А. А. Прощеряков

# ТЕМПЕРАТУРНАЯ КОРРЕКЦИЯ ФИЗИЧЕСКИ НЕКЛОНИРУЕМЫХ ФУНКЦИЙ КОЛЬЦЕВЫХ ГЕНЕРАТОРОВ

*В работе приводится методика температурной коррекции работы физически неклонируемых функций кольцевых генераторов на основе введения правил подмены пар кольцевых генераторов.*

В наиболее популярной реализации RO-PUF (Ring Oscillator Phisycal Unclonable Function) для получения идентификатора сравниваются частоты пар кольцевых генераторов ($RO$). Если частота $f_i$ генератора $RO_i$ больше частоты $f_j$ генератора $RO_j$, то в качестве выходного значения RO-PUF принимается '1', иначе '0'. Однако подобная PUF ведет себя нестабильно в условиях изменения температуры кристалла.

Как рассмотрено в [1], с увеличением температуры кристалла, частоты $RO$ понижаются с различными коэффициентами линейной регрессии. В случаях, когда частоты кольцевых генераторов достаточно различны, их температурно-частотные кривые не пересекаются в диапозоне рабочих температур. Но возможен случай, когда частота одного $RO$ при определённой температуре становится выше другой, что вносит ошибку в работу PUF. Рассмотрим методику, позволяющую скорректировать работу RO-PUF в такой ситуации.

Введём понятие интервала близких частот: таким интервалом будем называть диапазон $[f_{low}; f_{high}]$, в котором $f_i$ и $f_j$ настолько близки, что нельзя достоверно сказать, какой из $RO$ в паре быстрей. В соответсвие данному интервалу можно поставить диапазон неразрешённых температур $[k_{low}; k_{high}]$ из [2], где $k_{low}$ соответсвует температуре, при которой $f_i = f_{high}$. Пары $RO$, у которых интервал близких частот находится в диапозоне рабочих температур устройства, будем называть нестабильными.

Для нестабильных пар $RO$, на этапе присваивания устройству идентификатора, определяются *подменяемые* пары $RO$ – такие пары, у которых интервалы близких частот не пересекаются. Они делятся на репрезентативные и комплементарные: у репрезентартивных пар значения подменяются без изменений, у комплементарных – с инверсией.

При получении значений RO-PUF будем использовать следующие правила (здесь и далее $RO_1$ выступает в роли ведущего):
A: Если $f_1 > f_{high}$, генерируется бит '0' в случае если $f_1 > f_2$, и бит '1' если $f_1 < f_2$;
B: Если $f_1 < f_{low}$, генерируется бит '0' в случае если $f_1 < f_2$, и бит '1' если $f_1 > f_2$;
C: Если $f_1 \in [f_{low}; f_{high}]$, используется значение подменяемой пары.

Например, для шести пар $RO$ (см. рис. 1), в классическом RO-PUF, при температуре $K_1$ получаем идентификатор $ID_{K1}$ = "010001", при $K_2$ $-ID_{K2}$ = "101010", при $K$ $-ID_K$ = "0?00?1".

Применяя нашу методику: при $K_1$ по правилу A получаем идентификатор $ID_{K1}$ = "010001", при $K_2$ по правилу A для пары 4 и правилу B для остальных пар, получаем тот же $ID$. При $K$ мы не можем получить достоверный $ID$ из-за попадания $f_1$ в диапозон близких частот в парах 2 и 5. Для пары 2 можем опередить подменяемыми пары 3, 4 или 6 – для примера выберем пару 4, а для пары 5 – подменяемой пару 3. При этом пары 2–4 комплементарные, а 3–5 репрезентативные. Теперь для температуры $K$ получаем идентификатор $ID_K$ = "010001".

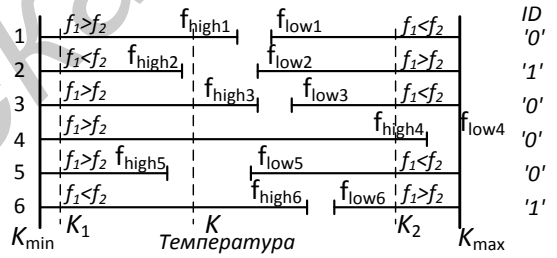


Рис. 1 – Нестабильные пары RO-PUF

Интервалы близких частот, подменяемые пары и их тип могут храниться в виде таблицы и располагаться в энергонезависимой памяти, поскольку получение данной информации не даёт злоумышленнику полного представления о PUF [2].

Так как частоту $RO$ можно определить средствами самой ПЛИС, то рассмотренная методика позволяет реализовать стабильный RO-PUF на ПЛИС общего назначения, не задействуя дополнительной аппаратуры, например температурного датчика.

1. Прощеряков А. А., Иванюк А. А. Кольцевой генератор и его неповторимый коэффициент линейной регрессии // ИТС 2011 : материалы международной научной конференции / редкол. : Л. Ю. Шилин [и др.]. – Минск : БГУИР, 2012. – с.204–205
2. G. Qu and C. Yin, Temperature–Aware Cooperative Ring Oscillator PUF, Workshop on HOST, 2009, pp. 36–42

*Прощеряков Александр Александрович*, аспирант кафедры вычислительных методов и программирования БГУИР, proshcheryakov@gmail.com.

*Научный руководитель: Иванюк Александр Александрович*, заведующий кафедрой вычислительных методов и программирования БГУИР, доктор технических наук, доцент, ivaniuk@bsuir.by.