DDH
$\mathsf{MAC}_{\mathsf{HPS}}$	$\mathbb{Z}_p^3$	$\mathbb{G}^3$	uf-cmva	DDH
$\mathsf{MAC}_{\mathsf{hwPRF}}$	$\mathbb{Z}_p^2$	$\mathbb{G}^2$	suf-cma	DDH
$\mathsf{MAC}_{\mathsf{WhwPRF}}$	$\mathbb{Z}_p^{\lambda+2}$	$\mathbb{G}^2$	uf-cma	DDH
$\mathsf{MAC}_{\mathsf{BB}}$	$\mathbb{Z}_p^3$	$\mathbb{G}^2$	suf-cma	gap-CDH
$\mathsf{MAC}_{\mathsf{TBB}}$	$\mathbb{Z}_p^5$	$\mathbb{G}^3$	suf-cma	CDH
$\mathsf{MAC}_{\mathsf{Waters}}$	$\mathbb{Z}_p^{\lambda+2}$	$\mathbb{G}^2$	uf-cmva	gap-CDH
$\mathsf{PRF}_{\mathsf{NR}}$	$\mathbb{Z}_p^{\lambda} \times \mathbb{G}$	$\mathbb{G}$	PRF	DDH

Our Results (2) Constructions of algebraic MACs

General templates using

- CCA-secure pubilc-key encryption, Hash-proof systems.
- Key-homomorphic weak PRFs.
- Signatures schemes.

DL based Instantitations

construction	sk $\in$	Tag σ on m	Security	Assumption
$\mathsf{MAC}_{\mathsf{CS}}$	$\mathbb{Z}_p^4 \times \mathbb{G}$	$\mathbb{G}^4$	uf-cmva	DDH
$\mathsf{MAC}_{\mathsf{HPS}}$	$\mathbb{Z}_p^3$	$\mathbb{G}^3$	uf-cmva	DDH
$\mathsf{MAC}_{\mathsf{hwPRF}}$	$\mathbb{Z}_p^2$	$\mathbb{G}^2$	suf-cma	DDH
$\mathsf{MAC}_{\mathsf{WhwPRF}}$	$\mathbb{Z}_p^{\lambda+2}$	$\mathbb{G}^2$	uf-cma	DDH
$\mathsf{MAC}_{\mathsf{BB}}$	$\mathbb{Z}_p^3$	$\mathbb{G}^2$	suf-cma	gap-CDH
$\mathsf{MAC}_{\mathsf{TBB}}$	$\mathbb{Z}_p^5$	$\mathbb{G}^3$	suf-cma	CDH
$\mathsf{MAC}_{\mathsf{Waters}}$	$\mathbb{Z}_p^{\lambda+2}$	$\mathbb{G}^2$	uf-cmva	gap-CDH
$\mathsf{PRF}_{\mathsf{NR}}$	$\mathbb{Z}_p^{\lambda} \times \mathbb{G}$	$\mathbb{G}$	PRF	DDH

Our Results (2) Constructions of algebraic MACs

DL based Instantitations

construction	sk $\in$	Tag σ on m	Security	Assumption
$\mathsf{MAC}_{\mathsf{CS}}$	$\mathbb{Z}_p^4 \times \mathbb{G}$	$\mathbb{G}^4$	uf-cmva	DDH
$\mathsf{MAC}_{\mathsf{HPS}}$	$\mathbb{Z}_p^3$	$\mathbb{G}^3$	uf-cmva	DDH
$\mathsf{MAC}_{\mathsf{hwPRF}}$	$\mathbb{Z}_p^2$	$\mathbb{G}^2$	suf-cma	DDH
$\mathsf{MAC}_{\mathsf{WhwPRF}}$	$\mathbb{Z}_p^{\lambda+2}$	$\mathbb{G}^2$	uf-cma	DDH
$\mathsf{MAC}_{\mathsf{BB}}$	$\mathbb{Z}_p^3$	$\mathbb{G}^2$	suf-cma	gap-CDH
$\mathsf{MAC}_{\mathsf{TBB}}$	$\mathbb{Z}_p^5$	$\mathbb{G}^3$	suf-cma	CDH
$\mathsf{MAC}_{\mathsf{Waters}}$	$\mathbb{Z}_p^{\lambda+2}$	$\mathbb{G}^2$	uf-cmva	gap-CDH
$\mathsf{PRF}_{\mathsf{NR}}$	$\mathbb{Z}_p^{\lambda} \times \mathbb{G}$	$\mathbb{G}$	PRF	DDH

From [KPCJV11]

construction	sk $\in$	Tag σ on m	Security	Assumption
$\mathsf{MAC}_{\mathsf{LPN}}$	$\mathbb{Z}_2^{2\ell}$	$\mathbb{Z}_2^{(\ell+1)\times n}$	suf-cma	LPN
$\mathsf{MAC}_{\mathsf{BilinLPN}}$	$\mathbb{Z}_2^{\ell\times\lambda}$	$\mathbb{Z}_2^{(\ell+1)\times n}$	uf-cma	LPN

Transformations

From one to many verification queries

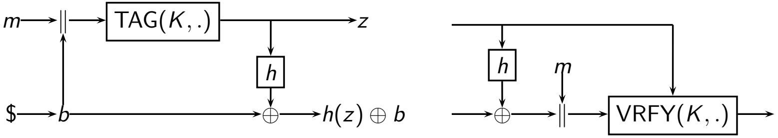


Figure: $\overline{\text{TAG}}$ and $\overline{\text{VRFY}}$ with key (K, h) for message m using randomness b. h is pairwise independent with range $\{0, 1\}^{\mu}$.

From one to many verification queries

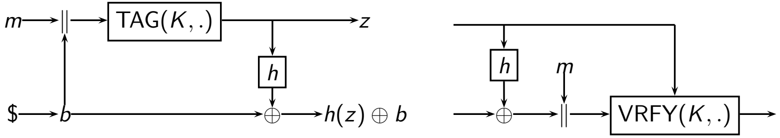


Figure: $\overline{\text{TAG}}$ and $\overline{\text{VRFY}}$ with key (K, h) for message m using randomness b. h is pairwise independent with range $\{0, 1\}^{\mu}$.

Theorem (uf-cma + ind-cma ⇒ uf-cmva)

For any $t, Q_T, Q_V \in \mathbb{N}$, $\epsilon > 0$, *if* MAC *is*

- (t, Q_T, ϵ)-uf-cma *secure*
- (t, Q_T, ϵ)-ind-cma *secure*

then $\overline{\text{MAC}}$ *is* (t, Q_T, Q_V, ϵ')-uf-cmva *secure where*

$$\epsilon' = 2Q_V\epsilon + 2Q_V Q_T/2^{\mu}.$$

From selective to full security & domain extension

Selective to full security

Any MAC with message domain $\{0,1\}^\mu$

$$(t, Q, \varepsilon)\text{-suf-cma} \quad \Rightarrow \quad (t, Q, \varepsilon 2^\mu)\text{-uf-cma}$$

Domain Extension

Pairwise independent $g : \{0,1\}^m \to \{0,1\}^\mu$ to increase domain.

$$\mathsf{TAG}'(K, M) = \mathsf{TAG}(K, g(M))$$

$$\begin{array}{rcl} (t, Q, \varepsilon)\text{-uf-cma} & \& & (t, Q, \varepsilon)\text{-ind-cma} \\ & \Rightarrow & \\ (t, Q, 2\varepsilon + Q/2^\mu)\text{-uf-cma} & \& & (t, Q, \varepsilon)\text{-ind-cma} \end{array}$$

Constructions

Construction from key-homomorphic weak PRF

Key-homomorphic weak PRF

Keyed family of functions $\{f_k \ : \ \mathcal{X} \to \mathcal{Y}\}_{k \in \mathcal{K}}$.

1. wPRF: $f_k(.)$ indistinguishable from random *on random inputs.*
2. key-homomorphic: $f_{a \cdot k_1 + b \cdot k_2}(x) = a \cdot f_{k_1}(x) + b \cdot f_{k_2}(x)$.

kwPRF from DDH

$\{f_k \ : \ \mathbb{G} \to \mathbb{G}\}_{k \in \mathbb{Z}_p}$ defined as $f_k(x) = x^k$.

1. wPRF under DDH.
2. key-homomorphic:
   $f_{a \cdot k_1 + b \cdot k_2}(x) = x^{a \cdot k_1 + b \cdot k_2} = (f_{k_1}(x))^a (f_{k_2}(x))^b$.

Construction from key-homomorphic weak PRF

$\{f_k \;:\; \mathcal{X} \mapsto \mathcal{Y}\}_{k\in\mathcal{K}}$

$$\begin{aligned} \mathsf{KG}:&\quad k_1, k_2 \in_\$ \mathcal{K}. \\ \mathsf{TAG}_{(k_1,k_2)}(m):&\quad x, f_{m\cdot k_1+k_2}(x)\;,\; x \in_\$ \mathcal{X} \\ \mathsf{VRFY}_{(k_1,k_2)}(m,(x,y)):&\quad f_{m\cdot k_1+k_2}(x) \stackrel{?}{=} y. \end{aligned}$$

Theorem

If f is a key-homomorphic weak PRF then MAC *is* suf-cma *and* ind-cma *secure MAC.*

Instantiation with DDH

$$\begin{aligned} \mathsf{KG}:&\quad k_1, k_2 \in_\$ \mathbb{Z}_p \\ \mathsf{TAG}_{(k_1,k_2)}(m):&\quad x, x^{m\cdot k_1+k_2}\;,\; x \in_\$ \mathbb{G} \\ \mathsf{VRFY}_{(k_1,k_2)}(m,(x,y)):&\quad x^{m\cdot k_1+k_2} \stackrel{?}{=} y \end{aligned}$$

Constructions from signatures

- uf-cma secure signature scheme is a uf-cmva secure MAC.

Constructions from signatures

- uf-cma secure signature scheme is a uf-cmva secure MAC.
- Overkill as MACs don't need public verification.

Constructions from signatures

- uf-cma secure signature scheme is a uf-cmva secure MAC.
- Overkill as MACs don't need public verification.
- Take signature scheme and "downgrade" it: loose public verifiability but gain efficiency.

Constructions from signatures

- uf-cma secure signature scheme is a uf-cmva secure MAC.
- Overkill as MACs don't need public verification.
- Take signature scheme and "downgrade" it: loose public verifiability but gain efficiency.

$\mathsf{MAC}_{\mathsf{BB}}$ from downgraded BB (prime-order instead bilinear group)

$$\begin{aligned}
\mathsf{KG}: &\ k = (x, x', y) \in_{\$} \mathbb{Z}_p^3. \\
\mathsf{TAG}_k(m): &\ (U, g^{xy} \cdot U^{xm+x'}) \in \mathbb{G}^2 \text{ where } U \in_{\$} \mathbb{G}. \\
\mathsf{VRFY}_k(m, (U, V)): &\ g^{xy} \cdot U^{xm+x'} \stackrel{?}{=} V.
\end{aligned}$$

Theorem

If gap-CDH holds in $\mathbb{G}$ then $\mathsf{MAC}_{\mathsf{BB}}$ is suf-cma secure.

Constructions from signatures

- uf-cma secure signature scheme is a uf-cmva secure MAC.
- Overkill as MACs don't need public verification.
- Take signature scheme and "downgrade" it: loose public verifiability but gain efficiency.
- Can go from gap-CDH to CDH using twinning Cash et. al EC'08.

$\mathsf{MAC}_{\mathsf{TBB}}$ downgraded BB plus twinning

$$\mathsf{KG}: \quad k = (x_1, x_1', x_2, x_2', y) \in_\$ \mathbb{Z}_p^5.$$

$$\mathsf{TAG}_k(m): \quad U, g^{x_1 y} U^{x_1 m + x_1'}, g^{x_2 y} U^{x_2 m + x_2'} \text{ where } U \in_\$ \mathbb{G}.$$

$$\mathsf{VRFY}_k(m, (U, V)): \quad g^{xy} \cdot U^{xm + x'} \stackrel{?}{=} V.$$

Theorem

If CDH holds in $\mathbb{G}$ then $\mathsf{MAC}_{\mathsf{TBB}}$ *is* suf-cma *secure.*

Construction from LPN [KPCJV11]

MAC_{TBB} downgraded BB plus twinning

$$\text{KG}: \ \mathbf{x} \in_\$ \mathbb{Z}_2^{2\ell}$$

$$\text{TAG}_k(\mathbf{m}): \ (\mathbf{R}, \mathbf{R}^T \cdot \mathbf{x}_{\downarrow \mathbf{m}} + \mathbf{e}) \text{ where } \mathbf{R} \in_\$ \mathbb{Z}_2^{\ell \times n} \text{ and } \mathbf{e} \in \mathbb{Z}_2^n \text{ has low weight.}$$

$$\text{VRFY}_k(\mathbf{m}, (\mathbf{R}, \mathbf{z})): \ |\mathbf{R}^T \cdot \mathbf{x}_{\downarrow \mathbf{m}} - \mathbf{z}| \text{ has low weight.}$$

Theorem (KPCJV11)

If LPN is hard, then MAC_{LPN} *is* suf-cma *and* ind-cma.

Questions?